International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Challenges in Steganography

MR Seshan Ram[1]

[1]Assistant professor, Dept. of Computer science, Shri Krishnaa College of Engineering, Pondicherry-605501

Abstract— The primary reason for selecting steganography among the list was due to the unfamiliarity of the word that twigged an interest in the subject. that claims terrorists, may be using steganography to communicate with each other in planning terrorist attacks. It is thought that images with hidden messages are placed on bulletin boards or dead drops for other terrorists to pick up and retrieve hidden messages. Thus far, this supposition has yet to be proven. The goal of the manuscript is to of steganography, mainly focused on embedding text data in digital images.

Keywords—steganography, encryption, cipher, TCP/IP, cryptography

I. INTRODUCTION

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction. Watermarking has the feature of robustness against attacks. Even if the existence and method of embedding the data is known, it may be difficult to destroy the hidden data. Data hiding and data embedding can be classified as methods between steganography and watermarking.

II. RESEARCH METHODOLOGY

The primary tool used in the research of steganography and watermarking is the Internet. The first objective was to understand the various terminologies related to the field. This was done through the Wikipedia and the hyperdictionary websites.

Additional technical details were obtained from various articles listed under the References and Bibliography section. The following points can be attributed to the renaissance of steganography: Government ban on digital cryptography. Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy. The increased need to protect intellectual property rights by digital content owners, using efficient watermarking. The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, steganographic software is becoming effective in hiding information in image, audio or text files.

III.RESOURCES

It was determined at an early stage of the requirements gathering that the paper will focus primarily on steganography for embedding text information in computer images. The steganography techniques covered include least significant bit insertion, masking and filtering, and algorithms and transformations. The paper does not cover other steganography techniques such as distortion, spread spectrum steganography, and statistical steganography.

Since “information hiding” refers to both watermarking and steganography, digital watermarking is briefly mentioned in the tutorial. As well, the paper contains a section on steganalysis.

Two steganographic program examples were selected from the Internet to include in the tutorial.

JPHS (Jpeg hide and seek) is a free program designed by Allan Latham.

4t HIT Mail Privacy LITE 1.01 is a tool provided free of charge by 4t Niagara Software.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Design

The tutorial is written in HTML. The main page is the *menu.htm* file. The tutorial was designed for easy navigation. An attempt was made to achieve a concise tutorial on the subject of steganography without losing the reader with excessive technical detail on the steganographic techniques.

B. Scheduling

The paper requirements and design were made exclusively by the single resource. Since the paper did not involve group dynamics the paper schedule was fairly well paced.

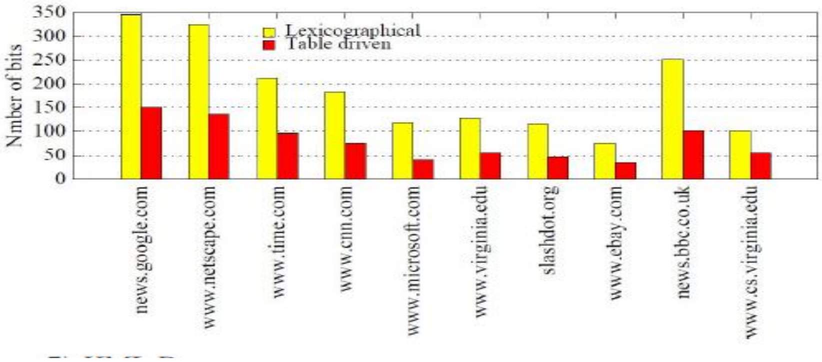
C. Steganography for Computer Images

The challenge of using steganography in computer images is to hide as much data as possible with the least noticeable difference in the image. There are a number of steganographic methods and applications available for download on the Internet.
In general, the steganography process consists of the following steps:

1) Identifying redundant bits in a cover image.
2) Selecting a subset of the redundant bits to be replaced with the secret message. The stego image is created by replacing these redundant bits with the message bits.

Information hidden by setting the least significant bits of the image pixels to the bits of the secret data may be invisible to the human eye but it is relatively easy to detect and remove by a third party who suspect the presence of the embedded data.
Steganography is more noticeable with JPEG images due to the lossy compression algorithm used in JPEG files. There may be a significant difference between the file size of the cover image and the stego image. The algorithm used also affects the probability of detection of the steganography. An algorithm used to hide large amounts of information typically result in greater change to the image appearance.

Fig1: No. of bits vs LXP



D. More Recent Use of Steganography

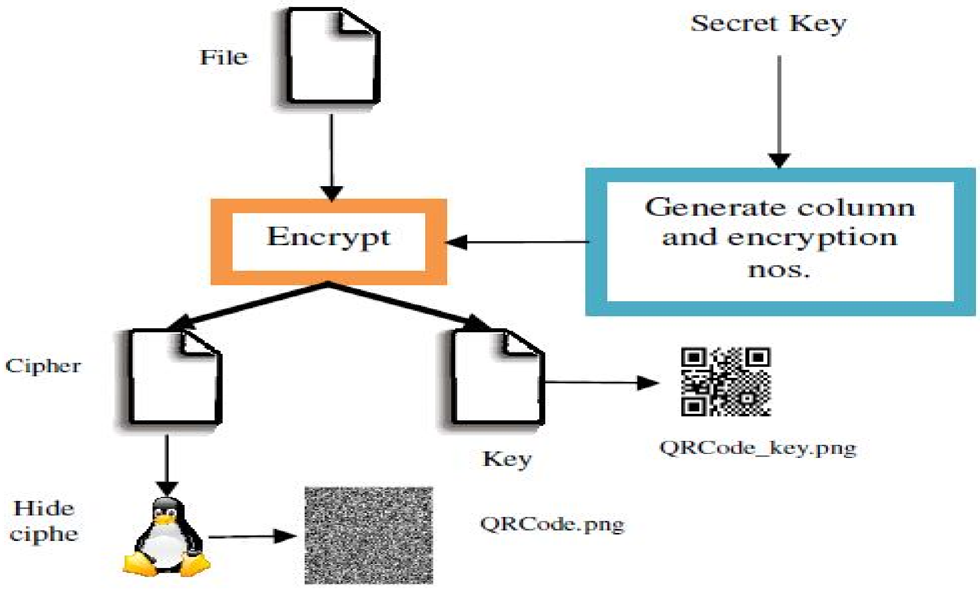
A more recent use of steganography is in the design of covered channels in TCP/IP for thwarting filters and firewalls.
The following is a simple explanation of the build-up of a TCP/IP connection:
For each connection there is a send sequence number and a receive sequence number. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of it in acknowledgment from the other side. Each side must receive the other side's initial sequence number and send a confirmation acknowledgment.

1) A --> B   SYN my sequence number is X
2) A <-- B   ACK your sequence number is X
3) A <-- B   SYN my sequence number is Y
4) A --> B   ACK your sequence number is Y

Since step 2 and 3 can be combined in a single message this is called a three-way handshake. In this three-way handshake hidden data can be embedded in the packet header.

For example, host A sends a synchronization package and an initial sequence number to host B requesting acknowledgement. Host B answers with an initial sequence number increased by one and its acknowledgement. The connection is established by the acknowledgement from host A to host B. By embedding hidden identification information in the header data it is possible to create a 'bounce' effect. Host A sends the package to host B, but this time, due to the hidden data in the header, host B sends the acknowledgement that was meant for host A to host C. Host C can establish the connection anonymously without host B knowing that host C is not host A.

Figure 2: Encoding Model



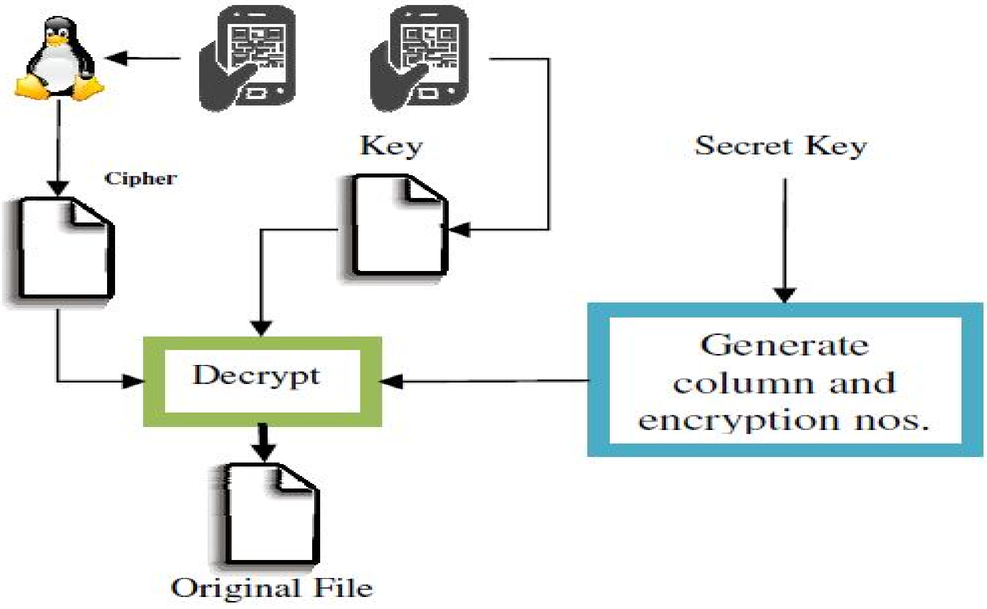


Figure 3: Encoding Model

IV. CONCLUSION

Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected.

Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage. Digital watermark technology is currently being used to track the copyright and ownership of digital content. Efforts to improve the robustness of the watermarks are necessary to ensure that the watermarks and embedded information can securely defend against watermarking attacks. With continuous advancements in technology it is expected that in the near future more efficient and advanced techniques in steganalysis will emerge that will help law enforcement to better detect illicit materials transmitted through the Internet. This paper ntroduces a tiny part of the art of steganography. Steganography goes well beyond simply hiding text information in an image. Steganography applies not only to digital images but to other media as well, such as audio files, communication channels, and other text and binary files.

REFERENCES

[1] F. Djebbar and B. Ayad, "Audio Steganograpgy by Phase Modification" The Eighth International Conference on Emerging Security Information, Systems and Technologies, 2014.

[2] F. Djebbar, B. Ayad, K. A Meraim and H. Hamam," Comparative study of digital audio steganography techniques", Journal on Audio, Speech, and Music Processing, 2012.

[3] H.I. Shahadi, R. Jidin and W.H. Way, "Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key," Indian Journal of Science and Technology, Vol 7-No. 3, March 2014.

[4] H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study", Journal of Global Research in Computer Science, vol. 3 (12), December 2012.

[5] K. Cho, S.H Bae, I.K Choi, N.S Kim, and M. Unoki, "Robust Audio Data Hiding Method Based on Phase of Modulated Complex Lapped Transform", Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing IEEE, 2013.

[6] K. Kaur and D. Verma, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4 (1), January 2014.

[7] Anjali A. Shejul, Prof. U. L. Kulkarni, “A DWT based Approach for Steganography using Biometric”, International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.

[8] Provos N. and HoneymanP, “Hide and Seek: An Introduction to Steganography”, IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.

[9] ShavetaMahajan, Arpinder Singh, “A Review of Methods and Approach for Secure Steganography”, International Journal of Advanced ResearchComputer Science and Software Engineering, vol 2, issue 10, pp. 67-70, October 2012.

[10] K. Gopalan. , “Audio steganography using bit modification”, IEEE International Conference on Acoustics, Speech, and Signal Processing,(ICASSP ’03), vol2, pp. 6-10, April 2003.