Esteganografía 1.0
Por La_Morsa Software Co.

Introducción

Dice la Wikipedia que la **esteganografía** (del griego *στεγανος* (*steganos*):cubierto u oculto, y *γραφος* (*graphos*): escritura), es la parte de la criptología en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados **portadores**, de modo que no se perciba su existencia. Es decir, se trata de ocultar mensajes dentro de otros y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase **inadvertido** para observadores que tienen acceso a ese canal.

La utilidad del uso de la esteganografía es mostrada en el llamado problema del prisionero (Gustavus J. Simmons, 1983). Resumidamente, en dicho problema tenemos dos prisioneros, A y B, que quieren comunicarse de forma confidencial para escapar. El problema es que sólo pueden intercambiar mensajes a través de un guardián. Este personaje puede leer, modificar o generar el mismo los mensajes. Si el guardián detecta cualquier comunicación que pueda ser utilizada para escapar (por ejemplo, detecta un cifrado) dejará de transmitir los mensajes. En este escenario los prisioneros necesitan establecer un canal encubierto.

El uso de la esteganografía permite disponer de un canal encubierto de forma que nos podamos comunicar sin ser detectados. La estrategia que sigue la esteganografía para resolver el problema del prisionero es esconder los datos que no queremos que sean detectados, entre los mensajes permitidos por el guardián.

Probablemente uno de los ejemplos más antiguos del uso de que la esteganografía sea el referido por Heródoto en Las historias. En este libro describe cómo un personaje tomó un cuadernillo de dos hojas o tablillas; rayó bien la cera que las cubría y en la madera misma grabó el mensaje y lo volvió a cubrir con cera regular. Otra historia, en el mismo libro, relata cómo otro personaje había rasurado a navaja la cabeza de su esclavo de mayor confianza, le tatuó el mensaje en el cuero cabelludo, esperó después a que le volviera a crecer el cabello y lo mandó al receptor del mensaje, con instrucciones de que le rasuraran la cabeza.

En el siglo XV, el científico italiano Giovanni Battista della Porta descubrió cómo esconder un mensaje dentro de un huevo cocido. El método consistía en preparar una tinta mezclando una onza de alumbre y una pinta de vinagre, y luego se escribía en la cáscara. La solución penetra en la cáscara porosa y deja un mensaje en la superficie de la albúmina del huevo duro, que sólo se puede leer si se pela el huevo.

Técnicas digitales modernas pata hacer esteganografía

Existen numerosos métodos y algoritmos utilizados para ocultar la información dentro de archivos multimedia: imágenes, audio y vídeo. A continuación se indican algunos de los más usados.

Enmascaramiento y filtrado

En este caso la información se oculta dentro de una imagen digital empleando marcas de agua que incluyen información, como el derecho de autor, la propiedad o licencias. El objetivo es diferente de la esteganografía tradicional (básicamente comunicación encubierta), ya que es añadir un atributo a la imagen que actúa como cubierta. De este modo se amplía la cantidad de información presentada.

Algoritmos y transformaciones

Esta técnica oculta datos basados en funciones matemáticas que se utilizan a menudo en algoritmos de la compresión de datos. La idea de este método es ocultar el mensaje en los bits de datos menos importantes.

Inserción en el bit menos significativo

Este es el método moderno más común y popular usado para esteganografía –y es el que usamos en este programa– también es uno de los llamados métodos de sustitución. Consiste en hacer uso del bit menos significativo de los pixels de una imagen y alterarlo. La misma técnica puede aplicarse a vídeo y audio, aunque no es lo más común. Hecho así, la distorsión de la imagen en general se mantiene al mínimo (la perceptibilidad es prácticamente nula), mientras que el mensaje es esparcido a lo largo de sus píxeles. Esta técnica funciona mejor cuando el archivo de imagen es grande, posee fuertes variaciones de color ("imagen ruidosa") y también aventaja cuanto mayor sea la profundidad de color. Asimismo esta técnica puede utilizarse eficazmente en imágenes a escala de gris, pero no es apropiada para aquellas en color de 8 bit paletizadas (misma estructura que las de escalas de gris, pero con paleta en color). En general, los mejores resultados se obtienen en imágenes con formato de color RGB (tres bytes, componentes de color, por píxel).

Por ejemplo:

El valor (1 1 1 1 1 1 1 1) es un número binario de 8 bits. Al bit ubicado más a la derecha se le llama "bit menos significativo" (LSB) porque es el de menor peso, alterándolo cambia en la menor medida posible el valor total del número representado.

Un ejemplo de esteganografía: Ocultamiento de la letra "A". Si se tiene parte de una imagen con píxeles con formato RGB (3 bytes), su representación original podría ser la siguiente (3 píxeles, 9 bytes):

(1 1 0 1 1 0 1 0) (0 1 0 0 1 0 0 1) (0 1 0 0 0 0 1 1)

(0 0 0 1 1 1 1 0) (0 1 0 1 1 0 1 1) (1 1 0 1 1 1 1 1)

(0 0 0 0 1 1 1 0) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

El mensaje a cifrar es ‘A’ cuya representación ASCII es (1 0 0 1 0 1 1 1), entonces los nuevos píxeles alterados serían:

(1 1 0 1 1 0 1 1) (0 1 0 0 1 0 0 0) (0 1 0 0 0 0 1 0)

(0 0 0 1 1 1 1 1) (0 1 0 1 1 0 1 0) (1 1 0 1 1 1 1 1)

(0 0 0 0 1 1 1 1) (0 1 0 0 0 1 1 1) (0 0 0 0 0 1 1 1)

Observar que se ha sustituido el bit del mensaje (letra A, marcados en negritas) en cada uno de los bits menos significativos de color de los 3 píxeles. Fueron necesarios 8 bytes para el cambio, uno por cada bit de la letra A, el noveno byte de color no se utilizó, pero es parte del tercer pixel (su tercera componente de color).

El método del LSB funciona mejor en los archivos de imágenes que tienen una alta resolución y usan gran cantidad de colores (por eso el software usa 24 bits de color incluyendo el canal alpha). En caso de archivos de audio, favorecen aquellos que tienen muchos y diferentes sonidos que poseen una alta tasa de bits.

Además este método no altera en absoluto el tamaño del archivo portador o cubierta (por eso es "una técnica de sustitución"). Posee la desventaja de que el tamaño del archivo portador debe ser mayor cuanto más grande sea el mensaje a embeber; se necesitan 8 bytes de imagen por cada byte de mensaje a ocultar; es decir, la capacidad máxima de una imagen para almacenar un mensaje oculto es de su 12,5%. Si se pretende emplear una mayor porción de bits de la imagen (por ejemplo, no sólo el último, sino los dos últimos), puede comenzar a ser percibible al ojo humano la alteración general provocada.

De hecho, usar el bit menos significativo (LSB) significa sumar o restar un uno al valor de cada componente de RGB y por ende, no es discernible fácilmente por el ojo humano. Por ello, es una buena alternativa para poder cifrar mensajes en donde el transmisor y receptor tienen una manera de recuperar la información codificada.

El programa

El software permite utilizar este mecanismo de sustitución del bit menos significativo para encriptar mensajes de texto en una imagen de 4 bits de resolución. Cabe decir que el formato debe ser BMP y que formatos como JPG podrían alterar la información encriptada en la propia imagen pues éste es un formato que comprime los datos, por lo cual, no se puede garantizar que no se corroma la información al ser comprimida por el propio formato JPG. Por ende, el programa crea y salva imágenes esteganográficas del tipo BPMP (bitmap)

El programa contiene el siguiente menú principal:

Archivo Procesar Ayuda

La opción Archivo contiene las siguientes subopciones:

- Leer imagen
- Guardar imagen esteganográfica
- Cargar texto a encriptar
- Salvar texto recuperado
- Terminar

La opción Procesar contiene las siguientes subopciones:

- Encriptar texto en la imagen
- Desencriptar texto de la imagen

Finalmente la opción Ayuda tiene estas subopciones:

- Manual en línea (lo que está leyendo en estos momentos)
- Acerca de este programa (los créditos del software)

Las opciones son evidentes por sí mismas. Hay detalles que aclarar, sin embargo. La imagen original se carga en la parte de la izquierda y se copia a la derecha. Ésta es la imagen en donde se oculta el texto. En la parte del fondo de la pantalla puede verse el campo para alimentar el texto o cargar un texto de la computadora directamente. Este documento es ASCII, sin caracteres de control, texto simple, sin comandos que permitan cursivas, negritas, etcétera.

Una vez procesada la imagen, puede guardarse la misma (la imagen de la derecha) como un archivo BMP. Si se desea recuperar el texto escondido en la imagen, cargue la imagen en el programa (con la opción Leer imagen) y pídale al sistema que la decodifique (opción segunda en Procesar). Listo. Tendrá el texto que está escondido en esa imagen.

Comentarios, quejas y sugerencias

Escriba a ***morsa@la-morsa.com***