*Atti dell'Accademia Peloritana dei Pericolanti*
*Classe I di Scienze Fis. Mat. e Nat.*
*Vol. LXXXI-LXXXII, C1A0401009 (2003-04)*
*Adunanza del 29 aprile 2004*

# TUTELA DEL DIRITTO DI PROPRIETÀ DELLE IMMAGINI DIGITALI: IMPLEMENTAZIONE DI UN ALGORITMO DI WATERMARK MEDIANTE FUNZIONI WAVELET

SANTA AGRESTE, NUCCIO CASTORINA, SALVATORE GIOVINAZZO, DANIELA PRESTIPINO AND LUIGIA PUCCIO*

(*socio aggregato)

ABSTRACT. Protection of copyright of the digital images is a critical element for the multimedia Web applications, e-books, virtual picture gallery. This problem is today receiving growing attention due to the pervasive diffusion of Internet technology. This work shows the watermark as solution to this problem and describes a new wavelet-based algorithm, called WM1.0, which is invisible, private, strong. WM1.0 *watermaks* a subset of digital images building the ecclesiastic on-line art collection. The Owner of the images and related information is the Italian Episcopal Conference, whereas the Publisher is I.D.S. , an ICT company located in Messina. The on-line service is BeWeb to the URL http://www.chiesacattolica.it/BeWeb.

## 1. Introduzione

Nel corso degli ultimi anni i sistemi di rappresentazione e divulgazione di documenti multimediali hanno conosciuto un rapido quanto indiscusso e vantaggioso sviluppo, inducendo però, al contempo, diversi problemi in relazione alla tutela del *copyright* o più genericamente degli IPR, *Intellectual Property Rights*. I dati multimediali, in genere, distribuiti in formato digitale, sono facili da: intercettare, copiare e ridistribuire indebitamente. Il problema, amplificato dalla diffusione ed utilizzo di Internet, impatta, in generale, le opere musicali e letterarie (documenti audio, video, e-book), le immagini digitali, il software, con un "gradiente" di illeciti e violazioni nell'utilizzo, che spaziando dalla semplice consultazione, al "download", all'archiviazione, appropriazione, modifica, riproduzione e rivendicazione indebita di informazioni e dati, ha, tra l'altro, notevolmente *raffinato* la giurisprudenza in materia.

Il presente lavoro è stato sviluppato ed implementato nell'ambito del Contratto di Ricerca Industriale "Algoritmi per la sicurezza informatica: con campi di applicazione al software, alle banche dati multimediali e alle reti", concordato tra l'Azienda IDS - Informatica Distribuita e Software S.r.l. di Messina e il Dipartimento di Matematica dell'Università di Messina.

Il problema, infatti, ha raggiunto dimensioni tali da richiedere opportuni interventi e contromisure sia in senso tecnologico che normativo. In riferimento alle immagini, il quadro normativo attuale in tema di diritto d'autore, fissato, per grandi linee:

- dalla legge n. 633 del 22 Aprile 1941;
- dalla Convenzione di Berna ratificata e resa esecutiva con la legge n. 399 del 20 Giugno 1978;
- dalle più recenti indicazioni comunitarie funzionali, in particolare, alla "globalizzazione telematica" imposta da Internet: direttive, linee guida, pareri, "green paper" nel senso dell'armonizzazione delle singole legislazioni dei paesi membri e concretizzatesi con la direttiva comunitaria 2001/29/CE;
- dal successivo recepimento in Italia con D.L. n. 68 del 9 Aprile 2003;

tutela dal punto di vista giuridico l'immagine stessa, salvaguardando il diritto di proprietà, perseguendo come illecito chi ne fa un uso non autorizzato e soprattutto estendendone il concetto anche ai casi in cui l'immagine sia realizzata, diffusa e duplicata con strumenti digitali.

Dal punto di vista tecnologico un primo approccio al problema della protezione dei documenti multimediali è stato il ricorso a tecniche di crittografia, con cui cifrare i documenti multimediali in modo da permettere l'accesso ai soli utenti autorizzati. Tali tecniche, tuttavia, rendendo disponibile, dopo la decodifica, il documento in forma originale, non risolvono completamente il problema della riproduzione non autorizzata.

Un approccio alternativo e più efficiente per soluzione ai problemi menzionati è rappresentato dall'utilizzo di tecniche di marchiatura elettronica (o digital watermarking). Questi sistemi pur non impedendo fisicamente la riproduzione delle immagini, forniscono uno strumento utilissimo: verso gli effettivi titolari delle immagini danno la possibilità di assolvere i propri diritti, verso chi ne abusa illegittimamente, invece, consentono di opporre la prova evidente della sottrazione indebita, che altrimenti, paradossalmente, potrebbe spesso non essere dimostrabile. [S3]
Le tecniche di marchiatura elettronica tendono a risolvere, specificatamente i seguenti problemi:

- disporre di procedure per un facile riconoscimento del proprietario del documento multimediale.
- fornire un deterrente efficiente, al fine di scoraggiare l'utilizzo e la distribuzione illegale del documento.
- fornire un test per determinare i diritti di copyright durante le procedure legali.
- fornire degli strumenti atti a verificare la diffusione dei dati multimediali su rete.

In questo contesto si considera in particolar modo il watermarking invisibile di immagini digitali, che è definito nel seguente modo:

*Il watermarking invisibile d'immagini digitali consiste nell'aggiungere all'immagine un marchio, detto watermark o messaggio di copyright, in modo che tale messaggio sia segretamente immerso nell'immagine. Il watermark deve risultare invisibile alla percezione dell'occhio umano.*

Di seguito viene descritto l'algoritmo di watermark d'immagini digitali a colori [12,13] - nel seguito denominato WM1.0 - sviluppato e implementato nell'ambito del Contratto di Ricerca Industriale "*Algoritmi per la sicurezza informatica: con campi di applicazione il*

*software, le banche dati multimediali e le reti*", concordato tra L'Azienda IDS - Informatica Distribuita e Software S.r.l. di Messina e il Dipartimento di Matematica dell'Università di Messina.

Il presente lavoro è organizzato come segue: il successivo paragrafo descrive la classificazione e le proprietà degli algoritmi di watermark; segue la descrizione delle principali tecniche di watermarking; delle caratteristiche generali di WM 1.0; quindi la descrizione delle fasi di generazione ed inserimento watermark con WM 1.0; quella del rilevamento del watermark con WM 1.0; vengono quindi descritti gli attacchi; i risultati e l'utilizzo di WM 1.0; conclude la descrizione dei prossimi possibili sviluppi.

## 2. Classificazione e proprietà degli algoritmi di watermark

Un *watermark* è un codice o un logo identificativo che può contenere informazioni sull'autore, il proprietario, il distributore o il consumatore autorizzato del documento multimediale; è permanentemente impresso nel documento digitale con lo scopo di proteggere i diritti gravanti sull'opera. Il termine watermarking, tende a sottolineare come nel caso di immagini digitali si tenti di realizzare una sorta di marchio digitale, che sia parte integrante dell'immagine stessa ma allo stesso tempo risulti impercettibile e quindi trasparente.

L'obiettivo del watermarking è di inserire informazioni, il marchio, all'interno dell'immagine senza degradarne la qualità, rendendo tuttavia l'informazione rilevabile ed estraibile per un uso successivo. Il watermarking ha origine dalla steganografia (dal greco stego -nascosto, occulto-, e grafe -scrittura-), con questo termine si classificano tutte le tecniche che hanno come obiettivo quello di nascondere le informazioni segrete all'interno dei documenti apparentemente insospettabili. Il watermarking supera questo concetto, in due sensi:

- tutelando l'informazione stessa, l'immagine nel caso specifico, indipendentemente se l'esistenza del marchio sia conosciuta o meno.
- soddisfacendo il requisito aggiuntivo della robustezza: non è possibile, almeno in teoria, rimuovere l'informazione inserita senza conoscere la chiave utilizzata per generarla anche se si suppone noto l'algoritmo usato per l'inserimento del watermark.

**2.1. Classificazione in base all'inserimento del watermark.** Si possono distinguere due tipi di marchiatura digitale a seconda se il watermark sia visibile o meno:

- *Watermark visibile* molto simile alle filigrane inserite nei fogli cartacei, in cui è possibile intravedere i segni di riconoscimento o il logo del produttore o del proprietario. Questo metodo è utilizzato dai canali televisivi: per proteggersi da registrazioni e ritrasmissioni illegali, le emittenti televisive aggiungono in un angolo dello schermo il proprio logo, che assolve la funzione di firma. Lo svantaggio principale è che l'immagine viene marcata in modo visibile, inaccettabile se si tratta di riproduzioni di opere d'arte, spartiti, ecc.
- *Watermark invisibile* (il vero watermark) consiste invece nell'inserire un codice identificativo nel file dell'immagine in modo che si possa risalire con sicurezza al detentore dei relativi diritti. L'informazione aggiuntiva, il marchio, inserita nell'immagine deve essere impercettibile, almeno per un osservatore comune. Se le

modifiche introdotte non sono tali da perturbare in maniera rilevante l'immagine, l'ipotetico, malizioso o meno, utente non avrà la possibilità di confrontarla con l'originale. I segni identificativi sono facilmente decodificabili in ogni momento da chi li ha introdotti in modo da identificare ogni copia non autorizzata.

**2.2. Classificazione in base al rilevamento del watermark.** Le varie tecniche di watermark, inoltre, possono essere classificate secondo il metodo di rilevamento in: *Public watermarking (o blind watermarking ), Private watermarking (o algoritmo non cieco), Semi-Private Watermarking e Asymmetric Watermarking*.

- *Public watermarking (o blind watermarking)*: per identificare il watermark del file marchiato non occorre ne il documento originale ne il watermark; di solito il rilevamento avviene calcolando l'autocorrelazione dei coefficienti che partecipano alla marchiatura. Le tecniche di questo tipo sono le più robuste e per questo hanno un numero di applicazioni molto elevato.
- *Private watermarking (o algoritmo non cieco)*: nella fase di rilevamento è necessario il documento originale e in alcuni casi anche del watermark. Il rilevamento avviene confrontando la copia marchiata con l'originale. Tale tipo di tecnica dà maggiori garanzie di corretto rilevamento (cioè un'alta probabilità di scarso errore), ma può essere sfruttata solo da chi possiede il documento originale, quindi consente un numero inferiore di applicazioni pratiche.
- *Semi-Private Watermarking*: il rilevamento viene effettuato con il documento marchiato e con il watermark stesso analizzando la correlazione tra i due, e fornendo in uscita un'espressione booleana che indica la presenza o meno del marchio. Bisogna evidenziare che, affinchè questa tecnica sia efficace, è fondamentale che l'algoritmo d'inserimento del watermark rimanga segreto; se così non fosse, chiunque si trovasse in possesso di un documento marchiato, del watermark e dell'algoritmo potrebbe applicarlo inversamente al documento estraendo il watermark e producendo così il documento originale.
- *Asymmetric Watermarking (o Public Key Watermarking)*: la chiave di rilevamento è pubblica, quindi ogni utente è in grado di leggere il watermark, mentre la chiave privata utilizzata dal possessore per l'inserimento del marchio è segreta. Con la chiave pubblica resta l'impossibilità di una rimozione o di una contraffazione del marchio e di calcolare la chiave privata. Non esistono ancora metodi validi in questa categoria, dato che finora non si è riusciti a garantire la lettura del marchio impedendo, allo stesso tempo, di poterlo rimuovere.

**2.3. Proprietà generali del watermarking.** Per essere efficace nel proteggere i diritti di proprietà intellettuale, ma allo stesso tempo nel preservare la qualità dell'immagine, il watermarking deve essere: *robusto, impercettibile, invertibile ed avere una bassa probabilità di errore*.

- *Watermark Robusto*: deve resistere agli attacchi digitali che hanno lo scopo di modificarlo, eliminarlo o sostituirlo in modo intenzionale o meno. Negli attacchi non intenzionali la manipolazione dell'immagine è eseguita con programmi di uso comune, come Paint Shop o PhotoShop, per mettere in atto dei cambiamenti all'immagine quali la compressione, il filtraggio, semplici operazioni di ritocco

fotografico,ecc. Gli attacchi intenzionali mirano, invece, alla rimozione del marchio studiando le proprietà dell'algoritmo di watermark e cercando di introdurre delle distorsioni per distruggere o, almeno rendere illeggibile, il marchio senza rovinare l'immagine. Un algoritmo robusto deve tenere conto che potrebbero essere inseriti diversi codici in istanti diversi, in modo da prevenire che il watermark successivo deteriori il precedente. In particolare si devono prevenire manomissioni, come il cambiamento del watermark provocato da attacchi collusivi, ovvero attacchi simultanei e incrociati.

- *Watermark Impercettibile*: il watermark sia visibile che invisibile non deve danneggiare in alcun modo la qualità visiva dell'immagine.

- *Watermark Invertibile*: anche se la robustezza è comunemente indicata come la più importante proprietà da soddisfare bisogna dare grande attenzione anche all'invertibilità. In letteratura il termine invertibilità viene utilizzato con significati differenti, il più naturale definisce un watermark invertibile se l'utente autorizzato può rimuoverlo dal documento. In molti casi, questo genere di invertibilità, chiamata reversibilità, è una caratteristica desiderabile, poichè permette la distribuzione di un "documento concesso", senza che esso nasconda troppi codici. Purtroppo la reversibilità è molto difficile da ottenere se il watermark è robusto. Un significato diverso è stato dato da Craver, che in [6, 7] giunge alla conclusione che affinchè uno schema di watermark venga usato con successo per dimostrare il diritto di proprietà, bisogna garantire la non-invertibilità e la quasi-non-invertibilità del marchio. Senza soffermarci troppo nei dettagli è possibile affermare che il termine invertibilità prende in considerazione il caso in cui è possibile generare un falso watermark e un falso documento originale uguale a quello originale, in modo tale che dall'inserimento del falso watermark si ottiene un documento che è perfettamente uguale (invertibilità) o solo percettibilmente uguale (quasi invertibilità) all'originale.

- *Watermark con bassa probabilità di errore:* l'estrazione del watermark dovrebbe permettere di identificare il proprietario in modo non ambiguo e di garantirne l'unicità, non deve, perciò, essere possibile avere falsi positivi, ossia che l'estrazione del marchio dia esito positivo anche nel caso di watermark diversi da quello inserito, o falsi negativi, ossia il mancato rilevamento del watermark esistente.

## 3. Principali tecniche su cui si basano gli algoritmi di watermark

Un algoritmo di watermark è costituito da due fasi: *inserimento del watermark (o signature casting) e rilevamento del watermark (o signature detection)*. La implementazione di quest'ultima fase dipende fortemente dalle scelte operative effettuate e dalle metodologie teoriche usate nella prima. Il processo di *inserimento di un watermark* in un'immagine digitale può essere rappresentato come l'inserimento di una componente di rumore nell'immagine stessa, aggiungendo, cioè, un valore random ad ogni pixel. Data quindi un'immagine digitale $I$ e dato il watermark $W = \{w_1, w_2, ..., w_n\}$ l'immagine risultante $I_W$, contenente il watermark, è ottenuta mediante una funzione di codifica $C$, dove non si

esclude la possibilità che il marchio $W$ dipenda dall'immagine $I$:

$$C\left(I, W\right) = I_W \tag{1}$$

Nella seconda fase di rilevamento del watermark, una funzione di decodifica $D$ estrae dall'immagine con watermark $I_W$ un watermark $W'$. In questo processo, nel caso di metodo privato, o non cieco, la versione originale dell'immagine $I$ viene richiesta dalla funzione $D$. Questo è dovuto al fatto che gli schemi di decodifica privati utilizzano un'immagine digitale per supportare una maggiore resistenza contro le alterazioni, intenzionali e non, dei valori dei pixel. Nel caso dei metodi non ciechi si ha dunque:

$$D\left(I, I_W\right) = W' \tag{2}$$

Mentre nel caso di watermark pubblici, o ciechi, si ha:

$$D\left(I_W\right) = W' \tag{3}$$

Al fine di riscontrare la presenza del marchio $W$, il watermark estratto $W'$ viene messo a confronto con quello originale attraverso una funzione di comparazione $C_\delta$ che indica se i due watermark corrispondono:

$$C\left(W', W\right) = c \tag{4}$$

se $c < \delta$, con $\delta$ un opportuno valore di soglia, $W$ e $W'$ corrispondono, diversamente non corrispondono.
Senza perdere di generalità uno schema di watermarking pubblico può essere trattato come una terna $(C, D, C_\delta)$ tale che $D\left(C, \left(I, W\right)\right) = W$ per qualsiasi immagine $I$ e qualsiasi watermark ammissibile $W$; mentre uno schema di watermarking privato può essere trattato come una terna $(C, D, C_\delta)$ tale che $D\left(C, \left(I, W\right), I\right) = W$ per qualsiasi immagine $I$ e qualsiasi watermark ammissibile $W$.
In letteratura sono stati proposti diversi processi di codifica con i corrispondenti processi di decodifica (V. [13] per un elenco abbastanza esaustivo).
L'approccio più utilizzato è quello che, dato un insieme di caratteristiche di un'immagine *feature* se ne determina un sottoinsieme $F = \{f_1, f_2, ..., f_n\}$ in cui codificare il watermark attraverso un operatore di inserimento $\oplus$:

$$f_i' = f' \oplus w_i \tag{5}$$

dove $F' = \{f_1', f_2', ..., f_n'\}$ sono le caratteristiche dell'immagine con il watermark. Al fine di effettuare il riconoscimento con il watermark si utilizza invece un operatore di estrazione $\ominus$, inverso al precedennte, tale che:

$$w_i' = f_i' \ominus f_i \tag{6}$$

dove $W' = \{w_1', w_2', ..., w_n'\}$ è il watermark estratto.
L'insieme $F$ può essere costituito dai valori assunti dai pixel dell'immagine, oppure dai coefficienti di una trasformata di dominio dell'immagine (tecnica del dominio delle frequenze) o dalle caratteristiche che possiedono i blocchi in cui è suddivisa un'immagine. Il sottoinsieme $F$ di caratteristiche dell'immagine in cui inserire il watermark è scelto in modo che:

- piccole modifiche su ogni caratteristica non peggiorino percettibilmente l'immagine.

- ogni caratteristica non cambi significativamente, salvo che l'immagine non sia stata modificata in modo percettibile.

Le tecniche per modificare un'immagine si suddividono in due categorie:

- *Tecniche che agiscono sul dominio spaziale*: vanno ad operare variazioni sui pixel che costituiscono l'immagine [22, 23].
- *Tecniche che agiscono sul dominio delle frequenze*: si basano sulle modifiche di una trasformata nel dominio delle frequenze[1-3, 9, 14, 15, 24, 25].

**3.1. Tecniche che agiscono sul dominio spaziale.** Generalmente le funzioni che appartengono a questa categoria possono essere espresse nella forma $g(x, y) = T[f(x, y)]$ dove la $f(x, y)$ è l'immagine da modificare, $g(x, y)$ è l'immagine modificata tramite l'operatore di trasformazione $T$ il quale agisce su $f$ ed è definito in un intorno del pixel $(x, y)$ in esame. L'effetto prodotto è la generazione di un'immagine in alto contrasto con l'originale per l'oscuramento dei livelli di grigio sotto un valore $h$ e lo schiacciamento dei livelli sopra $h$ nello spettro dei pixel originali. La scelta di intorni più o meno ampi, determinati dall'applicazione di opportuni filtri da origine ad una grande varietà di funzioni.

**3.2. Tecniche che agiscono sul dominio delle frequenze.** Le trasformazioni nel dominio delle frequenze prevedono l'applicazione di filtri lineari alla trasformata di Fourier (FT), o Coseno discreta (DCT), o Wavelet (DWT), dell'immagine considerata. Il procedimento viene effettuato in tre passi:

(1) calcolare la trasformata.
(2) moltiplicare il risultato per un particolare filtro.
(3) effettuare la trasformata inversa per tornare al dominio spaziale.

L'uso di tecniche nel domino delle frequenze ha principalmente i seguenti scopi:

- l'eliminazione di fenomeni di rumore periodico presenti nell'immagine.
- il restauro delle immagini, ovvero la ricostruzione di immagini degradate, basata sulla modellazione del processo di degradazione e l'applicazione di un processo inverso.
- l'analisi dei fenomeni periodici presenti nell'immagine.

Le trasformazioni delle immagini digitali sono molto importanti, sia per l'analisi della struttura delle stesse immagini, sia perchè risultano essere utili in diverse applicazioni, quali il filtraggio numerico, la compressione, l'inserimento del watermark.
Considerata un'immagine digitale di dimensione $N\,x\,M$, una trasformazione lineare invertibile può essere definita come:

$$F(u, v) = \sum_{x=1}^{N} \sum_{y=1}^{M} f(x, y) \cdot A(x, y, u, v) \tag{7}$$

dove $f(x, y)$ rappresenta il valore del pixel collocato in $(x, y)$ prima della trasformazione, mentre $A(x, y, u, v)$ rappresenta la *base* dell'operatore di trasformazione invertibile.

La trasformazione inversa ricava dai valori $F(u, v)$, con $u = 1, ..., N$ e $v = 1, ..., M$ ottenuti dalla precedente, il valore originario del pixel in posizione $(x, y)$ attraverso la

relazione:

$$f(x,y) = \sum_{u=1}^{N} \sum_{v=1}^{M} F(u,v) \cdot B(x,y,u,v) \tag{8}$$

dove $B(x,y,u,v)$ è la base dell'operatore di trasformazione inverso.

Osserviamo che le trasformazioni sopra indicate possono essere interpretate come una *analisi* dei dati dell'immagine in uno spettro bidimensionale generalizzato, in quanto ogni componente del dominio spettrale corrisponde alla quantità di energia che l'immagine originaria possiede rispetto a quella componente dello spettro.

## 4. Caratteristiche generali dell'algoritmo WM 1.0

*L'algoritmo WM 1.0 è un algoritmo di watermark privato, o non cieco, che opera nel dominio delle frequenze, il cui watermark è un numero reale aggiunto al valore dei coefficienti della DWT nelle sottobande relative alle alte frequenze.*

L'implementazione di questo algoritmo [12, 13], è realizzata in Matlab5 con il particolare uso del Toolbox Wavelet di Matlab [20], ed utilizzo delle funzioni: Daubechies Wavelets, Symlets, Biorthogonal Wavelets, Coiflets facenti parte della suddetta libreria [4, 10] per la valutazione della DWT e della trasformata inversa IDWT [18].

L'algoritmo lavora sul modello RGB, ogni colore è ottenuto come combinazione additiva dei tre colori primari: rosso, verde, blu. L'immagine digitale è una matrice tridimensionale i cui piani rappresentano l'intensità, rispettivamente, del rosso, del verde e del blu. Dalla matrice tridimensionale si estrae il piano su cui calcolare la DWT. Il watermark è inserito in alcuni coefficienti, relativi alle alte frequenze, di tale trasformata. Dopo tale inserimento si calcola la trasformata inversa IDWT per ottenere la nuova componente dell'immagine, rispetto al piano precedentemente scelto. Successivamente la matrice tridimensionale è ricomposta, ottenendo l'immagine a colori watermarkata, pronta per la distribuzione.

La scelta del piano solitamente verte sulla componente blu o verde; la prima si basa sul fatto che, come documentato in letteratura, l'occhio umano ha una scarsa percezione delle variazioni su tale componente, per cui ciò fornisce una maggiore qualità di invisibilità del watermark; di contro quella relativa al verde, dai test sperimentali effettuati su WM 1.0 [13], salvaguardia maggiormente la robustezza del watermark rispetto agli attacchi senza compromettere l'invisibilità del marchio.

WM 1.0 inserisce il watermark nella componente verde.

Quanto descritto si riferisce alla *fase di inserimento del watermark, o segnature casting*, dalla quale dipende ed è complementare la fase di *rilevamento del watermark , o segnature detection*, operazioni entrambe legate alla scelta di una chiave proprietaria.

**4.1. WM 1.0 - Generazione ed inserimento del watermark.** Le fasi di generazione ed inserimento del watermark vengono effettuate secondo i passi di seguito dettagliati, i parametri critici sono rappresentati dalla c*hiave e dal watermark*, entrambi proprietari al titolare dell'immagine.

Nell'ordine vengono eseguiti i seguenti passi:

(1) Scelta della *chiave*, parametro fornito in input, che contiene informazioni sulla base della funzione wavelet utilizzate nelle DWT e IDWT e il livello di decomposizione, $L$, che deve essere raggiunto dalla DWT nella fase di inserimento del watermark.
(2) Lettura dell'immagine originale in formato JPEG.
(3) Estrazione della componente relativa al verde dalla matrice tridimensionale ottenuta al passo precedente.
(4) Se la matrice è rettangolare con $m$ righe ed $n$ colonne si effettua la immersione in una matrice quadrata nulla di ordine $N = max(m, n)$, per poter valutare la DWT.
(5) Decomposizione dell'immagine ottenuta tramite la DWT mediante la base della funzione Wavelet ed il numero di livelli $L$ definiti al punto 1.Denotiamo con $I_j^\theta$ la sottobanda a livello di risoluzione $j = 0, 1, 2, 3$ con orientamento $\theta \in \{LL, LH, HL, HH\}$ (L e H rappresentano rispettivamente lo spazio delle basse (Low) frequenze e delle alte (High) frequenze di una decomposizione wavelet monodimensionale. Poichè la decomposizione wavelet bidimensionale si ottiene come prodotto tensoriale di due decomposizioni monodimensionali ad ogni livello $\theta$ si hanno quattro sottospasi (o sottomatrici) contraddistinti dalla doppia lettera, che corrispondono a quattro diverse bande di frequenza.
(6) Inserimento del watermark, con un peso diverso a secondo del numero di livello di decomposizione raggiunto, nelle sottobande relative alle alte frequenze dell'ultimo livello $L$ di decomposizione $I^L H_L, I^H L_L, I^H H_L$
(7) La riga $r$ di inserimento del watermark viene determinata con un operazione di modulo rispetto alle dimensioni della sottomatrice del livello $L$.
Indicando con $c$ l'ordine delle matrici relative alle sottobande e con $\tilde{I}_L^{\theta_1}, \tilde{I}_L^{\theta_2}, \tilde{I}_L^{\theta_3}$ le sottobande modificate, dove $\theta_i \in \{LH, HL, HH\}$ e $\theta_k \cap \theta_i = \oslash, \forall i \neq k$, l'inserimento del watermark avviene come di seguito descritto:

$$\tilde{I}_L^{\theta_1}(r, j) = I_L^{\theta_1}(r, j) + \omega; \tag{9}$$

$$\tilde{I}_L^{\theta_2}(i, j) = I_L^{\theta_2}(i, j) + \omega/p; \tag{10}$$

$$\tilde{I}_L^{\theta_3}(i, j) = I_L^{\theta_3}(i, j) + \omega/p; \tag{11}$$

$$\tag{12}$$

con $i = 1, ....c; j = 1, ....c$, $p$ costante positiva opportunamente definita e $\omega$ il watermark.
(8) Valutazione della relativa IDWT partendo dal livello L di decomposizione.
(9) Eliminazione di eventuali righe, o colonne, aggiunte.
(10) Ricomposizione della matrice tridimensionale con il nuovo piano, relativo al verde.
(11) Memorizzazione, in formato JPEG, dell'immagine a colori watermarkata in un file pronto per la distribuzione.

**4.2. WM 1.0 - Rilevamento del watermark.** Affinchè l'algoritmo di inserimento del watermark soddisfi a tutte le proprietà, definite nel paragrafo 2.3, deve essere sottoposto alla fase di rilevamento del watermark, che avviene effettuando i seguenti passi:

(1) Acquisizione della chiave utilizzata in fase di generazione ed inserimento.

(2) Lettura da file dell'immagine originale, $A$, e di quella watermarkata $B$.
(3) Estrazione del piano relativo alla componente verde, dalle due matrici tridimensionali $A$ e $B$.
(4) Prima di fare tale operazione, si deve effettuare il confronto tra le dimensioni delle due matrici. La variazione di dimensione può essere causata dalla memorizzazione, in formato JPEG, dell'immagine watermarkata (V. passo 11 del paragrafo 4.1). Nel caso di dimensioni diverse, si eguagliano applicando l'approssimazione cubica alla matrice B.
(5) Applicazione della trasformata DWT, ripetendo esattamente su $A$ e $B$ i passi 4 e 5 della fase di generazione ed inserimento.
(6) Rilevamento del watermark. Indicando con $I_L^{\theta_1}, I_L^{\theta_2}, I_L^{\theta_3}$ le sottobande relative alle alte frequenze dell'immagine originale $A$ e con $\tilde{I}_L^{\theta_1}, \tilde{I}_L^{\theta_2}, \tilde{I}_L^{\theta_3}$ quelle di $B$, con $\theta_i \in \{LH, HL, HH\}$ e $\theta_k \cap \theta_i = \oslash, \forall i \neq k$, si considerano le sottomatrici $I_L^{\theta_1}$ e $\tilde{I}_L^{\theta_1}$ in cui nella fase di inserimento è stato aggiunto il parametro $\omega$ e che rappresentano l'input per la *funzione di comparazione*.

FIGURA 1. Immagine originale

La funzione di comparazione analizza la variazione dei valori degli elementi delle sottobande in un intorno della riga modificata. Nell'implementazione della funzione di comparazione $C_\delta$ , si è tenuto conto, sia delle variazioni percentuali del valore dei pixel dovute alla compressione JPEG, che può ritenersi il primo attacco effettuato sull'immagine watermarkata, sia di eventuali modifiche su tali valori apportate da possibili altri attacchi. È stato determinato sperimentalmente un modo per generare un intervallo di confidenza in cui varia l'alterazione dei pixel coinvolti nella fase di inserimento del watermark. La funzione di comparazione $C_\delta$ realizzata fornisce le seguenti risposte:

- Watermark identificato, se la variazione rientra nell'intervallo di confidenza valutato.

FIGURA 2. Immagine watermarkata

- Watermark non identificato, se la variazione non rientra nell'intervallo di confidenza valutato. Questo implica che tale variazione è scaturita da un fattore diverso dal marchio.

Le figure 1 e 2 riportano rispettivamente un'immagine originale e la relativa watermarkata; le figure 3 e 4 mostrano la differenza tra l'immagine originale e la relativa watermarkata, rispettivamente prima e dopo la memorizzazione JPEG.

L'utilizzo delle immagini oggetto della sperimentazione è stato autorizzato dalla Conferenza Episcopale Italiana come da lettera di consegna al Dipartimento di Matematica dell'Università degli Studi di Messina, datata 20 Giugno 2003.

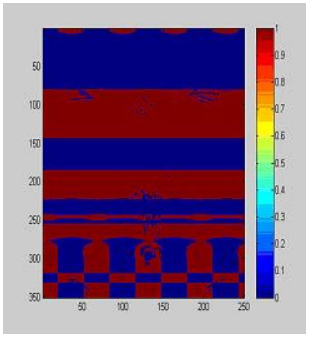


FIGURA 3. Differenza tra l'immagine 4 originale e watermarkata con DWT mediante funzione base Symlets Wavelets.3 (prima della memorizzazione su file JPEG)

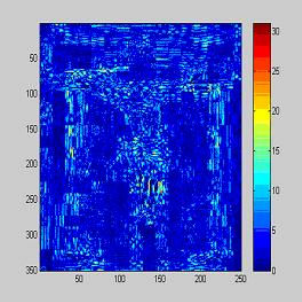

FIGURA 4. Confronto tra l'immagine originale e watermarkata, dopo il salvataggio in formato JPEG

## 5. Attacchi

Le immagini watermarkate con WM1.0 sono state sottoposte a diversi tipi di attacchi [12, 13] Al variare della chiave, hanno resistito alle più comuni prove di attacco ed ad una ulteriore compressione Wavelet effettuata con funzioni differenti da quelle usate nella fase di inserimento. Sono stati effettuati attacchi tipici dell'elaborazione di immagine applicando tecniche di filtraggio, compressione, cropping (ritaglio di una parte dell'immagine), riduzione di dimensione, cambiamento di formato, deformazioni geometriche, ma anche attacchi effettuati da programmi commerciali come: Jietter attack, StirMark [S5] e Mosaic attack. I prodotti di watermarking commerciali solitamente non sono robusti rispetto agli ultimi tre attacchi precedentemente citati. Dalle statistiche ottenute dopo numerose prove sperimentali si è messo in evidenza come il marchio inserito risulta essere abbastanza robusto ai diversi tipi di attacchi [12, 13].

## 6. Risultati e utilizzo di WM 1.0

**6.1. Risultati.** Le prove sperimentali dell'algoritmo WM 1.0 sono state inizialmente effettuate su oltre 140 immagini digitali a colori, estratte da un CD commerciale[12, 13]. Esse forniscono un buon campione di verifica, in quanto si differenziano per dimensione e caratteristiche, rappresentano, infatti, principalmente foto di città, monumenti e paesaggi sia di giorno che di notte sotto differenti illuminazioni. In [12, 13] è riportata anche una selezione di tali immagini. Su tutte le immagini è stato effettuato l'inserimento del watermark con differenti chiavi in modo da individuare, a parità di livello di decomposizione, quale base di funzioni wavelet fornisse i migliori risultati nel rilevamento del watermark, tenendo presente, comunque che la scelta della funzione wavelet dipende fortemente dalla caratteristica dell'immagine.

**6.2. Utilizzo di WM 1.0.** Dopo questa sperimentazione iniziale, l'algoritmo WM 1.0 è stato integrato nei sistemi esistenti sviluppati presso IDS Informatica, trovando in queste soluzioni un ambiente applicativo che favorisce sia per la propria architettura e funzionalità, sia per la tipologia, caratteristiche, e rilevanza delle immagini digitali trattate, l'integrazione con la procedura di watermark dalla quale, al contempo ne ricava un fattore di "valore aggiunto" per i servizi forniti.

I sistemi applicativi esistenti, infatti:

- forniscono funzionalità di gestione di banche dati documentali.
- sono progettati sia secondo un modello client/server a due livelli, sia secondo un'architettura a tre livelli con tecnologia e interfaccia Web, per rendere, quindi, servizi sia in ambiente intranet che internet, con un conseguente e differenziato requisito della tutela della proprietà delle immagini digitali.
- dispongono di una banca dati di circa 270.000 immagini, in alta e bassa risoluzione acquisite da scanner, fotocamere digitali, diapositive rispettando opportune direttive conformi alle linee guida indicate dalla Conferenza Episcopale Italiana. Tali immagini sono pubblicate sul Web in formato JPEG.

Fattori, questi, che indubbiamente hanno fortemente favorito ed indirizzato l'implementazione dell'algoritmo, e fornito una base sperimentale esaustiva e completa per quanto realizzato e per i successivi sviluppi. WM 1.0 è utilizzato nel servizio BeWeB, sviluppato da I.D.S. Informatica per watermarkare le immagini dei beni culturali ecclesiastici pubblicati su internet. Il servizio è raggiungibile all'URL: http://www.chiesacattolica.it/beweb/

## 7. Conclusioni e prossimi sviluppi

Dai test sperimentali effettuati [12, 13, 14] WM 1.0 ha un basso costo computazionale per immagini con dimensioni inferiori ai 20Kb e soddisfa i requisiti di impercettibilità, robustezza e bassa probabilità di errore. WM 1.0 inserisce infatti un watermark impercettibile all'occhio umano; ha superato positivamente diverse prove di attacco; variando opportunamente la chiave, il 90 per cento circa delle immagini campionate sono watermarkate con successo, con un limitato numero di errori per falsi positivi e falsi negativi.

Le caratteristiche intrinseche di WM 1.0, l'utilizzo delle wavelet, le modalità di inserimento, le caratteristiche e il formato delle immagini su cui applicare WM1.0 indirizzano possibili sviluppi futuri con un approccio mirato sia a definire più rigorosamente l'incidenza della compressione finale sull'immagine watermarkata sia a rendere il watermark maggiormente correlato e legato alle caratteristiche delle immagini.

In tal senso una primissima idea potrebbe essere quella, per il primo punto, di valutare le variazioni del livello di compressione JPEG dopo l'inserimento del watermark, e per il secondo, quello di suddividere, con un opportuno criterio, l'immagine originale in blocchi - sottomatrici quadrate potenza di 2 - sui quali applicare WM1.0. Ad una prima valutazione, questo approccio evitando di immergere in una opportuna matrice quadrata quelle a cui corrisponde una matrice rettangolare, lega maggiormente il watermark alle dimensioni effettive delle immagini; inoltre si rivela utilizzabile per watermarkare immagini di dimensioni superiori, anche, quindi immagini ad alta risoluzione.

## Riferimenti bibliografici

[1] F. Bartolini, R. Cardelli, V. Cappellini, A. De Rosa, A. Piva, Digital Watermarking: A Solution To Electronic Copyright Management System Requirements, Dipartimento di Elettronica e Telecomunicazioni. Università di Firenze, 2002. http://Medicif.org/Dig_Library/Stateart/Ipr/Piva/Piva_Doc.Html

[2] F. Bartolini, R. Cardelli, V. Cappellini, A. De Rosa, A. Piva, Digital Watermarking: A Solution To Electronic Copyright Management System Requirements, Dipartimento di Elettronica e Telecomunicazioni. Università di Firenze, 2002. http://Medicif.org/Dig_Library/Stateart/Ipr/Piva/Piva_Doc.Html

[3] F. Bartolini, R. Caldelli, V. Cappellini, A. De Rosa, A. Piva, Tecnologie di marchiatura elettronica per i Beni Culturali, Alta Frequenza Rivista di Elettronica, Vol. 13, N. 2, 2001
[4] A.G. Bors, I. Pitas, Image watermarking using block size selection and DCT domain constraints, Optics Express 512, Vol. 3 No.!12, 1998.
[5] C. K. Chui, An Introduction to Wavelet, Academic Press, Boston, 1992.
[6] S. Craver, N. Memon, B. Yeo And M. Yeung, Can Invisible Watermarks Resolve Rightful Ownerships?, IBM Thechnical Report RC 20509, July 25, 1996.
[7] S. Craver, N. Memon, B. Yeo And M. Yeung, On the Invertibility of Invisible Watermarking Techniques, In Proc. IEEE Internat. Conf, Image Processing '97, (Santa Barbara, CA), October 26-29, 1997, pp. 540-543. http://clip.informatik.uni-leipzig.de/ toelke/Watermark/ip971157.pdf
[8] S. Craver, N. Memon, B. Yeo and M. Yeung, Resolving Rightful Ownership With Invisible Watermarking Techniques: Limitation, Attacks, And Implications, IEEE Journal On Selected Areas in Commucation, 1998.
[9] M. Corvi, G. Picchiotti, Wavelet-based image watermarking for copyright protection, Proc. SCIA 1997, 1997, pp. 157-164.
[10] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure, Spread Spectrum Watermarking for Multimedia, IEEE Trans. on Image Processing, Vol. 6 No. 12, 1997, pp.1673-1687.
[11] I. Daubechies, Ten Lectures on Wavelets. SIAM, Philadelphia, 1992.
[12] Jiri Fridrich, Application of Data Hiding in Digital Images,
Tutorial for ISPACS'98 Conference in Melbourne, Australia Novembre 4-6, 1998.
http://varuna.ece.ucsb.edu/ece178W02/temp/fridrich98application.pdf
[13] S. Giovinazzo, Sviluppo di tecniche per la realizzazione di algoritmi di watermarking, Tesi di Diploma in Informatica, A.A.2000/2001, relatore L. Puccio.
[14] S. Giovinazzo, Tutela del diritto d'autore dell'immagine digitale, watermaking e tecniche di attacco, Tesi di Laurea in Informatica, A.A.2001/2002, relatore L. Puccio.
[15] S. Agreste, Tecniche di Watermarking mediante wavelet, Tesi di Laurea in Informatica, A.A.2002/2003, relatore L. Puccio.
[16] D. Kundur, Hatzinakos, Digital watermarking based on multiresolution wavelet data fusion, Proc. IEEE Special Issue on Inteligent Signal Processing, 1997.
[17] E. Koch, J. Zhao, Copyright protection for multimedia data, Proc. IEEE Workshop on Nonlinear Signal and Image Processing, NeosMarmaras, June 1995.
[18] M. Kutter and F.P.A .Peticolas, A Fair Benchmark for Image Watermarking System, Electronic Imaging'99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, 25-27 January 1999. http://www.cl.cam.ac.uk/ fapp2/publications/ei99-benchmark.pdf
[19] M.J.J. Maes, Twin peaks: The histogram Attack to Fixed Depth Image Watermark, Proc. Of of the Workshop on Information Hiding, Portland, April 1998.
[20] S.G. Mallat, Multiresolution Approximations and Wavelet Orthonormal Bases of , Transaction of the american mathematical society Volume 315,number 1, September 1989.
[21] Y. Meyer, Ondelettes et opreteurs, I: Ondelettes, Herman, Paris, 1990.
[22] M. Misiti, Y. Misiti, G.Oppenheim, J.M. Poggi, Wavelet Toolbox for use with MATLAB, The Math Works Inc., 1996.
[23] F.A.P. Peticolas, R.J.Anderson and M.G.Kuhn, Attacks on Copyright Marking Systems, Davi Aucsmith, Ed.,"Second waorkshop on information
[24] I. Pitas, T.Kaskalis, Signature Casting on Digital Images, Proc. IEEE Workshop on Nonlinear Signal and Image Processing, NeosMarmaras, June 1995.
[25] I. Pitas, A method for signature casting on digital images, Interational Conference on Image Processing, Vol. 3, 1996, pp.215-218.
[26] A. Piva, M. Barni, F. Bartolini, V. Cappellini, DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image, Proc. IEEE Internat. Conf, Image Processing '97, (Santa Barbara, CA), October 26-29, 1997, pp. 520-523.
[27] A. Piva, M. Barni, F.Bartolini, V. Cappellini, A DCT-Domain System for Robust Image Watermarking, Signal Processing, Special Issue on Watermarking, (66) 3, 1998, pp.357-372.
[28] M.d. Swanson, B. Zhu, A.H. Tewfik, Transparent Robust Image Watermarking, IEEE International Conference on Image Processing, Vol. 3, 1996, pp. 211-214.

[29] M.d. Swanson, B. Zhu, A.H.Tewfik, Robust Data Hiding for Image, 7th IEEE Digital Signal Processing Workshop, Loen (Norway), 1996, pp.37-40.
[30] M.d. Swanson, B. Zhu, A.H.Tewfik, Multiresolution Scene-Based Video Watermarking Using Perceptual Model, IEEE J. on Special Areas in Comunications, V. 16 No.4, 1998, pp.540-550.

Santa Agreste
e-mail: {sagreste.gina}@dipmat.unime.it
Nuccio Castorina, Salvatore Giovinazzo, Daniela Prestipino
e-mail: {n.castorina,s.giovinazzo,d.prestipino}@glauco.it
Luigia Puccio
e-mail: gina@dipmat.unime.it
Dipartimento di Matematica
Università degli Studi di Messina