**PRACTICAL-5**

**AIM:**

The transmission of information needs 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

**THEORY:**

* The word Steganography is derived from two Greek words- ‘**stegos**’ meaning ‘**to cover**’ and ‘**grayfia**’, meaning ‘**writing**’, thus translating to ‘covered writing’, or ‘hidden writing’
* Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file.
* The use of steganography can be combined with encryption as an extra step for hiding or protecting data

**ADVANTAGES:**

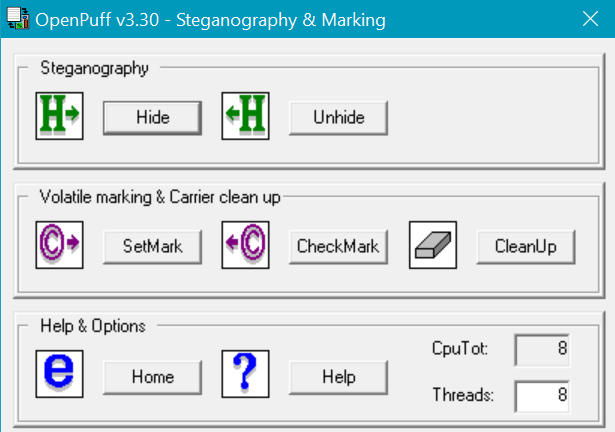
* Difficult to detect
* Can be applied differently in digital image, audio and video file

**DISADVANTAGES:**

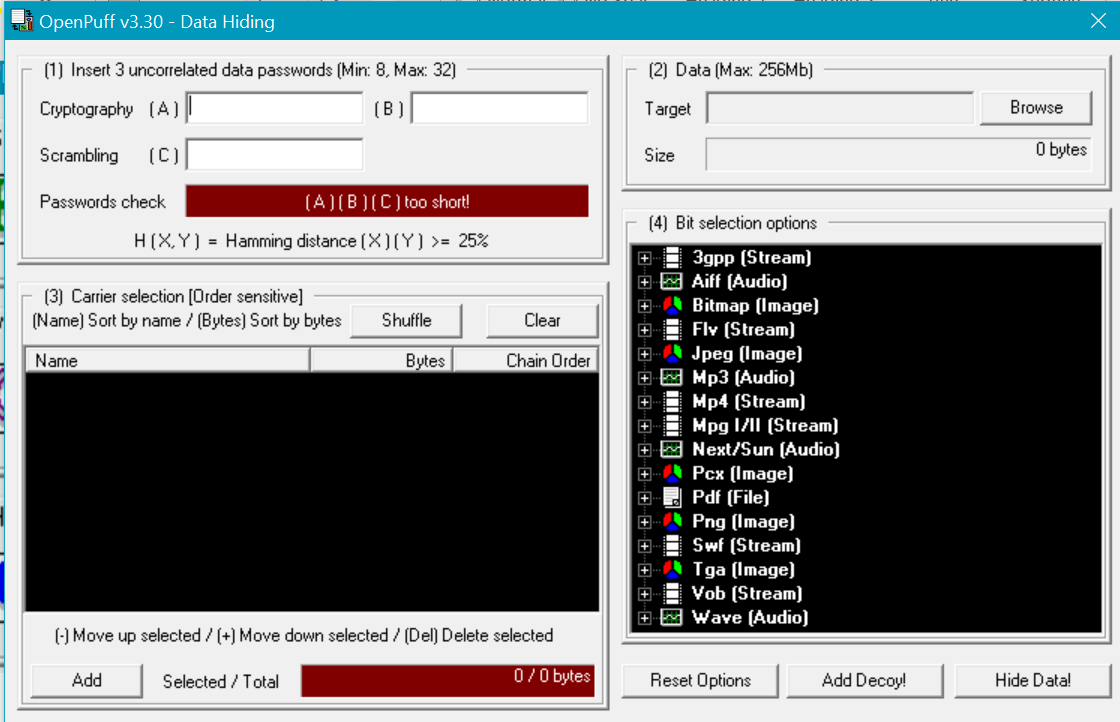
* File Size becomes large,

**OPENPUFF:**

* OpenPuff is a prevailing data hiding application made easy, safe and free that allows you to hide data into encrypted files in order to send it to other users
* This application aims to protect both secret messages and the persons who are exchanging messages.

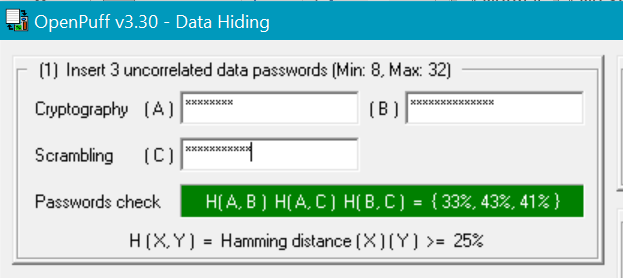


**MAIN SCREEN OF OPENPUFF**



**DATA HIDING SECTION**

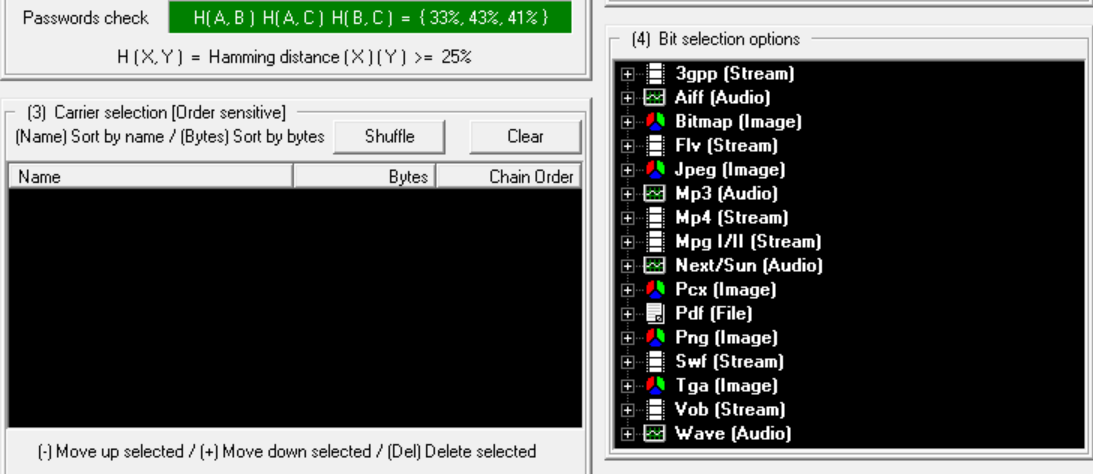
* Firstly, in section-1, insert 3 uncorrelated passwords.
* Password check panel will turn to green if Hamming Distance(X)(Y) is greater than 25%.



* Password panel turns green, which indicates that 3 passwords are uncorrelated



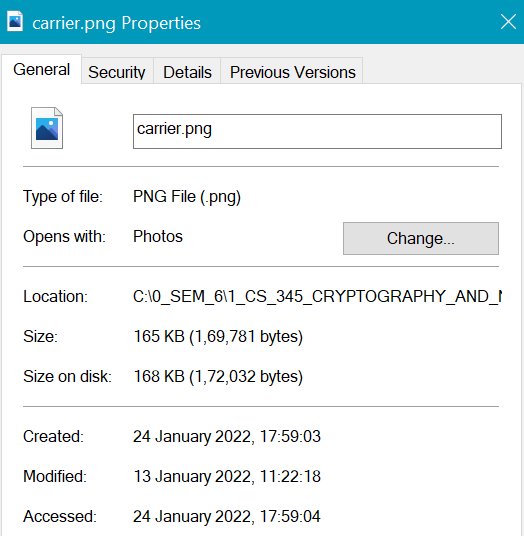
* In Section-2, you will need to upload the data that is to be hidden.



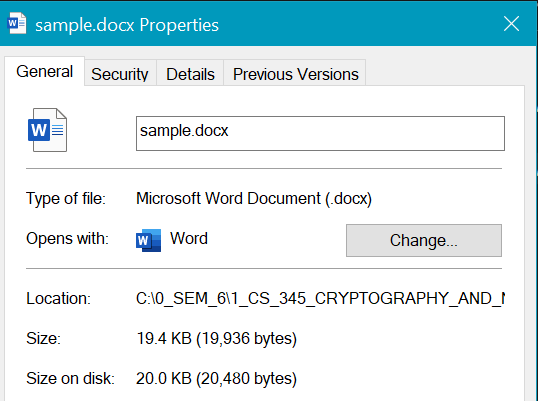
* In Section-3 and 4, you need to select and upload the carrier in which the message will be hidden.

**DATA HIDING:**

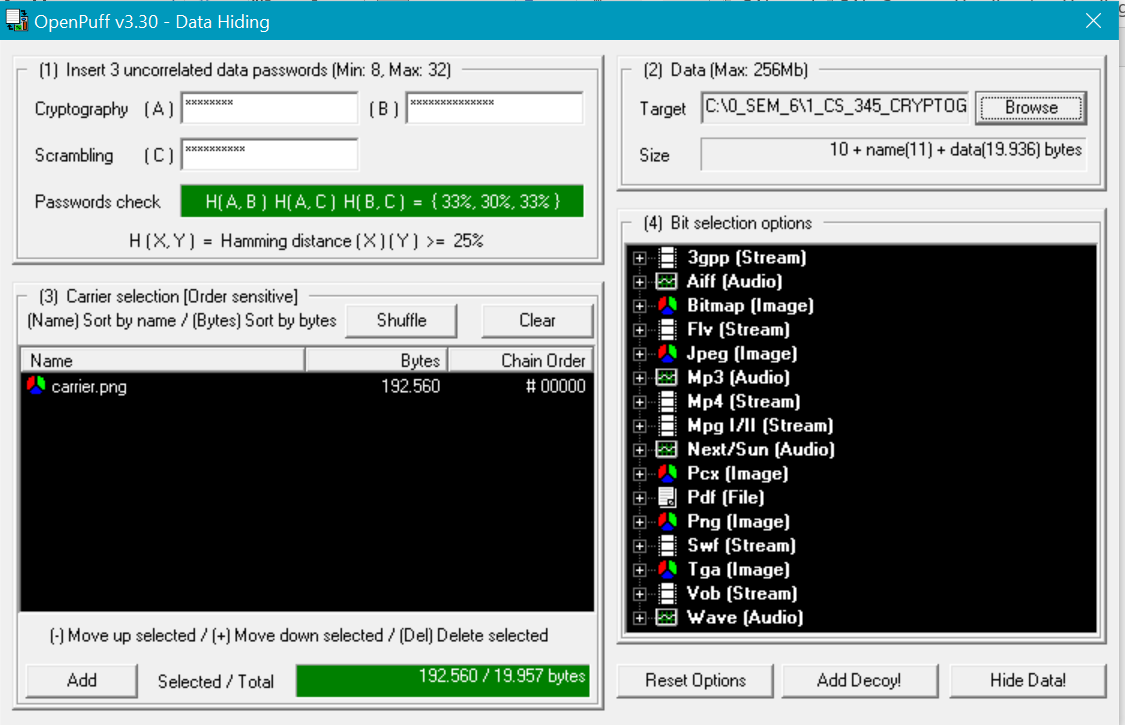
* We will hide a word file named sample.docx with the carrier of the format .png named carrier.png.



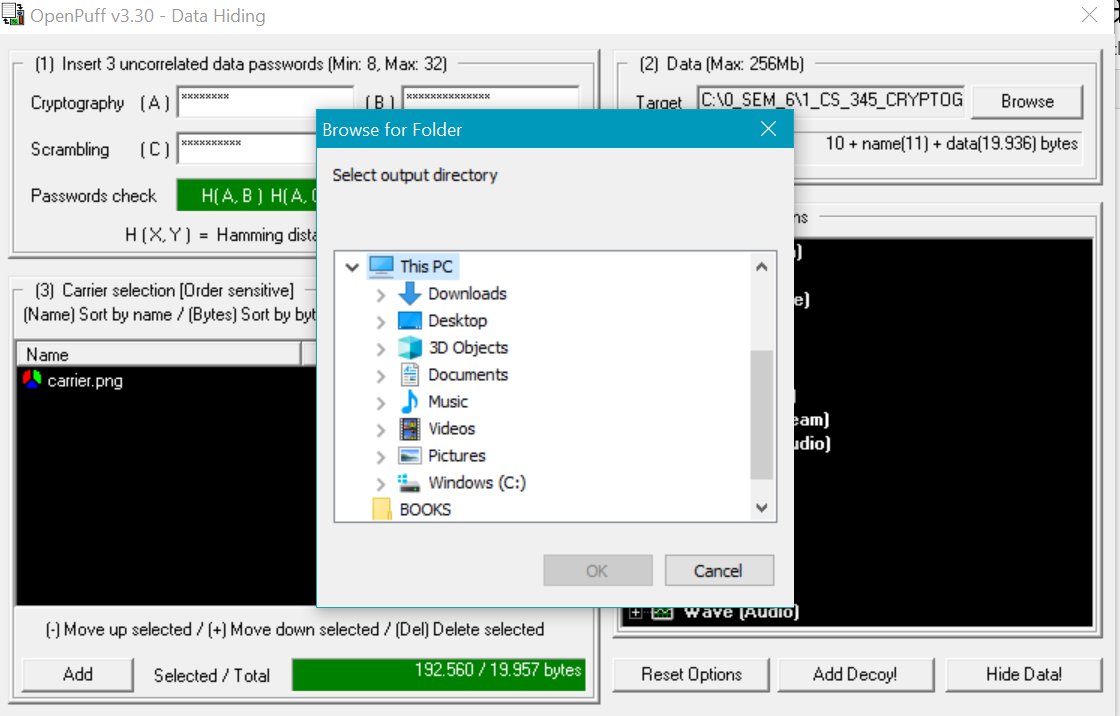
**SIZE OF CARRIER.PNG**



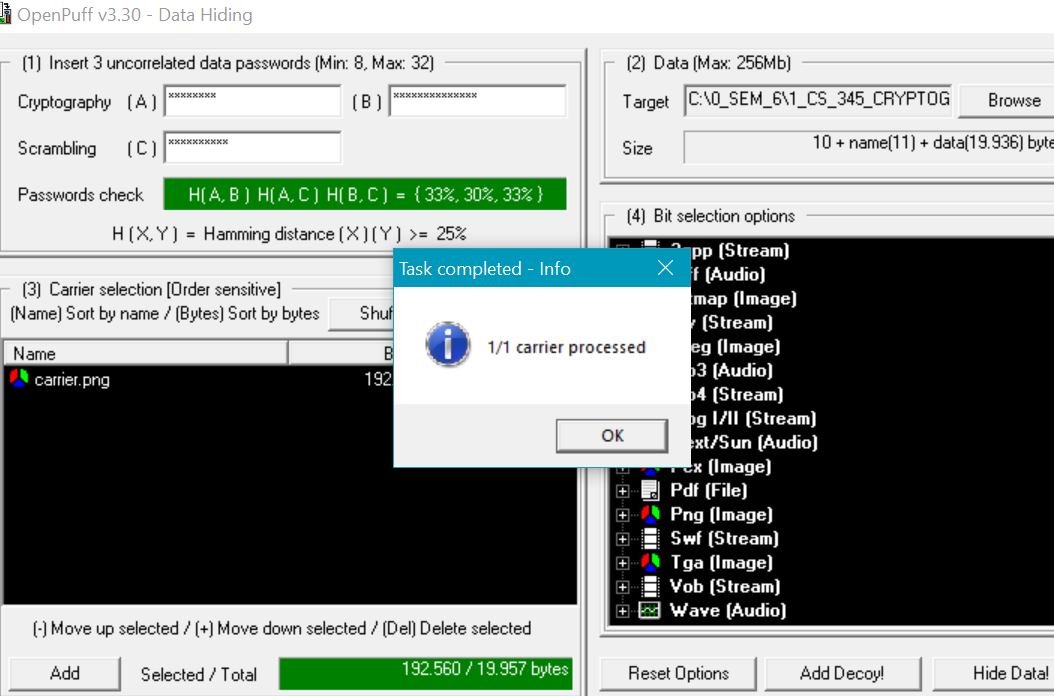
**SIZE OF SAMPLE.DOCX**



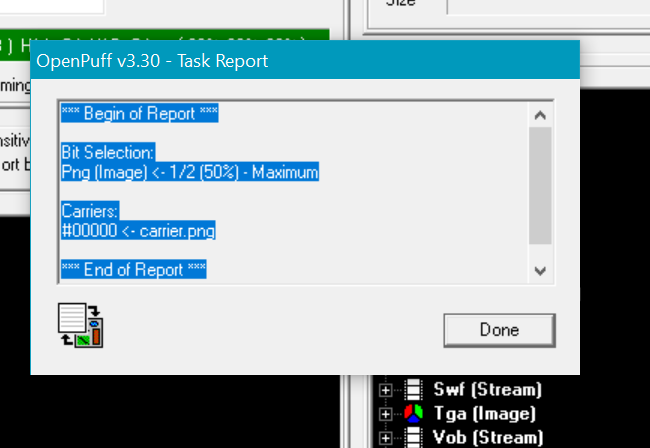
* As you can see in the above image, the carrier.png is uploaded in the Carrier Selection panel and sample.docx is uploaded in the Data Selection panel.
* We have used PNG image as carrier.



* If no error occurs, then, destination selection window will be prompted

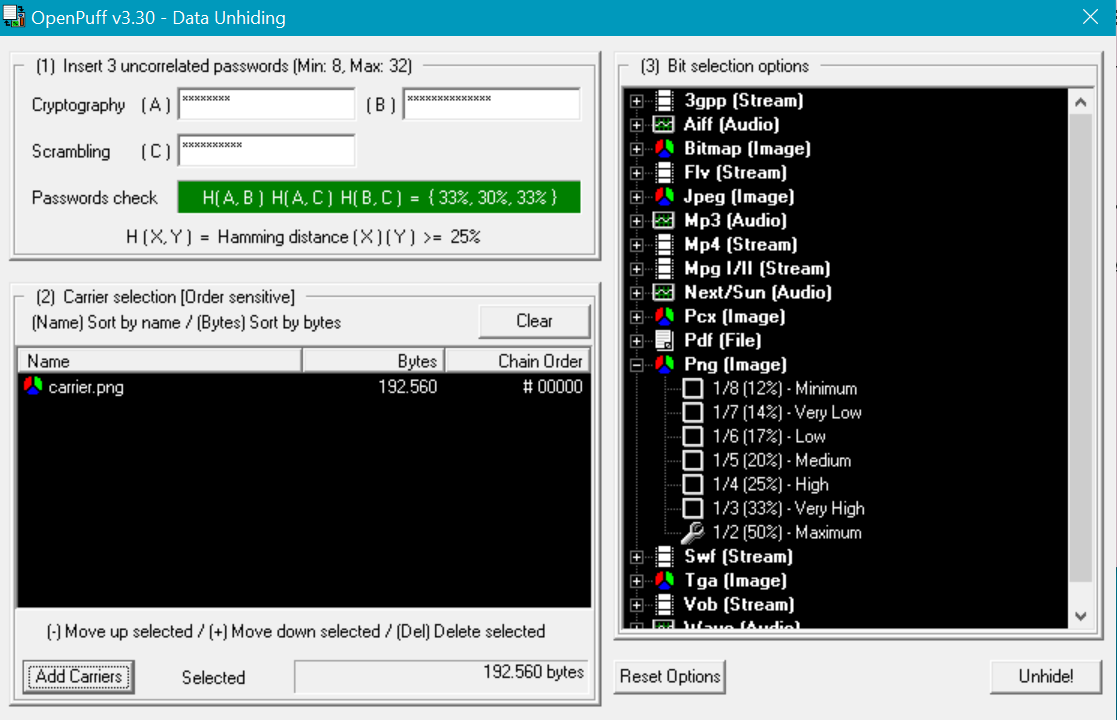


* Upon success, message will be displayed.

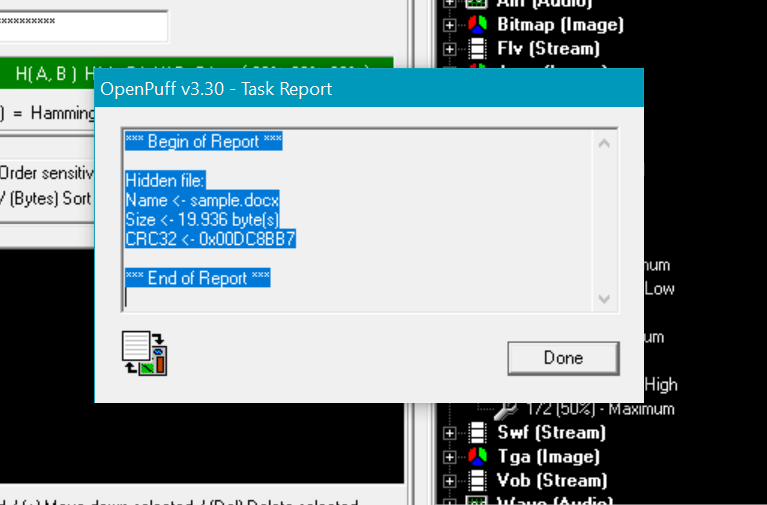


**DATA UNHIDING:**

* For data unhiding, we need to use the same passwords in the same order.
* All the other steps are same, we just need to unhide the image.



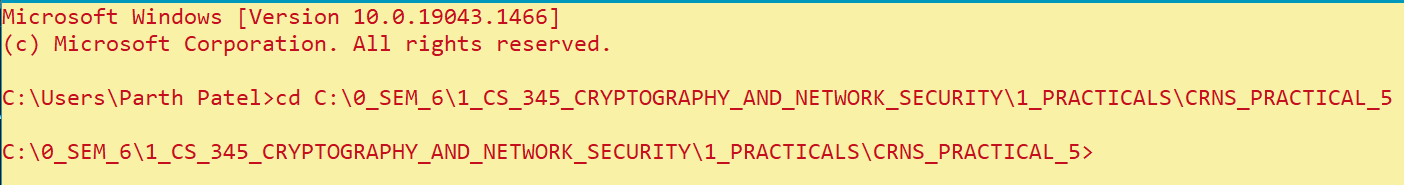
* In the unhiding section, we just need to enter the correct 3 passwords and upload the carrier that we intend to unhide.



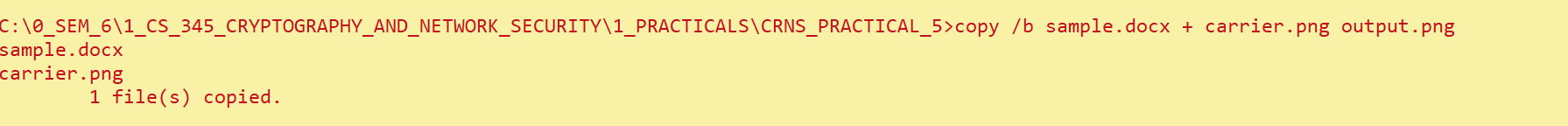
* Unhiding successful

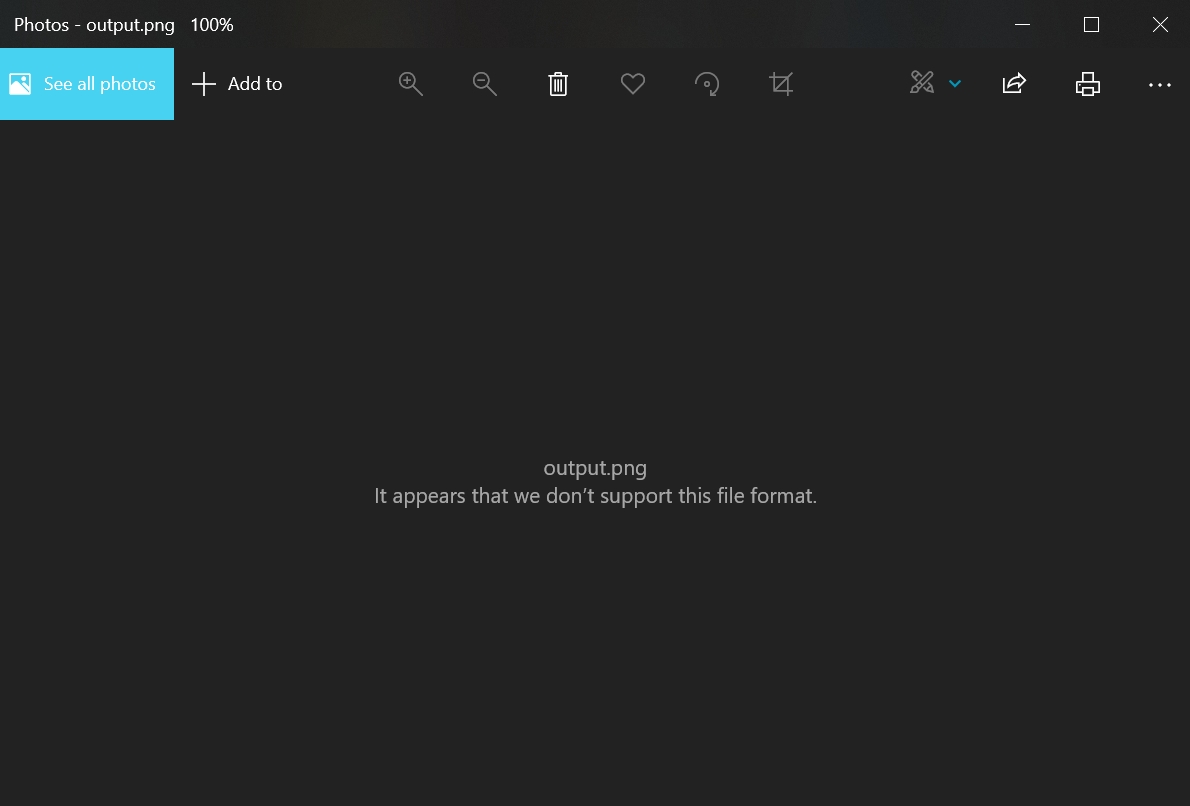
**USING CMD:**

* Open command prompt
* Enter the directory where you have your files.

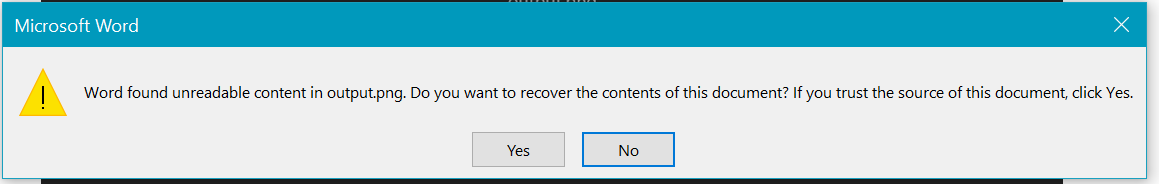


* Enter the following command to get the file with hidden data





* On opening the output.png file, error is shown because it appears to be a .png file but in reality has the hidden text.
* To unhide the data, we just need to open the file with notepad or notepad++ or word



* Message displayed and upon clicking yes, you will get the real data.



**CONCLUSION:**

By performing the above practical, I learned about the basics of Steganography and how to do data hiding and data unhiding using OPENPUFF and CMD.