

ALGORITMI STEGANOGRAFICI

Chi si trova a disegnare un algoritmo steganografico deve cercare di soddisfare due esigenze opposte: l'invisibilità del messaggio e la sua lunghezza (payload). Per invisibilità si intende sia all'analisi di persone (che il dato generato sia coerente, almeno alle apparenze, con dati simili) sia da parte di computer (quindi analisi matematiche, statistiche e di confronto con archivi).

Esistono tre principali categorie di algoritmi steganografici:

- **Steganografia selettiva:** consiste nel selezionare da un database un file che di per sé rappresenta un messaggio. Esempio: Alice ha un database di immagini ognuna delle quali rappresenta un messaggio, ad esempio un bit. E' poco utilizzato perché il payload è molto basso.
- **Steganografia generativa:** consiste nel creare un file (ad esempio una immagine o un video) che contiene il messaggio da trasmettere. Poco considerata fino a qualche anno fa a causa della sua difficoltà e di un payload comunque basso, è stata riconsiderata dopo l'invenzione delle Generative Adversarial Networks (GAN). Le GAN sono delle reti neurali che permettono di creare dal nulla immagini molto realistiche con delle caratteristiche predefinite.
- **Steganografia iniettiva:** E' di gran lunga il metodo più utilizzato. Consiste nell'inserire il messaggio segreto all'interno di un file già esistente. Per esempio, modificare il bit meno significativo per ogni pixel di una immagine, ma attenzione! Payload troppo alti possono lasciare tracce inaspettate!

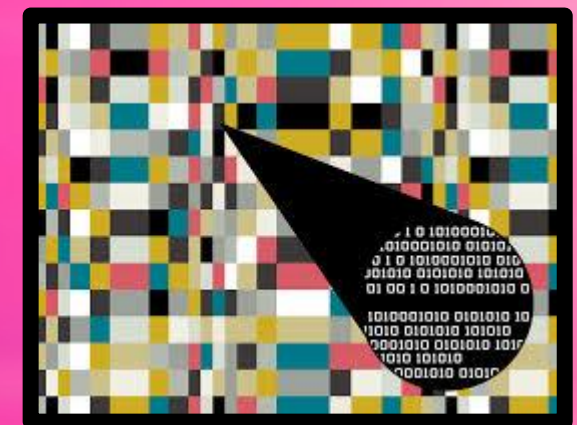
STEGANALISI

La steganalisi sta alla steganografia come la crittanalisi sta alla crittografia. L'obiettivo della steganalisi è infatti quello di capire se un file contiene un messaggio nascosto. La steganalisi utilizza soprattutto tecniche statistiche per individuare dei comportamenti anomali. Ad esempio l'istogramma di una immagine può rivelare se un messaggio è stato inserito modificando il bit meno significativo!



LA STEGANOGRAFIA

Scopri cos'è la steganografia e le tecniche utilizzate



RIFERIMENTI

- <https://www.c3t.it/projects/awareness/articoli&brochure/steganografia/>



CHE COS'E' LA STEGANOGRAFIA?

La steganografia (dal greco steganòs, nascosto, e gràphia, scrittura) è una tecnica che permette la comunicazione nascondendo l'esistenza stessa della comunicazione.

A differenza della crittografia, dove l'avversario è a conoscenza dell'esistenza di una comunicazione in atto, la steganografia si pone come obiettivo quello di nascondere la comunicazione stessa.

In altre parole, la crittografia fallisce quando l'attaccante ricostruisce il messaggio originale. La steganografia fallisce quando l'attaccante capisce che c'è un messaggio nascosto (senza necessariamente essere in grado di decifrarlo).

Questo avviene nascondendo il messaggio in un altro messaggio apparentemente innocuo. Nella steganografia digitale ad esempio, si possono utilizzare un file di documento, un file di immagine, un programma o un protocollo. I file multimediali sono ideali per la trasmissione steganografica a causa della loro grande dimensione. Chi invia il messaggio potrebbe inviare un file di immagine innocuo e regolare il colore di un pixel per farlo corrispondere a un carattere alfabetico. La modifica è così sottile che è improbabile che si noti la modifica.

La steganografia nella storia

La storia della steganografia è lunga quasi quanto quella del genere umano. I primi utilizzi risalgono al 440 a.C quando, come ci narra Erodoto, Demarato di Sparta, per avvisare i compatrioti di un imminente attacco persiano scrisse su una tavoletta un messaggio e poi la coprì di cera scrivendo sopra un messaggio innocuo.

Un esempio più recente è il microdot, utilizzato durante la guerra franco-prussiana. Consisteva nel rimpicciolire e nascondere il messaggio segreto in puntini del diametro inferiore al millimetro, che poteva essere nascosta nel puntino di una 'i' in una comunicazione banale

Al di fuori del contesto della guerra, nel 2010, durante l'importante torneo di scacchi a Khanty-Mansiysk (Russia), la squadra francese utilizzò un elaborato sistema per suggerire al giocatore una specifica casella della scacchiera. Un altro membro della squadra si sedeva in un determinato posto della sala e assumeva una certa posa, dopo che aveva ricevuto tramite messaggio cifrato la mossa migliore elaborata con l'ausilio di un computer. Tutti i componenti della squadra furono ovviamente squalificati.

Negli ultimi anni la diffusione del materiale digitale ha cambiato l'approccio allo studio della steganografia, trasformandola sempre più, un po' come la crittografia, da arte a scienza.

