**Digital Forensics Lab Report: 1**

Date: 27-07-2022

|  |  |
| --- | --- |
| Name: | Vedant H. Patel |
| Roll No: | 19BCP138 |
| Subject Code: | 20CP411P |
| Subject Name: | Digital Forensics Lab |

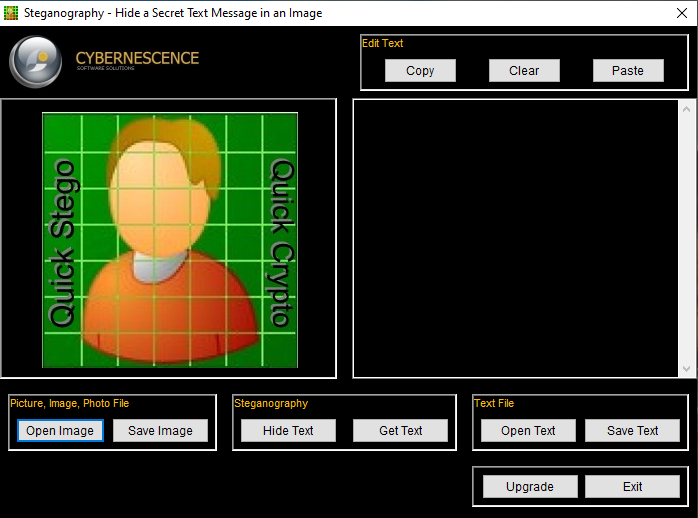
**Aim/Purpose:** Perform Steganography using Stegano tools

**Tool Names:** Quick Stego, Deep Sound, Oursecret, Wbstego, Quickcrypto, spam mimic

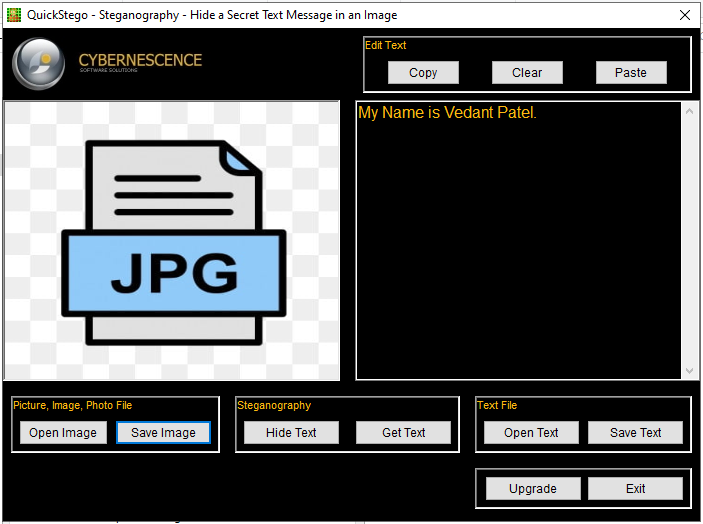
**Task 1:** Perform Image Steganography

**Steps:**

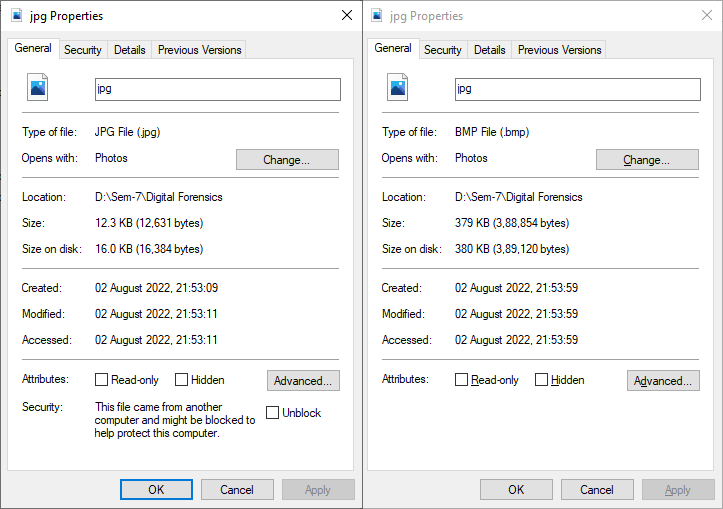
1. Install and run the Quickstego tool
2. Select the “Open Image” button to open a file browser and select the carrier file (image) to perform the stego operation
3. Write a secret message in an empty box situated on the right side of the tool and click on hide text
4. Click on “Save Image” to save the stego file



***Fig* Quick Stego Tool**



***Fig* Storing Secret Message**



***Fig* File comparison of the original file and Stego file**

**Analysis:**

1. While comparing the original file with the stego file (encoded file) we can see there are lots of differences in both files.
2. File format is different, file size is different and timestamp is different.

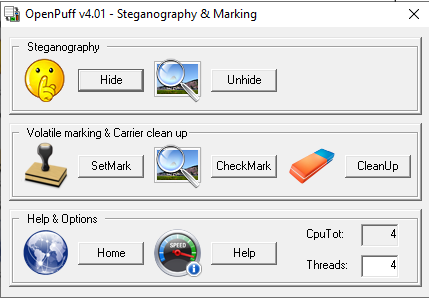
**Similar Tools:**

* Camouflage
* Ssuite Picsel
* Hide n Send
* Xiao Steganography
* Image stego
* Steghide
* crypture
* SteganographX Plus
* SteganPEG
* Open stego

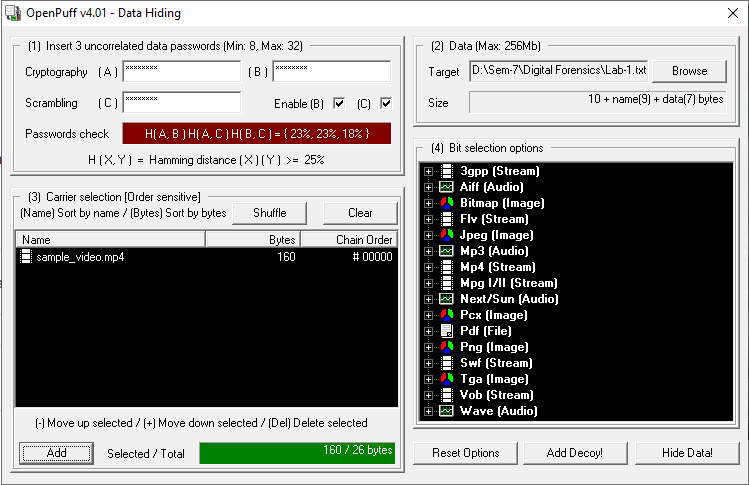
**Task 2:** Perform Video Steganography

**Steps:**

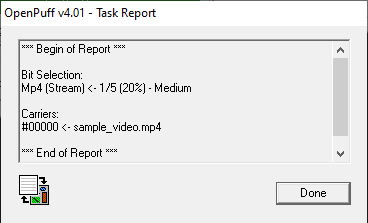
1. Download it from the link given above and after that run it from the directory where you have downloaded it.
2. Now, click on the Hide button to enter the main interface of OpenPuff.
3. Here in this window the interface is divided into 4 sections for performing different tasks. In the first section set the desired password for unhiding your data.
4. Navigate to the 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 the carrier video file and then hit the Hide Data button to complete the process.



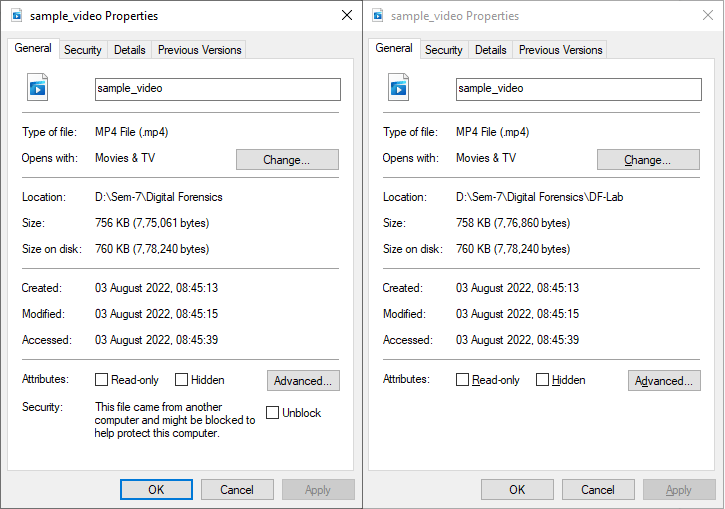
***Fig* OpenPuff tool**



***Fig* To encode video file to hide the text file**

****

**Fig Final report**

****

**Fig Size difference between both file**

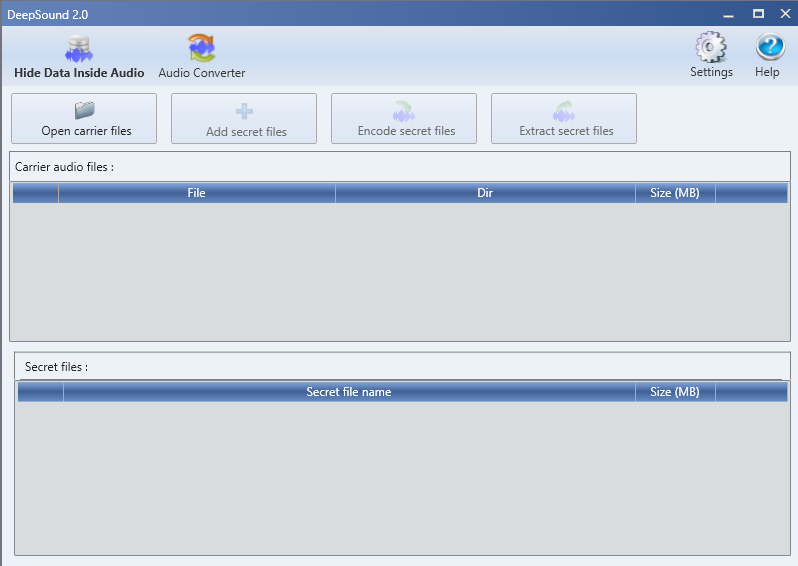
**Analysis:**

1. A Prototype for Secure Information using Embedding Algorithm and Extracting Algorithm which decrease the discolor pixels in every frame, to increase the embedded Capacity in compressed video steganography.

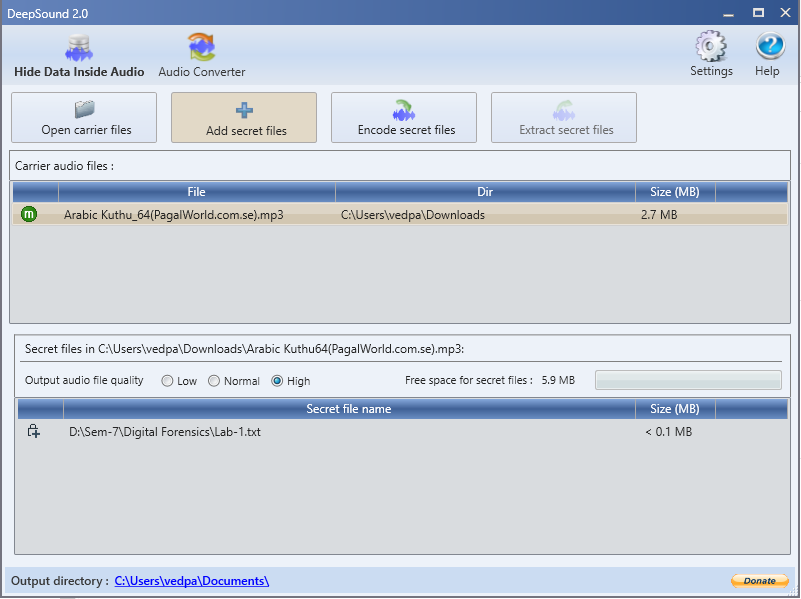
**Task 3:** Perform Audio Steganography

**Steps:**

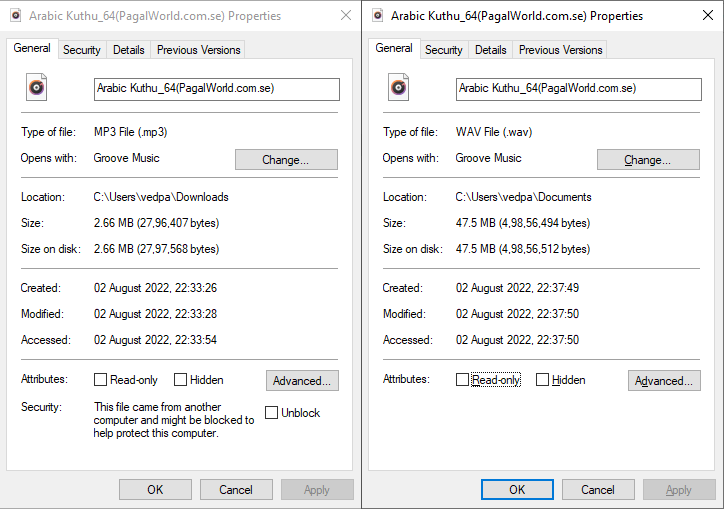
1. Install and run the Deep sound tool
2. Select the “Open Carrier File” button to open a file browser and select the carrier file (audio) to perform the stego operation
3. Select the “Add Secret Files” button to open a file browser and select the secret files to hide.
4. Click on the “Encode Secret File” button. Select the output file format and set the password for the stegno file and it will be saved to your set directory.



***Fig* DeepSound Tool**



***Fig* Storing Secret File to Audio carrier**



***Fig* File comparison of the original file and Stego file**

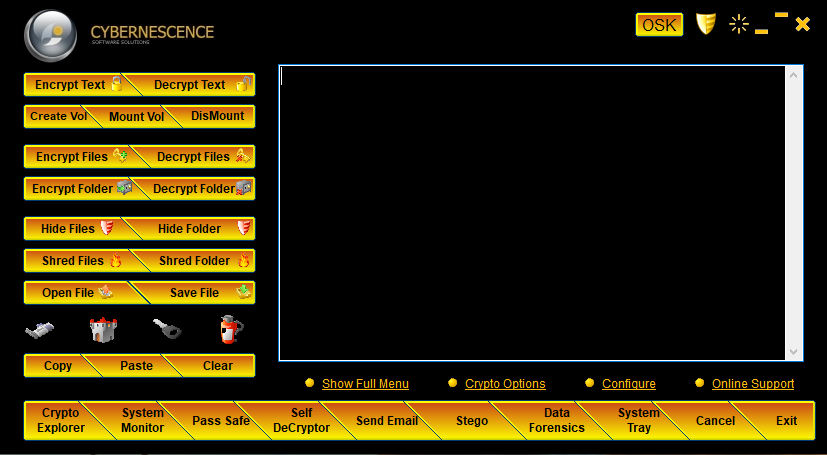
**Analysis:**

1. While comparing the original file with the stego file (encoded file) we can see many differences in both files
2. The file format is different, the file size is different and the timestamp is different.

**Task 4:** Perform Steganography using Quickcrypto Tool

**Steps:**

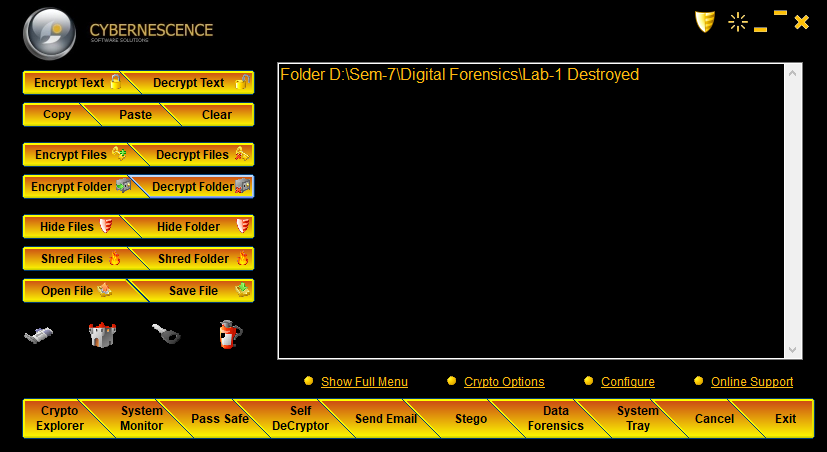
1. Install and run the Quickcrypto tool
2. Select the “Hide Folder” button to open a file browser and select the Folder to hide.
3. It will hide the folder and show messages as per figures.



***Fig* Quickcrypto Tool**



***Fig* Hiding the secret folder**

***Fig* Folder Hidden**

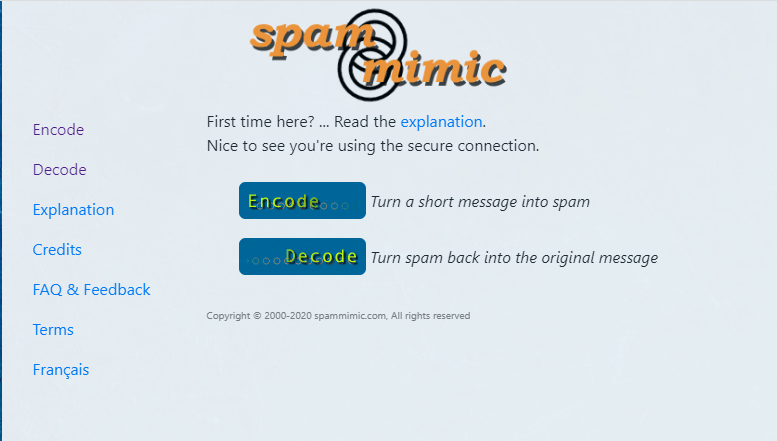
**Analysis:**

1. It allows you to hide files on your system so only you can recover and use them.
2. Also conceal sensitive data (text and files of any type) into innocent 'carrier' files: JPEG, GIF, BMP, MP3, and WAV. Easily blend encrypted files and messages into many other files.

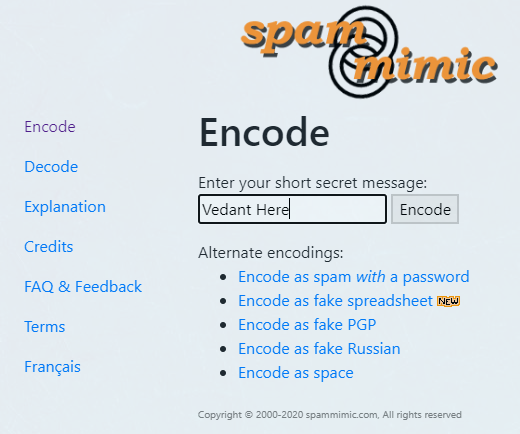
**Task 5:** Perform Steganography using Spammimic Tool

**Steps:**

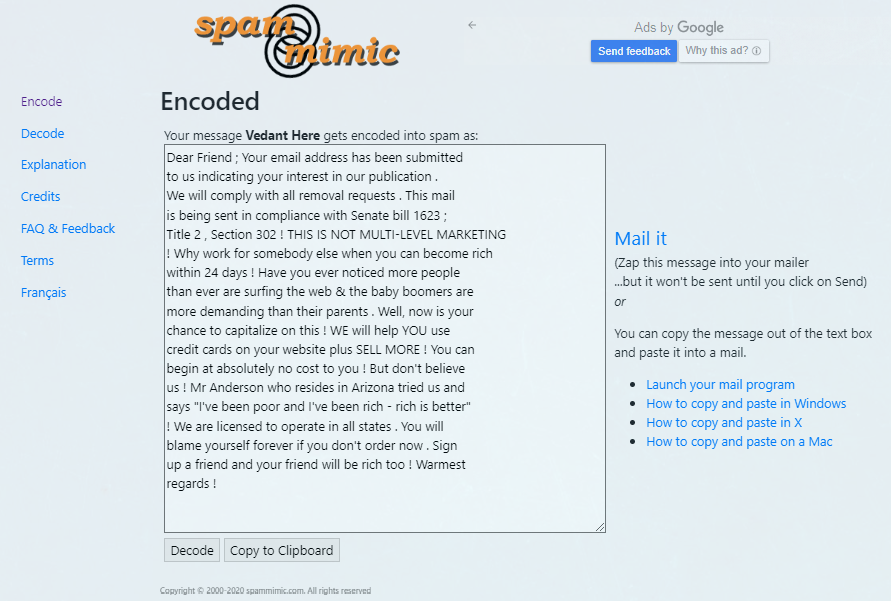
1. Open the website: [www.spammimic.com](https://www.spammimic.com/)
2. Select the Encoding method to encode your secret message.
3. Write your secret message and click on the “Encode” button.
4. To decode your secret message click on the “Decode” button and select the encoded format to decode.
5. Write your encoded message and click on the "Decode" button it will show you the secret message.



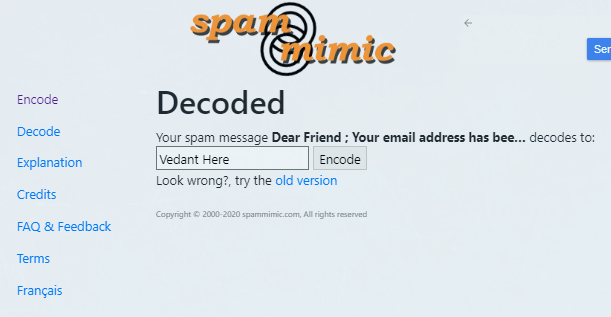
***Fig* Spammimic Tool**



***Fig* Encode secret message**



***Fig* Encoded message**



***Fig* Decode secret message**

**Analysis:**

1. It allows you to encode your small texts, emails, and messages with various different methods and also gives you the way to decode the specific encoded format text.

**Other Steganography Tools:**

* Camouflage (Imager Steganography)
* Ssuite Picsel (Imager Steganography)
* Hide n Send (Imager Steganography)
* OpenStego
* crypture
* Steghide
* Xiao Steganography (Imager Steganography)
* Quickstego (Imager Steganography)
* wbStego (Document Steganography)
* Our secret (Video Steganography)
* Quick crypto (Folder Steganography)
* Deep Sound
* Sonic visualizer
* Openpuff
* Netcross
* StegDetect
* Spammimic Web (Mail Steganography)