C17 A Response to the Threat of Stegware

Li Lin, Iowa State University - Mathematics, Ames, IA 50010; Abby Martin, BA, Iowa State University, Ankeny, IA 50023; Wenhao Chen, BS, Iowa State University - Coover Hall, Ames, IA 50011; Seth H. Pierre, Ames, IA 50014; Yong Guan, PhD, Iowa State University, Ames, IA 50011; Jennifer Newman, PhD*, Iowa State University, Mathematics Department, Ames, IA 50011*

Learning Overview: The goal of this presentation is to give a survey on the performance of the most popular steganalysis tools that claim they can detect the images with secretly embedded information by stegware. Recent research papers and algorithms for the defense against stegware that may have a chance to stop the threaten from stegware before the installation will be presented.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating the current situation of steganography software (or stegware for short) and steganalysis tools for illegal purposes, such as how popular and efficient they are. This will be the first report to talk about the performance of the most recent steganalysis tools in detecting a large set of stegware. The results will provide valuable guidance to the forensic communities to develop more powerful steg analyzers.

Stegware refers to software, programs, or apps that allow insertion of malware into a digital file, such as an image or video, using steganography techniques. Although it has been in action for around 15 years, “steganography” and “stegware” have just recently attracted the attention of law enforcement agencies as the use of stegware appears to be rising.[1] This technique has been used for international economic espionage, tracking of photos shared by users on social media platforms, and industrial and governmental espionage by hacker groups using Portable Network Graphics (PNG) images to hide malicious code.[2-4]

The war between the stegware and steganalysis tools is a typical cat-and-mouse game. Although many up-to-date steganalysis tools claim their abilities to prevent steganography by utilizing the most advanced detection algorithms from the academic worlds, these tools focus mainly on one or two embedding algorithms and lack support to detect a wide range of stego objects.[5] The capability of these current tools to prevent a stegware attack has never been tested.

In this research, more than 70 stego apps and image steganography software and ten of the most popular steganalysis tools were collected. A strategy is proposed to defend real-world attacks from stegware by combining functions from online steganalysis tools and algorithms from recent academic discoveries. This is believed to significantly increase the chance of identifying the threat from stegware by identifying files that have the potential to contain malicious code. Work is occurring to develop a prototype of such a comprehensive steganalysis tool that provides user-friendly software for non-experts such as digital evidence practitioners. The characteristics of the code for many stego apps are summarized by reverse engineering and program analysis. The coding characteristics reflect their core embedding algorithms and encryption techniques, allowing the classification of the intent of the app as stegware even before installing it on a mobile phone. An automatic tool to analyze app code can detect most Android™ stego apps that implement common spatial domain and frequency domain embedding algorithms with more than 95% accuracy.

Per research, this is the first study to evaluate the performance of most recent steganalysis tools in detecting a large set of stegware. The results will provide valuable guidance to the forensic communities to develop more powerful steg analyzers.

Reference(s):

1. Stegware—The latest trend in cybercrime. *SIMARGL.* https://simargl.eu/blog/technical/stegware-the-latest-trend-in-cybercrime.
2. *Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE’s Trade Secrets*. US Department of Justice, April 2019.
3. Facebook Embeds ‘Hidden Codes’ To Track Who Sees And Shares Your Photos.*Forbes*, July 2019.
4. OceanLotus APT Uses Steganography to Shroud Payloads. *ThreatPost*, April 2019.
5. *Steganography analysis tool, an online free tool developed by McAfee.* www.mcafee.com/enterprise/en-us/downloads/free-tools/steganography.html.

Digital Image Forensics, Steganalysis, Android™ Apps