Análisis comparativo de técnicas de esteganálisis en imágenes digitales LSB

Luis Sifuentes-Villarroel

En la presente investigación se evaluaron dos métodos de esteganálisis frente a imágenes LSB, comparando su efectividad en la detección de imágenes esteganográficas y del porcentaje que abarca el mensaje oculto en la imagen portadora (porcentaje de embebido) respecto a la totalidad de la imagen.

Comparative Analysis of Steganalysis Techniques in LSB Digital Images

In the present research, two methods of steganalysis were evaluated against LSB images, comparing their effectiveness in detecting steganographic images and the percentage covered by the hidden message in the carrier image (percentage of embedding) with respect to the entire image.

Análisis comparativo de técnicas de esteganálisis en imágenes digitales LSB

Luis Sifuentes-Villarroel
20101062@aloe.ulima.edu.pe

Resumen En la presente investigación se evaluaron dos métodos de esteganálisis frente a imágenes LSB comparando su efectividad en la detección de imágenes esteganográficas y de la proporción que abarca el mensaje oculto en la imagen portadora (porcentaje de embebido) respecto la totalidad de la imagen.

Introducción

• La pornografía infantil está disponible en Internet en proporciones epidémicas, y los investigadores en línea están haciendo todo lo posible para indagar, detener y procesar a estos depredadores sexuales. Para lograr su cometido, dichos individuos utilizan una herramienta disponible en la web y de libre acceso llamada *esteganografía,* la cuál usan para el ocultamiento y tráfico de este tipo de contenido ilícito.

• Hay más de 4000 sitios dedicados a la esteganografía, lo que les facilita ocultar una imagen de pornografía infantil dentro de otra aparentemente inocente.

• Con el pertinente conocimiento de esta herramienta (esteganografía), tanto los *software* comúnmente utilizados como las técnicas más frecuentes, un agente de la ley puede ser capaz de identificar de manera exitosa la posesión y transmisión de este tipo de contenido que normalmente pasaría desapercibido.

Marco teórico

• La *esteganografía* consiste en técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados *portadores*, de modo que no se perciba su existencia.

• El esteganálisis es el arte de detectar los mensajes ocultos dentro de un estego-objeto (imagen oculta dentro de otra).

• El *esteganálisis RS* (*regular and singular*) consiste en estimar las cuatro curvas del diagrama RS y calcular su intersección mediante extrapolación. La forma general de las cuatro curvas en el diagrama varía con la imagen de portada, casi perfectamente lineal a la curva.

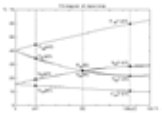


Diagrama RS de una imagen

El eje *x* es el porcentaje de píxeles con LSB invertidos, el eje *y* es el número relativo de grupos regulares y singulares con máscaras M y −M, M = [0 1 1 0]

• *Esteganálisis SPA* (*sample pair analysis*). El método SPA rastrea los conjuntos múltiples de pares de muestras antes y después de la incrustación LSB, y utiliza las relaciones entre conjuntos múltiples para resolver la longitud de los mensajes incrustados.

Resultados


Para el análisis de ambas técnicas se seleccionó la imagen Lenna en formato BMP. En primer lugar, se evaluó la técnica SPA con la imagen tanto a color como en escala de grises. Para el primer caso se mostraron los siguientes resultados:

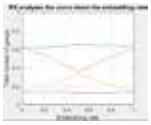
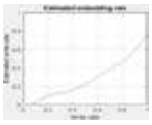
Señal	Tipo imagen	Ratio de embebido
R	Stego	0,095361
G	Stego	0,092576
B	Stego	0,125577

Los resultados mostraron el porcentaje de embebido estimado por cada frecuencia que compone el RGB siendo superior al 5 % de toda la imagen que es imagen esteganográfica. El mismo análisis se realizó para la misma imagen, pero en escala de grises.

Señal	Tipo imagen	Ratio de embebido
G	Stego	0,289529

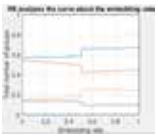
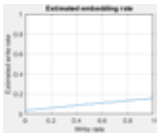
Para el segundo caso, a diferencia de la imagen a color, para la imagen en escala de grises solo se mostró una frecuencia y el porcentaje de embebido incrementó al estar concentrado en un solo plano.

En segundo lugar, se tomó como primera muestra la imagen Lenna en escala de grises obteniéndose la gráfica RS que muestra la asociación de los conjuntos regulares y singulares generados en el proceso. Posteriormente, se realizaron diversos embebidos en la imagen que iban del 0 al 100 % y estos fueron contrastados con los embebidos estimados por la técnica.

Adicionalmente, se realizó el esteganálisis (detección de la existencia de una imagen esteganográfica) en una imagen con una mayor complejidad para identificar la efectividad de la detección de los datos embebidos en un plano más amplio.


Finalmente, los datos de este embebido mostraron que el porcentaje estimado era mínimo a causa de la alta dispersión permitida por esta imagen debido a su dimensión mayor y gama de colores.

Conclusiones

• Si bien la técnica SPA puede detectar de manera confiable imágenes ocultas con tasas de bits de más de 0,05 y de igual forma funciona bastante bien con tasas de bits más bajas.

• El esteganálisis RS es notablemente eficaz; para evitar la detección, una incrustación de LSB tendría que ser rotada a menos de 0,05 bits por píxel en la imagen de portada, lo que significa que menos del 5 % de los píxeles han modificado su LSB.

• La robustez de la implementación de técnicas esteganográficas puede mejorar significativamente si las estego-imágenes (imagen que oculta otra dentro suya) se encuentran en escala de grises debido a que el ruido se vuelve más imperceptible por la baja variabilidad de tonalidades en este tipo de imágenes.

Referencias

Fridrich, J., Goljan , M., y Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. *IEEE Multimedia*, *8*(4), 22-28. doi:10.1109/93.959097

Kessler, G. C. (2004). Steganography: implications for the prosecutor and computer forensics examiner. *American Prosecutors Research Institute Child Sexual Exploitation Program*.

Raja, K. B., Venugopal, K. R., y Patnaik, L. M. (2004). A Secure steganographic algorithm using LSB, DCT and image compression on raw images [technical report]. Bangalore: Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University.

Xiangyang, L., Fenlin, L., y Peizhong, L. (2007). A LSB Steganography Approach against pixels sample pairs steganalysis. *International Journal of Innovative Computing, Information and Control*, *3*(3), 575-588.

Agradecimientos

Agradezco a mis padres y a mi hermana, por su constante apoyo y motivación durante mis estudios; al profesor del curso Seminario de Tesis 2, Daniel Cárdenas; y en especial a mi asesor, el profesor Carlos Torres, ya que sin su ayuda este trabajo no se hubiese podido realizar.