
**Corso di Elementi di Crittografia**
**A.A. 2010/11**

**Docente**

**Prof. Francesca Merola**

# STEGANOGRAFIA

**Studenti**

Roberto Sepe

Marek Krzysztof Wierzba

Fabio Garzaro

# STEGANOGRAFIA

1. Introduzione
2. Steganografia vs Crittografia
3. Tipi di Steganografia
4. Data Hiding
5. Document Marking
6. Audio/Video
7. Steganografia Fatta in Casa

# Introduzione

- Il termine steganografia è composto dalle parole greche ***stego*** (rendo occulto, nascondo) e ***grajh*** (scrittura)

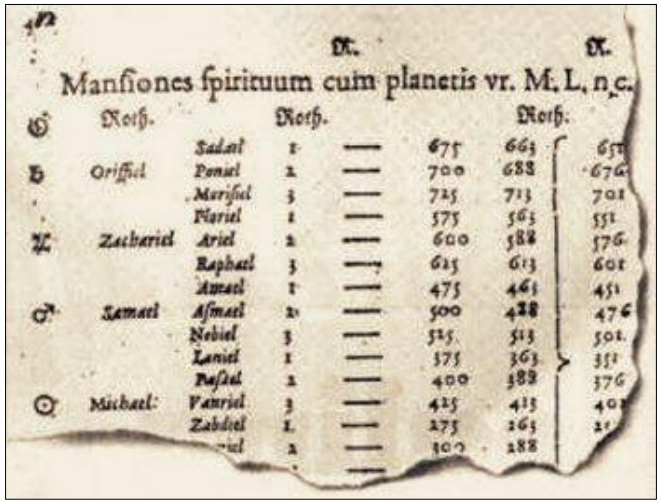
- È l'arte di nascondere un messaggio segreto dentro un messaggio palese in modo tale che passi del tutto inosservato a un possibile nemico

- Fu teorizzata dall'abate Tritemio attorno al 1500 nei tre volumi chiamati *Steganographia*

# Introduzione

- I primi due volumi contengono dozzine di esempi di codici crittografici abbastanza semplici, dei quali comunque l'autore fornisce una spiegazione

- Il terzo è costituito da lunghe tavole di numeri precedute da simboli zodiacali e planetari che fanno pensare a dati astrologici




- Per secoli gli studiosi hanno discusso sulla possibilità che in questo volume non vi fosse alcun codice cifrato, ma solo operazioni alchemiche di interesse per gli occultisti

# Introduzione

- Il dilemma è stato risolto nel marzo del 1998 da Jim Reeds della AT&T Labs
- In realtà, Thomas Ernst, un professore tedesco, aveva risolto parte del problema alcuni anni prima, quando era studente, pubblicando i risultati su un giornale tedesco, passato inosservato

- Si tratta di un testo abbastanza confuso, come se alcune parti si fossero perdute; quello che rimane è formato da frasi comuni in latino e tedesco della quali, per esempio, una suona più o meno così:

*"il latore di questa lettera è un brutto furfante ed un ladro"*

# Introduzione

- È interessante che il testo in questione è nascosto in un documento che trasporta un contenuto di informazione del tutto diverso
- Contenuto che è stato preso sul serio da molti

  (es. siti Internet e forum dedicati al soprannaturale)

- Quindi la steganografia può trovare uso in ogni forma di comunicazione
- È sufficiente che mittente e destinatario abbiano concordato un codice non vincolato ai soli simboli alfabetici

# Introduzione

- Es. Alice e Bob si accordano sull'uso di un sistema steganografico: *"il numero di virgole presente in una singola pagina sarà tra 1 e 21, questo numero corrisponderà ad una lettera dell'alfabeto"*

- Se Alice e Bob fossero controllati da Eve, potrebbero scrivere pagine di *copertura* scambiandosi informazioni prive di valore per loro, ma con un uso accurato delle virgole, riuscirebbero a nascondere il vero messaggio

# Steganografia vs Crittografia

- Nella crittografia si tiene nascosta la chiave con cui poter decodificare il testo segreto codificato

- Nella steganografia si tiene nascosto non tanto il contenuto, ma la stessa esistenza della comunicazione!

- In modo che un eventuale nemico nemmeno si accorga del passaggio di informazioni segrete!

- Vediamo ora alcuni esempi per chiarire meglio

# Steganografia vs Crittografia

## Esempi

1. Si racconta che un nobile persiano fece tagliare a zero i capelli di uno schiavo fidato scrivendo sulla testa il messaggio e, una volta ricresciuti i capelli, inviò lo schiavo a destinazione
2. Durante la seconda guerra mondiale fu inventata la tecnica dei micro punti fotografici: fotografie molto piccole che una volta sviluppate e ingrandite, diventano immagini di buona qualità, ma di contenuto diverso

# Steganografia vs Crittografia

## Esempi

3. Un acrostico è una poesia, o un testo di qualsiasi tipo, composta in modo che le prime lettere di ogni capoverso formino un messaggio di senso compiuto

*Apparently neutral's protest's is*
*Thoroughly discounted and ignored.*
*Isman hard hit. Blockade issue affects pretext*
*for embargo on by products, ejecting*
*suets and vegetable oils.*

*Pershing sails from NY June 1*

# Steganografia vs Crittografia

- Vantaggi :
  - Poter trasmettere messaggi segreti senza che si noti la loro trasmissione


- Svantaggi :
  - Riguardano gli innumerevoli dati necessari per nascondere anche solo una piccola quantità di informazioni
  - Quando un sistema steganografico viene scoperto, rivela completamente il messaggio segreto

- Quest'ultimo svantaggio può essere evitato combinando crittografia e steganografia, cifrando le informazioni prima di nasconderle

# Steganografia vs Crittografia

- In sostanza, nel caso della crittografia il nemico può rilevare, intercettare e modificare i messaggi senza però riuscire a capire i messaggi

- L'obiettivo della steganografia è invece quello di nascondere un messaggio dentro un altro messaggio, dall'aspetto innocuo, in modo che il nemico non possa neppure rilevare l'esistenza del primo messaggio

- Questo secondo messaggio è chiamato messaggio contenitore o più semplicemente contenitore

# Tipi di Steganografia

- Si hanno due possibili scopi per l'uso della steganografia:

1) La protezione contro l'individuazione di dati segreti (***data hiding***)
2) La protezione contro la rimozione di informazioni (***document marking***)
    a. ***Watermarking***
    b. ***Fingerprinting***

- Per quanto riguarda il primo scopo (***data hiding***) si hanno due tipi di classificazione

# Tipi di Steganografia

## 1. Data Hiding

- Prima classificazione:
  - ***Steganografia iniettiva***

    Consente di "iniettare" il messaggio segreto dentro un messaggio contenitore già esistente, modificandolo in modo tale da contenere il messaggio e risultare, ai sensi umani, praticamente indistinguibile dall'originale

  - ***Steganografia generativa***

    Ha capacità proprie di creare messaggi contenitori ed utilizza il messaggio segreto per la “generazione” di questi

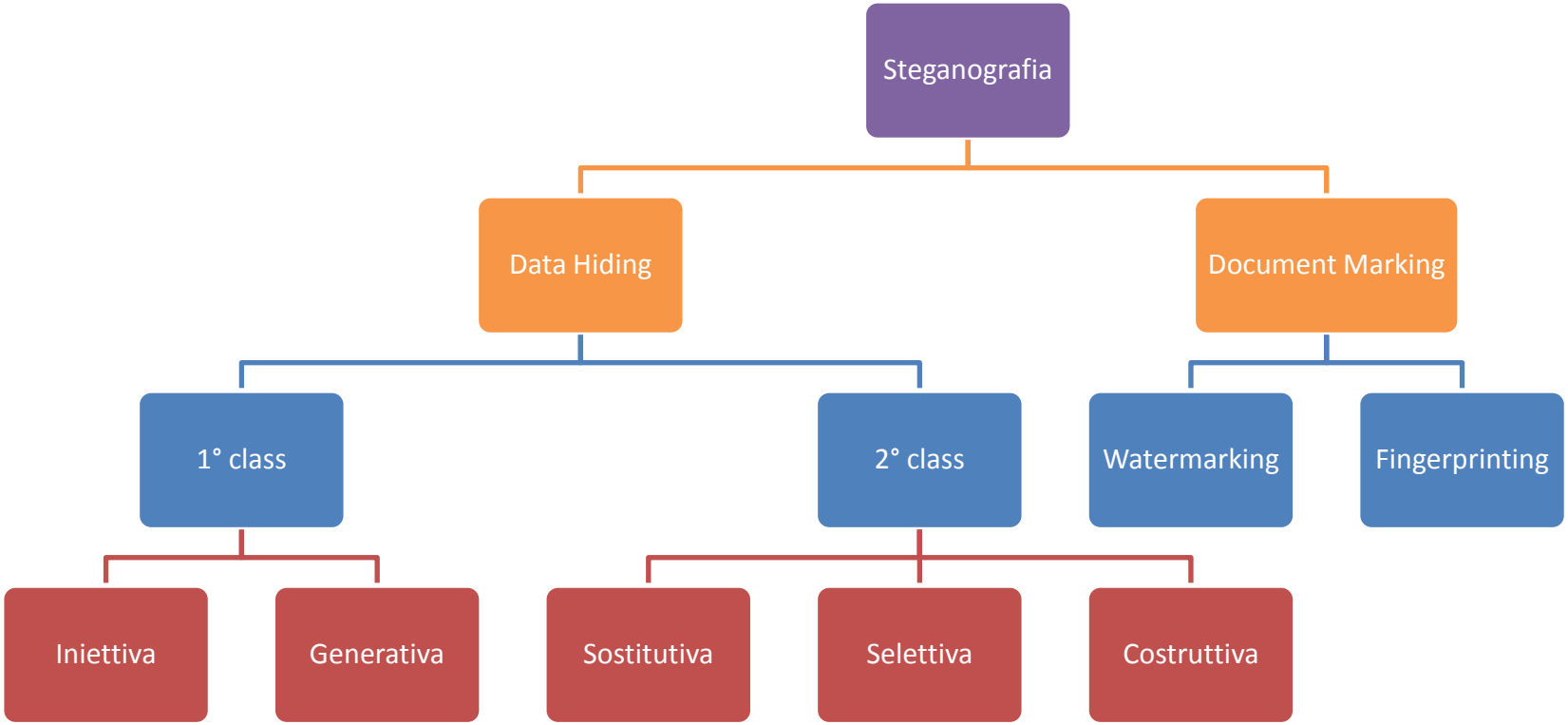
# Tipi di Steganografia

## 1. Data Hiding

- Il secondo sistema di classificazione può essere suddiviso in tre classi:
    a. ***Steganografia sostitutiva***
    b. ***Steganografia selettiva***
    c. ***Steganografia costruttiva***

- Parleremo di queste ultime tre

# Tipi di Steganografia



# Data Hiding

# 1.Data Hiding

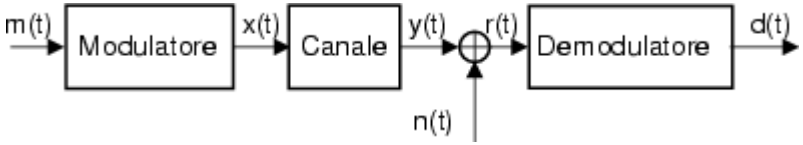
## a. Steganografia sostitutiva

- Di gran lunga la più diffusa, tanto che in genere con il termine steganografia ci si riferisce implicitamente ad essa

- **Idea**: la maggior parte dei canali di comunicazione (linee telefoniche, trasmissioni radio, ecc.) trasmettono segnali che sono sempre accompagnati da qualche tipo di rumore

- Tale rumore può essere sostituito da un segnale (il messaggio segreto)

- Segnale che è indistinguibile dal rumore vero e proprio, quindi può essere trasmesso senza destare sospetti



# 1.Data Hiding

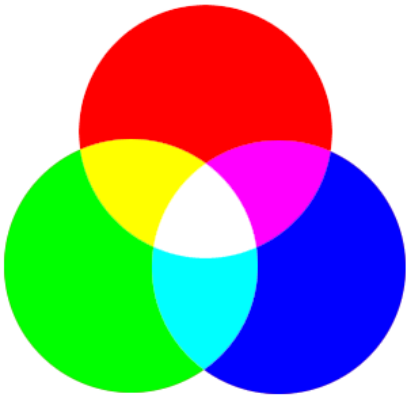
## a. Steganografia sostitutiva

- **In pratica**: la steganografia si basa sull'assunzione che è piuttosto facile confondere i sensi dell'uomo
- Dato un documento originale *d*, esiste una soglia *s* al di sotto della quale qualunque cambiamento apportato ai dati non sarà percepito da una persona
- *s* dipenderà dall'osservatore, ma esiste un livello minimo che va oltre le capacità dei sensi dell'uomo
- Possiamo dunque sempre sostituire *d* con *c*, senza che la modifica sia individuata, finché sarà soddisfatta la seguente disuguaglianza (*i* = informazioni nascoste)

$$c = d + i < s$$

# 1.Data Hiding

## a. Steganografia sostitutiva



- Facendo un esempio, i PC utilizzano il sistema **RGB** per visualizzare i colori

- Ciascun colore (**R**=Red, **G**=Green, **B**=Blue) varia da 0 a 255, che casualmente è anche il range dello standard di caratteri ISO 8859-1, uno dei più utilizzati nel mondo occidentale

- Per ogni pixel ci portiamo dietro 3 valori (quindi, potenzialmente, 3 caratteri)
- Certe immagini sono composte da milioni di pixel

- È quindi facile comprendere come l'alterazione di alcuni pixel non è visibile a occhio nudo

# 1.Data Hiding

## a. Steganografia sostitutiva

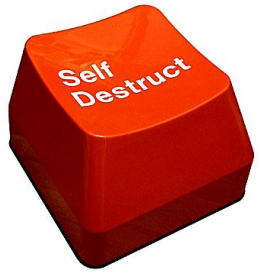
- La tecnica appena descritta rappresenta il cuore della steganografia sostitutiva, anche se di fatto ne esistono numerose variazioni

- È ovvio che tutto quello che abbiamo detto vale non solo per le immagini, ma anche per altri tipi di sorgenti dati, per esempio audio e video

# 1.Data Hiding

## a. Steganografia sostitutiva - Sicurezza

- Discutiamo adesso i problemi relativi alla sicurezza
- Innanzitutto le norme che valgono generalmente per i programmi di crittografia dovrebbero essere osservate anche per l'utilizzo dei programmi steganografici




- Per ciò che riguarda la steganografia:
  1) In primo luogo si deve evitare di usare come contenitori file prelevati da siti pubblici o comunque noti (per esempio, immagini incluse in pacchetti software, ecc.)
  2) In secondo luogo si deve evitare di usare più di una volta lo stesso file contenitore

# 1.Data Hiding

## a. Steganografia sostitutiva - Sicurezza

- Quello che viene ritenuto il principale difetto di queste tecniche è che in genere la sostituzione operata può alterare le caratteristiche statistiche del rumore presente nel media utilizzato

- Lo scenario è il seguente:
  - Si suppone che il nemico dispone di un modello del rumore e che utilizzi tale modello per controllare i file che riesce a intercettare
  - Se il rumore presente in un file non è conforme al modello, allora il file è da considerarsi sospetto

# 1.Data Hiding

## a. Steganografia sostitutiva - Sicurezza

- Si può osservare che questo tipo di attacco non è per niente facile da realizzare, data l'impossibilità pratica di costruire un modello che tenga conto di tutte le possibili sorgenti di errori/rumori

- Esistono degli studi che in casi molto specifici hanno avuto qualche successo

- La steganografia selettiva e quella costruttiva hanno proprio lo scopo di eliminare questo difetto della steganografia sostitutiva

# 1.Data Hiding

## b. Steganografia selettiva

- Entrambe hanno valore puramente teorico, per quanto se ne sappia, non vengono realmente utilizzate nella pratica
- L'idea è quella di procedere per tentativi, ripetendo una stessa misura fintanto che il risultato non soddisfa una certa condizione
- Con un esempio molto semplificativo e poco realistico:
  1. Abbiamo una funzione che vale 1 se il numero di bit uguali a 1 del file è pari, altrimenti vale 0
  2. Se vogliamo codificare il bit 0 procediamo a generare un'immagine
  3. Se il numero di bit uguali a 1 è dispari ripetiamo di nuovo la generazione, finché non si verifica la condizione opposta

# 1.Data Hiding

## b. Steganografia selettiva

- L'immagine ottenuta con questo metodo contiene l'informazione segreta, ma si tratta di un'immagine "naturale", cioè generata senza essere rimanipolata successivamente
- L'immagine è semplicemente sopravvissuta ad un **processo di selezione** (da cui il nome della tecnica), quindi non si può avere un modello di riferimento del rumore
- Questa tecnica risulta troppo dispendiosa rispetto alla scarsa quantità di informazione che è possibile nascondere

# 1.Data Hiding

## c. Steganografia costruttiva

- La steganografia costruttiva tenta di sostituire il rumore presente nel mezzo utilizzato con l'informazione segreta, in modo da imitare le caratteristiche statistiche del rumore originale
- Secondo questa concezione, un buon sistema dovrebbe basarsi su un modello del rumore ed adattare i parametri dei suoi algoritmi di codifica in modo tale che il falso rumore contenente il messaggio segreto sia il più possibile conforme al modello

- Questo approccio è senza dubbio valido, ma presenta anche alcuni svantaggi

# 1.Data Hiding

## c. Steganografia costruttiva

- Innanzitutto non è facile costruire un modello del rumore
- La costruzione richiede grossi sforzi ed è probabile che qualcuno, in grado di disporre di maggior tempo e di risorse migliori, riesca a costruire un modello più accurato per distinguere tra il rumore originale e un sostituto

- Inoltre, se il modello del rumore utilizzato dal metodo steganografico dovesse cadere nelle mani del nemico, egli lo potrebbe analizzare per cercarne possibili difetti
- Il modello fornirebbe involontariamente un metodo di attacco particolarmente efficace proprio contro lo stesso sistema

# Document Marking

Marek
Krzysztof Wierzba

# 2.Document Marking

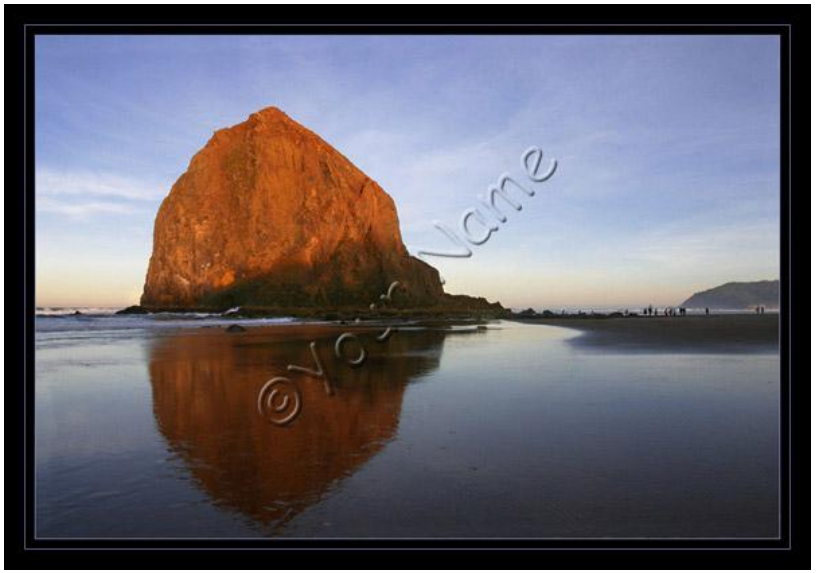
- Con il diffondersi dell'utilizzo di Internet, gli autori di documenti digitali (es. le immagini) hanno il problema di impedire che qualcuno si impossessi delle loro opere spacciandole per proprie
- Molti autori però vogliono poter distribuire i propri lavori in modo sicuro, sapendo cioè che nessuno potrà mai contestare la paternità dell'opera
- La soluzione è aggiungere delle informazioni dentro il documento in questione in modo tale che, nel caso ne venisse fatta una copia, il legittimo proprietario possa essere univocamente determinato
- Vi sono due tecniche diverse per farlo: Watermarking e Fingerprinting

# 2.Document Marking

## a. Watermarking

- Con il termine watermark (o digital watermarking) si indica una sorta di filigrana digitale destinata a marcare, come una vera e propria firma, determinati tipi di file immagine, prevalentemente allo scopo di contrassegnarne l'origine

- Il watermark può essere applicato in modo immediatamente visibile oppure può essere occultato con la steganografia



# 2.Document Marking

## a. Watermarking

- Nel primo caso viene utilizzato per codificare informazioni che devono essere rese pubbliche all'utente finale
- Un esempio è l'immagine che compare su una banconota quando la osserviamo in controluce

# 2.Document Marking

## a. Watermarking

- Il Watermark invisibile è invece proprio di quei contesti in cui il proprietario legittimo vuole garantirsi i diritti d'autore, nascondendo quindi il marchio nel documento

- In pratica la copia marcata è quasi identica all'originale, a meno di alcune differenze non riscontrabili dalle percezioni umane

- Un esempio è l'utilizzo della steganografia sostitutiva con il sistema **RGB** di cui abbiamo già parlato

# 2.Document Marking

## a. Watermarking

- Questa tecnica può essere usata anche per inserire un marker digitale all'interno di file audio o video e persino all'interno di stream digitali come quelli usati dalla televisione digitale (terrestre e satellitare)

- Viene usata anche per rendere rintracciabile la stampante che ha generato un determinato documento, come ad esempio una lettera di minaccia anonima

- In ogni caso, il marker deve essere molto difficile da rimuovere per avere qualche efficacia

# 2.Document Marking

## b. Fingerprinting

- I Fingerprint invece sono dei marchi (più watermark) che vengono inseriti in diverse copie della stessa immagine per distribuirla a persone diverse

- L'effetto è una specie di numero seriale

- Fa sì che il proprietario possa identificare le persone a cui ha distribuito il suo prodotto nel caso esse lo distribuiscano "gratuitamente" a terzi

# 2.Document Marking

## Proprietà

1. Non deve basarsi sulla segretezza dell'algoritmo

   Anche se la robustezza di molti prodotti commerciali disponibili sul mercato si basano su quest'assunzione

2. Impercettibilità

   La differenza tra il documento marcato e quello originale deve essere impercettibile (nel caso dell'immagine, invisibile all'occhio umano)

3. Individuabilità

   Deve essere efficientemente individuabile dal proprietario del file originale, anche se impercettibile all'osservatore medio, utile per un pronto reclamo di proprietà ed eventuale attacco legale nei confronti dei falsari

# 2.Document Marking

## Proprietà

4. Robustezza

   Per essere utilizzato il watermark deve poter essere estratto anche dopo distorsioni (compressioni, filtraggio, ridimensionamento ecc..)

5. Scalabilità

   Il costo computazionale di un codificatore e di un decodificatore è un fattore importante

   È necessario quindi costruire schemi di watermarking in cui il decodificatore sia scalabile all'aumentare/diminuire delle prestazioni del calcolatore

# 2.Document Marking

## Proprietà

### 6. Watermark modificabili e multipli

Alcune volte è richiesta la possibilità di modificare un watermark precedentemente inserito

Vi sono due modi per farlo:

1. Rimovendo il vecchio watermark e inserendo il nuovo
2. Inserendo un secondo watermark in modo tale che entrambi siano leggibili (individuabili)

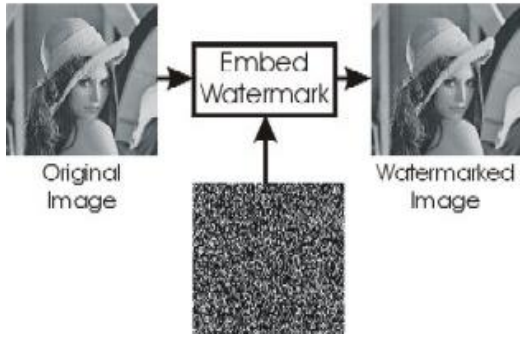
La prima alternativa rende il watermark non resistente agli attacchi (deve essere facilmente rimuovibile)

La seconda alternativa è migliore, poichè permettendo più watermark è possibile tenere traccia della storia del file

# 2.Document Marking

## Codifica

- L'inserimento del "marchio" è una funzione di tre fattori:
  - identificativo utente (watermark/marchio)
  - chiave dell'utente
  - file originale




- La funzione di codifica E prende il file I, un marchio W e la chiave segreta K del proprietario e genera un nuovo file $I_w$ (chiamato file marcato)

$$E(I, W, K) = I_w$$

- I passi della funzione dipendono dalla tecnica utilizzata
- Ci sono varie applicazioni e differenti schemi dipendenti dal grado di sicurezza che si vuole ottenere

# 2.Document Marking

## Decodifica

- Ci sono diversi tipi di decodifica che variano in base al tipo di sicurezza che si vuole ottenere:

- Rilevamento
  - Sistema di Marking Privato
  - Sistema di Marking Semi-Privato

- Estrazione
  - Sistema di Marking Pubblico
  - Sistema di Marking Simmetrico/Asimmetrico

# 2.Document Marking

## Rilevamento

- Permette di controllare solo se nel file è presente un watermark, simile a quello originariamente inserito, rispondendo alla domanda:

"Il documento contiene il marker W ?"

- Sistema di Marking Privato

  D(I, Iw , K, W) = SI/NO

- Sistema di Marking Semi-Privato

  D(Iw , K, W) = SI/NO

- Vengono impiegate per dimostrare la proprietà legale del documento

# 2.Document Marking

## Estrazione

- Il watermark deve essere estraibile ed individuabile per essere usato
- In alcuni schemi, il marchio può essere recuperato nella sua forma originale in tal caso si parla di estrazione
- Esiste una funzione di decodifica D che prende il file Iw e la chiave segreta K e ritorna il marchio W

$$D(Iw , K) = W$$

- L'integrità di W permette di stabilire se I è stata modificata
- Il Simmetrico/Asimmetrico è usato per abilitare chiunque a leggere il watermark ma impedendone la rimozione

# 2.Document Marking

## Attacchi

Attacco base

- Utilizzano le debolezze del design e delle tecniche di marcatura
- Ad esempio le tecniche di marking di un file audio basate sullo spettro, sono vulnerabili ai ritardi temporali

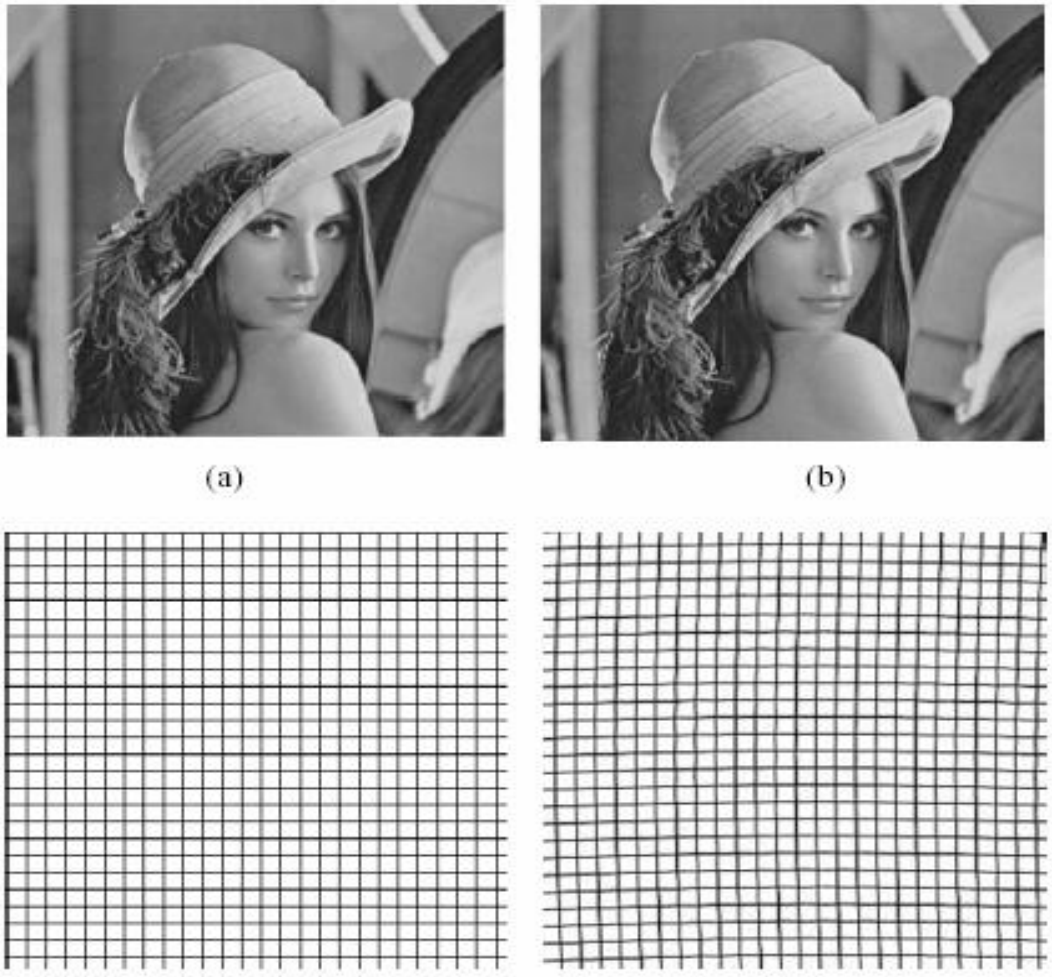
# 2.Document Marking

## Attacchi

- Attacco a Robustezza:

l'obiettivo è rimuovere o rendere illeggibile la presenza di watermark

- Si basano sull'applicazione di una serie di distorsioni minori che abbassano la qualità del documento in maniera quasi impercettibile ai sensi

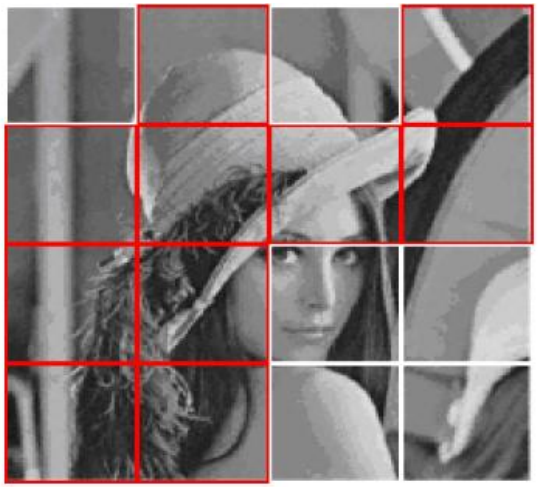


# 2.Document Marking

## Attacchi

- Attacco a Presentazione: modifica il contenuto del documento, sfruttando le dimensioni troppo grandi del watermark

- Attacco a Mosaico: suddivide un'immagine in parti troppo piccole da poter rilevare la presenza del watermark e poi ricompone l'immagine attraverso il browser



# 2.Document Marking

## Attacchi

- Se dovessero risultare presenti più di un marchio sulla stessa immagine, avrà la precedenza il più vecchio, essendo stato inserito prima di tutti gli altri

- Attacchi basati sull'interpretazione puntano ad aggiungere ulteriori marchi all'immagine cercando di rendere impossibile determinare quello più vecchio

# 2.Document Marking

## Conclusioni

**Il Watermark**

**non deve**:

- degradare troppo la qualità del documento
- compromettere la loro leggibilità nel caso di watermark multipli

**deve**:

- essere difficile da scoprire senza una conoscenza segreta, tipicamente una chiave
- sopravvivere alle manipolazioni che non degradano l'integrità del documento in maniera visibilmente percettibile

# Audio – Video

Fabio Garzaro

# Campi di Applicazione

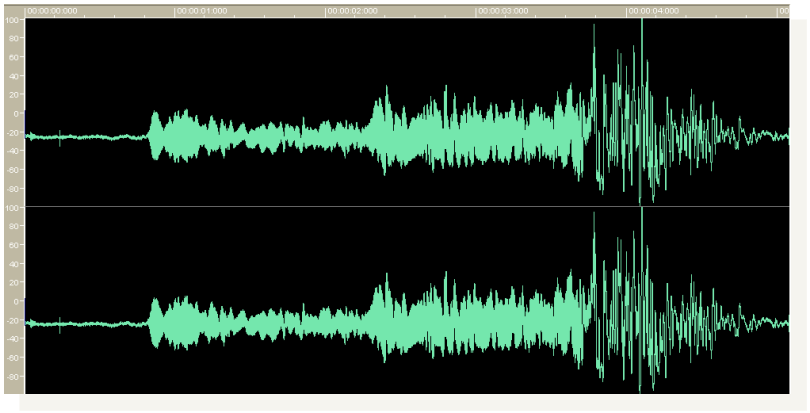
Famosa per le sue applicazioni con le immagini

Es. Alterando leggermente luminosità e colore in modo che l'operazione steganografica passi inosservata

Nulla vieta però di applicare questa tecnica al campo Audio e Video in ogni sua forma

# Steganografia Audio

## Wav



I file sonori **Wav** sono sequenze di stringhe di 8 o 16 bit (sono trai più diffusi)

**Esempio:**

Un file **Wav mono** a 44.100 Hz con 16 bit ha:

- Una Frequenza di 44.100 stringhe di 16 bit/sec
- Una stringa di 16 bit ogni 1/44.100 di secondo *(Periodo)*

***Ci si potrebbe nascondere qualche cosa dentro?***

***Eh se fosse stereo?***

# Steganografia Audio

## Wav

Bello, ma questo mezzo quanto consuma a byte?

Sapendo che un **file wav** **stereo** di **un minuto** ha una **dimensione** di:

16 bit x 44.100 Hz x **60** sec = 42.336.000 bit ≈ 5.168 Kb **x 2** = **10.336 Kb**

Sostituendo i **2** bit meno significativi per ogni stringa di **16** bit:

Si ha una disponibilità di (**84.762.000** bit / **16** bit) x **2** = 10.595.250 bit
Quindi circa **1.293** Kb

**Nota: la Divina Commedia in formato Ascii sta in 291 Kb**

# Steganografia Audio

## Mp3

Un file Mp3 è un file audio compresso (in grafica RAW -> Jpeg).

Due idee alla base di questo formato:

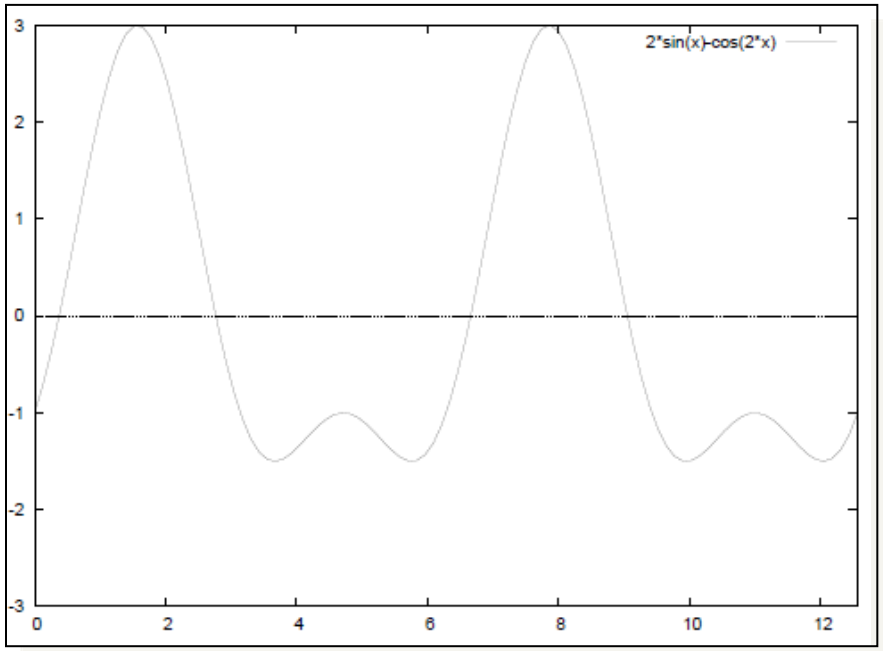
1) Psicometria (quello che non percepisco lo elimino)

2) **T**rasformata **V**eloce di **F**ourier (***FFT***)

Ogni funzione periodica ***f*** **: [0, 2] → R**
si può definire come una serie di Fourier,

**ovvero**

Una somma infinita di funzioni
trigonometriche semplici
(***armoniche fondamentali***)



# Steganografia Audio

## Mp3

*Non posso celare prima i dati in un file **Wav** e farne una **Mp3**!!*

***Soluzione:*** Nella generazione di un file Mp3 esiste la fase di

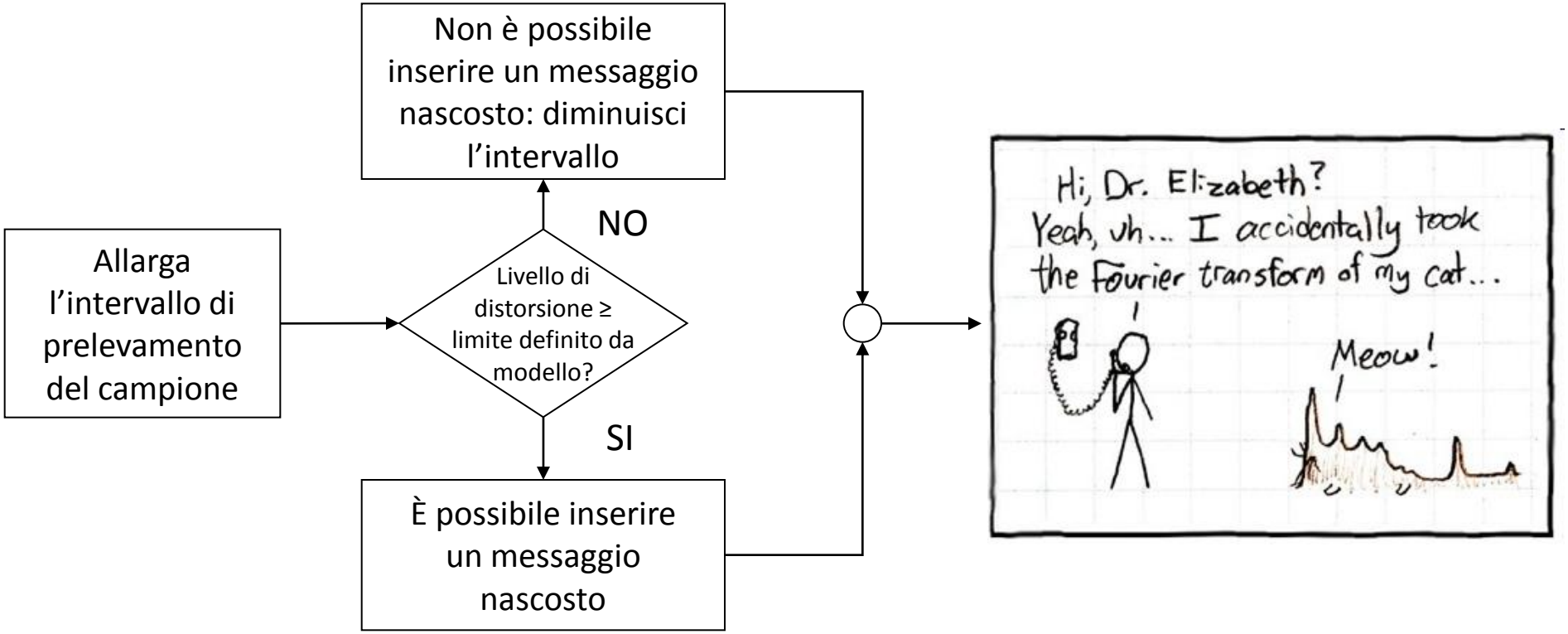
### *Inner loop*

- Allarga gli intervalli di prelevamento del campione

- Testa se il livello di distorsione introdotto è superiore ad un certo limite definito da un modello **psicoacustico** (***individua i bit più o meno importanti***!!)

# Steganografia Audio

## Mp3



# Steganografia Audio

Jpeg, Mpeg… stesso problema del Wav

Una seconda manipolazione può far cancellare le informazioni nascoste al loro interno!!

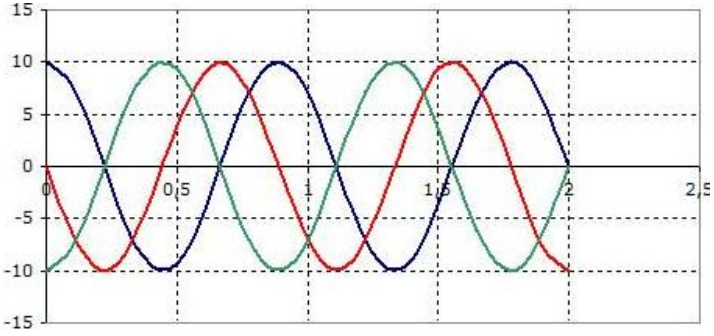
***(Può risultare utile per eliminare le tracce in certe situazioni!!)***

La rappresentazione digitale del segnale ed il mezzo di trasmissione

***Ambiente di ricampionatura con aumento/decremento***

***Trasmissione analogica e ricampionatura***

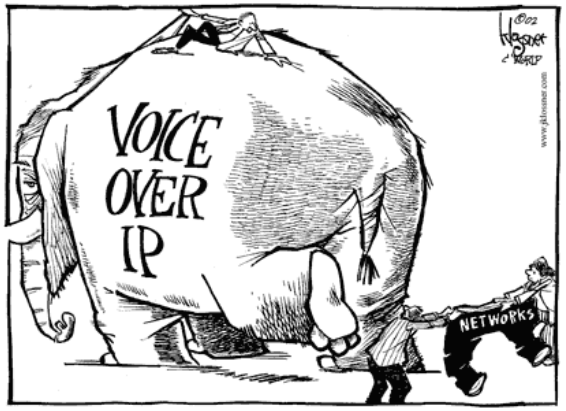
***Ambiente "Over the Air"***



# Steganografia Audio

## VoIP

Ragionando sull'audio e il video due ricercatori




**Wojciech Mazurczyk e Krzysztof Szczypiorski**

del

**Dipartimento di Electronics and Information Technology**

della **Warsaw University of Technology**

Hanno sviluppato due nuove tecniche steganografiche applicate al VoIP

Scarica Articolo Originale: **Steganography of VoIP Streams**

# Steganografia Audio

## VoIP

Generalemente, la connessione **VoIP** consta di due fasi:

1) Signalling Phase - (protocollo SIP)

2) Conversation Phase - (protocollo RTP per i dati e RTPC per i pacchetti di controllo)

Le tecniche convenzionali fanno uso di alcuni campi ridondanti dei protocolli TCP/UDP/IP

oppure

di analoghi campi dell'RTP, come il padding, l'extension header o anche l'authentication tag.

Un altro metodo per la creazione di ***covert channel*** consiste nell'utilizzo degli audio watermarking, usati per implementare il ***DRM*** (gestione dei diritti digitali)

# Steganografia Audio

## VoIP

## Performance

**Tcp/Udp**

Il problema, al momento, sembra essere l'ottimizzazione del sistema: il decadimento della qualità nella conversazione quando c'è un messaggio nascosto è troppo evidente e dunque chiunque potrebbe accorgersi che c'è qualcosa che non quadra.

(calcoli probabilistici aiutano a non degradare troppo la qualità)

**VoIP**

In un tempo medio di conversazione di 9 minuti si ha un trasferimento di circa 1.3 Mb di dati nascosti, Skype necessita  di 13 minuti (altri provider tra i 7 e gli 11 minuti).

# Steganografia Audio

## VoIP

### Contromisure

Se è già difficile mettere orecchio nelle chiamate sul VoIP di Skype, la probabilità che vengano individuate attraverso specifiche analisi forensi eventuali comunicazioni nascoste nelle chiamate vocali è remota

Questo almeno finché il progetto tedesco StegIT non darà i suoi primi frutti.

- Istituito presso l'Università di St. Poelten con il contributo, fra gli altri, del Ministero della Difesa e di quello per gli Affari Interni, StegIT avrà una durata stimata di 8 mesi e l'obiettivo dichiarato di sviluppare una soluzione anti-steganografica per le comunicazioni vocali, su VoIP così come sulle tradizionali reti cellulari GMS/UMTS

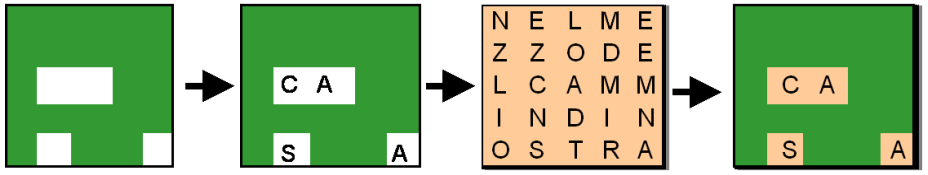
**Wikipedia:** Skype security

# Steganografia

## Fatta in Casa

# Steganografia

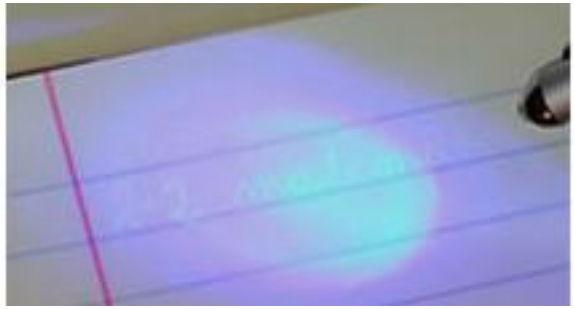
## Griglie di Cardano (Tecnica Adattiva)




1) Creare una Griglia
2) Posizionarla su un foglio bianco
3) Scrivere il messaggio segreto
4) Creare un testo che nasconda le informazioni scritte al punto 3

## Inchiostri invisibili

Utilizzando sostanze che non lasciano tracce visibili in condizioni normali, si possono scrivere messaggi ed attraverso una reagente oppure illuminazioni adatte è possibile leggere il messaggio.
Inchiostri famosi:
Succo di limone (**Inchiostro Simpatico**),
Soluzione acquosa di solfato rameico



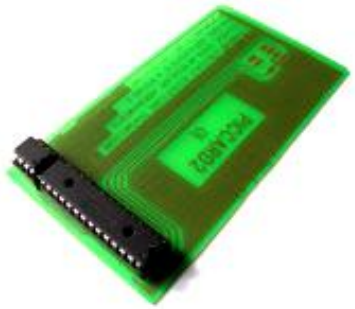
# Steganografia

## Attacchi Famosi

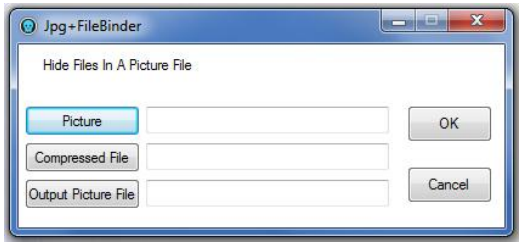
All'inizio del nuovo millennio ci fu un grande uso della Steganografia per far viaggiare in rete i codici per la decodifica di programmi tv satellitari.

Si nascondevano in insospettabili file Jpg i codici in formato binario (Ascii)

Tanto era usuale che l'Hardware si realizzava in casa per pochi euro bastava un semplice microcontrollore PIC 16F84 e una Eprom 24LC16B



# Steganografia




**Jpg+FileBinder**

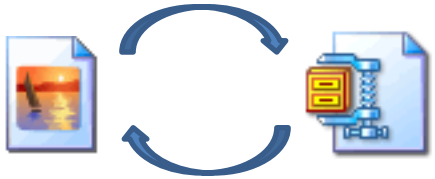
Un semplice software che trasforma un'immagine formato Jpg in un contenitore per un **file compresso** che contiene il messaggio da nascondere in formato compresso (Zip, Rar, 7zip)

**Estrattori File Compressi (es. WinRar)**

In maniera insospettabile permettono di estrarre il file nascosto nell'immagine

**Rinomina e Svela**

Una volta ottenuto il file Jpg di output, questo sarà leggibile da programmi di grafica come un immagine, ma se rinominato con l'estensione Zip si avrà accesso al contenuto segreto



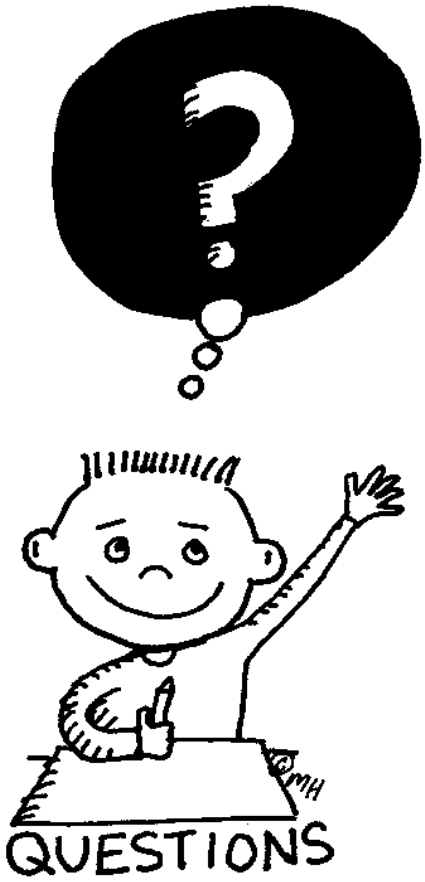
# Steganografia


Altri due esempi famosi di Steganografia nella storia contemporanea

Messaggi subliminari nei film ora vietati (Marketing)

I Beatles ne hanno fatto largo uso (forse) nei loro album

Come ad esempio: Alla fine di “*I'm So Tired*”, una voce ascoltata al contrario sembrerebbe dire "Paul is dead, man: miss him, miss him, miss him!“


QUESTIONS