C19 A Wild Manhunt for Stego Images Created by Mobile Apps

Li Lin, Iowa State University, Department of Mathematics, Ames, IA 50010; Wenhao Chen, BS, Iowa State University, Coover Hall, Ames, IA 50011; Stephanie Reinders, BA*, Iowa State University, Dept of Mathematics, Ames, IA 50011; Yong Guan, PhD, Iowa State University, Ames, IA 50011; Min Wu, PhD, University of Maryland, Electrical & Computer Engineering Department, College Park, MD 20742; Jennifer Newman, PhD*, Iowa State University, Department of Mathematics, Ames, IA 50011*

Learning Overview: The goal of this presentation is to describe the challenge of detecting images with secretly embedded information by mobile apps. This presentation will evaluate academic algorithms and commercial software for this problem and make great progress with the proposed methods.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by increasing the realization of the situation of wide-spread usage of stego apps for illegal purposes and the possibility of detecting them. This presentation will also introduce some fast and high-accuracy tools aimed at some specific photo editing apps.

Digital image forensics is a young but maturing field, encompassing areas such as camera identification, forgery detection, and steganalysis. Steganalysis is the analysis of image data to discover if hidden content is contained within the image, and, if so, to uncover further information about the hidden content. Most of the academic research on steganalysis has focused on identifying or classifying an image as cover (innocent) or stego (with hidden content). However, large gaps exist between academic results and applications used by practicing forensic analysts.

To move academic discoveries closer to real-world implementations, it is necessary to use data that represent “in the wild” scenarios. This project looks at stego images created by mobile apps. For the past three years, research has been conducted on collecting stego images from different phones and different stego apps. One of the main contributions is a procedure for generating a large image database by using Android® emulators and reverse engineering techniques. In 2019, StegoAppDB, the first database consisting of stego images produced from mobile apps, was built and put online.[1] With the large amount of data from the StegoAppDB, for the first time, the performance of software that is designed for stego detection can be tested. Although most stego apps implement some classical embedding algorithms, none of those commercial programs have successfully detected images from apps. One main reason is that those old detection programs rely on the hidden fixed patterns, such as signatures or watermarking, for the algorithm developers, which are completely erased by the app developers.

In the December of 2019, another work was presented to discuss steg detection on images from mobile apps by using two different approaches: “signature” detection and Machine Learning (ML) methods.[2] This study analyzed Android® apps that implement steganography algorithms by applying reverse-engineering techniques to the binary code. In analyzing the code, it was determined that most algorithms used to hide the message are far from the advanced algorithms published in academic research papers. Some apps provide little security, even if a complicated embedding method was used but strangely had a unique “signature” embedded, and make the stego image and its app easily identifiable as such. Moreover, the extraction of hidden information for those app can be achieved. This study developed detection tools for all images with well-defined “signature” patterns and achieved nearly 100% accuracy. For the apps that do not have the “signature”, the study applied the ML-based detection methods to identify stego images. ML has been wildly used in the academic community. However, applying those ML algorithms to the real-world data is not trivial. First, the real-world data has more variance in exposure settings and embedding rates, which is not the typical case in the academic world. Second, an input image provided by the user is processed before the embedding step by the app, and, therefore, an input image is not necessarily the cover image in the traditional definition. This study summarized most pre-processing methods and output the post-processed images as cover images for training the classifiers. This study used instrumentation techniques to perform the non-trivial task to batch-generate cover-stego image pairs for ML steganalysis. These proposed ML methods can detect both spatial domain and JPEG domain stego images with a decent accuracy. Per research, this is the first time an ML detection algorithm was applied to identify stego images generated by mobile stego apps.

Reference(s):

1. J. Newman, L. Lin, W. Chen, S. Reinders, Y. Wang, M. Wu, Y. Guan: “StegoAppDB: A steganography apps forensics image database,” IS&T Int’l. Symp. on Electronic Imaging, Media Watermarking,Security, and Forensics 2019, Burlingame, CA, 2019.
2. W. Chen, L. Lin, M. Wu, and J. Newman: “Tackling Android Stego Apps in the Wild,” IEEE APSIPA Annual Summit and Conference, Hawaii, 2018.

Digital Image Forensics, Steganalysis, Android™ Apps

*Presenting Author