# Parte 2: Esteganografía

**Integrantes:**

- Kimberly Calderón Prado - 2017088598
- Jose Ortega González - 2017101758
- Andrey Sibaja Garro - 2017101898

## 1. Pregunta 1.

A partir del documento *stego.pdf* y su debida investigación se obtuvo la información necesaria para la creación de la infografía. Esta se muestra a continuación (si se desea observar con mayor claridad dirigirse al siguiente link):

# ESTEGANOGRAFÍA

## ¿En qué consiste la técnica de esteganografía en imágenes?

Se refiere a la técnica de incrustar mensajes secretos dentro de diferentes medios de cobertura como texto, audio, imagen y video sin ninguna sospecha.

## ¿Qué relación tiene la esteganografía con la criptografía?

**Propósito común:** proporcionar confidencialidad.

**Esteganografía** significa 'escritura escondida'.
**Criptografía** significa 'escritura secreta'.

## Algunas diferencias:

- La esteganografía busca lograr una comunicación segura e indetectable. La criptografía busca hacer que el mensaje sea legible sólo para el destinatario de destino.
- La esteganografía, la estructura principal del mensaje no se modifica. La criptografía impone un cambio en el mensaje secreto.
- La esteganografía se puede emplear en cualquier medio, como texto, audio, vídeo e imagen, mientras que la criptografía se implementa sólo en el archivo de texto.

## Características deseables

**Capacidad inserción**
Cantidad de información que se puede integrar en el medio sin un deterioro visible.

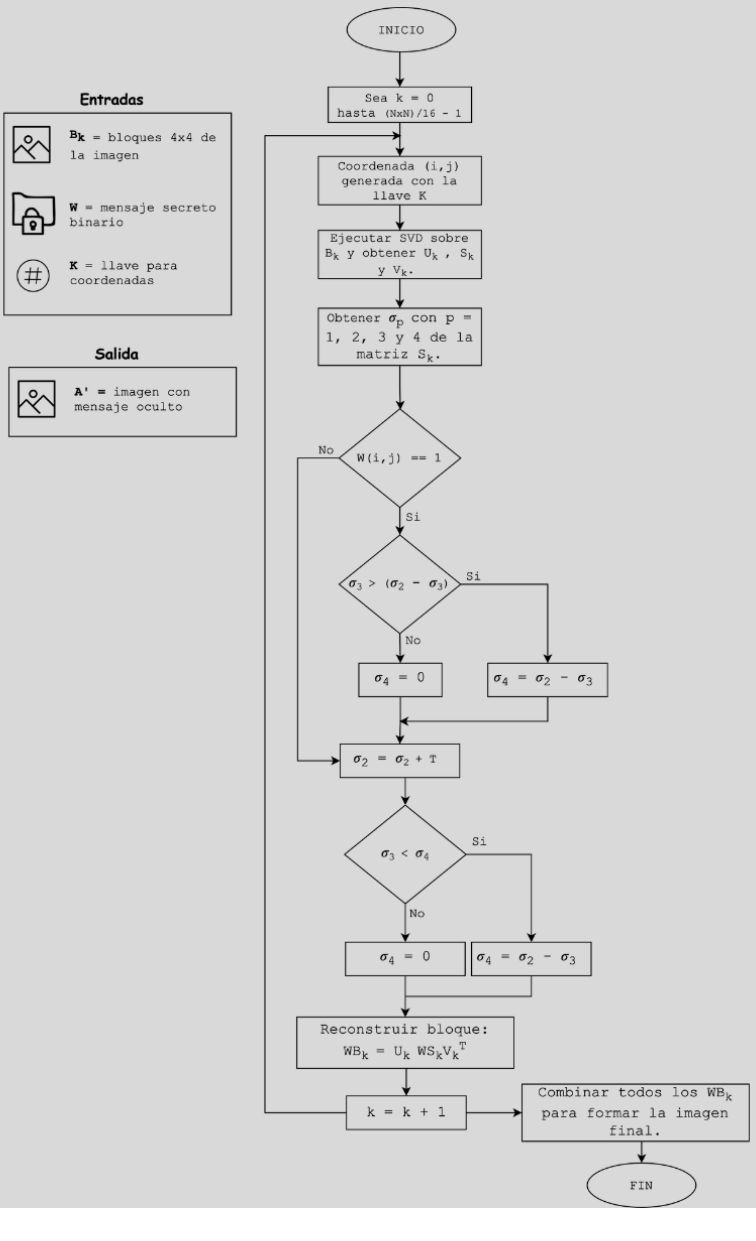
**Robusto**
Resistencia a ataques de transformaciones

**Invisibilidad**
Garantizar que el medio no se vea perturbado.

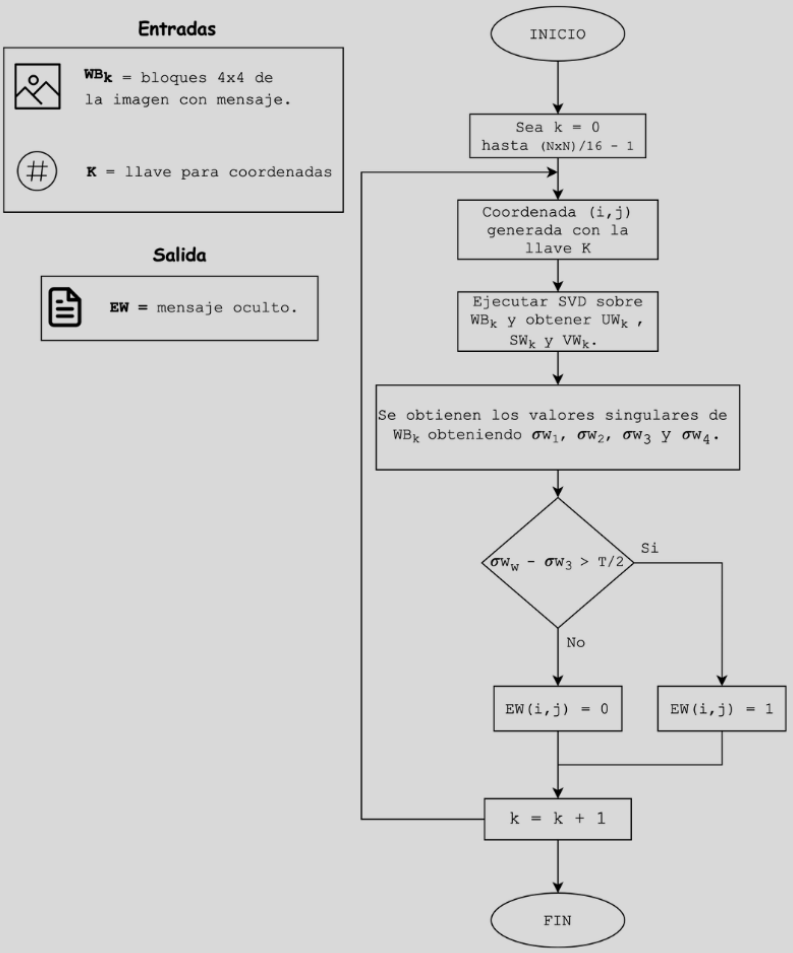
## Clasificación de sistemas de esteganografía

- **Texto:** Para ocultar el mensaje se puede cambiar una palabra o línea, usar espacios en blanco, incluso el número y la posición de las vocales se utilizan para ocultar el mensaje secreto. Por ejemplo, una serie que contenga las posiciones de las letras de cada palabra para al final armar un mensaje.
- **Audio:** Se puede lograr fácilmente, ya que un archivo típico de 16 bits tiene 216 niveles de sonido, y el oído humano no puede detectar una diferencia de unos pocos niveles.
- **Video:** Es una combinación de imagen y sonido. Por lo tanto, también se pueden emplear técnicas de esteganografía de imagen y audio en el video.
- **Imagen:** es la forma más utilizada de esteganografía, la razón detrás de esto es que causa menos sospecha.

## Algoritmo para embeber un mensaje



## Algoritmo para extraer un mensaje




## Aplicaciones del método de esteganografía en imágenes

- Comunicación confidencial y almacenado de datos confidenciales.
- Protección para la alteración de datos.
- Sistema de control de acceso para distribución de contenido digital.

Por ejemplo:

- Para el espionaje corporativo mediante el envío de secretos comerciales sin que nadie de la empresa se dé cuenta.
- Ocultar una fórmula química secreta o planes para un nuevo invento.

## REFERENCIAS

Y. Chanu, K. Manglem and T. Tuithung, A Robust Steganographic Method based on Singular Value Decomposition. International Research Publications House, 2014, pp. 717-726."

Diferencia entre esteganografía y criptografía", 2019. [Online]. Available: https://es.gadget-info.com/difference-between-steganography.

A. Khaldi, "Steganographic Techniques Classification According to Image Format", International Annals of Science, vol. 8, no. 1, p. 144, 2020. Available: https://core.ac.uk/download/pdf/270073287.pdf.

R. Doshi, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research, vol. 2, no. 6, p 4635, 2012. Avalaible: http://www.ijmer.com/papers/Vol2_Issue6/EN2646344638.pdf

## 2. Pregunta 2

Para la primera parte se creó el archivo *p2_p1.m* que contiene el algoritmo para la encriptación de un mensaje sobre una imagen, se utilizó como imagen de prueba *barbara.jpg* con un mensaje generado aleatoriamente (ver Fig 2) con una semilla de valor 3 y un threshold de 0.5. Los resultados obtenidos son los siguientes:


Fig 1: Resultados de encriptar mensaje en *barbara.jpg*.

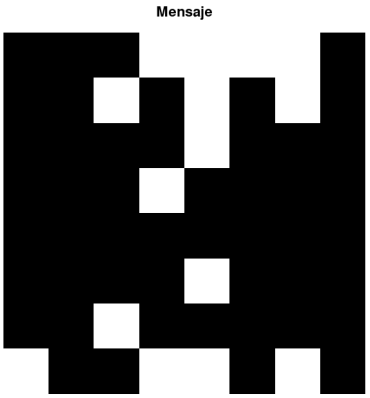



Fig 2: Mensaje encriptado en la imagen de *barbara.jpg*.

Se obtiene un error de 2.1217 obteniendo la norma de Frobenius entre ambas imágenes.

Para la ejecución del *script p2_p1.m* solo basta en ejecutar el archivo, ya que este contiene una prueba al final que se ejecutará para obtener los resultados mostrados en la Fig 1.

Para la segunda parte se generó el algoritmo de desencriptación del mensaje, el archivo con esta función tiene el nombre de *p2_p2.m* y se encarga de obtener el mensaje de una imagen a la que se le ha aplicado el algoritmo de esteganografía. Siguiendo con el ejemplo anterior, se obtiene el mensaje encriptado en la imagen de *barbara.jpg* obteniendo los siguientes resultados:

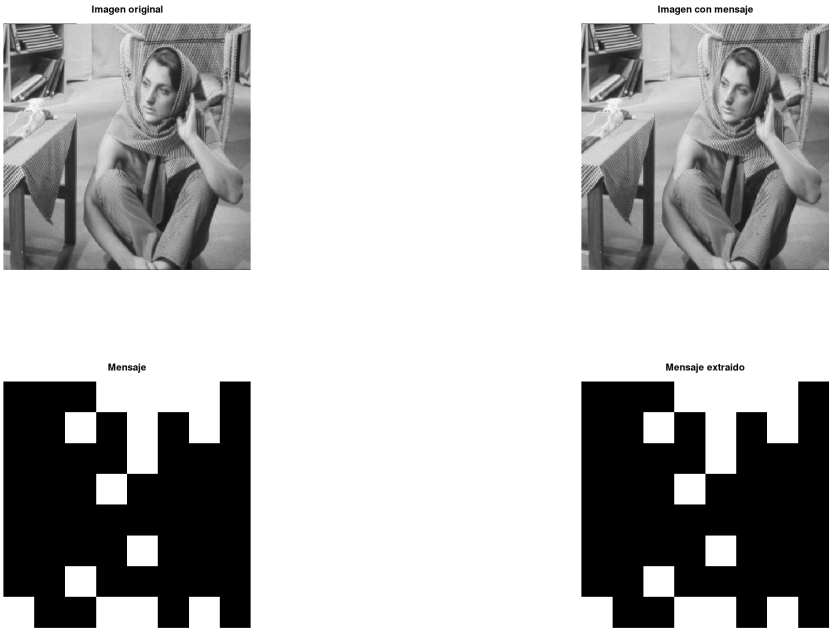



Fig 3: Resultados de desencriptar mensaje en *barbara.jpg*.

Como se observa, el mensaje obtenido comparado con el original es exactamente igual, lo que generó un porcentaje de 100% de extracción del mensaje, es decir, no hubo error. Esto puede variar y mostrar errores en la desencriptación del mensaje.

Finalmente, para la tercera parte se realizaron dos gráficas para observar el comportamiento de error del mensaje y la similitud de la imagen con respecto al threshold, el cual aumenta en 0.5 con cada iteración (desde 0 hasta 5). Los resultados obtenidos se observan en la siguiente figura:

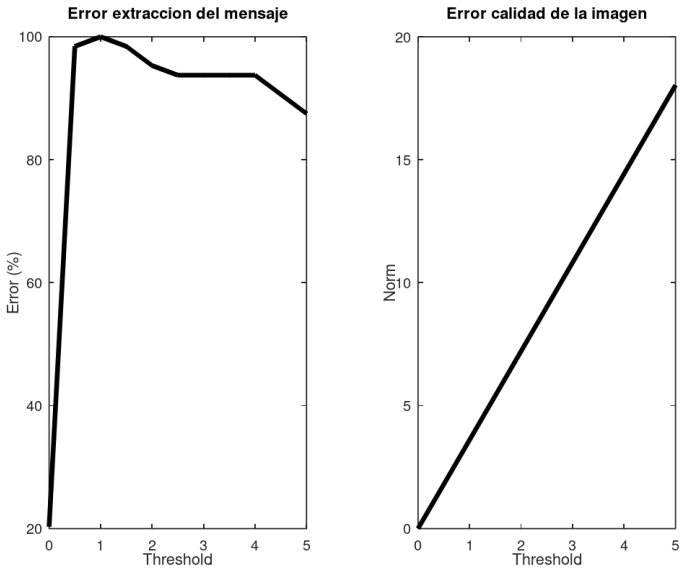



Fig 4: Primer gráfico: *Threshold* vs porcentaje error mensaje.
Segundo gráfico: *Threshold* vs error calidad de imagen.

Como se observa, a medida que el *threshold* aumenta, el error en la calidad de la imagen también aumenta, esto se debe a que se agrega una mayor cantidad de ruido a los valores singulares de la descomposición en *SVD* de la imagen original y afecta en los valores de los píxeles originales. Sucede lo mismo con la extracción del mensaje, ya que los valores de *SVD* están con un mayor ruido en cada iteración.

## 3. Pregunta 3

Utilizando el *script* para la pregunta 2 (*p2_p2.m*) es posible obtener el mensaje de la imagen dada como referencia *barbara_encriptada.m.* Aplicando el algoritmo con un threshhold de 0.05 y una semilla con valor de 3 se obtiene el siguiente mensaje de la imagen:

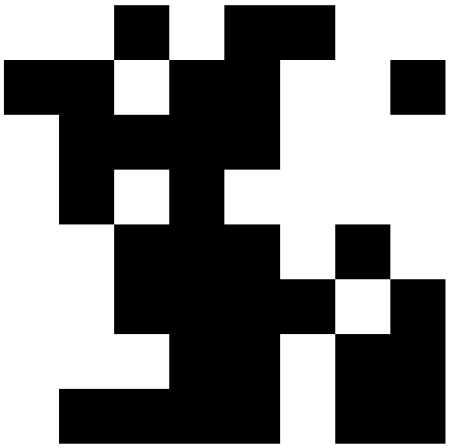


Fig 5: Resultados de desencriptar mensaje en *barbara.jpg.*