UNIVERSITÀ DEGLI STUDI DI SALERNO

Digital Watermarking

Corso di Sicurezza su Reti 2

Prof. Alfredo De Santis

Daniele Giardino

0521000834

A.A. 2008/09

Sommario

Indice delle figure

1 Introduzione

L'avvento di **Internet**, della distribuzione digitale dei dati ed i progressi delle tecnologie di trasmissione dell'informazione hanno messo a disposizione degli utenti un numero sempre maggiore d'informazioni in formato digitale. La rete, i protocolli e tutte quelle applicazioni che permettono di scambiare informazioni, costituiscono una struttura informativa sviluppata per rendere condivisibile grosse quantità di dati multimediali.

Un fattore che limita lo sviluppo di tale struttura consiste nel fatto che i proprietari delle informazioni sono riluttanti all'idea di distribuire i propri dati in un ambiente insicuro come la rete. Infatti é molto alto il timore che prodotti quali file musicali, video e immagini possano essere copiati e spacciati per propri da chiunque abbia accesso alla rete. Questo ha portato nell'industria della musica, dell'arte e del cinema l'esigenza di tutelare i propri prodotti.

Nell'ultimo ventennio la **crittografia** ha realizzato sistemi e protocolli in grado di garantire **riservatezza**, **autenticità** ed **integrità** delle comunicazioni e delle informazioni digitali. Le tecniche crittografiche però non risolvono completamente il problema di una diffusione affidabile: una volta che l'utente ha decifrato l'informazione che un dato venditore gli inviato tramite la rete in forma cifrata, per evitare che gli altri possano impossessarsene e usufruirne gratuitamente, non c'è più nessun tipo di controllo su di essa.

L'informazione di per se non presenta alcun legame con il suo gestore/proprietario. Il proprietario si potrebbe trovare di fronte a copie illegali, redistribuzione non autorizzate e contraffazioni che metterebbero inevitabilmente in discussione la paternità dei propri documenti. C'è quindi bisogno di una infrastruttura che riesca a garantire la protezione globale dei dati in modo tale che i diritti di *"produttori"* e *"consumatori"* di informazioni siano tutelati. Occorre cioè realizzare protocolli che riescano a garantire tutte le parti che entrano in gioco nella comunicazione digitale. La risposta a questa esigenza è il **watermarking**.

Volendo effettuare una *classificazione* (1), possiamo dire che il watermarking è utile per la:

- Copy protection;
- Copyright protection.

Copy protection cerca di trovare un modo che limiti l'accesso a materiale protetto da copyright e/o inibisca il processo di copia dello stesso. Esempi di copy protection includono:

- Trasmissione della TV digitale crittografata;
- Controllo dell'accesso a software proprietario attraverso l'utilizzo di server di licenze;
- Meccanismi di protezione dalla copia nei supporti multimediali.

Copyright protection inserisce informazioni sul copyright stesso all'interno di documenti digitali, senza che questi ultimi subiscano perdite di qualità. Nel momento in cui c'è la necessità di verificare il copyright di un documento, tali informazioni vengono estratte per identificare il proprietario dei diritti. È anche possibile codificare l'identità dell'acquirente originale insieme con l'identità del detentore del copyright permettendo così di tenere traccia delle copie non autorizzate.

Il *digital watermarking* tenta di fornire una soluzione a questi problemi. Quindi lo scopo di questo documento è quello di fornire informazioni utili su questa tecnologia.

1.1 Di cosa parliamo

Il termine **digital watermarking** letteralmente significa *"filigrana digitale"*. Come la filigrana assicura autenticità ed integrità delle banconote, così i *watermark* (2) dovrebbero garantire autenticità ed integrità dei documenti digitali (testuali, grafici, audio, video, etc.) in cui sono inseriti. L'idea di base di questa nuova tecnologia è di inserire all'interno del documento da proteggere una **sequenza** di bit (W) detta watermark.

In sintesi uno schema di watermarking stabilisce semplicemente due cose:

- come la stringa W deve essere inserita nel documento;
- come la stringa W deve essere recuperata.

Il digital watermarking affonda le proprie radici negli studi *steganografici*.

La **steganografia** (3) permette di incapsulare un messaggio segreto, quale potrebbe essere un copyright o un numero seriale, in un cosiddetto messaggio di copertura. L'inserimento di tali informazioni è tipicamente parametrizzato da una chiave, senza la conoscenza della quale è difficile rimuovere o riconoscere il materiale incapsulato. Una volta che l'inserimento è stato effettuato il messaggio ottenuto viene inviato a destinazione.

Negli ultimi anni si è verificato un rapido aumento dell'interesse (4) verso questa disciplina. Infatti molte industrie che producono materiale digitale, quali digital film, audio recording e prodotti multimediali, volendo affiancare ai comuni canali di distribuzione quello della rete, si sono interessate alla possibilità di inserire informazioni di *"paternità"* e di controllo nei loro prodotti.

C'è da sottolineare una differenza di fondo. Per la steganografia il documento è soltanto una maschera, quindi senza valore, mentre quello che vale è il messaggio nascosto al suo interno. Tale corrispondenza è invertita nel digital watermark in cui il messaggio nascosto non ha valore, visto che funge solo da protezione, mentre il documento è il vero portatore di *valore*.

Alcune possibili motivazioni (5) che conducono all'utilizzo delle tecniche di *watermarking* sono:

- Rendere visibile a tutti gli utenti il legittimo proprietario;
- Dimostrare l'originalità di un documento non contraffatto;
- Evitare la distribuzione di copie non autorizzate;
- Marcare alcune caratteristiche specifiche del documento;
- Segnare il percorso di vendita.

1.2 Un po' di storia

Anche se il digital watermarking è una tecnica relativamente recente, il watermark è conosciuto sin dal XIII secolo.

1.2.1 Dandy Roll

Un watermark **dandy roll** (6) è creato imprimendo uno stampo metallico sulla carta durante il processo di produzione. Questa tecnica fu introdotta a Bologna nel 1282 e venne usata dai produttori di carta per identificare il proprio prodotto, ma anche per francobolli e altri documenti amministrativi, per scoraggiarne la contraffazione.

Il dandy roll è un rullo ricoperto di materiale simile alla fibra di vetro con un pattern. Le linee meno marcate sono create tramite cavi tesi che girano parallelamente all'asse del rullo, mentre quelle più marcate sono costituite da catene di fili metallici posti attorno alla circonferenza. Lo stampo è trasferito sulle fibre di carta, comprimendo e riducendo lo spessore del foglio nell'area interessata.

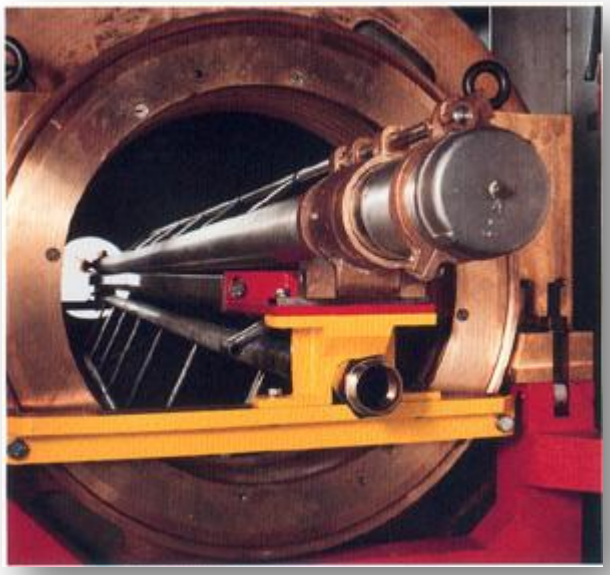

Figura 1: Rullo utilizzato per il watermark

1.2.2 Cylinder Mould

Un altro tipo di watermark è chiamato **cylinder mould** (6). Usato per la prima volta nel 1848, permette la creazione di immagini in scala di grigi tramite la gestione della profondità della tonalità del colore. Al contrario della tecnica precedente, è creato tramite aree di rilievo sulla superficie del rullo. Il watermark risultante è generalmente molto più pulito e dettagliato e veniva stato usato per banconote, passaporti ed altri documenti importanti.

Figura 2: Testa di elefante usata su antiche stampe in India

1.2.3 Watermark su francobolli

In filatelia, il watermark è la caratteristica principale della stampa e spesso costituisce la differenza tra una stampa comune ed una rara. Il classico watermark è una piccola corona sul simbolo nazionale, usato sia nel diciannovesimo che ventesimo secolo, ma generalmente il suo utilizzo è diminuito di molto e non è più comunemente usato nelle tecniche moderne.

1.3 Scenari Applicativi

In questa sezione andiamo a considerare alcuni ambiti di applicazione (1) per la tecnologia del watermark e le rispettive proprietà che dovrebbe soddisfare.

1.3.1 Autenticazione ed integrità dei dati

Supponiamo che un fotoreporter catturi delle immagini con una camera digitale e vuole essere sicuro che tali immagini non vengano modificate e/o falsificate. Per rendere possibile ciò al momento dello scatto viene incluso un watermark cosicché il suo corretto rilevamento al momento dell'uso indichi se l'immagine sia stata alterata o meno.

Affinché una tecnica di watermark sia effettivamente usata in questo tipo di applicazione, il codice incluso nell'immagine dovrebbe essere invisibile all'occhio umano ed alterato da ogni modifica dell'immagine. Inoltre dovrebbe essere difficile inserire un watermark falso e dovrebbe essere possibile capire in quale punto sono avvenute le modifiche.

1.3.2 Copie non autorizzate

Un venditore di immagini vuole evitare la distribuzione illegale del proprio materiale. Per far fronte a ciò il proprietario incapsula in ogni immagine il suo marchio. In tal caso, un web crawler potrebbe poi essere usato per individuare su Internet le immagini contenenti il marchio del venditore per poter cosi rilevare distribuzioni di copie non autorizzate.

In questo caso il marchio dovrebbe essere invisibile, robusto e facilmente estraibile dal proprietario dell'immagine.

1.3.3 Identificazione del distributore illegale

Il venditore può voler conoscere chi distribuisce illegalmente le sue immagini. A questo proposito può essere inserito un watermark distinto per ogni utente al tempo della distribuzione che indica chi ha comprato l'immagine. Tramite il recupero del marchio si può risalire al rivenditore disonesto che ha venduto l'immagine senza autorizzazione.

Questo tipo di approccio è utilizzato quindi come deterrente per evitare che copie illegali vengano immesse sul mercato.

1.3.4 Affermazione di paternità

Grazie alle tecniche di watermark possono essere inserite nell'immagine informazioni come la sigla o il logo del proprietario e rendere poi l'immagine marcata pubblica.

Se il proprietario sospetta che una delle sue immagini sia stata modificata e pubblicata senza il suo permesso può estrarre il watermark dall'immagine e provare la paternità sull'immagine.

1.3.5 Protezione dei contenuti

In alcune applicazioni il proprietario può voler rendere utilizzabile il dato solo per un determinato periodo di tempo. Quindi anche a tale scopo il watermark può essere utilizzato per stabilire il periodo e le restrizioni d'uso che possono essere comunicate alla device di visualizzazione o di riproduzione del documento.

1.3.6 Aggiunta di informazione

I bit incapsulati possono anche aggiungere varie informazioni. Una foto può annotare al suo interno il tempo, il posto ed il fotografo che l'ha scattata come anche altre informazioni generiche. Inoltre possono essere aggiunte informazioni di controllo atte ad aiutare l'utente nell'utilizzo appropriato dell'informazione.

1.4 Tipologie di watermarking

C'è abbastanza confusione sui nomi delle diverse tecniche di watermarking (1). La ragione principale è che le persone coinvolte in questo campo di studio hanno diversi background, in particolare *signal processing* e *computer security.* Inoltre una parte della terminologia usata è stata importata dalla *steganografia*.

Per rendere generico il discorso effettuato sulle diverse tipologie di watermark, di seguito si utilizzerà il termine *segnale* per indicare le informazioni su cui vengono applicate le tecniche di watermaking.

Public watermarking e **blind watermarking** hanno lo stesso significato, anche se spesso la prima terminologia viene confusa con *public-key watermarking.* In questi schemi, il segnale originale non è necessario durante il processo di individuazione del watermark. È richiesta solamente la chiave, che è tipicamente usata per generare alcuni valori random utilizzati durante il processo di inserimento. Si tratta della tecnica più difficile da implementare, ma anche di quella che garantisce la migliore flessibilità del sistema.

Alcuni schemi di watermark richiedono l'accesso ad informazioni addizionali, come il segnale originale subito dopo aver aggiunto il watermark, per individuare correttamente il watermark. Questi schemi vengono chiamati **semi-blind**. Di solito al decodificatore viene fornito il watermark ed in output si ottiene un booleano che ne identifica la presenza o meno all'interno dell'immagine.

Private watermarking e **non-blind watermarking** sono sinonimi. Durante il processo di individuazione del watermark è necessario il segnale originale. Si tratta della tecnica più semplice e più affidabile, ma la necessità di possedere anche l'originale ne limita l'utilità.

Infine, con **asymmetric watermarking** o **public-key watermarking**, ci si riferisce a schemi di watermarking che sfruttano delle proprietà dei sistemi di cifratura asimmetrici (o a chiave pubblica). In realtà ancora non esistono schemi di watermarking commerciali con queste caratteristiche, ma sono state date alcune linee guida. Il processo di individuazione, ed in particolare la chiave utilizzata, è di pubblico dominio, al contrario degli schemi *blind* in cui rappresenta un segreto. Quindi è necessaria una *chiave pubblica* per la sola verifica ed una *chiave privata segreta* per l'inserimento. La conoscenza della chiave pubblica non aiuta nel calcolo della chiave privata (in un tempo ragionevole), ad un attaccante non permette né la rimozione del watermark, né l'inserimento di uno nuovo.

Gli schemi watermarking che sono stati sviluppati negli ultimi anni, possono essere classificati ulteriormente come segue (in questa classificazione si parlerà specificatamente di *immagini*):

- **visibili** e **invisibili;**
- **fragili**, **semifragili** e **robusti**;
- **pubblici** e **privati**.

1.4.1 Watermark visibili

I watermark visibili (7) sono costituiti da immagini semitrasparenti sovrapposte ad immagini principali. Consistono di solito in loghi o marchi delle organizzazioni che detengono i diritti delle immagini principali. Sono fatti in modo tale da essere facilmente individuabili da chi vede le immagini ed identificare chiaramente l'autore; il watermark non può tuttavia essere estratto dal contenuto dell'immagine. Il principale vantaggio dei watermark visibili è la loro forza nello scoraggiare l'uso illegale delle immagini. Un esempio che si può portare viene dal mondo televisivo dove la RAI e le altre tv pongono il loro logo in un angolo dell'immagine principale. Esse ritengono di gran lunga superiori i vantaggi legali al fatto di avere un marchio sempre visibile sullo schermo e che permane anche dopo una videoregistrazione al pericolo di annoiare o distrarre lo spettatore.

Le immagini seguenti mostrano un watermark ed un esempio di immagine su cui è stato sovrapposta una versione in scala dell'immagine watermark. L'unione delle due immagini viene eseguita in maniera tale da preservare le caratteristiche dell'immagine principale, senza degradarne la qualità e l'utilità.

Figura 3: Watermark

Figura 4: Immagine con watermark

1.4.2 Watermark invisibili

I watermark invisibili (7) non sono percettibili dall'occhio umano sotto le normali condizioni visive. Essi sono maggiormente d'aiuto nell' individuare e perseguire, piuttosto che nello scoraggiare, un eventuale ladro.

Sono costituiti da un'immagine sovrimpressa che non può essere vista ma che può essere individuato algoritmicamente.

Il seguente esempio mostra un'immagine, con la parte in alto a destra marcata con un watermark invisibile e la parte in basso a sinistra senza watermark.

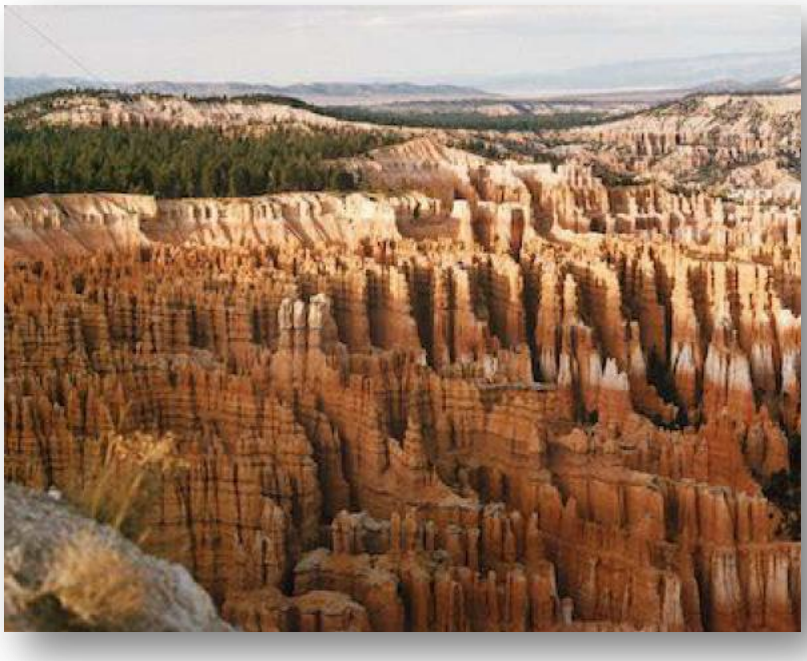

Figura 5: Immagine con watermark invisibile

Figura 6: Watermark estratti dall'immagine precedente

Nella figura 6 possiamo distinguere il watermark estratto dalla parte in alto a destra della figura 5 (in alto) dal watermark estratto dalla parte in basso a sinistra (in basso).

Le differenti applicazioni di questa tecnologia distinguono due diverse tipologie di watermark invisibili.

1.4.2.1 Watermark fragili

Un watermark è detto **fragile** se viene distrutto, quando l'immagine è manipolata digitalmente, in un qualunque modo utile a provare l'autenticità dell'immagine. Se il watermark si presenta ancora intatto, significa che questa non è stata modificata. Queste caratteristiche possono essere importanti per ammettere le immagini digitali come prova in ambito giudiziario.

I **watermark semifragili** sono progettati in modo da andare distrutti in seguito a qualsiasi cambiamento che superi una certa soglia specificata dall'utente: una soglia zero individua perciò un watermark fragile.

1.4.2.2 Watermark robusto

Un watermark **invisibile** che è molto **resistente** verso ogni tipo di manipolazione che un'immagine può subire, utile per verificare la proprietà di un'immagine di cui si sospetta un'appropriazione indebita.

La qualità di un watermark robusto si definisce in termini di *livello di degradazione*. Serve per "trasportare" informazioni che devono accompagnare sempre il documento originale, come per esempio informazioni sul copyright.

1.5 Proprietà del Watermarking

In questa sezione vengono presentate alcune delle caratteristiche principali (1) che uno schema di watermark dovrebbe avere.

1.5.1 Sicurezza

La sicurezza non deve essere basata sulla segretezza dell'algoritmo (Kerckhoffs). Come per la crittografia l'efficacia di una algoritmo non deve essere basarsi sulla sua segretezza. Ciononostante la robustezza di molti prodotti commerciali disponibili sul mercato si basano su quest'assunzione.

1.5.2 Impercettibilità

La differenza tra il documento marcato e quello originale deve essere impercettibile. Il termine impercettibile riferito ad un'immagine marcata indica che il marchio incapsulato è invisibile all'occhio umano così da non alterare la qualità dell'immagine.

1.5.3 Individuabilità

Il watermark deve essere efficientemente individuabile dal proprietario del dato originale, anche se impercettibile all'osservatore medio. Tale efficienza nell' individuazione è necessaria per un pronto reclamo di proprietà ed eventuale attacco legale nei confronti dei falsari. L'individuazione del marchio dovrebbe consentire di scoprire il proprietario senza *ambiguità*.

1.5.4 Robustezza

L'uso di dati in formato digitale, comunemente è soggetto a molti tipi di distorsioni come compressioni, o, nel caso d'immagini, filtraggio, ridimensionamento etc. Per essere utilizzato il watermark deve poter essere estratto anche se l'originale ha subito *distorsioni*.

Esiste una comune opinione che la robustezza contro i segnali di distorsione è soddisfatta meglio se il watermark è inserito in una parte significativa dell'informazione. Questo dipende dal fatto che la maggior parte degli algoritmi di compressione rimuove la percentuale meno significativa del dato visto che tale

eliminazione non deteriora i dati in modo sensibile. Di conseguenza, se il marchio fosse inserito nella parte meno significativa dei dati non resisterebbe alla compressione.

Nel caso di watermark di immagini la resistenza alle manipolazioni geometriche come traslazioni e rotazioni è un problema ancora aperto poiché sono operazioni molto comuni. Una soluzione a tale problema deve essere trovata prima che le tecniche di watermarking siano applicate con successo per la protezione delle immagini. Il watermark robusto, è spesso poco flessibile rispetto all'estrazione esatta del marchio; spesso schemi di watermark robusti consentono solo un semplice rilevamento del marchio.

1.5.5 Watermark modificabili e multipli

La possibilità di modificare il valore di un watermark precedentemente immerso nei dati è una caratteristica a volte richiesta. La modifica del valore del watermark può essere effettuata in due diversi modi:

- rimovendo il vecchio watermark e inserendo il nuovo valore;
- inserendo un secondo watermark in modo tale che entrambi siano leggibili.

La prima alternativa rende il watermark non resistente agli attacchi, in quanto essa implica che il watermark possa essere facilmente rimosso dai dati.

La seconda alternativa è migliore, anche perché permettere la presenza di più watermark diversi nello stesso prodotto. In questo modo, infatti, si può inserire in ogni punto della catena distributiva del prodotto, un watermark diverso, riuscendo così a tracciare la storia del prodotto.

1.5.6 Scalabilità

Nelle applicazioni commerciali, il costo computazionale di un codificatore e di un decodificatore è un fattore importante. In alcune applicazioni, l'inserimento del watermark è effettuato una sola volta e può avvenire off-line; per cui il costo del codificatore è meno importante rispetto al costo del decodificatore, in quanto quest'ultimo può invece operare on-line ed essere invocato innumerevoli volte. Le richieste, in termini computazionali, costringono a progettare watermark relativamente semplici, ma tale semplicità può a volte tradursi in una significativa riduzione della robustezza e della resistenza agli attacchi dello schema di watermarking. Comunque, se si tiene conto del fatto che approssimativamente la crescita della potenza e della velocità dei computer raddoppia ogni diciotto mesi, allora un'applicazione, che oggi richiederebbe risorse computazionali elevate, può in un domani molto prossimo diventare un'applicazione facilmente eseguibile in tempi ragionevoli. Tutto ciò porta al concetto di scalabilità, cioè alla necessità di costruire schemi di watermarking in cui il decodificatore sia scalabile ad ogni generazione di computer. Se fino ad oggi la progettazione di un decodificatore, che risolva problemi complessi quali la gestione delle distorsioni geometriche, non è realizzabile per la difficoltà intrinseca del problema, con la prossima generazione di computer la nuova potenza di calcolo e i ridotti costi possono permettere di superare tali difficoltà.

1.6 Schemi generali

A seconda del campo di applicazione, un processo di watermarking deve soddisfare differenti requisiti e, di conseguenza, deve implementare determinate tecniche. Tuttavia ogni processo di watermarking può

essere schematizzato ad alto livello come composto da due sotto-processi che prendono il nome di **encoding** e **decoding**, o anche di inserimento e verifica.

L'encoding, mostrato nella seguente figura, si occupa di inserire il watermark all'interno dell'immagine e può essere formulato per mezzo della relazione:

$$E\,(W,I) = I_m$$

dove E rappresenta il processo di inserimento, W il watermark, I l'immagine originale e I_m l'immagine marchiata.

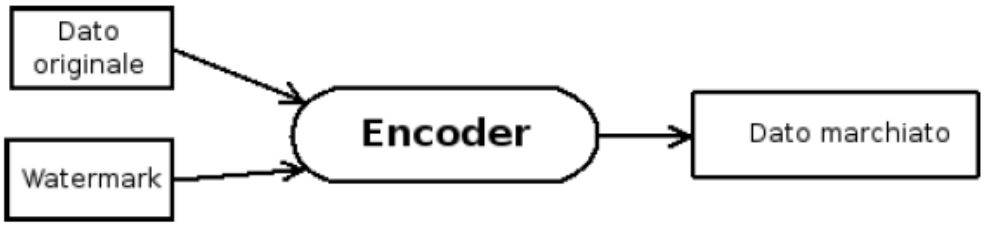

Figura 7: Fase di encoding

Tuttavia si tratta di una generalizzazione non troppo efficace, in quanto non tiene conto di eventuali attacchi alla sicurezza del metodo. L'utilizzo di **chiavi** di inserimento per aumentare la robustezza e di altri fattori di cui si discuterà in seguito consentono di realizzare un sistema di marchiatura sicuro ed efficace. In tutti i processi di watermarking, infatti, si dovrebbe tenere conto del principio di Kerckhoffs precedentemente enunciato.

In questo caso il watermarking non differisce dalla crittografia e per questo motivo è lecito, nonché necessario, ridefinire lo schema presentato in precedenza come

$$E\,(W,I,K) = I_m$$

dove K rappresenta la chiave.

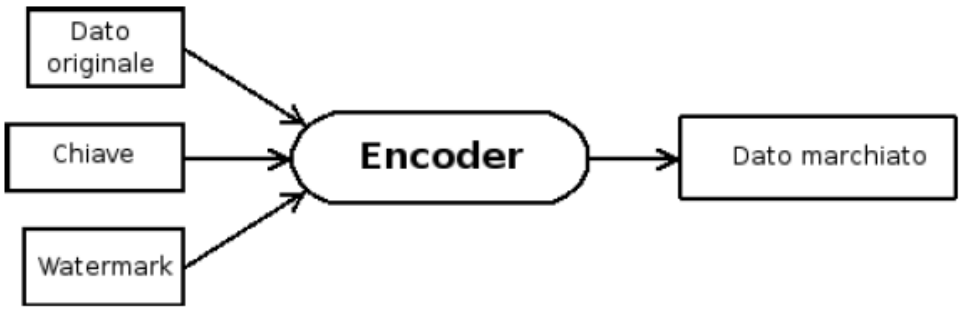

Figura 8: Fase di encoding con chiave

Per quanto riguarda il decoding si possono fare considerazioni analoghe, pertanto si prende in considerazione direttamente lo schema comprendente la chiave:

$$D\,(I_m,K) = W$$

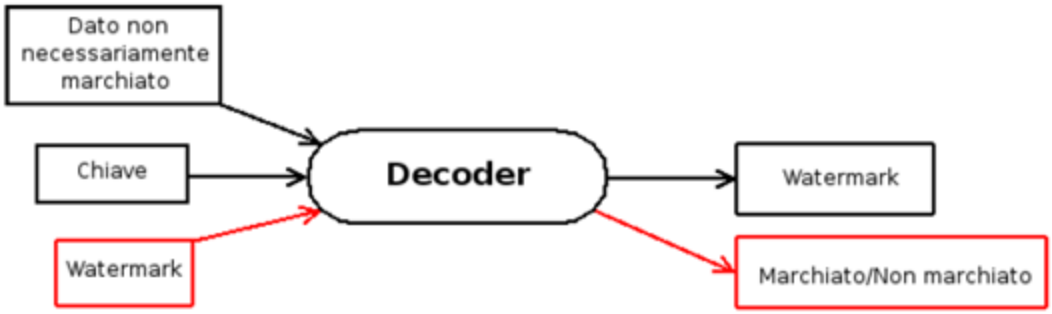

Figura 9: Fase di decoding

Da notare come lo schema comprenda anche il caso di algoritmi di watermarking in cui il risultato del decoding non sia il watermark, ma un valore booleano che identifica o meno la presenza del watermark nel dato.

$$D(I_m, K, W) = true/false$$

2 Image Watermarking

Parlando specificatamente di watermarking in ambito delle immagini, la gran parte degli schemi di watermarking (8) operano essenzialmente in due modalità:

- dominio **spaziale**;
- dominio delle **trasformate**.

Figura 10: Immagine originale
(SHA1: 7cfd6a1838d56b47f8f398a16eeca42828e8f172)

Figura 11: Immagine marcata
(SHA1: 3cf51bdacd5b2e2f3d40a40da41958757018470d)

Nel caso del dominio spaziale di un'immagine significa agire direttamente sui valori dei pixel che la costituiscono. Se questo da un lato può rendere più semplici ed immediate le operazioni di gestione del watermark, dall'altro è stato dimostrato essere inaccettabile dal punto di vista delle caratteristiche di visibilità del watermark così come dal punto di vista della robustezza. L'esempio più semplice di watermarking spaziale è conosciuto con il nome di LSB (Less Significative Bits), in cui vengono modificati i bit meno significativi di ogni pixel dell'immagine.

Il secondo metodo utilizzato per la creazione di watermark prevede di operare nel dominio delle trasformate. Questa tecnica consiste nell'applicare una specifica trasformata all'immagine, successivamente eseguire le operazioni necessarie al'inserimento/rilevazione del marchio e, infine, invertire la trasformata per ottenere l'immagine marchiata o estrarre il marchio. Le trasformate più utilizzate sono **DCT** (Discrete Cosine Transform), **DFT** (Discrete Fourier Transform) e **DWT** (Discrete Wavelet Transform).

2.1 Modello generale

Una immagine può essere vista come una **matrice**, i cui elementi sono i pixel. Ogni pixel è associato ad una stringa binaria di 8, 16, 24, 32 bit:

- il numero di bit utilizzati per descrivere il pixel è la *risoluzione in ampiezza*;
- il numero di righe della matrice è la *risoluzione orizzontale*;
- il numero di colonne della matrice è la *risoluzione verticale*.

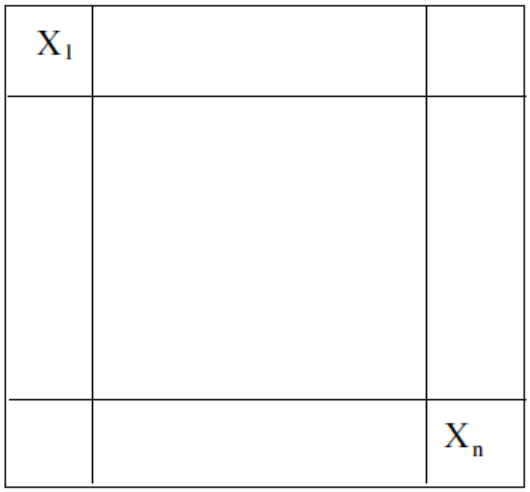

Figura 12: Matrice rappresentante un'immagine

Possiamo immagine che ogni stringa punti ad una matrice di colori. La figura seguente mostra il collegamento tra un'immagine a toni di grigio (parte sinistra) e la matrice di colori (parte destra) tramite una stringa di 8 bit, con i quali si possono rappresentare 256 colori diversi.

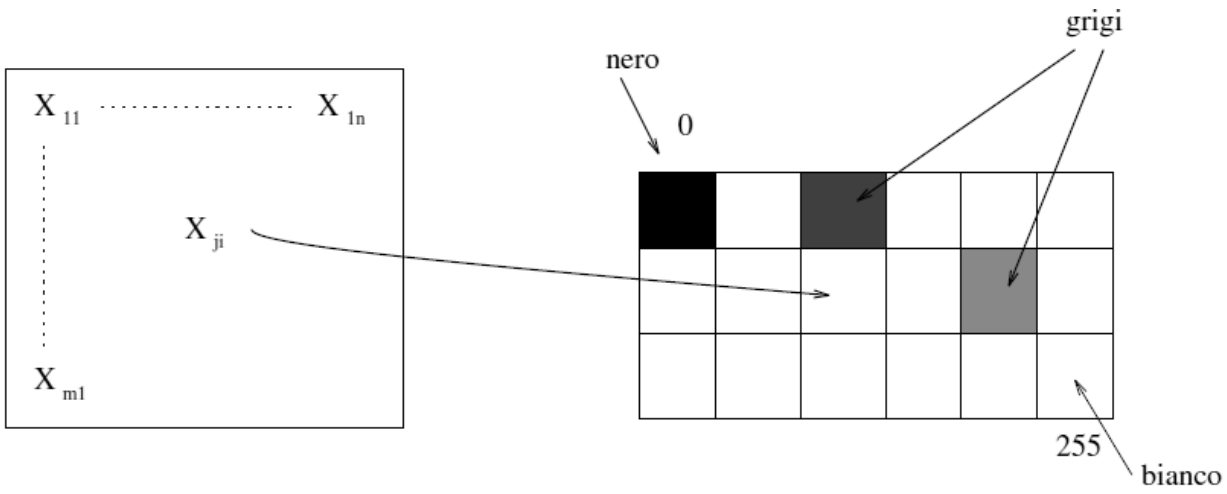

Figura 13: Matrice dei toni di grigio

Le immagini a colori sono anch'esse rappresentate da matrici i cui pixel sono associate stringhe binarie. Il **colore** è espresso mediante la combinazione di tre componenti:

- Rosso;
- Verde;
- Blu.

Le tre componenti variano in modo indipendente, ed insieme formano uno spazio tridimensionale noto come **RGB** (Red Green Blue). Quindi un'immagine è costituita da tre matrici R, G e B una per ogni colore base.

Un'immagine può infatti essere scomposta, attraverso filtri o altre tecniche, in questi colori base che, miscelati tra loro, danno quasi tutto lo spettro dei colori visibili, con l'eccezione delle porpore.

L'RGB è un modello additivo: unendo i tre colori con la loro intensità massima si ottiene il bianco (tutta la luce viene riflessa). La combinazione delle coppie di colori dà il ciano, il magenta e il giallo.

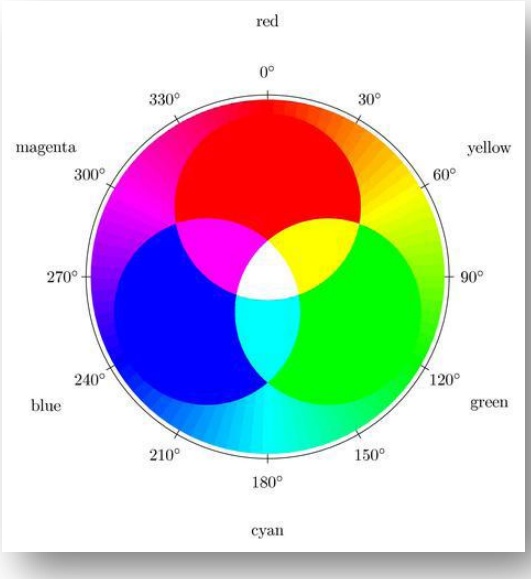

Figura 14: Miscelazione additiva di RGB

Una rappresentazione alternativa è la **YUV**. Utilizza altre caratteristiche del colore: luminosità, tonalità e saturazione:

- la **luminosità** descrive l'intensità della luce (rivelando se il colore è bianco, grigio o nero);
- la **tonalità** descrive la presenza del colore (rosso, verde, giallo, ecc.);
- la **saturazione** descrive quanto è vivo il colore (molto forte, pastello, quasi bianco, ecc.).

La luminosità di un pixel è ottenuta sommando i tre colori, del sistema RGB, nelle proporzioni approssimate di 30% per il rosso, 60% per il verde e 10% per il blu.

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

La crominanza invece è definita come la differenza tra un colore e la luminosità:

$$V = R - Y$$
$$U = B - Y$$

I sistemi di spazi del colore, nei quali una componente è la luminosità e le altre due dipendono dalla tonalità e dalla saturazione, sono dette rappresentazioni luminosità – crominanza. La rappresentazione luminosità – crominanza è più utile rispetto a RGB per ottenere buone compressioni di immagini. È possibile scartare più informazione nelle componenti cromatiche, a cui l'occhio umano è meno sensibile, che in quella di luminosità.

2.2 Dominio Spaziale

Gli schemi più semplici di digital watermarking sono quelli del dominio spaziale. Vengono utilizzati da molto tempo e sono alla base di numerosi schemi utilizzati ancora oggi.

Le tecniche basate su questo dominio eseguono modifiche dei valori dei pixel dell'immagine in funzione del watermark che deve essere inserito. All'inizio della ricerca nel campo del digital watermarking si tendeva a

proporre schemi che aggiungevano pattern pseudo casuali all'immagine originale, modificando la luminosità dei pixel.

La forza delle tecniche nel dominio spaziale è basata nello sfruttare le caratteristiche del sistema visivo umano in relazione alla *sensibilità dei disturbi*. Gli svantaggi di tale modalità sono vari, in quanto risultano poco resistenti sia alle compressioni che alle comuni operazioni di modifica dell'immagine e non possono essere applicate nella pratica a causa dell'elevato tempo computazionale per modificare i pixel.

Esistono due modi per effettuare la modifica:

1) Aggiungere a tutti i pixel valori pseudocasuali che dipendono dalla chiave inserita dall'utente nelle operazioni di inserimento ed estrazione del watermark;
2) Scegliere un insieme di pixel casualmente ed apportare a questi la modifica.

Illustriamo ora due schemi che lavorano nel dominio spaziale. Il primo più semplice che chiameremo schema generale, il secondo proposto da **Langelaar** a cui ci riferiremo con il nome dell'autore.

2.2.1 Schema Generale

Lo schema consiste nel dividere in due insiemi, A e B, i pixel (vedi Appendice 5.2) dell'immagine da marcare, con $|A| \approx |B|$.

La "**partizione**" viene effettuata in accordo alla chiave segreta da inserire nell'operazione di inserimento ed estrazione del watermark.

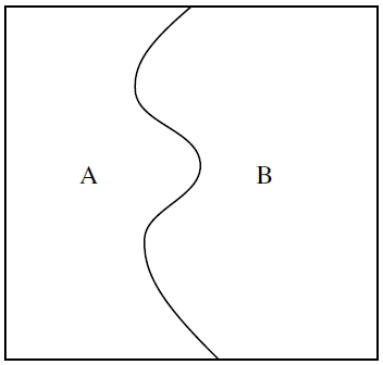

Figura 15: Partizionamento immagine

Fissato un intero k piccolo, che rappresenta il marchio da inserire, lo si aggiunge al valore dell'intensità di tutti i pixel di A e lo si sottrae a quelli di B.

Ovvero viene applicato lo schema descritto sopra ad ogni blocco. Lo schema è migliore del precedente, ma ha un tempo di computazione ancora più alto.

2.2.2 Schema di Langelaar

Tale schema (9) inserisce una stringa di bit nel dominio spaziale dell'immagine. Per fare ciò viene manipolata la luminanza dei pixel in blocchi 8 x 8. Questo da $XY/64$ possibili blocchi dove inserire il watermark, con X e Y che rappresentano le dimensioni dell'immagine in pixel.

La scelta dei blocchi dove inserire il watermark è casuale, ma nello schema non viene effettuata una scelta qualitativa.

Viene creato un pattern pseudocasuale delle stesse dimensioni del blocco. Tale pattern viene utilizzato per tutte le procedure di inserimento:

$$pat(x,y) \in \{0,1\}\ dove\ 0 \leq x,y < 8$$

Per inserire il bit s del watermark nel blocco $B = \{l(x + x_0, y + y_0)\ dove\ 0 \leq x,y < 8\}$, quest'ultimo viene diviso in due sottoinsiemi B_0 e B_1 usando il seguente pattern:

$$B_0 = \{l(x + x_0, y + y_0)\ dove\ pat(x,y) = 0\}$$

$$B_1 = \{l(x + x_0, y + y_0)\ dove\ pat(x,y) = 1\}$$

Il valore della luminanza media è calcolata per entrambi: l_0, l_1. La differenza tra i due valori rappresenta la presenza del bit del watermark (α è un valore soglia):

$$l_0 - l_1 > +\alpha \quad se\ s = 1$$

$$l_0 - l_1 < -\alpha \quad se\ s = 0$$

Se la relazione non occorre naturalmente, si incrementa o decrementa la luminanza dei pixel in B_1.

Per rendere l'algoritmo più robusto rispetto alla compressione JPEG, il blocco viene predistorto tramite l'esecuzione delle seguenti operazioni:

- trasformazione DCT;
- quantizzazione dei coefficienti con un fattore di qualità Q;
- trasformazione DCT inversa.

Il risultato è un blocco lievemente modificato. La luminanza media viene ricalcolata, ottenendo i valori $\widehat{l_0}$ e $\widehat{l_1}$ che vengono utilizzati insieme ai valori calcolati precedentemente:

$$\left.\begin{matrix} l_0 - l_1 > +\alpha \\ \widehat{l_0} - \widehat{l_1} > +\alpha \end{matrix}\right\} \quad se\ s = 1$$

$$\left.\begin{matrix} l_0 - l_1 < -\alpha \\ \widehat{l_0} - \widehat{l_1} < -\alpha \end{matrix}\right\} \quad se\ s = 0$$

La procedura di estrazione di un bit s del watermark da un blocco B, che non necessita dell'immagine originale, prevede il calcolo della luminanza media usando il pattern: l_0'' e l_1''. La differenza tra questi due valori permette di ricavare il bit del watermark inserito nell'immagine:

$$s_k'' = \begin{cases} 0 & se\ l_0'' - l_1'' < 0 \\ 1 & se\ l_0'' - l_1'' > 0 \end{cases}$$

La figura seguente rappresenta la differenza tra l'immagine originale e quella con il watermark. Tale immagine è invertita e scalata in modo tale che il bianco indichi "nessuna differenza" ed il nero "differenza massima".

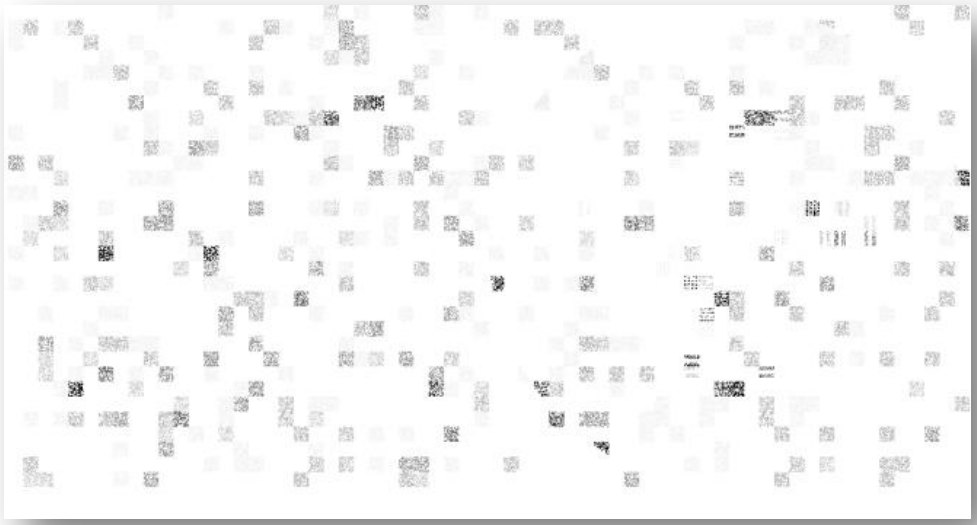

Figura 16: Watermark creato dall'algoritmo di Langelaar, i blocchi modificati sono visibili chiaramente

2.3 Dominio delle frequenze

Le tecniche nel dominio delle frequenze permettono l'inserimento di un grande numero di bit senza **degradare** la qualità visiva dell'immagine. Sono eseguite con le comuni trasformazioni, quali **DCT** (Discrete Cosine Trasform), la trasformazione **wavelet** e la trasformazione di **Fourier**, applicate all'immagine prima di inserire il marchio.

2.3.1 Discrete Cosine Trasform (DCT)

Formalmente, la DCT è una funzione lineare, invertibile $F : R^N \rightarrow R^N$ (dove R indica l'insieme dei numeri reali). Gli N numeri reali $x_0, x_1, \ldots, x_{N-1}$ sono trasformati nei numeri reali $X_0, X_1, \ldots, X_{N-1}$ in accordo ad una delle seguenti formule:

DCT-I

$$X_k = \frac{1}{2}x_0 \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi}{N} n \left(k + \frac{1}{2}\right)\right] \quad k = 0, \ldots, N-1$$

DCT-II

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right)k\right] \quad k = 0, \ldots, N-1$$

DCT-III (DCT inversa)

$$X_k = \frac{1}{2}x_0 + \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N} n \left(k + \frac{1}{2}\right)\right] \quad k = 0, \ldots, N-1$$

Esistono anche altre varianti, poco usate. (10)

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

L'immagine seguente mostra un tipico scenario di schema di watermarking che fa uso della DCT.

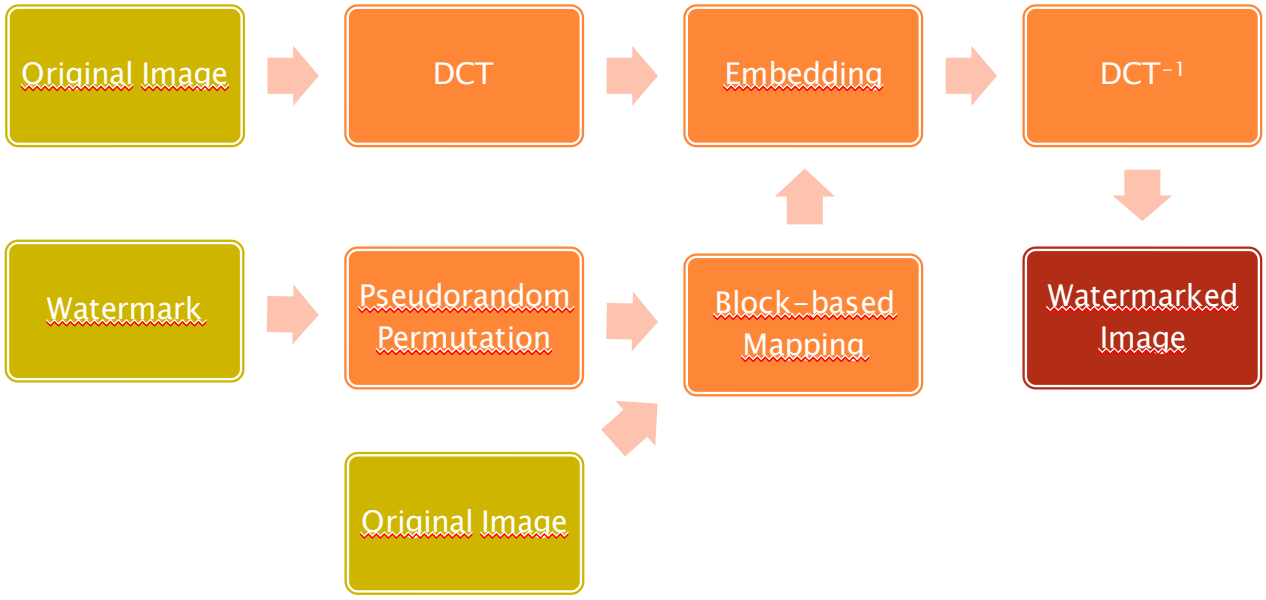

Figura 17: Tipico schema di inserimento con DCT

Figura 18: Esempio DCT (originale)

Figura 19: Esempio DCT (immagine marcata)

Figura 20: Esempio DCT (watermark)

I coefficienti vengono conformati a tre relazioni che rappresentano rispettivamente 0, 1, $invalido$. Non sempre l'inserimento di un bit in un blocco va a buon esito. La trasformazione dei coefficienti può risultare pesante e provocare un degrado della qualità dell'immagine. In tali casi il coefficiente viene marcato invalido per indicare che nel rispettivo blocco non ci sono informazioni aggiunte. Per la verifica del marchio viene effettuata l'operazione inversa. Ottenuti i coefficienti DCT, vengono confrontati con quelli dell'immagine originale, si identificano così i coefficienti modificati e si risale alla relazione che li ha conformati. A questo punto è facile ottenere il watermark.

2.3.2 DCT Watermarking

Illustriamo di seguito un algoritmo per l'inserimento del watermark che usa la DCT e che viene usato per immagini codificate in formato JPEG grazie alla sua caratteristica di resistere alla compressione apportata da questo formato.

Data un'immagine di partenza I, questa viene divisa e considerata come una **matrice** di blocchi 8x8.

1. Si scelgono in modo pseudocasuale un numero di blocchi pari alla lunghezza del watermark da inserire.
2. Si effettua la trasformazione DCT e si considerano nella rappresentazione dello spazio delle frequenze i blocchi corrispondenti a quelli scelti. Ricordiamo che c'è una corrispondenza uno ad uno tra i blocchi dell'immagine I e dell'immagine dopo la trasformazione.
3. Si effettua l'operazione di quantizzazione (conversione del segnale a valori continui in uno a valori discreti), ottenendo una matrice di valori approssimati con coefficienti uniformati.
4. Fase di Inserimento.

L'inserimento della marca viene effettuato apportando modifiche ai valori dei coefficienti DCT ovviamente dei blocchi scelti precedentemente. Sia w il watermark, ovvero la stringa binaria che si desidera inserire nell'immagine. Consideriamo l'i-esimo bit di tale stringa che deve essere inserito nell'i-esimo blocco, del quale si hanno a disposizione i coefficienti DCT. Se tale bit è uno 0 allora si modifica il primo coefficiente e la modifica viene fatta in modo tale che rappresenti uno 0, viceversa il primo coefficiente è modificato in modo tale che rappresenti 1.

La fase di inserimento viene ripetuta fino a quando non si saranno considerati tutti i bit del marchio.

Con un tale schema è facile osservare che i coefficienti vengono conformati a due relazioni che rappresentano rispettivamente uno 0 ed un 1.

Vi è da fare una precisazione: non sempre l'inserimento di un bit in un blocco va a buon esito. Infatti la trasformazione dei coefficienti può risultare pesante e provocare un degrado della qualità dell'immagine; in tali casi allora il coefficiente viene marcato quale invalido per indicare che nel rispettivo blocco non ci sono informazioni aggiunte. Di conseguenza i coefficienti DCT vengono conformati a tre relazioni.

Per quanto riguarda la **verifica** del marchio viene essenzialmente effettuata l'operazione inversa.

Ottenuti i coefficienti DCT, dall'applicazione di una decompressione parziale dell'immagine marcata, vengono confrontati con quelli dell'immagine originale. Si identificano così quei coefficienti modificati e si risale alla relazione tramite la quale sono stati conformati ed a questo punto è facile ottenere il marchio inserito.

Il vantaggio delle tecniche di watermark basati sulla trasformazione DCT nell'ambito del dominio delle frequenze è che l'inserimento e la verifica del watermark possono essere effettuati anche su una rappresentazione compressa dell'immagine effettuando però sempre una decompressione parziale.

2.3.3 Lo schema di Cox et al

Lo schema studiato da **Cox** et al. (11) non è altro che una variazione dell'algoritmo discusso in precedenza. L'osservazione su cui si basa questo schema è di scegliere i blocchi nei quali inserire l'informazione in modo oculato.

Infatti una volta applicata la DCT, la matrice risultante ha una struttura ben precisa: ci sono aree in cui sono presenti coefficienti nulli (che non portano informazioni) e aree in cui sono presenti i coefficienti più significativi (quelli che hanno i valori più alti). Occorrerebbe quindi, andare a marcare i valori più significativi in quanto, se si decidesse di marcare i valori nulli si otterrebbe una perdita dell'informazione, poiché tali valori vengono tagliati via dagli algoritmi di compressione.

Prima di affrontare la tecnica di Cox et altri, ricordiamo come è possibile schematizzare una tecnica di watermark. La si può considerare come una tripla (E, D, C) dove E è la funzione che permette di inserire il watermark, D è utilizzata per estrarlo, mentre C è il fattore di correlazione tra i watermark.

Lo schema di Cox utilizza uno schema che è detto *feature-based*, in quanto una watermark S è inclusa in alcuni degli elementi $D(I) = \{f_1(I), f_2(I), ..\}$, detto insieme delle caratteristiche dell'immagine I.

Nello schema che stiamo trattando, le caratteristiche dell'immagine $D(I)$ corrispondono agli n coefficienti più significativi ottenuti dalla **DCT** (Discrete Cosine Trasformation) dell'immagine I.

Un watermark risultante da uno schema di questo tipo è costituita da una serie di valori casuali $P = p_0, p_1, \dots, p_n$ scelti secondo una distribuzione di tipo gaussiano.

Per inserire tale marca all'interno dell'immagine bisogna prima di tutto calcolare la DCT dell'immagine poi andando a sommare i valori P ed infine si applica la DCT^{-1} ottenendo così l'immagine marcata.

L'operazione di verifica è inversa all'inserimento. Schematizzando:

Inserimento del watermark:

- Siano $r_1, \dots, r_n$ valori positivi piccoli casuali (watermark)
- Si applichi la DCT all'immagine di partenza I
- Sia $D(I)$ l'insieme degli n coefficienti DCT più significativi
- I_1 è tale che vi in $D(I)$ risulta uguale a $v_{i1} = v_i + r_i$
- Si applichi la DCT^{-1} alla matrice dei coefficienti modificata
- Si restituisca I_1 immagina marcata

Recupero del watermark:

- Si applichi la DCT all'immagine I
- Sia $D(I)$ l'insieme dei coefficienti più significativi
- Si applichi la DCT^{-1} a I_1
- Sia $D(I_1)$ l'insieme dei coefficienti più significativi
- Sia $r_{i1} = v_{i1} - v_i$ per tutti gli $i = 1..n$
- Calcolo di $Corr(r, r_1)$.

Se $Corr$ è maggiore di una certa soglia allora la sequenza r_1 viene considerata come r (watermark).

2.3.4 Discrete Wavelet Transform (DWT) Watermarking

La Discrete Wavelet Transform (DWT) è una **trasformata invertibile**, pertanto è possibile applicare il passo inverso e riottenere esattamente l'informazione iniziale. Questa trasformata agisce scomponendo le componenti di un segnale ad alta frequenza da quelle a bassa frequenza. Applicata ad un'immagine, la DWT divide l'immagine considerata in quattro quadranti, chiamati (partendo dall'alto e muovendosi in senso orario) LL, HL, LH e HH, ognuno dei quali di dimensioni pari alla metà dell'originale (nel caso di DWT di livello 1). La sottobanda LL (in alto a sinistra), attraverso l'utilizzo di un filtro passa-basso, contiene le basse frequenze del segnale analizzato; queste frequenze sono anche dette coefficienti di approssimazione. Le restanti tre sottobande contengono le alte frequenze e sono quelle meno percepibili dall'occhio umano, nel caso di immagini; per questa ragione, sono le tre sottobande sulle quali normalmente agiscono gli algoritmi

di watermarking. In particolare, le tre bande HL, LH e HH contengono rispettivamente i coefficienti relativi ai dettagli orizzontali, verticali e diagonali dell'immagine considerata. Da notare che la sottobanda LL può essere divisa ulteriormente, per ottenere un ulteriore livello di scomposizione. Risulta quindi possibile applicare in fasi successive (dette anche passi) la trasformata, in modo da scomporre l'immagine in una molteplicità di livelli ed applicare il procedimento di marchiatura/rilevazione in ogni livello. Il risultato di un tale metodo si traduce in una maggiore diffusione e robustezza del marchio inserito nell'immagine.

Per comprendere meglio il comportamento della trasformata, viene fornito in figura 23 lo schema generale dell'applicazione di una DWT su due livelli ed i relativi risultati ottenuti utilizzando un'immagine di test (figure 24, 25 e 26). A causa delle caratteristiche di ogni sottobanda, la scelta di quelle da utilizzare per l'embedding conduce ad una serie di vantaggi e problematiche. Ad esempio potrebbe essere molto vantaggioso utilizzare la sottobanda LL in virtù dell'importanza che possiede in termini di quantità di informazione che contiene. Per eliminare un watermark presente in LL è infatti necessario modificare una parte molto significativa, di conseguenza visibile, dell'immagine. Per le stesse ragioni, tuttavia, è difficile effettuare un embedding senza rendere visibile il marchio inserito.

Secondo tale classificazione, si può affermare che:

- L'embedding nella banda LL è più resistente a compressione JPEG, aggiunta di disturbo Gaussiano, ridimensionamento, rotazione, blurring, ritaglio, pixelation e sharpening.
- L'embedding nelle bande HL, LH e HH è più resistente a correzione di intensità, correzione della gamma e histogram equalization.
- L'embedding in tutte e quattro le bande risulta in estrazioni identiche per attacchi di re-watermarking e di collusione.

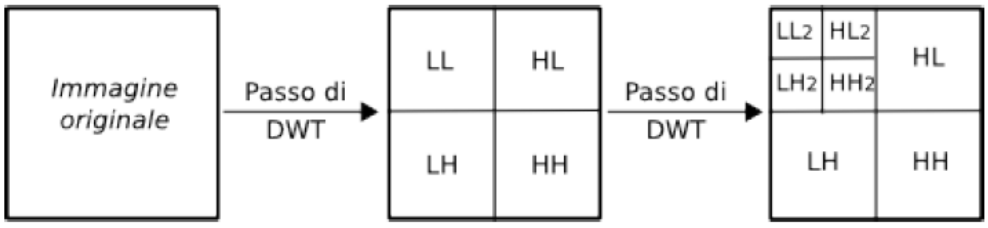

Figura 21: Schema di suddivisione in sottobande della DWT

Figura 22: Esempio DWT (originale)

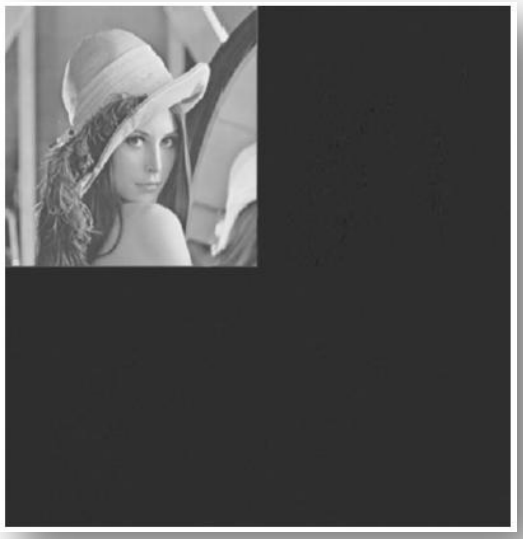

Figura 23: Esempio DWT (prima applicazione della DWT)

Figura 24: Esempio DWT (seconda applicazione della DWT)

2.3.5 Schema di Dugad

Lo schema di Dugad (12) un algoritmo blind, che opera nel dominio delle wavelet e utilizza una tecnica additiva di embedding; questo significa che i coefficienti modificati nella fase di inserimento del marchio sono un incremento, secondo determinati parametri, dei coefficienti originali. La trasformata wavelet utilizzata è di terzo livello.

Nessun watermark viene inserito nella sottobanda LL. Lo schema di Dugad inoltre effettua un mascheramento visivo implicito del watermark, dal momento che vengono selezionati per l'embedding solo

i coefficienti wavelet con una frequenza abbastanza elevata. Come è stato descritto in precedenza, i coefficienti di elevata frequenza corrispondono alle regioni di texture e bordi di un'immagine e questo ha l'effetto di rendere difficile, da parte dell'occhio umano, l'individuazione delle degradazioni dell'immagine dovute all'inserimento del watermark. Inoltre questi coefficienti sono altamente significativi dal punto di vista di percettibilità, per cui rendono molto difficile la rimozione del watermark senza degradare severamente l'immagine marchiata.

2.3.6 Schema di Inoue

Lo schema di Inoue (12) utilizza anch'esso una trasformata wavelet al livello tre. A differenza dello schema presentato da Dugad effettua l'inserimento del watermark esclusivamente nelle sottobande del terzo livello della trasformata. Anche in questo caso la sottobanda LL viene esclusa dal processo.

Si tratta di uno schema basato su una tecnica di quantizzazione, la quale mira a modificare i coefficienti wavelet di elevata frequenza al pari dello schema precedente, ma in questo caso i coefficienti vengono sostituiti e non incrementati. Il processo di quantizzazione usato da questo schema richiede l'utilizzo di un file nel quale registrare le posizioni in cui i bit del watermark sono stati inseriti. Per questo motivo è considerato uno schema semi-blind.

2.3.7 Vantaggi e svantaggi degli schemi di Dugad e Inoue

L'algoritmo di Dugad presenta tre vantaggi principali:

1. E' un algoritmo di watermarking blind
2. Incorpora un mascheramento visivo implicito
3. Utilizza un watermark di grandezza pari all'immagine

Il terzo punto rappresenta un grande punto di forza, dal momento che consente di mantenere una certa indipendenza dall'ordine dei coefficienti significativi nel processo di rilevazione.

Tuttavia presenta anche due svantaggi:

1. Effettua l'inserimento utilizzando una tecnica additiva
2. Effettua esclusivamente una rilevazione del watermark e non un'estrazione

Il primo punto è negativo, in quanto i rilevatori per schemi che adottano tecniche additive devono correlare i coefficienti dell'immagine possibilmente marchiata con un watermark noto, in maniera da determinare se l'immagine è stata o meno marchiata. Quindi l'immagine stessa deve essere trattata come rumore che rende la rilevazione del watermark estremamente difficile. Per fare in modo di evitare questo fattore, è necessario correlare un numero molto alto di coefficienti, il che richiede di inserire il watermark in molti coefficienti dell'immagine. Questo ha l'effetto di aumentare il grado di degradazione dell'immagine marchiata.

L'algoritmo di Inoue, a sua volta, presenta tre vantaggi principali:

1. Utilizza un processo di quantizzazione per inserire il watermark
2. Effettua l'estrazione del watermark, rendendone quindi possibile la visualizzazione
3. Incorpora anch'esso un mascheramento visivo implicito

Il fatto di utilizzare un processo di quantizzazione permette di non essere influenzati da interferenze dell'immagine originale, a differenza degli schemi additivi. La conseguenza risulta essere che i rilevatori richiedono un watermark molto più piccolo, riducendo il grado di degradazione.

Lo svantaggio di questo schema è fondamentalmente quello di essere uno schema semiblind, per il fatto che necessita per funzionare correttamente dell'insieme di posizioni in cui è stato inserito il watermark.

2.3.8 Schema di Fraser

Nello schema di Fraser (12) vengono condivisi i vantaggi di Dugad e Inoue, rimuovendo la maggior parte degli svantaggi. Questo è possibile utilizzando l'idea di Dugad di un watermark di dimensioni pari all'immagine, in congiunzione con una versione adattata delle tecniche di inserimento e rilevazione basate su quantizzazione dello schema di Inoue. Lo schema risultante è quindi una sorta di versione di Dugad basata su quantizzazione.

Un diagramma che specifica i passi necessari per raggiungere l'obbiettivo viene mostrato nella seguente figura.

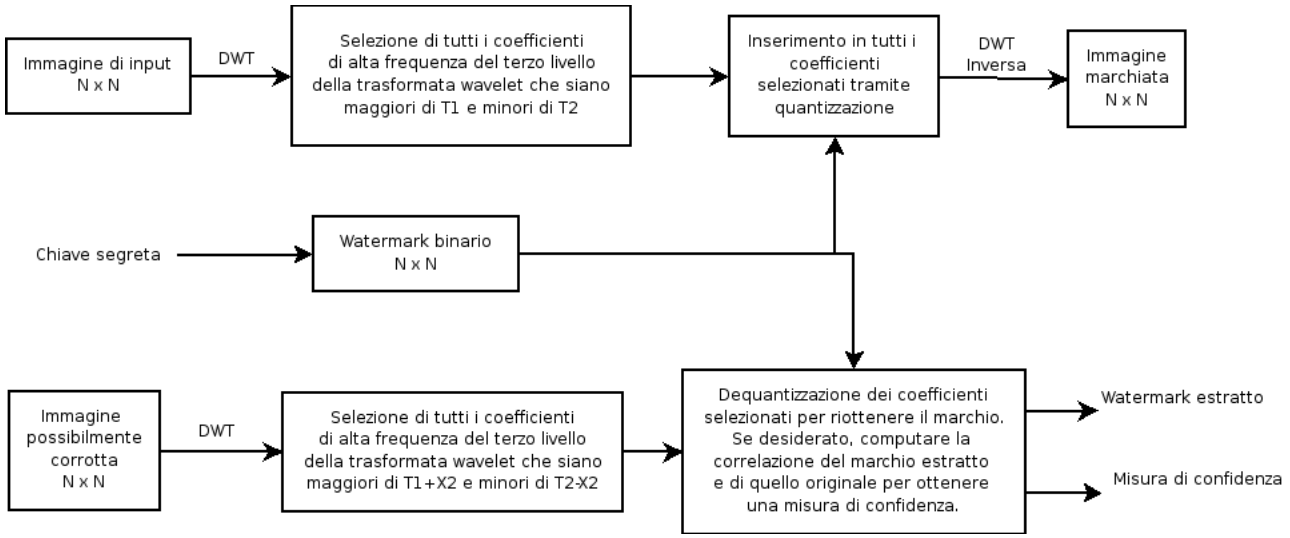

Figura 25: Schema di Fraser. La parte superiore mostra il processo di inserimento, mentre quella inferiore il processo di estrazione

2.3.9 Schema di Watermarking con certificati digitali

In questa sezione verrà illustrato un sistema di digital watermarking per immagini ad alta definizione (12).

2.3.9.1 Scenario di applicazione

Lo scenario di applicazione in cui il sistema risulta funzionale riguarda la necessità di un singolo o di un'organizzazione di pubblicare su Internet un insieme di fotografie. In genere, in queste situazioni è desiderabile l'essere in grado di rintracciare eventuali usi impropri delle immagini oltre a voler fornire agli utenti fruitori delle immagini la possibilità di verificare che una data immagine sia effettivamente di proprietà di un determinato soggetto. Si tratta di uno scenario abbastanza comune e dal momento che il detentore dei diritti di copyright ha la necessità, da un lato di prevenire abusi e dall'altro di mostrare le proprie immagini senza degradazione, la scelta ricade su un sistema di digital image watermarking.

Tuttavia, per garantire la possibilità di effettuare la verifica pubblica delle risorse marchiate, è necessaria l'aggiunta di una sovrastruttura che fornisca lo strato di certificazione del quale è carente un classico sistema di watermarking. In pratica risulta necessario, oltre al garantire il funzionamento dell'inserimento ed estrazione del watermark, fornire un livello che assicuri la validità del watermark stesso.

2.3.9.2 Descrizione del sistema

Il sistema si propone di fornire un'infrastruttura per la gestione di watermarking applicato ad immagini, che possa soddisfare le necessità dei soggetti descritti precedentemente. L'intera infrastruttura permette non soltanto di marchiare immagini e verificare la presenza di un marchio, ma soprattutto di garantire l'autenticità dello stesso.

Per raggiungere il duplice scopo di tutelare da una parte l'utente che intende pubblicare le proprie immagini e, in secondo luogo, la necessità di garantire utente generico da false attestazioni di possesso, è sorta la problematica di dover aggiungere una terza parte che si ponesse come garante. Di seguito si descriverà il metodo adottato.

Analizzandolo ad alto livello, il sistema si scompone in due *sottosistemi*:

- il primo, che permette all'utente di marchiare le proprie immagini, definisce il processo di inserimento e validazione della marchiatura
- il secondo, in maniera complementare, permette ad un utente generico di verificare l'autenticità della marchiatura di una data immagine, dunque di definire con notevole certezza il legittimo detentore dei diritti di autore della stessa.

Parleremo nel primo caso di processo di inserimento, mentre nel secondo caso di processo di verifica; al centro dell'intero sistema è presente il marchiatore/verificatore, il quale risiede ad esempio su di un server, e copre il ruolo di garante o terza parte accennato sopra. Per comprendere maggiormente lo schema è necessario entrare nel dettaglio dei sottosistemi appena citati.

2.3.9.3 Processo di Inserimento

L'inserimento prevede un'interazione tra l'utente interessato alla marchiatura delle proprie immagini e il marchiatore.

I requisiti per avviare il processo sono:

- possedere un proprio certificato di chiave pubblica
- possedere l'immagine che desidera marchiare.

L'utente invia in input al marchiatore l'immagine, ed una chiave KEY; questa viene prodotta semplicemente firmando il proprio certificato di chiave pubblica.

Ricevuta la coppia di input, il marchiatore si occupa di verificare tramite il certificato dell'utente, la validità di KEY. In caso di verifica andata a buon fine memorizza KEY in un database. Tale scelta è dettata, come si vedrà nel processo di verifica, dal bisogno di risalire ad una certa KEY partendo da un certificato. Si noti che è anche possibile associare alla chiave l'identificativo del relativo certificato utente, in modo da velocizzare la successiva verifica delle firme.

Una volta completate queste operazioni il marchiatore si occupa di effettuare l'inserimento di un watermark nell'immagine. Allo scopo di aumentare la robustezza del sistema, il watermark è prodotto a partire da KEY.

A questo punto l'immagine è stata marchiata ed è pronta per essere inviata nuovamente all'utente, il quale può utilizzarla per i propri scopi.

Per ottenere un maggiore livello di sicurezza nell'intero sistema, l'immagine originale dovrebbe essere distrutta, in modo da evitare un'ulteriore marchiatura della stessa con chiave differente. E' necessario sottolineare, inoltre, l'importanza di garantire un canale sicuro di comunicazione tra l'utente e il marchiatore sia in fase di invio dell'input, sia in fase di invio dell'output. Infatti è fondamentale assicurare l'integrità dei dati in input, così come dell'immagine marchiata, al fine di evitare attacchi di tipo *Man in the Middle*.

2.3.9.4 Processo di verifica di un'immagine marchiata

Il sottosistema di verifica è fortemente influenzato, come si può ben comprendere, dal presupposto di creare un sistema di validazione della marchiatura che permetta a chiunque, in possesso di determinate informazioni, di verificare la presenza e l'autenticità di una marchiatura in una o più immagini.

Le informazioni necessarie per avviare il processo di verifica da parte di un utente generico sono:

- un'immagine marchiata con il processo di inserimento descritto
- il certificato dell'utente che si propone come detentore dei diritti d'autore sull'immagine.

Come si può facilmente notare, si tratta di informazioni che chiunque risulta essere in grado di procurarsi, nel momento in cui le immagini siano pubblicate su Internet e il certificato venga reso pubblico tramite le apposite Certification Authority (CA).

Non appena in possesso dell'immagine e del certificato del presunto utente marchiatore, il validatore procede con il reperimento della KEY dal database. In particolare, attraverso una verifica della firma del certificato è possibile recuperare la KEY relativa allo specifico certificato. In caso di ritrovamento della KEY, il verificatore utilizza tale chiave per il processo di estrazione del watermark dall'immagine ottenuta precedentemente. Si noti che per velocizzare l'operazione di ricerca della KEY è possibile far uso dell'identificativo del certificato come chiave di ricerca.

Come espresso nel capitolo precedente, un sistema di marchiatura che non si limita a rilevare la presenza del watermark ma ne effettua l'estrazione permette non solo di provare ma anche di verificare la l'identità del possessore di una determinata immagine.

Questo è esattamente lo scopo che il processo di estrazione si prefigge di raggiungere: infatti, in caso di immagine marchiata correttamente, si procede con il processo di estrazione del watermark. Se quest'operazione da esito positivo, è possibile affermare con ragionevole certezza che il possessore del certificato utilizzato ha marchiato l'immagine analizzata.

In caso il marchio non venga trovato nell'immagine analizzata, si può concludere che tale immagine non appartiene all'utente possessore del certificato di chiave pubblica utilizzato nel processo di verifica.

2.3.9.5 Descrizione dell'algoritmo di Watermarking

L'algoritmo adottato come nucleo del sistema è una implementazione di quello proposto da Steward I. Fraser e Alastair R. Allen.

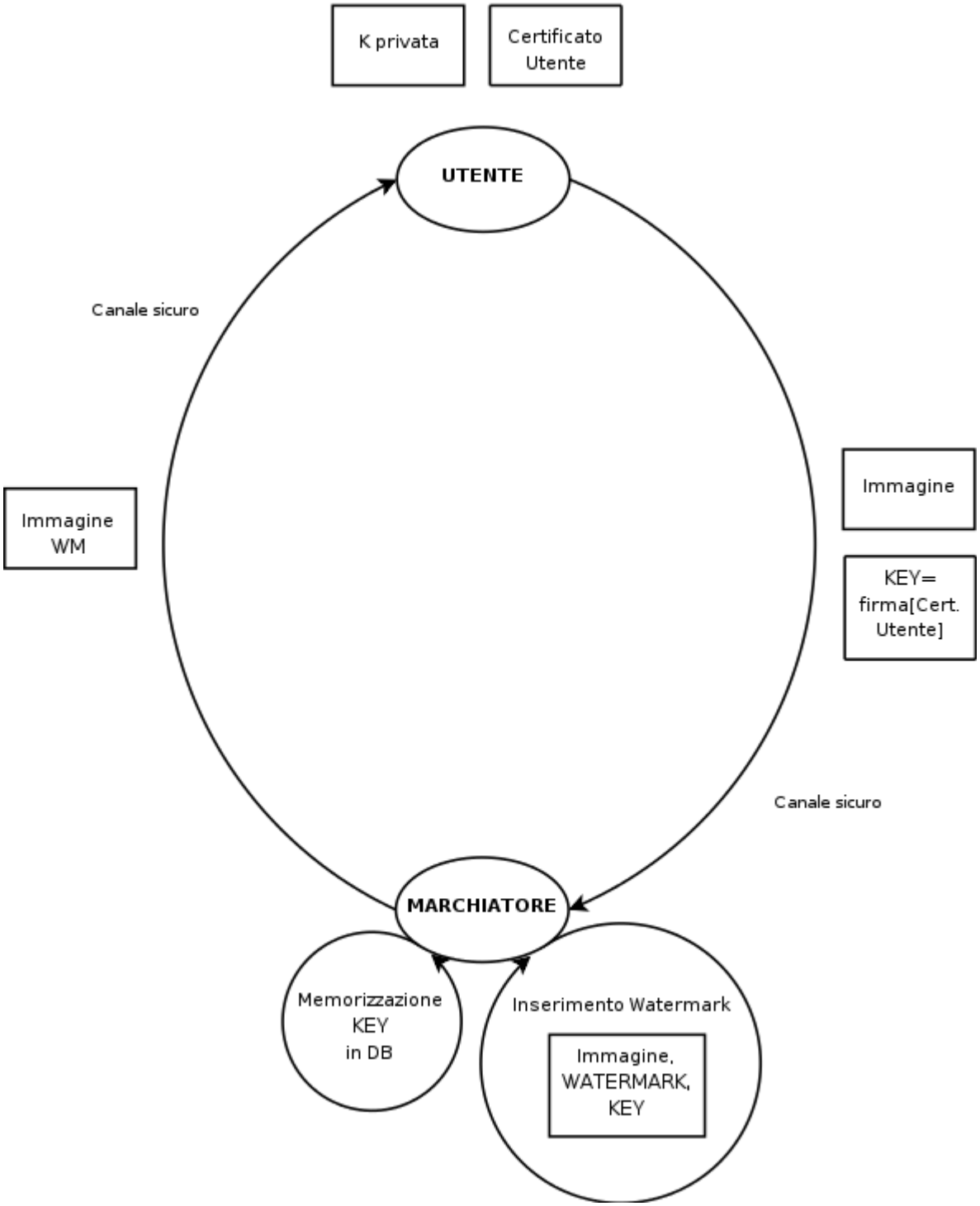

Figura 26: Schema di inserimento

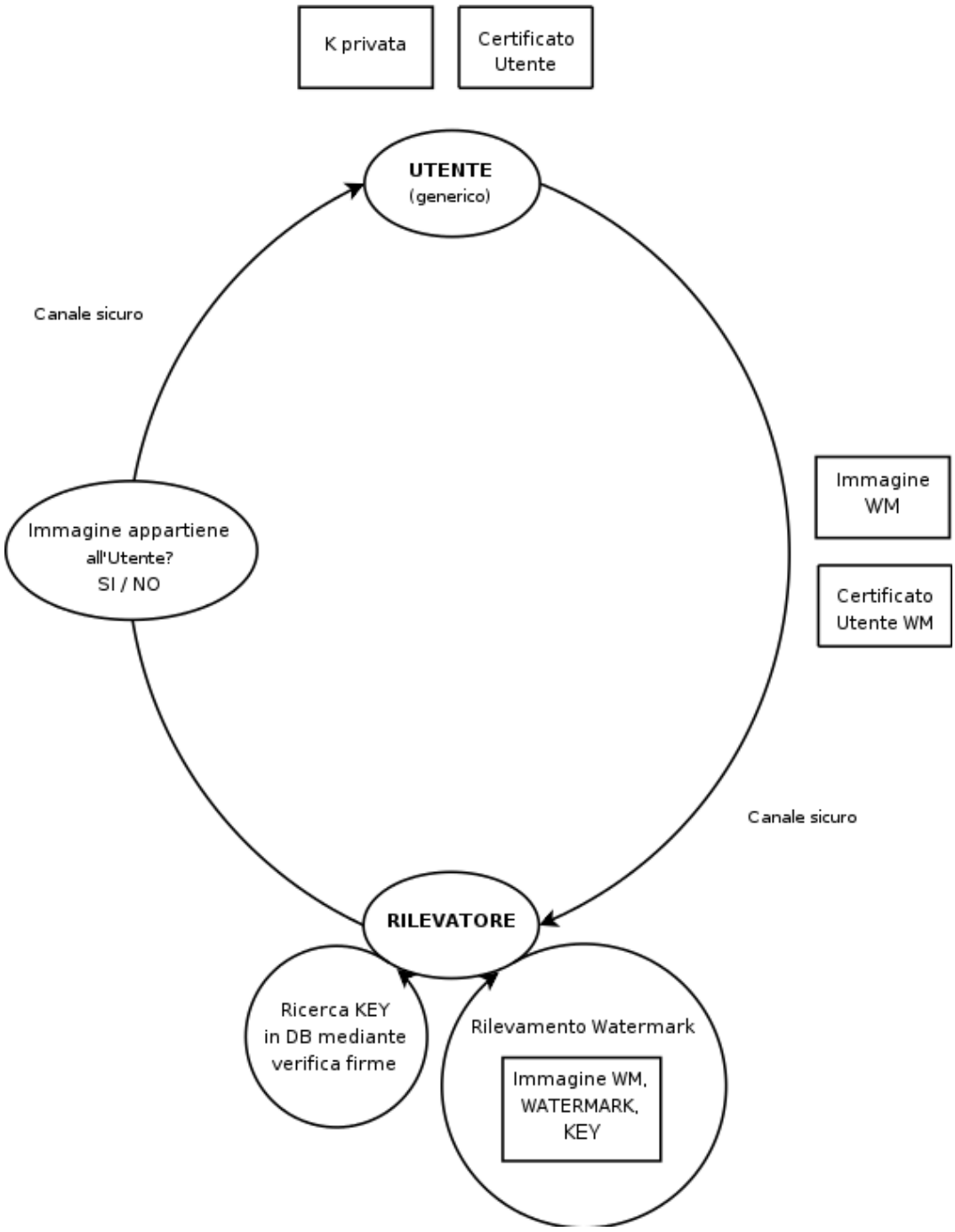

Figura 27: Schema di verifica

2.4 Possibili attacchi

La robustezza del watermark è necessaria ma non sufficiente a garantire la sicurezza. Con questi paragrafi mostriamo che uno schema di watermarking può essere attaccato in diversi modi.

2.4.1 Attacchi alla Robustezza

Questo tipo di attacco mira a rendere inutile oppure a rimuovere il marchio cercando però di non degradare l'immagine. Tali attacchi vanno a modificare il valore dei pixel e possono essere di due tipi: quelli basati trasformazione del dato, e quelli basati su un algoritmo analitico.

Attacchi del primo tipo sfruttano le tipiche trasformazioni dell'immagine quali compressioni, filtraggio, ridimensionamento, stampa, scannerizzazione. Tali operazioni vengono compiute normalmente per dare la possibilità di diminuire la dimensione delle immagini, così da rendere più veloce il download dalla rete.

Attacchi del secondo tipo sfruttano l'analisi degli algoritmi di inserimento o di individuazione del marchio così da ricavare, quando è possibile, vantaggi per l'attacco al marchio, una descrizione più approfondita di tali attacchi non può essere data visto che, tali tecniche, sono diverse a seconda dell'algoritmo usato.

2.4.2 Attacchi di presentazione

Tali attacchi sono diversi dai precedenti perché non necessariamente rimuovono il marchio dall'immagine marcata ma la modificano in modo che l'algoritmo di verifica non sia utilizzabile. Per esempio, un attacco di presentazione può essere usato per ingannare un detector di watermark, come può essere un agente Web-based.

Un buon esempio di tale attacco è stato proposto da F. Peticolas dell'Università di Cambridge, l'attacco si basa sul cut, dell'immagine marcata, in piccole porzioni che poi vengono riassemblate su una pagina Web con appropriati tag HTML. Un *webcrawler*, che è preposto all'individuazione del marchio, non riesce ad individuarlo perché "vede" i blocchi individualmente, e tali blocchi sono troppo piccoli per contenere un watermark. Il vantaggio di questo tipo di attacco è che l'immagine non subisce alcuna modifica e di conseguenza non si ha degrado della stessa.

L'idea di base dell'attacco di presentazione è dovuta al fatto che uno schema di watermark può richiedere che un'immagine marcata debba essere perfettamente allineata prima che il marchio possa essere verificato.

2.4.3 Attacchi di interpretazione

Un attaccante può inserire all'interno dell'immagine marcata un suo marchio, in modo tale da andare a confutare in fase di disputa, la paternità dell'immagine.

Per fare ciò, però, un tipico attacco di interpretazione richiede un'analisi approfondita dello specifico algoritmo di watermark utilizzato per l'inserimento del marchio.

Qui di seguito andiamo ad esporre un attacco per interpretazione.

L'attacco lavora su una classe di algoritmi che, senza perdere in generalità, possono essere descritti usando la formula $I_w = I + W$; ad un'immagine I viene aggiunto un marchio W che è costituito da piccoli valori per non causare degradazione dell'immagine.

L'immagine marcata è denotata con I_w. Alice proprietaria dell'immagine originale I e del marchio W distribuisce I_w. Il marchio può essere estratto da un'immagine applicando il processo inverso rispetto all'inserimento, proprio per questo bisogna andare a studiare l'algoritmo di inserimento del watermark (nel nostro caso supponiamo, per semplicità che il marchio venga inserito andandolo a sommare all'immagine originale). Per dimostrare che tale immagine è originale bisogna che il marchio estratto sia uguale o quasi a quello inserito W. Così avendo un'immagine sospetta I' è possibile computare $W' = I' - I$ e $P = C(W, (I - I'))$, dove $C(W, W')$ misura la "somiglianza" tra i due marchi; tale tipo di schema però per funzionare ha bisogno dell'immagine originale in fase di rilevazione.

Per eseguire un attacco di interpretazione, un attaccante Bob, inverte la procedura di inserzione del marchio; cioè va a sottrarre un marchio W_b. Bob computa $I_b = I_w - W_b$ ed afferma che I_b è l'immagine originale e W_b è il marchio.

A questo punto sia Alice che Bob possono affermare di aver creato I_w; infatti ciascuno dei due può calcolare il proprio originale, generando così una disputa:

$$N_a = I_b - I_a = W_a - W_b$$

$$P_a = C(N_a, W_a) = C(W_a - W_b, W_a)$$

$$N_b = I_a - I_b = W_b - W_a$$

$$P_b = C(N_b, W_b) = C(W_b - W_a, W_b)$$

Così la presenza del marchio di Alice nell'immagine di Bob è P_b, mentre la presenza del marchio di Bob in quella di Alice è P_a. Il grosso problema adesso è la simmetria: "Vi è la presenza multipla del marchio di Bob nell'immagine di Alice o il contrario?" A questo punto si ha il conflitto che ci porta ad una situazione di stallo.

2.4.4 Attacchi legali

Questo tipo d'attacco è molto diverso dai precedenti, infatti mentre gli attacchi visti prima si basavano sulle vere e proprie tecniche di inserimento, questi ultimi si basano sui *cavilli legali* e sulle diverse interpretazioni delle leggi in merito alla protezione del copyright, sulla credibilità del proprietario e dell'attaccante, sull'abilità da parte di un attaccante di dimostrare la paternità dell'immagine in un'aula di tribunale e così via.

Lo studio di attacchi legali esula dagli attacchi basati su algoritmi precisi. Inoltre oggigiorno tutta l'infrastruttura legale che dovrebbe garantire la salvaguardia del copyright, si trova impreparata rispetto a tale problema e questo è un fattore molto limitativo che diminuisce la protezione che il watermark dovrebbe garantire.

Attacchi tipici sulle immagini marcate sono i seguenti:

- Attacchi con aggiunta di rumore. Il watermark viene attaccato aggiungendo un valore random ad ogni pixel. I valori devono essere abbastanza piccoli al ne di non degradare pesantemente l'immagine.
- Attacchi con marcature multiple. L'attaccante spera di danneggiare il watermark iniziale inserendo nell'immagine un secondo watermark nella stessa immagine.
- Attacchi interattivi. Tali attacchi sono apportabili quando e pubblica la procedura di rilevamento del watermark. In tal caso, infatti, e possibile modi care l'immagine, estrarre il watermark per valutare il danno apportato e ripetere l'operazione no a quando la presenza del watermark non viene eliminata.
- Attacchi di inversione. L'attaccante cerca prima di individuare il watermark nel documento. Poi cerca di determinarlo e in ne di rimuoverlo. Il processo di rimozione in questo caso e l'inverso di quello di immersione (se il watermark e stato aggiunto attraverso un'addizione, la rimozione avviene tramite una sottrazione...).
- Attacchi per cospirazione. Più cospiratori posseggono copie diverse della stessa immagine, che differiscono soltanto perché ognuna di essa ha un differente watermark. L'attacco consiste nel

produrre una nuova immagine i cui pixel sono ottenuti mediando i pixel delle immagini in possesso dei cospiratori ed eventualmente aggiungendo del rumore. L'auspicio e che la nuova immagine dovrebbe essere ancora “vicina” a quelle vendute ai cospiratori ma non dovrebbe presentare più le marche in esse presenti.

2.4.5 Altri attacchi

- Compressioni lossy: molti schemi di compressione come JPEG, eliminano, allo scopo di comprimere l'immagine, le informazioni meno visibili all'occhio umano. Queste stesse informazioni vengono spesso utilizzate dagli schemi di watermarking per inserire il watermark.
- Distorsioni geometriche: questa tipologia di attacchi include la rotazione, la traslazione, il ridimensionamento e il ritaglio dell'immagine.
- Comuni operazioni di Signal Processing: in questo caso si tratta di operazioni di signal processing quali conversioni A/D e D/A8, resampling, requantization, linear filtering (filtri passa-alto e passa-basso), non-linear filtering (median filtering), riduzione di colori, aggiunta di un offset costante al valore dei pixel, aggiunta di rumore Gaussiano e non Gaussiano, scambio locale di pixel, ecc.
- Altri attacchi intenzionali: si tratta di una serie di attacchi che vengono operati intenzionalmente con lo scopo di bypassare o invalidare il sistema di watermarking. Tra questi identifichiamo:
    - Stampa e scannerizzazione. Nel passaggio da digitale a cartaceo e viceversa è possibile che vengano perse le informazioni contenenti il marchio.
    - Rewatermarking, ovvero il watermarking di un'immagine marchiata. In questo caso lo scopo è di sovrascrivere il marchio o di ingannare il sistema di watermarking.
    - Collusione. I possessori autorizzati di una serie di copie della stessa immagine marchiata differentemente non dovrebbero essere in grado di generare l'immagine originale non marchiata.
    - Forgery. I possessori autorizzati di un'immagine non dovrebbero essere in grado di generare una copia marchiata con informazioni riguardanti una terza parte.
    - IBM Attack. Non dovrebbe essere possibile produrre un falso originale che sia uguale all'originale e inoltre permetta l'estrazione di un watermark come affermato dal possessore della falsa copia.

3 Audio Watermarking

3.1 Introduzione

Il digital audio watermarking (13) riguarda l'occultamento di dati all'interno di un file audio. Le applicazioni per questa tecnologia sono numerose. La protezione della proprietà intellettuale è la motivazione principale che spinge la ricerca in quest'area. Per combattere la **pirateria musicale** online, un watermark digitale potrebbe essere aggiunto ad un file audio prima del suo rilascio, portando con se informazioni non solo sull'autore ma anche sull'utente che ne ha acquistato legittimamente acquistato una copia. I sistemi operative più recenti, dotati di software per il **Digital Rights Management** (DRM) possono estrarre il watermark da un file audio prima di riprodurlo in modo tale da assicurare che l'utente abbia pagato l'ascolto confrontando il watermark estratto con la licenza presente sul sistema.

Altri utilizzi della tecnologia di watermarking non relativi alla gestione dei diritti riguardano l'inclusione di informazioni ausiliarie relative ad una particolare canzone, come il testo, informazioni sull'album, etc. Tecniche di audio watermarking possono essere utilizzate in voice conferencing system per indicare alla controparte l'oratore corrente.

Quanto trattato in seguito richiede nozioni relative all'elaborazione dei segnali, con particolare attenzione al processo di conversione analogico/digitale, brevemente ripreso nelle sezioni successive.

3.1.1 I segnali audio ed i file audio

L' elaborazione dei segnali audio, è un aspetto particolare di un importante settore dell'informatica che si occupa dell'acquisizione e dell'elaborazione di segnali analogici dipendenti da grandezze fisiche di varia natura, al fine di effettuare il controllo della grandezza in esame o anche semplicemente la visualizzazione, la memorizzazione o la trasmissione dei valori che essa assume. Affinché i segnali analogici (qual è il segnale audio) possano essere elaborati da un calcolatore digitale, è necessario che essi vengano convertiti in segnali digitali; i dati elaborati verranno poi eventualmente riconvertiti in forma analogica per essere utilizzati. Nel nostro caso il segnale audio verrà convertito in segnale digitale, subirà il watermarking, verrà memorizzato in un file, ed infine, ogni volta che ne ascolteremo il contenuto, implicitamente effettueremo una conversione digitale/analogico. E' in seguito riportato uno schema generale di un sistema di acquisizione dati, evidenziando poi il significato che i vari blocchi assumono nel nostro caso particolare.

Il primo blocco, il trasduttore, ha la funzione di fornire in uscita una grandezza elettrica di valore proporzionale all'entità o alla variazione della grandezza fisica in esame. Nel nostro caso il trasduttore è costituito dal microfono, che fornisce un segnale proporzionale alla pressione dell'onda sonora. Dopo che i dati analogici provenienti dal "mondo reale" sono stati convertiti in forma digitale e memorizzati o elaborati, spesso il risultato delle elaborazioni deve nuovamente interagire con il mondo esterno. L'ultimo blocco assolve a tale compito; nel nostro caso esso è costituito dalle casse del PC, dalle cuffie, o da qualsiasi tipo di altoparlante.

3.1.2 La Conversione Analogico/Digitale.

Un segnale è una grandezza che varia nel tempo. Più formalmente, può essere definito come una funzione il cui dominio è il tempo ed i valori che essa assume rappresentano valori di tensione. Il segnale elettrico in uscita dal microfono è un segnale analogico: esso può assumere infiniti valori di tensione in un intervallo di tempo continuo.

Un segnale, nel periodo di tempo T, assume infiniti valori compresi tra un massimo e un minimo. Lo scopo del convertitore analogico digitale è far in modo che il segnale assuma soltanto un numero finito di valori discreti di tensione, ed associare ad ogni valore discreto di tensione, una sequenza di bit. Per far ciò, viene introdotto il concetto di **quantizzazione**, secondo il quale, gli infiniti valori del segnale analogico devono essere quantizzati ovvero raggruppati in un certo numero di fasce delimitate da livelli fissi detti livelli di quantizzazione; a ciascuna fascia di valori analogici corrisponderà un solo valore digitale. La distanza fra due livelli di quantizzazione contigui costituisce il passo di quantizzazione Q a cui corrisponde il valore del bit meno significativo (LSB: least significant bit). Un dato digitale ad n bit può esprimere $2n$ valori, da 0 a $2n-1$; il valore digitale $2n-1$ viene pertanto associato al valore di fondo scala (FS o FSR: full scale range, valore massimo di tensione che può assumere il segnale) della grandezza analogica. Conseguentemente il valore analogico corrispondente al bit meno significativo sarà $FS/_{2n}$. Ad esempio, un convertitore A/D con tre bit di uscita potrà quantizzare il segnale di ingresso con $2^3 = 8$ valori, essendo solo otto le possibili combinazioni di tre bit. Se lo stesso convertitore ha un fondo scala $FS = 8\,V$, il passo di quantizzazione, pari cioè al valore dell' LSB, è di $1\,V$.

In un ADC (analog to digital converter) i valori digitali di uscita non riproducono dunque fedelmente il segnale di ingresso ma ne danno una rappresentazione approssimata, tanto più precisa quanto minore è il passo di quantizzazione Q, cioè quanto più numerosi sono i livelli di quantizzazione. Questi ultimi, d'altra parte, sono legati al numero di bit utilizzati per la rappresentazione digitale e quindi sono necessariamente in numero limitato. Sono comuni convertitori A/D con uscite a 8, 10, 12 bit, che consentono, rispettivamente, $2^8 = 256$, $2^{10} = 1024$, $2^{12} = 4096$ livelli di quantizzazione. Il numero di bit di uscita di un convertitore A/D, viene generalmente chiamato risoluzione poiché implicitamente indica qual è la minima variazione del segnale di ingresso che può essere rivelata in uscita (pari a $FS/_{2n}$ per un convertitore ad n bit).

3.1.3 Campionamento

Un altro concetto implicito nella conversione A/D è quello di campionamento del segnale in vari istanti successivi. Infatti la conversione consiste nel prelevamento di un campione del segnale ad un dato istante e nella determinazione del corrispondente valore digitale, che resterà fisso finché non verrà prelevato un altro campione per una nuova conversione. La frequenza con cui il segnale viene prelevato è detta **frequenza di campionamento**; essa ha un'importanza fondamentale in riferimento al contenuto informativo del segnale campionato e alle possibilità di ricostruire fedelmente il segnale analogico originario.

Per enunciare il teorema del campionamento è necessario descrivere brevemente **l'analisi di Fourier**. Si ricordi innanzitutto che una funzione sinusoidale, quale il seno o il coseno, è caratterizzata da alcuni parametri:

- *ampiezza* A: la differenza fra il valore massimo ed il minimo;
- *periodo* T: la quantità di tempo trascorsa nella quale la funzione si ripete;
- *frequenza* F: il reciproco del periodo $F = 1/_T$, misurata in cicli al secondo (Hz).

Fourier (matematico francese dell'800) dimostrò che una funzione $g(t)$, definita in un intervallo T, può essere espressa come una somma di un numero infinito di funzioni sinusoidali:

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L} \right)$$

Dunque, un segnale variabile nel tempo è di fatto equivalente ad una somma di funzioni sinusoidali aventi ciascuna una propria ampiezza e frequenza. Si può quindi rappresentare un segnale $g(t)$ di durata T in un modo diverso, e cioè attraverso il suo spettro di frequenze, ossia attraverso la sua scomposizione in sinusoidi.

Qualunque segnale è pertanto caratterizzato da un intervallo di frequenze nel quale sono comprese le frequenze delle sinusoidi che lo descrivono. Esso va sotto il nome di banda di frequenza (frequency band) del segnale.

Il teorema del campionamento, noto anche come **teorema di Shannon**, stabilisce che la frequenza di campionamento deve essere maggiore o uguale al doppio di quella della componente di frequenza più elevata del segnale in esame. Pertanto un segnale analogico $V_a(t)$, la cui componente armonica più elevata abbia frequenza f_m, potrà essere determinato univocamente a partire dai valori campionati se la frequenza di campionamento $f_c \geq 2f_m$.

Frequenze di campionamenti tipiche vanno dagli 8kHz ai 48 kHz. La frequenza di 8 kHz copre frequenze fino a 4kHz, che è il limite massimo di frequenza di suoni prodotti dalla voce umana. La frequenza di campionamento di 48 kHz copre invece frequenze fino a 24 kHz, ed inoltre, copre l'intero intervallo di frequenze udibili dall' orecchio mano, che si estende dai 100 Hz ai 20 kHz.

Riassumendo, la conversione analogico digitale consiste nel campionare il segnale audio d'input ad intervalli regolari di tempo e nel raggruppare i valori ottenuti in un numero discreto di livelli. Il segnale digitale consiste dunque di una sequenza di valori binari ognuno dei quali rappresenta il valore quantizzato del corrispondente campione audio. Tale sequenza, memorizzata su un dispositivo di memoria di massa, costituirà il file audio relativo al segnale convertito.

3.1.4 Effetto mascheramento e watermarking

Recenti ricerche sul copyright audio, video e d'immagine, hanno mostrato che la percezione audio umana non può determinare piccoli cambiamenti in certe componenti di frequenza del segnale audio. Questa proprietà è definita **mascheramento**, in accordo alla quale un debole ma percettibile segnale audio diviene non percettibile in presenza di un forte segnale audio di frequenza leggermente superiore. Tale fenomeno si verifica quando nel segnale che viene inviato all'orecchio sono presenti più segnali: se abbiamo ad esempio un segnale ad una data frequenza ed un altro segnale, di livello più basso e ad una frequenza leggermente inferiore, quest'ultimo viene *"mascherato"* dal primo e l' orecchio non lo percepisce.

La sensibilità dell'orecchio umano è alta per valori di frequenza tra 2.5 e 5 kHz, e decresce man mano che ci si allontana da questo intervallo di frequenze. La sensibilità è rappresentata dalla curva *"soglia in quiete";* ogni suono al di sotto di tale soglia non sarà percepito. Ciò significa che un suono con frequenza di 3kHz e di un livello bassissimo sarà udito senza problemi dall' orecchio umano; mentre affinché venga percepito un suono con frequenza di 10 kHz, esso deve misurare all' incirca 10dB. La curva *"soglia mascherante"* rappresenta la variazione di sensibilità dell' orecchio umano sottoposto ad un segnale di altissimo livello. Il segnale mascherato, pur essendo percettibile in condizioni normali in quanto al di sopra della soglia d'udibilità, diviene non percettibile a causa dell' altro segnale.

L'effetto del mascheramento ha varie applicazioni. Esso viene sfruttato nell'algoritmo di compressione **MPEG**, il quale va a *"scovare"* nel segnale audio tutti i segnali di livello alto ed elimina quelli immediatamente adiacenti (di frequenza leggermente inferiore) di livello più basso. In alcuni schemi di watermarking tale effetto viene sfruttato *"al contrario"* di come avviene nell' algoritmo MPEG: affinché il segnale marcato sia inconfondibile da quello originario, il segnale watermark viene inserito in prossimità di segnali di livello alto, in modo tale che esso venga mascherato da quest'ultimi.

Si noti che tali schemi sono fragili, in quanto una successiva codifica MPEG eliminerebbe il watermark. Altri metodi di watermark consistono nell'inserire un segnale watermark la cui frequenza sia al di fuori dell'intervallo di frequenze udibili dall'orecchio umano (quindi segnali di frequenza minore di 100Hz, o maggiore di 20 KHz). Lo schema di watermark che trattiamo è un potenziale metodo di watermark che tiene in considerazione le specifiche della percezione umana. Tale schema di w. modifica ogni campione audio considerando la sua ampiezza e se esso è effettivamente percettibile. Diversamente da altri metodi proposti esso non richiede il segnale originale per la sua individuazione. In tal modo il proprietario dei dati non ha bisogno di mantenere due copie, l'una per il prodotto originale, l'altra per quello marcato.

3.2 An Affine Resistant Watermarking Scheme for Audio Signals

Questo schema (14) si basa su un nuovo approccio per inserire un watermark digitale non udibile all'interno di un file audio, nel dominio temporale. Tale approccio consiste nel codificare un watermark all'interno di una portante di un segnale audio, shiftando nel tempo blocchi del segnale portante in tutta la banda o in sottobande. Ci sono differenti tecniche, anche per quanto riguarda il watermarking analogico, che utilizzano lo shifting del segnale portante, questo schema sfrutta la somiglianza dei dati audio nei due canali di un segnale stereo.

Lo schema proposto non richiede il segnale sorgente per l'estrazione del watermark (blind) ed è resistente ai più comuni attacchi quali: requantization, transcoding, manipolazioni dell'onda e dello spettro. All'interno del segnale audio vengono nascoste due tipi di informazioni:

- relative al proprietario, sottoforma di immagine binaria;
- un template di sincronizzazione, generato in modo casuale e controllato da una chiave segreta, utilizzato per sincronizzare le alterazioni causate dagli attacchi di time shifting, cropping e time scaling.

I due tipi di informazioni sono combinate e *"disperse"* da un'altra chiave segreta, prima della procedura di embedding. L'estrazione del watermark non è possibile senza tali chiavi.

La chiave è univoca per ogni segnale sorgente e dipende solo dalla dimensione del watermark da inserire, non dal suo contenuto.

La tecnica proposta può essere utilizzata per implementare la ricerca di file audio protetti da un database (come il World Wide Web) cercando prima il template di sincronizzazione e mostrando poi le informazioni sul proprietario, se il file è dotato di watermark.

3.3 DC Watermarking Scheme

Il DC watermarking scheme (15) nasconde i dati del watermark nelle componenti a più bassa frequenza di un segnale audio, che sono di solito al di sotto della soglia di percezione del sistema uditivo umano.

3.3.1 Inserimento del Watermark

Il processo di inserimento di un watermark digitale all'interno di un file audio può essere diviso in 4 processi principali. Il file audio originale in formato wave è dato in pasto al sistema, dove viene in seguito sottoposto alle seguenti operazioni:

- Divisione in frame;
- Analisi dei frame creati precedentemente;
- Inserimento del watermark al segnale in output.

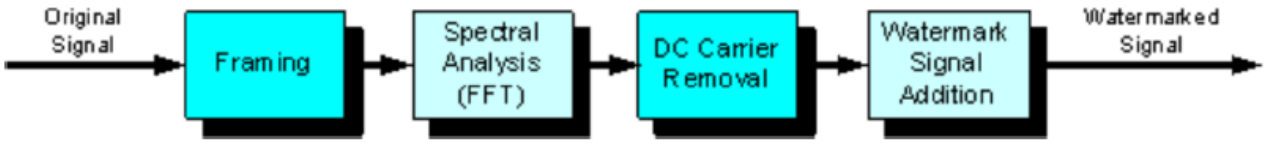

Figura 28: Procedura di inserimento del watermark

3.3.1.1 Framing

Il file audio è partizionato in frame della durata di 90ms. La dimensione del frame è scelta in modo tale da non introdurre distorsioni udibili nel file. Con un frame di questa dimensione possiamo inserire $^{1}/_{0{,}09} = 11.1\ bit/s$ di dati.

3.3.1.2 Spectral Analysis

Questa fase consiste nell'applicazione della **Fast Fourier Transform** (FFT), che consente di calcolare le componenti a bassa frequenza per ogni frame:

$$F(k) = \sum_{n=1}^{N} f(n) e^{\frac{-j2n(n-1)(k-1)}{N}} \quad k = 1,2, \dots, N$$

dove con N denotiamo l'ultimo frame.

Con un file audio standard di qualità CD a 16 bit con frequenza di campionamento $F_s = 44{,}100\ samples\ per\ second$, un frame consiste di 3969 samples. Se la FTT viene eseguita su un frame di questa dimensione con $N = 3969$, la frequency resolution risultate è:

$$\frac{44.100\ Hz}{2 * \frac{3969}{2} samples} = 5{,}6\ Hz\ resolution$$

Dalla FFT è ora possibile calcolare la componente a bassa frequenza (DC) del frame $F(1)$, così come la frame spectral power:

$$P_{Frame}(n) = \frac{1}{\left(\frac{3969}{2} + 1\right)} \sum_{k=1}^{3969+1} F(k)^2 \quad n = 1,2, \dots, N$$

La figura seguente mostra un esempio dell'analisi di cui sopra, completata sui primi 8 frame di un file audio di esempio.

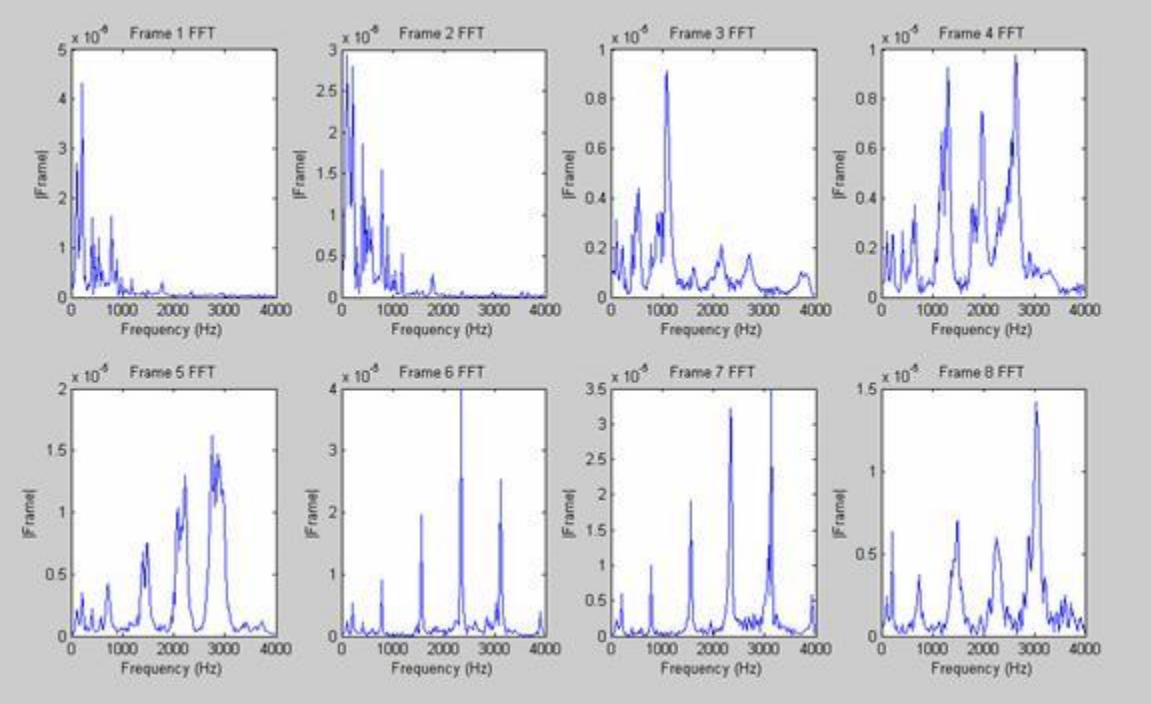

Figura 29: Analisi dello spettro di un file audio di esempio

3.3.1.3 DC Removal

Dall'analisi dello spettro di ogni frame è stato possibile calcolare la componente a bassa frequenza (DC) $F(1)$, la quale può essere ora rimossa sottraendola da ogni frame usando la seguente formula:

$$f(n) = \sum_{k=1}^{3969n} f(k) - F(1) \qquad n = 1,2,\dots,N$$

3.3.1.4 Watermark Signal Addition

Dall'analisi dello spettro di ogni frame completata precedentemente, si è calcolata anche la spectral power per ogni frame utile per l'inserimento del watermark nel segnale audio. La potenza in ogni frame determina l'ampiezza del watermark che può essere aggiunto allo spettro delle basse frequenze. Il watermark è quindi aggiunto in accordo alla seguente formula:

$$f(n) = \sum_{k=1}^{3969n} f(k) + K_s * w(n) * P_{frame}(n) \qquad n = 1,2,\dots,N$$

Dove K_s è un fattore di scala, il quale assicura che il watermark sia aggiunto al di sotto della soglia di impercettibilità e $w(n)$ rappresenta il segnale binario del watermark, avente valori 1 o -1.

3.3.2 Estrazione del Watermark

Il processo di estrazione del watermark digitale dal file audio è simile alla tecnica di inserimento. I requisiti di potenza di calcolo necessaria per l'estrazione sono leggermente minori.

Un file audio marcato in formato wave è dato in pasto al sistema che procede alle stesse operazioni della fase di inserimento:

- Divisione in frame;
- Analisi dei frame creati precedentemente;
- Estrazione del watermark dal segnale in input.

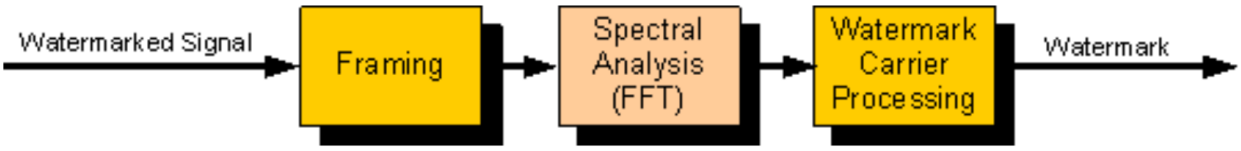

Figura 30: Processo di estrazione del watermark

3.3.2.1 Framing

Così come nel processo di inserimento, il file audio è partizionato in frame della durata di 90ms. Con un frame di questa dimensione possiamo inserire $^{1}/_{0,09} = 11.1\ bit/s$ di dati.

3.3.2.2 Spectral Analysis

La spectral analysis del segnale consiste nell'applicazione della fast Fourier transform (FFT), che di nuovo consente di calcolare le componenti a bassa frequenza di ogni frame, così come la potenza complessiva del frame.

3.3.2.3 Watermark Signal Extraction

Dall'analisi dello spettro completata precedentemente è possibile calcolare la spectral power per ogni frame, la quale consente di esaminare la potenza a bassa frequenza di ogni frame e quindi estrarre il watermark, in accordo alla seguente formula:

$$w(n) = \begin{cases} 1\ if\ F_x(1) \geq 0 \\ 0\ if\ F_x(1) \leq 0 \end{cases} \quad n = 1,2,\dots N$$

Il watermark estratto, $w(n)$, dovrebbe essere una replica esatta del watermark originale se il file audio in input aveva abbastanza potenza per frame da permettere l'inclusione di informazioni al di sotto della soglia di impercettibilità ed al si sopra della soglia di quantizzazione.

3.3.2.4 Limitazioni

Questo schema di DC watermarking soffre di alcune importanti limitazioni che riguardano la robustezza e la densità dei dati. La robustezza dello schema può essere incrementata in file audio più lunghi, inserendo il segnale di watermark più volte. Questa tecnica aiuta il processo di estrazione del watermark e permette di correggere il segnale da errori se questo è stato manipolato.

Al fine di ottenere una densità dei dati nascosti maggiore devono essere utilizzate tecniche di watermarking più avanzate come *spread spectrum, phase encoding* o *echo hiding*. Lo schema di watermarking più sicuro, più versatile e più affidabile consisterebbe in una combinazione dei precedenti in modo tale da sfruttare le caratteristiche peculiari di ognuno.

3.4 Altre tecniche di audio watermarking

Ci sono numerose altre tecniche di watermarking, ancora oggetto di studio, che sono in grado di offrire maggiore robustezza e data-rate dei metodi trattati in questo documento.

3.4.1 Phase Encoding

Questa tecnica di watermarking sfrutta l'impercettibilità, per il sistema auditivo umano, dei cambiamenti di fase assoluti codificando i dati del watermark in un segnale di fase *artificiale*. Phase Encoding lavora dividendo il segnale audio originale in frame ed eseguendo l'analisi dello spettro per ogni frame. Una volta che tale analisi viene completata, viene confrontata l'ampiezza e la fase di frame consecutivi ed un segnale di fase artificiale viene creato per trasmettere dati. La fase artificiale è modulata in modo tale che la fase di ogni frame e la nuova fase combinate tra di loro formino il segnale con watermark.

La fase modificata può anche essere approssimata per limitare la distorsione che questo processo introduce nel segnale audio, in questo modo però l'ammontare di dati inseribili diminuisce.

Questa tecnica di watermarking offre un data-rate medio da 8 a 32 bit/s, ancora più efficace in presenza di rumore.

3.4.2 Spread Spectrum Watermarking

Questa tecnica di watermarking si basa su **Direct Sequence Spread Spectrum** (DSSS) per diffondere il segnale con watermark su tutto lo spettro delle frequenza udibili in modo tale che questo venga approssimato con il rumore, ad un livello di potenza tale da essere inudibile. Viene usata una sequenza pseudocasuale per modulare un'onda portante che crea un codice del segnale del watermark. Tale codice è attenuato ad un livello approssimativamente uguale allo 0,5% del range dinamico del file audio originale, prima di essere mixato con quest'ultimo.

Il data-rate di questa tecnica è minore rispetto ai metodi precedenti, la media è intorno ai 4 bit/s. Il basso data-rate è compensato dalla maggiore robustezza dovuta al fatto che non risente della presenza di rumore nel segnale audio.

3.4.3 Echo Watermarking

Questa tecnica si basa sulla distorsione di un segnale audio in modo tale che questa venga riconosciuta dal sistema uditivo umano come una *distorsione ambientale*. Il segnale originale viene copiato in due segmenti (kernel), il primo contiene il segnale audio originale, il secondo lo stesso segnale ma ritardato nel tempo. Ogni kernel rappresenta un bit dei dati del watermark da trasmettere. Lo stream di bit del watermark è usato per mixare i due kernel insieme. I segnali sono mixati con delle transizioni graduali in modo tale da ridurre la distorsione.

3.4.4 Applicazioni future

Le tecnologie riguardanti l'audio digital watermarking sono un settore di ricerca molto attivo. La motivazione principale che guida attualmente lo sviluppo, è la tutela della proprietà intellettuale, tramite sistemi di prevenzione dalla copia e sistemi di rilevazione. Il digital watermarking ha un grande potenziale per essere utilizzato come parte di un sistema globale di gestione dei diritti della proprietà intellettuale, e può essere utilizzato non solo per indicare l'autore di un file audio in particolare, ma catalogando il percorso di un file particolare, se questo è stato distribuito in un modo non autorizzato. Con la nascita di siti web per il download di musica come iTunes di Apple, vi è un aumento della pressione per implementare un sistema completo di gestione dei contenuti. Aziende come Verance hanno già rilasciato strumenti di watermarking per il mercato commerciale, ed altri seguiranno l'esempio. Questo è un settore di ricerca, che continuerà a crescere nei prossimi anni. Un aumento di connessioni a internet a banda larga ha inoltre indotto l'industria cinematografica a prendere atto delle perdite di gettito possibile grazie alla distribuzione di film non autorizzati via Internet. Microsoft sta attualmente sviluppando nuove tecnologie di

watermarking ed è i sistemi operativi attualmente in commercio sono dotati di DRM per tutti i tipi di media. Il successo dei sistemi di protezione della proprietà intellettuale negli ultimi anni, comprese le più attuali tecnologie di watermarking, è limitato. Praticamente tutte le tecnologie introdotte fino ad oggi sono state rotti o si sono dimostrate inadeguati a causa della degradazione e distorsione che introducono nel segnale audio. Applicare tecniche di watermarking diventa particolarmente difficile quando il file è soggetto ad una perdita di informazioni dovuta a sistemi di compressione come MP3 o WMA. Questi schemi percettivi di compressione, e gli attuali sistemi di watermarking, usufruiscono di molte delle stesse limitazioni del sistema uditivo dell'uomo.

3.5 Tecniche di Audio Watermarking per localizzare i Movie Pirates

Nel tentativo di scoraggiare la camcorder piracy, i ricercatori hanno sviluppato tecniche di watermarking che incorporano un messaggio segreto in un filmato, che indica dove e quando il film è stato mostrato. Una volta che il filmato è pubblicato su Internet, il messaggio segreto può essere estratto e rivelare il cinema in cui è stato registrato e il momento della riproduzione. Tuttavia, queste tecniche di watermarking non sono in grado di identificare la posizione di registrazione nel teatro e quindi il "pirata" se non con l'ausilio di sistemi di sorveglianza interni al teatro.

Un nuovo sistema (16) proposto è ancora più efficace. Tramite l'utilizzo di un segnale audio con un watermark incorporato, per esempio, nella colonna sonora del film, è possibile stimare l'ubicazione della videocamera in un teatro con una precisione di mezzo metro. Yuta Nakashima, Ryuki Tachibana, e Noboru Babaguchi della Osaka University hanno sviluppato la nuova tecnica, ed i loro risultati sono stati pubblicati su *IEEE Transactions on Multimedia.*

Come spiegano i ricercatori nel loro studio, il sistema di stima della posizione funziona sfruttando i vari canali della colonna sonora, chiamati *"host signal".* Un embedder genera un segnale di watermark per ogni host signal, generando un *"watermarked host signal"* (WHS). Diversi altoparlanti emettono diversi WHS, e una videocamera registra l'audio come un miscuglio di tutti i WHS in un unico segnale registrato.

In questo segnale monofonico registrato, il WHS è in ritardo in proporzione alla distanza dal suo altoparlante (la fonte) al microfono della videocamera. Il detector del watermark è in grado di calcolare questi ritardi, riuscendo quindi ad effettuare una stima piuttosto accurata della posizione del microfono che ha registrato il segnale.

Come spiegano i ricercatori, questo metodo audio watermarking potrebbe essere combinato con uno dei metodi convenzionali di watermarking, che, insieme, potrebbero determinare tutte le informazioni riguardanti il teatro. Poi, un sistema di identificazione delle persone – come ad esempio un sistemi avanzati di ticketing o di video sorveglianza – può essere in grado di identificare il pirata.

Anche se, negli esperimenti, il sistema si è rivelato abbastanza affidabile, i ricercatori intendono approfondire ulteriormente la tecnica. Una sfida che devono affrontare è garantire che la qualità dell'audio rimanga alta in mezzo a vari fattori ambientali e rumore di fondo. I ricercatori hanno anche intenzione di studiare la robustezza del sistema contro gli attacchi che possono portare il sistema a valutare una posizione irrilevante.

4 Curiosità

4.1 Il caso dei Broadcast Flag per l'HDTV

A metà del 2005 è scoppiato un vero e proprio caso politico e legale (17) riguardo all'uso di tecniche di digital watermarking nei flussi video della TV digitale. La FCC americana, evidentemente posta sotto pressione dall'industria dell'entertainement, ha tentato di far passare abusivamente una regola che imponeva l'uso di appositi *"Broadcast flags"* nelle trasmissioni video digitali della televisione ad alta definizione (HDTV).

Un **broadcast flag** (18) è un insieme di bit di stato (o *"flag"*) inviato nel flusso di dati di un programma televisivo digitale che indica se il flusso di dati può essere registrato, o se ci sono restrizioni sul contenuto. Le possibili restrizioni includono l'impossibilità di salvare un programma digitale in chiaro su un disco rigido o altri dispositivi di archiviazione, l'incapacità di fare copie di contenuti registrati (in modo da condividere o archiviare), la riduzione forzata della qualità durante la registrazione (come ad esempio la riduzione della risoluzione video a quella TV standard), e l'incapacità di saltare la pubblicità.

Secondo questa regola, sarebbe diventato illegale vendere e distribuire sul territorio americano prodotti che non tenessero conto di questi broadcast flag e che non li usassero per limitare l'uso della trasmissione video (registrazione, copia, visualizzazione) in modo conforme a quanto deciso dal detentore dei diritti.

Questa regola della FCC è stata dichiarata illegale ad inizio 2006.

4.2 Il caso delle Stampanti

Nel 2003, la **Electronic Frontier Foundation** ha scoperto che HP, Xerox ed altri produttori di stampanti usano delle tecniche di watermarking per marcare ogni foglio stampato in modo che sia sempre possibile tracciarne la provenienza.

La *printer steganography* è un tipo di steganografia prodotta da stampanti a colori, tra cui HP, Xerox ed Epson, in cui piccoli puntini gialli vengono aggiunti a ogni pagina. I punti sono appena visibili e codificati contengono i numeri di serie della stampante, come pure il timestamp di quando è stata effettuata la stampa.

Le stampanti laser a colori sembrano essere le più coinvolte. Tale tecnologia venne impiegata per la prima volta all'inizio degli anni '90 da società come Xerox che cercavano di rassicurare i governi che le loro stampanti non sarebbe state utilizzate per scopi di falsificazione.

Nel 2005, la Electronic Frontier Foundation ha pubblicato una guida online alla loro individuazione. I codici della maggior parte delle stampanti non sono stati ancora decodificati, anche se il quadro di funzionamento è abbastanza chiaro.

Figura 31: Esempio di Printer steganography

5 Appendice

5.1 JPEG

JPEG è l'acronimo di **Joint Photographic Experts Group**, un comitato ISO/CCITT che ha definito il primo standard internazionale di compressione per immagini a tono continuo, sia a livelli di grigio che a colori. È un formato gratuito e open-source.

Attualmente JPEG è lo standard di compressione delle immagini fotografiche più utilizzato. Le estensioni più comuni per questo formato sono .jpeg, .jpg, .jfif, .JPG, .JPE, anche se il più comune in tutte le piattaforme è .jpg.

JPEG specifica solamente come una immagine può essere trasformata in uno stream di byte, ma non come questo può essere incapsulato in supporti di memorizzazione. Un ulteriore standard chiamato **JFIF** (JPEG File Interchange Format), creato da **Independent JPEG Group**, specifica come produrre un file appropriato per la memorizzazione su computer di uno stream JPEG. Nell'uso comune, quando qualcuno parla di "file JPEG" generalmente intende un file JFIF o alcune volte un file Exif JPEG. Ci sono, comunque, altri formati di file basati su JPEG, come ad esempio JNG.

Essenzialmente il JPEG opera in 3 passi fondamentali per trasformare un'immagine raster in una JPEG e viceversa. Tali passi sono:

1. **Rappresentazione** in ambito frequenziale tramite **DCT** (trasformata discreta del coseno) se opera in modalità lossy, uso dei predittori in modalità lossless.
2. **Quantizzazione** effettuata tramite opportune matrici, che solitamente, pesano i coefficienti di ordine più basso (rappresentano le basse frequenza spaziali) in maniera più decisa, in quanto, per le proprietà della DCT, sono più importanti ai fini della sintesi dell'immagine. Questo perché il sistema visivo umano percepisce maggiormente le basse frequenze spaziali rispetto alle alte frequenze, risulta quindi necessario dare maggior importanza alle basse frequenze spaziali.
3. **Codifica entropica** ed **eliminazione delle ridondanze** di tipo statistico tramite codifica RLE e codici di Huffman; la componente continua della DCT invece è codificata in DPCM.

Il fattore di compressione che si può raggiungere è determinato essenzialmente da un parametro di *scalature* per le matrici di quantizzazione. Tanto più piccolo è questo parametro, tanto peggiore è la qualità. Si può ottenere un fattore di compressione 15:1 senza alterare visibilmente la qualità dell'immagine.

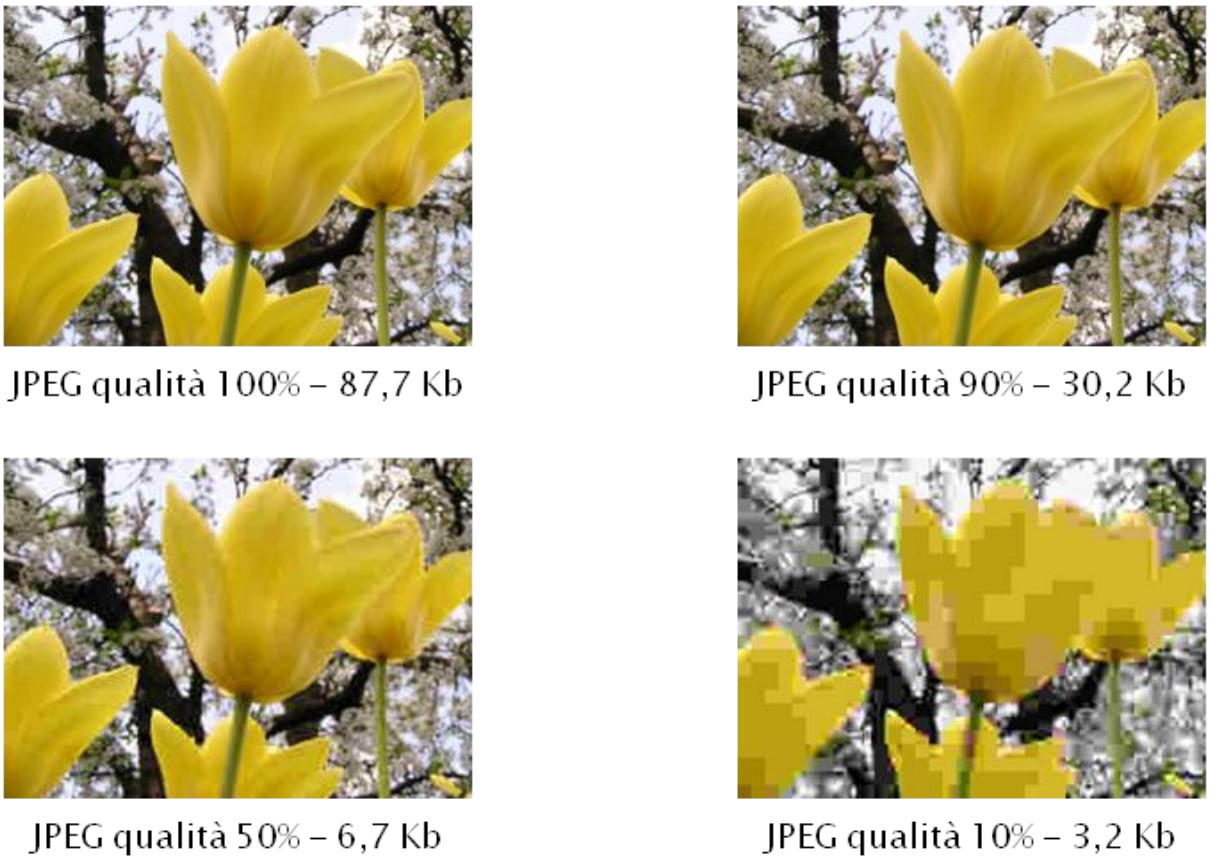

Figura 32: Esempi degradazione della compressione JPEG

5.2 Pixel

Il termine **pixel** (19) (contrazione della locuzione inglese *picture element*) si indica ciascuno degli elementi puntiformi che compongono la rappresentazione di una immagine raster nella memoria di un computer.

Nella **grafica raster** l'immagine viene vista come una scacchiera in cui ogni elemento della scacchiera, pixel, viene associato uno specifico colore. Il colore può essere definito con due tecniche:

- se l'immagine contiene pochi colori (massimo 256) si crea un elenco dei colori da utilizzare e nella scacchiera viene inserito l'indice che punta allo specifico colore del pixel;
- nel caso si vogliano utilizzare molti più colori il singolo pixel non definisce più l'indice a una tavolozza di colori ma definisce il colore direttamente.

Solitamente i punti sono così piccoli e numerosi da non essere distinguibili ad occhio nudo, apparendo fusi in un'unica immagine quando vengono stampati su carta o visualizzati su un monitor. Ciascun pixel, che rappresenta il più piccolo elemento autonomo dell'immagine, è caratterizzato dalla propria posizione e da valori quali colore e intensità, variabili in funzione del sistema di rappresentazione adottato.

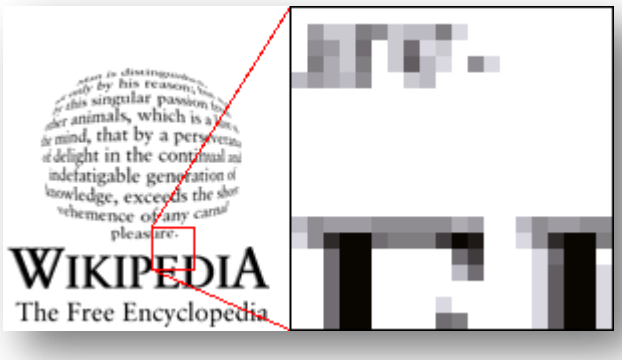

Figura 33: Logo Wikipedia in grafica raster ingrandito in modo da evidenziare i singoli pixel

L'esempio qui a destra mostra un logo in grafica raster ingrandito in modo da evidenziare i singoli pixel. Si noti che in questo caso l'illusione di una immagine uniforme è resa più realistica mediante l'uso di sfumature di grigio sul bordo dei caratteri, evitando bruschi passaggi di colore (tale processo è detto di **antialiasing**).

Il numero di pixel in un'immagine (talvolta detto **risoluzione** dell'immagine) determina la quantità di dettagli fini che possono essere rappresentati. Sebbene il concetto di pixel si applichi in tutti i contesti con il medesimo significato, per l'indicazione del numero di pixel da cui è costituita una immagine sono in uso diverse convenzioni per diverse tecnologie specifiche. Per esempio, il numero di pixel di cui è costituita l'immagine prodotta da una fotocamera digitale viene espresso come un singolo valore, in megapixel (milioni di pixel), mentre il numero di pixel di un display viene in genere espresso come un prodotto (pixel in altezza per pixel in larghezza), per esempio 640 × 480.

I punti colorati che formano un'immagine digitale (come una JPEG) vengono chiamati anch'essi pixel. Possono non essere in corrispondenza uno-a-uno con i pixel dello schermo. Nei casi in cui questa distinzione è importante, i punti del file possono essere chiamati **texel**.

Ogni pixel di un'immagine *monocroma* ha la sua **luminosità**. Un valore pari a zero di norma rappresenta il nero, mentre il valore massimo rappresenta il bianco. Ad esempio, in un'immagine a otto bit, il massimo valore senza segno che può essere immagazzinato è 255, così questo è il valore usato per il bianco.

Nelle immagini a *colori*, ogni pixel ha la sua **luminosità** e **colore**, tipicamente rappresentate da una tripletta di intensità di rosso, verde e blu (RGB). Il numero di colori distinti che possono essere rappresentati da un pixel dipende dal numero di bit per pixel (BPP). Valori comuni sono:

- 8 bpp (256 colori)
- 16 bpp (65.536 colori, noto come **Highcolour**)
- 24 bpp (16.777.216 colori, noto come Truecolour).

6 Bibliografia

1. **WatermarkingWorld.** Digital Watermarking. *watermarkingworld.org.* [Online] http://www.watermarkingworld.org.

2. **Yeung, M.M.** Digital Watermarking. *Communications of the ACM.* 1998, Vol. 41, 7.

3. **Petitcolas, Fabien.** Steganography and Digital Watermarking. *The information hiding.* [Online] http://www.petitcolas.net/fabien/steganography/.

4. **Acken, J.M.** How Watermarking Adds Value to Digital Content. *Communications of the ACM.* 1998, Vol. 41, 7.

5. **Mintzer, F., Braudaway, G.W. and Bell, A.E:.** Opportunities for Watermarking Standards. *Communications of the ACM.* 1998, Vol. 41, 7.

6. Watermark. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Watermark.

7. **IBM Research.** Watermarks: Protecting the image. *IBM Research.* [Online] http://www.research.ibm.com/image_apps/watermark.html.

8. **Memon, N. and Wong, P.W.** Protecting Digital Meida Content. *Communications of the ACM.* 1998, Vol. 41, 7.

9. **Jellinek, Brigitte.** Invisible Watermarking of Digital Images for Copyright Protection. [Online] 2000. http://welten.horus.at/wp-content/uploads/2000/05/bjelli-di-1.2.pdf.zip.

10. Discrete Cosine Transform. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Discrete_cosine_transform.

11. **Cox, I.J., et al.** Secure Spread Spectrum Watermarking for Multimedia. [Online] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=650120&userType=inst.

12. **Basso, Alessandro and Vernone, Annamaria.** Realizzazione di un sistema di Digital Watermarking per immagini ad alta definizione. [Online] www.di.unito.it/~basso/papers/watermarking-RT99-07.pdf.

13. **Boney, L., Zhu, B. and Hamdy, K.N.** Digital watermarks for audio signals. *University of Minnesota, Department of Electrical Engineering.* [Online] http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/watermark/riferimenti/eufinal.ps.Z.

14. **Chen, Ding-Yun.** An Affine Resistant Watermarking Scheme. *Public Audio Watermark.* [Online] http://www.cmlab.csie.ntu.edu.tw/~dynamic/AWM/.

15. **Bengert, Joanne and Upward, Allen.** Digital Audio Watermarking. *Perceptual Audio Project.* [Online] http://www.ece.uvic.ca/~aupward/w/watermarking.htm.

16. **PhysOrg.com.** Audio Watermarking Technique Could Locate Movie Pirates. *PhysOrg.com.* [Online] http://www.physorg.com/news154880123.html.

17. **Bottoni, Alessandro.** Introduzione al Watermarking. *La Spina nel Fianco.* [Online] http://laspinanelfianco.wordpress.com/2006/02/21/introduzione-al-watermarking/.

18. Broadcast flag. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Broadcast_flag.

19. Pixel. *Wikipedia.* [Online] http://it.wikipedia.org/wiki/Pixel.

20. **Radzishevsky, Alex.** Information on proprietary audio watermarking technique. *AudioWatermarking.info.* [Online] http://audiowatermarking.info.

21. Digital Watermarking. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/Digital_watermarking.