Asmita Haveliya / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.1672-1674

A New Approach for secret concealing in Executable File

Asmita Haveliya
M.Tech. (Pursuing), Dept. Of Electronics, ASET
Amity University
Lucknow, India

ABSTRACT

There are by now a number of varieties in techniques existing for concealing a little secret in a set of file. These techniques comes under Steganography, which actually don't allow any third party to even be acquainted with the survival of the secret behind. There were numerous schemes in ancient times to keep secrets but as the technology grows the secrets nurtured and so, necessitate for technique to put in the ground those little secrets grew more rapidly. This paper mainly deals with the concept of hiding the image files of format PNG, JPEG AND BMP in the executable files which have the .exe extension. The results for the proposed work are obtained using the MATLAB version 7.10.0.499 (R2010a).

Keywords - **Steganography, hiding data, image encryption, image decryption, covert writing, exe cover data, executable file data hiding.**

I. INTRODUCTION

Steganography is a word which corresponds to concealing secret contained by any file. The projected work is been tested for JPEG, PNG and BMP image types as secret messages while the executable files with .exe extension are taken as the cover file. Thus, in this paper, we investigate a Steganography technique for image hiding in an executable file.

Anything that has some great value for the user or transmitter of the communication system followed is termed as the secret information which is to be concealed. The file that will store or mask the secret information is termed as a cover file. In the proposed work the secret information is the image files and the cover file is the executable file.

II. IMAGE FILES

Image file formats are standardized means of organizing and storing digital images. Image files are composed of either pixels vector (geometric) data, or a combination of the two. Whatever the format, the files are rasterized to pixels when displayed on most graphic displays. The PNG, JPEG, and BMP formats are most often used to display images on the Internet. Therefore in the proposed work these three image types are been used. JPEG is an acronym for Joint Photographic Experts Group.JPEG compression is (in most cases) lossy compression. Nearly every digital camera can save images in the JPEG format, but JPEG files suffer generational degradation when repeatedly edited and saved. So when we add a secret file to jpeg file format it has a propensity to be a lossy image. To remove this dilemma the proposed work is done such that the size of the stego-media will increase in the direction to have a save for the image to be lossless.

The PNG (Portable Network Graphics) file format was created as the free, open-source successor to the GIF. The PNG file format supports true color (16 million colors) while the GIF supports only 256 colors. The PNG file excels when the image has large, uniformly colored areas. The lossless PNG format is best suited for editing pictures, and the lossy formats, like JPG, are best for the final distribution of photographic images, because in this case JPG files are usually smaller than PNG files.

PNG is designed to work well in online viewing applications like web browsers so it is fully stream able with a progressive display option. PNG is robust, providing both full file integrity checking and simple detection of common transmission errors. Therefore other than jpg author has taken PNG image type.

The BMP file format (Windows bitmap) handles graphics files within the Microsoft Windows OS. Typically, BMP files are uncompressed, hence they are large; the advantage is their simplicity and wide acceptance in Windows programs.

III. EXE FILE

An exe file (said as letters E-X-E) is a computer file that ends with the extension ".exe" is known as an executable file. Executable files, make things take place in a computer system. Windows EXE files commence programs, begin development, and operate the same as the initiation knob for the majority of the actions you perform while working on the computers. It is fundamentally a file format with the intention to directly execute the computers. as soon as an individual hit on an exe file, an integral custom frequently carry out set of laws or conventions with the intention to situate a number of task into action. Exe files are brought into play to establish, install in addition to running codes and routines.

An exe file is no more than one of numerous file format varieties that are accepted through a variety of operating systems. Contrasting to the source files, executable files cannot be comprehended, read and examined by humans without any compilation through computers.

The exe file is one of the most functional and useful types of files in particular for the reason that it runs programs; on the other hand, this as well makes it potentially injurious, destructive and damaging file type. It is capable to be used as a deliverance scheme for viruses or other malevolent routines. Exe files are in general are not intended to be edited, and altering an exe file, will essentially turn it into a deadly untreatable file. In view of the fact that the exe file is mainly a program, it is regularly sheltered by copyright commandment's, as per the associated authorization agreement issue by its creator. Hacking an exe file is against the law in this case. Seeing that, it is out of harm's way to make a mistake on the side of caution and carefulness. Professional suggests maintaining virus checkers the latest and erasing email's from unfamiliar and strange foundations.

IV. RESULT

In the resultant set of images we have taken the covert messages of different sizes and extension but in image format and cover file is of exe extension. In the ensuing images author has taken an executable file of EXE format as the cover file and image files with JPG extension (fig 1), BMP format (fig 3), PNG format (fig 5) is taken as the covert message file. While figure 2, 4, 6 shows their respective histograms for stego object i.e. the encrypted file.

For the embedding of the JPG image file into the cover object of exe extension the summary report is as follows:

summary_report =

Cover file Name: coverobject.exe
Secret file name: messagetocovert.jpg
Size of cover file(bytes): 12387832
Size of secret file(bytes): 213120
Stego file name: stegoobject.exe
Time to encrypt (secs):226.890832

For the decrypting of the JPG image file from the cover object of exe extension the summary report is as follows:

Summary_Report =

Stego file name: StegoObject.exe
Secret file name : MessageExtracted.jpg
stego file size(bytes):12387832
secret file size(bytes):213120
Time to decrypt(secs) : 224.418790

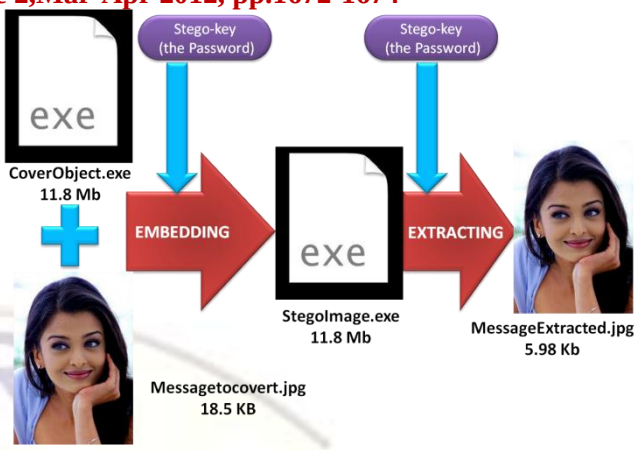

Fig 1: Images in use for investigation : cover file .exe extension and secret file with .jpg extension

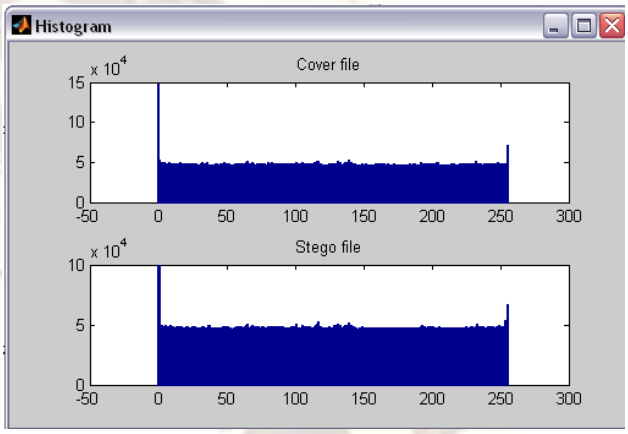

Fig 2: Histogram for cover file .exe extension and secret file with .jpg extension

For the embedding of the PNG image file into the cover object of exe extension the summary report is as follows

summary_report =

Cover file Name: coverobject.exe
Secret file name: messagetocovert.png
Size of cover file(bytes): 12387832
Size of secret file(bytes): 14283
Stego file name: stegoobject.exe
Time to encrypt(secs):8.106469

For the decrypting of the JPG image file from the cover object of exe extension the summary report is as follows:

Summary_Report =

Stego file name: StegoObject.exe
Secret file name : MessageExtracted.png
stego file size(bytes):12387832
secret file size(bytes):14283
Time to decrypt(secs) :9.335530

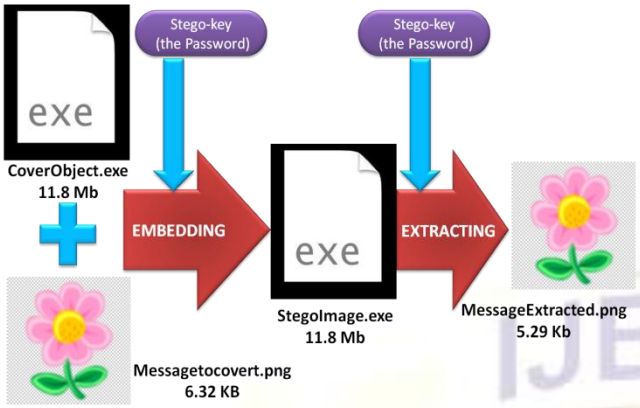

Fig 3: Images in use for investigation : cover file .exe extension and secret file with .png extension

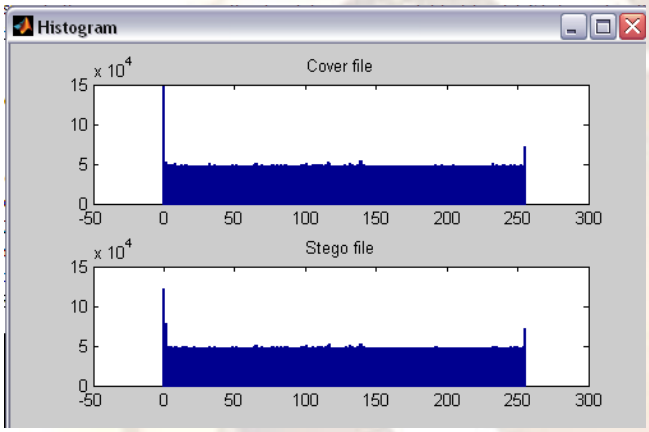

Fig 4: Histogram for cover file .exe extension and secret file with .png extension

For the embedding of the BMP image file into the cover object of exe extension the summary report is as follows:

summary_report =

Cover file Name: coverobject.exe
Secret file name: messagetocovert.png
Size of cover file(bytes): 12387832
Size of secret file(bytes): 5568 bytes
Stego file name: stegoobject.exe
Time to encrypt (secs): 2.441098

For the decrypting of the BMP image file from the cover object of exe extension the summary report is as follows:

Summary_Report =

Stego file name: StegoObject.exe
Secret file name : MessageExtracted.png
stego file size(bytes):12387832
secret file size(bytes):5568
Time to decrypt(secs) :2.346620

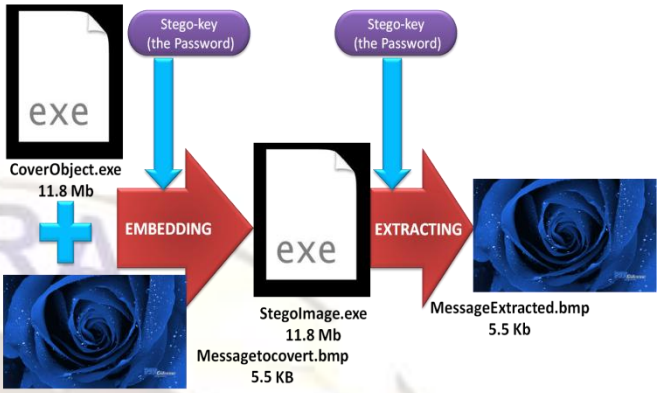

Fig 5: Images in use for investigation : cover file .exe extension and secret file with .bmp extension

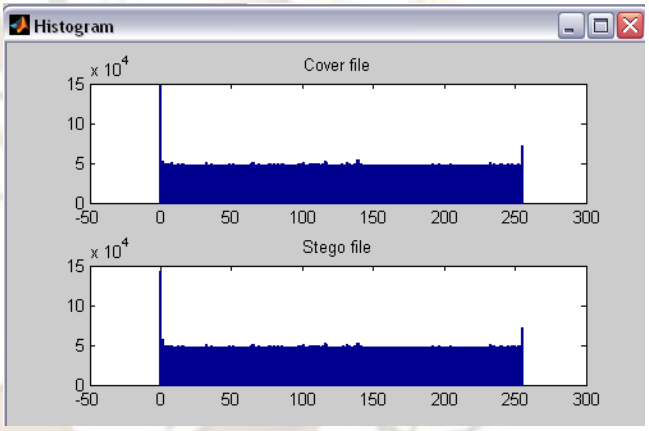

Fig 6: Histogram for cover file .exe extension and secret file with .bmp extension

REFERENCES

[1] Neil Johnson and sushil Jagodia, "Exploring Steganography: Seeing the Unseen" George Manson University, Computer, Vol 31, No 2 (26-34), Feb 1998.

[2] R. Anderson and F. Petitcolas, "On the Limits of Stegano graphy", IEEE Journal On Selected Areas in Communications, Vol 16, No. 4 (474-481), May 1998.

[3] R. Anderson, "Information Hiding", Cambridge, UK, C omputers, Vol 1174, 1996.

[4] A.A.Zaidan, B.B.Zaidan, Fazidah Othman, "New Technique of Hidden Data in PE-File with in Unused Area One", International Journal of Computer and Electrical Engineering (IJCEE), Vol.1, No.5, ISSN: 1793-8198, pp 669-678.