Digital Watermarking Technology

Internet- Web: Database multimediale distribuito sul globo terrestre

- testo
- grafica
- audio
- video

Ogni utente connesso alla rete ha la possibilità di accedere alle informazioni ovunque esse siano localizzate fisicamente

Rete, protocolli di comunicazione, applicazioni hanno reso …

… grosse quantità di dati condivisibili …

Ricerca negli anni passati: rappresentazioni e modalità di trasmissione delle informazioni in grado di garantire affidabilità e costi contenuti.

La crescita delle informazione e dei servizi in rete ha portato alla crescita degli accessi e degli usi illegali delle informazioni disponibili.

A partire dagli anni '70 … Crittografia!

- Confidenzialità
- Autenticità
- Integrità
- Non Ripudio

Esiste però un altro livello del problema della protezione dei dati *digitali*

- diritti d'autore (copyright)
- distribuzioni e copie illegali di documenti
- contraffazioni
- dispute concernenti l'affermazione di paternità

Mentre per le forme tradizionali di rappresentazione e comunicazione delle informazioni soluzioni più o meno efficienti sono state trovate, per i *dati digitali* sono tutte da inventare!

Concetto di copia digitale

Identica all'originale

Invece …

- fotocopie cartacee
- cassette musicali
- videocassette VHS
- …

… sono tutte affette da forme di degradazione più o meno evidenti che si amplificano con la copia della copia della copia …

Problema: trovare dei meccanismi di protezione che riescano a garantire un uso corretto dei dati.

I diritti dei "produttori" e dei "consumatori" di Informazione debbono essere tutelati

Inserire all'interno del documento digitale Una sequenza di bit (watermark) che risulti

- **Impercettibile** – Il documento con marca e quello senza debbono apparire identici
- **Legata al documento** - la marca deve dipendere e rappresentare tutto il documento.
- **Robusta** – la marca deve resistere a tutte quelle trasformazioni che non ne riducono il valore oltre una certa soglia

L'idea non è del tutto nuova …
Watermark in italiano significa filigrana

Come la filigrana garantisce autenticità ed integrità delle banconote, così il watermark dovrebbe garantire integrità ed autenticità dei documenti digitali (testuali, grafici, audio e video …)

Il watermark nascosto nel documento funziona come una sorta di prova del proprietario o del responsabile del documento.

I watermark permettono di realizzare protocolli di protezione dei dati che offrono differenti gradi di sicurezza.

Un semplice esempio …

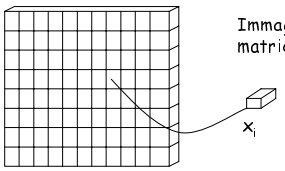


Immagine in **toni di grigio**: matrice di **n** pixel.

pixel = **stringa di 8 bit** che indica l'intensità del grigio.

Sia $w_1 \ldots w_n = 01\ldots10$ il watermark che si vuole immergere.
Basta sostituire l'ultimo bit di x_i con il bit w_i per i=1,…,n

x_i = 10101110 ⇒ x'_i = 1010111w_i

Proprietà …

- Impercettibilità ok!
- **w** funzione del documento ok!
- robustezza?

Si noti che semplicemente modificando **a caso** gli ultimi bit della rappresentazione di ogni pixel si ottiene una nuova immagine indistinguibile dalla precedente ma priva della marca.

Scenario 1

Un'agenzia vende ad un gruppo di acquirenti un file grafico e lo invia in forma cifrata

- come può assicurarsi che un acquirente, decifrato il file, non lo rivenda ad altri?
- può individuare le copie illegali?
- può rintracciare gli acquirenti – distributori (illegali)?
- un acquirente corretto come può provare i suoi diritti?

Scenario 2

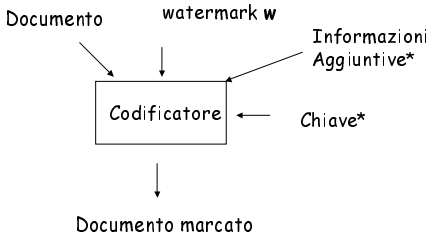
Un artista espone in rete le proprie opere digitali.

- come può affermare in modo equivocabile la propria Paternità sulle opere in presenza di un contenzioso?
- può proibire le contraffazioni?

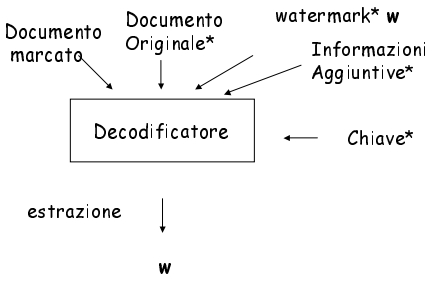
Schema di watermarking

- come il watermark viene **immerso** nel documento
- come il watermark viene **recuperato** dal documento marcato e reso pubblico

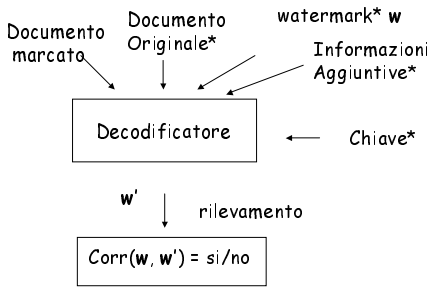
Inserimento della marca

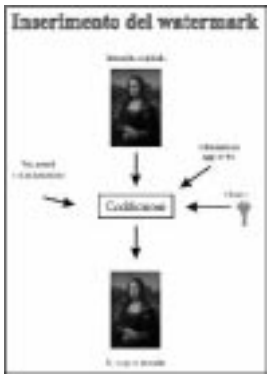


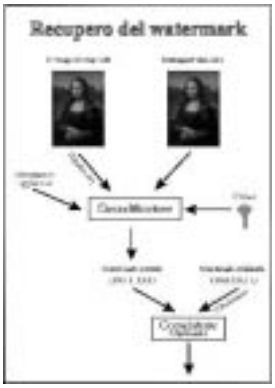
Recupero della marca



Recupero della marca







Risoluzione di alcuni dei problemi precedenti

- Affermazione di paternità (falsificazioni)

Imm ⇨ Imm(w) ⇨ Pubblica Imm(w)

- Distributori illegali

Imm ⇨ Imm(w_1), …, Imm(w_n)

- Prova dei propri diritti.
Se w incorpora "qualche" informazione segreta dell'utente quest'ultimo può provare di essere autorizzato all'uso del documento

…nel Mondo Reale …

MP3 (file audio)
www.mp3.com
www.sdmi.org
DVD
Biblioteche, musei, archivi storici e fotografici on-line
Iniziative commerciali private

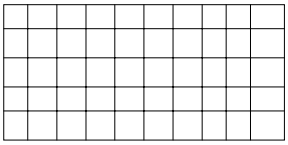
… altri usi del watermark …

"Aggiungere" informazioni ai documenti

- macchina fotografica digitale che aggiunge automaticamente data, ora della foto …
- documenti "medici" (informazioni visualizzazione)
- informazioni di controllo d'uso

Immagini

Un'immagine è una matrice di pixel



Ogni pixel è rappresentato da una stringa di bit.

Risoluzione: verticale, orizzontale e in ampiezza

Esistono diverse rappresentazioni per le immagini a colori

Modello **RGB**: a partire dai tre colori fondamentali (rosso, verde e blu) vengono generati tutti gli altri.

Ogni pixel è una stringa di 24 bit. (3 byte)
Ogni byte rappresenta un valore di intensità per il rispettivo colore

1° byte 2° byte 3° byte

01101010 10110101 01010101

Rappresentazioni luminosità - crominanza

Modello YUV:
- luminosità (intensità della luce)
- tonalità (presenza dei colori)
- saturazione (quanto è vivo il colore)

E' possibile passare da una rappresentazione all'altra

$$Y \leftarrow 0.3\,R + 0.6\,G + 0.1\,B$$

$$V \leftarrow R - Y \quad U \leftarrow B - Y$$

Modello YCbCr: simile ad YUV

Utili per gli alg. di compress.

Immagini: taglia troppo grande

Le immagini contengono informazione ridondante

- Ridondanza spaziale
- Ridondanza percettiva

Possono essere sfruttate per rappresentazioni più compatte

Esistono diversi formati per immagini che implementano **algoritmi di compressione** al fine di ridurre la taglia dell'immagine originale.

- lossy
- lossyless

… ne descriveremo brevemente due

- GIF (Graphic Interchange Format)
- JPEG (Joint Photographic Experts Group)

GIF

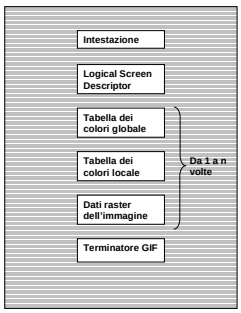
Il formato GIF utilizza un numero limitato di colori contenuti in una palette o tavolozza dei colori associata all'immagine.

Ogni pixel **è un puntatore ad un'entrata della tavolozza**

Un'immagine GIF può usare al massimo 256 colori

Figura 4.2 Il formato della Tabella dei Colori.

Formato Gif
Struttura del file



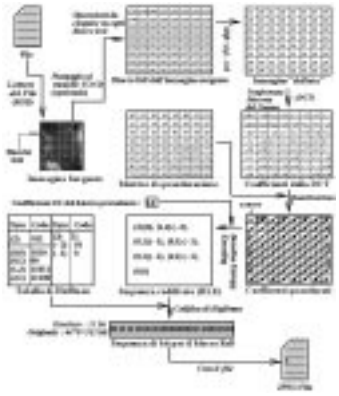
I "dati raster" sono compressi con l'algoritmo LZW

Lo standard Jpeg – compressione per immagini

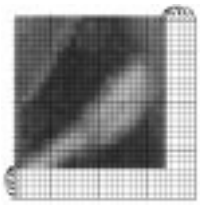
I passi che l'algoritmo di compressione effettua sono

- lettura del file sorgente (modello RGB)
- trasformazione RGB-YUV e riduzione di U e V
- shift dei valori dell'immagine
- trasformata discreta del coseno (DCT)
- quantizzazione
- run lenght encoding
- codifica di Huffman

Algoritmo Jpeg

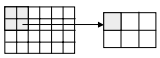


Lettura del file sorgente

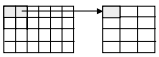


Alcune righe e colonne vengono duplicate per poter dividere l'immagine in blocchi di dim. 8x8

Trasformazione RGB – YUV e riduzione di UV

2h2v 

Oppure ..

2h1v 

I valori delle nuove matrici sono shiftati **X ← X - 128**.

Valori blocco originale

139	144	149	153	155	155	155	155
144	151	153	156	159	156	156	156
150	155	160	163	158	156	156	156
159	161	162	160	160	159	159	159
159	160	161	162	162	155	155	155
161	161	161	161	160	157	157	157
162	162	161	163	162	157	157	157
162	162	161	161	163	158	158	158

Valori DCT

235,6	-1,0	-12,1	-5,2	2,1	-1,7	-2,7	1,3
-22,6	-17,5	-6,2	-3,2	-2,9	-0,1	0,4	-1,2
-10,9	-9,3	-1,6	-1,5	0,2	-0,9	-0,6	-0,1
-7,1	-1,9	0,2	1,5	0,9	-0,1	0,0	0,3
-0,6	-0,8	1,5	1,6	-0,1	-0,7	0,6	1,3
1,8	-0,2	1,6	-0,3	-0,8	1,5	1,0	-1,0
-1,3	-0,4	-0,3	-1,5	-0,5	1,7	1,1	-0,8
-2,6	1,6	-3,8	-1,8	1,9	1,2	-0,6	-0,4

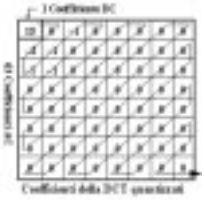
Matrice di quantizzazione

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

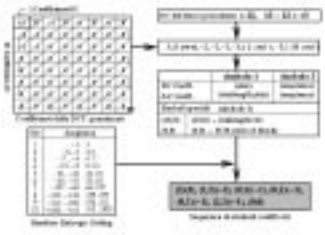
Valori quantizzati

15	0	-1	0	0	0	0	0
-2	-1	0	0	0	0	0	0
-1	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Organizzazione a zig-zag dei coefficienti quantizzati

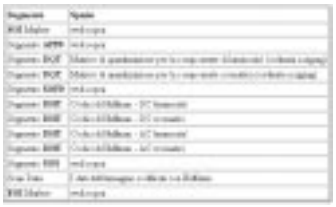


Run lenght encoding RLE



La sequenza così ottenuta viene compressa con i codici di Huffman

Struttura di un file Jpeg



Una nota: il processo di quantizzazione induce perdita di informazione nella compressione Jpeg

Blocco "dequantizzato"

240	0	-10	0	0	0	0	0
-24	-12	0	0	0	0	0	0
-14	-13	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

DCT^{-1} del blocco "dequantizzato"

144	146	149	152	154	156	156	156
148	150	152	154	156	156	156	156
155	156	157	158	158	157	156	155
160	161	161	162	161	159	157	155
163	163	164	163	162	160	158	156
163	164	164	164	162	160	158	157
160	161	162	162	162	161	159	158
158	159	161	161	161	162	159	158

Discrete cosine transformation

Un' immagine è una funzione $f(x,y)$

La DCT esprime f(x,y) in termini di funzioni coseno

$$F(v,u)=\frac{1}{4}C(u)C(v)\sum_{x=0,y=0}^{7}\sum^{7}f(x,y)\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2x+1)v\pi}{16}$$

I coefficienti DCT costituiscono una **nuova rappresentazione** dell'immagine rispetto ad una **base "più comoda"**.

Video: formato Mpeg

Il video digitale è una sequenza di immagini digitali.
I parametri che caratterizzano un video digitale sono

- numero di immagini al secondo
- risoluzione verticale
- risoluzione orizzontale
- risoluzione in ampiezza (profondità)

Per minimizzare la quantità di informazione necessaria a rappresentare un video si potrebbe codificare ogni immagine con Jpeg … (si può fare di meglio ☺ !!!)

… anche nei video c'è ridondanza

- spaziale
- percettiva
- temporale

La ridondanza temporale è presente perché immagini "vicine" differiscono di poco. Per cui piuttosto che codificarle ogni volta per intero, è più efficiente codificare le differenze.

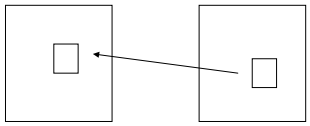
La sequenza video viene divisa in GOP (gruppi di immagini) nella codifica Mpeg

Ogni Gop è una sequenza di immagini che vengono visualizzate in modo contiguo.

Ogni immagine del Gop può essere di 3 tipi
- **I** (intrapictures)
- **P** (predicted pictures)
- **B** (bidirectional pictures)

I frame di tipo **I vengono codificati con Jpeg.**
Gli altri vengono "predetti" (vettore di spostamento).

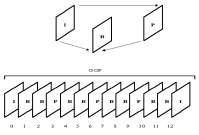
L'intuizione alla base di Mpeg



istante i istante i+1

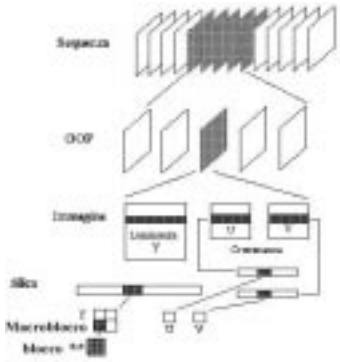
Piuttosto che codificare tutta l'immagine basta codificare
- il vettore che indica lo spostamento del macroblocco
- differenze con il blocco precedente

Schema di un GOP



Relazione tra
I tre tipi di frame

Algoritmo
Mpeg



Schemi di watermarking

Fragili

Robusti

Visibili

Invisibili

Gli schemi si dividono inoltre in
- **pubblici** (non occorre l'img. originale per verificare **w**)
- **privati** (…occorre!)

Proprietà di robustezza per le immagini

- Compressione lossy (Jpeg)
- Distorsioni geometriche
  - rotazioni
  - traslazioni
  - resizing
  - cropping
- elaborazioni varie
  - dithering
  - ricompressione
  - alterazione del contrasto
  - manipolazioni dei colori
- conversioni analogico-digitali

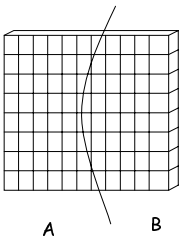
Gli schemi di watermarking per immagini operano essenzialmante in **due modalità**

- **dominio spaziale**: manipolano direttamente le rappresentazioni dei pixel dell'immagine

- **dominio delle fraquenze**: rappresentano l'immagine in un'altra forma, modificano gli elementi della forma trasformata e ritornano al dominio spaziale

Schemi che operano nel **dominio spaziale**

Immagine in toni di grigio



A e B approssimativamente della stessa taglia

Supponiamo che i valori dell'intesità dei pixel siano **uniformemente distribuiti**

Immersione watermark (valore k piccolo).
Si aggiunge **k** a tutti i pixel di **A** e si sottrae a quelli di **B**

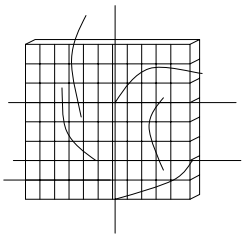
Recupero del watermark
Si calcola la differenze delle intensità medie.

$$\frac{\sum x \in A}{|A|} - \frac{\sum x \in B}{|B|}$$

2k

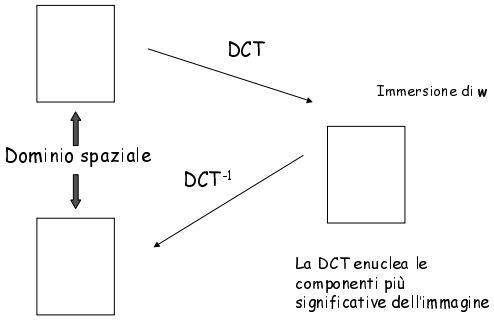
0

Miglioramento dello schema



L'immagine viene divisa in blocchi.
Ogni blocco viene diviso in due regioni all'incirca uguali.
In ognuno di essi viene inserito un diverso valore k_i

Schemi che operano nel **dominio delle frequenze**



Cox et al.

Idea: individuare le componenti più significative ed immergervi la marca

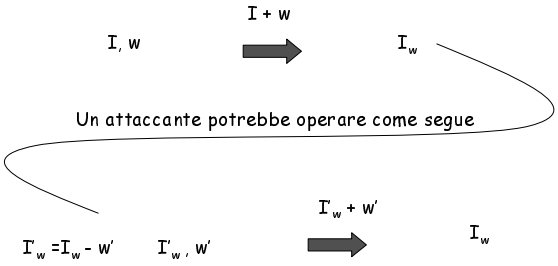
Immersione della marca
- siano $r_1,\ldots, r_n$ valori positivi piccoli casuali (marca)
- si applichi la DCT all'immagine di partenza I
- sia D(I) l'insieme degli n coeff. AC più significativi
- I' è tale che v_i in D(I) ------> $v'_i = v_i + r_i$
- si applichi la DCT^{-1} alla matrice dei coeff. modificata
- si restituisca I' (immagine marcata)

Recupero della marca
- si applichi la DCT all'immagine I
- sia D(I) l'insieme n coeff. più significativi
- si applichi la DCT^{-1} a I'
- sia D(I') l'insieme n coeff. più significativi
- sia $r'_i = v'_i - v_i$ per tutti gli i=1,…,n
- calcola della corr(r, r')

$$Corr(r,r') = \frac{\sum r_i r'_i}{\sqrt{\sum r_i^2 \left(\sum r'^2_i\right)}}$$

Se Corr(r,r') è maggiore di una certa soglia la sequenza r' viene considerata come r.

Proprietà di **non-invertibilità**



Esistono due coppie (I,w) e (I'_w,w') che generano I_w!

Lo schema di Cox et al. può essere reso **non invertibile** usando una funzione hash

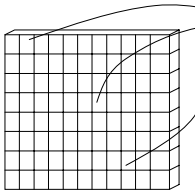
Idea:
- hash (I)
- considero i primi n bit
- $v'_i = v_i + r_i$ se b_i è 1, altrimenti $v'_i = v_i - r_i$

In questo modo solo il proprietario di I è in grado di **provare** l'inserimento della marca.

Schemi fragili

Usati per il controllo dell'integrità dell'immagine

Idea: "far puntare" i pixel al watermark in una stringa random



r=01001…100101100101111
stringa di bit casuali

w=11011…0 watermark

Ogni bit x_i è un puntatore ad un elemento r_i della stringa r

Immersione di w
Per tutti gli i=1,…,n
se $r_i = w_i$ OK!
altrimenti modifico uno degli ultimi bit di x_i fino a che $r_i = w_i$

Schema con funzioni hash

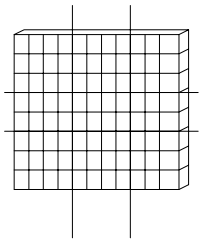


Immagine partizionata in blocchi 8x8

Per ogni blocco …

x_i = 010011001 x_j = 010010001

lsb(x_i) lsb(x_j)

…0100110001001000… stringa

Immersione w
- si rimuovano gli lsb(x_i) di tutti gli x_i
- si concatenino i restanti di tutti gli x_i
- si effettui l'hash della stringa ottenuta
- b= hash(stringa) XOR **w**
- si inseriscano i bit b_i di b al posto dei rimossi lsb(x_i)

Schema con crittografia a chiave pubblica

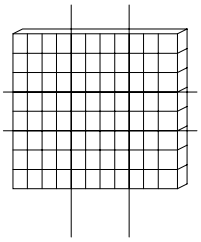


Immagine partizionata in blocchi 8x8

Per ogni blocco …

x_i = 010011001 x_j = 010010001

lsb(x_i) lsb(x_j)

…0100110001001000… stringa

Immersione w
- si rimuovano gli lsb(x_i) di tutti gli x_i
- si concatenino i restanti di tutti gli x_i
- si effettui l'hash della stringa ottenuta
- b= sig_{sk}(hash(stringa)) XOR **w**
- si inseriscano i bit b_i di b al posto dei rimossi lsb(x_i)

Esempio di watermark visibile

Attacchi dei pirati

- Aggiunta di rumore
- Marcature multiple (attacchi di interpretazione)
- Interattivi
- Attacchi di inversione
- Attacchi per coalizione

… gli schemi debbono essere robusti anche contro queste trasformazioni …

Caratteristiche desiderabili in uno schema

- Universalità (testo, grafica, audio e video)
- Parametrizzabilità
- Scalabilità (costo/protezione)

Inoltre sarebbe desiderabile disporre di

- Interfacce standard
- Buoni strumenti di valutazione (benchmark)

Conclusioni

La tecnologia del watermark

- aumenta la condivisione sicura dei dati
- aggiunge valore ai documenti
- crea un ponte tra i mondi analogico e digitale

... pertanto può essere l'**agente abilitante** di nuovi e corposi business!