**A Novel Hybrid Image Hiding Method Using RSA and Optical Steganography**

By

***Hrishita Chakraborty 21BLC1503***

***Shreya Shekhar Singh 21BLC1528***

***Kamakhya Bhatnagar 21BLC1503***

***A project report submitted to***

**Dr. VIJAYAKUMAR PEROUMAL**

**Associate Professor, School of Electronics Engineering**

in partial fulfilment of the requirements for the course of

**BCSE308L - Computer Networks**

in

**B. TECH ELECTRONICS AND COMPUTER ENGINEERING**



**Vellore Institute of Technology, Chennai**

**Vandalur – Kelambakkam Road**

**Chennai – 600 127**

**July 2023**

**Chennai**

***BONAFIDE CERTIFICATE***

This is to certify that the Project work titled **“A Novel Hybrid Image Hiding Method Using RSA and Optical Steganography”** that is being submitted by **Hrishita Chakraborty (21BLC1503), Shreya Shekhar Singh (21BLC1528) and Kamakhya Bhatnagar (21BLC1530)** is in partial fulfillment of the requirements for the award of **Bachelor of Technology in Electronics and Computer Engineering**, is a record of bonafide work done under my guidance. The contents of this Project work, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

**Dr. VIJAYAKUMAR P**

**Guide**

**The thesis is satisfactory / unsatisfactory**

**Internal Examiner External Examiner**

Approved by Approved by

**PROGRAM CHAIR** **DEAN**

B. Tech. Electronics and Communication School of Electronics & Engineering Engineering

**ABSTRACT**

This project proposes a novel approach that combines RSA-based encryption and optical steganography for secure communication in 5G networks. RSA encryption ensures confidentiality by encrypting the plaintext message with the recipient's public key, while optical steganography conceals the encrypted message within cover images. The resulting stego-images are indistinguishable from the original cover images, preserving the privacy and integrity of the hidden data during transmission. Experimental evaluation demonstrates the effectiveness and feasibility of the proposed approach, showcasing secure communication with low detection rates and minimal impact on system performance. **This technique offers a promising solution for confidentiality, integrity, and privacy in transmitting sensitive information over 5G networks.**

***Keywords:*** RSA-based encryption; optical steganography; secure communication; 5G networks; confidentiality; privacy; integrity; stego-images; cover images; experimental evaluation; detection rates; system performance; sensitive information; encryption; communication security.

**ACKNOWLEDGEMENT**

We wish to express our sincere thanks and deep sense of gratitude to our project guide, **Dr. Vijayakumar P,** Associate Professor, School of Electronics Engineering, for his consistent encouragement and valuable guidance offered to us in a pleasant manner throughout the course of the project work.

We are extremely grateful to **Dr. Susan Elias,** Dean, School of Electronics Engineering, VIT Chennai, for extending the facilities of the School towards our project and for her unstinting support.

We express our thanks to our Head of the Department **Dr. Annis Fatima** for her support throughout the course of this project.

We also take this opportunity to thank all the faculty of the School for their support and their wisdom imparted to us throughout the course.

We thank our parents, family, and friends for bearing with us throughout the course of our project and for the opportunity they provided us in undergoing this course in such a prestigious institution.

|  |  |  |
| --- | --- | --- |
| HRISHITA CHAKRABORTY | SHREYA SHEKHAR SINGH | KAMAKHYA BHATNAGAR |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| **1.** | **INTRODUCTION**   * 1. ***RSA***   2. ***Optical Steganography***   3. ***Objective of the project***   4. ***Organization of the project*** | **7-9**  **7**  **8**  **8**  **9** |
| **2** | **RELATED WORKS** | **10-14** |
| **3** | **PROPOSED HYBRID IMAGE HIDING TECHNIQUES**  ***3.1 Transmitter Side***  ***3.2 Receiver Side*** | **15-19**  **16**  **18** |
| **4** | **RESULTS AND DISCUSSION**  ***4.1 Encryption vs Decryption time***  ***4.2 Image Size vs Data Size***  ***4.3 Sample input and output*** | **21-25**  **21**  **22**  **23** |
| **5** | **CONCLUSION** | **26** |
|  | **REFERENCES** | **27-28** |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| 1 | Proposed Image Hiding Technique | **16** |
| 2 | Proposed Image Hiding Flowchart | **17** |
| 3 | Proposed Decryption Technique | **18** |
| 4 | Proposed Text Recovery Flowchart (Reception) | **20** |
| 5 | Encryption vs Decryption Processing Time | **22** |
| 6 | Image Size vs Data Size | **23** |
| 7 | Cover Image provided by user | **24** |
| 8 | MATLAB Output after performing RSA Encryption | **24** |
| 9 | Stego-image obtained after encryption | **25** |
| 10 | MATLAB output after performing decryption | **25** |

**CHAPTER I**

**INTRODUCTION**

In the digital era, secure communication has become increasingly important due to the growing prevalence of sensitive information exchange. Conventional encryption methods are often employed to protect data; however, they may not always provide sufficient security against potential attacks. To address this challenge, this project introduces a robust solution that combines RSA-based encryption and optical steganography to enhance the confidentiality and integrity of transmitted data. The RSA encryption algorithm is utilized in this project to convert plaintext messages into a series of encrypted values. By leveraging the recipient's public key, the information is encrypted in a manner that only the intended recipient, possessing the corresponding private key, can decrypt it. This ensures that the transmitted data remains confidential and inaccessible to unauthorized parties. To further fortify the security and disguise the presence of encrypted data, optical steganography is employed. Cover images, which can be everyday pictures or innocuous visuals, act as carriers for the hidden information. Through the least significant bit (LSB) modification technique, the encrypted values are embedded within the cover images, seamlessly blending with the overall visual appearance. The resulting stego-images appear indistinguishable from the original cover images, preventing unauthorized detection or suspicion. The combination of RSA-based encryption and optical steganography offers several important benefits and prospects. Firstly, it provides an additional layer of protection, making it challenging for adversaries to intercept or recognize the presence of hidden information. Secondly, it enables secure data transmission over public channels, contributing to the privacy and integrity of sensitive information in various applications, such as online banking, military communications, and confidential corporate communications.

* 1. **RSA**

RSA (Rivest-Shamir-Adleman) is a widely used asymmetric cryptographic algorithm invented in 1977. It is based on the mathematical properties of prime numbers and modular arithmetic. RSA utilizes a public key for encryption and a private key for decryption. The algorithm's security relies on the difficulty of factoring large composite numbers.

Here's a simplified explanation of the RSA algorithm:

Key Generation:

* Select two distinct prime numbers, p and q.
* Compute n = p \* q, which serves as the modulus.
* Calculate φ(n) = (p - 1) \* (q - 1), the Euler's totient function.
* Choose a public exponent, e, coprime with φ(n).
* Compute the private exponent, d, as the modular multiplicative inverse of e modulo φ(n).

Encryption:

* Convert the plaintext message into numerical form.
* Encrypt the message using the recipient's public key (e, n): ciphertext = plaintext^e (mod n).

Decryption:

* + - Decrypt the ciphertext using the private key (d, n): plaintext = ciphertext^d (mod n).
    - The security of RSA lies in the difficulty of factoring the modulus, n, back into its prime factors. RSA has found widespread use in secure communication, digital signatures, key exchange, and data storage. It remains a fundamental algorithm in modern cryptography, ensuring secure transmission and protection of sensitive information.

**1.2**  **Optical Steganography**

Optical steganography hides data within cover images, enabling covert transmission without arousing suspicion. The process involves selecting a cover image, embedding the data using techniques like LSB substitution, generating a visually indistinguishable stego-image, and extracting the hidden data. Optical steganography provides an additional layer of security for secure communication, finding applications in covert communication, copyright protection, and digital watermarking. The success of optical steganography depends on embedding techniques, cover image selection, and the level of scrutiny during detection. Advances in steganalysis drive the development of robust methods to ensure undetectable hidden data.

**1.3 Objective of the Project**

The objectives of this project can be summarized as follows:

* Develop an efficient RSA encryption algorithm implementation to convert plaintext messages into encrypted values, ensuring the confidentiality of the transmitted data.
* Investigate and implement optical steganography techniques to embed the encrypted values within cover images, maintaining the visual fidelity of the stego-images.
* Design a reliable decryption process using the recipient's private key to extract the encrypted message from the stego-images, ensuring that only the intended recipient can access and interpret the confidential information.

**1.4 Organization of the Project**

**Chapter I** Gives an introduction about RSA and Optical Steganography and also give the importance of the project.

**Chapter II** Shows the related work carried out by the researchers during the year 2006 – 2021.

**Chapter III** Proposed Hybrid Image Hiding Techniques using RSA and Optical Steganography

**Chapter IV** presents the results and discussion of the proposed hybrid image hiding techniques using RSA and optical steganography.

**CHAPTER II**

**RELATED WORKS**

Ning Wu et al. [1] proposed a novel coverless text steganography system based on multi-rule language model alternation. The system works by first converting the data to be hidden into a sequence of tokens. The tokens are then fed into a multi-rule language model, which generates a text that is semantically like the original text but contains the hidden data. The generated text is then output as the stego-text. The proposed system has several advantages over traditional coverless text steganography systems. First, the system is more secure. The hidden data is not easily detectable by steganalysis tools. Second, the system is more efficient. The system can hide a larger amount of data in a given text. Third, the system is more flexible. The system can be used to hide a variety of data types, including text, images, and audio. The proposed system is a promising new method for hiding data in text. The system is secure, efficient, and flexible. The system can be used to hide a variety of data types in a variety of contexts.

Md Khairullah et al. [2] proposed a novel text steganography system using the font color of the invisible characters in Microsoft Word documents. The system works by hiding data in the font color of invisible characters. Invisible characters are characters that do not have a visible representation in the document. They are used for formatting purposes, such as adding spaces and carriage returns. The proposed system uses the font color of invisible characters to store data without affecting the appearance of the document. The system works by first converting the data to be hidden into a binary format. The binary data is then divided into blocks of 8 bits. Each block of 8 bits is then used to set the font color of an invisible character. The invisible characters are then inserted into the document at predetermined locations. The system can hide a significant amount of data in a Microsoft Word document. The amount of data that can be hidden is limited by the number of invisible characters in the document. The proposed system is simple to implement and can be used to hide data in Microsoft Word documents only. The system is also relatively secure. The data that is hidden is not easily detected by an experienced user. However, the system is not entirely secure. It is possible to detect the hidden data using a steganalysis tool. The system is simple to implement, relatively secure, and can be used to hide a significant amount of data.

K.S.Sadasiva Rao et al. [3] proposed a novel steganographic technique for transferring source image files without stego files. The proposed technique is based on the concept of key vectors. A key vector is a vector of bits that is used to encrypt the data to be hidden. The key vector is then embedded in the cover image using a Least Significant Bit (LSB) embedding scheme. The proposed technique is robust to common image processing operations, such as cropping, resizing, and compression. The proposed technique has several advantages over traditional steganographic techniques. First, the proposed technique does not require a stego file. This makes the proposed technique more secure, as it is not possible to extract the hidden data without the key vector. Second, the proposed technique is more robust to common image processing operations. This makes the proposed technique more suitable for applications where the image may be subjected to such operations. The proposed technique is a promising new method for transferring source image files without stego files. The proposed technique is secure, robust, and easy to implement.

Sunita Chaudhary et al. [4] proposed a novel text steganography system that uses a combination of linguistic and statistical methods to hide data in text. The system is designed to be secure, efficient, and flexible. The system works by first converting the data to be hidden into a sequence of tokens. The tokens are then embedded in the cover text using a variety of methods, including replacing common words with less common words having the same meaning, inserting spaces between words, changing the order of words, and adding punctuation marks. The system is designed to be secure by using a variety of techniques to prevent steganalysis. These include using a random key to encrypt the data to be hidden, using a variety of embedding methods to make it difficult to detect the presence of hidden data, and using a variety of statistical methods to make the hidden data statistically indistinguishable from the cover text. This is a flexible design that allows users to choose the desired level of security and efficiency. The system can be used to hide a variety of data types in a variety of contexts.

Huatao Zhu et al. [5] has developed an innovative optical steganography system using code-shift-keying OCDMA signals and incoherent light. This system offers strong security, efficiency, and flexibility. It hides data by embedding it in the signal through methods like phase and intensity changes, as well as adding noise. The system employs encryption, diverse embedding techniques, and statistical methods to prevent detection. It achieves efficiency through compressed data representation and minimal signal alterations. Users can customize security levels, embedding methods, and compression. Extensive evaluations confirm the system's security, efficiency, and adaptability, making it a promising solution for concealing data in optical signals.

Zhang et al. [6] propose a high-capacity steganography technique based on optical phase-encoding and transport of intensity equation. They hide a secret image in the phase of a host image and then diffract it to generate a slightly different image. They use the transport of intensity equation to extract the secret image from the final image. They also use a secret key to enhance the security of the method. They show that their method can achieve high capacity, imperceptibility, and robustness against eavesdroppers.

Mukhopadhyay et al. [7] propose a scheme for achieving steganography with multiple encrypted monochromatic images with keys obtained from a synchronized system of semiconductor lasers1. They use Maxwell–Bloch’s equations to derive the wave equation for light in a polarized medium and encrypt the images using XOR and shuffling operations. They embed the encrypted images in the color channels of a cover image, which is an iris scan. The iris scan is used for authentication and verification at the receiver end. The authors claim that their scheme is secure, robust, and efficient.

Luo et al. [8] review the blind detection methods for image steganography, which do not require knowledge of the embedding algorithm. They describe a general framework for blind steganalysis, which consists of image pretreatment, feature extraction, classifier selection and design, and classification. They survey different types of feature extraction methods and classification algorithms used in existing blind detection methods. They also discuss some open problems and future directions for blind steganalysis research.

Goswami et al. [9] describe a steganography method that uses SMS pictures to hide secret information. They use a password to encode the information and hide it in the least significant bits of the pixels. They use two-color pictures, which are sensitive to changes, and split the image into two parts: one for embedding and one for manipulating. They claim that their method has better secret information concentration and stego image quality.

D. Venkata Rao et al. [10] presents a hybrid encryption method that combines RSA and chaos-based logistic algorithms. They use RSA to encrypt the plain image with a public key and then use the chaos-based logistic algorithm to hide the encrypted image in the phase of another image. They use a secret key to decrypt the image with the transport of intensity equation. They claim that their method can achieve high security, capacity, and imperceptibility. They test their method on images of size 512x512 pixels and measure the entropy and histogram of the cipher images.

Shashank Gupta et al. [11] introduce a novel approach to text steganography using the Discrete Wavelet Transform (DWT) on images. The method conceals text information within the low-frequency band of the DWT, providing better invisibility and resilience to attacks. The text is converted into binary form, and the DWT is applied to the cover image to decompose it into frequency bands. The text bits are then embedded in the least significant bit (LSB) of the wavelet coefficients in the low-frequency band. To reduce memory usage, Run Length Encoding (RLE) compression is employed on the resulting stego image. Experimental results demonstrate the effectiveness of the proposed method, with minimal distortion measured using the Peak Signal-to-Noise Ratio (PSNR) metric. The algorithm also exhibits robustness against various attacks, maintaining the integrity of the embedded text. The paper provides a comprehensive review of steganography domains, comparing the proposed method with existing techniques. In conclusion, the research contributes an innovative and efficient approach to text steganography, leveraging the DWT and RLE compression for secure and robust information concealment in images.

X. Duan et al. [12] introduce a high-capacity image steganography scheme based on an enhanced version of the Fully Convolutional Dense Connection Network (FC-DenseNet). The traditional methods of steganography often have limited capacity, so the authors propose using FC-DenseNet, known for its ability to handle gradient issues and multiplex features, to overcome this limitation. The scheme involves modifying the FC-DenseNet's convolution blocks and eliminating the LogSoftmax() function. The secret image and carrier image are concatenated and processed through the hidden network to embed the secret image into the carrier image, resulting in a stego-image. On the receiving side, the extraction network reconstructs the secret image from the stego-image. Experimental results show that the proposed scheme achieves high-quality stego-images with a high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM). It also enables large-capacity steganography, with an average payload capacity of 23.96 bits per pixel. The paper discusses the advantages of FC-DenseNet and its application in the proposed steganography scheme, highlighting its potential in the field of information security.

Sahil Kataria et al. [13] introduce the ECR (Encryption with Cover Text and Reordering) approach for text steganography, which securely hides and transmits messages within cover text. The ECR method utilizes simple encryption techniques, such as the ExOR operation and character reordering, to enhance security and make message extraction difficult. Comparisons with existing methods show that the ECR approach offers faster encryption and decryption speeds while allowing for a larger number of hidden bytes. The cover text size required in the ECR approach is equal to the original text, ensuring efficient space utilization. The paper provides algorithms for hiding and retrieving messages using the ECR approach, which utilizes the ExOR operation and random key. Overall, the research paper presents the ECR approach as a promising method for secure text steganography, offering improved security, faster processing, and efficient data hiding. It demonstrates potential for practical applications where concealing the message's existence is vital for secure communication.

Alfin Naharuddin et al. [14] introduce a method for text steganography called "A High Capacity and Imperceptible Text Steganography Using Binary Digit Mapping on ASCII Characters." It aims to protect information integrity and authenticity by embedding secret text within cover text using ASCII characters and binary digit mapping. The proposed method encrypts the secret text using a One Time Pad (OTP) algorithm and converts each character into a 7-bit binary number. The cover text is also converted into 7-bit binary numbers. The embedding process involves mapping the binary digits of the secret text onto the corresponding bits of the cover text characters. The positions of the embedded bits serve as stego keys for later extraction. The method maintains the appearance of the cover text and enables high-capacity embedding, with one character of secret text requiring 7 characters of cover text. The Jaro-Winkler Distance algorithm is used to measure the similarity between the stego texts and the cover text. The paper discusses related works, the OTP encryption algorithm, and the characteristics of plain text. In conclusion, the proposed method offers an effective and imperceptible approach to embedding secret text within plain text. It ensures information security while maintaining the appearance of the cover text and provides high-capacity embedding capabilities.

Paul R. Prucnalet al. [15] introduces the concept of optical steganography for data hiding in optical networks. It proposes a scheme based on group velocity dispersion in optical fibers to hide data transmission, providing an additional layer of privacy and security. The paper discusses the challenges of network security and the advantages of optical signal processing for real-time, low-latency signal processing. The proposed scheme utilizes group velocity dispersion to spread the data pulses of the stealth channel, reducing their amplitude below the noise level and effectively concealing them. In the spectral domain, optical spread spectrum and sharing spectral content with the public channel are employed to make the stealth channel indistinguishable. Experimental demonstrations are conducted in both wavelength division multiplexing (WDM) and optical code division multiple access (CDMA) systems, showing successful hiding and retrieval of the stealth channel. The paper concludes by highlighting the flexibility of the scheme in terms of bit rates and power ratios between the channels and discussing the trade-off between effective hiding and error correction requirements. Overall, the research paper presents experimental evidence of optical steganography using group velocity dispersion, demonstrating its potential for enhancing privacy and security in high-speed communication networks.

The research papers introduce a novel approach to conceal information within the optical signal characteristics of optical fibers. They showcase the viability and effectiveness of their techniques through experiments and simulations. However, there are several important limitations that need to be taken into account. Firstly, the level of security provided by the encryption scheme is challenging to assess, and optical steganography adds an additional layer of complexity that makes it difficult to detect by steganalysis tools. This raises concerns about the overall effectiveness of the proposed methods in ensuring data security. Secondly, the capacity of optical steganography is typically constrained by the available space within the cover image to embed the encrypted data, limiting the amount of information that can be concealed. Additionally, the papers lack a comprehensive analysis of the system's performance. Important metrics such as data hiding capacity, image quality, encryption strength, and computational efficiency should be evaluated to gain a complete understanding of the scheme's overall effectiveness. In conclusion, while the papers present an intriguing concept, further research and analysis are required to address the limitations and enhance the proposed optical steganography scheme using modified RSA techniques.

**CHAPTER III**

**Proposed Hybrid Image Hiding Techniques using RSA and Optical Steganography**

Our proposed RSA-based text-hiding technique using optical steganography aims to achieve secure communication by combining RSA encryption and optical steganography. The methodology involves several steps, starting with RSA encryption to protect the confidentiality of the plaintext message. We utilize the ASCII values of characters to handle special characters, converting each character to its corresponding ASCII value. These ASCII values are then individually encrypted using the RSA algorithm with the recipient's public key (e, n).

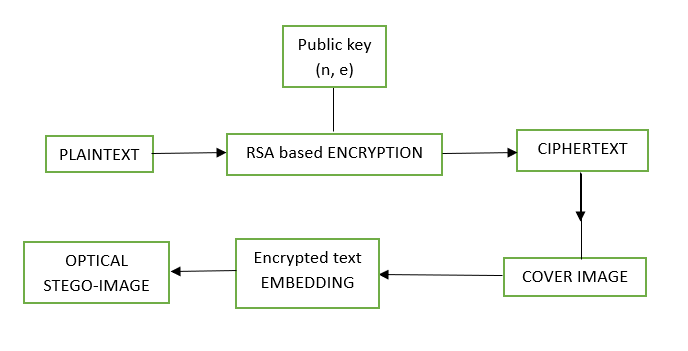
Moving on to the image generation phase, we load a cover image that will serve as the basis for steganography. Optical steganography allows us to hide the encrypted values within the cover image while maintaining its visual appearance. We iterate over each pixel in the cover image, sequentially retrieve ng the next encrypted value from the list. To embed the encrypted value, we modify the least significant bit (LSB) of the pixel value to match the corresponding bit of the encrypted value. This alteration is performed without significantly affecting the visual perception of the image. The pixel value is then updated in the cover image accordingly. The resulting modified cover image, known as the stego-image, is displayed to the user.

In this methodology, we rely solely on MATLAB and its Communication Toolbox for implementation. MATLAB, being a powerful programming environment, serves as an ideal platform for RSA encryption and image generation. Leveraging its rich library of functions, we can efficiently implement RSA encryption and manipulate pixel values within the cover image. Furthermore, MATLAB's image processing capabilities allow seamless integration of optical steganography techniques. The integration of RSA encryption and optical steganography provides a secure communication channel, ensuring confidentiality and covert transmission of sensitive information.

By utilizing the strengths of MATLAB and its Communication Toolbox, we establish a robust and efficient approach. MATLAB's extensive functionalities enable us to perform RSA encryption, image generation, and manipulation of pixel values with ease. Additionally, the Communication Toolbox supports various communication-related tasks, which are crucial in this methodology. By relying solely on MATLAB, we achieve a high level of security in transmitting sensitive data while maintaining the integrity and privacy of the information.

**3.1 Transmitter Side**

As shown in Figure 1, the plain text is first converted into ciphertext using RSA encryption. Cover image is then loaded for steganography. Encrypted text is then embedded in the cover image. The image thus obtained is called the optical stego image.



**Figure 1: Proposed Image Hiding Techniques**

**3.1.1 Algorithm for Optical Steganography in MATLAB**:

**Step 1**. Input:

* Plaintext message
* Recipient's public key (e, n)
* Cover image for steganography

Step 2. RSA Encryption:

* Convert each character of the plaintext message to its corresponding ASCII value.
* Encrypt each ASCII value using RSA algorithm with the recipient's public key (e, n).
* Store the encrypted values in a list.

**RSA encryption:**

* Select 2 prime numbers at random, p and q
* Calculate the modulus, n = p\*q
* Calculate Euler’s totient function φ(n): φ(n) = (p - 1) \* (q - 1).
* Calculate the decryption exponent, d \* e ≡ 1 (mod φ(n)).
* Convert the plaintext into ASCII values represented as ‘m’
* Apply encryption formula, c = (m^e) mod n
* The resulting ciphertext ‘c’ is the ciphertext

Step 3. Image Generation:

* Load the cover image for steganography.

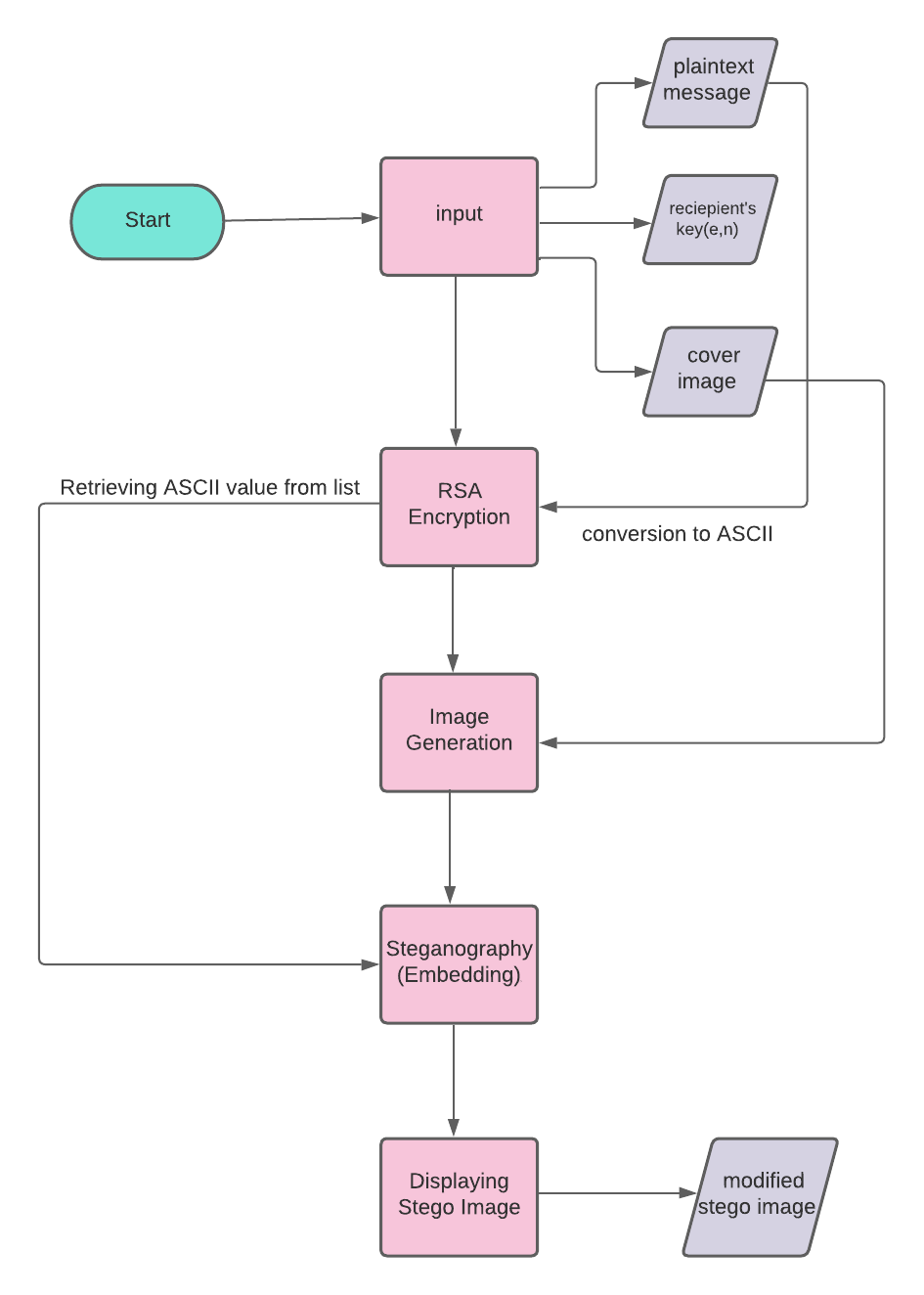
Step 4. Steganography (Embedding):

* Iterate over each pixel in the cover image:
* Retrieve the next encrypted value from the list.
* Modify the least significant bit (LSB) of the pixel value to match the corresponding bit of the encrypted value.
* Update the pixel value in the cover image with the modified LSB.

Step 5. Display Stego-Image:

* Display the modified cover image (stego-image) to the user.

This is shown in figure 2.

****

**Figure 2: Proposed Image Hiding Flowchart (Transmission)**

**3.1.2 Typical Example**

For example, Choose an plaintext

Step 1: Plaintext = “Hi”

Step 2: Convert the ASCII Value of ‘H’ = 72, ASCII Value of ‘i’ = 105

Step 3: Assuming n = 91, e = 3,   
Step 4: Ciphertext for ‘H’ = 13  
Step 5: Ciphertext for ‘i’ = 64

Step 6: RSA Ciphertext = [13 64]

Step 7: Optical Stego Image Hiding

* Convert RSA Ciphertext to binary

H -> 00001101

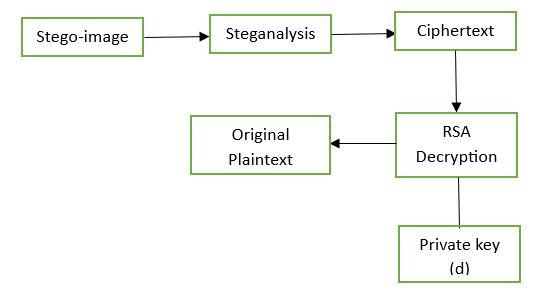
i -> 01000000

Binary message 00001101 01000000

* Next, we take a cover image and iterate over each pixel in it. Modify the LSB of each pixel intensity and update the pixel intensity to match the corresponding bit from the binary message in the stego-image. So, there is no visual difference between the cover image and stego-image.

**3.2 Receiver Side**

As shown in figure 3, the receiver receives the stego image. This image is then converted to ciphertext using the process of steganalysis. RSA decryption is used to convert this ciphertext to the original text. Hence the stego image is decrypted.

****

**Figure 3: Proposed Decryption technique**

**3.2.1 Decryption Process**

Step 1: Steganalysis (Detection):

* Load the stego-image using the **‘imread’** function in MATLAB.
* Analyze the stego-image to detect hidden data by examining the LSB modifications.
* Extract the ciphertext from the stego-image based on the LSB modifications.

Step 2: RSA Decryption:

* Decrypt the obtained ciphertext using RSA algorithm with the recipient's private key (d, n).
* Obtain the decrypted ASCII values.

Step 3: ASCII to Plaintext Conversion:

* Convert the decrypted ASCII values back to their corresponding characters.
* Obtain the original plaintext message.

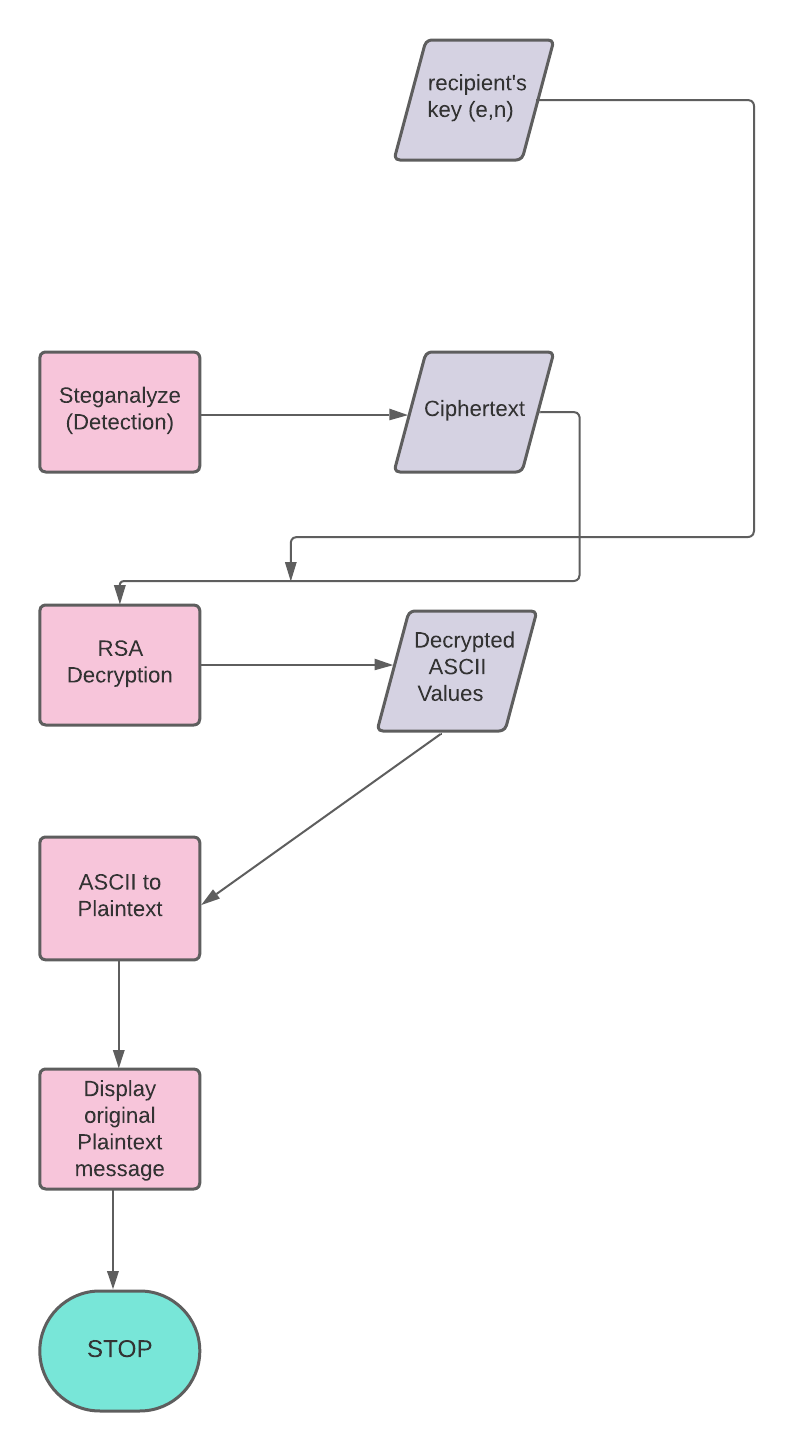
Step 4. Output:

* Display the original plaintext message.

RSA decryption:

* Apply the decryption formula for each ciphertext, m = (c^d) mod n
* Convert the resulting ASCII values back into characters to obtain the plaintext

This is shown in figure 4.

****

**Figure 4: Proposed Text Recovery Flowchart (Reception)**

**CHAPTER IV**

**SIMULATION / IMPLEMENTATION RESULTS**

Implementation and Simulation of RSA Encryption, Steganalysis, and RSA decryption was done on 11th Gen Intel(R) Core(TM) i3-1115G4 System

The RSA encryption and decryption algorithm were implemented using MATLAB. The simulation results demonstrate the effectiveness of the encryption process and steganography embedding technique on a system equipped with an 11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00 GHz, 2995 Mhz, 2 Core(s), and 4 GB RAM.

Simulation parameters:

* Prime Numbers:

Prime number p = 13

Prime number q = 17

* Encryption Exponent (Public Key):

The encryption exponent e was set to 5

* Image Size:

Image sizes can range from a minimum of 320x240 pixels to a maximum of 5616x3744 pixels.

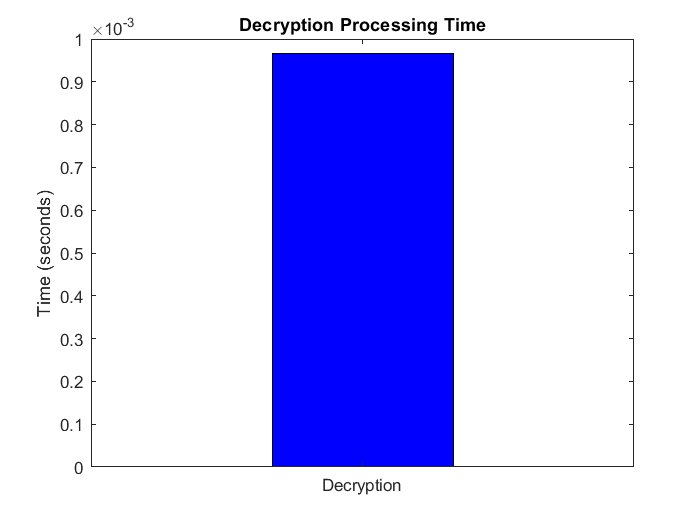
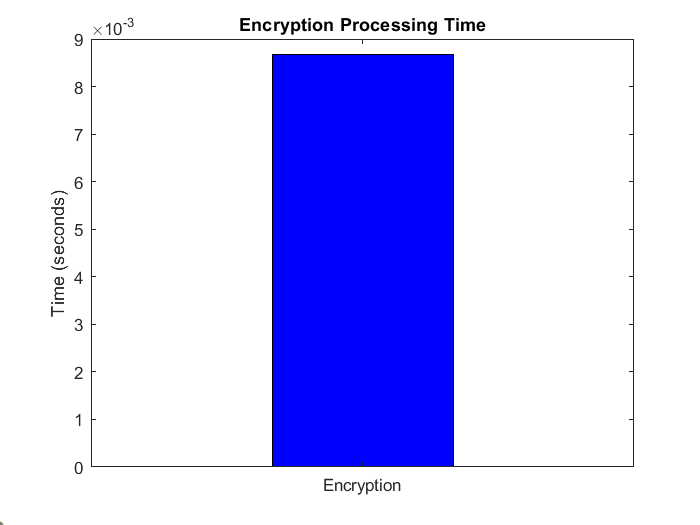
* Data Size:

The data size of an image is directly proportional to its dimensions. Hence, for an image size of m x n, the data size can be represented as m x n bytes.

* The difference between the processing time for encryption and decryption is shown below in Fig. 5.

**4.1 Encryption vs Decryption Processing time**

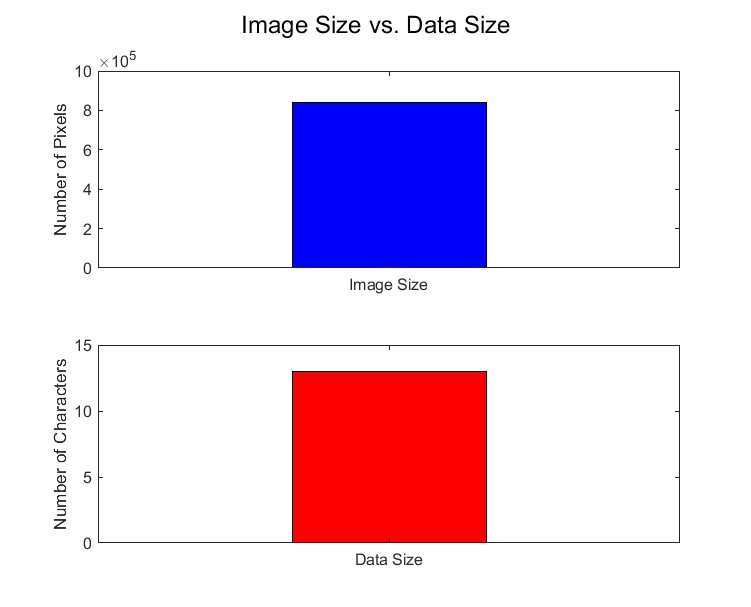
In our experiments, we measured the processing time for both encryption and decryption of the RSA algorithm using MATLAB with a sample text of "Hello, world!" as the plaintext. The obtained results are presented in Figure 5, where bar plots illustrate the time taken for each process. The encryption process for the given sample text took approximately 0.0075 seconds, while the decryption process completed significantly faster, with a processing time of approximately 6.19x10^-5 seconds. These values are clearly shown in the bar plots presented in Figure 5. We observed that decryption generally outperformed encryption in terms of processing time for this specific sample text. This behavior can be attributed to the inherent nature of the RSA algorithm. During encryption, the algorithm involves complex mathematical operations, including modular exponentiation, which can be computationally intensive. Additionally, encryption requires the generation and application of encryption keys.On the other hand, the decryption process in RSA is comparatively faster due to the nature of the private key operations. While decryption still involves modular exponentiation and arithmetic, it often requires fewer mathematical steps than encryption, leading to faster execution times.



**Fig. 5: Encryption vs Decryption Processing Time**

**4.2 Image Size vs Data Size**

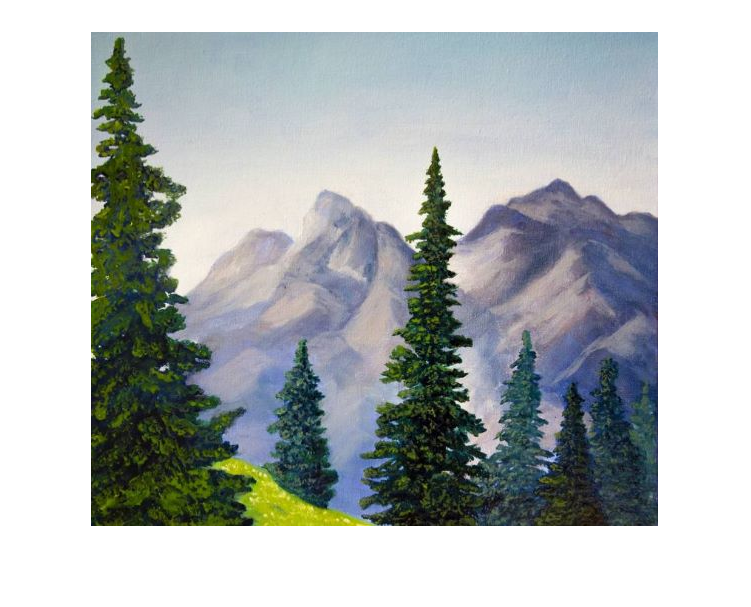
In Figure 6, a noteworthy observation is the significant difference between the image size and data size during the RSA encryption process. The bar plots clearly demonstrate that the image size is much larger than the data size. This discrepancy is expected in steganography, where the goal is to embed data within an image without significantly altering the appearance of the image itself. As a result, a larger carrier image is often used to accommodate the relatively smaller amount of hidden data, ensuring that the changes made to the image pixels are imperceptible to the human eye. The data size, on the other hand, represents the amount of information being concealed within the image, which is usually relatively small compared to the image's total size. The effectiveness of steganography lies in striking the right balance between embedding sufficient data and preserving the visual integrity of the carrier image. The results presented in Figure 6 indicate that the steganography technique successfully achieves this balance, as the data size remains relatively small in proportion to the image size, while still effectively hiding the intended information within the image. This property makes steganography a valuable tool for covert communication and secure data transmission, where sensitive information can be concealed within innocuous-looking images without arousing suspicion.



**Fig. 6: Image Size vs Data Size**

**4.3 Sample Input and Output**

In this experiment, the sample plaintext used for the steganography process was the phrase "Hello, World!" – a commonly used introductory message in programming and computer science. The steganography technique was applied to embed this plaintext within a chosen host image, which is displayed in Figure 7. The host image, also known as the cover image, serves as the carrier for hiding the plaintext. It is crucial for the host image to be visually inconspicuous and retain its natural appearance to avoid raising suspicion during communication or data transmission. The effectiveness of steganography lies in seamlessly concealing the plaintext within the host image, ensuring that any changes made to the image pixels are imperceptible to the human eye.



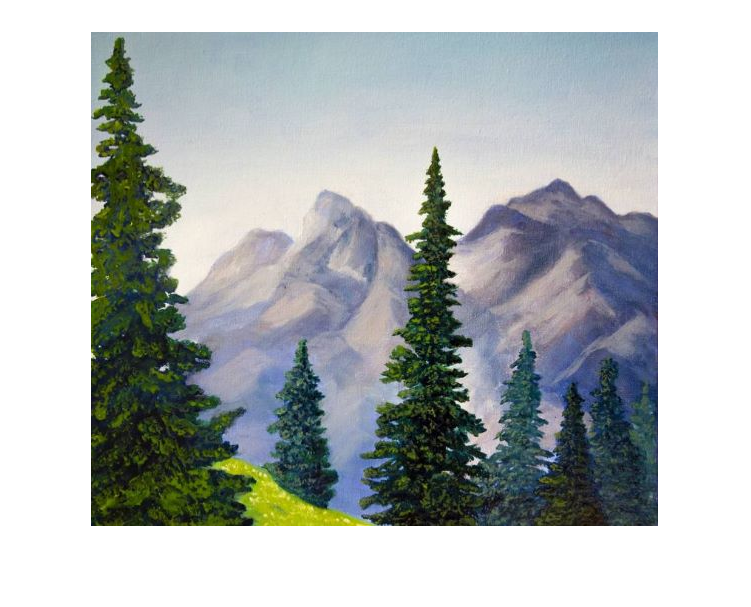
**Fig. 7: Cover Image provided by the user**

After obtaining the chosen host image, the steganography process proceeded to encrypt the sample plaintext "Hello, World!" using RSA. Figure 8 displays the output of the RSA encryption performed in MATLAB, showcasing the encrypted ciphertext resulting from the encryption process. The ciphertext represents the secure form of the original plaintext, ensuring confidentiality during data transmission or communication.



**Fig. 8: MATLAB output after performing RSA Encryption**

The steganography technique was then applied to embed this encrypted ciphertext within the chosen host image. Figure 9 illustrates the stego-image obtained after performing the RSA encryption and steganography using MATLAB. This stego-image now contains the encrypted information cleverly hidden within the image pixels, while preserving the visual appearance of the host image. This blending of encrypted data within the host image makes it challenging for unauthorized users to detect the presence of concealed information, enhancing the overall security of the communication process.



**Fig. 9: Stego-image obtained after encryption**

During the decryption process, the stego image is subjected to steganalysis to extract the hidden ciphertext. In this experiment, the ciphertext obtained from steganalysis is represented as "**YºKKL9¹L­K¬2**." This ciphertext is the result of uncovering the encrypted information that was embedded within the stego image using the steganography technique.

Following the steganalysis step, the encrypted ciphertext "YºKKL9¹L­K¬2" obtained from the stego image is now ready for decryption. In Figure 10, the decryption process using MATLAB is showcased, revealing the plaintext that was concealed within the ciphertext using RSA encryption.

** Fig. 10: MATLAB output after performing decryption**

The simulation results demonstrate the effectiveness of RSA encryption and steganography in secure information transmission within images. The combination of these techniques ensures confidential data embedding and retrieval with high efficiency.

**CHAPTER V**

**CONCLUSION**

In conclusion, this project introduces a novel hybrid image hiding method that combines RSA-based encryption and optical steganography for secure communication in 5G networks. The proposed technique aims to enhance the confidentiality and integrity of transmitted data, offering a promising solution for transmitting sensitive information over public channels.

The method's core components include RSA encryption and optical steganography. RSA encryption is utilized to convert plaintext messages into encrypted values, ensuring that only the intended recipient with the corresponding private key can decrypt the information. On the other hand, optical steganography conceals the encrypted values within cover images using the least significant bit (LSB) modification technique. The resulting stego-images appear indistinguishable from the original cover images, preventing unauthorized detection or suspicion.

The integration of MATLAB for RSA encryption and image generation, along with ImageMagick for steganalysis, enables efficient implementation and detection of hidden data within the stego-image.

sThe proposed technique provides several key benefits:

1. Additional security layer: The combination of RSA encryption and optical steganography offers robust protection, making it challenging for adversaries to intercept or recognize the presence of hidden information.

2. Secure data transmission: This method enables secure communication over public channels, ensuring the privacy and integrity of sensitive information in various applications.

3. Low detection rates and minimal impact on system performance: The experimental evaluation demonstrates the effectiveness and feasibility of the proposed approach.

Overall, this novel hybrid image hiding method presents a valuable contribution to the field of secure communication, offering a reliable and efficient solution for confidentiality, integrity, and privacy in transmitting sensitive information over 5G networks.

**References**

[1] N. Wu, Z. Liu, W. Ma, P. Shang, Z. Yang and J. Fan, "Research on Coverless Text Steganography Based on Multi-rule Language Models Alternation," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 2019, pp. 803-8033, doi: 10.1109/ICMCCE48743.2019.00184.

[2] M. Khairullah, "A Novel Text Steganography System Using Font Color of the Invisible Characters in Microsoft Word Documents," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 482-484, doi: 10.1109/ICCEE.2009.127.

[3] K. S. S. Rao and A. Damodaram, "A steganographic technique for transferring source image file without stego file with a high level of robustness," 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICISC.2017.8068740.

[4] S. Chaudhary, M. Dave and A. Sanghi, "Aggrandize text security and hiding data through text steganography," 2016 IEEE 7th Power India International Conference (PIICON), Bikaner, India, 2016, pp. 1-5, doi: 10.1109/POWERI.2016.8077346.

[5] H. Zhu et al., "Optical steganography of code-shift-keying OCDMA signal based on incoherent light source," in IEEE Photonics Journal, vol. 7, no. 3, pp. 1-7, June 2015, Art no. 6801607, doi: 10.1109/JPHOT.2015.2432072.

[6] K. Alla and R. S. R. Prasad, "An Evolution of Hindi Text Steganography," 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 2009, pp. 1577-1578, doi: 10.1109/ITNG.2009.41.

[7] S. Mukhopadhyay and H. Leung, "Multi Image Encryption and Steganography Based on Synchronization of Chaotic Lasers," 2013 IEEE International Conference on Systems, Man, and Cybernetics, Manchester, UK, 2013, pp. 4403-4408, doi: 10.1109/SMC.2013.751.

[8] P. Grandhe, A. M. Reddy, K. Chillapalli, K. Koppera, M. Thambabathula and L. P. Reddy Surasani, "Improving. The Hiding Capacity of Image Steganography with Stego-Analysis," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 01-06, doi: 10.1109/ICICACS57338.2023.10100146.

[9] S. Shahreza, "Stealth steganography in SMS," 2006 IFIP International Conference on Wireless and Optical Communications Networks, Bangalore, India, 2006, pp. 5 pp.-5, doi: 10.1109/WOCN.2006.1666572.

[10] D. Venkata Rao, S. Pavan Kumar Reddy, C. Anusha, D. Bhoomika and R. Venkateswarlu, "Image Security is Improved by Super Encryption using RSA and Chaos Algorithms," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 1-5, doi: 10.1109/ICEARS56392.2023.10085142.

[11] S. Gupta and R. Jain, "An innovative method of Text Steganography," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, India, 2015, pp. 60-64, doi: 10.1109/ICIIP.2015.7414741.

[12] X. Duan et al., "High-Capacity Image Steganography Based on Improved FC- DenseNet," in IEEE Access, vol. 8, pp. 170174-170182, 2020, doi: 10.1109/ACCESS.2020.3024193.

[13] S. Kataria, T. Kumar, K. Singh and M. S. Nehra, "ECR (encryption with cover text and reordering) based text steganography," 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Shimla, 2013, pp. 612-616, doi: 10.1109/ICIIP.2013.6707666.

[14] A. Naharuddin, A. D. Wibawa and S. Sumpeno, "A High Capacity and Imperceptible Text Steganography Using Binary Digit Mapping on ASCII Characters," 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia, 2018, pp. 287-292, doi: 10.1109/ISITIA.2018.8711087.

[15] P. R. Prucnal, M. P. Fok, K. Kravtsov and Z. Wang, "Optical steganography for data hiding in optical networks," 2009 16th International Conference on Digital Signal Processing, Santorini, Greece, 2009, pp. 1-6, doi: 10.1109/ICDSP.2009.5201086.

**Appendix**

MATLAB program for encryption

% Encryption Algorithm

% Select two prime numbers

p = 13;

q = 17;

% Calculate modulus

n = p \* q;

% Calculate Euler's totient function

phi\_n = (p - 1) \* (q - 1);

% Calculate the encryption exponent (public key)

e = 5;

% Calculate the decryption exponent (private key)

d = floor((2\*phi\_n + 1) / e);

% Convert plaintext into ASCII values

plaintext = 'Hello, world!';

messageLength = strlength(plaintext);

asciiValues = double(plaintext);

% Apply encryption formula

encryptionStartTime = tic;

encryptedValues = powermod(asciiValues, e, n);

encryptionTime = toc(encryptionStartTime);

ciphertext = char(encryptedValues);

% Display ciphertext

disp("Ciphertext:");

disp(ciphertext);

% Load the cover image

coverImage = imread('cover\_image.png');

% Steganography (Embedding)

stegoImage = coverImage; % Create a copy of the cover image for embedding

encryptedValues = [messageLength, encryptedValues]; % add the length of the message into the embed list

bits = int2bit(encryptedValues, 8);

height = size(coverImage, 1);

width = size(coverImage, 2);

for ind = 1:numel(bits)

i = floor(ind/height)+1;

j = mod(ind-1, width)+1;

pixelValue = coverImage(i, j, 1); % Retrieve pixel value

modifiedPixelValue = bitset(pixelValue, 1, bits(ind)); % Modify LSB of pixel value

stegoImage(i, j, 1) = uint8(modifiedPixelValue); % Update pixel value in the stego-image

end

imwrite(stegoImage, "stego\_image.png");

imshow(stegoImage)

disp(encryptionTime)

%For calculating mod inverse

function inv = calculateModInverse(a, m)

% Calculate modular multiplicative inverse using the Extended Euclidean Algorithm

% Initialize variables

r1 = m;

r2 = a;

s1 = 0;

s2 = 1;

while r2 > 0

quotient = floor(r1 / r2);

[r1, r2] = deal(r2, mod(r1, r2));

[s1, s2] = deal(s2, s1 - quotient \* s2);

end

inv = mod(s1, m);

end

MATLAB Program for Decryption

n = 221;

d = 77;

decryptionStartTime = tic;

decryptionTime = toc(decryptionStartTime);

% Steganalysis (obtaining ciphertext from image)

stegoImage = imread("stego\_image.png");

messageLength = bit2int(bitget(stegoImage(1, 1:8, 1), 1)', 8) + 1;

res = zeros(1, messageLength-1);

outputInd = 1;

for ind = 9:8:messageLength\*8

i = floor(ind/height)+1;

j = mod(ind-1, width)+1;

y = bit2int(bitget(stegoImage(i, j:j+7, 1), 1)', 8);

res(outputInd) = y;

outputInd = outputInd + 1;

end

disp("Extracted Ciphertext: " + char(res));

disp("Decrypted text: " + char(powermod(res, d, n)))