**A**

**MINI PROJECT REPORT**

**on**

**BEHIND THE IMAGES**

**BE(AI&DS)-III Sem**

**By**

**Akshitha Thokala (160121771072)**

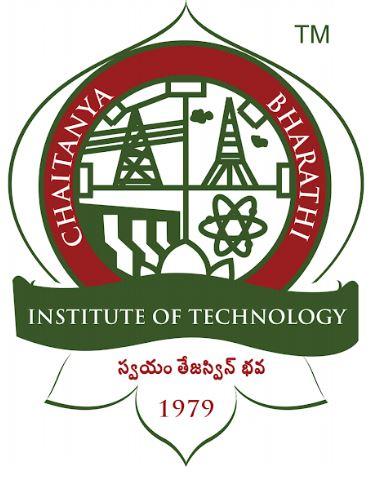
**Buggala Jahnavi (160121771075)**

**Under the guidance of**

**Dr. Pragati Priyadarshinee**

**Assistant Professor**

**IT Department**



**DEPARTMENT OF INFORMATION TECHNOLOGY   
CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)**

**(Affiliated to Osmania University; Accredited by NBA(AICTE) and NAAC(UGC), ISO Certified 9001:2015)**

**KOKAPET(V), GANDIPET(M), RR District HYDERABAD - 75**

**Website:** [**www.cbit.ac.in**](http://www.cbit.ac.in/)

**2022-2023**

****

This is to certify that the project work entitled “**BEHIND THE IMAGES**” submitted to CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY, in fulfillment of the requirements for the completion of Mini Project-I of III Semester B.E. in Artificial Intelligence and Data Science, during the Academic Year 2022-2023, is a record of original work done by **Akshitha Thokala (160121771075) and Buggala Jahnavi (160121771075)** during the period of study in the Department of IT, CBIT, HYDERABAD, under our guidance.

|  |  |
| --- | --- |
| **Project Guide** | **Head of the Department** |
| **Dr. Pragati Priyadarshinee** | **Dr. K. Radhika** |
| Assistant Professor, Dept. of IT, | Professor, Dept. of IT, |
| CBIT, Hyderabad. | CBIT, Hyderabad. |

## ACKNOWLEDGEMENTS

We would like to express our heartfelt gratitude to **Dr. Pragati Priyadarshinee**, our project guide, for her invaluable guidance and constant support, along with her capable instruction and persistent encouragement.

We are grateful to our Head of Department, **Dr. K. Radhika**, for her steady support and for the provision of every resource required for the completion of this project.

We would like to take this opportunity to thank our Principal, **Dr. P. Ravinder Reddy**, as well as the Management of the Institute, for having designed an excellent learning atmosphere.

Our thanks are due to all members of the staff and our lab assistants for providing us with the help required to carry out the groundwork of this project.

**ABSTRACT**

Image steganography using passwords developed with Python programming is a technique for hiding secret information inside an image while encrypting it with a password to ensure security. This method involves utilizing the LSB (Least Significant Bit) algorithm to embed the secret message into the pixels of the cover image. The password is then used to encrypt the secret message and the modified cover image using an LSB algorithm. The developed program provides an intuitive and easy-to-use interface for users to select the cover image, input the secret message and password, and generate the steganographic image. The program utilizes Python libraries such as tkinter to implement the steganography algorithm and encryption process. This technique offers a high level of security and confidentiality for communication and data exchange. The program is efficient, reliable, and can be used for various applications that require secure communication and data exchange.

**CONTENTS**

|  |  |  |
| --- | --- | --- |
| **S. No** | **Topics** | **Page. No** |
|  | **Acknowledgements** |  |
|  | **List of figures** |  |
|  | **Abstract** | iv |
| 1 | **Introduction** | 1 |
| * 1. Motivation | 1 |
| 1.2 Problem Statement | 1 |
| 2 | **System Requirements** | 2 |
| 2.1 Hardware specifications | 2 |
| 2.2 Software specifications | 2 |
| 3 | **Proposed Methodology** | 2 |
| 3.1 System Design | 3 |
| 3.2 Existing System | 3 |
| 3.3Proposed System | 4 |
| 4 | **Implementation** | 5-9 |
| 5 | **Results** | 10-18 |
| 6 | **Conclusion** | 19 |
| 7 | **Future Scope** | 20 |
| 8 | **Bibliography** | 21 |

## 

1. **INTRODUCTION**

Image steganography using password encryption is a technique that hides secret information inside an image while also encrypting it with a password to ensure security. The approach involves embedding the secret message into the least significant bits of the pixels of the cover image. The password is then used to encrypt the secret message and the modified cover image. This method ensures that only the intended recipient, who has the correct password, can extract the secret message. The technique is efficient, secure, and can be used for various applications such as military, medical, and personal communication.

Image steganography is a technique used to hide secret information inside an image without altering its visual quality. It is a form of data hiding that aims to protect sensitive information by embedding it into a cover image that is innocuous and unremarkable. The objective of image steganography is to ensure that only the intended recipient can extract the secret information, while others are unable to detect its presence. The technique involves manipulating the least significant bits (LSBs) of the pixels in the image to store the hidden message. The LSBs are modified in a way that is imperceptible to the human eye but can be detected by a steganalysis tool. Image steganography can be used for various applications, including military, medical, and personal communication, where confidentiality and security are of utmost importance. The effectiveness of image steganography depends on the algorithm used to embed the secret message, the cover image selected, and the steganalysis techniques used to detect the hidden message.

**LITERATURE SURVEY**

Steganography is the art of hiding secret messages or information within an innocuous medium in such a way that the existence of the message is undetectable. Steganography techniques are widely used in various fields such as military, intelligence, and cybersecurity to protect information from unauthorized access. Here is a literature survey on steganography:

"A Survey of Steganography Techniques in Image, Audio and Video Files" by S. S. Maitra and S. K. Bakshi. This paper provides a comprehensive survey of the different types of steganography techniques used in image, audio and video files. The paper discusses the advantages and disadvantages of each technique and also provides a comparison between the techniques.

"A Review of Audio Steganography Techniques" by R. P. Singh and P. Gupta. This paper focuses on the steganography techniques used in audio files. The paper presents a comprehensive survey of the different types of audio steganography techniques and also provides a comparison between them.

"A Review of Text Steganography Techniques" by A. Jain and A. Kumar. This paper presents a survey of the different types of text steganography techniques. The paper provides an overview of the different techniques used for hiding information in text files.

"A Survey of Steganography in Social Media" by J. M. Al-Jarrah and A. M. Al-Qadi. This paper provides a comprehensive survey of steganography techniques used in social media. The paper discusses the advantages and disadvantages of each technique and also provides a comparison between them.

"A Review of Steganalysis Techniques for Detecting Hidden Information" by V. K. Sharma and R. Kumar. This paper focuses on steganalysis techniques used for detecting hidden information. The paper provides an overview of the different techniques used for detecting hidden information in image, audio, and video files.

"A Survey of Steganography Techniques in Cloud Computing" by Y. Zhang, C. Wang, and X. Liu. This paper presents a survey of the different types of steganography techniques used in cloud computing. The paper provides an overview of the different techniques used for hiding information in cloud storage systems.

"A Review of Steganography Techniques in Biometric Systems" by R. S. Das and S. K. Lenka. This paper presents a survey of steganography techniques used in biometric systems. The paper discusses the different types of steganography techniques used in biometric systems and also provides a comparison between them.

These papers provide a comprehensive overview of the different types of steganography techniques used in various fields. They also discuss the advantages and disadvantages of each technique and provide a comparison between the techniques

* 1. **MOTIVATION**

The motivation behind image steganography is to ensure the confidentiality and security of sensitive information while exchanging it through public communication channels. Traditional encryption techniques can be detected by an adversary, and once detected, they can be broken. However, steganography ensures that the presence of secret information is concealed, making it difficult for an adversary to detect and extract the hidden message. This provides an added layer of security, especially in applications such as military, espionage, and personal communication, where secrecy and confidentiality are paramount. In addition to security, image steganography also offers the advantage of being able to transmit additional data in an image that appears innocuous and unremarkable. As a result, it can also be used for digital watermarking, copyright protection, and other applications that require hiding data inside an image. The effectiveness of steganography techniques is always improving, making it an essential tool for secure communication and data exchange.

* 1. **PROBLEM STATEMENT**

One of the primary problems with traditional image steganography techniques is that anyone who has access to the steganographic image can extract the hidden message without any authentication. This poses a significant security risk, especially if the message is confidential and intended only for specific recipients. To address this problem, the use of password encryption has been proposed as an effective solution. However, the challenge is to design a robust image steganography technique that can not only hide the message but also encrypt it with a password to provide enhanced security. The proposed technique should be able to withstand various steganalysis attacks and maintain the quality of the cover image while hiding the secret message. Another challenge is to develop an efficient and user-friendly program to implement the steganography algorithm with password encryption, which can be used by both technical and non-technical users. Therefore, the problem statement for image steganography using password is to develop a robust and efficient steganography algorithm that can embed a secret message in an image while encrypting it with a password, and to create an intuitive program to implement the technique.

**2. SYSTEM REQUIREMENTS**

**2.1 HARDWARE SPECIFICATIONS-**

* + 1. Processor: intel COREi5, 5th Gen
    2. RAM: 8GB
    3. Disk Space: 10GB or more
  1. **SOFTWARE SPECIFICATIONS-**
     1. Operating System: Windows 10
     2. Programming Language: Python
     3. Other Applications: Visual studio code

**3. PROPOSED METHODOLOGY**

**3.1 SYSTEM DESIGN-**

**Visual Studio Code**, also commonly referred to as **VS Code**, is a [source-code editor](https://en.wikipedia.org/wiki/Source-code_editor) made by [Microsoft](https://en.wikipedia.org/wiki/Microsoft) with the [Electron Framework](https://en.wikipedia.org/wiki/Electron_(software_framework)), for [Windows](https://en.wikipedia.org/wiki/Windows), [Linux](https://en.wikipedia.org/wiki/Linux) and [macOS](https://en.wikipedia.org/wiki/MacOS).Features include support for [debugging](https://en.wikipedia.org/wiki/Debugging), [syntax highlighting](https://en.wikipedia.org/wiki/Syntax_highlighting), [intelligent code completion](https://en.wikipedia.org/wiki/Intelligent_code_completion), [snippets](https://en.wikipedia.org/wiki/Snippet_(programming)), [code refactoring](https://en.wikipedia.org/wiki/Code_refactoring), and embedded [Git](https://en.wikipedia.org/wiki/Git). Users can change the [theme](https://en.wikipedia.org/wiki/Theme_(computing)), [keyboard shortcuts](https://en.wikipedia.org/wiki/Keyboard_shortcut), preferences, and install [extensions](https://en.wikipedia.org/wiki/Plug-in_(computing)) that add additional functionality.

Visual Studio Code is a source-code editor that can be used with a variety of programming languages,including [C#](https://en.wikipedia.org/wiki/C_Sharp_(programming_language)), [Java](https://en.wikipedia.org/wiki/Java_(programming_language)), [JavaScript](https://en.wikipedia.org/wiki/JavaScript), [Go](https://en.wikipedia.org/wiki/Go_(programming_language)), [Node.js](https://en.wikipedia.org/wiki/Node.js), [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [C++](https://en.wikipedia.org/wiki/C%2B%2B), [C](https://en.wikipedia.org/wiki/C_(programming_language)), [Rust](https://en.wikipedia.org/wiki/Rust_(programming_language)) and [Fortran](https://en.wikipedia.org/wiki/Fortran).It is based on the [Electron](https://en.wikipedia.org/wiki/Electron_(software_framework)) framework,which is used to develop [Node.js](https://en.wikipedia.org/wiki/Node.js) [web applications](https://en.wikipedia.org/wiki/Web_application) that run on the [Blink layout engine](https://en.wikipedia.org/wiki/Blink_layout_engine). Visual Studio Code employs the same editor component (codenamed "Monaco") used in [Azure DevOps](https://en.wikipedia.org/wiki/Azure_DevOps_Server) (formerly called Visual Studio Online and Visual Studio Team Services).

Out of the box, Visual Studio Code includes basic support for most common programming languages. This basic support includes [syntax highlighting](https://en.wikipedia.org/wiki/Syntax_highlighting), [bracket matching](https://en.wikipedia.org/wiki/Bracket_matching), [code folding](https://en.wikipedia.org/wiki/Code_folding), and configurable snippets. Visual Studio Code also ships with [IntelliSense](https://en.wikipedia.org/wiki/Intelligent_code_completion) for JavaScript, TypeScript, [JSON](https://en.wikipedia.org/wiki/JSON), [CSS](https://en.wikipedia.org/wiki/CSS), and [HTML](https://en.wikipedia.org/wiki/HTML), as well as debugging support for Node.js. Support for additional languages can be provided by freely available extensions on the VS Code Marketplace.

Instead of a project system, it allows users to open one or more directories, which can then be saved in workspaces for future reuse. This allows it to operate as a [language-agnostic](https://en.wikipedia.org/wiki/Language-agnostic) code editor for any language. It supports many programming languages and a set of features that differs per language. Unwanted files and folders can be excluded from the project tree via the settings. Many Visual Studio Code features are not exposed through menus or the user interface but can be accessed via the command palette.

Visual Studio Code can be extended via [extensions](https://en.wikipedia.org/wiki/Plug-in_(computing)), available through a central repository. This includes additions to the editor and language support. A notable feature is the ability to create extensions that add support for new [languages](https://en.wikipedia.org/wiki/Programming_language), [themes](https://en.wikipedia.org/wiki/Theme_(computing)), [debuggers](https://en.wikipedia.org/wiki/Debugger), [time travel debuggers](https://en.wikipedia.org/wiki/Time_travel_debugging), perform [static code analysis](https://en.wikipedia.org/wiki/Static_code_analysis), and add [code linters](https://en.wikipedia.org/wiki/Lint_(software)) using the [Language Server Protocol](https://en.wikipedia.org/wiki/Language_Server_Protocol).

**3.2 EXISTING SYSTEM-**

There are several existing systems for image steganography that do not use password encryption. These systems primarily use the least significant bit (LSB) algorithm to hide the secret message in the image. One of the most popular methods is LSB replacement, which involves replacing the LSB of each pixel in the cover image with the corresponding bit of the secret message. Another method is LSB matching, which involves modifying the LSBs of the cover image to match the secret message. These techniques are simple and efficient, but they lack security since anyone who has access to the steganographic image can extract the hidden message.

Other existing systems use more sophisticated algorithms to improve security, such as the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT). These methods involve transforming the image to a different domain, where the secret message is embedded, and then transformed back to the image domain. These methods provide increased security, but they are more complex and require more processing power.

Overall, the existing systems for image steganography are effective in hiding the secret message, but they lack the added security of password encryption. Therefore, there is a need for a more robust system that uses password encryption to ensure the confidentiality and security of the hidden message.

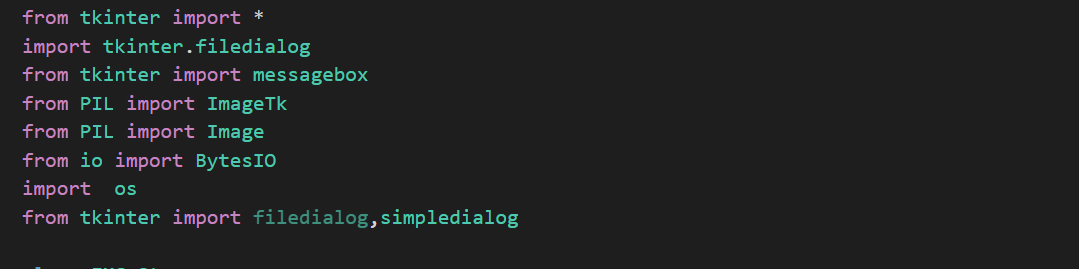
**3.3 PROPOSED SYSTEM-**

The application is based on the user. Here users are the receiver and sender.

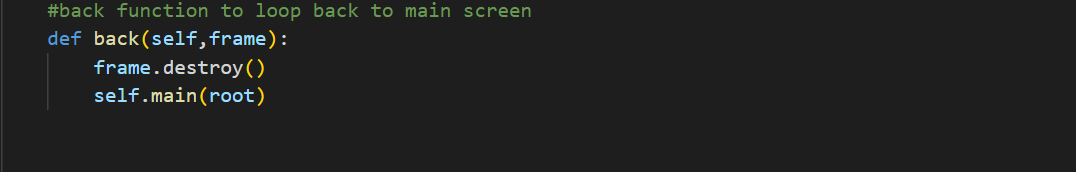
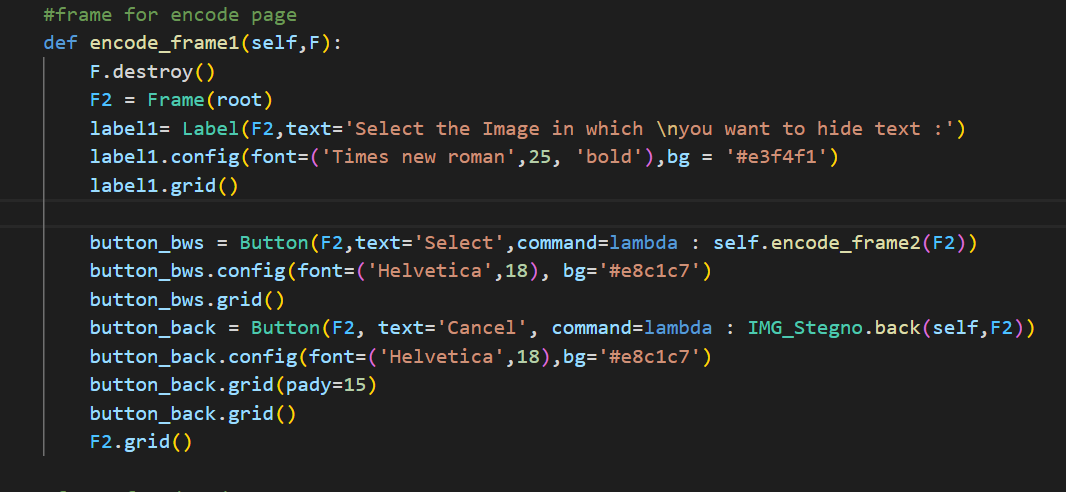
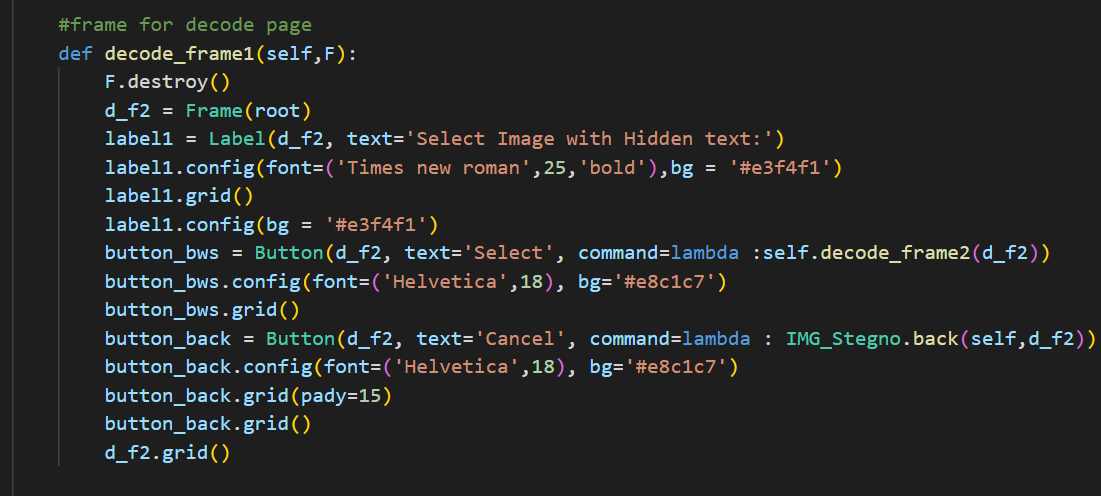
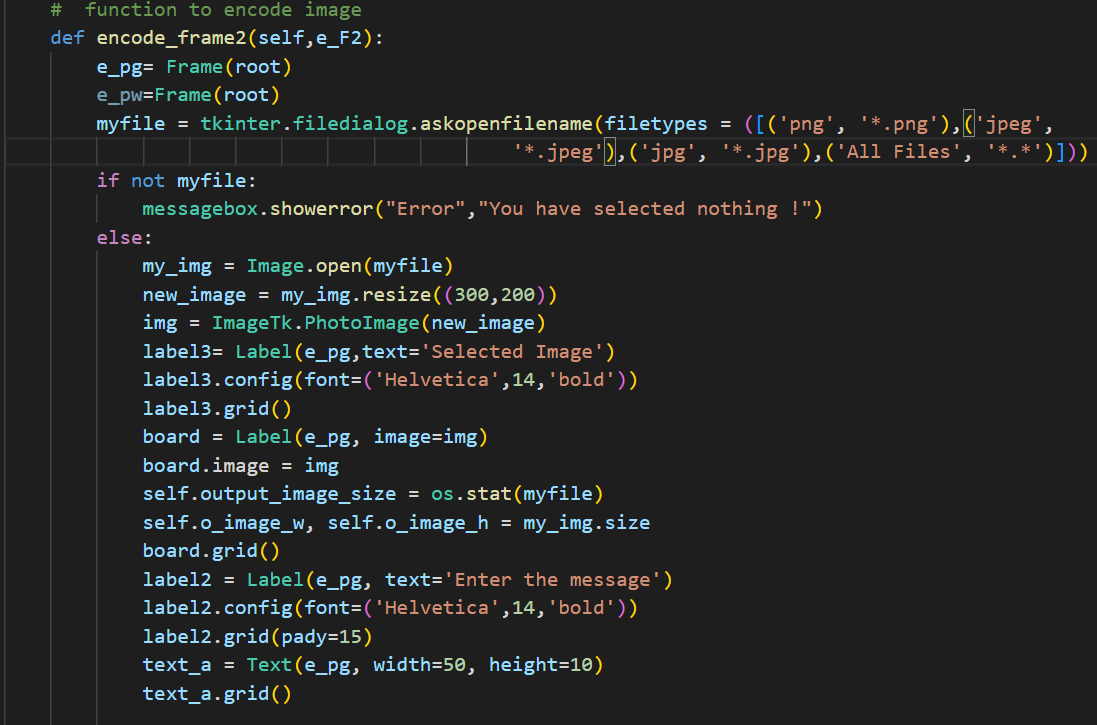
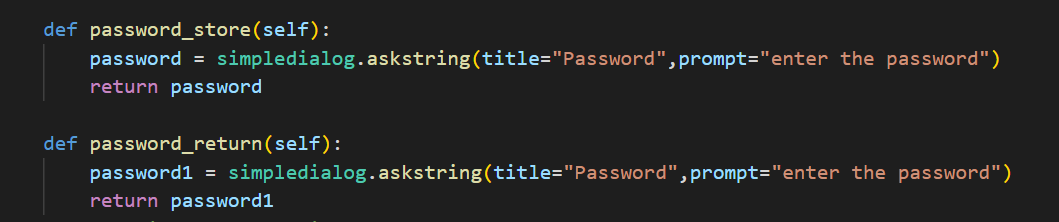
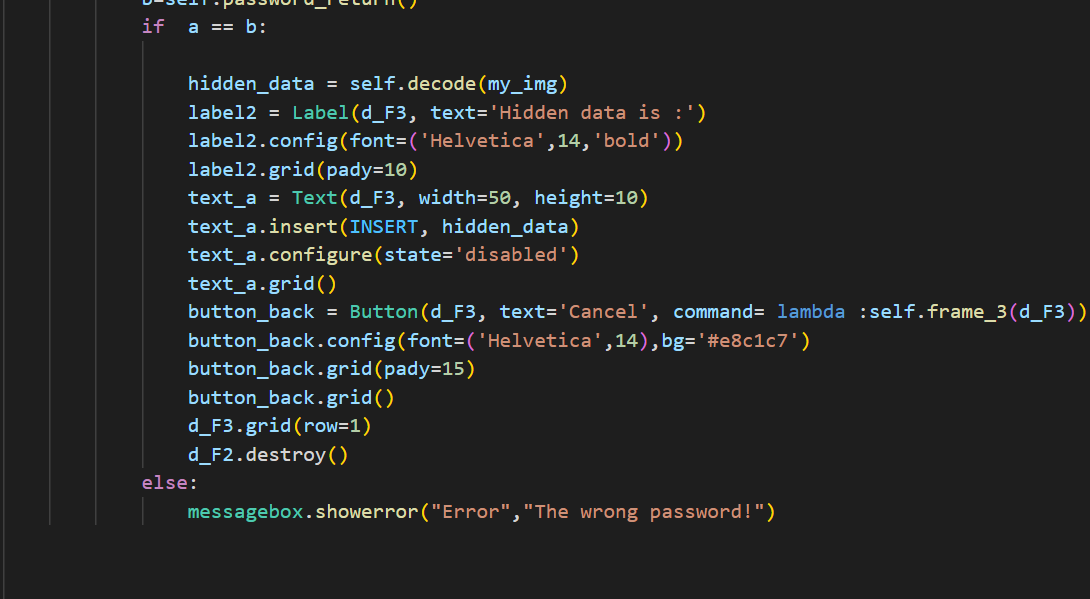
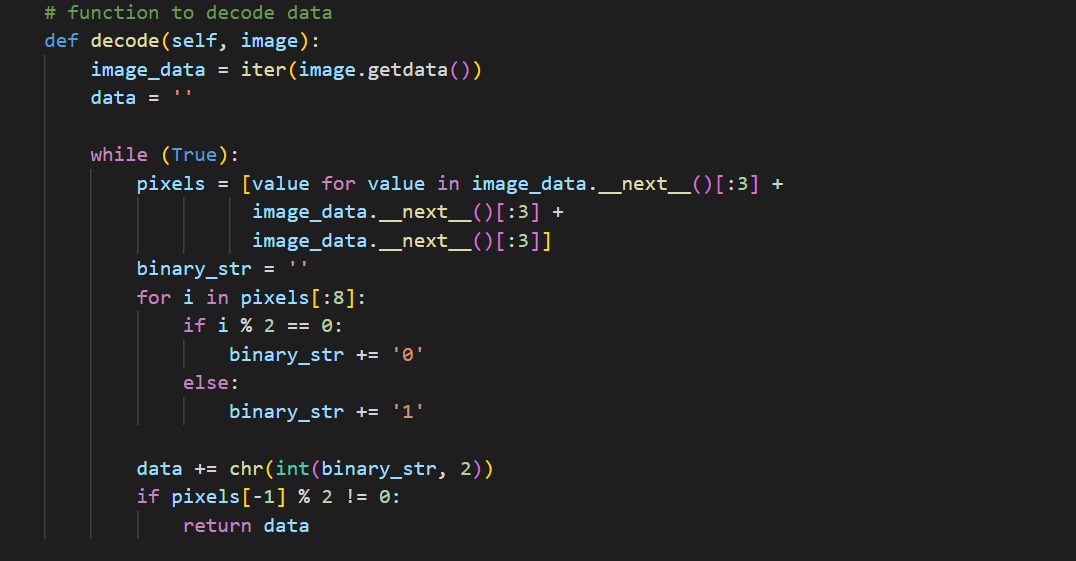
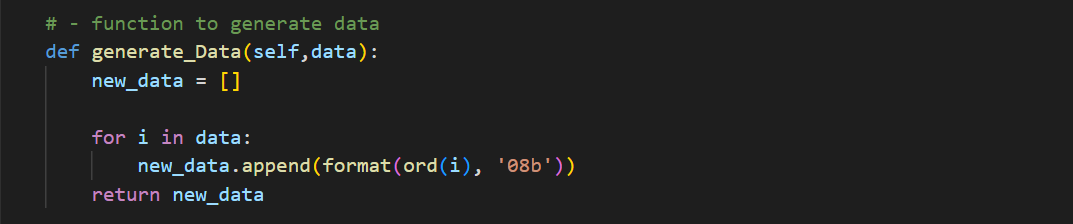
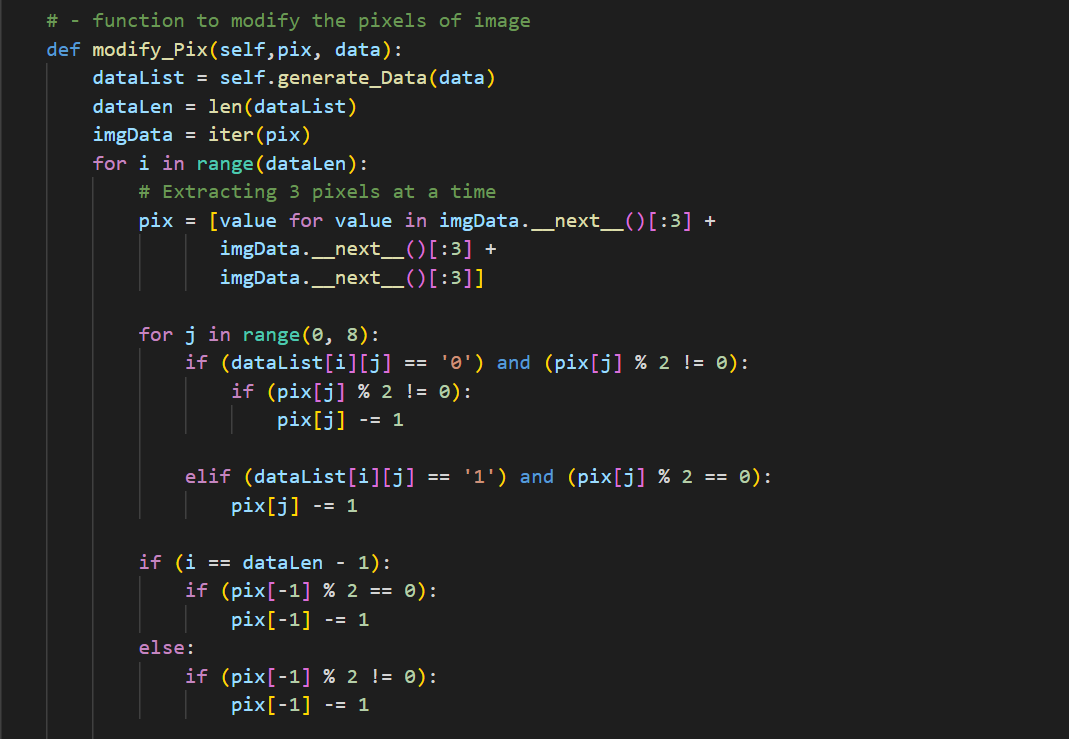
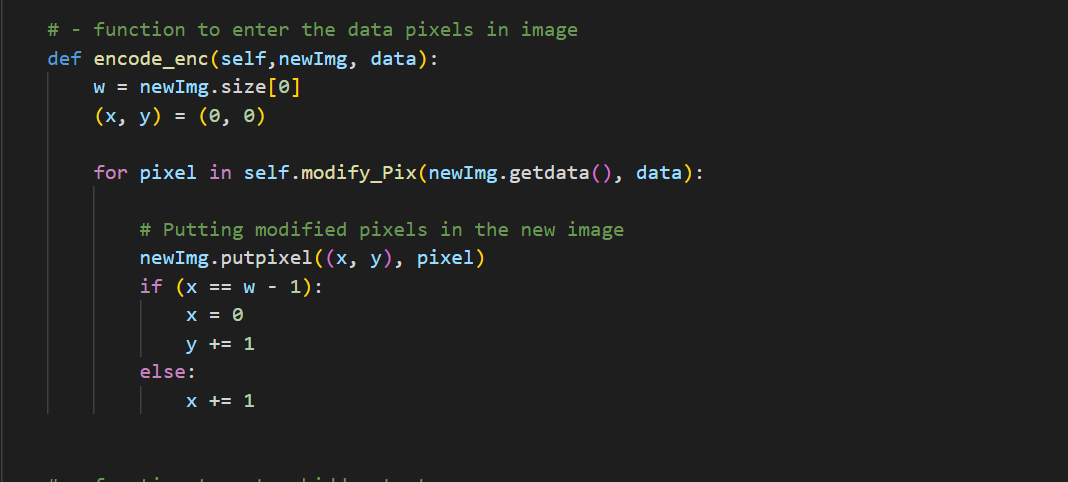
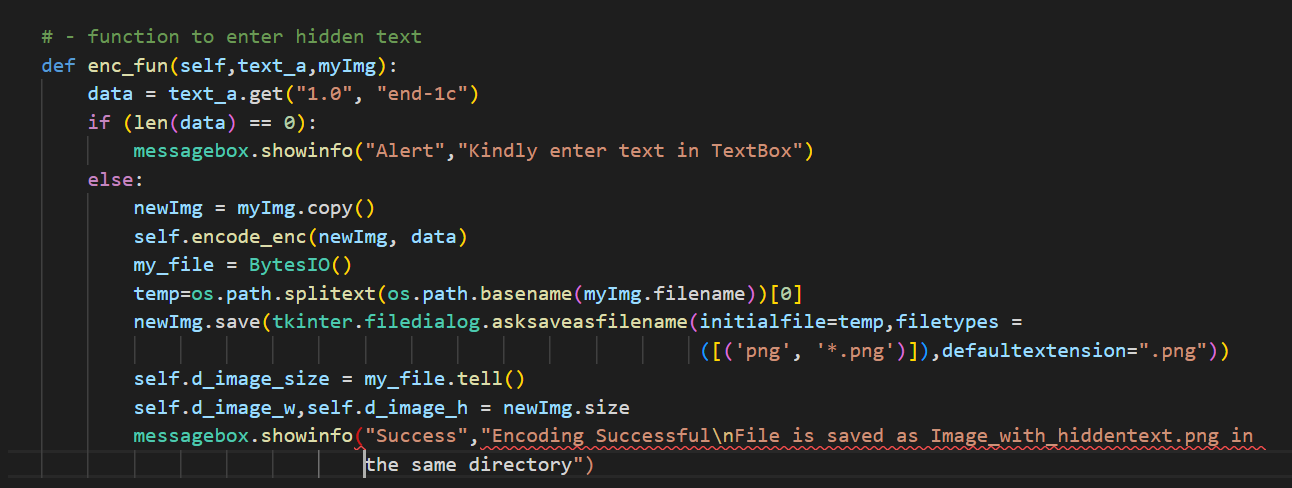
When the user is the sender, the user needs to specify the image file in which he want to hide the message and need to give the secret message. Before this step the user needs to specify the secret password. The secret message is hidden in the file using the LSB method. Now the file is along with the secret file but in binary format. The binary file is again converted back to a normal file using LSB**.**

When the user is the receiver, first the user needs to enter the password, if the password does not match then error message is shown. If the password matches then the user can get the secret message.

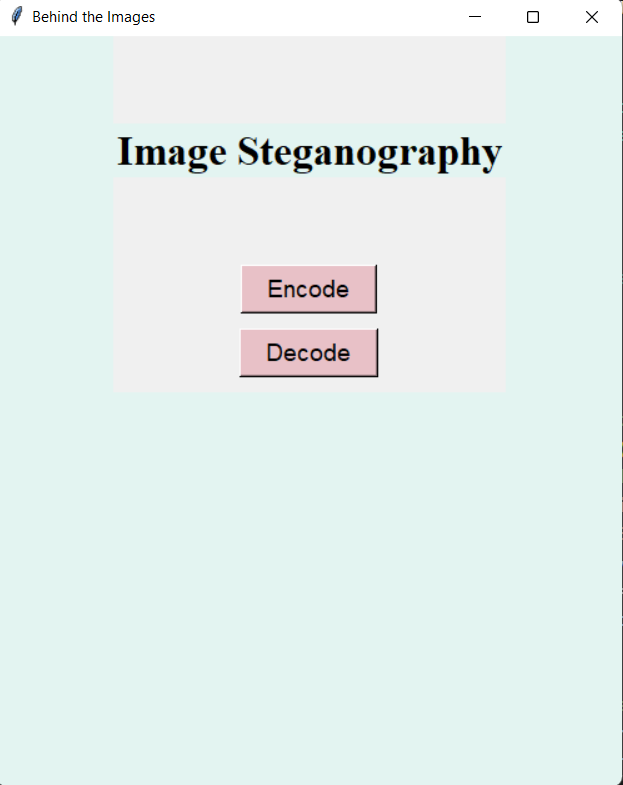
**4. IMPLEMENTATION**

****

****

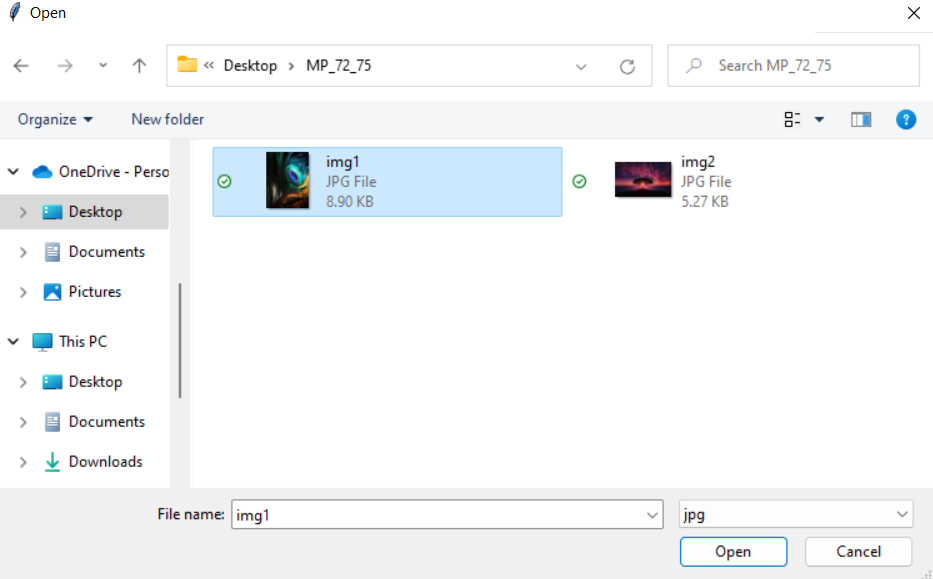
**5. RESULTS**

****

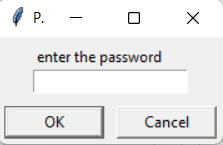
Interface to select the encoding process or decoding process.



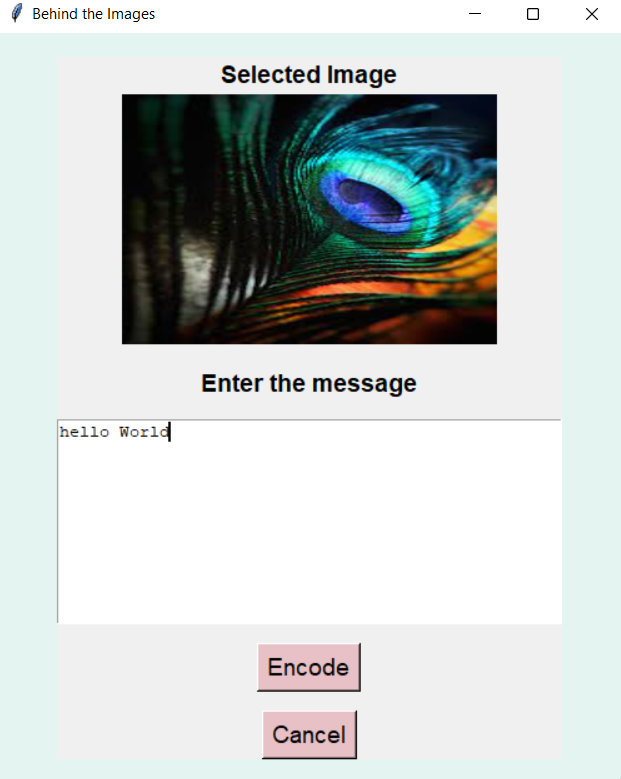
Window for image selection.



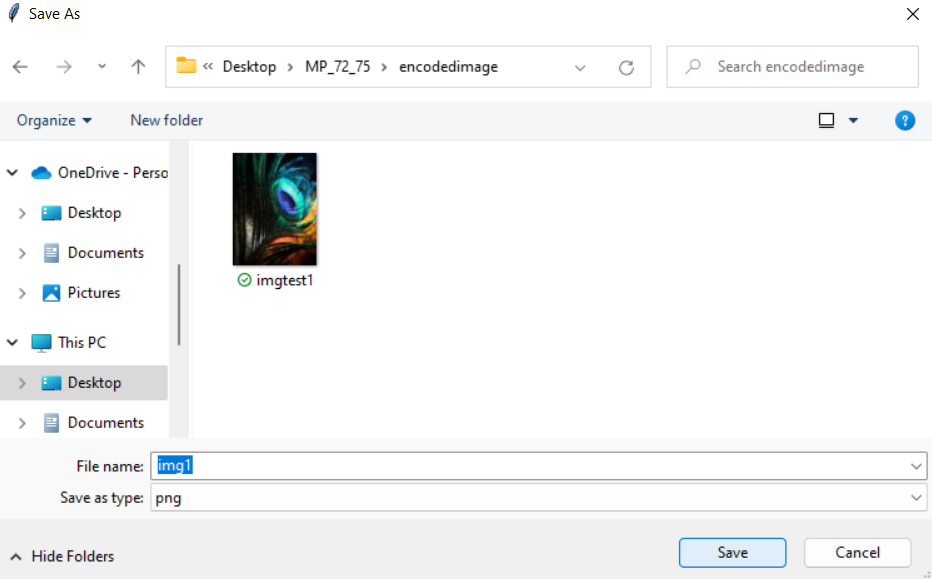
Selecting the image from your device.

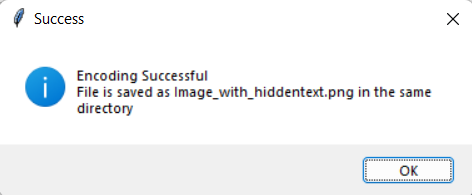
****

Before Encoding the image set a password.

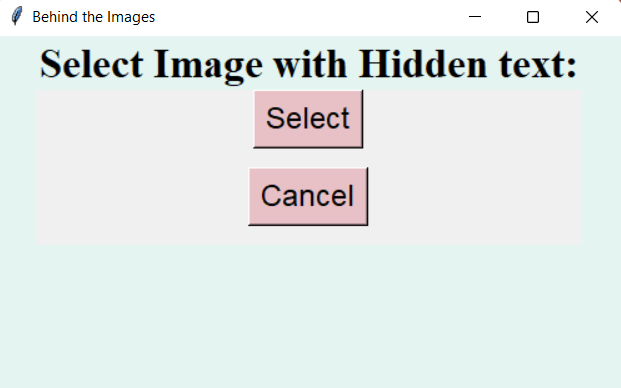
****

Enter the Secret information

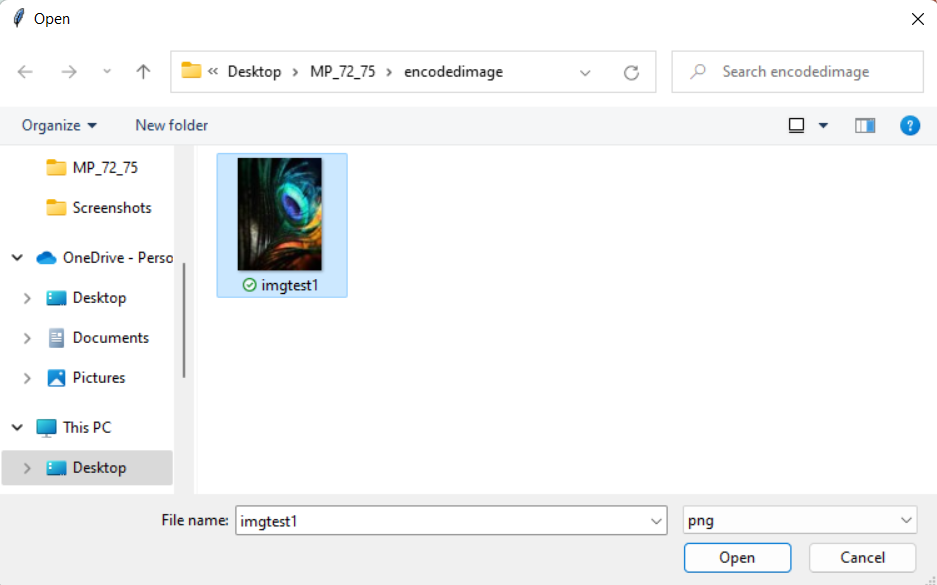
 The new encoded image is formed and saved into the desired folder.



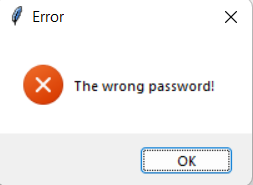
Message displayed after encoding.

Behind the scenes of Decoding

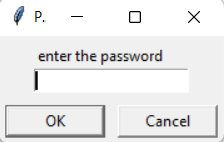
Window for selecting the hidden text image.



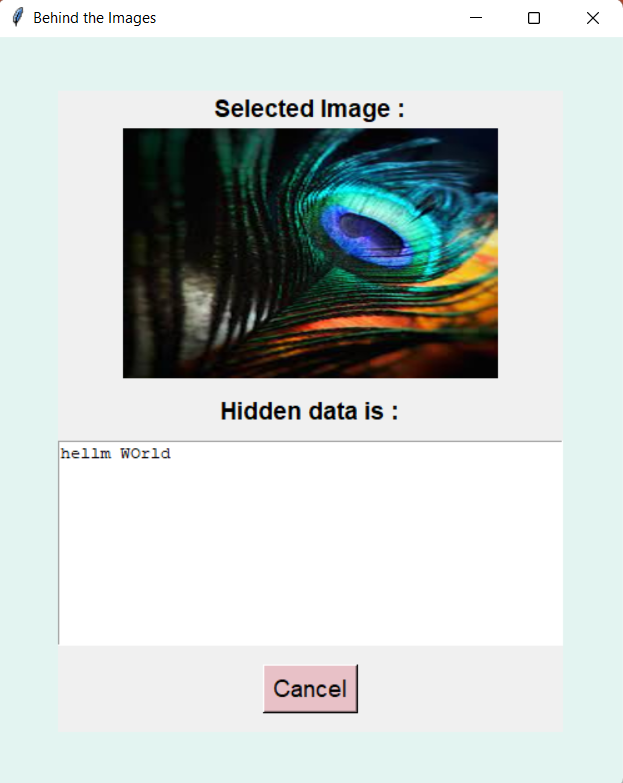
The image which has the hidden message is selected.



If the password entered is Wrong. The below error message is shown.



The password given by the user should be correctly entered by the receiver in order to get the hidden text.



The secret message is finally revealed out.

**6. CONCLUSION**

In conclusion, image steganography is a powerful technique for hiding secret information in digital images. It provides an added layer of security and confidentiality to sensitive data, which is essential in many applications, including military, medical, and personal communication. While traditional steganography methods can be vulnerable to detection and extraction by an adversary, more advanced techniques using machine learning and cryptography have shown promise in enhancing the security and efficiency of steganography.

The use of password encryption in image steganography can also provide enhanced security by encrypting the hidden message and ensuring only authorized recipients can access it. The development of user-friendly programs and tools for implementing steganography algorithms with password encryption can make it more accessible to both technical and non-technical users.

Overall, image steganography has a promising future, with potential for further development and improvement in efficiency and security. The continued advancement of image steganography techniques and their integration with other security technologies will continue to play a vital role in ensuring secure and confidential data transmission in various applications

**7. FUTURE SCOPE**

The future scope of image steganography using password encryption is promising, as it has the potential to provide a higher level of security and confidentiality to the hidden message. One area of future research is the development of more robust and efficient steganography algorithms that can withstand various steganalysis attacks while maintaining the quality of the cover image. The use of advanced cryptography techniques, such as elliptic curve cryptography (ECC) and advanced encryption standard (AES), can also enhance the security of the hidden message.

Another area of future research is the development of more user-friendly and accessible software and tools for implementing steganography algorithms with password encryption. This can make steganography more widely available to both technical and non-technical users and enable secure communication of sensitive information.

The integration of image steganography with other security technologies, such as digital watermarking and blockchain, is also an area of future research. The combination of steganography and watermarking can provide an effective way to protect the ownership of digital media and ensure authenticity. The use of blockchain technology can provide a more secure and decentralized platform for storing and transmitting steganographic information.

In conclusion, the future of image steganography using password encryption is promising, with potential for developing more advanced and efficient techniques that can provide a high level of security and confidentiality to the hidden message. The continued advancement of steganography techniques and their integration with other security technologies will play an essential role in ensuring secure and confidential data transmission in various applications

**8. BIBLIOGRAPHY**

1. <https://youtu.be/F18Rxw6ftcM>

2. <https://youtu.be/oSIv-E60NiU>

3. <https://youtu.be/BLl32FvcdVM>

4. <https://youtu.be/7H_QH9nipNs>

5. <https://youtu.be/DYdVXqXhWyw>

6. <https://ijirt.org/Article?manuscript=150860>