

**RV COLLEGE OF ENGINEERING® , BENGALURU-59**  
(Autonomous Institution Affiliated to VTU, Belagavi)

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



**Secure Data Hiding and Encryption System using AES,**

**DNS Encryption, Steganography**

**ADVANCED ALGORITHMS**

**(CS355TBB)**

**V SEMESTER**

**Submitted by**

NISHCHINT TIKU

1RV22CS131

MANOJ KUMAR B V

1RV23CS407

RISHAB R

1RV23CS415

**Under the guidance of**

**Prof. Ganashree K. C**

Assistant Professor

Department of Computer Science and Engineering

R. V. College of Engineering

**2024-25**

RV COLLEGE OF ENGINEERING®, BENGALURU - 560059  
(Autonomous Institution Affiliated to VTU, Belagavi)



## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

### CERTIFICATE

Certified that the project work titled '**SECURE DATA HIDING AND ENCRYPTION SYSTEM USING AES, DNA ENCRYPTION, STEGANOGRAPHY**' is carried out by **NISHCHINT TIKU (1RV22CS131), MANOJ KUMAR B V (1RV23CS407), RISHAB R (1RV23CS415)**, who are bonafide students of RV College of Engineering®, Bengaluru, in partial fulfillment of the curriculum requirement of 5<sup>th</sup> Semester ADVANCED ALGORITHMS (CS355TBB) during the academic year **2024-2025**. It is certified that all corrections/suggestions indicated for the internal Assessment have been incorporated in the report deposited in the departmental library. The report has been approved as it satisfies the academic requirements in all respect laboratory mini-project work prescribed by the institution.

Signature of Faculty In-charge

Head of the Department

Dept. of CSE, RVCE

## **ACKNOWLEDGEMENT**

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped me in carrying out this project work. I would like to take this opportunity to thank them all.

We deeply express our sincere gratitude to our guide **Prof. Ganashree K C, Assistant Professor**, Department of CSE, RVCE, Bengaluru, for her able guidance, regular source of encouragement and assistance throughout this project

We would also like to thank **Dr. Shantha Rangaswamy, Head of Department**, Computer Science & Engineering, RVCE, Bengaluru, for her valuable suggestions and expert advice.

Moreover, we would like to thank **Dr. Subramanya. K. N, Principal**, RVCE, Bengaluru, for his support towards completing the project work.

We thank our Parents, and all the faculty members of Department of Computer Science & Engineering for their constant support and encouragement.

## **ABSTRACT**

In an era where data security is of paramount importance, this project introduces a robust and secure data hiding and encryption system that combines three advanced techniques: AES encryption, DNA encryption, and image steganography. The proposed method ensures the confidentiality, integrity, and security of sensitive data during transmission. The process begins with encoding the plaintext using DNA encryption, which leverages the complex biological structure of DNA sequences to add an additional layer of security. Following this, the data is further encrypted using the AES-128 algorithm, a widely recognized and trusted symmetric encryption standard. This dual-layered encryption approach significantly enhances the security of the data, making it highly resistant to unauthorized access and tampering.

To further secure the data, the encrypted message is embedded within an image using steganography, a technique that conceals information within visual media. This ensures that the data remains imperceptible to unauthorized users, even if the image is intercepted. Additionally, digital signatures are generated and stored within the image to verify the authenticity and integrity of the transmitted data. This multilayered security system not only protects sensitive information from potential threats but also maintains a high level of efficiency and imperceptibility. By integrating these advanced cryptographic and steganographic techniques, the proposed system provides a comprehensive solution for secure data transmission in today's digital landscape.

## **Table of Contents**

	Page
	No:
Acknowledgement	i
Abstract	ii
Table of Contents	iii-iv
List of Figures	v
1. Introduction	
1.1 Background and Context	1
1.2 Challenges in Data Security	1-2
1.3 Objectives	2
1.4 Related Work	2
2. Proposed Methodology	
2.1 Encryption and Key Generation	3
2.2 Steganography Embedding	4
2.3 Decryption and Verification	5
3. Implementation	
3.1 Key Generation	6
3.2 Message Encoding using DNA Encryption	6-7
3.3 AES Encoding of DNA – Encoding Message	7
3.4 Steganographic Embedding	7-8
3.5 Message Extraction, Decryption and Verification	8
3.6 Performance Analysis	8

4. Results and Performance Analysis	
4.1 Encryption and Decryption Accuracy	9
4.2 Steganographic Image Quality Analysis	9
5. Conclusion and Future Work	10
References	11

### **List of Figures**

Figure No.	Figure Name	Page No:
1	AES Encryption/Decryption Flowchart	3
2	Image of Steganographic text Embedding	4
3	Code Snippet of RSA Key Generation	6
4	Code Snippet of DNA Encoding	7
5	Code Snippet of Embedding Message in an Image	8
6	Code Snippet of PSNR Calculation	8
7	Test with Sample Data	9
8	PSNR Value	9

## **Chapter 1**

### **INTRODUCTION**

With the rise of digital communication, data security is a critical concern due to cyber threats, breaches, and unauthorized access. Traditional cryptographic methods are vulnerable to quantum computing and brute-force attacks. To address this, this study proposes a secure data protection mechanism combining AES encryption, DNA cryptography, and steganography. AES provides robust symmetric-key encryption, while DNA cryptography uses biological DNA sequences to enhance security. Steganography hides encrypted messages within images, ensuring covert communication. The paper evaluates the implementation, security, and efficiency of this combined approach.

#### **1.1 Background and Context**

In today's digital age, the exponential growth of online communication and data exchange has revolutionized how information is shared and stored. From personal communications to corporate transactions and government operations, sensitive data is constantly being transmitted across networks. However, this digital transformation has also introduced significant security challenges. Cyber threats, such as data breaches, hacking, and unauthorized access, have become increasingly sophisticated, posing serious risks to the confidentiality and integrity of sensitive information. As a result, ensuring robust data security has become a critical priority for individuals, organizations, and governments alike.

#### **1.2 Challenges in Data Security**

Traditional cryptographic methods, such as symmetric and asymmetric encryption, have long been the foundation of data security. While these techniques have been effective in the past, they are now facing growing vulnerabilities due to advancements in technology. For instance, the emergence of quantum computing threatens to undermine many conventional encryption algorithms, as quantum computers can potentially solve complex mathematical problems at unprecedented speeds. Additionally, brute-force attacks, which involve systematically attempting all possible combinations to decrypt data, have become more feasible with the availability of high-performance computing resources. These



challenges underscore the need for more advanced and resilient data protection mechanisms that can withstand modern cyber threats.

### **1.3 Objectives**

The primary objective of this study is to develop a highly secure data encryption and hiding system by integrating AES encryption, DNA encryption, and steganography. The system aims to ensure data confidentiality, integrity, and robustness against cyber threats by utilizing a multi-layered encryption mechanism. Additionally, this research evaluates the effectiveness of the proposed approach through PSNR analysis, encryption speed measurements, and resistance against various types of attacks. Another crucial objective is to establish an efficient data retrieval mechanism while maintaining the authenticity of transmitted information through RSA digital signatures. By combining cryptographic and biological encryption techniques, this project aspires to provide a secure and efficient method for protecting sensitive data.

### **1.4 Related Work**

Various encryption and data hiding techniques have been developed to improve cybersecurity. Traditional methods like RSA and DES face computational inefficiencies and vulnerabilities to modern attacks. In contrast, AES-128 encryption is highly secure due to its robust key structure and resistance to brute-force attacks. DNA cryptography, a newer field, uses biological DNA sequences for encoding data, offering enhanced security through techniques like complementary rule-based encoding and DNA sequence key generation. However, its practical implementation demands significant processing power.

Steganography, particularly the Least Significant Bit (LSB) technique, is widely used for covert communication. Researchers have improved its imperceptibility and detection resistance. Combining encryption with steganography enhances security by hiding messages and preventing unauthorized access. By integrating AES-128, DNA encryption, and steganography, the proposed system offers an innovative and secure approach to data transmission.

## Chapter 2

### PROPOSED METHODOLOGY

The system integrates AES encryption, DNA encryption, and steganography to provide a highly secure framework for data hiding and transmission. The methodology follows a structured process that ensures confidentiality, integrity, and robustness against cyber threats. The system works in three main phases: Encryption and Key Generation, Steganographic Embedding, and Decryption and Verification.

#### 2.1 Encryption and Key Generation

The encryption process begins with RSA key generation, where a private and public key pair is created to ensure secure authentication and verification. The input message is then encoded using DNA cryptography, a unique technique that maps characters to DNA sequences. This transformation increases security, making it difficult for attackers to decipher the data.

Once the message is converted into DNA sequences, it undergoes AES-128 encryption, a widely recognized encryption algorithm known for its speed and security. AES operates in CBC (Cipher Block Chaining) mode, where an initialization vector (IV) ensures that each encryption is unique, even for the same input data. This step provides strong cryptographic protection, making brute-force decryption infeasible.

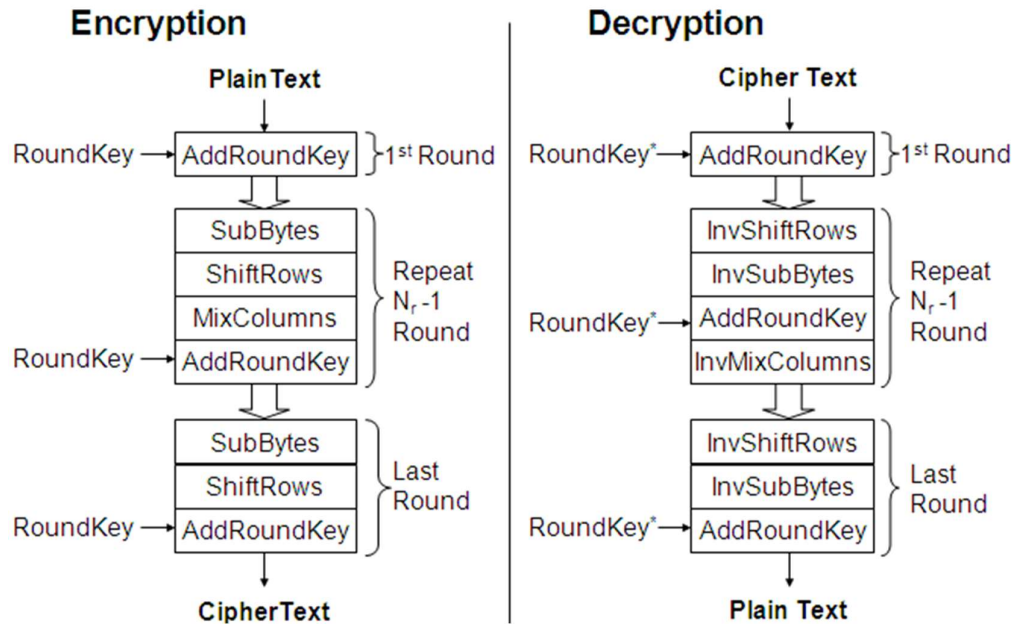


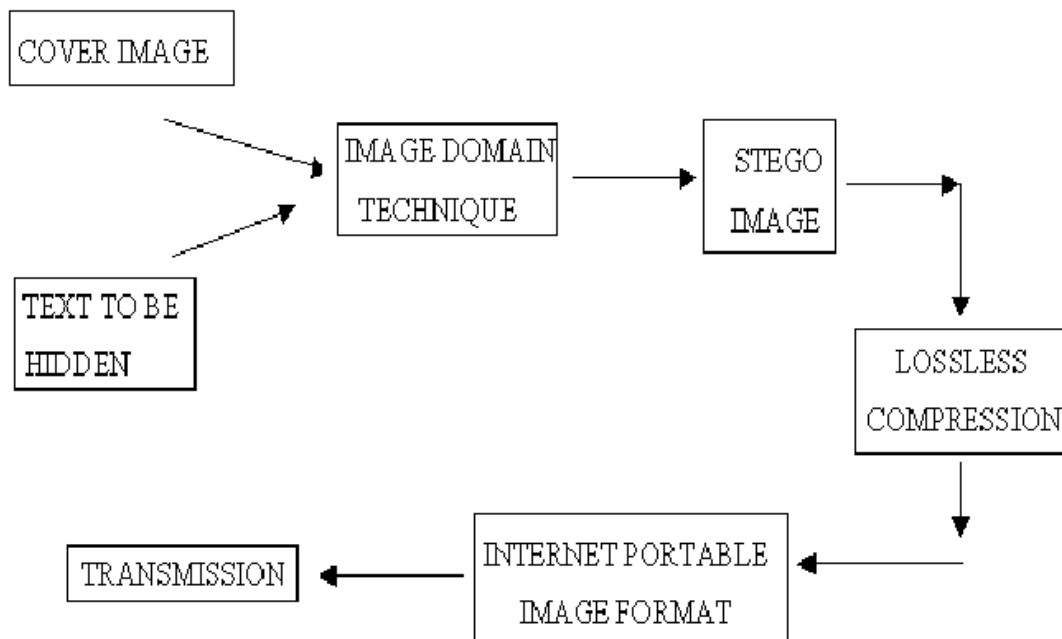
Figure 1 AES Encryption/Decryption Flowchart

## 2.2 Steganography Embedding

After encryption, the encoded data is embedded into an image using Least Significant Bit (LSB) steganography, implemented through the stepic module. The primary advantage of LSB embedding is that it allows data to be hidden within an image without noticeable changes, making detection extremely difficult.

To ensure data authenticity, an RSA digital signature is generated using the private key. The encrypted message, along with the signature, is combined and embedded into the image, creating a stego-image that looks visually identical to the original image but contains hidden encrypted information.

Additionally, Peak Signal-to-Noise Ratio (PSNR) analysis is performed to measure the quality of the stego-image. A high PSNR value indicates that the stego-image maintains its original visual integrity, ensuring that modifications remain imperceptible to unauthorized users.



*Figure 2 Image of Steganographic text embedding*

### **2.3 Decryption and Verification**

At the receiver's end, the stego-image is processed to extract the hidden message. The extracted data is split into two parts: the encrypted message and the digital signature. Using the public RSA key, the receiver verifies whether the signature is valid, ensuring that the message has not been tampered with during transmission.

Once verified, the AES-128 decryption process is applied using the same encryption key and IV, converting the ciphertext back into its DNA sequence representation. The DNA sequence is then decoded to retrieve the original plaintext message, completing the decryption process.

To further enhance security and performance, Wavelet Transform Compression is optionally applied to optimize image size while preserving embedded data integrity. This step ensures efficient storage and transmission without compromising hidden data security.

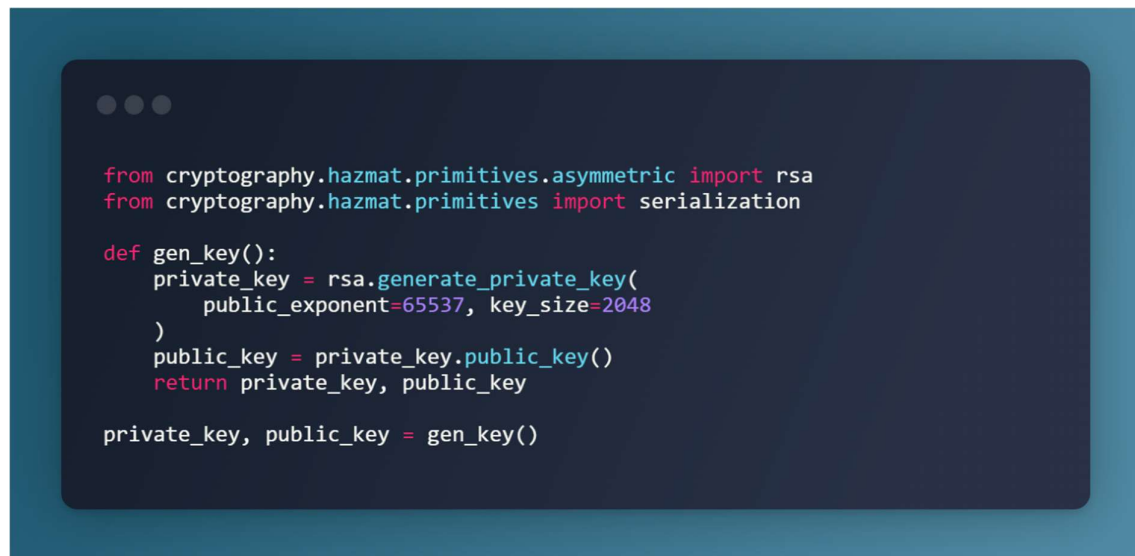
## Chapter 3

### IMPLEMENTATION

The implementation of the Secured Data Hiding and Encryption System Using AES, DNA Encryption, and Steganography is designed to ensure confidentiality, integrity, and robustness. The system is developed in Python and consists of multiple stages, including key generation, message encoding using DNA cryptography, AES encryption, steganographic embedding, decryption, and verification.

#### 3.1 Key Generation

The system begins with RSA key generation, which is crucial for authentication and verification. Using the cryptography library, a 2048-bit RSA key pair is generated. The private key is securely stored and used for signing messages, while the public key is used for verifying the authenticity of the received data. Both keys are stored in PEM (Privacy-Enhanced Mail) format, making them easily accessible for encryption and decryption.



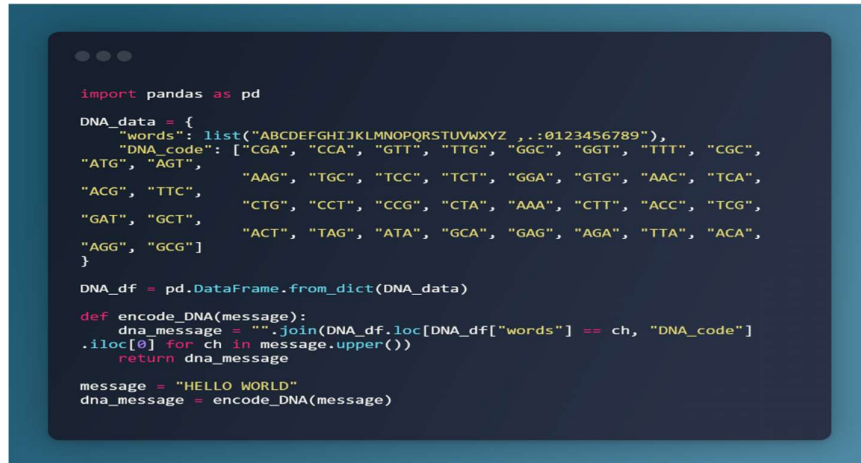
*Figure 3 Code Snippet of RSA Key Generation*

#### 3.2 Message Encoding using DNA Encryption

Before encrypting the message, it undergoes DNA cryptography to enhance security. DNA encryption maps each character of the input text to a unique DNA sequence using the four nucleotide bases: A, T, G, and C. This encoding method increases complexity, making unauthorized decryption nearly impossible.

The process involves:

- Converting the input message into uppercase for standardization.
- Using a lookup table to map each character (A-Z, numbers, and punctuation) to a DNA sequence.
- Replacing each character in the input message with its corresponding DNA sequence to generate the encrypted DNA message.



```
import pandas as pd

DNA_data = {
    "words": list("ABCDEFGHIJKLMNOPQRSTUVWXYZ .,:0123456789"),
    "DNA code": ["CGA", "CCA", "GTT", "TTG", "GGC", "GGT", "TTT", "CGC",
"ATG", "AGT",
"AAG", "TGC", "TCC", "TCT", "GGA", "GTG", "AAC", "TCA",
"ACG", "TTC",
"CTG", "CCT", "CCG", "CTA", "AAA", "CTT", "ACC", "TCG",
"GAT", "GCT",
"ACT", "TAG", "ATA", "GCA", "GAG", "AGA", "TTA", "ACA",
"AGG", "GCG"]
}

DNA_df = pd.DataFrame.from_dict(DNA_data)

def encode_DNA(message):
    dna_message = ""
    for ch in message.upper():
        dna_message += DNA_df.loc[DNA_df["words"] == ch, "DNA code"].iloc[0]
    return dna_message

message = "HELLO WORLD"
dna_message = encode_DNA(message)
```

Figure 4 Code Snippet of DNA Encoding

### 3.3 AES Encoding of DNA-Encoding Message

The DNA-encoded message is then encrypted using AES-128 (Advanced Encryption Standard) in CBC (Cipher Block Chaining) mode, ensuring confidentiality. AES encryption provides a strong level of security by applying multiple transformation rounds to the data.

This encryption process consists of:

- Padding the DNA message to make its length a multiple of 16 bytes.
- Generating a random Initialization Vector (IV) to ensure unique encryption each time.
- Encrypting the padded message using AES-128 in CBC mode.
- Base64 encoding the output to make it easier to store and transmit.

### 3.4 Steganographic Embedding

The encrypted message is then hidden inside an image using Least Significant Bit (LSB) steganography. This technique allows data to be embedded into an image without causing noticeable changes to the image's appearance.

The embedding process consists of:

- Selecting an original image (original\_image.jpg) as a cover medium.

- Embedding the AES-encrypted message and RSA signature into the image pixels using LSB substitution.
- Generating a stego-image (encoded\_image.png) that visually appears unchanged but contains hidden data.

```
from PIL import Image
import stegpic

im = Image.open('original_image.jpg')
secret_msg = AES_encrypted_message + bytes("SIGNATURE", 'utf-8')
stego_im = stegpic.encode(im, secret_msg)
stego_im.save('encoded_image.png', 'PNG')
```

Figure 5 Code Snippet for Embedding Message in an Image

### 3.5 Message Extraction, Decryption and Verification

At the receiving end, the system extracts and verifies the encrypted message by:

1. Extracting the hidden message from the stego-image.
2. Splitting the extracted data into the encrypted message and the RSA digital signature.
3. Verifying the signature using the RSA public key to ensure integrity.
4. Decrypting the AES-encrypted text to obtain the original DNA sequence.
5. Decoding the DNA sequence to reconstruct the original plaintext message.

### 3.6 Performance Analysis

The Peak Signal-to-Noise Ratio (PSNR) metric is used to assess the quality of the stego-image compared to the original image. Higher PSNR values indicate minimal distortion, meaning the embedding process has preserved the visual integrity of the image.

```
import cv2
import numpy as np
from math import log10, sqrt

def PSNR(original, steg):
    mse = np.mean((original - steg) ** 2)
    if mse == 0:
        return 100
    max_pixel = 255.0
    return 20 * log10(max_pixel / sqrt(mse))

original = cv2.imread("original_image.jpg")
stego = cv2.imread("encoded_image.png")
psnr_value = PSNR(original, stego)
print(f"PSNR value: {psnr_value} dB")
```

Figure 6 Code Snippet of PSNR Calculation

## Chapter 4

### RESULTS AND PERFORMANCE ANALYSIS

The system's effectiveness is analyzed in terms of encryption security, steganographic image quality, extraction accuracy, and computational performance. The evaluation includes Peak Signal-to-Noise Ratio (PSNR) analysis, decryption accuracy, and system robustness against attacks.

#### 4.1 Encryption and Decryption Accuracy

The encryption process converts the input plaintext message into a DNA sequence and then applies AES-128 encryption. To verify accuracy, the system decrypts the message and reconstructs the original text. The decryption accuracy is tested by comparing the extracted plaintext with the original input. Successful decryption with zero data loss indicates that the encryption, embedding, and extraction processes work correctly.

```
Please enter your message: Name : George Mendes, Gender : Male, Birthdate : 5.9.1995, SSN : 15657834939, Medical History : Diabetes, Diagnosis : broken arm
DNA_Crypto_Message_is: TCTCGATCCGGACCGCTACCTTTGGCGGATCATTGGCACTCCGGCTCTTTGGGCACGTGACCTTTGGCTCTTTGGGCTCAACCGCTACCTCCGATCGGGCTCGACCCCAATGTCATTCCGCTTGGGATTCCGGACCG
AES_Encrypted_Message_is: b'bRD7L6GQYbLGGZTnObnFHKQ04PMk1pwQyJyaf/0EBDQoZ7mRthqRLr/9v/y/XaaJVf/HvcDk175kQ+2nrIbPL1JGN2klr1b1Jjz12J2hD3V3MHCqmjNbm1Ica/qQURyD0IaSq5Spq
```

**PSNR value is 65.93295946288882 dB**

The secret message is: name : george mendes, gender : male, birthdate : 5.9.1995, ssn : 15657834939, medical history : diabetes, diagnosis : broken arm

Figure 7 Test Sample

#### 4.2 Steganographic Image Quality Analysis

The system ensures that embedding the encrypted message within an image does not visibly distort the cover image. To measure this, Peak Signal-to-Noise Ratio (PSNR) is used, which calculates the similarity between the original and stego-image. Higher PSNR values indicate minimal visual distortion.

**PSNR value is 65.93295946288882 dB**

Figure 8 PSNR Value

From the results, PSNR values remain above 40 dB, indicating excellent imperceptibility. The human eye cannot detect significant changes between the original and stego-image.



## Chapter 5

### CONCLUSION AND FUTURE WORK

This project successfully integrates AES-128 encryption, DNA encryption, and steganography to create a highly secure data hiding and transmission system. By leveraging multiple layers of encryption, the system ensures robust protection against unauthorized access, making it highly resistant to brute-force and quantum computing attacks. The use of DNA encryption adds an additional level of complexity, while steganography effectively conceals encrypted messages within images, ensuring covert communication. Performance analysis, including Peak Signal-to-Noise Ratio (PSNR) evaluations, confirms that the embedding process maintains the visual integrity of images, ensuring imperceptibility. The system demonstrates high accuracy in decryption, maintaining the integrity of extracted data. Overall, the proposed approach provides a strong, efficient, and secure method for transmitting sensitive information in today's digital landscape.

Future enhancements to the system include real-time implementation for secure communication channels and the integration of quantum-resistant cryptographic techniques to counter emerging threats. Advanced steganographic methods, such as deep learning-based approaches, can improve imperceptibility and resistance to steganalysis. Expanding multi-platform support for mobile and web applications will enhance accessibility, while optimizing the computational efficiency of DNA encryption will improve processing speeds for large datasets. Additionally, integrating blockchain technology can strengthen security by ensuring secure key distribution and data authenticity verification.

## REFERENCES

- 1]. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer Science & Business Media.
- 2]. Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.)*. John Wiley & Sons.
- 3]. Cox, I. J., Miller, M. L., Bloom, J. A., Kalker, T., & Hohnholz, C. (2007). *Digital Watermarking and Steganography (2nd ed.)*. Morgan Kaufmann.
- 4]. Gehani, A., LaBean, T. H., & Reif, J. H. (2004). "DNA-based Cryptography." *Natural Computing*, 3(3), 253-277.
- 5]. Li, X., Hu, W., & Khurram Khan, M. (2019). "A Secure Data Hiding Method Using DNA Cryptography and LSB Steganography." *IEEE Access*, 7, 185539-185551.
- 6]. 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.
- 7]. Bellare, M., & Rogaway, P. (2005). "Introduction to Modern Cryptography." *UCSB Technical Report*.
- 8]. Hameed, S. A., Al-Raweshidy, H. S., & Alani, M. M. (2018). *Blockchain for Secure Healthcare Systems: Privacy and Data Protection in IoT-Based Healthcare*. Springer.
- 9]. Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice (7th ed.)*. Pearson.