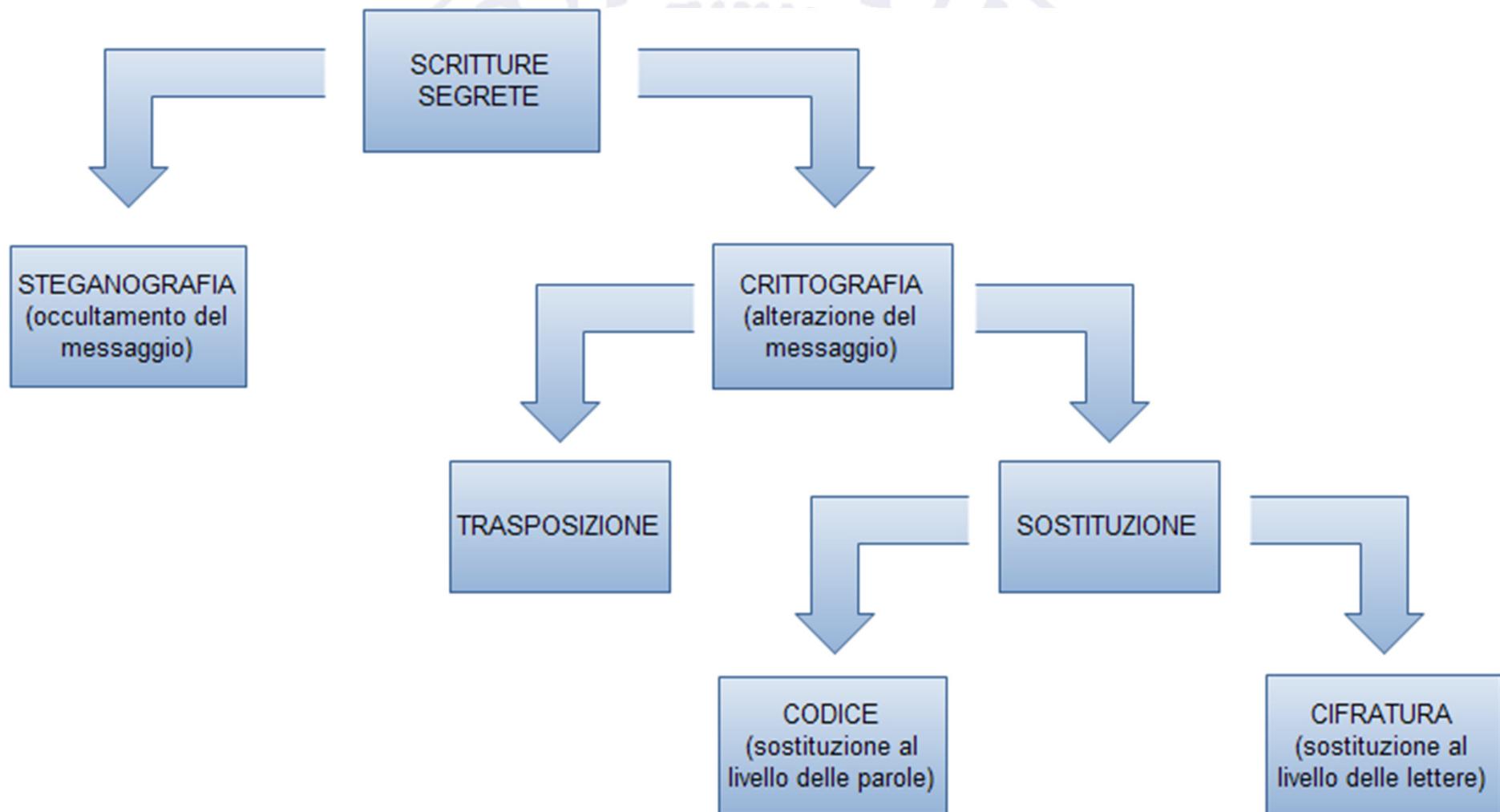


Le scritture segrete



Steganografia

La steganografia

- Steganografia (dal greco *steganòs*, nascosto, e *gràphia*, scrittura): tecnica che permette di nascondere un messaggio segreto all'interno di un messaggio pubblico di copertura
- Da non confondere con la crittografia, tecnica mirata a rendere incomprensibile un messaggio per chiunque, tranne che per il destinatario.
- 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 dire quale)

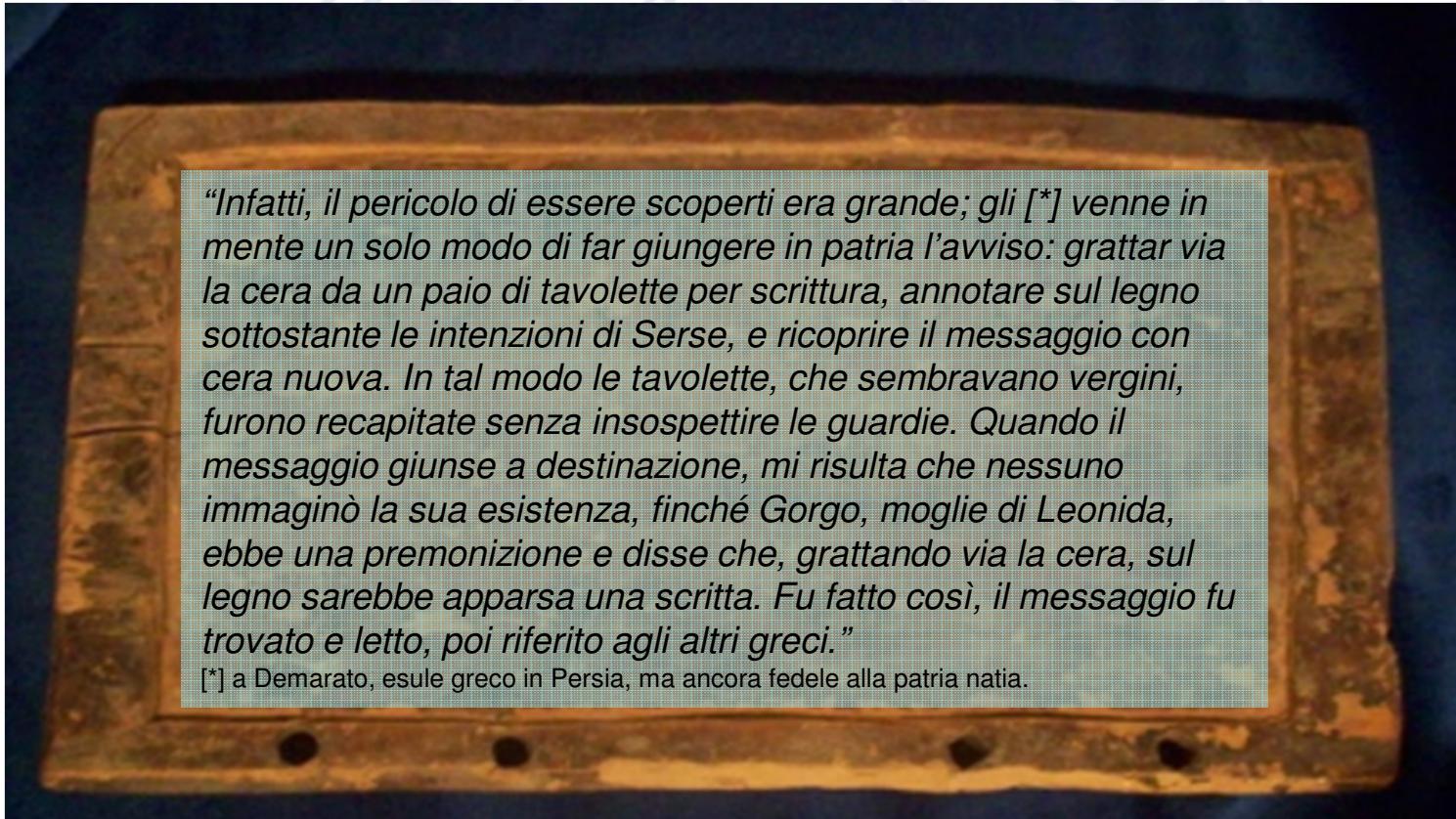
Nota: la steganografia non ha niente a che vedere con la stenografia! (sembra scontato ma...)

Vantaggi e svantaggi...

- Pro: a volte si vuole nascondere il fatto stesso di stare comunicando con qualcuno, indipendentemente dal tipo di messaggio trasmesso
- Contro: contrariamente a quanto accade con la crittografia, l'intercettazione mette a rischio il messaggio

Esempi storici

- Secondo Erodoto, i greci usarono più volte le tecniche steganografiche nella guerra contro i persiani di Serse...



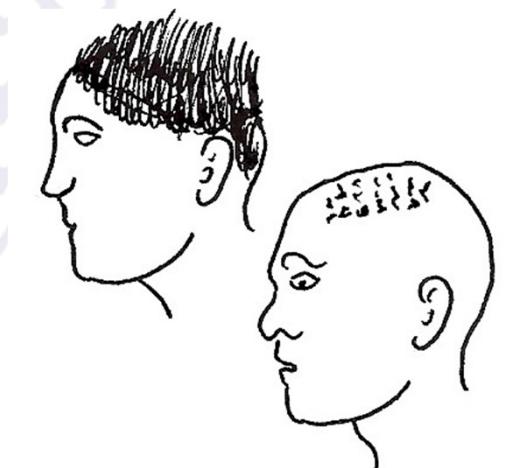
Fu così che, grazie all'astuzia di Demarato e all'intuito di Gorgo, i greci poterono prepararsi alla battaglia e vincerla in un sol giorno

Esempi storici / 2

- Altro aneddoto raccontato da Erodoto:

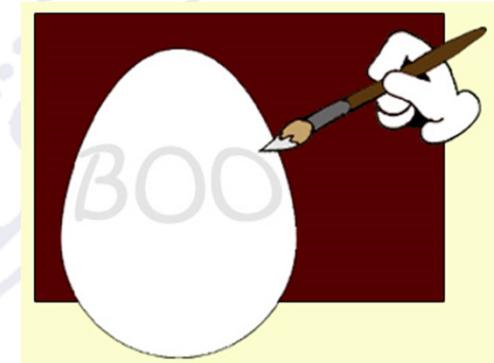
Istieo voleva incoraggiare Aristagora di Mileto a ribellarsi al re persiano. Per far giungere le relative istruzioni in modo sicuro, egli fece rasare il capo a un corriere, gli scrisse il messaggio sulla cute e aspettò che gli ricrescessero i capelli.

(evidentemente Istieo non aveva molta fretta...)



Esempi storici / 3

- Nel XVI secolo il filosofo e alchimista Giovanni Battista Della Porta consigliava di scrivere sul guscio di un uovo sodo usando una soluzione di mezzo litro di aceto e 30 g. di allume
- La soluzione penetra nel guscio senza lasciare traccia, ma tinge l'albuminato solidificato sottostante



Funziona anche se si cuoce l'uovo dopo aver scritto il messaggio:

<http://www.wonderhowto.com/wonderment/send-secret-messages-hard-boiled-eggs-0113016/>

Esempi storici / 4

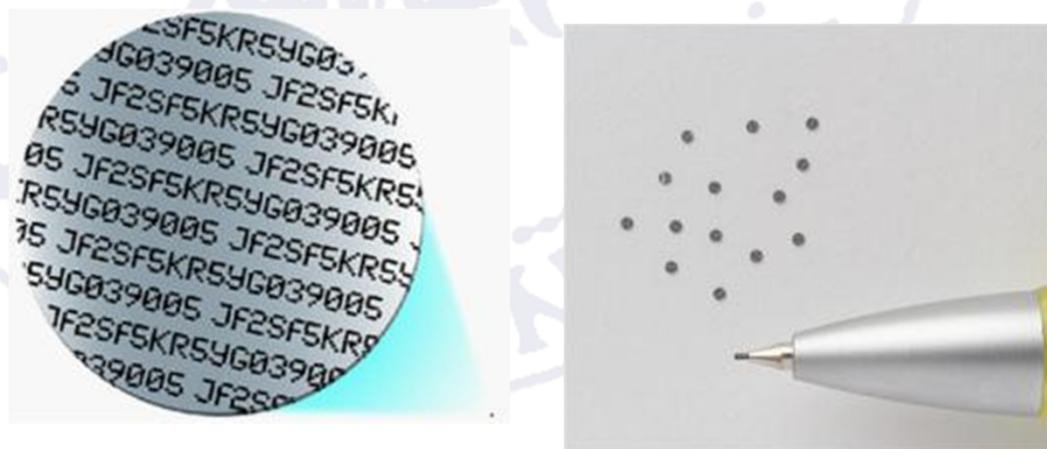
- Nel XV secolo, l'abate Giovanni Tritemio (1462-1516) scrisse "Steganographia", il primo trattato stampato (nel 1600) dell'antichità sulla steganografia.
- Conteneva più di 40 tecniche di steganografia (e crittografia) differenti! Venne messo all'indice soprattutto a causa del terzo libro, apparentemente misterioso e incomprendibile, e quindi "demoniaco". Si trattava naturalmente di un testo steganografato/crittato...
- Venne decifrato solo nel 1996. Contiene una serie di frasi in tedesco e latino di scarsa rilevanza, come ad esempio "il latore di questa lettera è un brutto furfante ed un ladro"

S. Hora 1.	X. Hor. 2.	S. hor. 3.	X. grad.	X. punct.	S. hor. 1.
640	635	22	25	634	632
642	X. 646	S. 647	X. 3	646	32
634	25	646	2	S. 648	S. 640
646	640	632	1	632	650
635	646	634	4	639	644
646	642	12	1	617	639

X. hor. 2.	S. hor. 3.	X. grad.	S.
632	632	650	X.
640	640	640	646
24	S. 633	X. 646	S.
647	632	639	X.
638	632	650	626
639	640	626	X.

Esempi più recenti

Durante la seconda guerra mondiale, venne spesso utilizzata la tecnica dei “microdot”: tramite un procedimento fotografico, gli agenti tedeschi in America latina trasformavano una pagina scritta in una “macchia” del diametro inferiore al millimetro, che poteva essere nascosta nel puntino di una ‘i’ in una comunicazione banale. Il primo microdot fu scoperto dall’FBI solo nel 1941, grazie ad una soffiata.



Esempi più recenti / 2

- La tecnica delle “cifre nulle” consiste nel nascondere il testo in un altro, in modo che possa essere estratto selezionando solo alcuni caratteri del messaggio originale.
- Il seguente messaggio è stato realmente inviato da una spia tedesca durante la seconda guerra mondiale:

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

prendendo solo la seconda lettera di ogni parola diventa:

Pershing sails from NY (r) June 1

Esempi più recenti / 3

- Si dice che negli anni '80, Margaret Thatcher, preoccupata per la fuga di notizie riservate, lasciate filtrare alla stampa da parte di suoi non troppo fedeli collaboratori, fece programmare i loro word processor in modo che il nome dello scrivente fosse codificato nella spaziatura delle parole.
- Un messaggio del governatore Schwarzenegger ai membri della California State Assembly:

To the Members of the California State Assembly:

I am returning Assembly Bill 1176 without my signature.

For some time now I have lamented the fact that major issues are overlooked while many unnecessary bills come to me for consideration. Water reform, prison reform, and health care are major issues my Administration has brought to the table, but the Legislature just kicks the can down the alley.

Yet another legislative year has come and gone without the major reforms Californians overwhelmingly deserve. In light of this, and after careful consideration, I believe it is unnecessary to sign this measure at this time.

Sincerely,

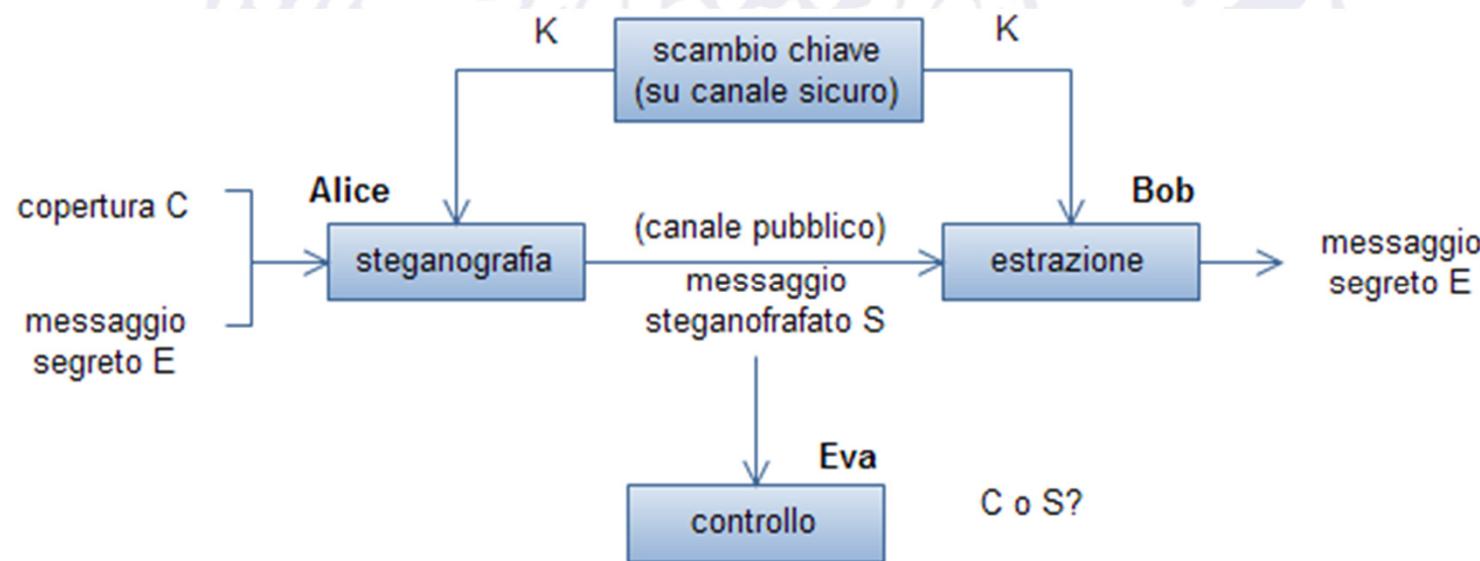
Arnold Schwarzenegger

Steganografia moderna

- Oggi usiamo principalmente due criteri per distinguere le tecniche steganografiche:
 - Steganografia ad attaccante passivo vs. steganografia ad attaccante attivo (a quali attacchi è in grado di resistere il messaggio steganografato?)
 - Steganografia generativa vs. steganografia iniettiva (come viene nascosto il messaggio steganografato nel messaggio contenitore?)

Steganografia ad attaccante passivo

- Si ipotizza un ruolo passivo dell'attaccante, che semplicemente non deve accorgersi della presenza di un messaggio nascosto
- Formalizzato da Simmons (*) come il “problema dei prigionieri”



(*) Simmons, Gustavus J. "The Prisoner's Problem and the Subliminal Channel," *Advances in Cryptology: Proceedings of CRYPTO '83*, Plenum Press, 1984, pp. 51-67.

Steganografia ad attaccante passivo

- Problema dei prigionieri: Alice e Bob sono prigionieri e stanno pianificando la loro fuga. Devono comunicare tramite un canale pubblico, ma se la guardia Eva avrà anche il minimo sospetto che Alice e Bob si stiano scambiando messaggi illeciti, li metterà in cella di isolamento.
- Alice usa un testo contenitore C per nascondere il messaggio E in un testo S da trasmettere a Bob (il quale potrà recuperare E usando eventualmente una chiave segreta K nota solo ai due).
- Eva non deve essere in grado di distinguere S da un normale testo di copertura (come C).

Steganografia ad attaccante attivo

- In questo caso Eva non si limita ad osservare passivamente il messaggio S , ma lo modifica attivamente, in modo da non alterare il senso di S ma rischiando di distruggere E .
- Eva non sa dove è nascosto il messaggio E , quindi può solo modificare S facendo delle ipotesi... compito di Alice è quello di generare un S il più possibile robusto a questi attacchi
- Vedremo più avanti come i watermark siano un tipico esempio di messaggi steganografici studiati per resistere agli attacchi attivi

Steganografia generativa vs. iniettiva

- Steganografia generativa:
Il contenitore viene generato a partire dal testo da nascondere. Viene quindi “costruito su misura” per contenere un certo messaggio.
- Steganografia iniettiva:
Il contenitore è dato a priori, e vi si inietta il messaggio da nascondere tentando di rendere le modifiche impercettibili

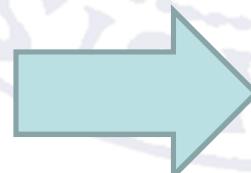
Steganografia generativa

- Esempio: SpamMimic crea un finto messaggio di spam, in cui in realtà è nascosto il messaggio segreto.
- Il messaggio può essere inviato per e-mail: un eventuale attaccante passivo lo scambierà per un comunissimo messaggio di spam, senza sospettare che nasconde un messaggio segreto
- Si tratta di un approccio generativo perché il contenitore (il messaggio di spam) viene generato ad hoc per contenere il messaggio desiderato

Problemi:

- solo messaggi brevi
- attenzione ai filtri antispam!

ciao



Dear Cybercitizen , You made the right decision when you signed up for our club ! We will comply with all removal requests . This mail is being sent in compliance with Senate bill 2516 , Title 9 , Section 307 . Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich inside 98 DAYS ! Have you ever noticed how long the line-ups are at bank machines & how many people you know are on the Internet ! Well, now is your chance to capitalize on this ! We will help you decrease perceived waiting time by 190% and deliver goods right to the customer's doorstep ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Mrs Simpson of Maryland tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws ! We implore you - act now ! Sign up a friend and you get half off . Thanks .

SpamMimic

- SpamMimic è liberamente utilizzabile in rete:
<http://www.spammimic.com>
- Utilizzate SpamMimic per leggere il messaggio nascosto in questo testo di spam:
<http://users.dimil.uniud.it/~claudio.piciarelli/teach/sicurezza2010/spam.txt>

Steganografia iniettiva

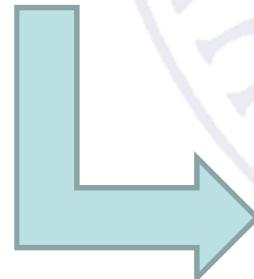
- E' il tipo di steganografia di gran lunga più diffuso
- Consiste nel nascondere il messaggio segreto in un messaggio contenitore preesistente
- Attenzione: "messaggio" ha qui una valenza generica (ad es. può essere un'immagine)



Esempio di steganografia iniettiva in file di testo

- Snow (<http://www.darkside.com.au/snow/>) nasconde i messaggi codificandoli negli spazi tra una parola e l'altra di un file di testo

Quel ramo del lago di Como, che volge a mezzogiorno, tra due catene non interrotte di monti, tutto a seni e a golfi, a seconda dello sporgere e del rientrare di quelli, vien quasi a un tratto, tra un promontorio a destra e un'ampia costiera dall'altra parte; e il ponte, che ivi congiunge le due rive par che renda ancor più sensibile all'occhio questa trasformazione e segni il punto in cui il lago cessa, e l'Adda ricomincia per ripigliar poi nome di lago dove le rive, allontanandosi di nuovo, lascian l'acqua distendersi e rallentarsi in nuovi golfi e in nuovi seni...



Quel ramo del lago di Como, che volge a mezzogiorno, tra due catene non interrotte di monti, tutto a seni e a golfi, a seconda dello sporgere e del rientrare di quelli, vien quasi a un tratto, tra un promontorio a destra e un'ampia costiera dall'altra parte; e il ponte, che ivi congiunge le due rive par che renda ancor più sensibile all'occhio questa trasformazione e segni il punto in cui il lago cessa, e l'Adda ricomincia per ripigliar poi nome di lago dove le rive, allontanandosi di nuovo, lascian l'acqua distendersi e rallentarsi in nuovi golfi e in nuovi seni.

Steganografia iniettiva / 2

- Proprietà fondamentale: il contenitore deve apparire inalterato
- Un approccio possibile: il contenitore possiede del rumore che può essere sostituito da un segnale



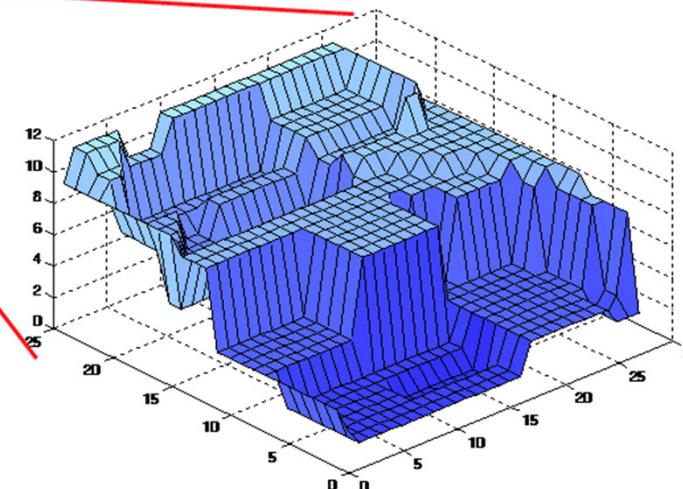
Definizioni

Rumore: informazione incoerente e casuale (ad es. il fruscio in una traccia audio, le fluttuazioni dei pixel in una fotografia digitale...)

Segnale: informazione coerente (una canzone, il soggetto di una foto...)

Steganografia LSB

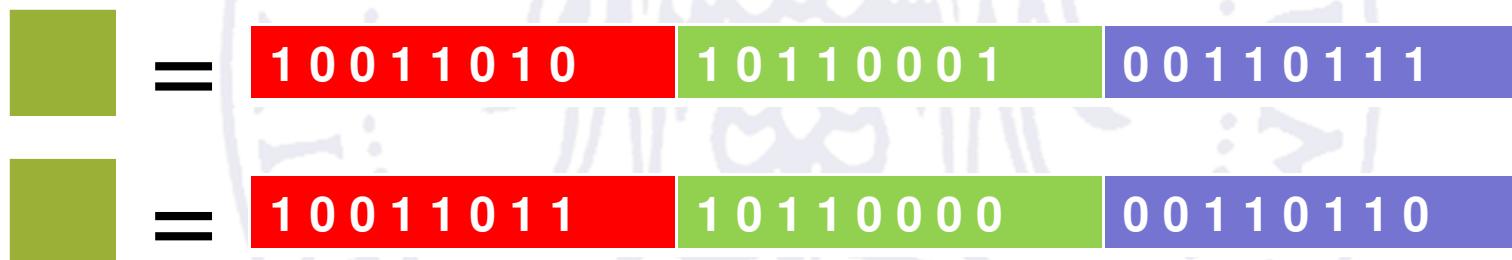
- I pixel di una fotografia digitale sono soggetti a piccole fluttuazioni casuali (rumore)



- Il rumore può essere sostituito da un messaggio segreto

Steganografia LSB / 2

- Codifica RGB: 8 bit per canale
- I bit meno significativi (Least Significant Bits) sono quelli più affetti da rumore. Modificandoli, il cambiamento è impercettibile



- Infatti, il bit più significativo indica se il canale per un determinato pixel assume un valore maggiore o minore di 128, mentre il bit meno significativo dice solo se il valore del pixel è pari o dispari

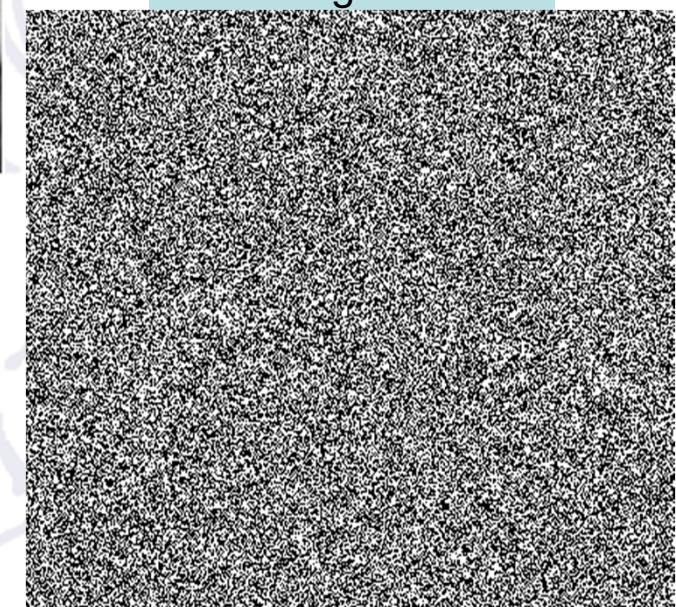
Steganografia LSB / 3



Informazione
contenuta nel bit
più significativo



Immagine
originale



Informazione
contenuta nel bit
meno significativo

Steganografia LSB / 4

- Consiste nell'usare i bit meno significativi di una immagine digitale per nascondere un messaggio.
- Limite massimo alla dimensione del messaggio, ipotizzando di usare un solo bit per canale:

Se l'immagine ha dimensioni 640x480 pixel, allora...

$$640 \times 480 \times 3 \text{ canali} = 921.600 \text{ bit utilizzabili}$$

$$921.600 / 8 = 115.200 \text{ byte}$$

→ il messaggio può essere lungo al max. ~100 KB

Si potrebbero usare più bit, ma il rischio è quello di produrre un'alterazione visibile del segnale (si percepisce un degrado nella qualità dell'immagine)

Steganografia LSB / 5

- Lo stesso procedimento si può applicare ad altri dati multimediali. Ad esempio, in un file audio di un minuto (qualità CD)...

60 secondi x 44100 campioni al secondo x 2 canali = 5.292.000 bit
5.292.000 / 8 = ~660 KB disponibili per inserire un messaggio segreto.

Esercizio (facile)

- Che dimensione deve avere un'immagine per steganografare un messaggio di 5KB usando solo i due bit meno significativi del canale verde?

$$5 \text{ KB} = 5 * 1024 * 8 \text{ bit} = 51240 \text{ bit}$$

2 bit utilizzabili per ogni pixel

Numero di pixel necessari: $51240 / 2 = 25620$ pixel

Qualsiasi immagine con almeno 25620 pixel va bene, ad esempio un'immagine con dimensione 260x100

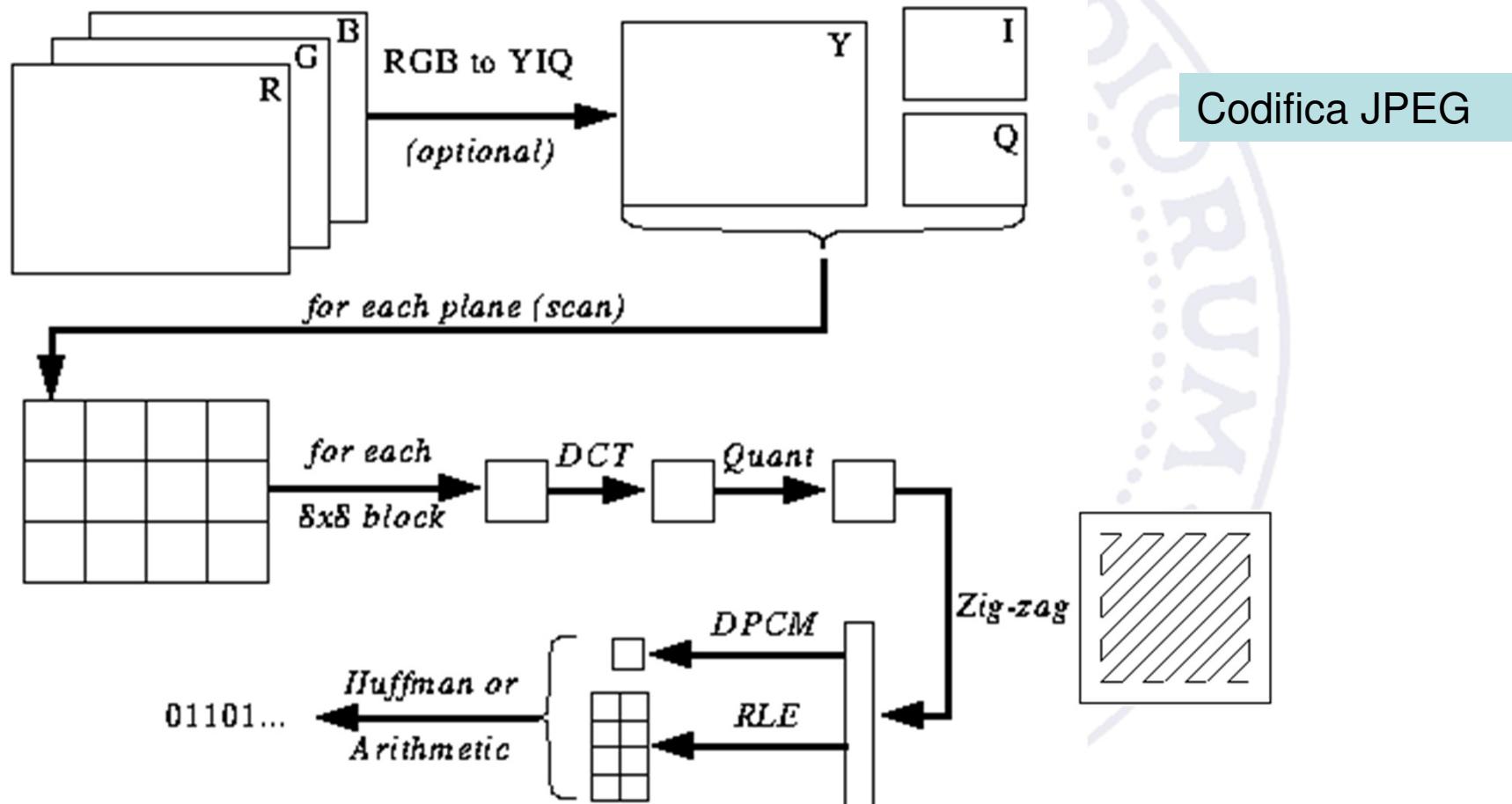
Steganografia LSB / 7

- Problema della steganografia LSB: funziona solo se l'immagine è successivamente memorizzata usando un formato lossless (immagini BMP o PNG, audio WAV, ecc...)
- Un'eventuale compressione distruggerebbe il messaggio segreto. I meccanismi di compressione funzionano proprio eliminando il rumore (inutile in quanto impercettibile)!
- Nei formati compressi, non esiste una rappresentazione ‘semplice’ del singolo pixel o del singolo campione audio.

Steganografia nelle immagini JPEG

- Il formato JPEG lavora nel dominio delle frequenze di un'immagine, e funziona salvando solo i coefficienti più significativi di una trasformata DCT (discrete cosine transform)
- Soluzione: applicare la tecnica LSB sui coefficienti DCT anziché sui singoli pixel
- Esempio di software steganografico per immagini JPEG:
JSteg <http://jsteg.org/>

Steganografia nelle immagini JPEG / 2



Steganalisi

- La steganalisi studia come capire se un contenitore sta veicolando o meno un messaggio segreto
- Approcci banali:
 - È stato usato un contenitore pubblico (ad es. un'immagine presa da internet, accessibile anche allo steganalista)
 - È stato usato lo stesso contenitore per trasmettere messaggi diversi

In entrambi i casi un confronto tra il contenitore originale e quello contenente il messaggio steganografato, o tra due contenitori con messaggi diversi, evidenzia delle differenze che rivelano la presenza di un messaggio nascosto

Steganalisi / 2

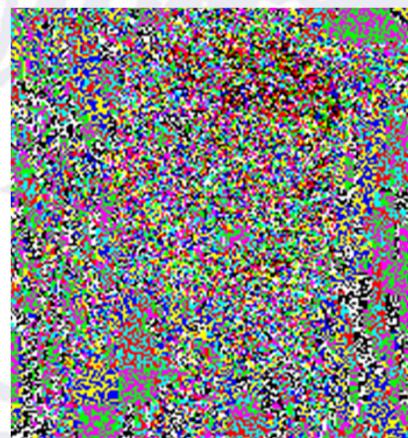
- Esercizio: inserire un messaggio steganografato in un'immagine contenitore (in alternativa, usare le seguenti immagini:
http://users.dimini.uniud.it/~claudio.piciarelli/teach/sicurezza2010/albero_orig.jpg
http://users.dimini.uniud.it/~claudio.piciarelli/teach/sicurezza2010/albero_jsteg.jpg
- Usare Photoshop per trovare le differenze tra l'immagine con e senza messaggio nascosto

Steganalisi / 3

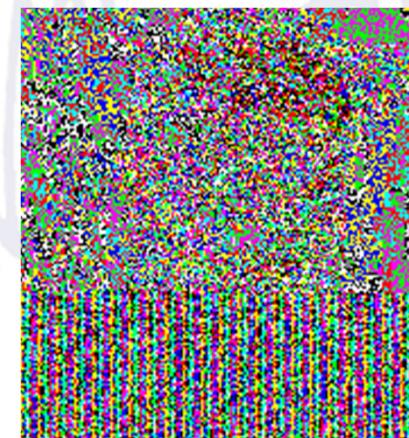
- Il messaggio cambia le caratteristiche del rumore, sostituendosi ad esso
- Rilevabile se si possiede un modello statistico del rumore



Immagine originale



LSB dell'immagine
originale



LSB dell'immagine + messaggio segreto
(il pattern del messaggio è chiaramente
visibile e rilevabile automaticamente
tramite analisi statistica)

Steganalisi / 4

- In un sistema steganografico ideale, non è possibile distinguere il messaggio dal rumore... [1]
- Questo si può ottenere:
 - Generando messaggi statisticamente simili al rumore stesso (ad es. tramite eliminazione della ridondanza, ammesso che il rumore del contenitore sia davvero casuale)
 - Alterando il resto del contenitore in modo da “bilanciare” l’introduzione del messaggio segreto, cosicché le statistiche finali risultino inalterate

Un algoritmo inizialmente studiato per la steganografia statisticamente robusta: F5. Sfortunatamente si è in seguito dimostrato come F5 sia comunque suscettibile ad attacchi statistici [2]

[1] C. Cachin. *An information-theoretic model for steganography*, 2nd international workshop on Information Hiding, pages 306–318., New York, 1998

[2] J. Fridrich, M. Goljan, and D. Hogea, *Steganalysis of JPEG Images: Breaking the F5 Algorithm*. Pre-proceedings of 5th Information Hiding Workshop, Netherlands, Oct. 7–9, 2002.

Watermarking

- Watermark: informazione inserita in un documento digitale che ne identifica il legittimo proprietario, qualora ne venga fatta una copia
- Lo scopo del watermarking non è quindi quello di veicolare un messaggio segreto, ma quello di “marchiare” in maniera indelebile un documento. Serve ad esempio a garantire il copyright su un documento (ad es. una foto pubblicata su internet).
- Somiglianze con la steganografia classica: il watermark deve essere invisibile, non deve alterare in maniera significativa il contenitore
- Differenze: *la rimozione del watermark dal file originale deve essere impossibile!*

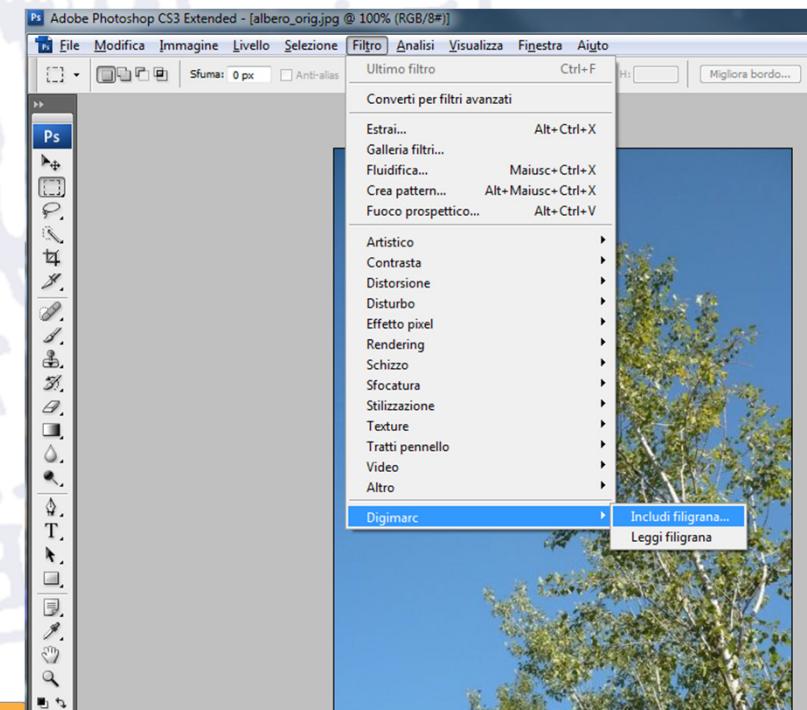
Watermarking / 2

- La caratteristica principale del watermark è quindi l'impossibilità della sua rimozione o alterazione.
- Il watermark deve essere robusto a modifiche del file contenitore (ad esempio rotazioni, cambiamenti di scala o cropping dell'immagine protetta).
- Per questo motivo è importante che il watermark sia “diffuso” in tutto il documento da proteggere, onde evitare la sua rimozione tramite l'eliminazione della porzione di documento in cui il watermark risiede.

Watermarking / 3

- Digimarc è un software per inserire dei watermark con note di copyright in documenti multimediali (immagini, file audio, video).
- E' l'unico plug-in sviluppato da terze parti abilitato di default in Photoshop.

Esercizio: usando Photoshop, provate ad applicare un watermark su un'immagine. Verificate poi le differenze con l'immagine originale.



Watermarking / 4

- I cosiddetti watermark visibili, invece, non hanno niente a che vedere con la steganografia



(immagine di Natasha Milosevic)

Watermarking / 5

- Tutti noi abbiamo quotidianamente a che fare con i watermark, anche se non ce ne accorgiamo...
- Un watermark grafico, la cui esatta natura è tuttora ignota al pubblico, è inserito in tutte le banconote delle principali valute
- Molti software di elaborazione di immagini (tra cui Photoshop e Paint Shop Pro) rilevano questo watermark e limitano le possibilità di lavorare su immagini di banconote (ad es. Photoshop impedisce di stamparle).
- Provate ad aprire con Photoshop questa immagine:
<http://users.dimil.uniud.it/~claudio.piciarelli/teach/sicurezza2010/banconota.png>
- Il watermark risulta particolarmente ostico da rimuovere:
<http://www.cl.cam.ac.uk/~sjm217/projects/currency/>
- Maggiori informazioni su: <http://www.rulesforuse.org/>

Fingerprinting

- Un fingerprint è concettualmente simile ad un watermark, ma ogni copia del documento “marchiato” ha un fingerprint differente, in modo da identificarne il possessore (e non l'autore).
- Ad esempio un file MP3 acquistato online potrebbe contenere un fingerprint che ne identifica univocamente l'acquirente. Se questi ne facesse una copia da distribuire illegalmente ad altri, si potrebbe risalire al possessore originario.

Fingerprinting / 2

- Watermark: univoco per tutte le copie, identifica l'autore
- Fingerprint: differente per ogni copia, identifica il possessore finale.

Fingerprinting / 3

- Un caso molto particolare di fingerprint...
- Molte stampanti laser a colori stampano, ad insaputa dell'utente, una serie di punti gialli difficilmente visibili ad occhio nudo, in cui è codificato il numero di serie della stampante e optionalmente la data di stampa
- Pare che la cosa sia stata richiesta dal governo USA come metodo per risalire agli autori di stampe “pericolose”
- Per maggiori informazioni: <http://www.seeingyellow.com/>
- Lista delle stampanti che utilizzano questa tecnica:
<http://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots>