



**Excelssior Education Society's
K.C.College Of Engineering and Management Studies and
Research**

**(Affiliated to the University of Mumbai)
Mith Bunder Road, Near Hume Pipe, Kopri, Thane (E)-400603**

Encoder - Decoder

Submitted in partial fulfillment of the requirements of
SECOND YEAR IN COMPUTER ENGINEERING

By

Sahil Sawant B-17

Aditya Shinde B-25

Vinayak Utekar B-42

Supervisor

Dr. Poulami Das Roy



Department of Computer Engineering

K.C. College of Engineering and Management Studies and Research

Mith Bunder Road, Kopri, Thane (E)-400603

University of Mumbai

(AY 2021-22)

CERTIFICATE

This is to certify that the Mini Project entitled “ **Encoder - Decoder** ” is a bonafide work of **Sahil Sawant (B-17), Aditya Shinde (B-25), Vinayak Utekar (B-42)** submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of “**Bachelor of Engineering**” in “**Computer Engineering**” .

Supervisor

Dr. Poulami Das Roy

Head of Department

Prof. Mandar Ganjapurkar

Principal

Dr. Vilas Nitnaware

Mini Project Approval

This Mini Project entitled “**Encoder - Decoder**” by **Sahil Sawant (B-17), Aditya Shinde (B-25), Vinayak Utekar (B-42)** is approved for the degree of **Bachelor of Engineering in Computer Engineering.**

Examiners

1.....
(Internal Examiner Name & Sign)

2.....
(External Examiner name & Sign)

Date:

Place:

Contents

Abstract	ii
Acknowledgments	iii
List of Abbreviations	iv
List of Figures	v
List of Tables	vi
List of Symbols	vii
1 Introduction	1
1.1 Introduction	
1.2 Motivation	
1.3 Problem Statement & Objectives	
1.4 Organization of the Report	
2 Literature Survey	11
2.1 Survey of Existing System	
2.2 Limitation Existing system or research gap	
2.3 Mini Project Contribution	
3 Proposed System (eg New Approach of Data Summarization)	18
3.1 Introduction	
3.2 Architecture/ Framework	
3.3 Algorithm and Process Design	
3.4 Details of Hardware & Software	
3.5 Experiment and Results	
3.6 Conclusion and Future work.	
4 References	32

Abstract

Encoder-Decoder – Secure your Information by Encoding the messages. Encoding is the process that transforms the text or information to the unrecognizable form and decryption is the process to convert the encrypted message into its original form. The objective of this project is to encode and decode messages using Caesar Cipher and Steganography.

Message encoding is the process to first convert the original text to the random and meaningless text called ciphertext. This process is called encoding. Decoding is the process to convert that ciphertext to the original text. While in Steganography the existence of the text is hidden in normal unsecure image until it is decoded.

In this project, users have to enter the message and decide whether to encode or decode. To build this project we have used the basic concept of python, Tkinter and Stegano.

Tkinter : Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Tkinter provides a powerful object-oriented interface to the Tk GUI toolkit.

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection

ACKNOWLEDGEMENT

No project is ever complete without the guidance of those experts who have already traded their past before and hence became master of it and as a result, our mentor. So we would like to take this opportunity to take all those individuals who have helped us in visualizing this project.

The guidance of **Dr. POULAMI DAS ROY** played a great role in our research work. Her guidance helped us in finding relevant information about our topic. We are grateful to get an opportunity to present our work to everyone. We would like to express our gratitude to the '**K.C. College of Engineering and Management studies & Research**' as well as our Head of Department, professor "**Mandar Ganjapurkar**" for promoting students to express their ideas and research. Our sincere vote of thanks goes to our college Principal, "**Dr. Vilas Nitnaware**" for believing in the work of their students and pushing our limits to do better in our field of study.

LIST OF ABBREVIATIONS

stg - stegano

char - character

Tk - Tkinter

bg - background

fg - foreground

config - configure

padx - padding X-axis

pady - padding Y-axis

bd - border

relx = relative X-axis

rely = relative Y-axis

List of Figures

Figure no.	Figure name.	Figure pg.no.
1.	Main Screen flowchart	16
2.	Steganography working flowchart	16
3.	Caesar Working Flowchart	17
4.	Main Screen Output	19
5.	Steganography working Output	19
6.	Caesar Working Output	19

List of Tables

Table no.	Table name	Table pg.no.
1.	Literature Survey for Caesar	12
2.	Literature Survey for Steganography	12

1. Introduction

1.1 Introduction

- In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.
- The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.
- Few common items that are encrypted include text files, images, e-mail messages, user data and directories. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. It may also be performed with a set of keys or passwords.
- The word Steganography is derived from two Greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.
- Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.
- In this project we have used Caesar Cipher & Steganography which are the most used techniques for secret messaging and exchanging of confidential data.

1.2 Motivation

- Being under Cyber attack and losing confidential data is the most harmful thing in today's world which could lead to frauds, misuse of your information and criminal usage.
- More vital/secret data handled by distributed components.
- Security: protecting data stored in and transferred between distributed components from unauthorized access.
- Security is a non-functional requirement that cannot be added as a component but has to be built into all components.

1.3 PROBLEM STATEMENT & OBJECTIVES

PROBLEM STATEMENT :

- How to secure your information from unauthorized access?
- Secure message/ data transfer.
- Encoder-Decoder – Secures your Information by Encoding the Messages.

OBJECTIVES :

- To explore the problems encountered in Cyber attacks.
- To design a system that will make information more secure, easy to operate and difficult for hackers to hack.
- To implement a mechanism that will help people to secure their information and transfer data more securely.

1.4 Organization of the Report

1. In Chapter 2, we will see the Literature survey which will tell us more about the background of the project including the work that has already been done in this field.
2. In Chapter 3, Proposed System is introduced which will tell the deep specification which of the project and will tell how the different modules of the system will work.
3. In Chapter 4, we see the conclusion and future scope of the project.

2. Literature Survey

2.1 Survey of Existing System

Technology used	Python, Tkinter, Stegano
Technique	Steganography
Person who introduced	Johannes Trithemius
Year	1499
Specification	One of the earliest and widely used method for hiding existence messages.
Example	It is known that during both world wars, female spies used knitting to send messages, perhaps making an irregular stitch or leaving an intentional hole in the fabric.
Breaking stegano	Same as that of encryption but reverse.
Representation	Every text is distributed into 3 pixels, and after every 3 pixel a binary number is added which hides the given text
Use for	Securing / hiding the confidential text or data existence.
Problem solved	Cyber attacks, Secure data transfer and also Securing confidential information

Technique	Caesar Cipher
Person who introduced	Julius Caesar
Year	Around 100 BC
Specification	One of the earliest and widely used method for encryption messages.
Cipher type	Substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.
Rotation Type	Mono-alphabetic Rotation
Example	If A is the 1st letter in message then with a shift of 1, A would be replaced by B, B would become C, and so on.
Representation	Modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
Encryption Formula	$E_n(x) = (x + n) \bmod 26$
Breaking cipher	Ciphertext-only scenario.
Decryption Formula	$D_n(x) = (x - n) \bmod 26$
Use for	Securing data and Secure messaging

2.2 Limitations of Existing system or Research gap:

- **Forgetting Passwords/Key:**
Generally most people forget the password/keys so they find difficulties to access the message or data.
- **Requiring Cooperation:**
Using encrypted files that are designed to be opened and shared by two or more people can be disadvantageous when one or more participants finds it a burden to use encryption.
- **Developing a False Sense of Security:**
A disadvantage of encrypted files is that relying on them to keep things secret could lull you into a false sense of security. A determined person may marshal overwhelming computer resources to decrypt your secret files.

2.3 Mini Project Contribution:

There was an equal contribution to this project. Giving new ideas, proposing the designs and adding the content to it. Gathering Information, Coding & Executing the final result .

3. Proposed System

3.1 INTRODUCTION

The proposed system is a Securing mechanism which will secure your data & help you to transfer highly confidential information to others . This system allows only authorized users to access the encrypted information using their respective key . Users can decide whether to encrypt his data in text format using Caesar cipher or in image format using Steganography.

3.2 Architecture/Framework

- Tkinter : Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Tkinter provides a powerful object-oriented interface to the Tk GUI toolkit.
- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection

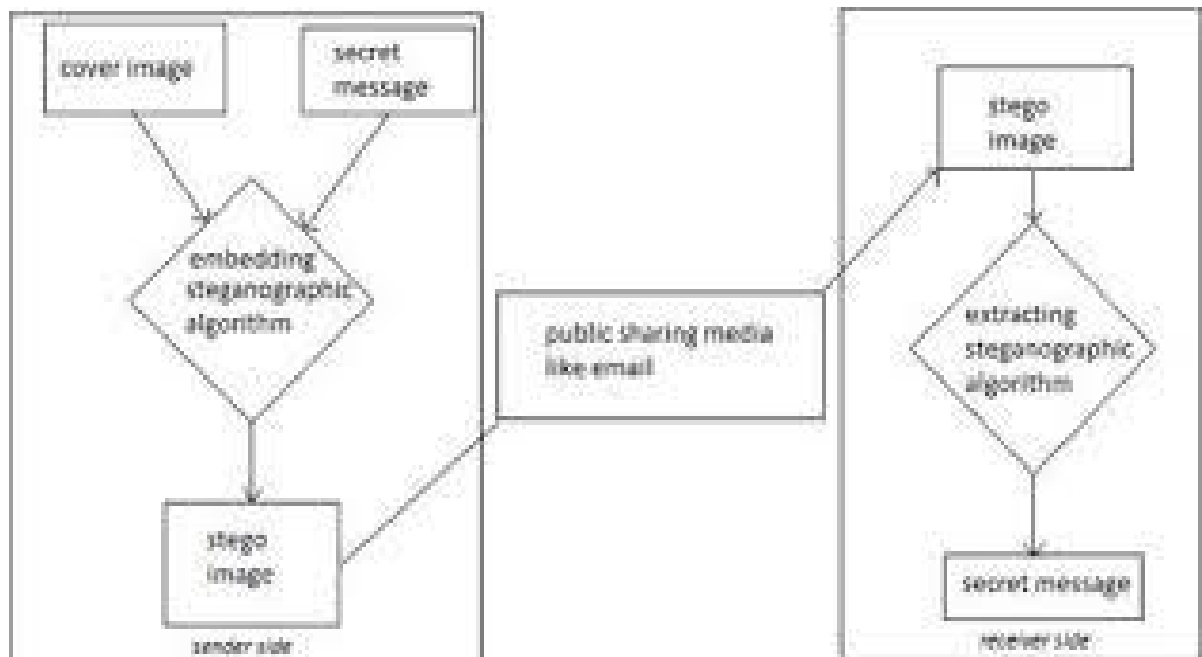
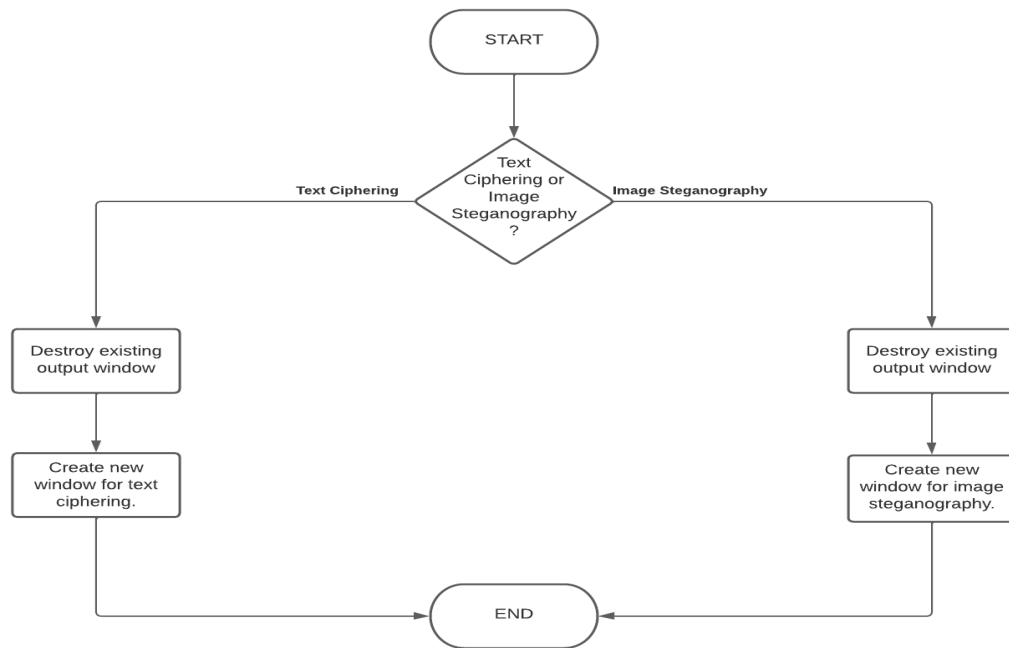
3.3 Algorithm and Process Design

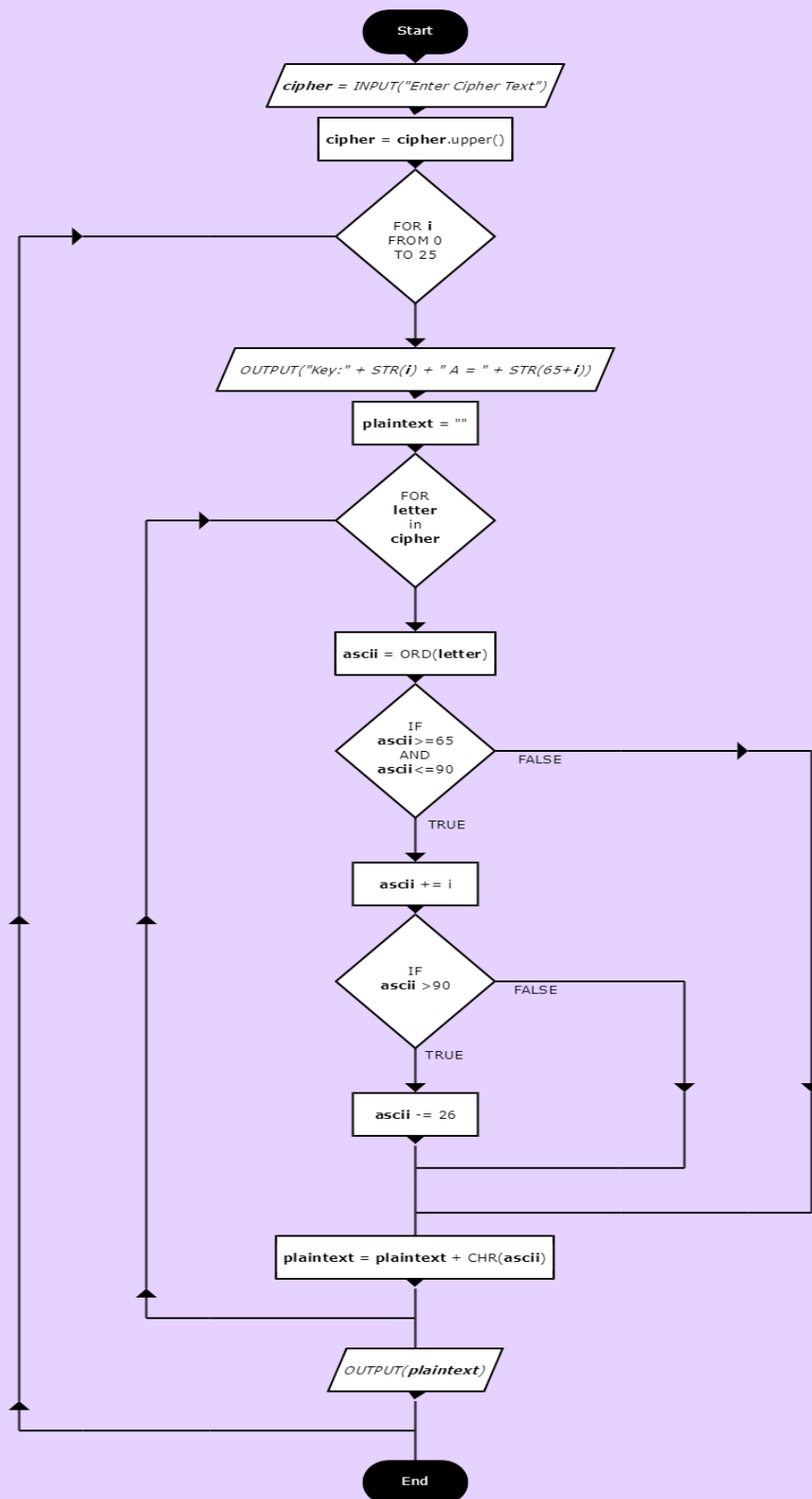
Algorithm

STEP 1 : START
STEP 2 : Initialize window.
STEP 3 : Enter name, key and message.
STEP 4 : Type 'e' to encrypt code in mode input field.
STEP 5 : Click on "Show Message" button for result.
STEP 6 : Copy the encrypted message.
STEP 7 : Click on "Reset" button.
STEP 8 : Now, Enter name, key, message and type 'd' to decrypt code.
STEP 9 : Click on "Show Message" button for result.
STEP 10 : Click on "Exit" button to exit program.
STEP 11 : STOP

STEP 1 : START
STEP 2 : Initialize window.
STEP 3 : Enter message and upload address of cover image.
STEP 4 : Type 'e' to encrypt code in mode input field.
STEP 5 : Click on "Go" button to encode.
STEP 6 : Now, upload the encoded cover image.
STEP 7 : Type 'd' to decrypt code in mode input field.
STEP 8 : Click on "Go" button.
STEP 9 : STOP

Process Design





3.4 Hardware & Software Requirements

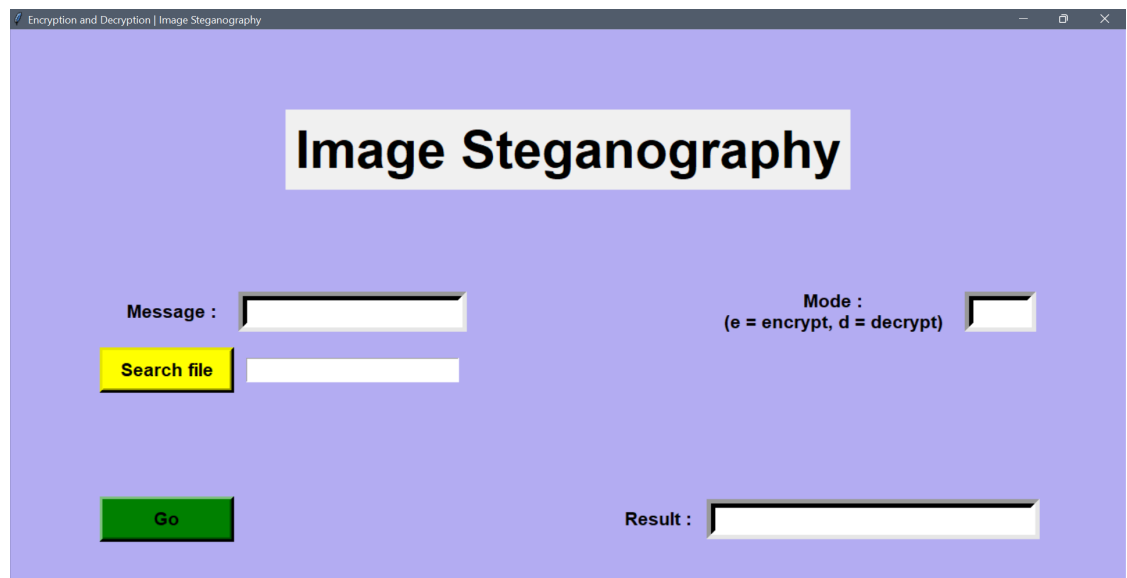
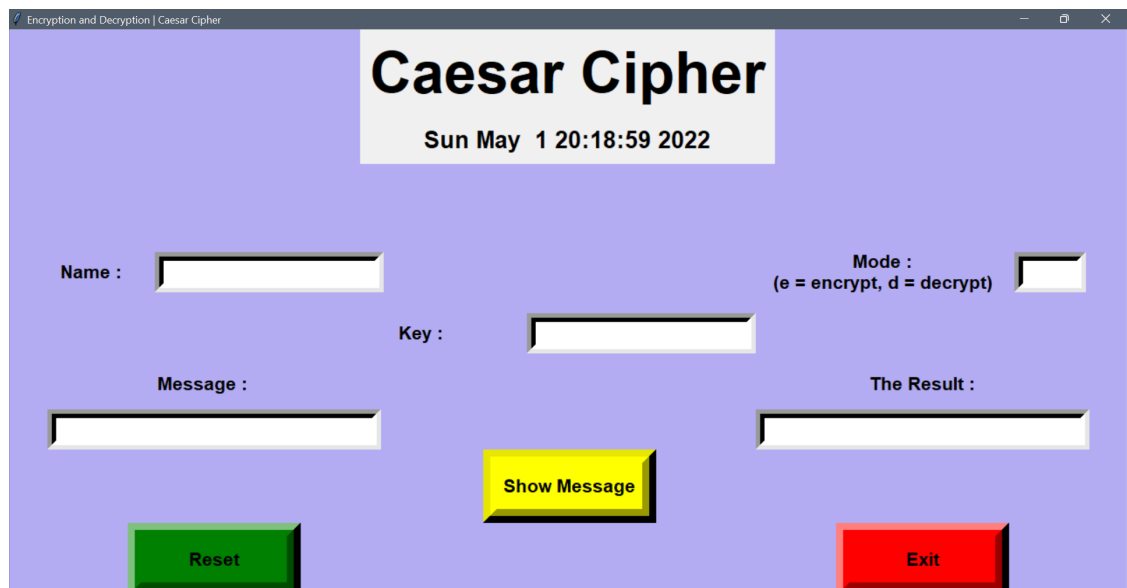
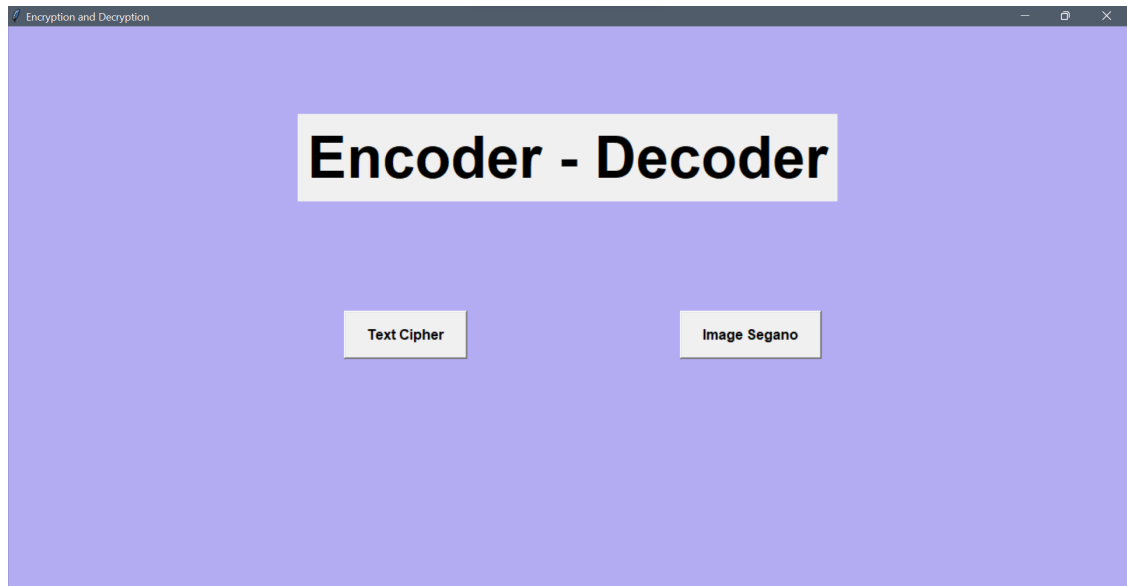
Hardware Requirements :

System :- intel core i3 (minimum)
hard disk :- 512 gb (minimum)
monitor :- standard led monitor
input devices :- keyboard
ram:- 4 gb and above
processor:- x32 and x64 bit.

Software Requirements :

Operating system :- windows 7 (min)
Programming language :- python
Code editor :- vs code / atom
Libraries used :- tkinter & stegano
Encrypting method :- caesar cipher & steganography

3.4 Experiment & Result



3.5 Conclusion and Future Scope

CONCLUSION

Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing. In today's world as Cyber Attacks have grown in large numbers there is a need to secure our data.

Thus, we have successfully developed an Encoder-Decoder project in Python. We used the popular tkinter library for rendering graphics on a display window and encoded - decoded using the Caesar Cipher method and Steganography. In this way, we can encode our message, images and decode the encoded message, image in a secure way by using the key.

FUTURE SCOPE

- More encoding cipher options could be added such as :
- **Advanced Encryption Standard (AES),**
- **Triple DES (Data Encryption Standard).**
- More secure and user oriented encryption can be done.
- It will be used in all purpose such as Internet banking, Sharing Personal details, Military & Defence connections and also identifying Terrorist threats, Securing your data in own devices more safely.

REFERENCES

1) Tkinter library:

- <https://docs.python.org/3/library/tkinter.html>
- https://www.tutorialspoint.com/python/python_gui_programming.htm#:~:text=Tkinter%20is%20the%20standard%20GUI,to%20the%20Tk%20GUI%20toolkit.&text=Import%20the%20Tkinter%20module

2) Cesar Cipher:

- https://en.wikipedia.org/wiki/Caesar_cipher
- https://cryptography.fandom.com/wiki/Caesar_cipher

3) Steganography:

- <https://en.wikipedia.org/wiki/Steganography>
- <https://www.techtarget.com/searchsecurity/definition/steganography>