Least Significant Bit Steganography and its Steganalysis

TJHSST Computer Systems Lab, 2009-2010

By: Deniz Oran

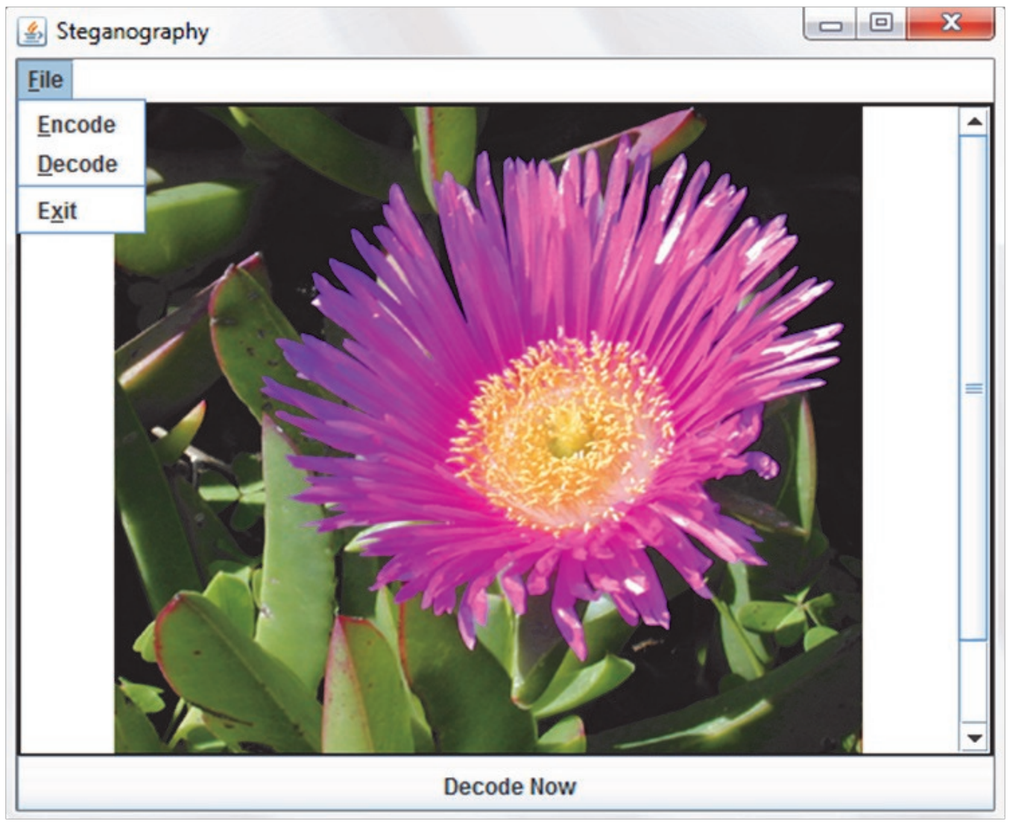
Abstract

Image Steganography has become more viable because of "noise" found in most image formats. Least Significant Bit (LSB) steganographical techniques can covertly encode a message without visibly altering an image. A program that enables encoding and extraction into an image file will be coded in conjunction with a Graphical User Interface that facilitates use.

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.

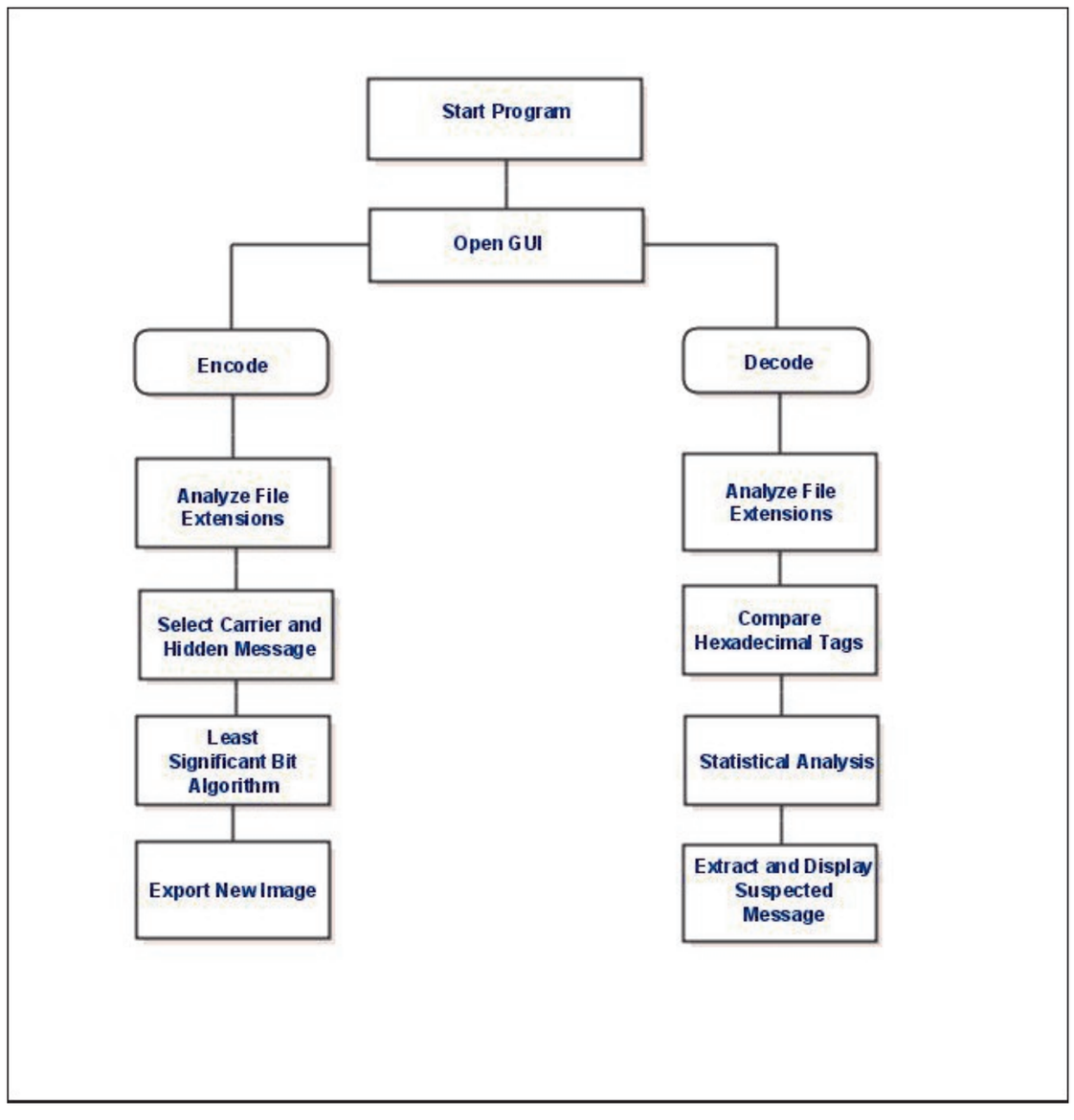
Steganography is opposite of encryption, in which a message is made unintelligible, because the message is openly transmitted through public means. The concealment of the fact that a message is even being transferred is the true essence of steganography. The classic struggle of covertly communicating 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.



Procedure

Lossless image formats are best for encoding. 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 reads the entire binary composition of the image into an array. The least significant bits are then altered and compiled together into a new matrix that is saved as a new image. 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 and will decode the message by reversing the LSB. Below are eight bytes of data from an image, the second with the letter G (01000111) encoded:

```
01110011 11100001 01101100 00111000 01100010 01011000 00100010 00101010
00001110 11000011 00000000 00000000 00001110 11000011 00000001 11000111
```



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.