Tecniche e strumenti di antiforensics

di William David Tänzer

3.1.2 Steganografia

La steganografia, dal greco *steganos* (στεγανός), nascosto, e graphei (γραφή), scrittura, s'intende la tecnica di nascondere le informazioni all'interno di altre informazioni.

Le informazioni possono essere inserite, per esempio, all'interno d'immagini, filmati, musica o testi.

A differenza della crittografia, la steganografia non attira l'attenzione di un eventuale investigatore. Un file crittato viene quasi certamente individuato durante l'analisi di un dispositivo digitale, un'informazione steganografata può essere trovata soltanto per mezzo di tecniche dette di stegoanalisi.

Le tecniche di stegoanalisi possono essere così catalogate:

- tecniche visive (su file jpeg, bmp, ecc.)
- tecniche sonore (su file wav, mp3, ecc)
- tecniche statistiche (cambiamenti nella struttura dei pixel meno significativi)
- tecniche strutturali (prendono in esame le proprietà dei file)

Per approfondire le tecniche di stegoanalisi si può consultare il sito http://www.sarc-wv.com/ (Steganography Analysis and Research Center).

In chiave anti forensics, è importante tenere presente che l'occultamento è tanto più sicuro, indipendentemente dalla bontà dell'algoritmo utilizzato, tanto più piccolo è il contenuto da occultare confrontato con la dimensione del medium utilizzato.

Al fine di aumentare ulteriormente la sicurezza e la forza anti forensics dell'informazione occultata, questa può essere prima crittata e poi steganografata.

Questa tecnica è ideale per trasferire informazioni tra un soggetto e un altro.

Una delle tecniche più efficaci è la steganografia nelle immagini.

Questa tecnica sfrutta la debolezza del sistema visivo umano.

Un'immagine digitale a colori non compressa è un file composto di 8 bit per pixel (se l'immagine è a 256 colori) o da 24 bit per pixel (per immagini a 16 Milioni di colori). Per esempio, un'immagine di 1920x1440 pixel con profondità di 24 bit (16 M colori) è un file composto di 2.764.800 byte.

Le immagini in formato raw non sono comunemente utilizzate per l'enorme dimensione dei file ottenuti. Vengono per cui normalmente compresse. La stessa immagine dell'esempio, compressa con l'algoritmo jpeg, ha la dimensione di 918.688 byte.

Ovviamente un'immagine raw offre più spazio per celare un messaggio ma questo tipo di oggetti, salvo che chi li detiene sia un fotografo, non venendo comunemente usati, attirerebbero troppo l'attenzione di un investigatore.

Affinché le modifiche apportate alle immagini appaiano invisibili ad occhio nudo, la quantità di dati inseribili deve essere per forza di cose piccola confrontata al contenitore.

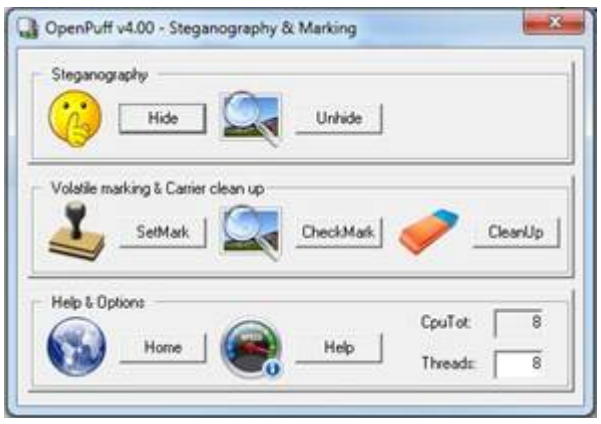
La tecnica più diffusa è la steganografia LSB (Rumore di Fondo) (17), che può essere applicata solo ad immagine non compresse o ad immagini compresse con metodi senza perdita di dati (png, bmp, Gif, tiff). Si basa sulla teoria che apportando modifiche impercettibili a un'immagine ad alta definizione questa non cambia. Si può ottenere una modifica impercettibile di un'immagine modificando il bit meno significativo di ogni byte componente l'immagine.

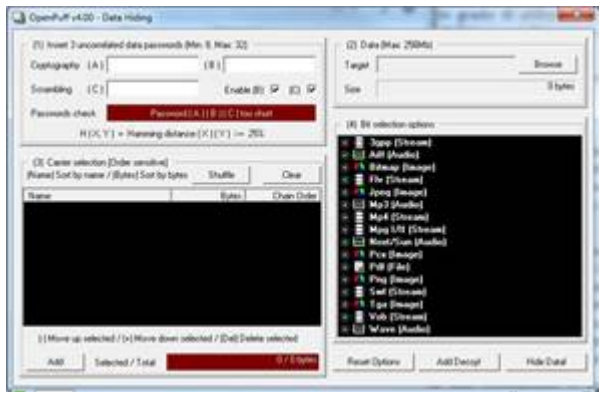
Senza l'intervento di tecniche steganografiche, questo già avviene normalmente a causa delle normali imperfezioni del sistema di acquisizione (scanner, fotocamera, ecc), appunto il rumore di fondo, o a causa dei filtri correttivi propri dei software di gestione del sistema di acquisizione (aumento del contrasto, miglioramento cromatico, ecc).

Come già precisato, questa tecnica può essere utilizzata solo con immagini non compresse o compresse con algoritmi lossless. Per utilizzare invece le diffusissime immagini in formato jpeg, che è un algoritmo di compressione con perdita (lossy), ottenute per esempio da fotocamere, si deve operare a un livello di rappresentazione intermedio, cioè bisogna iniettare le informazioni nei coefficienti di Fourier ottenuti nella prima fase di compressione (18) (19).

I messaggi segreti, che possono essere file di qualsiasi tipo (testo, immagini, binari, ecc), per quanto detto, devono avere dimensioni molto inferiori al contenitore; per ovviare a questa difficolta si può suddividere il messaggio in più contenitori.

Il migliore, a mio avviso, tool stegografico per Microsoft Windows è **OpenPuff** (http://embeddedsw.net/).





È un programma freeware le cui caratteristiche anti forensics sono:

· Generatore HW di numeri pseudo-casuali (CSPRNG)[2]

· Steganografia negabile [3]

· Catene di carrier (fino a 256Mb di dati nascosti)

· Selezione del livello di utilizzo dei bit dei carrier

· Multi crittografia moderna (16 algoritmi)

· Offuscamento dei dati a più livelli (3 password)

· Resistenza alla steganalisi X-quadro[4]

· OpenPuff supporta molti **formati di carrier**:

Immagini (BMP, JPG, PCX, PNG, TGA)

Audio (AIFF, MP3, NEXT/SUN, WAV)

Video (3GP, MP4, MPG, VOB)

Flash-Adobe (FLV, SWF, PDF)

· Crittografia a chiave simmetrica a 256bit+256bit con estensione della password KDF4

· Scrambling a chiave simmetrica a 256bit (Shuffling basato su CSPRNG)[5]

· Whitening (Mix con rumore basato su CSPRNG)[6]

· Codifica dei carrier bit adattiva e non-lineare[7]

· Struttura nativa portatile (nessuna installazione, chiavi di registro, file .ini)

· Si esegue in user mode con DEP (Data Execution Prevention) on

· Supporto multithread (fino a 16 CPU) = Esecuzione più veloce

· Spyware/adware-free

· Liberamente ridistribuibile

· Nucleo della libreria crittografica OpenSource (libObfuscate)

È un software per la stegografia completo e molto sicuro. L'unico che ho trovato in grado di utilizzare come carrier anche i filmati, con la possibilità per cui di inserire moltissime informazioni al loro interno.

Può inoltre lavorare con catene di carrier ottenendo così la possibilità di nascondere file anche molto grossi.

Dal punto di vista anti forensics è molto interessante il concetto di steganografia negabile. Concettualmente assomiglia alla tecnica utilizzata da Truecrypt che permette l'inserimento di un disco virtuale crittato nascosto all'interno di un disco virtuale crittato noto.

La crittografia/steganografia negabile, è una tecnica basata sull'uso di un'esca che permette di negare in maniera convincente di stare nascondendo dati sensibili, anche se gli attaccanti possono dimostrare che si sta nascondendo qualcosa. Basta semplicemente fornire un'esca sacrificabile che plausibilmente deve rimanere confidenziale. Verrà rivelata all'attaccante, sostenendo che questa è l'unico contenuto.

Come è possibile? I dati crittografati e sottoposti a scrambling, prima di essere iniettati nei carrier, sono sottoposti a whitening con una grande quantità di rumore. I dati esca possono sostituire un po' del rumore senza compromettere le proprietà finali di resistenza alla crittoanalisi. I dati sensibili e i dati esca sono crittografati usando password differenti. Si devono scegliere due diversi insiemi di diverse password. (20)