NAME

steghide − un programa de estenografía

SYNOPSIS

steghide *comando* [*argumentos*]

DESCRIPCIÓN

Steghide es un programa de estenografía que permite ocultar datos en varios tipos de imagen- y archivos de audio. Los respectivos muestreos de frecuencia de color no varían lo que hace que el adjunto soporte pruebas estadísticas del primer orden.

Sus características incluyen el compactado y el encriptado de los datos adjuntos, y revisión automática de integridad usando un checksum. Se reconocen los formatos de archivo JPEG, BMP, WAV y AU para usar como archivos de portada. No existen restricciones en el formato de los datos ocultos.

Steghide aplica un enfoque estenográfico 'gráfico-teórico'(e.i.'graph-theoretic'). No necesitamos saber nada sobre teorías gráficas para usar steghide. Tranquilamente podemos saltearnos el resto del párrafo si no nos interesan los detalles técnicos. El algoritmo de adjunto funciona así a groso modo: Primero, se compacta y encripta la información secreta. Luego se crea una secuencia de posiciones de pixels en el archivo portada basado en un generador pseudo-aleatorio de números inicializado con un salvoconducto (los datos secretos se adjuntarán en los pixels de estas posiciones). En estas posiciones,se excluyen los que no necesitan cambiarse (porque ya tienen el valor correcto, por casualidad). Luego, un algoritmo gráfico-teórico de concordancia halla pares de posiciones de forma que al intercambiar sus valores dejemos adjunta la parte correspondiente a los datos secretos. Cuando el algoritmo encuentra el último par, se realiza el intercambio. Los pixels de las posiciones sobrantes(las posiciones que no conforman dichos pares) también se modifican para llevar los datos adjuntos(pero esto se hace sobreescribiéndolos, no intercambiándolos con otros pixels). El hecho de que (en su mayor parte) se adjunta intercambiando valores de píxels implica que las estadísticas de primer orden (x.e. las veces que se usa un color en la imagen) no se alteran. En los archivos de audio se usa el mismo algoritmo, aunque se usan muestras de audio en lugar de pixels.

El algoritmo de encriptado por omisión es el Rijndael con clave de 128 bits de tamaño (que es EAE (e.i.AES)− Encriptado Avanzado Estandar) en la modalidad de encadenado de bloques de cifras. Si esta combinación, por el motivo que sea, no nos da confianza, tenemos la libertad de elegir otra combinación de algoritmo/tipo (el comando **encinfo** nos muestra información sobre todas las combinaciones de algoritmos y tipos). El checksum se calcula usando el algoritmo CRC32.

COMANDOS

En esta sección se listan los comandos de steghide. El primer argumento deberá ser siempre uno de los siguientes comandos. Podemos agregarle argumentos adicionales a los comandos **embed**, **extract** y **info**. Los demás comandos no llevan ningún argumento.

embed, --embed
: Adjuntar datos secretos en un archivo portada creando un archivo stego.

extract, --extract
: Extraer datos secretos de un archivo stego.

info, --info
: Mostrar información sobre un archivo portada o uno stego.

encinfo, --encinfo
: Mostrar una lista de algoritmos y tipos que pueden usarse. No necesita argumentos.

version, --version
Mostrar una breve información sobre la version. No necesita argumentos.

license, --license
Mostrar la licencia de steghide. No necesita argumentos.

help, --help
Mostrar una pantalla de ayuda. No necesita argumentos.

ADJUNTO

Deberíamos usar el comando **embed** cuando queremos adjuntar datos secretos en un archivo de portada. Con el comando **embed** pueden usarse los siguientes argumentos:

-ef, --embedfile *nomArchivo*
Declarar el archivo a adjuntar(el archivo que tiene el mensaje secreto). Notar que steghide adjunta el nombre original del archivo en el archivo stego. Cuando extraemos los datos (ver más abajo) tiende, por omisión, a grabar el archivo adjunto en el directorio actual y con su nombre de archivo original. Si se omite este argumento o *nomArchivo* es **-**, steghide leerá los datos secretos desde la entrada estandar.

-cf, --coverfile *nomArchivo*
Declarar el nombre del archivo de portada que usaremos para adjuntar los datos. El archivo de portada debe tener uno de los siguientes formatos: AU, BMP, JPEG o WAV. El formato del archivo se detecta automáticamente basándose en la información de su cabecera (no importa su extensión). Si omitimos este argumento o *nomArchivo* es **-**, steghide leerá el archivo de portada desde la entrada estandar.

-sf, --stegofile *nomArchivo*
Declarar el nombre del archivo stego a crearse. Si omitimos este argumento cuando llamamos a steghide con el comando **embed**, las modificaciones para adjuntar los datos secretos se harán directamente en el archivo portada sin grabarlo con un nombre nuevo.

-e, --encryption *algo* [*tipo*] | *tipo* [*algo*]
Declarar parámetros de encriptado. A esta opción debe seguirle una o dos cadenas que definan un algoritmo de encriptado y/o un tipo. Los nombres de todos los algoritmos y tipos posibles pueden obtenerse con el comando **encinfo**. El encriptado por omisión es **rijndael-128** (EAE) de tipo **cbc**. Si no quisiéramos usar ningún encriptado, usaríamos **-e none**.

-z, --compress *nivel*
Declarar el nivel de compactado. El nivel de compactado es de 1...9. Donde 1 representa el más rápido y 9 representa el mejor compactado.

-Z, --dontcompress
No compactar la información secreta antes de adjuntarla.

-K, --nochecksum
No adjuntar el checksum CRC32. Podemos usar esto si los datos secretos ya tienen algún tipo de checksum o si no queremos adjuntar esos 32 bits extras para hacer el checksum.

-N, --dontembedname
No adjuntar el nombre del archivo secreto. Si se usa esta opinión, el extractor necesitará declarar un nombre de archivo para decirle a steghide en donde escribiremos los datos adjuntos.

EXTRACCIÓN

Si hemos recibido un archivo que tiene un mensaje adjunto con steghide, usaremos el comando **extract** para extraerlo. Pueden usarse los siguientes argumentos con este comando.

-sf, --stegofile *nomArchivo*
Declara el archivo stego (el archivo que contiene los datos adjuntos). Si se omite este argumento o *nomArchivo* es **-**, steghide leerá un archivo stego desde la entrada estandar.

-xf, --extractfile *nomArchivo*
Crear un archivo con nombre *nomArchivo* y grabar los datos adjuntos del archivo stego en él. Esta opción sobreescribe el nombre del archivo adjuntado en el archivo stego. Si se omite este argumento, los datos adjuntos se grabarán en el directorio actual con su nombre original.

OBTENIENDO INFORMACIÓN DE UN ARCHIVO DE PORTADA/STEGO

Podemos usar el comando **info** para obtener información sobre un archivo portada o stego (por ejemplo su tamaño). Podríamos necesitar usarlo cuando recibimos un archivo y no estamos seguros de que contenga un mensaje adjunto o si pensamos usar cierto archivo como archivo portada y queremos averiguar su tamaño.

El comando de linea **steghide info** <*nomArchivo*> devolverá información sobre <*nomArchivo*> y luego nos preguntará si queremos ver la información sobre los datos adjuntos en ese archivo. Si respondemos 'yes' tendremos que escribir el salvoconducto que se usó para adjuntar los datos en ese archivo.

También podemos agregarle el argumento **-p, --passphrase** (ver abajo) al comando **info** para que steghide intente obtener automáticamente la información adjunta usando el salvoconducto declarado.

OPCIONES COMUNES

Las siguientes opciones pueden usarse en todos los comandos (donde tenga algún sentido).

-p, --passphrase
Usar como salvoconducto, la cadena que le sigue a este argumento. Si nuestro salvoconducto contiene espacios en blanco, habremos de encerrar todo entre comillas, por ejemplo: **-p "un salvoconducto muy extenso "**.

-v, --verbose
Mostrar información muy detallada sobre el estado del proceso de adjuntado o del de extracción.

-q, --quiet
Evitar mensajes informativos.

-f, --force
Siempre sobreescribir los archivos existentes.

OPCIONES DE NOMBRE DE ARCHIVO

Todos los argumentos de nombre de archivo (**-cf**, **-ef**, **-sf**, **-xf**) también aceptan **-** como nombre de archivo lo que hará que steghide use la entrada o salida estandar (lo que tenga sentido). Omitiendo el argumento correspondiente a su nombre de archivo es lo mismo que escribir **-** excepto en dos casos: Si se omite **-sf** en el comando embed, se harán las modificaciones directamente sobre el archivo de cubierta. Si se omite **-xf** para la extracción, los datos adjuntos se grabarán con el nombre de archivo que figura en el archivo stego. Así que cuando queramos asegurarnos de que se use la entrada/salida estandar, usaremos **-** como nombre de archivo.

EJEMPLOS

Básicamente se usa así:

```
$ steghide embed -cf imagen.jpg -ef secreto.txt
Ingrese salvoconducto:
Re-ingrese salvoconducto:
adjuntando "secreto.txt" en "imagen.jpg"... hecho
```

Este comando adjuntará el archivo secreto.txt en el archivo de portada imagen.jpg.

Una vez adjuntado nuestro archivo de datos secretos como vimos antes se puede enviar el archivo imagen.jpg a la persona que debería recibir el mensaje secreto. El receptor debe usar steghide de la siguiente manera:

```
$ steghide extract -sf imagen.jpg
Ingrese salvoconducto:
los datos extraídos se grabaron en "secreto.txt".
```

Si el salvoconducto declarado es el correcto, el contenido del archivo original secreto.txt se extraerá del archivo stego imagen.jpg y se grabará en el directorio actual.

Si hemos recibido un archivo que contiene datos adjuntos y quisiéramos tener más información sobre el mismo antes de extraerlo, usaremos el comando info:

```
$ steghide info archivo_recibido.wav
"archivo_recibido.wav":
  formato: wave audio, PCM encoding
  capacidad: 3.5 KB
¿ Intento extraer información sobre los datos adjuntos? (y/n) y
Ingrese salvoconducto:
  archivo adjunto "secreto.txt":
    tamaño: 1.6 KB
    encriptado: rijndael-128, cbc
    comprimido: si
```

Luego de emitir algunos datos generales sobre el archivo stego (formato, capacidad) se nos preguntará si queremos que steghide obtenga información sobre los datos adjuntos. Si respondemos con yes tendremos que declarar un salvoconducto. Steghide entonces intentará extraer los datos adjuntos con ese salvoconducto y - si tiene 'éxito - emitirá un informe sobre el mismo.

VALOR DE RESPUESTA

Steghide devuelve 0 si tiene éxito 1 si ocurre un fallo y debe terminar antes de terminar la operación solicitada. Las advertencias no tienen efecto en los valores de respuesta.

AUTOR

Stefan Hetzl <shetzl@chello.at>

Traducción al castellano

versión 1 - Alberto Adrián Schiano <chanio@users.sourceforge.net>