Steganografia nei File Audio

Simona Di Ienno

Steganografia e Comunicazioni Audio

La steganografia nelle comunicazioni audio viene utilizzata sin dai tempi delle guerre mondiali, per via dell'esigenza di comunicazioni sicure. Queste tecniche sono arrivate fino ai giorni nostri in quanto i principali canali di comunicazione (linee telefoniche, trasmissioni radio, ...) trasmettono segnali accompagnati da qualche tipo di rumore che ben si presta a nascondere messaggi

Il segnale audio digitale

Il segnale audio è per sua natura un segnale analogico, la cui ampiezza può assumere un'infinità di valori passando da un valore minimo ad uno massimo.
I computer gestiscono invece l'informazione digitalmente, è però possibile rappresentare un segnale audio campionandolo.

La funzione assumerà dei valori numerici discreti, e presenterà dei salti fra un valore e l'altro, poiché abbiamo assegnato un singolo valore ad un intervallo di tempo che prima ne presentava infiniti.
In questa operazione viene introdotto del rumore.
Il segnale da considerare perfetto sarà quello di qualità CD, con passo di campionamento pari a 44100Hz e quantizzazione dei campioni a 16 bit.

File Audio come Cover

Le ridondanze che si creano nei file audio digitali li rendono adatti a recitare il ruolo di cover. Come per le immagini, la tecnica più usata per nascondere messaggi segreti nei files audio consiste nel rimpiazzare i bits meno significativi. Lo “spazio” che le tecniche steganografiche utilizzano per nascondere i file nasce da come il file audio digitale viene manipolato per

Compressione

Le procedure di compressione dell'audio sono numerose ed utilizzano tecniche anche molto differenti una dall'altra. Esistono però tre categorie principali:

- **codifica nel dominio del tempo:** caratterizzata dal fatto di esaminare il segnale nel dominio del tempo, ma nel dominio della frequenza.

Il Mascheramento

Oltre al mascheramento in frequenza, esiste un altro tipo di mascheramento, quello temporale.

L'orecchio umano è maggiormente sensibile alle frequenze comprese fra 2 e 4 KHz, che richiedono pochissimi dB per essere percepite.

ESEMPIO

Supponiamo di avere due toni, uno forte e l'altro, che gli è vicino in frequenza, piuttosto debole. Sappiamo già che il nostro orecchio sente solo il tono più forte, ma se improvvisamente il tono maschera cessasse di esistere, non si avvertirebbe subito il tono più debole.

Per questo motivo, risulta importante la scelta della sorgente audio più appropriata, perciò sarà più semplice nascondere informazioni in un file audio di heavy-metal rispetto ad uno di musica leggera.

In conclusione, l'effetto complessivo del mascheramento è che molti toni non saranno mai udibili perché collocati nel dominio della frequenza e del tempo troppo vicino a toni forti.

ESEMPIO Supponiamo che venga diffuso un tono alla frequenza di 1 KHz, detto tono maschera, tenuto fisso a 60 dB (volume alto) ed un secondo tono, detto tono di test. Risulterà necessario alzare il volume del tono test per riuscire a distinguerlo. Oltre i 4 KHz e al di sotto degli 0.5 la situazione torna normale però nell' intorno di 1KHz i due toni sono praticamente indistinguibili a meno di non alzare pesantemente il volume del tono test.

La Trasmissione

Quando i segnali audio devono essere trasmessi, bisogna considerare il mezzo di trasmissione attraverso il quale il segnale dovrà essere propagato.
Esistono quattro diversi ambienti di trasmissione:

Ambiente digitale: se un file sonoro è copiato direttamente da una macchina ad un'altra: il campione del segnale resta lo stesso fra la sorgente e la destinazione.

Ambiente di ricampionatura con aumento/decremento: il segnale viene rimodellato secondo un nuovo tasso di campionatura, ma resta digitale dal principio alla fine. Le caratteristiche temporali del segnale cambiano.

Ambiente "over the air": questo avviene quando il segnale viene "suonato nell'aria" e rimodellato con l'aiuto di un microfono. In tal caso il segnale potrà essere soggetto a possibili modifiche non lineari, che causeranno variazioni di fase e di ampiezza, accumulo di componenti di frequenza diverse, ecc.

Trasmissione analogica e ricampionatura: questo accade quando il segnale viene convertito in uno stato analogico e rimodellato. Solo la fase resta invariata.

L’Occultamento

La rappresentazione digitale del segnale ed il mezzo di trasmissione dello stesso sono i due principali elementi che devono essere presi in considerazione nell’analisi di una procedura di data hiding in file sonori. La quantità di informazioni che si potranno nascondere dipenderà dal tasso di campionatura e dal tipo di suono che dovrà essere modificato.
Il processo di occultamento dei dati in file audio si può effettuare in diversi modi

L'Occultamento: codifica nei bit "bassi"

Uno è il cosiddetto metodo di **codifica nei bit "bassi"**: tale procedura sostituisce i bit di informazione meno significativi di ogni punto campione del segnale con una stringa binaria codificata. Può però introdurre un fastidioso rumore di fondo.

Il maggiore inconveniente di tale metodo è la scarsa resistenza ad eventuali manipolazioni, quali l'introduzione di segnali di disturbo nel canale di trasmissione o la ricampionatura del segnale, a meno dell'utilizzo di tecniche di ridondanza.

L'Occultamento: codifica delle fasi

Un secondo metodo di data hiding in file audio è la **codifica delle fasi**: tale procedura funziona sostituendo la fase di un segmento iniziale del file audio con una fase di riferimento che rappresenta i dati.

L’Occultamento: spread spectrum

Una terza tecnica è lo **spread spectrum** che diffonde i dati codificati attraverso lo spettro delle frequenze, rendendo difficile scovare le informazioni, a meno di non conoscere la chiave pseudocasuale. Il ricevente dovrà conoscere oltre alla chiave anche i punti di inizio e di fine del messaggio nascosto nel file audio.

Lo spread spectrum introduce un rumore di fondo casuale al suono al di sotto della soglia di percezione; inoltre, opportuni codici di correzione dell’errore garantiscono l’integrità dei dati. La quantità di informazioni che si

L'Occultamento: echo data hiding

L'ultima procedura è l'**echo data hiding** che inserisce le informazioni in un segnale ospite introducendo un'eco. I dati vengono celati modificando tre parametri dell'eco: l'ampiezza iniziale, il tasso di indebolimento del suono ed il ritardo.

Mentre il ritardo tra il suono originale e l'eco diminuisce, i due segnali si mescolano fino a che l'orecchio umano non può più distinguerli.

Usando due diversi ritardi possiamo codificare le cifre 1 o 0. Per codificare più di un bit, il segnale originale viene diviso in parti, su ognuna delle quali viene introdotta un'eco.

ESEMPIO: file .WAV con codifica dei bit “bassi”

Ad esempio i file sonori WAV in Windows sono immagazzinati usando 8 o 16 bit (che vengono poi eventualmente convertiti da una scheda sonora). Un file da 8 bit implica che i valori possono essere in un range da 0 a 255. Il range dei 16 bit varia invece da 0 a 65535. Tutto quello che un programma steganografico esegue, è distribuire la sequenza di bit che corrispondono al file da nascondere nei bit meno significativi del file sonoro.

Ad esempio, ammettiamo che siano presenti i seguenti byte:

132	134	137	141
121	101	74	38

che in binario diventano:

10000100	10000110	10001001	10001101
01111001	01100101	01001010	00100110

Supponendo di voler nascondere il byte **11010101** (cioè 213) in questa sequenza, il programma semplicemente sostituisce i bit meno significativi di ogni byte con il corrispondente bit estratto dal byte che si vuole nascondere:

10000101	10000110	10001000	10001101
01111000	01100101	01001010	00100111

133	135	136	141
120	101	74	39

ESEMPIO: file .WAV con codifica dei bit “bassi”

Per averne un idea, un file wav stereo di un minuto è grande:

16bits x 44100Hz x 60sec = 42336000bits = 5168Kb

da raddoppiare perché il file è stereo, quindi

10336 Kb = 84762000 bits circa

Se decidessimo di utilizzare i 2 bits meno significativi per ogni stringa di 16 bits otterremmo una disponibilità di

84762000bits/16bits x 2 = 1059525bits = 1293Kb

Come si può quindi vedere, i valori del file sonoro sono cambiati, al massimo, di un valore per ciascun byte. Questa differenza non sarà assolutamente percepibile all'orecchio umano, circa, infatti, a 16 bit, per esempio, indica che è stata generata una stringa di 16 bits ogni 1/44100 di secondo. Nel caso di un wav stereo, le stringhe di 16 bits ottenute sono due, una per il canale destro ed una per il sinistro.

Usi Illegali

Messaggi subliminali: Tracce sonore, ascoltate in avanti o anche all'indietro, incise su dischi, nastri o CD al di sotto del livello di percezione.

Steganalisi

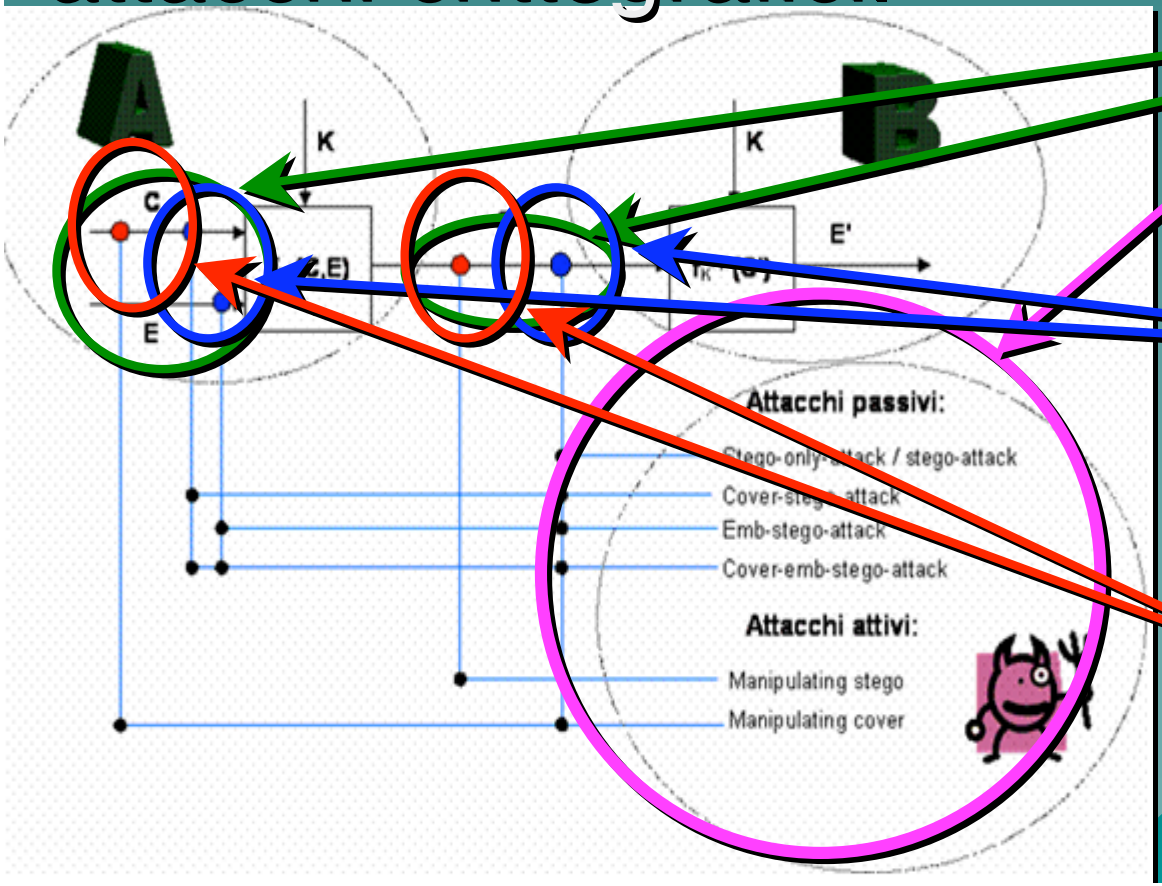
Steganalisi

Mentre un crittanalista applica la crittanalisi per cercare di decodificare o rompere messaggi criptati, lo steganalista è colui che applica la steganalisi cercando di determinare l'esistenza di eventuali informazioni nascoste. In crittografia si poteva partire dal confronto di porzioni di testo in chiaro e parti di testo cifrato. Con la steganografia invece, il confronto può essere fatto tra il testo di copertura, il messaggio steganografato ed eventuali porzioni di testo segreto.

Uno stegosistema sicuro potrebbe essere un sistema nel quale nessun intruso possa accorgersi di differenze tra il testo di copertura C e il testo steganografato S contenente l'informazione nascosta E, a meno che non conosca la chiave K.

Steganalisi

Questo stegosistema può essere esteso per includere situazioni di attacchi simili agli attacchi crittografici.



C'è un cerchio tra (rosso o blu) e attaccante può avere accesso: l'attaccante ha accesso

Un cerchio tra (rosso o blu) e Alice un punto in cui un attaccante può avere accesso: i punti in cui l'attaccante ha accesso

mentre nel primo tipo gli attaccanti riescono solo ad intercettare i dati, nel secondo riescono anche a manipolarli.

definiscono il tipo di attacco.

Steganalisi

Tipi di attacchi:

stego-only-attack

stego-attack

cover-stego-attack

cover-emb-stego-attack

manipulating the stego data

manipulating the cover data

Lo stego-attack e il cover-stego-attack possono essere prevenuti se il mittente agisce con cautela.

Un utente non dovrebbe mai usare come cover più volte lo stesso file, né files facilmente reperibili o di uso comune.

Steganografia

FUTURE APPLICAZIONI

Attualmente si sta lavorando al concetto di Steganografia di Internet, e cioè alla possibilità di nascondere informazioni ed eventualmente essere in grado di recuperarle dagli header dei pacchetti TCP/IP o da altre trasmissioni di rete. Inoltre anche se la steganografia e la crittografia sono discipline indipendenti, possono essere impiegate per alterare ed occultare un testo, garantendo un livello di sicurezza molto superiore.

CONCLUSIONI

Si potrebbe obiettare che se dei criminali potessero nascondere le informazioni in modi così efficaci la difesa dei cittadini diventerebbe più difficile, ma a questo si può rispondere dicendo che i disonesti non obbediranno mai ad una legge che imponga loro di non utilizzare alcuna forma di steganografia o altro, il problema fondamentale è fornire all'onesto cittadino gli strumenti che gli consentiranno di proteggere la propria privacy: la crittografia e la steganografia.

Fine