**IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PROJECT REPORT**

***Submitted by***

Parth Galhotra(RA2111032010029)

Kumar Aniruddh Singh(RA2111032010032)

***Under the Guidance of***

Dr. Soumiya

**Assistant Professor, Department of Networking and Communications**

***In partial Satisfaction of the requirements for the degree of***

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND TECHNOLOGY

with specialization in Internet of Things



SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TCEHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY  
KATTANKULATHUR-603203

**NOVEMBER 2023**

**BONAFIDE**

This is to certify that this project titled “**Image Encryption and Decryption using AES Algorithm**” is the bonafide work of **Parth Galhotra(RA2111032010029)** and **Kumar Aniruddh Singh(RA2111032010032)** who undertook the task of completing the project within the allotted time.

**Signature of the Guide** **Signature of the II Year Academic Advisor**

Dr. Soumiya \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Assistant Professor** **Professor and Head**

Department of NWC Department of NWC

SRM Institute of Science and Technology SRM Institute of Science and Technology

# Abstract

Now a day the use of devices such as computer, mobile and many more other devices for communication as well as for data storage and transmission has increased. As a result, there is increase in number of users. Along with these users, there is also increase in number of unauthorized users which are trying to access a data by unfair means. This arises the problem of data security. Images are sent over an insecure transmission channel from different sources, some image data contains secret data, some images itself are highly confidential hence, securing them from any attack is essentially required.

To solve this problem, we are using AES algorithm for encrypting and decrypting image. This encrypted data is unreadable to the unauthorized user. This encrypted data can be sent over network and can be decrypted using AES at the receiving end. Hence it ensures secure transmission of image.

# Aim of the project

The project aims to develop a secure transfer of images between sender and receiver. Image should be encrypted before it is sent on a network and it should be correctly decrypted on the receiver side.

# Objective of the project

* Encryption of an Image to unreadable format
* Decryption of encrypted image to original image
* Secure transfer of an image over the network such as internet
* Ensure no modifications are made while transferring over the network.

# Scope of the project

**Product scope**

The project works by encrypting the given image using AES algorithm so that this image can be sent securely over the network. At the receiver side, the receiver has code for decrypting the image so that he can get the original image. This helps in sending confidential and sensitive information securely over the internet. Main application of this can be very helpful in medical and military fields.

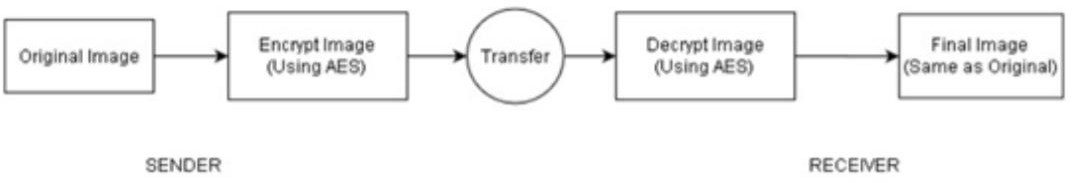


Figure 1

**Design and Implementation constraints**

* + Python must be used for front end
  + Encryption and Decryption should be done using AES algorithm
  + Original Image must be in .jpeg/.png format.

**Assumptions and Dependencies**

* + Sender and Receiver are connected on a network

# Functional Requirements

* The system shall encrypt the given image to an unreadable format. This is done using AES encryption function.
* The system shall decrypt the received encrypted image to a readable format. This is done using AES decryption function. The output image should be same as the original image.
* The system ensures that the image is securely sent over any transmission medium. Third party system cannot make modifications to the file being sent since unauthorised access is not supported.

# Non-Functional Requirements

**Performance Requirements**

* + For smooth & efficient encryption, image size must be less than 5MB.
  + Decryption should not take more than 10 seconds.

**Safety and Security Requirements**

* + If the decryption takes more than 10 seconds, then discard the message (because the message might have been corrupted during transmission) and ask sender to re-send it.
  + Encryption is done using encryption key. Decryption will happen only when same encryption key is used at the receiver side.

**Software Quality Attributes**

## Reliability

External factors do not affect the system. AES algorithm is universally accepted and generates consistent results therefore there are very less chances of errors. Error can occur only if there is a transmission glitch (the probability of which is very rare). So, the system is reliable.

## Usability

It uses python based GUI which is user friendly and provides buttons for easy navigation. A person with basic understanding of computer can easily use this software for encrypting/decrypting image using key.

## Testability

The system is easy to test and find defects. The system is divided into different modules performing specific functions that can be tested individually.

# External Interface Requirements

**User Interfaces**

The interface window gives us a box for entering the location of image. Along with this box, it also contains two buttons for encoding and decoding the image. After clicking on one of these button, next window has a textbox to enter the password and a submit button. After submitting, it shows the filename of new image file generated.

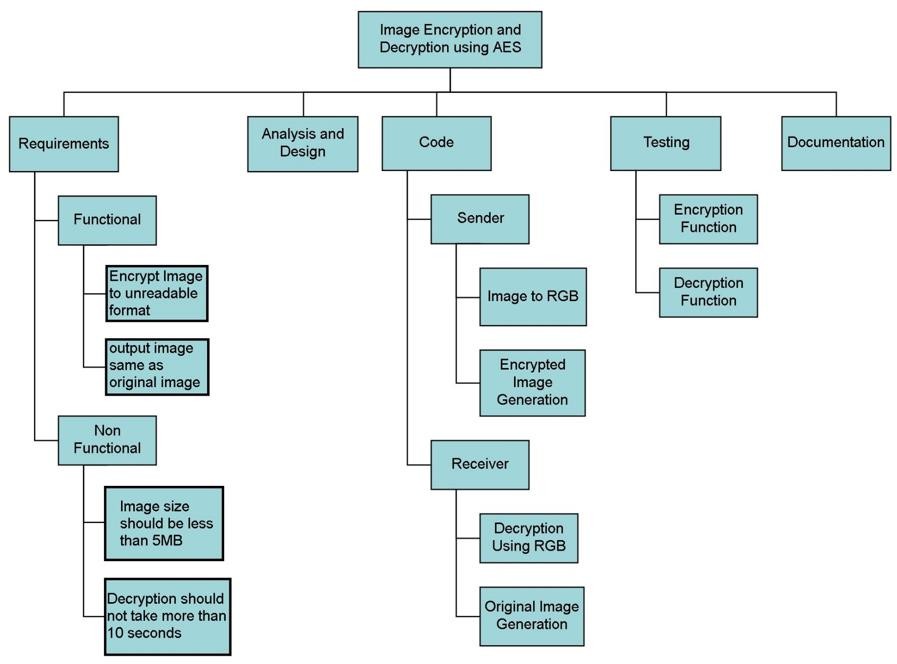
**Hardware Interfaces**

* + Sender Computer: for seeing the original and encrypted image
  + Receiver Computer: for seeing the decrypted image

**Software Interfaces**

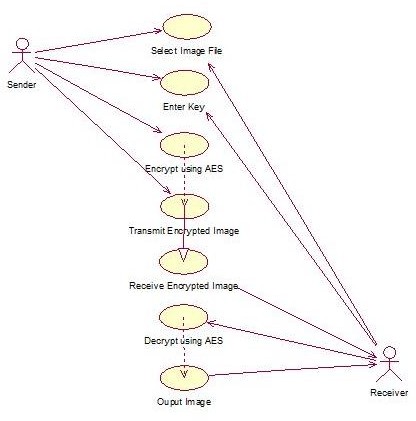
We have frontend made using python module named Tkinter(). This provides an interactive window for the user. The user need to provide the location of the image to be encoded/decoded. After this, user can either go for encoding or decoding the image. It asks for a password, which is basically your encryption key. After these details are entered, we use the python functions declared in the code to encode/decode the image using AES file from crypto.cypher module of python. When this process is done, the user will get encrypted/decrypted image as output which will be saved in the same directory as input image file.

# Work Breakdown Structure

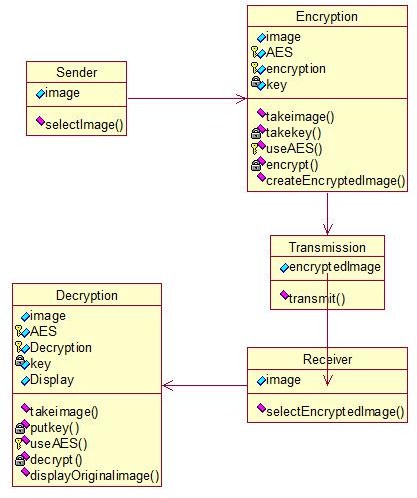


**Design Diagrams**

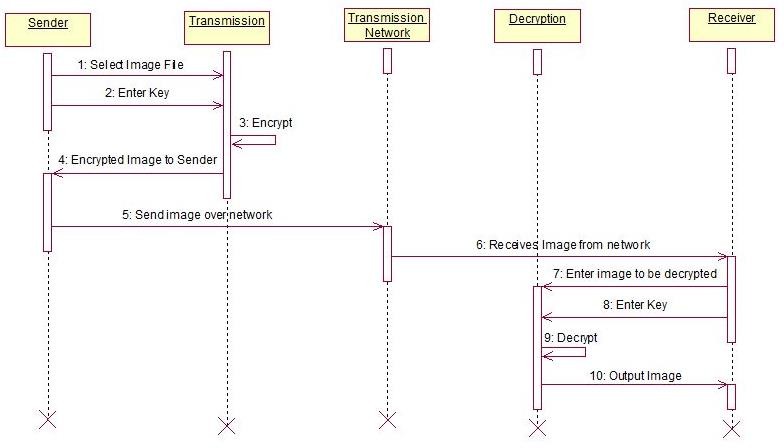
**Usecase Diagram:**



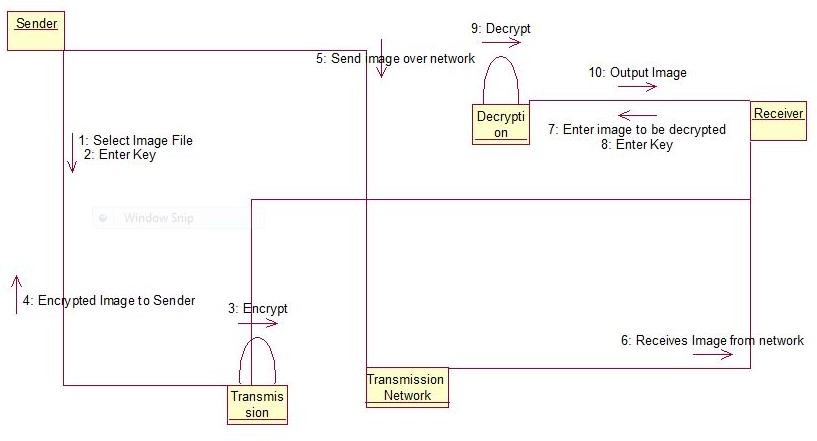
**Class Diagram:**



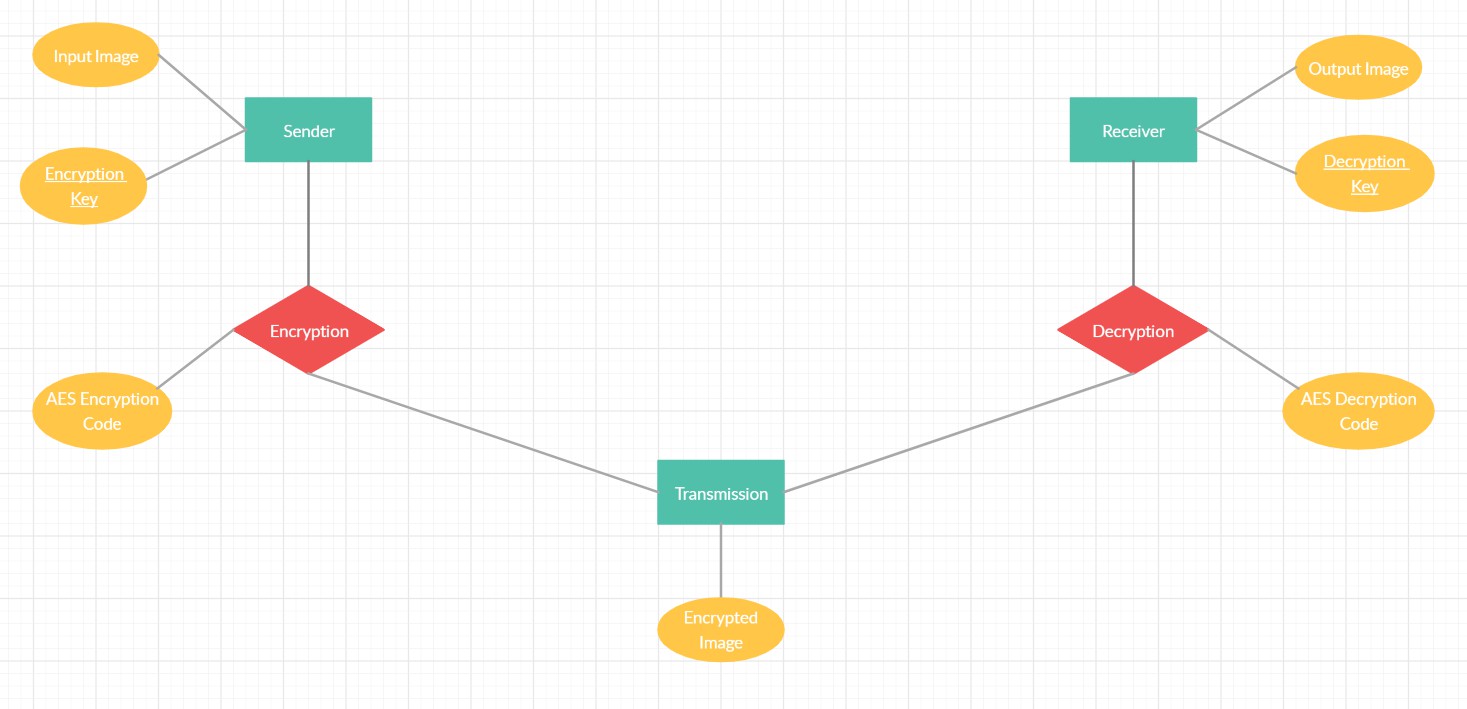
**Sequence Diagram:**



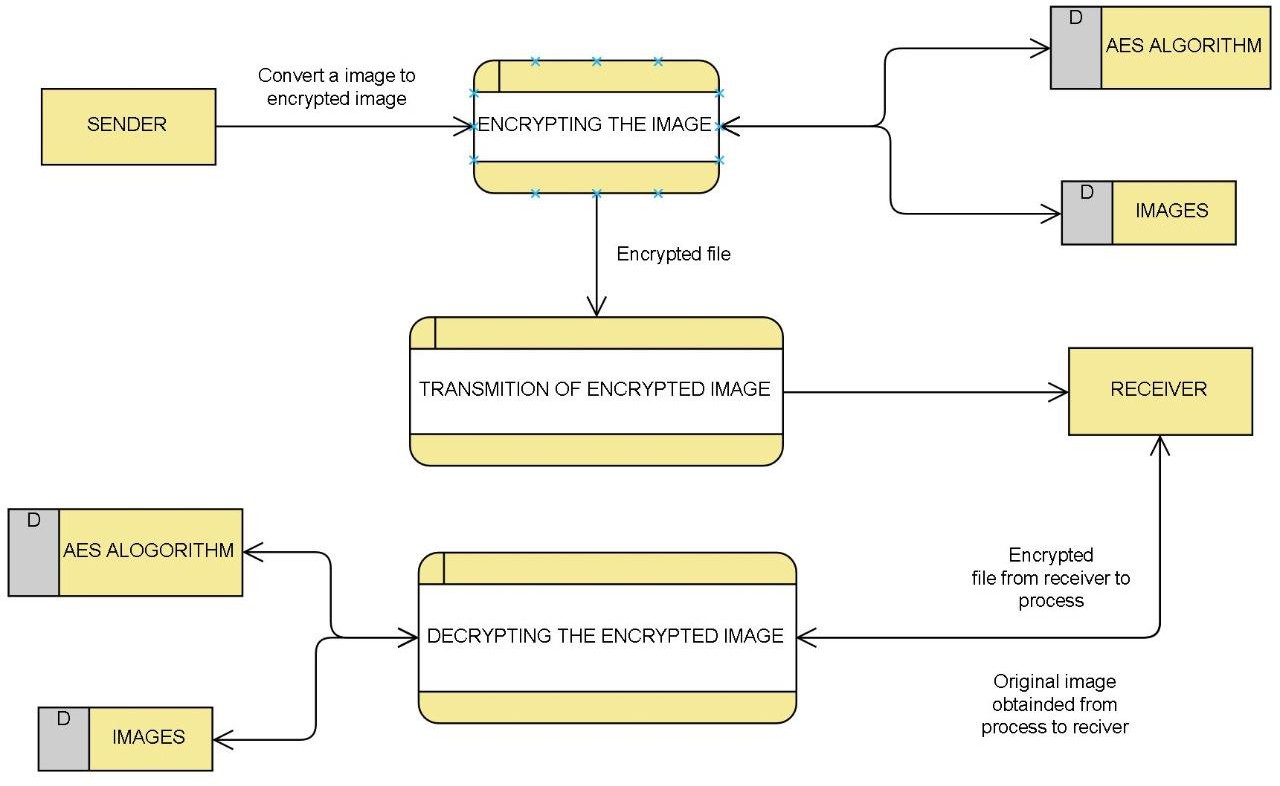
**Collaboration Diagram:**

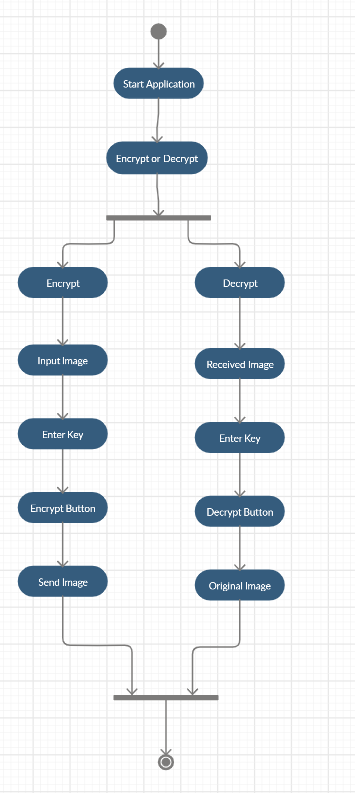


**ER Diagram:**

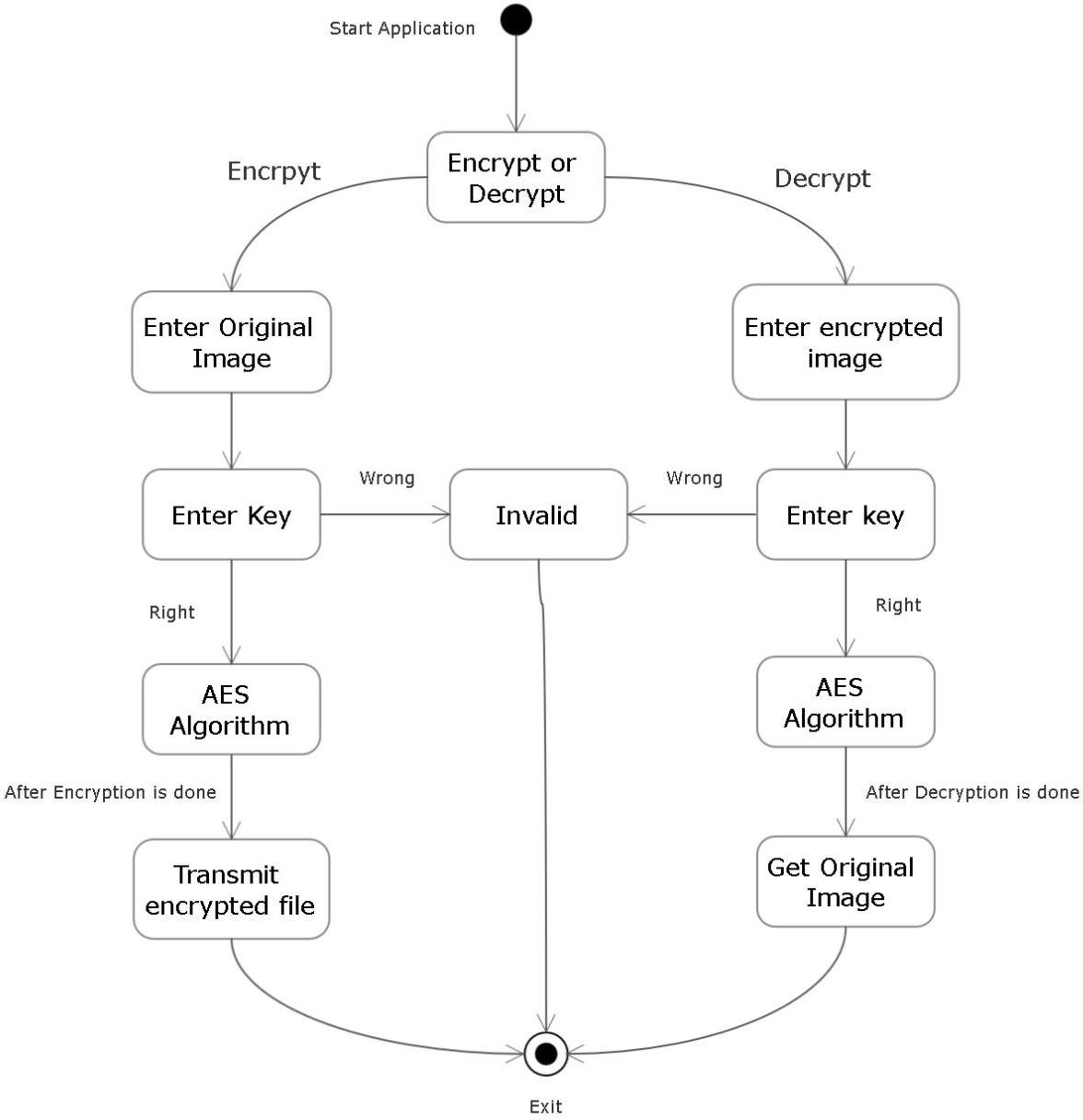


**Dataflow Diagram:**



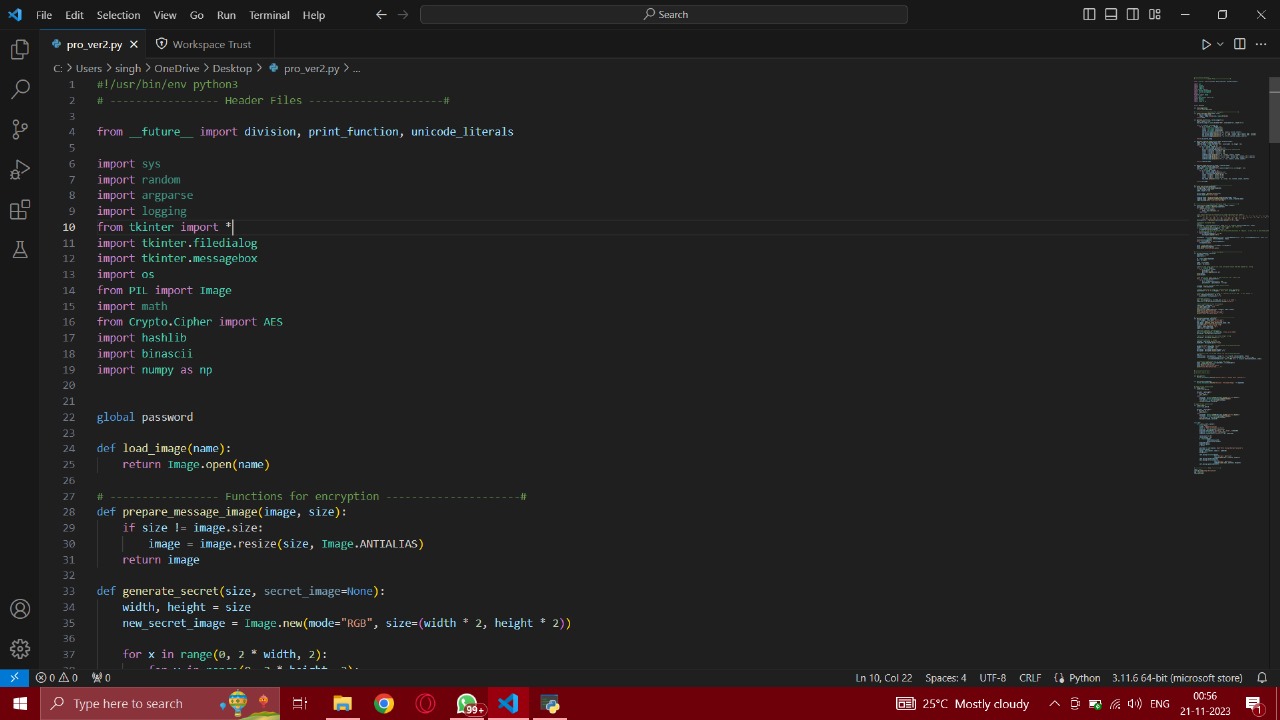
**Activity Diagram:**

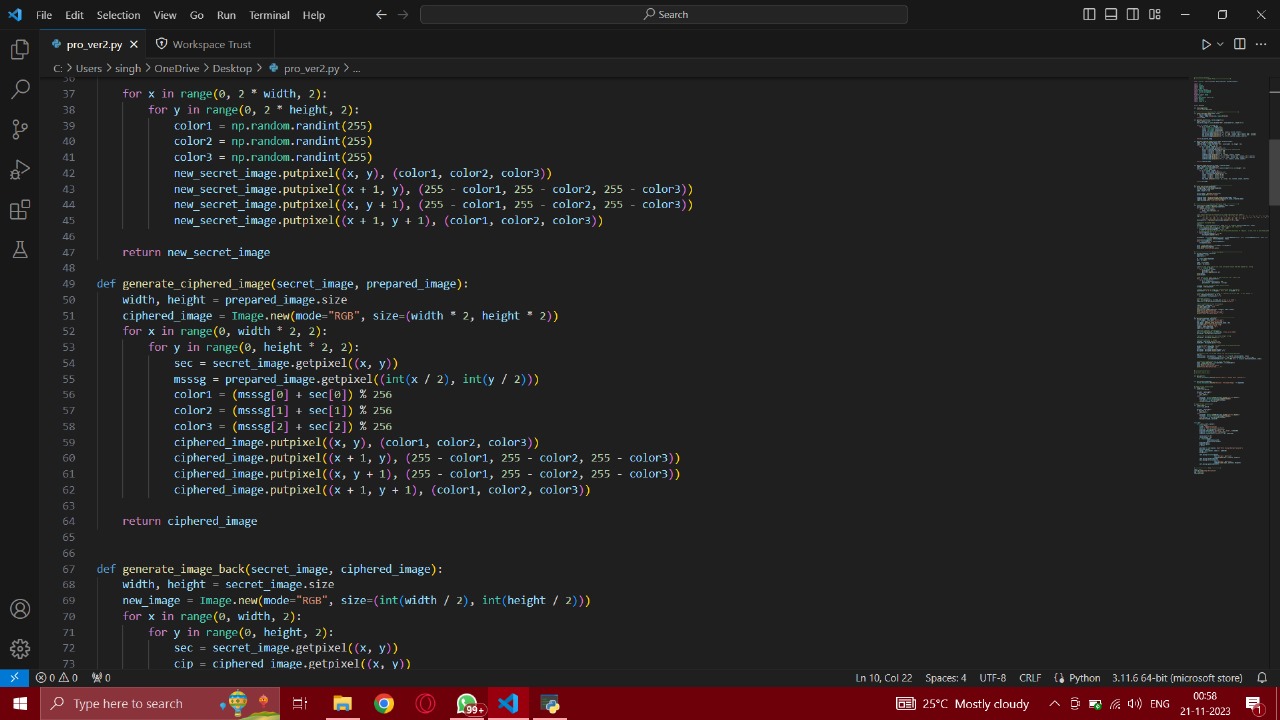
**State Chart Diagram:**

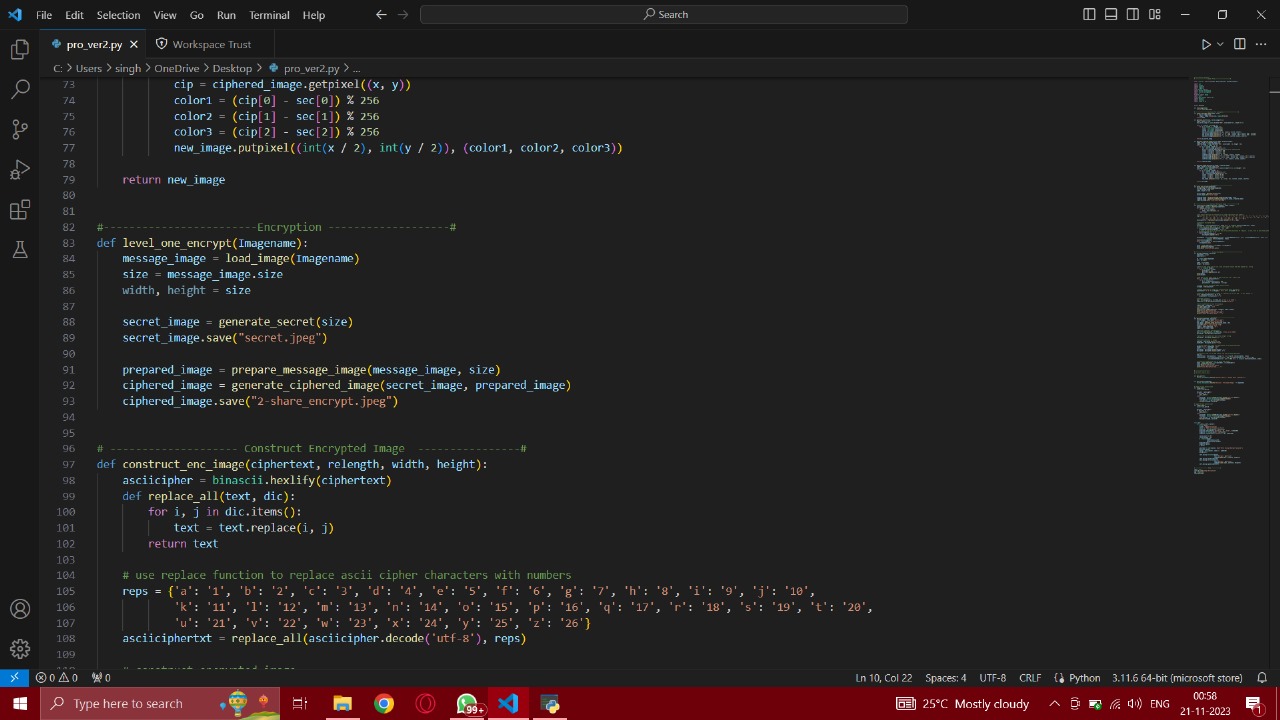


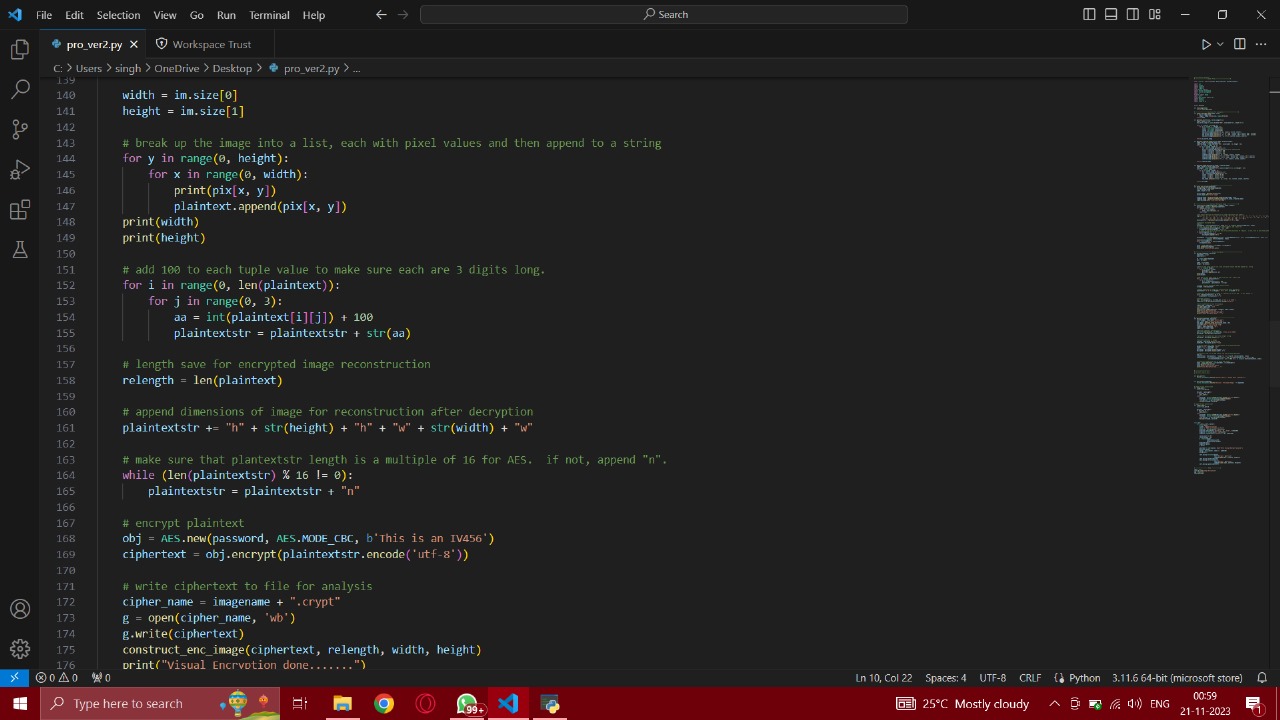
# Screenshot of Implementation

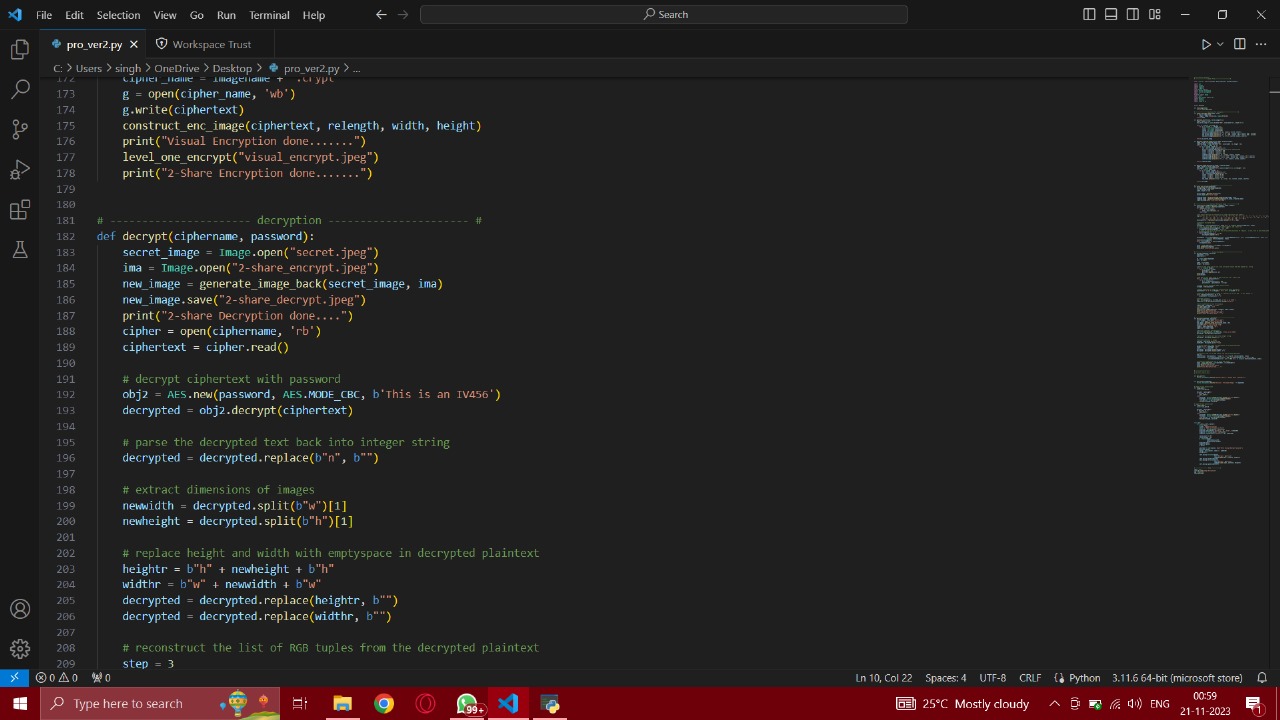
**Code**

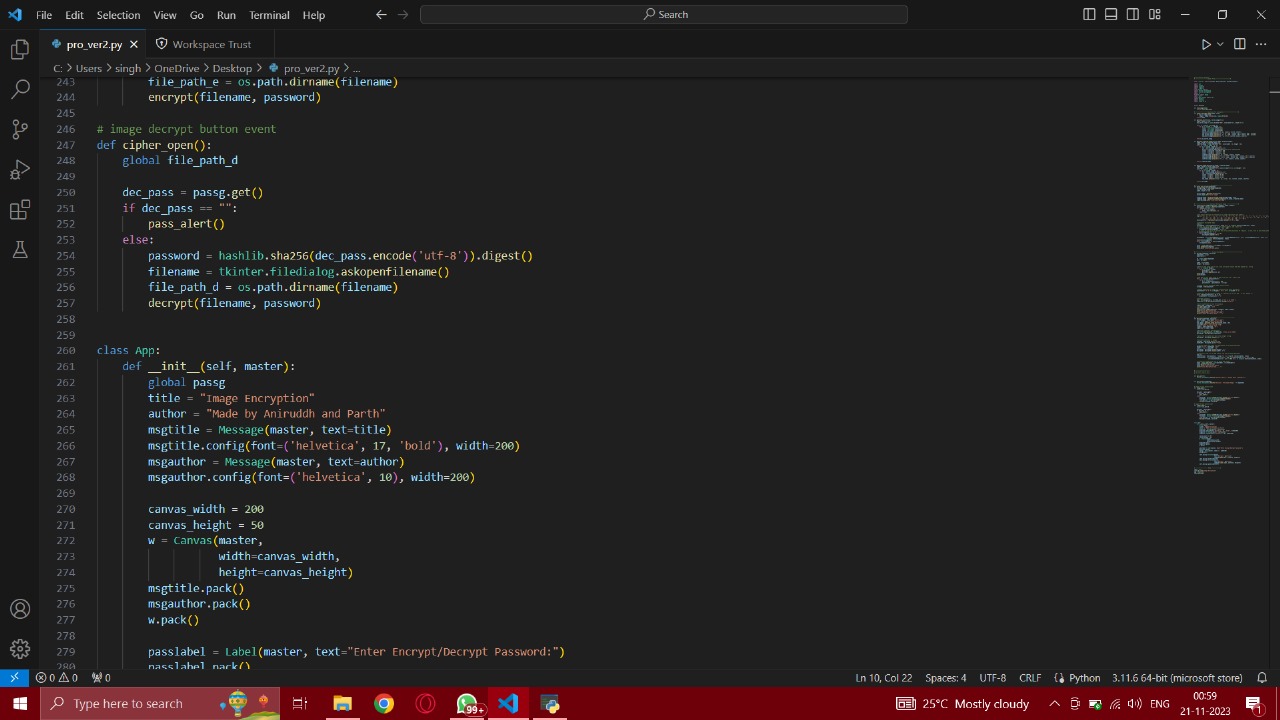
****

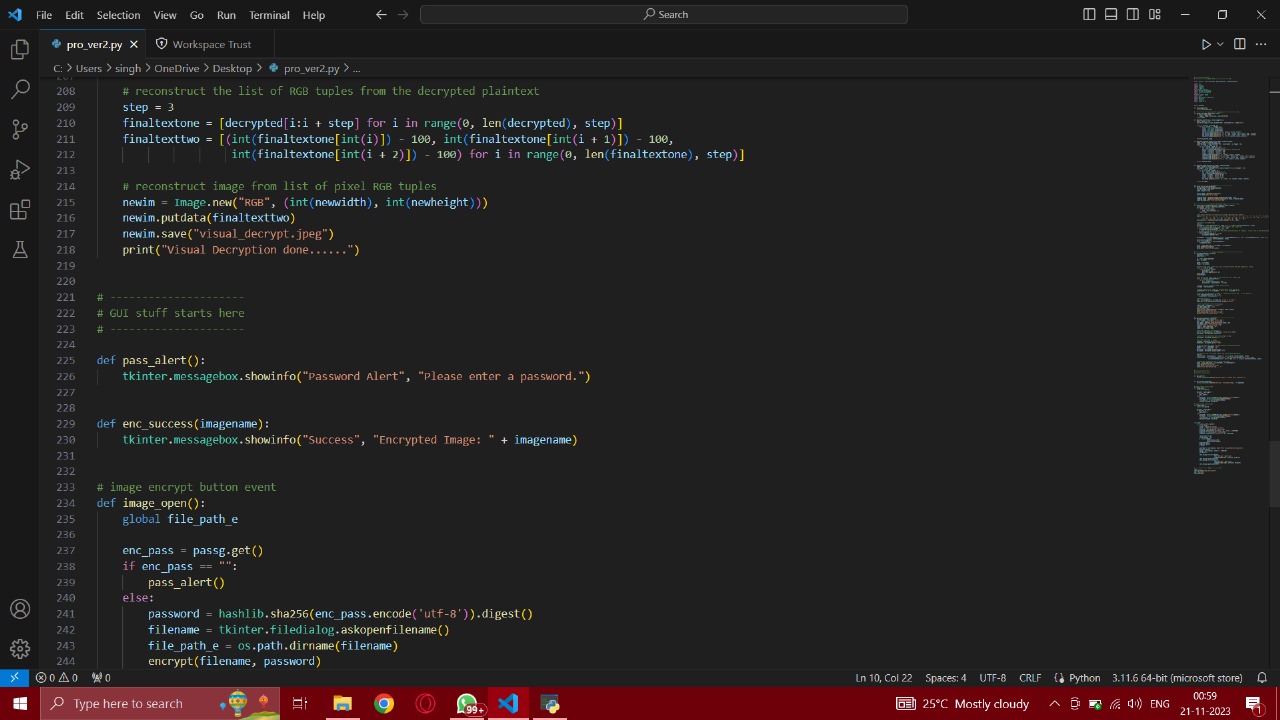
****

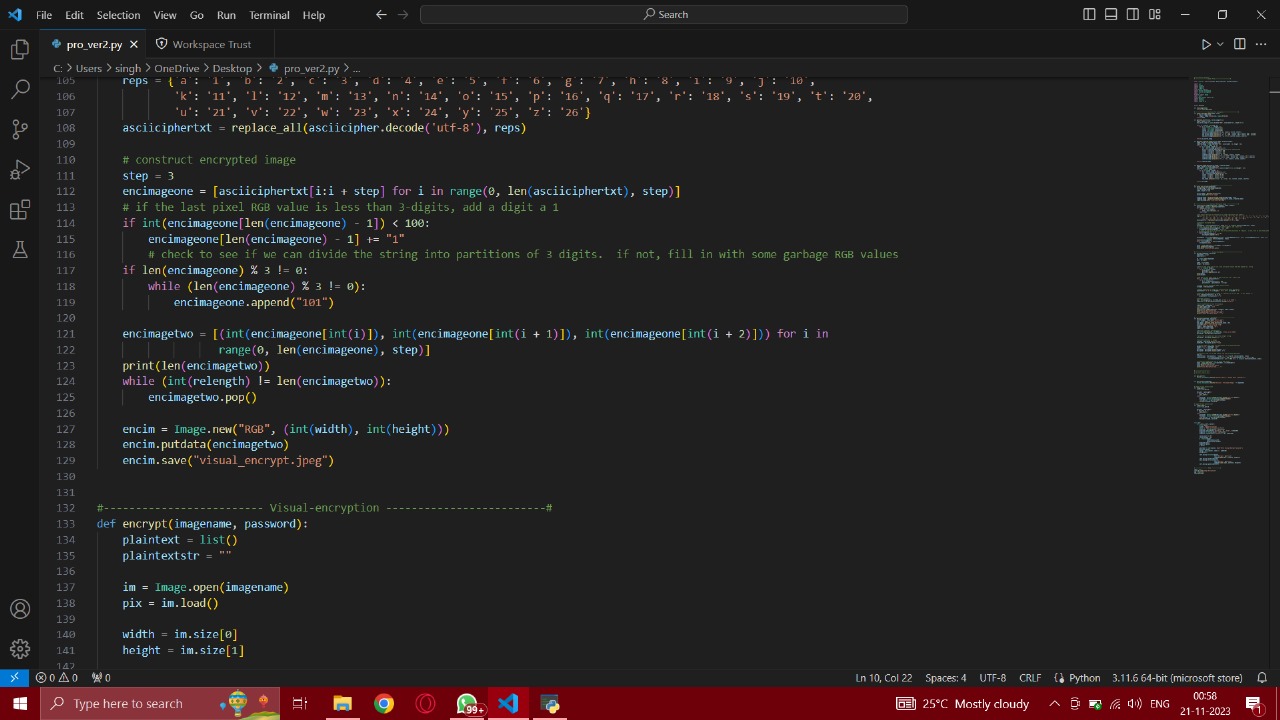
****

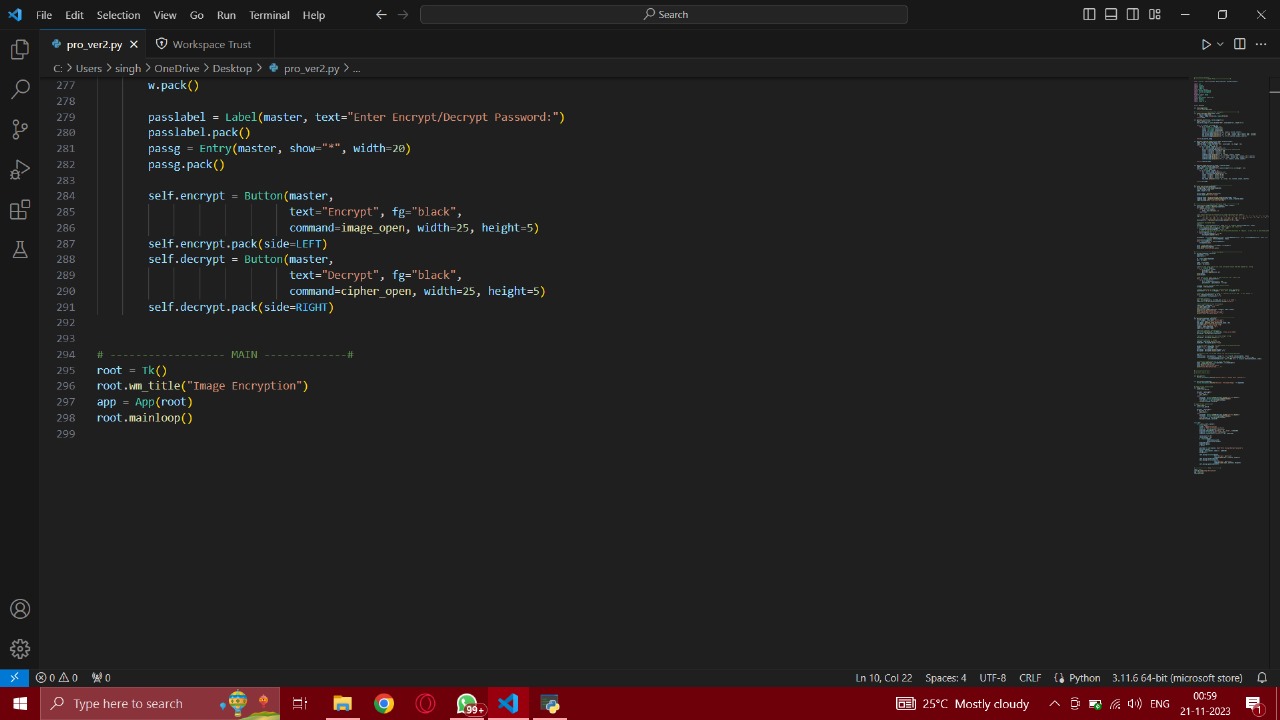
****

****

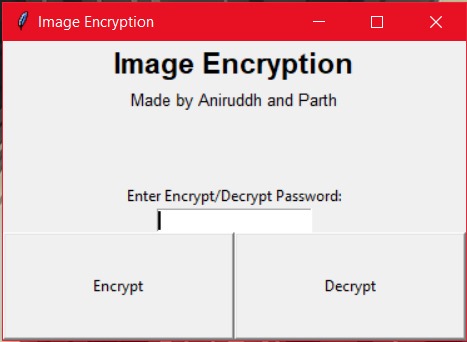
****

****

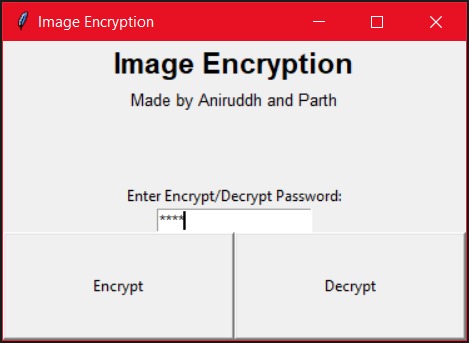
****

****

**Application’s first screen asking for key:**

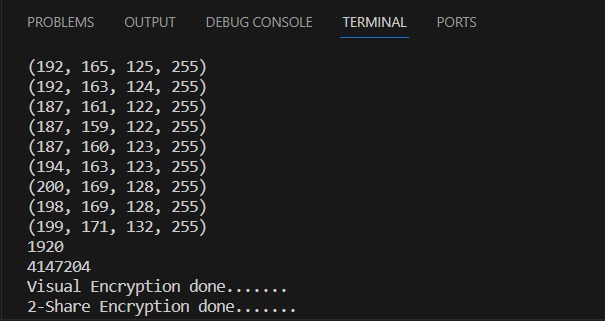
****

**Key is entered:**



**After clicking Encrypt button:**

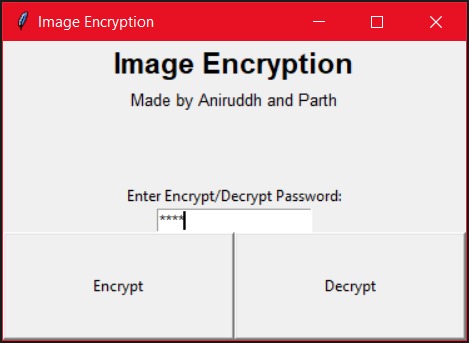
Select the directory and then the original file to be encrypted



The Encryption is completed and a file named ‘images.jpeg.crypt’ is created.

This is our Encrypted file.

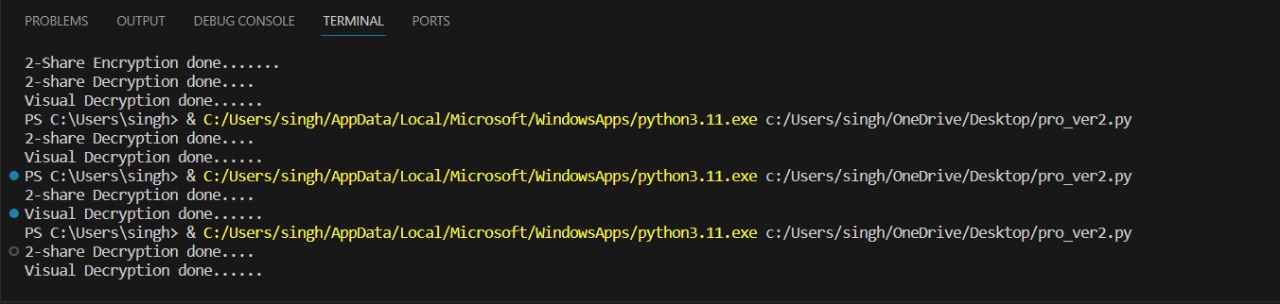
**For decryption, enter same key:**

****

**After clicking decryption button:**

Select the same directory and then select the file named ‘images.jpeg.crypt

**Terminal and desktop screen after clicking ‘open’:**

****

Decryption is complete and file named ‘visual\_decrypt.jpeg’ is the decrypted file

**Conclusion**

We have successfully developed a program that encrypts and decrypts the image files accurately. This will help in minimizing the problem of data theft and leaks of other sensitive information. The file that we obtained after encryption is very safe and no one can steal data from this file. So, this file can be sent on a network without worrying. Our developed solution is a small contribution that can be very helpful for military or medical fields in future times.