Università di Catania
Dipartimento di Matematica e Informatica

Progetto Digital Forensics

Segreti Digitali: Un'Introduzione alla Steganografia

Sergio Mancini - 1000022352

Anno Accademico 2022/2023

1 Introduzione alla Steganografia

La Steganografia è l'arte di nascondere un messaggio segreto all'interno di qualcosa che non è segreto. Questo qualcosa può essere praticamente tutto ciò che si vuole, per esempio incorporare un pezzo segreto di testo all'interno di un'immagine. Oppure nascondendo un messaggio segreto o uno script all'interno di un documento Word o Excel.

Lo scopo della Steganografia è quello di nascondere e ingannare, è una forma di comunicazione segreta e può comportare l'uso di qualsiasi mezzo per nascondere i messaggi. Ma la Steganografia non è una forma di crittografia, perché non comporta la cifratura dei dati o l'utilizzo di una chiave. La crittografia è una scienza che consente in gran parte la privacy, la Steganografia è una pratica che consente la segretezza e l'inganno.

1.1 Applicazioni moderne

La Steganografia è stata utilizzata per secoli, ma al giorno d'oggi gli hacker e i professionisti IT l'hanno digitalizzata per fare alcune cose piuttosto creative. Ci sono un certo numero di app che possono essere utilizzate per la Steganografia, tra cui Steghide, Xiao, Stegais e Concealment. La parola Steganografia sembra fantasiosa, ma in realtà proviene da un luogo abbastanza normale. La radice "steganos" è greca per "nascosto" o "coperto", e la radice "grafico" è greco per "scrivere". Insieme queste parole formano qualcosa di simile alla "scrittura nascosta" o alla "scrittura segreta".

2 Strumenti e software per la Steganografia

La Steganografia nasconde informazioni importanti all'interno di testi, immagini, audio, video e qualsiasi file digitale.

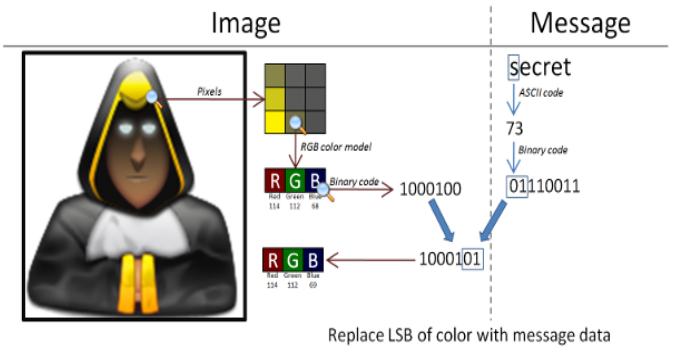


Figure 1: Esempio di Steganografia

2.1 Steganografia a livello di immagine

Le immagini sono uno dei file più utilizzati per nascondere testi nascosti, poichè l'alterazione di bit non è semplice da rilevare. Le tecniche utilizzate sono principalmente due:

1. Inserimento del messaggio nell'immagine, modificando i bit.
2. Modifica dell'immagine e successivamente inserimento del messaggio.

La tecnica più frequente è la LSB (Least Significant Bit) e consiste nel rimpiazzare l'ultimo bit di ogni pixel con una parte del messaggio.
Nella codifica di un'immagine, ogni pixel è composto da tre canali di colore: rosso (R), verde (G) e blu (B). Ogni canale è rappresentato da un valore numerico da 0 a 255, dove 0 è il valore più basso (nessun colore) e 255 è il valore più alto (massimo colore).

Con questa tecnica, i bit meno significativi di ciascun canale di colore vengono modificati per contenere i dati nascosti. Poiché i bit meno significativi contribuiscono meno al valore complessivo del colore, le modifiche sono spesso poco visibili all'occhio umano, consentendo di nascondere informazioni senza alterare in modo significativo l'aspetto dell'immagine.

Un esempio potrebbe essere:

1. Immagine originale:
    - Supponiamo di avere un pixel rappresentato dai seguenti valori di colore: R=215, G=132, B=98.
2. Testo da nascondere:
    - Nascondere il messaggio "HELLO" all'interno dell'immagine.
    - "HELLO" viene convertito in binario: "01001000 01000101 01001100 01001100 01001111".
3. Inserimento dei dati nascosti:
    - Iniziamo inserendo il primo bit "0" del messaggio all'interno del bit meno significativo del canale rosso (R) del pixel. Il nuovo valore di R diventa 214 (215 in binario è 11010111, e cambiando il bit meno significativo da 1 a 0, otteniamo 11010110, che è 214 in decimale).
    - Continuiamo a inserire i bit successivi del messaggio, uno alla volta, nel bit meno significativo di ciascun canale di colore (R, G, B) del pixel successivo nell'immagine.

L'immagine modificata sembrerà molto simile all'originale, ma con il messaggio "HELLO" nascosto nei bit meno significativi dei pixel.

L'inserimento di grandi quantità di dati o informazioni molto complesse può influenzare l'aspetto dell'immagine, rendendo più evidente la presenza dei dati nascosti. La steganografia LSB è una tecnica di base e relativamente semplice, ma ci sono altre varianti più avanzate che possono garantire maggiore sicurezza e minore rilevabilità dell'informazione nascosta.

2.1.1 Steghide

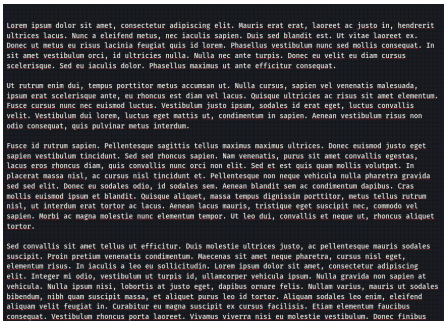
Steghide è un popolare strumento per la steganografia LSB che permette di nascondere dati all'interno di file immagine e audio. È disponibile per diverse piattaforme ed è abbastanza facile da utilizzare.

Verrà usato questo tool per fare una dimostrazione del suo funzionamento, per poter nascondere del testo all'interno di un'immagine:

1. Prima di tutto bisogna installare il tool, dal sito ufficiale "https://steghide.sourceforge.net/index.php"

2. Bisogna scegliere un'immagine su cui vogliamo nascondere il testo, in questo caso verrà usata l'immagine "jack.jpg" e il testo "secret.txt".

Figure 2: Immagine Originale



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris erat erat, laoreet ac justo in, hendrerit ultrices lacus. Nunc a eleifend metus, nec iaculis sapien. Duis sed blandit est. Ut vitae laoreet ex. Donec ut metus eu risus lacinia feugiat quis id lorem. Phasellus vestibulum nunc sed mollis consequat. In sit amet vestibulum orci, id ultricies nulla. Nulla nec ante turpis. Donec eu velit eu diam cursus scelerisque. Sed eu iaculis dolor. Phasellus maximus ut ante efficitur consequat.

Ut rutrum enim dui, tempus porttitor metus accumsan ut. Nulla cursus, sapien vel venenatis malesuada, ipsum erat scelerisque ante, eu rhoncus est diam vel lacus. Quisque ultricies ac risus sit amet elementum. Fusce cursus nunc nec euismod luctus. Vestibulum justo ipsum, sodales id erat eget, luctus convallis velit. Vestibulum dui lorem, luctus eget mattis ut, condimentum in sapien. Aenean vestibulum risus non odio consequat, quis pulvinar metus interdum.

Fusce id rutrum sapien. Pellentesque sagittis tellus maximus maximus ultrices. Donec euismod justo eget sapien vestibulum tincidunt. Sed sed rhoncus sapien. Nam venenatis, purus sit amet convallis egestas, lacus eros rhoncus diam, quis convallis nunc orci non elit. Sed et est quis quam mollis volutpat. In placerat massa nisl, ac cursus nisl tincidunt et. Pellentesque non neque vehicula nulla pharetra gravida sed sed elit. Donec eu sodales odio, id sodales sem. Aenean blandit sem ac condimentum dapibus. Cras mollis euismod ipsum et blandit. Quisque aliquet, massa tempus dignissim porttitor, metus tellus rutrum nisl, ut interdum erat tortor ac lacus. Aenean lacus mauris, tristique eget suscipit nec, commodo vel sapien. Morbi ac magna molestie nunc elementum tempor. Ut leo dui, convallis et neque ut, rhoncus aliquet tortor.

Sed convallis sit amet tellus ut efficitur. Duis molestie ultrices justo, ac pellentesque mauris sodales suscipit. Proin pretium venenatis condimentum. Maecenas sit amet neque pharetra, cursus nisl eget, elementum risus. In iaculis a leo eu sollicitudin. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer ni odio, vestibulum ut turpis id, ullamcorper vehicula ipsum. Nulla gravida non sapien at vehicula. Nulla ipsum nisi, lobortis at justo eget, dapibus ornare felis. Nullam varius, mauris ut sodales bibendum, nibh quam suscipit massa, et aliquet purus leo id tortor. Aliquam sodales leo enim, eleifend aliquam velit feugiat in. Curabitur eu magna suscipit ex cursus facilisis. Etiam elementum faucibus consequat. Vestibulum rhoncus porta laoreet. Vivamus viverra nisi eu molestie vestibulum. Donec finibus

Figure 3: Testo segreto

3. Questo comando permette di inserire il file di testo all'interno dell'immagine originale:

```
┌──(user㉿bad)-[~/Scrivania]
└─$ steghide embed -ef '/home/user/Scrivania/secret.txt' -cf '/home/user/Scrivania/jack.jpg' -p jack123
embedding "/home/user/Scrivania/secret.txt" in "/home/user/Scrivania/jack.jpg"... done
```

Figure 4: Embed

4. Questo comando permette di estrarre il file di testo contenuto all'interno dell'immagine modificata, il testo verrà salvato dentro il file "secretOutput.txt":

```
┌──(user㉿bad)-[~/Scrivania]
└─$ steghide extract -sf "/home/user/Scrivania/jack.jpg" -p jack123 -xf "/home/user/Scrivania/secretOutput.txt"
wrote extracted data to "/home/user/Scrivania/secretOutput.txt".
```

Figure 5: Extract

5. Confrontando l'immagine originale e l'immagine modificata, si può notare un aumento della dimensione dell'immagine a cui è stato inserito il segreto.

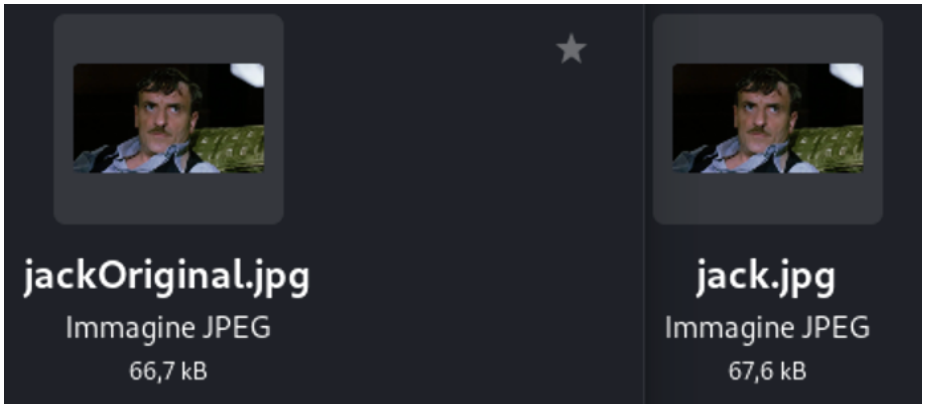


Figure 6: Dimensione dei file

2.2 Steganografia a livello di audio

La steganografia audio permette di nascondere un messaggio all'interno di un file audio senza comprometterlo. L'informazione può essere nascosta utilizzando la tecnica LSB o creando un file con frequenza > 20.000 Hz (in modo che non sia udibile all'orecchio umano), un esempio è lo spettro espanso.

1. Per prima cosa scegliamo l'immagine da inserire all'interno del file audio:

Figure 7: Segreto per il file audio

2. Convertendo l'immagine in formato "BitMap" e aprendola con Coagula (Un sintetizzatore di immagini. Ciò significa che è sia un semplice editor di immagini, sia un programma per produrre suoni da quelle immagini) possiamo fare il render dal segreto:

Figure 8: Coagula

3. Dopo aver esportato il file audio con Coagula, è necessario salvarlo in formato "WAV" e successivamente aprirlo su Audacity (Software per l'editing audio multitraccia e multipiattaforma, distribuito sotto la GNU General Public License. Il programma di base permette la registrazione di audio multitraccia, la loro modifica e il relativo mixaggio):

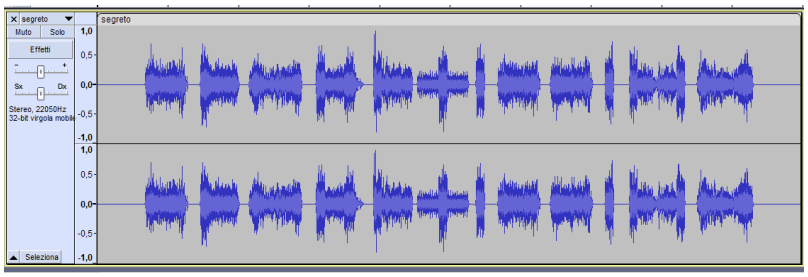


Figure 9: Audacity

4. Usando la visualizzazione dello spettrogramma è possibile vedere lo spettro del segreto:

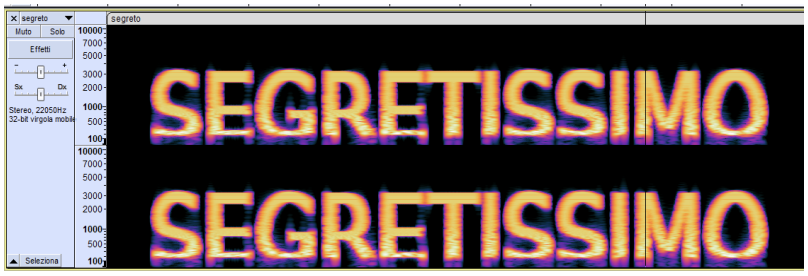


Figure 10: Spettrogramma segreto

5. Possiamo anche importare un altro file audio insieme al segreto, e dopodichè esportarlo, così da avere un nuovo file contenente sia il segreto e sia l'altro file:

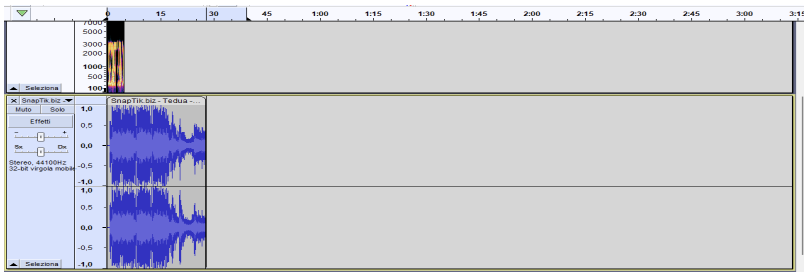


Figure 11: Spettrogramma segreto

6. Aprendo il nuovo file audio (segreto + canzone), e visualizzando lo spettrogramma, è possibile vedere lo spettro del segreto insieme allo spettro della canzone:

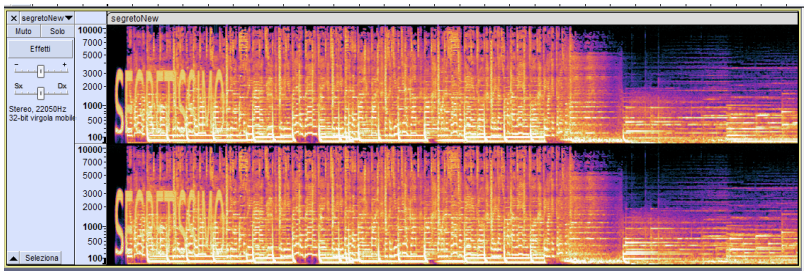


Figure 12: Spettrogramma segreto

2.3 Steganografia a livello di testo

Processo simile a quello delle immagini, consiste nel nascondere messaggi all'interno di un testo.
Esistono diversi metodi per fare Steganografia con il testo:

1. Capital letters
2. Letter marking
3. "Zero width spaces"

Usando "CrypTool 2" è possibile fare delle demo per questi metodi.
Per i primi due metodi, esiste anche la versione binaria.

2.3.1 Capital Letters

Viene usato un testo per nascondere un messaggio segreto, usando le lettere maiuscole.

- **Messaggio di partenza**:
  "today nothing special happened, the front line was quite, company bravo takes it easy, only a few shots were fired, many men are on their way home. we stay calm."
- **Segreto**:
  "attack tomorrow"
- **Messaggio modificato**: "tod**A**y no**T**hing special happened, **T**he front line w**A**s quite, **C**ompany bravo ta**K**es i**T** easy, **O**nly a few shots were fired, **M**any men are **O**n thei**R** way h**O**me. **W**e stay calm"

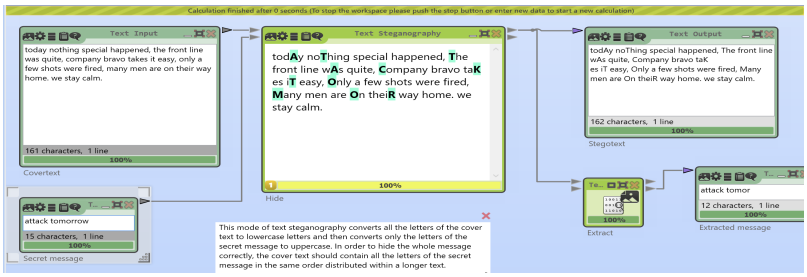


Figure 13: CrypTool Capital Letters

La versione in codice binario consiste nell'inserire nel messaggio modificato le lettere in maiuscolo o in minuscolo per formare il codice binario, per esempio:

- Lettere maiuscole = 1
- Lettere minuscole = 0

2.3.2 Marking Letters

Viene usato un testo per nascondere un messaggio segreto, "marcando" delle lettere.

- **Messaggio di partenza**:
  "today nothing special happened, the front line was quite, company bravo takes it easy, only a few shots were fired, many men are on their way home. we stay calm."
- **Segreto**:
  "attack tomorrow"
- **Messaggio modificato**: "tod$\dot{a}$y no$\dot{t}$hing special happened, $\dot{t}$he front line w$\dot{a}$s quite, $\dot{c}$ompany bravo $\dot{t}$akes it easy, $\dot{o}$nly a few shots were fired, $\dot{m}$any men are $\dot{o}$n thei$\dot{r}$ way h$\dot{o}$me. $\dot{w}$e stay calm"

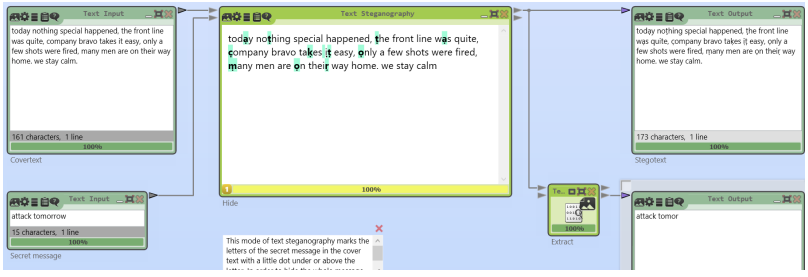


Figure 14: CrypTool Marking Letters

2.3.3 Zero Width Spaces

La "zero width spaces" è una tecnica di steganografia avanzata che sfrutta uno spazio invisibile per nascondere informazioni all'interno di un testo, un carattere speciale presente nella codifica Unicode che non ha una larghezza visibile quando visualizzato, ma viene comunque interpretato dai sistemi di elaborazione del testo.

L'idea principale di questa tecnica è quella di inserire la ZWSP all'interno del testo in posizioni specifiche per rappresentare il messaggio segreto. Questi spazi invisibili possono essere posizionati in modo strategico tra le lettere o parole del testo senza influenzarne l'aspetto visivo. Pertanto, solo chi conosce la posizione e l'interpretazione corretta della ZWSP può estrarre l'informazione nascosta.

- **Messaggio di partenza**:
  "The weather is lovely today"
- **Segreto**:
  "hello"
- **Messaggio modificato**: "The weather is lovely today"

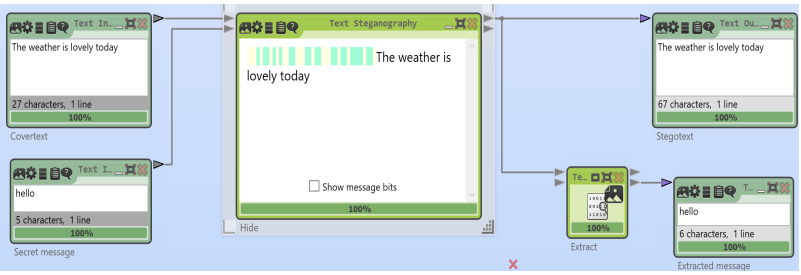


Figure 15: CrypTool ZWSP

3 Steganalisi: Identificazione delle informazioni nascoste

La steganalisi è l'arte di rilevare dati nascosti, estraendoli o distruggendoli, è il rilevamento della steganografia visualizzando le differenze tra i modelli di bit e le dimensioni insolitamente elevate dei file.

L'obiettivo principale della steganalisi è riconoscere i flussi di dati sospetti, determinare se hanno o meno messaggi nascosti codificati in essi e, se possibile, recuperare i segreti. Il processo di steganalisi è generalmente completato con l'analisi statistica utilizzando tecniche statistiche avanzate.

Al giorno d'oggi esistono diverse tecniche di steganalisi, per esempio:

1. Metodo del "Chi-Quadro":

   - Un test statistico per misurare se un insieme di dati osservati e un insieme di dati attesi, sono simili o no.
     La versione originale di questo attacco poteva rilevare messaggi incorporati in sequenza e successivamente è stata generalizzata a messaggi sparsi casualmente.

2. Distinguere i metodi statistici:

   - In questo approccio, lo steganalista prima ispeziona attentamente l'algoritmo di incorporamento e quindi identifica una quantità (le statistiche distintive) che cambia in modo prevedibile con la lunghezza del messaggio incorporato.
     La filosofia di rilevamento non è limitata a nessun tipo specifico di operazione di incorporamento e funziona anche per messaggi sparsi casualmente. Uno svantaggio di questo approccio è che il rilevamento deve essere personalizzato per ogni paradigma di incorporamento e la progettazione di statistiche di distinzione corrette non può essere facilmente automatizzata.

3. Metodi di classificazione cieca:

   - In primo luogo, un rilevatore cieco deve imparare come appare una tipica immagine non modificata da più prospettive. Quindi, un classificatore viene addestrato per apprendere le differenze tra un'immagine non modificata e una stegoimage (un'immagine che è stata modificata). Questa metodologia combinata con un potente classificatore dà risultati molto impressionanti.

3.1 Tecniche e metodi comuni

La steganalisi si basa sull'uso di tecniche e metodi per scoprire la steganografia. Questi metodi cercano indizi e pattern anomali all'interno dei file al fine di rilevare le informazioni segrete.

1. Analisi dei Bit:

   - Questa tecnica è utilizzata per individuare la steganografia nei file a livello di bit. Consiste nell'esaminare le modifiche sottili apportate ai bit meno significativi dei pixel di un'immagine o dei campioni di un file audio. La steganalisi cerca modelli che potrebbero rivelare la presenza di dati nascosti.

2. Analisi delle Distribuzioni:

    - Un altro approccio comune è l'analisi delle distribuzioni statistiche all'interno dei file di copertura. Nelle immagini, ad esempio, si studiano le distribuzioni dei livelli di grigio o dei colori per individuare deviazioni significative. Deviazioni non casuali potrebbero suggerire la presenza di dati steganografici.

3. Rilevazione di Pattern:

    - Questa tecninca si basa sulla ricerca di pattern o strutturazioni insolite all'interno dei file. Ad esempio, potrebbe essere utilizzata l'analisi delle autocorrelazioni per individuare l'eventuale disposizione dei dati nascosti all'interno di un file audio.

4. Estrazione dei Metadata:

    - L'analisi dei metadata incorporati nei file può rivelarsi utile nella steganalisi. Le informazioni sulle dimensioni, la data di creazione o il formato del file potrebbero rivelare discrepanze o incongruenze con la natura dichiarata del file.

5. Analisi della Compressione:

    - Le tecniche di compressione utilizzate per ridurre le dimensioni dei file possono influenzare il comportamento delle informazioni nascoste, concentrandosi sull'osservare gli effetti della compressione sui file di copertura per individuare possibili alterazioni.

6. Test di Turing:

    - Questo metodo coinvolge l'uso di test di Turing o test di stego-Turing per determinare se un file contiene informazioni nascoste. Il file viene esposto a interrogazioni e analizzato in base alle risposte per rilevare comportamenti atipici.

7. Analisi del Rumore:

    - Nelle immagini, il rumore visuale può essere alterato dalle informazioni nascoste. L'analisi del rumore può rivelare anomalie o differenze nelle frequenze spettrali, suggerendo la presenza di dati segreti.

Esistono anche metodi di steganalisi che usano tecniche di machine learning per rilevare le informazioni nascoste all'interno di file di copertura.

Questi approcci sfruttano algoritmi di machine learning per apprendere da un insieme di dataset contenente file sia con che senza informazioni steganografiche. Il modello acquisisce così la capacità di distinguere tra file normali e file con informazioni nascoste, consentendo di identificare file sospetti in fase di analisi.

1. Classificazione binaria:

    - In questo approccio, il modello di machine learning viene addestrato per classificare i file in due categorie: "contiene informazioni nascoste" e "non contiene informazioni nascoste". Il modello apprende da caratteristiche estratte dai file di addestramento e cerca di generalizzare queste conoscenze per classificare nuovi file.

2. Rilevamento delle anomalie:

    - Questo metodo si concentra sull'identificazione di file sospetti e anomali rispetto ai file normali. Il modello viene addestrato su un dataset di file normali e quindi cerca di individuare eventuali deviazioni significative all'interno di file sconosciuti, che potrebbero essere attribuite alla presenza di dati nascosti.

3. Feature engineering:

    - Un'importante fase è l'estrazione delle caratteristiche rilevanti dai file di copertura. Queste caratteristiche possono includere distribuzioni statistiche, modelli di bit, informazioni sulle dimensioni dei file e altro ancora.

4. Ensemble methods:

    - Gli ensemble methods combinano diversi modelli di machine learning per migliorare le prestazioni complessive della steganalisi. Ad esempio, l'ensemble può essere composto da diversi classificatori binari, o da classificatori e modelli di rilevamento delle anomalie.

L'uso del machine learning nella steganalisi può portare a risultati promettenti, ma è importante notare che gli autori di file steganografici possono cercare di eludere questi modelli adattando le loro tecniche. Pertanto, gli approcci basati su machine learning devono essere continuamente aggiornati e affinati per rimanere efficaci contro le tecniche di steganografia in continua evoluzione.

4 Applicazioni forensi della Steganografia

La steganografia, con la sua capacità di nascondere informazioni all'interno di file apparentemente innocui, ha suscitato un crescente interesse nel campo delle investigazioni forensi. L'uso di tecniche di occultamento digitale per trasmettere messaggi segreti o informazioni illecite ha portato alla necessità di sviluppare strumenti e metodologie per rilevare e analizzare tali contenuti nascosti.

4.1 Ruolo della steganografia nelle indagini criminali

La steganografia è diventata una componente significativa delle indagini criminali, poiché i criminali sfruttano sempre più tecniche sofisticate per nascondere

prove o comunicare tra loro in modo segreto. L'ambito delle applicazioni forensi della steganografia si estende a varie sfere, tra cui il terrorismo, la criminalità informatica, il traffico di droga, la pedofilia online e altre attività illegali.

L'adozione della steganografia da parte dei criminali è spesso guidata dalla consapevolezza che le tradizionali tecniche di analisi dei dati potrebbero non rilevare le informazioni nascoste. Pertanto, è fondamentale che gli investigatori acquisiscano una comprensione approfondita delle tecniche di steganografia e dei metodi per rilevare i contenuti occultati, al fine di preservare l'integrità delle prove digitali e assicurare giustizia nelle indagini penali.

4.2 Procedure forensi per analizzare file steganografici

Gli investigatori forensi devono essere dotati di strumenti e competenze specializzate per rilevare e analizzare file steganografici. A tal fine, esistono software e applicazioni appositamente progettati che aiutano a individuare e recuperare le informazioni nascoste all'interno dei file. Questi strumenti consentono di analizzare diverse tipologie di file, come immagini, audio, video e testo, alla ricerca di eventuali alterazioni non visibili superficialmente.

Alcuni dei software popolari utilizzati per analisi steganografiche:

1. **Xiao Steganography:**
   Permette di nascondere i file segreti dietro immagini e altre tipi multimediali. La parte migliore di questo strumento è che è facile da gestire e utilizzare. Tutto quello che devi fare è aprire il software e caricare l'immagine di un file nell'interfaccia. Questa applicazione supporta anche la crittografia, è possibile selezionare qualsiasi algoritmo come DES, 3DES, RC2, RC4 e hashing SHA e molti altri.

   Per leggere il messaggio nascosto, è importante avere lo stesso strumento. Questo strumento aiuterà anche a decodificare il file nascosto e permette di leggere il messaggio. È importante determinare che non è possibile estrarre il messaggio con l'aiuto di qualsiasi altro software. Il software è considerato il migliore per tutti coloro che desiderano ottenere uno strumento di stenografia semplice ed efficace. Oltre a questo, questo software è facile da usare e gratuito da scaricare.

2. **Steghide:**
   La parte migliore di questa applicazione è che il file immagine o il file audio non cambierà nemmeno dopo aver nascosto il messaggio segreto. È un software da riga di comando. Quindi, è importante imparare i comandi in modo da poter utilizzare lo strumento. Con l'aiuto dei comandi, puoi facilmente codificare i file audio o i file immagine forniti. Inoltre, con l'aiuto dei soli comandi, sarai in grado di estrarre il file dall'audio o dall'immagine.

3. **OpenStego:**
   La parte migliore di questo strumento è che è facile impostare qualsiasi tipo di file di messaggio segreto e nasconderlo accanto al formato PNG se il file è BMP o WBMP. Inoltre, se si è disposti a estrarre il messaggio, è necessario utilizzare lo stesso software, è possibile anche aggiungere una password per rendere più sicuro il tuo messaggio nascosto. Questo software open source è stato sviluppato su Java. Questo software è molto facile da usare per nascondere i messaggi segreti senza avere alcuna complessità.

5 Utilizzo come forma di attacco

La steganografia, originariamente concepita come una forma di comunicazione segreta, è stata purtroppo adottata anche come mezzo per condurre attacchi informatici e attività criminali. Questa forma sofisticata di occultamento digitale offre ai malintenzionati l'opportunità di nascondere informazioni sensibili all'interno di file apparentemente innocui, come immagini, audio, video o documenti di testo, al fine di eludere i sistemi di sicurezza e trasmettere dati illeciti senza destare sospetti.

Alcune delle principali modalità in cui la steganografia viene utilizzata come forma di attacco:

1. Diffusione di malware e virus:
   - Gli aggressori possono nascondere codice dannoso all'interno di immagini o file multimediali, per diffondere malware attraverso le normali attività di condivisione di file.
2. Comunicazioni clandestine:
   - Organizzazioni criminali o gruppi di hacker possono utilizzare la steganografia per trasmettere messaggi segreti e piani operativi tra i membri senza attirare l'attenzione delle autorità.
3. Furto di dati sensibili:
   - I dati rubati, come informazioni finanziarie o dati personali, possono essere nascosti all'interno di file steganografici e poi recuperati in modo illecito, facilitando il furto e il traffico di informazioni sensibili.

Per mitigare gli attacchi basati sulla steganografia, gli esperti di sicurezza informatica utilizzano tecniche di steganalisi e strumenti avanzati per rilevare la presenza di informazioni nascoste all'interno dei file.

In conclusione, la steganografia, sebbene possa essere utilizzata a fini legittimi, rappresenta anche una minaccia significativa per la sicurezza informatica quando impiegata per scopi criminali. La costante evoluzione delle tecnologie

di sicurezza e dell'analisi forense digitale è fondamentale per contrastare gli attacchi basati sulla steganografia e proteggere le organizzazioni e gli utenti dalle conseguenze dannose di tali azioni illecite.

6 Bibliografia

- "Cos'è la steganografia?"
  https://www.comptia.org/blog/what-is-steganography
- "Tecniche e classificazioni della steganografia"
  https://hacktips.it/tecniche-classificazione-della-steganografia/
- "Steganografia a livello di immagini"
  https://www.youtube.com/watch?v=sLkdtjJc6mc
- "Steganografia a livello di audio" https://www.youtube.com/watch?v=VzAoH99ZMRc
- "Steganalisi"
  https://tinyurl.com/kfe9bje3
- "Tool per la Steganografia"
  https://technicalustad.com/steganography-tools/