Steganography

To start with I looked at Wikipedia to see what steganography is. I quickly learned that it involved manipulating the data on an image in such a way that some data could be hidden inside of it but undetectable to the human eye. My research resulted in me discovering how to hide data and decode the image separately so that a message could be sent without needing to have the original image.

I started working on the project before we had done any labs so I thought that we weren’t allowed to use the original image to decode the picture and audio. To get around this I built a program that would change the RGB values to even or odd depending if a 1 or 0 was needed for the photo. The first 2 bytes of red and green were dedicated to the dimensions. After that it was just data. This encryption method made it possible to hide any image and send it to anyone.

When I moved onto audio it became too complex to get the audio to work and then I found out that I had to hide both at the same time, both of the algorithms started from the first pixel on the red channel. After the lab I learnt how data could easily be hidden, the only downside was this was more detectable. One thing that was useful was I had built a prime factor finder in JavaScript so I could quickly factorize the number of sample I had taken to find what the optimum dimensions were (greatest height).

This technology is surprisingly powerful. The programs I have built could be used to send a message hidden to another computer and the manipulation is undetectable and according to some sources some intelligence organizations have been using this to communicate with illegal spies. One major risk for the average computer user is if someone had encoded some malicious software inside the image. A viral image could be edited and released to the Internet and then a virtual pandemic would occur causing significant damage to the Internet.