ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Steganography: Exploring an ancient art of Hiding Information from Past to the Future

Govinda Borse, Vijay Anand, Kailash Patel

Abstract— In today's world, keeping the information secure is very important. Steganography is one of the techniques used to keep the information secure. It is the art of hiding information in various ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "Covered Writing." It includes a large collection of various methods that conceal the message's very existence. These methods include invisible inks, tiny pin punctures on selected words, digital signature, microdots, character arrangement, covered channels & spectrum communications. With the systems based on computers, Steganography refers to the ability to hide one file inside the other file. In this paper various steganographic methods used to hide the information or any secret message from past to the future are included.

Index Terms—**Steganography, Ciphertext**

I. INTRODUCTION

The Steganography term refers to the art of covert communications. A rough Greek translation of the term Steganography is secret writing. The Steganography technique can be implemented in secure communication where a person can send a secret message to another person in such a way that no-one else will know that the message exists. Typically in this technique, the message is embedded within another object known as cover work, by tweaking its properties. Briefly stated, Steganography is the term applied to many number of processes that will hide a message within an object, where the hidden message will not be apparent to an through hiding information in other information, thus hiding the existence of the communicated information. The word Steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image Steganography the information is hidden exclusively in images. Steganography & cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

II. PAST OF STEGANOGRAPHY

Johannes Trithemius (1462-1516) was a German Abbot. His writing, "Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" is ostensibly a work describing methods to communicate with spirits(2). A very rough translation of this Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men. Published as a trilogy in Latin, the first two parts of his works are apparently some of the first books on cryptology describing methods to hide messages in writing. The third part of the trilogy is outwardly a book on occult Astrology. The third book contains a number of tables containing numbers. This technique has been using in various applications like military, diplomatic, personal & intellectual property applications.

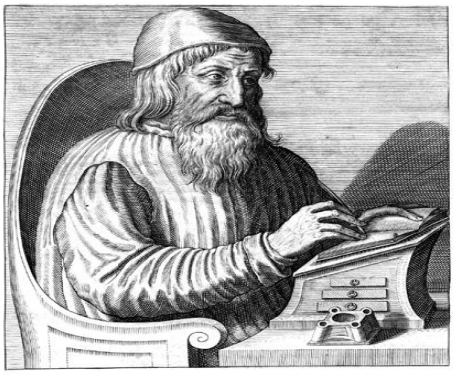

Fig 1: Johanes Trithemius [1]

Steganography is the art and science of invisible communication. Although "Steganographia" is the work that we derive the term steganography from, it is certainly not the first example of hidden writing. There are examples from history that serve to illustrate the desire to hide messages or some type of intelligence from others. Mary Queen of Scots used a combination of cryptography and steganography to hide letters. Her letters were hidden in the bunghole of a beer barrel, which freely passed in and out of her prison. Other uses of steganography weren't limited to normal writing materials. One may consider the huge geoglyphs of the Nazca in Peru to be a form of steganography. The geoglyphs are obviously open to view, yet many of the images were not detected until viewed from the air. Human vectors include the efforts of Histaiacus in the 5th century BC. Histaiacus shaved the head of a messenger, wrote a note encouraging Aristagoras of Miletus to revolt against the king of Persia. After the messenger's hair grew back, the messenger was dispatched with the message. Obviously, this message wasn't especially time constrained. Another human vector example includes writing messages on silk, which would then be compressed into a ball and covered with wax. The messenger would swallow the wax ball. The method of retrieval was not described in my source. In 480 BC a Greek by the name of Demaratus sent a message to the Spartans warning of a pending invasion by Xerxes. Heroclotus described the method used by Demaratus : *"As the danger of discovery was great, there was only one way in which he could contrive to*

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

get the message through: this was by scraping the wax off a pair of wooden folding tables, writing on the wood underneath what Xerxes intended to do, and then covering the message over with the wax again. In this way the tablets, being apparently blank, would cause no trouble with the guards along the road…."

Fig 2: Demeratus [1]

In more recent history, several stenographic methods were used during World War II. Microdots developed by the Nazis are essentially microfilm chips created at high magnification (usually over 200X). These microfilm chips are the size of periods on a standard typewriter. These dots could contain pages of information, drawings, etc. The Nazis also employed invisible inks and null ciphers. One steganographic method employed by the United States Marines during World War II, was the use of Navajo "code talkers." While the code talkers employed a simplistic cryptographic technique, the messages were sent in clear text. Another example of steganography involves the use of the Cardano grill. This device, named after its inventor Girolama Cardano, can be as simple as a piece of paper with holes cut in it. When the grill is laid over printed text, the intended message can be retrieved. In techniques related to the Cardano grill, classical steganography techniques include pin punctures in text (e.g. newspapers), and overwriting printed text with pencil. These are the various techniques in Steganography those were used in the past to hide the message.

III. PRESENT OF STEGANOGRAPHY

Now days the technologies used in Steganography are quite different. The main focus has been given to the various forms of digital Steganography. The current digital Steganography includes various text files, still images, moving images, sound etc. Today all the available digital files can be used for the purpose of hiding message in Steganography. But the file format having more redundancy is mostly suitable for this. We can say redundancy as the bits of an object that provide more accuracy. The redundant bits of an object can be altered without the alteration being detected easily. Mostly image & audio files complete this requirement while research will also uncover some other file formats that can be used for information hiding. Text Steganography is the most important Steganography used to hide text message. The basic method to do is to hide a secret message in every n^{th} letter of every word of a text message. Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

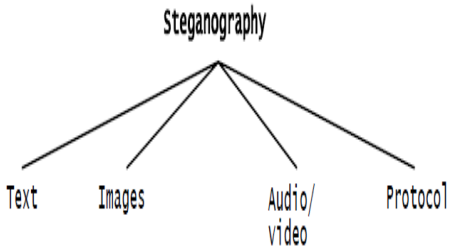

Fig 3: Categories of Steganography

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

IV. FUTURE OF STEGANOGRAPHY

Now a day's many researchers are working in the field of Steganography to find the new ways to keep the message secure. Researchers are spending too much time in inventing new platform from the current platform. The traditional categories of Steganography like Text, Images, Audio/Video, Protocol etc are being analyzed & experimented by the researchers to innovate the new method. Such research efforts have rekindled the research and development efforts oriented towards steganography platforms and steganalysis and a number of researchers are working towards discovering new platforms that miscreants could potentially use to hide information. For instance, researchers have shown that voice over Internet protocol (VoIP) could emerge into a popular platform for steganography owing to its ubiquity and the difficulty in detecting hidden information in VoIP streams. In addition to VoIP, platforms such as images and other multimedia content are expected to be widely used for concealing information. "Current research in steganography is focused on identifying various platforms through which one can hide information,' notes the analyst of this research service. "Apart from the traditional platforms such as audio, video, and images, researchers are looking for additional platforms through which information can be hidden." An interesting idea under consideration is to have a separate

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

steganographic channel in a network to send messages. Although each mode has many benefits, it is very difficult to ascertain the single best platform to send hidden messages. Steganography is capable of mitigating piracy by aiding copyright marking. In the future, digital camera manufacturers could implement steganographic features as a part of camera firmware to annotate pictures with the photographer's copyright information. Camcorder manufacturers could also follow suit and implement steganography and watermarking techniques for protecting video content captured on camcorders and video cameras. Going forward, legitimate applications such as tagging of multimedia content with hidden information could become an important application area for steganography.

V. LITERATURE SURVEY

In 2001, James C. Judge et al [1] proposed that steganogaphy has been used in various forms for 2500 years. Two researchers, Dr. Thomas Earnst & Dr. Jim Reeds et al [1] convinced regarding the history of Trithemius. They convinced that the third tome contained hidden code. Dr Ernst, while a graduate student at the University of Pittsburgh published a 200 page paper, but it was written in German, published in 1996 in a Dutch Journal Daphnis, and attracted little attention. Dr. Reeds, a mathematician at AT&T Labs independently began delving into this tome. As he searched for information on Trithemius' works, he discovered Dr. Ernst paper. VenkatramanS., Abraham A. & Paprzycki, M et al[2] have given an overview of image steganography. Thay have attempted to identify the requirements of a good steganographic algorithm & reflected which steganographic algorithms are more suitable for which application.

VI. CONCLUSION

In this way steganography, an art of hiding message has been in use from thousands of years. But according to time the techniques used behind it is changing.

REFERENCES

[1] James C Judge "Steganography- Past, Present, Future" SANS Institute, InfoSec Reading Room, SANS Institute 2001.

[2] Venkatraman S., Abraham A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.

[3] U. B. Pfitzmann, "Information Hiding Terminology," Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin, 1996, pp. 347-356.

[4] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[6] Chandramouli R., Kharrazi, M. & Memon N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[7] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.

[8] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.

[9] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.

[10] Chandramouli R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[11] Johnson N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[12] Venkatraman S., Abraham A. & Paprzycki M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.