

HIDING DATA COMMUNICATION USING STEGNOGRAPHY TECHNIQUE

Kirti Kakde¹

ABSTRACT

Steganography is the technique of hiding any secret information like password, data and image behind any cover file. The word steganography comes from the Greek Steganos, which means covered or secret and -graphy means writing or drawing. The purpose of steganography is covert communication-to hide the existence of a message from a third party. In this paper, a penetration testing tool Kali Linux is used for Image Steganography to hide secret message i.e. Text, Image, Audio and Video in an Image which makes it harder for unauthorized people to extract the original message.

Keywords: Steganography, Steghide, Kali Linux

I. INTRODUCTION

Many times, users on the internet have to send, share or receive confidential information. Due to rapid development in both computer technologies and Internet, the security of information is regarded as one of the most important factors of Information Technology and communication. Steganography has emerged as a powerful and efficient tool which provides high level for security particularly when it is combined with encryption.

STEGANOGRAPHY

Steganography is a combination of two words Stegano + Graptos. Stegano means “Covered” and Graptos means “Writing” which exactly means “cover writing”. So Steganography means covered writing. Steganography is a exclusive technique of hiding data in some medium so that it doesn't awaken doubt to the hackers. The key concept behind Steganography is that message to be transmitted is not detectable to the casual eye. In this, the sender embedded its message into the text, image, video, or audio file so that hackers will not be aware of the message. The most well-liked Steganographic methods used by spies contain invisible ink and microdots. People used design messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grow back and then saving it again when he arrived at his contact point to reveal the message.

¹ Asst.Prof., YMT College of Management, Kharghar, kirtik@ymtcollegeofmanagement.org

II. NEED OF STEGANOGRAPHY

One of the most important area which attracted by people is security which is related to internet and also related to communication. At present, security for hiding data is most popular technique which receives more attention than cryptography. Various methods such as cryptography, coding Steganography, etc. are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hides the data inside other data in such a way that no other person recipient, even know the existence of it. Terms used in Steganography are:

- Cover Image: The medium in which information is to be hidden. It may be an audio, video, image or a text file. Key: It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.
- Stego-image: A medium within which information is hidden.
- Message: The data to be hidden or to be extracted.

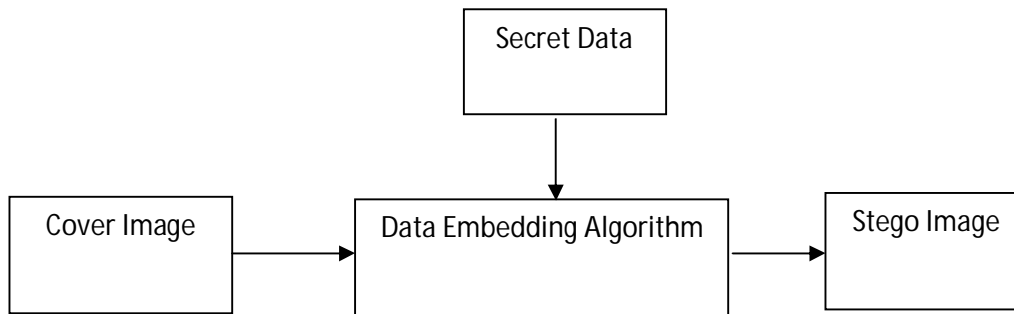


Fig.1 Steganography diagram

Steganography methods are classified based on cover media as follows:

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

III. PROBLEM DEFINITION

IMAGE STEGANOGRAPHY:

Images are the most popular cover objects for steganography. A message is embedded in a digital image (cover image) through an embedding algorithm by using secret key. The resulting stego image is transmitted to the receiver. On the other hand, it is processed by the extraction algorithm using the same key. During the transmission of the stego image, it can be monitored by some unauthenticated person who will only notice the transmission of an image but cannot guess the existence of the hidden image.

AUDIO STEGANOGRAPHY

Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound becomes inaudible in the presence of another louder audible sound. This property allows to select the channel in which to hide information. Although it is similar to images in steganography potential, the larger size of meaningful audio files makes them less popular to use than images.

VIDEO STEGANOGRAPHY

Video steganography is a technique to hide any kind of files or information into digital video format. Video (combinations of picture) is used as a carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g. 8.667 to 9) which is used to hide information in each of the images in the video, which is not noticeable by human eye. Video steganography uses such as H.264, MP4, MPEG, AVI or other video formats.

Below are some combinations of cover file and secret message types .

S.No	Cover File Type	Secret file type used
1.	.BMP	.DOC,.TXT,.WAV,.MP3,.XLS,.PPT,.AVI,.JPG,.EXE,.COM
2.	.JPG	.BMP,.DOC,.TXT,.WAV,.MP3,XLS,.PPT,.JPG,.COM
3.	.DOC	.TXT
4.	.WAV	.BMP,.JPG,.TXT,.DOC
5.	.AVI	.TXT,.JPG,.WAV

IV. Steganography Tools

a. Steghide

Steghide is a steganography program that is able to hide data in various kinds of image- and audio-files. The color- respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests.

Features:

- compression of embedded data
- encryption of embedded data
- embedding of a checksum to verify the integrity of the extracted data
- support for JPEG, BMP, WAV and AU files

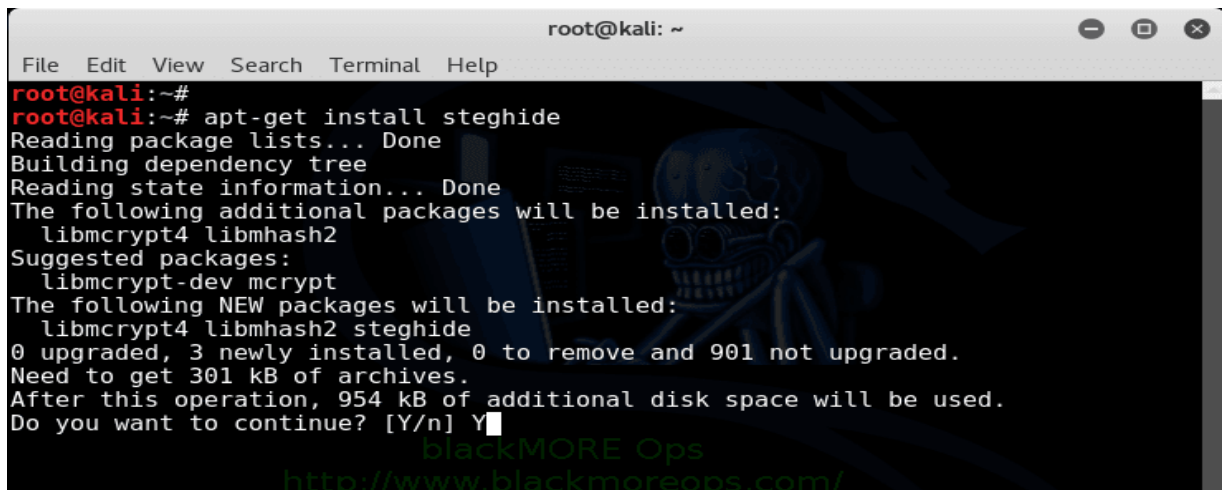
b. StegoSuite

Stegosuite is used to hide information in image files.

Features:

- BMP, GIF and JPG supported
- AES encryption of embedded data
- Automatic avoidance of homogenous areas (only embed data in noisy areas)
- Embed text messages and multiple files of any type
- Easy to use[4]

V. Hiding data in image using steghide

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'apt-get install steghide' being executed. The output indicates that three new packages (libmhash2, libmhash2-dev, and steghide) will be installed, along with two additional packages (libmhash2 and libmhash2-dev). The terminal also shows the disk space requirements and a confirmation prompt '[Y/n] Y'. At the bottom of the terminal, there is a watermark for 'blackMORE Ops' and the website 'http://www.blackmoreops.com/'.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# apt-get install steghide
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libmhash2 libmhash2-dev
Suggested packages:
  libmhash2-dev mhash
The following NEW packages will be installed:
  libmhash2 libmhash2-dev steghide
0 upgraded, 3 newly installed, 0 to remove and 901 not upgraded.
Need to get 301 kB of archives.
After this operation, 954 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
blackMORE Ops
http://www.blackmoreops.com/
```

Hide text file in Image

A folder steghide is created in root home folder and placed picture.jpg and secret.txt file in there. picture.jpg file is used to hide secret.txt file.

To hide text file in Image in Kali Linux using steghide, following commands are used.

```
root@kali:~/steghide# steghide embed -cf picture.jpg -ef secret.txt

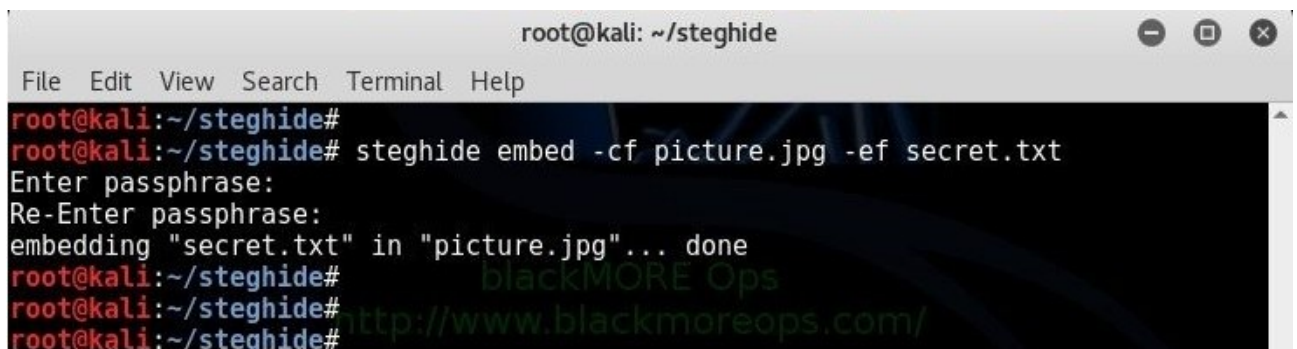
Enter passphrase:

Re-Enter passphrase:

embedding "secret.txt" in "picture.jpg"... done

root@kali:~/steghide#
```

This command will embed the file secret.txt in the cover file picture.jpg.

A screenshot of a terminal window titled "root@kali: ~/steghide". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the execution of the steghide embed command, including prompts for a passphrase and confirmation of embedding. A watermark for "blackMORE Ops" and a URL "http://www.blackmoreops.com/" is visible in the background.

```
root@kali:~/steghide
File Edit View Search Terminal Help
root@kali:~/steghide#
root@kali:~/steghide# steghide embed -cf picture.jpg -ef secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "picture.jpg"... done
root@kali:~/steghide#
root@kali:~/steghide#
root@kali:~/steghide#
```

We can email, share or do anything with this new picture.jpg file without having to worry about exposing data.

Extracting text file from Image

The receiver has to use steghide in the following way:

```
root@kali:~/steghide# steghide extract -sf picture.jpg

Enter passphrase:

the file "secret.txt" does already exist. overwrite ? (y/n)
y

wrote extracted data to "secret.txt".
```

If the supplied passphrase is correct, the contents of the original file secret.txt will be extracted from the stego file picture.jpg and saved in the current directory.

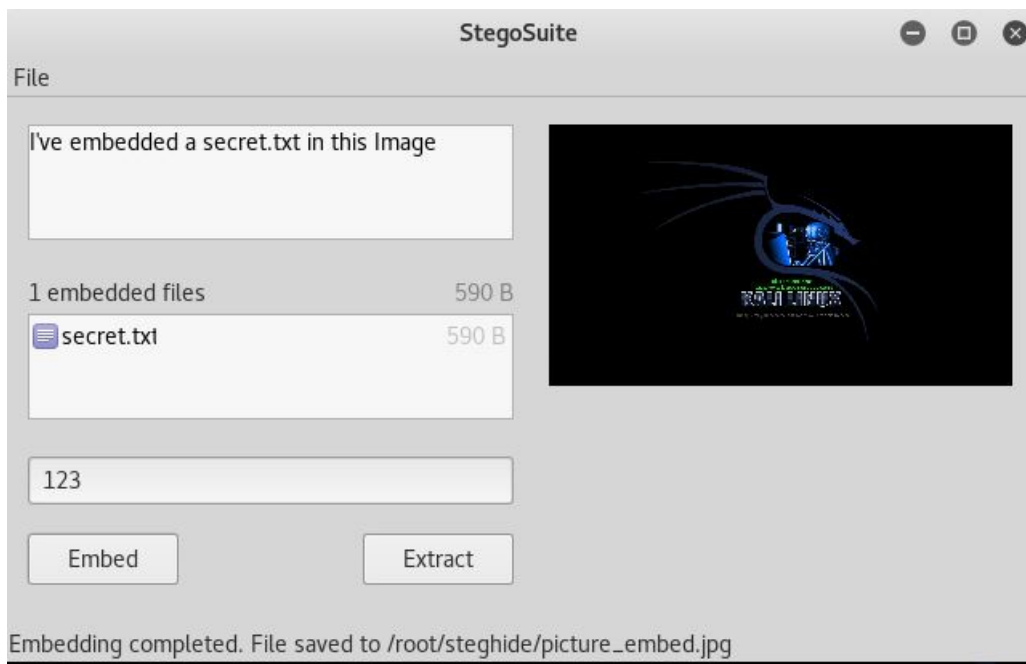
Check the content of the secret.txt which is extracted.

```
root@kali:~/steghide# head -3 secret.txt

Linux. It's been around since the mid '90s, and has since
reached a user-base that spans industries and continents.
For those in the know, you understand that Linux is
actually everywhere. It's in your phones, in your cars, in
your refrigerators, your Roku devices.
```

Embed text file in Image using Stegosuite

We can run it from Application menu (or you can just search it). Go to File > Open and open the image we want to use. Right-click on the file section and select add files and select your secret.txt file. Type in a passphrase and click on embed. Few seconds and it will create a new file picture_embed.jpg



VI. Applications

1. Spies: Intelligence and counter intelligence agencies.
2. Militaries: Unobstructive communication.
3. Terrorist: It arouses less suspicion.
4. Copyright: Watermarks and fingerprints.
5. Spam: Email forgery.

VII: CONCLUSION

It enhances Confidentiality of information and provides a means of communicating privately. Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography, hides the existence of message such that intruder can't even guess that communication is going on and thus provides a higher level of security. A penetration testing tool Kali Linux is used for the purpose such as penetration testing and digital forensics.

REFERENCES

1. Ramanpreet Kaur, Prof. Baljit Singh, "Survey and Analysis of various Steganographic Techniques" , ISSN:2250-3676, Volume-2, Issue-3, 561-566
2. T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview Of Image Stegnography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
3. Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques" , International Journal of Advanced Science and Technology Vol. 54, May, 2013
4. <https://www.blackmoreops.com/2017/01/11/steganography-in-kali-linux-hiding-data-in-image>