Activity Examples

For all of the example cases, the image below (purpleFlower.png) is the file that was modified using steganography in.

purple flower
(original file)

The top secret image has a hidden message using RGB bit-modification technique. You cannot see it. For the cryptography method, each letter of a secret message is broken down to a number. That number is converted to binary and that binary number is spread across three pixels as the last digit of each pixel's RGB values. To decrypt the image, letters are decrypted by looking at the RGB values for three consecutive pixels. If they are odd or even numbers they are converted into 1s or 0s respectively. By building the binary number one digit at a time we can convert the digit to base 10 (decimal). Once in decimal form, we can using the ASCII value of the number to convert to text. The process is repeated until we come to the end of the file.

top secret

In the 8-bit and black and white examples below, no message is hidden. These were a natural extension of the activity to show what can be done with image modification. The modified image is exactly what is labeled and no more. Immediately below, we turned an image into an 8-bit version of itself, forcing each color to a nearby color, only 27 colors to choose from. For the 8-bit version, each color of the RGB spectrum is rounded to 0, 127 or 255, whichever is closest. Normally, colors are on a 0-255 spectrum so this limits the options to three for each color.

8-bit

The last example came from a realization that if you average the red, green, blue of a pixel and set each of the RGB values to the average, you get a black and white version of the image. We thought that was cool. Each pixel has its red, green, blue values averaged and each RGB is set to that average number. The result is a grey-scale version of the image.

black and white