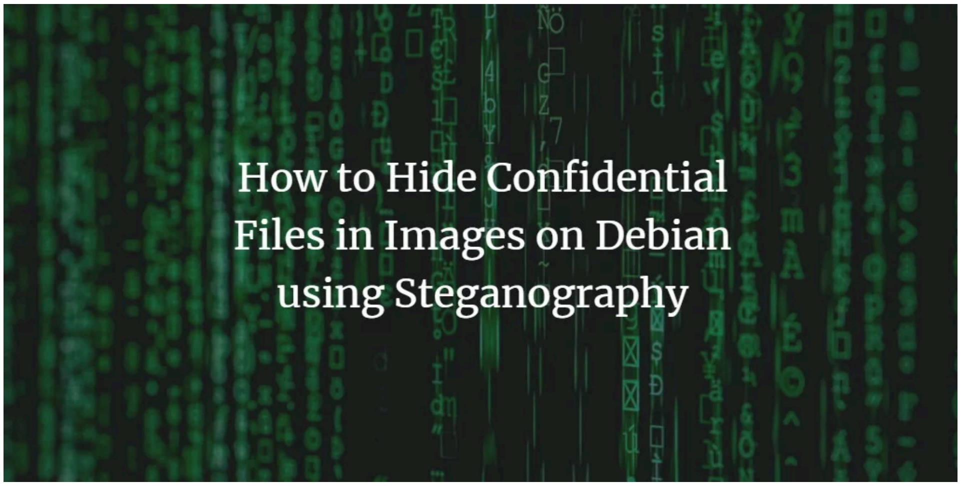


How to Hide Confidential Files in Images on Debian using Steganography

April 24, 2020 by Karim Buzdar

Sometimes we have to hide our data to protect it from third-party access to the system. However, one way to achieve this is through encryption. But today we are going to talk about another method, namely steganography, which makes it possible to hide the existence of secret data in order to keep communications private.

In steganography, the confidential data is embedded in a camouflage file in such a way that no one but the sender and recipient can suspect the existence of confidential information in it. It is also useful if you want to send confidential data to someone without compromising security. The cover file in which you want to hide the confidential data can be a text, picture, audio or any video file.

Why Steganography?

Although steganography is not as secure as encryption, it has several other advantages, such as the fact that no one will notice it because the embedded file looks like an ordinary file. On the other hand, an encrypted file also generates curiosity in the viewers.

In this article, we will explain how to hide the confidential files in an ordinary image file using various tools (including the command line and the GUI).

Note that we have done the procedure mentioned in this article on a Debian 10 system.

Method 1: Through the Steghide utility (command line)

Steghide Installation

First, launch the Terminal in your OS. Go to the Activities tab in the top left corner of your desktop. Then search for the Terminal application by typing the relevant keyword in the search bar. From the results, click on the Terminal icon to open.

Update the system's repository index using the following command:

Latest Tutorials

[How to Install ISPConfig Hosting Control Panel with Apache Web Server on Ubuntu 24.04]

[How to Test your Email Server (SMTP) Using the Telnet Command]

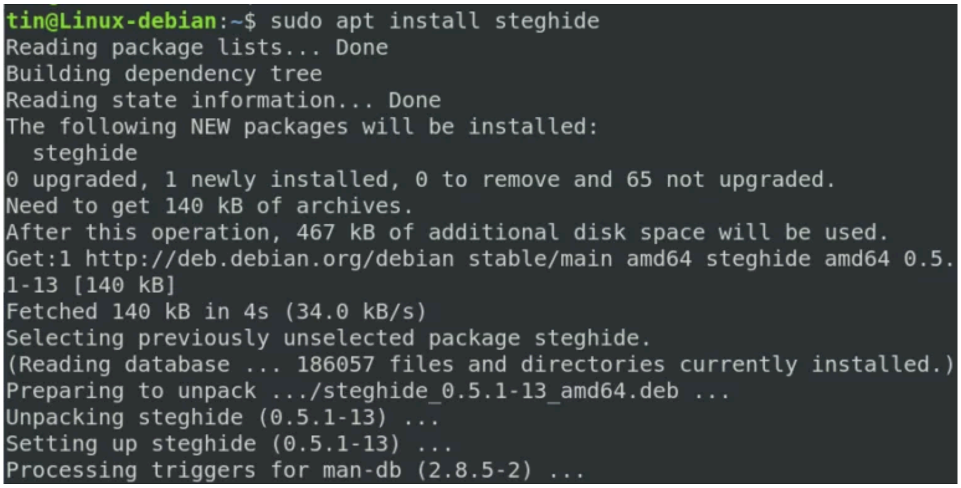
[Managing Network Interfaces and Settings on Ubuntu 24.04 with nmcli]

[Using Restic Backup on Ubuntu 24.04]

```
$ sudo apt update
```

Then install Steghide using the apt command as follows:

```
$ sudo apt install steghide
```



```
tin@Linux-debian:~$ sudo apt install steghide
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  steghide
0 upgraded, 1 newly installed, 0 to remove and 65 not upgraded.
Need to get 140 kB of archives.
After this operation, 467 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian stable/main amd64 steghide amd64 0.5.
1-13 [140 kB]
Fetched 140 kB in 4s (34.0 kB/s)
Selecting previously unselected package steghide.
(Reading database ... 186057 files and directories currently installed.)
Preparing to unpack .../steghide_0.5.1-13_amd64.deb ...
Unpacking steghide (0.5.1-13) ...
Setting up steghide (0.5.1-13) ...
Processing triggers for man-db (2.8.5-2) ...
```

The system might prompt for confirmation with **Y/n** option, hit **y,** and then **Enter** to confirm. After that, the Steghide will be installed on your system.

Embedding files with Steghide

To hide a confidential file using Steghide embed feature, you will need the file that you want to hide and an image or audio file in which you want to hide the data. It supports embedding the file into WAV, JPEG, AU, BMP formats.

The syntax to embed a file into a JPEG format is:

```
$ steghide embed -ef <file-to-embed> -cf <image.jp>
```

Installing phpMyAdmin on Rocky Linux 9 and Securing it with Let’s Encrypt SSL

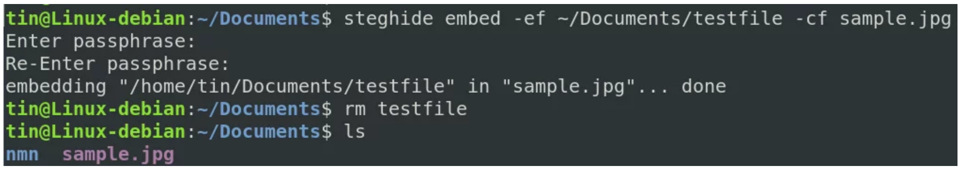
In our example, the file named “testfile” is in ~/Documents directory and we want to embed it into the “sample.jpg” image file. So will first navigate to the ~/Documents directory and then run the embed command. Alternatively, you can also mention the complete path to the file instead of navigating to the directory.

Example:

```
$ steghide embed –ef ~/Documents/testfile –cf sample.jpg
```

Then enter the paraphrase twice for embedding the file. This paraphrase will be used when you need to extract or decrypt the file. If you do not want to set a paraphrase for embedding, just hit Enter twice. After that, your file will be embedded.

Now we can only keep the image file “sample.jpg” while deleting the confidential file, that is the “testfile” in our example.



```
tin@Linux-debian:~/Documents$ steghide embed -ef ~/Documents/testfile -cf sample.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "/home/tin/Documents/testfile" in "sample.jpg"... done
tin@Linux-debian:~/Documents$ rm testfile
tin@Linux-debian:~/Documents$ ls
nmn  sample.jpg
```

File Extraction

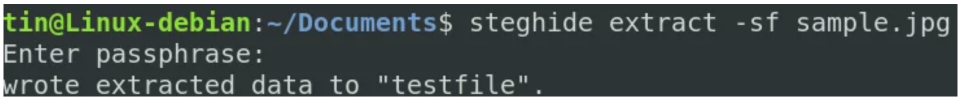
When you need to extract the confidential file from the image file, use the following syntax:

```
$ steghide extract –sf image.jpg
```

Example:

```
$ Steghide extract –sf sample.jpg
```

The system will ask for the passphrase you have set while embedding the file into the image file. Enter the passphrase and your confidential file will be extracted from the image file.



```
tin@Linux-debian:~/Documents$ steghide extract -sf sample.jpg
Enter passphrase:
wrote extracted data to "testfile".
```

Remove/Uninstall

In case, you want to remove the Steghide from your system, run the following command in the Terminal:

```
$ sudo apt remove steghide
```

Method 2: Through the Outguess utility (command line)

Outguess is also a Steganography command-line tool that lets secret information be inserted into the redundant bits of data sources. With Outguess, you can also hide the confidential data inside of an image file.

Outguess Installation

Open the Terminal and update the system's repository index using the following command:

```
$ sudo apt update
```

Now install the Outguess as follows:

```
$ sudo apt install outguess
```

The system might prompt for confirmation with **Y/n** option, hit **y** and then **Enter** to confirm. After that, the Outguess will be installed on your system.

Embedding files with Outguess

To embed a confidential file using Outguess, you will need the file that you want to hide and a image file in which you want to hide the data.

Some of the flags we will use with Outguess are:

d: Specify the filename which contains a message that needs to be hidden.

k: Specify the secret key you want to use for encryption

r: Extracts the message from the encrypted file

The syntax to embed a file into a JPEG format is:

```
$ outguess -d examplefile.txt image.jpg image-output.jpg
```

The examplefile.txt will be embedded in to a new "image-output.jpg" file.

In order to set the password for the embedded file, the syntax would be:

```
$ outguess -k “secret key” -d examplefile.txt image.jpg image-ou
```

If your file is residing at some directory other than ~/Home directory, you will have to navigate to that directory and then run the above command. Alternatively, you can mention the complete path to the files.

In our case, both the confidential file and the image file are residing at the ~/Documents directory, and we want the encrypted file to be also in the same directory. An example of this would be:

```
$ cd ~/Documents
```

```
$ outguess -k “123” -d testfile sample.jpg sample-out.jpg
```

After running this command, a "sample-out.jpg" file will be created in our current directory. Once the encryption is completed, you can remove the original confidential file and just keep the output image file which will be used later for extracting the confidential file.

File Extraction

In order to retrieve the original confidential file from the output image file it was embedded in, use the following syntax:

```
$ outguess -r image-output.jpg secret.txt
```

If you have specified the secret key during the encryption, then the syntax would be as follows:

```
$ outguess -k “secret key” -r image-output.jpg secret.txt
```

An example of this would be:

```
$ outguess -k “123” -r sample-out.jpg testfile
```

The Outguess method also verifies statistics after extraction to ensure the original file is exactly as it was before embedding.

Remove/Uninstall

In case, you want to remove the Outguess from your system, simply execute the following command in the Terminal:

```
$ sudo apt-get remove outguess
```

Method 3: Through the Stegosuite tool (UI)

The Stegosuite is a GUI based free and open-source tool that can be sued to hide confidential file in an image file.

Stegosuite Installation

In order to install Stegosuite, first update the system repository index. Execute the following command in Terminal to do so:

```
$ sudo apt update
```

Then execute the following command to install Stegosuite:

```
$ sudo apt install stegosuite
```

The system might prompt for confirmation with **Y/n** option, hit **y** and then **Enter** to confirm. After that the Stegosuite will be installed on your system.

Launch Stegosuite

Once installed, you can launch Stegosuite either via command line or via GUI.

In order to launch Stegosuite via command line, simply type *stegosuite* in your Terminal as follows:

```
$ stegosuite
```

To launch Stegosuite via GUI, hit the super key on your keyboard and type *stegosuite*. When the Stegosuite icon appears as follows, click on it to launch it.

Embedding files with Stegosuite

When the Stegosuite will be launched, you will see the following view. In order to hide the confidential file in an image file, first load the image file by navigating to **File** > **Open.**

Then select any image file (in MP, GIF, JPG or PNG format) in which you want to hide the confidential file. Once you selected the file, click **Ok**.

Now the image file will be loaded in to the Stegosuite window. Now follow the below simple steps:

1. Type any secret message.

2. Right-click on the blank area in the second field and choose **Add file**. Then select the confidential file you want to embed in an image file.

3. Type a password that will be used when extracting the file.

Once you have performed the above steps, click the **Embed** button as follows:

Now your confidential file will be embedded and saved with the name “filename_embed” format. As the file name contains “embed“, so it is better to rename this file later to make it look ordinary and unsuspicious.

Now you can delete the original confidential file from you system and keep only the output embedded image file.

File Extraction

In order to extract the confidential file from the image file it was embedded in to, follow the below simple steps:

open the embedded image file in File Manager. Then right-click and select **Open With Other Application** as follows:

Then from the **Select Application** dialog box, click **Stegosuite**.

Now the file will be loaded in to the Stegosuite application. Enter the password for the file and click **Extract** button.

Now the original confidential file will be extracted to. your system

Remove/Uninstall

In case, you want to remove the Outguess from your system, simply execute the following command in the Terminal:

```
$ sudo apt remove stegosuite
```

Conclusion

In this article, we have discussed both the command line and the GUI based tools to hide the confidential files in an image file.

Using either of the above-discussed Steganography tools, you can conceal the confidential data in a seemingly ordinary looking image file.

Debian, Linux, Shell

‹ 5 Ways to check how much RAM is installed and used on CentOS 8
› How to install vim editor on Rocky Linux

Privacy Policy Imprint