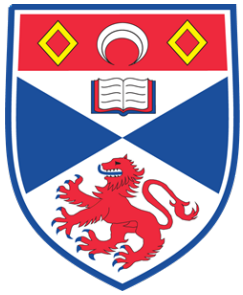
University of St Andrews

CS4203 Coursework 2

# Security Tools

*Author:*
150008022

November 23, 2018



# Goal

The goal of this practical was to use and evaluate common tools and techniques used in security: steganography and penetration testing.

# Part I
# Steganography

Least Significant Bit (LSB) steganography - specifically LSB1 - involves replacing the last bit of each byte of an image file (called the cover image) with a bit from the message to be hidden. For example, if each character in the message requires a single byte, then it can be hidden in 8 bytes of the cover image. If we instead use the two least significant bits, we can half the image size needed to mask our message, but this can result in more obvious distortion in the original image. The message being hidden doesn't necessarily have to be text either, images can be masked using other images as well.

The goal of steganography is not to make the message impossible to understand, but to instead make its presence unknown to all but those that know to look for it. Because of this, we can focus our attention on what human vision will not notice so that we can exploit it to efficiently mask messages.

Experiment 1 compares various images after LSB steganography is applied. In experiment 2, a comparison is made between LSBs effectiveness with RGB and a more perceptually focused format: YCbCr.

## Experiment 1

### 1.1 Introduction

Images can contain a range of spatial frequencies. High frequency images show fine details, whilst low frequency images consist of smoother transitions between dark and light (See figure 1). In this experiment, the effect of LSB on images of varying spatial frequencies is compared, using an online image steganography tool [1].

(a) High spatial frequency image (b) Low spatial frequency image

Figure 1: Comparison of spatial frequencies in images [2]

## 1.2 Aims

The aims of this experiment were:

1. to determine whether a high, medium, or low frequency image is a better candidate for a cover file.

2. to determine which combination of high or low frequency cover image and high or low frequency hidden image provides the best concealment.

## 1.3 Methods

In order to reduce the number of variables in this experiment and simplify masking one image in another, the images used were all cropped and scaled to the size of $640 \times 396$ pixels. Three images were used that contained either low, medium or high values spatial frequency components. The images were viewed on a 15.6" Matte FHD LED IPS display with a resolution of $1920 \times 1080$. The *Eye of GNOME* application was used to open and display the image files

A Matlab® script was written (*showDCT.m*) that converted the images to grayscale and used Discrete Cosine Transform to show the distribution of spatial frequencies. The images used and their spatial frequencies are shown in figures 2 to 6. The DCT plots show the lowest frequencies in the top left and the highest frequencies in the bottom right.

Using the online image steganography tool, each of three images (Figure 2 to 4) were combined, using the first, second, and fourth lowest bit planes.


Figure 2: High frequency image (left) and spatial frequency distribution (right).

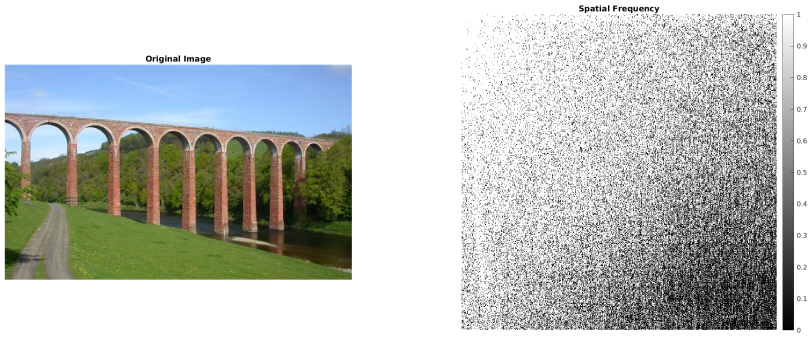



Figure 3: Mid frequency image (left) and spatial frequency distribution (right).

The two high frequency images (Figure 2 and Figure 6) and the two low frequency images (Figures 4 and 5) were also merged.

For aim 1, the best cover file would be the one that after hiding have the least visible changes compared to the original. The same metric could

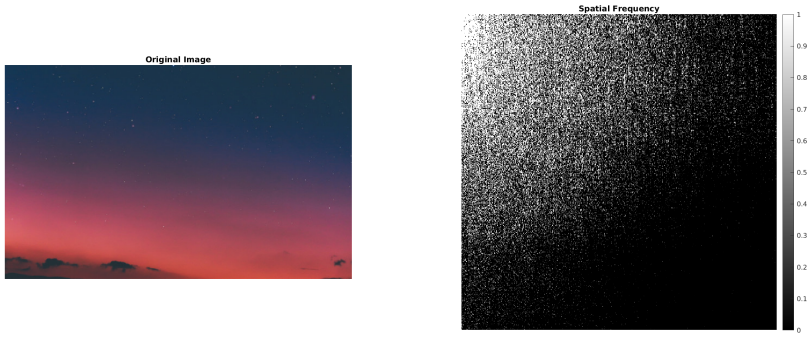



Figure 4: Low frequency image [3] (left) and spatial frequency distribution (right)

.

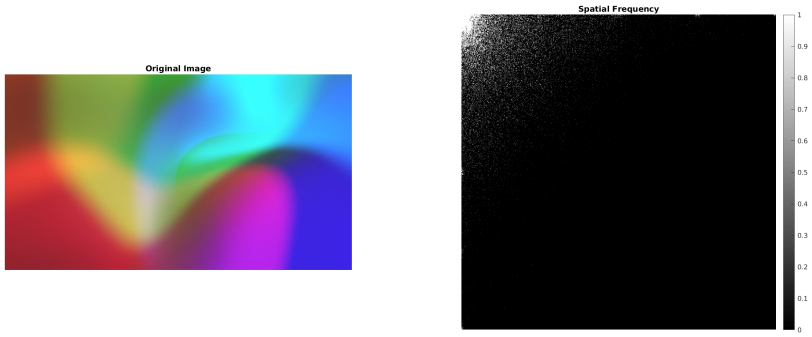



Figure 5: Low frequency image (left) and spatial frequency distribution (right)

.

be used for aim 2. The cover image with another hidden would first be compared to the original image, and then to the hidden image. If artefacts can be spotted when compared with the original, then the cover image offers


Figure 6: High frequency image (left) and spatial frequency distribution (right)

.

very weak protection, but if it can only be noticed when the hidden image is also shown, then the cover image offers some protection. If neither, then the cover image is very effective.

## 1.4 Experimental Trials

The resuls are shown in the style of a Cayley table, where the horizontal headers correspond to the cover image used, and the vertical headers correspond to the image that was hidden. A score of 1 to 10 is used for each combination, where 1 shows clearly the hidden image, and 10 is indecernible from the original cover image. An asterisk is used where no data was recorded.

### 1.4.1 LSB1

| Hidden \ Cover | Colourful | Viaduct | Sky |
|---|---|---|---|
| Colourful | * | 10 | 7 |
| Viaduct | 10 | * | 6 |
| Sky | 10 | 10 | * |
| Blurry | * | * | 10 |
| Galette | 10 | * | * |

### 1.4.2 LSB2

| Hidden \ Cover | Colourful | Viaduct | Sky |
|---|---|---|---|
| Colourful | * | 8 | 4 |
| Viaduct | 10 | * | 3 |
| Sky | 10 | 9 | * |
| Blurry | * | * | 9 |
| Galette | 10 | * | * |

### 1.4.3 LSB4

| Hidden \ Cover | Colourful | Viaduct | Sky |
|---|---|---|---|
| Colourful | * | 3 | 2 |
| Viaduct | 7 | * | 2 |
| Sky | 10 | 5 | * |
| Blurry | * | * | 4 |
| Galette | 8 | * | * |

## 1.5 Outcomes

## 1.6 Discussion

# Experiment 2

YCbCr uses values for the luminance, and red and blue chromaticities, which produces a different colour gamut to RGB. However, since the human eye is

more sensitive to black and white information than to changes in colour, the number of bytes used for the Cb and Cr channels can be reduced (called chroma subsampling) without any significant effect on image perception, which means its often used for data-in-motion. Some modern approaches to steganography are based on domain transformations on YCbCr images. Bits of the message can be submitted for the coefficients of the discrete cosine transform (DCT) or Discrete Wavelet Transform (DWT) of the image [4] [5].

# Part II
# Penetration Testing

# Conclusion


[1] James Stanley. How to defeat naive image steganography, 2016.

[2] 2018.

[3] Diego PH (@jdiegoph). Shooting star, 2017.

[4] Shweta Maurya and Vishal Shrivastava. An improved novel steganographic technique for rgb and ycbcr colorspace. *IOSR Journal of Computer Engineering*, 16(2):155–157, 2014.

[5] Hemalatha S, U Dinesh Acharya, and Renuka A. Comparison of secure and high capacity color image steganography techniques in rgb and ycbcr domains. *International journal of advanced Information technology*, 3(3):1–9, 2013.