**Advanced Steganography Lab**

**Purpose and Objective:**

This lab was created to demonstrate how steganography works, why it’s used, and if it’s even worth using. The goal of this lab is to familiarize the participant with the various techniques and types of data that can be concealed. We will analyze this in different forms such as images, audio files, and video files.

***Lab deliverables:***

1. Were you familiar with the concept of Steganography before this lab? If so, what were you familiar with? What did you learn?
2. Using your knowledge of cryptography from class, what are the key differences between steganography and cryptography? Why would you use one over the other?
3. What can be said about the legality and ethics regarding steganography? How could this technology be used in a harmful way?
4. Which steganographic method was your favorite? Why?
5. Given the results from task1 and task2, which method would you say does a better job at concealing the hidden message? Why?
6. Was this lab enjoyable? Is there anything that can be improved in this lab?

**TASK 1: Steganography Basics**

This task is designed to familiarize you with the basics of Steganography by having you conceal two local files. To start, we will have you conceal a custom text file in a provided image.

1. Create a .txt file with a secrete message of your choosing. Name this file secretmessage.txt. Place the .txt file and the stegimage.png from the repository alone in a directory.
2. Zip the .txt in a text.zip file. If you do not have archiving software, download something like [7-zip](https://www.7-zip.org/) or [WinRAR.](https://www.win-rar.com/start.html?&L=0)
3. Open your command line and cd into the “Task1” directory. Once there, type “ls” to list the contents of the directory.
4. Enter “copy /b stegimage.png+secretmessage.zip image2.png” into the console.

Text

Description automatically generated

1. When opening this new image, there should be no differences. Great! You should note that the original image is slightly smaller than the new image2.png.

vs 

This is because image2.png is holding the bit values of the text file.

1. Now try opening this image with archiving software, and you should see the original stegimage.png and text.txt files. You’ve successfully concealed a secret message in an image file!

**Task 1 deliverable:** Include this new image, the original image, and the secret message text file in your deliverable under the Task1 directory.

**TASK 2: Steganography Tools p1. (Image to Audio)**

In this task, we will be using a free tool called Coagula to generate audio from an image. Recall that in the last task, the newly generated image modified the LSB of the image file to conceal the secret message. This time, the LSB of an audio file will be modified with the data of the provided image file.

1. Download Coagula [here](https://www.abc.se/~re/Coagula/Coagula.html).
2. Once installed, open the application and import the secretimage.png. File -> Open Image -> project files -> task2 -> files(secret image) -> secretimage.bmp.
3. Graphical user interface, application, PowerPoint

   Description automatically generatedWith the image open in Coagula. Select Sound -> Render Image. (TURN DOWN YOUR AUDIO!) Coagula will play the audio that is generated from the image!
4. With this new audio generated under file, select “save sound as…” to download this newly generated audio. Save it as secretaudio.mp3

**Task 2 deliverable:** Include your new audio file named “secretaudio.mp3” in the task2 directory.

**TASK 3: Steganography Tools p2. (Image to Video)**

Now, we will be concealing an image file into a video file using the free software [OpenPuff](https://www.embeddedsw.net/OpenPuff_Steganography_Home.html).

**TASK 4: Least Significant Bit (LSB) Implementation**

In this task, we will be getting hands-on experience with LSB by modifying the bits of the file itself.

(write code using Python or download tool to modify LSB)