IMPLEMENTING SECURITY LAYERS ON FILE SYSTEM

A TECHNICAL REPORT

ASHIKALI M. HASAN

Researcher of CelNet Web Security And IT Consultancy

E-mail: ashikali1208@yahoo.com
Web: - http://www.ashikali.com

http://www.celnet.co.in

ABSTRACT

STEGANOGRAPHY is defined as the art of hiding information. STEGANOGRAPHY and cryptology are similar in the way that they both are used to protect important information. The difference between the two is that STEGANOGRAPHY involves hiding information so it appears that no information is hidden at all therefore the person will not attempt to decrypt the information. In STEGANOGRAPHY the different file formats can be used for the purpose of hiding the information like for example the video or audio etc. STEGANOGRAPHY comes from the Greek words STEGANÓS (Covered) and GRAPTOS (Writing). STEGANOGRAPHY in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file.

Keywords: *Steganography, Hidden Information, Graptos, Decryption, Information Hiding*

1. INTRODUCTION

STEGANOGRAPHY is defined as the art of hiding information, data or messages in an image. The information hiding is done with the help of computer programs and these programs sets the least significant bits of the pixels of image according to the embedded information bits [1]. Even the different file formats can be used for the purpose of hiding the information like for example the video or audio etc. The purpose is to pass on the information without any regard or knowledge of others safely to the destination simply human eye is not able to detect the information [2]. The advantage of STEGANOGRAPHY is that those who are outside the party even do not realize that some sort of communication is being done. This is an alternative method used instead of encryption. In case of the images the bits are used and the contrast size of the image matters a lot. If the computer criminal has used some sort of STEGANOGRAPHY then it is required for the computer forensics professional to decode that information to acquire valid evidence that can be produced in the court of law. The advantage of unused bits within the structure of a file or those bits those are mostly not detectable if altered are used. If not identified as a STEGANOGRAPHIC message; there is no chance of any leakage of information. The message rides safely and secretly to its destination. For good results different sort of compression techniques are applied by using a suitable embedded method. In case of .GIF images we can use the swapping technique of colors [4] while in case of files using JPEG compression the best way is to embed the file at multiple locations [6], [7] or another better solution is to embed the file in the frequency domain in which we have to alter the components of the file or image's discrete cosine function and its detail is described in [8]. The message can be decrypted only if it is identified. So it has an advantage over the encryption process. In case of the encrypted text; however complicated may be the cipher applied but at least the encrypted message is detectable as an encrypted message.

2. TECHNICAL OVERVIEW

In general a STEGANOGRAPHIC message can appear in many different formats. Only the person or the destination will be able to understand the hidden meaning. It appears as something else like for example an article, shopping list, a picture, or some other cover message. If the message is much larger then data content terms are also even more. The content terms here relate to the number of bits used. They are relative to the hidden messages.

More number of bits will result in much ease to hide. Hence the digital pictures and images are used for the purpose of STEGANOGRAPHY. Usually the images with large amount of data are used for this purpose. They can be easily stored in the computer or any other storage media. Good systems used for this purpose share a secret key between sender and receiver and a sort of conventional keystream generator [5] is also used which helps to create a pseudo-random keystream. This keystream is used to find out the pixels or sound samples in order to locate the embedded ciphertext bits [3]. A computer forensics even if encounters the data is also not even able to realize the evidence. These STEGANOGRAPHIC images can be easily used over the internet to pass the messages for communication. The principle of STEGANOGRAPHY is basically from olden days. Let us consider an example that can be used to describe how the task of STEGANOGRAPHY is actually achieved. For example a 24 bit bitmap image will have 8 bits representing the color values. Each of the three color values that is the red, green, and blue has a relative value at each pixel. The difference between say 1111111111 and 1111111110 in the value for blue intensity is unlikely to be detected by a human eye. Hence, it is possible to represent the least significant bit for something else rather than color information bit. It is possible to get one letter in an ASCII character set if we do it with the other colors such as green and the red as well. So for each of the three pixels it is possible to have one letter of ASCII text. Winnowing and Chaffing are the recent techniques in STEGANOGRAPHY. Also Null ciphers can be used.

3. BRIEF DETAIL

STEGANOGRAPHY can be done with the file also. Whenever any file is being created. Computers assist that file as understanding its binary data. When a file is being created it contain lots of junk data. Every time file is being create the junk data will be automatically create within the file therefore it is possible to replace junk data with other data. For example if user is creating a txt file name example.txt at the time example.txt contain many junk data. It is possible to replace this data with another data. Every file contains data and this data is converted into binary form so the junk data is also in form of binary data if it is replaced still the output of file will not be change. The new data is taking place of junk data therefore after injecting new data in place of junk data file size will be same as before.

4. EXPERIMENT

As we know two techniques of data protection but according to research it is possible to join two methods with together and can be apply on the file system. As a proof of concept if in place of junk data we can inject encrypted data. This concept can be increase another layer of security. By this concept it is possible compress file on major level because when ever data is being encrypted at this point encryption algorithm compress that data in different size. For example if 2 file we have one file has size 10 kb name as example1.txt another file has size 10 KB name example2.txt both file converted into binary form into the computer. If file 2 name example2.txt is being compressed through the encryption method and then the size of file will be change. The binary of this file will not be same as it has original after the encryption. And it can be inject into the file name example1.txt however we can merge all the security aspects together and can be apply on one particular file. Example lets have file example.txt and example2.txt now first we insert some character string into example2.txt file by converting string by any strong encryption methods like RSA even we can use our own algorithm now after we can covert file name example2.txt into custom file type format by our custom algorithm. So whenever we need to read this file then we must have to use this same algorithm again to change file type. If we have focus practically on this example then as we know when we use WINRAR to pack that file at the time WINRAR change the type of file and converting it to in RAR format this format only is readable by that particular software. We can use this similar concept to develop custom algorithm for converting file type. Let’s take example we have developed such program which convert file into some custom type and give extension as ashu so now our file example1.txt which contain encrypted information inside will be convert by our software and will be become “example1.ashu” now if we can add another extra layer on our file type system as password protection for covert it again as original file. And then we can inject this file to example.txt file.

5. CONCLUSION

The security of file system can be increase at major level because this concept is applying four layer of security on the file system. Because of every layer of security are performing heavy compression methods. So it is possible to perform this same operation on packet. It is possible to send 100 MB data using 10 KB of packet. Even if this method has four layer of security so this data cannot be decrypt by sniffer if the intruders grab the packet among from network.

REFERENCES:

[1] "A Digital Watermark", RG van Schyndel, AZ Tirkel, CF Osborne, in International Conference on Image Processing, (IEEE, 1994) v 2 pp 86–90

[2] "A Cautionary Note on Image Downgrading", C Kurak, J McHugh, Computer Security Applications Conference, (IEEE, 1992) pp 153–159

[3] "Computer Based Steganography", E Franz, A Jerichow, S M¨oller, A Pfitzmann, I Stierand, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 7–21

[4] 'Steganography in Digital Images', G Jagpal, Thesis, Cambridge University Computer Laboratory, May 1995

[5] "Applied Cryptography-Protocols, Algorithms and Source Code in C" B Schneier (second edition), Wiley 1995

[6] "Towards Robust and Hidden Image

Copyright Labeling", E Koch, J Zhao, Proceedings of 1995 IEEE Workshop on Non-linear Signal and Image Processing (Neos Marmaras, Halkidiki, Greece, June 20–22, 1995)

[7] "Copy Protection for Multimedia Data based on Labeling Techniques", GC Langelaar, JCA van der Lubbe, J Biemond, 17th Symposium on Information Theory in the Benelux, Enschede,

The Netherlands, May 1996

[8] "A Secure, Robust Watermark for Multimedia", IJ Cox, J Kilian, T Leighton, T Shamoon, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 183–206

AUTHOR PROFILE:

Ashikali M. Hasan received the degree in MCA from Gujarat University, in 2010. He is a researcher of CelNet Company. Currently, His interests are in computer security and investigation of various cyber attacks and exploit building.