

# Ejercicio 1

## Enunciado

Investiga que es la esteganografía

## Resolución

La esteganografía es el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos. El objetivo de la esteganografía es el de esconder el mensaje haciéndolo pasar desapercibido.

En informática se usa esta técnica principalmente incorporando texto en imágenes, vídeos o audio. Su uso puede ser meramente por diversión o por seguridad, haciendo posible la correspondencia secreta o protegiendo un archivo de copias ilegales.

La esteganografía se puede clasificar según los métodos utilizados, basándose en cómo y dónde se ocultan los datos.

- **Técnicas basadas en la inserción** (Insertion-Based). Se basa en insertar datos en un archivo sin afectar la representación de este, aunque si se produce un incremento en su tamaño.
- **Técnicas basadas en la sustitución** (Substitution-Based). Se basa en sustituir ciertas partes de un archivo por los datos que se quieren ocultar. Con este método hay que tener cuidado ya que puedes llegar a sobrescribir información hasta tal punto de hacerlo inservible o visualmente defectuoso.
- **Técnicas de generación** (Generation-Based). Este método ayuda a evitar la detección de la esteganografía, con esta técnica se coge el archivo a ocultar y se usa para crear el archivo contenedor.

En cuanto a ciberseguridad se refiere, la esteganografía presenta un grave problema debido a la difícil detección que puede llegar a suponer una realizada con un cierto nivel de calidad. La práctica de detectar la esteganografía es llamada “esteganoanálisis”. Los diferentes tipos de esta técnica son:

- **Esteganoanálisis manual**. Consiste en buscar de forma manual diferencias entre el archivo original y el esteganografiado, buscando cambios en la estructura. Para esta técnica es necesario tener el archivo original y es casi imposible descifrar el mensaje.
- **Esteganoanálisis estadístico**. Es una técnica lenta para la que es necesaria usar software especializado, coteja en el caso de las imágenes la frecuencia de distribución de colores. Los mensajes ocultos son casi imposibles de detectar con este método.

## Práctica

Para realizar esta práctica lo haré desde una máquina virtual con Linux. El primer paso que realizo es el de descargar la herramienta con la que voy a realizar el ejercicio, la herramienta es "steghide".

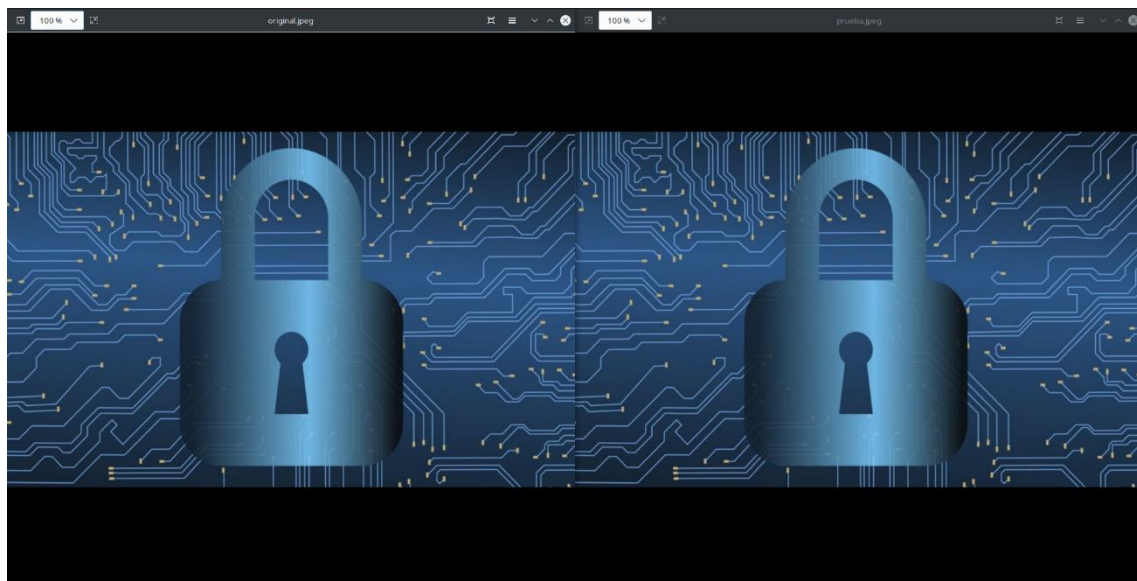
```
usuario@pruebas-ubuntu:~$ sudo apt-get install steghide
```

Una vez instalado, descargo una fotografía (prueba.jpeg) y creo un archivo de texto (ocultar.txt). Introduzco el siguiente comando:

```
usuario@pruebas-ubuntu:~$ echo "prueba esteganografía" > ocultar.txt
usuario@pruebas-ubuntu:~$ steghide embed -cf prueba.jpeg -ef ocultar.txt
```

Ahora compruebo la imagen modificada frente a la original para ver si hay un cambio significativo.

```
usuario@pruebas-ubuntu:~$ ls -sh original.jpeg
108K original.jpeg
usuario@pruebas-ubuntu:~$ ls -sh prueba.jpeg
112K prueba.jpeg
```



Para sacar el mensaje oculto, se usa el siguiente comando:

```
usuario@pruebas-ubuntu:~$ steghide extract -sf original.jpeg
Anotar salvoconducto:
steghide: no pude extraer ningun dato con ese salvoconducto!
usuario@pruebas-ubuntu:~$ steghide extract -sf prueba.jpeg
Anotar salvoconducto:
ya existe el archivo "ocultar.txt". ¿lo sobrescribo? (s/n) s
anote los datos extraidos e/"ocultar.txt".
usuario@pruebas-ubuntu:~$ cat ocultar.txt
prueba esteganografía
```

## Bibliografía

### Definición:

<https://es.wikipedia.org/wiki/Esteganograf%C3%ADa>

<https://www.kaspersky.es/blog/digital-steganography/18791/>

### Desarrollo:

<https://ciberseguridad.com/guias/esteganografia/>

<https://www.kaspersky.es/blog/digital-steganography/18791/>

<https://es.wikipedia.org/wiki/Estegoan%C3%A1lisis>

### Práctica:

[https://www.linuxadictos.com/steghide-esteganografia-para-ocultar-texto-en-  
imagenes.html](https://www.linuxadictos.com/steghide-esteganografia-para-ocultar-texto-en-<br/>imagenes.html)