LA STEGANOGRAFIA

Indice:

By Bl4ckD0t

1) Definizione e teoria

La steganografia è una tecnica nata in tempi antichi che consiste nel **nascondere** un **messaggio** o un **oggetto all'interno di un altro**, in modo tale da **nasconderlo ad occhi indiscreti** e renderlo quindi più sicuro e segreto. Solitamente tale tecnica veniva utilizzata tra due o più parti, entrambe a conoscenza del metodo per trovare il messaggio segreto, per scambiarsi messaggi senza destare sospetti ad occhi estranei o a persone predisposte per il controllo/intercettazione dei messaggi.

La parola "steganografia" deriva al greco ed è composta dalle parole "coperto" e "scrittura".

2) Differenze tra steganografia e crittografia

Generalmente, soprattutto per i neofiti, si pensa che crittografia e steganografia siano "sinonimi", o perlomeno strettamente correlati dal punto di vista dello scopo.

Bisogna dire però che sebbene entrambe le attività mirino a proteggere un qualcosa, la **steganografia non modifica l'oggetto di per sé**, ma semplicemente **lo nasconde** in un altro, lasciando però l'oggetto da proteggere "in chiaro". Tale pratica dunque mira a nascondere un oggetto in un mezzo, per proteggerne il trasporto da occhi indiscreti.

La crittografia invece ha come scopo criptare il messaggio stesso, senza nasconderlo agli altri, poiché la stessa cifratura funge da protezione verso chi non conosce il metodo per decriptarne il contenuto.

Steganography vs. Cryptography

Steganography	Cryptography
Hide the message	Does not hide message
Only sender and receiver knows the existence of message	Everybody knows the existence of message
End result is stego-media	End result is cipher-text
Used from ancient time till modern era	Used in modern era

Le due **funzioni** quindi sono leggermente **differenti**, e poiché non sono obbligatoriamente interscambiabili è permesso applicale assieme, dunque criptare prima un messaggio, e successivamente nasconderlo all'interno del contenitore (o comunque effettuare uno dei tanti processi di steganografia).
Vedremo perché non è consentito fare l'opposto nel capitolo 7.

3) Storia e prime apparizioni

Fin dall'antichità (e per antichità si intende al tempo degli Egizi e Greci) si è sempre cercato un modo per poter comunicare segretamente con altre persone senza venir scoperti. Le motivazioni ai tempi potevano essere "soffiate" sui futuri attacchi di popolazioni straniere, avvertimenti di guerra o patti tra sovrani.

Tale necessità portò a inventarsi un metodo alternativo per comunicare segretamente, e il primo caso di steganografia conosciuto al mondo fu narrato da Erodoto, il quale disse che per avvisare di una possibile invasione Persiana, **incise su delle tavole** di cera **il messaggio**, e poi, ricoperte a loro volta da altra cera, **incise sopra un messaggio fittizio** su un carico di cereali, in modo che a prima vista le tavolette sembrassero semplici documenti di importazione ed esportazione di cibo, ma in realtà fosse una soffiata su un futuro attacco.

La stessa idea venne poi utilizzata per comunicare con un vassallo un avviso segreto. Venne **inciso sul cuoio capelluto** di uno schiavo un messaggio, in modo tale che quando i capelli fossero stati abbastanza lunghi tale messaggio sarebbe stato al sicuro. Così lo schiavo venne spedito in viaggio, col messaggio segreto inciso in testa, e una volta giunto a destinazione e rasato dal vassallo, il messaggio sarebbe stato recepito.

Oggi giorno la steganografia è un concetto più virtuale che fisico, ma basti pensare alle "penne dall'inchiostro simpatico" per capire che anche la pratica fisica esiste ancora.

4) Prima classificazione

Le tecniche steganografiche si possono classificare in base alla relazione col contenitore oppure alle operazioni sul messaggio

La **prima classificazione** (relazioni col contenitore) permette di suddividere la pratica steganografica in due macro-gruppi:

a) **Steganografia iniettiva**: è la **più comune** e utilizzata. Consiste **nell'inserire un messaggio all'interno di un contenitore già esistente**, al fine di

nasconderlo all'occhio umano. Il contenitore all'apparenza risulterà sempre uguale, ma se analizzato mostrerà il messaggio.

b) **Steganografia generativa**: consiste nel **costruire un contenitore apposta** per il messaggio, in modo tale da personalizzarlo secondo le esigenze.

5) Seconda classificazione

La **seconda classificazione** (in base alle operazioni sul messaggio) permette di suddividere le tecniche in tre applicazioni:

a) **Steganografia sostitutiva**: come per la iniettiva, è il metodo preferito dalla maggior parte degli applicatori. Consiste nel **sostituire parti di contenitore che** anche se modificate **non influiscono** nel modo in cui esso appare (quindi nel caso di foto si parla di bit non significativi, nel caso di video di frame e nel caso di audio di rumore di fondo). In questo modo anche se si sostituiscono porzioni di contenitore, siccome queste sono poco significative, non si modifica il risultato finale, facendo apparire il contenitore uguale a prima dell'iniezione del messaggio.
   Inoltre maggiore è la qualità del contenitore, maggiori saranno le porzioni di contenitore sostituibili (basti pensare a una foto a 500x500 e una 1920x1080)

b) **Steganografia selettiva**: è un'applicazione **puramente teorica** e poco utilizzata, poiché dispendiosa in termini di tempo e poco proficua (non permette di scambiare grandi messaggi). Si basa prettamente **sull'analisi dei contenitori** per ricavarsi il messaggio. Per funzionare deve esservi un **accordo orale tra i due comunicanti**, che determinano delle regole generali e utilizzano i contenitori per rispettarle.

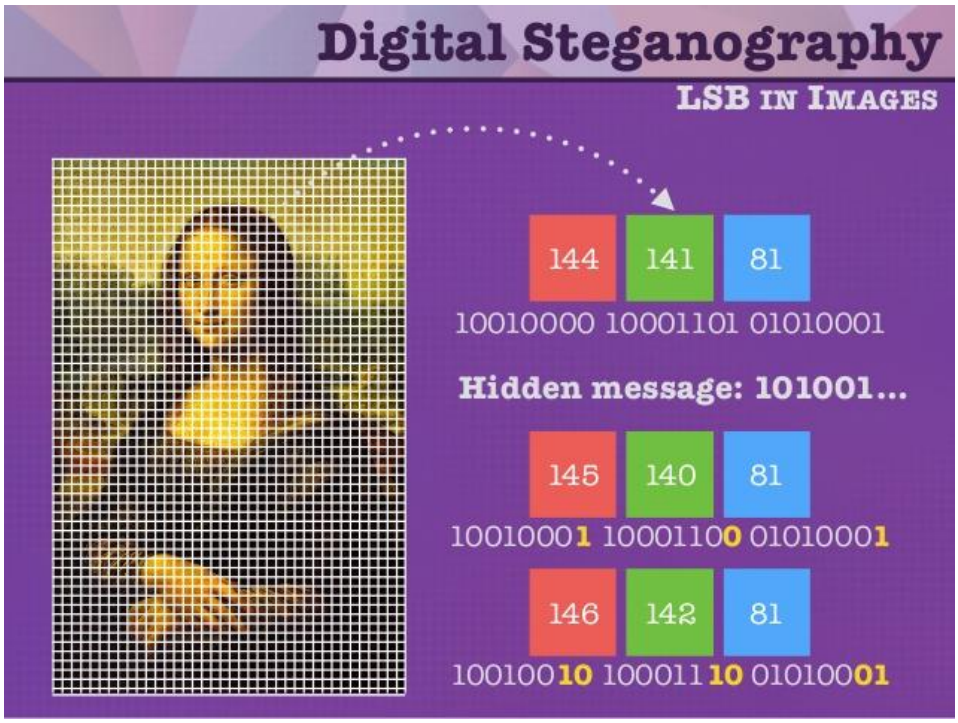
c) **Steganografia costruttiva**: è una particolare steganografia sostitutiva che punta alla **sostituzione di porzione di contenitore mantenendone** però le stesse **caratteristiche** (es. la sostituzione del rumore di fondo viene fatta con un messaggio che emuli il rumore di fondo.)

6) Esempi di steganografia

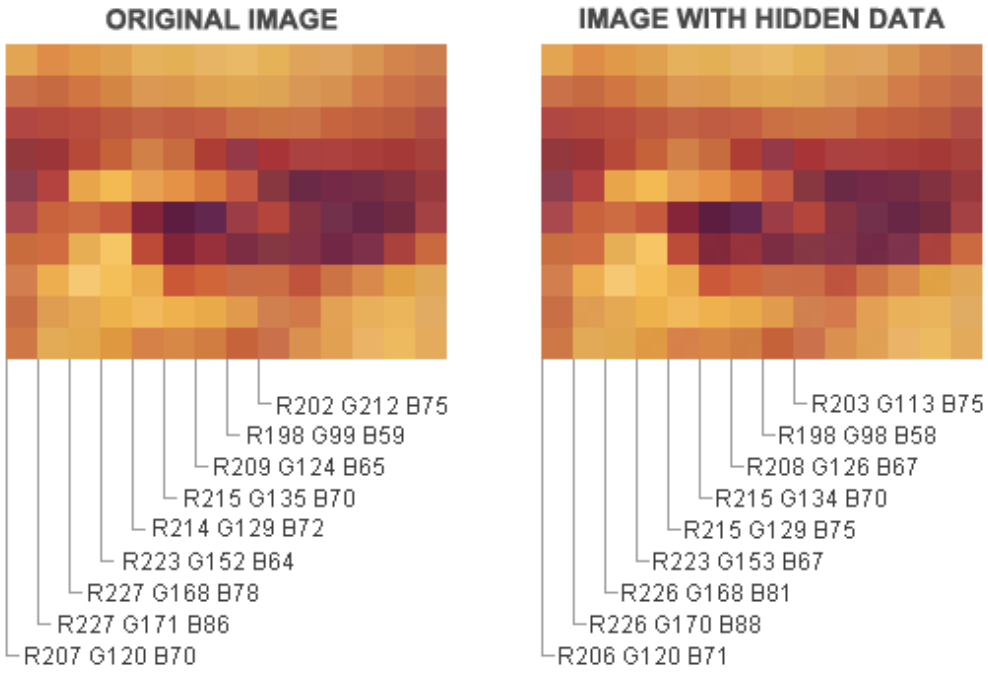
Nel capitolo precedente abbiamo parlato di diversi tipi di steganografia ma dal puro punto di vista teorico. Ora invece ci addentreremo nell'aspetto pratico della faccenda.

a) Sostitutiva: come già accennato, alla base di questa tipologia ci sta la sostituzione di parte del contenitore con quella del messaggio da iniettare.

Il metodo più utilizzato è l' **LSB** (**Less Significant Bit**), dove a venir sostituiti sono i bit meno importanti e appariscenti.



Sebbene i bit vengano modificati, non verranno percepite differenze dall'occhio umano, e tolta un'accurata analisi, nulla potrà mai rivelare che si tratta di un contenitore e non di una normalissima foto.



Di fatto, la tecnica è quelle di incrementare o diminuire di una sola unità i bit meno significativi, in modo che le modifiche siano impercettibili, e che

anche un'analisi delle perdite di qualità non riesca a definire se si tratti di una compressione, dovuta alla piattaforma o al mezzo trasmissivo, o meno.

b) Selettiva: è la più difficile da applicare, poiché lunga e poco performante. Si tratta di analizzare i contenitori per generare attraverso la sola osservazione, il messaggio finale. Facciamo un esempio.

Mattia e Paola si devono scambiare un messaggio corto, ma non vogliono utilizzare le normali tecniche. Decidono dunque di utilizzare la steganografia selettiva. Decidono che **ogni SMS** che si scambiano **sarà il contenitore** da analizzare. La loro **regola** è che il **numero di lettere della prima riga** del SMS **corrisponde al numero decimale della lettera** del messaggio vero.

Quindi, per scrivere solo un messaggio come "**ciao**", si dovranno utilizzare **4 SMS** (uno per lettera), e il **primo** dovrà contenere **3 lettere** nella prima riga, il **secondo 9**, il **terzo una** e **l'ultimo 15** (C=3; I=9; A=1; O=15).

In questo modo il messaggio non sarà presente direttamente nel contenitore, ma dovrà venir generato da esso.

7) Software steganogafici

Software per la steganografia ormai ne è pieno il web. Ognuno varia di poco o nulla dagli altri, e lo scopo e sempre lo stesso. Sono in grado di nascondere messaggi dentro qualunque tipo di file (audio, video, immagine) e decidere quale sia il migliore è difficile, se non impossibile, dipende tutto dai propri gusti.

Di seguito un elenco di alcuni di questi e dei formati gestiti per l'iniezione:

- **DeepSound**: permette di iniettare all'interno di file audio. Supporta inoltre una criptazione con chiave a 256bit e protocollo AES.
- **SilentEye**: tool con GUI multipiattaforma (Win, Linux e Mac)
- OpenPuff: numerosi tipi di file e crypt AES, opensource e per Win.
- StegHide: da CLI, disponibile per Win e Linux. Molte opzioni.
- **Spammimic.com**: sito per la creazione di steganografia con metodo spam.

8) Problematiche e pericoli

Le problematiche maggiori sono legate al fatto che **il contenitore**, una volta che il messaggio è stato iniettato al suo interno, **deve restare invariato**.

Anche **la più piccola modifica** di un pixel, o di un bit, può portare alla **corruzione del messaggio** segreto e alla relativa perdita di esso.
Ecco perchè non si può prima iniettare il messaggio e poi criptare il file. Perché una decriptazione fatta male, rischia di non restituire più il file messaggio originale. E' sempre quindi un bene prima criptare il messaggio, e poi nasconderlo nel contenitore.
Inoltre bisogna stare **attenti** ai **canali di trasmissione**, come social network e alcune email, che **comprimono automaticamente il file/allegato spedito**.
Una compressione, come un ridimensionamento dell'immagine, o un pitch dell'audio, o un fotogramma scartato in un video, o qualche modifica di qualche colore o parametro, porterebbero alla perdita del messaggio.
Siate quindi prudenti!