IDEA GROUP PUBLISHING

ITB13042

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos© 2006, Idea Group Inc.

Chapter IX

Basic Steganalysis Techniques for the Digital Media Forensics Examiner

Sos S. Agaian, University of Texas, USA

Benjamin M. Rodriguez, Air Force Institute of Technology, USA

Abstract

This chapter focuses on the development of digital forensic steganalysis tools/methods through analysis and evaluation of the most popular "sample pair" steganalysis techniques—the key concept in cyber crime—for the digital media forensics examiner, specializing in the analysis, identification, and interpretation of concealed digital evidence. Success and proper implementation of a digital forensic steganalysis system is dependent of several necessary steps. The basic steps are to describe and implement a new generation of steganalysis systems applicable for various embedding methods in order to allow efficient, accurate, low-cost, and fast digital forensic analysis; and to make these methods applicable for automatic detection of steganographic information within noisy network environments while striving to provide a satisfactory performance in comparison with present technology. All efforts will allow the final goal to be reached which is the development of a digital forensic steganalysis system to aid law enforcement agencies involved in the field of cyber crime investigation. The presented techniques will be based on the statistics of sample pairs (the basic unit), rather than individual samples, which are very sensitive to least significant bit embedding. Particularly, in this chapter we discuss the process and necessary considerations *inherent in the development of steganalysis methods applied for problems of reliable detection, estimation length, and localization of hidden data within various forms/ models of digital images.*

Introduction

The ever-expanding growth of digital networks, the dwindling cost of computers, CDs, DVDs, digital cameras, digital devices, and the technological efficiency of digital transmission have made digital media an increasingly popular alternative to conventional analog media. Whether expensive stand-alone equipment or the economically manufactured units commonly incorporated into wireless devices, digital media/imaging is becoming prevalent throughout the Internet and data networks. The Internet has its positive sides. It is a commonplace containing billions of bits; the difficult challenge is discovering hidden information within these bits. The negatives are that the enormous onset of various digital media also gives rise to wide-ranging opportunities for mass piracy of copyrighted material, that is, “criminal communication/transmission” of information, and a multitude of windows facilitating malicious intent of ever-expanding technology.

New technologies and new applications bring the latest threats, and force us to invent new protection mechanisms. Developing digital technologies and then adapting them to benefit from forensic analysis techniques would be an irrational and unfruitful approach. Every few years, computer security has to re-invent itself. As a result of such, there is a critical necessity in law enforcement for an assurance in the reliability of available computer forensic tools. Law enforcement is in perpetual competition with criminals in the application of digital technologies, requiring constant development of new forensic tools to systematically search digital systems for pertinent evidence.

One area of *forensic science* specializes in the analysis, identification, and interpretation of concealed digital evidence. An annual report on high technology crime (The High Technology Crime Advisory Committee) “High Technology Crime in California” http://www.ocjp.ca.gov/publications/pub_htk1.pdf lists nine common types of computer crime: criminal communications, fraud, hacking, electronic payments, gambling and pornography, harassment, intellectual property offenses, viruses, and pedophilia.

In Johnson, Duric, and Jajodia (2000) and Johnson and Jajodia (1998a) computer forensic investigations is described as the analysis and investigation of digital information. There are numerous methods used to conceal the existence of malicious data that could pose a threat to digital forensic analysts. In the realm of cyber-warfare, the analyst must consider a much broader scope of information that includes activities of investigation and analysis on attacks and intrusions of systems. The forensic activities may include analyzing audit logs, intrusion detection in the computer and communication networks, locating relevant files and data to the investigation, obtaining data from encrypted or deleted files, and possibly even recovering systems after attacks. It is not enough that the investigator possess tools and techniques for handling password-protected files, but they must also be involved in locating and recovering data hidden within seemingly