TJHSST Computer Systems Lab Senior Research Project Implementation of Least Significant Bit Steganography and its Steganalysis 2009-2010

Deniz Oran

October 28, 2009

Abstract

Although steganography is an ancient form of unobtrusive and covert communications, its I mplementation has become significantly more efficient due to the advent of image storage technology and the associated amounts of space available to encode a message. An implementation of Least Significant Bit (LSB) steganographical techniques with image files to covertly encode both text and image communications will be coded in the JAVA programming l anguage. After enabling the encoding of the images, a Graphical User Interface will display the status of the operation and will enable the detection of both steganographically compromised host or carrier images and will attempt to display the communication hidden within.

Keywords: Steganography, Steganalysis, Least Significant Bit encoding, image carrier

1 Introduction - Elaboration on the problem statement, purpose, and project scope

1.1 Scope of Study

The art and science of steganography has existed since the time of the Ancient Greeks and continues to be used for secure and covert communication. The initial method of unobtrusively concealing a sent message was to shave the hair off of a servant, inscribe the desired message, wait for the hair to grow back, and then send the servant to the recipient. A method that involved writing a on a wax tablet, covering it with fresh wax, and sending it by public means to the recipient was an even more progressive and economical method of secret communication. Steganography is therefore the opposite of encryption, in which a message is made unintelligible, but openly transmitted through public means. The concealment of the fact that a message is even being transferred is the true essence of steganography. The classic struggle of covertly communicating is best illustrated through the prisoners' dilemma, in which two prisoners must exchange plans to escape without provoking the suspicion of the warden. Encryption would be an ineffective method in this situation because as soon as the warden does not comprehend the communication he immediately shuts down all forms of communication between the prisoners, thus foiling their attempt at escaping.

2 Procedures and Methodology

The JAVA programming language will be used because of it's secure and stable structure along with its popularity. The most effective and most common way of covertly encoding a message or image is by hiding it in unused portions of commonly used lossless image formats such as .GIF and .PNG. To do this, a technique called Least Significant Bit encoding is employed to edit numerous picayune parts of the image and placing parts of binary code that can be compiled by the reader to form an image or a test message. The program therefore reads the entire binary composition of the image into a matrix or two dimensional array. The least significant bits are then extracted and compiled together into a new matrix that is saved as either a new image or text message.

The second portion of the project is detecting the efficacy of the steganog-

raphy. Clearly the first test would simply be visually ensuring that the original image and the carrier appear identical. The second, and more sophisticated, method, is through statistical analysis. A program will convert the suspected image into Hexadecimal code and will analyze the tag that is associated with the image format. Another method involves analyzing the consistency of the color transitions among the pixels of the image. In addition, a commercial steganalysis program may be used to either confirm or deny the professional quality of the program.

3 Expected Results

An advanced implementation of steganography that passes at least a visual inspection will be able to be used and will not incite the suspicions of someone intercepting the message. Because of the GUI, the program will be incredibly easy to use and will display the image and what is being encoded. Then, if the decoding feature is used, it will display what is purportedly being hidden. In order to demonstrate that the program worked, the compromised image will be compared to the original. The the binary code for each will be compared and will yield the discrepancy due to the usage of steganography.