Criptografía y Seguridad
Esteganografía

Giorgi Pablo (49222)
Perez De Rosso, Santiago (48274)
Zemín Luciano (48394)

27 de mayo de 2011

Índice

1. Introducción

En el presente documento se analizan cuestiones referentes al campo de la esteganografía.
Se elaboran conclusiones respecto al método en sí mismo, y cómo se lo podría mejorar. Además se lo combina con conceptos de criptografía para complementarlo y aumentar su seguridad.

2. Cuestiones a analizar

2.1. Ejercicio 6.1

Respecto de dónde comezar a guardar el archivo a ocultar se debe tener en cuenta un punto importante.
En la encriptación, comunmente se conoce que la información existe, pero se desea ocultarla. En la esteganogrfía, por el contrario, lo que se desea ocultar es la existencia misma de la información. Por tal motivo, a menos que se use esteganografía y encriptación en conjunto, si se sospechara de la existencia de la información no sería difícil que eventualmente se pudiera acceder a ella.
Por lo tanto, en un escenario de esteganogrfía puro (sin encriptar la información antes de ser ocultada), es altamente deseable que una vez que el archivo portador ya fue modificado, dicha modificación sea lo mas imperceptible posible.
Partiendo de esta base se puede pensar que la mejor forma de guardar información dentro de un archivo sea comenzar en aquel lugar donde el cambio sufrido por el archivo portador sea mínimo. Se puede afirmar que por cada bit que se desea almacenar, la probabilidad de producir un cambio en el archivo es de un 50 %, dado que si se desea guardar un 0, hay un 50 % de chances de que en la posición a modificar haya un 0 (no habría cambio) o haya un 1 (habría cambio). Al guardar un 1, el caso es análogo.
Por lo tanto, una buena estrategia para decidir dónde conviene comenzar a modificar el archivo es haciendo un análisis previo del mismo analizando tal cuestión.
Para verlo con un ejemplo simple. Se tiene que guardar la cadena 0011 en un archivo de 6 muestras de 2 bytes cada una de la siguiente manera:
01100101 11001001
00110001 11000010

00101011 00110011
01011000 00111101
10111001 10100110
00111100 01100110
Al tener el archivo portador 6 muestras de 2 bytes, y al tener que ocultar 4 bits, sólo se podría comenzar en las muestras 1, 2 o 3.
Para facilitar el análisis nos quedaremos con los bits que son factibles de ser modificados (los menos significativos de cada muestra), teniendo así la cadena 101100. Las 3 diferentes opciones para comenzar nos darían como resultado las cadenas:
001100 para la primera.
100110 para la segunda.
100011 para la tercera.
El porcentaje de cambio sufrido en cada una es de:
1/6 para la primera.
2/6 para la segunda.
4/6 para la tercera.
Lo que da como resultado que la posición más conveniente donde comenzar a guardar los datos es a partir de la primera muestra.
Es importante aclarar que si se considera la posibilidad de comenzar a guardar la información en una posición que puede cambiar, también ésta debe ser almacenada en el archivo, dado que de lo contrario no sería posible recuperar la información oculta. Una opción sería ahora sí guardarla a partir de la primera muestra, dado que el ruido que puede producir una modificación tan pequeña como para sólo guardar un número con una posición es mucho menor probabilísticamente al que produce la modificación de tantas muestras seguidas como lo requiere guardar la información que se desea ocultar.