CYBER SECURITY & DIGITAL FORENSICS

Image Encryption and Decryption Using AES Algorithm

Name: Abdul Ghafoor
Roll No: S25BINCE1M04017
Degree Program: BS Cyber Security & Digital Forensics
Course Name: Cryptography
Instructor: Asjad Amin
University: The Islamia University of Bahawalpur

Submission Date: 30th December 2025

Abstract

Now a day the use of devices such as computers, mobile phones and many more other devices for communication as well as for data storage and transmission has increased. As a result, there is an increase in the number of users. Along with these users, there is also an increase in the number of unauthorized users which are trying to access data by unfair means. This arises from 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 the AES algorithm for encrypting and decrypting images. 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 images.

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

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.

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.

Tools and Technologies Used

• Python Programming Language
• Visual Studio Code
• PyCrypto Library
• Python Imaging Library (PIL)
• MacOS Operating System.

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 buttons, 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 NEEDS 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.

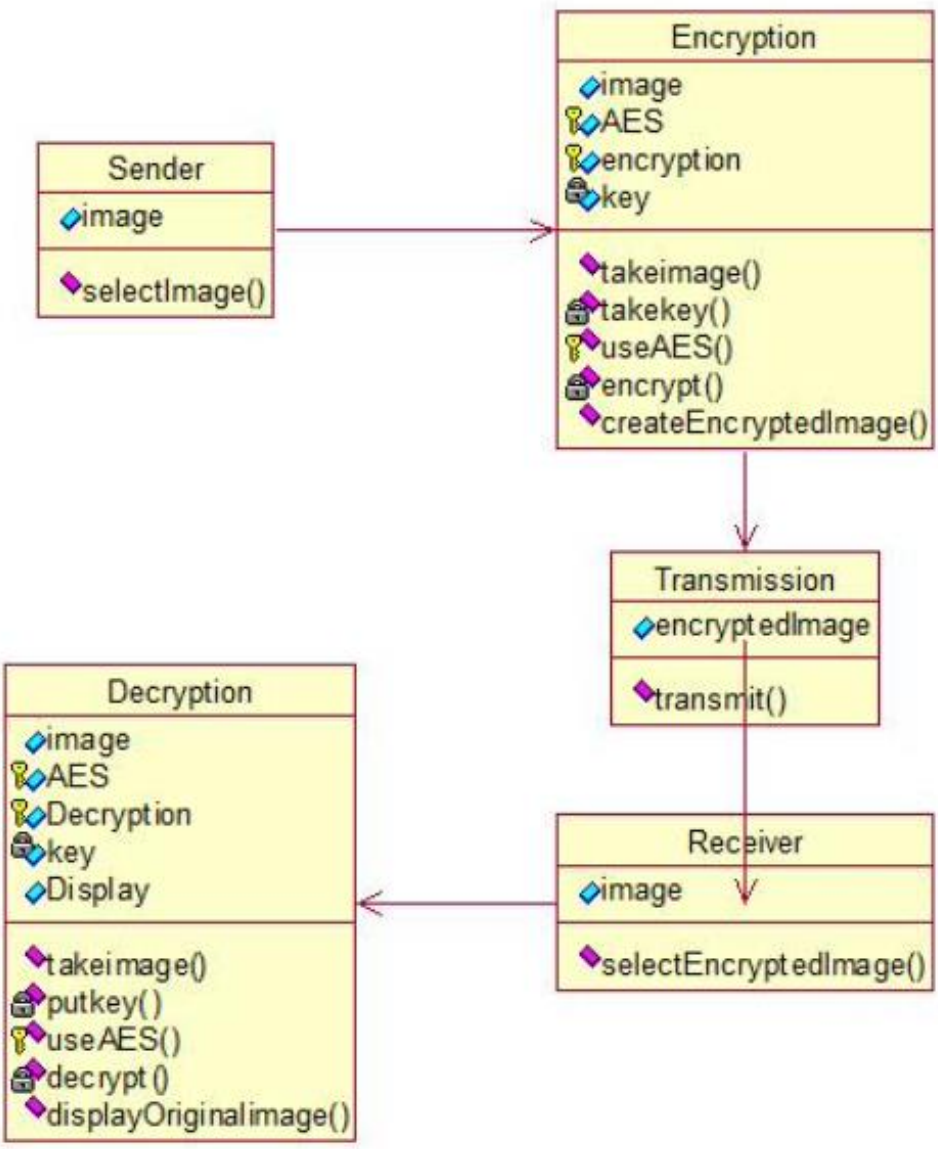
Implementation Overview

In Python, the image is read and converted into bytes. AES encryption is applied using a secret key. The encrypted output is saved as an encrypted image file. During decryption, the same key is used to convert the encrypted data back into its original image format. Only authorized users with the correct key can decrypt the image.

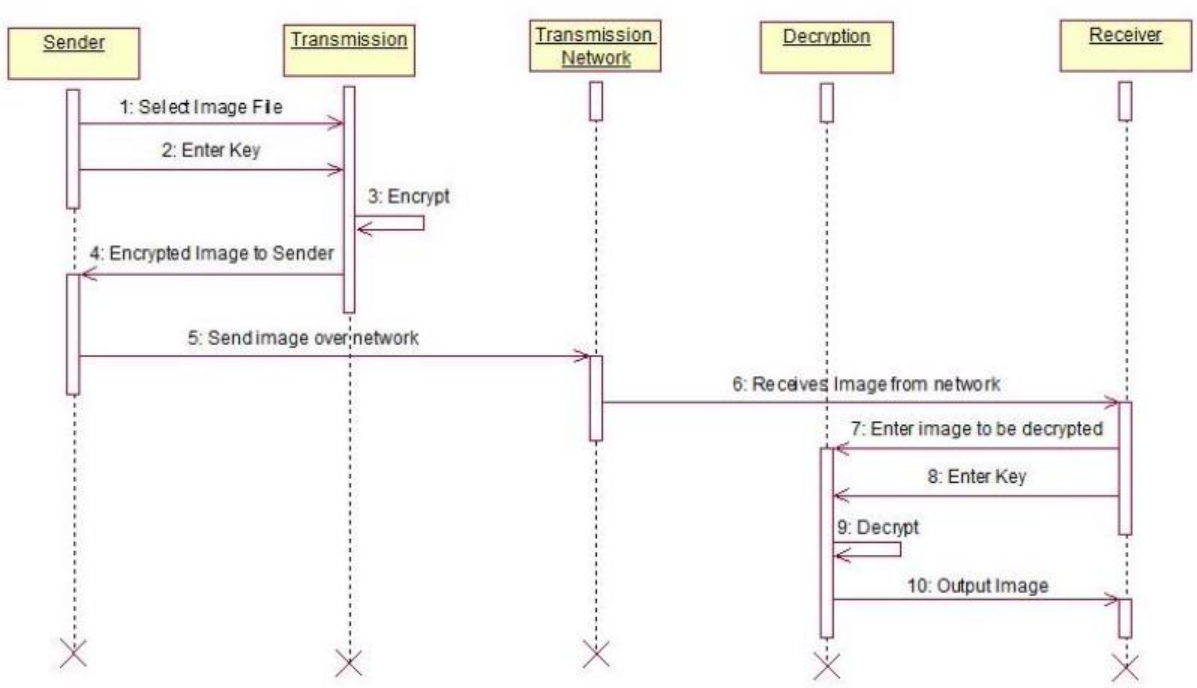
Results and Discussion

The project successfully encrypts the input image into an unreadable form. The encrypted image does not reveal any visual information. After applying the correct AES key, the original image is restored without any data loss. This proves the effectiveness and reliability of AES for image security.

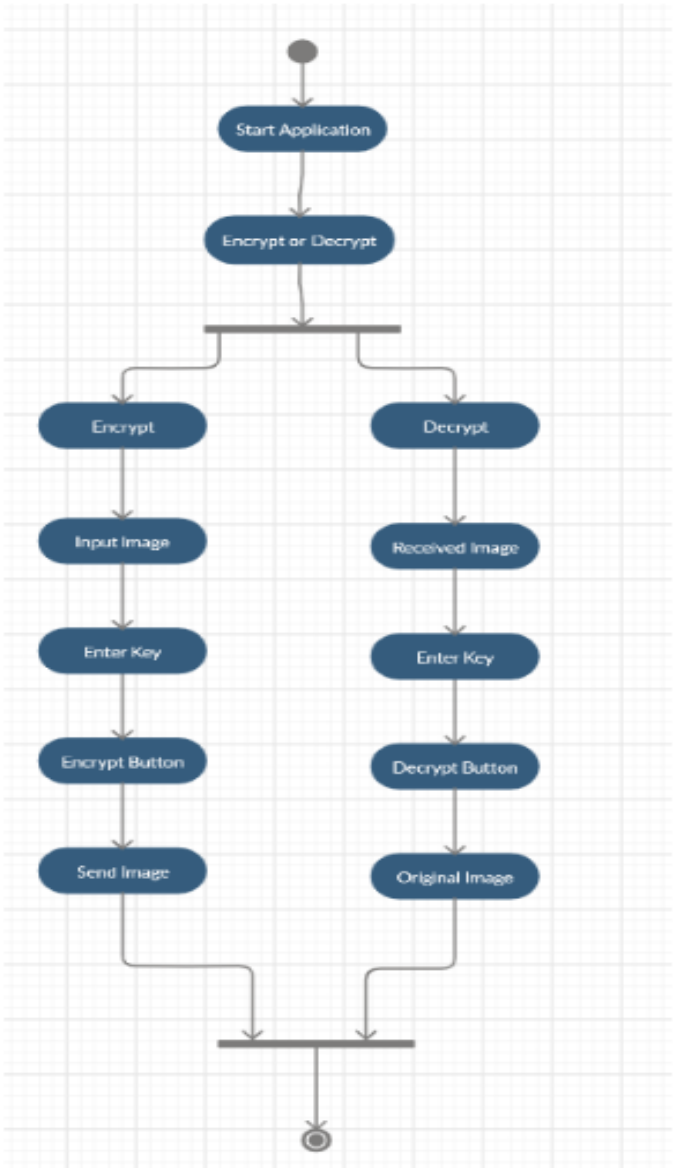
Working Diagram:



Data Flow Diagram

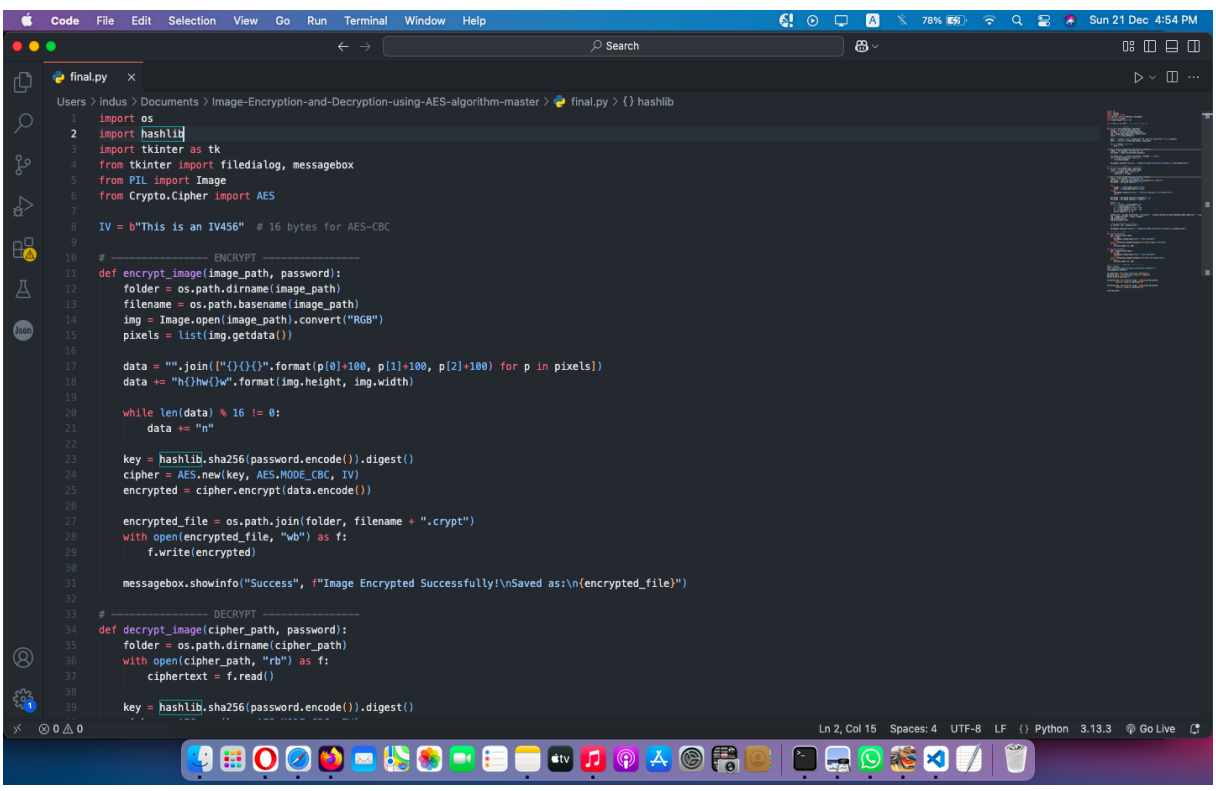


Activity Diagram

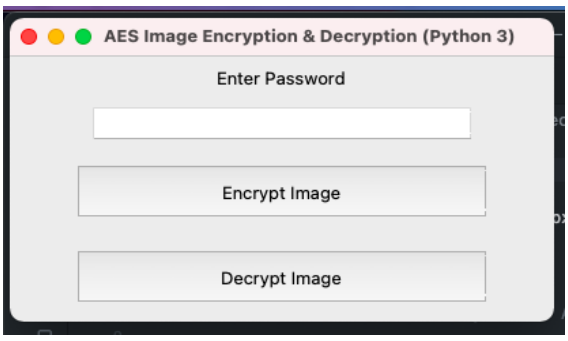


Screenshot of implementation

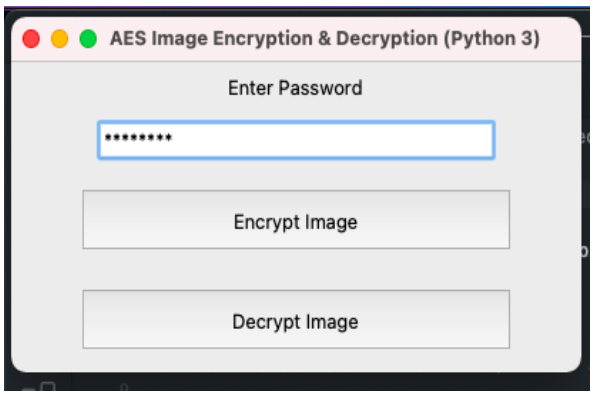
CODE



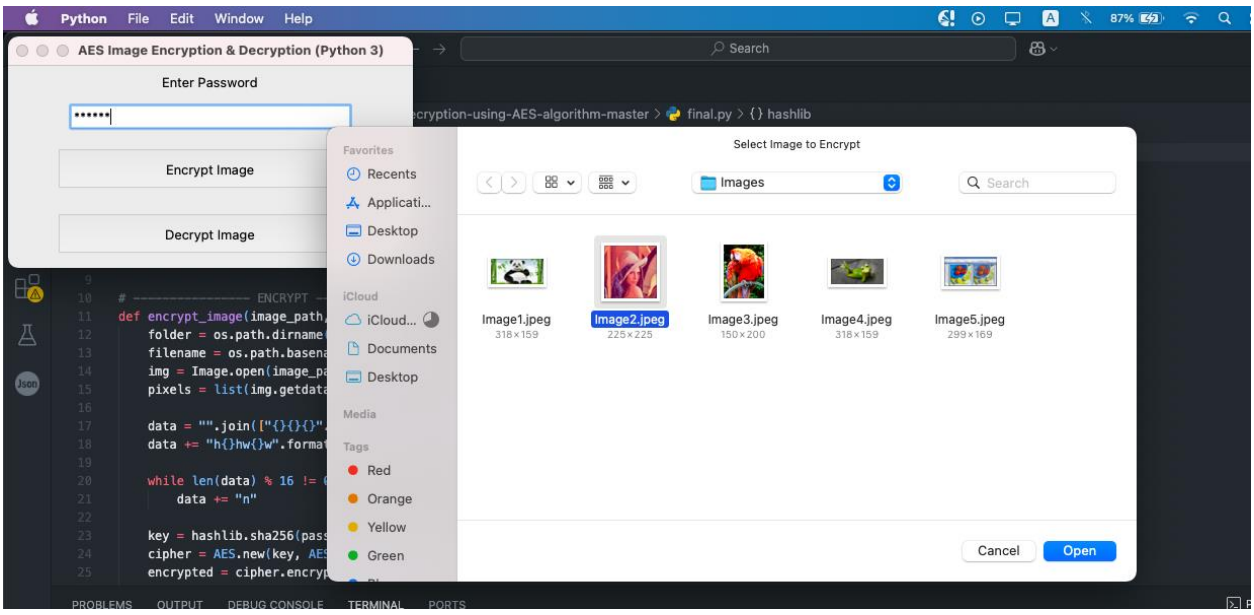
Step 1: Screen open



Step 2: Enter key

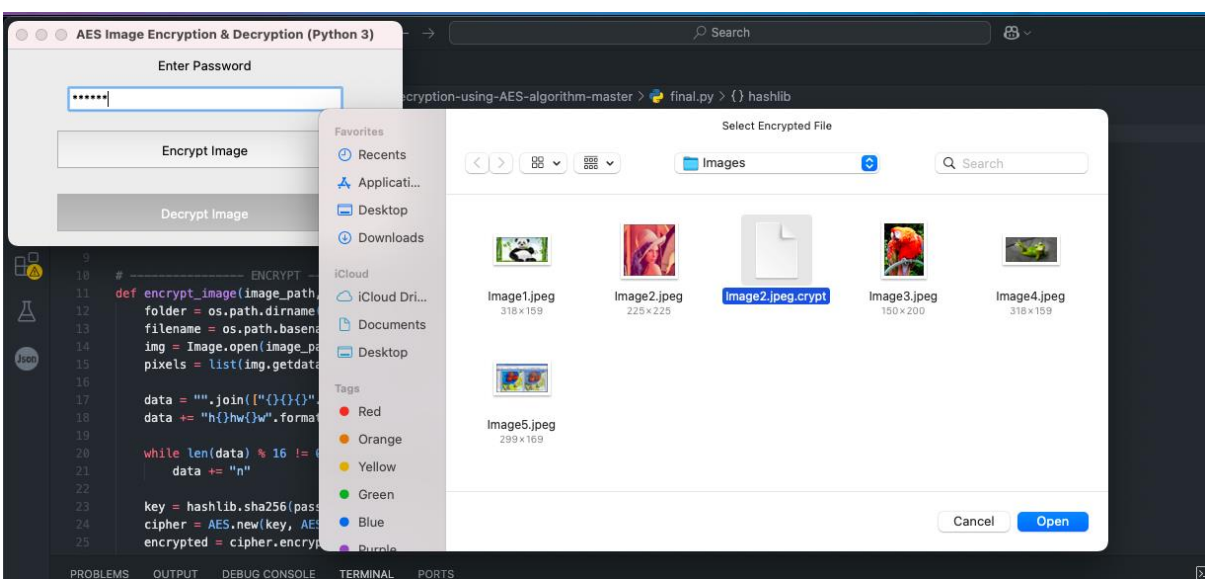


Step 3: Select Picture for Encryption

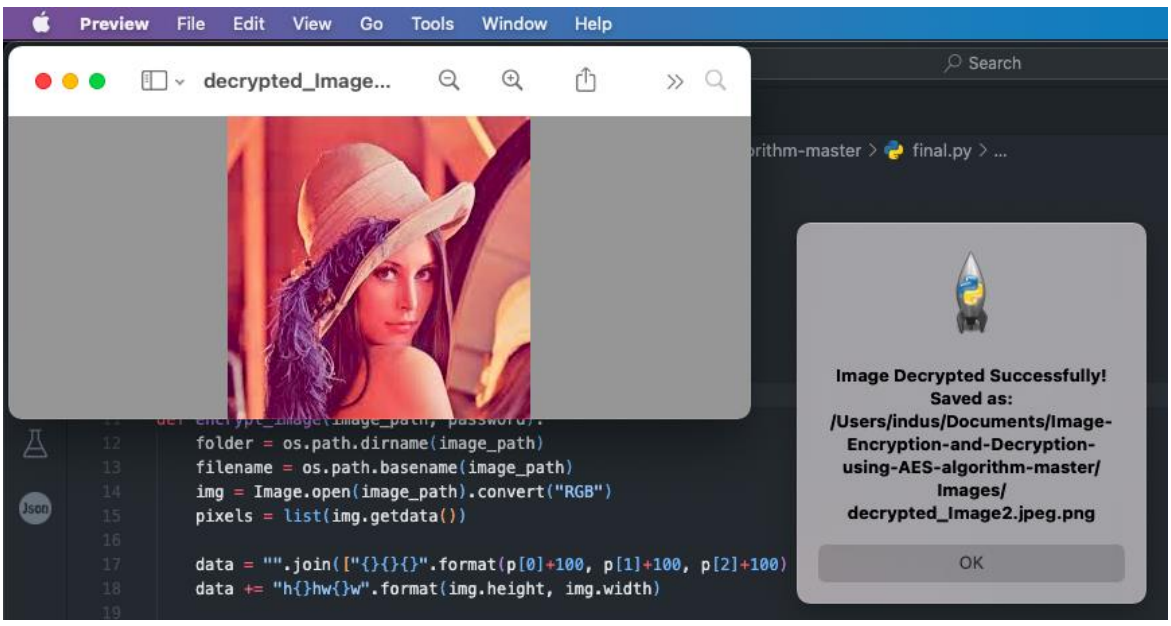


Hence Picture Encrypted successfully

Now Decrypt the image using same key



Hence image Decrypted successfully



Conclusion

We have successfully developed a program that encrypts and decrypts the image files accurately. This will help in minimising 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

THE END