Análisis de técnicas esteganográficas y estegoanálisis en canales encubiertos, imágenes y archivos de sonido

Gustavo A. Isaza E. [*]
Carlos Alberto Espinosa A.[**]
Sandra M. Ocampo C.[***]

Resumen

La esteganografia es una ciencia que se perfila como tecnología de punta en los procesos de ocultamiento de información. Facilita el tránsito de archivos con buenos niveles de seguridad en la privacidad de los mensajes. El estegoanálisis permite aplicar estrategias y procedimientos para la detección, identificación y análisis de información oculta en imágenes, sonidos y canales encubiertos. En este artículo se presenta una revisión y reflexión del contexto de la esteganografía y el estegoanálisis y un análisis de la aplicación de algunas de sus técnicas.

Palabras Clave: Esteganografía, estegoanálisis, ocultamiento, detección, identificación, análisis de información, canales encubiertos.

Analysis of steganographic techniques and steganalysis in hidden channels, images and sound files

Abstract

Steganography is a science that is profiled as state of the art technology in the processes of information concealment. It facilitates the traffic of files with good levels of security in the privacy of messages. Steganalysis allows the application of strategies and procedures for the detection, identification and analysis of hidden information in images, sounds and hidden channels. This text presents a revision and reflection of the context and usage techniques of steganography and steganalysis.

Key words: Steganography, steganalysis, hidden information, detection, identification, information analysis, hidden channels.

[*] Ingeniero de Sistemas y Computación - Especialista en Software para Redes. Docente Departamento de Sistemas e Informática, Universidad de Caldas. E-mail: gustavo.isaza@ucaldas.edu.co
[**] Ingeniero de Sistemas. Universidad Tecnológica de Pereira. E-mail: caae@utp.edu.co
[***] Ingeniera de Sistemas. Universidad Tecnológica de Pereira. E-mail: sammy@utp.edu.co

Introducción

La esteganografía, al igual que el estegoanálisis, son herramientas tendientes a aplicarse en situaciones y casos específicos, es decir, si se desea ocultar algún mensaje basta con que se aplique alguna de las técnicas para adelantar el ocultamiento, generando un objeto con el mensaje encubierto [22].

El siglo XXI ha continuado posicionando la era de la revolución digital que con la ayuda de excelentes medios de transmisión de alta velocidad, tecnologías satelitales, redes, de computadores, etc., constituyen una verdadera infraestructura del ciberespacio [16].

Esta revolución, que encuentra en Internet su máxima expresión, ha ocasionado grandes problemas por su uso indiscriminado en la privacidad de la información publicada en la Web y en el intercambio de información generando situaciones difíciles de controlar.

La presencia de fraudes en las redes públicas, la falsa representación y la reproducción ilegal van en aumento haciendo que sus propietarios requieran de sistemas eficientes de detección de datos ocultos en canales encubiertos, imágenes y archivos de sonido, cuyos formatos permiten camuflar todo tipo de información [9].

La esteganografía es utilizada, entre otros, por grupos terroristas que envían mensajes clandestinos, delitos informáticos que son ocasionados continuamente a través de la red, o aficionados que juegan a pasarse mensajes secretos que en realidad llegan a ser menos inofensivos que los propios archivos en los que éstos son camuflados [14].

Estas situaciones han despertado un interés generalizado en todas las organizaciones gubernamentales, sociales y académicas por mantener la confidencialidad en sus comunicaciones y protegerse de cualquier intrusión, así como de poder detectar y develar todo tipo de envío de información oculta que pone en peligro las estructuras físicas, económicas, políticas o sociales de un país, lo que puede lograrse con la aplicación del estegoanálisis [4].

En este artículo se detallan algunos elementos de la esteganografía, sus principales estrategias, algoritmos y limitaciones, las principales técnicas empleadas para adelantar estegoanálisis en archivos que son objeto de estudio para la computación forense, además de identificar, analizar y detallar técnicas esteganográficas y estrategias para aplicar el estegoanálisis sobre imágenes, archivos de sonido y canales encubiertos en investigaciones forenses de informática.

Estado del arte de la esteganografía

La esteganografía está definida como el arte de ocultar información en archivos de imágenes, sonidos o en canales encubiertos a través de métodos y técnicas computacionales. Se encuentra enmarcada en el ámbito de transportar información a través de las redes informáticas [1][21].

Existen diferentes técnicas que permiten implementar la esteganografía, sin embargo, las más utilizadas son las que aplican el método LSB (*Least Significant Bit*), que se basa en la utilización del dígito menos significativo para ocultar el mensaje [8]. Otros métodos se fundamentan sobre la estadística, que busca los valores más redundantes del archivo y ubican allí los bits que hacen referencia al mensaje que se desea ocultar. Éste es uno de los métodos más potentes y seguros.

Las técnicas de esteganografía se deben apoyar en dos principios básicos: el primero, en seleccionar muy bien el medio en el que se desea aplicar dicha técnica, refiriéndose a que el archivo encubierto, a pesar de que pierde calidad, no sea perceptible a dicha pérdida; el segundo principio, trata de aprovechar las limitaciones del hombre referidas a la percepción de algunas señales visuales (gama de colores) y auditivas (algunas frecuencias que el oído humano no alcanza a percibir) [4] [7].

En la Figura 1 se esboza el proceso que se lleva a cabo en el momento en que se oculta un mensaje en cualquier medio disponible que se haya escogido [1].

Figura 1. Proceso para transmitir un mensaje oculto por la red.

El esteganograma es el resultado de embeber el mensaje secreto en la cubierta. Para revelar el esteganograma no se requiere del archivo oculto original [12].

Esteganografía

Esteganografía en Imágenes

Se refiere a la técnica de ocultar mensajes en archivos de imágenes por medio de un mapa de bits, cambiando el valor de algunos bits, normalmente los que menos afectan la apariencia de la imagen [10].

Los colores que utiliza una imagen también se ven representados por la cantidad de bits que disponga, esto significa que si posee 3 bytes existen en la imagen un color rojo, uno azul y uno amarillo, los que al combinarse pueden dar cualquier color, formando una paleta de colores [5]. Por esta razón, cuando se cambia un bit, como lo es el menos significativo en la imagen cubierta, el color de la imagen puede variar dentro de su paleta de un estado al siguiente o al anterior, ocasionando que dicho cambio no sea perceptible.

Existen varios métodos encargados de encubrir la información, uno de ellos es el LSB, *Least Significant Bit*, el bit menos significativo, consiste en codificar cada bit de la información a lo largo de la imagen quitando un bit de la misma y colocando el bit del mensaje, normalmente esto se hace en las áreas más ruidosas de la imagen que no atrae la atención, como por ejemplo, un prado o el cielo [7].

Una imagen de alta calidad tiene las proporciones de 1024 X 768 Píxeles. La calidad de imagen es de 24 bits (3 bytes por píxel), por tal motivo posee 1024 X 768 X 3 = 2'359.296 bytes de tamaño. Así mismo si se utiliza el último bit de cada byte se deduce que se tiene un espacio de 2'359.296 / 8 = 294.912 bytes disponibles para ocultar el mensaje [11][12][13].

La esteganografía es una ciencia que abarca mucho más allá del simple ocultamiento de mensajes en imágenes, a pesar de que es una de las técnicas más desarrolladas en el momento, también estudia con profundidad el sonido y cómo a través de este medio puede transportar y camuflar grandes volúmenes de información [15]. Las imágenes a pesar de que poseen técnicas muy avanzadas, siempre se encuentran con el obstáculo de la cantidad de espacio disponible para ocultar un mensaje.

Esteganografía en archivos de sonido

Los archivos de sonido cuentan con características especiales que tienen una gran virtud para la aplicación de la esteganografía; éstos cuentan no sólo con un buen tamaño disponible para los mensajes que se quieran incluir, sino además con la limitación que tiene el hombre de escuchar algunas frecuencias de sonido [10][11].

En el sector de datos de los archivos de sonido se encuentran en forma de bits secuenciales las muestras. Esto deja implícito entonces, que es en este sector donde sucede todo el proceso de ocultamiento del mensaje.

Existen varios métodos para ocultar información en archivos de sonido, éstos son: LSB (cambiando el bit menos significativo), el otro es utilizando frecuencias en los sonidos que son inaudibles para los humanos, se puede además reemplazar tonos musicales por codificación binaria. Esto es, el tono F representa 0 y el tono C representa 1, por tal motivo cada vez que suenen éstos en una melodía se formarán cadenas de 0 y 1 que llevan el mensaje oculto [4][7].

A continuación se presenta un ejemplo de la técnica LSB en un archivo de sonido, a partir del cual se extraen varias muestras de 8 bytes con información: 45 23 120 31 128 44 76 89 y convirtiéndolos a binarios de la siguiente forma [2]:

00101101 00010111 01111100 00011111 10000000
00101100 01001100 01011001

El bit menos significativo es el que se encuentra primero de derecha a izquierda en cada byte. Ahora, si se desea ocultar la información 200, lo que en bits equivale a 11001000, sólo se debe ingresar cada bit de ésta en cada uno de los bytes de la muestra, así:

00101101 00010111 01111100 00011110 10000001
00101100 01001100 01011000

Convirtiéndolos de nuevo a decimales queda: 45 23 120 30 129 44 76 88, como se puede observar las variaciones fueron mínimas, comparadas con los valores decimales que se tenían anteriormente, ahora, si se realiza este proceso con cada una de las muestras de un sonido se obtiene que se ha podido ocultar un mensaje completo sin ningún problema y sin cambios radicales. Por esto, estadísticamente, hay un 50% de probabilidad de que el bit cambie, asegurando que el sonido no cambiará notablemente.

El fundamento principal para ocultar un mensaje en un ancho de banda determinado, se basa en un canal muy estrecho entre el espectro del medio y de un nivel que pueda considerarse como ruido, este último buscando que sea inaudible por el hombre. Este proceso queda así camuflado en medio del ruido característico de las señales análogas [3][6][11].

Los canales encubiertos son otro vehículo para aplicar la esteganografía. Tienen la característica primordial de enfocarse en las formas de comunicación existentes a través de la Internet y están estrechamente relacionados con el juego de protocolos de algunas de las capas del modelo OSI [11][13].

Esteganografía en canales encubiertos

Un canal encubierto se puede definir como: "Cualquier canal de comunicación que puede ser aprovechado por un proceso para transferir información de tal manera que viola una política de seguridad del sistema" [5][3].

Las diferentes formas de esteganografía en canales encubiertos, se encuentran remitidas a la violación del manejo del protocolo TCP/IP. Esto deja implícito que cualquier envío de información "no autorizada" por políticas de seguridad de la red se denomina canal encubierto [5][15].

Para implementar correctamente un canal encubierto, es necesario tener dos aplicaciones corriendo simultáneamente, una aplicación debe estar en la máquina del atacante, actuando como un servidor http [5], usualmente esta máquina se encuentra en la red pública y a la escucha de un puerto TCP para procesar los llamados de la otra aplicación; otra aplicación debe estar instalada dentro de la red que se quiere vulnerar [10].

El protocolo TCP/IP es apropiado para crear canales encubiertos de comunicación, ya que a través de las cabeceras se pueden enviar datos relevantes para los autores; usando este método es posible pasar datos entre los anfitriones en los paquetes que aparentan ser peticiones de conexión iniciales, secuencias de datos establecidas, u otros pasos intermedios [20].

Existen tres métodos o formas de transmitir comunicación encubierta por el protocolo TCP/IP:

- **Campo de identificación del paquete IP.** Substituye el valor del campo de identificación del IP por la representación numérica del ASCII del carácter que se codificará. Esto permite la transmisión fácil a un destino cualquiera, que debe sólo leer este campo y convertir el código ASCII a una *clasificación de octetos usados normalmente en este proceso, por lo tanto los datos del paquete son convertidos al ASCII equivalente dividiéndose por 256. Por ejemplo, si se quisiese enviar la palabra "He" quedaría así* [5][7]:

Paquete Uno: 18:50:13.551117 nemesis.psionic.com. 7180 > blast.psionic.com.www: Triunfo 512 (TTL 64, identificación 18432) de S 537657344:537657344(0). El número de identificación enviada fue 18432, el cual al dividirlo entre 256 da un valor de 72, el que representa un dato ASCII, que al convertirlo representa la letra **H.**

Paquete Dos: 18:50:14.551117 nemesis.psionic.com. 51727 > blast.psionic.com.www: S1393295360 :1393295360(0) triunfo 512 (TTL 64, identificación 17664). Igual que el anterior, se toma 17664 se divide entre 256 y da 69, que en código ASCII es la letra **E.**

Paquete Tres: 18:50:18.551117 nemesis.psionic.com. 21004 > blast.psionic.com.www: S3843751936: 3843751936(0) triunfo 512 (TTL 64, identificación 2560). Igual que el primero, se toma 2560 se divide entre 256 y da 10, que representa la finalización del envío de datos.

Se debe observar que este método confía en la manipulación de la información de la cabecera del IP, y puede ser muy susceptible al cambio de dirección del paquete ya que puede ser rescrita en el tránsito del origen al destino, especialmente si está localizada detrás de un *Firewall*. Si sucede esto, la pérdida de los datos enviados es inevitable.

- **Campo inicial del número de serie (ISN) TCP.** Permite a un cliente establecer una negociación confiable con un servidor. El ISN sirve como medio perfecto para transmitir datos clandestinos debido a su gran tamaño (32 bits). Se puede desarrollar una gran cantidad de posibilidades o técnicas para aplicar. En este caso se va a utilizar una muy sencilla: se modifica el valor que representa la sincronización definido por la letra S. Esto implica que se busca el ASCII de la letra o el valor que se vaya a enviar y se multiplica por 16777216, lo único que debe hacer quien recibe, es dividir el valor que llega en la sincronización entre 16777216 para develar el ASCII recibido. Por ejemplo, para enviar el mismo mensaje de ahora "He":

Paquete Uno: 18:50:29.071117 nemesis.psionic.com. 45321 > blast.psionic.com.www: S 1207959552: 1207959552(0) win 512 (ttl 64, id 49408). Bien, se coge el número de S, 1207959552 se divide entre 16777216 y se obtiene como resultado el ASCII 72, que representa la letra **H**.

***Paquete Dos*:** 18:50:30.071117 nemesis.psionic.com. 65292 > blast.psionic.com.www: S 1157627904: 1157627904(0) win 512 (ttl 64, id 47616). Igual que el paso anterior, se toma el valor de S, 1157627904 se divide entre 16777216 y se obtiene como resultado el ASCII 69, que representa la letra **E**.

Paquete Tres: 18:50:34.071117 nemesis.psionic.com. 64535 > blast.psionic.com.www: S 167772160: 167772160(0) win 512 (ttl 64, id 54528). Igual que el primero, se toma 167772160 se divide entre 16777216 y da 10, que representa la finalización del envío de datos.

- **Número de secuencia del salto de campo TCP *Acknowledge*.** Este método cuenta con la realización de un *spoofing* a la dirección IP, para habilitar una dirección a la máquina que envía un paquete de información a un sitio remoto y este sitio lo envíe a la dirección real. Esto es con el objetivo de cambiar la dirección del remitente original del paquete, en caso de que se haga una investigación de dónde se originó el paquete. Con este método se puede crear una red anónima o falsa, que sería muy difícil de descubrir, todo con el fin de ocultar la procedencia del paquete y para engañar con un tránsito aleatorio del paquete en caso dado que se esté escuchando algún canal. Además, si el servidor de red se encuentra bastante ocupado haciendo verificaciones de saltos de red, es prácticamente indetectable [5][20].

Este método confía plenamente en TCP/IP que utiliza los acuses de recibo (ACK) para establecer una comunicación entre dos *hosts*. Para llevar a cabo este acto, lo que hace el remitente es construir un paquete con la siguiente información: la fuente de la dirección IP falsa, un puerto falso de la fuente, la dirección IP destino falsa, el puerto de destino falso y el número de sincronización TCP con los datos codificados del destino real; en conclusión, este método consiste en engañar al servidor remoto enviando un paquete y unos datos encapsulados con una falsa dirección IP de origen.

Estegoanálisis

El estegoanálisis se define como el arte y la ciencia de romper la seguridad de un sistema esteganográfico [18]. Existen dos tipos de estegoanálisis según la intención con que se hagan: ataque pasivo, donde sólo se busca detectar el archivo con mensaje oculto; y el ataque activo, donde se manipula la información secreta [12][16].

Estrategias para identificar y analizar datos ocultos

Los ataques a la esteganografía se refieren a las estrategias implementadas para identificar, analizar y detallar archivos que contengan elementos ocultos. Se pueden clasificar en [12]:

- **Ataques al esteganograma.** El atacante intercepta el esteganograma y por lo tanto puede analizarlo.

- **Ataque por repetición de cubierta.** Quien creó los esteganogramas ha utilizado el mismo método para ocultar diferente mensajes. Por lo tanto, el atacante posee diferentes esteganogramas que fueron generados del mismo archivo encubierto.

- **Ataque por cubierta conocida.** El atacante intercepta el esteganograma y conoce la cubierta que usó para crearlo. Esto facilita demasiado el trabajo porque detecta inmediatamente cualquier variación por más mínima que sea.

- **Ataque por manipulación.** El atacante tiene la habilidad de manipular los datos del esteganograma. Esto le da la gran ventaja de poder eliminar el mensaje oculto en el esteganograma.

Estegoanálisis en imágenes

El estegoanálisis en imágenes es la detección de esteganogramas utilizados para ocultar información en éstas, como uno de los medios más comunes para transportar mensajes ocultos [13].

Se distinguen dos formas para este tipo de ataques: ataques visuales, que se basan en las capacidades de la vista humana; y los ataques estadísticos, que se basan en la realización de tests al archivo esteganográfico [12][13].

- **Ataque visual.** Es un ataque al esteganograma, que se basa en la observación de los bits menos significativos ocultando mensajes de forma aleatoria en los mismos. Este tipo de ataque se basa en el juicio humano, que es el que determina si en un archivo de imagen después de pasar un filtro determina que existe un mensaje oculto o no. El algoritmo de filtrado elimina las partes de la imagen que cubren el mensaje. Después de filtrado queda una imagen conformada únicamente de los bits que potencialmente podrían haber sido utilizados para incrustar los bits del mensaje oculto. El filtrado que se vaya a aplicar a la imagen esteganográfica depende totalmente de la función de incrustación que se analice [11].

Una de las formas más sencillas de deshabilitar la probabilidad de la existencia de mensaje oculto en las imágenes es comprimiendo el archivo, pasándolo a formato JPG; así no se reconozca en él la existencia de algún mensaje, se realiza este proceso y esto garantiza que si existe el mensaje oculto éste desaparecerá. Aunque es una medida un poco fuerte ya que se ataca de forma deliberada cualquier imagen, garantiza que a la red no va a entrar ningún mensaje oculto en una imagen [13].

Estegoanálisis en archivos de sonido

El método del análisis estadístico también puede usarse contra los archivos audio, ya que utilizan el mismo principio del bit menos significativo que se utiliza en la esteganografía con imágenes [8].

Otras de las formas de remover información sin necesidad de verificar la existencia de mensajes ocultos es cambiando los formatos de los archivos de sonido, lo que ocasiona indudablemente un cambio en la estructura del sonido y por tanto pérdida de las características del mismo, lo que da como resultado necesariamente la pérdida de información.

Para remover mensajes en archivos de sonido, se quitan todas las frecuencias que se presenten en los sonidos y que sean inaudibles por el hombre. Esto garantiza que cualquier dato camuflado se perderá indudablemente [11].

Otra técnica para eliminar mensajes ocultos es disminuyendo la velocidad con la que se transmiten los bits a través del medio en el archivo de sonido. Esto ocasiona una pérdida de calidad y por tanto de datos. Adicional a ésto reduce también el espacio disponible para guardar información extra en los archivos de sonido.

Estegoanálisis en canales encubiertos

La principal fuente de ocultamiento de mensajes se encuentra en las cabeceras del protocolo TCP/IP y en las solicitudes de HTML, por tal motivo para contrarrestar este medio de propagación de información se deben revisar los acuses de recibo para establecer la comunicación entre dos medios y las solicitudes de apertura de sitios Web.

Una de las formas de detectar y prevenir el uso de canales encubiertos es manejando todas las técnicas existentes de detección de intrusos. La esteganografía deja de cumplir su objetivo cuando se detecta que un archivo contiene información oculta. Esta detección se puede volver bastante tediosa si se utiliza una estego-clave o llave. Por eso se utilizan diversos programas para la detección de posible información encubierta [5].

Para realizar un ataque efectivo a los canales encubiertos se requiere poner a funcionar una serie de filtros que intercepten los paquetes de protocolos existentes en TCP/IP y verifiquen la consistencia de los mismos y que apliquen alguna de las técnicas generales para adelantar esteganografía en canales encubiertos [8].

Conclusiones y recomendaciones

- Con el desarrollo de la esteganografía se genera también el crecimiento del estegoanálisis como la ciencia que se encarga de detectar, identificar y analizar archivos que contienen información oculta con el fin de develar y tener acceso a los mensajes camuflados.

- El éxito de la esteganografía se basa en la selección deliberada del medio en el que se desea camuflar la información, existiendo tantos mecanismos para llevar a cabo el camuflaje de información como la imaginación lo permita.

- La esteganografía se ha posicionado en los últimos años en el campo de la seguridad, pero de ninguna forma reemplaza la criptografía, ambas pueden complementarse para lograr buenos resultados en el ocultamiento de información.

- La esteganografía ha tomado más fuerza en el campo militar, sin embargo, en poco tiempo podremos aplicar estas técnicas en nuestros computadores personales ocultando información en creaciones artísticas de audio y/o video.

- Es interesante aventurarse con ingenio y creatividad a la producción de prototipos experimentales, tanto para camuflar información como para develarla.

Referencias

[1] ARDITA, Julio, CARATTI, Mariana, DO CABO, Roberto, GIUSTO, Mariel, ISAR, Guido, PAGOUAPÉ, Matías, SCHELLHASE, Livio, STAVRINAKIS, Florencia. *Esteganografía*. Universidad Jhon F. Kennedy, 2001, Buenos Aires, Argentina.

[2] ARTZ, Donovan. Digital Steganography: Hiding Data within Data. p. 77 ss. Junio 2001. Los Alamos National Laboratory. Spotlight.

[3] CARRILLO, Juan F., OSPINA, Carlos, RANGEL, Mauricio, ROJAS, Jaime A., VERGARA, Camilo. Covert Channel. pp. 1-3. Febrero de 2003. Universidad de los Andes.

[4] COLE, Eric. "Book Excerpt: Hiding in Plain Sight" Published on 4.Computerworld August 4th 2003. http://www.computerworld.com/printthis/2003/0,4814,83714,00.html

[5] CRAIG H., Rowland. Covert Channels in the TCP/IP Protocol Suite. 2002.

[6] FABIEN A., P. Petitcolas. Watermarking schemes evaluation. I.E.E.E. Signal Processing, Vol. 17, No. 5, pp. 58-64, September 2000.

[7] Fridrich, Goljan, Du. "Reliable Detection of LSB Steganography in Color and 2. Grayscale Images 2003". http://www.ws.binghamton.edu/fridrich/Research/acmwrkshp_version.pdf

[8] HORNET, Charles. "Steganography". 9th April 2002. Published on 11. Infosecwriters.com. URL:http://www.infosecwriters.com/texts.php?op=display&id=2

[9] IRS Criminal Investigation Electronic Crimes Program ILook InvestigatorElliot Spencer 2004: http://www.ilookforensics.org/

[10] JOHNSON Neilf F. Johnson & Johnson Tecnology Consultants. Steganography & Digital Watermarking –Information Hiding– Copyright, 2003.

[11] JOHNSON Neil F. y JAJODIA Sushil. Exploring Steganography: Seeing the Unseen. pp. 26-30. 2002. Universidad de George Mason 2026.

[12] JOHNSON Neil F. and JAJODIA Sushil. Steganalysis: The Investigation of Hidden Information. Septiembre de 2003, New York. p. 3.

[13] JOHNSON, Neil F. and Sushil Jajodia. 2004. "Steganalysis of Images Created Using Current Steganography Software". http://www.jjtc.com/ihws98/jjgmu.html

[14] KELLEY, Jack. "Terror groups hide behind Web encryption". USA Today, Feburary 2001. http://www.landfield.com/isn/mailarchive/2001/Feb/0038.html

[15] KIPPER, Greg. "Investigator's Guide to Steganography". Auerbach Publications, 1.2004.

[16] KRENN Robert. Steganography and Steganalysis. p. 3 ss.

[17] KURAK, C. y MCHUGH, J. Acautionary Note on Image Downgrading. IEEE Press Poscataway, New York, 1999.

[18] MIROSLAV Dobsícek. Modern Steganography. Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague.

[19] PROVOS, Niels, HONEYMAN, Peter "Detecting Steganographic Content on the Internet". 2001. http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf

[20] RANGEL, Mauricio, CARRILLO, Juan F, OSPINA, Carlos, ROJAS, Jaime A., VERGARA, Camilo. Covert Channels sobre HTTP. Universidad de Los Andes.

[21] SELLARS, Duncan. "An Introduction to Steganography". 9. http://www.totse.com/en/privacy/encryption/163947.html