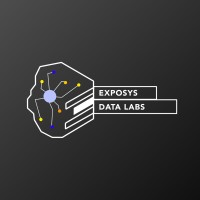
# Image Encryption using 3DES

# By **Mayur Rattan Jaisingha**ni

**TYCS, VESIT, Mumbai.**

****

**For Exposys Data labs Internship**

**P.M R. Residency, Ground Floor, No-5/3 Sy. No.10/6-1**

**Opp Nithyotsava Wedding Hall, Doddaballapur Main Road,**

**Singanayakanahalli, Yelahanka, Bengaluru, Karnataka 560064**

# Contents

## Abstract ii

**Acknowledgement iii**

## List of Figures iv

## Introduction 1

* 1. Introduction
  2. Motivation
  3. Problem Statement & Objectives
  4. Organization of the Report

1. **Literature Survey 2**
   1. Survey of Existing System/**SRS**
   2. Project Contribution

## Proposed System 3

* 1. Introduction
  2. Algorithm and Process Design
  3. Details of Hardware & Software
  4. Experiment and Results for Validation and Verification
  5. Analysis
  6. Conclusion and Future work.

## References 8

**Abstract:**

Digital Images and video encryption plays an important role in today’s multimedia world. Many encryption schemes have been proposed to provide security for digital images. Usually, the symmetric key ciphering algorithms are used in encrypting digital images because it is fast and use the techniques for block and stream ciphers. Data Encryption Standard is symmetric key encryption algorithm. In spite of the successful cracking of the data encryption standard by massive brute force attacks, data encryption standard algorithm is an entrenched technology and still useful for many purposes. In this paper, we use some of the image quality encryption measuring factors to study the effect of data encryption standard algorithm in image ciphering. The results show that the data encryption standard algorithm is fast and it achieves a good encryption rate for image ciphering using different modes of operation.

**Keywords: -DES, Image Encryption.**

**Acknowledgement:**

I would like to give a special thanks to Divyanshu Kumar from NIT silchar for guiding me through this project. His previous work has helped a lot in understanding the concepts of image security and triple des.

**List of Figures:**

1. 3DES process
2. 3DES process
3. Encryption process
4. Decryption process
5. Original image
6. Encryption done
7. Post encryption
8. Decryption done
9. Post decryption

**Chapter 1:**

**1.1 Introduction:**

These days the data security is the important aspect of digital data communications. Since this information happen to more significance and secrecy like managing account information, military information, delicate data like medical records, and multimedia data, for example image, sound, or video. This requires a need of satisfactory and successful cryptographic algorithm to secure these sorts of information transmissions from an unauthorized user revealing. Then again, the pace of the innovation and the improvements in the field of computational processing speed in our lives is turning out to be quicker and speedier. These improvements facilitate the threats and attacks on the information or data to uncover its secrecy progressively and load the enormous test of fulfill the undertaking of securing the communications.

Best approach of security assurance is Encryption. For changing input image into another image, encryption system used many techniques. So that changed image is difficult to understand by other unauthorized person and to maintain the secret of images between clients. Another advantages of encryption technique is can’t access the image information without decryption key. Main application of image encryption is multimedia frame work.

Here we are using established cryptographic algorithm that is Data Encryption Standard (DES). DES was a generally utilized cryptosystem for securing the characterized information transmissions. DES is a symmetric key cryptosystem that is nothing but for both encryption process and decryption process, using same secret key. Many algorithms keep DES as their core design for cryptographic design.

**1.2 Motivation:**

The main purpose of doing this project is to learn more about machine learning using python. As a part of my internship trial, this project is not only a test but also a way for me to learn.

**1.3 Problem Statement and Objective:**

The problem statement is: Encryption of an image using the 3DES algorithm in python.

The objective is: To pass the one-month trial of the internship and learn about image encryption.

**1.4 Organization of the Report:**

Chapter 1 consists of a brief introduction to the project of data encryption. Along with this, the problem statement and objectives of the project have also been stated clearly.

Chapter 2 consists of the literature survey, where research papers have been studied and concepts that are useful have been picked. It also states the contribution I have made to the project.

Chapter 3 consists of the entire procedure in which the project has been implemented along with the output. It also includes a brief analysis of the project with different inputs to showcase that the code is working perfectly. Some improvements have also been suggested at the very end.

**Chapter 2:**

**2.1: Literature Survey:**

Said F. El-Zoghdy, in his paper [10] talk about how the DES algorithm is fast and has a good encryption rate. Despite the fact that it can be easily beaten with brute force attacks, DES is still a very useful algorithm. Simulation shows that the average enciphering and deciphering speed is 3.0 MB/s, on 2 GHz Pentium IV. In terms of security, DES is powerful but AES is a modified and better version that gets the preference. Post encryption had coefficient correlation values of, horizontal: 0.0275, vertical: 0.0411 and diagonal: 0.0572.

In this paper, the author Aarti Devi [7], makes a comparison between the encryption techniques DES, AES and blowfish. Using some test cases, they derived their conclusions and also provided some tips for future use.

Mahajan et al. 2013 [11] implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Manjula K G et al. 2016 [12] has done a brief study on encryption of color images using triple des algorithm. Right from the cryptosystem to the des algorithm, have been explained in detail. The implementation approach shows the encrypted and decrypted image and also historical analysis is done with enhanced techniques.

Karthik.S et al. 2014 [9] conducts his research over symmetric encryption techniques. His experiments yield results that show 3DES being the most efficient in EBC and CBC. It also shows that, in case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. Concept of hashing the password was picked from this paper.

**2.2 Project Contribution:**

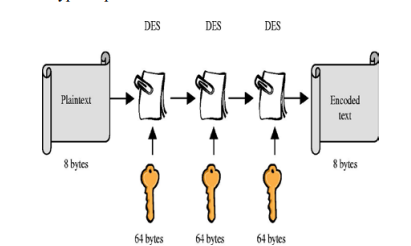
In the project, to improve security, hashing and salting of the password is also done. Apart from that, any image can be encrypted and decrypted. This has been tested with multiple images of types jpeg and Png. The project aims at making the transmission of data via images more secure, reliable and private.

**Chapter 3:**

**3.1 Introduction:**

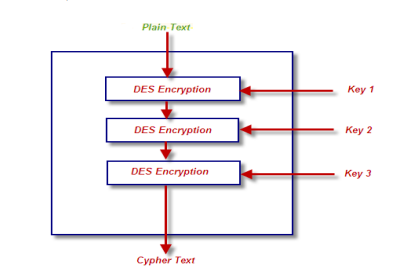
3DES was created because DES algorithm, invented in the early 1970s using 56-bit key. The effective security 3DES provides is only 112 bits due to meet-in-the-middle attacks. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. In DES, data is encrypted and decrypted in 64 -bit chunks.

The input key for DES is 64 bits long; the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.



**Figure 1: 3DES process**

The above Figure 3.2 as shown in Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards: a. All keys being independent b. Key 1 and key 2 being independent keys c. All three keys being identical Key option 3 as shown in Figure 3.3: triples DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.



**Figure 2: 3DES process**

**3.2 Algorithm and Process Design:**

**Algorithm:** Run DES three times:

ECB mode:

If K2 = K3, this is DES Backwards compatibility Known not to be just DES with K4.

Has 112 bits of security, not 3\*56 = 168

Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys.

• Encryption using the first secret key

• Decryption using the second secret key

• Encryption using the third secret key

Encryption: c = E3 (D2 (E1 (m)))

Decryption: m = D1 (E2 (D3(c)))

Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In this case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m)

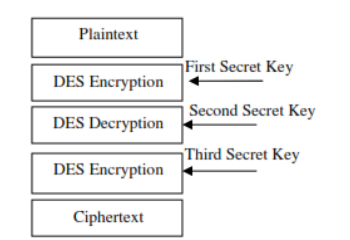
c = E3 (D3 (E1 (m))) = E1 (m)

It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

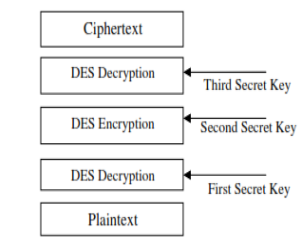
c = E1 (D2 (E1 (m)))

**Process Design:**

Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion. The following Figure 3 and Figure 4 are the block diagrams of 3DES as shown below:



**Figure 3: Encryption process**



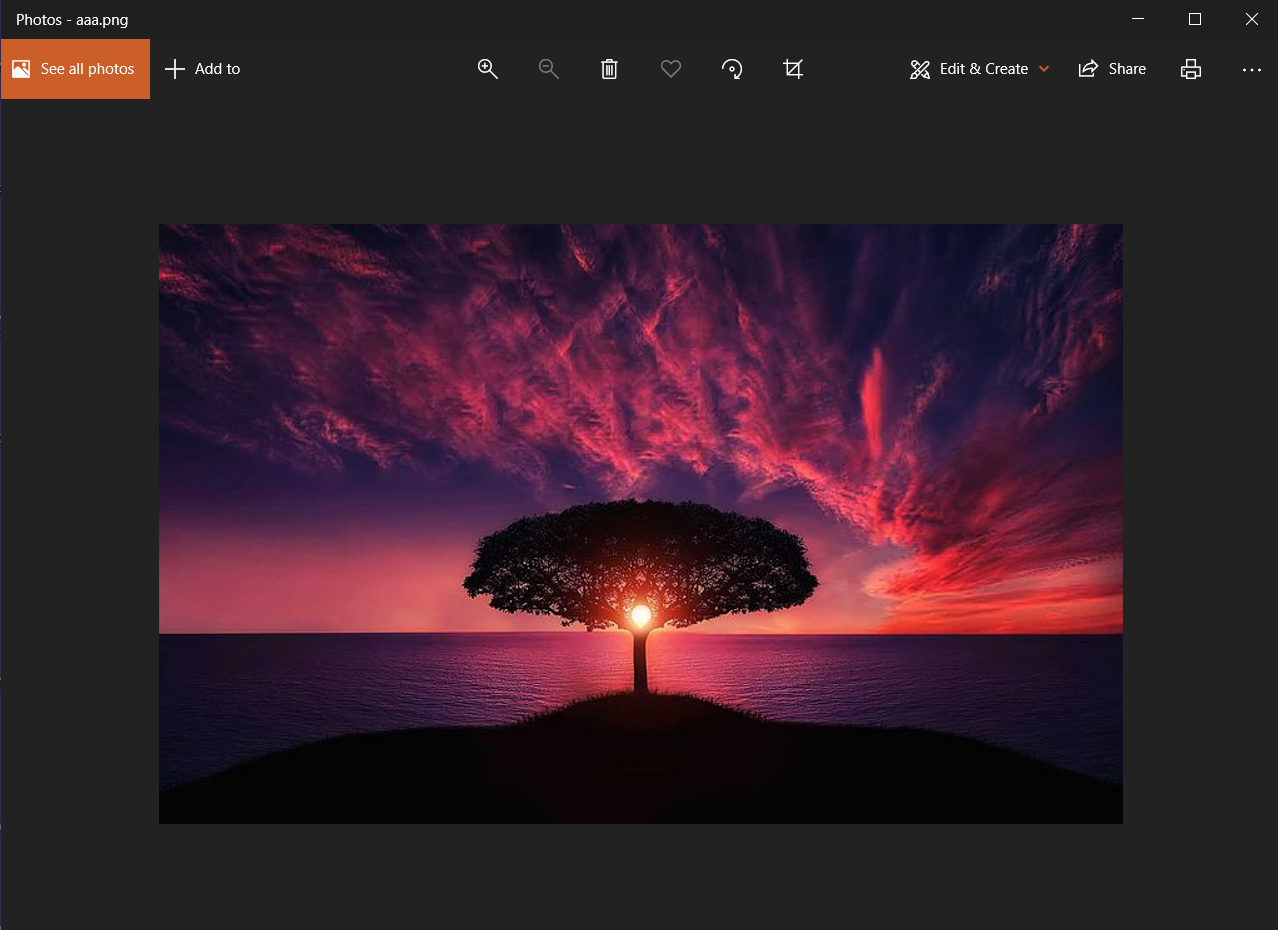
**Figure 4: Decryption process**

**3.3 Hardware and Software Details:**

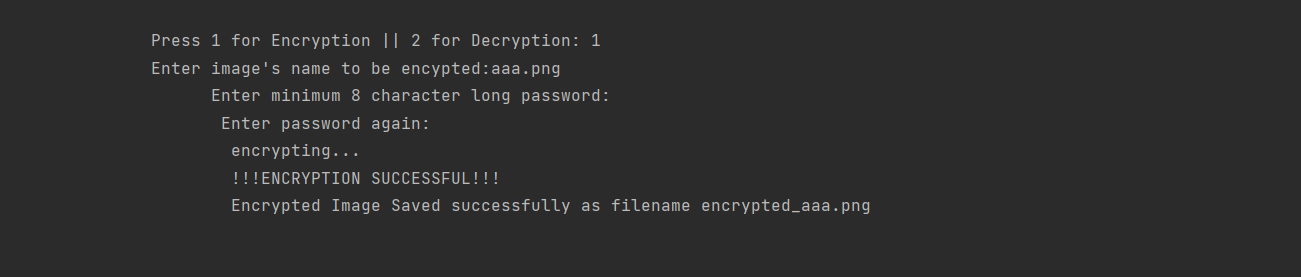
Hardware: Dell xps 13, 8gb, intel core i5 7th gen

Software: Pycharm (code written in python), interpreter python 3.9

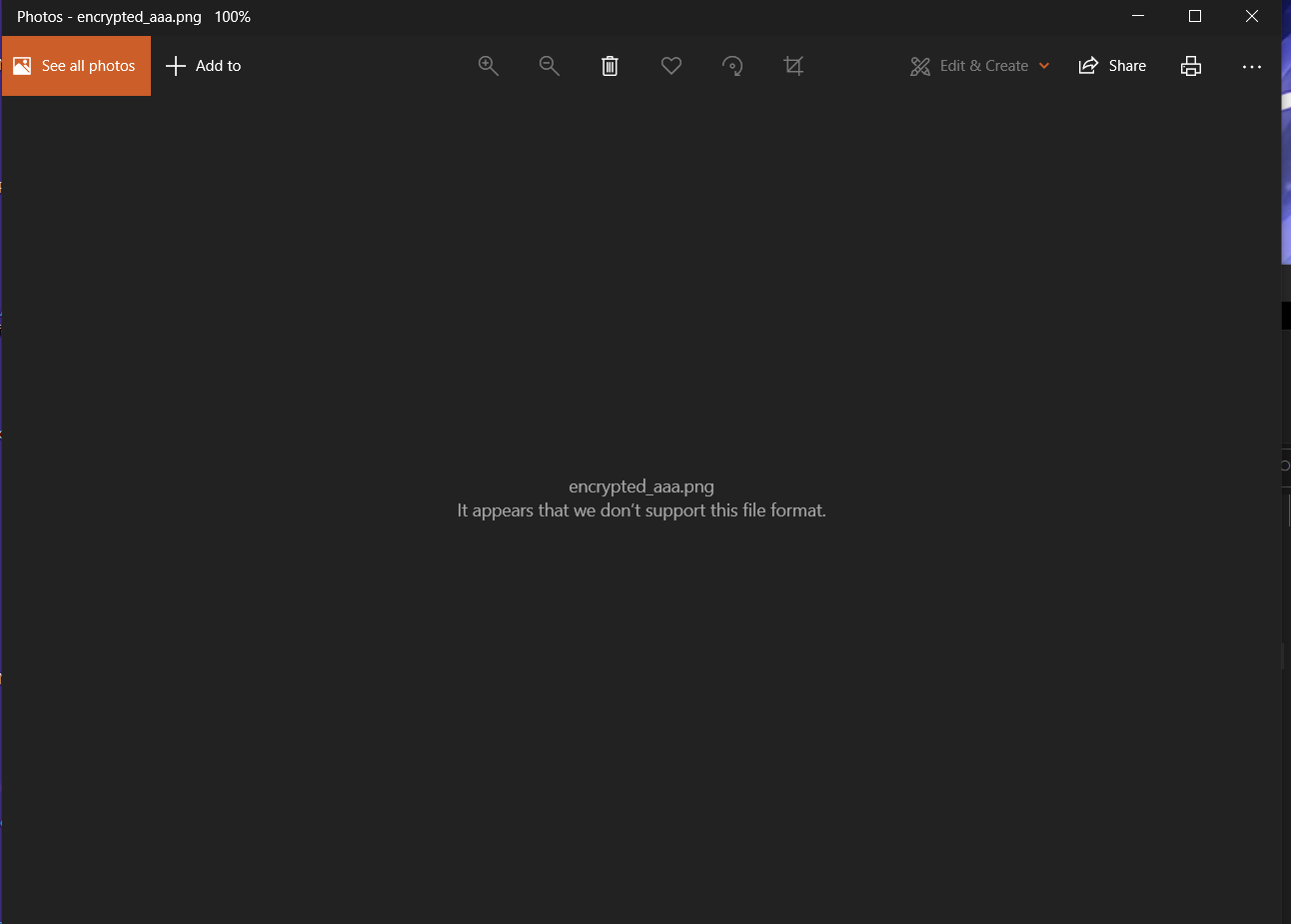
**3.4 Experiments and Results:**



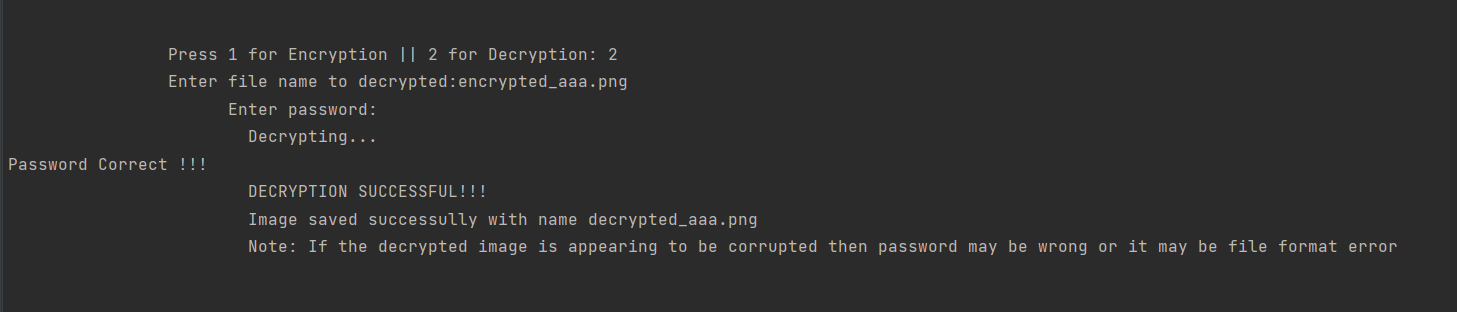
**Figure 5: Original image**



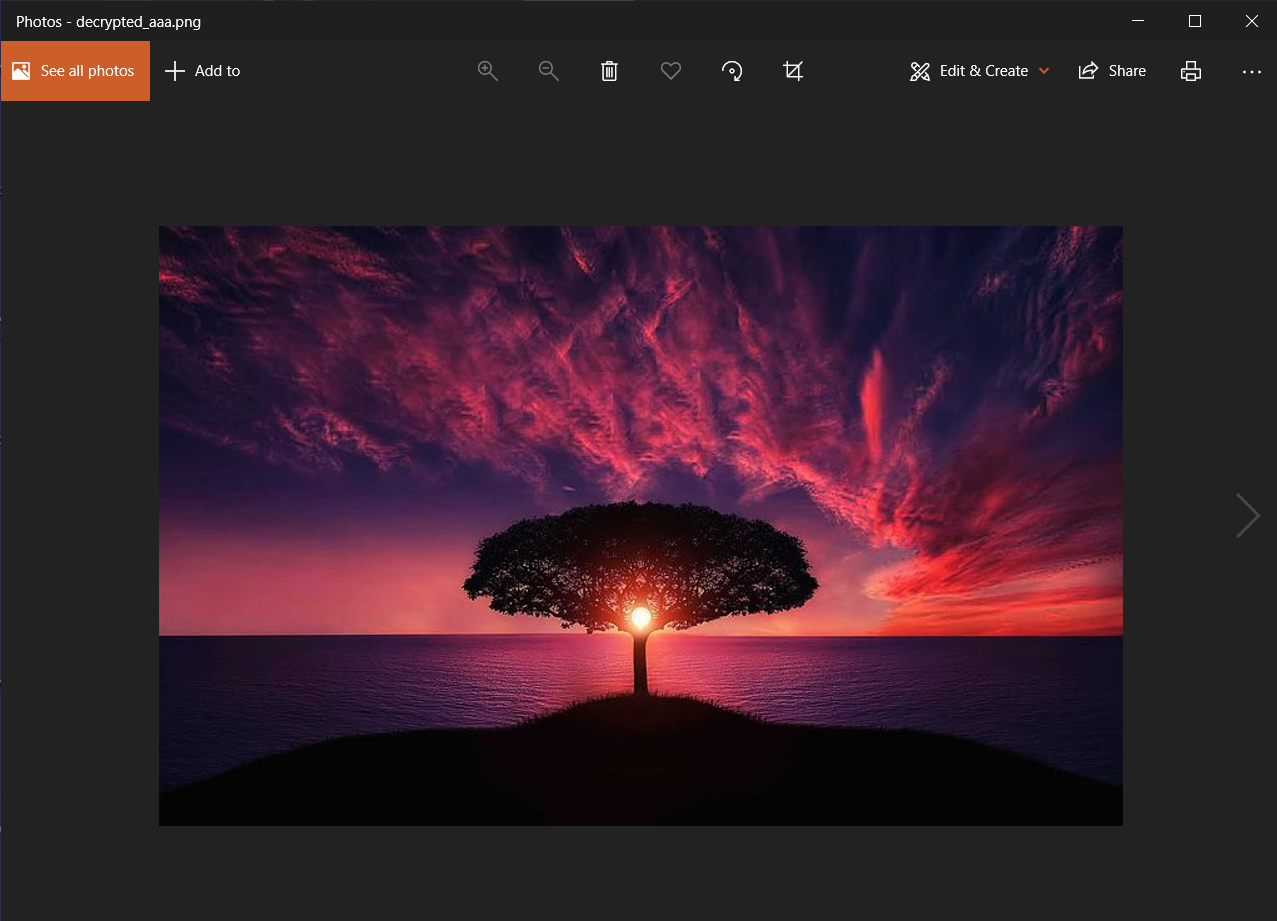
**Figure 6: Encryption process done**



**Figure 7: After encryption of image**



**Figure 8: Decryption process done**



**Figure 9: After decryption**

**3.5 Analysis:**

After trying this process on multiple images, I can conclude that the 3DES algorithm is working perfectly with great precision and low time requirement. The code was also given inputs of wrong password and the response was as expected. To check for Hashing [9] and salting, print statements were added after the block of code and the response was as expected. Wrong file name inputs and incorrect option for encryption and decryption when chosen, gave expected outputs. The code works fine and can be improved upon in the future.

**3.6 Conclusion and Future Work:**

Conclusion: The results show that the 3DES algorithm is fast and it achieves a good image encryption rate. Despite being slower than the original DES algorithm, the security analysis [9] shows better performance by 3DES.

Future Work: 1. different initialization vector for the three DES Stages derived from 48-bit hash of the password.

2. Better password hashing method script, ballon, argon2 etc.

3. Graphic user interface

4. Converting into a library

5. Standalone application for windows, Linux, mac os, android etc.

**References:**

1. <https://github.com/divyanshukumarpcm/tripleDESanyfile/blob/main/3des.py>
2. <https://github.com/Vatshayan/Image-Security-by-Triple-DES-Final-Year-Project>
3. <https://pycryptodome.readthedocs.io/en/latest/>
4. <https://docs.microsoft.com/en-us/windows/win32/seccrypto/data-encryption-and-decryption#:~:text=Encryption%20is%20the%20process%20of,converting%20ciphertext%20back%20to%20plaintext.&text=To%20decrypt%20a%20particular%20piece,the%20data%20must%20be%20used>.
5. <https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm>
6. <https://www.tutorialspoint.com/cryptography/triple_des.htm>
7. A Review on DES, AES and Blowfish for Image Encryption & Decryption - Aarti Devi, Ankush Sharma, Anamika Rangra
8. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher - Elaine Barker and Nicky Mouha
9. Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System - Karthik. S, Muruganandam .A
10. How Good Is the DES Algorithm in Image Ciphering? - Said F. El-Zoghdy, Yasser A. Nada, A. A. Abdo
11. Dr. Prerna Mahajan & Abhishek Sachdeva “A Study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security (GJCSTNWS), Volume 13 Issue 15 Version 1.0 Year 2013.

12) Color Image Encryption and Decryption Using DES Algorithm - Manjula K. G, M.N.Ravikumar