Esteganografía en imágenes

Autores: Nahuel Aguilar, Agustín Barrachina, Gonzalo Castelli, Augusto Viotti Bozzini

La esteganografía es el acto de ocultar información dentro de un archivo. Se implementó un algoritmo de esteganografía en el dominio de frecuencias basado en la compresión JPEG, una de las más utilizadas para compartir imágenes en internet. Se diferencia de la criptografía ya que la información se esconde dentro de los datos del archivo portador, sin llamar la atención.

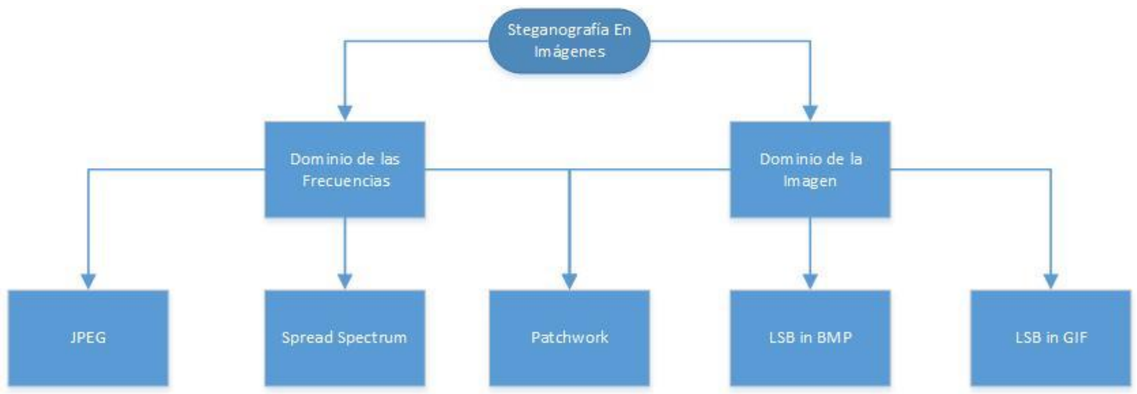
Introducción

Esteganografía es el acto de ocultar un documento, mensaje o imagen en algún otro archivo. En un mundo donde se comparten grandes cantidades de archivos por internet, la propiedad intelectual y los derechos de autor son difíciles de proteger. La esteganografía, aplicada en el "watermarking", sirve como una solución práctica y robusta al ocultar información del autor en archivos multimedia.

Objetivos

Se busca ocultar información (texto, fotos u otros archivos) dentro de una imagen en formato JPG mediante métodos de esteganografía. Se desea que el método sea [2]:

- Imperceptible al ojo humano
- Robusto frente al esteganálisis
- Resistente a manipulaciones sobre la imagen
- Permita almacenar la mayor cantidad de información posible.



Método

Para realizar la esteganografía, se comienza transformando el mapa RGB a YCbCr. Sobre las componentes de crominancia, se divide la imagen en bloques de pixeles de 8x8. Se realiza la transformada de coseno discreta (DCT) sobre los bloques y se obtienen 64 coeficientes enteros, que son luego divididos por una tabla de cuantización y posteriormente redondeados. Es aquí donde se sufre la pérdida de calidad asociada a la compresión JPEG.

$$\begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -3 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figura 1: Ejemplo de matriz resultante después de la DCT. Remarcados, los coeficientes sobre los cuales se oculta información en LSB

Como se muestra en la *figura 1*, la esteganografía se realiza en los LSB de los ocho primeros coeficientes, exceptuando el de continua. Al aplicar la IDCT y el resto de los pasos en orden inverso, se obtiene una imagen que porta la información escondida y cuya diferencia con la original es imperceptible al ojo humano.

Resultados

Se muestra un ejemplo de esteganografía JPEG en la *figura 2*.

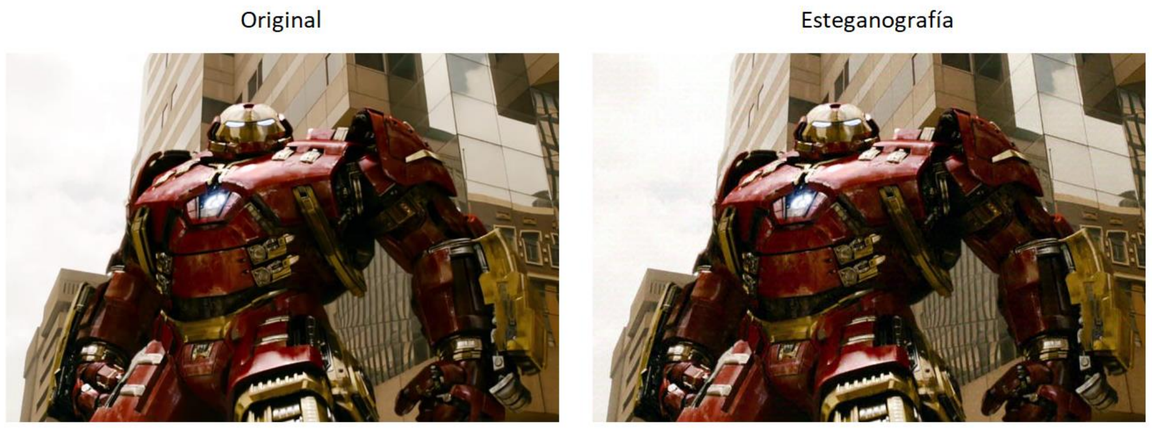


Figura 2: imagen original (izquierda) y la que presenta esteganografía (derecha)

Para estudiar las diferencias entre la imagen original y la que presenta la esteganografía se recurrió a análisis PSNR y SSIM. PSNR (Peak Signal to Noise Ratio) define la relación en dB entre la máxima energía posible de una señal y el ruido que afecta a su representación fidedigna. Por otro lado, SSIM (Structural Similarity Index) incorpora fenómenos estructurales como el lumus o el contraste, considerando la idea de que los pixeles tienen una fuerte dependencia con los que están cercanos a ellos. Es un índice entre 0 y 1, donde la unidad representa imágenes idénticas.

Figura 3: mapa SSIM y análisis PSNR para una imagen que presenta esteganografía

En la *figura 3* se puede observar que el mayor error se encuentra en las altas frecuencias ya que se puede ver la figura del personaje y el contorno de los objetos. Sin embargo, el error es menor en el cielo del fondo (bajas frecuencias).

Figura 4: imágenes anidadas mediante método LSB

En la *figura 4* se puede apreciar la mayor capacidad del método LSB, al anidar múltiples imágenes en la portadora. Sin embargo, esta forma de esteganografía es más fácil de detectar que la basada en JPEG.

Conclusiones

Se realizó esteganografía de texto e imágenes usando LSB y DCT. La esteganografía DCT probó ser resistente a la compresión. Se comprobó que para la conservación del mensaje es preferible utilizar calidades bajas para su escritura y calidades altas para su compresión. También se notó un problema al utilizar calidades muy altas de compresión debido a un problema con el mapeo de YCbCr y RGB. Fue interesante poder trabajar con tecnologías nuevas (toda la bibliografía es de ésta época) además de aprender sobre un tema que nos resultó intrigante a todos los integrantes del grupo.

Referencias / Bibliografía

[1] R. Poornima & R. J. Iswarya *An Overview of Digital Image Steganography*. 2013.

[2] T. Morkel, J. H. P. Eloff & M. S. Olivier. *An Overview of Image Steganography.*

[3] N. F. Johonson & S. Jajodia. *Exploring Steganography Seeing the Unseen. 2014.*

[4] Sherif M. Badr, Gouda I. Salama, Gamal M. I. Selim & Ashgan H. Khalil. *A review of Steganalysis Techinques: From Image Format Point of View.* 2014