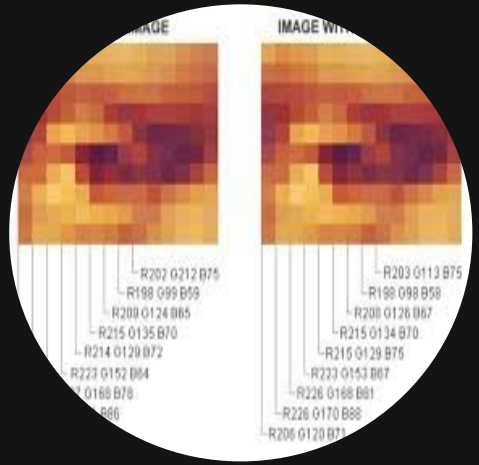
ocultamiento de
información en entornos
digitales

Estegano-grafía



Contenidos

1/

Historia
Criptografía
Motivación

Introducción

¿Qué es?

Ciencia que estudia y desarrolla métodos para ocultar información dentro de un medio portador.

Aprovecha la redundancia presente en los archivos portadores, permitiendo inyectar información **sin generar alteraciones perceptibles** a simple vista o al oído.

del griego ***steganos*** que significa "oculto" y ***graphos*** que significa "escrito".

Etimología

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE

DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE

ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE DECODE ENCODE


Antigua Grecia
Tallado de mensajes en madera, cubiertos en en cera
Antigua Roma
Uso de tintas invisibles foto y termosensibles
Siglo XX
Ocultamiento de mensajes en fotografías y tejidos
hoy
Esteganografía digitalizada

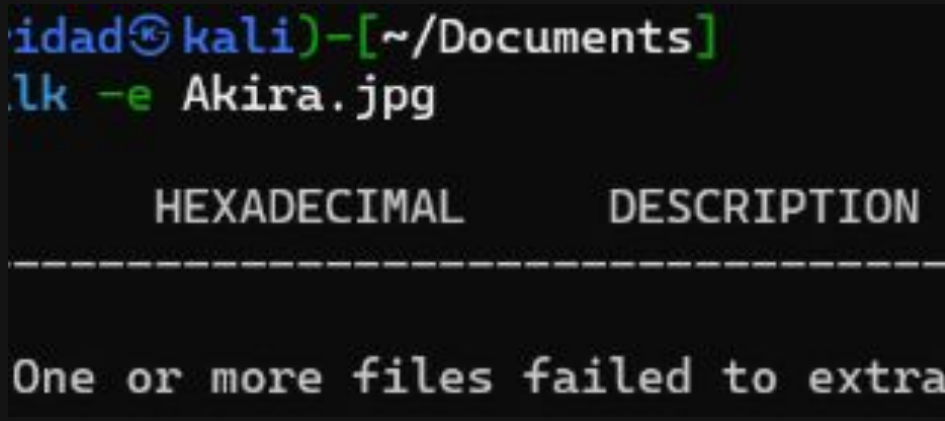
Historia

Campo que se ocupa del diseño, análisis y utilización de **algoritmos para el cifrado y descifrado** de información; *arte de escribir con clave secreta o de un modo enigmático.*

Cripto-grafía

La **criptografía** hace evidente que hay un mensaje cifrado; su objetivo es **proteger el mensaje**.

La **esteganografía** pretende pasar completamente **desapercibida**.



- Contextos donde mantener la privacidad y confidencialidad de las comunicaciones.
- Técnica especialmente valiosa en situaciones de alta sensibilidad.
- Posibilidad de ejecución automática de código.

Relevancia en seguridad

2/

Métodos y herramientas

Técnicas generales de ocultamiento y estegoanálisis
Implementación práctica
Comparación con herramientas

Aspectos fundamentales: **medio portador** que será utilizado, el **contenido y formato del mensaje** a ocultar, y la **técnica** específica empleada.

Algunos de los medios más comunes incluyen **imágenes** (PNG, BMP), **audio** (MP3, WAV), **video** (MP4, AVI) y **archivos de texto**.

Considera-ciones

- Least Significant Bit (LSB). Frecuentemente usada en imágenes y audio.
- Dominio de frecuencias.
- Planos de bits (Bit Planes).

Técnicas generales

Imágenes

La **elección del formato** del archivo portador afecta significativamente la **técnica de ocultamiento**, debido a que diferentes formatos poseen **características** propias.

- JPEG. Método de compresión con pérdida (lossy compression).
- PNG. Formato sin pérdida (lossless).

- **Sustitución del bit menos significativo (LSB).**
- **Enmascarado y filtrado.**
- **Técnicas de dominio transformado.**
- **Técnicas basadas en paletas.**
- **Sustitución de segmentos de imagen.**
- **Codificación de píxeles redundantes.**
- **Pixel Value Differencing (PVD)**

Audio y video

El ser humano sólo escucha un rango de frecuencia. LSB.
Los archivos de video generalmente son una colección de imágenes y sonidos. DCT.

Protocolos de comunicación UDP

Sistemas de archivos

Texto

Otros formatos

Ocultamiento de mensajes de texto

Ocultamiento de archivos completos

Extracción del contenido oculto

```
def to_bin ( data ):
def encode ( image_name , secret_data , n_bits = 2 ):
def decode ( image_name , n_bits = 1 , in_bytes = False ):
def set_args ():
```

Implementación práctica

Resultados

Técnica de sustitución de bits menos significativos (LSB) y bit planes sobre distintos tipos de archivos:

- texto plano,
- un documento PDF y
- un archivo de video.

En todos los casos se emplearon imágenes en formato PNG como archivos portadores.

Encoding

Archivos

```
python3
<programa>
-e
<imagen_origen>
-f
<archivo_a_ocultar>
-b
<cant_bits>
```

Invocación del programa

Texto

```
python3
<programa>
-e
<imagen_origen>
-t
<texto_a_ocultar>
-b
<cant_bits>
```

Decoding

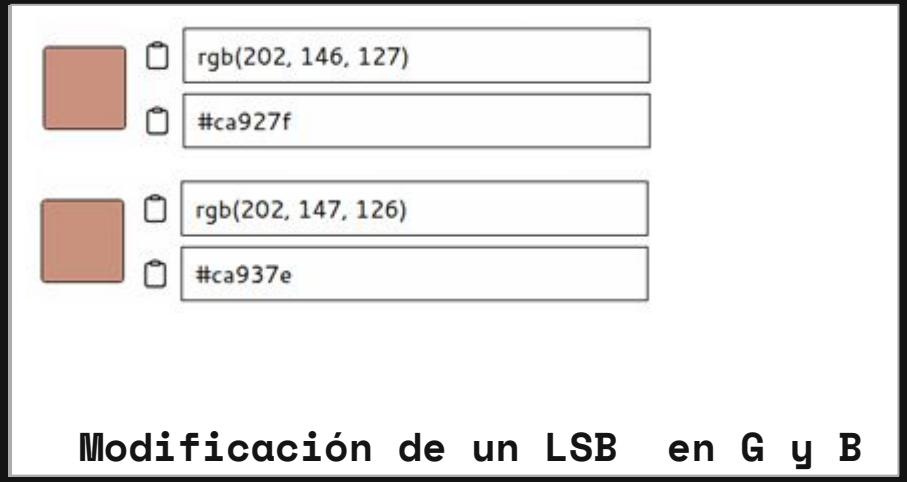
Archivos

```
<programa>
-d
<imagen_encoded>
-f
<archivo_decoded>
-b 1
<cant_bits>

(descarga)
```

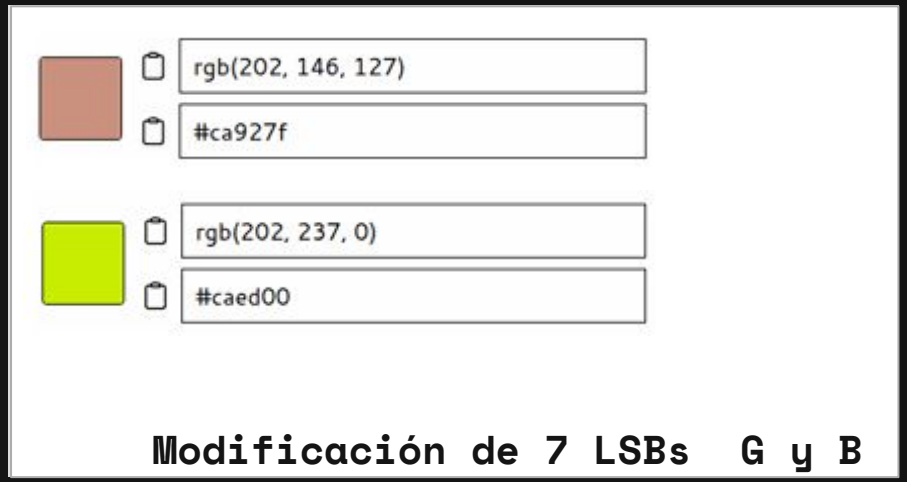
Invocación del programa

Texto

```
python3
<programa>
-d
<imagen_encoded>
-b 1
<cant_bits>

(impresion en linea
de comandos)
```



Modificación de un LSB en G y B



Modificación de 7 LSBs G y B

Funciona-miento

Los resultados obtenidos permiten reflexionar sobre el equilibrio entre capacidad de ocultamiento y perceptibilidad visual. En los casos donde se utiliza 1 bit LSB, tanto para ocultar texto como un archivo PDF, las imágenes resultantes no presentaron cambios perceptibles a simple vista.

Steghide → Oculta datos en diferentes tipos de imagen, audio y video. Soporta formatos JPEG, BMP, WAV y AU. Este programa cifra por defecto el archivo resultante

Strings → Herramienta predeterminada de Linux que muestra por pantalla las cadenas de caracteres de un archivo.

Binwalk → Permite buscar archivos binarios como archivos de imagen o audio embebidos en terceros. Permite la detección de datos agregados pero, por la naturaleza del cifrado, no puede siempre mostrarlos.

Otras herramientas

Casos de uso

- Comunicación segura
- Protección de derechos de autor mediante esteganografía y marca de agua oculta
- Protección de datos médicos en imágenes clínicas
- Espionaje gubernamental
- Comunicaciones terroristas encubiertas
- Distribución de malware

- Técnica que combina ocultamiento de información con explotación de vulnerabilidades del navegador. A diferencia del malware tradicional, que suele requerir la descarga o ejecución de archivos, Stegosploit permite insertar código malicioso directamente dentro de una imagen.
- Hay evasión y ejecución sin interacción.

Distribución de malware
Stegosploit

CAPTURA DE STEGOSPLOIT EN FUNCIONAMIENTO

4/

Ética

1/	La esteganografía oculta no solo el contenido, sino también la existencia de la comunicación.
2/	Puede combinarse con criptografía para mayor seguridad.
3/	Su eficacia depende del medio, método y canal utilizado.
4/	Presenta desafíos éticos cuando se usa con fines maliciosos (malware, espionaje).
5/	Herramientas de detección existen, pero no garantizan resultados sin análisis experto.

Conclusiones

“you get the best of both worlds”, **Hannah Montana**

¿Preguntas?

https://github.com/ludmilaprolygin/ProyectoSeguridad

1. A. Fadheli, “Steganography: How to Hide Data in Images in Python - The Python Code,” thepythoncode.com . https://thepythoncode.com/article/hide-secret-data-in-images-using-steganography-p ython . Consultado: 2 de julio de 2025.
2. N. Meghanathan, “Steganography.” Disponible: https://www.jsums.edu/nmeghanathan/files/2015/05/CSC439-Sp2013-10-Steganogra phy.pdf . Consultado: 2 de julio de 2025.
3. Material de clase - Seguridad en Sistemas. Profesor Lic. Leonardo de Matteis. Herramientas: criptografía. Departamento de Ciencias e Ingeniería de la Computación. Universidad Nacional del Sur.
4. “Selector de color RGB,” rgbcolorpicker.com . https://rgbcolorpicker.com/ . Consultado: 2 de julio de 2025.
5. “Universidad de Buenos Aires.” Disponible: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1765_SanchezArteagaJM.pdf . Consultado: 2 de julio de 2025.
6. Material de clase - Sistemas Operativos y Distribuidos. Profesor Lic. Gustavo Distel. Memoria principal. Departamento de Ciencias e Ingeniería de la Computación. Universidad Nacional del Sur.

Referencias

7. Wannida Sae-Tang and Adisorn Sirikham, “Image Steganography-based Copyright and Privacy-Protected Image Trading Systems,” ECTI Transactions on Computer and Information Technology (ECTI-CIT) , vol. 17, no. 3, pp. 358–375, Aug. 2023, doi: https://doi.org/10.37936/ecti-cit.2023173.252500.
8. D. Grover, “Steganography for identifying ownership of copyright,” Computer Law & Security Review , vol. 14, no. 2, pp. 121–122, Mar. 1998, doi: https://doi.org/10.1016/s0267-3649(97)82141-3 .
9. Hua, C., Wu, Y., Shi, Y., Hu, M., Xie, R., Zhai, G., & Zhang, X. P. (2023). Steganography for medical record image. Computers in biology and medicin e, 165, 107344. https://doi.org/10.1016/j.compbiomed.2023.107344
10. A. Nag, “Low-Tech Steganography for Covert Operations,” International Journal of Mathematical Sciences and Computing , vol. 5, no. 1, pp. 18–30, Jan. 2019, doi: https://doi.org/10.5815/ijmsc.2019.01.02 .
11. S. Murphy, “Steganography-the New Intelligence Threat EWS 2004 Subject Area Intelligence.” Disponible: https://apps.dtic.mil/sti/tr/pdf/ADA520517.pdf . Consultado: 5 de julio de 2025.
12. M. Warkentin, E. Bekkering, and M. Schmidt, “Steganography: Forensic, Security, and Legal Issues,” Journal of Digital Forensics, Security and Law , vol. 3, no. 2, 2008, doi: https://doi.org/10.15394/jdfsl.2008.1039 .

Referencias

13. Vielhauer, C., Loewe, F., & Pilgermann, M. (2025). Towards modeling hidden & steganographic malware communication based on images. In Proceedings of the 2025 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '25) (pp. 52–63). Association for Computing Machinery. doi: https://doi.org/10.1145/3733102.3733152
14. J. Fridrich, “Esteganálisis,” Academic Press , 2007, págs. 349–381. doi: https://doi.org/10.1016/B978-012369476-8/50016-6 . Consultado: 8 de julio de 2025.
15. J. De, T. Ahmad, and F. Han, “Comprehensive Survey on Image Steganalysis Using Deep Learning,” Array , pp. 100353–100353, Jun. 2024, doi: https://doi.org/10.1016/j.array.2024.100353 . Consultado: 8 de julio de 2025.
16. Kali, “Kali Tools | Kali Linux Tools,” Kali Linux . https://www.kali.org/tools/ . Consultado: 8 de julio de 2025.
17. L. Caviglione and W. Mazurczyk, “Never Mind the Malware, Here’s the Stegomalware,” IEEE Security & Privacy, vol. 20, no. 5, pp. 101–106, Sep. 2022, doi: https://doi.org/10.1109/msec.2022.3178205 . Consultado: 8 de julio de 2025.

Referencias