### Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption

A mini project report submitted in partial fulfillment of the requirements for the degree of Third Year Engineering in Information Technology

By

Sonia Bhandi (171051002)

Kamesh Phegade (171051030)

Amritdas Vaishnav (171051063)

Guide

Mrs. Supriya Joshi



Department of Information Technology

A. C. Patil College of Engineering, Kharghar, Navi Mumbai University of Mumbai

2020-2021

Jawahar Education Society’s

1. C. Patil College of Engineering, Kharghar

CERTIFICATE

This is to certify that the Mini Project entitled

**Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption**

is a bonafide work of Sonia bhandi,Kamesh Phegade,Amritdas Vaishnav

submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of Third Year Engineering in Information Technology.

Guide \_\_\_\_\_\_\_\_\_\_\_\_\_\_ HOD \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Principal

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Final Project Report Approval for B. E.

This project report entitled Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption by Amritdas, Sonia, Kamesh is approved for the degree of Fourth Year Engineering in Information Technology.

Examiner1 Examiner 2

Name: Name:

Date: Date:

Place: Place:

DECLARATION

I declare that this written submission represents my ideas in my own words and where others ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea / data / fact / source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Signatures

Sonia Bhandi (171051002)

Kamesh Phegade (171051030)

Amritdas Vaishnav (171051063)

Date:

Abstract

Reversible data hiding (RDH) in images is a technique, by which the original cover can be lossless recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed. Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content’s confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.

# Contents

|  |  |
| --- | --- |
| **Abstract**  **List of Figures**  **1 Introduction** | **i iii 1** |
| 1.1 Proposed system . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 2 |
| 1.2 Scope . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 2 |
| **2 Literature Survey** | **3** |
| **3 Description of Modules** | **8** |
| 3.1 Working Features . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 8 |
| 3.1.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 8 |
| 3.1.2 Working. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 8 |
| 3.1.3 Description of Modules . . . . . . . . . . . . . . . . . . . . . . . . .. | 9 |
| 3.2 Design . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 13 |
| 3.2.3 Use Case Diagram . . . . . . . . . . . . . . . . . . . . . . . . . . .. | 15 |
| **4 Result** | **16** |
| **5 Gantt chart** | **17** |
| **6 Conclusion** | **18** |

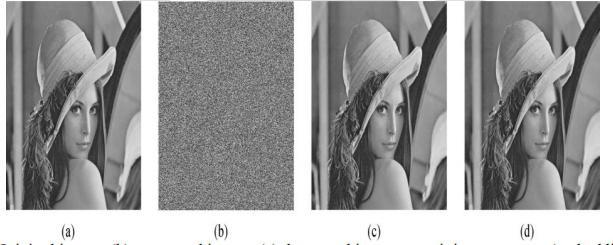
# List of Figures

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Description** | **Page No.** |
| 1.1 | Images after encryption & decryption. | 03 |
| 3.1 | Use Case Diagram | 12 |
| 4.1 | Result | 12 |
| 4.2 | Result | 13 |
| 5.1 | Gantt chart | 16 |

## Chapter 1 Introduction

Nowadays, the amount of digital images has increased rapidly hence the protection of multimedia data is becoming very important for many applications, e.g., confidential transmission, military and medical applications.The transmission of images is a daily routine and to decrease the transmission time it is necessary to find an efficient way to transmit them over networks.This can be done with the help of various RDH algorithms.

The proposed method in this project is a framework same as the reserving room before encryption. In the previous method the data embedded can be available without any error after the decryption of the encoded data. But the cover that is the image which contains the data cannot be effectively rebuilt. That is the major drawback of the frame woke mentioned previously. To overcome this, in this project the reversible data hiding scheme is replaced by a rational rhombus method. It is the best technique to use in RDH. The algorithm used for the rational rhombus method is simple and it provide cover image without any loss.



#### Existing System

1. Steganography is a technique used to hide a message inside an image. Reversible steganography aims at recovering cover image without distortions while extracting secret messages at the receiver side. The two main existing problems in steganography are, how to obtain high embedding capacity without compromising on the cover image quality, and confidentiality of embedded messages. In this paper, we present a new technique of reversible steganography using the IMNP algorithm with DES preprocessing of embedded messages. IMNP algorithm allows to maintain good image quality and increases embedding capacity. DES preprocessing provides an extra layer of security to message. The experimental results show that the proposed technique outperforms existing techniques of Steganography in terms of embedding capacity and image quality. It further provides good security to messages. By M.Murali Krishna, Nirmal Roberts.
2. Reversible data hiding by reserving room becomes more prominent, since the original cover is restored without any loss after the hidden data is extracted.

Encryption is performed to provide the confidentiality for the image content. In this project,space for embedding data is reserved with pairwise prediction error expansion(PEE) and histogram shift before encryption has been performed, so that data hider can reversibly embed data into an encrypted image easily. Image redundancy is better exploited in prediction error expansion which leads to superior performance. But in the current PEE based method, correlation within prediction error is not better exploited. Hence to better exploit the correlation among prediction errors, two prediction errors are jointly considered. Then the embedding is based on the prediction error pair and its 2D prediction-error histogram, which leads to improved performance. Secret data extraction and image restoration in this method.

By this method, higher PSNR is achieved than any other method in reversible data hiding.\_by S. Ariavazhang,c. Karthika.

1. In the past two decades, reversible data hiding (RDH), also referred to as lossless or invertible data hiding, has gradually become a very active research area in the field of data hiding. This has been verified by more and more papers on increasingly wide- spread subjects in the field of RDH research that have been published these days. In this paper, the various RDH algorithms and researches have been classified into the following six categories: 1) RDH into image spatial domain; 2) RDH into image compressed domain (e.g., JPEG); 3) RDH suitable for image semi-fragile authentication; 4) RDH with image contrast enhancement; 5) RDH into encrypted images, which is expected to have wide application in the cloud computation; and 6) RDH into video and into audio. For each of these six categories, the history of technical developments, the current state of the arts, and the possible future research are presented and discussed. It is expected that the RDH technology and its applications in the real word will continue to move ahead.\_by Yun-Qing shi,

XiaoLong Li

1. Reversible data hiding in encrypted images (RDHEI) is an effective technique to embed data in the encrypted domain. An original image is encrypted with a secret key and during or after its transmission, it is possible to embed additional information in the encrypted image, without knowing the encryption key or the original content of the image. During the decoding process, the secret message can be extracted and the original image can be reconstructed. In the last few years, RDHEI has started to draw research interest. Indeed, with the development of cloud computing, data privacy has become a real issue. However, none of the existing methods allow us to hide a large amount of information in a reversible manner. In this paper, we propose a new reversible method based on MSB (most significant bit) prediction with a very high

capacity. We present two approaches, these are: high capacity reversible data hiding approach with correction of prediction errors and high capacity reversible data hiding approach with embedded prediction errors. With this method, regardless of the approach used, our results are better than those obtained with current state of the art methods, both in terms of reconstructed image quality and embedding capacity. By Pauline Puteaux,William puech

#### Problem Definition

To develop a GUI based Desktop application for encryption and decryption in an image,with the cryptography and steganography techniques and using RSA algorithm without changing or disturbing the quality of the picture or image.

## Chapter 2 Literature survey

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Paper | Authors, year | Technique Used | Advantages | Drawbacks |
| Reversible image watermarking using interpolation technique [1]L. Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong, "Reversible Image Watermarking Using Interpolation Technique," March 2010. | Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong .2010 | the interpolation-error, the difference between interpolation value and corresponding pixel value | Can achieve better image quality.  Cost of computation is small | Any mistake in the calculation of interpolation will affect the secret information |
| Separable reversible data hiding in encrypted image[2]X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," April 2012. | X,Zhang, 2012 | image encryption,data embedding and data extraction/image-recovery phases | Simple Less computation | Data compression is not efficient |
| Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption[4] K. Ma, W. Zhang, X. Zhao, N. Yu and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," March 2013 | Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li | Traditional RDH method ,Histogram shifting. | achieve real reversibility, separate data extraction | Overflow/underflow occurs |
| Improving various reversible data hiding schemes via optimal codes for binary covers[3] W. Zhang, B. Chen and N. Yu, "Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers," June 2012. | W. Zhang, B. Chen, and &. Yu2012 | Decompression algorithm as the coding scheme for embedding data | proved to be optimal | problem is whether there exists other more effective modifying methods or not |

**Chapter 3 Description of Modules**

* 1. **Working Features**
     1. **Introduction:**

RSA algorithm RSA (Rivest–Shamir–Adleman) is an [algorithm](https://simple.wikipedia.org/wiki/Algorithm) used by modern computers to [encrypt](https://simple.wikipedia.org/wiki/Encryption) and decrypt messages. It is an asymmetric [cryptographic](https://simple.wikipedia.org/wiki/Cryptography) [algorithm](https://simple.wikipedia.org/wiki/Algorithm). Asymmetric means that there are two different [keys](https://simple.wikipedia.org/wiki/Key_(cryptography)). This is also called [public key cryptography](https://simple.wikipedia.org/wiki/Public-key_cryptography), because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the [factors](https://simple.wikipedia.org/wiki/Factorization) of a large [composite number](https://simple.wikipedia.org/wiki/Composite_number) is difficult: when the factors are [prime numbers](https://simple.wikipedia.org/wiki/Prime_number), the problem is called [prime factorization](https://simple.wikipedia.org/wiki/Prime_factorization). It is also a key pair (public and private key) generator.

Steganography-

Steganography is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties. Unlike cryptography, which conceals the contents of a secret message, steganography conceals the very fact that a message is communicated.

* + 1. **Working:**

The user can browse the image from the files.After browsing of the image,the user can redefine the value of n , e, and d or they can go with the default value.After selection of n ,d, and e the user will be prompted to enter the text and it will be converted into Ciphertext.The blocks of cipher text will be printed.This is the process of encryption.

For the process of Decryption the user can select the image which he or she wants to decrypt and with the help of RSA algorithm the cipher text is decrypted and the text hidden is retrived.

* + 1. **Description of Modules:**

Modules under Proposed System are:

**Encrypted image generation:**

Encryption using RSA algorithm.

**Image encryption :**

The encryption is done by XORing the image with the key.

#### Data hiding in encrypted image :

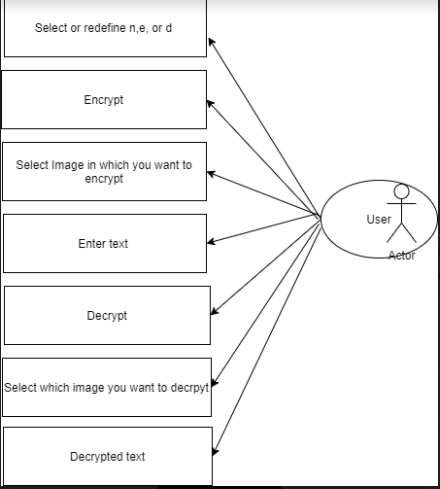
We can embed some data into it , although we cannot get the access to the original image.

#### Data extraction and image recovery :The data can be recovered from the image without the loss of the quality of image.

#### 3.1.4 Software and Hardware Requirements:

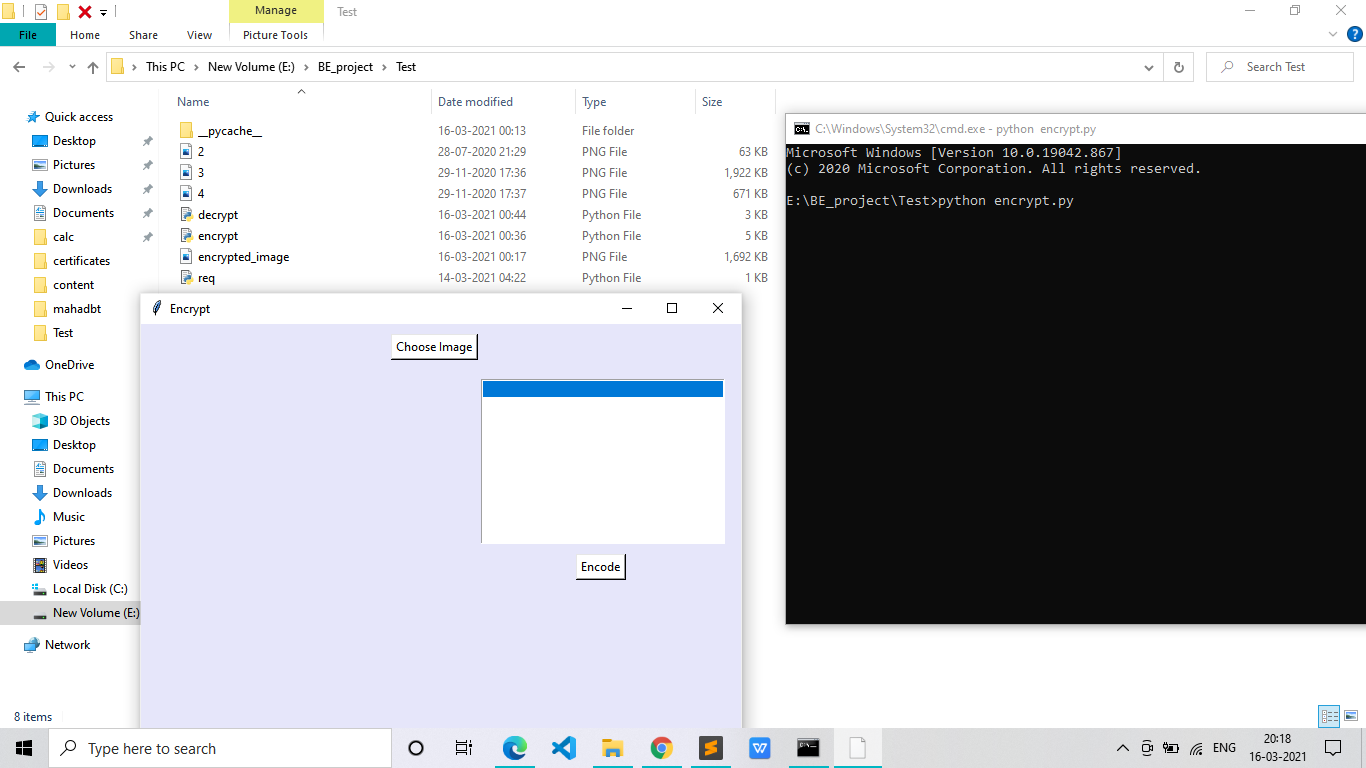
* + - 1. **Software** – Sublime text editor.Python
      2. **Hardware** – Computer/Laptop
      3. **Mechanism**– Front end and Back end development with database and API

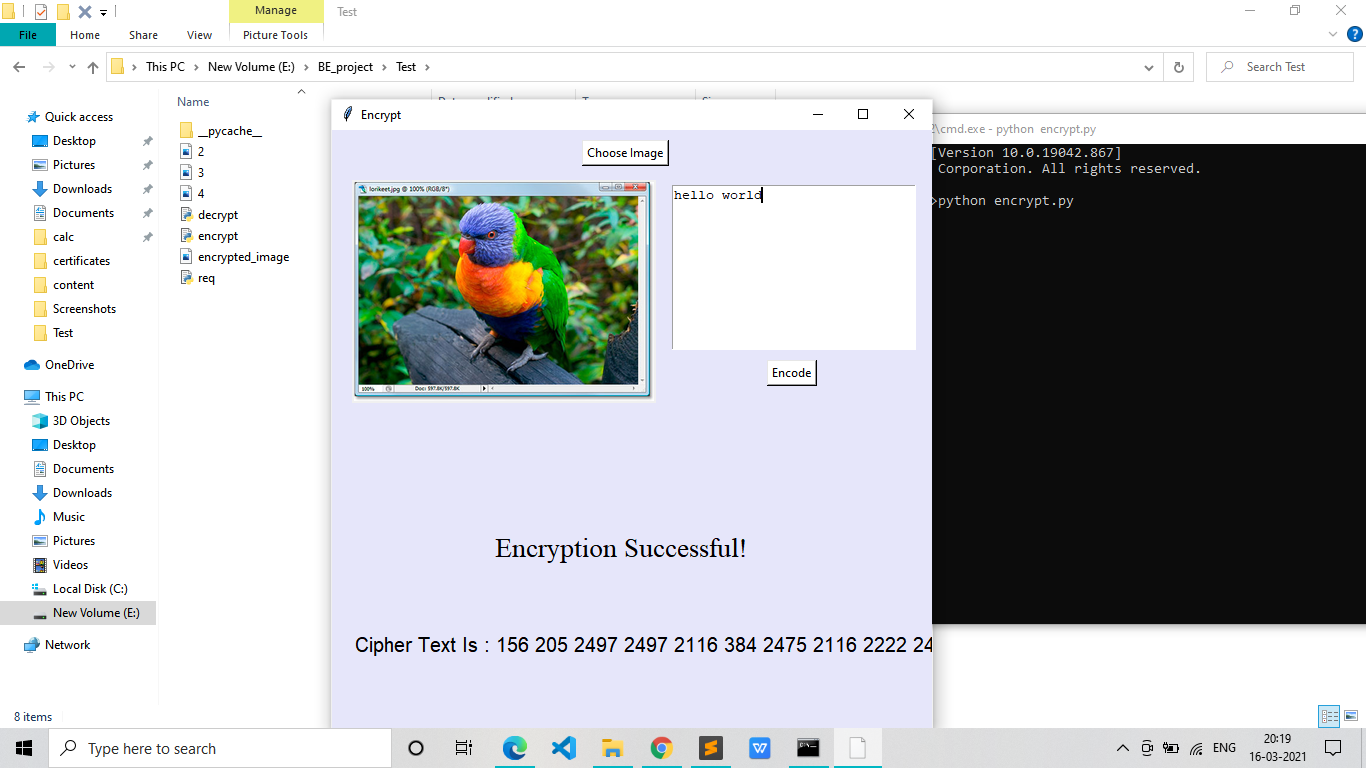
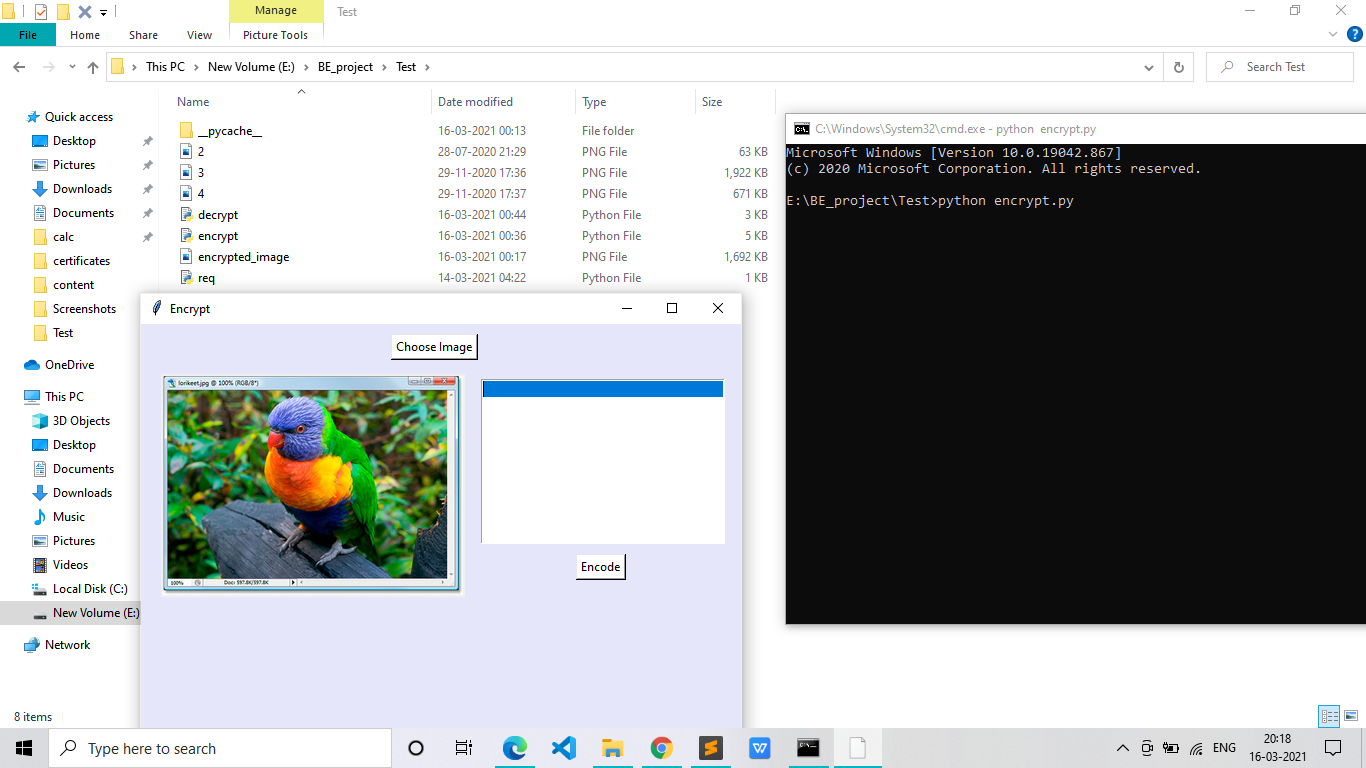
**Fig 3.2 Use case diagram**

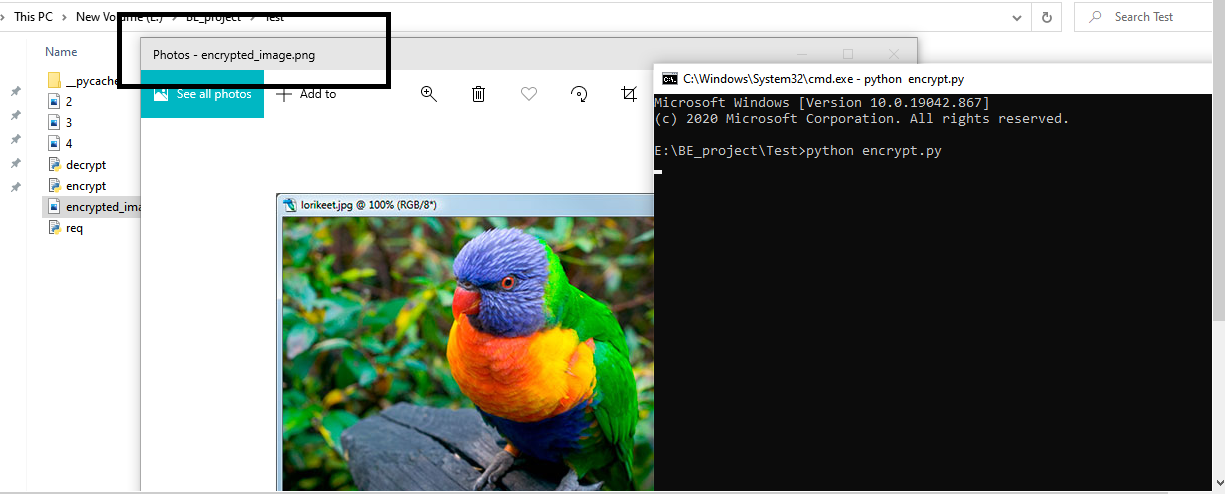


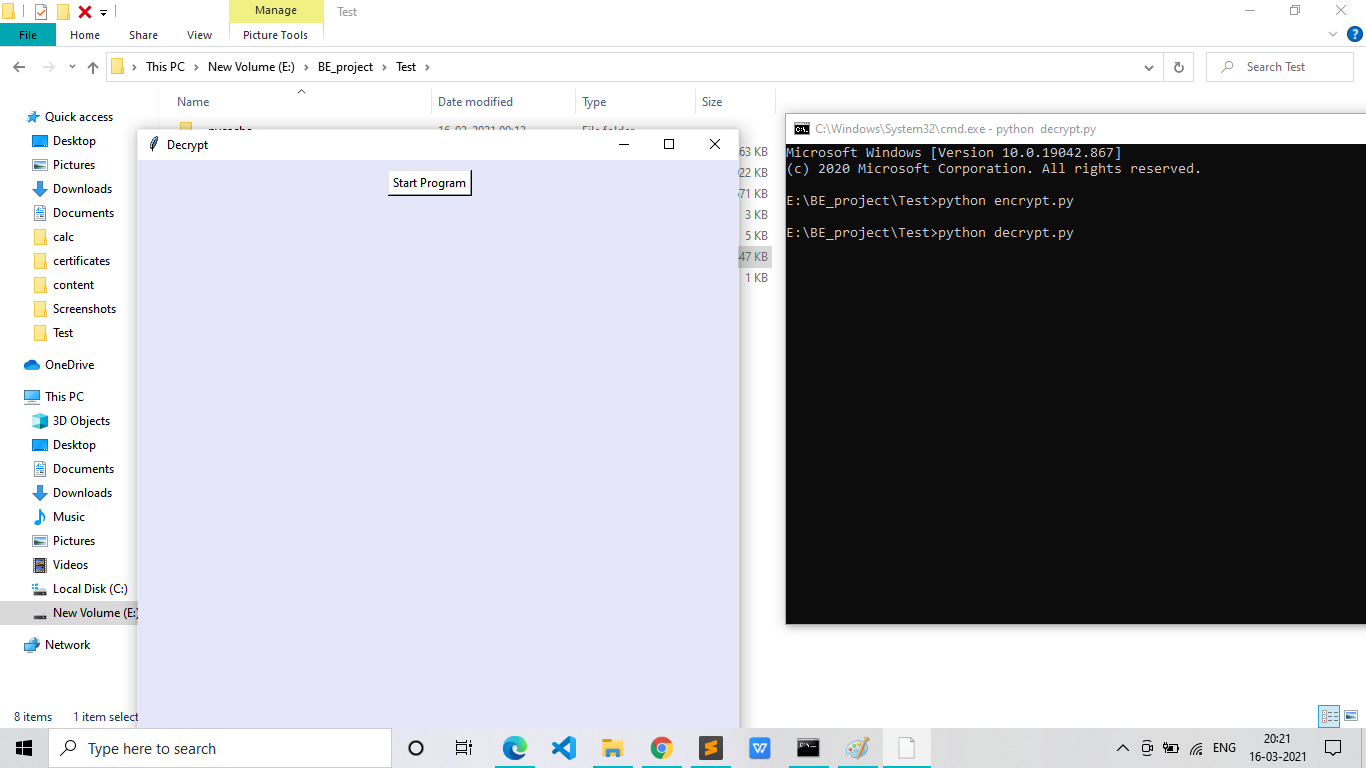
Chapter 4

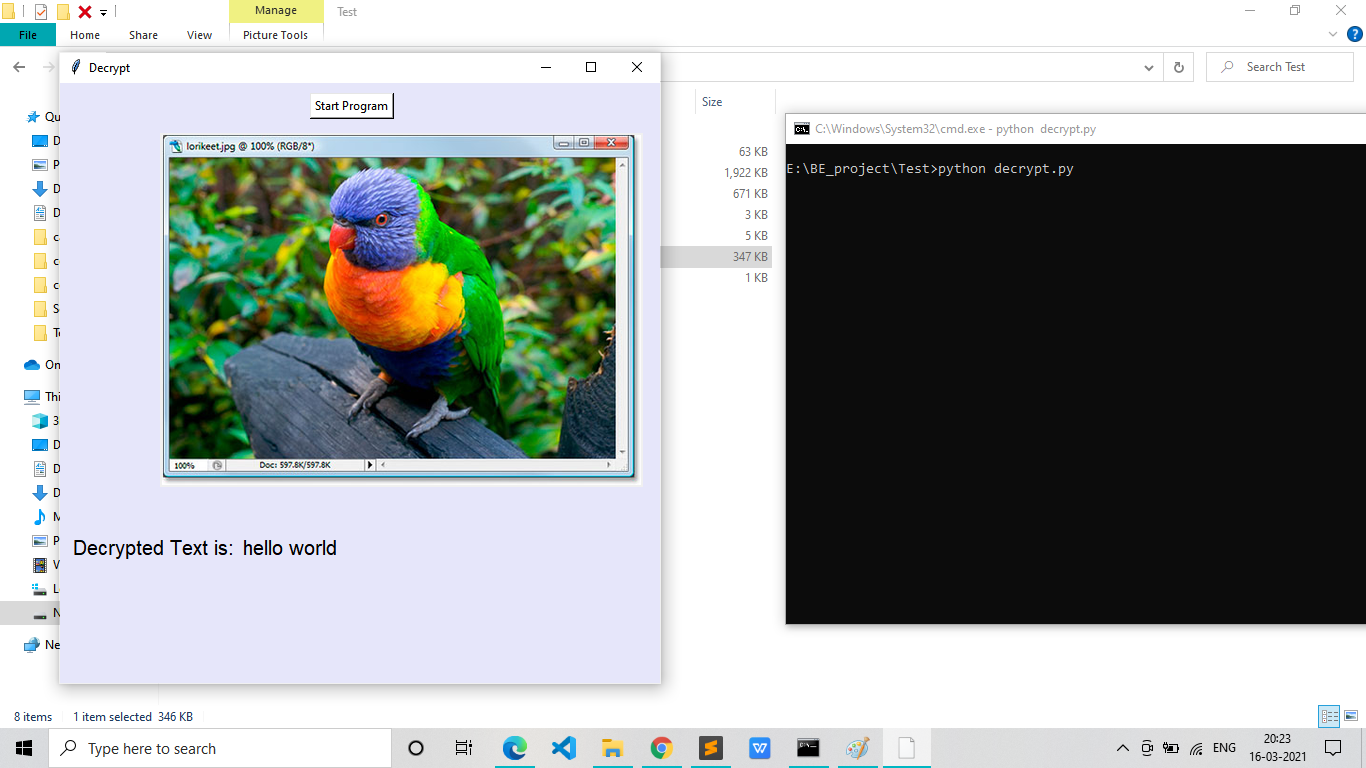
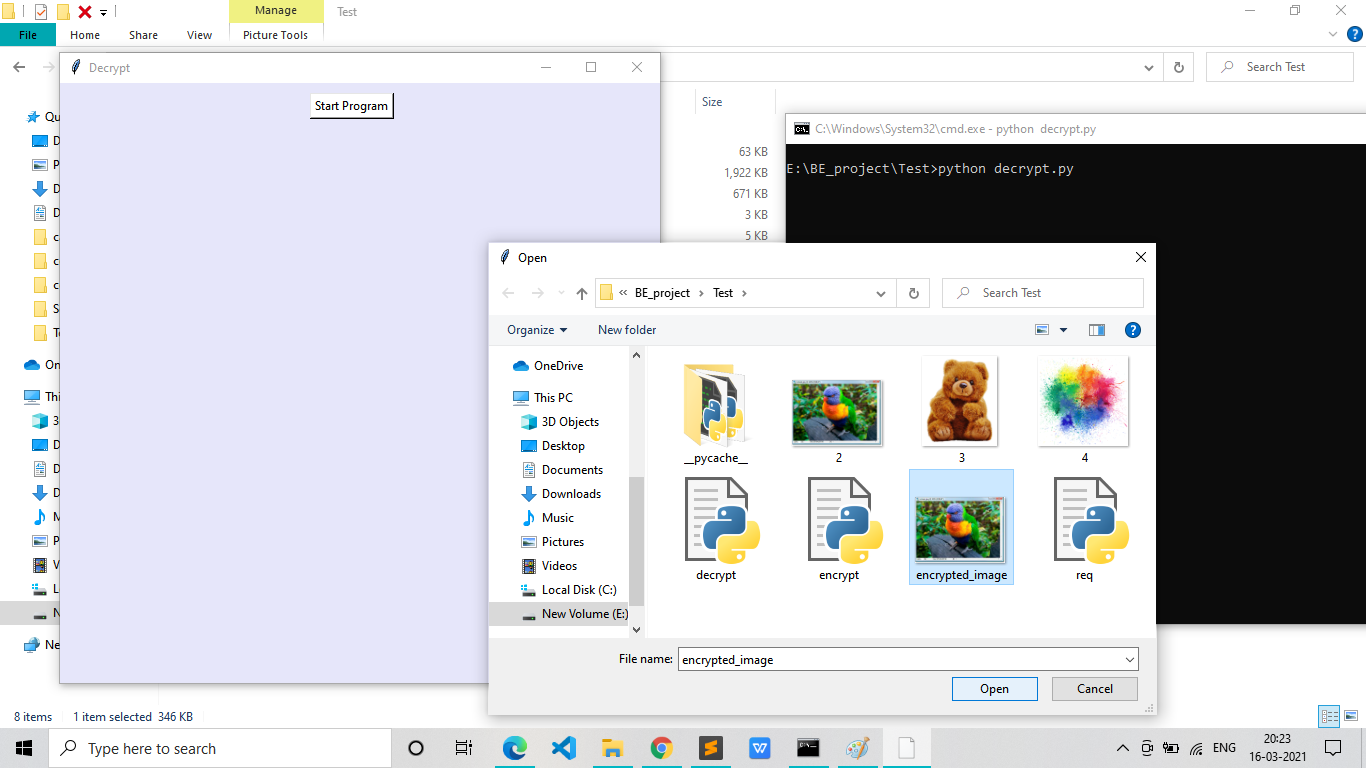
Result











Chapter 5 Plan of work

In this section, we shall show the month wise plan to complete our project (timeline/Gantt chart).



**Fig 5.1: Gantt chart**

Chapter 6 Conclusion

Reversible data hiding (RDH) in encrypted images is widely used to obtain security . Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to our proposed method which is by reserving room before encryption. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

As a result,the original quality is not deteriorated unlike in the existing system.

The sender and the receiver are able to obtain the image with the same resolution and quality.

# Bibliography

##### 1.Reversible data hiding in encrypted images by reserving room before encryption,Veena N Bhat,Navin Y.

2.M.U.Celik,G.Sharma,A.M.Tekalp,”Lossless generalized-LSB data embedding”.

3. L. Luo, Z. Chen, M. Chen, X. Zeng and Z. Xiong, "Reversible Image Watermarking Using Interpolation Technique," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 187-193, March 2010.

4. X. Zhang, "Separable Reversible Data Hiding in Encrypted Image," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 826-832, April 2012.

5. W. Zhang, B. Chen and N. Yu, "Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers," in IEEE Transactions on Image Processing, vol. 21, no. 6, pp. 2991-3003, June 2012.

Acknowledgment

We thank our college Principal Dr. V. N. Pawar sir for providing the required resources for the development of the project. Our sincere thanks to my Project Guide Mrs.Supriya Joshi Maam for helping, suggesting new ideas and guiding us throughout the semester. I am also grateful to all the faculty members for their support and encouragement.

Date: