**PRACTICAL 4**

**Aim:** The transmission of information need to be secure over the communication channel and the data has to be confidential. Study and implement the practical approach for Steganography.

-Using DOS commands

-Using OpenPuff Tool

-Using StegoStick Tool

**Hardware Requirement:** Computer/Laptop.

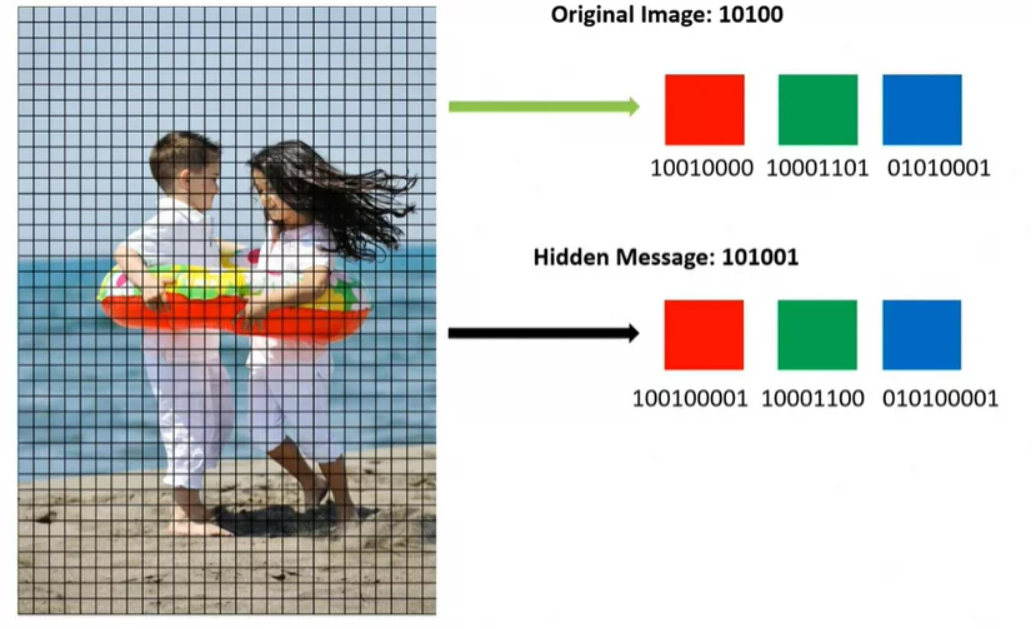
**Software Requirement:** WindowsCMD, OpenPuff Tool, 7Zip Extracting tool.

**Theory:**

Steganography is art and science of hiding facts behind a false or useless but interesting element. In this process no one other than the sender and the and the recipient can view this. Cryptography is combined with steganography just for the reason that, if also the message is discovered it cannot be read. The main difference lies in the existence of cryptography and steganography.

In Cryptography one can know that a message is encrypted. But in Steganography one cannot know or observe about it simply because its hidden behind an image, video or an audio etc… which without keen observation might go without any suspicion. Steganography was widely used by the terrorists. In 9/11 attacks of the World Trade Center Stenography was used at a higher rate. This was discovered during the post attack investigation.

We can create such Files using cmd or using some tools like OpenPuff, OpenStego, OutGuess etc…



1. **Using DOS Commands:**

**Steps:**

Step 1: Place the Image file and the Document in a folder.

Step 2: Zip the document file.

Step 3: Now, Open the Command Prompt and navigate to the folder where you’re having the image and document zip file.

Step 4: Now type copy /b imagefilename + zipfilename [filename with extensions] and hit enter.

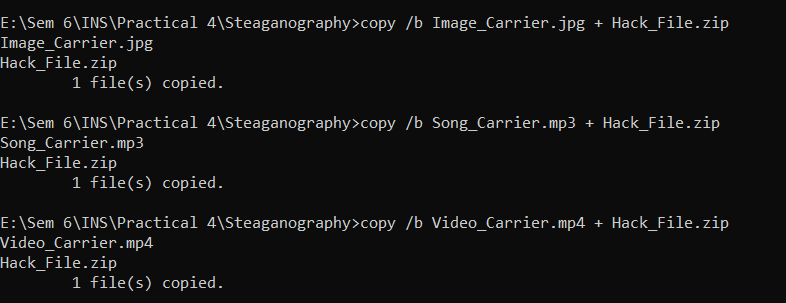
Eg: copy /b 1.jpg + 2.zip

Step 5: Now You can see the size of the image file has been increased.

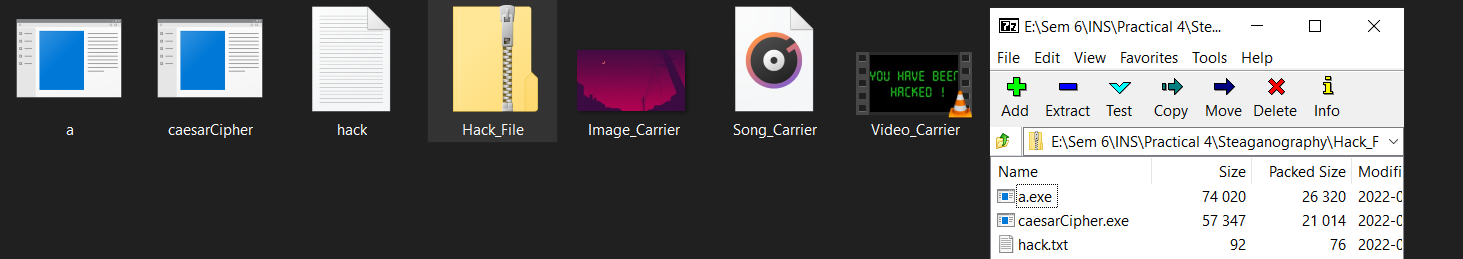
Step 6: You can now send the image alone to anyone and it contains the document inside it.

**Command:**

copy /b (image/video/audio) filename + zip filename

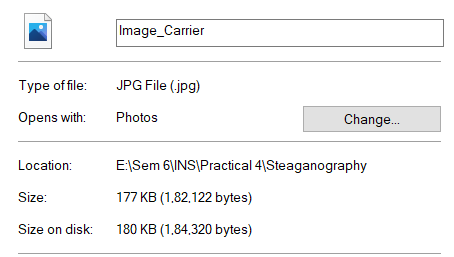


**Output:**

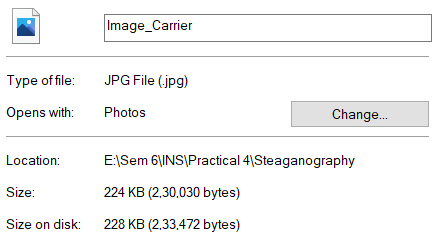


1. Image File Size

Before:

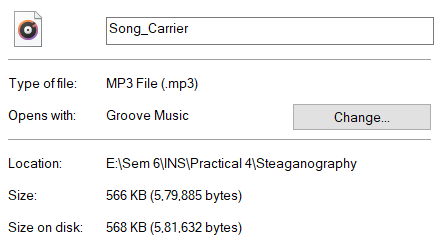


After:

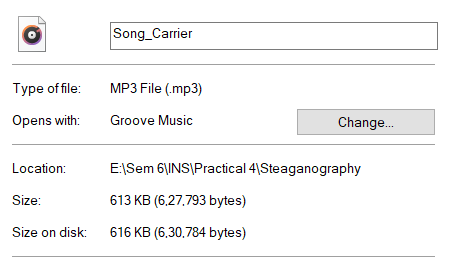


1. Audio File Size

Before:

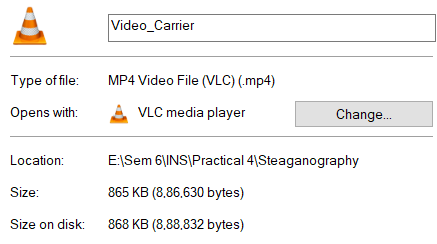


After:

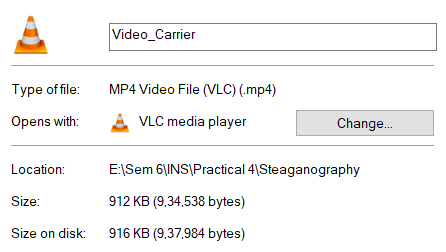


1. Video File Size

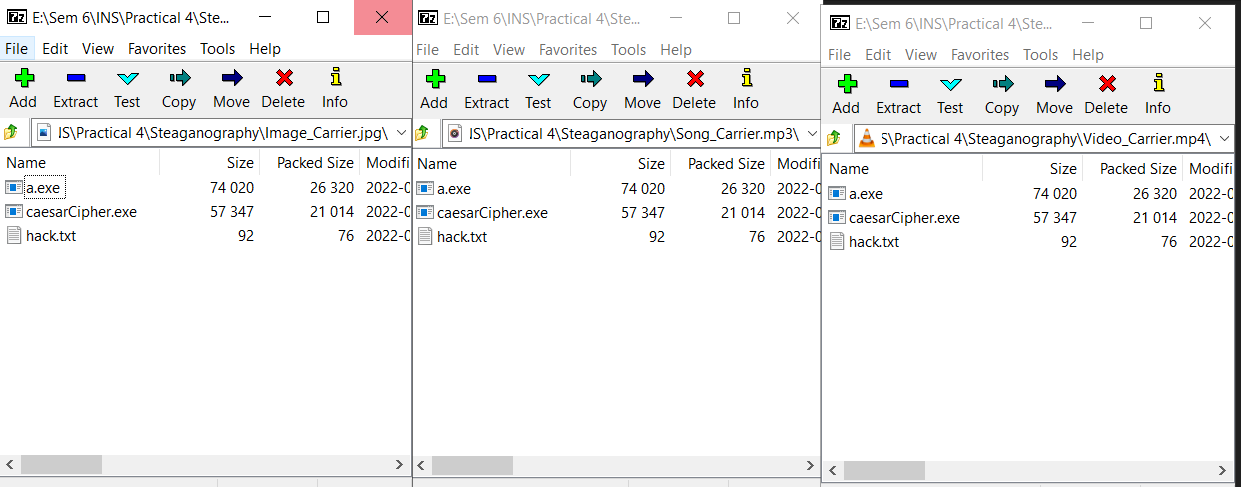
Before:



After:



Using 7Zip to show these files:



1. **Using OpenPuff Tool:**

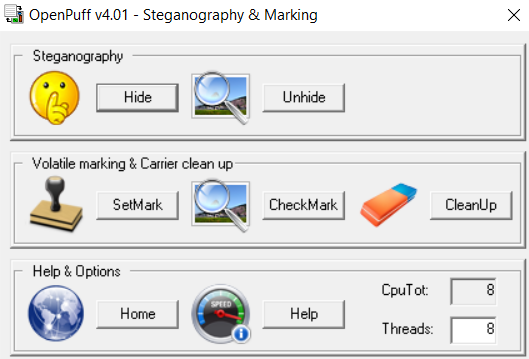
**Steps:**

1. Download it after that run it from the directory where you have downloaded it. You will see the home window of the software as below.
2. Now, click on Hide button to enter the main interface of OpenPuff.
3. Here in this window the interface is divided into 4 sections for performing different tasks. In the first section set the desired password for unhiding your data.
4. Navigate to second section that is Carrier Selection, and provide the carrier video file that you want to use for hiding your messages/documents. Here you can also add multiple carrier video files to hide your data in them. And all the carrier videos that you use will play in the same manner as they were before. You will not be able to identify whether a video has any hidden file in it or not.
5. Provide the target file that you want to hide in carrier video file and then hit the Hide Data button to complete the process.Openpuff in action

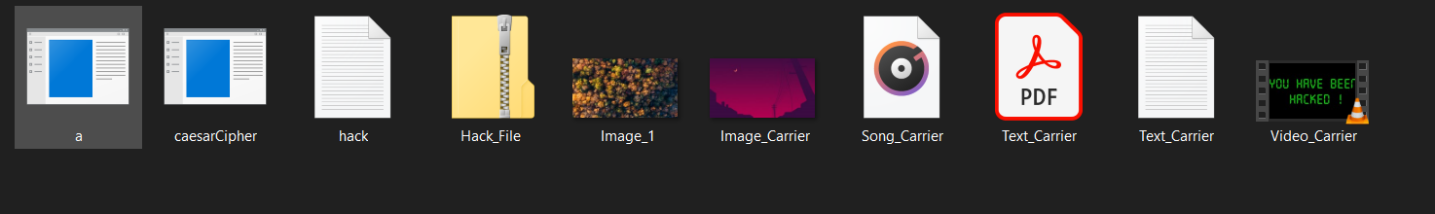
After going through the above steps, a final dialog will appear, asking you to specify the folder where you want to save the final video file that contains your hidden messages and documents. This will save the video file, with your files hidden in it.

For extracting the data from an existing carrier video file/file that you created, the process is almost the same. You just have to select the unhide option from the main window of OpenPuff. Next, provide the password that you set during hiding your file and provide the location where you want to store the extracted file.

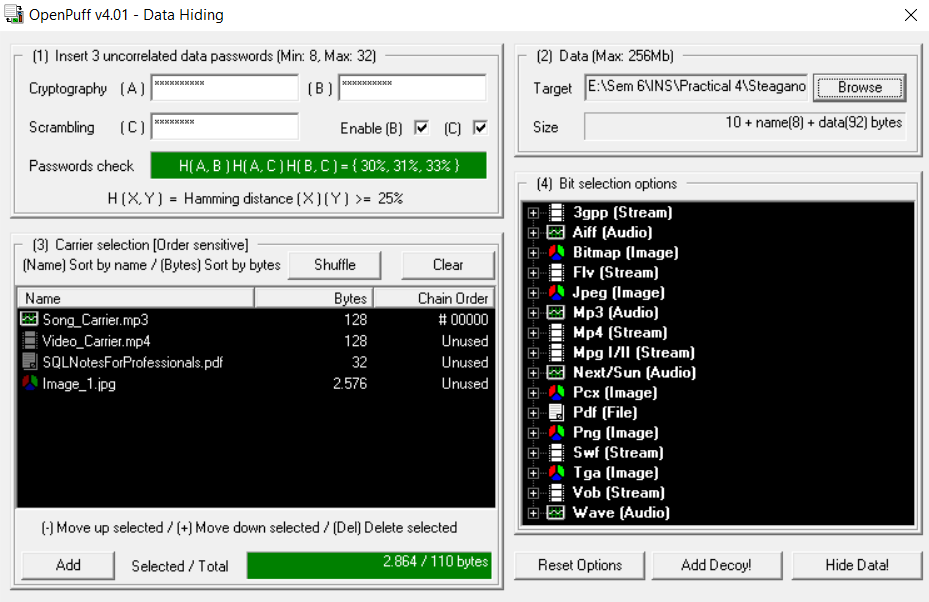
**OpenPuff GUI:**



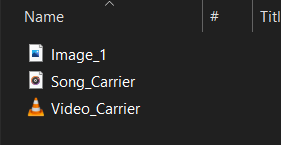
**OUTPUT:**



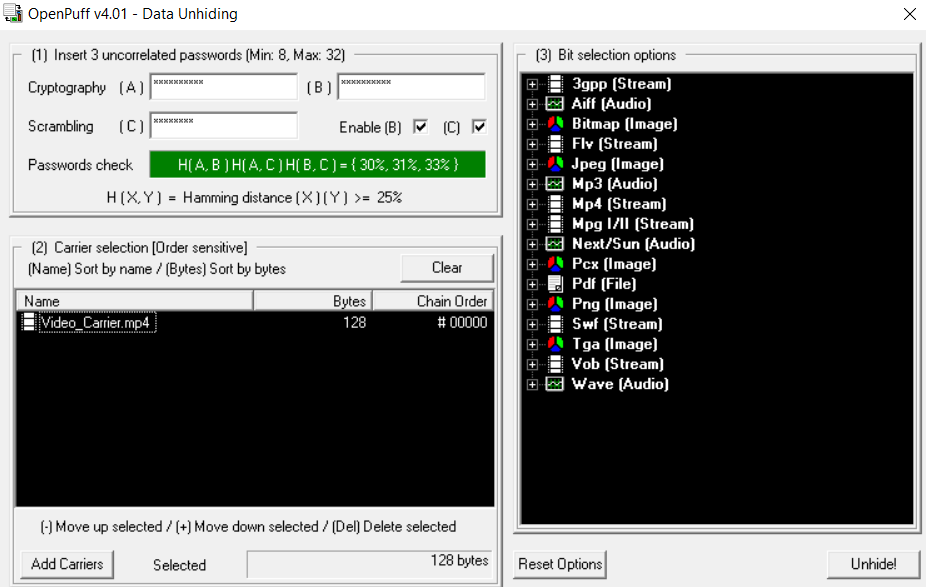
Hiding Zip file in different files:



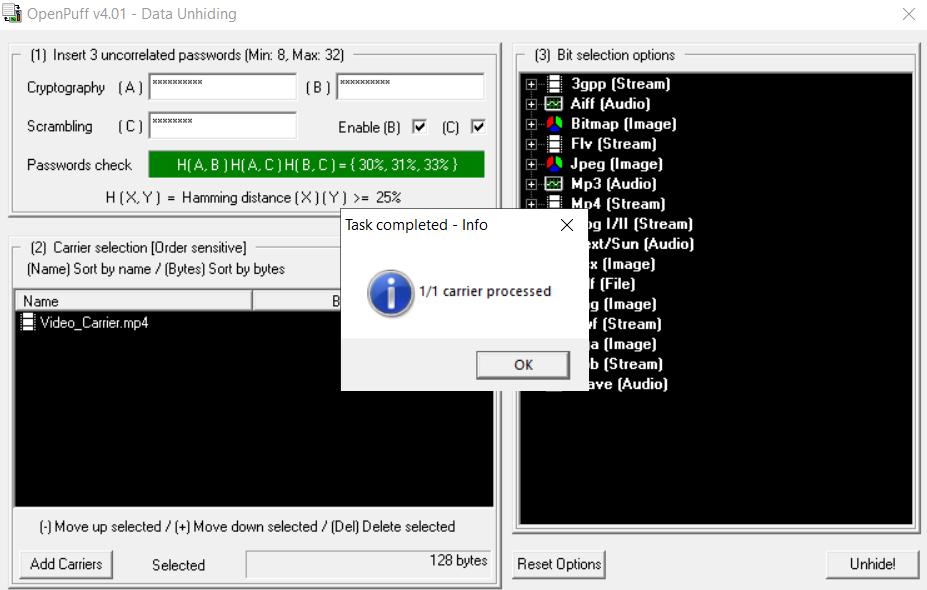
Click Hide and Save these files:

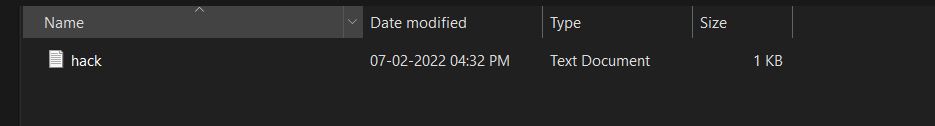


Unhide Files

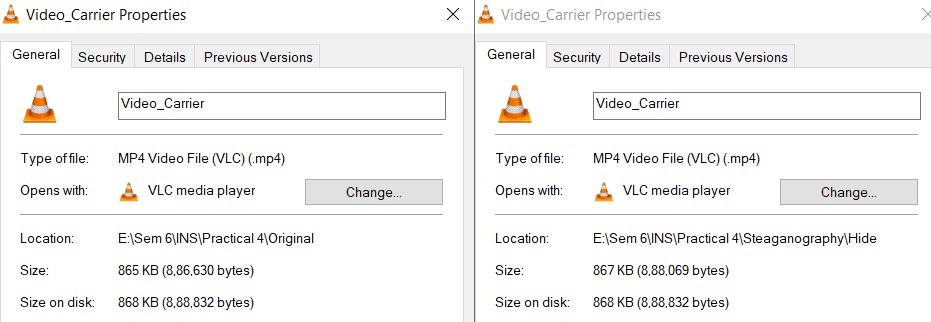


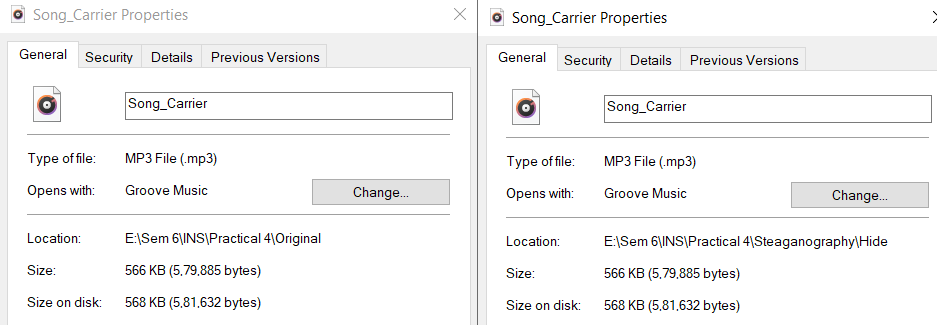
Save Harmful Files after unhiding





File’s Size Differences:





1. **Using StegoStick Tool:**

**Steps:**

1. Run it from the directory where you have downloaded it. You will see the first page of the software which asks you to choose an encryption technique. Check Default encryption option and hit OK button.
2. Now, you will see the interface where it shows you two tabs; one for hiding files in another and second for hiding message in a file. You can choose any option, in my case I will use Hide File tab.
3. Provide the secret file, Cover File (this is the video file in which you want to hide) and destination path where you like to store the resulted file.
4. Finally, enter a desired password, then hit the Hide button and you will see that your cover file is exported to the same directory that you provided.

At this point, you have done hiding your secret file inside video file of your choice.

**StegoStick GUI:**

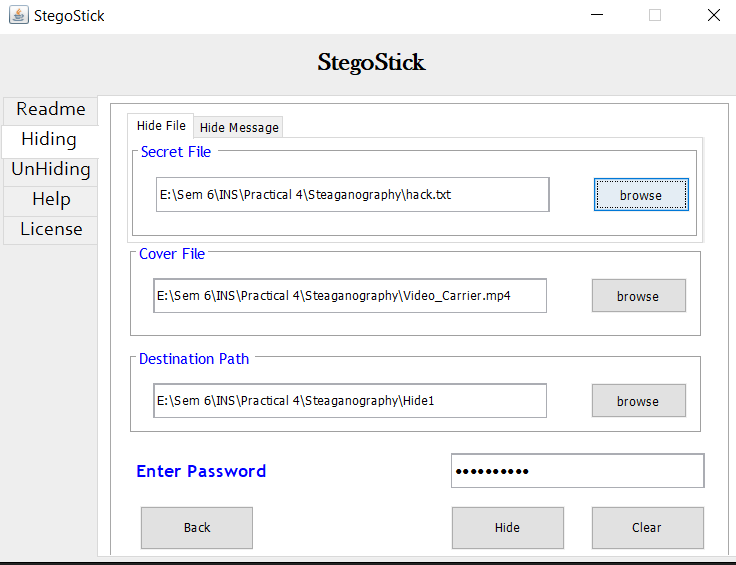


**Output:**

Hiding Files in Video/Image/Text/Audio Files

Select a Secret File and a Cover File and Add password (In Default Mode).

We can increase complexity by choosing other Algorithms.



Do same for Video, Audio, Text:

File’s Size Differences:

