Research Paper

Volume : 4 | Issue : 12 | December 2015 • ISSN No 2277 - 8179

Steganography and Terrorism

Computer Science

KEYWORDS : Cover Message, Digital Watermarking, Information hiding, Secret Message, Steganalysis

Rajinder Singh Minhas Department of Computer Science, M.L.U.D.A.V. College, Phagwara, Punjab, India.

ABSTRACT

What the increase in popularity of internet due to its ease of use, cost and availability, there occurred an increase in development of methods to exchange valuable information securely over this publicly open channel. Steganography is a method of securing data by obscuring the context in which it is transferred; you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing the existence of the secret message. Theory and techniques behind steganalysis is also discussed in this paper. Misuse of steganography in terrorist activities along with various articles and surveys are also emphasized.

Introduction

Information hiding was not taken care by research community and industry until early nineties. But with time, its need was felt and the first academic conference on the subject was organized in 1996. After that it has become a hot topic of research and application. The main scope of this research filed includes protecting copyright of audio, video and other works become available in digital form. It has been renamed as 'watermarking' (hidden copyright messages) and 'fingerprinting' (hidden serial numbers or a set of characteristics that tend to distinguish an object from other similar objects). The theme behind this is that the latter can be used to detect copyright violators and the former to prosecute them.

What is Steganography?

With the increase in popularity and use of internet and information, data has become more and more valuable. People started exchanging large amount of confidential and valuable data over the internet which is open to public. The cost-effectiveness and wide availability of internet is the reason for its popularity. So, digital watermarking came into existence. But with time, techniques for hiding watermarks became more sophisticated and robust to cryptographic attack. But as human has the tendency to break anything kept secret, so it is realized that the security must be kept secret i.e. invisibly secure. As a result Steganography came into existence. Steganography is a method of securing data by obscuring the context in which it is transferred. This word comes from the Greek *steganos* (covered or secret) and – *graphy* (writing or drawing) and literally means, covered writing [1]. The unused, useless, redundant or unnecessary bits of the original file are used to create a watermark by replacing them with bits of critical information. Steganalysis is science of detecting Steganography. The process of Steganography includes the original file called **cover media** [2] containing the hidden information and is combined with the **secret message** to create the **stego-carrier/ stego-medium** which is the modified carrier file containing the hidden information. Extra measures could also be taken by using **stego-key** which is a secret password to take extra measure against steganalysis attacks. The process is detailed in Figure 1.

The sensitive information is hidden behind an innocent looking document that is not undetectable to human eye. It has been found to be used in nefarious applications for hiding records of illegal activity, financial fraud, industrial espionage, and communication among members of criminal or terrorist organizations. It has also been observed to be used by terrorists involved in 11 September 2001 demolition of World Trade Centre [3].

Steganalysis

Steganalysis is the field of research that deals with the detection and recovery of hidden information. It is an art and a science [4]. The art side of steganalysis helps to select features or characteristics of a typical stego message while the science side helps in reliably testing the selected features for the presence of hidden information. It includes two steps.

Figure 1: Process of Steganography

The detecting phase to detect unusual, repetitive patterns and unused areas in a file. It could be 'perceptible noise' that is detectable when embedded information distorts sounds or images [5] or unusual color schemes and patterns in image.

Embed phase in which the information is embedded by exploiting this detected information [6].

With promotion in Steganography, its counters are also rising. The **Steganography Analysis and Research Center** is a Center of Excellence within Backbone Security focused exclusively on steganography research and development of steganalysis products and services [7]. Some of these are discussed below.

Steganography Application Fingerprint Database: The main purpose of SARC is to collect steganography, watermarking, and other data-hiding applications from various sources and review them on seized media by matching file profiles in the SAFDB which is the most extensive steganography hash set publicly available. These hash values could be used to determine the presence of a steganography

Steganography Analyzer Artifact Scanner (StegAlyzerAS) It gives the capability to scan the entire file system, or individual directories, on suspect media for the presence of steganography application artifacts. This forensic tool performs an automated or manual search of the Windows Registry to identify if Registry keys are available that are associated with a particular steganography application.

Steganography Analyzer Signature Scanner (StegAlyzerSS) It provides the capability to scan the suspected file for the presence of hexadecimal byte patterns, or signatures, of particular steganography applications in the files.

Steganography Analyzer Real-Time Scanner (StegAlyzerRTS) It has the ability to commercially provide network security by detecting the fingerprints and signatures of digital steganography applications in real-time.

Although these are not full proof methods but these could be further enhanced for total steganlysis. One of the steganography detection framework developed by [8] is discussed below.

- A web crawler that saves JPG images.

- Its output is piped into stegdetect, a tool for automatic detection of steganographic content.
- The positive results are distributed to a loosely couple cluster of workstations with disconcert. *Disconcert* provides a distributed computing framework for loosely-coupled workstations. It is meant to distribute problems that are inherently parallel, like dictionary attack on keys or passwords.
- On the clients, stegbreak is used to launch a dictionary attack against the positive images. A normal stegbreak job runs on a few hundred clients.

Steganography and Terrorism

As Steganography has the ability to hide secret message, it has been inclined by terrorists too. It is difficult to verify these claims. Large numbers of steganographic tools are freely and easily available that is used by the terrorists for ill deeds.

A terrorist needs a stego (carrier that could be used to carry information), a message and it is emailed or post to a publicly available site. The same pass phrase and software are used by the sender and receiver of the message. Because steganography is not known to non-technical common people and technologically viable images are available on internet in abundance, there is a high chance of message to reach its destination unnoticed. It is this ease to use of this technology that it is becoming favorite tool for terrorists. This flexibility has made steganography problematic for digital forensics investigators and prosecutors. A cloudless blue sky over a snow covered ski paradise or a waterfall in a forest are possible targets of Steganography. A large number of such images are available on internet which even worsens the situation

According to an article "Are terrorists using hidden **messages?" by Duncan Campbell 31.10.2001, the media and some western government agencies have repeatedly suggested that the Al network organizes terror using hidden messages sent through the media and on the internet. In this article,** a web site has been introduced where Dr Koontz has used Steganalysis to inform about the planned new attacks [9].

These days government agencies especially in USA are funding many experts to work on steganalysis. University of Delaware research team has received National Science Foundation funding to combat terrorism by developing techniques to detect the use of steganography, which encompasses various methods of hiding messages in apparently ordinary digital images and videos. This is what is the need of the hour.

Conclusion

Steganography is a powerful tool that has enabled people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. It has advanced a lot in past few years. With advancement in techniques and applications of Steganography, the rescue has also been advanced. Number of techniques for Steganalysis has been discussed in this paper. Use of Steganography for terrorism has also been discussed with its possible consequences.

REFERENCE

[1]. Krenn, R. (2004). Steganography and steganalysis. Retrieved September, 8, 2007. [2]. Komathi, A., Revathy, M., Sivasankari, K., & ME, M. K. S. Steganographic Techniques of Data Hiding using Digital Images. [3] Chanu, Y. J., Tuithung, T., & Manglem Singh, K. (2012, March). A short survey on image steganography and steganalysis techniques. In Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on (pp. 52-55). IEEE. [4] Are terrorists using hidden messages? By Duncan Campbell 31.10.2001. Available at: http://www.heise.de/tp/artikel/11/11027/1.html (Accesssed on 25.08.2015). [5] Katzenbeisser, S., & Petitcolas, F. (2000). Information hiding techniques for steganography and digital watermarking. Artech house. [6] Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. International Journal of Computer Science and Security (IJCSS), 6(3), 168-187. [7] SARC - Steganography Analysis and Research Center. https://www.sarc-wv.com/ (Accessed on 18.09.2015). [8] Ker, A. D., Bas, P., Böhme, R., Cogranne, R., Craver, S., Filler, T., ... & Pevný, T. (2013, June). Moving steganography and steganalysis from the laboratory into the real world. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 45-58). ACM. [9] Clarke David "Technology and Terrorism". New Brunswick: Transaction Publishers, 2004, pp 178.