

Steganography

Steganography is the method of hiding information within a file. You can hide data in an image, audio, or video, or in a network protocol. There are many tools to practice steganography, like Steghide (an image or audio file) or OpenPuff (an image, audio, or video file).

In this document, we use Steghide to demonstrate how steganography works in an image file.

Embed a text file in an image file. Steghide comes with encryption, so you need to enter a password to extract it later, or leave it unencrypted by entering twice.

```
steghide embed -ef <your_secret_msg_file> -cf <filename_to_be_cover>
```

```
(yoky@yoky)-[~/steg/hallway]
$ touch flag.txt

(yoky@yoky)-[~/steg/hallway]
$ nano flag.txt
# Source Code of
ZoeYzoeY(1).ovpn

(yoky@yoky)-[~/steg/hallway]
$ steghide embed -ef flag.txt -cf Hallway.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "flag.txt" in "Hallway.jpg" ... done
```

Extraction of a file

```
steghide extract -sf <filename>
```

```
(yoky@yoky)-[~/steg/hallway]
$ steghide extract -sf Hallway.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
starting point_ZoeYzoeY.ovpn

(yoky@yoky)-[~/steg/hallway]
$ ls
flag.txt Hallway.jpg

(yoky@yoky)-[~/steg/hallway]
$ cat flag.txt
Hiding_in_the_dark
```

I add some comment to the image file so people who will extract it have some clue to the encryption password.

```
(yoky@yoky)-[~/steg/hallway]
$ ls
Hallway.jpg

(yoky@yoky)-[~/steg/hallway]
$ mogrify -set comment "old building" Hallway.jpg

(yoky@yoky)-[~/steg/hallway]
$ exiftool Hallway.jpg
ExifTool Version Number      : 12.41
File Name                    : Hallway.jpg
Directory                   : .
File Size                    : 618 KiB
File Modification Date/Time  : 2023:02:02 19:04:04+08:00
File Access Date/Time       : 2023:02:02 19:04:04+08:00
File Inode Change Date/Time  : 2023:02:02 19:04:04+08:00
File Permissions             : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Comment                     : old building
```