ABSTRACT

Information exchange has always been an important aspect of our lives, and with the rapid advancement of information and communication technology, communication and information exchange have become much easier and faster, but data security and privacy have become a major concern for us. Cryptography and Steganography are two popular data hiding practices that also can be combined to enhance data security. Because of recent advancements in steganalysis, one can easily reveal the existence of secreted information in carrier files. So this project aims to introduce a new method of steganography for communication between two private parties. We used a merged technique for data security that employs both cryptography and steganography techniques to enhance information security. In cryptography, we are using the RSA algorithm for the process of key generation and information encryption decryption. And in Steganography we are using Image Steganography for hiding the encrypted data. Image Steganography refers to the technique of hiding the presence of data within an image file, whereas cryptography is related to the act of transforming plain text into incomprehensible text and vice versa. Cryptography guarantees privacy whereas Steganography guarantees secrecy. We have also used base 64 and SHA-256, which is a patented cryptographic hash function. We are hiding the encrypted data in a distinct image file to securely send over the network without any suspicion of the data being hidden. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

Keywords: *Rivest Shamir Adleman (RSA), Key, Cryptography, Steganography, base 64, SHA-256*

Table of Content

List of Figures

CHAPTER 1

1 INTRODUCTION

1.1 Background

The extensive use of the internet for communication has increased the outbreaks on users. Information security is a critical concern for privacy and safety during storage and transmission. As a result, secure communication sessions must be available. Security and authenticity are two vital concerns when transferring data over the Internet. The purpose of security is to protect data from unauthorized users or attackers. Steganography and Cryptography are two vital techniques that are used to provide network security.

This project aims to develop a new approach to hiding a piece of secret information in an image, by taking advantage of the benefits of merging cryptography and steganography. Cryptography is the art and science of securing the data from unwanted access by changing it into a form that is unintelligible to attackers while being stored and transferred. Steganography is the art and science of communicating in a way that hides the presence of communication. Cryptography scrambles a message so it cannot be understood whereas Steganography hides the message so that it cannot be seen. Cryptography guarantees privacy whereas Steganography guarantees secrecy. Steganography and cryptography are both used to ensure data confidentiality. Cryptography and Steganography are often interconnected and share the common goals and services of protecting the confidentiality, integrity, and accessibility of information; which are some of the most important fields in computer security. Steganography and cryptography by themselves are insufficient for information security; both techniques have flaws, so combining them may overcome some of the issues that these techniques may face separately, and using it as this option may be a better idea because we can generate a more reliable and strong approach. Information security will be improved by combining these two approaches along with base-64 encoder and SHA-256 where we convert base-64 strings into the hash key by using SHA-256, which is a patented cryptographic hash function that outputs a value that is 256 bits long.

1.2 MOTIVATION

The main reason and motivation for choosing this project is the security of data transmitted across a global network has turned into a key factor in the network performance measures. So, confidentiality and the integrity of data are needed to prevent eavesdroppers from retrieving and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security. The cryptography problem is that the ciphertext looks hollow, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. The steganography problem is that once the presence of hidden information is revealed or even suspected, the message becomes known. According to the work in this paper, a merged technique for data security has been projected using Cryptography and Steganography techniques to improve the security of the information.

1.3 PROBLEM STATEMENT

For some of the users, the data might be lost during the communication process in the network and for some, the data might be changed by the unauthorized person in the network and there are some other security problems in the network. Our application will give you more security to the data present in the network and there will be able to lessen the loss of data in the network which will be transmitted from the sender to the receiver using the latest technologies. Only the Authorized persons i.e., who are using our application will be there in the Network. The cryptography problem is that it does not hide the fact that secret information is being transferred and the steganography problem is due to recent developments in stego analysis, providing security to personal contents, messages, or digital images using steganography has become tough. The proposed algorithm is to hide the data effectively in an image without any suspicion of the data being hidden in the image. It is to work against the attacks by using a distinct new image that isn’t possible to compare. The project aims to hide the data in an image using steganography and ensure that the quality of concealing data must not be lost. We used a technique for hiding the data in a distinct image file to securely send over the network without any suspicion of the data being hidden. This algorithm though requires a distinct image that we can use as a carrier and hide the data which is well within the limits of the threshold that the image can hide, which will protect the data.

1.4 OBJECTIVES

The objective of this project is:

▪ To develop a system that provides a high level of security by a merged technique for data security using Cryptography and Steganography techniques.

CHAPTER 2

2 LITERATURE REVIEW

The significance of network security is enlarged day by day as the size of data is being transferred across the Internet. There has been a constant rise in the number of data security threats in the recent past and it has become a matter of concern for security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together. Many studies propose methods to combine cryptography with steganography systems in one system. This Project has been executed based on the requirements of security i.e. authentication, confidentiality, and robustness. We present a method based on combining both the strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure, and extremely hard to decode.

The RSA encryption algorithm was developed in the year 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. This algorithm used two randomly generated prime numbers and the strength of the algorithm lies in the computational complexity of factorizing the product of prime numbers. RSA algorithm has been one of the most used algorithms for the asymmetric method of encryption. The patent for RSA was granted to MIT on 20th September 1983. For image steganography, we are using Spatial methods. In a spatial method, the most common method used is the LSB substitution method. The least significant bit (LSB) method is a common, simple approach to embedding information in a cover file. In steganography, the LSB substitution method is used. The research on the topic was done by Subarna Shakya and published the article in a journal of Advanced College of Engineering and Management[1] and International Journal of Engineering Research & Technology (IJERT)[2] and various Universities of India[3]. Results showed that the proposed algorithm has a very good hidden invisibility, good security, and robustness for a lot of hidden attacks.[4]

CHAPTER 3

3 REQUIREMENT ANALYSIS

3.1 FUNCTIONAL REQUIREMENTS

- **Key generation**

  For every new user registration, the system will generate private and public keys and store them in their respective database table
- **Hash of message**

  Hash messages are generated by using SHA.
- **Encryption of messages**

  The text message is encrypted by using the public key of the receiver and stored in the database in the encrypted form
- **Stego image**

  The encrypted message is embedded in the cover image.
- **Decryption of encrypted image**

  The encrypted ciphertext must be retrievable by the receiver from the database and it is decrypted using the private key

3.2 Non-functional requirements

- reliability
- accuracy
- maintainability
- usability

- availability

3.3 Software requirements

Operating system: Windows 7 or higher

Programming software: Python3, HTML,CSS, Flask

3.4 Hardware requirements:

Processor: Intel or Ryzen processor

RAM: 2GB RAM or higher

HDD: almost 1GB of disk space

Keyboard: Standard 110 keys keyboard.

CHAPTER 4

4 METHODOLOGY

4.1 METHODS USED

4.1.1 Base-64

Base 64 is an encoding scheme that converts binary data into text format so that encoded textual data can be easily transported over the network un-corrupted and without any data loss and makes it more reliable to be stored in databases. It allows data to encode in a way that it's easily transferred over clear text or plain text protocol.

Base-64 encoding

Base encoding is the process of converting binary data into a limited character set of 64-bit characters. the characters are A-Z,a-z,0-9,+and /. The Base64 encoded data ends up being longer than the original data, so that, for every 3 bytes of binary data, there are at least 4 bytes of Base64 encoded data. This is due to the fact that we are squeezing the data into a smaller set of characters.

Base-64 decoding

Base64 decoding is the opposite of Base64 encoding. In other words, it is carried out by reversing the steps described in the Encoding. So, Each character in the string is changed to its Base64 decimal value. The decimal values obtained are converted into binary equivalents. The first two bits of the binary numbers are truncated from each of the binary numbers obtained, and the sets of 6 bits are combined, forming one large string of binary digits. The large string of binary digits obtained in the previous step is split into groups of 8 bits. The 8-bit binary numbers are converted into their decimal equivalents. Finally, the decimal values obtained are converted into their ASCII equivalent.

4.1.2 Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. It is a method of storing and transmitting data in a particular form so that only those for whom it is projected can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like confidentiality, privacy, nonrepudiation, key exchange, and authentication.

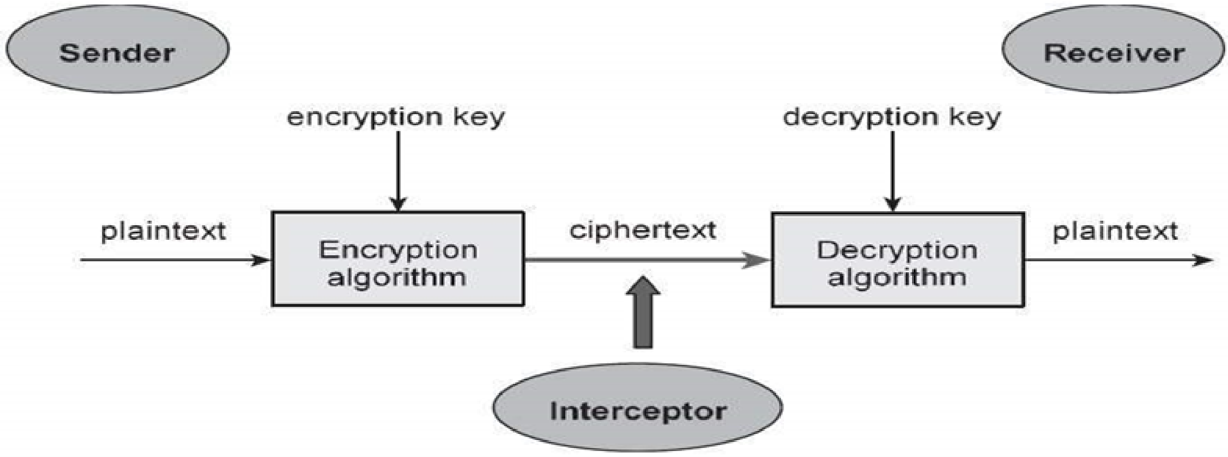


Figure 1:Cryptography

Asymmetric / Public Key Cryptography

We can call this technique asymmetric cryptosystem or public-key cryptosystem, this technique uses two keys that are mathematically associated, use separately for encrypting and decrypting the information. In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. The key used for encryption is stored public therefore it’s called a public key, and the decryption key is stored secret and called a private key. An example of an Asymmetric-Key Algorithm is RSA.

4.1.3 Steganography

Steganography is a method of art and science through which communication is done undetectably. It is accomplished by hiding information in some cover medium, thus hiding the existence of the information. Steganography consists of 3 basic components as shown in Figure. The cover object in the image is a selected medium (audio, video, text, or image) to hide the message to be transmitted. Stego-key is used to hide into a cover object and recover the original message from the cover object. The figure represents the different steganographic components. The cover object in the steganographic process is used to hide the information inside it, i.e. data is entrenched inside the cover object. It may be a text, image, audio, or video. Stego-key is used for embedding and recovering the data from the cover object. Once the data is being entrenched into the cover object, this results in the stego-object, which is sent over the network for communication. This stego-object is then received by the intended recipient and with the help of stego-key, the user can recover the original data content.

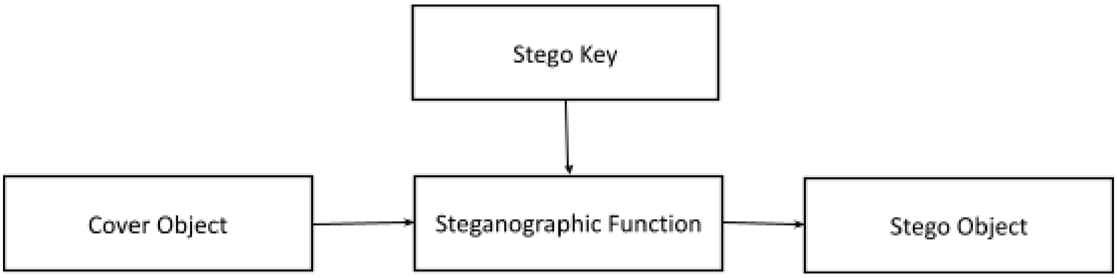


Figure 2: Steganography

Both the techniques have their vulnerabilities so integrating them may overcome several issues that these techniques may be facing individually and using it as this option can be a better idea.

Combination of Cryptography and steganography

It is noted that steganography and cryptography alone is insufficient for the security of information, both techniques have their vulnerabilities so integrating them may overcome several issues that these techniques may be facing individually and using it as this option can be a better idea as we can generate more reliable and strong approach. The combination of these two approaches will improve the security of the information. This combined will fulfill the fundamentals, for example, memory space, security, and strength for important information transmission across an open channel. The secret message that is sent by the sender takes the form of plain text. This plain text is then transformed into the ciphertext using some encrypting algorithm. This ciphertext is then used as an input to the steganography systems i.e. the ciphertext is then used to embed into the cover image resulting in the stego-image. Now, the generated stego-image is transferred to the receiver over a communication link without revealing that the secret information has been transmitted. This is known as a direct approach where cryptography and steganography are combined; one is used for encrypting the secret message and the other, to conceal its existence.

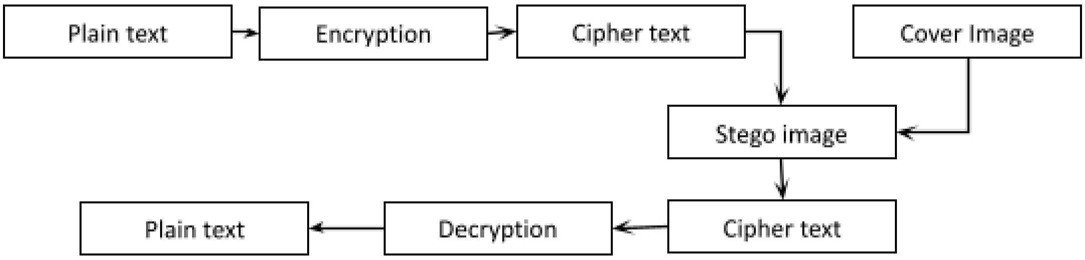


Figure 3: Combination of cryptography and steganography

RSA

The RSA algorithm is the basis of a cryptosystem that is used for specific security services which enable public-key encryption and are widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm, it provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.

The whole concept of RSA lies in the fact that during the multiplication of any prime numbers the size and computational complexity increase linearly but the in case of factorization the computational complexity increases exponentially. So, if the two numbers are not known or the private key is not known to the person decoding the message then the decoding process may require years to complete. Three steps are involved in RSA: Key generation, Encryption, and Decryption. It is a method of safe and secure data transmission without making the third party aware of data transfer. RSA algorithm is based on the integer factorization problem.

RSA security relies on the computational difficulty of factoring large integers. As computing power increases and more efficient factoring algorithms are discovered, the ability to factor in larger and larger numbers also increases. Encryption strength is direct to key size, and doubling key length can deliver an exponential increase in strength, although it does impair performance.

· The plaintext is taken from a specified file and then encrypted using RSA Algorithm. · Encryption and decryption are of the following form for the same plaintext M and ciphertext C.

· C=(M^e)mode

· M=(C^d)mode

· M=((M^e)^d)mode

· M=(M^ed)mode

· Both sender and receiver must know the value of n.

· The sender knows the value of e, and the receiver knows the value of d. · Thus this is a public key encryption algorithm with a public key of PU = {c, n} and a private key of PR= {d, n}.

Image steganography

In this minor project, we are going to use Image steganography. Image Steganography deals with the hiding of text within the image. We have to wrap up the ciphertext using an image. We have chosen to bind text in an image. This kind of embedding a text in an image helps to authenticate the sender, verify whether a valid user is receiving the text or not, and to find whether a third-party attacker is present in the channel of communication or not. Since the image is used as a cover file, we have to make sure that the image must be accountable for the text that is being embedded. Hence a 24-bit image format proved to be the best solution for hiding the text since it holds a large memory space and is convenient to hide a considerable amount of text. Furthermore, the threshold sure of the image must be calculated for the given image size which will be explained in the later parts.

LSB Positioning Method

This method is the simplest method of hiding text within the given image. We utilize the LSB bits of the pixels within the given image. When converting the image to digital format, we usually choose between three different ways of representing colors:

· 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red(R), green(G), blue(b) given by 8 bits (256) each.

· 8-bit color: every pixel can have one in 256 (2^28) colors, chosen from a palette, or a table of colors.

· 8-bit gray-scale: every pixel can have one in 256 (2^28) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images or the LSBs of the 8-bit value for 8-bit images. The most basic of LSBs insertion for 24-bit pictures inserts 3 bits/pixel.

For image steganography, we are using Spatial methods. In the spatial method, the most common method used is the LSB substitution method. The least significant bit (LSB) method is a common, simple approach to embedding information in a cover file. In steganography, the LSB substitution method is used. I.e. since every image has three components (RGB). This pixel information is stored in an encoded format in one byte. The first bits containing this information for every pixel can be modified to store the hidden text. For this, the preliminary condition is that the text to be stored has to be smaller or of equal size to the image used to hide the text. The LSB-based method is a spatial domain method. But this is vulnerable to cropping and noise. In this method, the MSB (most significant bits) of the message image to be hidden are stored in the LSB (least significant bits) of the image used as the cover image.

4.1.4 SHA-256

The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

4.2 SYSTEM DESIGN AND ARCHITECTURE

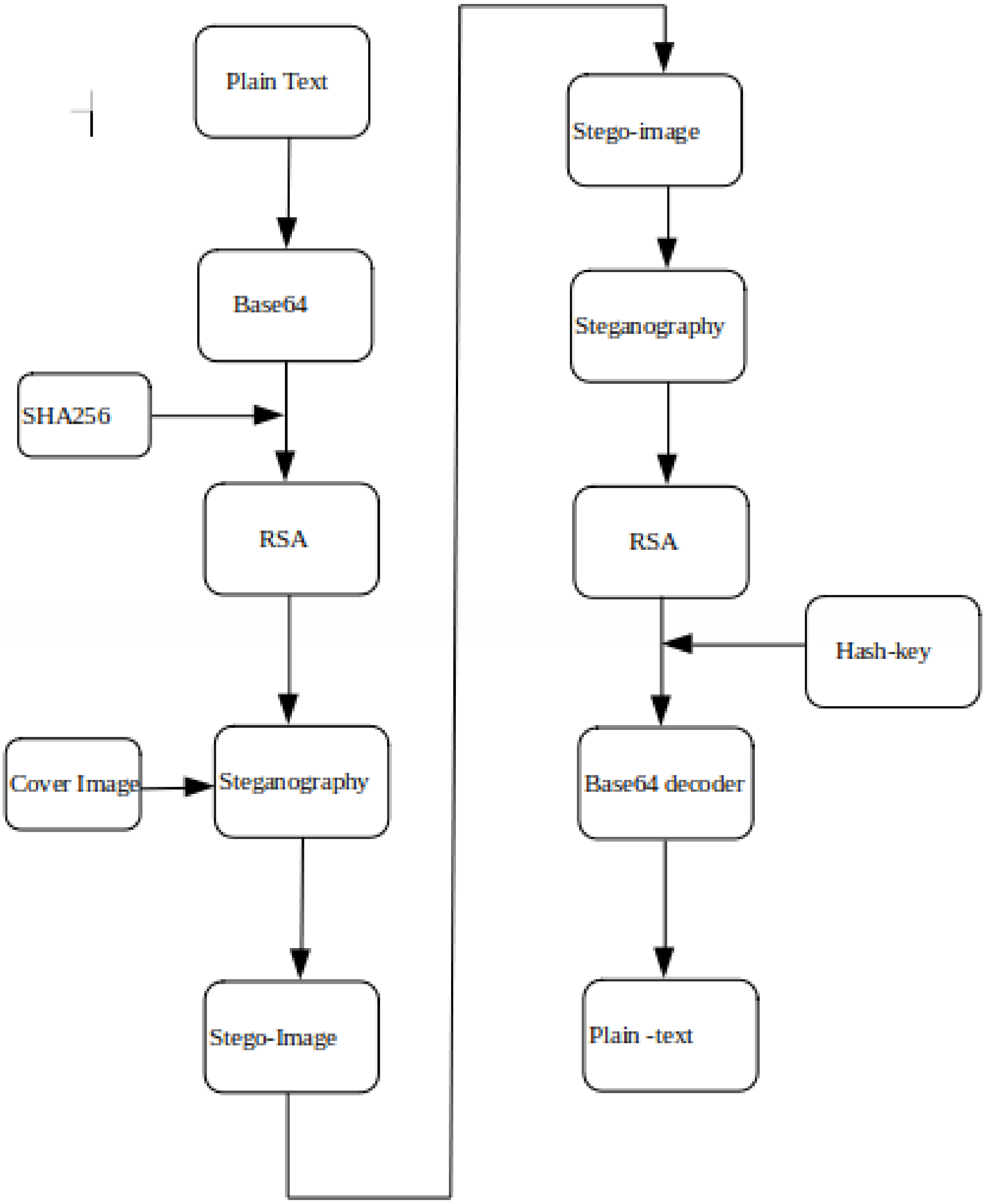


Figure 4: System Block Diagram

4.3 Algorithms and flowcharts

4.3.1 RSA algorithm

a) Key Generation:

· Select p and q such that both are the prime numbers, p≠q.

· Calculate n=p×q

· Calculate q(n) = (p-1) (q-1)

· Select an integer e such that: g (d ((n), e)) =1 & 1< e < (n)

· Calculate d; de = 1 mod (q(n))

· Public Key, PU= {e, n}

· Private Key, PR ={d,n}

b) Encryption:

· Plaintext: M

· Ciphertext: C = (M^e) mod n

c) Decryption:

· Ciphertext: C

· Plaintext: M= (C^d) mod n

· Note 1: (n) -> Euler's totient function

· Note 2: Relationship between C and d is expressed as:

ed (mod (n)) =1

ed = 1 mod (n)

d =e−1 mod (n)

4.3.2 Algorithm of Image Steganography

Inputs: Image, Message.

1) Initially Sender considers a Cover Image.

2) Hide the Encrypted message in the image.

3) After Hiding the Image is considered as a Stego-Image. Which consists of images and data which is encrypted.

4) The Receiver will receive the Stego-Image.

5) The receiver can view the data hidden in the image by providing the newly formed cover image.

7) Thus, the receiver can receive the message safely.

4.3.3 ALGORITHM ILLUSTRATION

Encryption:

Inputs: Message, Image

Step 1: Consider an Input message.

Step 2: Encode input message using Base-64 encoder.

Step 3: Generate Hash of encoded message using SHA-256.

Step 4: Append encoded message and hash of encoded message.

Step 5: Encrypt the final message by using the RSA algorithm.

Step 6: By Using RSA, we will be getting Cipher Text.

Step 7: Consider cover image, and hide the cipher text in the given image Using Steganography Algorithm.

Step 8: Now send the Stego-Image, Private key and Hash of message to the Receiver.

DECRYPTION:

Inputs: Stego Image, Hash of message, Private Key

Step 1: Consider the input to be Stego-Image.

Step 2: Obtain the hidden Cipher text from the Stego Image.

Step 4: Decrypt the cipher text using the RSA algorithm.

Step 5: Compare the input hash of the message with the decrypted string.

Step 6: Decode decrypted message using base 64 decoder.

Step 6: We will get the actual Text as output.

4.3.4 Flowchart of RSA Algorithm

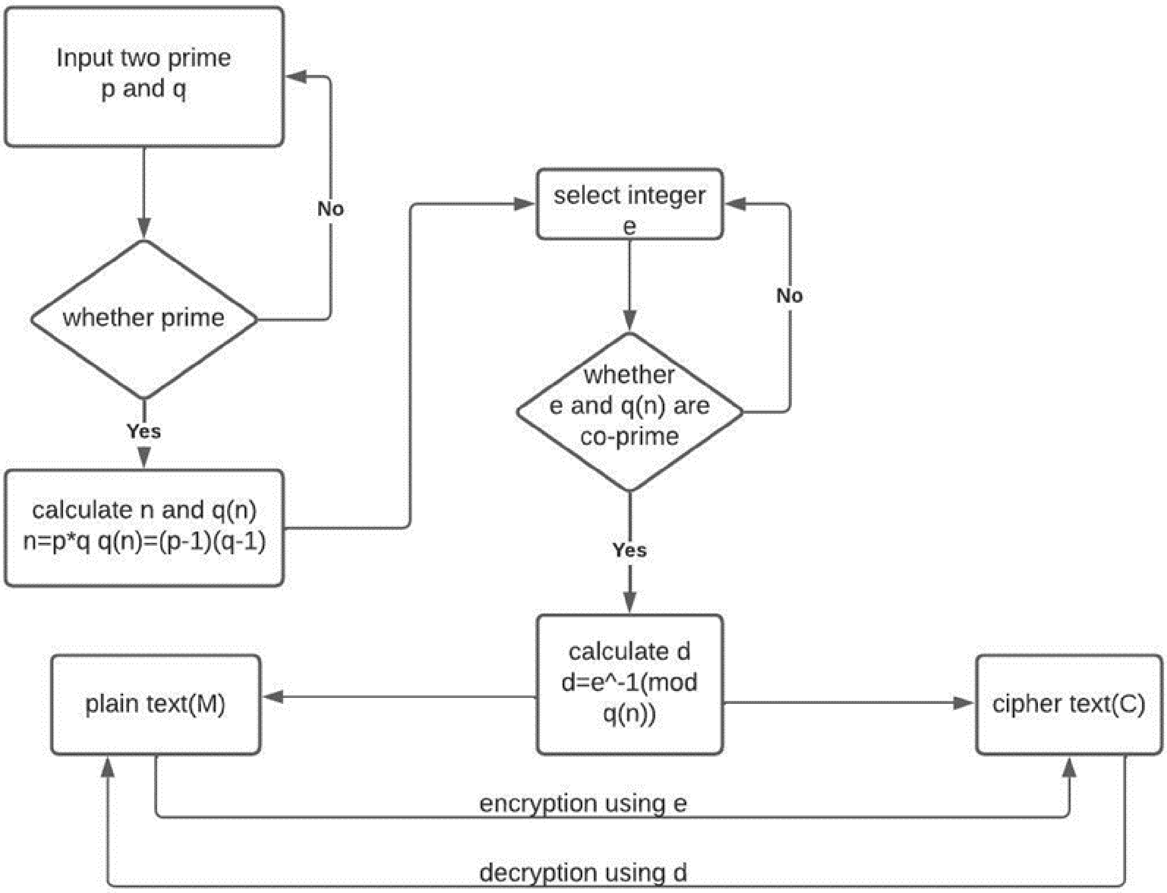


Figure 5: Flowchart of RSA

4.3.5 System flowchart

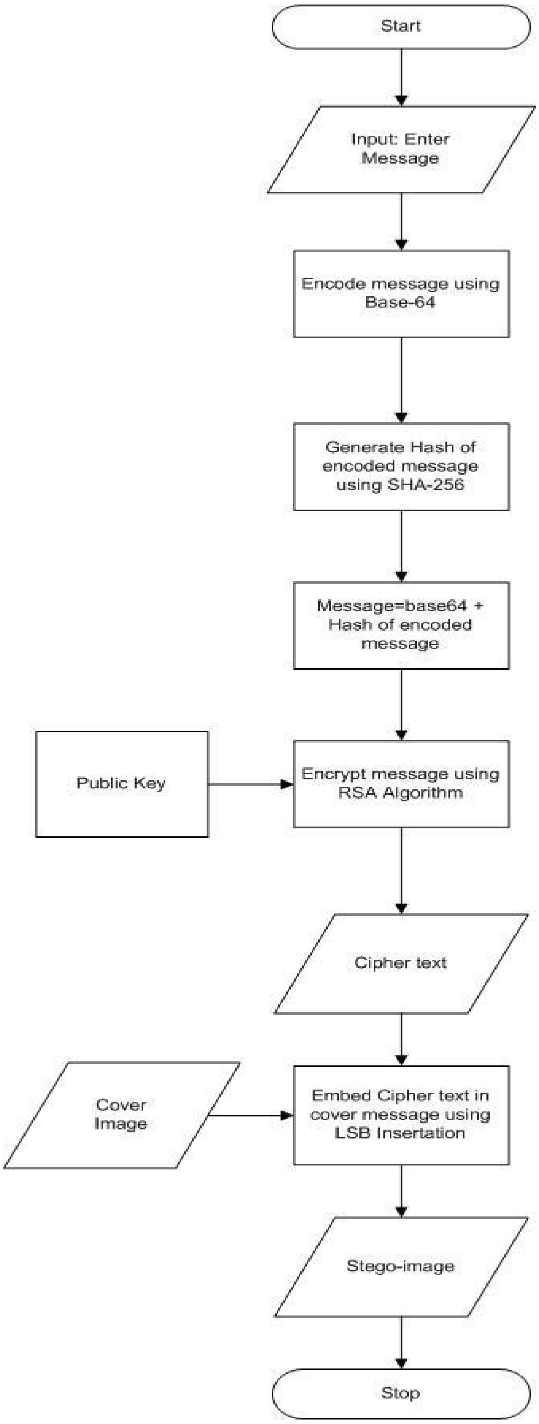

Start
Input: Enter Message
Encode message using Base-64
Generate Hash of encoded message using SHA-256
Message=base64 + Hash of encoded message
Public Key
Encrypt message using RSA Algorithm
Cipher text
Cover Image
Embed Cipher text in cover message using LSB Insertation
Stego-image
Stop

Figure 6: Flowchart of encryption Algorithm

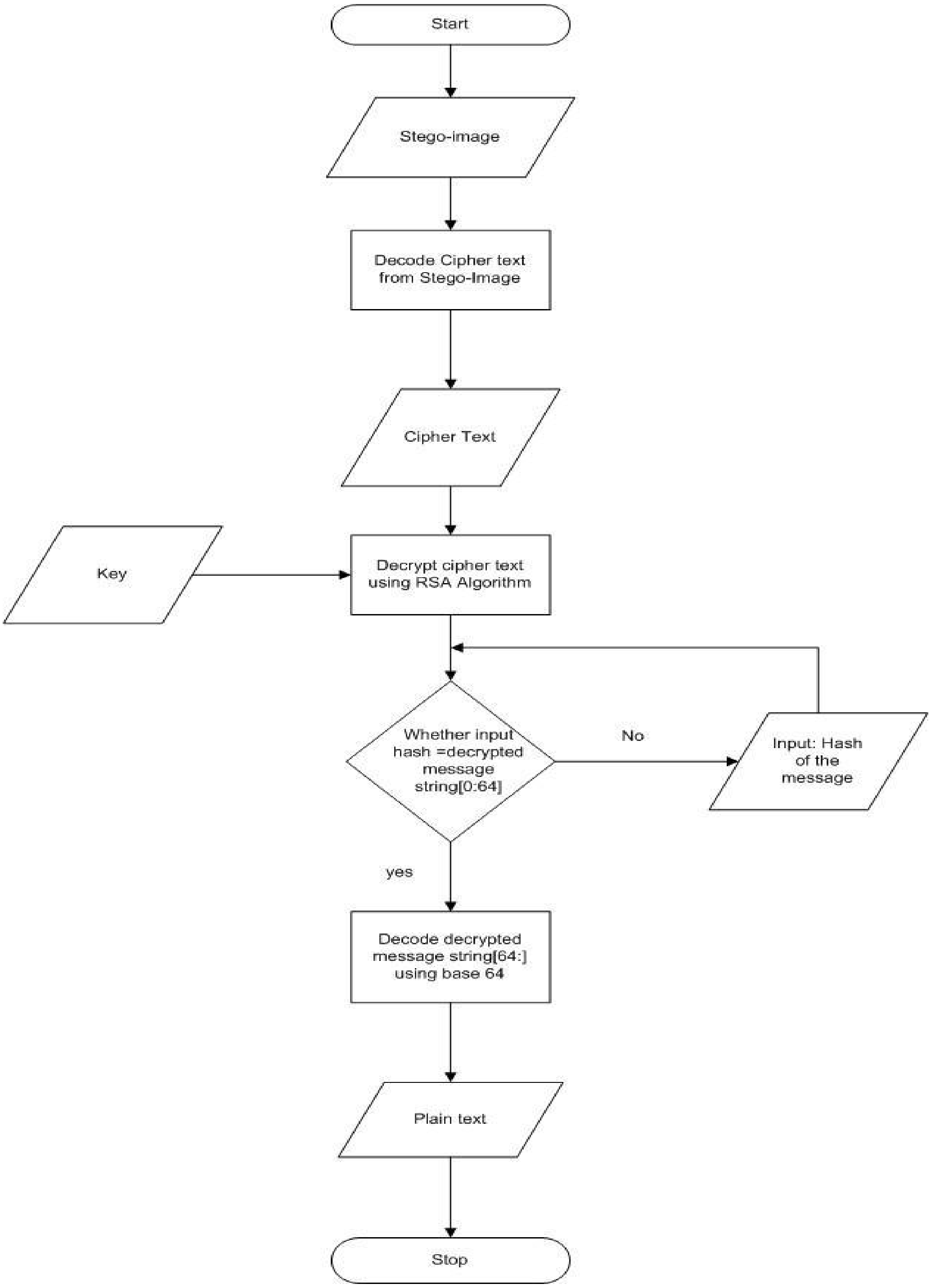

Start
Stego-image
Decode Cipher text from Stego-Image
Cipher Text
Key
Decrypt cipher text using RSA Algorithm
Whether input hash =decrypted message string[0:64]
No
Input: Hash of the message
yes
Decode decrypted message string[64:] using base 64
Plain text
Stop

Figure 7: Flowchart of Decryption Algorithm

4.4 UML DIAGRAMS

DFD LEVEL 0

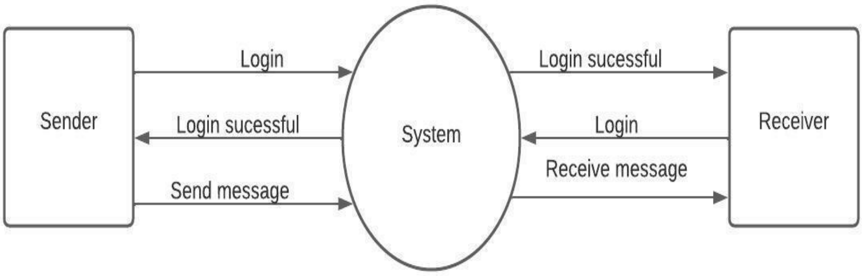


Figure 8: DFD level 0

Use case Diagram

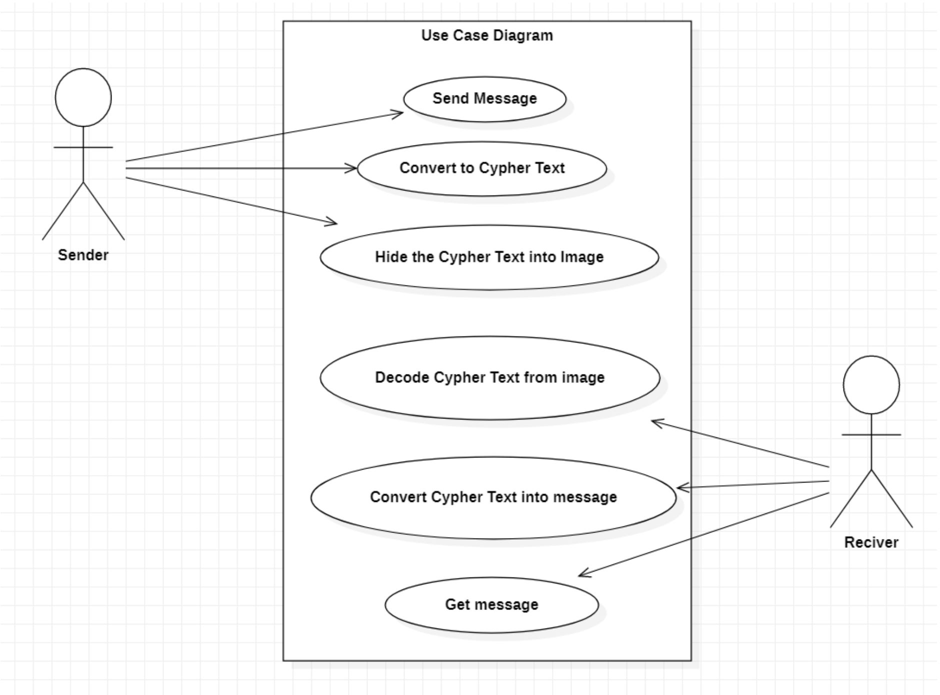

Use Case Diagram
Sender
Send Message
Convert to Cypher Text
Hide the Cypher Text into Image
Decode Cypher Text from image
Convert Cypher Text into message
Get message
Reciver

Figure 9: Use case diagram

SEQUENTIAL DIAGRAM

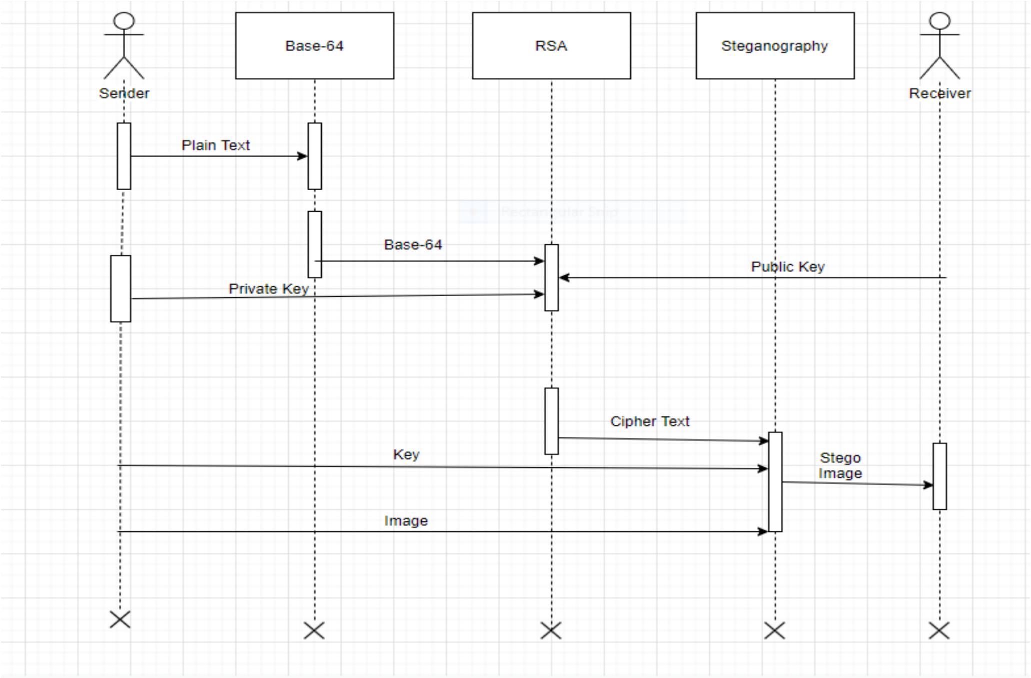


Figure 10: Sequential Diagram

Class diagram

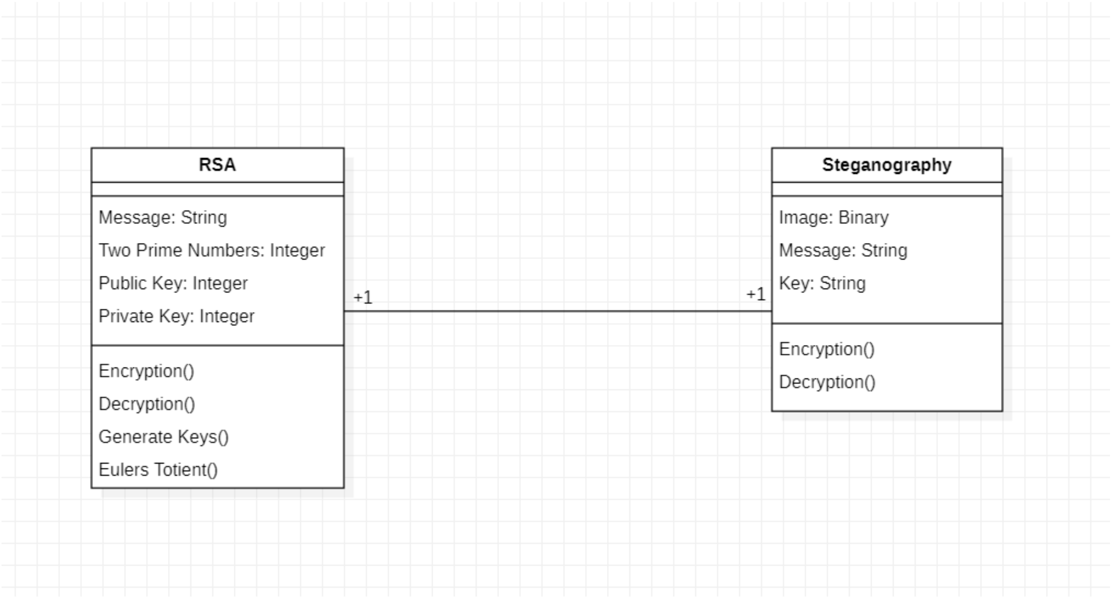


Figure 11: Class Diagram

CHAPTER 5

5 Software development model

Prototyping model

In this project, we use the prototyping model. By using this model we can welcome late changes in our program. For example, we planned on importing the RSA algorithm and encoding the language. but later instead of importing we set up its proper RSA algorithm.

- This prototype is developed based on the currently known
- By using this prototype, the client can get an “actually feel” of the system, since the interactions with the prototype can enable the client to better understand the requirements of the desired
- Prototyping is an attractive idea for complicated and large systems for which there is no manual process or existing system to help to determine the
- The prototype is usually not a complete system and many of the details are not built in the prototype. The goal is to provide a system with overall functionality.

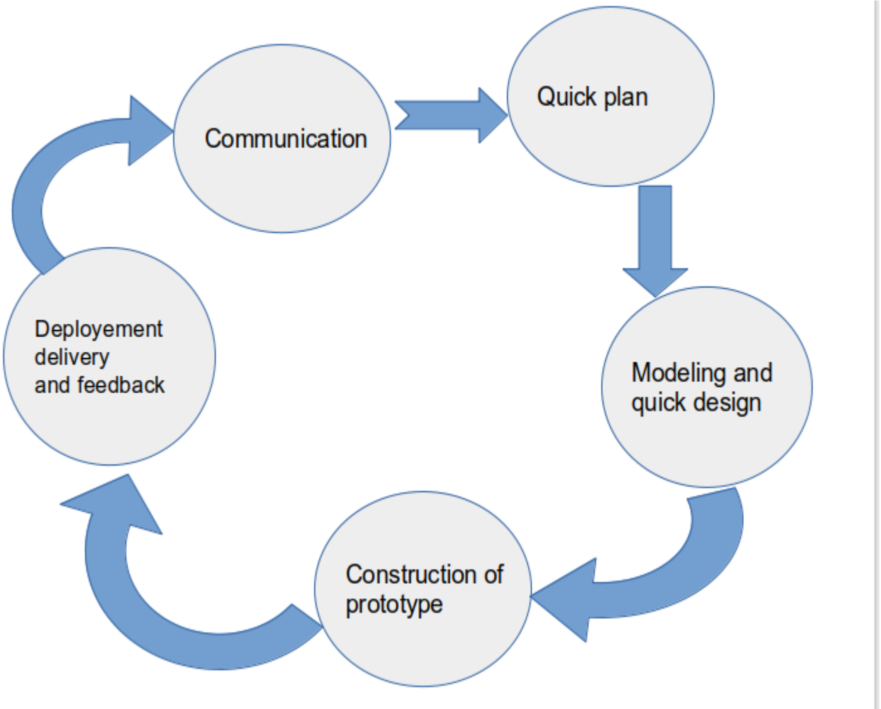

Communication
Quick plan
Modeling and quick design
Construction of prototype
Deployement delivery and feedback

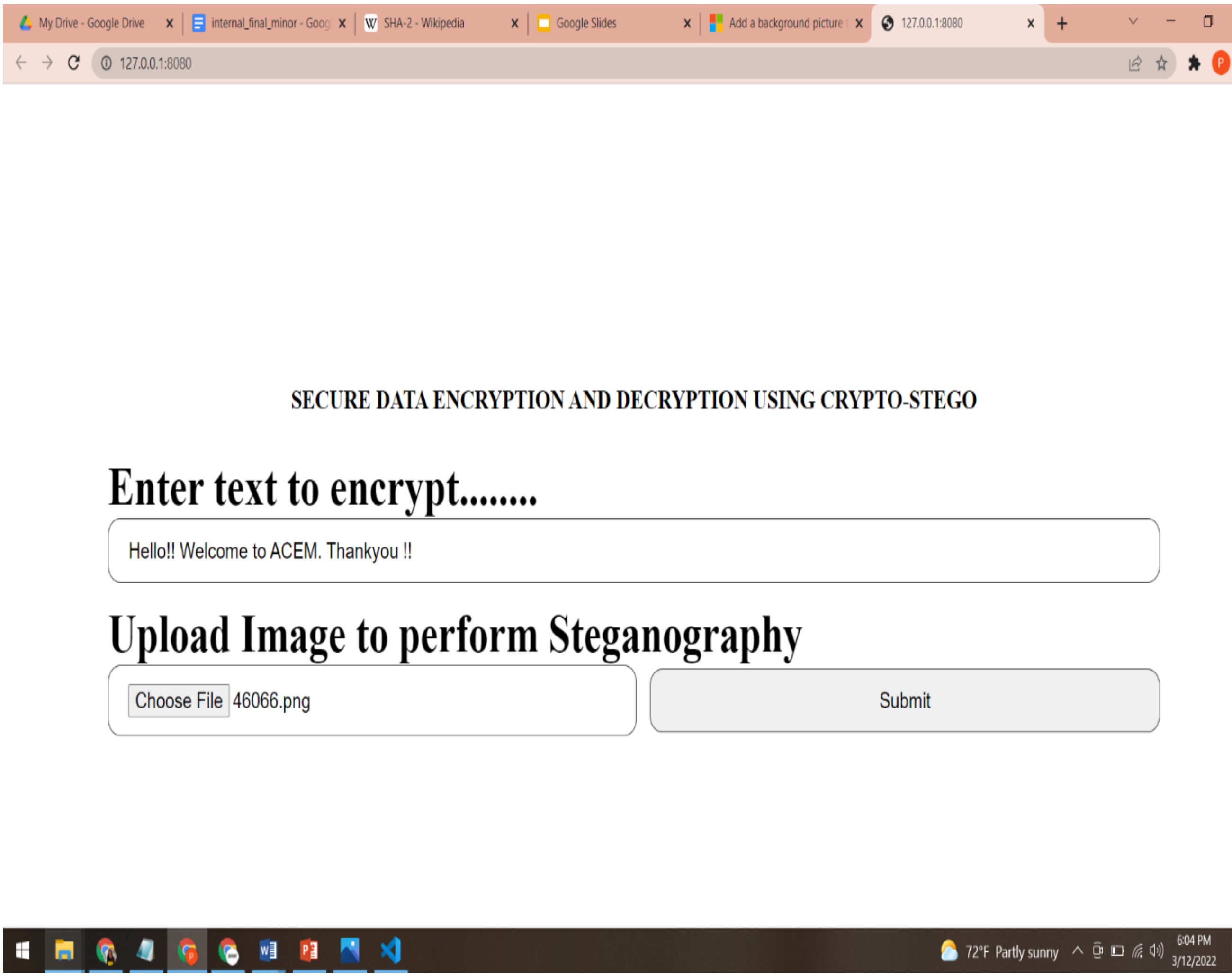
Figure 12: Prototyping model

CHAPTER 6

6 RESULT AND ANALYSIS

This web app was built using core python so that we can set proper algorithms in it. We set both proper algorithms of RSA and LSB insertion. We are able to encrypt a message and hide the cipher text in an image and also able to decrypt the message from an image.

Encryption page



SECURE DATA ENCRYPTION AND DECRYPTION USING CRYPTO-STEGO

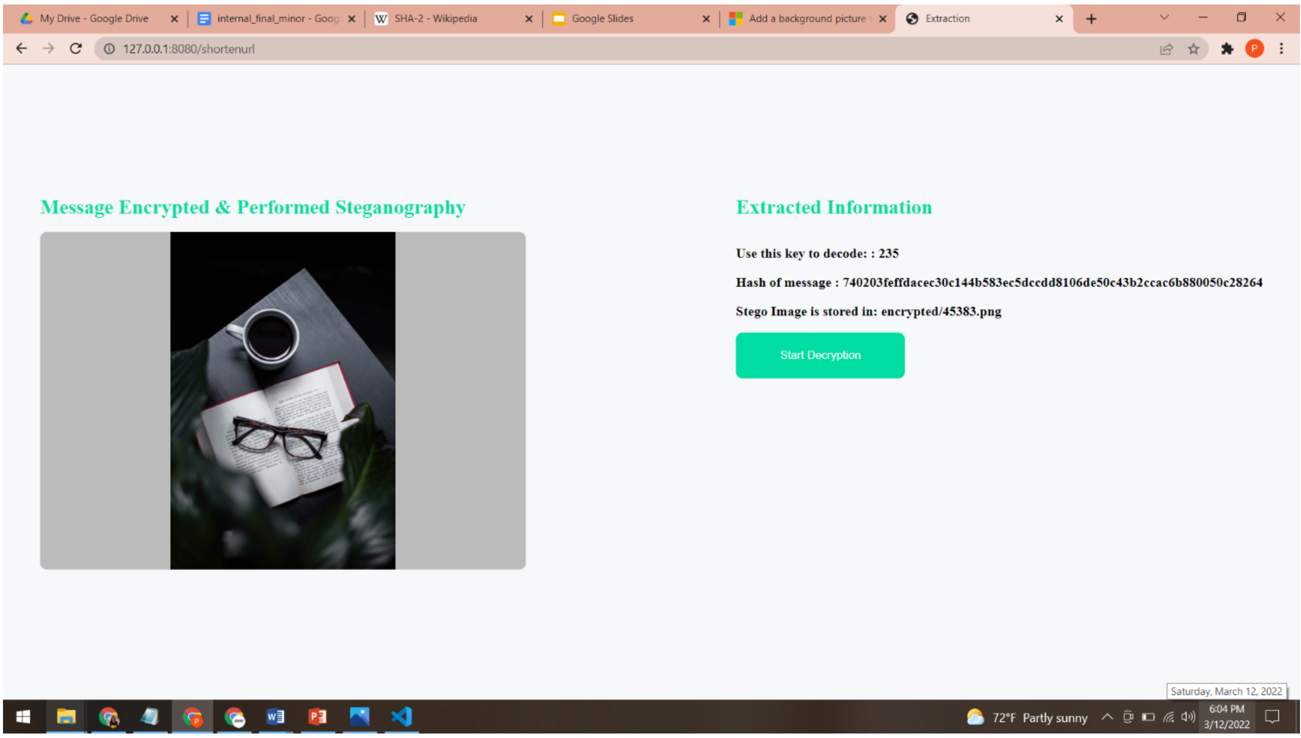
Enter text to encrypt........

Hello!! Welcome to ACEM. Thankyou !!

Upload Image to perform Steganography

Choose File 46066.png

Submit



Message Encrypted & Performed Steganography

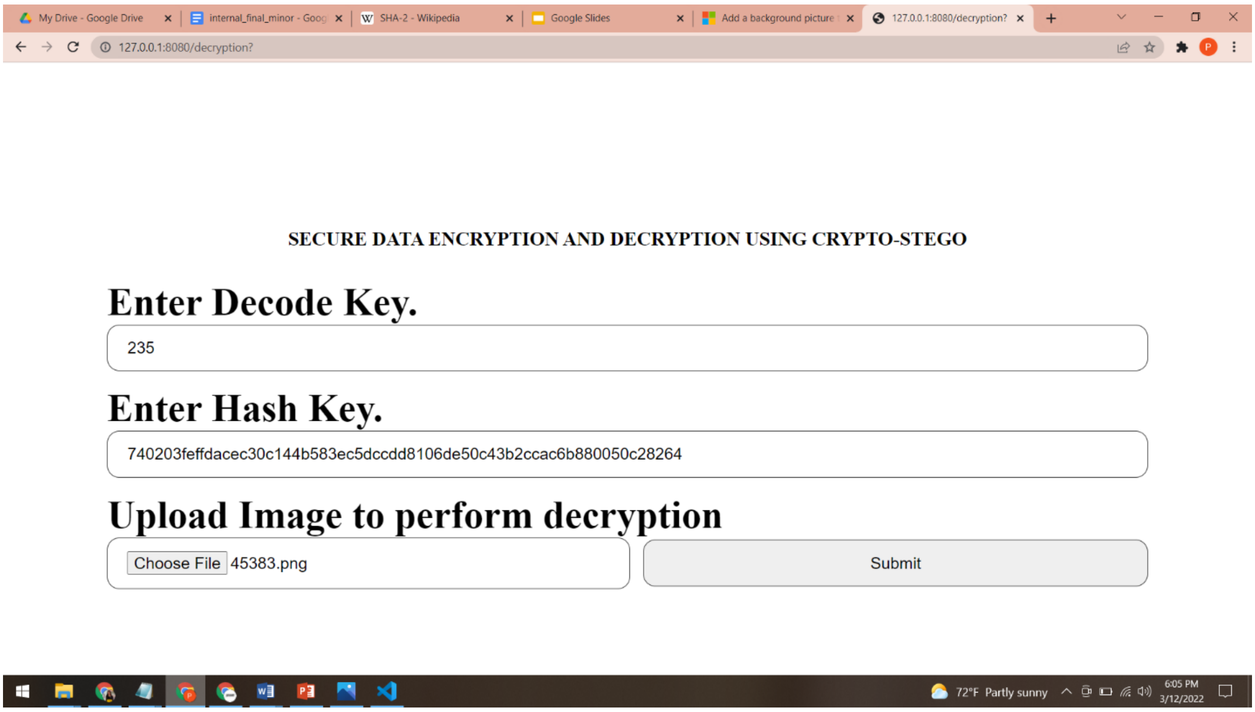
Extracted Information

Use this key to decode: : 235

Hash of message : 740203feffdacec30c144b583ec5dccdd8106de50c43b2ccac6b880050c28264

Stego Image is stored in: encrypted/45383.png

Decryption Page



SECURE DATA ENCRYPTION AND DECRYPTION USING CRYPTO-STEGO

Enter Decode Key.

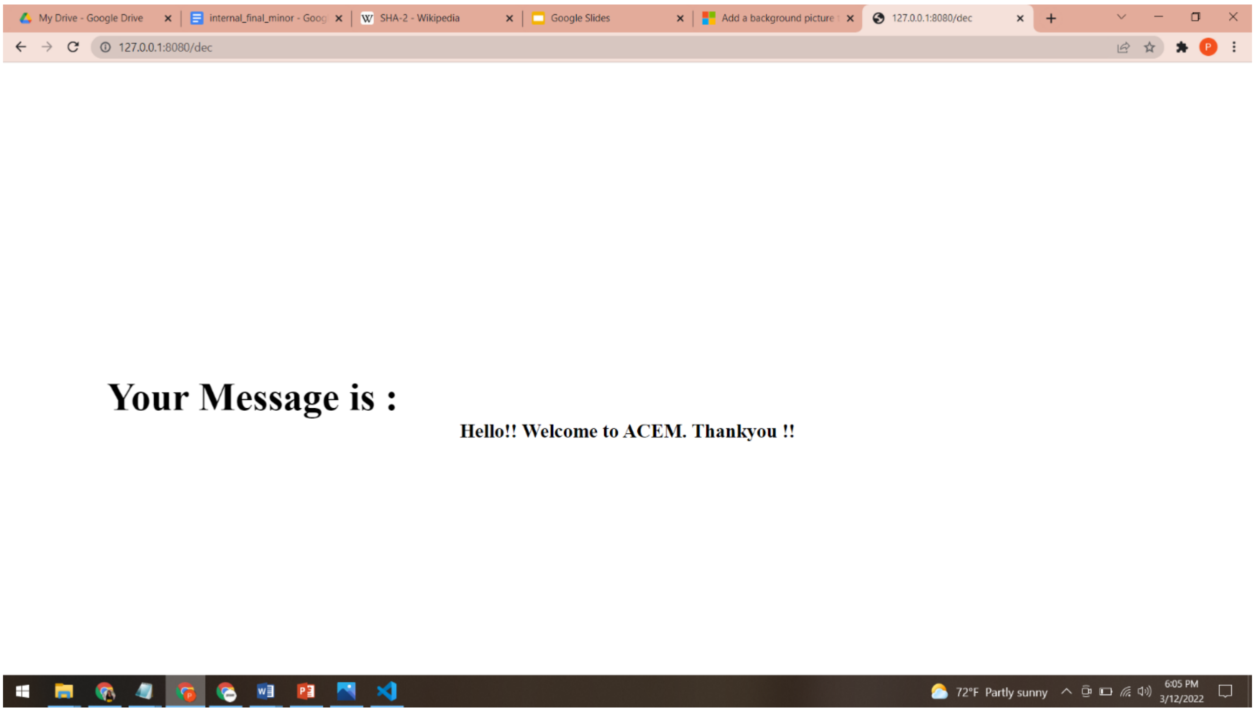
235

Enter Hash Key.

740203feffdacec30c144b583ec5dccdd8106de50c43b2ccac6b880050c28264

Upload Image to perform decryption

45383.png



Your Message is :

Hello!! Welcome to ACEM. Thankyou !!

Cover Image before hiding cipher text

Stego-image after hiding Cipher text

CHAPTER 7

7 Conclusion

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed by combining the steganography and cryptography features factors for better performance. We performed a new crypto-stego method by combining cryptography and steganography. The proposed algorithm is to hide the data effectively in an image without any suspicion of the data being hidden in the image. We performed our method on an image by implementing a program written in Python language. The method proposed has proved successful in hiding Text in color images. We concluded that in our project we can successfully encrypt any message and hide the encrypted message i.e. cipher text in an Image.

CHAPTER 8

8 LIMITATION AND FUTURE ENHANCEMENT

8.1 Limitation of the study

In our project, we can successfully encrypt any message and hide the encrypted message i.e. cipher text in an Image. However, there are some limitations to our project. Our project is a public key cryptosystem (asymmetric cryptography) which is slow compared to symmetric cryptography. In our project if any of the keys either private or hash keys are lost then all received messages cannot be decrypted but security-wise, it's great

8.2 Future enhancement

So basically in our project, we can encrypt only text messages, in the future program we are planning to encrypt audio, video, and image files. All the digital services internet communication system, medical and military system, multimedia system requires the image to be stored and transmitted over a network. And another major thing for future programs is to make two Factor Authentication for more security.

9 References

[1] “Secured crypto stegano data hiding using least significant bit substitution and encryption” journal of Advanced College of Engineering and Management

[2] D. Seth, L. Ramanathan, and A. Pandey, “Security enhancement: Combining cryptography and steganography,” International Journal of Computer Applications (0975–8887) Volume, 2010.

[3] H. Abdulzahra, R. AHMAD, and N. M. NOOR, “Combining cryptography and steganography for data hiding in images,” ACACOS, Applied Computational Science, pp. 978–960, 2014.

[4] William Stallings, Cryptography and Network Security-Principles and Practice, Fifth Edition, Pearson publication, pp. 259-262.