Daniel Lowry Essay: Module 6

Steganography is a remarkably interesting art. Someone could literally be looking right at your data but have no clue its meaning due to how it is hidden. Steganography has become a "go-to" for many individuals with nefarious intent. There is a field that focuses specifically on detecting steganography. This field focuses on the estimation of message length, extraction, and other aspects of how steganography is implemented. This field is called Steganalysis. It has become a vital tool for law enforcement agencies and has helped to thwart many security breaches.

"There are many different methods for detecting if an image has been modified. One of the easiest ones is developed by using the idea that a camera does not use all the different colors in the nature. Cameras approximate some of the colors to a near color, so they do not need to manage a big number of different values in the color palette. For example, let us assume that we have a grey-scaled image with grey intensities from 0 to 255, it is easier to use only half of those values by rounding the odds values to the next even number." (Olguin, 2016)

There are various methods and procedures used when using steganalysis to determine if data is hidden in other data, however these can all be categorized into 3 branches. First, we look at the "Chi-square Methods". In this method a statistical test in preformed to basically make sure that the data being observed is the same as what is expected. "The Chi Square Method deals with categorical data, meaning that the data which has been accumulated is categorized. Therefore, the Chi Square Test does not work with parametric or continuous data." (2017)

The second branch would be the "Distinguishing Statistic Methods". "The steganalyst first carefully inspects the embedding algorithm and then identifies a quantity (the distinguishing

statistics) that changes predictably with the length of the embedded message. The detection philosophy is not limited to any specific type of the embedding operation and works for randomly scattered messages as well. One disadvantage of this approach is that the detection needs to be customized to each embedding paradigm and the design of proper distinguishing statistics cannot be easily automatized." (Olguin, 2016)

The final branch is "Blind Classifier Methods". In this method a detector is educated on what a standard image, one that has not been modified, looks like from various viewpoints. Next a qualified classifier is used to determine the differences between modified and unmodified images. "This methodology combined with a powerful classifier gives very impressive results." (Olguin, 2016)

Stegonography continues to grow as a method of hiding data, and steganalysis must grow with it. Steganalysts must continue to find new methods that will help to make certain that the images we are looking at are just images and nothing else is hiding just under the top layer.

References

Olguin, person_outlineJesus. “Steganalysis, the Counterpart of Steganography.” Trustwave, 22 Dec. 2016, www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/steganalysis-the-counterpart-of-steganography/.

What is Chi Square Method & How to Use it? AskOpinion. 2017 https://askopinion.com/what-is-chi-square-method.