Steganografia

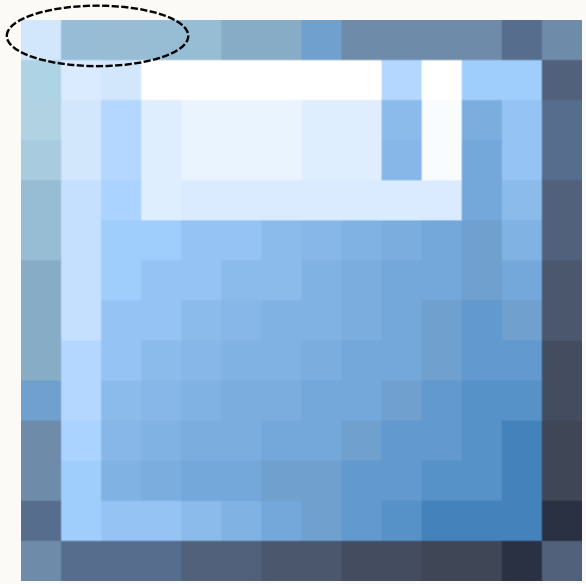
RICCARDO BASTIANINI
LAURA FERRONI
-
CORSO DI SICUREZZA INFORMATICA
-
UNIVERSITÀ DI PERUGIA

Che cos'è?

- Steganografia: scrittura nascosta
- Antica Grecia: tavolette di cera
- Inchiostro simpatico
- Codice morse sulla lana di indumenti

Steganografia con immagini

01110110011001010110010001101001011
00001011011010.1101111011000110110 10
vediamoci alle 12
01001000000110000101101100011011 0
00110010100100000001100010011001 0

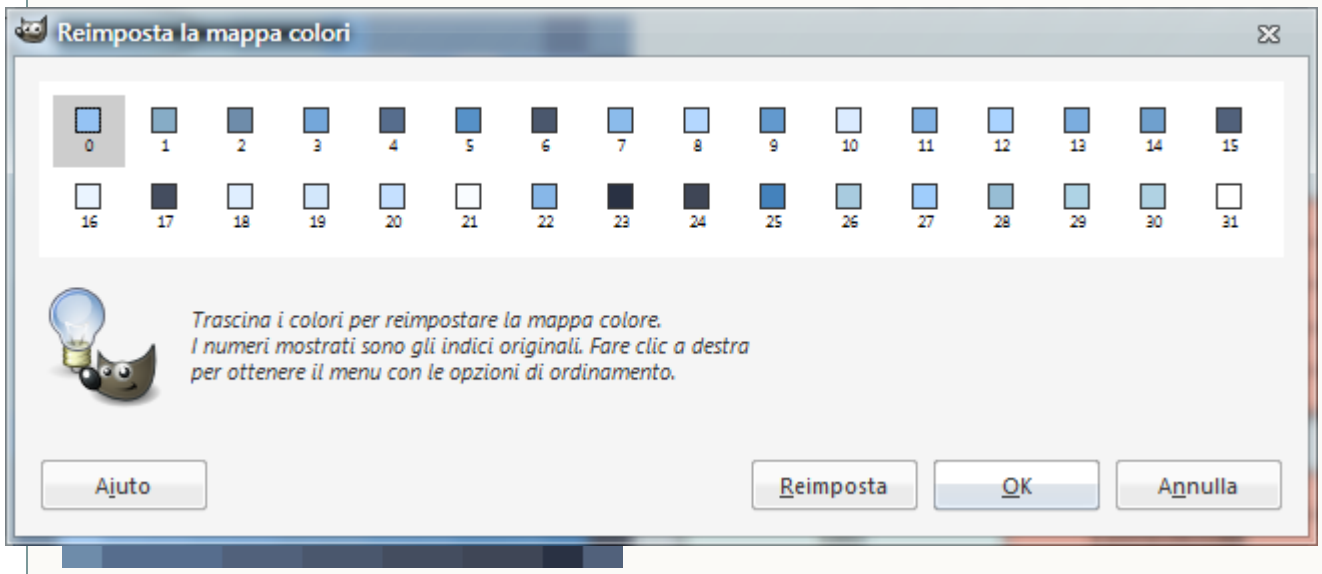


Pixel	ROSSO	VERDE	BLU
00	11010010	11100111	11111011
01	10010111	10111101	11010100
02	10010111	10111101	11010100
03	10010111	10111101	11010100

Pixel	ROSSO	VERDE	BLU
00	1101001**0**	1110011**1**	1111101**1**
01	1001011**1**	10111101**0**	1101010**1**
02	1001011**1**	1011110**0**	1101010**0**
03	1001011**1**	1011110**1**	1101010**0**

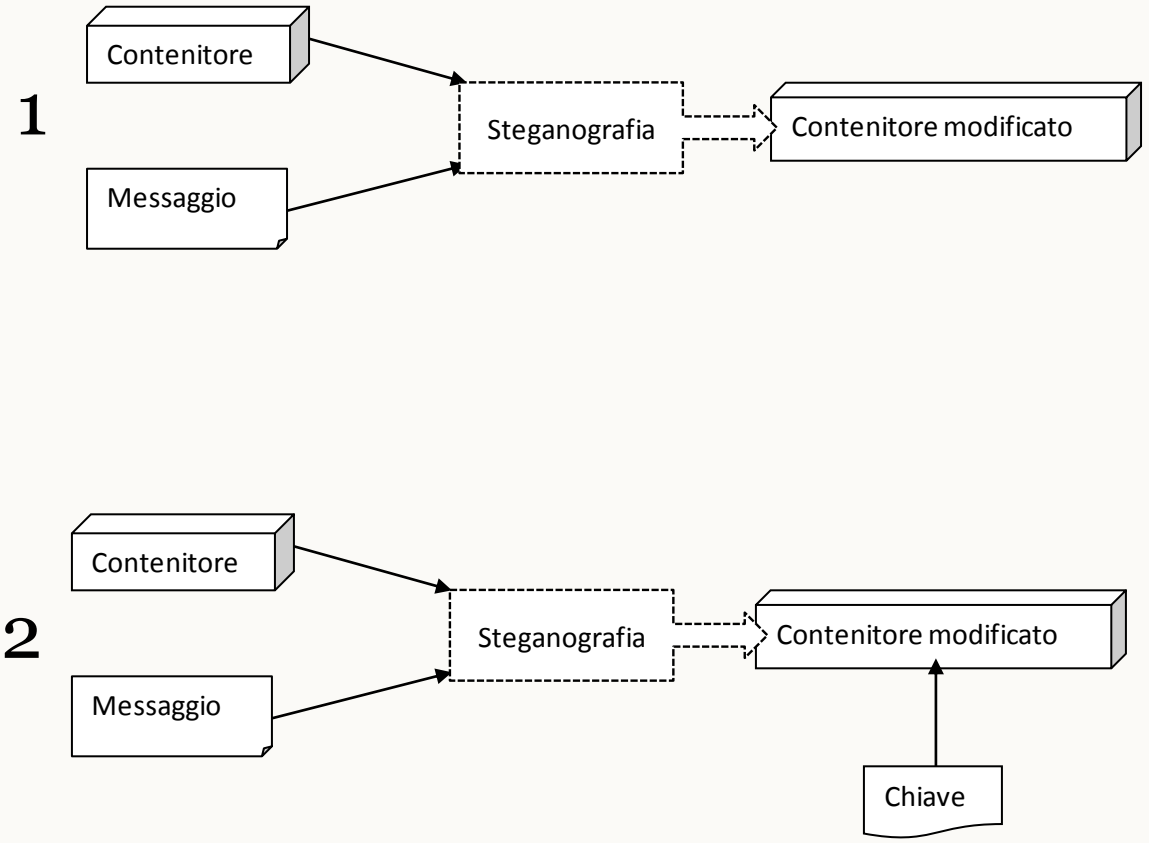
Steganografia con immagini indicizzate

Indice	ROSSO	VERDE	BLU
0	11010010	11100111	11111011
1	10010111	10111101	11010100
2	1101111	10100000	11001110



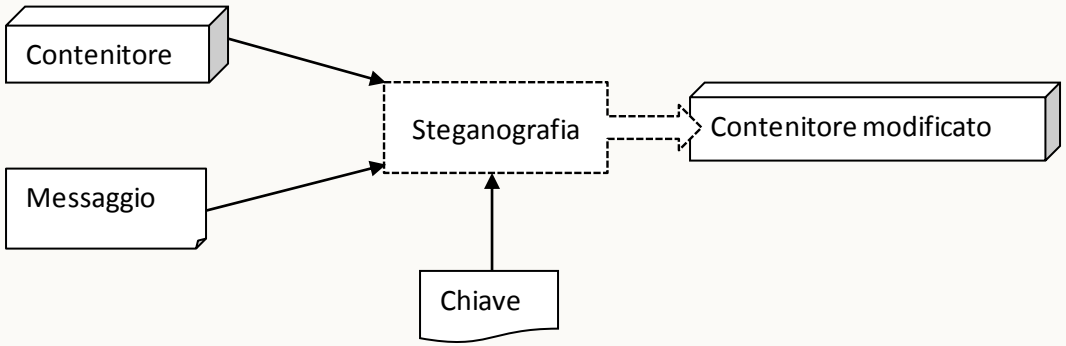
- Bit meno significativo
- Riordinare la palette
- Aggiungere colori inutili
- …

Livelli di protezione

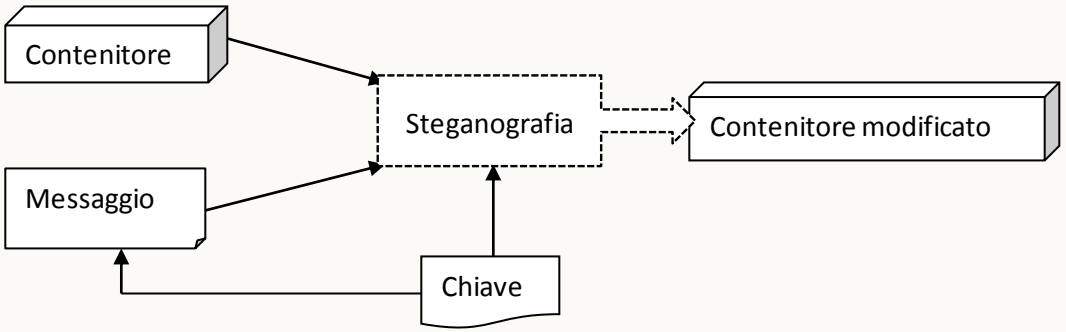


Livelli di protezione

3

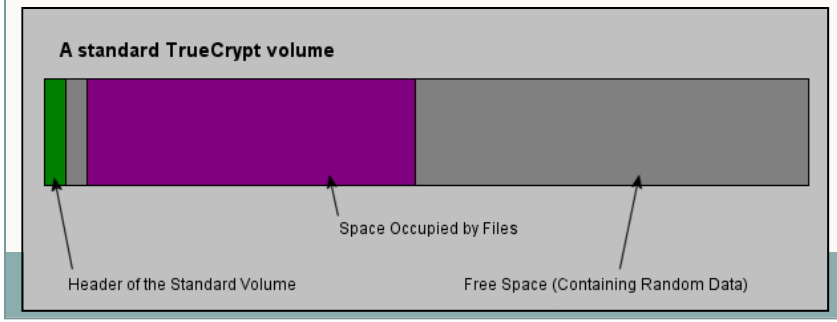


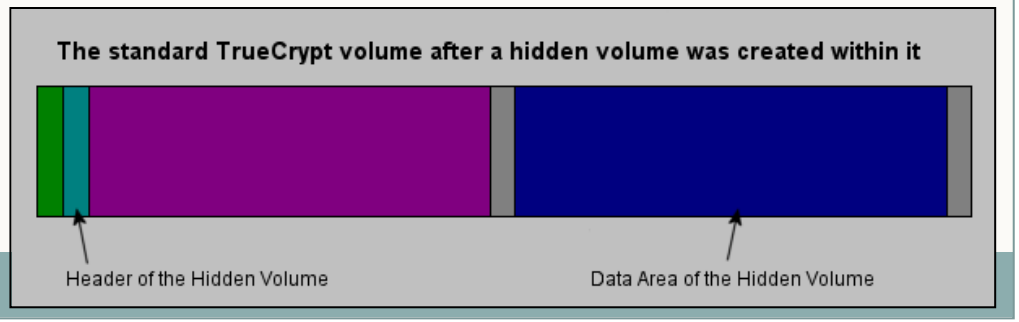
4



Altri esempi

- Blog-steganography
  - Nascondere messaggi in commenti a blog o in messaggi di forum
  - Messaggi nascosti negli avatar nei forum e nelle foto degli annunci eBay
- Steganografia all'interno di dati casuali o crittografati
  - TrueCrypt nasconde un archivio crittografato dentro un altro archivio crittografato.





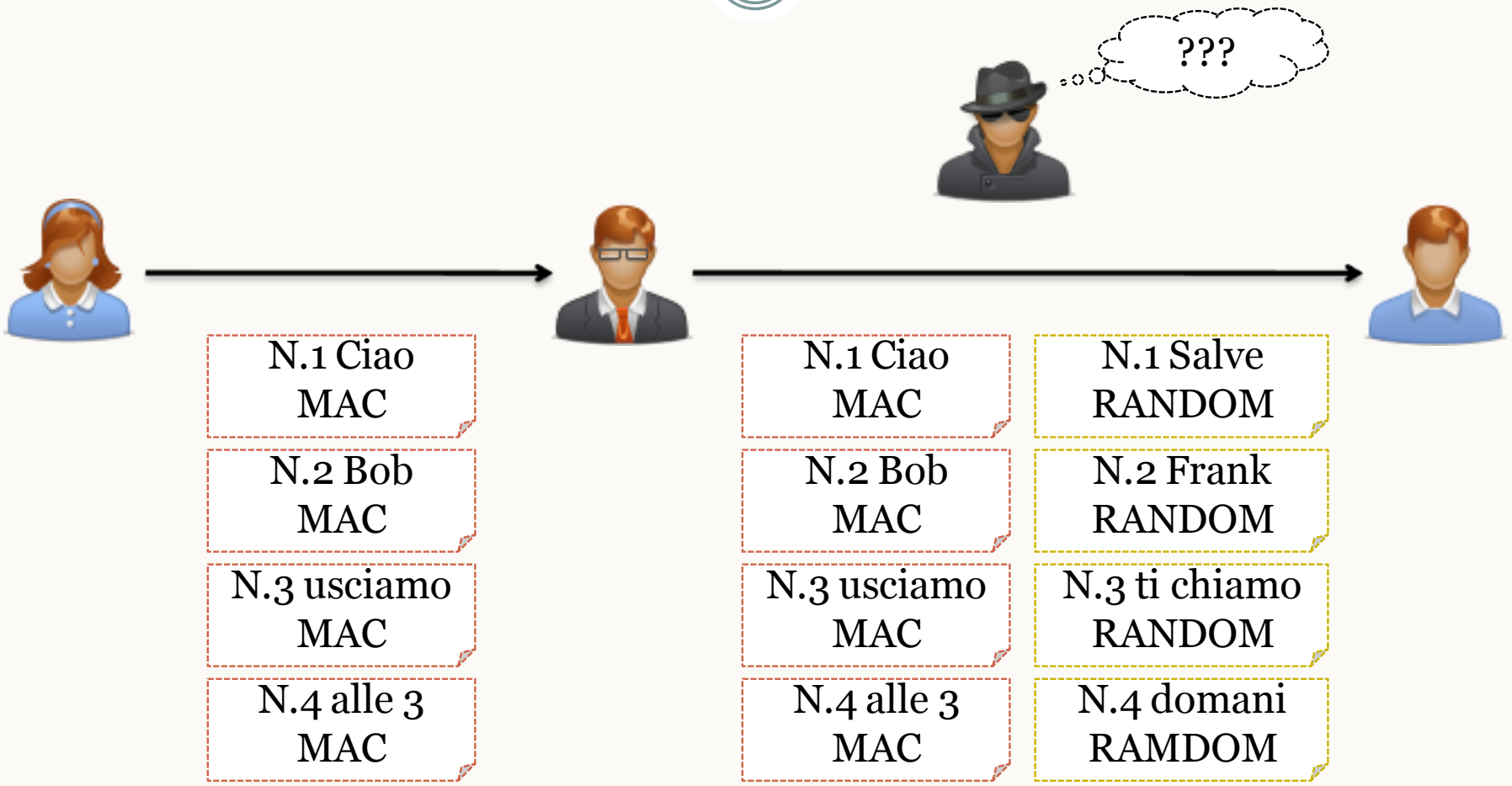
Steganografia di rete

- Modifica del contenuto dei pacchetti di un protocollo
- Ritardo dei pacchetti di un protocollo
- Entrambe le tecniche
- Utilizzo di più protocolli contemporaneamente
- Confidenzialità senza crittografia: Chaffing and Winnowing

Chaffing and Winnowing

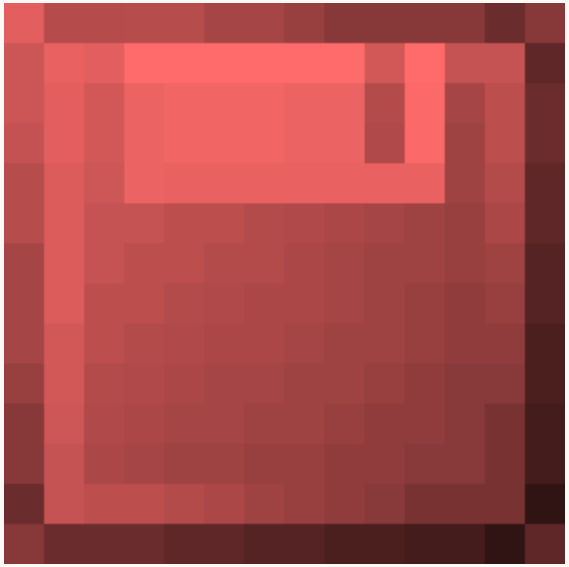
NUM_MESSAGGIO | BIT | MAC(NUM_MESSAGGIO,BIT,)

Chaffing and Winnowing



Steganografia e Watermarking

- Marchio impresso in forma esplicita o nascosta
  - Proprietà
  - Integrità
  - Identificazione fughe di informazioni



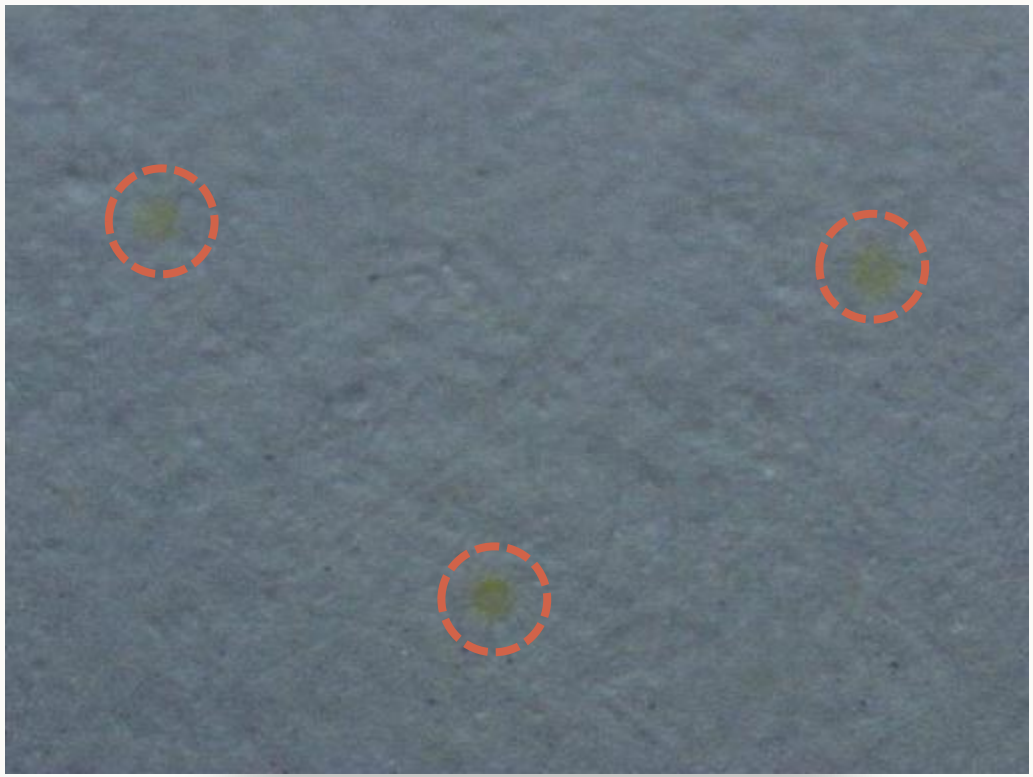
Canary Trap Printer steganography

Coded Anti Piracy (CAP)

Steganografia e Watermarking

- Printer steganography

Canon, Dell, Epson, Xerox, IBM, Lexmark, Panasonic, Samsung, Toshiba. Fuji ...

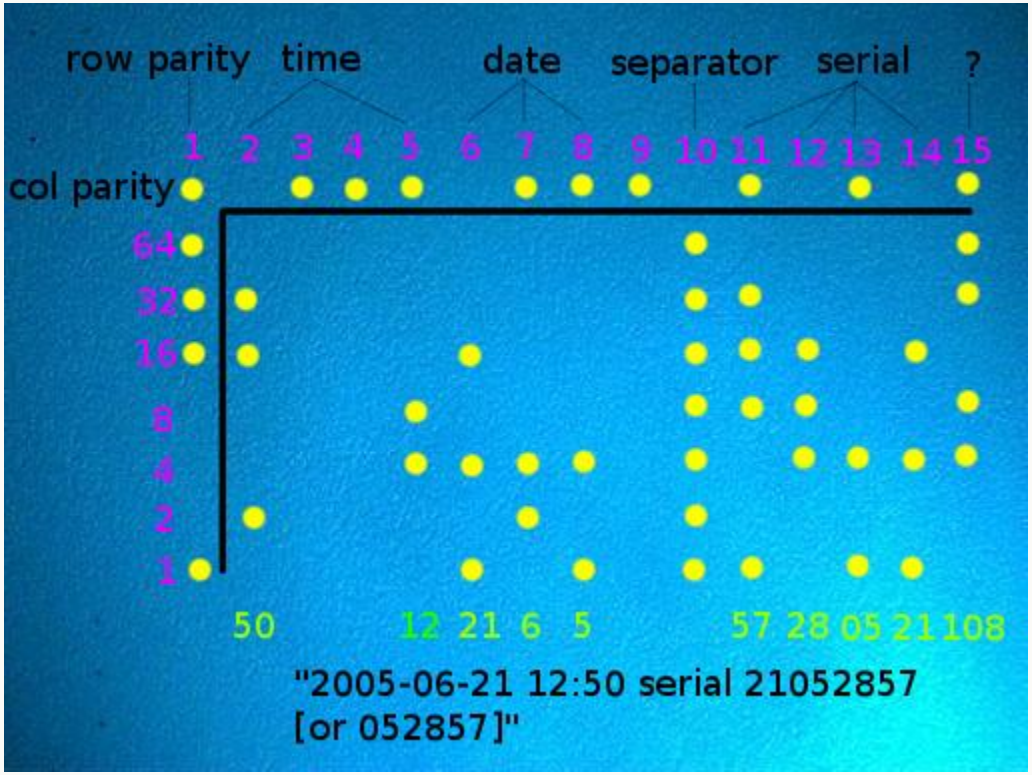


60x zoom

Steganografia e Watermarking

- Printer steganography

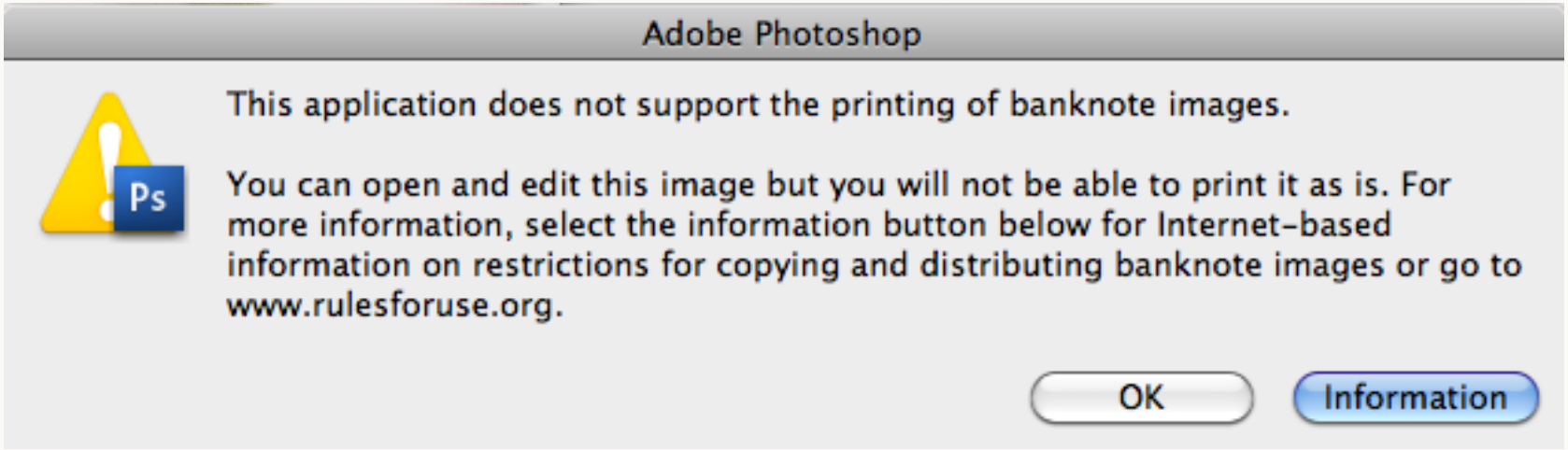
Canon, Dell, Epson, Xerox, IBM, Lexmark, Panasonic, Samsung, Toshiba. Fuji ...



10x zoom + luce blu

Steganografia e Watermarking

- Stampanti, fotocopiatrici e scanner smettono di funzionare quando si lavora con le banconote.



Steganografia e Watermarking

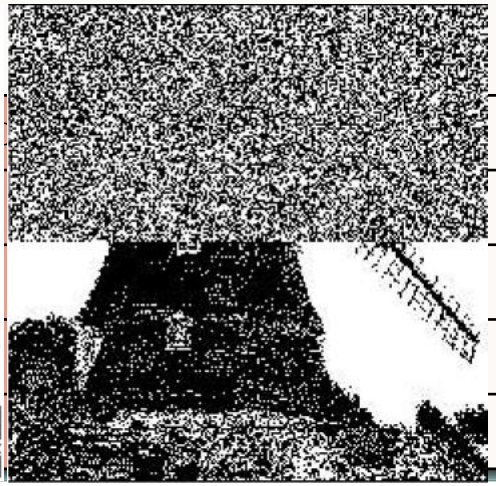
Steganalisi

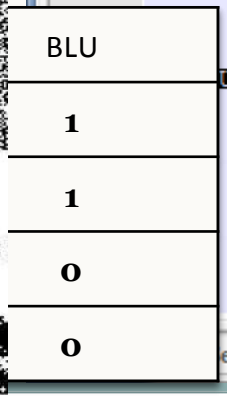
Individuazione messaggi nascosti

- Analisi visuale/uditiva,
- Confronto delle proprietà dei file con gli originali,
- Ricerca di tracce nel sistema dell'utente,
- Analisi statistica,
- Ricerca di firme.

Analisi visuale/uditiva

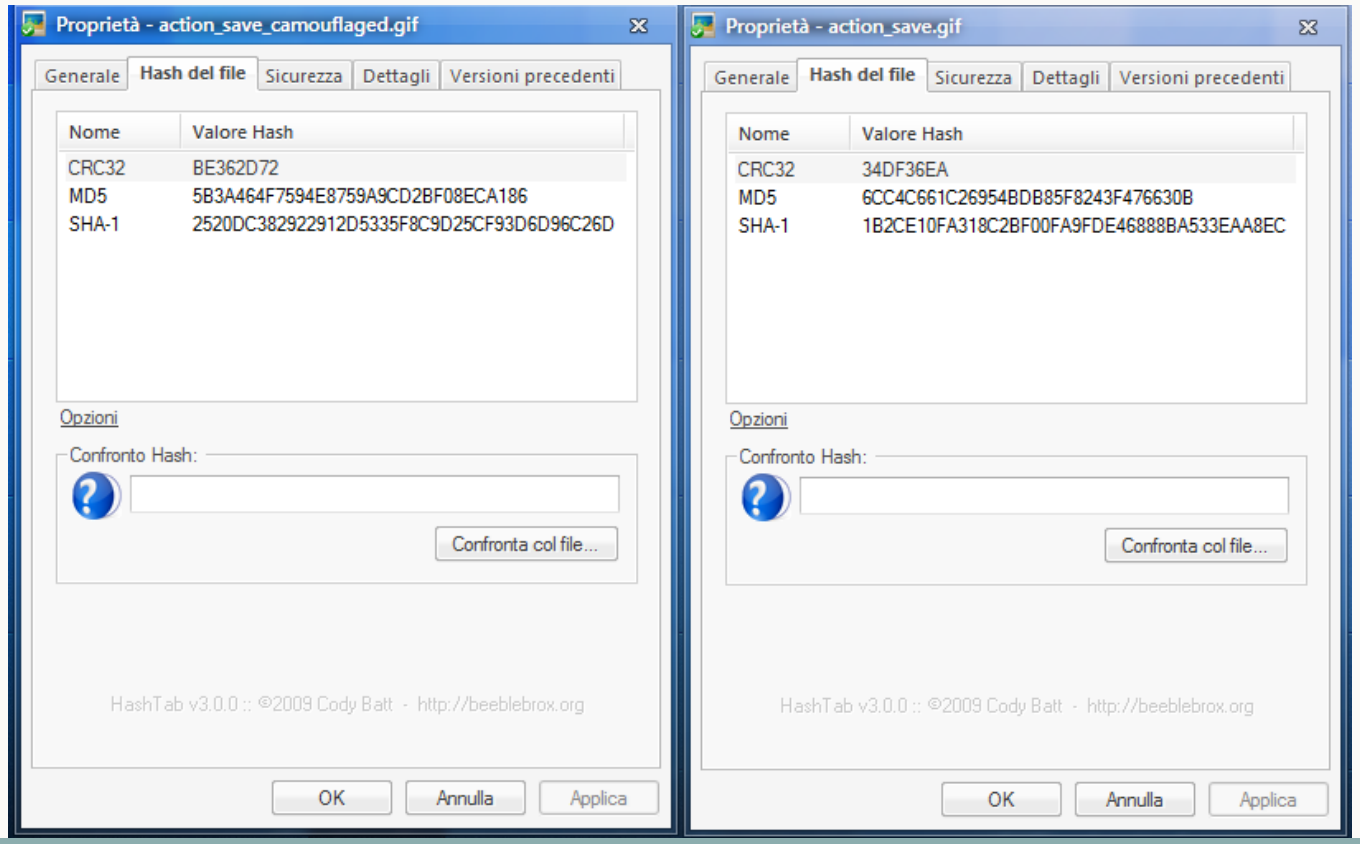
- Contenitori inadatti
- Troppe informazioni
- Riduzione del contenitore alla sola parte soggetta a modifica



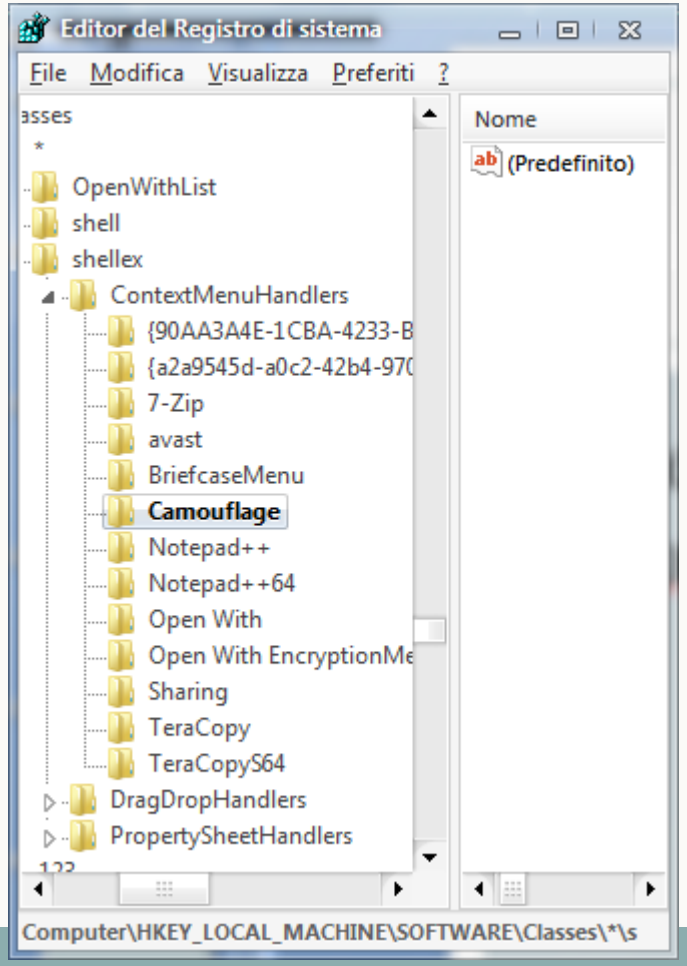


Confronto delle proprietà dei file

- Verifica degli attributi (dimensione,data di modifica, hash…) con originali noti



Ricerca di tracce nel sistema dell'utente



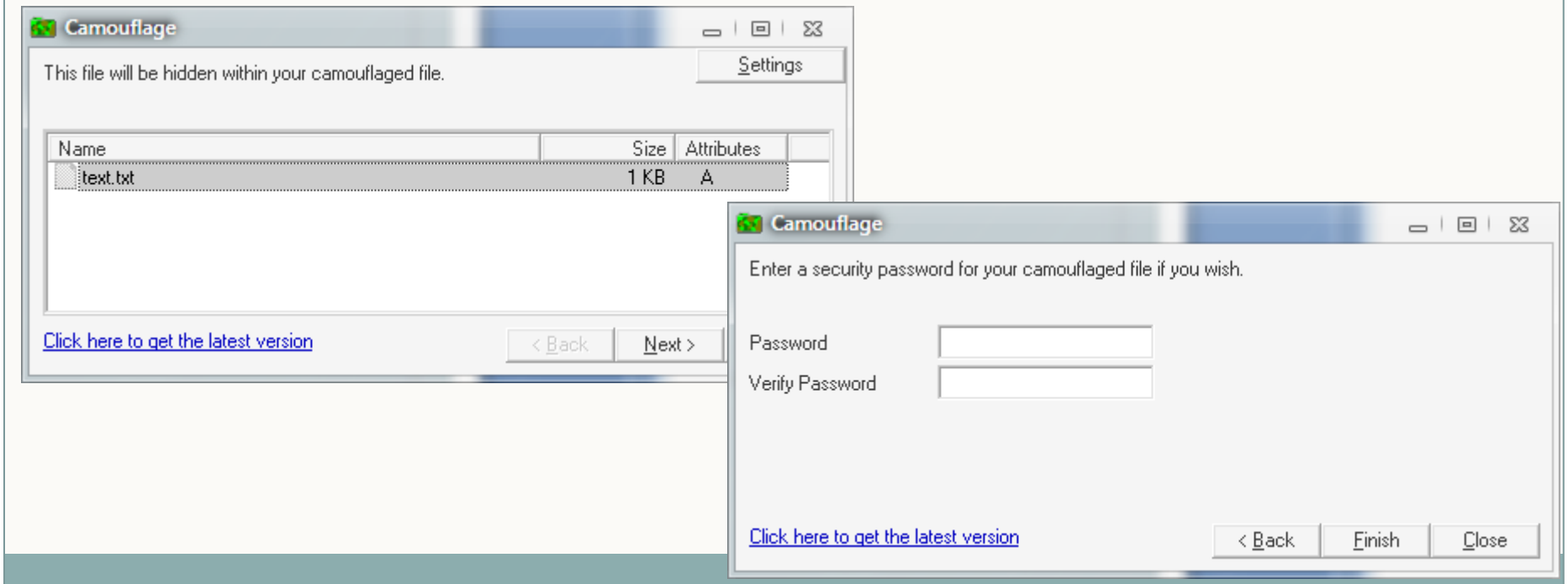
- Ricerca di tracce nel sistema dell'utente
  - File temporanei
  - Chiavi di registro
  - Copie doppie di file (con attributi diversi)

Ricerca di firme

- Firma: modifica sistematica ai file contenitore dipendente esclusivamente dal programma di steganografia utilizzato.
  - Una firma indica chiaramente la presenza di contenuto segreto
  - La firma indica anche il software utilizzato
  - Conoscere il software potrebbe permettere di recuperare il contenuto

Camouflage

- Software di steganografia gratuito per Windows
- Closed source
- Rilascio intorno all'anno 2000



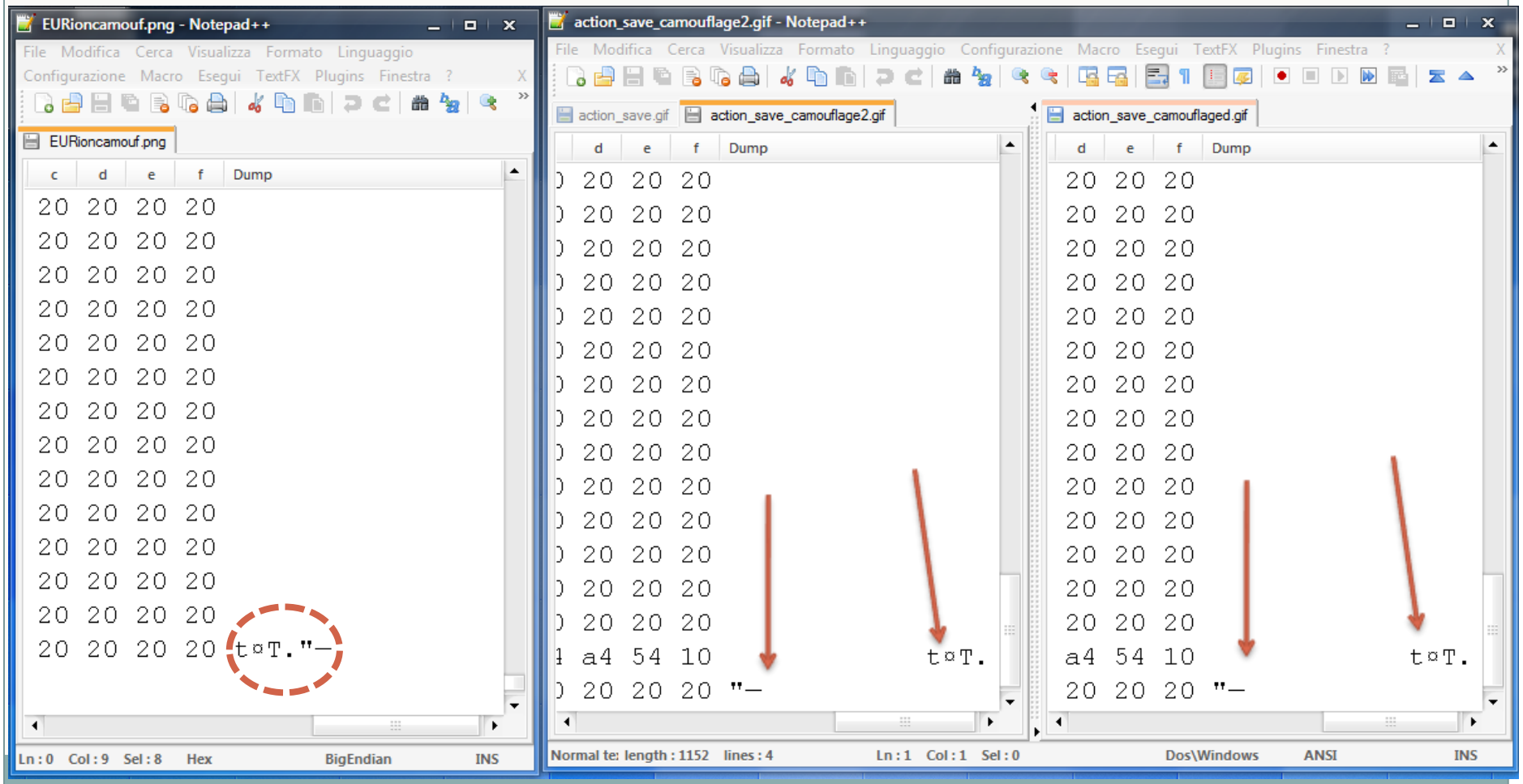
Il funzionamento di Camouflage

- Nessuna restrizione di formato per il contenitore
  - Improbabile presenza di tecniche ad-hoc per qualche formato
- Nessuna restrizione di dimensione per il contenitore
  - Come può il contenitore essere piccolo a piacere?
- Nessuna restrizione di dimensione e numero di file da nascondere
  - Come può il contenuto essere grande a piacere?

Cerchiamo di capire com'è possibile tutto questo analizzando i file output

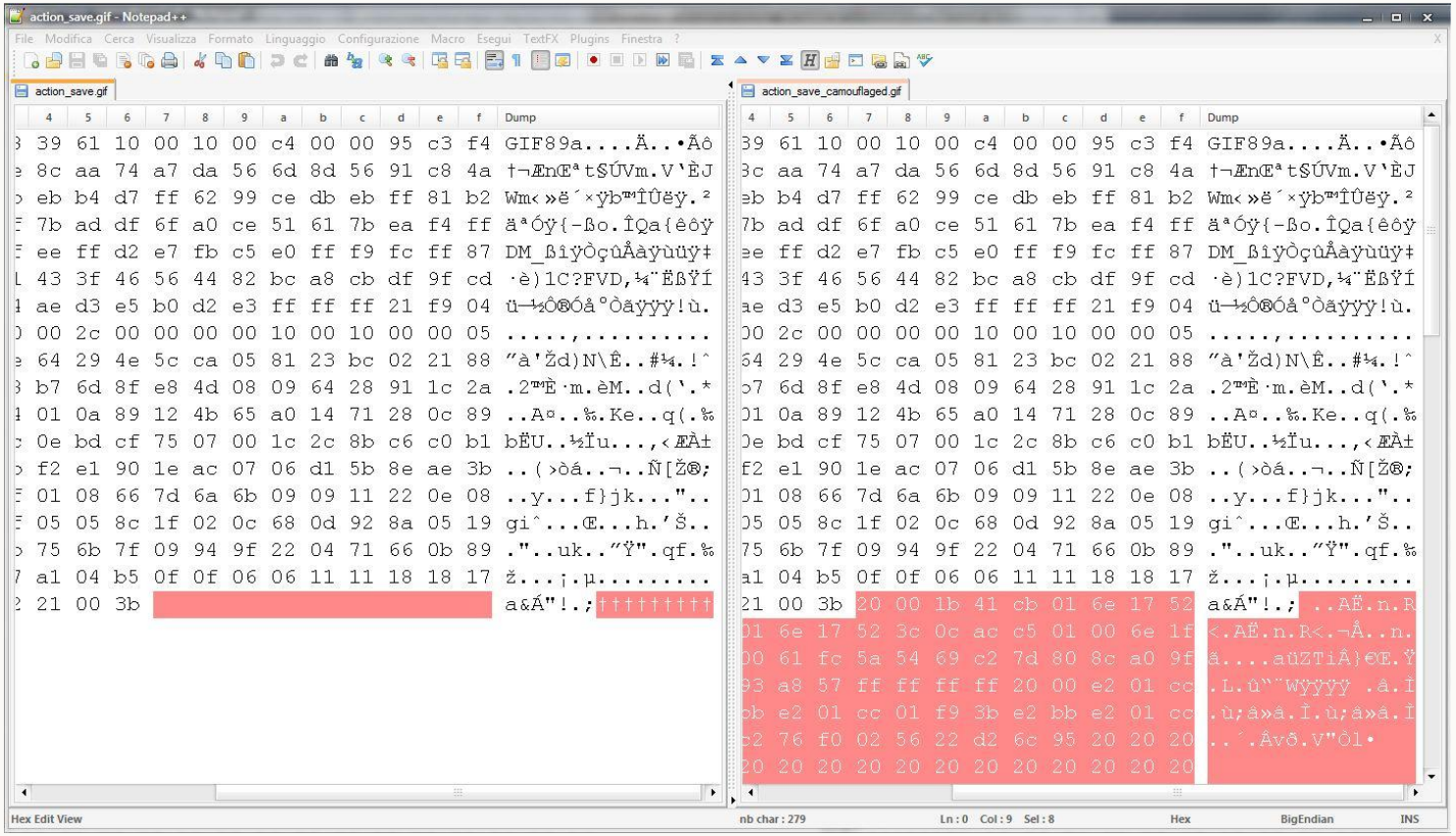
La firma di Camouflage

- Confronto tra diverse immagini modificate per individuare una firma



Metodo di embedding

- Differenze tra un file originale ed uno modificato



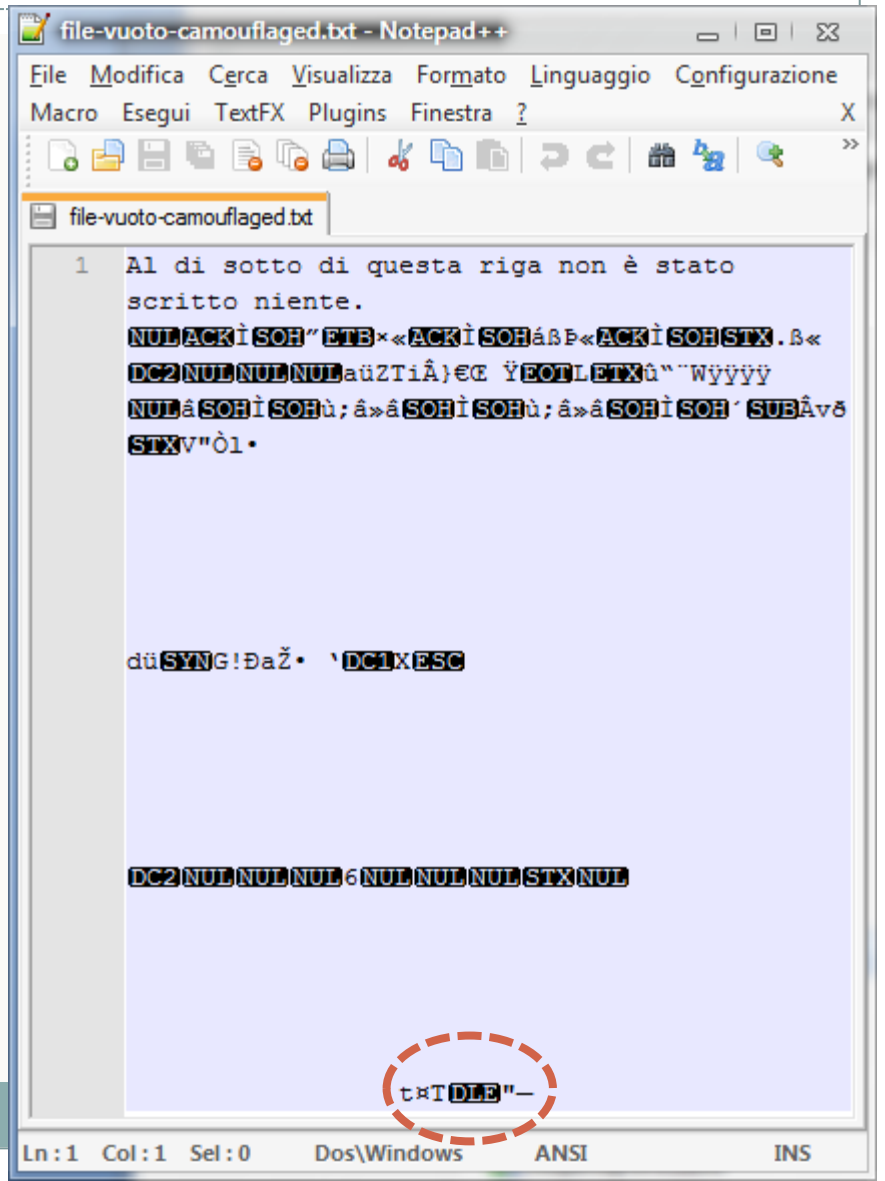
Nessuna modifica all'immagine: vengono solo aggiunti dei dati!

Metodo di embedding

- I dati da inglobare nel contenitore vengono aggiunti in coda
  - Inserire più file
  - Inserire file più grandi del contenitore
- Molti formati file hanno dei delimitatori di sezione all'interno
  - I dati considerati dai programmi di visualizzazione/modifica sono quelli PRIMA del delimitatore di fine file
  - Camouflage aggiunge dati IN FONDO al file

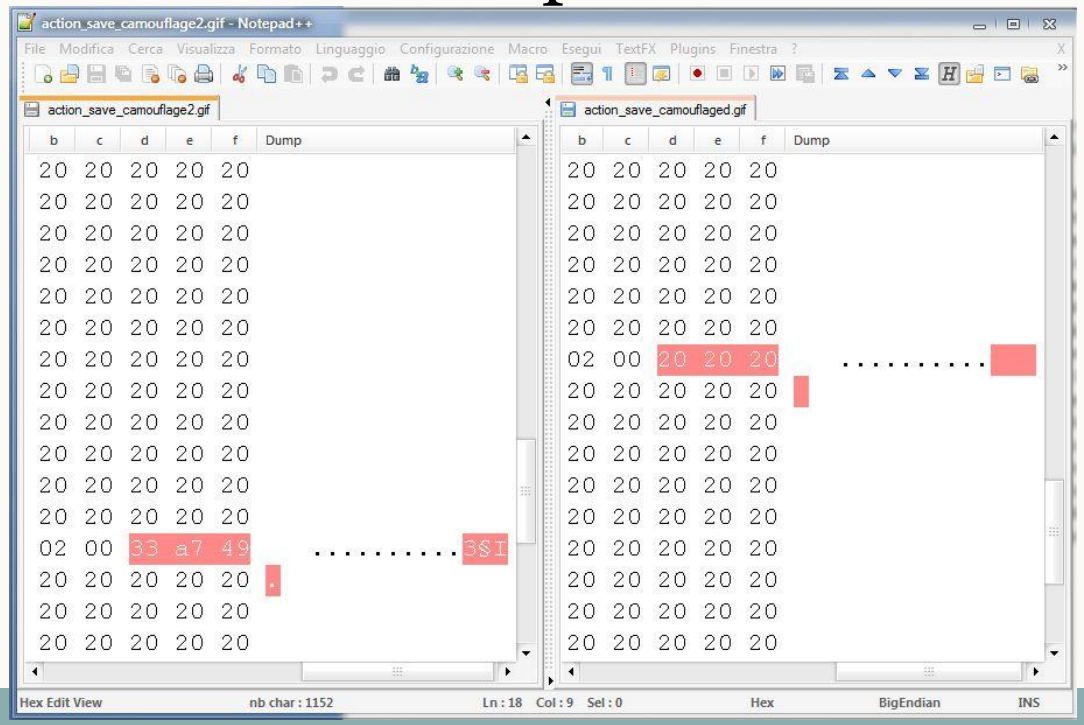
Metodo di embedding

- Non è sempre vero!
- E’ bene utilizzare tecniche diverse a seconda del tipo di contenitore
  - Per file testuali, si possono aggiungere spazi, ritorni a capo e caratteri di tabulazione in modo quasi invisibile per l’utente.



Metodo di embedding

- I dati inseriti non sono in chiaro
  - Anche se l'utente non inserisce nessuna password.
- Cosa succede nascondendo lo stesso messaggio nello stesso contenitore con due password diverse?



Metodo di embedding

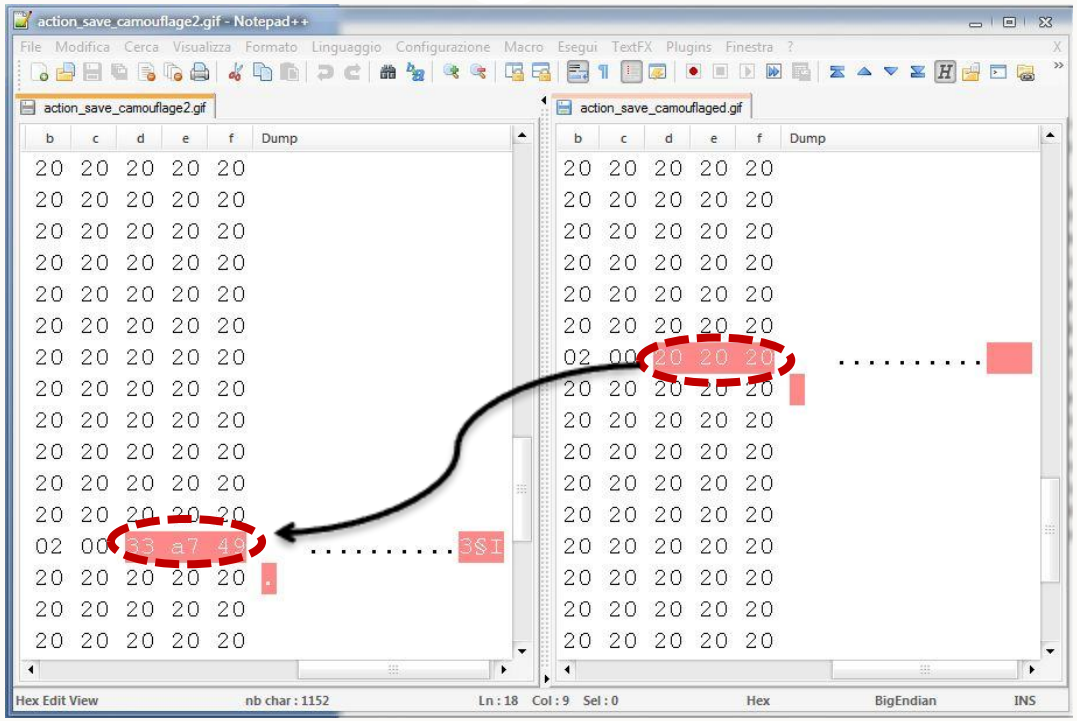
- I file sono quasi identici!
  - La codifica dei contenuti non dipende dalla password inserita
  - La password viene scritta nel file e controllata al momento dell'estrazione del contenuto
    - Potremmo modificare il codice assembly di Camouflage per saltare il controllo della password!

Infrangere la sicurezza

- Si può fare ancora di meglio!
  - La password deve essere salvata in una posizione costante (o comunque calcolabile) della porzione di dati aggiunta
  - Se si individua la posizione, è possibile rimuovere la password direttamente dal file (più facile)!

Infrangere la sicurezza

Contenuto binario nel file con password



Serie di spazi nel file senza password

Inserendo gli spazi al posto del contenuto binario si rimuove la password!

Attacchi basati su analisi statistiche delle immagini

Sicurezza di un metodo steganografico

- E' influenzata dai seguenti fattori:
  - Scelta del formato dell'immagine,
  - Scelta del contenuto dell'immagine
- Principio di Kerckhoff
  - In un sistema crittografico sicuro, se la chiave è confidenziale, l'algoritmo (crittografico) può essere pubblico.
- L'utilità di una definizione di "sicurezza" nella steganografia è limitata.
  - Lo scopo è di non essere rilevabile
  - Infinita scelta di immagini

LSB Embedding

LSB = Least Significant Bit

GIF

Indice della palette

BMP in scala di grigi 8-bit

Gradazione di grigio

JPEG

Coefficiente DCT

LSB Embedding

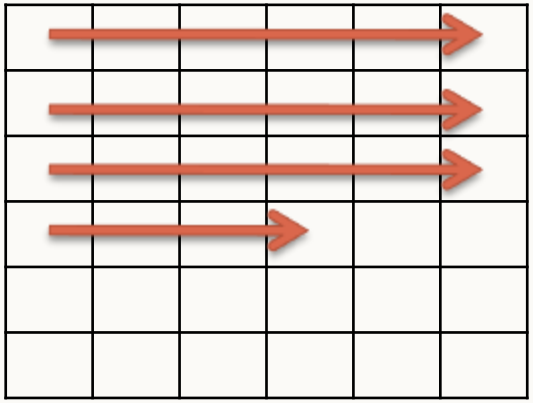
- LSB Replacement
  - I bit del messaggio sostituiscono gli LSB dell'immagine.
  - In tal caso viene modificato solo il LSB Plane.

Bit Plane = Successione dei bit che hanno la stessa posizione nei rispettivi numeri binari.

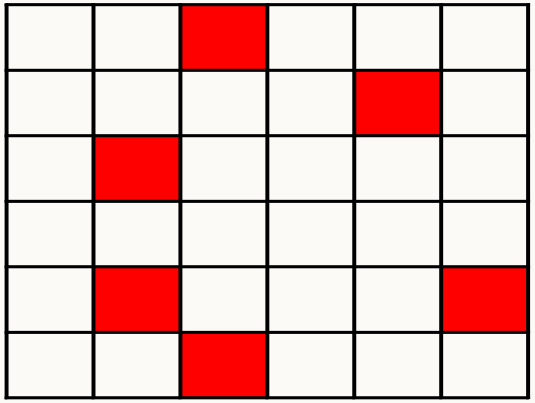
- LSB Matching
  - Si fa corrispondere il LSB del valore del valore di ciascun pixel al bit del messaggio da inserire.
  - Si incrementa o decrementa di 1 il valore del pixel di supporto.

Embedding

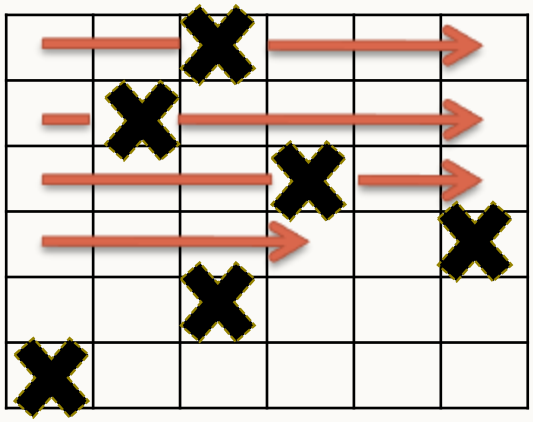
- Sequenziale



- Pseudo-random



- Selettiva



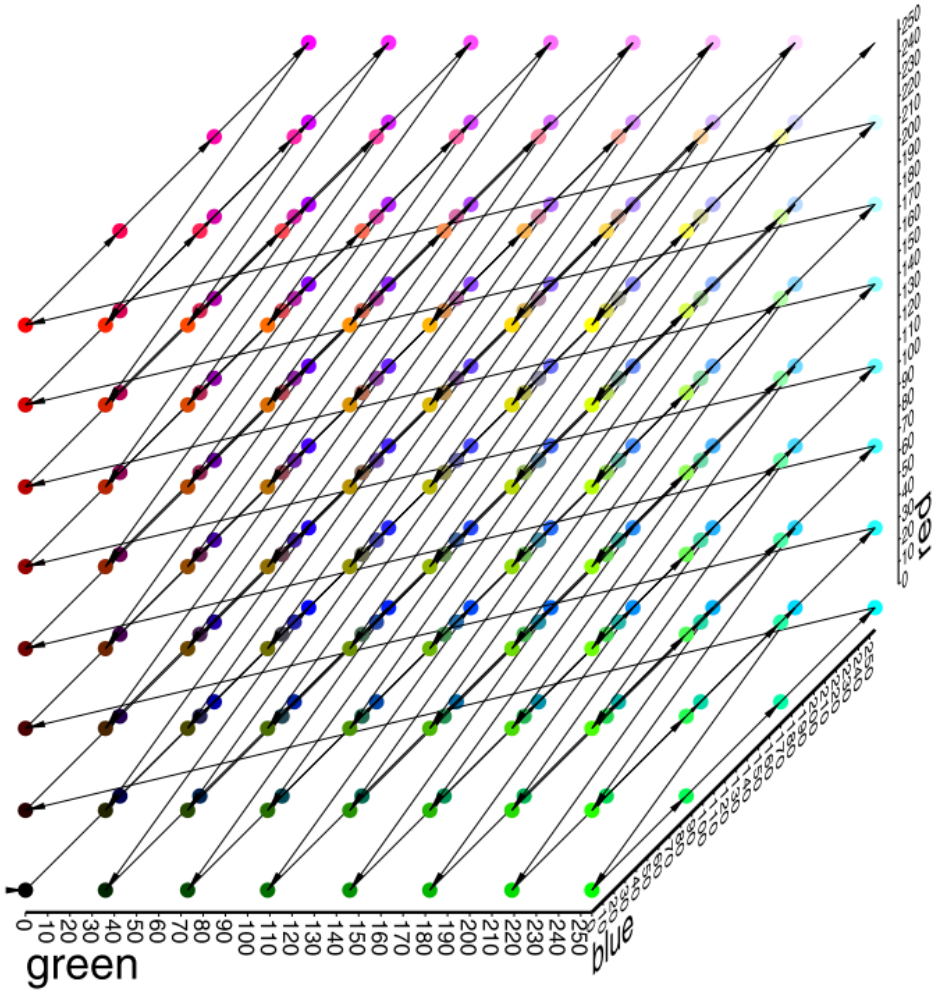
Attacchi statistici

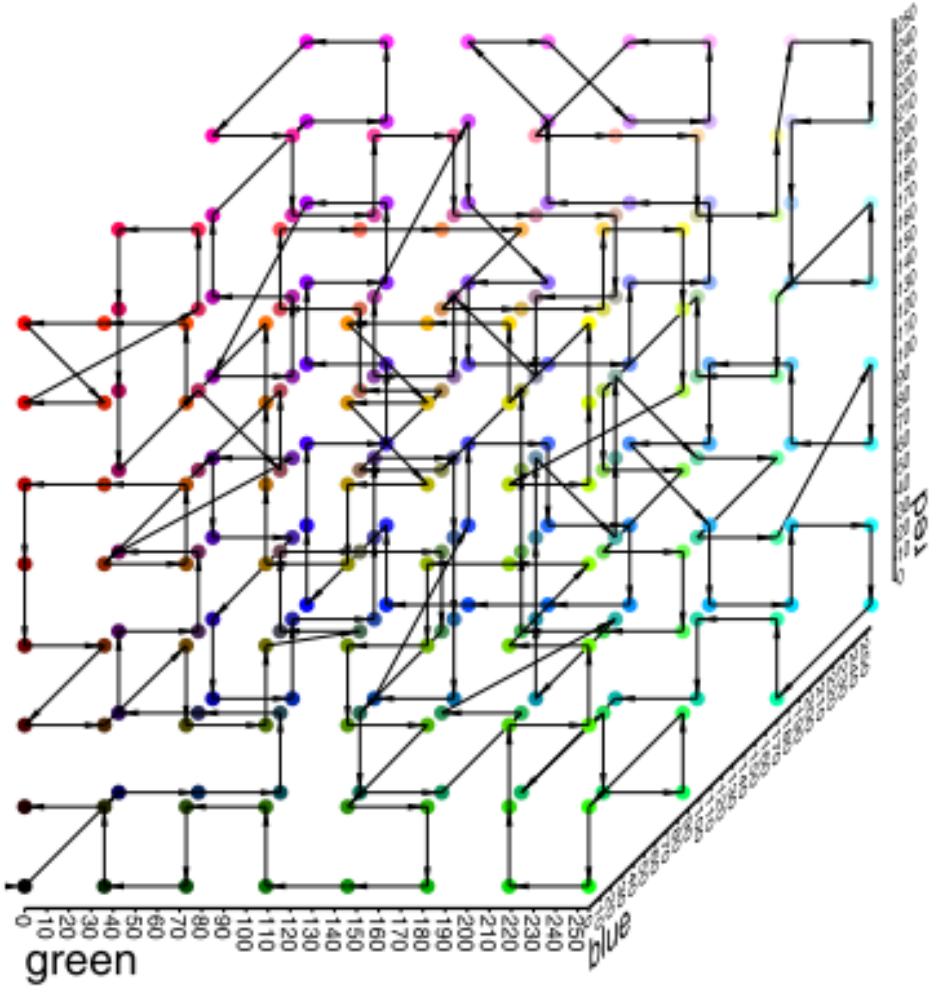
- Attacco χ^2
  - Basato sull'osservazione che durante il processo di embedding si formano di coppie di valori che si interscambiano.
  - Calcolando la probabilità della presenza di un messaggio è in grado di stimarne la lunghezza.
  - Attacco χ^2 generalizzato
    - Applicabile ad immagini modificate con LSB embedding pseudo-random.

Attacchi statistici

- Metodo RS o delle doppie statistiche (Dual statistics)
  - Considera tutti i bit plane e la posizione dei pixel nell'immagine.
- Analisi degli Istogrammi
- Blind Anlysis
  - Ricerca di un set di grandezze sensibili al processo di embedding di cui viene studiato il comportamento su centinaia di immagini campione facendo variare la lunghezza del messaggio e il processo di embedding.

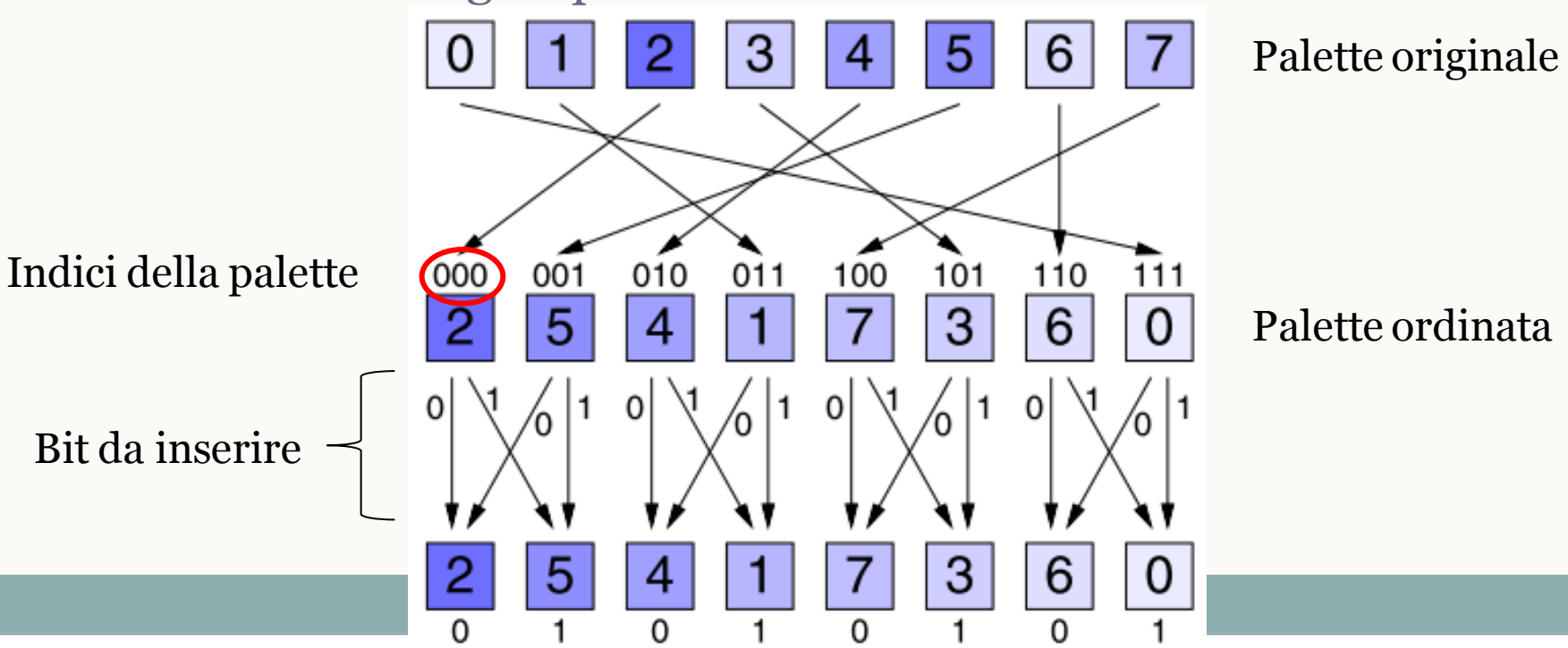
Attacco χ^2





Attacco χ^2

- Utility: EzStego
  - Formato: GIF
  - Ordina gli indici della palette avvicinando tra loro i colori simili all'occhio.
  - LSB Embedding sequenziale



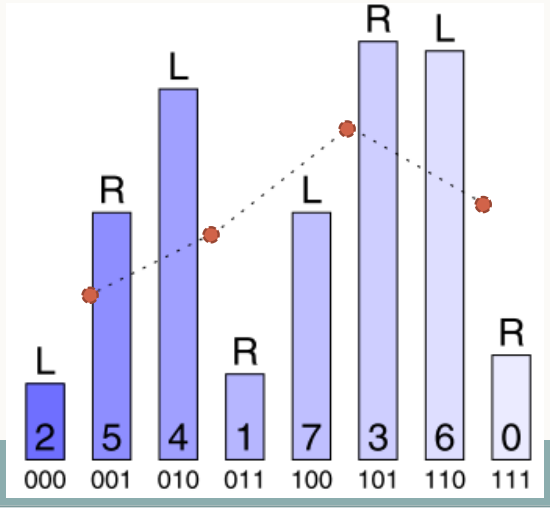
Attacco χ^2

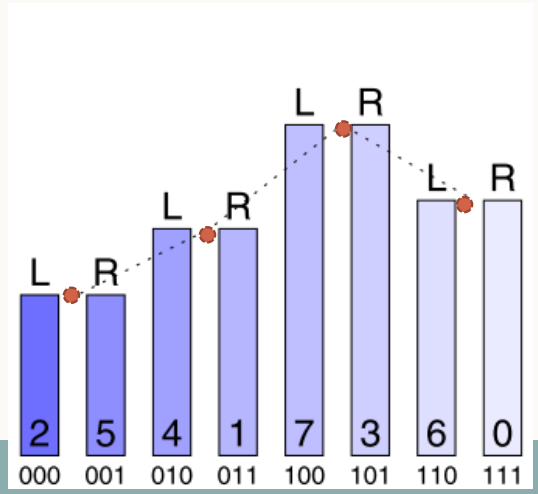
- PoVs (Pairs of Values)

$$0 \longleftrightarrow 1 \qquad 2 \longleftrightarrow 3 \qquad \ldots \qquad 2i \longleftrightarrow 2i+1 \qquad \ldots \qquad 254 \longleftrightarrow 255$$

- Per un'immagine naturale i due valori di ogni coppia si presentano con frequenze differenti.
- In una stego-immagine, invece, queste frequenze tendono ad eguagliarsi.

La somma delle due frequenze resta però invariata.





Attacco χ^2

- x_i = occorrenze del colore 2i
- y_i = occorrenze del colore 2i+1
- $z_i = (x_i + y_i)/ 2$
- $\Longrightarrow$ z_i è il numero di occorrenze attese per una stego-immagine.

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(x_i - z_i)^2}{z_i}$$

Statistica $\chi 2$ con (k-1) gradi di libertà

χ^2 piccolo $\Longrightarrow$ $x_i \sim z_i$
χ^2 grande $\Longrightarrow$ $x_i \neq z_i$

Abbiamo eliminato quelle coppie di colori con $x_i \leq 4$

Attacco χ^2

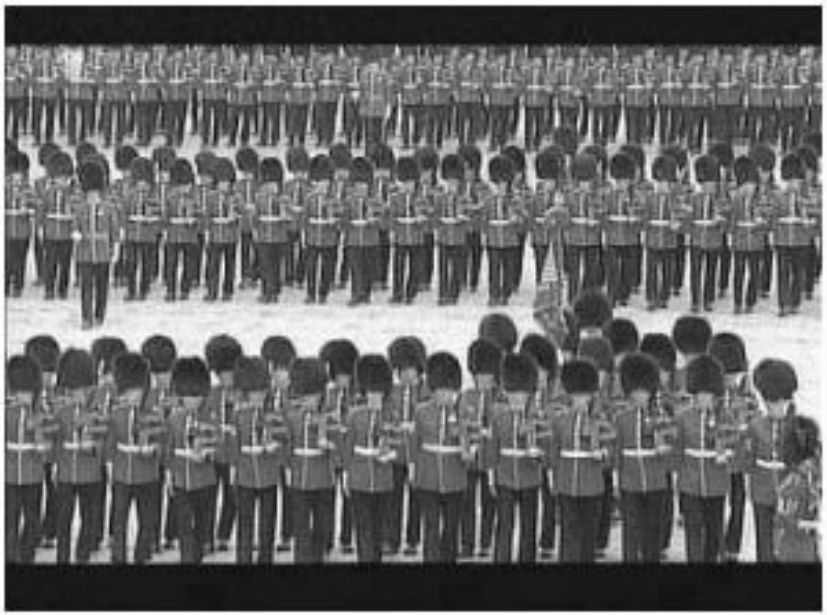
- La probabilità che l'adattamento sia "buono" è

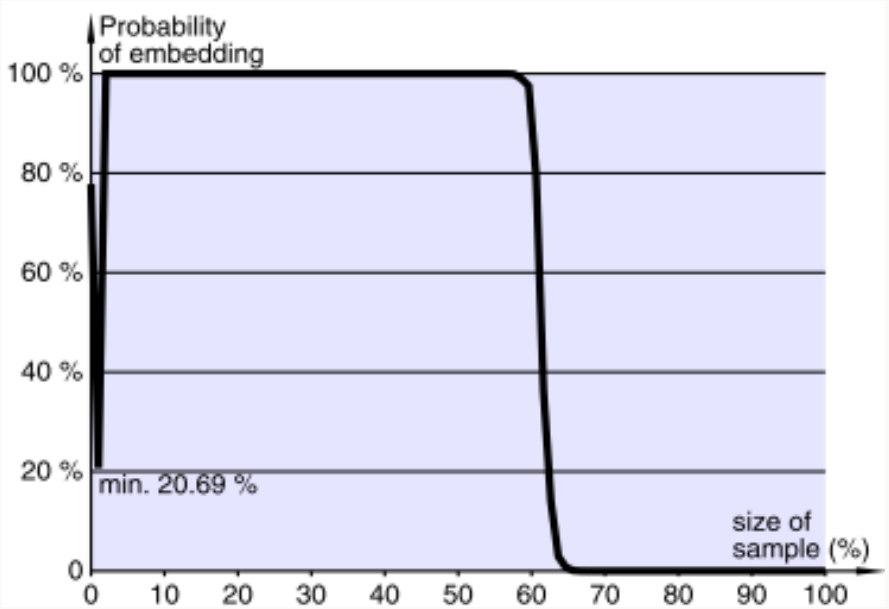
$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\,\Gamma\left(\frac{k-1}{2}\right)} \int_0^{X^2_{k-1}} e^{\frac{-x}{2}}\, x^{\frac{k-1}{2}-1}\, dx$$

- p è la probabilità che l'immagine sia steganografata.

Attacco χ^2

- Disegnando un grafico che esprime questa probabilità al variare della percentuale di immagine scansionata





- E’ possibile dare una stima della lunghezza del messaggio.

FINE