REVA UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

Bachelor of Technology
in
Computer Science and Systems Engineering

Major Project Phase-I Report

The Silent Cipher - Steganography using Caesar cipher and Vigenère cipher

By

Dhanush H	**- R22EK802**
Jayaprakash Gouda	**- R22EK805**
Nitish T	**- R22EK808**
Vinayaka S	**- R22EK809**

Under the supervision of

Mr. Kiran J
Assistant Professor
School of Computing and Information Technology

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064
www.reva.edu.in

November 2024-25

REVA
UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064

CERTIFICATE

This is to certify that the Major Project Phase-1 work titled **“The Silent Cipher - Steganography using Caesar cipher and Vigenère cipher”** is carried out by **Dhanush H(R22EK802), Jayaprakash Gouda(R22EK805), Nitish T(R22KE808), Vinayaka S(R22EK809),** are bonafide students of Bachelor of Technology in **Computer Science and Systems Engineering** at the School of Computing and Information Technology, REVA University, Bangalore in partial fulfillment for the award of degree in Bachelor of Technology in **Computer Science and Systems Engineering**, during the year **2024-2025**.

Prof Kiran J
Assistant Professor
School of Computing and Information Technology
REVA University

Date :

Dr. Muthukumar Balasubramanian
HOD, CSSE
Professor
School of Computing and Information Technology
REVA University
Date :

Name of the Examiner

Signature of Examiner

1.

2.

DECLARATION

We, **Dhanush H(R22EK802), Jayaprakash Gouda(R22EK805), Nitish T(R22KE808), Vinayaka S(R22EK809),** are student's of seventh semester B.Tech in **Computer Science and Systems Engineering**, at the **School of Computing and Information Technology, REVA University, Bangalore**, hereby declare that the Major Project Phase-1 titled **"The Silent Cipher - Steganography using Caesar cipher and Vigenère cipher"** has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Computer Science and Systems Engineering** during the academic year **2024- 2025**.

Student **Signature**

Name 1:
SRN :
Name 2
SRN :
Name 3:
SRN :
Name 4:
SRN :

Place : Bangalore
Date :

ACKNOWLEDGEMENT

It is a great pleasure for us to acknowledge the assistance and support of many individuals who have been responsible for the successful completion of this project work.

First, we take this opportunity to express our sincere gratitude to School of Computing and Information Technology, REVA University for providing us with a great opportunity to pursue our bachelor's degree in this institution.

A special thanks to our **Dr. Muthukumar Balasubramanian, HOD, Computer Science and Systems Engineering** for his continues support and providing the necessary facilities with guidance for carryout the project work.

We would like to thank our guide **Kiran J**, **Assistant Professor**, **School of Computing and Information Technology, REVA University**, for sparing his/her valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.

We are also grateful to our family and friends who provided us with every requirement throughout the course.

We would like to thank one and all who directly or indirectly helped us in the Project work.

TABLE OF CONTENTS

LIST OF ABBREVATIONS

LSB	Least Significant Bit
PNG	Portable Network Graphics
JPG	Joint Photographic Group
BMP	Bitmap Image File
WAV	Waveform Audio File Format
GUI	Graphic User Interface

LIST OF FIGURES

ABSTRACT

Nowadays, reaching people is mainly done through digital communication, so data security should be given a crucial importance. Steganography is a novel approach for protected data communication because “The Silent Cipher – Steganography using Caesar and Vigenère Cipher” combines steganography with cryptography. This paper considers a combination of Vigenère and Caesar encrypting procedures in the field of steganography in order to improve the level of effective data secrecy. Combined with the fact that the stego image is actually an encrypted image of the original data, the system achieves the complete change of cover image’s visual content as well as additional layers of protection against attempts at breaking the encryption.

- **Message Encryption:** The message to be conveyed in this text is not a message of the normal type rather is encrypted using Vigenère cipher and a standard keyword. This encryption process distorts the message and this is something which the unauthorized persons will not be able to understand.
- **LSB Embedding:** In this process, the message is in the form of bits and inserted into the LSB of the cover image pixels. This task is done gradually to overcome maximum interference to the stego-image aesthetics.
- **Stego-Image Generation**: The modified image which includes the author’s secret message is produced. It is very hard to notice any difference between the two pictures and this means that even though a stego-image contain hidden information, it may not easily be detected.

The work flow of the project starts when the user logs into a secure application which is used for encryption and decryption. Restriction of access is implemented by a strong login and signup procedure, as well as by individual secret keys. To do this, the intended users can upload an image, enter a message that should be passed on, and then choose encryption mode. The encryption process involves a two-step ciphering mechanism: first, the message is encrypted using the Vigenère cipher, polyalphabetic cipher that uses a user defined key for shifting based on a series of letters to make the text patterns complex. After that, the Vigenère type message is encoded once more through the use of Padua or Caesar cipher, which is a very basic but surely reliable monoalphabetic letter substitution algorithm that is implemented on the basis of a number. It is considered that this double security measure makes it virtually impossible for a third party to breach the information shield even in the event of a breach of the Crypt II seal since the data will remain encoded under the secret key.

The encrypted message is then placed into the imagethrough the process of LSB steganography, one of the most common forms of hiding information in the least bits of image pixels. The resultant is a stego image that looks exactly like the host image, which hides any signs of the secret message. The stego-image can be shared through Google Drive and only the authorized people can recover and decrypt the data with the help of the application through using the correct keys.

This work was done with usability in mind, so that it could be used to securely communicate with others even if the connection being used is a public or insecure connection. The two-tier encryption not only complicates the system but also enhances the system’s defense against any form of cryptographic and steganographic attack. This system has uses ranging from secure messaging, computer investigations, to secure storage.

Testing of the proposed system also prove its effectiveness with successful encryption, embedding, extraction and decryption. The described method demonstrates how the modern digital steganography can be incorporated with the classical cryptographic schemes as an efficient solution for real life problems of data security. It is about the future improvement of combining new and history ciphers, which is the basis of constructing new data hiding technology.

CHAPTER 1 INTRODUCTION

Steganography, the cover term for hiding some message in other innocuous ones, has been in use since historical times. Although different approaches have been invented in due course, the requirement for effective and secure methods is still crucial. The present work proposes a new approach improving the traditional LSB steganography with the Vigenère cipher to increase the stego-object protection against malicious actions.

The specific goals of this project are as follows: The development of a new secure method for transmission of messages in which the messages are encrypted using both the classical symmetric cryptographic algorithms such as the Vigenère and Caesar ciphers, and then concealed within digital images, through steganography. The project layers these techniques to guarantee that if the steganographic layer is discovered the data contents remain unreadable without the proper decryption keys.

The first step of the overall work flow is a web based application that makes the project very convenient to use. On registration, a user enters secure login details and proceeds to choose an image in which their secret message would be concealed. The method of encryption is a two step procedure. First of all, the text is encoded using the Vigenère cipher – polyalphabetic substitution that encipher and deciphers with a keyword as key. This training makes sure that the final cipher text has undergone through a through process of making it look very random. Then, the text encrypted with the use of Vigenère cipher is further encrypted with another type of monoalphabetic substitution called as Caesar cipher. These two layers of encoding strengthens the security of the message much than the normal encryption.

After that the required information to send is encrypted and is then hidden in the selected image through Least Significant Bit (LSB) Steganography, it is a technique in which data is hidden in the least significant bits of an image. The stego-image which is obtained is nearly imperceptible from the original image which makes the presence of the hidden data non-detectable. This image can then be safely shared through normal means such as through Google Drive among other platforms. On the recipient side, the data can be also retrieved and decrypted with the help of the application only in case the proper keys are provided.

This project does not only consider security but also improve the level of interaction to it so that people with normal understanding of internet handling can also make use of this invention. The double layer encryption partly solves the problems of threats in certain encryption types; at the same time, the integration of steganography adds another layer of protection that conceals the message behind a harmless picture.

Therefore, the series is practical, unique, and safe strategy for contemporary data safety and security concerns. Some of its uses include; privacy protection, electronic investigations, and secure data storage, that is why security is a powerful weapon against the modern trends of cyber security threats.

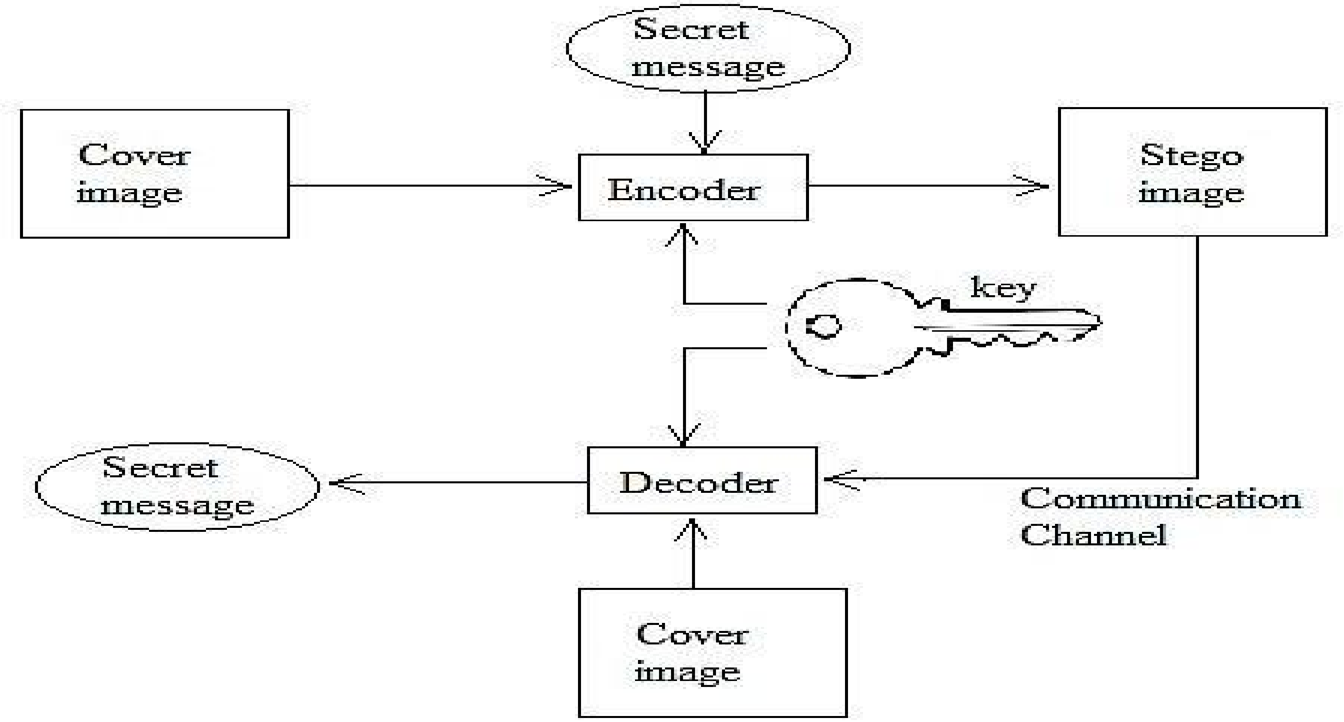


Fig 1.1 Steganography block diagram

1.1 Overview or background and motivation

Over nearly a decade, companies have witnessed increased simplicity in connectivity through one or more forms of digital communication, yet they face more challenges with secure data. Data theft, hacking, and other sorts of invasions are growing prevalent, and, as a result, there is an urgent requirement for better and more secure approaches to the preservation of sensitive data. Cryptography and steganography that have been practiced heretofore are useful methodologies but their performance is somewhat inadequate in combating modern day complexities. Cryptography means keeping information secret and encoding it, steganography means that the existence of the information is non-existent. But if we use both these methods then it becomes quite reliable as it becomes difficult for the attacker to get access to or even identify the hidden information.

The reason for undertaking this project is informed by a new and increasing demand for security of information in individual, business, and governmental realms. Given that data pertains to financial details, identification data and documents containing restricted information are vulnerable most of the time, this project aims at offering a feasible means to protect data. Both sides use High frequency of simple classical encryption algorithms, like Vigenère or Caesar ciphers, because of their efficiency and wide usage in history of cryptography. These ciphers when combined provide a novel method in protecting data from a direct attack and other forms of decryption.

In addition, the problem of covert communication can be solved by integrating steganography where digital images are used as the carriers. This project achieved this by encrypting messages within seemingly irrelevant images, thus, guaranteeing that if the encrypted data is accessed, its existence cannot be noticed.

These techniques used in integrating the project are also supported by the easily understandable and usable application. Due to the shortcomings of the models of plain cryptography and steganography, this paper proposes a dual-layered security model for data protection. The project aims to meet the need for a reliable and multifunctional means for the private or organizational use in the context of modern global interconnectedness.

1.2 Problem Statement

In the current world of internet and socio-technological development, the production of data, the speed and frequency of the data exchange have caused tremendous issues about the security of the information transmitted. Hackers, intruders, and hackers have had their way with personal data, organizations and even governments. Conventional approaches to security such as data encryption and firewall, though useful, cannot adequately contain new and constantly changing threats, however.

A well known method of securing data is through encryption which is insecure, although it maintains the confidentiality of data presence in encrypted form discernible. Whereas steganography, which trends on the idea of hiding information, usually suffers from lack of adequate encryption capabilities, to fall easy prey to enhanced forensic software's. Standalone previous solutions for cryptography and steganography do not offer a cohesive solution that features multiple layers to overcome these problems adequately while not offering an integrated solution that combines data security and stealth communication.

The problem more revolve around the integration of a secure, high throughput and friendly to the user method for data protection while in storage and during transfer. This includes ensuring that:

Encryption makes data impermeable and cannot be decrypted by anyone who is unauthorized to do so.
Encrypted data overlaps seamlessly with other regular data, thus making it very hard for anyone to intercept or raise suspicion.
They are presented in a format which do not require higher IT skills from the users, so the implementations are possible on a large scale.
This project will therefore seek to overcome these restrictions by creating a two tier security model. Therefore, through integrating aspects from two major information security approaches characteristic for this type of project, namely combining the Varatrigesimal and Caesar cipher encryption types, followed by embedding encrypted messages within a selection of two graphical representations of digital images, the project aims to offer a volatile, powerful, and easy-to-use framework for shielding data by preventing access and detection by unauthorized parties.

CHAPTER 2 LITERATURE SURVEY

[1]. The study by Mayank Srivastava, Unnati Srivastava, S. Srivastava published in 6th International Conference in 2023 named “Modified Ceasar Cipher with Image Steganography”

[2]. The study by Arun kumar sing, Juhi Singh, Harsh Vikram Singh in 2023 named Steganography in image using LSB Technique

[3]. The study by Vipul Sharmai, and Madhusudan in 2015 Third International Conference on Image Information Processing (ICIIP) introduced an improvement to the standard Least Significant Bit (LSB) steganography method and including and including a Ciphering technique to enhance the security of the data hidden inside the image.

In contrast, our project, "The Silent Cipher-Steganography using Caesar cipher and Vigenere cipher," advances beyond visual quality improvements to address both security and usability. You enhance the classic LSB approach by integrating a secure key-based system, requiring users to enter a secret key to hide and reveal data, Also adding two ciphering techniques such as Caesar cipher and Vigenere cipher which gives us enhanced security to encrypt the data. This feature adds a vital layer of security that protects the hidden information from unauthorized access, which the 2015 study’s approach did not address.

Least Significant Bit (LSB) Method

LSB method is widely known and frequently used technique in the image based steganography technology because of its effectiveness and ease in implementation. The technique here used was that the least significant bits of the pixel values in the image were replaced with the secret message. This leads to low distortion and when the information is embedded it cannot easily be noticed by other users. Anderson and Petitcolas (1998) pointed out that LSB-based methods work well in terms of hiding data and pointed out that the technique presented is easy to implement if the distortion level in the host image is to be kept to a minimum.

However, as popularity of steganography grew, researchers started to realize that LSB- based techniques had flaws in terms of security and were vulnerable to statistical detection specialized detection tools. For instance, Fridrich et al. (2001) called for better steganalging methods for LSB steganography by proposing some strategies including the distribution of pixel values in an image.

Caesar Cipher

The Caesar cipher is one of the examples of shift cipher belonging to the simplest and most famous methods of the classical cryptography. It is a simple alphanumeric substitution method used to encode the…the plaintext, so that each character in it is replaced with another character a fixed. For instance, with shift of 3 it becomes LGBT starting from A as A shifts to D, B to E and so forth getting back to the start of alphabet if it gets to the end. Whereas the encoding depends on shifting in the contrary, the decryption process will require seeking in the contrary as well. Despite being very simple to apply, the Caesar cipher has a very serious flaw of being prone to rules of attackers since the set of possible keys is relatively small – this code is suitable for applications in simple educational systems or as an element of successive protection schemes.

Vigenère Cipher

The Vigenère cipher is yet another type of polyalphabetic substitution cipher that increases the security level of theросто a simple keyword can be used to set up the encryption sequence. Each group of one or more letters in the plaintext is shifted for a quantity from 0 to L-1 positions in the alphabet according to the corresponding alphabet letter in the repeating keyword. For example, if the keyword is ‘KEY’ then the shifts are the alphabetical position of ‘K,’ ‘E,’ ‘Y’. This method greatly enhances the frequencies from the being analyzed as compared to other monoalphabetic cipher methods like Caesar. However compared to other methods where security is dependent on the length of the keyword this method is more secure because the longer and random the keyword is the more secure it is for cryptanalysis.

Advancements in Steganographic Techniques

Due to these limitations, many researchers have tried to make enhancements on traditional LSB methods as well as coming up with much advanced steganographic algorithms. These ones include adaptive steganography, which change the process of embedding depending on the content of an image, and transform domain steganography, where steganography is done working with the frequency transforms like DCT or DWT of the image and hence it is hard to detect it.

For instance, in Krennet al., (2006), the authors proposed adaptive embedding, where the message embedding depends on the image area making the detection incredibly hard.

Steganography Frameworks

There are multiple frameworks exist to incorporate and evaluate steganalitic methods which plan itself. Stegano is one of them, which is developed to provide easy interface for hiding and retrieving messages within several media types such as image and audio. This is due to the Stegano framework that make it possible to interconnect many algorithms, including LSB, and allows users to hide information effectively and safely. Further, the framework supports various image formats such as PNG, JPG, BMP which are compatible with the proposed method to hide data

Current Trends in Steganography and Security

Presently, many researchers have pointed out the use of integration between steganography and other form of security mechanisms including encryption and hashing. With the application of encryption, the embedded data becomes invisible and at the same time protected from hacking. Further, analyzing Steganography's future, the authors have begun to utilize machine learning and artificial intelligence to detect and combat the steganographic techniques, making a new era in both the use and countermeasures of digital Steganography.

CHAPTER 3 PROBLEM DEFINITION

Computer technology has made people send and receive various information over the internet varying from general information to secretive information so it became important to establish ways of enhancing privacy and security of such information. Nevertheless, the conventional methods of encryption do not appear to be efficient in deeply protecting against these advanced cyber threats. Moreover, ensuring safe transmission of encrypted data without getting attention of smart noises, is another challenge because if data are encrypted they can easily be noticed and this causes attention. This poses a considerable risk to anyone and every entity entrusted with sensitive information including; personal information, financial data or intellectual property.

The problem is even worse when encrypted data is being transfer through shared quantum like Google Drive. Despite the fact that these platforms serve as storage and sharing solutions, they generally do not include end-to-end encryption or schemes to protect against unauthorized access. As we all know, they are still can be breeched and this is especially dangerous if there is no added layer of protection. This underscores the importance of a method of data encryption that also hides the very existence of the data to would-be attackers.

There are a number of historic encryption methods for example the Caesar cipher and the Vigenère cipher of which if used independently are vulnerable to for example pattern detection and lack of key strength. However, it is possible to achieve considerably higher levels of security by applying the described techniques in a tiered manner.

The first and foremost issue can likely be summarized in a question: how to incorporated these encryption techniques into a user-friendly application that would allow for secure embedding of an encrypted data into an image. This approach not only makes the data encrypted but it also blends the data in a small innocuous medium that makes it hard for the unauthorized persons to detect it. This problem can be solved only by creating an easy-to-use but reliable application that would enable secure encryption/decryption and save the data, and thus substantially decrease the potential threats involving unauthorized access to the information to be encrypted/shown or exposure of such information to unauthorized parties.

CHAPTER 4 PROJECT DESCRIPTION

In this particular project, the core focus lies in designing a security, and thus a ciphering, model of the data using an innovative two-stage approach of encryption, accompanied by steganographic methods in order to improve the efficiency and security of the data processing system. The main purpose is to prevent data leakage during transmission and storage by making data both encrypted and as inconspicuous as possible.

The system initiates by an admin control panel where an eligible user can login or sign up into the application. After successful authentication, the user chooses an image of his or her preference through which the data is to be concealed. The first line of encryption is the Vigenère cipher, a polyalphabetic substitution which uses the keyword for encoding the data and that cannot be easily broken by the frequency analysis methods. Further to this the output of this stage is encrypted by a Caesar cipher, a monoalphabetic cipher in which letters are shifted by a fixed key value. As for me the use of two different encryption types to protect the two different kinds of information add a layer of security.

When the data has been encrypted, the data is then incorporated in the chosen image through steganography. This image itself acts as a veil so as to conceal the fact that this data is supplemented by encrypted information. The resulting picture is as good as the original thus being suitable for secure storage or transmitting over other services such as Google Drive.

On the receiver's end, the system allows for decryption by reversing the process: calling the image, decrypting it by the help of the Caesar cipher, and decoding it with the help of the Vigenère code. This makes it possible for only those users who posses the right keys to get to the raw data. These objectives will mean the use of easy to understand fundamentals, basic operation and a thoroughly reliable security proposition to guard against the growing threats of data loss and hacks.

1.1 PROPOSED DESIGN

- **Login/Signup Screen**:Users will be required to log in or sign up to access the application,Login credentials will be stored securely.User profiles will be maintained to track usage and preferences.

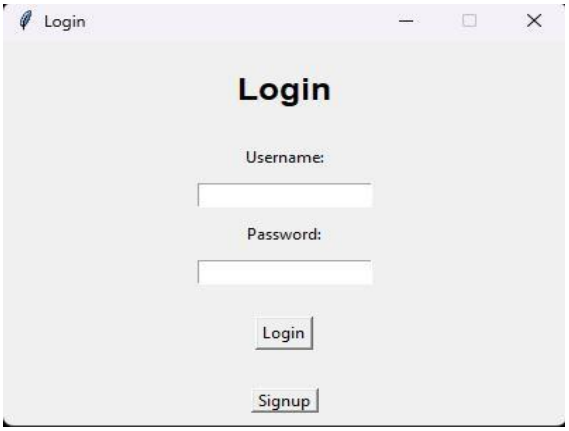


Fig 4.1 login/signup tab

- **User Interface(UI)** :A graphical user interface built with Python’s Tkinter library. The UI allows users to select the image or audio file in which they wish to hide data, enter the message to be hidden, and retrieve the hidden message later.

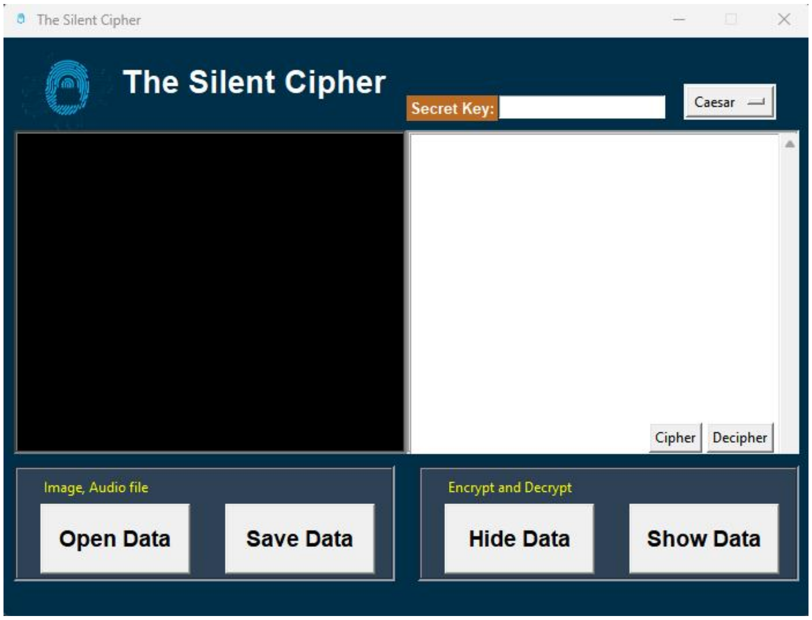


Fig 4.2 User Interface

- **Data Embedding**: The LSB technique is employed to hide data in the least significant bits of an image or audio file, ensuring that the changes are imperceptible to the human eye or ear.

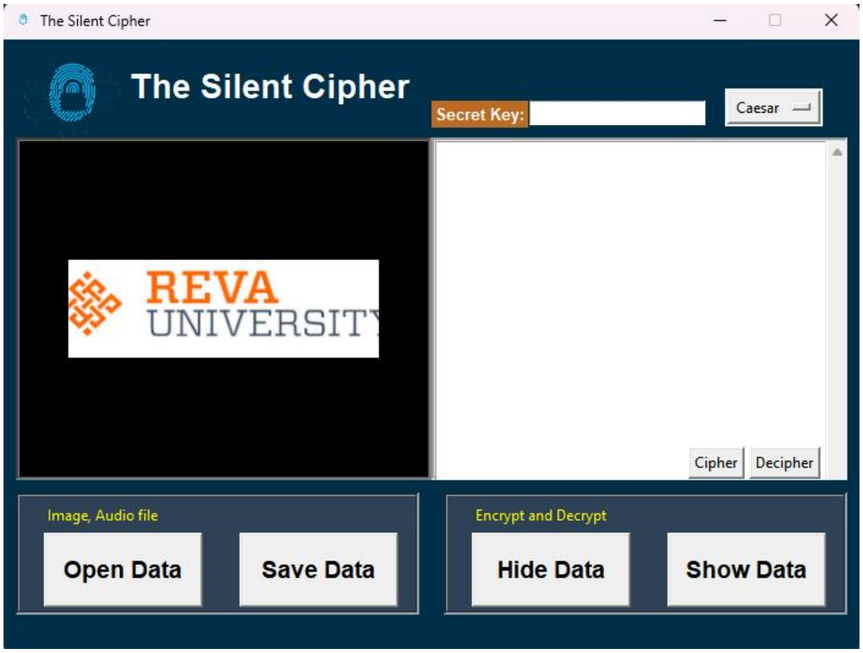
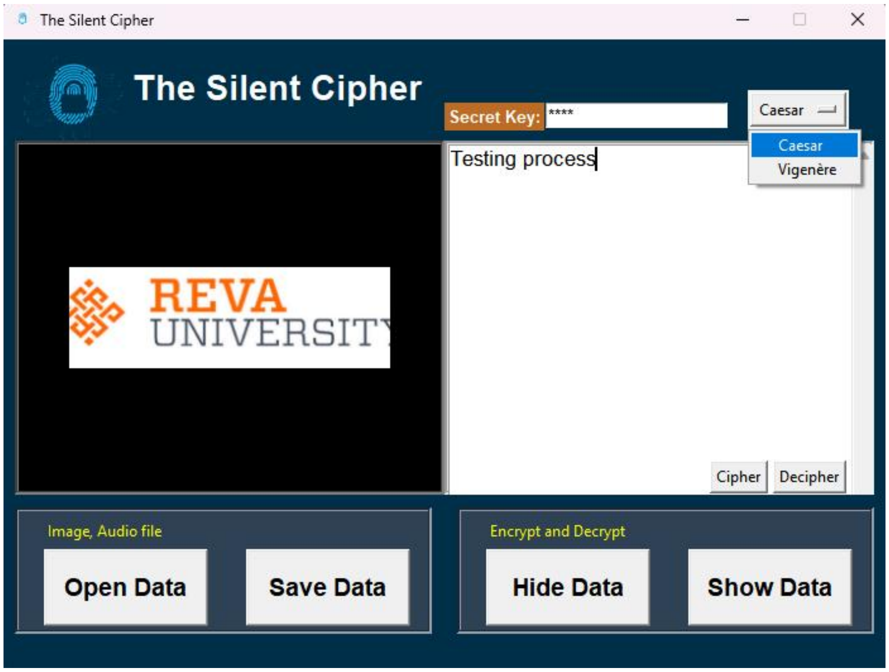


Fig 4.3 Data Embedding

- **Security Features**: Users are required to input a password to secure the hidden data. This ensures that only authorized individuals can access the secret information.



Secret Key: ****

Caesar

Testing process

Fig 4.4 Ciphering the data

- **File Handling**: The project supports a variety of common media formats, including .png, .jpg, .bmp for images, and .wav for audio files. After the data embedding process, the modified file is saved, and users can retrieve it using the decryption process.

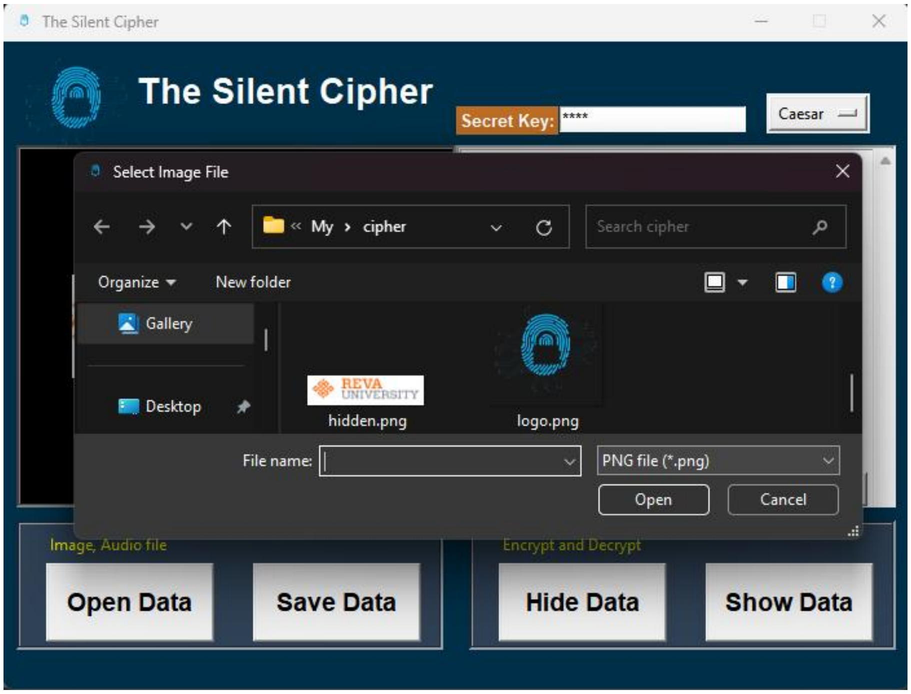


Fig 4.5 File handling

Assumptions and Dependencies:

Assumptions:

- The application is installed on a compatible device mean for using it such as PC or laptop.They are: This image file for steganography is of appropriate size and good quality so that the encrypted data can be installed within the image without distortion.· The secret keys for encryption and decryption are well known to the sender and the receiver only.· The user has fundamental knowledge about how the application operates to perform encryption and decryption.·· The secret keys for encryption and decryption are shared securely between the sender and receiver.
- The user has basic knowledge of operating the application and understanding the encryption-decryption process.
- The transfer of the steganographic image via platforms like Google Drive is secure and not intercepted by unauthorized parties.
- The end-user possesses the necessary tools and credentials to extract and decrypt the data correctly.

Dependencies:

- The application presupposes a stable programming environment for performing the processes of encryption and steganography, such as, for example, Python or analogues.
- The functionality of the project is based on the correct computation of the Vigenère and Caesar cipher algorithms.
- The sender and the receiver need a cloud storage where data will be shared possibly could be Google Drive.
- The image file should not be interpolated during transmission in order to ensure that data embedded here is not corrupted.
- Proper measures relating to key management are important in order to promote secure usage of the key for encryption purposes.
- The high reliance on efficient steganographic techniques assures that the concealed data does not elicit suspicion.

These assumptions and dependencies are crucial for the successful implementation and operation of the project, ensuring data security and integrity throughout the process.

CHAPTER 5 REQUIREMENTS

The Silent Cipher - Steganography using LSB and Vigenère cipher project involves various requirements to ensure smooth functioning and usability. These requirements are categorized into two main groups: **functional** and **non-functional** requirements.

5.1 Functional Requirements:

- **Data Embedding**: The system should enable the user to hide text or a message in an image or audio under the LSB technique.
- **Data Extraction:** Finally, the system must enable the selection of desired data as well as the extraction of the data which is embedded in an image or an Audio file.
- **Password Protection:** There should be a password in order to view the hidden information within the system. It should only be possible to view the hidden message a certain number of times by only those individuals who have the password to view this data..As for the media type, the system should support Images type in .png, .jpg, .bmp and audio type as .wav.g the Least Significant Bit (LSB) method.
- **Data Extraction:** The system must allow the user to extract the hidden data from an image or audio file.
- **Password Protection:** The system should require a password to access the hidden data. Only authorized users with the correct password should be able to retrieve the hidden message.
- **File Format Support:** The system should support multiple media formats, including .png, .jpg, .bmp for images, and .wav for audio files.
- **File Input and Output:** The users should be able to put point to select a media file either in image or audio format and then be able to save the newly embedded file. A user must be able to upload a file that the system will use to extract data.
- **Graphical User Interface (GUI):** Concisely, this means the core code must be installed with a user-friendly interface developed through the application of Python’s Tkinter to enable a user conveniently select files and input data for encoding and decoding messages.

5.2 Non-Functional Requirements:

- **Usability:** The system must be user friendly, employing a GUI that will not require training of the users.
- **Efficiency:** This means that the system should well execute data embedding and extraction operation in terms of time without hinderance for medium sized media files.
- **Portability:** The system should be compatible with the two major operating systems; windows and MAC operating system without much modification.
- **Reliability:** It should be efficient in its functioning during normal operation and deliver the correct outcome to the data embedding and extracting processes. It should also gracefully respond to scenarios that there are errors.
- **Scalability:** Introducing larger files or additional media format should be possible without great changes in the system in the future.
- **Maintainability:** The system should be easy to maintain and update, including key documentation like your code, and your design, so that changes can be made simpler with things like enhanced features that might be added to your site.
- **Performance:** The system should guarantee that processes of data embedding and extraction affect the media file in such a way that its usability is not compromised.

CHAPTER 6 METHODOLOGY

First, the call sign is written in capitals and encrypted using the vigener cipher and cesar 13 (!) with an implemented key. After that, the encrypted message is partitioned again into bits and hidden into the least significant bits of the cover image pixels using LSB technique. A new image with the message formed is produced and it looks like the normal image.

In order to extract a hidden message, the stego-image is processed in the opposite order as it was created. The extracted bits are decrypted using the Vigenère cipher, and Caesar cipher with the help of secret key hosted on the stego-image. The encrypted information is extracted and thus decoded, to retrieve the hidden secret information.

The performance of the proposed method is compared with reference to parameters such as steganographic capacity, image quality and security. The performance of the proposed system is evaluated with respect to the amount of data that can be concealed, the quality of the stego-image and robustness against different types of attacks.

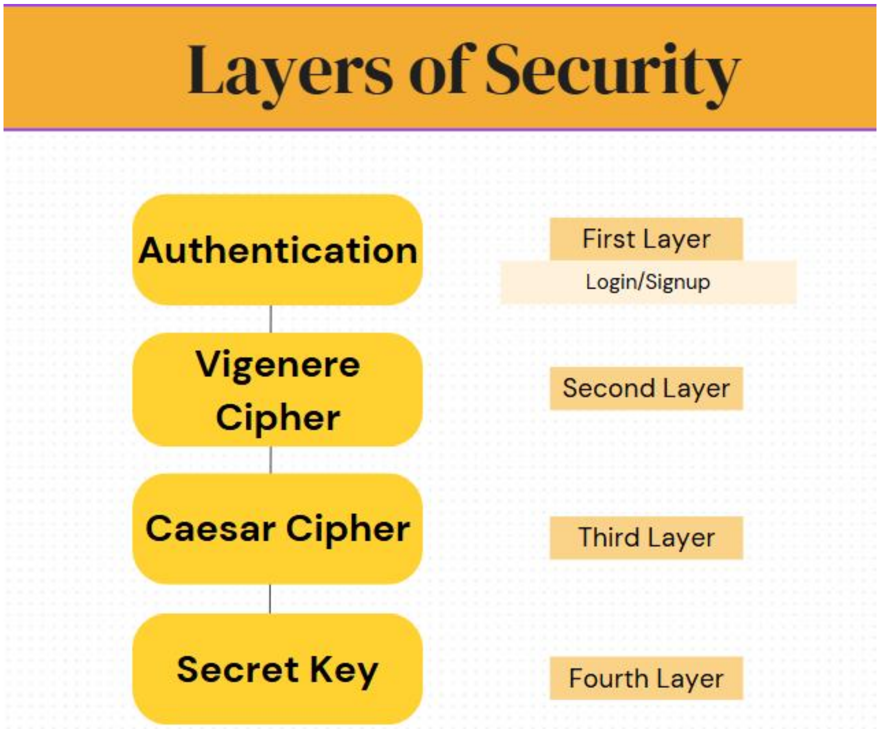


Fig 5.1 Security layers of this project

Caesar Cipher

The Caesar cipher is one of the examples of shift cipher belonging to the simplest and most famous methods of the classical cryptography. It is a simple alphanumeric substitution method used to encode the…the plaintext, so that each character in it is replaced with another character a fixed. For instance, with shift of 3 it becomes LGBT starting from A as A shifts to D, B to E and so forth getting back to the start of alphabet if it gets to the end. Whereas the encoding depends on shifting in the contrary, the decryption process will require seeking in the contrary as well.

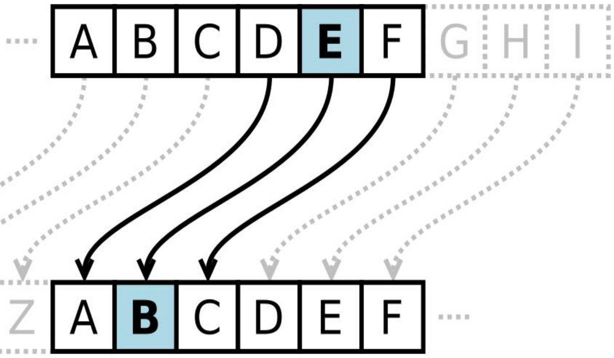
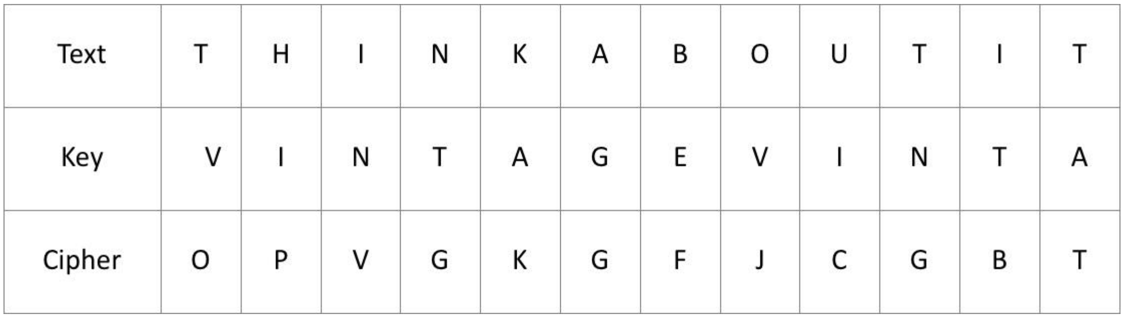


Fig 5.2 Caesar cipher working

Vigenère Cipher

The Vigenère cipher is yet another type of polyalphabetic substitution cipher that increases the security level of the project, a simple keyword can be used to set up the encryption sequence. Each group of one or more letters in the plaintext is shifted for a quantity from 0 to L-1 positions in the alphabet according to the corresponding alphabet letter in the repeating keyword. For example, if the keyword is ‘KEY’ then the shifts are the alphabetical position of ‘K,’ ‘E,’ ‘Y’. This method greatly enhances the frequencies from the being analyzed as compared to other monoalphabetic cipher methods like Caesar.



Text	T	H	I	N	K	A	B	O	U	T	I	T
Key	V	I	N	T	A	G	E	V	I	N	T	A
Cipher	O	P	V	G	K	G	F	J	C	G	B	T

Fig 5.3 Vigenère cipher working

LSB(Least significant bit) TECHNIQUE

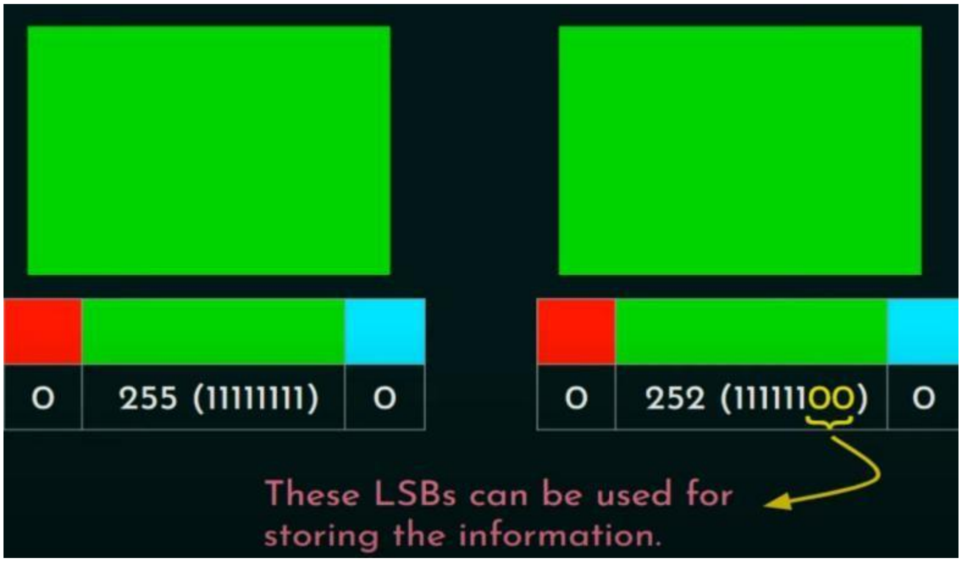


Fig 5.4 LSB technique working

The Least Significant Bit (LSB) technique is a core method in The Silent Cipher - Steganography using LSB and Vigenère cipher, allowing secure and subtle data embedding within image and audio files. This technique operates by modifying the least significant bit of each pixel's color value in an image or sound wave sample in an audio file. Since these slight changes are nearly invisible to the human eye and inaudible to the ear, LSB ensures that the hidden data remains undetected.

In this project, LSB steganography is implemented through the Stegano framework, which efficiently handles bit manipulation required to encode and decode messages within various file formats, such as .png, .jpg, .bmp, and .wav. By embedding data at this bit level, the project achieves secure, low-profile communication, ideal for scenarios where confidentiality and data integrity are critical. This approach provides a simple yet effective solution for concealing information in digital files.

CHAPTER 7 DELIVERABLES

The primary deliverables of this project include a functional steganography system, a comprehensive project report, well-structured source code, a user-friendly manual, and engaging presentation slides.

The steganography system will be designed with a user-friendly interface that allows users to intuitively select cover images, input secret messages, and initiate the steganography process. The system will employ the Vigenère cipher to encrypt the secret message, adding a layer of security. Subsequently, the encrypted message will be embedded into the least significant bits of the cover image pixels using LSB steganography, resulting in a stego-image that is visually indistinguishable from the original image. To extract the hidden message, the system will employ a reverse process, involving LSB extraction and Vigenère decryption.

The project report will provide a detailed account of the entire development process. It will include a comprehensive literature review, a clear problem statement, a detailed description of the proposed methodology, a technical explanation of the implementation, a thorough analysis of experimental results, a summary of key findings and limitations, and potential avenues for future research.

The source code will be well-structured, commented, and organized to enhance readability and maintainability. It will include the implementation of the user interface, encryption/decryption algorithms, and image processing functions.

The user manual will provide clear and concise instructions on how to install, configure, and use the steganography system. It will guide users through the process of selecting cover images, inputting secret messages, and extracting hidden messages. Additionally, the manual will include troubleshooting tips and FAQs to assist users in resolving common issues.

The presentation slides will effectively convey the project's objectives, methodology, results, and conclusions. Visual aids, such as diagrams and charts, will be used to enhance understanding and engagement. The presentation will be tailored to the specific audience, whether it be technical experts or non-technical stakeholders.

REFERENCES

1. Vincent Smith, Maximilian Mendoza, Insaf Ullah on September 2024 published in Journal of Information Systems and technology research displayed us the Data Security Techniques Using Vigenere Cipher And Steganography Methods In Inserting Text Messages In Images
2. The study by Mayank Srivastava, Unnati Srivastava, S. Srivastava published in 6th International Conference in 2023 named “Modified Ceasar Cipher with Image Steganography”
3. The study by Arun kumar sing, Juhi Singh, Harsh Vikram Singh in 2023 named Steganography in image using LSB Technique
4. R. Chandramouli, M. Kharrazi, and N. Memon, “Image Steganography and Steganalysis: Concepts and Practice,” in Digital Watermarking, Springer Berlin Heidelberg, 2004, pp. 35–49.
5. E. E. A. Elgabar and H. A. A. Alamin, “Comparison of LSB Steganography in GIF and BMP Images,” International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 4, pp. 79–83, 2013.
6. N. Akhtar, P. Johri, and S. Khan, “Enhancing the Security and Quality of LSB Based Image Steganography,” in Proceeding of 5th International Conference on Computational Intelligence and Communication Networks, 2013, pp. 385 – 390.
7. M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” Computer Science Review, vol. 13–14, pp. 95–113, 2014.
8. The study by Vipul Sharmai, and Madhusudan in 2015 Third International Conference on Image Information Processing (ICIIP) introduced an improvement to the standard Least Significant Bit (LSB) steganography method and including and including a Ciphering technique to enhance the security of the data hidden inside the image.