Ocultar datos en archivos de sonido

Juan Antonio Cano Salado Borja Moreno Fernández
Pascual Javier Ruiz Benítez

16 de mayo de 2011

Índice

1. Resumen

Este trabajo aborda la ocultación de datos en archivos de sonido o, lo que es lo mismo, la esteganografía de audio. El objetivo de esta disciplina consiste básicamente en ocultar información (de cualquier tipo) en archivos de sonido, de forma que los cambios llevados a cabo en el archivo original resulten imperceptibles para una persona.

Comenzaremos estudiando los principios básicos de la esteganografía en general, y de la esteganografía de audio en particular. A continuación, analizaremos algunos de los métodos más comúnmente utilizados en esteganografía de audio. Hecho esto, estudiaremos uno de los formatos de audio más populares: el formato WAV. Finalmente, incluiremos una descripción de la implementación realizada y proporcionaremos un manual de instalación y manejo de la aplicación desarrollada.

2. Introducción

2.1. Esteganografía

La esteganografía es la disciplina 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.

Los orígenes de la esteganografía datan de la antigua Grecia. Heródoto, famoso historiador griego, informa del uso de la esteganografía en informes de Grecia a Persia. El método consistía en afeitar la cabeza de un esclavo y tatuar allí un mensaje. Dicho mensaje quedaba oculto cuando el pelo del esclavo volvía a crecer. Para leer el mensaje sólo era necesario volver a afeitarle la cabeza al esclavo. La idea era que nadie sospechase de la existencia de dicho mensaje.

La esteganografía ha sido usada en numerosas ocasiones a lo largo de la historia: tintas invisibles, acrósticos o mensajes microscópicos son sólo algunas de sus formas. Recientemente, en plena era digital, la estaganografía ha adquirido gran importancia como tecnología utilizada en el campo de la seguridad informática. Pueden ocultarse mensajes secretos en correos electrónicos, imágenes, audio e incluso vídeo.

Diversos grupos han mostrado tener un gran interés en las aplicaciones de la esteganografía. Algunos, interesados en la protección de derechos de au-

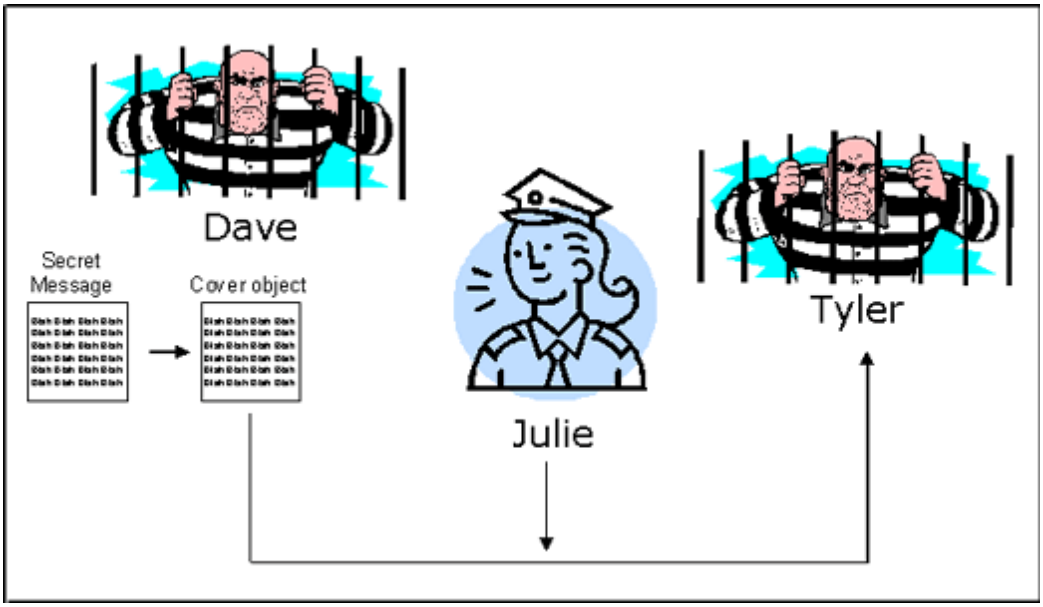

Figura 1: Problema de los prisioneros

tor. Otros, preocupados por proteger la privacidad de sus mensajes. Muchos gobiernos temen que la esteganografía podría convertirse en una herramienta de gran utilidad para criminales y grupos terroristas. En cualquier caso, parece claro que existen multitud de aplicaciones y usos para la esteganografía, y la mayoría de los expertos están de acuerdo en que será un tema de gran interés durante los próximos años.

La figura 1 ilustra un ejemplo simple de un problema en el que el uso de la esteganografía puede ser de utilidad.

Tyler y Dave están en la cárcel. Necesitan comunicarse para ultimar los detalles de un plan de fuga, pero tienen un gran problema: Julie, guardia de la prisión, tiene acceso a toda la correspondencia entre los prisioneros. La criptografía por sí sola no es una solución. Un mensaje cifrado levantaría todo tipo de sospechas. Los prisioneros deben idear un sistema que les permita pasar mensajes de apariencia inocente, con información oculta que sólo ellos puedan entender.

La esteganografía puede además combinarse con la criptografía para crear sistemas más seguros. Así, distinguimos:

- Esteganografía pura

La fortaleza del sistema recae en los algoritmos de ocultación y extracción de la información, que solo el emisor y el receptor del mensaje deberían conocer.

- Esteganografía de clave privada

  Fruto de la combinación de esteganografía pura con criptosistemas simétricos. Se asume que un atacante podría conocer los algoritmos de ocultación y extracción de la información. Por este motivo, el mensaje se cifra utilizando un cifrado simétrico antes de ocultarlo. De esta manera, incluso si el atacante intercepta la transmisión y logra extraer la información aún tendrá que enfrentarse al criptoanálisis del criptosistema utilizado.

- Esteganografía de clave pública

  Basada en unir esteganografía pura y criptosistemas de clave pública. De esta manera, el emisor y el receptor evitan tener que compartir una clave privada.

3. Descripción del problema

4. Soluciones presentadas

5. Conclusiones

6. Problemas abiertos

7. Implementación realizada

8. Manual de instalación y manejo de la aplicación

9. Bibliografía

10. Tabla de tiempo