Chapter VII
Steganography

Merrill Warkentin
Mississippi State University, USA

Mark B. Schmidt
St. Cloud State University, USA

Ernst Bekkering
Northeastern State University, USA

ABSTRACT

Steganography, the process of hiding information, can be used to embed information or messages in digital files. Some uses are legitimate, such as digital watermarking or the combination of text with medical images. But the technique can also be used for criminal purposes or by terrorists to disguise communications between individuals. We discuss some commonly available steganographic tools, the detection of stegonography through steganalysis, and future challenges in this domain. In the future, the legality of steganography may depend on legal issues and challenges. Jurisdictional differences may play a role. Privacy will have to be balanced by the duty of authorities to safeguard public safety, both from threats by criminals and terrorists. Techniques for steganalysis will become increasingly important, and will be complicated by the use of the Internet and emerging technologies such as VOIP. Packet routing complicates analysis of files, and new data streams offer new opportunities for hiding information. An internationally coordinated response to threats may be necessary.

INTRODUCTION

Steganography is the process of hiding information. In the digital environment, steganography (which literally means "covered writing") involves hiding data or messages within files, so that the files, which might appear to be legitimate, would be ignored by authorities. Steganography has been practiced since the times of ancient Greece. Ancient steganographic methods where simple yet effective; for example, a

message in a wooden tablet was covered with wax thereby hiding the message. Another method was to shave a messenger's head, tattoo a message on his scalp, and let the hair grow back only to shave it again when the messenger arrived at his destination (Jupitermedia Corporation, 2003). More technical forms of steganography have been in existence for several years. In fact, 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). 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), so that anyone intercepting and viewing the file (image, document, e-mail, etc.) would not be readily aware of the hidden bits. Modern technologies have enabled the embedding of hidden messages efficiently and easily. These computerized tools encode the message, and then hide it within another file.

BACKGROUND: LEGITIMATE USE OF STEGANOGRAPHY

There are several useful applications for steganography. Much like "watermarks" and embossing have been used for many years to identify banknotes or other important documents, "digital watermarks" can be introduced into files to identify the ownership of the digital content, such as an image or music file. This tool for preserving intellectual property rights (copyright, trademark, etc.) enhances the ability of the creator to safely distribute his or her work without fear of copyright infringement (Nikolaidis & Pitas, 1996). It also enables legitimate monitoring of the use of such files. Intelligent software agents ("bots") can be used to search the Web for files (JPG-image files, for example), which might encompass the embedded string of ownership information (the digital watermark). In this way, for example, a journalist or artist might ensure that their digital signature (typically a unique serial number used as a virtual "fingerprint") is found only in images displayed on Web pages that have licensed their use and not for unauthorized uses (Moulin & O'Sullivan, 2003).

Another use of steganography involves sending a secret message (Anderson & Petitcolas, 1998). Other uses include hiding messages in radio advertisements to verify that they are run as contracted, embedding comments in a file, embedding a patient's name in medical image data, and embedding multilingual soundtracks in pay-per-view television programs (Anderson & Petitcolas, 1998; Moulin & O'Sullivan, 2003). Embedded digital watermarks also have been used to identify copyrighted software (Hachez, 2003) and to prevent music and video files from being illegally copied.

RISKS POSED BY STEGANOGRAPHY

Though most individuals generally utilize the benefits of modern technology to increase productivity or for other positive outcomes, other individuals will use technology for detrimental activities, such as cyber theft and the planning of terrorist attacks. One need look no further than Osama bin Laden and his terrorist network, Al Qaeda, to see evidence of the latter. U.S. intelligence has evidence that Al Qaeda uses the Web to conduct operations (Cohen, 2001). Known examples include Mohamed Atta making airline reservations on Americanairlines.com, members using Yahoo e-mail, and members using the Web to research crop dusters in an effort to determine how effective they could be in chemical attacks. A more recent example concerns the use of steganography by a radical Muslim infiltrator of the Dutch Intelligence Service (Reporter, 2004). Similarly, steganography has been used for criminal purposes. An extortionist in The Netherlands demanded that the victim, a food producer, hide information regarding a bank account with the ransom in a picture placed on the Web site of a major newspaper (Ringelestijn, 2004).