A STUDY ON OVERVIEW OF STEGANOGRAPHY WITH SPECIFIC TOOLS

A.Sankara Narayanan
Department of Information Technology
Salalah College of Technology, Salalah, Sultanate of Oman

Abstract **-Steganography is a science for invisible communication and play vital role on the network security. The security process is manipulated with the different tools and technology. The technology is provided secured environment to the network user via Least Significant Bit Insertion, Masking and Filtering Algorithm and Transformations. Using this technology many applications are developed to implement Steganography in the real time applications. This paper discussed the implementation procedure of available tool for encoding and decoding which covers all the data formats including Text, Image, Audio, and Video. All the tools and the implementation of online and off line implications are addressed along with the procedure.**

Keywords: **Steganography, Network Security, Least Significant Bit Insertion, Masking and Filtering**

I. INTRODUCTION

Steganography refers to the science of "**invisible**" communication. The word stega derived from Greek word **stegos** or **roof** which refers to ***covered*** and nography derived from the same Greek word **graphia** which refers to ***writing***. Its purpose is to hide the very presence of communication by embedding messages into "innocent looking" cover objects. It is based on replacing the least significant bit in image, music, or video files with the concealed message data. It can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt, and .wav. Steganography in short is hiding a secret message inside in an ordinary message.

Background

The rise of the internet is one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this is called Steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of communication information.

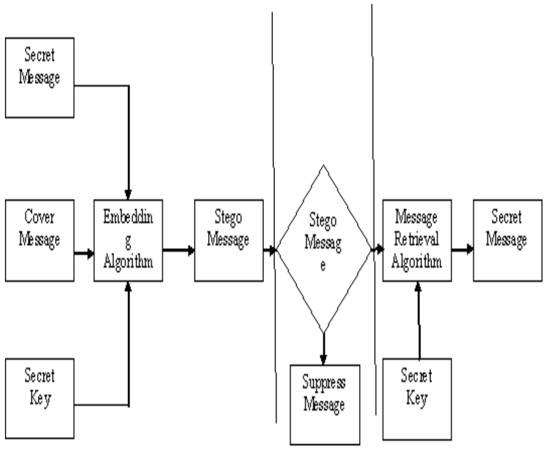
Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography focuses on keeping the existence of a message secret.

Research in Steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether forcing people to study other methods of secure information transfer. Business has also started to realize the potentials of Steganography in communicating trade secrets or new product information. This study intends to offer a stage of the art overview of the different algorithms used for image Steganography to illustrate the security potential of Steganography for business and personal use.

Evolution of Steganography

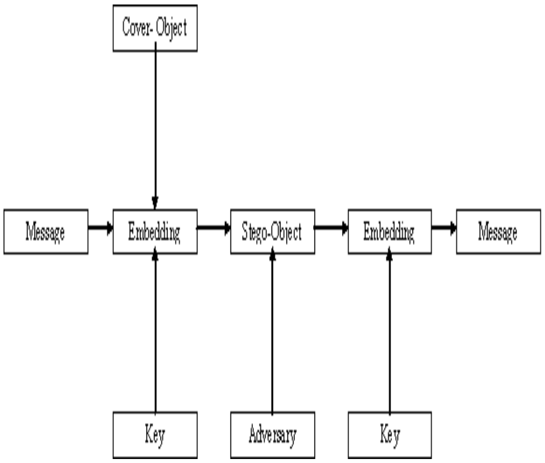
Steganography has been used to secretly communicate information between different users.

- During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper.
- In action Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message the recipient would shave off the messengers' hair to see the secret message.
- Another method used in Greece was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax. The recipient of the message would simply remove the wax from the tablet to view the message.



Carrier File refers to a file which has hidden information inside of it. Steganalysis means the process of detecting hidden information inside of a file. Stego-Medium is the medium in which the information is hidden. Redundant Bits are piece of information inside a file which can be "overwritten (or) altered" without damaging the file and payload said to be the information which is concealed.

Modern Terminology



II. TECHNIQUES OF STEGANOGRAPHY

There are many ways to hide information in digital images. The following are certain approaches

a. Least Significant Bit Insertion

b. Masking and Filtering

c. Algorithm and Transformations

a. Least Significant Bit Insertion (LSB)

Many stego tools make use of Least Significant Bit (LSB) for example, 11111111 is an 8 bit binary number. The "right most bit" is called the LSB because changing it has the least effect on the value of the number. The idea is that the LSB of every byte can be replaced with little change to the overall file. The binary data of the secret message is broken up and then inserted into the LSB of the each pixel in the image file.

Using the Red, Green, Blue (RGB) model a stego tool make a copy of an image palette say an 8-bit image. The copy is rearranged so that colors near each other in the RGB model are near each other in the palette. The LSB of each pixels 8-bit binary number is replaced with one bit from the hidden message. A new RGB color in the copied palette is found. A new 8-bit binary number of the RGB color in the original palette is found. The pixel is changed to the 8-bit binary number of the new RGB color.

The stego tool finds the 8-bit binary number of each pixel's 8-bit binary number is one bit of the hidden data file. Each LSB is then written to an output file. To hide information in the LSBs of each byte of a 24-bit image, it is possible to store 3 bits in each pixel.

LSB insertion works well with gray-scale image as well. It is possible to hide data in the least and second least significant bits and the human eye would still not be able to discern it.

Unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression. For example converting a GIF (or) BMP image, which reconstruct the original message exactly (lossless compression), to a JPEG format, which does not (lossy compression), and then converting back, can destroy the data in the LSBs.

b. Masking and Filtering

Masking and filtering techniques hide information by marking an image and is usually restricted to 24-bit and gray-scale images. Digital watermarks include information such as copyright, ownership (or) license. While traditional Steganography conceals information, watermarks extend information since it becomes an attribute of the cover image.

Masking techniques hide information in such way that the hidden message is more integral to the cover image than simply hiding data in the "noise" level. Masking adds redundancy to the hidden information. This makes the masking technique more suitable than LSB with lossy JPEG images. It may also help protect against some image processing such as cropping and rotating.

c. Algorithm and Transformations

Another Steganography technique is to hide data in mathematical functions that are in compression algorithms.

The idea is to hide the data bits in the least significant coefficients.

A key advantage of the JPEG images over other format is its lossy compression methods. It enables high quality images to be stored in relatively small files. The compressed data is stored as integers but the calculations for the quantization process require floating point calculations for the quantization process require floating point calculations which are rounded. Errors introduced by rounding define the lossy characteristic of the JPEG compression method. JPEG images use the Discrete Cosine Transform (DCT) technique to achieve image compression. The DCT is a technique for expressing a waveform as a weighted sum of cosines. In a JPEG file the image is made up of DCT coefficient. When a file is Steganography embedded into a JPEG image, the relation of these coefficients is altered. Instead of actual bits in the image being changed as in LSB Steganography, it is the relation of the coefficient to one another that is altered.

In addition to DCT images can be processed with Fast Fourier Transform (FFT). FFT is an algorithm for computing the Fourier Transform of a set of discrete data values. The FFT expresses a finite set of data points in terms of components frequencies. It also solves the identical inverse problem of reconstructing a signal from the frequency data.

The wavelet transform is a transformation to basic functions that are localized in frequency. The wavelet compression methods are better at representing transients, such as an image of stars on a night sky. This means that elements of some data signal that are transient can be represented by small amount of information than would be the case if some other transform, such as the more widespread discrete cosine transform, had been used. Wavelet compression are good for transient signal characteristics but not for smooth, periodic signals.

Many transform domain method are not dependent on the image format so that the hidden message is retained after conversion between lossless and lossly formats.

The steps are to take the DCT (or) Wavelet transform of the cover image and find the coefficients below a specific threshold. Replace these bits with bits to be hidden (for example, use LSB insertion) and then take the inverse transform and store it as a regular image.

To extract the hidden data take the transform of the modified image and find the coefficients below a specific threshold. Extract bits of data from these coefficients and combine the bits into an actual message.

III. TOOLS

a. WbStego4

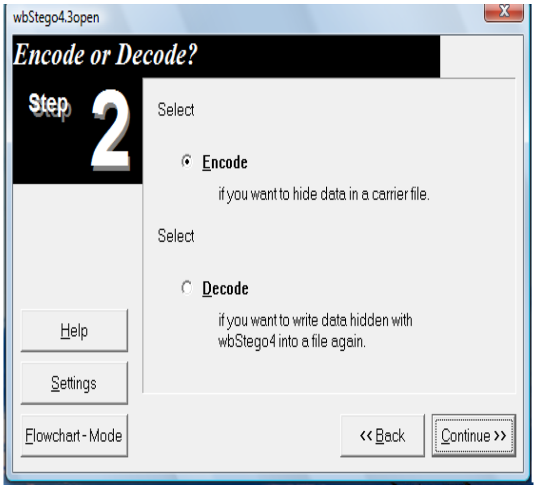
Encode

➢ Download this file wbs43open-win32.zip (422KB).

➢ Have a Bmp image and a text file ready for use.

➢ Run the wbStego4.3open.exe file. Select continue, the following screen should

➢ Display.



wbStego4.3open

Encode or Decode?

Step 2

Select

● Encode

if you want to hide data in a carrier file.

Select

○ Decode

if you want to write data hidden with wbStego4 into a file again.

➢ Select encode click continue; select the data you want to hide, then click continue

➢ Select the carrier file in which you want to hide data and then click continue

➢ Cryptography setting click continue

➢ Destination of manipulated carrier file, e.g.123 click save and then click continue

➢ Click Continue, o.k.

Decode

➢ Select decode click continue; select the carrier file from which you want to extract Data.

➢ Select e.g.123 click continue, leave the empty input field and then click continue

➢ Filename of destination file for decoded data

b. Invisible Secrets 4

Hide Files

➢ Download this file invsecr-trail (3202KB).

➢ Have a JPEG image and a WAV file ready for use.

➢ Install the invsecr-trail file. Accept the terms outlined. The following screen should display

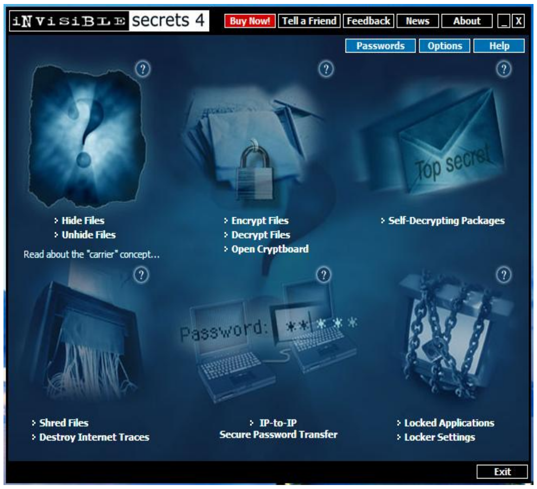
➢ Select Hide files and then click add files; select the WAV file click open

➢ Click next and select the carrier file JPEG, click next

- Set the encryption setting password e.g.123, confirm the password type 123

- Click next and enter the destination (or) target file name e.g.1234

- Click hide



Unhide Files

- Click unhide files and select carrier file, click next enter the decryption password

- Enter the destination file name e.g.12345, click unhide and click finish.

c.Masker 7.5

Hide Files

- Download this file mskseptup (2601KB).

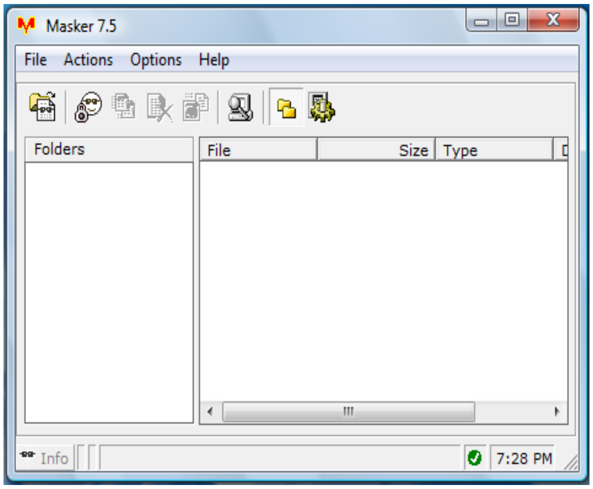
- Have a video file .AVI and Image .JPEG file ready for use.

- Install the msksetup file. Accept the terms outlined. The following screen should display.

- Click actions, select hide and browse the video file .AVI, click o.k.

- Enter password e.g.123, re-enter the password 123, click o.k.

- Select the file you want to hide .JPEG, click next and click hide.



Unhide Files

- Click file, select open carrier file, click browse and select the file, click o.k.

- Open hideout password enter e.g.123, click o.k.

- Select the file right click extract, select the target folder and click extract.

d. Magic Folders

Hide Files

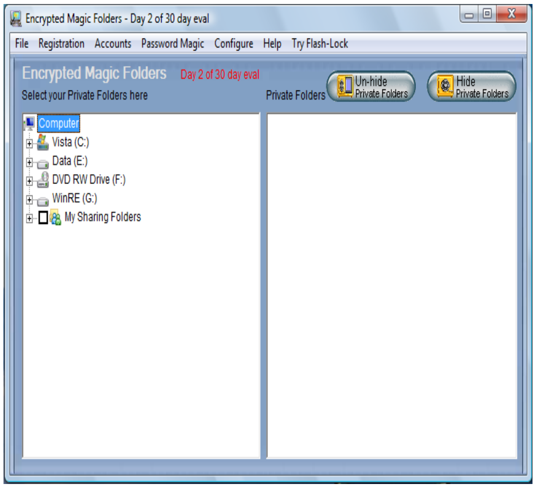
- Download this file mfx (774KB).

- Have a folder ready for use. Select encrypted magic folders.

- Install the mfx file. Accept the terms outlined.

- Enter password e.g.123, re-enter password 123, click o.k.

- The following screen should display.



- Select your private folders here and click hide private folders.

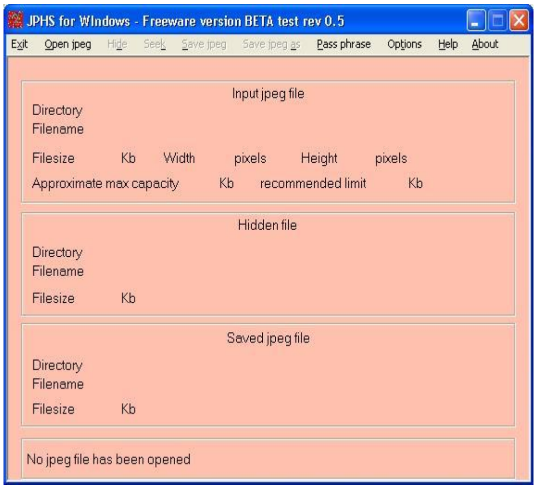
Unhide Files

- Open encrypted magic folders, enter the password e.g.123, and click o.k.
- Select private folder right side and click unhide private folders.

e) JPHS

Hide Files

- Download this file jphs05.zip (180KB) if you are a Windows user. Otherwise, go to http://linux01.gwdg.de/~alatham/stego.html to download the Linux version.
- Have a jpeg image and a text file ready for use. Alternatively, you can download and use my image My jpeg, and text file My message.
- For Windows users, run the Jphswin.exe file. Accept the terms outlined. The following screen should display:



JPHS for Windows - Freeware version BETA test rev 0.5

Input jpeg file
Directory
Filename
Filesize Kb Width pixels Height pixels
Approximate max capacity Kb recommended limit Kb

Hidden file
Directory
Filename
Filesize Kb

Saved jpeg file
Directory
Filename
Filesize Kb

No jpeg file has been opened

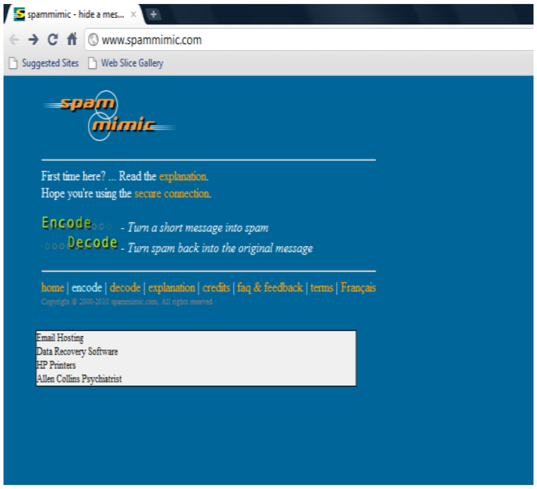
- Select 'Open jpeg'. Choose any jpeg image.
- Select the 'Hide' option. Enter the same pass phrase to both boxes, e.g. 12345. Choose any text file that contains the hidden message.
- Select 'Save jpeg as'. Enter a file name for the new image file.

Unhide Files

- Now Select 'Open jpeg'. Choose the new jpeg file you saved in the previous step.
- Select the 'Seek' option. Enter the pass phrase you used, e.g. 12345, in both boxes.
- Enter a name for the recovered message file. *Caution*: provide the '.txt' extension in the file name.
- Go to the folder where you saved the recovered message file and click to view. The hidden message is displayed.

IV ONLINE TOOLS

a. *www.Spammimic.com*



spammimic - hide a mes...
www.spammimic.com

First time here? ... Read the explanation.
Hope you're using the secure connection.

Encode - *Turn a short message into spam*
Decode - *Turn spam back into the original message*

home | encode | decode | explanation | credits | faq & feedback | terms | Français
Copyright © 2000-2010 spammimic.com, All rights reserved

Email Hosting
Data Recovery Software
HP Printers
Allen Collins Psychiatrist

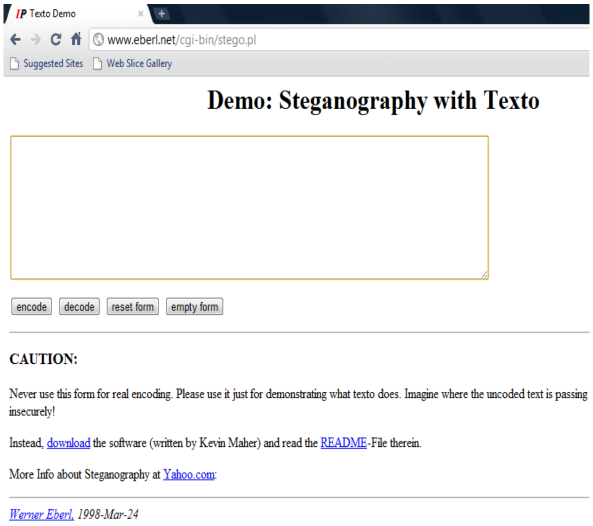
Encode

- Select encode, enter your short secret message type e.g.**123,** click encode.
- Spam message will appear; you can copy the message out of the text box and paste it into a mail.

Decode

- Select decode you can copy the message it into the textbox, click decode.

b. *Steganography with Texto (http://www.eberl.net/cgi-bin/stego.pl)*



Texto Demo
www.eberl.net/cgi-bin/stego.pl

Demo: Steganography with Texto

CAUTION:

Never use this form for real encoding. Please use it just for demonstrating what texto does. Imagine where the uncoded text is passing insecurely!

Instead, download the software (written by Kevin Maher) and read the README-File therein.

More Info about Steganography at Yahoo.com:

Werner Eberl, 1998-Mar-24

Encode

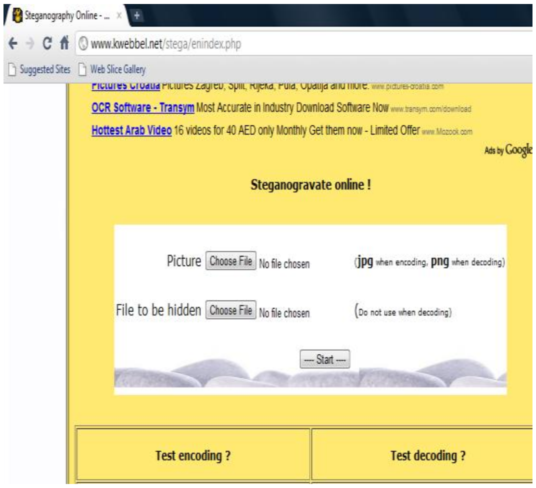
- Select encode, enter your short secret message type e.g.**123,** click encode.

- Text message will appear, you can copy the message out of the text box and paste it into a mail.

Decode

- Select decode you can copy the message it into the textbox, click decode.

c. *Hide secret text in image file JPG. (http://www.kwebbel.net/stega/enindex.php)*



Pictures Croatia Pictures Zagreb, Split, Rijeka, Pula, Opatija and more. www.pictures-croatia.com

OCR Software - Transym Most Accurate in Industry Download Software Now www.transym.com/download

Hottest Arab Video 16 videos for 40 AED only Monthly Get them now - Limited Offer www.Mozook.com

Ads by Google

Steganogravate online !

Picture No file chosen (jpg when encoding, png when decoding)

File to be hidden No file chosen (Do not use when decoding)

Encoding

- Open your text editor and create a file.
- Save this file.
- Click above at "picture" on "browse"
- Take a picture at random on your hard disk and select it
- Click above at "file to be hidden" at "browse"
- Select your text file on your hard disk
- Click on "Start"

Decoding

- Click on this picture with your right mouse key
- Select "save image as"
- Save the picture on your hard disk
- Click above at "picture" on "browse"
- Select the picture (vis.png) on your hard disk
- Click on "Start"
- You can try it also with the background of this site.

V.CONCLUSION

The study focuses on the pros and cons of Steganography in detail. It also highlights the tools used to send the data hidden by Steganography to the recipient of the information. It also outlined the different online tools which enable the corporate, individuals, businessman and the society in general to Steganography the important data. In short a single word could yield the output of the message sent from one to another within short duration in confidential environment.

REFERENCES

[1] Aelphaeis Mangarae. Steganography [http://Zone-h.Org](March 18.2006).Available:http://infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

[2] Gary C. Kessler. An Overview of Steganography for the Computer Forensics Examiner (July-2004).Available: http://www.garykessler.net/library/fsc_stego.html

[3] Kevin Curran, Karen Bailey. An Evaluation of Image Based Steganography Methods (2003). Available : http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf

[4] Kwang-Soo Lee.Digital Image Steganalysis. Available: http://www.isit.or.jp/lab2/kouryu/2004-2005/NICT/program/K-J%20workshop%20presentation%20file/CIST/CIST_presentation/Model%20and%20Techniques%20for%20Image%20Steganalysis.ppt

[5] Neil Johnson's. Steganography and Digital Watermarking page. Available: http://www.jjtc.com/Steganography/

[6] Morkel.T, J.H.P. Eloff, M.S.Olivier An Overview of Image Steganography. Available: http://mo.co.za/open/stegoverview.pdf

[7] Robert Krenn. Steganography Implementation & Detection(January 21.2004). Available: http://www.krenn.nl/univ/cry/steg/presentation/2004-01-21-presentation-steganography.pdf

[8] Yang, Li “Digital Watermarking”. Canada, Ontario. University of Windsor, November 13, 2003.

AUTHORS PROFILE

A.Sankara Narayanan is presently working as a Technical Support in Department of Information Technology at Salalah College of Technology, Salalah, Sultanate of Oman. He has 9 years of Networking/System experience and 4 years of Information Security experience. He has published 7 international journals. His research interests include ethical hacking, computer forensics, malware and information Security.