

Assignment Steganography

If you are concerned about installing any of the software in these projects on your regular computer, you can instead install the software in the Windows virtual machine, ask the instructor for details.

Part 1 Using OpenPuff Steganography

Unlike cryptography that scrambles a message so that it cannot be viewed, steganography hides the existence of the data. In this project, you will use OpenPuff to create a hidden message.

1. Use your web browser to go to
embeddedsd.net/OpenPuff_Steganography_Home.html

It is not unusual for websites to change the location of where files are stored. If the URL above no longer functions, open a search engine and search for "OpenPuff."

2. Click **Manual** to open the OpenPuff manual. Save this file to your computer. Read through the manual to see the different features available.
3. Click **OpenPuff** to download the program.
4. Click **Screenshot** to view a screen capture of OpenPuff. Right-click on this image and save this image **OpenPuff_Screenshot.jpg** to your computer. This will be the carrier file that will contain the secret message.

For added security OpenPuff allows a message to be spread across several carrier files.

5. Navigate to the location of the download and uncompress the Zip file on your computer.
6. Now create the secret message to be hidden. Open Notepad and enter **This is a secret message**.
7. Save this file as **Message.txt** and close Notepad.
8. Create a Zip file from the **Message** file. Navigate to the location of this file through Windows Explorer and click the right mouse button.
9. Click **Send to** and select **Compressed (zipped) folder** to create the Zip file.
10. Navigate to the OpenPuff directory and double-click **OpenPuff.exe**.
11. Click **Hide**.

Under Bit selection options, note the wide variety of file types that can be used to hide a message.

12. Under **(1)** create three unrelated passwords and enter them into **Cryptography (A)**, **(B)**, and **(C)**. Be sure that the **Scrambling (C)** password is long enough to turn the **Password check** bar from red to green.
13. Under **(2)** locate the message to be hidden. Click **Browse** and navigate to the file **Message.zip**. Click **Open**.
14. Under **(3)** select the carrier file. Click **Add** and navigate to **OpenPuff_Screenshot.jpg** as shown in Figure 3-11.
15. Click **Hide Data!**
16. Navigate to a different location than that of the carrier files and click **OK**.
17. After the processing has completed, navigate to the location of the carrier file that contains the message and open the file. Can you detect anything different with the file now that it contains the message?
18. Now uncover the message. Close the OpenPuff Data Hiding screen to return to the main menu.
19. Click **Unhide**.
20. Enter the three passwords.
21. Click **Add Carriers** and navigate to the location of **Carrier1** that contains the hidden message.
22. Click **Unhide!** and navigate to a location to deposit the hidden message. When it has finished processing click **OK**.
23. Click **Done** after reading the report.
24. Go to that location and you will see **Message.zip**.
25. Close OpenPuff and close all windows.

Deliverable

1. Submit a screenshot showing the images bytes without the hidden file and show the bytes of the file with the hidden file. You can use Windows Explore.
2. Submit a screenshot showing successful hiding and unhiding the document.

Part 2 Hiding an image in multiple images or video.

Using what you have learned in part 1. Identify a word document file that is not more than 15Kb. Using sample images or videos as Carriers. Hide the Word document into a group of images or videos.

Use only 1 password to secure the files and deactivate the other passwords.

3. Submit a screenshot showing the images bytes without the hidden file and show the bytes of the file with the hidden file. You can use Windows Explore.
4. Submit a screenshot showing successful hiding and unhiding the document.

Part 3 Questions

1. Which areas of a file *cannot* be used by steganography to hide data?
2. What are the advantages and disadvantages of using steganography versus symmetric or asymmetric encryption?
3. Which of the 5 security fundamentals principals for defense can be found using steganography,
4. Explain how each principal is used from questions 3.

Grading Rubric

Correct submission of Part 1	30 points
Correct submission of Part 2	30 points
Correct submission of Part 3	40 points
Total	100 points