An Innovative Way of Data Security: STEGANOGRAPHY

Sunil Khullar[1], Amanpal Singh Rayat[2], Inderjit Singh[3], Amandeep Kumar[4]
[1]Sr. Lect., [2]Lect., [3]M.tech Student,
RIEIT, Ropar,
[4]Lecturer,
Slite, Longwal

Abstract: *The main purpose of steganography is to hide the presence of communication. While most methods in use today are invisible to an observer's senses, mathematical analysis may reveal statistical anomalies in the stego medium. These discrepancies expose the fact that hidden communication is happening. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Discovering and rendering useless such covert messages is a new art form known as steganalysis. In this Paper, we provide an overview of some characteristics in information hiding methods that direct the steganalyst to the existence of a hidden message and identify where to look for hidden information.*

Keywords: *Steganography, steganalysis, stegomedia etc*

Introduction

The word Steganography comes from the Greek steganos (covered or secret) and graphien (writing or drawing) and thus means covered writing. Steganography is usually given as a synonym for Cryptography but it is not normally used in that way. Through recent usage, Steganography has come to mean hidden writing, i.e., writing that is not readily discernible to the casual

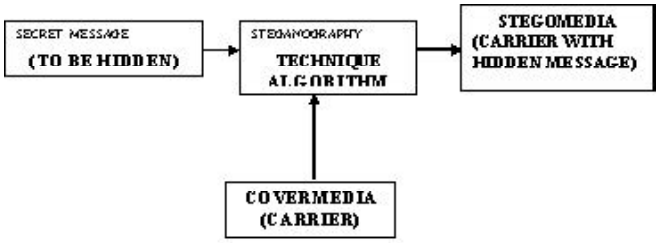
observer. For example, the childhood practice of writing messages in 'invisible ink' would qualify as Steganography since the writing is hidden in the sense that it is not obvious that it is there unless you know to look for it. Recent advances in computing power and interest in privacy has led to the development of techniques to hide messages in otherwise innocuous computer files such as digital pictures and digitized audio. These techniques are now referred to in the aggregate as Steganography. Using these techniques, it is possible to send a secret message to someone in the know and no one else will even know that the message is there. Note that the hidden messages need not be encrypted to qualify as steganographic messages. The message itself can be in plain everyday English and still be a hidden message. However if message is too important than it may be first encrypted, after that we can hide it in an image file. This way, even if someone discovers that a hidden message is present, He will still be unable to read it.

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. Steganography is a means of storing information in such a way that it hides private information and even the existence of the information within the other medium.

To human eyes, data usually contains known forms like images, e-mail, sounds and text. Most internet data naturally includes gratuitous headers, too. There are media exploited using new controversial logical encodings: steganograph and marking. It is the art and science of communicating which hides the existence of the communication. The purpose of Steganography is to convey a message to a receiver in such a way that the very presence of the message is undetectable by a third party. In the computer world, Steganography means hiding secret messages in graphics, pictures or movie

Steganography Process:

The steganography process can be best explained by the below figure:



In the figure, Cover-media is the carrier medium – such as text, image, audio, video, and even the network packet. The secret message is the private message that can be hidden in the cover media. The steganographic technique is the algorithm applied to the cover media and the secret message, to hide the message inside the cover media. Only possible drawback of using above method of hiding messages inside image files is that a good Steganalysis technique can detect the presence of hidden communication and thus purpose of Steganography is not achieved (Steganography is being used to hide the presence of communication!).

Steganography Algorithms

Generally the steganographic algorithm, thus making the detection of hidden information even difficult, uses some key. Steganography algorithms can be made in such a manner so that extracting information from the bitmap image becomes very difficult. Two such algorithms were discussed in this section. First algorithm is based on leaving some of the bits in the image data unchanged, while second algorithm uses the concept of storing the image data in a two dimensional buffer. First algorithm may introduce some statistical noise in the cover media because some bits are not being used for hiding the encrypted message. Such possibilities do not exist in the second algorithm, and hence second algorithm is superior to the first one.

Algorithm 1: For hiding the data

1. Open the image file.
2. Open the text file.

3. Get the session key from (Ks).
4. Skip the 54 bytes header of the image file.
5. Store the bitmap file in a buffer. A hash function can be used to obtain a unique number I for every Km, compute J = I%8.
6. A character of the text file is read. The first bit of the character byte read is stored in the LSB of the first image byte. The next bit of the character byte is stored in the LSB of the next image byte and so on, until J consecutive bytes have been used, at this stage one byte is left unused and we go to the next byte.
7. Step number 6 is carried out for all the characters of the text file.
8. Close the image file.
9. Close the text file.

For extracting the hidden information

1. Open the image file.
2. Open the target text file.
3. Get the Session key (Ks).
4. Skip the 54 bytes header of the image file.
5. Ks is used to calculate a unique number I, by using a hash function. Calculate J = I%8. Image file data is stored in a buffer, and bytes are read from the buffer and LSB of each byte is extracted, until J consecutive bytes have been read. At this point one byte is skipped. When 8 bytes have been read from the bitmap data, one byte of the target file has been obtained. This byte is written to the text file.
6. Step number 5 is repeated until the entire bitmap file has been read, or until End Of File (EOF) is encountered, when such a condition occurs go to step 7.
7. Close the image file.
8. Close the target text file.

Algorithm 2: For hiding the data

1. Open the image file.
2. Open the text file.
3. Get the session key from (Ks).
4. Skip the 54 bytes header of the image file.

5. Store the bitmap file in a two dimensional array one of whose dimension (say Y) is calculated by using the key (Ks) and other is calculated at run time by using the known dimension (Y), and size of the bitmap image. A hash function can be used to obtain a unique Y for every Km.
6. A character of the text file is read. The first bit of the character byte read is stored in the LSB of the first image byte. The next bit of the character byte is stored in the LSB of the next image byte but this byte is taken not in the direction of Y (known dimension), but in the direction of X. when one column has been completely used value of Y is incremented.
7. Step number 5 is carried out for all the characters of the text file.
8. Close the image file.
9. Close the text file.

For extracting the hidden information

1. Open the image file.
2. Open the target text file.
3. Get the Session key (Ks).
4. Skip the 54 bytes header of the image file.
5. Store the image in a two dimensional buffer. One of whose dimension is calculated from the Key (Ks). Now start reading the bytes from first column. Extract the LSB, until LSB's of 8 bytes have been obtained. These 8 bits constitute one byte of the text file. The resulting character is written to the target. When all bytes in this column have been exhausted increment the number of column.
6. Step number 5 is repeated until the entire bitmap file has been read, or until End Of File (EOF) is encountered, when such a condition occurs go to step 7.
7. Close the image file.
8. Close the target text file.

Conclusion:

Steganography can protect data by hiding it but using it alone may not guarantee total protection. It is possible that by using a steganalysis technique (steganalysis techniques are used for detecting steganography) enemy detects presence of text message in the image file and then he/she may

succeed in extracting information from the picture, which can be disastrous in real life situations. This is same for plain encryption. In this case by seeing the meaningless appearing sequence of bits enemy can detect that some illegal message is being sent (unless he/she is a fool), and we may land – up in a problematic situation. However, if one uses both methods, this will lead to 'security in depth'. The message should first be encoded using a strong encryption algorithm and then embedded into a carrier.

References:

Books and Papers

[1] Tanenbaum Andrew S., Computer Networks, 3rd edition, PHI

[2] Forouzan Behrouz A., Data Communication and Networking, 2nd edition, TATA McGraw Hill Publishing Company Ltd.

[3] Pressman Roger S., Software Engineering A Practitioner's Approach, 4th edition, TATA McGraw Hill Publishing Company Ltd.

[4] Jalote P mnb vmbankaj, An Integrated Approach to Software Engineering, Second Edition, Narosa Publishing House

[5] Schildt Herbert, JAVA The Complete Reference, 3rd Edition, TATA McGraw Hill Publishing Company Ltd.

[6] Johnson Neil F, Duric Zoran, Jajodia Sushil Information Hiding Chapter 1. "Steganography and Watermarking - Attacks and Countermeasures", Academic Publishers.

[7] Elke Franz, others, University of Dresden, January 6, 1996, "Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best"

[8] Johnson Neil, Steganography seeing the unseen, February 1998 IEEE paper, 26-34.

Web Sites

[1] http://world.std.com/~franl/

[2] http://www.jjtc.com/neil/

[3] http://www.petitcolas.net/fabien/steganography/