


How to win a CTF competition

Step 1. Have at least 20 yrs of experience in the field.

Step 2. Bribe the authors.

Step 3. Cheat and steal flags.

Step 4. If you are still thinking this is true, go back to step 1.

What is Steganography exactly? It is just the art of .

Who invented it? Some Greek guys share stories of sending messages in the form of tattoos on the scalp of slaves. Don't trust me? Check out this [link](#).

.

Next, I would like to show you some documentation about steganography.

ABSTRACT

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic technique.

KEYWORDS

Steganography, Steganalysis, Digital watermarking, Stego key, Stego image and Cryptography.

1. INTRODUCTION

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. A solution to this problem is steganography. The ancient art of hiding messages so that they are not detectable. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

Before the invention of digital means, traditional methods were being used for sending or receiving messages. Before phones, before mail messages were sent on foot. For the messages where privacy was of prime concern, the ways of implementing security were following:

1. Choosing the messenger capable of delivering the message securely.
2. Write the message using such notations that actual meaning of the

message was concealed.

3. Hide the message such that even its presence can't be predicted.

In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier.

Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image.

A possible formula of the process may be represented as: cover medium + embedded message + stego key = stego-medium

Figure 1.1 Graphical Version of the Steganographic System

fE : steganographic function "embedding"

fE-1 : steganographic function "extracting"

cover: cover data in which emb will be hidden

emb: message to be hidden

stego: cover data with the hidden message

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of our cat could conceal the plans for our company's latest technical innovation.

2. HISTORY OF STEGANOGRAPHY

It is believed that steganography was first practiced during the Golden Age in Greece. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax.

An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, International Journal of Computer Applications (0975 – 8887)

Volume 9– No.7, November 2010

20

giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax.

Later on Germans developed microdot technology which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage. Microdots are photographs the size of a printed period

regarding trade secrets or new product information.

6. The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

Figure 3.2 Steganography on the Internet

4. STEGANOGRAPHY AND

CRYPTOGRAPHY

4.1 Comparison of Steganography and Cryptography

Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

International Journal of Computer Applications (0975 – 8887)

Volume 9– No.7, November 2010

21

4.2 Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium.

In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

5. STEGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if

possible, recover the hidden information. Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message.

Figure 1. A Graphical Version of the Steganographic System

Steganalysis generally starts with several suspect information streams but uncertainty whether any of these contain hidden message. The steganalyst starts by reducing the set of suspect information streams to a subset of most likely altered information streams. This is usually done with statistical analysis using advanced statistics techniques.

6. STEGANALYSIS TECHNIQUES

Hiding information within an electronic medium cause alteration of the medium properties that can result in some form of degradation or unusual characteristics.

6.1. Unusual patterns

Unusual patterns in a stego image are suspicious. For example, there are some disk analysis utilities that can filter hidden information in unused partitions in storage devices. Filters can also be used to identify TCP/IP packets that contain hidden or invalid information in the packet headers. TCP/IP packets used to transport information across the Internet have unused or reserved space in the packet headers.

6.2. Visual detection

Analyzing repetitive patterns may reveal the identification of a steganography tool or hidden information. To inspect these patterns an approach is to compare the original cover image with the stego image and note visible differences. This is called a known-carrier attack. By comparing numerous images it is possible that patterns emerge as signatures to a steganography tool. Another visual clue to the presence of hidden information is padding or cropping of an image. With some stego tools if an image does not fit into a fixed size it is cropped or padded with black spaces. There may also be a difference in the file size between the stego-image and the cover image. Another indicator is a large increase or decrease in the number of unique colors, or colors in a palette which increase incrementally rather than randomly.

6.3. Tools to detect Steganography

The disabling or removal of hidden information in images is dependent on the image processing techniques. For example, with LSB methods of inserting data, simply compressing the image using lossy compression is enough to disable or remove the hidden message. There are several available steganographic detection tools such as Encase by Guidance Software Inc., ILook Investigator by Electronic Crimes Program, Washington DC, various MD5 hashing utilities, etc.

7. IMPLEMENTATION AND RESULTS

All of the approaches to steganography have one thing in common that they hide the secret message in the physical object which is sent.

The following figure shows the steganography process of the cover image being passed into the embedding function with the message to encode resulting in a steganographic image containing the hidden message. A key is often used to protect the hidden message. This key is usually a password, so this key is also used to encrypt and decrypt the message before and after the embedding.

Secrets can be hidden inside all sorts of cover information: text, images, audio, video and more. However, there are tools available to store secrets inside almost any type of cover source. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover.

Figure 5.1 Steganography Procedure

International Journal of Computer Applications (0975 – 8887)

Volume 9– No.7, November 2010

22

In this phase, here we are going to implement steganography technique on the following images.

Figure 5.2 Cover Image

Figure 5.3 Secret Image

The figure 5.2 is our Cover Image and Figure 5.3 is our Secret Image. After applying this technique on it we get the following image. This will be known as Stego Image.

Figure 5.4 Stego Image

After implementation of this technique if we take a look on the histogram of both the images cover image and stego image respectively we will find both are very different from each other. The following figures show the histogram of cover image and stego image.

Figure 5.5 Histogram of Cover Image

Figure 5.6 Histogram of Stego Image

The above two Figure 5.5 shows the histogram of our Cover Image and Figure 5.6 shows the histogram of Stego Image. Both the images are different from each other.

8. STEGANOGRAPHY SOFTWARE APPLICATION

8.1 Digital Watermarking

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time.

8.1.1 Visible Watermarking

In this, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media.

When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

8.1.2 Invisible Watermarking

In this, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden). The watermark may be intended for widespread use and is thus made easy to retrieve or it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

23

visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It is also possible to use hidden embedded information as a means of covert communication between individuals.

Digital Watermarking can be used for a wide range of applications such as: Copyright protection Source Tracking (Different recipients get differently watermarked content). The numbers of possible applications for digital watermarking technologies are increasing rapidly. For example, in the field of data security, watermarks may be used for certification, authentication, and conditional access.

Certification is an important issue for official documents, such as identity cards or passports. Digital watermarks are created by converting copyright information into apparently random digital "noise" using an algorithm that is imperceptible to all but special watermark reading software. So while a JPEG file that is read by a Web browser may display a pretty picture, that same file will display the copyright when read by the watermark software.

9. CONCLUSION AND FUTURE SCOPE

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates, steganography and Steganalysis will continually develop new techniques to counter each other.

In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

The possible use of steganography technique is as following:

Hiding data on the network in case of a breach.
Peer-to-peer private communications.
Posting secret communications on the Web to avoid transmission.

Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

REFERENCES

- [1] Ahsan K., and Kundur D., “Practical Internet Steganography: Data Hiding in IP” found online at <http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf>.
- [2] Anderson R.J. and Petitcolas F.A.P., “On the Limits of steganography,” J. Selected Areas in Comm., vol. 16, no.4, 1998, pp. 474–481.
- [3] Bailey, K. and Curran, K. “An evaluation of image-based steganography methods”. International Journal of Digital Evidence, Fall 2003.
- [4] Chapman, M. Davida G, and Rennhard M.. “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography” found online at <http://www.nicetext.com/doc/isc01.pdf>
- [5] Dai Y., Liu G., and WangBreaking Z., “Predictive-Coding-Based Steganography and Modification for Enhanced Security”, IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.
- [6] Chin-Chen Chang , Iuan-Chang Lin, and Yaun-Hui YU, “ A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, 20 December 2006.
- [7] Shareza Shirali, M.H, “Anew Approach to persain/Arabic Text Stegraphy”, Computer and Information Science, 2006, ICIS-COMSAR 2006, 5th IEEE/ACIS International Conference, 10-12 July 2006 pp 310-315.
- [8] Fabien A.P., and Petitcolas, “Information Hiding: Techniques for Steganography and Digital Watermarking.”, 2000.
- [9] National Academy of Sciences, How do Wavelets work? National Academes of Sciences, <http://www.beyonddiscovery.org/content/view.page.asp?I=1956>, 2003 .
- [10] Digital Watermarking for Digital Media, Information Science Publishing.
- [11] Hiding in Plain Sight: Steganography and the Art of Covert Communication Cole, Eric.
- [12] Information Hiding: Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security, Volume 1) Johnson, Neil F. / Doric, Zoran / Jajodia.
- [13] Computerworld. Steganography: Hidden Data. Quick study by

Deborah Radcliff. [Online] 2002.
<http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html>.

Yeah, I know it is just copy-paste, but you still can't find the flag, can you?