Universidad Nacional Autónoma de México
Facultad de Ciencias

Facultad de CIencias

Criptografía y Seguridad

Semestre: 2025-1

Equipo: Pingüicoders

Práctica 8:
Esteganografia

Arrieta Mancera Luis Sebastián - 318174116
Cruz Cruz Alan Josue - 319327133
García Ponce José Camilo - 319210536
Matute Cantón Sara Lorena - 319331622

Introducción:

Esta práctica tiene como objetivo dar a conocer la esteganografía como una técnica para ocultar y transmitir mensajes a la vista de todos. En la criptografía se tiene consciencia de que un mensaje fue encriptado (independientemente del algoritmo de encriptación), sin embargo, en la esteganografía se supone que los objetos visibles a simple vista no contienen mayor información que la que se presenta, es decir, ocultar un mensaje en otro mensaje. Son técnicas diferentes pero que tienen el mismo objetivo, la transmisión de información con voluntad de comunicación encubierta entre el emisor y el receptor.

Desarrollo:

Parte 1:

Se utilizó la biblioteca de pillow para el procesamiento de imágenes. Como se menciona en el pdf de la práctica, en los primeros 2 bytes (16 bits) se insertó la longitud del mensaje. Se utilizó argparse para poder pasar argumentos al momento de ejecutar el programa y utilizar las banderas **-h**, **-r** y **-i**. El único detalle es que la bandera **-h** argparse la reserva para mostrar la ayuda del programa, entonces se utilizó la bandera **-hi** para ocultar un mensaje en una imagen. Por ejemplo para cifrar un mensaje en una imagen se utiliza el siguiente comando:

```
python3 practica08.py -i ./imagenes/perrito.jpg -hi "Hola mundo"
./imagenes/perrito_con_mensaje.png
```

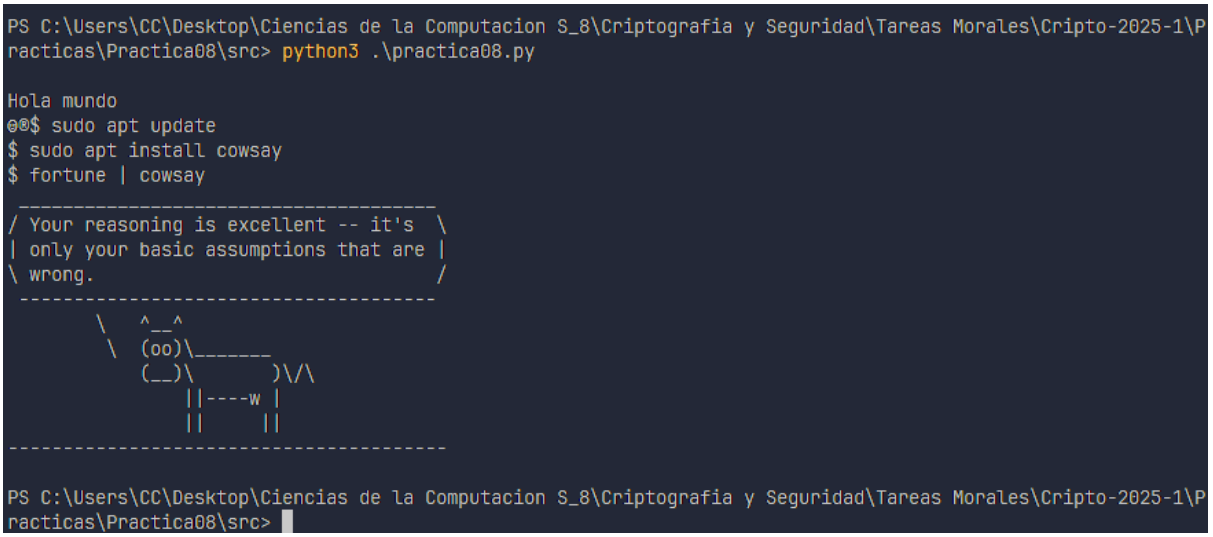
Para descifrar un mensaje en una imagen se utiliza el siguiente comando:

```
python3 practica08.py -i ./imagenes/perrito_con_mensaje.png -r
```

También se utiliza colorama para mostrar colorcitos en la terminal.

Parte 2:

En un inicio se creía que era la longitud en bits que tenía el mensaje, sin embargo, después de probar con la imagen **chess.py** no funcionaba. Se comenzó la práctica el mismo día que la dejaron y utilizamos esta imagen, pero días después nos dimos cuenta que la imagen había sido cambiada por otra que se llamaba **chessboard.py**, se supuso que habían subido la imagen equivocada, probamos con esta nueva imagen y tampoco funcionaba, después de mandar algunas dudas al ayudante nos dimos cuenta de que estábamos guardando mal la longitud ya que teníamos que guardar la longitud de caracteres del mensaje y no la longitud en bits. Hicimos las modificaciones al código y finalmente obtuvimos el mensaje:



Para descifrar el mensaje de la imagen **chessboard** se utiliza el siguiente comando:

```
python3 practica08.py -i ./imagenes/chessboard.png -r
```

Nota: Nos facilitó mucho haber tomado la optativa de **Proceso Digital de Imágenes**. Se anexa un README con las instrucciones de ejecución.

Preguntas:

1.- ¿Por qué la esteganografía forma parte de la criptografía? ¿Cuál es el elemento en común?

Respuesta: Aunque la esteganografía y la criptografía usan técnicas diferentes para cumplir sus propósitos tienen en común que mantienen la integridad y confidencialidad de la información, al igual que protegerla de terceros. La esteganografía se puede usar en conjunto con la criptografía para aumentar la seguridad de la información que queramos comunicar con alguien más.

2.- ¿Es detectable el LSB por los algoritmos de mensajería como Whatsapp o Instagram?

Respuesta: No hay mucha información pública acerca de algoritmos de detección de LSB o estenografía de estas redes sociales, o al menos de las de Meta. Sin embargo podemos darnos a la idea que si los hay realmente no son muy eficientes porque al menos hasta 2021, según un artículo, hay o había formas de ocultar información o mensajes de forma ilícita en Whatsapp, Instagram, Facebook, Twitter y Youtube. Las publicaciones o mensajes podían enviarse y recibirse sin problema así que estas redes sociales fallan en detectar el uso de técnicas como LSB y que se han dado casos en los que se usó la estenografía para chantaje e incluso alteración psicológica. Sin embargo aún las empresas encargadas de estas redes sociales siguen trabajando para perfeccionar su aplicaciones y evitar los ataques de estenografía.

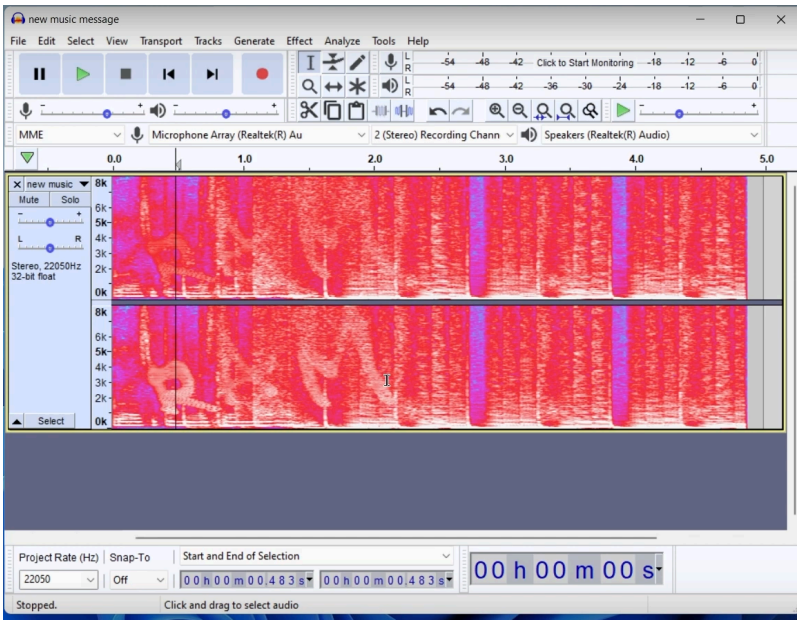
La estenografía no siempre se usa para el mal, también se ha usado como una alternativa para proteger información que puede comprometer a un individuo por lo que junto con LSB se han usado otros algoritmos (como AES) para ocultar información y que sin ningún problema pueda enviarse por los servicios de mensajería de las redes sociales, también hay un artículo que lo explica.

3.- ¿Por qué no podemos guardar mensajes en cualquier tipo de archivo? ¿Por qué solo en imágenes, audio y tal vez video?

Respuesta: En el caso de la esteganografía se debe a que tiene limitantes en cuanto a la capacidad de información que se maneja y siga permaneciendo oculta y que a su vez no afecte la calidad del archivo original (antes de insertar un mensaje), en vídeos y audios se usa LSB coding, parity coding y echo data hiding. También es posible ocultar información en archivos de texto pero esto es más complicado debido a la falta de redundancia en información (datos que se repiten y que no son realmente necesarios), es por esto que suele usarse como cubierta de otros archivos para ocultar la información en texto si es que contienen.

En otro tipo de archivos es notable cuando se altera la información y lo que se busca en la estenografía es que estas alteraciones sean imperceptibles, en archivos como ejecutables o código fuente podría alterar el funcionamiento al tratar de ejecutarse.

También otra razón es que ese tipo de archivos contiene mucha información que al ser alterada de forma mínima no es perceptible del todo por el ser humano común, por ejemplo las imágenes tienen muchos pixeles y alterar algunos para ocultar un mensaje puede que no sea percibido por el ojo humano, con los audios también es posible ocultar información jugando con la ampliación de sonidos y que se pueda ver en programas de edición de audio, como por ejemplo:



4.- ¿Podría ser que la estenografía pueda estar relacionada con mensajes subliminales?

Respuesta: Según Wikipedia, un **mensaje subliminal** es un mensaje o señal diseñada para pasar por debajo el mensaje de los límites normales de percepción. Algunos ejemplos son mencionar un mensaje en una canción, inaudible para la mente consciente pero audible para la mente inconsciente o profundo. Esto es justo lo que se hizo con el

segundo mensaje oculto de esta práctica, ya que hay un mensaje muy tenue que a simple vista no se puede ver a menos que pongas mucha atención, tratándose de una práctica de esteganografía podríamos pensar que si se relaciona con los mensajes subliminales. También según Wikipedia la esteganografía se trata del estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, para que no se perciba su existencia. La diferencia con la criptografía es que en la esteganografía oculta la información en un objeto (también llamado portador) de modo que no se advierta de la existencia de un mensaje, mientras que la criptografía cifra o codifica información de manera que no pueda ser entendido por un intruso. Por lo que sí la esteganografía se relaciona con los mensajes subliminales

5.- Teniendo una imagen de $n \times m$ píxeles, ¿cuál es la longitud máxima de mensaje (caracteres) que podemos incluir usando el último bit?

Respuesta: Una imagen de $n \times m$ píxeles, va a tener $n \times m \times 3$ bits (ya que son 3 canales) que podemos modificar (solo modificando el último bit), pero sabemos que primero usamos 16 bits para poner la longitud y luego 8 bits para poner ocho 0s, por lo tanto nos quedan $(n \times m \times 3) - 24$ bits para poner el mensaje y como por cada carácter usamos 8 bits, tenemos que la cantidad máxima de caracteres es $\frac{(n \times m \times 3) - 24}{8}$.

6.- ¿A cuántos bits de diferencia podemos diferenciar colores con el ojo humano?

Respuesta: Aunque no se sabe a ciencia cierta exactamente cuántos colores puede ver el ojo humano actualmente se estima una cota superior de 10 millones de colores los cuales, en la computadora representamos a un color con una secuencia de bits. Con un bit podemos representar 2 colores, blanco y negro, por lo cual para poder representar a los 10 millones de colores distinguibles por el ser humano necesitamos 24 bits, lo cual nos da un total de **16777216** posibles colores. Sin embargo solo podemos ver un aproximado de 10 millones, esto hace que algunos colores se vean más “brillantes” o colorido.

En teoría para distinguir dos colores solo es necesario cambiar un bit, sin embargo puede que este cambio no sea predecible para todos. También es importante notar en que canal se realiza el cambio del bit, en una estructura de 24 bits por color estos se dividen en 3 canales de 8 bits cada uno.

7.- ¿Puedes encontrar los 2 mensajes ocultos en este PDF? ¿Cuáles son?

Respuesta: Sí, uno está en la portada de la práctica:

“El arte de esconder información a simple vista”

Si usamos photoshop y aplicamos filtros de **brillo/contraste** y **exposición** podemos ver el mensaje **“Practice makes perfect”**

Conclusiones:

La esteganografía es una técnica interesante, creativa y una potencial amenaza para transmitir mensajes, ya que se aprovecha de la incredulidad de que un objeto no tiene mayor información a la presentada. La criptografía y la esteganografía pueden complementarse, dando un nivel de seguridad extra a la información, ya que si el mensaje es previamente cifrado, en caso de ser descubierta por un eventual intruso,

no solo le costará advertir la presencia de la mensajería oculta, sino que, la encontraría cifrada.

Referencias:

1.- Mensaje subliminal. (2024, 5 de Mayo). Wikipedia. https://es.wikipedia.org/wiki/Mensaje_subliminal#:~:text=Entre%20los%20ejemplos%2C%20puede%20mencionarse,consciente%20pero%2C%20aun%20as%C3%AD%2C%20percibida

2.- Esteganografía. (2024, 3 de septiembre). Wikipedia https://es.wikipedia.org/wiki/Esteganograf%C3%ADa

3.- KAPOOR SARMAH, D. (s. f.). Proposed System for data hiding using Cryptography and Steganography. En *University of twente*. https://ris.utwente.nl/ws/portalfiles/portal/363665854/1009.2826v1.pdf

4.- Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series Materials Science And Engineering*, *518*(5), 052003. https://doi.org/10.1088/1757-899x/518/5/052003

5.- Vtech. (2022, 26 agosto). Color bit depth and perception in human Vision - High-Definition Pro - Medium. *Medium*. https://medium.com/hd-pro/color-bit-depth-and-perception-in-human-vision-ca97313722d3

6.- *Profundidad de color | Apoyo a la edición Web*. (s. f.). https://biblioteca.ucm.es/edicionweb/profundidad-de-color#:~:text=Los%20formatos%20que%20usan%20esta%20profundidad%20de%20bits%20son%20JPG,.216%20color%20(true%20color)

7- Mohammed, Ibrahim, Mahdi. (2022). Refining Medical Image Steganography Scheme Based on Pixels Disparity Value and Huffman Coding. Journal of Image Processing and Intelligent Remote Sensing, 28-52. doi: 10.55529/jipirs.25.28.52

8-Iwugo, D. (2023, 13 julio). What is Steganography? How to Hide Data Inside Data. freeCodeCamp.org. https://www.freecodecamp.org/news/what-is-steganography-hide-data-inside-data/

9-Gurunath, R., Klaib, M. F. J., Samanta, D., & Khan, M. Z. (2021). Social media and steganography: use, risks and current status. Ieee Access, 9, 153656-153665.

10- Prabhakar, M., Krishnan, A., Nadanasabapathi, L., Majumdar, M., & Saveetha, D. (2018). Secret Messages in Social Media Using LSB And AES Algorithms. *International Journal of Engineering and Technical Research (IJETR)*, *8*(10), 8-11.