

APPENDIX 1

**I.V.A. Message Security
(STEGANOGRAPHY USING PYTHON)**

END TERM REPORT

by

ISHIKA AGGARWAL

(Section: __K19PV__)

(Roll Number(s): __A-23__)

(Registration Number(s): __11904047__)

VIKRAM SHARMA

(Section: __K19PV__)

(Roll Number(s): __B-51__)

(Registration Number(s): __11908980__)

KUMAR ARMAN SIKRIWAL

(Section: __K19PV__)

(Roll Number(s): __B-47__)

(Registration Number(s): __11910423__)



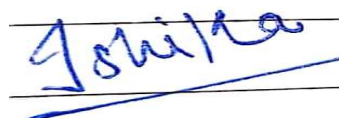
**Department of Intelligent Systems,
School of Computer Science Engineering,
Lovely Professional University, Jalandhar**

November, 2020

APPENDIX 2

STUDENT DECLARATION

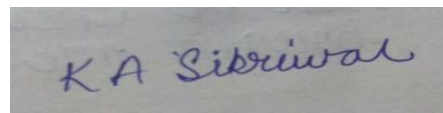
This is to declare that this report has been written by me/us. No part of the report is copied from other sources. All information included from other sources have been duly acknowledged. I/We aver that if any part of the report is found to be copied, I/we are shall take full responsibility for it.



Ishika Aggarwal
Roll number: _A-23__



Vikram Sharma
Roll number: _B-51__



Kumar Arman Sikriwal
Roll number: _B-47__

29- November- 2020
Jalandhar

APPENDIX 3
(A typical specimen of table of contents)

TABLE OF CONTENTS

TITLE	PAGE NO.
1. Background and objectives of project assigned	5
1.1 Introduction.....	5
1.2 Objective.....	6
1.3 Proposed System.....	6
1.4 Motivation and Outcomes.....	7
2. Description Of Project.....	8
3. Work Division.....	11
4. Implementation of the project	12
5. Technology used.....	14
6. SWOT Analysis.....	15
7. Bibliography.....	16

APPENDIX 4

BONAFIDE CERTIFICATE

Certified that this project report “I.V.A Message Security” is the bonafide work of “ISHIKA AGGARWAL, VIKRAM SHARMA and KUMAR ARMAN SIKRIWAL” who carried out the project work under my supervision.

<<Signature of the Supervisor>>

(Due to Covid 19, signature is exempted)

<<Name of supervisor>>

<<Academic Designation>>

<<ID of Supervisor>>

<<Department of Supervisor>>

1. BACKGROUND

1.1 Introduction

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.

Steganography can be defined as the science of hiding the data like file, image, video or any message to the other file, image, video or message. In Steganography the useless bits are actually replaced by the useful bits in order to hide the required file into any of the files or data mentioned above. It plays a vital role in cybersecurity by allowing the legitimate users or peers to send the data in a way which is highly secured so that it could be protected from the hacker or malicious users who are intended to harm or abuse the system. It can be done using software that is available in the market for free or paid.

Steganography can also be considered as the practice of concealing the crucial data into any of the files so that it could be transmitted securely. The applications like SteganPEG, OpenStego and so on are used to fulfill the purpose of wrapping up one file into another. The applications used for Steganography hide the bits of the required file into another file in a manner so that the original file doesn't lose its characteristics. It can be considered pretty more secure than encryption or hashing as in these cases the attacker can sniff at least the junks but in the case of Steganography, they won't be able to detect if anything important has been transmitted. It is usually applied at a place where the data has to be sent secretly.

The idea behind image-based Steganography is very simple. Images are composed of digital data (pixels), which describes what's inside the picture, usually the colours of all the pixels. Since we know every image is made up of pixels and every pixel contains 3-values (red, green, blue).

Basic concepts of Pixel and colour models:

Pixels are the smallest individual element of an image. So, each pixel represents a part of the original image. It means, higher the pixel-higher or much accurate representations of the actual picture.

- In a black and white image (not greyscale), black pixel has a value 1 and a white pixel as a value of 0.

- In coloured images, they have three main colour components (RGB- Red, Green, Blue), with pixel values of 0-255 for each pixel. So, a pixel of (255, 255, 255) will represent a white and (0,0,0) means black.
- As the maximum number an 8-bit binary number can represent 255, is the maximum number we can go.

Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image.

Text Steganography

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts.

1.2 Objective

The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages.

The aim of this project is to:

- A. Input of the hidden message from the user that user wants to keep hidden using a security key and perform operations like encryption and decryption.
- B. Encrypt the message from the user into either a file or an image.
- C. Decrypt the message from either the file or image in which the message is hidden and show it to the user as output.

1.3 Proposed System

The application has a simple interface that lets the user submit the details like which file they want to use for this purpose like either they want to save it in a text file format or in an image file format, what message they want to hide behind it and so on. Once the user provides all the

required details, the application performs the required operations and makes the message hidden and ready to be forwarded through the provided file.

1.4 Motivation & Outcomes

Steganography is really handy to use, because people won't even suspect that they're looking at a secret message—making it less likely that they'll want to try to crack your code. It's just similar to one of those code games we used to play as a kid using either invisible ink, lemon juice technique or the secret keywords but the only difference between them and steganography is- it's technical and more practical with high level of security.

2. DESCRIPTION OF PROJECT

In this, we're going to tell you about the different libraries we used in order to make this project.

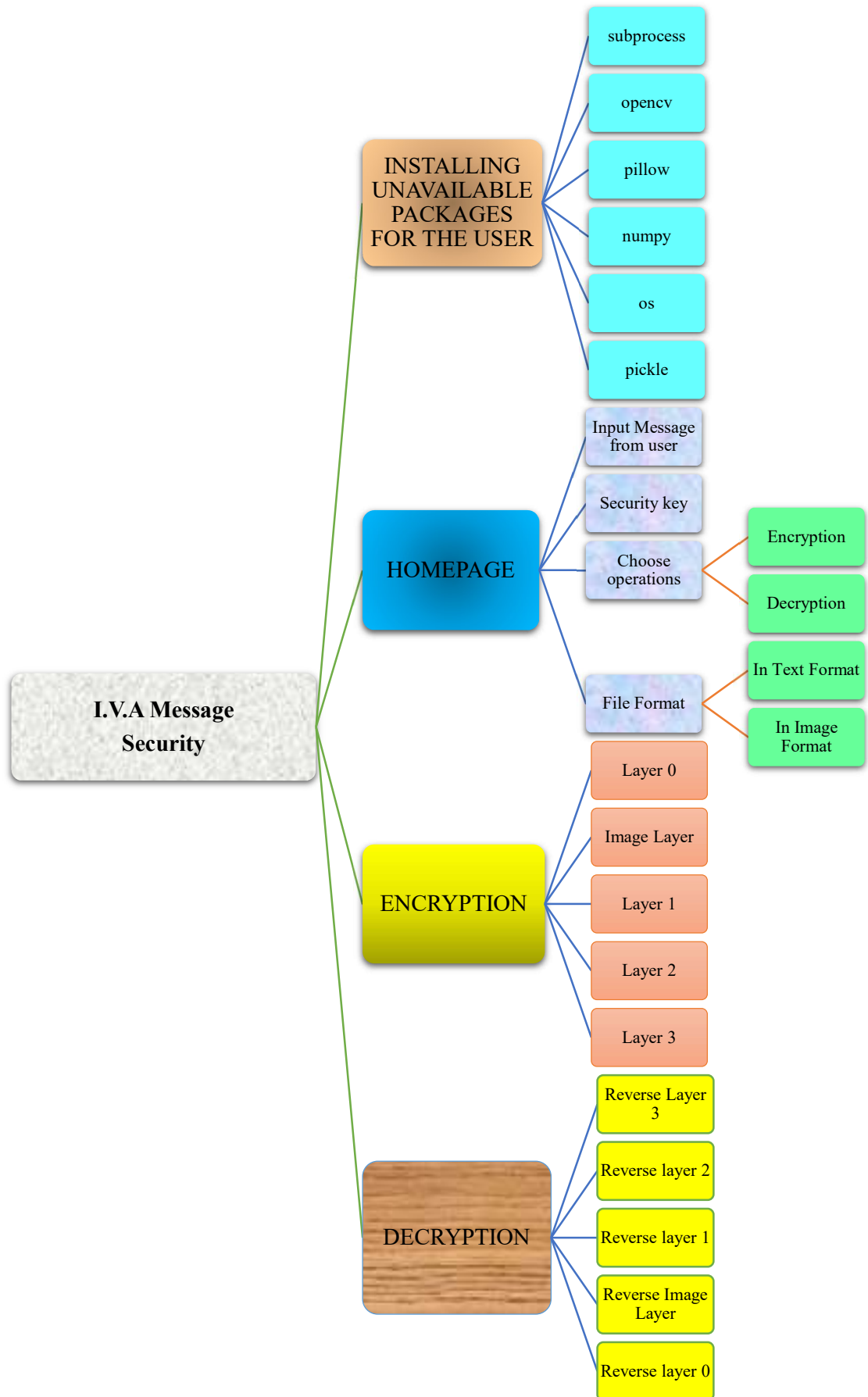
Libraries & Modules Used in Python

- I. **subprocess:** The subprocess module enables you to start new applications from your Python program.
- II. **pillow:** Pillow is a free and open source library for the Python programming language that allows you to easily create & manipulate digital images.
- III. **OpenCV:** OpenCV is a Python library which is designed to solve computer vision problems.
- IV. **Numpy:** NumPy is a library for the Python programming language, adding support for large, multi-dimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays.
- V. **Tkinter:** Tkinter is the most commonly used library for developing GUI (Graphical User Interface) in Python.
- VI. **OS:** The OS module in python provides functions for interacting with the operating system. OS, comes under Python's standard utility modules. This module provides a portable way of using operating system dependent functionality.
- VII. **Pickle:** Python pickle module is used for serializing and de-serializing a Python object structure. Any object in Python can be pickled so that it can be saved on disk. Pickling is a way to convert a python object (list, dict, etc.) into a character stream. The idea is that this character stream contains all the information necessary to reconstruct the object in another python script.

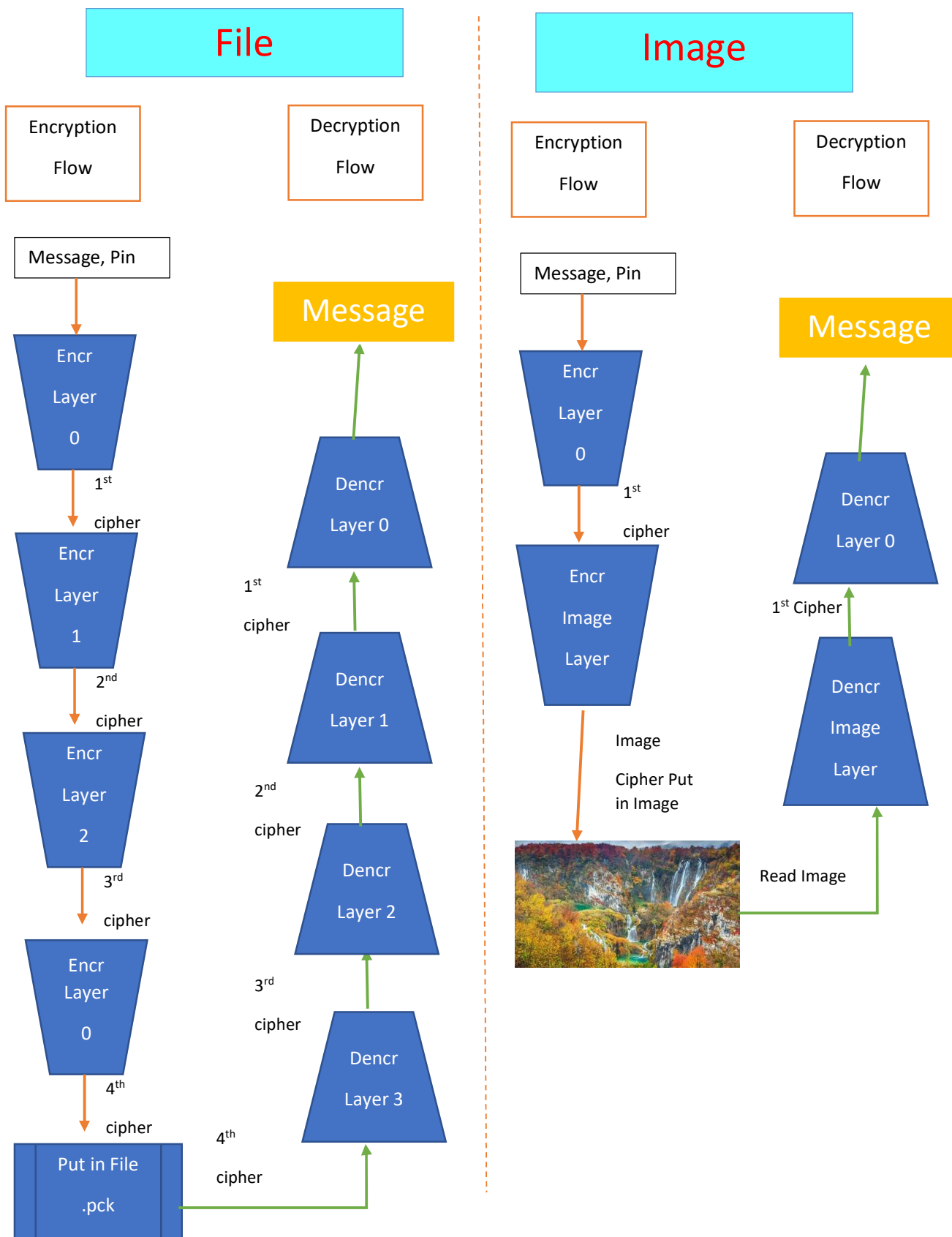
Encryption: Encryption is the process of converting plain text into cipher text i.e. converting the text from readable format to non-readable format to secure the conversation between two parties or from the unauthorized person. A secret key is used to encrypt the plain text in a secure way.

Decryption: It is a procedure of modifying data which has been accomplished as undecipherable material via encryption to its decipherable state. In the process, the system obtains and converts the confusing data into words and pictures that are simply comprehensible both for the reader and system. It might be performed automatically or manually. It might even be accomplished with an assortment of codes or passwords.

BASIC LAYOUT OF THE PROJECT IN FLOW CHART



Flow of Encryption and Decryption



3.WORK DIVISION

A. VIKRAM SHARMA

1. Made translation module to convert the string into relevant code.
2. Made encryption modules along with layers.
3. Final Checking and bug fixing in every part and Brain Storming on Encryption ways and Decryption.
4. Manages the Project and allocate works.

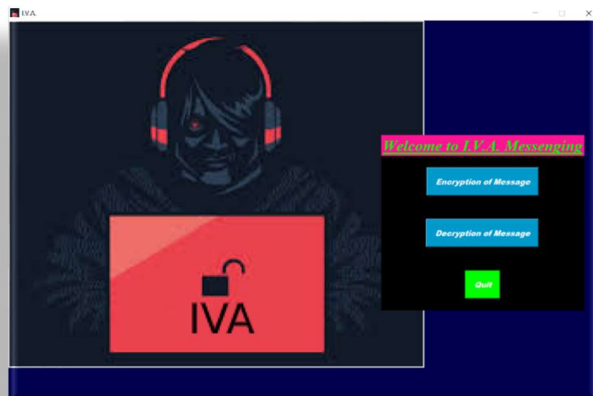
B. ISHIKA AGGARWAL

1. Design and Construct GUI.
2. Made the final report.
3. Testing of Layers of Encryption.

C. KUMAR ARMAN SIKRIWAL

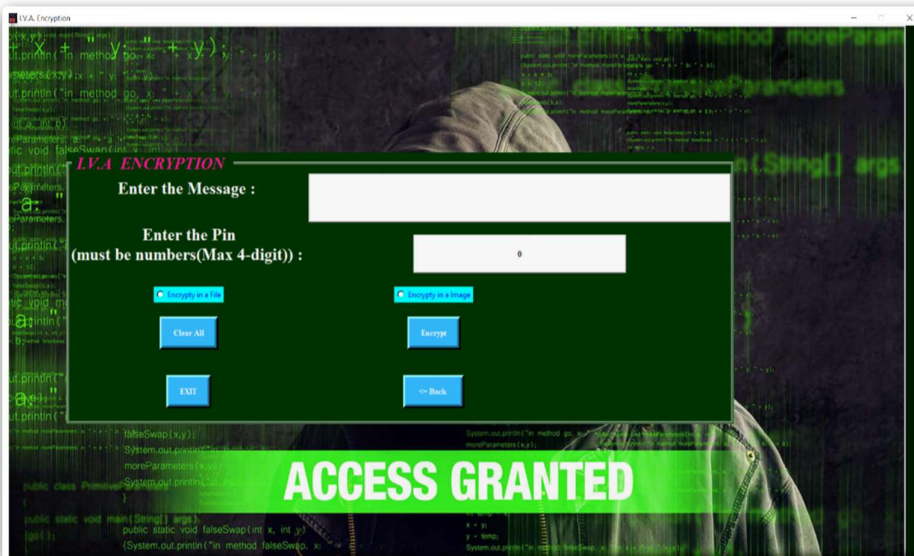
1. Made the decryption module along with all reverse layers.
2. Designing GUI.
3. Made the installation modules for the user.

4.IMPLEMENTATION OF THE PROJECT



Homepage

- ✓ It is our homepage. From here you can redirect to encryption or decryption page respective of your click.
- ✓ The Background is our logo.
- ✓ You can only off the application by quit button.
- ✓ This page is not resizable.



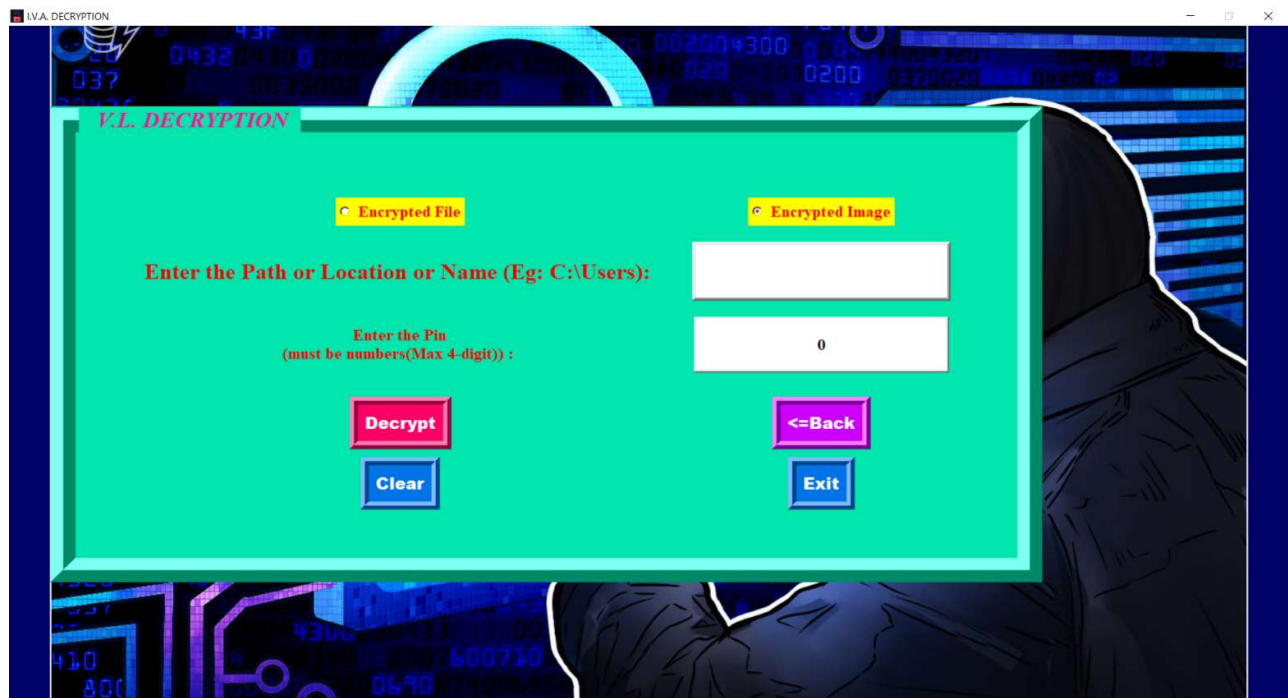
Encryption Page

- ✓ It is our Encryption Page.
- ✓ It accepts Message (Max 255 characters), Pin (4-Digit No)
- ✓ Select the Format
- ✓ It has Clear, Exit , Encrypt and Back button.
- ✓ It covers all the Exceptions like empty fields, No Format selected, etc.
- ✓ If All data is right according to check then a message box show success and in case the format is image , Encrypted Image is also shown.



Decryption Page (Initial)

- ✓ It is our Decryption Page (Initially).
- ✓ It asks User to select the choice i.e. he/she has which encrypted file format as it is selected it shows the below GUI.
- ✓ It has Back and Exit Button, Back Go back to Homepage.



Decryption Page (Final)

- ✓ It is our Decryption Page (Final).
- ✓ It asks User to select the choice i.e. he/she has which encrypted file format as it is selected it shows the below GUI.
- ✓ It has Back and Exit Button, Back Go back to Decryption Page (Initial).
- ✓ It accepts path of Image/File, a 4-digit pin of numbers.
- ✓ It handles exception when Decrypt Button like Validate Pin , Path given ,File Formats and finally if all the data given is correct like pin then it shows the message in message box.
- ✓ But, if Pin is incorrect then
 - ▶ Back and Exit is Disabled.
 - ▶ You have 2 attempts it is shown in warning message box.
 - ▶ Even in last attempt you give correct pin then the destroyer stops
 - ▶ But even in last attempt pin is wrong then the encrypted file is deleted either it is a image or pck file from Hard Disk. And then it show a error message box show removing files.
- ✓ Clear Button Clear all the text fields.

5. TECHNOLOGY

User Interface	:	Python Language
Platforms used	:	Python IDLE Shell, Jupyter Notebook, Anaconda Navigator, VS code.
Libraries Used in Python	:	tkinter, opencv, pickle, pillow, os, numpy, subprocess
Methods Used	:	Encryption , Decryption, Homepage, MakeTrans, TranslateE
Formats that can be used	:	.pck for text files and .png for image files.

6. SWOT ANALYSIS

S - > STRENGTHS

- It is a completely secured system.
- Authorization key of user is required to encrypt or decrypt data.
- Termination of program if the user enters the incorrect key 3 times.
- The data that has been required to be wrapped and the data under which it has to be wrapped, both are being used by the application to merge them in a specific way. The working with these applications is very simple so that even someone from a non-technical background can also use it properly.

W - > WEAKNESS

It is not compatible for the format with .jpeg extensions as they have their own level of security and even if we tried to relate or execute the program using these extensions then we might not get our required output and may not be able to encrypt message properly.

O - > OPPORTUNITY

This system provides the opportunity to those users who don't want the unwanted party to read the data without their explicit permission and provides a sense of security. Steganography is one of the most important methodologies used in cybersecurity in order to protect the crucial data before getting transmitted to the public or private network. It is leveraged by military and organizations to transmit critical messages from one host to another.

T - > THREATS

The data in ram might be a threat. As Deleted Data can be recovered. It can take message of length 255 char more than that is feasible for encrypted file but in case of image it can be a threat.

BIBLIOGRAPHY

- www.slideshare.com
- www.wiki.org
- www.inettutor.com
- www.w3school.com
- www.projectsgeek.com
- www.freeprojectz.com
- www.educba.org
- www.edureka.com
- www.blog.justsophie.com
- www.tutorialspoint.com