

Minor Project: Hiding Text Files in Images Using Command Line Tools

Name: Aenugu Omkar Reddy

Cyber Security

August Batch

INTRODUCTION

Steganography: Steganography is the technique of hiding data within an ordinary, non secret file or message to avoid detection; the hidden data is then extracted at its destination. Steganography use can be combined with encryption as an extra step for hiding or protecting data. The word *steganography* is derived from the Greek word *steganos*, meaning "hidden or covered," and the Greek root *graph*, meaning "to write."

Steganography can be used to hide almost any type of digital content, including text, images, video, and audio. Some examples of steganography include:

- **Text steganography**

Hiding a message within text by using typos, punctuation, or the first letter of each sentence

- **Image steganography**

Hiding information in a digital image by taking advantage of the fact that small changes in image noise or colour are hard to detect.

Steganography can be used for both good and ill purposes. For example, hackers may use steganography to hide their attacks, while cybersecurity professionals may use it to detect unauthorized data transmission.

Steganography is important because it helps hide sensitive information in a way that's less likely to attract attention than other methods:

- **Secures information**

Steganography can be used to send sensitive information to other parties without raising suspicion. For example, law enforcement and government agencies can use steganography to protect sensitive information.

- **Hides the fact that a message is being sent**

Steganography hides the fact that a message is being sent, unlike cryptography, which encodes the message and makes it appear unrecognizable.

- **Protects confidential documents**

Steganography can be used to hide sensitive information in innocuous files or images, adding an extra layer of protection against unauthorized access.

- **Combines well with encryption**

When used in combination with encryption, steganography can help obscure the fact that sensitive data is hidden.

Some common methods used in image steganography include:

- **Least significant bit (LSB) substitution:** This method replaces the least significant bits of pixel values with secret data. The difference in color is usually minimal and difficult for the human eye to detect.
- **Spatial domain techniques:** These techniques modify pixel values directly to embed secret data.
- **Discrete Fourier transform (DFT):** This method uses the mathematical technique of discrete Fourier transformation to hide information inside a multimedia file.
- **Masking:** This technique is similar to watermarking.
- **Palette-based technique:** This method embeds messages in palette-based images like PNG or GIF.

Other steganography techniques include:

- Wavelet transform, which is used to shift edges
- Modulation data hiding, which is used for tamper detection and correction

PROJECT DESIGN

A steganography project aims to develop a system that can discreetly embed secret information within seemingly normal media like images, audio, or video files, with the primary objective of hiding the presence of the hidden message while maintaining the integrity of the carrier media, thus enabling secure covert communication where the existence of the secret data is not readily apparent to unauthorized parties; the scope typically includes selecting a suitable steganographic algorithm, implementing the embedding and extraction processes, and ensuring the system is robust against potential detection methods.

Key aspects of the scope and objectives:

- Concealment:

The primary objective is to hide sensitive data within a carrier file without noticeably altering its appearance, making it difficult to detect the presence of the hidden information.

- Data types:

The project could focus on embedding data within various media types like images, audio files, or even text documents, depending on the application requirements.

- Algorithm selection:

Choosing a suitable steganographic algorithm based on factors like embedding capacity, robustness against attacks, and computational complexity.

- Embedding process:

Implementing the mechanism to embed the secret data into the carrier file, often by modifying the least significant bits (LSB) of the pixel values in images.

- Extraction process:

Developing the method to extract the hidden data from the stego-file using the appropriate key or password.

- Security considerations:

Evaluating potential attacks against the steganographic system, such as steganalysis techniques aimed at detecting the presence of hidden data, and implementing countermeasures to enhance security.

- User interface:

Designing a user-friendly interface to facilitate the process of embedding and extracting secret data.




Potential applications of a steganography project:

- Secure communication in sensitive scenarios
- Protecting intellectual property by embedding watermarks in digital
- Hiding sensitive information in medical imaging and Data protection in forensic investigations.

IMPLEMENTATION

Steps:

Environment Setup: Firstly I have created a folder named minors on desktop so that it will be easy to locate the path and in that folder I have added an image after that I created a text file in that folder and I have given fake banking information and I named the file as text. After that I have created another compressed text file by using 7zip select the option “add to text.zip”, another file is created.

Name	Status	Date modified	Type	Size
 image	✖	10-09-2024 15:21	JPEG File	7 KB
 text	✖	10-09-2024 15:26	WinRAR archive	1 KB
 text	✖	10-09-2024 15:25	Text Document	1 KB

Hiding Text in Image: In command prompt we have give the directory to the path where we have created the folder which I have named minors for that I have given the command “**cd desktop/minors**”. After that we have to press enter and it will got directory minors. If I type DIR command it will give all images and all files present in that. Now we have to enter the command to hide the text into the image the command is “**copy /b image.jpeg+text.zip image2.jpeg**”. How this command works means it will merge the text into the image. Here **image** is the name I have given in which I want to hide the text, **.jpeg** is the extension, we need to be very serious about our extensions, text.zip is the text file I have converted to 7zip file and **image2.jpeg** is the image which we will get as output by hiding the text into the image. After giving the command if we type enter we will get the result as **one files is copied**. So Our command is correct. In that folder minors this image will be added. There will be no difference in the image and image2.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.4037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\OMKAR>cd desktop/minorcs

C:\Users\OMKAR\Desktop\minorcs>copy /b image.png+text.zip image2.png
The system cannot find the file specified.

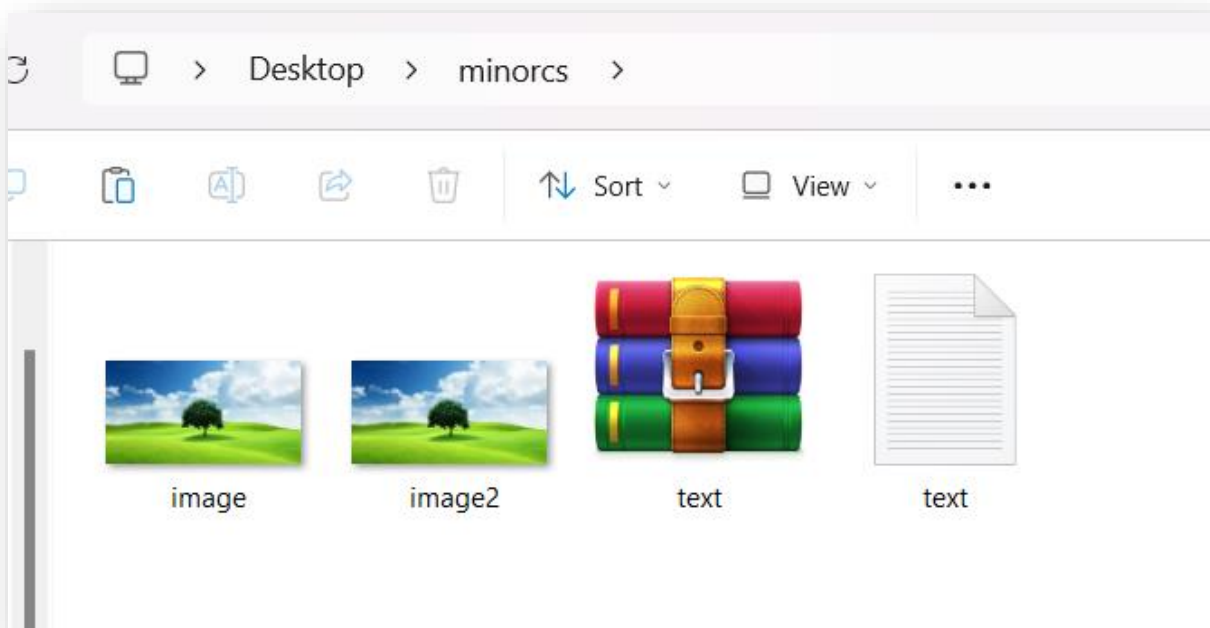
C:\Users\OMKAR\Desktop\minorcs>dir
Volume in drive C is Windows
Volume Serial Number is 9C59-8BB0

Directory of C:\Users\OMKAR\Desktop\minorcs

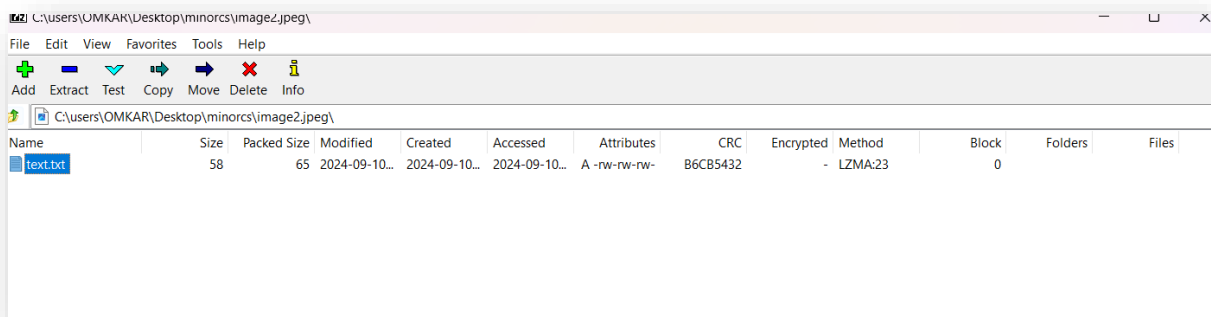
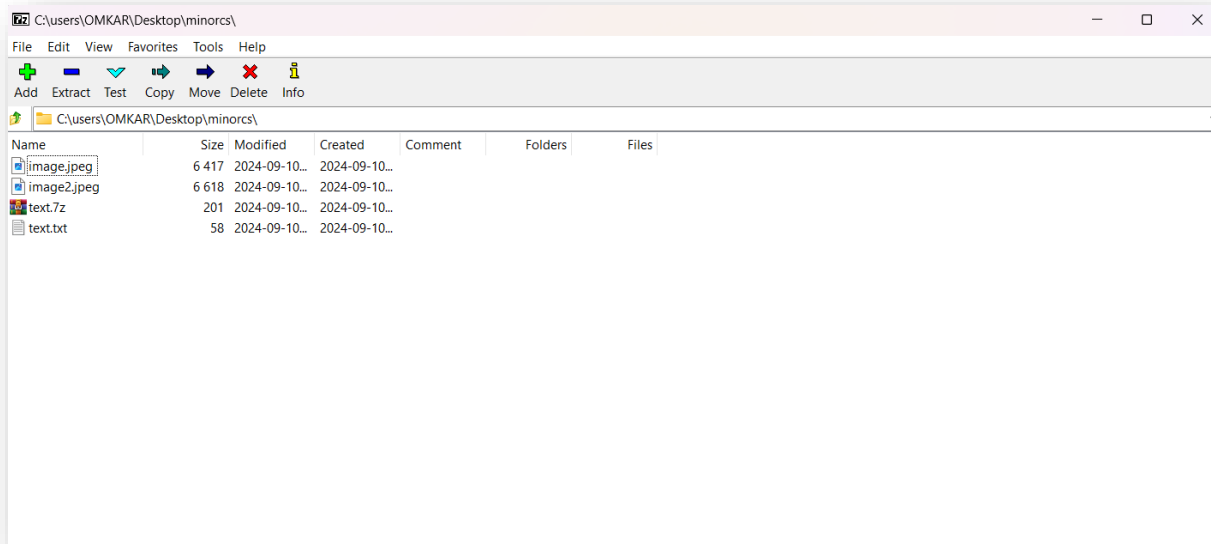
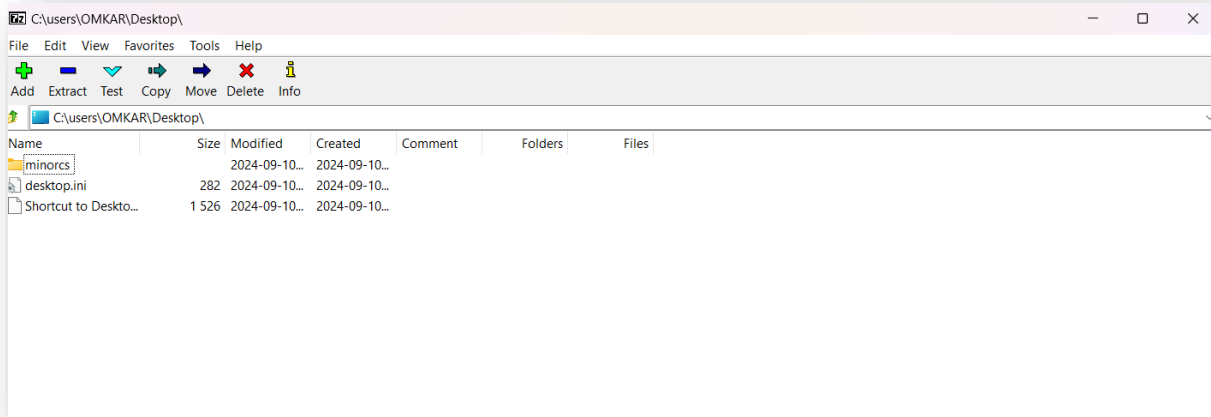
10-09-2024 16:07 <DIR>      .
10-09-2024 16:07 <DIR>      ..
10-09-2024 15:21          6,417 image.jpeg
10-09-2024 15:26          201 text.7z
10-09-2024 15:25          58 text.txt
                3 File(s)      6,676 bytes
                2 Dir(s)  47,470,174,208 bytes free

C:\Users\OMKAR\Desktop\minorcs>copy /b image.jpeg+text.7z image2.jpeg
image.jpeg
text.7z
        1 file(s) copied.

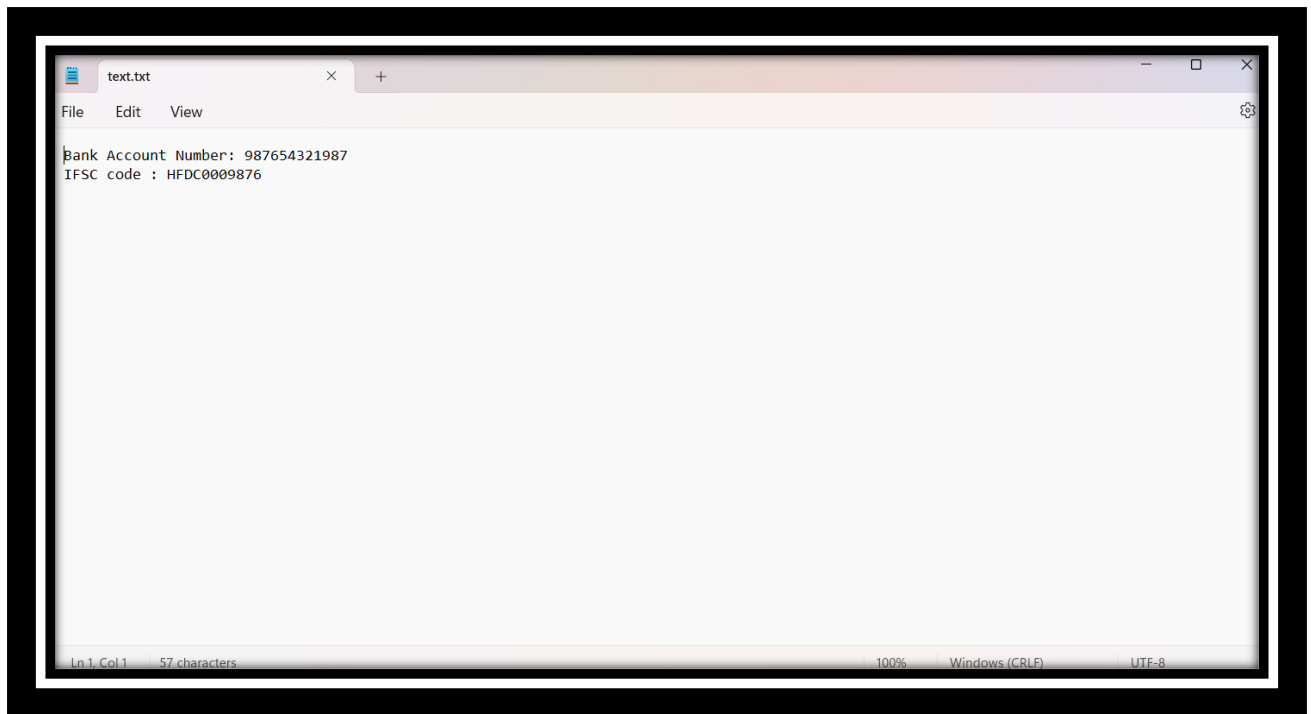
C:\Users\OMKAR\Desktop\minorcs>
```



Extracting Text from Image: We have to open the 7zip file manager to extract text behind the image. After opening we have to open the folder where we have stored the image and we have to select the image from which we want to extract the text that is image2 if we click on that we will get text document in which I have given fake banking information. Size of the image which contains text will be increased as compared to original image.



Ensuring data Integrity: After the extraction the data is safe, correct and retrieved.



TESTING & VALIDATION

I have tested this with various images and extracted the text it worked correctly. After extraction the data which I have written in text file it is accurate.

CONCLUSION

Steganography, as demonstrated in the project, offers a powerful technique for concealing sensitive information within seemingly harmless media, such as images, without attracting attention. This method enables secure covert communication by hiding the existence of the secret message. The process of embedding text within an image through commands, followed by successful extraction using tools like 7zip, proves that steganography can be effectively implemented and is robust in maintaining data integrity.

In this project, the use of Least Significant Bit (LSB) substitution for hiding text in an image has proven effective, as the human eye cannot easily detect the changes in the image. The process involves compressing the data to be hidden, embedding it into the image, and later extracting it with no loss or corruption.

of the original data. Through testing, it has been confirmed that the system works as intended with various images, providing accuracy and reliability.

By combining steganography with encryption, an additional layer of security is achieved, making it a useful tool for protecting confidential information in sensitive communication and ensuring that even if the hidden data is detected, it remains inaccessible without the proper decryption methods.

In conclusion, the project showcases steganography's versatility in secure communication, data protection, and information integrity, demonstrating its potential applications in fields such as cybersecurity, intellectual property protection, and forensic investigations

THANK
YOU