Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 6; April-June, 2015 pp. 513-516

http://www.krishisanskriti.org/acsit.html

Data Hiding Method Using Steganography Technique

Heena Ahuja[1], Chitra Setia[2] and Divya Sharma[3]

[1,2]M.Tech-CSE (Pursuing), ITM University Sector 23, Gurgaon, Haryana, India
3ITM University Sector 23, Gurgaon, Haryana, India
E-mail: [1]heenaahuja34@mail.com, [2]anjalipahwa1912@gmail.com, [3]divya@itmindia.edu

Abstract—*With the increase in number of attacks during the exchange of messages between sender and receiver, a more robust method should be called for to secure the data transfer. Steganography is a well known technique that converts the information in such a manner so as to hide their existence. It protects the data from unauthorized access i.e. invisible messages are written in such a manner that no intruder or illegal users can read or modify the message that has been sent. It can also be defined as the art of hiding the fact that even the communication has taken place. Since the measures have been taken to hide the data for confidentiality, this approach can further be enhanced to copyright protection for digital media Now a day's Steganography technique has been used widely in some modern printers like HP and Xerox popularly known as Printer Steganography which implies hiding the data within the data. Thus in order to enhance robustness, several processing algorithms and steganographic tools are used and in order to enhance the security, steganography can be combined with cryptography like encryption, decryption.*

1. INTRODUCTION

Steganography can be defined as a process where you write invisible messages in a manner that no intruder or illegal user can read or modified the message that has been sent.

Moreover it can also be defined as the art of hiding the fact that even the communication has taken place, so as to protect data in other form. It is an art that provides invisible communication since the image file which contains the secret information embedded within it is send to the receiver instead of the secret information itself. Since the measures have been taken to hide the data for confidentiality, this approach can further be enhanced to copyright protection for digital media.

2. HISTORY

Steganography word comes from the Greek words that shows "concealed (covered) writing".

Stegano means "covered or protected" and other graphy means "writing". Now, in modern applications the aim of steganographic is a usual: to cover secret information in an innocently looking cover and send it to the proper receiver who is aware from the hiding information procedure.

In this condition the existence of secret communication cannot be replaced by third parties. Steganography is not only emphasizing on the way of hiding information but also the art and science of covering the information that take place. It can be traced back to earlier Greek centuries when the data is tattooed on the messengers shaved heads.

The hair that grows to cover the message. Their head will be shaved when they reach the recipient of the message. Another steganography method that was used during those days is tablet wax. Main task is to hide the message, the tablet was removed by wax and then text was etched on and then again covered it by wax and after that it appeared blank upon inspections. During the century, the methods of using invisible inks were extremely popular.

During the World War II where people used ink for writing hidden messages, this was true. The mixture will turn darker and the written message becomes visible upon heating. After some time, the Germans introduced the microdot technique where microdots are considered as photographs is break as small as a printed period, but with a accurate format of a typewritten page. They were included in a letter or an envelope, and due to their tiny sizes, they could be difficult.

Microdots were also hidden in body parts including nostrils, ears, or under fingernails. The military and several governmental agencies are looking into steganography for their own secret transmissions of information. They are also able to quick understanding of secret information communicated by criminals, terrorists, and other main forces.

3. CHARACTERISTICS

Despite of the fact that the main goal of steganography is to prevent the data from unauthenticated users, there are several other useful objectives too which are generally used to judge a method's stenographic strength and stability

The strength can thus be judged by capacity, invisibility, undetectability, robustness, tamper resistance, and also signal to noise ratio i.e. how much data is to be encoded versus how much unrelated data is to be encoded. There are in all three

main attributes which work in opposition to one another, i.e. capacity, unperceivable, and hardiness. If we try to enhance any one of these causes then the others go down; hence we can say that no stenographic techniques can be perfect in removing and retaining the maximum capacity. Thus this greatly affects the robustness of the system.

In most of the cases, capacity is not considered as important criteria than other two, and whereas watermarking technique considers the fact that out of all three, hardiness attribute must be very strong, but in general steganography considers the unperceivable as the most important.

4. ADVANTAGES AND DISADVANTAGES OF STEGANOGRAPHY

Advantages-

1. It is generally used to transfer the data and information stored in the messages secretly with the constraint that transmission must be undiscovered.
2. It is used for private communications.
3. It acts as powerful tool in the present age of information.
4. It gives better security for sharing data on LAN,WAN.
5. It is difficult to be detected by anyone except the receiver.

Disadvantages-

1. Password leakage can occur and lead to unauthorized access of data.
2. If hackers get to know about this technique then it would be very dangerous for all.
3. The choice of images and the format, generally the problem arises because of the size of file which usually involves the selection of the format. Though not usual, but whenever huge files are transmitted between two peers it is likely that it will arise suspicion.
4. There is considerable overhead to hide very small amounts of information.
5. It also leads to the conflict between an original image without hidden message and the steganated image with the hidden message.

1. Need of Steganography

1. Steganography is used now- a -days for a variety of reasons. It may be good, or bad. But the story goes around legitimate purposes which include things like watermarking images for purposes like copyright protection.
2. It can be used to maintain the valuable confidential information, in order to save and hide the data from unauthenticated or those persons who don't have the authority to use that private information
3. It can also be used for unlawful reasons. For instance, if an unauthorized person issues a request to purchase the data, then what we can do is first hide the confidential information in some other file and then send that information to any of the immoral looking email or file transfer. In this the objective remains the same that is to use it as a means of hide the entire data transferred so as to maintain the privacy.
4. It also serves as a means for the replacement of a one-way hash value.

5. APPLICATIONS

1. 1. Now a day's Steganography technique has been used widely in some modern printers popularly known as Printer Steganography which implies hiding the data within the data. Major company brands like HP and Xerox are highly implementing this technique where in small yellow dots are inserted on to each and every page but are not recognizable at all but in order to maintain the security they enclose the printer serial numbers which are encoded, and it further also includes date and time stamps. In general, not only the image files can host hidden information, but the other file formats can also be used to conceal the data such as audio files, text files, web pages and many other file formats.
2. This technique can also be employed for digital watermarking, in which original message is hidden in the form of an image such that we can easily track or verify the source.
3. It is used to enhance the strength of an search engines where we search by an image and the smart identity cards generally used in organizations where the details of the working employees are embedded in their photographs for various purposes.
4. Other applications include video-audio synchronization, TV broadcasting, TCP/IP packets where a unique ID is embedded in an image to analyze the network traffic of particular users.
5. Medical Imaging Systems can be used in Steganography where a separation is accepted between the patients. Image data or DNA sequences and their captions for security or confidentiality reasons. Thus, embedding the patient's information in the image could be a security measure to help solving security issues.

6. ARCHITECTURE OF STEGANOGRAPHY

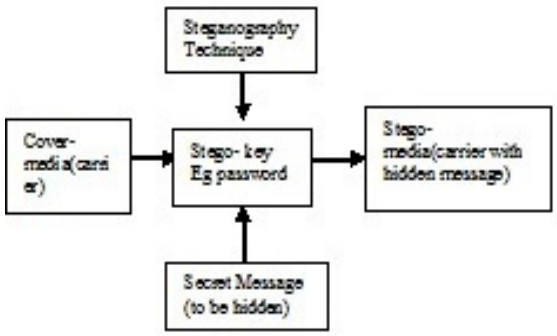
Carrier

The carrier in steganography can be defined as the major element of secure communication into which the secret data is hidden in the form of signal, streams and data files such that it can be prevented by making any further modifications. The examples of such modifications can be in the form of either an image, audio, documents, or executable files but the main aim should be to hide the data such that the intruder could not find that the messages are travelling inside them. It must be kept in mind that these files so modified should look and work the same as that of the original unmodified carrier, and must also start to appear to anyone for inspecting it.

There are several properties that can bring up a doubt in mind that a file is carrying hidden data. However one of the possibility can be that if the confidential data is huge enough as compared to the carrier content, as in for example an empty document that is megabyte in size. The other one includes using poor formats or obsolete-supported extensions which break commonly used tools. Hence it is highly recommended as a cryptographic requirement that the carrier (e.g. photo) must be actual one and not a copy of something which is available publicly e.g., downloaded from some internet site.

The reason being that the source data which is downloaded and available publically can be compared and resembled with the concealed message embedded. Hence there might be a weaker requirement that the embedded message or the modified file does not change the carrier's statistics such that it becomes noticeable.

The content which is modified and encoded using cryptographic techniques should be first compressed and then encrypted. This process of encrypting allocates a uniform noise source that can get modulated into the carrier. It can be resembled as the problem of fox-and-rabbit just as hiders and finders which involves camouflage encapsulation in a sense of signal detection. Thus it can be said that the prey gets better at hiding and the predators at detection. Moreover now a days the high-bandwidth media for instance: eBay, youtube.com, facebook etc. adds fuel to the fire by adding sheer volume hence giving an opportunity to intruders to covert the communication.



Block diagram of Steganography

Fig. 1: Block Diagram of Steganography

Chain: - The data which is hidden might get split into a set of files, thus producing a carrier chain. This chain must retain the property such that all the carriers must be present without any manipulation, and also refined in the exact order

Robustness and cryptography

Steganography tools must ensure robustness such that they can be prevented against all the modern forensic methods, such as statistical steganalysis. Thus the robustness against such methods may be achieved by a mixed balance of 3 i.e.: ·

1. A cryptography process which is stream based,

2. a technique called data whitening;

3. Any type of encoding process.

If however the data is detected somehow then the technique called cryptography is helpful in order to lower down the resulting damage. Since the advantage is that the data is not revealed yet, only the intruder came to know about the fact that a secret message was transmitted. But being known this fact that some private message was being transmitted the person or the sender of the message will become vulnerable as he may be enforced to provide the necessary information by decrypting the data once it is recognized, but in order to save our data, the technique called as deniable encryption can be applied so as to make the decrypted data look benign.

Carrier engine

The carrier engine is the heart of any steganography tool. Several file formats are defined in different ways, so that the data which needs to be hidden from the intruders can be inserted easily inside them.

The processing algorithms so used includes: ·

1. Injection (when it becomes highly doubtful because of the content i.e. the unrelated file size increments) ·
2. Generation (it is doubtful because they easily trace all the carriers so generated). ·
3. Ancillary data and metadata substitution.
4. LSB or adaptive substitution ·
5. Frequency space manipulation

7. COMPARISON OF TECHNIQUES SIMILAR TO STEGANOGRAPHY

Three techniques i.e. steganography, watermarking and cryptography are interrelated to each other. The first two are difficult and they are coming from different disciplines. The work represented here to revolves around data hiding using steganography. The table below is the comparison of all these three techniques comparison of all these three techniques:-

Table 1: Comparison of techniques

Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	usually text based, with some addition of image files
hidden data	Payload	Watermark	Plain text
Key	Optional	Optional	required
Detection	Blind	usually information	Blind
Authentication	full retrieval of data	generally achieved by cross correlation	full retrieval of data
Aim	secrete communication	Saving copyright	data protection

output	stego-file	watermarked-file	Cipher text
Visibility	Not at all	occasionally	Always
Ceases when	Discovered	discarded	Deciphered

Data hiding algorithm Input: Video

Output: Stego video

Step 1: Enter the input Video

Step 2: Perform frame separation

Step 3: Apply Integer DCT on each 8×8 block.

Step 4: Apply Zigzag Scanning on each 8×8block.

Step 5: Use Huffman coding to shorten the size of frame.

Step 6: Apply secret key to secure the data to access through unauthorized user.

Step 7: Apply LSB Algorithm to split data

Step 8: Generate Stego video

8. CONCLUSION

From the past times people are using steganography as the most fascinating and effective method of hiding data. There is no doubt that such methods can be employed to uncover such oblique tactics or false means, but the first step is to spread the awareness such that methods even exist. There are many justifications of using steganography as a major technique for hiding our vulnerable data from intruders, and we can also include watermarking. Moreover the security can be enhanced by using more secure central storage methods like passwords, or key processes like encryption, decryption public or private key cryptography. Hence regardless of the fact that, this technology is comparatively easy to use but it is difficult to detect even the fact and recognize that any secret message is being transmitted. Hence the more we research and study its features and functionality, the more we discover the magic of this technology.

REFERENCES

[1] http://www.artofmanliness.com/2011/09/09/man-lnowledge-the-history-of-invisible-ink/
[2] http://www.lib.umich.edu/papyrology-collection/ancient-writing-materials-wax-tablets
[3] Schildet, H.(2001).Java2: The Complete Reference. New Delhi: Tata McGraw Hill Publishing company.
[4] Pressman, R.S (2010). Software Engineering: A Practitioner's Approach(seventh Edition ed.) Singapore: McGraw Hill
[5] http://www.forensics.nl/steganography