University of St Andrews

CS4203 Coursework 2

Practical Security Tools

Author:
150008022

November 22, 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

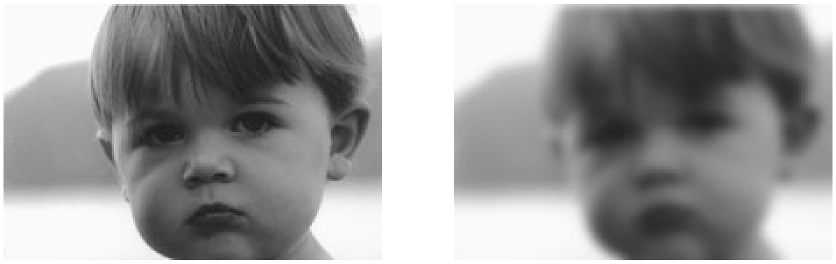
Least Significant Bit (LSB) steganography - specifically LSB1 - involves replacing the last bit of each byte of an image file (called the cover image) with a bit from the message to be hidden. For example, if each character in the message requires a single byte, then it can be hidden in 8 bytes of the 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 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

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 the stegoUI [1] program to perform the LSB.



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

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

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. Some modern approaches to steganography are based on domain transformations, such as using bits of the message as part of the coefficients after a discrete cosine transform (DCT) [3] [4].

Part II

Penetration Testing

Conclusion

[1] MPhil Yunjia Wang. stegoui. `https://github.com/YunjiaGH/stegoUI`, 2017.

[2] 2018.

[3] 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.

[4] 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.