Abstract

Steganography is the art of, "covered or hidden writing," and it has existed in various forms for over two thousand years. With the emergence of computers and technology, steganography techniques have moved into the digital realm. “Steganography can be used to commit fraud, terrorist activities and other illegal acts” (National Institute of Justice, 2010, p. 4). The purpose of this study was to compare and evaluate the existing digital steganography detection software. The goals were to establish whether the existing computer programs adequately detect steganography programs and files known to be associated with them, as well as file that have been altered with steganographic software. The study accomplished these goals through a combination of a review of existing literature and of direct study. The reviewed literature detailed the types of digital steganography along with techniques for detecting steganography. Additionally, it provided background information on the software evaluated and if applicable, reviews of that software. The direct study created a test set of image, audio, video, and other files created with various available steganographic programs. This test set was used to evaluate the current detection software. The results of the study show more research is needed in the area of detecting digital steganography. Most of the programs had difficulty detecting files that were not images. Many programs only detected images or steganography programs and none of the types of files. The findings of this project determined that the current commercially available digital steganography programs are not sufficient in detecting all ranges of steganography.

Digital Steganography: The Effectiveness of Current Detection Software

By

Jacob Benjamin

A Capstone Project Submitted to Faculty of

Utica College

May, 2012

In Partial Fulfillment of the Requirements for the Degree

Master of Science

Copyright by Jacob Benjamin. 2012

Table of Contents

Digital Steganography: The Effectiveness of Current Detection Software

Steganography is the art of, "covered or hidden writing," and it has existed in various forms for over two thousand years. The earliest usage dates back to the ancient Greeks, during their battles against Xerxses (Kessler, 2002). In *The Histories*, the Greek historian Herodotus, cites an example of steganography, which dates back 440 BC. Demartus, a Greek living in Persia, sent a warning message to the Spartans of the incoming invasion by Xerxses. He was able to send this message by carving a message into the wooden backing of wax tablets. These tablets were commonly used, as a rewritable surface, so their presence was not suspicious. Because the wax covered the message, the Greeks were able to receive the message before Xerxses invaded (Petitcolas 1999).

According to the National Institute of Justice (2010), "One of the most common illicit uses for steganography is for the possession and storage of child pornography images. However, steganography can also be used to commit fraud, terrorist activities and other illegal acts" (para. 4). With the emergence of computers and technology, steganography techniques have moved into the digital realm. Today, there are hundreds of digital steganography applications easily available on the Internet. Steganography applications have also expanded to mobile phones with applications on both Android and iOS operating platforms. There were in excess of fifty applications for mobile phones released in 2011. Many of these applications are free and can be used from the mobile device to send covert messages (Hosmer, 2012).

This data hiding technology is potentially harmful, because it can easily avoid detection by digital security software. Through these digital steganographic programs, innocuous files, such as pictures of the Grand Canyon, can be modified to conceal messages or files. Upon initial inspection, these files would appear unaltered and offer no indication of the information hidden

within them (Judge, 2001). Steganographic programs are not considered malicious software (malware) and are not included in standard antivirus or malware protection (Westphal, 2010).

The purpose of this study was to compare and evaluate the existing digital steganography detection software. The programs being evaluated were StegoHunt, StegAlzyerSS, StegAlzyerSA, Trait Analytic Profiling Search (TAPS) and Stegdetect.

- Do the existing computer programs adequately detect steganography programs and files known to be associated with them?
- Do the existing computer programs adequately detect files that have been altered with steganographic software?
- If the current programs can detect an altered file, are they able to extract the hidden data?
- Are there any steganography applications or carrier files that none of the current programs can detect?

There has been much research on specific steganalysis techniques like specific statistical tests or machine learning algorithms, but there has been little research in specific program evaluations (Meghanathan & Nayak, 2010). The National Institute of Justice, WetStone Technologies, the University of Rhode Island, and the Defense Cyber Crime Center are working together and conducting research to improve steganography detection. According to the National Institute of Justice, current programs lack some features that forensic investigators need. These features include software that identifies altered files and flags them for further investigation, "breaks" the file to extract the hidden data, and analyzes the Windows registry for evidence of steganographic programs whether or not they were run from external media (National Institute of Justice, 2010).

The University of Rhode Island has been researching detecting data hidden within an MP3 music file. The goal of their research is to be able to detect steganography in MP3 and image files with greater than ninety five percent accuracy, down to twenty percent embedding rate (University of Rhode Island, 2009). Moscow State University has been researching and released a new technique for hiding data within video files. The product of their research, MSUStego, successfully hides data within Audio Video Interleave (AVI) files (Vatolin, 2011). Chinese scholars from Beijing University have authored a paper, proposing a technique for detecting hidden data in files altered by MSUStego, however the proposed technique has yet to be implemented (Wu, 2010).

In June 2010, the Federal Bureau of Investigation (FBI) arrested eleven Russian spies who were using digital steganographic technology to covertly communicate (Higgans, 2010). The spies were using these messages to "arrange meetings, cash drops, deliveries of laptops and further information exchanges" (Shachtman, 2010). This case shows that steganography is no longer solely used by child pornographers and financial fraudsters (Higgans, 2010). According to the National Institute of Justice (2010), "Newer steganography-encoding techniques are being rapidly developed, rendering the current detection tools ineffective" (para. 6). The rise of new digital steganography techniques can cause the effectiveness of the current of steganalysis techniques and programs to be questioned.

Digital steganography is not limited to using image files as carriers. There are steganographic programs that can use video files, audio files, and Voice over Internet Protocol (VoIP) network traffic as carriers for hiding data. These altered files: photos, mp3s, and videos can be posted on publicly available websites without suspicion, making it for easy distribution (Shachtman, 2010). Digital steganography can be used to extract valuable intellectual property

out of a secure facility (Greene, 2010). Though there are detection programs that can identify non-image carrier files, there are currently no programs that can identify altered video files (National Institute of Justice, 2010).

Colorado Engineering Inc. has developed *Stegi@Work*, a program built for the Air Force Research Labs that detects steganographic content within media files and either destroys the contents or quarantines the altered files. This software can be used to monitor network traffic and prevent data loss through steganographic means. However, it uses *Stegdetect* to identify potential carriers which can only identify altered image files (Colorado Engineering, 2008).

As previously discussed, there are steganography applications that use many other types of carrier files. WetStone Technologies has developed a product called *StegoBreak* which specializes in cracking passwords for suspected carrier files. It uses password lists to try crack the carrier and reveal its hidden data. It has signature cracks for some steganography applications, but it can extract the hidden data without the need to crack the password (WetStone Technologies, 2012a). "Although there have been some advances in steganography detection and breaking, there is currently no single easy-to-use tool available to law enforcement …" (National Institute of Justice, 2010, para. 6).

The evaluations of the existing digital steganographic detection software were based upon previous research conducted on digital steganography and detection techniques. Moreover, this study created test sets of images, videos, audio files, and other digital media using a wide range of steganographic applications and techniques. Additionally, the test sets included a variety of hidden messages or files which also varied in terms of size and file types. Based upon the research and evaluations of the steganography detection programs, recommendations will be made to offset the gaps between modern steganographic programs and the current means of

detection. These recommendations may include, but are not limited to, documented software algorithms, approaches, or techniques, and even hardware. In the case that current detection means are sufficient, the author will discuss the future of the technology, including emerging techniques and theoretical detection schemes for forensic investigators and other law enforcement officials.

Literature Review

Currently, the most common use of digital steganography is with watermarks to combat intellectual property piracy. There have been rumors of terrorist groups, such as Al-Qaeda, using digital steganography to covertly communicate, but as of yet no definite evidence has been found. While steganography could play a role in several computer crimes, such as fraud, piracy, hacking, and gambling, it has been directly linked to the crime of child pornography. Steganography could be used to circumvent network censorship, and work place restrictions. Studies have shown that steganography alone does not pose a direct threat, but used in conjunction with malware it could become an offensive weapon. By itself steganography cannot be used as a weapon (Judge, 2001).

The purpose of this research was to evaluate the effectiveness of existing steganography detection software. The selected literature sources specifically addressed digital steganography and the varying techniques used to detect digital steganography. The chosen sources were a combination of scholarly articles, news and magazine articles, professional projects, and published books. The sources presented in this study were intended to provide a greater understanding of digital steganography and digital steganography detection.

Steganography in the Past

In 480 B.C., Demartus, a Greek citizen, was able to send a message to the Spartans warning them of the pending invasion by Xerxes. Demartus carved a message into the wooden backing of wax tablets and then hid the message with a new layer of wax. These tablets were commonly used as writing surfaces; their presence was not suspicious to guards while they were in transit (Judge, 2001).

In World War II, the Nazis used steganographic techniques such as Microdots and invisible ink. Microdots are microfilm chips created at high magnification. They are the size of a period on a standard typewriter. However, they could potentially contain maps, drawings, plans, and other highly valuable data (Judge, 2001).

Digital Steganography

Many digital steganography techniques are complex and difficult to understand, but the basic concepts of digital steganography are quite simple. Steganography strips less important information from a digital file and injects hidden data in its place (Kay, 2002). The simplest and most common type of digital steganography uses least significant bit (LSB) embedding on images (Kessler, 2002).

Today, there are hundreds of digital steganography applications easily available on the Internet. Steganography applications have also expanded to mobile phones with applications on both Android and iOS operating platforms. In 2011, there were in excess of fifty applications released for mobile phones. Many of these applications are free and can be used from the mobile device to send covert messages (Hosmer, 2012).

Digital Steganography Software. There are hundreds of available programs such as S-tools, Camouflage, and JP-Hide that can hide data with in image files. MP3Stego, MP3Stegz,

and Hide4PGP are a few of the available steganographic programs which can hide data in audio files. Lastly, there are several steganography programs available that hide data within video files, most notably, MSUStego, Puff and OpenPuff (Johnson, 2011).

Image Steganography. Fulton (1998) states that digital images are comprised of pixels. A pixel is represented by a 24-bitmap value, consisting of three 8-bit bytes that represent the color of the pixel in terms of RGB values. These values can range from 0 to 255. These values are normally represented in hexadecimal (Base-16) format as opposed to the standard Base-10 format for numbers. A pixel with an RGB value of FF 9B 00 (255, 165, 0) is represented as orange. It has a red value of 255(FF), a green value of 165 (9B), and a blue value of 0.

Meghanathan and Nayak (2010), state that the most common carrier type for steganography is image files. Steganography programs that use images as the carrier type include S-Tools, Camouflage, and JP Hide and Seek, as well as countless others. These programs, as with most image steganography algorithms, utilize least significant bit (LSB) embedding mechanism. LSB embedding works by exploiting the fact that changing the least significant bit of each of the red, green, blue (RGB) value of an image would produce only a "minor change in the intensity of the color represented by the pixel and this change is not perceptible to the human eye" (p. 44).

LSB works by changing these RGB values only slightly. For example, if a pixel has a value of FF FF FF (255,255, 255), this is represented as white. If the RGB color values are changed to FE FE FE (254,254, 254), it would only make the color darker by a factor of 1/256. This difference is negligible and cannot be noticed by the human eye. Some LSB algorithms modify randomly chosen pixels, while others only use those located in certain areas of the image.

LSB for paletted images is slightly different. Paletted images include Graphic Interchange Format (GIF), Portable Network Graphics (PNG), and bitmap (BMP) image files. Like other images, paletted images are made up of pixels. The color of the pixel is referenced from a palette table of up to 256 distinct colors. LSB embedding of a paletted image changes the 24-bit RGB value of a pixel. This change could also cause a change in the palette color of the pixel. Steganographic algorithms that only use paletted images focus on "reducing the probability of a change in the palette color of the pixel" in addition to "minimizing the visible distortion that embedding of the secret image can potentially introduce" (p. 45).

Some steganography techniques use BMP images that are characterized by a lossless LSB plane, or raw images. When LSB embedding is used on such images, it results in the two grayscale values of the image being flipped. The hidden message, or payload, is embedded by averaging the frequency of occurrence of the pixels with the two gray-scale values. These pixel values are modified to store the payload.

Textual Steganography. This type of steganography refers to hiding messages within text of digital documents. There are several techniques for textual steganography, including open space methods, line shift coding, word shift coding, syntactic methods, semantic methods, and feature coding. Open space methods refer to adding extra spaces at the end of paragraphs or periods in order to hide a message. Line shift and word shift coding embed a file or message based upon the words or lines in a source document. The output is a document of words but it often looks like nonsense. Syntactic methods refer to actions such as adding punctuation in particular places so they hide a message but still look normal. Semantic methods on the other hand refer to such actions as misspellings of words or using alternative spellings to hide a message within text. Lastly, feature coding refers to altering some of the features of the text such

as elongating certain characters. Feature coding can be used easily with languages that have many similar characters such as Hindi or Chinese. There are also several programs to aid users in hiding messages within text, even some which do not use line or word shifting. However, these applications tend to make the cover message much larger than before. WbStego is popular program for hiding messages within text files. TextHide and NICETEXT are also popular textual steganography applications (Judge, 2001).

Voice over Internet Protocol (VoIP) Steganography. VoIP is one of the most popular services in Internet Protocol (IP) networks, which is being utilized around the world. VoIP is a real-time service that allows individuals to have voice conversations through IP networks. It is used to communicate through the Internet in a similar manner to the telephone. VoIP transmits the data in packets to both parties through one of the following protocols: IP, User Datagram Protocol (UDP), or Transmission Control Protocol (TCP). It is well suited to hide messages or other payloads, because the high volume of traffic it generates VoIP steganography exploits the fact that only a few fields of the headers in the packet are changed during the communication process. The headers of IP, UDP, and TCP have many fields that are either unused or optional. The hidden message, or payload, is inserted into redundant fields for IP, UDP, and TCP then transferred to the receiving side. These headers offer a great place to hide a message or other payload because they are often overlooked (Mazurczyk & Sczcypiorski, 2008).

Audio Steganography. Meghanathan and Nayak (2010) state that audio files provide an ideal format for hiding data. There are very few resources for detecting audio files that have been altered by steganographic means. This can be attributed to the nature of audio signals as well the strength of the steganographic algorithms. Because of this, steganalysis of audio files tends to be inconsistent at best. Audio files are excellent candidates for steganography because they have

"characteristic redundancy and an unpredictable nature that make them ideal to be used as a cover for covert communications to hide secret messages" (p. 47).

Bender (1996) presents information that phase coding is based on the principle that certain components of sound are not as perceptible to the human ear, specifically phase components. The hidden message bits are encoded as phase shifts in the phase spectrum of a digital signal. Hiding the message in this manner is inaudible manner. This concept allows the secret message to be camouflaged within the audio signal.

Huang & Yeo (2002) state that echo hiding embeds information by introducing an echo into the discrete audio signal. Echo hiding modifies the amplitude, decay rate, and delay time from the original signal below the human audible threshold limit, so the changes are not discernible to humans. The actual hidden message is concealed within the values of the delay time.

Video Steganography. MSUStego allows hiding of any file in a video sequence and offers many different codecs and redundancy settings. It is one of the few programs that allow data to be hidden within audio video interleave (AVI) files. The hidden data can be extracted even if the video is later compressed (Meghanathan & Nayak, 2010).

MSUStego was developed by the computer science department of Lomonosov Moscow State University. The quality of information extracted from compressed video depends on the codec used, the amount of data redundancy, and the frame size. The probability of extracting file info without errors increases depending upon information redundancy (Vatolin, 2011).

Digital Steganography for Legitimate Purposes

Digital steganography was used by British Prime Minister Margaret Thatcher to identify disloyal ministers within her cabinet. In the 1980s, there were several cabinet documents that

were leaked to the press. Thatcher ordered the word processors of the cabinet ministry configured to encode a number within the spacing of the words of documents. This number corresponded to a specific word processor. By knowing which word processor produced the documents, Prime Minister Thatcher was able to pinpoint which individuals were responsible for leaking documents.

Similar techniques are being employed to hide serial numbers or other identification methods within documents and other forms of copyrighted media. For example, many production studios embed serial numbers within the frames of a movie. The serial number corresponds to a specific theatre or the geographical region of the theatres where that movie was being shown. If an infringer digitally records the movie and distributes it, the hidden serial number is retained in the copy. Investigators can use this serial number to help copyright owners track down and prosecute infringers These techniques of imbedding information are called digital watermarking and they are forms of digital steganography (Maxemchuk, 1994).

There are different types of digital watermarking with varying ranges of robustness and perceptibility. A robust watermark can still be detected after modifications to the file. A fragile watermark cannot be detected after even slight modifications to the file. Perceptible watermarks are not hidden from view and are easily noticeable within the file. Contrarily, imperceptible watermarks are hidden and require secondary resources to be viewed. Preferences on the perceptibility of a watermark differ depending upon the application and purpose of the watermark (Kraetzer, 2007).

The Institute for Information Technology Security Research at St. Poelten University of Applied Sciences in Poelten, Austria, has developed a solution for concealing an entire file system in existing image or music files through steganographic means. This solution along with

other steganographic techniques offers significant opportunities for protecting national security. This added layer of security can ensure that data is protected from unauthorized access. By hiding encrypted data through steganographic means drastically lowers the chances that it will be found, extracted, and eventually cracked. Additionally, steganography offers a means of securing sensitive data in countries where there are restrictions have been place upon data encryption (Homeland Security Newswire, 2010).

Digital Steganography for Illegal Activity

Digital Steganography is not only limited to legitimate uses, such as protecting national security secrets and copyrighted material. It can also be used by criminals to hide their illegal activities. For example, steganography has frequently been used by those who possess and send child pornography, as well as those persons committing financial fraud. Conversely, prior to the terrorist attacks on September 11, 2001 (9/11), digital steganography had long been considered too obscure or complex for mainstream criminals and terrorists (Higgins, 2010).

After the attacks on 9/11, many government intelligence agencies and industry experts believed the terrorist group al-Qaeda was using digital steganography to communicate among its terrorist cells. A group of researchers from the University of Michigan scanned websites, such as the auction listings on eBay, looking for potential terrorist communications hidden within the user uploaded images; no messages were found (Judge, 2001).

In June 2010, the Federal Bureau of Investigation (FBI) arrested eleven Russian spies who were using digital steganographic technology to covertly communicate (Higgans, 2010). When the FBI searched the home of one of the spies, they found a computer disk that contained a computer program which allowed the spies to encrypt data and then embedded this data into images on websites. FBI agents also discovered links to several websites on a seized computer

hard-drive. These websites were visited and images were downloaded. Utilizing digital steganography detection software, the agents discovered the images contained hidden messages (United States of America v. Anna Chapman, and Mikhail Sememko, 2010).

Shachtman (2010) states that while there was rumors that al-Qaeda had begun hiding messages in images on pornographic websites, these rumors were never confirmed. However, al-Qaeda could certainly use digital steganography. It is likely that usage of these methods would be similar to that of the spies in the FBI case involving the eleven spies. The spies were using these messages "to arrange meetings, cash drops, deliveries of laptops and further information exchanges" (para. 7).

Many enterprises want to protect their assets and trade secrets. They may turn to network or host based solutions that restrict users from certain activities, such as installing applications or visiting certain websites. However, steganography can allow users to get around these protections. Disgruntled employees or other insiders can use steganography to remove trade secrets from their companies or send these secrets to competitors without detection. Corporate Espionage has become a rising trend. According to the FBI and the U.S. Chamber of Commerce, U.S. companies lose approximately $2 billion a month to corporate espionage. It is suspected that many of the losses either go undetected or companies, wanting to protect their reputation, do not report these losses (Jones, 1999).

Steganalysis: Digital Steganography Detection

Meghanathan and Nayak (2010) conducted a study which detailed several steganalysis algorithms for many different kinds of cover media, including images, audio, and video. With the rise of digital steganography also came the emergence of steganalysis. Steganalysis is the science or practice of detecting the presence of data hidden within the cover media such as images,

audio, or video files. Because of the scarcity of knowledge regarding the specific characteristics of the cover media, steganalysis is a difficult field of study.

Steganalysis often uses complex statistical tests as well as looking for signatures or traces of known steganography techniques. Each type of cover media requires different analysis algorithms to focus on particular characteristics. Image steganalysis algorithms center on the "strong inter-pixel dependencies" that are characteristic of natural images (p. 44). Audio steganalysis algorithms use the distortion measure of the audio signal and high-order statistics as a focal point for investigation. Lastly, video steganalysis algorithms target the "spatial and temporal redundancies in the video signals within the individual frames and at inter-frame level" (p. 44).

Image Steganalysis. Image steganalysis refers to identifying if Joint Photographic Expert Group (JPEG), raw, or paletted images have been altered through steganographic means. Most research regarding detecting digital steganography focuses on image steganography. This is because image steganography is the common form of digital steganography and has more available steganography programs than any other carrier file type (Johnson, 2011).

Joint Photographic Expert Group (JPEG) Steganalysis. JPEG is the most common format for storing and transmitting photographs on the Internet. It is a lossy compression, a compression in which unnecessary information is discarded, that typically gets a 10:1 compression without a significant drop in image quality. JPEG steganography programs usually use one of two algorithms, F-5 or outguess. The F-5 algorithm works by using matrix embedding to embed bits in the discrete cosine transform (DCT) coefficients. This mutates the histogram of DCT coefficients but minimizes the number of changes to a message (Meghanathan & Nayak, 2010). The outguess algorithm makes, "…a random walk and embeds its message bits in the

LSB of some of the DCT coefficients. The other DCT coefficients are then adjusted to keep the original histogram intact" (Meghanathan & Nayak, 2010, p. 46).

Jessica Fridrich a computer engineering professor at Binghamton University has proposed methods of detecting both of these steganography methods. Her algorithm for detecting F-5 involves, determining the unaltered histogram to find to deduce the length of the secret message as well as the number of changes to the file. This unaltered histogram can also be used to help identify or detect images affected by the Outguess algorithm. Fridrich's algorithm generates this unaltered histogram by first cropping the image into four columns and then re-compressing the image using values in the quantization table stored within the image. The resulting DCT coefficient histogram is a close estimate of the original image before it was altered through steganographic means. Fridrich proposed that by embedding an additional message into the stegged image, the discontinuities of the DCT coefficients caused by the original LSB embedding would be smaller this time around. This process is used to measure the size of the hidden message (Fridrich, 2003).

Raw Image Steganalysis. A new technique for detecting raw image steganography was proposed by Jessica Fridrich of Binghamton University. This technique involves analyzing what is called close color pairs. The color palette of a raw image that has been altered by LSB is characterized by a higher number of close color pairs. The original number of unique colors for a raw image can be determined by dividing the number of pixels in the image by two (Meghanathan & Nayak, 2010).

Paletted Image Steganalysis. Paletted image steganalysis is usually reserved for GIF images. However, these techniques can be used against BMP and PNG images that are paletted. The steganalysis of a GIF image is conducted by performing a statistical analysis of the palette

table. The detection is made when there is a significant increase in the variation in the palette colors. The larger the hidden message, the greater the variation in the palette colors of the image (Meghanathan & Nayak, 2010).

Audio Steganalysis. Wenjun Zeng, a computer science professor at the University of Missouri, has proposed methods for detecting both phase and echo encoding. Zeng's algorithm to detect phase coding steganography performs a statistical analysis of phase discontinuities within the audio file. The statistical analysis consists of monitoring the changes in the phase difference and training the classifiers of his machine-learning algorithm to differentiate an embedded audio signal from a clean audio signal (Zeng, 2007).

Zeng (2008) developed an algorithm for detecting echo hiding utilizing support vector machines to analyze data and identify patterns. Specifically, it uses support vector machines to analyze the peak frequency. A support vector machine is an algorithm that analyzes data and recognizes patterns. Zeng's support vector machine calculates the eighth high order center moments of peak frequency as feature vectors to be given as input to the support vector machine. The support vector machine differentiates between audio signals with and without data.

There are several more audio embedding techniques, such as low-bit encoding and special spectrum encoding. These techniques, like phase coding and echo hiding, are difficult to detect and require classifiers, such as a support vector machine. The most significant problem with classifiers is that they are only as good as the training models with which they are provided (Meghanathan & Nayak, 2010).

Video Steganalysis. There have been several algorithms proposed to analyze videos for traces of steganography, but, like audio files, few resources are readily available. The simplest technique is to split the video into frames and analyze the frames using image detection

algorithms. Another technique would be to separate the audio from the video and apply detection algorithms for audio files. However, this approach is far from efficient (Meghanathan & Nayak, 2010).

An algorithm for detecting videos modified by MSUStego was proposed by Su, Zhang, Wang, and Zhang. The algorithm uses the correlation between adjacent frames to detect a special distribution mode across the frames After correlation analysis between adjacent frames, the algorithm calculates the ratio of pixel blocks with a specific distribution mode to the total number of pixel blocks in the video sequence If that ratio is above a threshold value, then the video is likely to be a carrier for an embedded message (Su, Zhang, Wang, & Zhang, 2008).

Digital Steganography Detection Programs

Most programs that aid in steganography detection search a computer's file systems for steganographic programs. The presence of these steganographic applications usually indicates that the owner of the computer has been employing steganography. However, most detection programs do not narrow down suspicious files that may be carriers of hidden data through steganographic means (Westphal, 2010).

Forensic Computing Limited is a reference website for forensic investigators to choose a forensic expert and or digital forensic applications. They have compiled a list of the best digital forensic programs available. For steganography detection, their list includes the programs within WetStone Technologies' StegoSuite, a suite of products they call the "most advanced bundle available for investigation, detection, analysis, and recovery" (Forensic Computing Limited, 2004). At the time this list was compiled Stego Suite contained StegoAnalyst, StegoBreak, StegoHunter, and StegoWatch. Since then, WetStone Technologies has combined StegoWatch and StegoHunter into one product called StegoHunt (WetStone Technologies, 2012a).

Gupta and Garg (2008) authored the paper *Detecting LSB Steganography in Images*. In this study they evaluated StegDetect, a steganography detection program written by Neil Provos. They found StegDetect was able to identify all but three of the images created by the steganography program JPHide. They hypothesized that images with large homogeneous regions and small clusters of high frequencies are able to evade detection by StegDetect.

In 2010, Dr. Dobb's software journal presented an article about Backbone Security releasing steganography detection policy for companies protected by Fidelis XPS session-level security solution. This product along, with their StegAlyzerSA product, uses their Steganography Application Fingerprint Database (SAFDB). Dr. Dobbs claims SAFDB is the largest commercially available database of steganography software (Dr. Dobbs Journal, 2010).

In 2010, the National Institute of Justice in conjunction with the University of Rhode Island, and WetStone Technologies developed Trait Analytic Profiling Search (TAPS) (NIJ, 2010). The product uses high speed Fibonacci Hashes in conjunction with stronger hashing algorithms, such as SHA-256 and MD5. If file matches the Fibonacci Hash database it is then validated by a full MD5 or SHA-256. This process lowers the computational cost of by not doing a full SHA-256 or MD5 hash for every file. TAPS also employs Advanced JPEG Artifact Detection, which uses machine learning algorithms proposed by expert Jessica Fridrich, to identify JPEG images that have been modified through steganographic means (WetStone Technologies, 2012b). SC Magazine, a magazine for information technology professionals, gave TAPS a five-star rating. They said while it is fairly limited, referring to its carrier search only detecting JPEG files, it performs well (Norwich University Students, 2011).

Steganography Detection Programs Evaluated in this Study

Stegdetect and StegAlyzerSS focus on finding potential carrier files, files that may have been altered by steganographic means. Stegdetect uses statistical probabilities to determine if image files are suspicious or likely to contain hidden data (Provos, 2008). StegAlzyerSS looks for signatures that fifty five common steganography programs leave on carrier files regardless of their file type (Steganography Analysis and Research Center, 2010b). StegAlzyerSA searches attached file systems for files and registry keys known to be associated with steganography applications. It identifies these files by their hash, a one way mathematical calculation that uniquely represents that file (Steganography Analysis and Research Center, 2010a).

TAPS and StegoHunt both search for programs and possible carrier files. Similar to StegAlzyerSA, TAPS and StegoHunt identify programs associated with steganography by their hash values. A hash value is a calculation that can be performed on a file that uniquely represents that file. If anything in the file changes, its hash value will change. TAPS was funded by the National Institute of Justice (NIJ) in an effort to combat the threats posed by steganography. Like Stegdetect, TAPS focuses on finding carrier files that are images. It implemented statistical algorithms proposed by steganography expert Jessica Fridrich. Like StegAlzyerSS, StegoHunt's carrier scan is not limited to image files. However, StegoHunt's approach differs slightly. While StegoHunt looks for signatures left on the file by known steganography programs, it also performs complex analytical statistics on these files to look for anomalies that are not program specific (WetStone Technologies, 2012a). These products each have strengths and weaknesses but the National Institute of Justice feels that there is still a lack of an easy, all-purpose steganography detection program for law enforcement (National Institute of Justice, 2010).

This concludes the literature review for digital steganography. Much of the available literature is specific for detection techniques and not implementations of those techniques in current software. A direct study of the effectiveness of current steganography detection software was conducted to counteract this deficiency. In the following section, the methodology of the direct study is detailed.

Methodology

This study evaluated the current state of steganography detection programs available for forensic investigators. In conjunction with a review of existing literature, this study also tested several steganography detection programs. Moreover, this study created test sets of images, videos, audio files, and other digital media using a wide range of steganographic applications and techniques. The test set also included a various hidden payloads. These payload were either messages or files and varied in terms of file size and file type.

The purpose of this study was to answer the questions: Do the existing detection programs adequately detect steganography programs and files known to be associated with them? Do the existing detection programs adequately detect files that have been altered with steganographic software? If the current detection programs can detect an altered file, are they able to extract the hidden data? Are there any steganography applications or carrier files that none of the current detection programs can detect?

Steganography Programs Used to Create Test Sets

Steganography expert Dr. Neil Johnson has compiled a list of available digital steganography programs. The programs used to create the test set were acquired from his list. Included programs are s-tools, WbStego, OpenPuff, Camouflage, Tcsteg, MSUStego, MP3Stego, MP3StegZ, jp-hide and seek, invisible secrets, and spypix (Johnson, 2011). These applications

were selected from Dr. Johnson's list based upon the type of carrier files they used and the ease of their availability. Refer to Appendix A for the list of programs, and their versions that were used in creating the test set.

Image Test Set. The image test set included five images of each of the following types: jpeg, gif, png, and bmp. These images were altered by the following programs: s-tools, jp-hide and seek, invisible secrets, OpenPuff and spypix. The payload for these carrier images was a text file filled with instructions. This file simulated two parties covertly communicating through steganography. Refer to Appendix B for a list of the images in test.

Audio Test Set. The audio test set included five MP3 files and five WAV files. These files were altered with the following programs: s-tools, MP3Stego, MP3StegZ, and OpenPuff. The payload for these files was a text document containing several e-books. This file simulated two parties sending large message, the size of several books, covertly. Refer to Appendix C for a list of audio files in the test set.

Video Test Set. The video test contained five MP4 files altered by TcSteg, five MP4files altered by OpenPuff, and five AVI files altered by MSUstego. The payload for the files altered by Tcsteg was a file container holding several files of varying type. The payload for OpenPuff was a text file containing several e-books. Lastly, the payload for files altered by MSUStego was also a text file containing several e-books. Refer to Appendix D for a list of video files in the test set.

Other Test Set. This category within the test set refers to any carrier file that is not an image, audio, or video file. For this test set, the payload was a large text file containing several e-books. This file was hidden with five pdf files, five html files, and five documents. The programs

used to make this test set included WbStego, OpenPuff, and Camouflage. Refer to Appendix E for files in the test set that are carrier files but not audio, video, or image files.

Digital Steganography Detection Testing

Before testing each detection program the testing computer was restarted, then the detection program to be tested was started. Next, the author pointed the program to the sample directory on the computer's hard drive, which contained the steganography test sets and their original files. Once the scan was complete, the author noted the results and began the process over again.

Results

StegDetect detected thirty-three percent of the images in the test set and zero from any of the other categories. StegAlzyerSA did not identify any files carrier files in the test set, however it detected sixty percent of the programs in the test set. StegAlyzerSS was able to detect a few images and html files in the test set, but it failed to detect any video, audio or programs.

TAPS detected all of the images in the test set. Additionally, it identified thirty-three percent of the audio files and ninety percent of the programs in the test set. However, it was unable to detect any video carrier files or any carriers in the 'other' category.

StegoHunt was able to identify all of the images, all of the audio files, thirty-three percent of the video files, and ninety percent of the programs. However, it was unable to detect any of the carrier files in the 'other' category. Refer to Table 1 for the results of the testing.

Detection Program	Detected Images	Detected Audio	Detected Video	Detected Other	Detected Program
StegDetect	5/15	0/10	0/15	0/15	0/10
StegAlyzerSA	0/15	0/15	0/15	0/15	6/10
StegAlyzerSS	3/15	0/15	0/15	2/15	0/10
TAPS	15/15	3/10	0/15	0/15	9/10
StegoHunt	15/15	10/10	5/15	0/15	9/10

Table 1 Testing Results

In the next section, the Discussion of the Findings, the author will further detail the results and what they mean. Each program evaluated will be discussed, highlighting their strengths and weaknesses. Additionally, the results will be compared and contrasted with the findings in the literature review.

Discussion of the Findings

The emergence of the Internet and the digital age brought new steganographic techniques involving digital media. Forensic investigators can use programs such as StegoHunt, StegAlzyerSS, StegAlzyerSA, Trait Analytic Profiling Search (TAPS) and Stegdetect to search a suspect's computer for steganography programs or for files that have been modified by steganography. According to the National Institute of Justice (2010), programs available to investigators for steganography detection are insufficient.

This study aimed to answer the following questions about the current state of steganography detection programs:

- Do the existing detection programs adequately detect steganography programs and files known to be associated with them?

- Do the existing detection programs adequately detect files that have been altered with steganographic software?
- If the current detection programs can detect an altered file, are they able to extract the hidden data?
- Are there any steganography applications or carrier files that none of the current detection programs can detect?

This study evaluated these programs utilizing previous research. In addition, each program was tested against a set of digital media files that were altered by steganography programs.

Major Findings

Existing Literature. The literature reviewed for this study confirmed that digital steganography can be both a benefit and a threat depending upon how the technology is utilized. When used by government agencies, it can help deter leaks of information, thus not jeopardizing national security (Maxemchuck, 1994). However, when this technology is used by the criminal element, such as terrorist and child pornographers, it can be a difficult obstacle for forensic investigators to overcome (United States of America v. Anna Chapman, and Mikhail Sememko, 2010).

Different types of digital steganography including, textual, image, audio, video, and network were presented in the literature review. Additionally, known methods of detecting altered image, audio, and video files were detailed. However, while there is a significant amount of literature related to steganalysis of image files, there is only a small amount of literature available related to steganalysis of other file types (Meghanathan & Nayak, 2010).

Most of the literature regarding detecting digital steganography refers to individual techniques, but not available programs that implement the techniques. There are some product

reviews available for some of the commercially available steganography detection programs. These product reviews found that the commercially available programs detected images altered by steganography with an acceptable degree of accuracy (Gupta & Garg, 2008). These product reviews did not test the programs for their ability to detect other carrier types, such as video and audio files.

Testing of Detection Programs. The literature review found that an insufficient amount of current or up to date literature was available regarding the effectiveness of steganography detection programs. This void of literature prompted the direct testing in this study. The direct testing in this study evaluated current available steganography detection programs against a test set of varying carrier files and programs.

The results of the study support the hypothesis that the current steganography detection programs are insufficient for forensic investigators. There were files in the test set that were altered by techniques that none of the programs could detect. However there were also techniques that were identified by multiple programs. As a whole, steganography detection programs are not abysmal, but all of the programs could benefit from improvements.

Stegdetect. Stegdetect was able to detect some of the images altered by steganography. It was able to detect several of the JPEG test files. However, it could not detect altered BMP, GIF, and PNG image files. Stegdetect also failed to identify neither any of the altered audio and video files nor any steganographic programs in the test set. The results regarding Stegdetect were not surprising; the program only claims to be able to detect altered JPEG files. However, Stegdetect still remains one of the leading programs in steganography detection.

StegAlyzerSA. StegAlyzerSA was able to identify several steganography applications, their associated files, and registry information. However, it failed to identify any potential carrier

files. StegAlyzerSA easily identified most of the steganography programs, but struggled finding applications designed for mobile operating systems like Android and iOS.

StegAlyzerSS. StegAlzyerSS was able to identify some of the carrier files altered by steganographic means. This program works by looking for signatures left behind by steganographic programs, so any carrier file that was altered by a program that was not in its signature database was undetected. It should be noted that StegAlyzerSS's signature database contains fifty-five steganography applications, but there are over thousand available on the Internet (Steganography Analysis and Research Center, 2010b). In addition to not identifying the steganography programs in the test set, StegAlyzerSS failed to discover any carrier files that were an audio or video file type.

TAPS. TAPS was able to identify most of the altered images as well as most of the steganography programs in the test set. While it excelled in identifying steganography programs and altered images, it failed to find any of the audio or video carriers in the test set. TAPS was not able to identify altered file types, such as documents, pdf, and html files.

StegoHunt. StegoHunt identified all but one of the steganography applications. It identified all of the altered images, several of the altered audio files, and some of the altered video files in the test set. The area where StegoHunt struggled is with carrier files of document, pdf, or html format; it was unable to identify any of these files.

Comparison of the Findings

All of the steganography detection programs require improvements in order to adequately detect current steganography techniques. None of the programs were able to detect a sufficient number of video files. This confirms a statement made by the National Institute of Justice that

there are techniques for hiding data within videos to which no current programs that can identify (National Institute of Justice, 2010).

According to her study, Jessica Fridrich's machine learning algorithm accurately detects altered JPEGs with incredible accuracy (Meghanathan & Nayak, 2010). TAPS implemented Fridrich's JPEG detection algorithms into their detection program. SC Magazine reviewed TAPS and stated that the program only found JPEG carrier files (Norwich University Students, 2011). However, this study found that TAPS was able to detect other image types in addition to JPEG images in its carrier scan. Nonetheless, it was unable to find any altered videos and only a few altered audio files. TAPS was able to identify ninety percent of the steganography applications in the test set. The Fibonacci hashing technology allowed it do have the second fastest time in scanning for programs. Based on the results of this study, the limited carrier detection ability of TAPS concurs with the review by SC Magazine, but the program performs its job well.

In Gupta and Garg's (2008) paper, *Detecting LSB Steganography in Images*, Neil Provos' StegDetect was evaluated. Their study found that StegDetect was able to identify all but three of the images created by the steganography program JPHide. The finding of this study concurs with finding of Gupta & Garg's study. StegDetect was able to detect JPEG images altered by JPHide. However, StegDetect's capabilities are only limited to JPEG images. It was unable to detect any other image type or carrier file type.

StegAlyzerSA boasts having the largest commercially available steganography program detection database (Dobbs, 2010). However, it was only able to find sixty percent of the programs in the test set. Three out of the five programs evaluated had program detection capabilities. StegAlyzerSA performed the worst out of the three. While their database may be the largest, this study shows it is not the most accurate.

Forensic Computing Limited called StegoSuite the most advanced available software bundle for forensic investigators (Forensic Computing Limited, 2004). While this study did not evaluate all of the programs in that suite, it did evaluate the main one, StegoHunt. StegoHunt was able to find altered, image, audio, and video files as well as ninety percent of the steganography programs in the test set. StegoHunt was the most complete detection program evaluated. Overall, it outperformed every other program tested in this study.

Limitations of the Studies

As with any study, the study is not without limitations. The limitations for this study include small sample sizes, lack of prior research on the topic, self-reported data and lack of participants. The small sample size refers to the number of digital media files altered as well as the number of programs used to create the test set. This study created a test set with ten different programs, however there are over one thousand available steganography programs (Steganography Analysis and Research Center, 2010b). Further research should be done using a wider range of programs to create the test set. Additionally, the payloads, the hidden data, was always less than or equal to twenty percent of the cover media. A test set with a wider range of embedding percentage should be further implemented.

The lack of prior research limitation refers to studies done on program evaluations. Much research has been conducted on techniques, but studies evaluating implementations of these techniques into programs available for forensic investigators are limited. Program evaluations were limited to magazine articles conducting a product review. Extensive scholarly evaluations of available programs are nonexistent.

The experiment for this study was conducted and was self-reported by the author. This limitation can rarely be independently verified. Additional problems with self-reported data

include forms of bias such as selective memory, telescoping, and exaggeration. Selective memory refers to either remembering or not remembering events that happened in the past. Telescoping refers to remembering an event happening at a certain time, when it actually happened at a different time. Lastly, exaggeration refers to representing outcomes as more significant than what the data actually represents.

The lack of participants refers to the limited number of steganography detection programs commercially available to test. Many steganography detection techniques are written about, but not implemented into programs. Often these techniques are implemented in a manner that simply verifies that the technique works. Examples include Zeng's work with audio files and Su, Zhang, Wang and Zhang's work with video files.

Recommendations

The article *Steganalysis Algorithms For Detecting the Hidden Information in Image, Audio, and Video Cover Media* suggests that research on audio and video steganography detection is limited (Meghanathan & Nayak, 2010). Despite the rapid growth of steganography software, little research has been done to evaluate steganography detection programs. It is important to measure the efficiency, accuracy, and effectiveness of steganography detection programs in order to identify their strengths and weaknesses and make improvements where needed.

Additional methodologies may be necessary for adequate evaluations of steganography detection programs. Standards for evaluating steganography detection programs should be developed. However, standardized techniques for evaluating any software product currently exist and could be adapted to or used in research related to the evaluation of steganography detection programs.

Forensic investigation professionals are impeded by the almost complete absence of empirical research on the effectiveness of available steganography detection programs. Forensic investigators require programs that adequately detect the latest threats in order to remain current with the criminal element. Research regarding the effectiveness of these programs would aid forensic investigators in choosing the program that best fits their needs and budgets.

Further research could also be conducted to determine the effectiveness of steganography detection programs against network, audio, and video steganography. Research has been done on detection techniques for audio and video and network steganography, however many of the programs have yet to implement the suggestions from the research. None of the commercially available programs claim to be able to detect network steganography. Ten years ago most digital steganography programs only employed simple techniques such as LSB embedding in images. However, in the last decade steganography technology has evolved to use more advanced methods as well as a broader range of carrier file types. Research needs to be done on detecting these newer steganography methods and carrier files, and implementing the findings into programs that are available to forensic investigators.

Recommendations for Future Research

Future research in the area of detecting digital steganography is vital to forensic investigators whether they are employed by the government or the private sector. Recommended topics for further research include researching and evaluating the effectiveness of steganographic blocking techniques, steganographic breaking techniques and programs, and detecting network steganography.

Researching steganography blocking techniques would help government or corporate officials secure classified or other sensitive projects form espionage. The National Institute of

Justice specifically wants a steganography detection suite that includes breaking programs that would aid forensic investigators on their cases (National Institute of Justice, 2010). Network steganography is one of the forms of digital steganography that was not tested in this study's test set. Additionally, none of the current detection programs even claim to identify it. These three topics will need further research if forensic investigators wish to keep up with new technology.

The purpose of this study was to simply identify suspicious files and not to attempt to extract the hidden data from them. Nevertheless, research in breaking steganography techniques is needed. The National Institute of Justice is funding projects in an attempt to obtain a program that can both flag suspicious as well as begin extracting the hidden data (National Institute of Justice, 2010). Additional research in detecting steganography and the programs to do so will aid law enforcement officials and forensic investigators in their investigations.

Limitations of the Study

A limitation of this study was that it did not include network steganography detection programs. Network steganography is still in its infancy compared to the more refined techniques of image and audio steganography, and available programs are limited. As network steganography continues to develop and more network steganography applications become available, research on detecting these techniques will be needed.

Conclusion

The purpose of this study was to compare and evaluate the existing digital steganography detection software. The programs being evaluated were *StegoHunt, StegAlzyerSS, StegAlzyerSA*, *Trait Analytic Profiling Search (TAPS)* and *Stegdetect.* The evaluations of the existing digital steganographic detection software were based upon previous research conducted on digital steganography and detection techniques. Moreover, this study created test sets of images, audio,

video files, and other digital media using a wide range of steganographic applications and techniques. A direct evaluation of these software programs was conducted against the test set.

Much research has been done on detecting different types of steganography, but sources researching or evaluating program implementations of these techniques are limited. Detecting steganography is achieved by searching for remnants of steganographic applications on a target system, searching for files likely to have been altered by said applications or both. This study evaluated several programs and their abilities to do perform both of these approaches.

Collectively, the detection programs evaluated this study were not sufficient to combat the current steganography threat. Most of the programs were able to identify altered JPEG image files, which is the most common carrier type used in digital steganography. Though being able to detect altered JPEG images is a positive asset in combating steganography, in the last several years steganography programs have expanded to include other carrier file types.

As programs with more diversified carrier file options gain popularity, these file types, which can hide larger amounts of data, may surpass JPEG images in their prevalence. Many of the evaluated detection programs failed to identify any carrier files that were not images. There were audio and video files altered with techniques that none of the current detection programs could identify. Only two of the programs were capable of finding both steganographic programs along with the files altered by these programs. Lastly, none of the programs were able to detect network steganography.

Digital steganography is a viable threat to the security of the United States, and a significant means for criminals to conduct their illegal activities. Forensic investigators, law enforcement, and government officials require programs that can detect most, if not all, forms of digital steganography. The deficiencies in the current steganography detection programs leave

criminals, terrorists, or other entities a means to communicate covertly, and transfer information without detection.

Appendix A

Programs in the Program Evaluation Test Set

Program	**Version**
Camouflage	1.21
Invisible Secrets	4.0
JP Hide and Seek	0.3
MP3Stego	1.118
MP3StegZ	1.0
MSUStego	1.0
Spypix	1.0
S-tools	4.0
TcSteg	1.0
WbStego	4.2

Appendix B

Images in the Program Evaluation Test Set

Filename	**File Type**	**Steganography Program Used**
Image1_jpeg_stools.jpg	JPEG Image	S-tools
Image2_jpeg_jphs.jpg	JPEG Image	JP Hide and Seek
Image3_jpeg_invsec.jpg	JPEG Image	Invisible Secrets
Image4_jpeg_opp.jpg	JPEG Image	Open Puff
Image5_jpeg_spypix.jpg	JPEG Image	SpyPix
Image_6_bmp_stools.bmp	BMP Image	S-tools
Image_7_bmp_invsec.bmp	BMP Image	Invisible Secrets
Image_8_bmp_opp.bmp	BMP	OpenPuff
Image_9_bmp_spypix.bmp	BMP	SpyPix
Image_10_bmp_stools.bmp	BMP	S-tools
Image_11_png_spypix.png	PNG	SpyPix
Image_12_png_opp.png	PNG	OpenPuff
Image_13_png_spypix.png	PNG	SpyPix
Image_14_png_opp.png	PNG	OpenPuff
Image_15_png_spypix.png	PNG	SpyPix
Image_16_gif_stools.gif	GIF	S-tools
Image_17_gif_opp.gif	GIF	OpenPuff

Image_18_gif_stools.gif	GIF	S-tools
Image_19_gif_opp.gif	GIF	OpenPuff
Image_20_gif_stools.gif	GIF	S-tools

Appendix C

Audio Files in the Program Evaluation Test Set

Filename	**File Type**	**Steganography Program Used**
Audio_1_wav_stools.wav	Wav	S-tools
Audio_2_wav_opp.wav	Wav	OpenPuff
Audio_3_wav_stools.wav	Wav	S-tools
Audio_4_wav_opp.wav	Wav	OpenPuff
Audio_5_wav_opp.wav	Wav	OpenPuff
Audio_6_mp3_mp3Stego.mp3	MP3	MP3Stego
Audio_7_mp3_mp3Stegz.mp3	MP3	MP3StegZ
Audio_8_mp3_opp.mp3	MP3	OpenPuff
Audio_9_mp3_mp3Stego.mp3	MP3	MP3Stego
Audio_10_mp3_mp3StegZ.mp3	MP3	MP3Stegz

Appendix D

Video Files in the Program Evaluation Test Set

File Name	**File Type**	**Steganography Program Used**
Video_1_mp4_tcsteg.mp4	MP4	TcSteg
Video_2_mp4_tcsteg.mp4	MP4	TcSteg
Video_3_mp4_tcsteg.mp4	MP4	TcSteg
Video_4_mp4_tcsteg.mp4	MP4	TcSteg
Video_5_mp4_tcsteg.mp4	MP4	TcSteg
Video_6_mp4_opp.mp4	MP4	OpenPuff
Video_7_mp4_opp.mp4	MP4	OpenPuff
Video_8_mp4_opp.mp4	MP4	OpenPuff
Video_9_mp4_opp.mp4	MP4	OpenPuff
Video_10_mp4_opp.mp4	MP4	OpenPuff
Video_11_avi.avi	AVI	MSUStego
Video_12_avi.avi	AVI	MSUStego
Video_13_avi.avi	AVI	MSUStego
Video_14_avi.avi	AVI	MSUStego
Video_15_avi.avi	AVI	MSUStego

Appendix E

Other Files in the Program Evaluation Test Set

File Name	**File Type**	**Steganography Program Used**
Other_1_pdf.pdf	PDF	OpenPuff
Other_2_pdf.pdf	PDF	WbStego
Other_3_pdf.pdf	PDF	Camouflage
Other_4_pdf.pdf	PDF	OpenPuff
Other_5_pdf.pdf	PDF	WbStego
Other_6_html.html	HTML	Camouflage
Other_7_html.html	HTML	WbStego
Other_8_html.html	HTML	Camouflage
Other_9_html.html	HTML	WbStego
Other_10_html.html	HTML	WbStego

Bibliography

Bender, B., Gruhl, D., Morimoto, N. (1996). Techniques for Data Hiding, *IBM Systems Journal*, vol. 35, no. 3, pp. 313 – 336

Colorado Engineering Inc. (2008). In Stegi@Work. *CEI.* Retrieved from http://www.coloradoengineeringinc.com/products/Software/Stegi@Work.htm

Dr. Dobb's Journal. (2010). Steganography Detection Tool Released. Retrieved from http://drdobbs.com/parallel/227100488

Forensic Computing Limited. (2004). *Computer Forensic Software Tools*. Retrieved from http://www.forensic-computing.ltd.uk/tools.htm

Fridrich, J., Goljan, M., Hogea, D., Soukal, D. (2003) Quantitative Steganalysis of Digital Images: Estimating the Secret Message Length. *ACM Multimedia Systems Journal*. Special issue on Multimedia Security, vol. 9, no. 3, pp. 288 – 302

Greene, Tim. (April 09, 2010). In Steganography discovery could help data thieves, but also improve radar, sonograms. *Network World.* Retrieved from http http://www.networkworld.com/news/2010/040910-steganography-data-loss.html

Gupta, A., Garg, R. (2008). Detecting LSB Steganography in Images. *Washington University*. from http://www.cs.washington.edu/homes/rahul/data/steg.pdf

Higgans, Kelly. (June 29, 2010). Busted Alleged Russian Spies Used Steganography to Conceal Communications. *Dark Reading*. Retrieved from http://www.darkreading.com/insider-threat/167801100/security/encryption /225701866/busted-alleged-russian-spies-used-steganography-to-conceal-communications.html

Homeland Security Newswire. (2010). In Stealth Data: A new Dimension in PC Data Protection. *Homeland Security News Wire.* Retrieved from

http://www.homelandsecuritynewswire.com/stealth-data-new-dimension-pc-data-protection-Reports.pdf

Hosmer, Chet. (February 2012). Steganography and Smart Phones. *DFI News.* Retrieved from http://www.dfinews.com/article/steganography-and-smart-phones

Huang, D, Yeo, T. (2002). Robust and Inaudible Multi-echo Audio Watermarking. *Proceedings of the IEEE Pacific-Rim Conference on Multimedia*, pp. 615 – 622, Taipei, China

Johnson, Neil. (2011). *Steganography & Digital Watermarking Tools*. In Steganography Software. Retrieved from http://www.jjtc.com/Steganography/tools.html

Jones, Del. (1999). FBI Reports: Spies Cost US $2B Monthly. *USA Today.* Retrieved from http://executiveworldservices.com/pdfs/FBI-Reports.pdf

Judge, James. (2001). Steganography: Past, Present, Future. *SANS InstituteInfoSec Reading Room.* Retrieved from http://www.sans.org/reading_room/whitepapers/stenganography/steganography-past-present-future_552

Kay, Russell. (June 10, 2002). How Steganography Works. *Computer World.* Retrieved from http://www.computerworld.com/s/article/71728/How_It_Works

Kessler, Gary. (April 2002). *Steganography: Hiding Data Within Data.* Retrieved from http://www.garykessler.net/library/steganography.html

Kraetzer, C; Franz, E;Dugelay, JL; Lang, A. (November 2007). Report on Watermarking Benchmarking And Steganalysis. *European Network of Excellence in Cryptology.* Retrieved from http://omen.cs.uni-magdeburg.de/ecrypt/deliverables/DWVL16_final.pdf

Maxemchuk, N.F. (September 1994). *Electronic Document Distribution*. AT & T Technical Journal v 73 no 5 pp 73–80. Retrieved from http://www.ee.columbia.edu/~nick/

Meghanathan, N., Nayak, L. (2010). Steganalysis Algorithms For Detecting the Hidden Information in Image, Audio, and Video Cover Media. *International Journal of Network Security & Its Application, Vol 2, No.1*

National Institute of Justice. (November 5, 2010). Digital Evidence Analysis: Steganography Detection. In NIJ: Research. Retrieved from http://nij.gov/topics/forensics/evidence/digital/analysis/steganography.htm

Norwich University Students. (2011). WetStone Technologies Trait Analytic Profiling Search. In SC Magazine. Retrieved from http://www.scmagazine.com/wetstone-technologies-trait-analytic-profiling-search/review/3470/

NSA. (2012). National Security Agency. In Defending Our Nation. Securing The Future. Retrieved from http://www.nsa.gov/about/values/index.shtml

Petitcolas, FA; Anderson, RJ; Kuhn, MG. (July 1999). Proceedings of the IEEE. In Information Hiding|A Survey. Retrieved from http://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf

Provos, Niels. (2008). Steganography Detection with Stegdetect. *OutGuess.* Retrieved from http://www.outguess.org/detection.php

SANS Institute. (2002). In Steganography: Why it Matters in a Post 911 World. *InfoSec Reading Room.* Retrieved from http://www.sans.org/reading_room/whitepapers/covert/steganography-matters-post-911-world_676

Shachtman, Noah. (June 29, 2010). In FBI: Spies Hid Secret Messages on Public Websites. *Wired.* Retrieved from http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on-public-websites/

Steganography Analysis and Research Center. (2010). StegAlyzerAS. In SARC. Retrieved from http://www.sarc-wv.com/products /stegalyzeras/learn_more.aspx

Steganography Analysis and Research Center. (2010). StegAlyzerSS. In SARC. Retrieved from http://www.sarc-wv.com/products/stegalyzerss/learn_more.aspx

Su,Y., Zhang, C., Wang, L., Zhang, C. (2008). A New Video Steganalysis based on Mode Detection. *Proceedings of the International Conference on Audio, Language and Image Processing*, pp. 1507– 1510

United States of America v. Anna Chapman, and Mikhail Sememko, 18 U.S.C. §,371 2010

University of Rhode Island. (2009). Digital Forensics and Cyber Security Center. In Steganography/Steganalysis Research. Retrieved from http://dfcsc.uri.edu/research/steg

Vatolin, Dmitriy. (2011). Moscow State University. In MSUStego. Retrieved, from http://compression.ru/video/stego_video/index_en.html

Westphal, Kristy. (November 2010). Steganography Revealed. In Symantec. Retrieved from http://www.symantec.com/connect/articles/steganography-revealed-data-in-data

WetStone Technologies. (2012). StegoHunt. Core Capabilities. Retrieved from http://www.wetstonetech.com/product/stegohunt/

WetStone Technologies. (2012). TAPS. In Trait Analytic Profiling Search. Retrieved from http://www.wetstonetech.com/taps.html/

Wu, Jia. (2010). "Steganalysis of MSU Stego Video based on discontinuous coefficient," *Computer Engineering and Technology 2010 2nd Internationl Conference*, pp. 96-99

Zeng,W., Ai, H., Hu, R. (2007). "A Novel Steganalysis Algorithm of Phase Coding in Audio Signal," *Proceedings of the 6th International Conference on Advanced Language Processing and Web Information Technology*, pp. 261 – 264

Zeng,W., Ai, H., Hu, R. (2008). "An Algorithm of Echo Steganalysis based on Power Cepstrum and Pattern Classification," *Proceedings of the International Conference on Information and Automation*, pp. 1667 – 1670