

# Chapter XIX

## Steganography and Steganalysis

**Merrill Warkentin**

*Mississippi State University, USA*

**Mark B. Schmidt**

*St. Cloud State University, USA*

**Ernest Bekkering**

*Northeastern State University, USA*

### ABSTRACT

*In the digital environment, steganography has increasingly received attention over the last decade. Steganography, which literally means “covered writing,” includes any process that conceals data or information within other data or conceals the fact that a message is being sent. Though the focus on use of steganography for criminal and terrorist purposes detracts from the potential use for legitimate purposes, the focus in this chapter is on its role as a security threat. The history of steganography as a tool for covert purposes is addressed. Recent technical innovations in computerized steganography are presented, and selected widely available steganography tools are presented. Finally, a brief discussion of the role of steganalysis is presented.*

### INTRODUCTION

In the digital environment, steganography has received increasing attention over the last decade. The steganography process conceals the fact that a message is being sent, thereby preventing an

observer from knowing that anything unusual is taking place. Neil F. Johnson of the Center for Secure Information Systems at George Mason University defines steganography as “the art of concealing the existence of information within seemingly innocuous carriers” (Johnson, 2003,

p. 2). Much of this attention has focused on the use of steganography for illegitimate purposes by terrorists and criminals, culminating in news stories about Al Qaeda's use of the technique in its communications. The extent of actual use by terrorists remains to be seen and, so far, has never been (publicly) proven. Yet, it has been suggested by government officials in the US and elsewhere that Al Qaeda and other organizations are hiding maps and photographs of terrorist targets and are also posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other Web sites.

The preoccupation with stenography as a tool for covert purposes can be explained by reviewing its history. Though the term itself is based on the Greek word for "covered writing," the term was first used in the 14<sup>th</sup> century by the German mathematician Johannes Trithemius (1606) as the title for his book *Steganographia*. On the surface, the book presents a system of angel magic, but it actually describes a highly sophisticated system of cryptography. The actual hiding of information is much older. In ancient Greece, messages might be tattooed on slaves' shaved heads and then their hair would be allowed to grow back before they were sent out as messengers. A more benign form of information hiding was inscribing messages on the wooden base of wax tablets, rather than on the surface of the wax itself (Jupitermedia Corporation, 2003). More recent forms of hiding messages were used in World War II when spies and resistance fighters used milk, fruit juice, or even urine to write invisible coded messages. Heating the source document would reveal the writing, which had turned invisible to the naked eye after the unusual form of ink had dried up. Thus, the history of steganography has long been associated with an air of secrecy, far removed from peaceful and productive purposes.

## **Steganography Today**

More technical forms of steganography have been in existence for several years. International workshops on information hiding and steganography have been held regularly since 1996 (Moulin & O'Sullivan, 2003). However, the majority of the development and use of computerized steganography has occurred since 2000 (Cole, 2003). Modern technology and connectivity have put steganographic capabilities within the reach of the average person with a computer and an Internet connection (Bartlett, 2002). Steganography does not necessarily encrypt a message, as is the case with cryptography. Instead, the goal is to conceal the fact that a message even exists in the first place (Anderson & Petitcolas, 1998). In today's fast-paced, high-tech society, people who want to send hidden messages have very efficient methods of getting a message to its destination with the use of computerized tools that encode a message in a graphic, sound, or other type of file.

## **New Practices for an Ancient Technique**

With the onset of the digital age, many new and innovative mechanisms became available for information hiding. Steganographic techniques and software focused on hiding information and messages in audiovisual files such as graphics files, sound files, and video files. Insignificant and unused parts of these files were replaced with the digital data for the hidden information. The information itself could be protected even further by use of cryptography, where the information was converted into a form incomprehensible without knowledge of the specific cryptographic technique and key. This highlights an important difference between steganography and cryp-

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/steganography-steganalysis/24110](http://www.igi-global.com/chapter/steganography-steganalysis/24110)

## Related Content

---

### Reviewing the Ethics and Philosophy Behind Social Media's Crowdsourced Panopticon

Amanda Furiasse (2022). *International Journal of Technoethics* (pp. 1-4).

[www.irma-international.org/article/reviewing-the-ethics-and-philosophy-behind-social-medias-crowdsourced-panopticon/302627](http://www.irma-international.org/article/reviewing-the-ethics-and-philosophy-behind-social-medias-crowdsourced-panopticon/302627)

### Technoethical Inquiry into Ethical Hacking at a Canadian University

Baha Abu-Shaqra and Rocci Luppigini (2016). *International Journal of Technoethics* (pp. 62-76).

[www.irma-international.org/article/technoethical-inquiry-into-ethical-hacking-at-a-canadian-university/144827](http://www.irma-international.org/article/technoethical-inquiry-into-ethical-hacking-at-a-canadian-university/144827)

### Belmont 2.0: Ethical Research Expectations for PII in AI, ML, and Data Mining/Scraping

Robin Throne and Michalina Hendon (2024). *Methodologies and Ethics for Social Sciences Research* (pp. 1-19).

[www.irma-international.org/chapter/belmont-20/337047](http://www.irma-international.org/chapter/belmont-20/337047)

### Multimedia Encryption Technology for Content Protection

Shiguo Lian (2008). *Intellectual Property Protection for Multimedia Information Technology* (pp. 70-92).

[www.irma-international.org/chapter/multimedia-encryption-technology-content-protection/24094](http://www.irma-international.org/chapter/multimedia-encryption-technology-content-protection/24094)

### The Bioethics of Digital Dystopias

Marcus Schulzke (2013). *International Journal of Technoethics* (pp. 46-57).

[www.irma-international.org/article/the-bioethics-of-digital-dystopias/90488](http://www.irma-international.org/article/the-bioethics-of-digital-dystopias/90488)