Least Significant Bit Steganography and its Steganalysis

TJHSST Computer Systems Lab, 2009-2010
By: Deniz Oran

Abstract

Although steganography is an ancient form of unobtrusive and covert communications, its implementation has become significantly more efficient due to the invention 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 language. 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.

Introduction

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 was unobtrusively concealing a sent message was to shave the hair 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 doesn't comprehend the communication he immediately shuts down all forms of communication between the prisoners, thus foiling their attempt at escaping.

Each byte is composed of eight bits or 1s and 0s

10010101 00001101 11001001 10010110
00001111 11001011 10011111 00010000

10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001

The second set of bytes represents the encoded ASCII character "G" (01000111)

Procedure

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. Above is 8 bytes of data from an image. 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. In order to detect encoding the program will convert the suspected image into hexadecimal code and will analyze the tag that is associated with the format.

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. If the decoding feature is used, it will display what is purportedly being hidden in a GUI.