UNA MIRADA A LA ESTEGANOGRAFÍA

A looking to steganography

RESUMEN
Existe un creciente interés por el conocimiento, difusión y utilización de la esteganografía, dinamizada por el avance tecnológico de los sistemas computacionales. La Esteganografía 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. Permite aplicar técnicas para ocultar información en imágenes, sonidos y canales encubiertos.

PALABRAS CLAVES: esteganografía, ocultamiento, información, mensajes.

ABSTRACT
A growing interest exists for the knowledge, diffusion and use of the steganography, energized by the technological advance of the computer systems. The steganography is a science that is profiled as tip technology in the processes of concealment of information. It facilitates the traffic of files with good levels of security in the privacy of the messages. It allows applying techniques to hide information in images, sounds and covert channels.

KEYWORDS: *steganography, hidden, information, messages.*

CARLOS ALBERTO ANGULO
Ingeniero de Sistemas y Computación. Universidad Tecnológica de Pereira.
caae@utp.edu.co

SANDRA MILENA OCAMPO
Ingeniero de Sistemas y Computación. Universidad Tecnológica de Pereira.
Especialista en Gestión de Calidad
sammy@utp.edu.co

LUIS HERNANDO BLANDON
Licenciado en Matemática y Física.
Especialista en Instrumentación Física. Universidad Tecnológica de Pereira.
lhbd@utp.edu.co

1. INTRODUCCIÓN

El área de investigación sobre la esteganografía en Colombia es reciente, sin el suficiente estudio, difusión y aplicación. Este artículo permite presentar algunos resultados del estado del arte realizado con el fin de difundir conocimientos tecnológicos sobre el tema, a toda la comunidad académica y científica de la Universidad Tecnológica de Pereira. Presenta las teorías y técnicas de la esteganografía que actúan sobre canales encubiertos, archivos de imagen y de sonido en cualquier tipo de formato que pueda ser llevado o trasformado a bits.

2. DESCRIPCIÓN DEL PROBLEMA

¿Qué teorías y técnicas de la esteganografía permiten realizar procesos de ocultamiento de información en imágenes, sonidos y canales encubiertos?

3. ESTEGANOGRAFIA

[1]. La definición científica de 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.

Un ejemplo: el caso de dos prisioneros que desean enviarse información para escaparse. Saben que solo pueden comunicarse a través del carcelero quién recibe el mensaje y lo pasa de un prisionero a otro. Ellos habían determinado que el mensaje oculto se encontraba sacando las primeras letras de cada palabra. Siendo esta la forma más simple de esteganografía.
Otra forma muy utilizada de esteganografía es utilizando plantillas sobre textos. Por ejemplo de la frase "Hay un ágape en casa de Carmela y Mariluz", existe un mensaje oculto el que se puede develar tan solo con una matriz:

H	A	Y		U	N		Á
G	A	P	E		E	N	
C	A	S	A		D	E	
C	A	R	M	E	L	A	
Y		M	A	R	I	L	U
Z							

Tabla 1. Matriz Inicial Esteganografía.

Seguidamente hay que realizar una especie de plantilla que sobreponiéndola a esta matriz deja ver el mensaje oculto:

Tabla 2. Plantilla a Sobreponer

Al sobreponerla sobre la matriz inicial, queda revelado el mensaje original que se necesitaba transmitir.

H							Á
G	A						
		S				E	
					L	A	
						L	U
Z							

Tabla 3. Plantilla Sobrepuesta en la Matriz

Fecha de Recepción: 07 Septiembre de 2007
Fecha de Aceptación: 30 Noviembre de 2007

Existe en la esteganografía gran cantidad de métodos para ser desarrollada, sin embargo los más utilizados son los de LSB (Least Significant Bit), que se basa en la utilización del digito menos significativo para ocultar el mensaje. El otro método es el estadístico, que busca los valores más redundantes del archivo y ubica allí los bits que hacen referencia al mensaje que se desea ocultar. Este es uno de los métodos más potentes y seguros.

[2] La técnica de esteganografía se debe apoyar en dos principios básicos: el primero en seleccionar muy bien el medio en el que se desea aplicar, refiriéndose a que el archivo cubierta a pesar de que pierde calidad no sea perceptible; el segundo aprovechando las limitaciones del hombre en cuanto a percepción se refiere, como lo es, la gama de colores que aunque varíen un poco el ojo humano no alcanza a percibir, al igual que existen frecuencias que el oído no alcanza a decodificar.

[3] este diagrama 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.

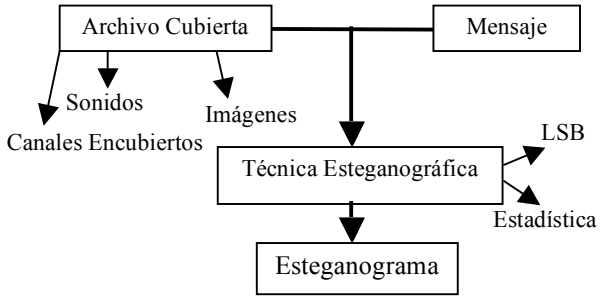


Figura 1. Proceso que transmite mensaje oculto en red.

[4] El esteganograma es el resultado de embeber el mensaje secreto en la cubierta. Para develar el esteganograma no se requiere de la cubierta original.

La esteganografía es aplicable a casi todo tipo de archivos, se ha descubierto en textos, en imágenes, en sonidos y hasta en canales encubiertos, haciendo de esta práctica una de las más versátiles en la actualidad. La esteganografía tiene tres formas especiales de utilizar cubiertas, que se detallarán a continuación.

3.1 ESTEGANOGRAFÍA EN IMÁGENES

[5] 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, los que menos afectan la apariencia de la imagen.

[6] los colores que utilizan 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, lo que al combinarse pueden dar cualquier color, formando una paleta de colores. 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. Tal y como se ve en la figura 2, se recomiendan las imágenes en escala de gris ya que estas asimilan mejor los cambios de colores y la variación realmente puede llegar a ser mínima. Se debe tener en cuenta que cada píxel se encontrará representado por 3 bytes en estos casos.

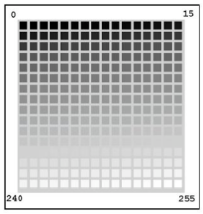


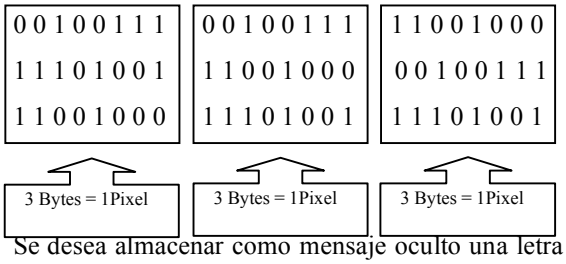
Figura 2. Paletas de Colores

[5] existen varios métodos encargados de encubrir la información, uno de ellos es el LSB. 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. 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. Esto significa que en una imagen de este tipo se puede camuflar información de unas 300 páginas hechas en Word sin tan siquiera levantar la menor sospecha por el ojo humano.

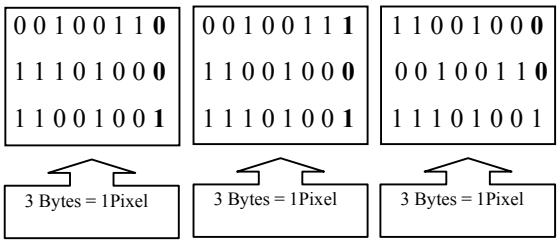
Por tal motivo si una imagen cuenta con los siguientes píxele**s:**

PÍXEL	PÍXEL	PÍXEL
PÍXEL	PÍXEL	PÍXEL
PIXEL	PÍXEL	PÍXEL

Seleccionando 3 píxeles se obtiene:



Se desea almacenar como mensaje oculto una letra como por ejemplo la "C", que en código ASCII es 67, en binario sería: 0 1 0 0 0 0 1 1. Se obtiene:



Este proceso no ocasiona un cambio radical en la figura y por tal motivo no es apreciable ni tan siquiera con el ojo humano. Se puede observar que los únicos valores que cambiaron con respecto a la imagen original son los que se encuentran en negrilla.

La esteganografía es una ciencia que abarca mucho más allá del simple ocultamiento de mensajes en imágenes, a pesar que es una de las técnicas más desarrolladas en el momento. Ella se encarga y estudia también con profundidad el sonido y como a través de ese vehículo puede transportar y camuflar grandes volúmenes de información.

3.2. ESTEGANOGRAFÍA EN ARCHIVOS DE SONIDO

Los sonidos son archivos con características especiales que 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 tan sólo algunas frecuencias de sonido.

El formato más usado y recomendado para el almacenamiento de sonido en una computadora es WAVE comúnmente conocido como .WAV. Posee 2 partes: el encabezado y el sector de datos.

El encabezado contiene la información de cómo se encuentra digitalizado el archivo de sonido. Cantidad de canales, frecuencia de muestreo y tamaño de muestra. Cuando se desea reproducir un sonido, el encabezado permite definir el formato de los bits permitiendo leerlos correctamente.

En el sector de datos se encuentran en forma de bits secuenciales las muestras, es decir el sonido. Esto deja implícito, que es en el sector de datos dónde sucede todo el proceso de ocultamiento del mensaje.

Existen varios métodos para ocultar información en archivos de sonido estos son: LSB. Utilizando frecuencias en los sonidos que son inaudibles para los humanos y reemplazando 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 esos tonos en una melodía se formaran cadenas de 0 y 1 que llevan el mensaje oculto.

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:
00101101 00010111 01111000 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, en bits equivale a 11001000, se debe ingresar cada bit en cada uno de los bytes de la muestra así:
00101101 00010111 01111000 00011110 10000001 00101100 01001100 01011000

Convirtiéndolos de nuevo a decimales queda: 45 23 120 30 129 44 76 88, las variaciones fueron mínimas, comparadas con los valores decimales que se tenían. 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. Basándose estadísticamente hay un 50% de probabilidad de que el bit cambie, asegurando que el sonido no cambiará notablemente.

Una pequeña muestra de lo que sucede cuando se oculta la información en un archivo de sonido se puede ver en las siguientes figuras:

Figura 3. Mapa del Aeropuerto de Burlington

La figura anterior es la que se desea ocultar en un archivo de sonido, que al ser ocultada por alguno de los programas que existen para este fin, el sonido original con respecto al portador del mensaje se ve de la siguiente forma:

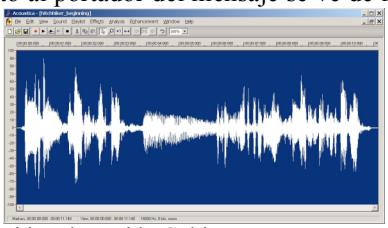


Figura 4. Archivo de sonido Cubierta

Este espectro de sonido se transformará en el siguiente espectro:

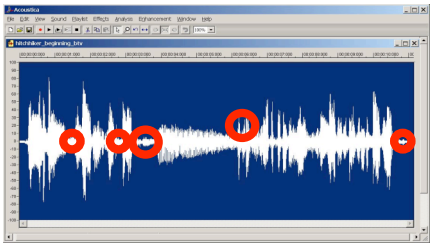


Figura 5. Archivo de sonido con el mensaje oculto

Esta figura describe una pequeña y sutil diferencia a la fuente de sonido original, comparada con la anterior varia un poco, como puede observarse en los círculos. El formato del archivo de sonido utilizado fue un .WAV. En los archivos de sonido se pueden ocultar imágenes, sonidos y textos.

Otro vehículo para adelantar esteganografía son los canales encubiertos. Tienen la característica primordial de enfocarse en las formas de comunicación existentes a

través del internet y están estrechamente relacionados con el juego de protocolos de algunas de las capas del modelo OSI.

3.3. 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". Las diferentes formas de esteganografía en canales encubiertos, se encuentran remitidas a la violación del manejo del protocolo TCP/IP.

Para la utilización de los canales encubiertos, hay que tener en cuenta que en las redes existen modelos de seguridad y esquemas de control de acceso que regulan el uso de los canales. [7], los NACS esquemas más comunes para control de acceso de la redes dependen del uso, combinado o no con herramientas que implementan algún tipo de filtro en algunos niveles del modelo OSI (firewall, routers, etc.).

HTTP, es uno de los protocolos de red más importantes en el internet, ya que es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de la web, remitiendo la información que se verá en pantalla y para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

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, 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 que debe estar instalada dentro de la red que se quiere vulnerar. Detallada en la siguiente figura.

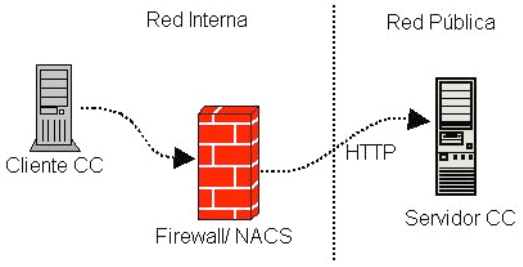


Figura 6. Diagrama de Red para tráfico HTTP

La aplicación cliente CC abre una conexión hacia el servidor CC y comienza a enviar información a través de los HTTP Request, la que se camufla a través de los encabezados de los paquetes HTTP. El servidor CC recibe la información, la reconstruye y envía las instrucciones de vuelta, camufladas a través de los HTTP Request, de esta forma el cliente CC recibe las instrucciones que se desean realizar sobre la redes reconstruyéndolas de los encabezados HTTP. Una de las ventajas de este método es que la mayoría de los firewalls están configurados para pasar por el puerto 80, por tal motivo se hace casi indetectable.

Se desarrolla el siguiente ejemplo: sacar una información desde un servidor FTP ubicado en una red privada, por medio de un computador con acceso a Internet que se encuentra dentro de la Intranet. Pero existe un firewall en dicha red que rechaza todo el tráfico entrante, excepto el que pasa por el puerto 80. Para esbozar mejor el caso se presenta en la siguiente figura:

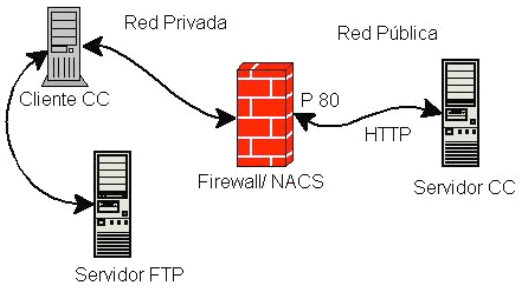


Figura 7. Red tráfico por el canal encubierto sin detección.

Para poder realizar esto se debe contar con un programa instalado dentro de la red interna, que en este caso se encuentra en Cliente CC. Crea paquetes http modificados y se comunica constantemente con un servidor http ubicado en la red pública en el Servidor CC. Este servidor tiene la capacidad de interpretar los mensajes del cliente dentro de la Intranet.

Para que suceda el proceso que se desea llevar a cabo se debe tener presente que la intrusión es coordinada por el servidor web, pero es iniciada por el cliente. Cuando el cliente levante su conexión a internet, este envía una llave que inicia el canal. El servidor pide al cliente que inicie una sesión en el servidor ftp. Después de realizada la conexión el servidor pide al cliente la lista de archivos del ftp, de donde escoge el archivo que le interesa para ser transmitido. Ahora, es el cliente quien envía el archivo cuando lo requiera el servidor.

[8] el número de formas distintas de crear canales subliminales o encubiertos sólo viene limitado por la imaginación. Sin embargo, los canales subliminales adolecen de una importante limitación: el ancho de banda. Dependiendo del tipo de canal elegido, se requieren grandes cantidades de texto para transmitir un solo bit de información encubierta. Por consiguiente, estos canales sólo pueden utilizarse para enviar cantidades pequeñas de información cada vez, no grandes volúmenes de datos. Por esto no debe despreciarse el potencial de un canal subliminal, siempre que se puedan enviar muchos mensajes o que la información a transmitir sea pequeña, por ejemplo, el PIN de un usuario o su clave secreta, datos de unos pocos caracteres.

[9] el protocolo TCP/IP permite establecer comunicación entre 2 dos usuarios; se hace muy apropiado para crear canales encubiertos de comunicación, ya que a través de las cabeceras se pueden enviar datos. 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. Se muestra en la siguiente figura la distribución de la cabecera TCP.

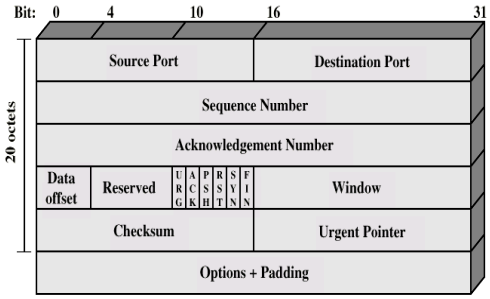


Figura 8. Cabecera TCP [9]

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. El que debe tan solo leer este campo y convertir el código ASCII. El campo en cuestión es el que se encuentra en paréntesis en el ejemplo. Este programa no realiza ningún tipo de función de 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 letra "H" quedaría así:

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). Observen que 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: 18:50:18.551117
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. El que representa que finaliza el envío de datos.

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 reescrita 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, ya que maneja 32 bits. Se puede desarrollar una cantidad de posibilidades o técnicas para aplicar. Ej: se modifica el valor que representa la sincronización definido por la letra S. Esto implica que se busca el ASCI 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: enviar la letra "H":

Paquete Uno: 18:50:29.071117 [10]
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, el que representa la letra **H**.
Paquete dos: 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. El que representa que finaliza el 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 donde partió el paquete. Con éste 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 transito 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.

Este método confía plenamente en TCP/IP que utiliza los acuses de recibo (ACK) para establecer una comunicación entre dos host. Para llevar a cabo este cometido 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.

Los puertos fuente y destino cambian al aplicarse esta técnica. Hay que tener en cuenta solamente que la dirección IP destino sea el servidor de la dirección IP a la que le deseo enviar la información. Un ejemplo de esto sería: un cliente A es quien envía la información, Un

servidor B es donde se va a realizar el salto y un servidor c es el que va a recibir la información:

- *Paso 1*: el cliente A envía el paquete falso con información codificada al servidor B. El paquete tiene la dirección del servidor c.
- *Paso 2:* el servidor B recibe el paquete y le asigna un acuse de recibo para la sincronización (SYN/ACK) o simplemente un SYN/RST del paquete, esto basado en el estado que se encuentre el paquete. El servidor B piensa que el paquete proviene del servidor C, por tanto el paquete es enviado a C. El número de secuencia de Acknowledge, que es el número de secuencia más uno, es enviado al servidor C.
- *Paso 3:* el servidor C recibe el paquete de B y decodifica los datos.

Por tanto éste método o técnica consiste en engañar al servidor remoto enviando un paquete y unos datos encapsulados con una falsa dirección IP de origen.

4. CONCLUSIONES Y RECOMENDACIONES

- Para utilizar las técnicas de la esteganografía se necesita simplemente de un medio de transmisión que contenga muchos bits para que el cambio de alguno de ellos no altere significativamente el archivo original y pueda transmitir el mensaje oculto sin que sea percibido.

- El ocultamiento de información utilizando las técnicas de la esteganografía sigue siendo confiable y válido en procesos que exigen privacidad en el tránsito de la información.

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

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

5. BIBLIOGRAFÍA

[1] MIROSLAV Dobsícek. Modern Steganography [online]. Página 3. (Sin editorial y demás datos). Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague. Disponible en: <http://www.scycore.com/papers/ow04_paper.pdf>

[2] MR BYTE, 1997-1998, Practical Privacy Guide: Steganography [online]. (Sin editorial y demás datos). All Net Tools - Library - Privacy Guide. Html. Disponible en: <http://www.all-nettools.com/library,privacy3>

[3] ARTZ Donovan. Digital Steganography: Hiding Data within Data [online]. (Sin editorial y demás datos). Páginas 77 en adelante. Junio 2001. Los Alamos National Laboratory. Spotlight. Disponible en: <http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf>

[4] TOLOSA Rubén, Esteganografía… No es lo que parece [online]. Febrero de 2003. Página 9 en adelante. (Sin editorial y demás datos). Disponible en: <http://webs.ono.com/usr011/r-tolosa/archivos/steg.pdf >

[5] ARDITA Julio, CARATTI Mariana, DO CABO Roberto, GIUSTO Mariel, ISAR Guido, PAGOUAPÉ Matías, SCHELLHASE Livio, STAVRINAKIS Florencia. Esteganografía [online]. (Sin editorial y demás datos). Universidad Jhon F. Kennedy, año 1998, Buenos Aires, Argentina. Disponible en: <http://www.cybsec.com/Stegano.pdf>

[6] JOHNSON Neil F. y JAJODIA Sushil. Exploring Steganography: Seeing the Unseen [online]. Páginas 26 a 30. Año 1998. (Sin editorial y demás datos). Universidad de George Mason 2026.pdf. Disponible en: <http://www.jjtc.com/pub/ r2026.pdf>

[7] CARRILLO Juan F., OSPINA Carlos, RANGEL Mauricio, ROJAS Jaime A., VERGARA Camilo. Covert Channels Sobre http. Páginas 1 a 3 [online]. Febrero de 2003. (Sin editorial y demás datos). Universidad de los Andes. Disponible en: <http://www.criptored.upm.es/guiateoria/gt_m142m.htm>

[8] ÁLVAREZ MARAÑÓN Gonzalo. Canales subliminales [online]. (Sin editorial y demás datos). Abril de 2001. Disponible en: <http://www.cibernauta.com/cibertecno/cibertecno_analisis_articulos.php?articulo=1329.php>

[9] CRAIG H. Rowland. Covert Channels in the TCP/IP Protocol Suite [online]. 1996. (Sin editorial y demás datos). Disponible en: <http://translate.google.com/translate?hl=es&sl=en&u=http://www.firstmonday.org/issues/issue2_5/rowland/&prev=/search%3Fq%3Dcovert%2Bchannel%2B%26hl%3Des%26lr%3D>

[10] OPTICDATA, Copyright © 1997-2005, S.L. *All rights reserved* [online]. Esta página fue Revisada/modificada: *22 de enero de 2004*. (Sin editorial y demás datos). Disponible en: <http://www.opticdata.es/ docs.htm>