

Steganography

Introduction:

The main goal of the lab is to learn about the relevance of steganography and its tools in terms of data concealment.

Activities:

This lab exercise improved participants' understanding of the idea of steganography as well as the method of concealing data in a variety of file types. Additionally, participants gained a general understanding of watermarking in cryptography. In addition, the practical knowledge gained via actual use of Steghide and Stegosuite commands and their applications. An in-depth comprehension of the other facet of the steganography detection tool in addition to a general grasp of the steganography detection tool is required.

Discussion:

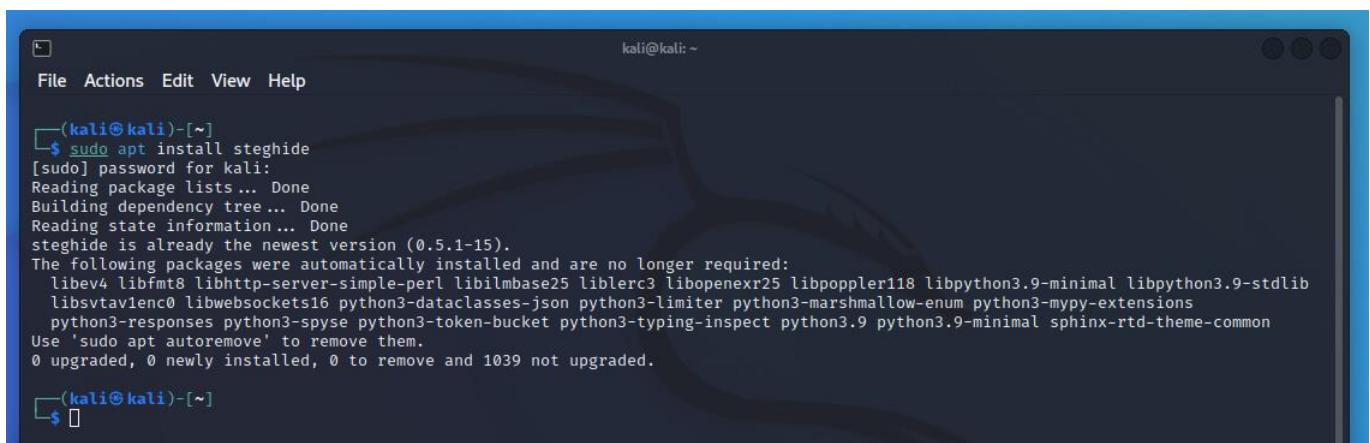
Steganography is a technology that is used to conceal sensitive information or protect it inside an ordinary file so that it cannot be discovered by unauthorized parties. Steganography is also known as "stealth computing." Its primary function is to ensure the confidentiality of the information. Text steganography, picture steganography, audio steganography, video steganography, and network steganography are all forms of steganography.

The process of watermarking involves superimposing a piece of text or an image on a photo file or document in order to verify the validity of the file's owner. Simply said, the portion of the phrase or the emblem that has supplied the concerned owner with their own identity.

The primary goal of steganography is to conceal information, while the watermarking technique employed in cryptography serves both that goal and that of protecting the information. In a similar fashion, watermarking is used to protect the copyright of their work as well as promote both the picture and text associated with their brand (Bhandari, n.d.). On the other hand, the goal of steganography is not so much to draw attention to anything as it is to conceal information via the use of covert communications. In addition, the process of watermarking takes a significant amount of time, but the method of steganography makes it exceedingly challenging to conceal even a little bit of information.

There are a variety of applications for steganography, including professional and non-professional settings. When used for professional reasons, this method transmits or exchanges information pertaining to businesses; when used for non-professional purposes, however, it is most often used for illicit operations (Ginni, 2022). A straightforward watermarking technique is used in order to strengthen the trademark. We are able to advertise the company while also concealing details by using watermarking. The use of watermarks during commerce may provide the company with more opportunities for promotional activity. In addition, the attackers have the capability of delivering an assault by using steganography (Stanger, 2020).

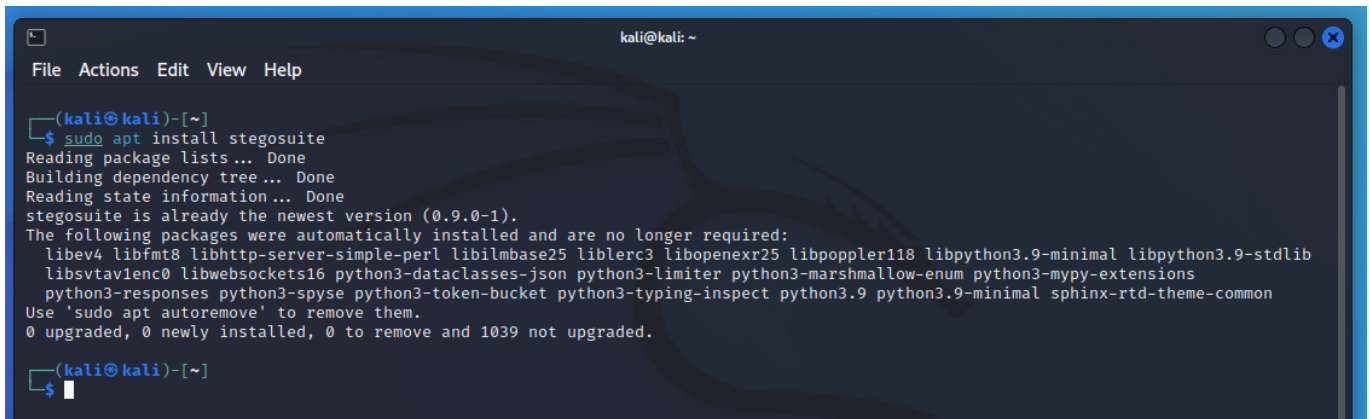
Steghide is a steganography application for concealing data inside multimedia files like JPEGs and MP3s (Bibi, 2021).

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the command 'sudo apt install steghide' being executed. The output indicates that steghide is already installed at version 0.5.1-15. It also lists several packages that were automatically installed and are no longer required, such as libev4, libfmt8, and python3-dataclasses-json. The terminal ends with a prompt for the user to enter a command.

```
(kali@kali)-[~]
$ sudo apt install steghide
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
steghide is already the newest version (0.5.1-15).
The following packages were automatically installed and are no longer required:
 libev4 libfmt8 libhttp-server-simple-perl liblmbase25 liblerc3 libopenexr25 libpoppler118 libpython3.9-minimal libpython3.9-stdlib
 libsvtav1enc0 libwebsockets16 python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions
 python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1039 not upgraded.
(kali@kali)-[~]
$
```

Figure 1: Installation of Steghide

In a manner similar to that of the Steghide, the Stegosuite may be used to conceal information inside picture files. Stegosuite, on the other hand, is a graphical steganography tool, but Steghide is not (Ialitmohantiwari7700, 2022).

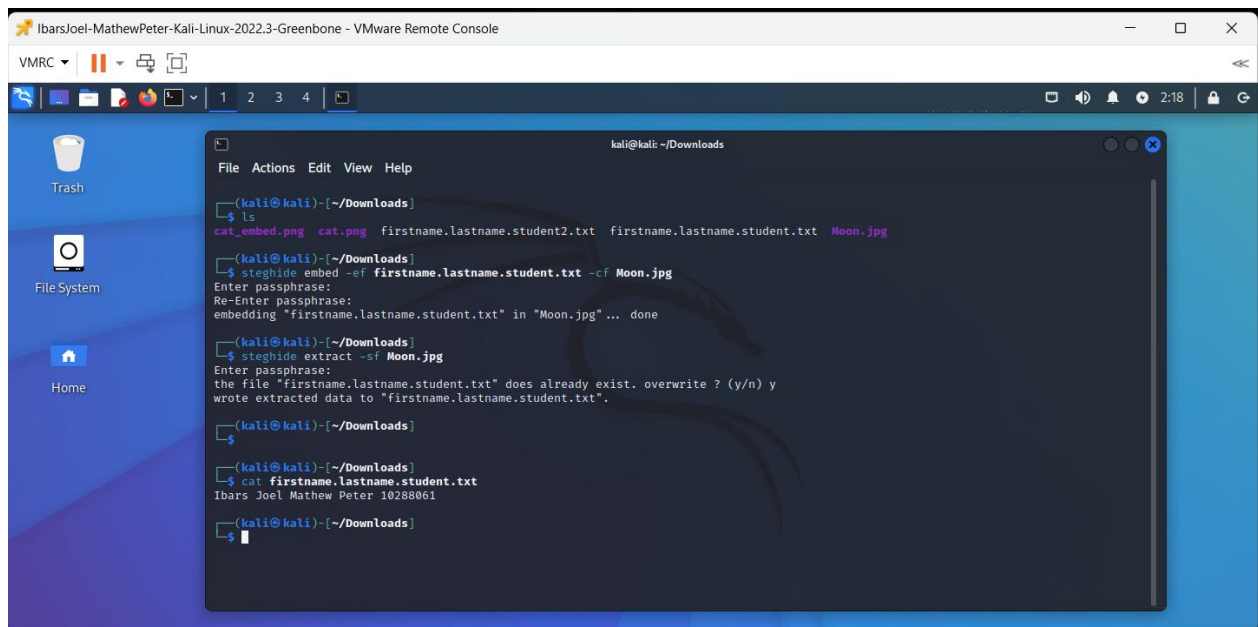


```
(kali@kali)-[~]
$ sudo apt install stegosuite
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
stegosuite is already the newest version (0.9.0-1).
The following packages were automatically installed and are no longer required:
 libev4 libfmt8 libhttp-server-simple-perl libilmbase25 liblerc3 libopenexr25 libpoppler118 libpython3.9-minimal libpython3.9-stdlib
 libsvtavien0 libwebsockets16 python3-dataclasses-json python3-limiter python3-marshmallow-enom python3-mypy-extensions
 python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1039 not upgraded.

(kali@kali)-[~]
$
```

Figure 2: Installation of Stegosuite

The main purpose of Steghide is to hide the data into the image file in command lines. The overall demonstration of the Steghide process file, naming firstname.lastname.steghide is uploaded for reference.



```
(kali@kali)-[~/Downloads]
$ ls
cat_embed.png  cat.png  firstname.lastname.student2.txt  firstname.lastname.student.txt  Moon.jpg
(kali@kali)-[~/Downloads]
$ steghide embed -ef firstname.lastname.student.txt -cf Moon.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "firstname.lastname.student.txt" in "Moon.jpg" ... done
(kali@kali)-[~/Downloads]
$ steghide extract -sf Moon.jpg
Enter passphrase:
the file "firstname.lastname.student.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "firstname.lastname.student.txt".
(kali@kali)-[~/Downloads]
$
(kali@kali)-[~/Downloads]
$ cat firstname.lastname.student.txt
Ibars Joel Mathew Peter 10288061
(kali@kali)-[~/Downloads]
$
```

Figure 3: Steghide Process

The key purpose of Stegosuite is to hide the information with graphical tools. The overall demonstration of the Stegosuite process video file, naming firstname.lastname.stegosuite is uploaded for reference.

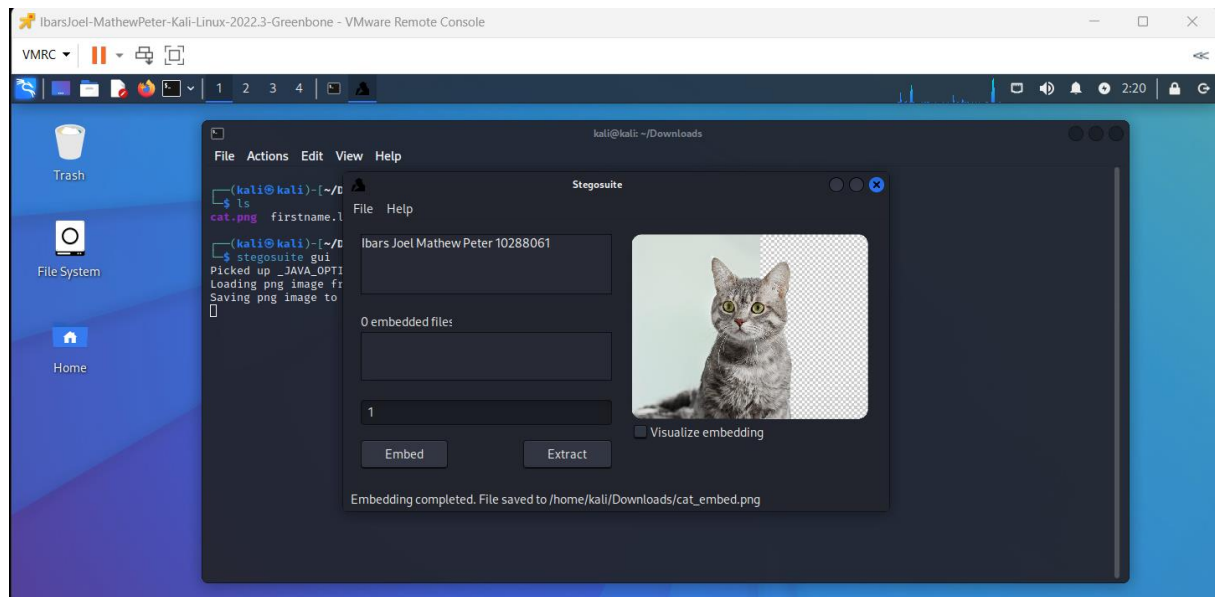


Figure 4: Stegosuite – Embedding Process

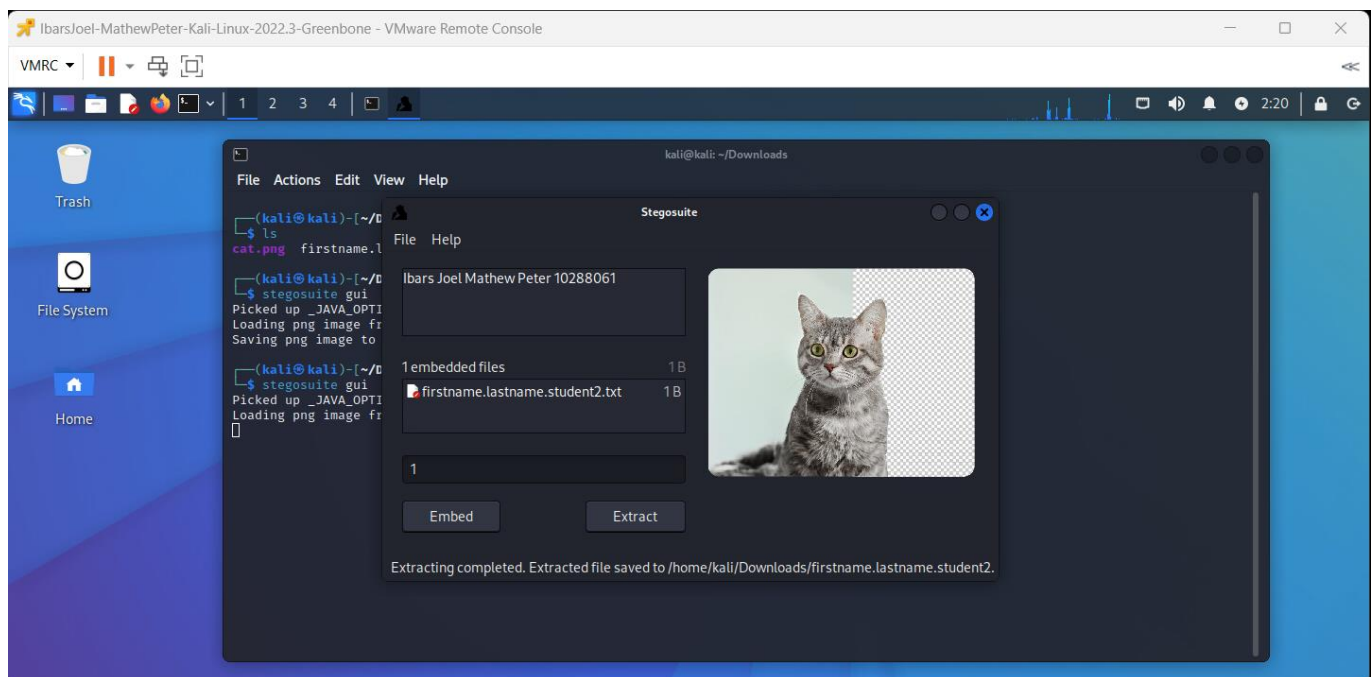


Figure 5: Stegosuite – Extraction Process

There are several tools also available for detect the hidden message that contains Steganography files. Some of the files are:

- StegExpose
- StegDetect
- VSL

- StegSpy
- Stegbreak

These are the some of tools that are used to detect the hidden data in an image.

StegExpose is a simple program that functions as a tool for examining certain directory pictures in order to determine whether or not such images contain any hidden messages. It makes use of more sophisticated algorithms that are able to give photos and the outcomes of their processing. It is a tool that works across several platforms (Suleman, 2018). In addition to being an open-source steganography program, Stegdetect can handle a variety of steganographic approaches. It can analyze photos produced by programs such as Jsteg and JPHide to determine whether or not they contain steganographic data.

An application that offers a framework that can be utilized with numerous techniques at the same time and also executes sophisticated procedures is known as the "Virtual Steganographic Laboratory," or VSL for short. VSL is an abbreviation for "Virtual Steganographic Laboratory" (Panhalkar, n.d.).

Both Steghide and StegoSuite are considered to be the most important tools for steganography. In a broad sense, these methods are used in order to conceal data inside a variety of picture formats. The most significant distinction between these two programs is that Steghide uses a command-line interface, but Stegosuite is developed in Java and includes a graphical representation tool. Stegosuite is much more user-friendly. When it comes to file types, Steghide is compatible with JPEG, BMP, WAVE, and AU, while StegoSuite is compatible with BMP, GIF, and JPG. Both solutions provide an additional layer of protection by encrypting the embedded data. The data that is contained in StegoSuite is encrypted using AES(Steganography in Kali Linux – Hiding data in image, 2017).

In the process of steganography, using StegoSuite on a daily basis is the most effective choice available. The graphical depiction, which is much simpler to comprehend in comparison to Steghide, is the primary aim of this project. It may be challenging to finish the process using

Steghide since it is based on a command line; nevertheless, StegoSuite, which is an enhanced version of Steghide and a better alternative to operating in a contemporary day, is the successor to Steghide.

Steganography may also be used to conceal information via the use of audio and video. Through the use of audio steganography, the information may be concealed by embedding it inside the audio signals. This is accomplished by modifying the binary sequence of the audio file that corresponds to the hidden information. However, carrying out this particular sort of steganography is more difficult than carrying out steganography that is connected to images. The parity encoding technique, the least significant bit encoding method, the phase coding method, and the spread spectrum approach are some of the audio steganography methods (Choudary, 2022).

In a similar manner, video steganography is used in order to conceal the information inside the framework of digital video. The fact that we are able to conceal a significant quantity of data is the primary advantage of the method. Video steganography may be broken down into two primary categories: the first involves concealing information in the uncompressed raw video and then compressing it at a later time, and the second involves concealing information directly inside a compressed data stream (Choudary, 2022).

Conclusion:

This laboratory exercise increased my understanding of the steganography concept while also highlighting the significance of data concealing and watermarking. In addition, the real-time execution of the Steghide and Stegosuite applications offered an overview of the techniques for concealing data as well as the manner in which the data was concealed in the various kinds of files. In a similar vein, a broad perspective regarding the steganography detection tools and the many sorts of steganography techniques other than the picture steganography method.

References:

- Bhandari, S. (n.d.). *Difference Between Watermarking and Steganography*. Retrieved from AskAnyDifference.com: <https://askanydifference.com/difference-between-watermarking-and-steganography/>
- Bibi, K. (2021). *Steghide tutorial for beginners*. Retrieved from Linux Hint: <https://linuxhint.com/steghide-beginners-tutorial/>
- Choudary, A. (2022, July 14). *Steganography Tutorial – A Complete Guide For Beginners*. Retrieved from Edureka: <https://www.edureka.co/blog/steganography-tutorial>
- Ginni. (2022, March 11). *What is the uses of Steganography?* Retrieved from Tutorialpoint: <https://www.tutorialspoint.com/what-is-the-uses-of-steganography>
- lalitmohantiwari7700. (2022, September 07). *Image Steganography using Stegosuite in Linux*. Retrieved from GeeksforGeeks: <https://www.geeksforgeeks.org/image-steganography-using-stegosuite-in-linux/>
- Panhalkar, T. (n.d.). *Detecting Steganography*. Retrieved from INFORSAVVY: <https://info-savvy.com/detecting-steganography/>
- Stanger, J. (2020, July 06). *The Ancient Practice of Steganography: What is it, How is it Used and Why Do Cybersecurity Pros Need to Understand it?* Retrieved from CompTIA: <https://www.comptia.org/blog/what-is-steganography#:~:text=The%20purpose%20of%20steganography%20is,be%20executed%20in%20clever%20ways.>
- Steganography in Kali Linux – Hiding data in image*. (2017, January 11). Retrieved from blackmoreops: <https://www.blackmoreops.com/2017/01/11/steganography-in-kali-linux-hiding-data-in-image/>
- Suleman, M. (2018, April 04). *3 FREE STEGANOGRAPHY DETECTION SOFTWARE TO DO STEGANALYSIS ON IMAGES*. Retrieved from ilovefreesoftware: <https://www.ilovefreesoftware.com/04/featured/free-steganography-detection-software-steganalysis-images.html>