



विद्या तत्त्व ज्योतिसमः

Information Security Lab

Mini Project

Report

Submitted by

S.No.	Enrollment No.	Batch	Name
1	20103183	B7	Joy Rattoo
2	20103336	B7	Piyush Kumar
3	20103193	B7	Abishek Kumar
4	20103181	B7	Sumit Singh
5	20103182	B7	Daksh Pal

In

Department of Computer Science

Jaypee Institute of Information Technology

To

Dr Arpita Jadhav Bhatt

November 2022

Acknowledgments

We are giving a lot of effort into this project. However, completing this project would not be possible without the support and guidance of a lot of individuals. We would like to extend our sincere thanks to all of them.

We are highly indebted to **Dr Arpita Jadhav Bhatt** for her guidance and supervision. We would like to thank her for providing the necessary information and resources for this project.

We would like to express our gratitude towards our parents & our friends for their kind cooperation and encouragement which helped us a lot in completing this project.

Our thanks and appreciations also go to our colleagues in developing the project. Thank you to all the people who have willingly helped us out with their abilities.

TABLE OF CONTENTS

TITLE

Introduction

Problem Statement

Flowchart

Screenshots

Conclusion

References

INTRODUCTION

The growing use of the Internet needs to take attention while we send and receive personal information in a secure manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form. A solution to this problem has already been achieved by using a “steganography” technique to hide data in a cover media so that others cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this project, we present a new system for hiding data that stands on many methods and algorithms for image hiding where we input a key for 3DES encryption then the text to be encrypted, later we enter the file path of the image to encode cipher using steganography. For retrieving the secret we decode the image's lsb (least significant bits) and then decrypt using the 3DES key.

Encryption

There is no better security protocol than data encryption in today's day and age.

Used in a plethora of security solutions, data encryption prevents unauthorized users from accessing your precious data. Whether you send data over network wiring or look at it on your disk at home, data encryption ensures that your files stay safe and locked.

Data encryption standard (DES)

In cryptography, Triple DES, officially the Triple Data Encryption Algorithm, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

Block sizes: 64 bits Key sizes: 168, 112 or 56 bits (keying option 1, 2, 3 respectively)

Data encryption standard (DES) uses 56 bit key to encrypt any plain text which can be easily cracked by using modern technologies. To prevent this from happening double DES and triple DES were introduced which are much more secured than the original DES because it uses 112 and 168 bit keys respectively. They offer much more security than DES

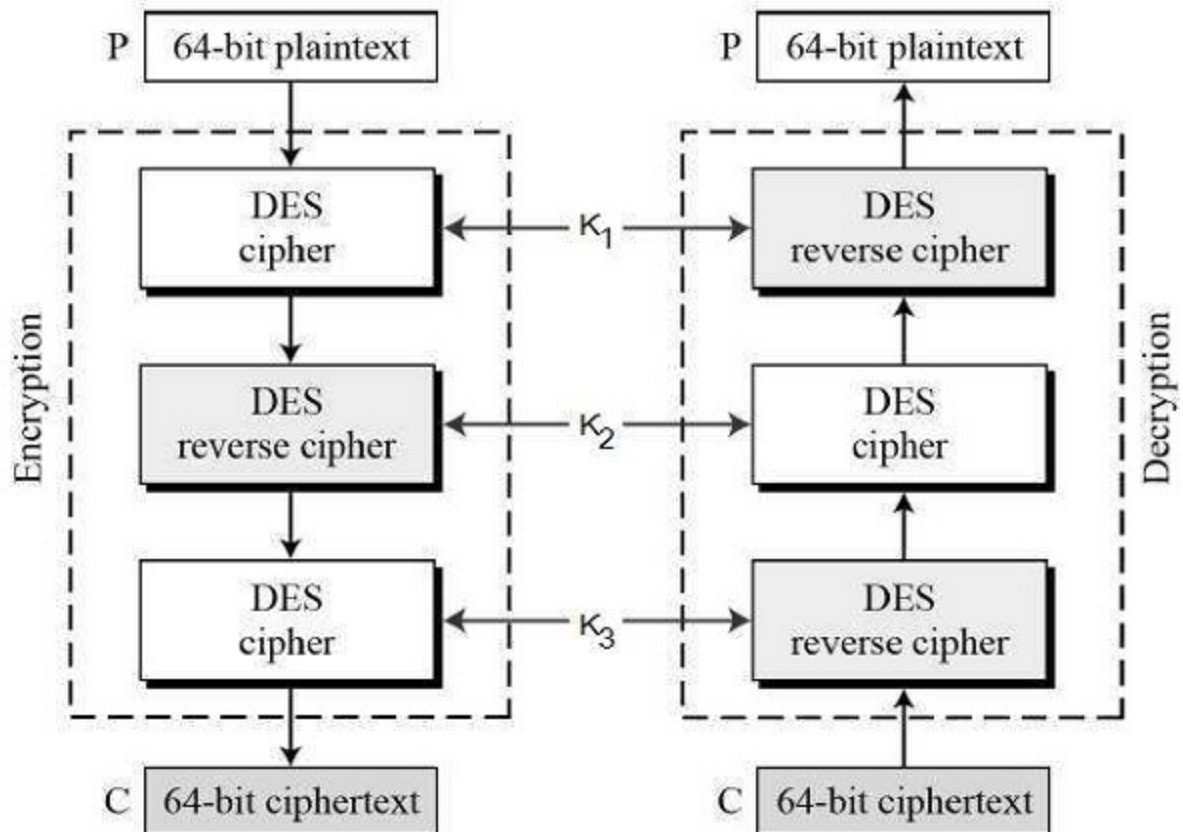
Triple DES

Triple DES is an encryption technique which uses three instance of DES on the same plain text. It uses three different types of key choosing technique. First all used keys are different and in second two keys are same and one is different and in third all keys are same.

Triple-DES encryption uses a triple-length DATA key comprised of three 8-byte DES keys to encipher 8 bytes of data using this method:

Encipher the data using the first key Decipher the result using the second key Encipher the second result using the third key The procedure is reversed to decipher data that has been triple-DES enciphered:

Decipher the data using the third key Encipher the result using the second key Decipher the second result using the first key



Steganography

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection. Therefore, some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover

Concept of LSB based data embedding:

LSB stands for Least Significant Bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

Python Packages

PyCryptodome is a self-contained Python package of low-level cryptographic primitives

Python Imaging Library (PIL) is the de facto image processing package for Python language. It incorporates lightweight image processing tools that aids in editing, creating and saving images

Python hashlib module provides a helper function for efficient hashing of a file or file-like object. We have used the md5 file digest() method..

Problem Statement

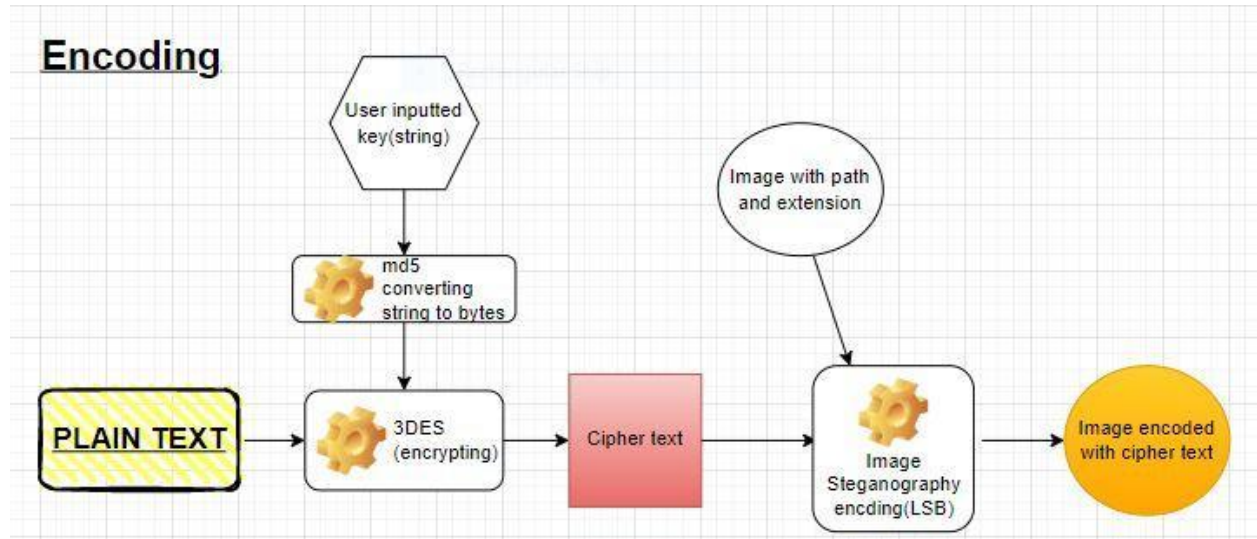
Daniel wants to throw a party only for his close hostel friends. In order to keep the location of the party hidden from the uninvited friends, he decided to deliberately set the location impromptu. He needs to send it in a hidden form, so that only his close friend can understand it and decode it efficiently and quickly, to get to the location.

Hidden message should be such that, even if the uninvited friend requires it, they cannot decode it without the private key.

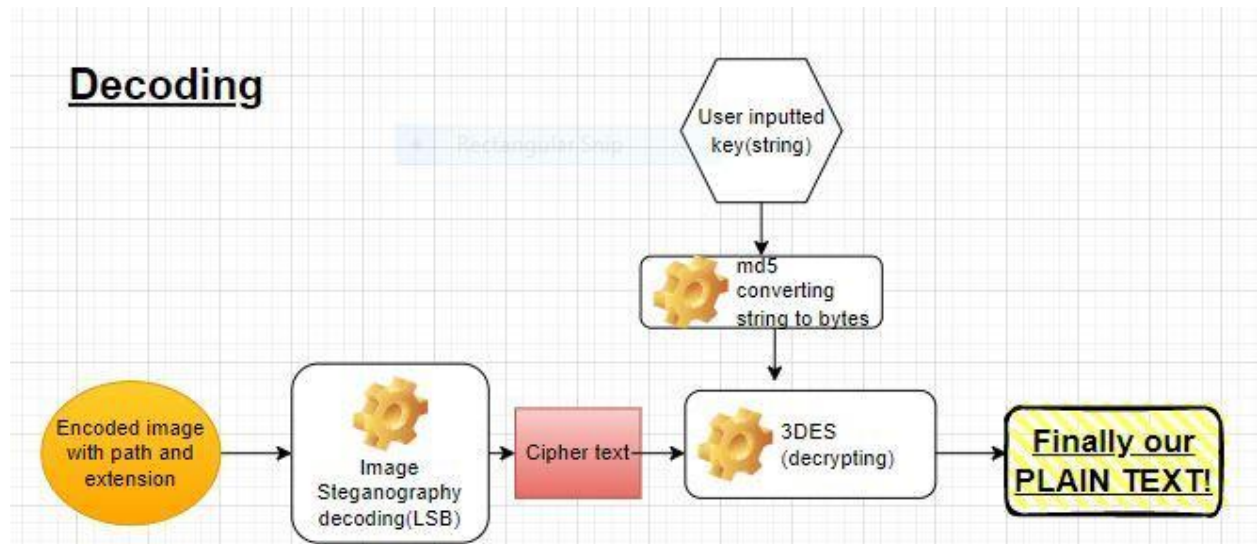
The private key is known only by his close friend, as told by Daniel.

Flowchart

Encoding

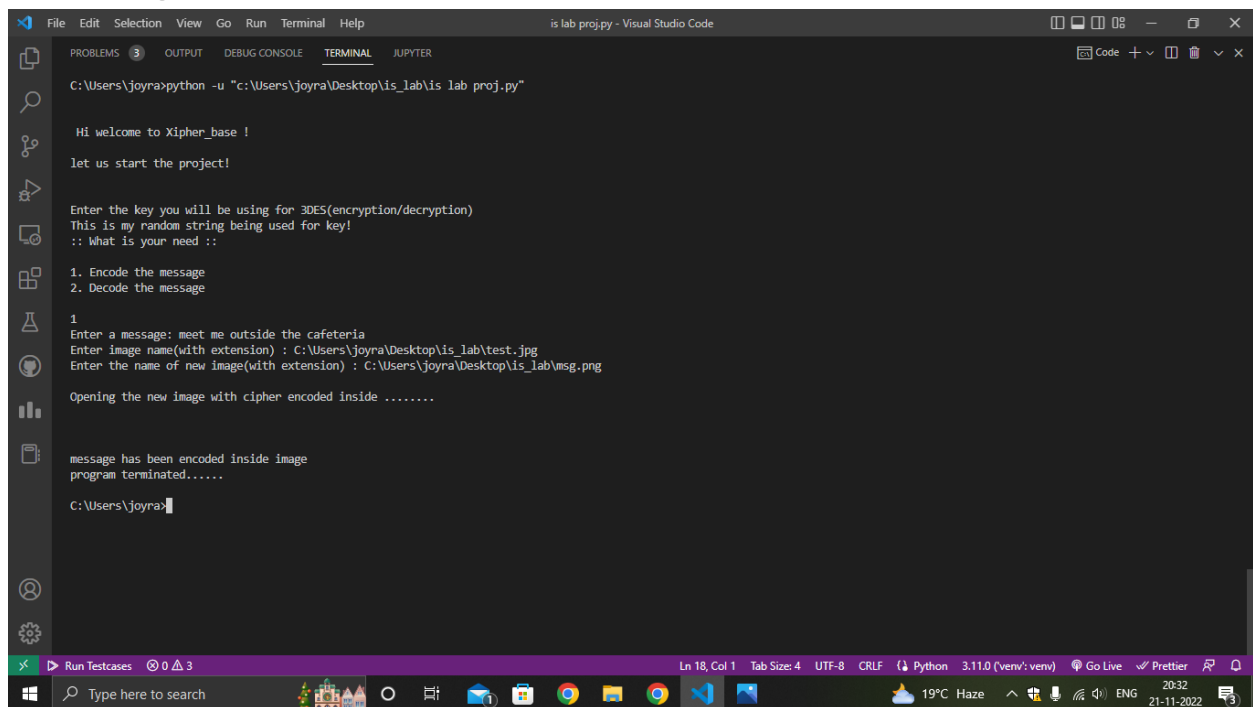


Decoding



Screenshots

Encoding output>>>>>>>>



```
C:\Users\joyra>python -u "c:\Users\joyra\Desktop\is_lab\is_lab proj.py"

Hi welcome to Xipher_base !
let us start the project!

Enter the key you will be using for 3DES(encryption/decryption)
This is my random string being used for key!
:: What is your need ::

1. Encode the message
2. Decode the message

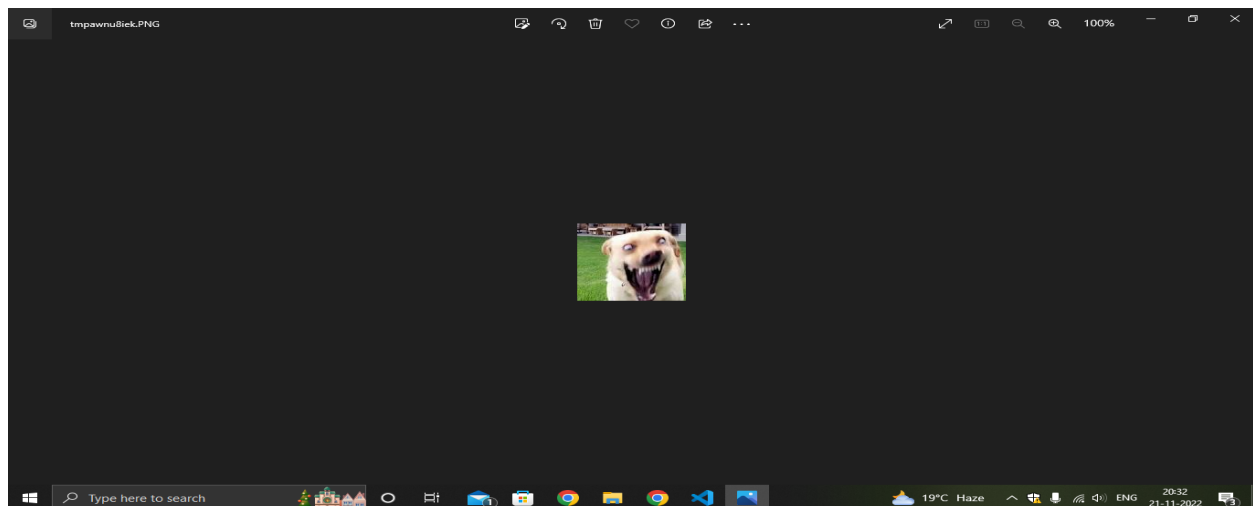
1
Enter a message: meet me outside the cafeteria
Enter image name(with extension) : C:\Users\joyra\Desktop\is_lab\test.jpg
Enter the name of new image(with extension) : C:\Users\joyra\Desktop\is_lab\msg.png

Opening the new image with cipher encoded inside .....

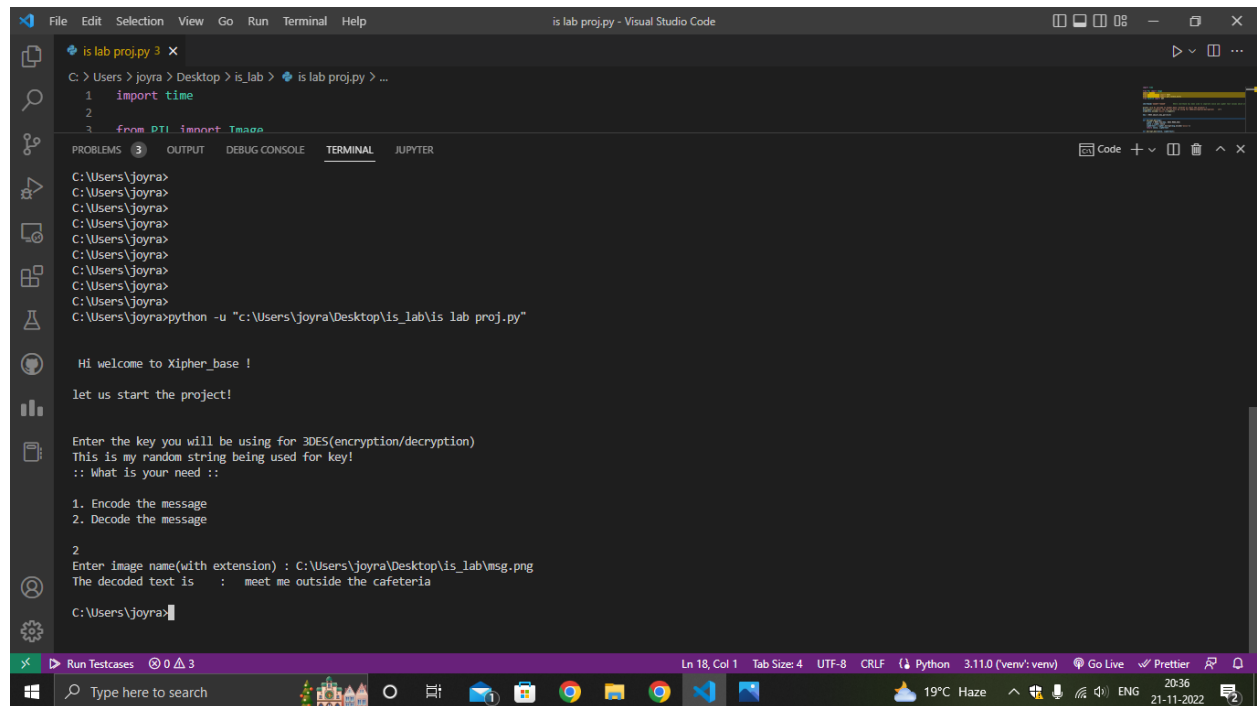
message has been encoded inside image
program terminated.....

C:\Users\joyra>
```

Encoded Image opened after steganography>>>>>>>>



Decoding output>>>>>>>



```
is lab proj.py 3 X
C:\Users\joyra> Desktop > is_lab > is lab proj.py > ...
1 import time
2
3 from PIL import Image

PROBLEMS 3 OUTPUT DEBUG CONSOLE TERMINAL JUPYTER
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>
C:\Users\joyra>python -u "c:\Users\joyra\Desktop\is_lab\is lab proj.py"

Hi welcome to Xipher_base !

let us start the project!

Enter the key you will be using for 3DES(encryption/decryption)
This is my random string being used for key!
:: What is your need ::

1. Encode the message
2. Decode the message

2
Enter image name(with extension) : C:\Users\joyra\Desktop\is_lab\msg.png
The decoded text is : meet me outside the cafeteria

C:\Users\joyra>
```

Conclusion

So, in order to maintain the confidentiality of the data various approaches like cryptography and steganography may be used.

In this project we have encoded the text(location of the party) using 3DES encryption technique via **Python's Pycryptodome package**.

Then to hide the ciphertext generated via 3DES, it is again encoded in an image using LSB based steganographic method for hiding the data by applying Least Significant Bit (LSB) algorithm for embedding the data into the images which is implemented through the **Python pillow package**

Whereas for decoding we take the encryption key used for 3DES from the user and convert it into bytes using md5 python package .Then the byte converted key is made to go through DES parity checker .We extract cipher from image using LSB technique of image Steganography and decrypt using the 3DES key.

References

- <https://www.geeksforgeeks.org/lsb-based-image-steganography-using-matlab/>
- <https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html>
- <https://www.ukessays.com/essays/information-technology/examining-the-importance-of-steganography-information-technology-essay.php>
- <https://www.geeksforgeeks.org/image-based-steganography-using-python/>