Math 414 Final Project – Steganography

Tyler Harmon

**Introduction**

Steganography, roughly meaning “covered writing” is a method of hiding a piece of information inside of another (Lo, Topiwala, & Wang, 1998). Take, for example, a letter with a secret message hidden inside. This may simply be that the first letter in every line can be taken and turned into a comprehensible sentence, or it may follow a more complex pattern. The letter itself may be innocuous and have a coherent message without knowing the key, but the interpreted message can be completely different than the plaintext one. Steganography is not limited to a particular medium or file type, and can vary in complexity.

In this project, the goal is to hide files of various types and sizes in images using their Haar and Baubechies decompositions. Then, the reconstructed images will be compared to their original counterparts to see how the technique affects the quality of the image.

**Mathematical Background**

Steganography shares many similarities with its cousin cryptography, but there are a few differences. Primarily, the purpose of the different techniques is usually different. While steganography tries to conceal a message, cryptography focuses on security. Cryptography assumes a bad-actor can intercept whatever encrypted message is being sent and tries to keep them from recovering the actual data. From a functional perspective, cryptography typically secures data by altering the message (image, text, or other data) sent using processes that are difficult to reverse without the proper key (typically some sort of backdoor that is usable only when one has the proper signature). In contrast to this, steganography tends to leave the message relatively unchanged, but instead breaks it up and embeds the chunks of message into the medium. Both of these techniques could be used in tandem to both obscure and secure a secret message being sent.

Some steganographic techniques for hiding data within images apply data directly to the individual pixel values of the image. However, this can affect the image quite drastically. For example, if two adjacent pixels are the same color in the original image but the adjacent bits of data in the hidden file are sufficiently different, the pixels in the reconstructed image will vary. This can make a passerby or recipient who is looking at the image suspicious, especially if the original image is available for quick visual comparison.

In contrast to this pixel-by-pixel technique, the wavelet-based technique doesn’t affect pixels on an individual basis. Instead, the coefficients generated by the decomposition are altered to contain the data. Since the decomposition “smooths” the value of adjacent units, the changes caused by reconstruction after a file is hidden are dispersed over a wider region of the image.

The MRAs used in this project are the Haar and Daubechie II. The Haar decomposition has compact support and is discrete, which is fine since the digital images are pixelated anyways. This wavelet is a simple baseline to test this processing on. The Daubechie MRAs are used often in image compression and processing for their ability to approximate the image well when reconstructing. The db2 wavelet is a continuous wavelet with compact support, which makes it one of the ideal wavelets for our processing (Boggess & Narcowich, 2009).

To extend the wavelet decomposition from 1-D to 2-D, additional steps are taken. Transforms are taken horizontally (row-wise), vertically (column-wise), and diagonally across the image to create three separate transformed images, which are synthesized to get the combined coefficients for the decomposed image.

**Application**

**Results**

**References**

“Chapter 6: The Daubechies Wavelets.” A First Course in Wavelets with Fourier Analysis, by Albert Boggess and Francis J. Narcowich, Wiley-Blackwell, 2009, pp. 234–249.

Lo, Han-Yang, et al. “Wavelet Based Steganography and Watermarking.”, Cornell University, 1998, www.cs.cornell.edu/topiwala/wavelets/report.html.