STEGANOGRAFIA

a cura di:

Maurizio Migliore

Significato etimologico

La parola steganografia deriva dal greco:

- *stèganos* = nascosto
- *gràfein* = scrivere

Quindi, è una tecnica per nascondere informazioni

Steganografia e crittografia

Spesso confusa con la crittografia, ma sono due tecniche diverse

- Crittografia: nasconde il contenuto di un messaggio
- Steganografia: nasconde il messaggio stesso

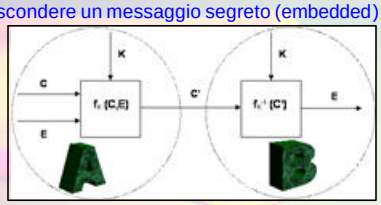
Steganografia nella storia

È nata nell'antica Grecia e si è sviluppata fino ad oggi

- Storie di Erodoto
- Griglie di Cardano
- Cifre nulle
- Shakespeare vs Bacon
- Inchiostri simpatici
- Micropunti fotografici
- Al-Queda su siti internet

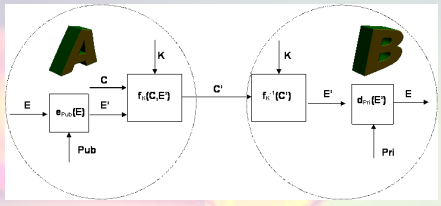
Il sistema steganografico

Il cover (o contenitore) è un file atto a contenere e nascondere un messaggio segreto (embedded)



La funzione steganografica incapsula il messaggio segreto all'interno del cover utilizzando una chiave K che sia la sorgente che ricevente devono conoscere

Steganografia a chiave pubblica



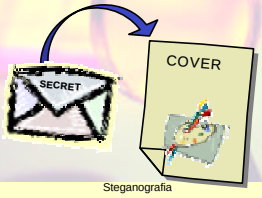
In più, vi è la codifica/decodifica del messaggio nascosto

- **Pro:** difficile interpretare il messaggio nascosto
- **Contro:** cercare di decifrare tutti i potenziali file stego può diventare una caccia al tesoro

Metodi steganografici: steganografia iniettiva

A seconda degli approcci utilizzati, distinguiamo i software steganografici in iniettivi e generativi

La steganografia iniettiva nasconde il messaggio segreto all'interno di un file contenitore già esistente



Metodi steganografici: steganografia generativa

Nei software di tipo generativo si parte dal messaggio segreto e si costruisce un contenitore ad hoc

Fasi steganografiche: trovare i bits ridondanti

I bits ridondanti sono bits del cover scelti per l'inserimento del messaggio nascosto

In genere, **bits ridondanti = bits meno significativi**

Altre tecniche analizzano il cover per ottimizzare l'operazione

Fasi steganografiche: scegliere i Cover Bits

Di solito, **#bits da nascondere ? #bits ridondanti**

- Se i bits da nascondere sono di più, l'embedding non può essere effettuato
- Se sono di meno, viene scelto un sottoinsieme dei bits ridondanti (Cover Bits) per nascondere il messaggio segreto

È desiderabile che ogni Cover Bit sia scelto in modo equiprobabile tra i bits ridondanti per scongiurare tipi di attacchi

Fasi steganografiche: Embedding

Consiste nell'incapsulamento dei dati nascosti

Di solito, non si fa altro che nascondere i bits segreti nei bits meno significativi

Diversa tecnica è la ***Matrix-Encoding***

Fasi steganografiche Embedding: Matrix-Encoding

Utilizza 3 parametri: *n, k, d*

n è il numero di bits selezionati tra i Cover Bits

k è il numero di bits da incapsulare

d è il numero di bits che si possono, **al più**, modificare

Fasi steganografiche Embedding: Matrix-Encoding

Caso tipico: *n*=3, *k*=2 e *d*=1

Se a, *b*, *c* sono i 3 Cover Bits in considerazione
e *x* e *y sono i 2 bits segreti*:

- Se *a*, *b* e *c* verificano *x=(a XOR c)* e *y=(b XOR c)* allora non si fa nulla
- Se *x=(a XOR c)* ma *y ?(b XOR c)* allora deve essere cambiato *b* (al suo valore negato)
- Viceversa, se *x?(a XOR c)* ma *y=(b XOR c)*, deve essere cambiato *a*
- Se entrambe le uguaglianze sono false allora è *c* a dover essere sostituito con il suo negato

Fasi steganografiche Embedding: Matrix-Encoding

Caso tipico: *n*=3, *k*=2 e *d*=1

Si inseriscono 2 bits segreti in 3 Cover Bits, modificando al più uno solo dei Cover Bits

Bits in considerazione
its segreti:

(b XOR c) allora non si fa nulla
- Se *x=(a XOR c)* ma *y ?(b XOR c)* allora deve essere cambiato *b* (al suo valore
- Viceve mbiato *a*
- Se entrambe le uguaglianze sono false allora è *c* a dover essere sostituito con il suo negato

Al più uno dei tre Cover Bits viene cambiato

Stegoanalisi

È definita come la scienza (nonché l'arte) del rompere la sicurezza di un sistema steganografico

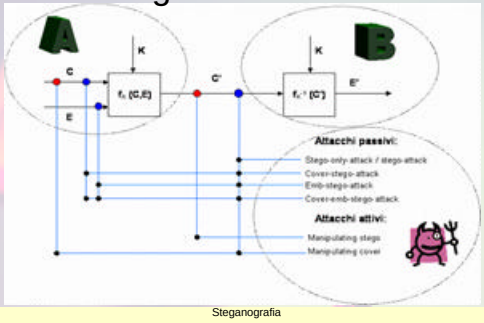
Un attacco con successo ad uno stegosistema consiste nello scoprire che un determinato file contiene dati nascosti anche senza conoscerne il significato

Stegoanalisi

Vale il ***principio di Kerckhoff***

- Il sistema steganografico è conosciuto dall'attaccante
- La sicurezza dipende dal solo fatto che la chiave segreta non è conosciuta dall'attaccante

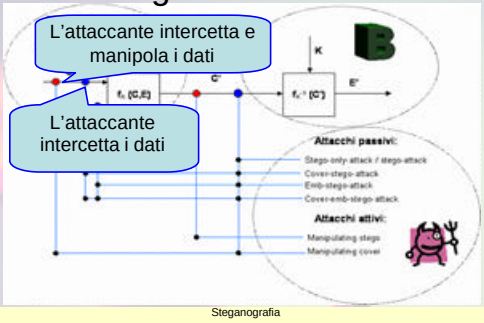
Stegoanalisi: lo stegosistema esteso



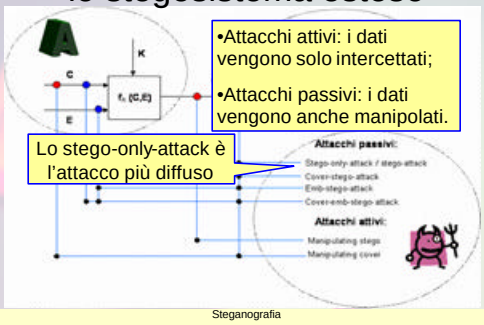
Stegoanalisi: lo stegosistema esteso

L'attaccante intercetta e manipola i dati

L'attaccante intercetta i dati



Stegoanalisi: lo stegosistema esteso



•Attacchi attivi: i dati vengono solo intercettati;

•Attacchi passivi: i dati vengono anche manipolati.

Lo stego-only-attack è l'attacco più diffuso

Applicazioni steganografiche steganografia audio: LSB

I files audio digitali sono molto flessibili e pertanto adatti a recitare il ruolo di cover

La tecnica più usata è la **LSB** (Least Significant Bit) e rimpiazza i bits meno significativi

Possono essere usati anche i 2 o i 3 bits meno significativi, ma tale scelta si ripercuote sulla qualità dell'operazione

Applicazioni steganografiche steganografia audio: LSB

Consideriamo un file wave a 44100 Hz, 16 bit e stereo

Nella trasformazione in digitale viene prodotta una stringa di 16 bits ogni 1/44100 secondi

Le stringhe generate sono due: una per il canale destro, l'altra per il canale sinistro

Applicazioni steganografiche steganografia audio: LSB

Consideriamo un file wave a 44100 Hz, 16 bit e stereo

La dimensione del file risulta essere
16 bit x 44100 Hz x 60 sec x 2 = 84762000 bit = 10366 Kb

La capacità (usando i due bit meno significativi) è
84762000 bit /16 bit x 2 = 10595250 bit = 1293 Kb

Steganografia audio: Echo-data-hiding

L'approccio visto modifica il file aggiungendo un forte rumore di fondo (noise) facilmente avvertibile

L'Echo-data-hiding è una tecnica che evita questo inconveniente

Steganografia audio: Echo-data-hiding

Se il suono originale e la sua eco sono divisi da uno spazio di tempo piccolo abbastanza, l'orecchio umano non riesce a distinguere i due suoni

I dati vengono codificati in questi eco rappresentando gli 0 e gli 1 come due offsets differenti di eco

Steganografia audio: LSB vs Echo-data-hiding

LSB: grande capacità dei cover, minore qualità del file stego

Echo-data-hiding: ottima qualità del file stego, scarsa capacità del cover

Steganografia audio: S-Tools

S-Tools è un software steganografico per audio e immagini

La parte dedicata all'audio lavora su file WAV e sfrutta la tecnica LSB

Steganografia audio: S-Tools

Scritto da Andy Brown

S-Tools è tra i programmi steganografici più diffusi

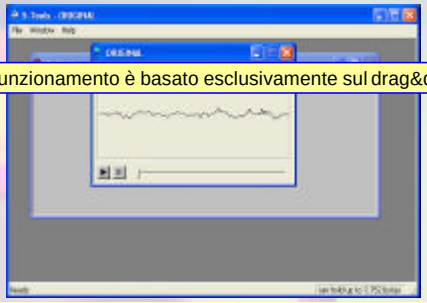
Facile da reperire in rete e freeware

La versione 4.0 è del 1997 ed è l'ultima rilasciata

Il programma gira su un qualunque PC con sistema operativo Windows in tutte le versioni

Supporta i formati WAV, BMP e GIF come file contenitori

Steganografia audio: S-Tools



Il funzionamento è basato esclusivamente sul drag&drop

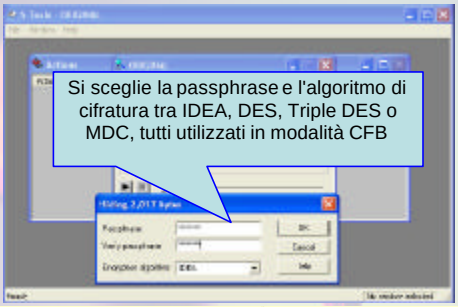
Steganografia audio: S-Tools

Si trascina il file contenitore

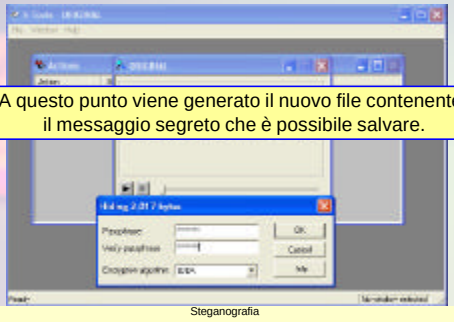
Steganografia audio: S-Tools

Si trascina il file segreto sul file contenitore

Steganografia audio: S-Tools



Steganografia audio: S-Tools



Steganografia audio: S-Tools

Per estrarre il messaggio segreto dal contenitore si segue uno schema simile all'embedding:

- Si trascina il file contenitore da una finestra di un file manager nella finestra principale di S-Tools
- Si seleziona *Reveal* cliccando col tasto destro del mouse sul file contenitore trascinato
- Si sceglie la passphrase e l'algoritmo di cifratura
- Se la passphrase è giusta compare un elenco dei file nascosti ed è possibile salvarli

Steganografia audio: Mp3Stego

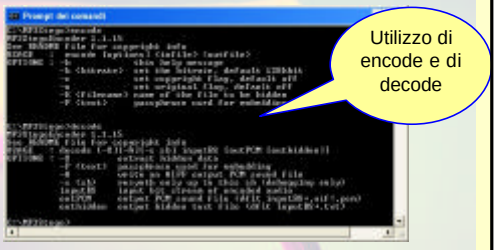
Mp3Stego l'Echo-bit-encoding

L'algoritmo Mp3 è lossy, ovvero comprime i dati in input con perdita di informazione

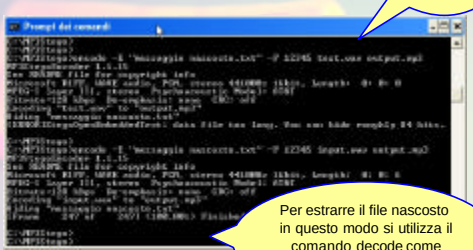
Per questo motivo, l'embedding deve essere effettuato nel processo di trasformazione da wav ad Mp3

Rilasciato nel 1998
Per ambienti Windows e Linux
e funziona come una shell

Steganografia audio: Mp3Stego



Steganografia audio: Mp3Stego



Steganografia nelle immagini: formato GIF

Le immagini, per le loro dimensioni e il loro comune utilizzo, sono ottime candidate per scopi steganografici

Il formato GIF fa uso di una palette di 256 colori, cioè un insieme di colori che formano l'immagine

I pixel non sono altro che puntatori ad uno dei colori della palette

Questo si traduce in un grosso risparmio di spazio nella rappresentazione del file

Steganografia nelle immagini: formato GIF

Una soluzione steganografica:

- Acquisire un'immagine
- Limitare il numero di colori utilizzati a 256
- Convertire in GIF riempiendo la parte restante della palette con dei colori molto simili a quelli rimasti
- Ogni volta che si dovrà rappresentare un colore si potrà scegliere di rappresentarlo o con il colore originale (0) oppure con il colore aggiunto simile all'originale (1)

Steganografia nelle immagini: formato GIF

Una soluzione steganografica:

- Acquisire un'immagine
- Lim
- Co ella palet
- Ogni volta che si dovrà rappresentare un colore si potrà scegliere di rappresentarlo o con il colore originale (0) oppure con il colore aggiunto simile all'originale (1)

È molto semplice scrivere un programma che analizzi la palette ed individui sottoinsiemi di colori simili e quindi la probabile presenza di un messaggio nascosto

Steganografia nelle immagini: formato GIF

Siccome non conta l'ordine con cui i colori sono memorizzati nella palette, **un'immagine GIF può essere rappresentata in 256! modi diversi**, purché venga cambiata opportunamente la sequenza dei puntatori

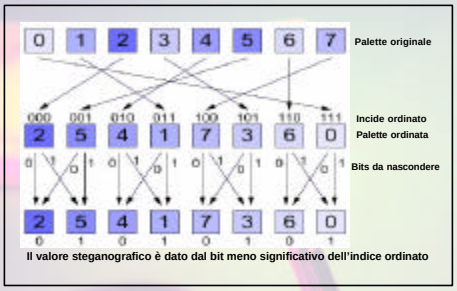
Quindi i bits che si possono nascondere sono **log(256!) = 1683 bit**, indipendentemente dalle dimensioni dell'immagine

Steganografia nelle immagini formato GIF: EzStego

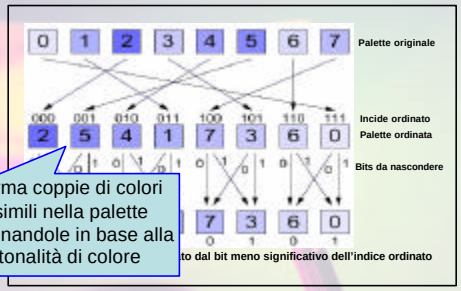
Il programma EzStego: sviluppato da Romana Machado nel 1996

- Lascia la palette inalterata (evita il problema precedente)
- Riesce a nascondere un bit di dati in ogni pixel di una data immagine

Steganografia nelle immagini formato GIF: EzStego

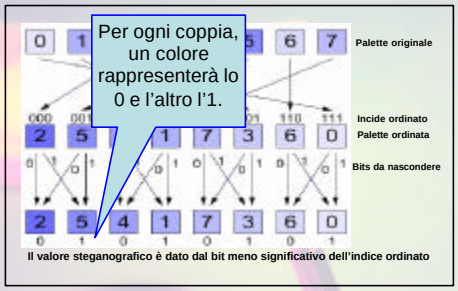


Steganografia nelle immagini formato GIF: EzStego



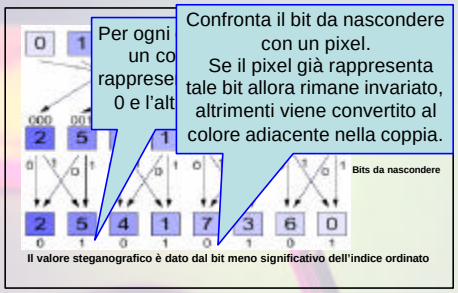
forma coppie di colori simili nella palette ordinandole in base alla tonalità di colore

Steganografia nelle immagini formato GIF: EzStego



Per ogni coppia, un colore rappresenterà lo 0 e l'altro l'1.

Steganografia nelle immagini formato GIF: EzStego



Per ogni un co rappres 0 e l'alt

Confronta il bit da nascondere con un pixel. Se il pixel già rappresenta tale bit allora rimane invariato, altrimenti viene convertito al colore adiacente nella coppia.

Steganografia nelle immagini formato GIF: EzStego

in correlazione con le capacità visive umane

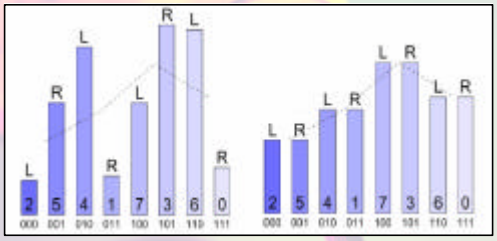
Questa tecnica si difende molto bene dagli ***attacchi visuali***

Gli ***attacchi statistici***, invece, riescono ad avere il soprevvento

Effettuano test statistici sul file stego

Steganografia nelle immagini formato GIF: EzStego

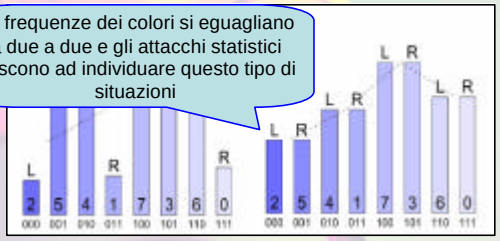
Ecco cosa succede agli istogrammi delle frequenze di colori prima e dopo l'embedding con EzStego.



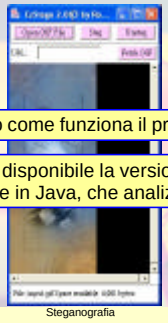
Steganografia nelle immagini formato GIF: EzStego

Ecco cosa succede agli istogrammi delle frequenze di colori prima e dopo l'embedding con EzStego.

Le frequenze dei colori si eguagliano a due a due e gli attacchi statistici riescono ad individuare questo tipo di situazioni



Steganografia nelle immagini formato GIF: EzStego 2.0

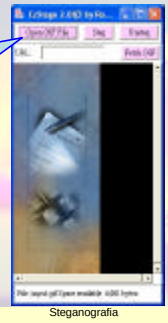


Vediamo come funziona il programma

In rete è disponibile la versione 2.0b3 sorgente in Java, che analizzeremo

Steganografia nelle immagini formato GIF: EzStego 2.0

Si sceglie il file GIF sul quale lavorare

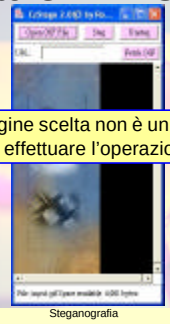


Steganografia nelle immagini formato GIF: EzStego 2.0

L'immagine viene visualizzata

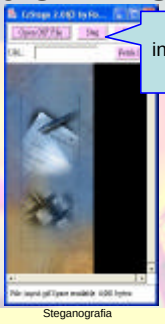
Steganografia nelle immagini formato GIF: EzStego 2.0

Se l'immagine scelta non è un file stego, bisogna effettuare l'operazione *Steg*



Steganografia nelle immagini formato GIF: EzStego 2.0

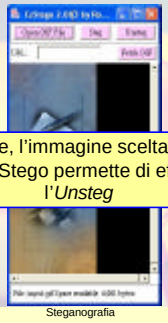
Si clicca su Steg per inserire il messaggio da nascondere



Steganografia nelle immagini formato GIF: EzStego 2.0

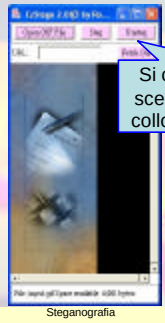
L'operazione viene effettuata con successo se le dimensioni del file da nascondere non superano la capacità del cover

Steganografia nelle immagini formato GIF: EzStego 2.0



Se, invece, l'immagine scelta è un file stego EzStego permette di effettuare l'*Unsteg*

Steganografia nelle immagini formato GIF: EzStego 2.0



Si clicca su Unsteg e si sceglie il percorso in cui collocare il file "scoperto"

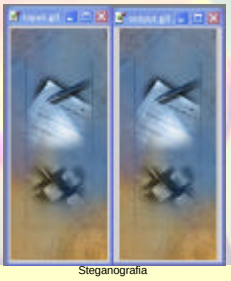
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento

Proviamo ad inserire un file di 1,5 Kb in un'immagine che ha una capienza massima di 6480 bytes.
Il messaggio nascosto rappresenta il 25% circa della capienza del cover.

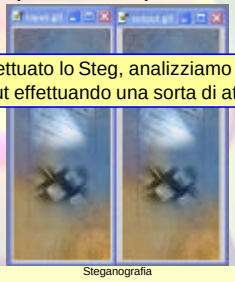
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



Dopo aver effettuato lo Steg, analizziamo il file di input e quello di output effettuando una sorta di attacco visuale.

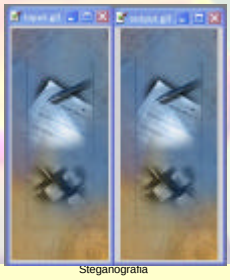
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento

A prima vista i due files sembrano identici

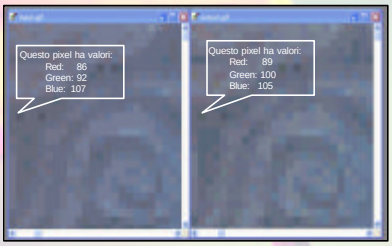
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



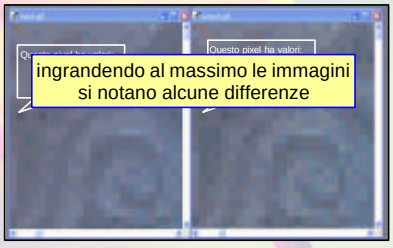
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



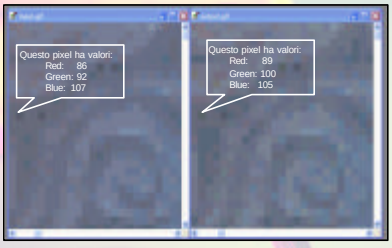
Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



Steganografia nelle immagini formato GIF: EzStego 2.0

Un piccolo esperimento



Steganografia nelle immagini: formato Jpeg

L'algoritmo di compressione Jpeg è **lossy**
- Mantiene le informazioni più importanti
- Scarta le informazioni meno significative dal punto di vista visivo

Questo è ciò che uno steganographer non vorrebbe mai vedere!

L'embedding deve essere effettuato in fase di compressione

Steganografia nelle immagini: formato Jpeg

La chiave della compressione è la DCT

DCT (discrete cosine transform) è un operatore matematico che cambia la natura della matrice fondamentale, convertendo un segnale dal dominio spaziale al dominio delle frequenze

I programmi steganografici non fanno altro che inserire informazioni laddove risiedono i coefficienti DCT meno importanti

Steganografia nelle immagini formato Jpeg: JSteg Shell

- Il programma riesce a nascondere un bit di dati segreti in ogni coefficiente non-zero
- Tutti i possibili valori dei coefficienti sono accoppiati ai valori simili e ad ognuno viene assegnato un 1 o uno 0
- Il coefficiente di ogni blocco viene poi cambiato per fissare lo stego bit

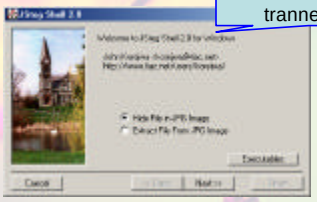
Steganografia nelle immagini formato Jpeg: JSteg Shell

I messaggi nascosti con JSteg non sono così vulnerabili come i file GIF agli attacchi visuali, ma, come EzStego, JSteg subisce il fatto che i coefficienti accoppiati tendono a bilanciarsi l'uno con l'altro, favorendo attacchi statistici

Steganografia nelle immagini formato Jpeg: JSteg Shell

L'utilizzo

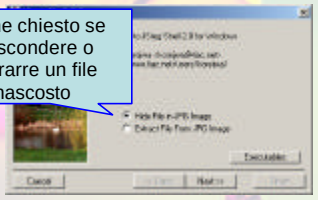
Funziona con tutte le versioni di Windows tranne la 2000



Steganografia nelle immagini formato Jpeg: JSteg Shell

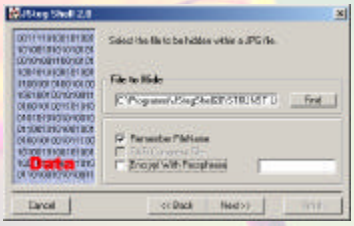
L'utilizzo

Viene chiesto se nascondere o estrarre un file nascosto



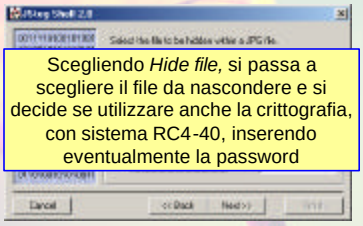
Steganografia nelle immagini formato Jpeg: JSteg Shell

L'utilizzo



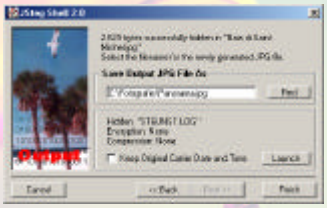
Steganografia nelle immagini formato Jpeg: JSteg Shell

L'utilizzo



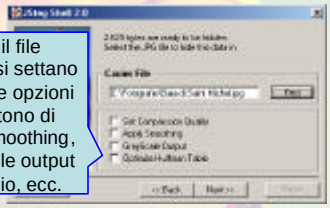
Scegliendo *Hide file,* si passa a scegliere il file da nascondere e si decide se utilizzare anche la crittografia, con sistema RC4-40, inserendo eventualmente la password

Steganografia nelle immagini formato Jpeg: JSteg Shell L'utilizzo



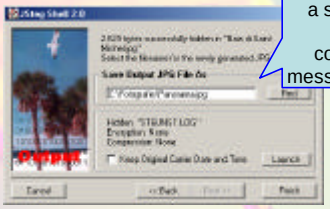
Steganografia nelle immagini formato Jpeg: JSteg Shell L'utilizzo

Si sceglie il file contenitore e si settano eventualmente opzioni che permettono di applicare lo smoothing, di produrre il file output in toni di grigio, ecc.



Steganografia nelle immagini formato Jpeg: JSteg Shell L'utilizzo

Infine si provvede a salvare il file prodotto, contenente il messaggio segreto



Steganografia nelle immagini formato Jpeg: JSteg Shell L'utilizzo

Infine si provvede a salvare il file

La funzione *Extract file* funziona in modo simile alla funzione Hide:

- si sceglie il file contenente il messaggio segreto
- si inserisce l'eventuale passphrase nel caso si sia utilizzata la crittografia
- si provvede a salvare il file segreto

Steganografia nelle immagini: formato BMP

Un immagine BMP, dal punto di vista digitale, è una matrice MxN di piccoli punti colorati detti pixel

Un file BMP true color a 24 bit è formato da pixels RGB

Un pixel RGB è formato da 3 byte ognuno dei quali rappresenta i livelli (da 0 a 255) dei colori primari (Red,Green e Blue) che costituiscono la tonalità di colore di quel determinato pixel

Steganografia nelle immagini: formato BMP

Un'operazione di steganografia sostitutiva su questo tipo di file consiste nel sostituire i bits meno significativi dei singoli byte con quelli del messaggio segreto

Ad occhio nudo, le variazioni di colore risultano praticamente **impercettibili**

Steganografia nelle immagini: formato BMP

Se abbiamo 3 bit di dati nascosti da inserire all'interno di questo pixel…

0 1 1

(11100001,00000100,00010111)

Steganografia nelle immagini: formato BMP

Se abbiamo 3 bit di dati nascosti da inserire all'interno di questo pixel…

(11100000,00000101,00010111)

Gli ultimi 3 bits del pixel vengono rimpiazzati

Steganografia nelle immagini: formato BMP

Per inserire un byte del messaggio segreto occorrono 8 byte del messaggio contenitore

In generale, per un file grafico MxN:
Dimensione messaggio segreto (in byte) = (M x N x 3) / 8

Steganografia nelle immagini: formato BMP

È possibile utilizzare i due, tre o quattro bits meno significativi di ogni byte, aumentando notevolmente la capacità del cover ma peggiorando la qualità dell'immagine stego che desterà più sospetti nell'attaccante

Si può procedere per tentativi e trovare un ragionevole compromesso

Steganografia nelle immagini formato BMP: BPCS Steganography

Sviluppata da Eiji Kawaguchi nel 1997

Tecnica che invece di considerare solo i bits meno significativi sceglie delle regioni dell'immagine nelle quali effettuare l'embedding senza alterare in modo significativo l'immagine

Steganografia nelle immagini formato BMP: BPCS Steganography

- L'immagine viene divisa in blocchi 8x8 pixels
- Su ogni blocco viene effettuato un test che ne determina la complessità
- Se la complessità è minore di una determinata soglia (parametro variabile dipendente dall'immagine) l'embedding può essere effettuato

Steganografia nelle immagini formato BMP: BPCS Steganography

Un'immagine RGB *P* può essere vista come:

P=(PR1,PR2,..,PRn,PG1,PG2,..,PGn,PB1,PB2,..,PBn),

Dove **PR1, PG1, PB1** è la bit-plan più significativa (immagine formata dai bit più significativi di tutti i pixels dell'immagine) e **PRn, PGn , PBn** è la bit-plan meno significativa

Steganografia nelle immagini formato BMP: BPCS Steganography

Più ci si allontana dalla bit-plan più significativa, più l'immagine diventa complessa

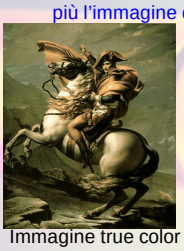


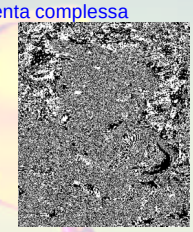
Immagine true color

PR3

Steganografia nelle immagini formato BMP: BPCS Steganography

Più ci si allontana dalla bit-plan più significativa, più l'immagine diventa complessa

PR4



PR5

Steganografia nelle immagini formato BMP: BPCS Steganography

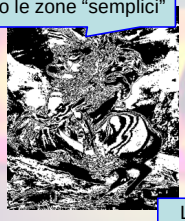
Ogni bit-plan viene divisa in regioni

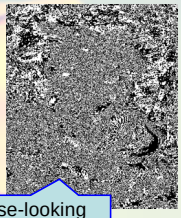
•Le regioni *shape-informative* non possono essere modificate perché contengono informazioni significative per l'immagine

•Le regioni *noise-looking* non contengono informazioni rilevanti e possono essere rimpiazzate

Steganografia nelle immagini formato BMP: BPCS Steganography

Le shape-informative sono le zone "semplici"





Le noise-looking sono le regioni più "complesse"

Steganografia nelle immagini formato BMP: Digital Picture Envelop

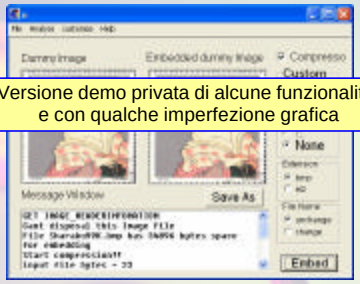
Software che usa la BPCS Steganography

Riesce a nascondere dati aventi dimensione fino al 50% di quella del cover (5-10 volte più degli altri software)

Ha due programmi: encoder e decoder

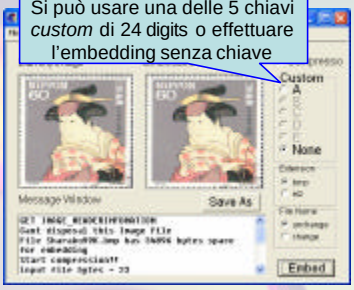
sviluppato dal Kit Digital Envelope Research Group

Steganografia nelle immagini formato BMP: Digital Picture Envelop



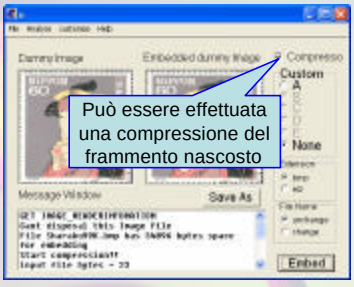
Steganografia nelle immagini formato BMP: Digital Picture Envelop

Steganografia nelle immagini formato BMP: Digital Picture Envelop

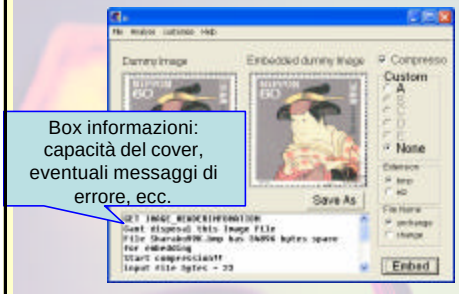


Steganografia nelle immagini formato BMP: Digital Picture Envelop

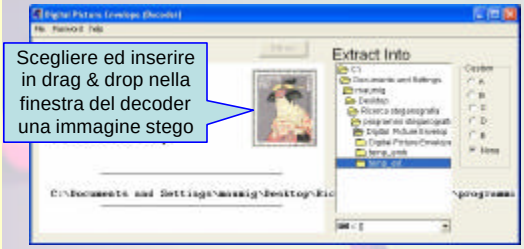
Steganografia nelle immagini formato BMP: Digital Picture Envelop



Steganografia nelle immagini formato BMP: Digital Picture Envelop

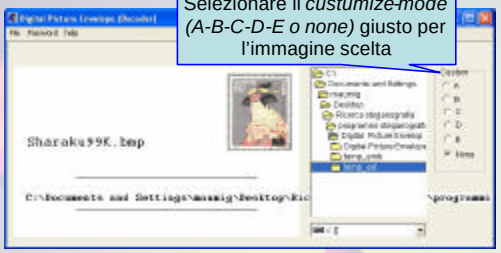


Steganografia nelle immagini formato BMP: Digital Picture Envelop



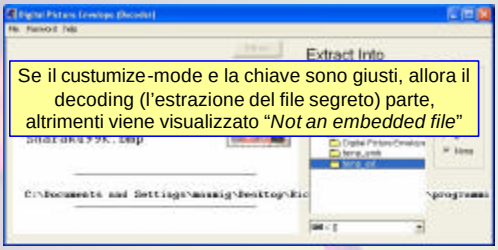
Scegliere ed inserire in drag & drop nella finestra del decoder una immagine stego

Steganografia nelle immagini formato BMP: Digital Picture Envelop



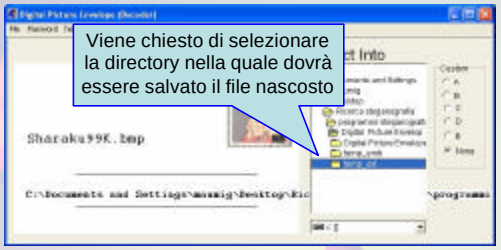
Selezionare il *custumize-mode (A-B-C-D-E o none)* giusto per l'immagine scelta

Steganografia nelle immagini formato BMP: Digital Picture Envelop



Se il custumize-mode e la chiave sono giusti, allora il decoding (l'estrazione del file segreto) parte, altrimenti viene visualizzato "*Not an embedded file*"

Steganografia nelle immagini formato BMP: Digital Picture Envelop



Viene chiesto di selezionare la directory nella quale dovrà essere salvato il file nascosto

Attacchi alle immagini

- ***Attacchi visuali***: sono in correlazione con le capacità visive umane
- ***Attacchi statistici***: effettuano test statistici sul file stego.

Attacchi alle immagini: attacchi visuali

- Il file stego viene filtrato con un algoritmo (di *filtering*) dipendente dalla funzione di embedding utilizzata per nascondere il messaggio
- L'immagine filtrata viene osservata per determinare se è stato nascosto un messaggio o meno

L'operazione risulta **lenta** se la mole di immagini da analizzare è considerevole

Attacchi alle immagini: attacchi visuali

Cover non modificato

Immagine stego che contiene un messaggio

Attacchi alle immagini: attacchi visuali

Cover filtrato

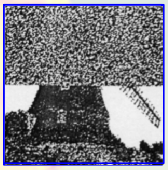
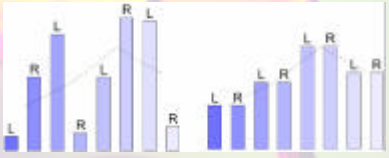


Immagine stego filtrata

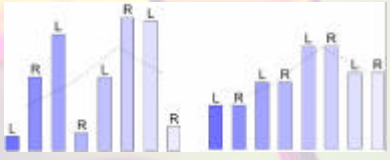
Attacchi alle immagini: attacchi statistici

L'idea dell'attacco statistico è di confrontare la distribuzione di frequenza dei colori di un potenziale file stego con la distribuzione di frequenza teoricamente attesa per un file stego



Attacchi alle immagini: attacchi statistici

In questo caso dopo l'embedding le frequenze si eguagliano a due a due



Attacchi alle immagini: attacchi statistici

Questo è il risultato dell'attacco statistico all'immagine vista in precedenza

Attacchi alle immagini: attacchi statistici

La prima parte dell'immagine nasconde dati segreti

La seconda parte non nasconde dati

Questo è il risultato dell'attacco statistico all'immagine vista in precedenza

Altri programmi steganografici
Steganos Security Suite 5

Il programma può essere scaricato gratuitamente in versione shareware.

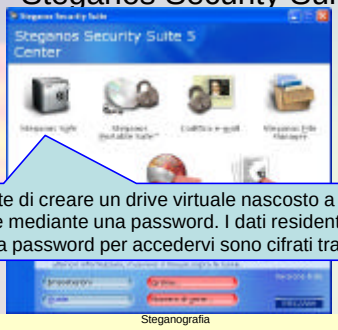
La versione 5 è per piattaforme Intel con sistema operativo Windows 95, 98, ME, NT 4.0 e 2000.

È una suite di strumenti per la sicurezza.

Sviluppato dalla DEMCOM di Francoforte in collaborazione con CenturionSoft di Washington

Altri programmi steganografici
Steganos Security Suite 5

Altri programmi steganografici
Steganos Security Suite 5

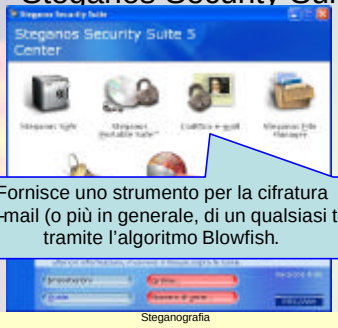


Permette di creare un drive virtuale nascosto a cui si può accedere mediante una password. I dati residenti su questo drive e la password per accedervi sono cifrati tramite AES.

Altri programmi steganografici
Steganos Security Suite 5

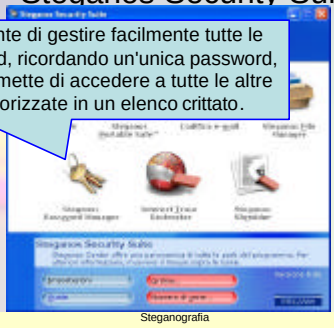
Portable Safe consente di trasportare i dati riservati in modo semplice e sicuro salvando i dati in un file crittato che viene poi masterizzato su un supporto dati, ad esempio un CD-R (W). Il tutto con l'uso di una password.

Altri programmi steganografici
Steganos Security Suite 5



Fornisce uno strumento per la cifratura delle e-mail (o più in generale, di un qualsiasi testo) tramite l'algoritmo Blowfish.

Altri programmi steganografici
Steganos Security Suite 5



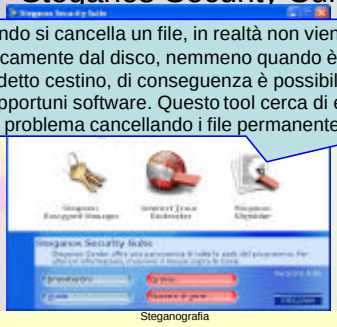
Consente di gestire facilmente tutte le password, ricordando un'unica password, che permette di accedere a tutte le altre memorizzate in un elenco crittato.

Altri programmi steganografici
Steganos Security Suite 5

Elimina le informazioni che memorizzano i browsers (cookies , cache, cronologia…).

Altri programmi steganografici
Steganos Security Suite 5

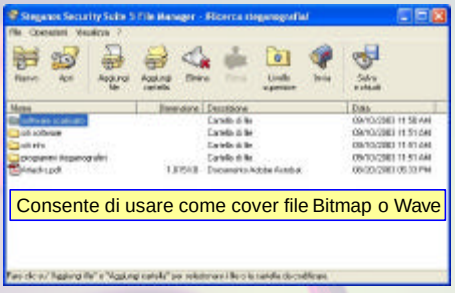
Quando si cancella un file, in realtà non viene cancellato fisicamente dal disco, nemmeno quando è svuotato il cosiddetto cestino, di conseguenza è possibile recuperarlo con opportuni software. Questo tool cerca di evitare questo problema cancellando i file permanentemente.



Altri programmi steganografici
Steganos Security Suite 5

La parte della suite che riguarda la steganografia più da vicino

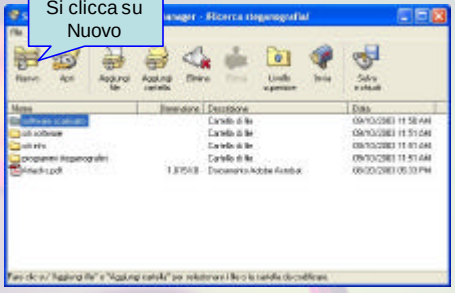
Altri programmi steganografici
Steganos Security Suite 5



Consente di usare come cover file Bitmap o Wave

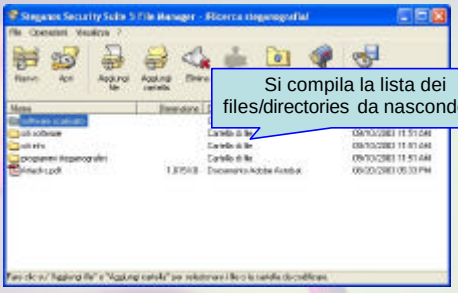
Altri programmi steganografici
Steganos Security Suite 5

Si clicca su Nuovo

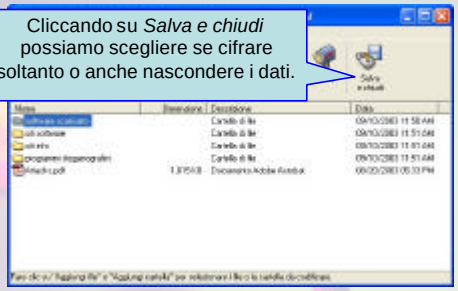


Altri programmi steganografici
Steganos Security Suite 5

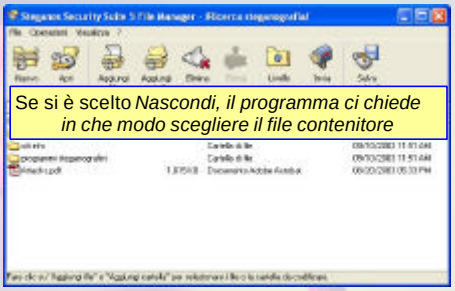
Si compila la lista dei files/directories da nascondere



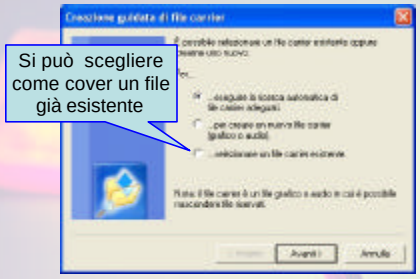
Altri programmi steganografici
Steganos Security Suite 5



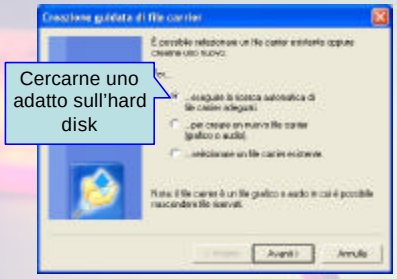
Altri programmi steganografici
Steganos Security Suite 5



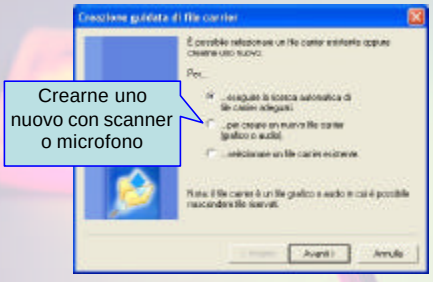
Altri programmi steganografici
Steganos Security Suite 5



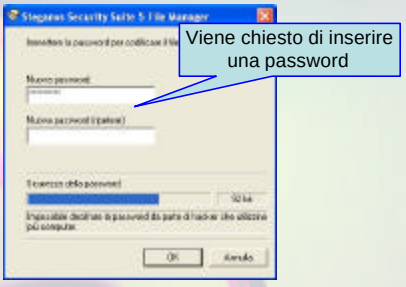
Altri programmi steganografici
Steganos Security Suite 5



Altri programmi steganografici
Steganos Security Suite 5



Altri programmi steganografici
Steganos Security Suite 5



Altri programmi steganografici
Steganos Security Suite 5

Per effettuare l'operazione inversa, cioè il recupero di dati nascosti, nella schermata principale basta cliccare su *Apri*, selezionare il file contenitore ed inserire la password opportuna

Anche in questo tool, come in tutti gli altri della suite, viene utilizzato l'algoritmo AES per la cifratura

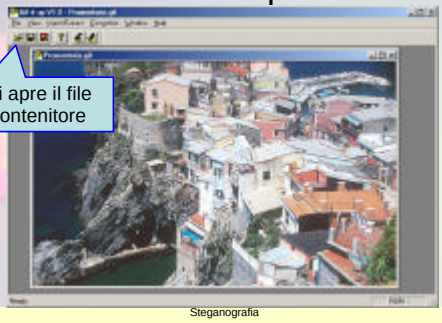
Altri programmi steganografici
Gif-it-up 1.0

Il programma supporta il formato GIF come contenitore.

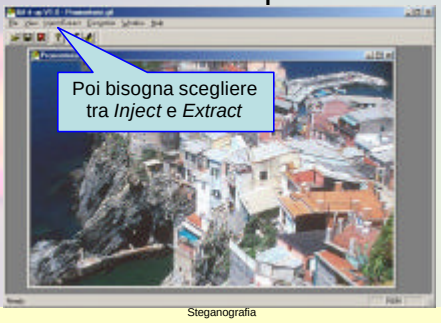
Funziona su tutte le versioni di Windows esclusa la 2000.

Realizzato nell'Università del Galles da Nelsonsoft e rilasciato nel 1998

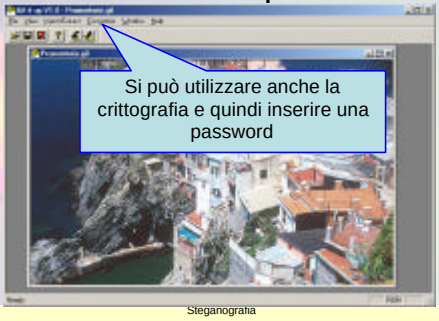
Altri programmi steganografici
Gif-it-up 1.0



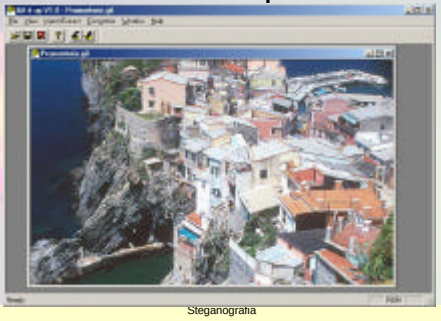
Altri programmi steganografici
Gif-it-up 1.0



Altri programmi steganografici
Gif-it-up 1.0



Altri programmi steganografici
Gif-it-up 1.0



Altri programmi steganografici
Gif-it-up 1.0

L'operazione di estrazione richiede semplicemente la password e ci permette di scegliere dove salvare il file estratto.