PRACTICAL: 2

AIM:

The transmission of information need to be secure over the communication channel and the data has to be confidential. To do so, steganography is the technique to concealing/hiding the secrete file, message, audio or video in some another format of file. OpenPuff is one of the free steganography tool for windows environment. Study and implement the practical approach for Steganography.

-Using DOS commands
-Using OpenPuff Tool

THEORY:

What is Steganography?

In Steganography, the useless bits are actually replaced by the useful bits in order to hide the required file into any of the files or data mentioned above. It plays a vital role in cybersecurity by allowing legitimate users or peers to send the data in a highly secured way so that it could be protected from the hacker or malicious users who are intended to harm or abuse the system. It can be done using software that is available in the market for free or paid.

Steganography can also be considered the practice of concealing the crucial data into any of the files to be transmitted securely. The applications like SteganPEG, OpenStego, and so on are used to fulfill the purpose of wrapping up one file into another. Steganography's applications hide the required file's bits into another file so that the original file doesn't lose its characteristics. It can be considered pretty more secure than encryption or hashing. In these cases, the attacker can sniff at least the junks, but in the case of Steganography, they won't be able to detect if anything important has been transmitted. It is usually applied at a place where the data has to be sent secretly.

Working with Steganography

In order to work with Steganography, we have several applications available in the market. As we mentioned earlier, OpenStego, SteganPEG, is one of the applications that are used to implement Steganography. The data required to be wrapped and the data under which it has to be wrapped are being used by the application to merge them in a specific way. Working with these applications is very simple so that even someone from a non-technical background can also use them properly. The application works in a manner like; it asks the user to upload the file that has to be hidden, and then it asks to upload the file under which the first has to be hidden, then it processes both of the files with the algorithm in order to hide one under another one.

What is OpenPuff?

OpenPuff is a professional steganography tool with unique features, suitable for highly sensitive data covert transmission.

With OpenPuff, data is split among many carriers. Only the correct carrier sequence enables unhiding. Moreover, up to 256Mb can be hidden, if you have enough carriers at disposal. Last carrier will be filled with random bits in order to make it undistinguishable from others.

CODE:

```
Copy /b 19IT016.png +19IT016_INPUT.txt 19IT016_OUTPUT.png
```

OUTPUT:

- Using DOS commands

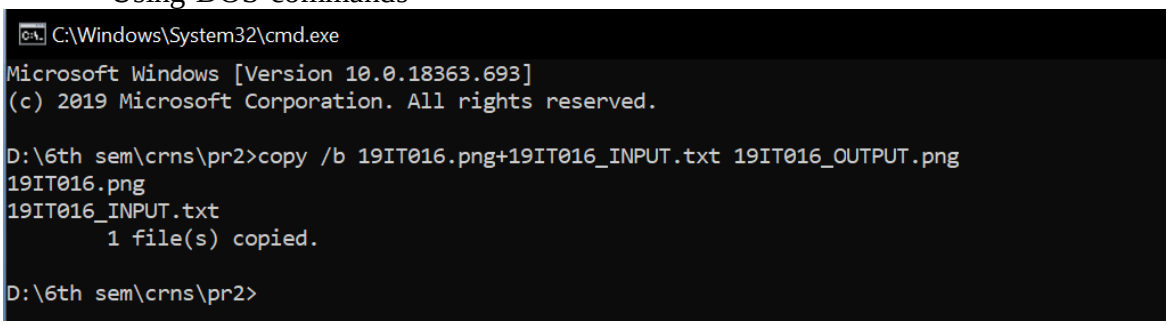

Figure 1: DOS command for add text at the end of image file using copy command for perform Steganography using DOS command

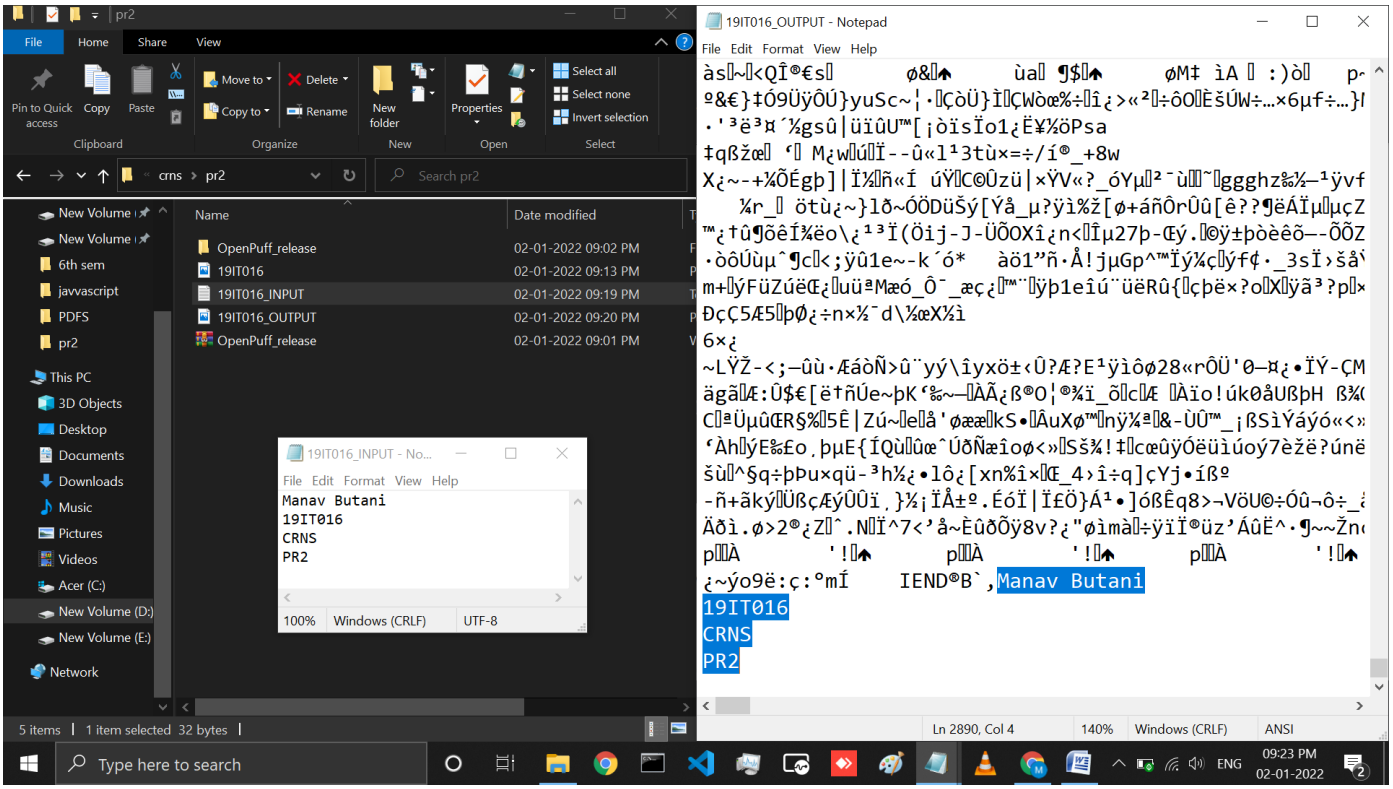

Figure 2: 19IT016_INPUT text file is added at the end of 19IT016 image file that you can see in 19IT016_OUTPUT file

- Steganography Process using OpenPuff Tool on image:
  - Hide

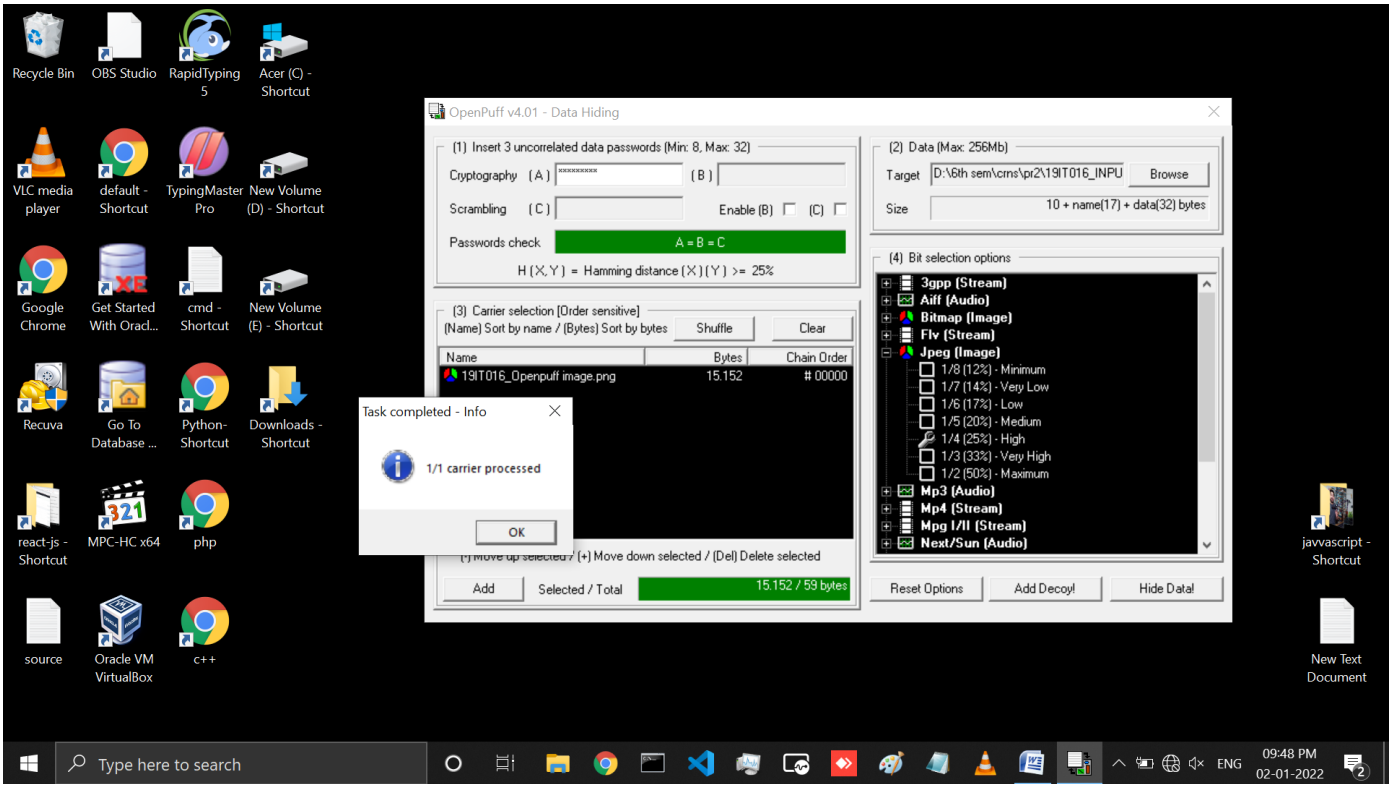

Figure 3: Steganography using openpuff for that first we need to add cryptography password , carrier selection ,data file and at last select the bit option and click on hide data button then select output file directory for store output file

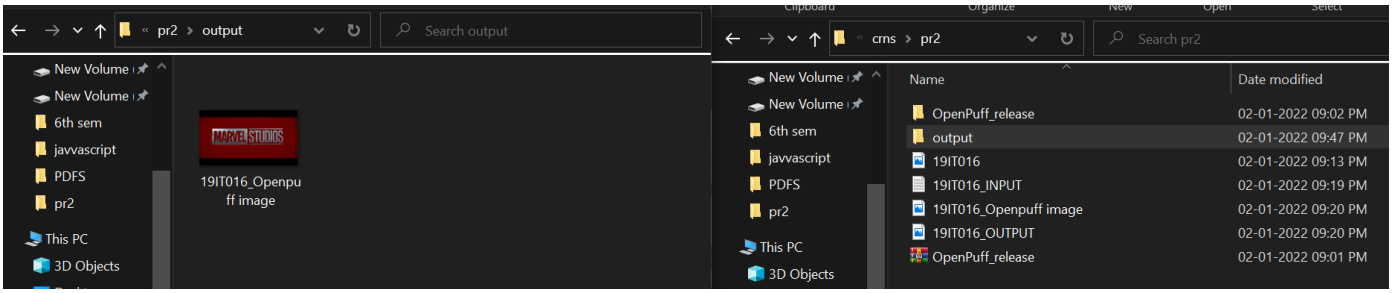

Figure 4: Input and Output file location

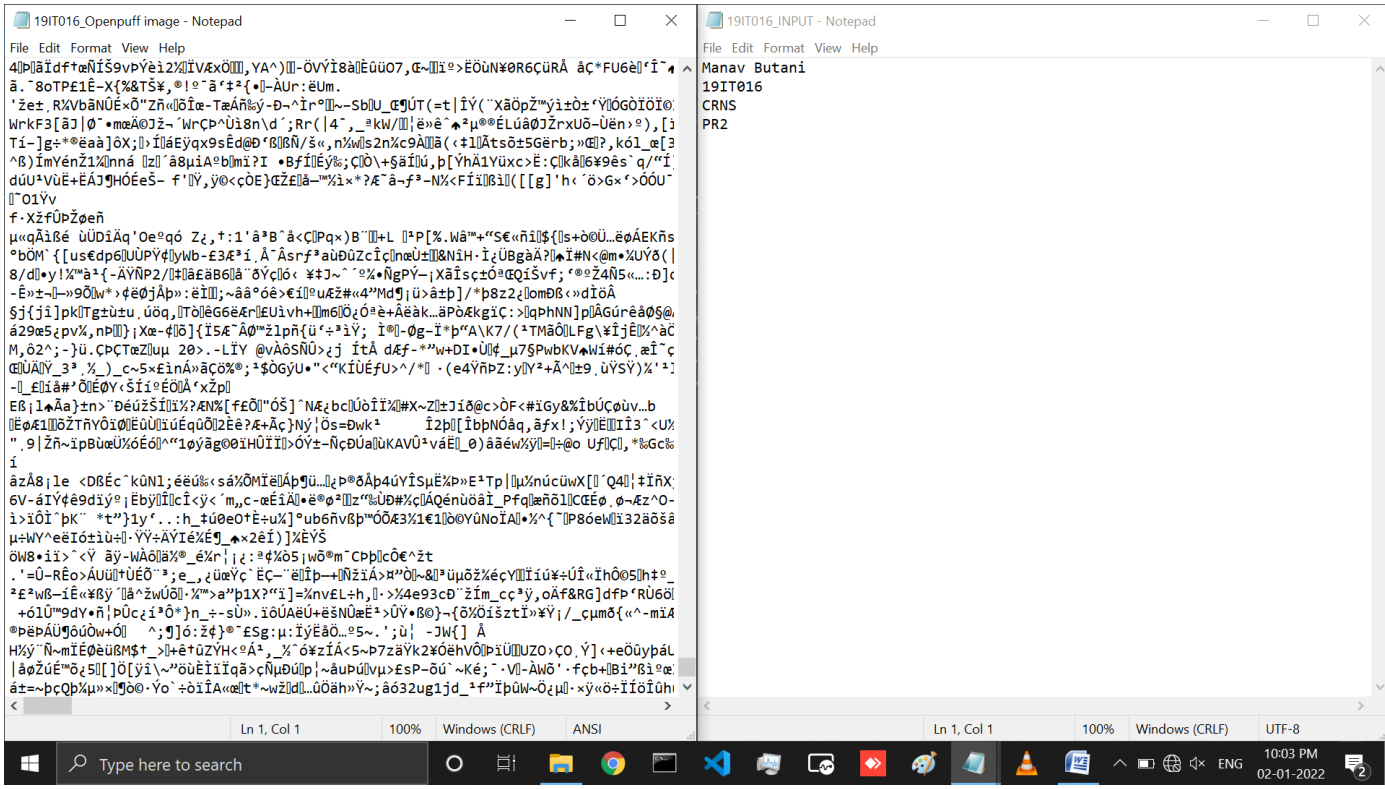

Figure 5: Output file for Steganography is created and openpuff report is also genrated and you can also see the input text file 19IT016_INPUT and created output file 19IT016_Openpuff image with steganography

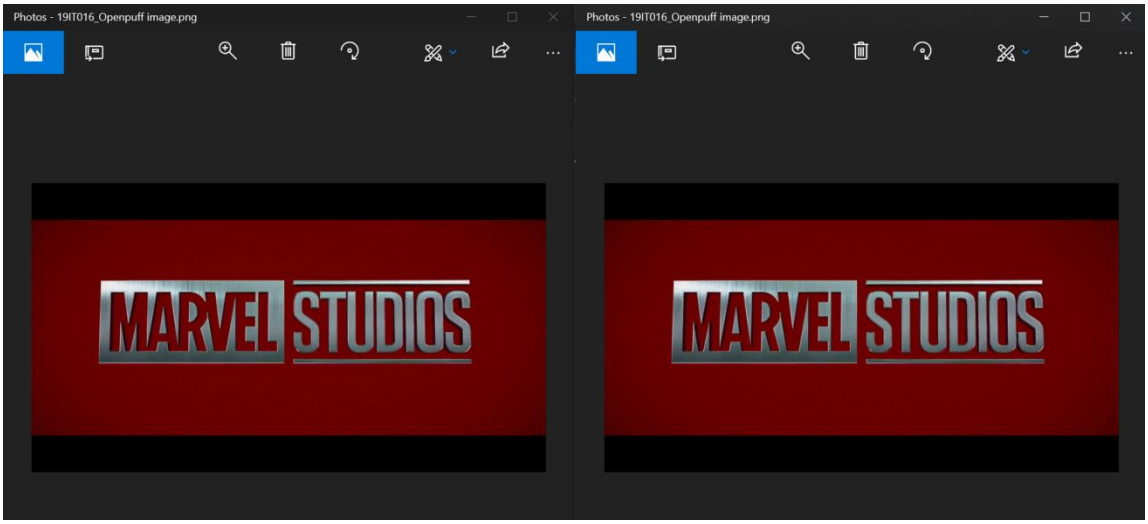

Figure 6: compare the image with steganography at left side and without steganography at right side

- Unhide

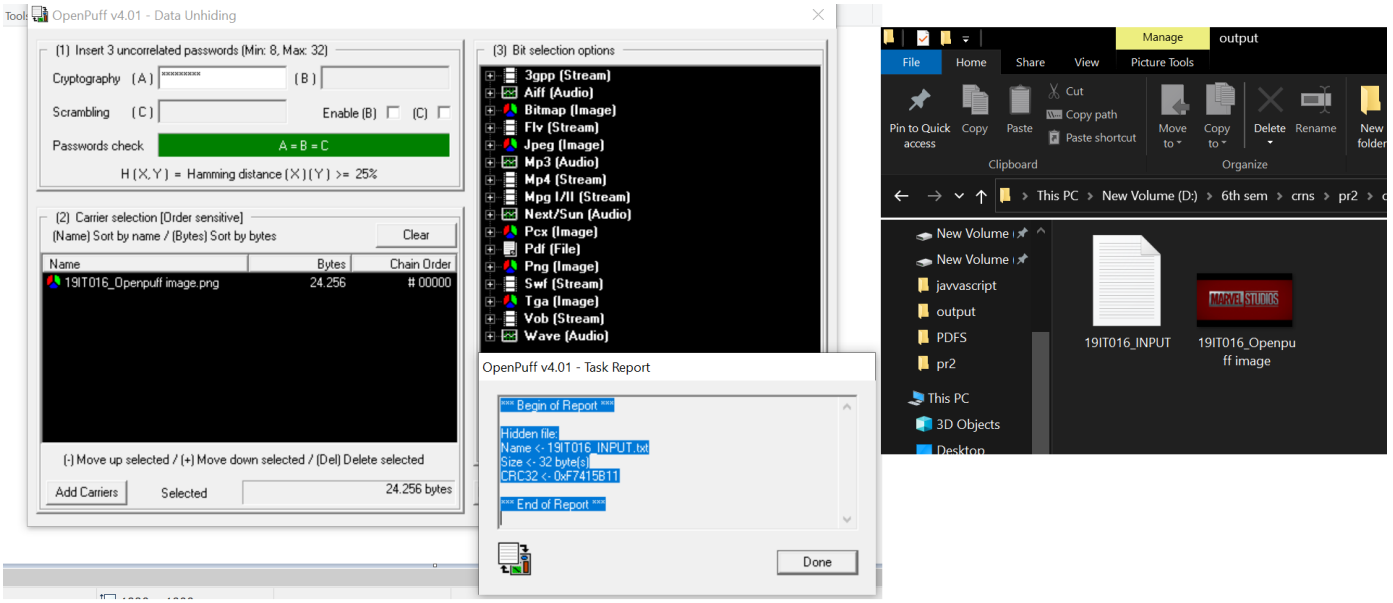

Figure 7: Remove steganography from output image file for that select unhide option in openpuff then write cryptography password ,output file and bit option and click on unhide option then select output text file location

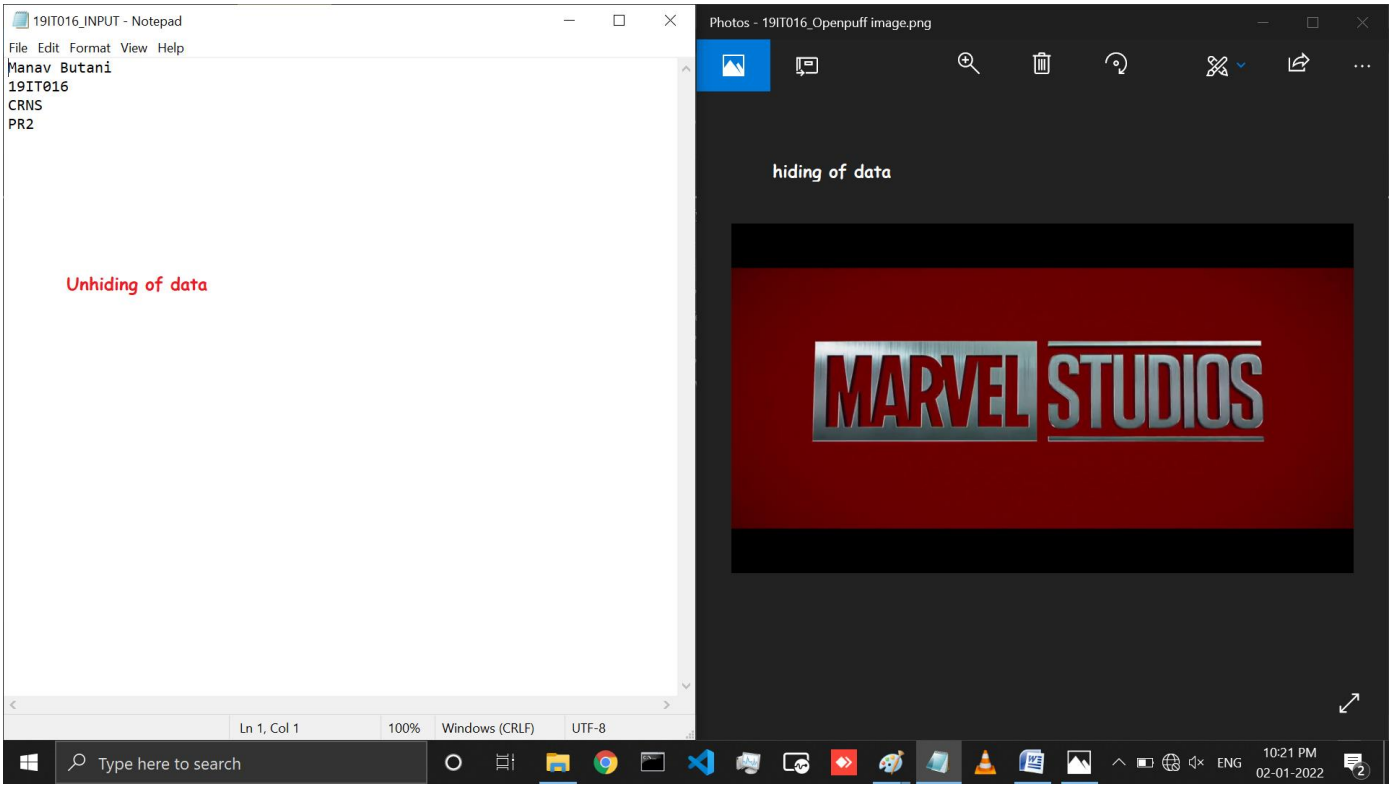

Figure 8: output text file is successfully generate and openpuff report is also generate and left side you can see the original output text file without steganography

- Steganography Process using OpenPuff Tool on video:
  - Hide

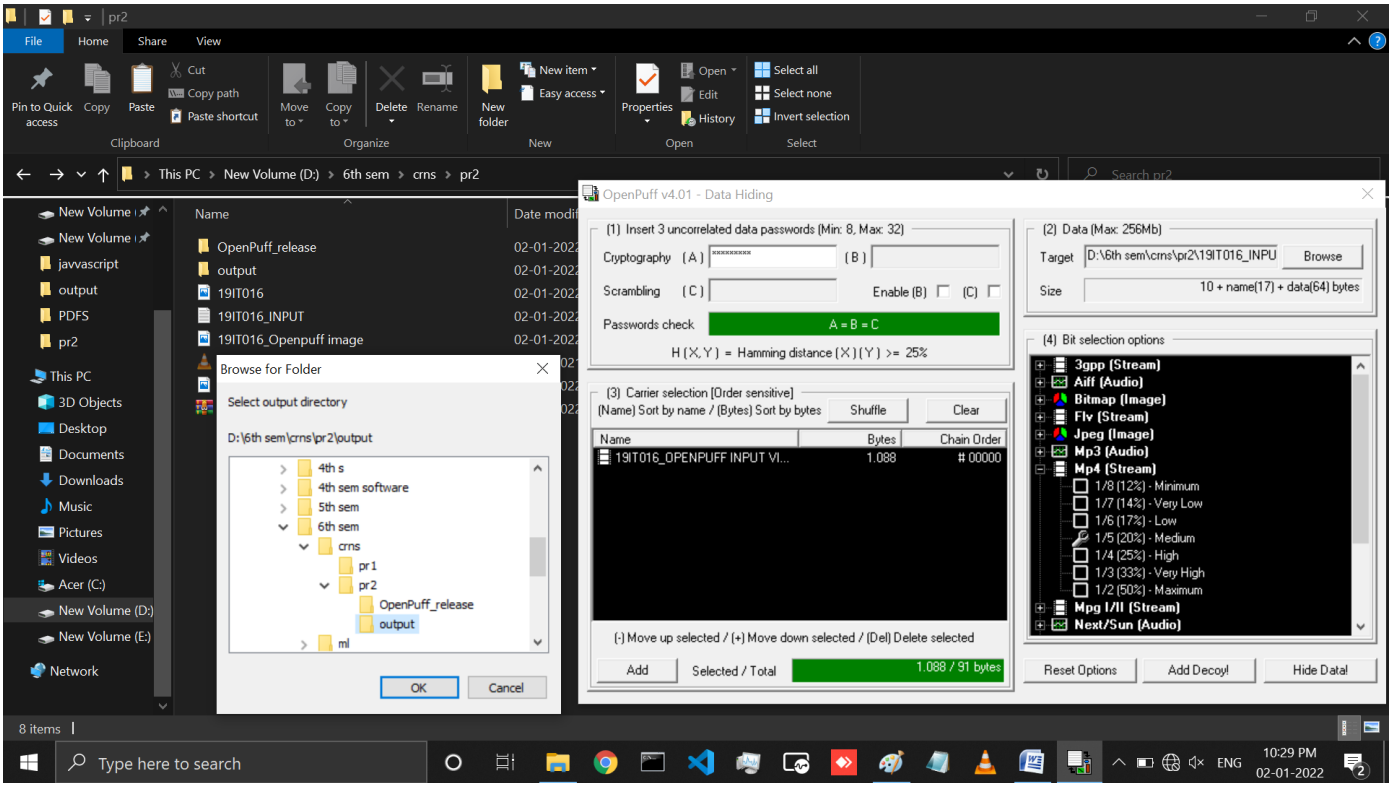

Figure 9: Performed same above process for applied steganography in mp4 file and hide text file in it and store output steganography file in output folder

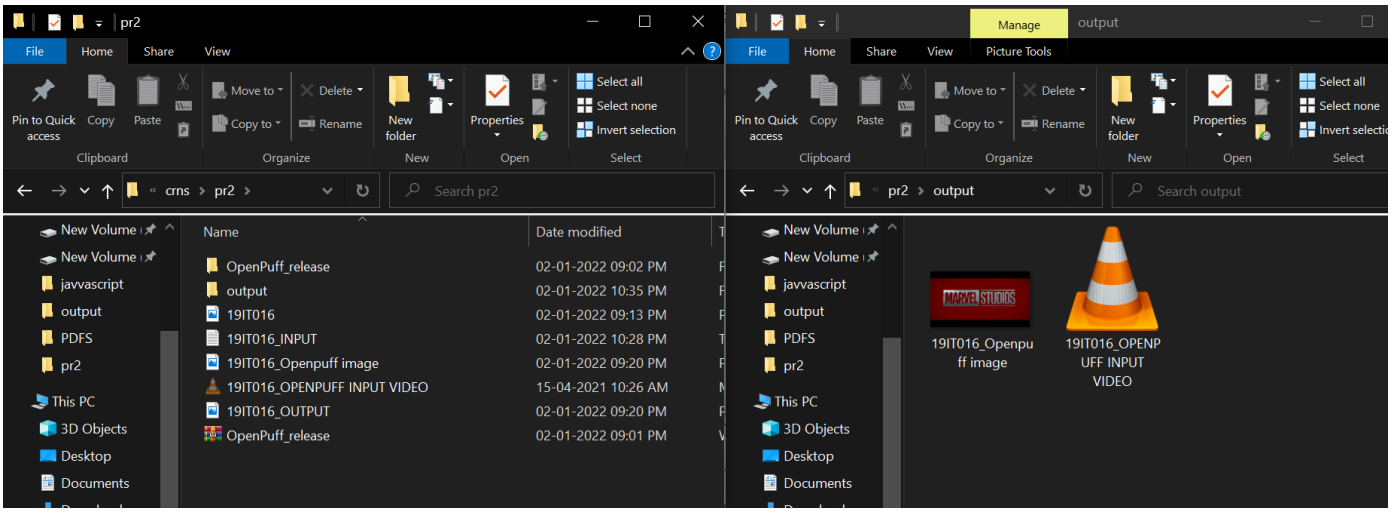

Figure 10: Input and Output file location

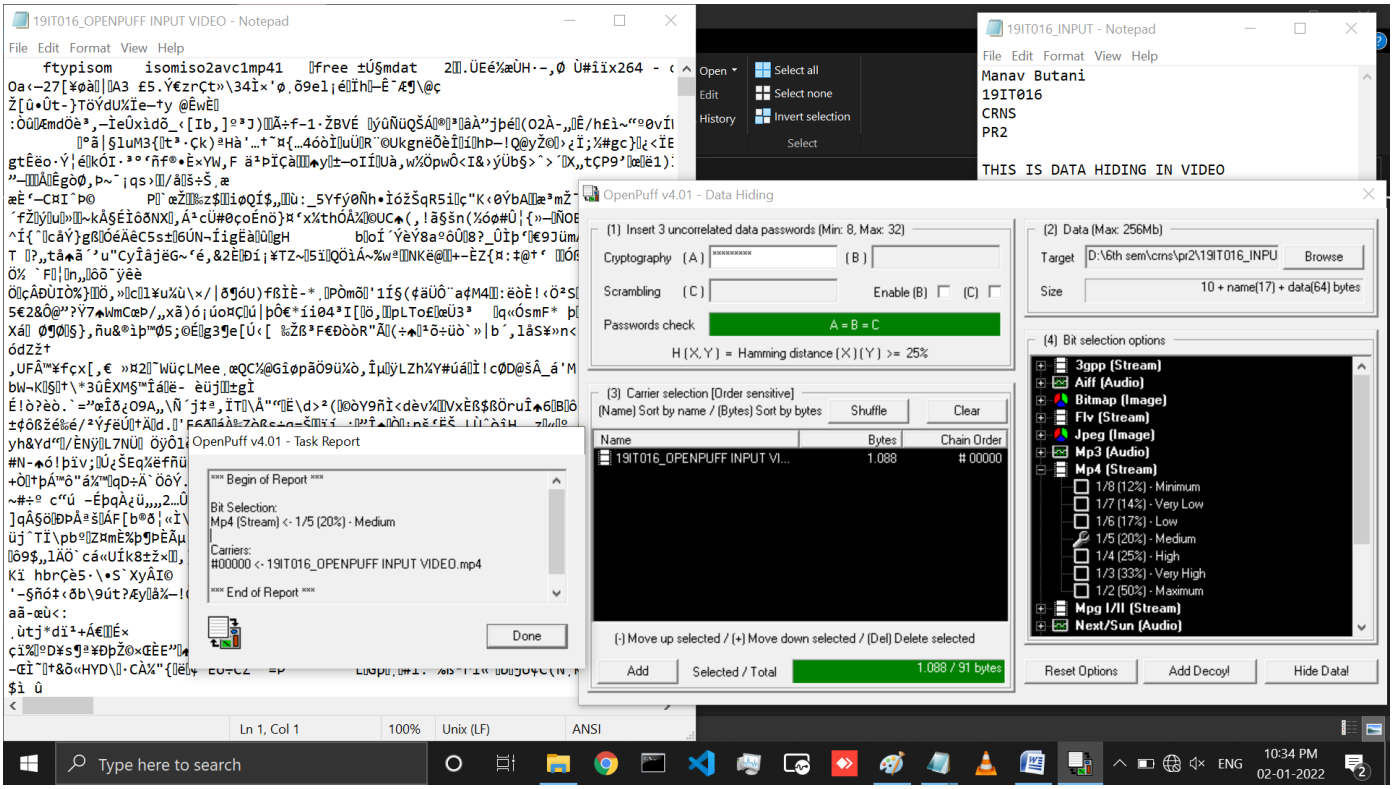

Figure 11: Openpuff report is generated and you can see the input text file 19IT016_INPUT datais hide inside 19IT016_OPENPUFF OUTPUT file

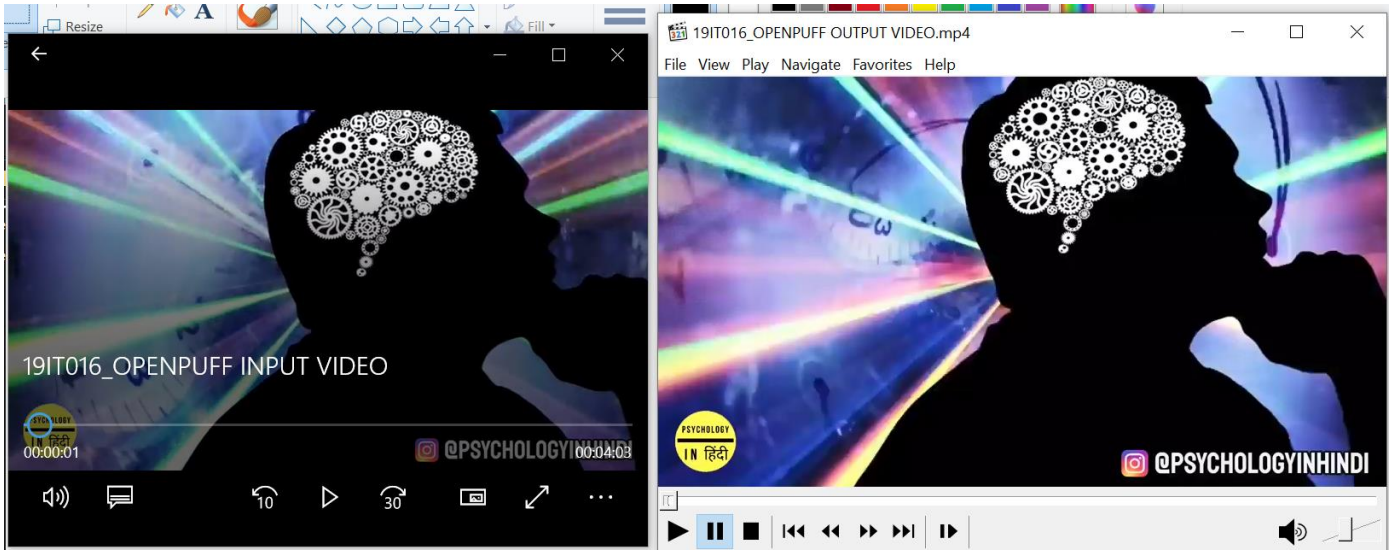

Figure 12: Left side you can see the 19IT016_openpuff input video input file without steganography and Right side you can see the 19IT016_OPENPUFF output video file with steganography and compareboth file

- Unhide

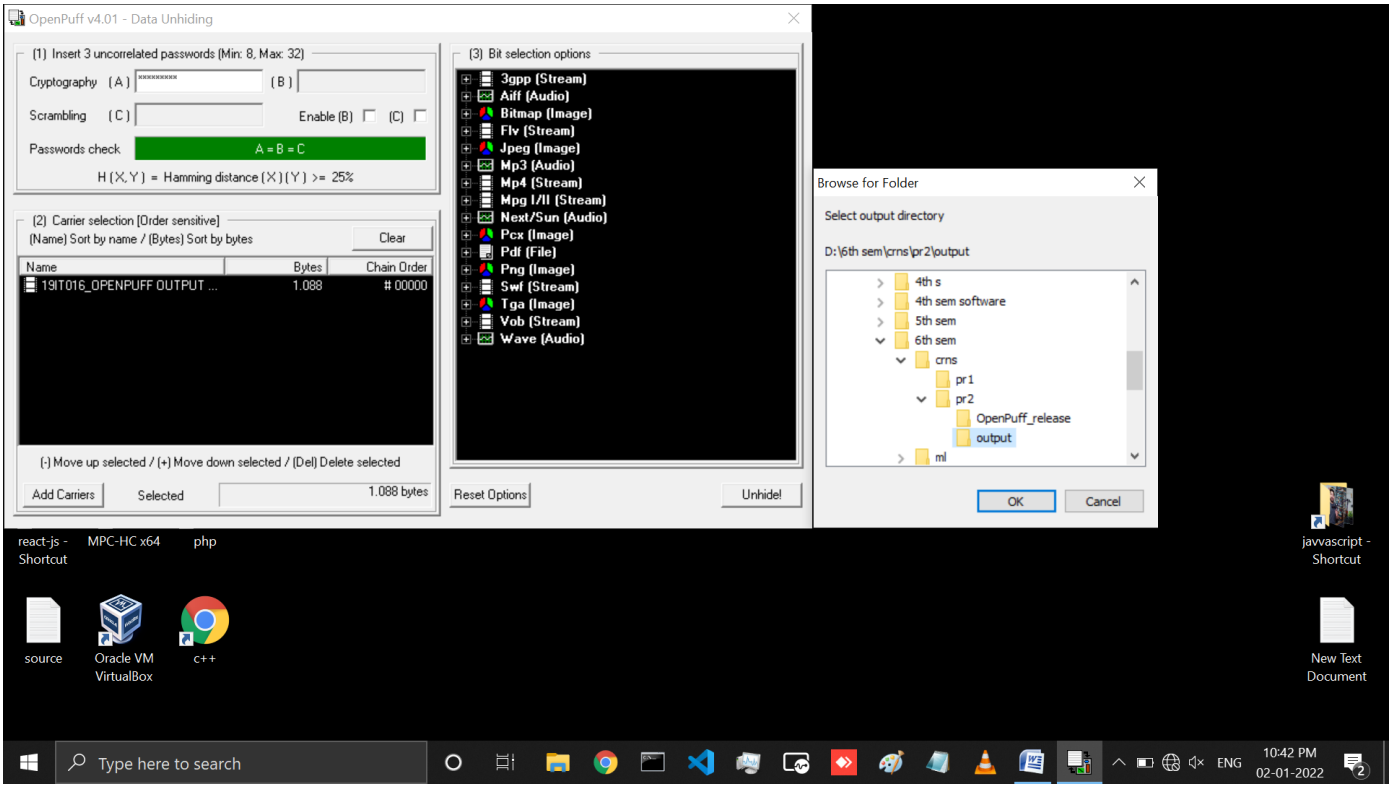

Figure 13: Remove steganography from output mp4 file and store in output folder for this Process follow same step that we have followed in above unhide process for image steganography

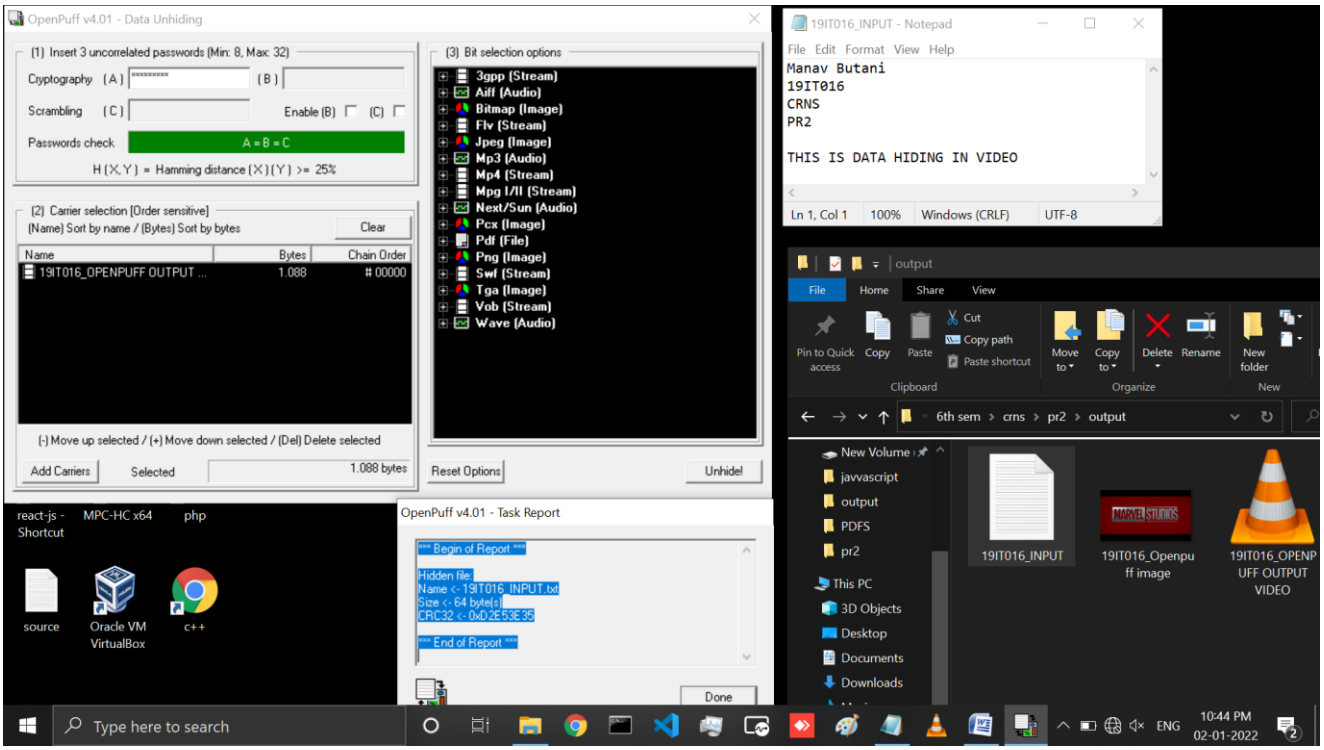

Figure 14: Here output text file is successfully generate from mp4 and openpuff report is also generate and left side you can see the original output text file without steganography

LATEST APPLICATIONS:

- Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. With these new techniques, a hidden message is indistinguishable from white noise. Even if the message is suspected, there is no proof of its existence. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser.
- Terrorists can also use steganography to keep their communications secret and to coordinate attacks. All of this sounds fairly nefarious, and in fact the obvious uses of steganography are for things like espionage. But there are a number of peaceful applications. The simplest and oldest are used in map making, where cartographers sometimes add a tiny fictional street to their maps, allowing them to prosecute copycats. A similar trick is to add fictional names to mailing lists as a check against unauthorized resellers.
- Most of the newer applications use steganography like a watermark, to protect a copyright on information. Photo collections, sold on CD, often have hidden messages in the photos which allow detection of unauthorized use. The same technique applied to DVDs is even more effective, since the industry builds DVD recorders to detect and disallow copying of protected DVDs.

LEARNING OUTCOME:

In this practical we have learned all about Steganography and also learned how we can hide text data in audio, video and image file using Steganography. In this practical we have performed Steganography practical using to approach one using DOS commands and another using OpenPuff Tool. In DOS approach we can see the message in readable formats but in Openpuff message is not readable and at least we have also learned about some latest applications related to Steganography.

REFERENCES:

1. OpenPuff: https://embeddedsw.net/OpenPuff_Steganography_Home.html
2. Theory: https://www.educba.com/what-is-steganography/
3. Applications: http://www.ijmer.com/papers/Vol2_Issue6/EN2646344638.pdf