

**Progetto di Informatica Forense: Tool Steganografia**

Prof. Ugo Lopez

Anno Accademico 2022/2023

Antonio **Gravina 735584**

Francesco **Farina 744009**

Mattia **Siragusa 735880**

Sommario

[**Obiettivo** 3](#_Toc136532348)

[**Generali** 3](#_Toc136532349)

[**Vari Tool** 4](#_Toc136532350)

[**Steghide** 4](#_Toc136532351)

[**OpenStego** 4](#_Toc136532352)

[**Forensically** 4](#_Toc136532353)

[**Esempio di come funziona il Tool** 6](#_Toc136532354)

[**Foto Originale:** 6](#_Toc136532355)

[**Foto Modificata:** 7](#_Toc136532356)

[**Steganalysis Tools Suite (S-tools)** 7](#_Toc136532357)

[**StegDetect** 7](#_Toc136532358)

[**OutGuess** 7](#_Toc136532359)

[**StegExpose** 8](#_Toc136532360)

[**Steganabara** 8](#_Toc136532361)

[**Casi Reali** 8](#_Toc136532362)

[**Operazione Aurora** 8](#_Toc136532363)

[**Attacchi terroristici di Al Qaeda** 8](#_Toc136532364)

[**Caso WikiLeaks** 8](#_Toc136532365)

[**Riferimenti** 9](#_Toc136532366)

# **Obiettivo**

Creare un tool che consenta di effettuare la steganografia su un immagine e poter estrarre il messaggio nascosto nell’immagine.

# **Generali**

La steganografia è una tecnica utilizzata per nascondere messaggio all'interno di file di vario tipo, audio video o immagini che sia, evitando che un osservatore che non sia autorizzato possa leggerlo e addirittura rilevarlo. Per quanto sembri simile alla crittografia, la differenza sta nel fatto che questo rende indecifrabile il messaggio, mentre la steganografia punta soprattutto al nasconderlo.

L'obiettivo della steganografia quindi è quello di creare un canale di comunicazione sicuro e segreto, consentendo lo scambio informazioni senza attirare l'attenzione o sospetti indesiderati. Per funzionare sfrutta le caratteristiche digitali dei file in cui nasconderà il messaggio, modificando in maniera velata alcuni bit in modo da non alterare all’esterno l’immagine, il video o la traccia audio.

Prendendo l’esempio di un’immagine, si possono sfruttare alcune caratteristiche intrinseche del file digitale, come ad esempio i bit non significativi o i valori variabili dei pixel che stabiliscono i colori. Il messaggio viene suddiviso in piccole porzioni e viene poi sparso e nascosto in vari punti dell’immagine. Dall’esterno l’immagine risulta perfettamente identica, ma se si conosce l’algoritmo utilizzato per nascondere il messaggio si può tranquillamente estrarre.

E’ importante anche sottolineare che la steganografia, come detto anche in precedenza, presenta la sua forza nell’occultamento del messaggio, non nella sua criptazione. Questo fa in modo che un esperto di steganografia in caso sospetti la presenza di messaggi nascosti possa comunque estrarre il messaggio anche senza conoscere realmente l’algoritmo originale.

Ci sono vari scopi del tutto legittimi per cui si può utilizzare la steganografia, come ad esempio per questioni legate al diritto d’autore, però può anche essere utilizzata in maniera illegale, per diffondere contenuti proibiti o per comunicare informazioni legate da bande criminali o attacchi terroristici. Quindi in vari paesi l’uso della steganografia potrebbe essere limitato dalla legge date le sue possibilità potenzialmente pericolose.

# **Vari Tool**

Ci sono moltissimi tipi di tool inerenti alla Steganografia come:

## **-Steghide: strumento di steganografia open source che consente di nascondere dati in vari tipi di file, come immagini e file audio.**

## 

## -**OpenStego**: OpenStego è un software gratuito e open source che supporta la steganografia in file di immagini e file audio.

## 

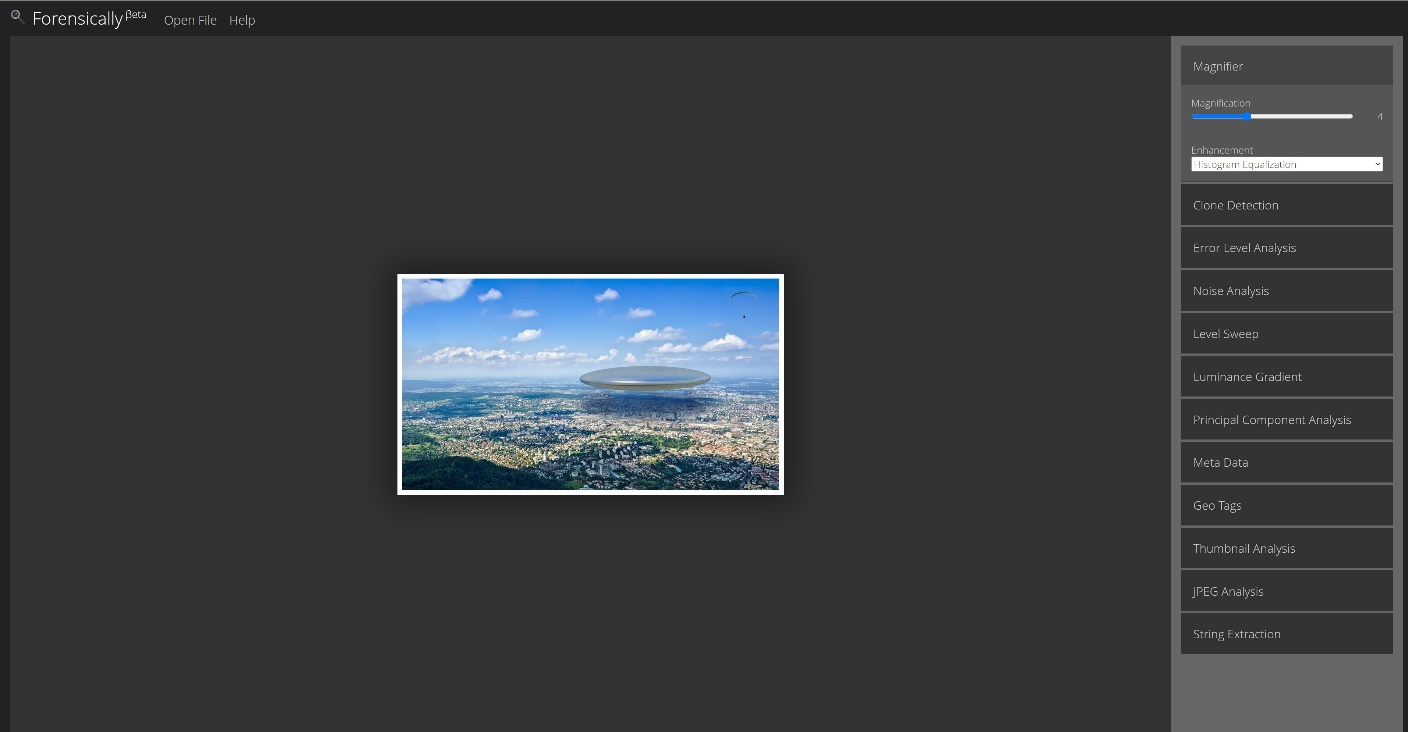
In quanto la Steganografia può essere utilizzata anche per casi malevoli sono stati creati dei tool per poter combattere queste forme di utilizzo chiamati tool AntiSteganografia. Un tool che abbiamo trovato in maniera molto accessibile e all’apparenza molto efficace è **Forensically**:

Uno strumento digitale utilizzato per l'analisi forense delle immagini. È progettato per aiutare gli investigatori digitali, gli esperti forensi e gli utenti comuni ad analizzare immagini col fine di individuare manipolazioni, verificare l'autenticità delle immagini e recuperare informazioni nascoste nei pixel.

Questo tool digitale presenta varie caratteristiche, tra cui:

* **Error Level Analysis (ELA):** tecnica che permette di rilevare le aree di un'immagine che potrebbero essere state alterate digitalmente.
* **Noise Analysis**: analizza i livelli di rumore presenti in un'immagine per rilevare modifiche o manipolazioni. Questo può rivelare aree in cui sono stati aggiunti o rimossi dettagli.
* **PRNU Analysis:** caratteristica unica di ogni sensore di immagine che può essere utilizzata per identificare la fotocamera o il dispositivo che ha catturato un'immagine.
* **Clone Detection:** consente di individuare copie di parti di un'immagine o di immagini simili, che potrebbero essere state modificate o manipolate.
* **Metadata Analysis:** analizza i metadati delle immagini, per ottenere informazioni sulle caratteristiche tecniche della fotocamera utilizzata, la data e l'ora di creazione dell'immagine e altre informazioni rilevanti per l'analisi forense.
* **Data Hiding Detection:** consente di individuare eventuali informazioni nascoste all'interno di un'immagine, come dati criptati o immagini nascoste

**Homepage Forensically:**



**Esempio di come funziona il Tool**

Attraverso il Noise Analysis di Forensically possiamo notare come in un’ immagine senza nessun messaggio criptato all’interno, il rumore sia minimo e non visibile.

Mentre in un’immagine che nasconde un messaggio criptato tramite Steganografia notiamo fin dai primi pixel un colore differente che dimostra la presenza maggiore di rumore e dunque il sospetto di un messaggio nascosto all’interno.

**Foto Originale:**  **Foto Modificata:**

Immagine che contiene testo, mammifero, arte, gatto

Descrizione generata automaticamente**Immagine che contiene mammifero, dipinto, arte, disegno

Descrizione generata automaticamente**

Altri esempi di tool AntiSteganografia sono:

* **Steganalysis Tools Suite (S-tools):** S-Tools, oltre ad essere uno strumento di steganografia, include anche funzionalità di steganalysis per rilevare e analizzare la presenza di dati nascosti all'interno di file di immagini, audio e video.
* **StegDetect**: StegDetect è uno strumento di steganalysis che può rilevare la presenza di informazioni nascoste all'interno di file di immagini. Utilizza algoritmi per identificare modelli o anomalie tipiche delle immagini steganografiche.
* **OutGuess:** Mentre OutGuess è principalmente un tool di steganografia, può anche essere utilizzato per rilevare la presenza di steganografia in un'immagine. Esistono alcune versioni modificate di OutGuess che consentono di decodificare e rivelare dati nascosti.
* **StegExpose**: StegExpose è uno strumento di steganalysis specificamente progettato per rilevare l'uso di steganografia in file di immagini. Analizza diversi indicatori e segnali di anomalie per identificare la presenza di dati nascosti.
* **Steganabara:** Steganabara è uno strumento open source di steganalysis che può rilevare informazioni nascoste all'interno di file di immagini. Utilizza algoritmi per analizzare e individuare segni di manipolazione e steganografia.

**Casi Reali**

**Operazione Aurora:** Nel 2010, un attacco informatico noto come "Operazione Aurora" ha colpito diverse grandi aziende, tra cui Google, Adobe e Juniper Networks. Gli attaccanti hanno utilizzato la steganografia per nascondere il malware all'interno di file PDF inviati come allegati e-mail.

**Attacchi terroristici di Al Qaeda:** Nel 2010, è emerso che i membri di Al Qaeda stavano utilizzando la steganografia per comunicare e coordinare gli attacchi. Gli attacchi terroristici di Al Qaeda a Londra nel 2005 e a Mumbai nel 2008 hanno coinvolto l'uso di messaggi nascosti all'interno di immagini digitali per evitare la rilevazione delle comunicazioni.

**Caso WikiLeaks:** Nel 2010, il soldato americano Chelsea Manning ha fornito a WikiLeaks una vasta quantità di documenti classificati. Si pensa che Manning aveva utilizzato la steganografia per nascondere alcuni dei documenti all'interno di file musicali. Ad esempio, si pensa che abbia nascosto documenti all'interno di file MP3 rinominandoli con estensione .jpg per eludere la sicurezza.

**CONCLUSIONI**

La steganografia è una metodologia che garantisce la privacy per gli enti che la adoperano per le comunicazioni, specialmente se utilizzata in combinazione con tecniche di crittografia.

L’efficacia di questo metodo è misurata in base a quanto riconoscibile è la manipolazione dell’immagine ed esistono numerose tecniche differenti.

Il tool realizzato dal nostro team non è il più efficace in tal senso, perché esistono dei software avanzati in grado di rilevare il rumore dell’immagine, ossia l’alterazione casuale dei pixel dell’immagine. Un rumore elevato coincide spesso con una manipolazione dell’immagine. Ciò riguarda anche l’utilizzo di steganografia mediante la manipolazione di file audio o video.

Questi software, che spesso si avvalgono di modelli di apprendimento automatico e che richiedono grande capacità computazionale, sono utilizzati nell’ambito dell’informatica forense per individuare informazioni che potrebbero essere state nascoste da un criminale, e che sarebbero fondamentali per risolvere un caso giudiziario.

La realizzazione del tool steganografico ci ha permesso di approfondire in dettaglio le varie metodologie utilizzate e, in particolare, l’utilizzo della tecnica dei bit meno significativi.

Conseguentemente, sono state approfondite le conoscenze riguardo la struttura di un’immagine virtuale, e quindi la manipolazione dei pixel, ma anche discipline trasversali come la crittografia, la realizzazione di un’interfaccia grafica per l’utente e la scrittura/lettura di file testuali.

**Riferimenti**

**<https://29a.ch/photo-forensics/#forensic-magnifier>**

[**https://steghide.sourceforge.net/**](https://steghide.sourceforge.net/)

[**https://www.openstego.com/**](https://www.openstego.com/)

[**https://www.rbcafe.it/software/outguess/**](https://www.rbcafe.it/software/outguess/)

[**https://github.com/b3dk7/StegExpose**](https://github.com/b3dk7/StegExpose)

[**https://github.com/quangntenemy/Steganabara**](https://github.com/quangntenemy/Steganabara)

[**https://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620**](https://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620)

[**https://en.wikipedia.org/wiki/GhostNet**](https://en.wikipedia.org/wiki/GhostNet)