Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):18-24
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

DIGITAL STEGANOGRAPHY AND ITS EXISTENCE IN CYBERCRIME

Natasha Garcia
Utica College, Utica, New York

ABSTRACT

The steganography evolution has been driven by the necessity for hiding a secret communication and eliminating its existence. The communication is conveyed between two parties. As a result, the primary objective with steganography is largely concealing the existence of said communication and protecting the embedded data against any modifications such as compression or format change that may happen during a transmission. As technology is adapting, computer users are seeking opportunities to protect the data they are sending. Digital steganography has had recent exposure due to its use for malicious activity and hiding illegal information across the Internet. The use of steganography online is a new practice and training in the law enforcement field has yet to be fully developed. This paper focuses on the specifications of digital steganography, its involvement in cybercrime, and the training opportunities for forensic examiners and law enforcement.

KEYWORDS: Computer steganography, cybercrime, digital forensics

INTRODUCTION

The creation of steganography has been transformed into the realm of the digital world due to the expansion of computer power, the Internet, digital signal processing (DSP), information theory, and coding theory. Digital steganography has created a climate of corporate cautiousness that has generated various intriguing applications and software; therefore its continuing evolution is ensured. The advancement in digital information has created new challenges for sending information in a secure and safe manner. Whichever method is chosen, the most vital question is its level of security. Various approaches have been created and developed over the years for addressing the issue of information/data security such as cryptography and steganography. This paper outlines the types of digital steganography covers, training opportunities for forensic examiners and law enforcement, and involvement of steganography in cybercrime.

WHAT IS STEGANOGRAPHY?

To understand digital steganography, it is essential to understand the term before its incorporation in technology- steganography. Steganography is the art and science of invisible communication (Sadek, Khalifa, & Mostafa, 2015). The source of the word *steganography* comes from the Greek language. It is derived from two Greek words *stegos* which means "cover" and *grafia* which means "writing" (Sadek et al., 2015). The steganography evolution has been driven by the necessity for hiding a secret communication and eliminating its existence. The communication is conveyed between two parties. As a result, the main objective with steganography is largely concealing the existence of said communication and protecting the embedded data against any modifications such as compression or format change that may happen during a transmission. A fundamental important feature of steganography is perceptual transparency (Sadek et al., 2015).

TECHNIQUES

There have been several methods when discussing digital steganography. However, one of the earliest methods to consider is credited to Charles Kurak and John McHugh, who proposed a method which resembles embedding into the four least significant bits (LSB) (Cheddad, Condell, Curran, & McKevitt, 2010). Both McHugh and Kurak analyzed image downgrading and contamination which is roughly known now as image-based steganography (Cheddad et al., 2010).

More recently in the cyber field, DNA-based steganography techniques have gained traction. The elevated randomness in a DNA sequence can be applied effectively in order to conceal any message or information without being detected. DNA-based steganography has been considered a valuable example of steganographic media, due to its note-worthy storage capacity and the ability to synthesize DNA sequences in any desirable length (Sadek et al., 2015).

Substitution-based techniques replace surplus data of the cover with the intended secret message (Sadek et al., 2015). The primary advantages of the use of substitution-based are the simplistic implementations with the addition of a high capacity for embedding in comparison to other techniques (Sadek et al., 2015). To name a few, substitution-based techniques include several methods such as the most frequent LSB technique, Bit-Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD), and many others (Sadek et al., 2015).

LSB technique is one of the oldest and most famous substitution-based procedures. Not only is it simplistic, but it is also capable of hiding large, hidden messages. LSB operates by replacing a few lease significant bits of pixels from a cover video, for example, with the hidden message bits. The secret message is a colored image of dimensions 670×670, and the cover is an audio video interleave (AVI) home video of a child playing. The video has 14 frames each of dimensions 640×480.

STEGANOGRAPHY COVERS

The majority of digital files can be hidden using steganography covers. However, particular formats have been deemed more appropriate than others for this job. To use file formats with a higher redundancy rate, it is important to note the primary goal of any steganographic technique or method; maximize the hiding capacity and to minimize the embedding distortion (Ballard et al., 2016). The redundant bits of a cover object are bits that can be altered without the adjustment being detected effortlessly (Ballard et al., 2016). Established on the type of the cover object, steganography can be divided into five key categories.

Text steganography is a notable method of steganography. Although text steganography is considered one of the more older methods, modern techniques for text steganography include line-shift encoding, feature specific encoding, word-shift encoding (Sadek et al., 2015). In recent years, text steganography has not been used to the extent that it used to. This is due to the fact that text files have an insufficient amount of redundant data which can, in turn, result in an inadequate amount of hiding capacity. Text files are also known to be easily altered which can lead to the secret message being lost.

Due to a high amount of redundant data, images are the most widespread cover objects used for steganography. In steganography, a digital image is seen as a collection of numbers that

represent different light intensities in various areas of the said image (Sadek et al., 2015). There are numerous types of digital image file formats. The most popular ones to note are Joint Photographic Experts Group (JPEG), Bitmap (BMP) format and Graphics Interchange Format (GIF). Although each format is a digital image, they each rely on different steganographic techniques.

Audio steganography is another type of steganography, and it can be viewed as camouflaging in a one-dimensional signal (Sadek et al., 2015). Audio steganography is able to carry out its purpose of hidden communication through the help of the masking phenomenon. This phenomenon suggests that if a loud audible sound exists, a lower audible sound will become inaudible. Examples of audio encoding techniques are phase coding and low-bit encoding.

Video steganography is considered an extension of the digital image steganography. A video stream involves a series of still images that are successive and uniformly spaced. This stream can be accompanied by audio as well. With these factors in mind, many steganographic techniques that are used with images can be applied to videos too. Video files are a favorable type of cover since it can carry a significant amount of data for hidden messages. Although there is more focus on digital images when it comes to steganography, video steganography is starting to evolve due to the repeated use and popularity of videos over the Internet.

Another type of steganography that is worth an honorable mention is protocol steganography. This type of object refers to the implantation of hidden information within a series of network packets. There are hidden channels in Open Systems Interconnection (OSI) network model layers where steganography can be put into place. Steganography can be implemented in the header of the Transmission Control Protocol/ Internet Protocol (TCP/IP) packet to hide data. The idea of retransmission steganography was also presented during a workshop that included a successfully received packet that was intentionally not acknowledged to invoke retransmission (Ahsan & Kundur, 2002). The retransmitted packet carried the secret message as opposed to the original data.

CASES INVOLVING DIGITAL STEGANOGRAPHY

Unfortunately, these object types and techniques can be used for wrongdoing. Cybercrime has proven to be the number one benefit from this digital revolution with steganography. An immediate concern was shown on the possible utilization of steganography by terrorists following a report in *USA TODAY* in 2001 (Cheddad, Condell, Curran, & McKevitt, 2010). The report stated that there was an influx of statements that Osama bin Laden and his al-Qaeda network had been communicating through secret messages on favorable websites (Cheddad et al., 2010). Niels Provos and Peter Honeyman, at the University of Michigan, inspected and analyzed over three million images from top websites looking for any trace of steganography (Cheddad et al., 2010). They were not able to find a single hidden message. Although Provos and Honeyman attributed several reasons for this result, it should be noted that steganography does not exist solely in still images. Embedding hidden messages into video and audio files have also been possible.

In 2010, a Russian spy ring conversed and connected by posting images encoded with secret messages to public websites (Stier, 2010). The Department of Justice (DOJ) recovered over one hundred messages that were concealed within online pictures. These online pictures were then linked to mentioned Russian spy group. After an image containing hidden data was posted online, the receiving Russian party then downloaded the image using steganography software to

interpret it. The spy group posted pictures to the Internet using websites such as eBay and took advantage of the fact that it is difficult to determine who precisely the pictures are for (Stier, 2010). The websites used were public websites that millions of computer users might visit, but only the Russians in the spy group would know that particular images contain hidden data. The numerous amount of pictures on the websites used also made the investigation challenging to find the images that contained the concealed messages between the spy ring.

In June of 2010, the Federal Bureau of Investigation (FBI) detained 11 Russian spies who were using digital steganographic technology to communicate amongst each other stealthily (Bell, 2015). Similar to the mentioned Russian spy ring, these Russian spies used images to communicate and transfer hidden text files. Investigators were able to conduct a search and find the 27-character password the spies were using as well as the steganographic software. Officials found the mentioned password on a piece of paper in one of the suspect's houses. With this discovered password, more than 100 text files were revealed and analyzed. Officials also noted that the spies made another mistake. The steganography software used by the spies were not commercially accessible. The software was developed in Moscow, allegedly linking the spies to the Russian Foreign Intelligence, Sluzhba Vneshney Razvedki (SVR) (Bell, 2015). An investigator stated in the report that the software was easily accessible on the confiscated computers. The steganography software was accessed by pressing *Ctrl + Alt + E* and the 27-character password was then entered (Bell, 2015).

In 2011, a suspected al-Qaeda member was arrested in Berlin, Germany in May. This suspect was he found with a memory card with a password-protected folder. Examiners discovered hidden files were contained in the protected folder. However, as the German newspaper *Die Zeit* reported, digital forensics examiners from the German Federal Criminal Police (BKA) claimed to have eventually uncovered its contents (Gallagher, 2012). The examiners reported that a video was uncovered and appeared to be a pornographic video. Within that video, forensic examiners were able to reveal 141 separate text files (Gallagher, 2012). They claim that the documents contained details regarding al-Qaeda operations and future operating plans. Among these documents were three documents labeled "Future Works," "Lessons Learned," and "Report on Operations" (Gallagher, 2012).

A Russian hacker group named Advanced Persistent Threat (APT) 29, used steganography in 2015 to disguise communication within pictures on GitHub (Bell, 2015). Specific instructions were given to infected machines to check various Twitter accounts. Every time a tweet was displayed, the malware located on the machines would be activated (Bell, 2015). A network security firm by the name of FireEye discovered the malware and a steganography technique the hacking group was able to implement. In their report, FireEye called the malware tool Hammertoss and admitted that hackers have become "more sophisticated with their ways to stay hidden" (Bell, 2015). APT29's tool Hammertoss consisted of several malware techniques as well as steganography techniques to accomplish its laden objectives.

In July of 2002, the European Police Office (Europol) exposed a pedophile group named the "Shadowz Brotherhood" (Wingate, 2006). Members of this group were reported to be concealing obscene material containing children in seemingly innocent image files. Although media outlets did not reference steganography as the main topic of the investigation, officials explained that one or more steganographic applications were used to hide the child pornography in the images and distribute them (Wingate, 2006).

TRAINING

It has been stated that digital steganography continues to find its way in child pornography cases as well as overseas incidents. However, despite the cases such as Hammertoss, the Shadowz Brotherhood, and possibly other cases that have not been the focus of public attention, the question of whether digital steganography is a danger continues to be a paradox. In recent years, the number of computer forensic examiners interested in specializing in digital steganography has decreased due to the fact that it has not been proven to be an immense threat in cybercrime (Sadek, Khalifa, & Mostafa, 2015). In order to continue research and prove that digital steganography is, indeed, a threat, forensic examiners need to have access to digital steganography training and shed light on research and information regarding the topic. Steganography has been used in various formats since the times of ancient Greece. However, digital steganography currently has a relatively low visibility to law enforcement agencies on the frontline (Bell, 2015).

When a case that involves digital steganography arises, managers should be mindful that law enforcement investigators and information technology (IT) staff may not have the expertise that a digital forensic professional could have. Creating training tools and material can be considered daunting. A suggested starting point is to begin the search for major commercial steganography vendors and combine the tools with information from the Steganography Application Fingerprint Database and the National Software Reference Library (Warkentin, Bekkering, & Schmidt, 2008). Whether the training is for law enforcement officials or examiners beginning their digital forensic careers, these sources can provide the proficiency to detect and decipher steganographic data.

It is important to consider that the criminals using digital steganography as a means to commit cybercrime are not to be defined as amateurs. The presence of steganographic software on a user's computer alone could have private or professional consequences. Known IT and Security companies have taken the extra step and offer steganography tools and training to increase exposure to digital steganography.

Digital forensic examiners that are familiar with EnCase have a steganographic application in their forensic workstation. Examiner can import a library or build their own library of hash sets (in this particular situation, a steganography software) with the library feature in EnCase. The hash sets are then used to identify the steganographic file matches (SANS Institute, 2003).

Black Hat offers a digital steganography course for examiners to practice with modern steganographic tools and techniques (Black Hat, 2007). This hands-on course also provides trainees with experience in the latest investigation methods such as analyzing and recovering hidden data in various cover types. Examiners that train with Black Hat will also be exposed to subject matter such as children exploitation, terrorists and criminal organizations that use the Internet as their means of communication, and corporate insiders.

Training courses such as the classes that Black Hat offer students the opportunities to learn detection, analysis, cracking, and recovery of hidden information. In laboratory settings, examiners are introduced to the newest and digital steganographic software where instructors can demonstrate and define their use in today's cases. Other companies such as Backbone Security and Alpine Security, emphasize the need for understanding how video/image data embedding work as well as the concept of TCP/IP covert channels (Warkentin et al., 2008). The training and

tools are present in the digital forensic community, but it is imperative that the opportunities be taken to crack down on digital steganography.

CONCLUSION

Steganography is the science of concealing data within data. Although digital steganography is becoming more progressive, it is still a topic in science that is not well-known. Steganography has a promising future on the Internet and, in turn, may spark the need for additional research and resources to combat it. This argument is the reason why law enforcement officials must persistently stay well-informed in this area of technology; there will always be a new program ready to obstruct their efforts. Law enforcement is not the only ones that are faced with this responsibility. Digital steganography also presents new challenges for security and cybersecurity personnel, enterprise managers, courts systems, and lawmakers. Future research of digital steganography and steganalysis should always be encouraged for both academics and specialists.

REFERENCES

1. Ahsan, K., & Kundur, D. (2002). Practical data hiding in TCP/IP. *ACM Multimedia and Security Workshop*. The Special Interest Group of Multimedia.
2. American Psychological Association. (2013). *Publication manual of the American psychological association* (Sixth ed.). Washington DC: American Psychological Association.
3. Ballard, J., Hornik, J., & McKenzie, D. (2016). Technological facilitation of terrorism. *American Behavioral Scientist, 45*(6), 989-1016.
4. Bell, R. (2015). Digital steganography: Its impact on mobile forensics, hacking, and social media. *ProQuest Dissertations Publishing*, 25-35.
5. Black Hat. (2007). *Discover the hidden – steganography investigation training*. Retrieved from https://www.blackhat.com/html/bh-usa-07/train-bh-us-07-ws-stego.html
6. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010, March). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752.
7. Gallagher, S. (2012, May 02). *Steganography: how al-Qaeda hid secret documents in a porn video*. Retrieved from https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/
8. Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2015, September). Video steganography: a comprehensive review. *Multimedia Tools and Applications, 74*(17), 7063-7094.
9. SANS Institute. (2003). *Steganalysis: Detecting hidden information with computer forensic analysis*. Retrieved from https://www.sans.org/reading-room/whitepapers/stenganography/steganalysis-detecting-hidden-information-computer-forensic-analysis-1014

10. Stier, C. (2010, July 02). *Russian spy ring hid secret messages on the web*. Retrieved from https://www.newscientist.com/article/dn19126-russian-spy-ring-hid-secret-messages-on-the-web/
11. Warkentin, M., Bekkering, E., & Schmidt, M. B. (2008). Steganography: Forensic, security, and legal issues. *Journal of Digital Forensics, 3*(2), 17-34.
12. Wingate, J. E. (2006). *Digital steganography: threat or hype?* Retrieved from http://www.infosectoday.com/Articles/digitalstego.htm#author