## A PROJECT REPORT ON

**Image Encryption And Decryption Using Data Encryption Standard (DES3)**

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

**SUBMITTED BY**

**SHRIKRISHNA RAJPUROHIT**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**ZEAL COLLEGE OF ENGINEERING, PUNE**

**SAVITRIBAI PHULE PUNE UNIVERSITY 2020 – 2021**

i

## CONTENTS

|  |  |  |
| --- | --- | --- |
| **SR NO.** | **CHAPTERS** | **PAGE NO** |
| 1 | ABSTRACT | 5 |
| 2 | INTRODUCTION | 6 |
| 3 | DATA ENCRYPTION STANDARD | 7 |
| 4 | IMAGE ENCRYPTION AND DECRYPTION | 8 |
| 5 | SNAPSHOT | 9 |
| 6 | ADVANTAGES AND DISADVANTAGES | 12 |
| 7 | CONCULSION | 19 |
| 8 | REFERENCE | 14 |

# ABSTRACT

Data Encryption Standard was the most well known utilized cryptographic scheme and it is symmetric key block cipher algorithm. DES was a widely used cryptosystem for securing the classified data transmissions. In this project DES algorithm is utilized to image file encryption and decryption. The acquired results demonstrate that DES algorithm could be utilized as a highly secure algorithm.

**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.

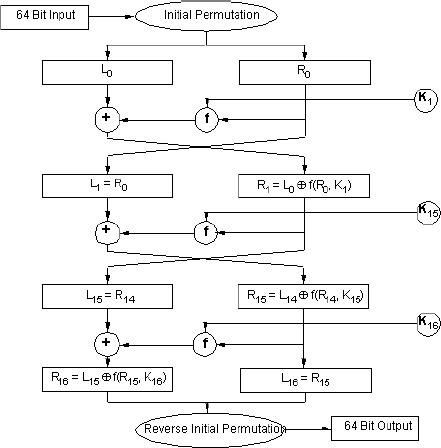
Best approach of security assurance is Encryption. For changing input image into another image, encryption system used many techniques. So that changed image is difficult to understand by other unauthorized person and to maintain the secret of images between clients. Another advantages of encryption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

By upgrading DES's security, other algorithm' security, for example, Triple-DES and IDEA will be improved. In this project, a capable change is proposed to bring the legacy DES to live by strengthening its security

**DATA ENCRYPTION STANDARD**

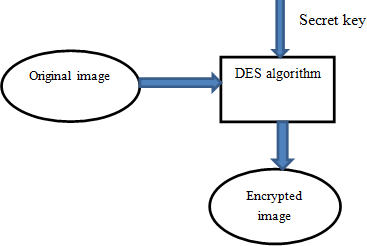
DES considered as symmetric key block cipher algorithm. The implementation structure of DES is Fiestel cipher. In Fiestel structure as 16 rounds of steps are used.64 bit block size is used for DES structure .It has 64 bit key length, but DES utilizes only 56 bit key. Remaining 8 bits is used later but not used for encryption

**Algorithm**

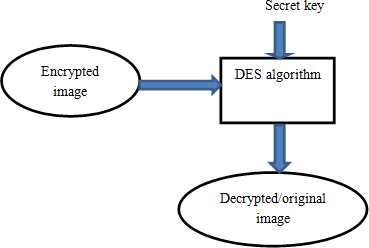
As already mentioned DES is symmetric key block cipher algorithm. Currently this algorithm use identical secret key for both encryption process and decryption process. General algorithm design 64 bit plaintext used as input. The algorithm transforms input into series of block which is 64 bit cipher text.16 rounds of encryption process is handled for every plaintext block. Decryption process is done in reverse manner of encryption method, by introducing sulky ki introduced by main key k where i=1……….16.

**IMAGE ENCRYPTION AND DECRYPTION**

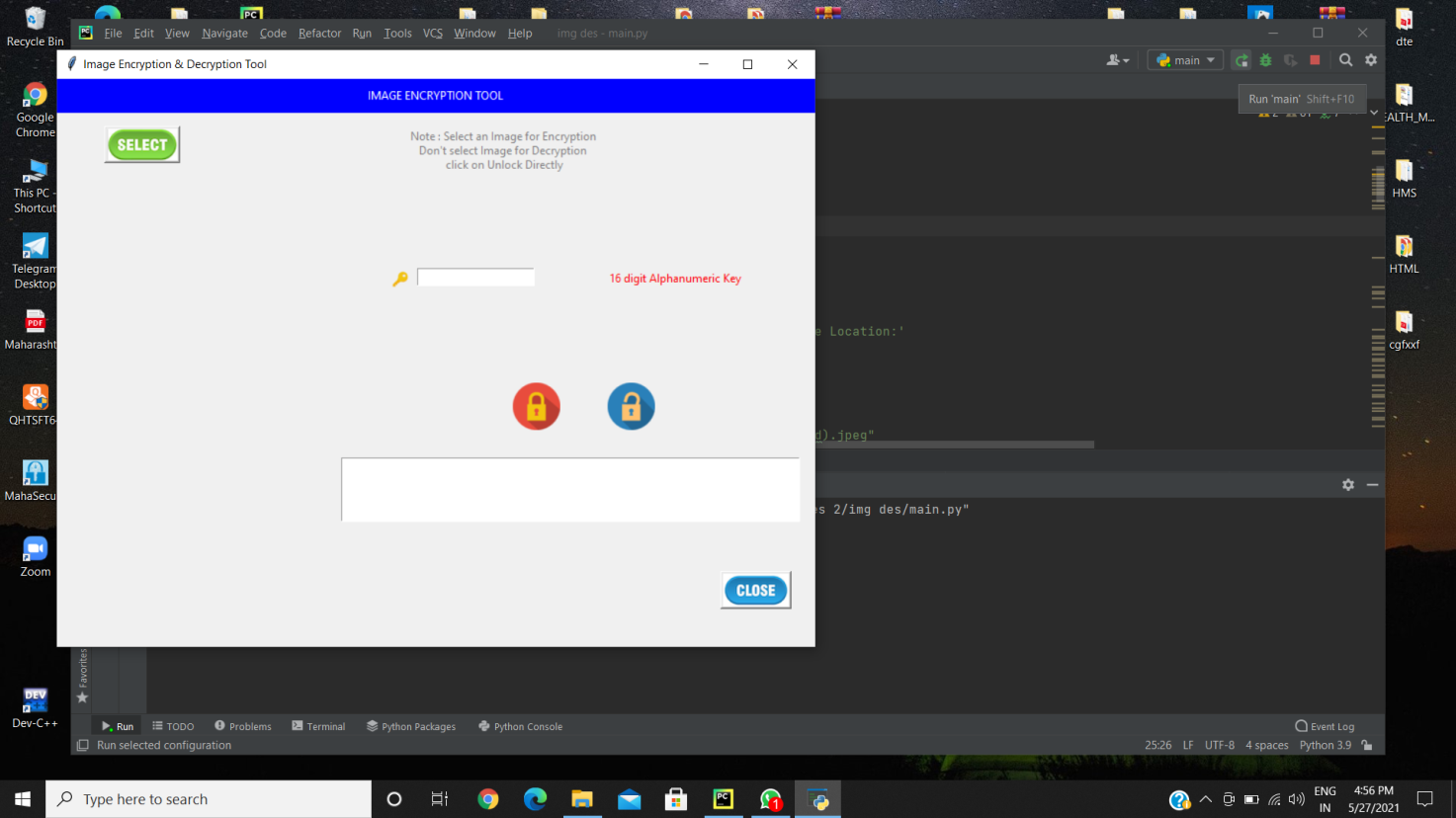
**Image Encryption**

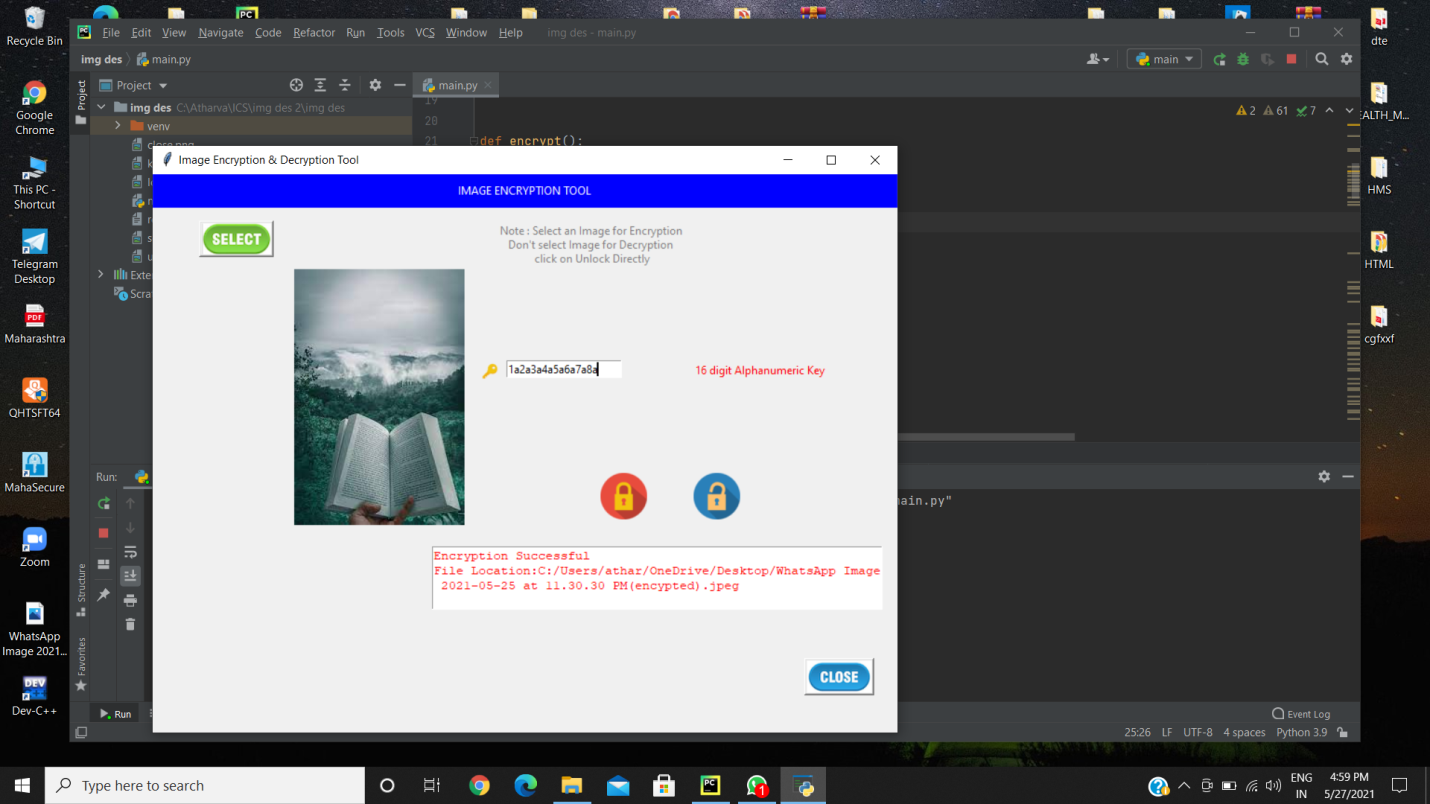
In the encryption method we considered two inputs, one is encryption secret key and another one is original color image. Image file can be reshaped or divided pixel block of original image and express DES encryption process and defining the key for encryption that is secret key. By using DES algorithm procedure finally original image is encrypted with security, this is encrypted image. Image file encryption practice is presented

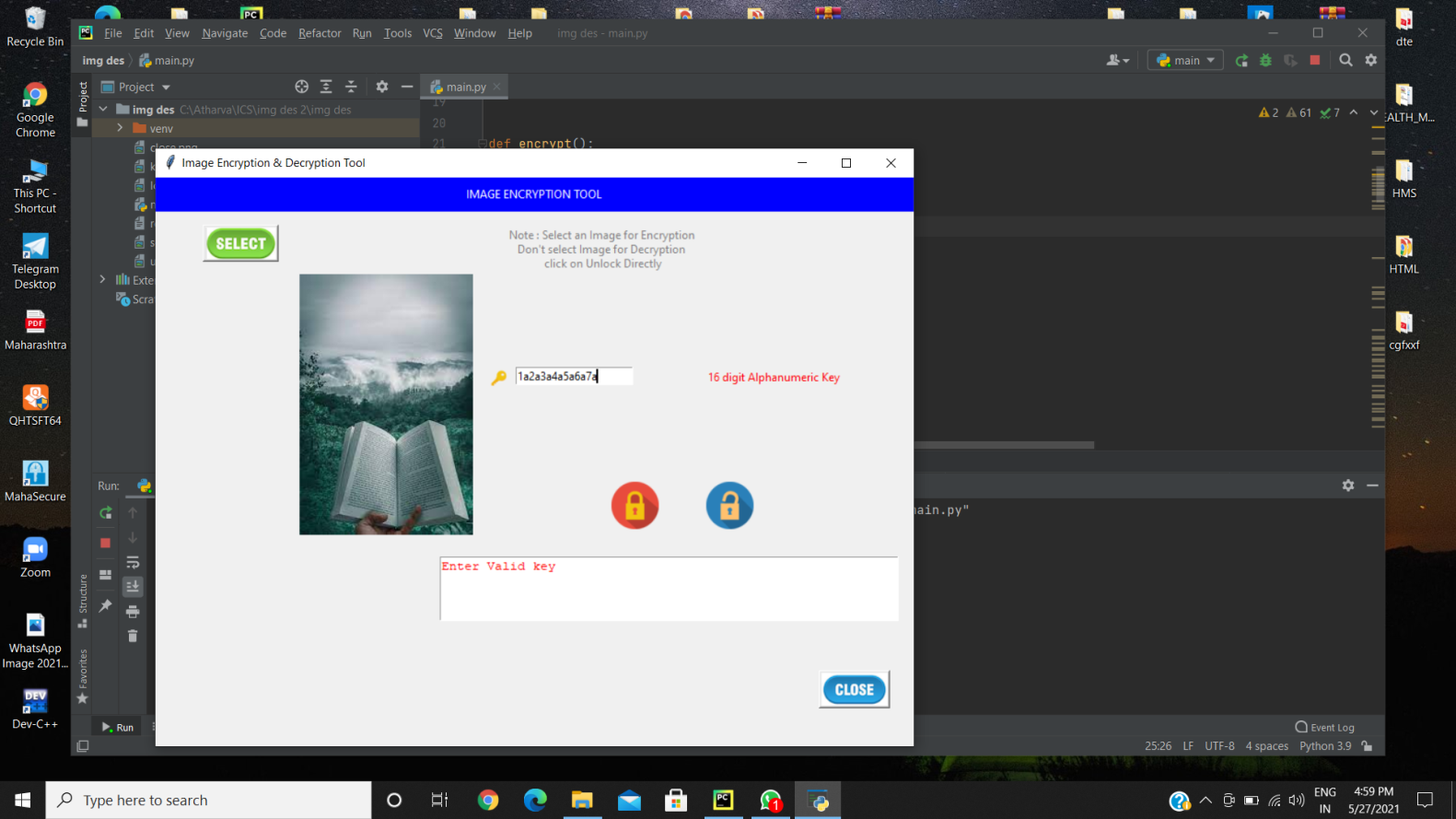
**Image Decryption**

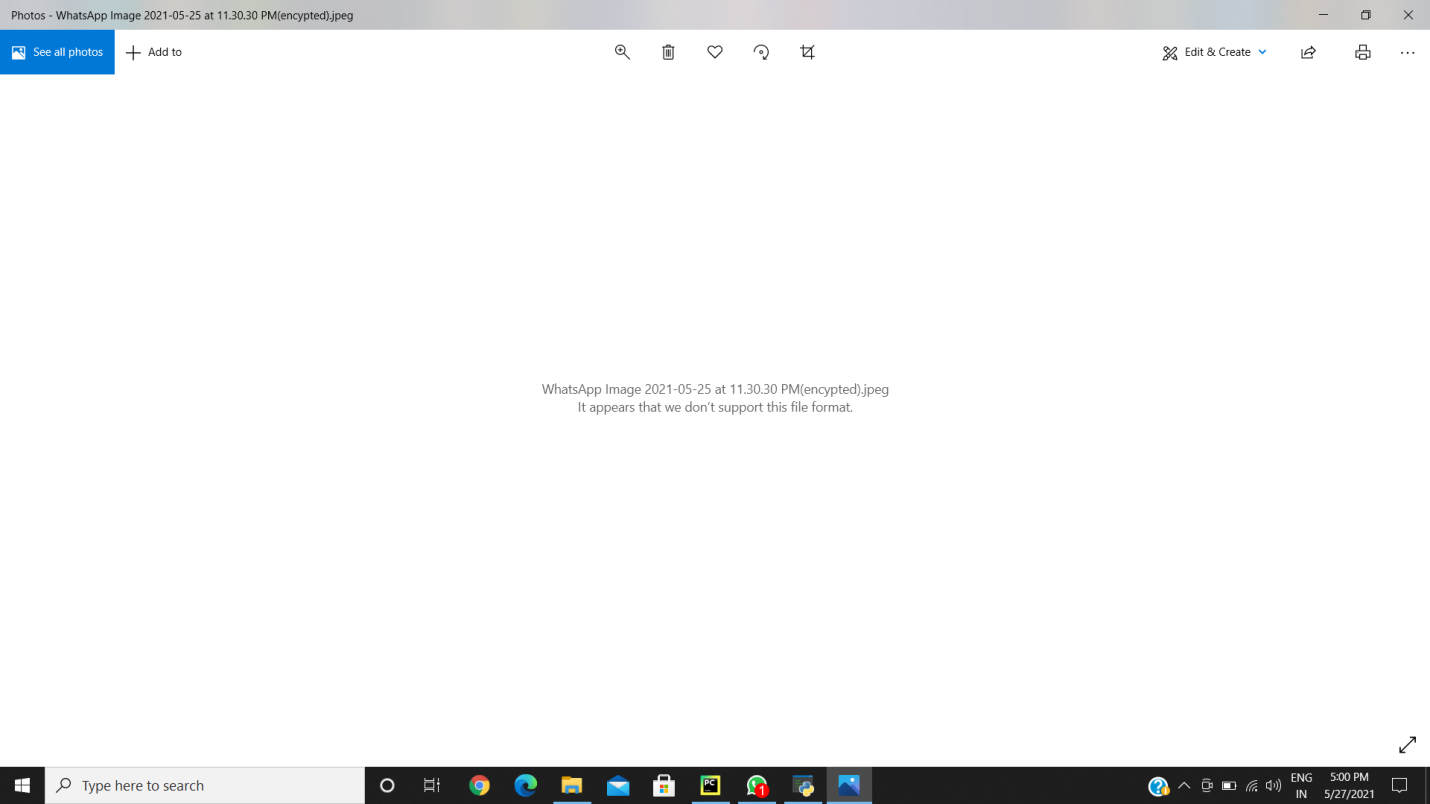
It is a reverse process of Image encryption. In this method encrypted image is considered as input for DES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are same as DES algorithm block length. Primarily function blocks of 64-bit size are entered. Then same secrecy key that is decryption key used for process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption. After completion of decryption, obtained output is considered as decrypted image, it follows the same characteristic of original image.

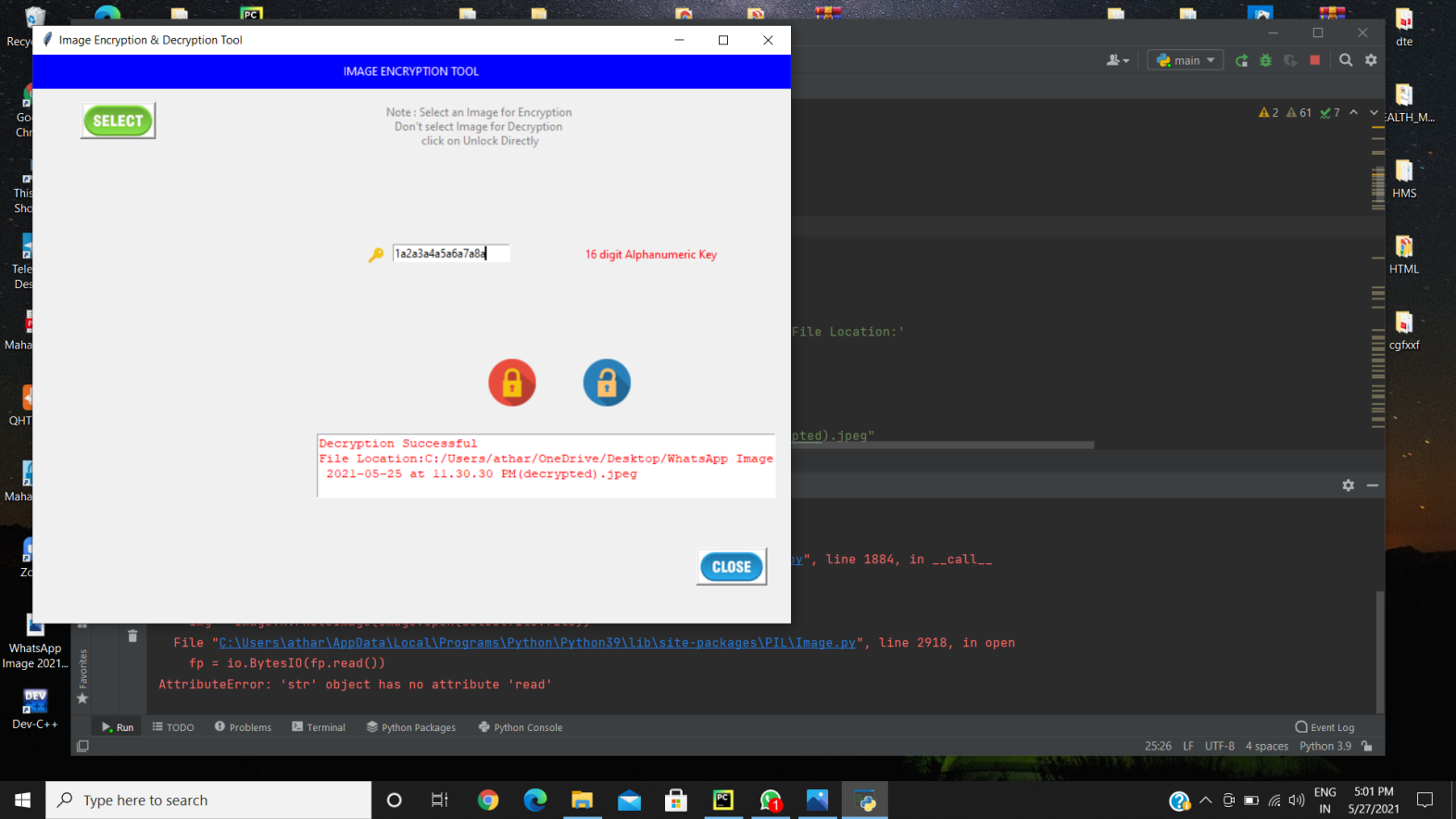
**SNAPSHOT**

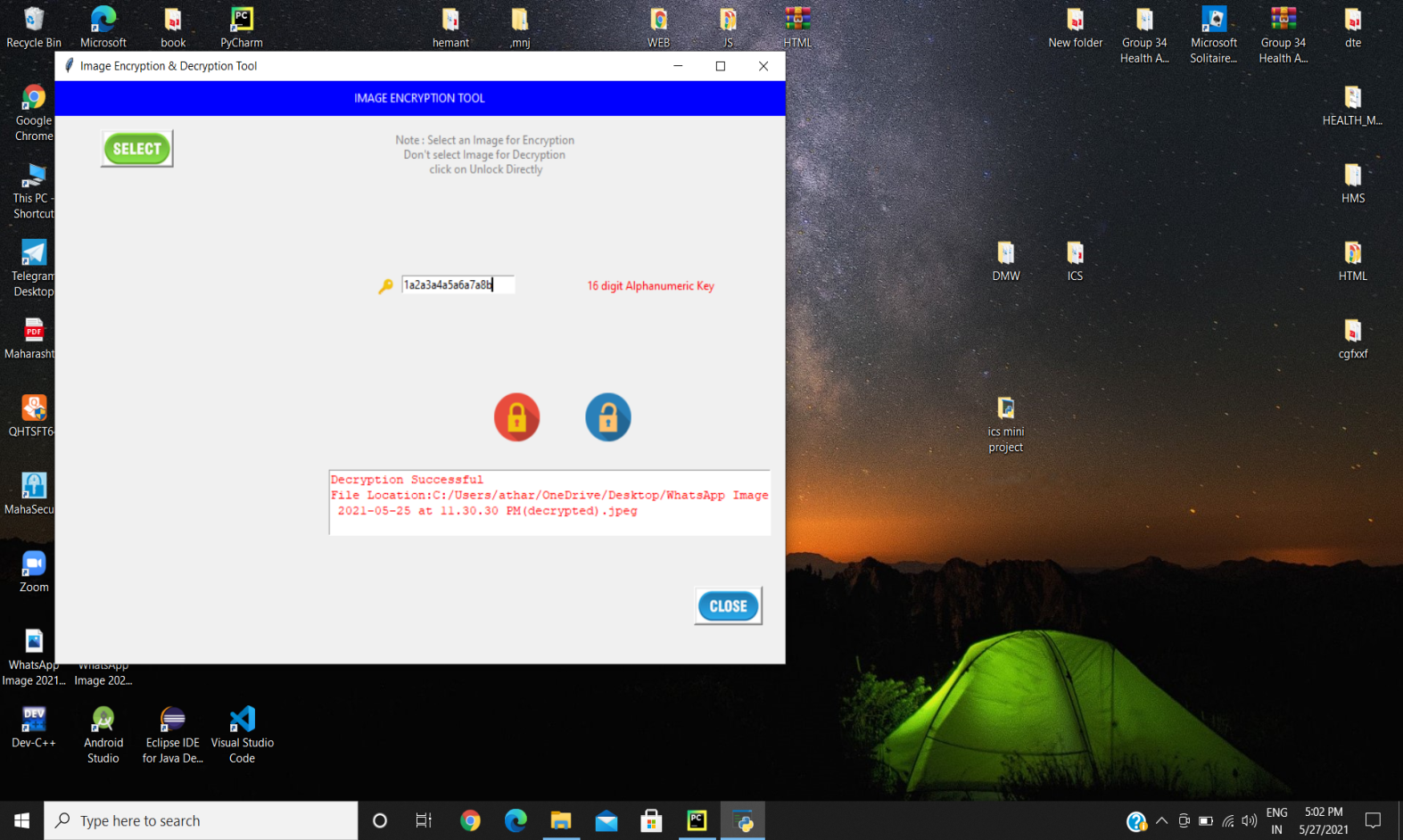












**ADVANTAGES AND DISADVANTAGES**

##### **Advantages**

* The image can only be viewed by the receiver as the image is encrypted using Triple DES and the key is only known to the sender and receiver.
* Since the image is encrypted using Triple DES, it is more secure than DES.
* Since the key is entered by the sender and receiver and is not stored in the database, it makes the encryption and decryption more secure.

##### **Disadvantages**

* The file size to be transmitted becomes large since it contains encrypted data.
* Since the file size is huge it can be suspected to contain some critical information.

**CONCULSION**

Encryption and decryption is done by using DES algorithm, by providing required security for image between two authorized users or clients. In our project DES guarantee the unbreakable security for color image. In the project image encryption is done using DES algorithm, Experimental consequences of proposed DES algorithm is very motivating.

The implementation approach shows the encrypted and decrypted image and also historical analysis is done with enhanced techniques.

Another future plan is of applying this proposed DES method for encrypting the video file to providing secure transmission in communication channels.

#### REFERENCES

1. R. Huang and K. Sakurai,“A robust and compression- combined digital image encryption method based on compressive sensing,”.The7t International Conference on IIH-MSP, Dalian, Oct.2014–16 2011, pp. 105–108.
2. A K Mandal, C Parakash and Mrs. A Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES”, IEEE Students’ Conference on E and E,C S, pp. 1-5, 2012.

[3]A. Yahya and A. Abdalla, “A shuffle image-encryption algorithm, “Journal of Computer Science, pp. 999–1002, Dec. 2008.

1. Zhang Yun, Liu Wei, Shui-ping, Zhai Z-jun , “Digital image encryption algorithm based on chaos and improved DES”, IEEE Conference on Systems, Man and Cybernetics, 2009.
2. Sesha P Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011
3. Mohammad Ali B Y and Aman J, “An Image Encryption Approach Using Combination of Permutation Technique Followed by Encryption”, International Journal of Computer Science and Network Security, VOL.8, April 2008.
4. Amitava Nag, Jyoti Prakash, Srabani Khan, Saswati Ghosh,” Image Encryption Using Affine Transform and XOR Operation “,International Conference on ICSCCN 2011.
5. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of CS and NS, VOL.8 No.12, pp. 280- 286, December 2008.
6. Shashi Mehrotra Seth, Rajan ishra, “Comparative Analysis of Encryption Algorithms for Data Communication”, International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.
7. W. Stallings, Cryptography and Network Security, 5th ed. New York, USA: Prentice Hall, 2011, pp. 77–96.