

2008


Steganography: Forensic, Security, and Legal Issues

Merrill Warkentin
Mississippi State University

Ernst Bekkering
Northeastern State University

Mark B. Schmidt
St. Cloud State University

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Warkentin, Merrill; Bekkering, Ernst; and Schmidt, Mark B. (2008) "Steganography: Forensic, Security, and Legal Issues," *Journal of Digital Forensics, Security and Law*. Vol. 3 : No. 2 , Article 2.

DOI: <https://doi.org/10.15394/jdfsl.2008.1039>

Available at: <https://commons.erau.edu/jdfsl/vol3/iss2/2>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



Steganography: Forensic, Security, and Legal Issues

Merrill Warkentin

Mississippi State University
m.warkentin@msstate.edu

Ernst Bekkering

Northeastern State University
bekkerin@nsuok.edu

Mark B. Schmidt

St. Cloud State University
mbschmidt@stcloudstate.edu

ABSTRACT

Steganography has long been regarded as a tool used for illicit and destructive purposes such as crime and warfare. Currently, digital tools are widely available to ordinary computer users also. Steganography software allows both illicit and legitimate users to hide messages so that they will not be detected in transit. This article provides a brief history of steganography, discusses the current status in the computer age, and relates this to forensic, security, and legal issues. The paper concludes with recommendations for digital forensics investigators, IT staff, individual users, and other stakeholders.

Keywords: steganography, data hiding, information hiding, digital forensics, computer law, computer security, steganalysis, privacy

1. INTRODUCTION

Steganography is the process of hiding information. In the digital realm, steganography (which literally means “covered writing”), involves hiding data or messages in digital files. The files themselves may appear to be innocuous, and would be ignored by a casual observer or even by authorities. The field of information hiding has grown sufficiently in recent years. Evidence of this growth can be seen at workshops on information hiding, and in occasional reports of use by criminals and terrorists appear in the popular press. In contrast to cryptography where the message is encoded, the purpose of steganography is to hide the fact that a message is being sent. Once encoded, a cryptographically altered message typically appears unrecognizable and would raise suspicions. The primary advantage of steganography over cryptography is that the “coverttext” (apparent messages) do not attract attention to themselves, to messengers, or to recipients.

Modern information technology enables novice computer users to hide, transmit, and unhide steganographic messages without special expertise. (Warkentin, et al, 2006) The remainder of this paper is organized as follows: A brief history (Section 2) is followed by an introduction to steganography (3), with contrasts to encryption, and an introduction to steganalysis (4). The following three sections focus on forensics issues (5), security issues (6), and legal issues (7). Section 8 has conclusions and recommendations for researchers and practitioners.

2. BRIEF HISTORY

2.1 Ancient Greece and Rome

Steganography has a long history, going back to the ancient Greek and Roman civilizations. Herodotus, the Greek historian, reports how king Darius shaved the head of a prisoner and wrote a secret message on his scalp. After the hair grew back, the prisoner was sent to the king's son-in-law Aristogoras in Miletus and effectively delivering the message undetected by the enemy. A less time-consuming method of delivering secret messages was used by a soldier named Demeratus who needed to send a message to Sparta that king Xerxes planned to invade Greece. Demeratus removed the wax from a writing tablet, wrote the message on the underlying wood, and re-applied the wax. Both examples explain why the word steganography is based on the Greek word for "covered writing" (steganos = unseen or hidden; graphia = writing): protection of the message is assured not through making the message undecipherable, but by hiding the existence of the message altogether. Sending undecipherable messages is the technique of cryptography (kryptos = hidden or secret), and both techniques are often used in conjunction. The Romans accomplished the goal of sending messages undetected by writing between the lines of innocuous documents with invisible ink made from fluids like milk, urine and fruit juices. When the document was heated, the invisible ink would darken and become visible.

2.2 Middle Ages

At the end of the Middle Ages, two authors produced seminal works on steganography. Johannes Trithemius (1462-1526) wrote the three volumes of *Steganographia* (ca. 1499) which superficially describe black magic, specifically using spirits to communicate over long distances. However, by deciphering the text with a simple substitution method, one can read treatises on both cryptography and steganography. More than a century later, Gaspari Schotti picked up where Trithemius left off and published *Steganographia* (1665), which focuses on techniques with text, invisible inks, and incorporating hidden messages in music.

2.3 More Recent History

In the mid 19th century, a global technology revolution dramatically altered information transmission speed so that what took days or weeks to convey (at the speed of ships and horses) could be achieved in minutes with the new telegraph. Almost immediately, businesses and individuals sought to conceal their true

message from telegraph operators, especially when the messages might be sensitive or might convey strategic business information. Some messages were simply enciphered, but others were creatively disguised using various steganographic schemes to prevent telegraph operators from becoming suspicious. (Standage, 1999)

In the late 19th century, Lord Baden-Powell was employed as a scout by the British army. To hide his drawings of positions of Boer artillery bases, he hid maps in drawings of butterflies. Certain markings on the wings of the butterflies were actually enemy installation positions. Thus, he would not be suspected even if he were caught. Hiding messages was further perfected by the German invention of the microdot, where photographs the size of printed periods contain images of standard size pages. FBI Director J. Edgar Hoover labeled this as “the enemy’s masterpiece of espionage.” Other advancements during World War I included the advent of null ciphers, where unencrypted messages about ordinary events contain hidden messages. For instance, the following message sent by the German embassy in Washington, DC, to their headquarters in Berlin “Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils” can be decoded by taking the second letter of each word, and results in “Pershing sails from NY June 1”. (Kahn, 1996) As evidenced by comparing the message sizes, this technique was relatively inefficient. Additionally, some of these messages are nonsensical, and therefore may raise suspicions.

2.4 Computer Age

The advent of the digital computer has introduced new opportunities for hiding messages, but also new challenges for forensic investigation. International workshops on information hiding and steganography have been held regularly since 1996 (Moulin and O’Sullivan, 2003), however, the majority of development and use of computerized steganography has occurred since 2000 (Cole, 2003). The use of steganography is now well within the reach of an average person with a computer and an Internet connection (Bartlett, 2003), and the most recent development is the potential use of steganography in Internet Telephony systems such as Skype (Mazurczyk and Szczypiorski, 2008).

3. DIGITAL STEGANOGRAPHY

3.1 Definitions

In the modern computer age, technology has enabled the embedding of hidden messages efficiently and easily. Computerized tools encode the message and hide it within another file. Johnson (2008) defines steganography as “the art of concealing the existence of information within seemingly innocuous carriers” and adds that “an encrypted message may draw suspicion while a hidden message will not.” Thus, the goal is to conceal that the fact that the message even exists in the first place (Anderson and Petitcolas, 1998), so that anyone intercepting and

viewing the file (image, document, e-mail, etc.) would not be readily aware of the hidden bits. In the 1996 Information Hiding Workshop in Cambridge (Pfitzmann, 1996), the following terminology in steganography was defined. The embedded data is the information to be hidden in the cover, the original, innocent file such as an image, audio, text, or video. The process itself is labeled embedding, and the cover and embedded data together form the stego data.

As mentioned earlier, both steganography and cryptography intend to hide information. Steganography hides the existence of the message, cryptography makes the message impossible to understand for outsiders, and both are often used together. Whereas cryptographic messages by themselves are easily identifiable by their random and unintelligible appearance, steganography messages appear to be normal at first sight. The combined use of steganography and cryptography can effectively provide a message sender two levels of protection.

Another related technology is watermarking, where digital files are visibly or invisibly marked with embedded information. For the sake of completeness, we will briefly discuss some cryptographic definitions and principles as they relate to steganography, compare steganography and watermarking, and focus the remainder of the paper only on steganography and related issues.

The classical principles of cryptography were defined by the Dutch linguist Auguste Kerckhoff (1883) as:

- the system should be, if not theoretically unbreakable, unbreakable in practice,
- the design of a system should not require secrecy,
- compromise of the system should not inconvenience the correspondents,
- the key should be memorable without notes and should be easily changeable,
- the cryptograms should be transmittable by telegraph,
- the apparatus or documents should be portable and operable by a single person, and
- the system should be easy, theater requiring knowledge of a long list of rules nor involving mental strain.

Clearly, some of these principles still apply today. Like steganography, cryptography has significantly improved both in use and in decryption since the advent of the modern computer. Ciphers are more complex, and any type of data can be converted in binary format. Separately and in combination, the techniques have been of great interest to the intelligence and law enforcement communities. We will address some of these issues in a later section.

In watermarking, the object of the communication is not in the embedded message but in the carrier itself. The watermark only serves to uniquely identify the carrier. This can be overt as a deterrent to digital copying, or hidden as proof of ownership and origin. Television broadcast companies routinely include a visible watermark in their programming, and copyright protection systems use invisible watermarks. This indicates the need for inseparability of watermark and carrier, since removal of the (visible or invisible) watermark destroys the deterrence to copying and proof of ownership. A special problem for both steganography and watermarking is the conversion of digital files to different formats or with different compression levels. Both can affect the embedded information, and the technology needs to be robust against this type of attack and signal modification. For example, only lossless compression algorithms (e.g. GIF, not JPEG) are appropriate for steganographic concealment, because the embedded data may become altered otherwise. Certain transmission protocols may also compress the signal in ways that could compromise the ability to discover the embedded data by the recipient. Finally, whereas steganographic content can lose significance when information becomes outdated or stale, watermarks retain their significance indefinitely. A brief comparison of the three technologies is included as Table 1.

Table 1: Comparison of Steganography, Cryptography, and Watermarking

Technique	Purpose	Comments
Steganography	Hiding existence of digital content from outsiders	Content generally of limited time value. Needs carrier file
Cryptography	Rendering the digital content inaccessible to outsiders	Content generally of limited time value. No need for carrier file
Watermarking	Protection of digital content of carrier	May or may not be readily detectable. Durability is essential

For the purposes of this paper, the remainder of the discussion will focus only on steganography.

3.2 Types of Steganography

The hidden content of stego messages can be embedded in the carrier file by three types of methods. The stego message can be injected inside the carrier, which does not alter the digital content of the carrier itself. Alternatively, part of the digital carrier content can be substituted with the stego message. The latter does change the digital content of the carrier. A relatively new method of hiding content is to use the stego message to generate a completely new file. Examples of each method

may serve to clarify how each can be used, or is used, in practice.

3.2.1 Injection Techniques

Hiding information in existing files routinely occurs in common computer applications. Properties of Microsoft Office documents are automatically recorded with information specified – perhaps years earlier – when the Office application was installed. The Author property is automatically culled from the User Information entry under the Tools/Options menu. Complete safe removal requires a special tool (<http://office.microsoft.com/en-us/help/HA011400341033.aspx>). Information Systems conferences and journals now routinely instruct authors how to remove identifying information in order not to compromise the blind review process. More intentionally, information can be invisibly hidden in Web pages by using the “hidden” tag. The regular view of the webpage does not show the content, but the source view reveals the `<input type="hidden">` tag. Other examples include storing data in unused space in file headers, data packets sent over networks, and unused disk space (Johnson et al, 2001). Using open space without any alteration to the carrier file is very limited in capacity, however. Therefore, more modern and secure techniques involve some level of modification of the carrier file.

3.2.2 Substitution Techniques

In substitution techniques, a limited amount of data of the carrier file is replaced with the coded representation of the hidden message. In techniques involving the Least Significant Bit (LSB), the binary representation of each picture element (pixel) in a graphic file is changed to encode the hidden message. This is done such that the effect on the visual image is negligible. Consider the following color encoding:

```
10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011
```

The LSB algorithm can hide the following nine bits 101101101 by changing the last bit in each octet as needed. This results in

```
10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011
```

This example demonstrates that to hide nine bits of information, the algorithm only needs to change four of the nine least significant bits in these nine bytes. Because changing the last bit causes an extremely small change in the color of a pixel, the change in the graphic is imperceptible to the human eye. For a more detailed description of this process, the reader can visit: <http://www.garykessler.net/library/steganography.html>. More complex algorithms

include Discrete Cosine Transformation (DCT), Fourier transformations, and the Patchwork Method of Bender. In audio files, techniques for information hiding include replacing the phases of short segments imperceptibly with reference phases representing the hidden data (phase coding), spreading a narrow band signal of the message over a wide spectrum of frequencies making it appear as random noise (spread spectrum encoding), dividing the bandwidth of the carrier into multiple channels and hopping between these channels (frequency hopping), and many others.

3.2.3 File Creation

Finally, the stego message can be used to generate a completely new, innocent-looking file. In essence, the message creates its own carrier. An example of this technique is the application SpamMimic (<http://spammimic.com/>). Using SpamMimic, a short message can easily be hiding in text that appears to be spam. This message then can be send to someone who would then use the website to decode the message. An advantage of this is that few people would be suspicious of spam messages. The technique is relatively inefficient, as evidenced by the conversion of the three words “steganography is interesting” to text with a word count of 574. Full sentences easily balloon to emails with thousands of words. However, given the advantages of such a method, the word count may be of little consequence.

3.3 Steganography Encryption Levels

Techniques of steganography can also be distinguished by the level of encryption. The least secure level, which does not require the exchange of a cipher such as a stego key, is pure steganography. Effectiveness of keeping the stego message secure relies only on the ability of the message to remain undetected. Using a secret stego key prior to communication makes the message more secure, but can also raise suspicions because exchange of the secret stego key must precede the transmission of the carrier with the stego message. Consequently, there is a trade-off between probability of detection on one hand, and the security of the embedded message if detected. The most secure technique uses a private and a public key to secure the message embedded in the carrier. The stego message is embedded with the use of a public key, and the message extracted with a private key. As in public key encryption, there is no need to exchange keys and therefore the risk of detection is not increased. It must also be emphasized that the keys in secret key steganography and public key steganography only serve to augment the execution of the steganography application, and do not constitute the use of encryption.

A summary of steganography techniques is included as Table 2.

Table 2: Steganography Techniques

Technique	Method	Effect on carrier file	Comments
Injection techniques	Using built-in information recording tools or “open” file space	No change of content	Very limited hiding capacity
Substitution techniques	Part of digital content of carrier file changed to reflect stego message	Some degradation of content quality	Increased risk of detection with increasing volume of stego content
File creation	Stego message hidden in larger amount of new, irrelevant digital content	None- new carrier file created	Inefficient, detection risk highly dependent on context of message
Stego encryption	Stego content is encrypted as it is included in carrier file	None beyond pure steganography	Key exchange increases risk detection

3.4 File types

Finally, steganography can use different types of files. Until recently, mostly audiovisual files were used as carrier files for inclusion of stego content. These files are generally large and have a large image hiding capacity. For instance, the color of a pixel in an icon can be changed imperceptibly by minimally changing the digital color code (e.g. from 01011011 01010011 01011001 to 01011010 01010011 01011001), whereas changing a single character in the word 'fat' to 'bat' is not only noticeable, but also changes the entire meaning of the word. Incidentally, both are represented by three bytes. As steganography is increasingly seen as a useful business tool, other file types are now being used as cover files. An example is the use of steganography for placing identifiers in database relationships (Agrawal et al, 2003).

4. STEGANALYSIS: DETECTION OF STEGANOGRAPHY:

4.1 Steganalysis

Just as digital technology can be used to hide messages, can it be used to detect and decode stego messages. Steganalysis is the process of hunting for small deviations in the expected patterns of a file (Cohen, 2001), so that the presence of hidden messages can be detected. Steganalysis and steganography are two sides of the same coin, similar to cryptography and cryptanalysis, and computer viruses and

antivirus software. Research in steganography involves both developing new techniques for hiding content and developing new tools for detection and deciphering of hidden content. This duality is similar to biologic warfare, where development of new biological weapons goes hand in hand with research of their antidotes.

4.2 Types of Steganalysis

Based on knowledge of the actual message, availability of the original cover file, steganography tool, the following types of steganalysis can be distinguished (Petitcolas, 2000):

- Stego only attack - only the stego object is available for analysis;
- Known cover attack - the cover and the stego object are both available;
- Known message attack - the message is known and can be compared with the stego object;
- Chosen stego attack - the stego object and the stego tool (algorithm) are available for analysis;
- Chosen message attack - choose a regular message, convert to stego message for further analysis;
- Known stego attack - the stego message, the stego tool (algorithm), and the cover message are all available for analysis.

In general, steganalysis becomes more efficient and effective as more elements are known. A further level of complexity is introduced as steganalysis moves from detection only, to detection and deciphering of the stego message.

4.3 Detection Vectors

Detection of steganography can be based on comparisons of the stego file and the original file, detection of files having larger than expected file sizes, and variation in statistical properties of the digital information in the files. Original files are often not available, unless they come from public sources. However, many steganography techniques increase the size of the digital carrier file, to the point that it becomes statistically significant. Moreover, as the structure of the stego message is superimposed on the digital carrier data, analysis of distribution of known properties often reveals the presence of the hidden message. For instance, bitmap files with more than 50 near-identical colors should be suspected of containing hidden messages (Petitcolas, 2000).

4.4 Destruction vs. Deciphering

Finally, deciphering of stego messages is not always necessary. If the hidden message can be destroyed before it reaches its destination, the attempt at hidden communication has effectively been thwarted. Graphical files can be altered by

changing file formats, compression algorithms, and compression levels, usually without noticeable visible impact on the integrity of the carrier file.

In summary, the detection and deciphering of steganographic content is complicated and has many challenges. Nevertheless, it is a subject that the security and legal communities cannot ignore.

5. DIGITAL FORENSICS ISSUES

5.1 Digital Forensics

Digital forensics focuses on the preservation and analysis of digital evidence. As defined in Palmer (2008), digital forensics are “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.” As steganography becomes more widely available and the amount of data on local machines and Internet increases, the issue of detection of the use of steganography by digital forensics personnel becomes increasingly important. In theory, this should be evaluated in any type of case involving computer use. In practice, most cases will involve audiovisual files, such as in child pornography. However, cases of industrial espionage and fraud could be encountered.

5.2 Approaches in Forensic Steganalysis

Digital Forensic experts employ many techniques, and we will limit the discussion to those applicable to steganography and steganalysis.

5.2.1 Detection of software

In some cases, steganography software itself may be discovered on computer equipment under investigation. The Steganography Application Fingerprint Database (SAFDB) currently contains identifying information on 625 applications associated with steganography, watermarking, and other data-hiding applications (Backbone Security, 2008a). Similarly, the National Institute of Standards and Technology (NIST) maintains a list of digital signatures in the National Software Reference Library, some of which are for steganography software. Even when software has been removed, traces can sometimes be found in places like the Windows registry or in system backup files. When steganography software installation has been identified, malicious intent should be assumed until proven otherwise.

5.2.2 Detecting pairs of carrier files and stego files

In addition to detecting the software used for steganography, digital forensics experts can detect files with similar visual properties but different file sizes, hash values, and statistical properties. If files have been deleted, they may be retrieved from the Recycle Bin or similar Trash container, or even reconstructed with special

forensics tools for file recovery.

5.2.3 Using Keywords

An additional method of detection uses a list of keywords to search for file names and content in program files and data files. The list should be specific with regard to steganography. For instance, the search term “steg*” can be used to identify steganography. The effectiveness and efficiency in detection, while preventing false positives and false negatives, depends on the quality of the keyword dictionary.

5.2.4 Specialized Steganalysis Software

In the past, most steganography detection tools targeted specific applications – frequently the same applications used for steganography. More recent software claims to detect stego files created with a wide variety of programs. One of these is Stegdetect 0.6, which uses linear discriminant analysis to locate probable images with hidden content by comparing them with a set of normal images (Provos, 2008). A second common tool is Stego Suite (Wetstone Technologies, 2008), which combines increasingly intense levels of detection with content cracking tools. The third example is the recent release of StegAnalyzerAS (Backbone Security, 2008b), which uses the values stored in the SAFDB to identify potential stego files. A comprehensive list of steganography tools is maintained at <http://www.jjtc.com/Steganography/tools.html>.

5.2.5 Physical crime scene investigation

Finally, physical crime scene investigation can reveal useful information. Passwords used for steganography tools can be written on notes stuck under keyboards, and environmental objects can generate clues about potential passwords.

6. DIGITAL SECURITY ISSUES

Though steganography tools may be used for legitimate business applications such as protecting strategic corporate information during transmission (Schmidt et al, 2004), they have emerged as a significant issue to forensic investigators and others who are concerned with malicious and illegal uses. As steganography tools become more widely available and easier to use, protection against malicious use demands attention, and the balance between protection from illicit use and interference with legitimate use emerges as a new challenge. In this section, we will focus on protection against malicious use, and not discuss specific potential business applications such as watermarking for protection of intellectual property (discussed above).

6.1 Prevention of Malicious Use

Organizations fight a continuous battle for control over the user desktop. Employees install unapproved applications such as Instant Messaging clients, screen savers, and peer-to-peer software if given the opportunity. Likewise,

employees could install steganography software from repositories such as JTTC.com (Johnson, 2008). The first lines of defense against these practices are – as for any unapproved software – company policies and limiting user permissions. Acceptable use policies should explicitly exclude steganography software, since users could argue that it does not fall under banned software due to some legitimate uses.

6.2 Detection of Unauthorized Steganography Software

Unfortunately, not all employees abide by company policy and some are able to circumvent restricted user permissions. The following measures should be considered:

- Use of network intrusion software to detect abnormal movement of graphics files. Most business practices do not involve a high level of graphics file use, and most traffic will be incoming as a result of web surfing. Outgoing graphics files, whether in isolation or as email attachments, should be scanned.
- Since stego files will not be detected unless they are sought, automatic scanning of networked computers should be considered. This can be done with a variety of commercial steganalysis software.
- Finally, computers brought in for maintenance or repair should be routinely scanned for steganography as well as computer viruses and malware.

Together, these measures will contribute to active identification of illicit steganography use in the enterprise.

6.3 Steganography as an Organizational Priority

Steganography is but one threat to the security of the enterprise. As with other security threats (e.g., computer viruses and network intrusion), prevention and allocation of resources will depend on the perceived relative importance of the threat. Wingate (2007) describes four typical stakeholder responses:

- unaware of the threat. Steganography is typically confused with shorthand writing (stenography).
- denial of the threat. Even some experts fall in this category, as evidenced by the statement made by Neils Provos to the press: “Steganography becomes the focus of attention, dies down, and then the public is all over it again, ... But it will never be pervasive, because the amount of data you can actually hide in the images is fairly small. And if someone wanted to steal intellectual property, it’d be easier to copy the data on a disk and carry it out in your pocket.” (Radcliff, 2002).

- resignation. Stakeholders typically state that nothing can be done about steganography due to a lack of good tools for detection and information extraction.
- perception of steganography as a legitimate threat. Wingate (2007) falls in this category: “A comprehensive enterprise security program should include countermeasures to the threat posed by insider use of steganography. The first step is to acknowledge the threat exists by developing and implementing policy to prohibit users from having steganography applications on their workstations. Finally, both passive and active detection tools and techniques should be employed to enforce the ‘no steg policy.’”

Users are encouraged to form their own opinion about the relevance and extent of the threat of steganography.

7. LEGAL ISSUES AND CHALLENGES

Laws involving technology are difficult to enact and even more difficult to enforce in the Internet age. Many Internet communications cross state lines and international borders, which creates the issue of jurisdiction. What may be illegal in one jurisdiction may be legal in another. In 1952, the United States enacted Section 1343 of the Federal Criminal Code. It included a wire fraud provision, which was later extended to encompass the Internet. Using any part of the telecommunications system in a criminal act is now a federal offense (Cole, 2003).

Court orders must be obtained from a judge to monitor phone conversations, but the order applies to a specific phone number only. Criminals can easily bypass this by using disposable cell phones (Charny, 2003). Other new technologies, such as the voice over Internet protocol (VoIP), pose new challenges. Internet Telephony breaks phone conversations into data packets, sends them over the Internet, and reassembles them at the destination. To monitor this traffic, a few central locations would have to be set up where voice streams could be diverted and then be copied before resending them to the intended destination (Wired News, 2003). It would be much more effective to monitor right after the starting point when packets are not separated over different routes or right before the destination, when all packets follow a single path.

7.1 Privacy vs. Security

A delicate balance exists between loss of personal privacy and the greater good of society. Groups like the American Civil Liberties Union (ACLU) are opposing law enforcement monitoring of communications. The ACLU’s position on privacy and technology is that the United States is at risk of becoming a surveillance society. Two concurrent developments form the basis for this trend (American Civil Liberties Union, 2003):

- The tremendous explosion in surveillance-enabling technologies. George Orwell's vision of 'Big Brother' has now become technologically possible.
- Even as this technological surveillance monster grows in our midst, we are [weakening] the legal restraints that keep it from trampling our privacy.

Another problem is the risk of unintended consequences of any new legislation. For example, a Michigan state law enacted March 31, 2003, based on the Digital Millennium Copyright Act (DMCA) and originally intended to protect cable TV operators and broadband providers, contained the provision "A person shall not assemble, develop, manufacture, possess, deliver, or use any type telecommunications access device by doing, but not limited to, any of the following: ... (b) Conceal the existence or place of origin or destination of any telecommunications service" (Act 328 of 1931, 2004). The law had to be amended in 2004 because in its original form, the legitimate use of technologies, such as steganography, was clearly prohibited. Likewise, some information gathered by authorities could be used for illegitimate purposes.

Recently, the U.S. government has tried to gain more access to communications and restrict the use of encryption technology. Similar to the Communications Assistance for Law Enforcement Act of 1994 (CALEA) in the United States, the European Parliament implemented the Communications Data Protection Directive in 2003. European member states can order telecommunications companies to store all electronic communications, including phone calls, e-mails, and Internet use, for indefinite periods. In general though, the European Union is more permissive with regard to specific technologies to hide data. Neither the United States nor the European Union has enacted laws restricting the use of steganography specifically, and it is unlikely that legal restrictions on the use of steganography will be implemented. Laws restricting the use of cryptography have existed for years (Koops, 2007), while legal limits on the use of steganography have yet to be implemented. Moreover, the potential thwarting of criminal activities may not outweigh the loss of privacy.

7.2 International Travel

Finally, though steganography may not be illegal, even the possession could be cause for alarm in some parts of the world. International travelers, including business travelers, should realize that unhidden coded messages, no matter how unbreakable, will arouse suspicion and may in themselves be incriminating in countries where encryption is illegal. If hidden digital messages would be found, the owner of the equipment could be in similar legal trouble abroad. The possession and use of steganography should therefore be considered very carefully.

8. CONCLUSIONS AND RECOMMENDATIONS

Steganography has a long history of both legitimate and illicit uses (Schmidt et al, 2004). With rapid development and improvements of information technology, the potential for use and abuse will continue to increase. Some legitimate uses exist, but the focus has been predominantly on detection of abuse and illicit use.

Legal restrictions are difficult to enforce, therefore Information Technology (IT) staff charged with organizational security should act proactively by seeking management support to limit or banish use of steganography that has no distinct organizational benefit. The specifics of the limitations should be incorporated as an integral part of the organizational policies and procedures, and should be actively enforced. If a ban on all steganographic software is not possible or desirable, specific exceptions of applications, individuals, and/or job categories allowed to use the software should be explicitly specified. To foster active prevention, managers must establish organizational policies which discourage or ban the use of steganography. Furthermore, these policies must be instantiated with specific procedures and guidelines that are communicated to all employees and other stakeholders during initial and ongoing routine Security Awareness, Training, and Education (SATA) programs. Compliance with these policies and procedures must be actively enforced as part of the organizational IT governance mechanisms. Networked computers can be actively scanned for steganographic software, similar to scanning for computer malware infections and scanning for proper software versions and patches. Network traffic can be scanned as it enters and leaves the organizational network boundaries, similar to scanning for email security threats. Finally, Technical Support staff can be instructed in identification of banned software, as well as the proper organizational procedures when it is found.

In cases of steganography uses in crimes or organizational espionage, where law enforcement investigators or organizational IT staff members (respectively) may lack the specific expertise, managers should consider bringing in the expertise of digital forensics professionals. Recommendations for specific steganalysis tools are likely to become rapidly stale as technology progresses, but a good starting point for selecting the proper tools could be to start with the major commercial steganalysis vendors in combination with the information in the Steganography Application Fingerprint Database and the National Software Reference Library. Together, these sources would provide optimal capability to detect and possibly decipher steganographic content. In any case, law enforcement and IT staff should consider that steganography may have advanced too far to be handled by non-security specialists, and that the specialized services of digital forensics professionals may be needed.

Finally, individual users should consider that the steganography technology has advanced well beyond the use by amateur enthusiasts, and that the mere

presence of steganographic software on their computers could have serious professional and private ramifications. Users should be aware of and stay within the restrictions of corporate policies and procedures, as well as legal limitations on possession and use of steganography software. When traveling abroad with steg software installed, the legal limitations of destination countries should be investigated.

Steganography also presents new challenges for digital forensic investigators, security personnel, enterprise managers, law enforcement officials, courts, and lawmakers. It will add to the complexity and quantity of the digital forensic workload, security measures, and development of case law. Future research of steganography and steganalysis should be encouraged for both academics and practitioners.

REFERENCES

- Act 328 of 1931, Michigan Penal Code. §750.540c (2004).
- Agrawal, R., Haas, P., and Kiernan, J. (2003). 'Watermarking Relational Data: Framework, Algorithms and Analysis', *The International Journal on Very Large Databases*, 12(2):157-159.
- American Civil Liberties Union. (2003). 'Privacy and Technology', <http://www.aclu.org/Privacy/PrivacyMain.cfm>, October 29.
- Anderson, R. J., and Petitcolas, F. A. P. (1998). 'On the limits of Steganography', *IEEE Journal on Selected Areas in Communications*, 16(4): 474-481.
- Backbone Security (2008a). 'Steganography Application Fingerprint Database', <http://www.sarc-wv.com/docs/safdb.pdf>, June 20.
- Backbone Security (2008b). 'Steganography Analyzer Artifact Scanner', <http://www.sarc-wv.com/docs/stegalyzeras.pdf>, June 25.
- Bartlett, J. (2003). 'The ease of steganography and camouflage', <http://www.sans.org/rr/paper.php?id=762>, October 29.
- Charny, B. (2003). 'Disposable cell phones spur debates', http://news.com./2102-1033_3-273084.html?tag=st_util_print, October 15.
- Cohen, A. (2001). 'When Terror Hides Online', *Time*, November 12.
- Cole, E. (2003). 'Hiding in plain sight: Steganography and the art of covert communication', Wiley Publishing, Inc., Indianapolis.
- Johnson, N. (2008). 'Steganography', <http://www.jjtc.com/stegdoc/steg1995.html>, June 25.
- Johnson, N. (2008). 'Steganography Software', <http://www.jjtc.com/Steganography/tools.html>, June 25.

- Johnson, N., Duric, Z., Jajodia, S. (2001) 'Information Hiding, and Watermarking - Attacks and Countermeasures', Kluwer.
- Kahn, D. (1996). Codebreakers: The Story of Secret Writing. Revised ed. Scribner, New York. Kerckhoff, A. (1883). 'La Cryptographie Militaire', Journal des Sciences Militaires.
- Koops, B-J. (2008). 'Summary of International Crypto Controls', <http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm>, June 25.
- Mazurczyk, W. and Szczypiorski, K.(2008) 'Steganography of VOIP Streams', <http://arxiv.org/ftp/arxiv/papers/0805/0805.2938.pdf>, June 25.
- Moulin, P., and O'Sullivan, J. A. (2003). 'Information-theoretic analysis of information hiding', IEEE Transactions on Information Theory, 49(3): 563-593.
- Palmer, G. (2008). 'A Road Map for Digital Forensic Research. Report from the First Digital Forensic Research Workshop', <http://www.dfrws.org/2001/dfrws-rm-final.pdf>, June 25.
- Petitcolas, F. (2000). 'Information Hiding: Techniques for Steganography and Digital Watermarking', Artech House Books.
- Pfitzmann, B. (1966). 'Information Hiding Terminology - Results of an Informal Plenary Meeting and Additional Proposals'. First International Workshop on Information Hiding, May 30 - June 1, Cambridge, U.K.
- Provos, N. (2008) 'Steganography Detection with Stegdetect', <http://www.outguess.org/detection.php>, June 20.
- Radcliff, D. (2002). 'Quickstudy: Steganography: Hidden Data', <http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html>, June 10.
- Schmidt, M. B., Bekkering, E., and Warkentin, M. (2004). 'On the Illicit Use of Steganography and Its Detection'. ISOOneWorld International Conference. April 14-16. Las Vegas, NV.
- Schotti, G. (1665). 'Steganographia'. Unknown publisher.
- Standage, T. (1999). 'The Victorian Internet', Berkley Books.
- Trithemius, J. (ca. 1499). 'Steganographia', Unknown publisher.
- Warkentin, M., Schmidt, M.B., and Bekkering, E. (2006). 'Steganography and Steganalysis', in Warkentin, M. and R. Vaughn (eds.) Enterprise Information Systems Assurance and System Security: Managerial and System Security. Idea Group Publishing, Hershey, PA.
- Wetstone Technologies (2008). 'Stego Suite', <https://www.wetstonetech.com/cgi/shop.cgi?view,1>, June 25.

Wingate, J. (2007). 'Digital Steganography: Threat or Hype?' *Homeland Defense Journal*, 5(4): 60-63.

Wired News. (2003). 'Internet phone calls stymie FBI', <http://www.wired.com/news/print/0,1294,58350,00.html>, October 27

AUTHORS

Merrill Warkentin is a Professor of MIS at Mississippi State University. His research, primarily in computer security management, eCommerce, and virtual teams, has been published in journals such as *MIS Quarterly*, *Decision Sciences*, *Decision Support Systems*, *Communications of the ACM*, *Communications of the AIS*, *Information Systems Journal*, *Journal of Organizational and End User Computing*, *Journal of Global Information Management*, and others. Professor Warkentin is the co-author or editor of four books, and is currently an Associate Editor of *Information Resources Management Journal*, *Journal of Information Systems Security*, and the Special Issue of *MIS Quarterly* on computer security, and is the co-Guest Editor for the special issue of the *European Journal of Information Systems* on computer security. His PhD is from the University of Nebraska.

Ernst Bekkering is an Assistant Professor in the Department of IS and Technology at Northeastern State University in Tahlequah, OK. Dr. Bekkering obtained his BS in Physical Therapy in his native Holland, and his MS and PhD in Information Systems at Mississippi State University. His research has been published in *Communications of the ACM*, *Journal of Organizational and End User Computing*, and the *Journal of Advancement in Marketing Education*.

Mark B. Schmidt is an Associate Professor of Business Computer Information Systems at St. Cloud State University in St. Cloud, Minnesota. He holds a BS from Southwest State University in Business and Agri-Business, an MBA from St. Cloud State University, and MSIS and Ph.D, degrees from Mississippi State University. He has works published in the *Communications of the ACM*, *Journal of Computer Information Systems*, *Journal of End User Computing*, *Journal of Global Information Management*, *Journal of Internet Commerce*, *Mountain Plains Journal of Business and Economics*, *International Journal of Information Security and Privacy*, *Information System Frontiers*, *International Journal of Information Systems and Change Management*, and in *Information Systems Security: A Global Perspective*. His research focuses on information security, end-user computing, and innovative information technologies.