

4. TEHNICI DE WATERMARKING PENTRU IMAGINI

Unul dintre motivele dezvoltării rapide a cercetării în domeniul watermarking-ului digital este necesitatea de a găsi soluții pentru protecția proprietății intelectuale a materialelor digitale. Chiar dacă există tehnici de watermarking pentru orice tip de date digitale, majoritatea lucrărilor din literatura de specialitate se adresează tehnicilor de watermarking pentru imagini pentru protecția drepturilor de autor. În acest capitol realizăm un rezumat al tehnicilor robuste de watermarking propuse în literatura de specialitate. Majoritatea tehnicilor descrise se aplică imaginilor cu nuanțe de gri, dar pot fi extinse ușor și pentru imagini color prin inserarea watermark-ului în toate componentele de cromatică și pentru secvențe video prin inserarea aceluiași watermark sau watermark-uri diferite în diferite cadre ale secvenței video. O să punctăm, în primul rând, ideile de bază și, apoi, să explicăm mai detaliat câteva metode pentru a ilustra modul în care principiile sunt puse în practică.

Foarte mulți algoritmi de watermarking sunt, de fapt, foarte asemănători și diferă doar parțial sau prin unul dintre următoarele patru aspecte singulare:

- **Alegerea locației de inserare a watermark-ului.** Aici adresăm metode ce nu iau în calcul, respectiv, ce iau în calcul Sistemul Vizual Uman (SVU).
- **Domeniul în care operează algoritmul.** De exemplu, un algoritm poate modifica imaginea direct în domeniul spațial pentru a insera un watermark sau poate întâi transforma imaginea originală într-un alt domeniu, de exemplu, în domeniul Transformatei Fourier Discrete, Transformatei Cosinus Discrete, Transformatei Wavelet Discrete, insera watermark-ul în domeniul transformat și, în cele din urmă, calcula transformata inversă pentru a obține imaginea cu watermark. Vor fi discutate avantajele și dezavantajele diferitelor domenii.

- **Codarea watermark-ului.** Este adresat modul de reprezentare a informației de inserat. Watermark-ul poate fi pur și simplu însumat la datele originale sau aceste date pot fi modificate pentru a oglindi prezența watermark-ului.
- **Formarea datelor cu watermark.** Aici sunt prezentate modurile în care watermark-ul este inserat în datele sursă.
- **Modul de extragere a watermark-ului.** Este strâns legat de modul de inserare. Deoarece watermark-ul are o putere mică în comparație cu datele sursă, decodorul operează într-un mediu cu raport semnal-zgomot mic. Există o serie de metode de îmbunătățire a performanțelor decodurului, inclusiv în cazul în care imaginea cu watermark a fost modificată de un atacator.

Fiecare dintre aceste categorii vor fi discutate mai pe larg în cele ce urmează.

4.1. Locația de inserare a watermark-ului

În literatura de specialitate problema imperceptibilității watermark-ului este tratată de regulă în două moduri diferite. Prima grupă de metode permite doar modificări arbitrare mici pentru inserarea watermark-ului într-o imagine sau secvență video în domeniul spațial sau transformat, pentru a nu cauza vreo distorsiune vizibilă. Metodele din a doua grupă abordează aceeași problemă prin utilizarea unor proprietăți explicite ale sistemului vizual uman pentru a satisface compromisul dintre imperceptibilitate și robustețe. Majoritatea metodelor din grupul doi sunt tehnici de watermarking cu spectru împrăștiat [44]. Tehnicile ce exploatează caracteristici ale SVU, ca de exemplu sensibilitatea spațială sau la luminanță [45], [46], pot fi, de asemenea, incluse în acest grup. Alte metode sunt bazate pe caracteristici de nivel mai înalt ale SVU, ca de exemplu mascarea în frecvență [47], mascarea entropiei [48], mascarea entropiei mișcării [49], fenomene de focalizare a ochiului uman [50] și unele caracteristici temporale ale SVU. Toate acestea cresc în mod clar complexitatea algoritmului. Aplicația cea mai importantă pentru astfel de metode este protecția drepturilor de autor unde complexitatea sau procesarea în timp real nu sunt cerințe prea importante.

4.1.1. Tehnici de watermarking ce nu folosesc caracteristicile SVU

Una dintre cele mai populare abordări din acest grup lucrează în domeniul spațial și inserează watermark-ul în cel mai puțin semnificativ bit al pixelilor imaginii [51]. Dezavantajul acestei metode este sensibilitatea la procesări de semnal. Koch și alții [52, 53] sugerează schimbarea ordinii unor perechi de coeficienți DCT de frecvență medie pentru a insera un watermark, deoarece frecvențele medii tind să supraviețuiască compresiei JPEG și produc o distorsiune vizuală mai mică decât frecvențele joase. O metodă asemănătoare [54] inserează un bit de watermark în cadrele Intra (I) a secvenței video codate MPEG prin schimbarea relației dintre coeficienții de frecvență medie din blocuri alăturate. Într-o abordare în domeniul Wavelet [55], cadrele Y ale secvenței video sunt descompuse în subnivele wavelet și watermark-ul este inserat în componentele de frecvență joasă printr-un proces controlat de cuantizare [56]. Wang și Kuo selectează coeficienți wavelet importanți pentru watermarking [57] bazându-se pe un codec wavelet cu mai multe praguri [58], dar algoritmul lor necesită imaginea originală pentru decodare. În lucrarea [59], watermark-ul este inserat în domeniul Transformatei Fourier Discrete 3-D. Pentru fiecare element al secvenței de watermark sunt selectați doi coeficienți din domeniul transformat și elementul secvenței de watermark este inserat în unul dintre ei în funcție de semn.

Alte metode din acest grup folosesc semnalul video comprimat ca intrare, iar watermark-ul este inserat direct în coeficienții codați sau în vectorii de mișcare după compresia video [60-63].

Din păcate, nici una dintre aceste metode nu ia în considerare SVU la inserarea watermark-ului pentru a exploata percepția umană.

4.1.2. Tehnici de watermarking ce folosesc caracteristicile SVU

În această clasă de metode, problema imperceptibilității este tratată folosind proprietățile SVU.

Ochiul uman este mai puțin sensibil la zgomot în zone cu textură decât în zone uniforme ale unei imagini sau cadru video. Sistemele de compresia tind și ele să păstreze intacte zonele cu textură și marginile, cuantizând în schimb zonele uniforme cu un pas de cuantizare mare. Din aceste motive Cox și alții [64,65] argumentează că watermark-ul ar trebui inserat în zone perceptual importante ale imaginii. Un atacator nu poate îndepărta ușor watermark-ul fără a cauza o distorsiune importantă. În această metodă, după aplicarea transformatei DCT imaginii, watermark-ul este ponderat cu o fracțiune a coeficientului DCT și adăugat la același

coeficient DCT. De fapt, ponderarea energiei watermark-ului în funcție de valoarea coeficientului din domeniul frecvență este o aproximare a principiului de mascare de contrast a SVU [47] care se referă la scăderea vizibilității unui semnal în prezența altui semnal mai puternic. În cadrul metodelor de watermarking cu spectru împrăștiat scăderea vizibilității se presupune direct proporțională cu amplitudinea coeficientului DCT, cu toate că în realitate dependența este neliniară [45, 47]. Un dezavantaj al acestei metode este posibilitatea apariției de artefacte vizibile în imagine, mai ales în regiuni uniforme [66].

Darmstaedtler și alții descriu o schemă de watermarking în domeniul spațial la care imaginea este divizată în blocuri, fiecare bloc este clasificat în funcție de contrastul său, iar watermark-ul este inserat corespunzător. Metodele de watermarking în diferite domenii vor fi discutate mai în detaliu în subcapitolul 5.2.

Tehnicile de watermarking cu spectru împrăștiat sunt, de asemenea, adaptate la secvențe video prin folosirea unei descompunerii 3-D multi-rezoluție. În [67], după ce semnalul video este descompus în sub-semnale folosind Transformata Wavelet 3-D, watermark-ul este însumat la coeficienții wavelet trece-sus la fiecare nivel de rezoluție, excluzând primul nivel. Într-o abordare asemănătoare, în [68] watermark-ul este însumat în domeniul wavelet 3-D prin ponderarea watermark-ului cu o mască definită în funcție de varianța și luminanța subbenzilor 3-D. Datorită aceluiași raționament ca și în cazul tehnicilor de watermarking cu spectru împrăștiat pentru imagini, dezavantajul acestor metode este o posibilă distorsiune de tip fluctuație în domeniul timp.

Tot din acest grup fac parte și tehnicile ce folosesc sensibilitatea spațială și la luminanță a SVU. Sensibilitatea spațială se referă la fenomenul de diferențiere mai ușoară a modificărilor din regiuni de contrast scăzut, în comparație cu schimbările din regiunile de contrast mare. Una dintre cele mai importante lucrări de watermarking în domeniul comprimat [69] utilizează sensibilitatea spațială prin folosirea unui coeficient de ponderare mai mic pentru inserarea watermark-ului în regiuni trece-jos și un coeficient mai mare pentru regiunile de contrast mare ale cadrului video. Ulterior a fost propusă în [70] o abordare asemănătoare pentru protecția la copiere pentru formatul DVD. În [71] același principiu este folosit pentru inserarea watermark-ului în obiecte video. Aici este aplicată Transformata Wavelet obiectelor video și este inserat un watermark în coeficienții de frecvență înaltă prin ponderarea cu o mască vizuală calculată din caracteristicile spațiale ale imaginii din subbanda respectivă. În [72] sensibilitatea spațială a SVU este exploatată în domeniul DCT. Pentru fiecare bloc DCT de luminozitate, de dimensiune 8x8 pixeli, al cadrelor I ale semnalului

video codat MPEG, este determinată puterea și regiunea de inserare a watermark-ului în funcție de energia totală a coeficienților AC din acel bloc, conform sensibilității spațiale a SVU. Pe lângă sensibilitatea spațială, este folosită și sensibilitatea la luminanță a SVU [73]. În acest caz, watermark-ul este ponderat cu o mască vizuală, având la bază faptul că ochiul uman este mai puțin sensibil la contrast în zone întunecate sau luminoase, în comparație cu zonele de luminanță medie [45].

Pentru toate metodele anterioare se folosește, de regulă, un factor de scalare ce satisface compromisul dintre imperceptibilitate și robustețe. În mod evident, dezavantajul unei astfel de abordări este necesitatea unui proces de control pentru a satisface criteriul de imperceptibilitate de fiecare dată când watermark-ul este inserat într-un conținut diferit.

Există și metode ce folosesc modele mai sofisticate ale SVU, utilizând măsurări perceptuale explicite, numite praguri de contrast, pentru determinarea locației și puterii watermark-ului. În general, pragul de contrast se referă la nivelul minim de contrast pentru ca o grilă sinusoidală să fie vizibilă [47]. Creșterea pragurilor de contrast pentru multe caracteristici diferite ale SVU, ca de exemplu mascarea luminanței [45], mascarea contrastului [45], mascarea entropiei [48], mascarea entropiei mișcării [49], mascarea temporală [74] și fenomene de focalizare a ochiului uman [50] este analizată prin teste perceptuale. Pragurile pentru aceste fenomene se numesc, pur și simplu, *Just Noticeable Differences* (JND - Diferențe Abia Perceptibile) [45]. În [66] JND sunt exploatate în contextul mascării luminanței și a contrastului pentru determinarea puterii și a locației de inserare a watermark-ului. Watermark-ul este inserat în blocuri de 8x8 coeficienți DCT care sunt mai mari decât JND, pentru a satisface imperceptibilitatea și robustețea la atacuri prin compresie. Într-o altă abordare [75] este folosită mascarea entropiei ce se referă la efectul de interacțiune dintre blocuri vecine la calcularea valorilor JND. Metodele mai sus menționate sunt extinse și pentru video codat MPEG prin inserarea watermark-ului în cadre I și aplicarea unei interpolări liniare simple în timp a watermark-urilor între două cadre I consecutive, pentru a evita pâlpâirea temporală la fiecare cadru intra din secvența video. Un dezavantaj al acestor metode este ineficiența în utilizarea „spațiului disponibil” pentru ascunderea datelor, deoarece cadrele inter sunt excluse din procesul de watermarking.

Problema imperceptibilității, în special pâlpâirea temporală, este, de asemenea, abordată în unele metode [76-78] prin luarea în calcul atât a dimensiunilor spațiale, cât și a celei temporale în procesul de inserare a watermark-ului. În [76] o Transformată Wavelet Temporală este aplicată fiecărui cadru video și în fiecare cadru de coeficienți wavelet este

inserat câte un watermark diferit, ponderat conform caracteristicilor SVU de mascare spațială și de contrast. O altă schemă de watermarking [77], ce se ocupă cu problema pâlpâirii temporale este propusă, în special pentru cinematografia digitală, inserând watermark-ul în valoarea medie a luminanței Y a semnalului video. Pentru a evita pâlpâirea temporală se inserează același bit de watermark într-un număr de cadre succesive. Ulterior, metoda a fost extinsă în [78] prin filtrarea trece-jos a watermark-ului înainte de inserare pentru a nu cauza o diferență majoră între pixeli consecutivi.

Pe lângă alegerea locației conform importanței lor vizuale, se poate folosi și o cheie, de regulă generată de un număr aleator, pentru selectarea coeficienților ce urmează să conțină watermark-ul. Un exemplu este algoritmul Patchwork [55] ce selectează n perechi de pixeli folosind o cheie K . Luminanța a jumătate dintre pixelii selectați este incrementată cu 1, pe când cealaltă jumătate este decrementată cu 1. Decodorul ce folosește aceeași cheie K selectează aceleași perechi de pixeli și compară diferența dintre mediile celor două jumătăți. Pornind de la prezumția că n este suficient de mare și că pixelii selectați sunt relativ independenți și distribuiți identic, diferența dintre cele două medii va fi aproximativ $2n$. Această metodă permite însă doar verificarea existenței watermark-ului și nu poate insera un watermark de dimensiune mai mare. Algoritmul din [79] folosește o cheie pentru a partiționa pixelii imaginii și a selecta un subset pentru watermarking. În comparație cu algoritmul Patchwork ce schimbă doar statistica imaginii, watermark-ul este adaptat perceptual imaginii. În sfârșit, se poate insera repetat watermark-ul în întreaga imagine și se pot evalua diferitele copii extrase la decodor conform autenticității lor [80].

4.2. Domeniul de inserare a watermark-ului

4.2.1. Watermarking în domeniul spațial

Primii algoritmi de watermarking au fost concepuți în domeniul spațial. Aceste metode sunt de obicei mult mai directe și, astfel, necesită și mult mai puțin efort de calcul decât cele ce lucrează în domeniul transformatei. De aceea, astfel de algoritmi sunt indicați pentru implementarea în timp real. În continuare sunt prezentate câteva dintre cele mai importante metode în domeniul spațial.

A) Watermark vizibil

O tehnică foarte simplă, dar folosită la scară largă, pentru inserarea watermark-ului în imagini este adăugarea unui simbol peste imaginea existentă. De obicei acest simbol este tot o imagine, un logo sau ceva asemănător care distorsionează imaginea gazdă.

În exemplul din Figura 4.1 simbolul este imaginea roșie din mijloc, iar imaginea gazdă este cea din stânga. Într-un editor standard de imagini este posibilă însumarea celor două imagini și obținerea imaginii cu watermark. Atâta timp cât watermark-ul este cunoscut, procesul invers este posibil fără efecte adverse, astfel încât imaginea originală nu trebuie păstrată. Watermark-ul este vizibil și, chiar și fără watermark-ul original, este posibilă eliminarea simbolului watermark fără prea mare efort.



Figura 4.1. Inserarea unui watermark vizibil

B) Modificarea celui mai puțin semnificativ bit

Dacă fiecare pixel al unei imagini în tonuri de gri este reprezentat pe 8 biți, imaginea poate fi împărțită în 8 planuri de biți. În Figura 4.2, aceste 8 planuri de bit sunt reprezentate pentru imaginea „Lena”, unde, în colțul stânga sus, este imaginea corespunzătoare celui mai semnificativ plan de biți, iar, în colțul dreapta jos, imaginea corespunzătoare celui mai puțin semnificativ plan de biți.

Deoarece cel mai puțin semnificativ plan de biți nu conține informație vizuală foarte importantă, poate fi înlocuit printr-o cantitate enormă de biți de watermark. În Figura 4.3 sunt prezentate patru exemple de ascundere a watermark-ului într-unul sau mai multe planuri de biți, unde imaginea din stânga este imaginea gazdă iar cea din dreapta este watermark-ul.

Există diferite variații ale acestei metode. În [81], autorul propune 2 metode: prima metodă înlocuiește cei mai puțin semnificativi biți ai fiecărui pixel cu un zgomot pseudo-aleator iar a doua însumează o secvență pseudo-aleatoare la planul de biți cel mai puțin



Figura 4.2. Planurile de biți pentru imaginea Lena

semnificativ. O altă metodă de watermarking calculează o sumă de verificare a imaginii originale și apoi o inserează în cel mai puțin semnificativ bit al unor pixeli aleși aleator [81-83].



Figura 4.3. Înlocuirea biților mai puțini semnificativi ai imaginii din stânga cu biții cei mai semnificativi ai imaginii din dreapta

Aceste tehnici de watermarking nu sunt prea sigure și nici prea robuste la tehnici de procesare, deoarece cel mai puțin semnificativ plan de biți poate fi ușor înlocuit cu biți aleatori, eliminând astfel eficient biții watermark-ului.

C) Tehnici de watermarking bazate pe corelație

O metodă directă de a insera un watermark într-o imagine în domeniul spațial este adăugarea unei secvențe de zgomot pseudo-aleator la valorile de luminanță ale pixelilor.

Multe metode sunt bazate pe acest principiu [84-87], [25], [88]. În general, secvența de zgomot pseudo-aleator constă din întregii $\{-1,0,1\}$, dar pot fi folosite și numere în virgulă mobilă. Secvența este generată pe baza unei chei, folosind, de exemplu, registre de deplasare sau numere binare deplasate aleator. Singura constrângere este ca energia secvenței să fie cât mai uniform distribuită și ca secvența să nu fie corelată cu conținutul imaginii sursă. Pentru a crea imaginea cu watermark $I_w(x,y)$, secvența pseudo-aleatoare $W(x,y)$ este multiplicată cu un factor de câștig k și apoi adunată la imaginea gazdă $I(x,y)$, ca în Figura 4.4.

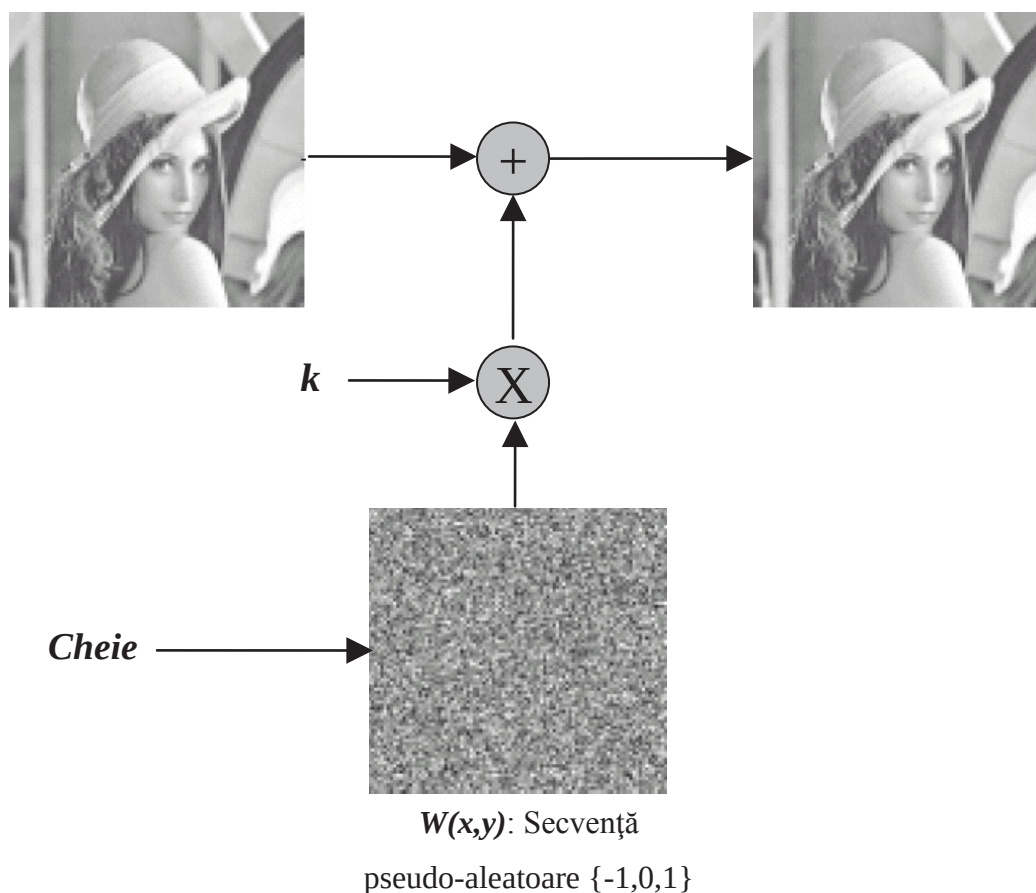


Figura 4.4. Procedura de inserare a watermark-ului

$$I(x, y) = I(x, y) + k \cdot W(x, y) \quad (4.1)$$

Pentru a detecta watermark-ul într-o imagine $I'_w(x, y)$, calculăm corelația dintre imaginea $I'_w(x, y)$ și secvența de zgomot pseudo-aleator $W(x, y)$. În general, înainte de efectuarea corelației $W(x, y)$ este normat, astfel încât să aibă medie nulă. Dacă corelația R_{xy} depășește un anumit prag T , detectorul determină că imaginea $I'_w(x, y)$ conține watermark-ul $W(x, y)$:

$$\begin{aligned} R_{I'_w(x, y)W(x, y)} > T &\rightarrow W(x, y) \text{ detectat} \\ < T &\rightarrow W(x, y) \text{ nedetectat} \end{aligned} \quad (4.2)$$

Dacă $W(x, y)$ conține doar întregii $\{-1, 1\}$ și numărul de „-1” este egal cu numărul de 1, atunci putem estima corelația conform relației (4.3).

$$\begin{aligned} R_{I'_w(x, y)W(x, y)} &= \frac{1}{Z} \sum_{i=1}^Z I'_{w_i}(x, y) W_i(x, y) = \frac{1}{Z} \sum_{i=1}^{Z/2} I'_{w_i} W_i^+ + \frac{1}{Z} \sum_{i=1}^{Z/2} I'_{w_i} W_i^- \\ &= \frac{1}{2} \left\{ \mu[I_w^+(x, y)] - \mu[I_w^-(x, y)] \right\} \end{aligned} \quad (4.3)$$

unde Z este numărul de pixeli ai imaginii I'_w , supraîndicii $^{+,-}$ indică setul de pixeli pentru care secvența de zgomot corespunzătoare este pozitivă sau negativă și $\mu[I_w^+(x, y)]$ este valoarea medie a pixelilor din $I_w^+(x, y)$. Din relația (4.3) rezultă că problema detecției watermark-ului corespunde testării ipotezei dacă două seturi aleatoare de pixeli au aceeași medie.

Detectorul de watermark poate face două tipuri de erori. În primul rând poate detecta existența watermark-ului, chiar dacă el nu există. Această eroare se numește pozitiv fals. În al doilea rând, detectorul poate rejecta existența watermark-ului, chiar dacă există. Această eroare se numește negativ fals. În [24] probabilitățile de apariție a acestor două tipuri de erori rezultă din modelul autoregresiv de ordinul întâi al imaginii:

$$P_{pf} = \frac{1}{2} \operatorname{erfc}\left(\frac{T\sqrt{Z}}{\sigma_w \sigma_I \sqrt{2}}\right) \quad \text{si} \quad P_{nf} = \frac{1}{2} \operatorname{erfc}\left(\frac{(\sigma_w^2 - T)\sqrt{Z}}{\sigma_w \sigma_I \sqrt{2}}\right) \quad (4.4)$$

unde

$$erfc(x) = \frac{1}{\sqrt{2\pi} \int_x^\infty e^{-t^2/2} dt} \quad (4.5)$$

În această relație, σ_w^2 reprezintă varianța pixelilor watermark-ului și σ_I^2 este varianța pixelilor imaginii. Dacă watermark-ul $W(x, y)$ este format doar din întregii $\{-1, 1\}$ și numărul de „-1” este egal cu numărul de „1”, atunci varianța watermark-ului σ_w^2 este egală cu k^2 . Erorile P_{fp} și P_{fn} pot fi minimizate prin creșterea factorului de câștig k . Dar, pe de altă parte, alegerea de valori mai mari pentru factorul de câștig duce la scăderea calității vizuale a imaginii cu watermark.

Deoarece conținutul imaginii poate avea interferențe cu watermark-ul, mai ales la componentele de frecvență joasă, performanța de detecție a detectorului poate fi îmbunătățită prin filtrare înainte de a calcula corelația. Acest lucru scade contribuția imaginii originale la corelație. De exemplu, poate fi folosit un simplu filtru de accentuare a conturilor cu funcția pondere F_{contur} dată de:

$$F_{contur} = \frac{1}{2} \begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix} \quad (4.6)$$

Aplicarea acestui filtru înaintea operației de corelație reduce semnificativ probabilitatea de eroare, chiar dacă calitatea vizuală a imaginii cu watermark a fost serios afectată de filtrare [23], [84].

Pentru o serie de aplicații se dorește creșterea capacității de inserare. Din punctul de vedere al detectorului, o imagine I poate fi privită ca un zgomot gaussian ce distorsionează informația de watermark W , iar imaginea cu watermark I_w poate fi privită ca ieșire a unui sistem de comunicație afectat de zgomot gaussian prin care este transmis watermark-ul. În acest caz, transmisia sigură a watermark-ului este teoretic posibilă dacă rata de informație nu depășește capacitatea canalului [89]:

$$C_c = W_b \log_2 \left(1 + \frac{\sigma_w^2}{\sigma_I^2} \right) \text{ biți/pixel} \quad (4.7)$$

unde C_c este dată în biți per pixel al imaginii și banda disponibilă W_b este egală cu 1 Hertz per pixel. Pentru sistemele reale, totuși, poate fi determinată empiric o limită mai redusă [90]:

$$C_C = W_b \log_2 \left(1 + \frac{\sigma_w^2}{\alpha \sigma_I^2} \right) \text{ biți/pixel} \quad (4.8)$$

unde α este un factor de scalare ales, de obicei, mai mare ca 1, în jurul valorii 3. Deoarece raportul semnal-zgomot σ_w^2 / σ_I^2 este mult mai mic decât unu, relația (4.8) poate fi aproximată cu:

$$C_C \approx \frac{1}{\ln 2} \left(\frac{\sigma_w^2}{\alpha \sigma_I^2} \right) \text{ biți/pixel} \quad (4.9)$$

Conform relației (4.9), este posibilă inserarea a mai mult de 1 bit de informație într-o imagine. De exemplu, un watermark alcătuit din numerele întregi $\{-k, k\}$, adăugat la imaginea Lena de rezoluție 512x512 pixeli (Figura 4.4), poate avea aproximativ 50, 200 sau 500 de biți de informație pentru $k=1, 2, 3$ și $\alpha=3$.

Există o serie de metode pentru a crește capacitatea tehnicii de watermarking de bază. Cea mai simplă metodă pentru a insera un șir de l biți de watermark $b_0 b_1 \dots b_{l-1}$ într-o imagine, este împărțirea imaginii I în l subimagini $I_0, I_1, \dots, I_{l-1}$ și inserarea unui watermark în fiecare subimagine, unde fiecare watermark reprezintă un bit al șirului [84, 90, 91]. Acest procedeu este descris în Figura 4.5.

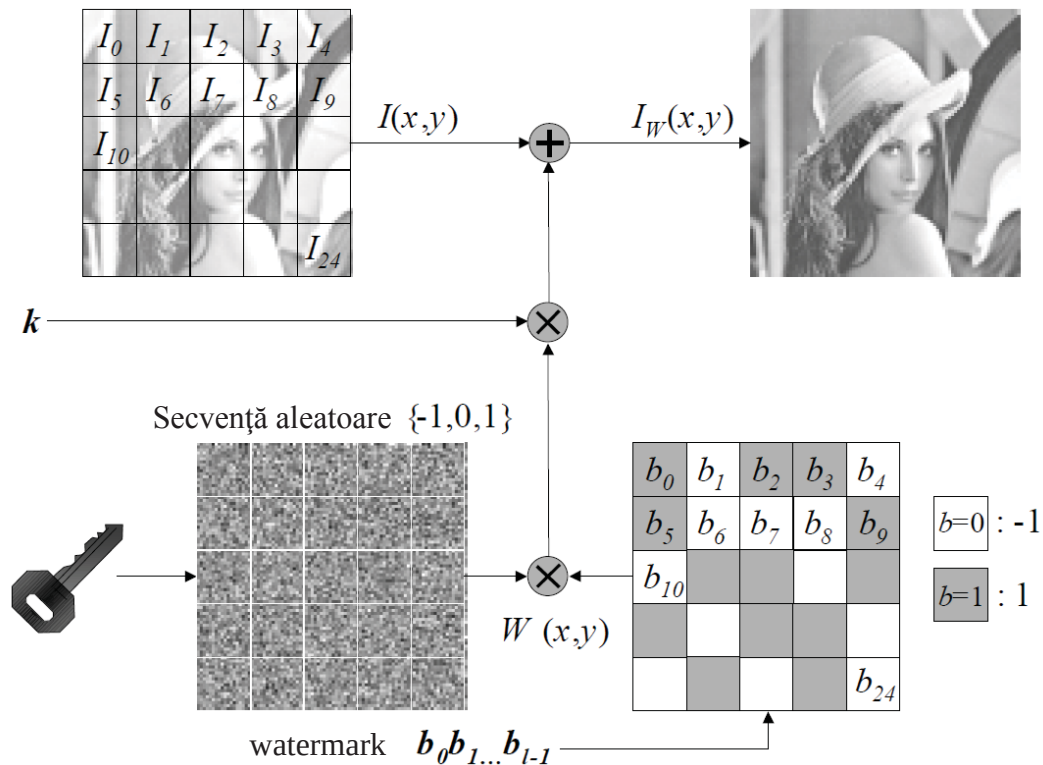


Figura 4.5. Procedura de inserare a watermark-ului

Folosind (4.9) se pot calcula numărul de pixeli P , necesari per subimagine, pentru detecția sigură a unui singur bit dintr-o subimagine:

$$P \approx \frac{\alpha \sigma_I^2 \ln 2}{\sigma_w^2} \text{ pixeli} \quad (4.10)$$

Biții watermark-ului pot fi reprezentați în mai multe moduri. Dacă bitul este 1, se adaugă o secvență pseudo-aleatoare, iar dacă este 0, subimaginea rămâne neatinsă. În acest caz, detectorul calculează corelația dintre subimagine și secvența pseudo-aleatoare și atribuie valoarea 1 bitului de watermark, când corelația depășește un anumit prag T , în caz contrar bitul de watermark se consideră zero. Folosirea unui prag poate fi evitată, prin adăugarea a două secvențe pseudo-aleatoare diferite, RP_0 și RP_1 , pentru biții de marcaj 0, respectiv 1. În acest caz, detectorul calculează corelația dintre subimagine și cele două secvențe. Bitului de watermark i se asignează valoarea asociată secvenței care generează corelația maximă. Cele două secvențe pseudo-aleatoare pot fi alese, astfel încât să difere doar prin semn, $RP_0 = -RP_1$ ca și în [90]. În acest caz, detectorul trebuie să calculeze doar o corelație dintre subimagine și una dintre secvențe, iar semnul corelației determină valoarea bitului de watermark.

Altă modalitate de a crește capacitatea watermark-ului este folosirea tehnicilor DS-CDMA (Direct Sequence-CDMA) [92, 93]. Pentru fiecare bit b_j al watermark-ului $b_0, b_1 \dots b_{l-1}$ este generată o secvență pseudo-aleatoare diferită, stohastic independentă, RP_j , de aceeași dimensiune ca și imaginea. Acest model este independent de valoarea bitului b_j . Se folosește modelul $+RP_j$ dacă b_j reprezintă un 0, și $-RP_j$ dacă b_j reprezintă un 1. Suma tuturor celor l secvențe aleatoare $\pm RP_j$ formează watermark-ul. Înainte de însumarea watermark-ului la imagine, acesta se poate scala cu un factor, sau se poate limita la un anumit domeniu. Un exemplu pentru generarea unui watermark unidimensional este prezentat în Figura 4.6. Sunt folosite șapte secvențe pseudo-aleatoare diferite, pentru inserarea celor șapte biți de watermark 0011010.

Fiecare bit b_j din șirul biților watermark-ului $b_0, b_1 \dots b_{l-1}$ poate fi extras prin calcularea corelației dintre imaginea normalizată I'_w și secvența pseudo-aleatoare corespunzătoare RP_j . Când corelația este pozitivă, este asignată bitului de watermark valoarea 0, altfel se presupune că bitul de watermark este 1. Figura 4.7 prezintă extragerea biților watermark-ului inserați conform Figurii 4.6.

128x32 pixeli într-o imagine de 512x512 pixeli folosind tehnicile descrise în acest capitol. Fiecare pixel al logo-ului este inserat într-un bloc de 8x8 pixeli al imaginii adăugând secvența pseudo-aleatoare +RP pentru un bit 0 sau -RP pentru un bit 1 la blocul imaginii. În Figura 4.8 sunt prezentate rezultatele extragerii watermark-ului după degradarea imaginii cu watermark prin compresie JPEG cu pierderi cu diferiți factori de calitate. Din figură se observă că logo-ul poate fi recunoscut, chiar dacă este distorsionat destul de puternic.

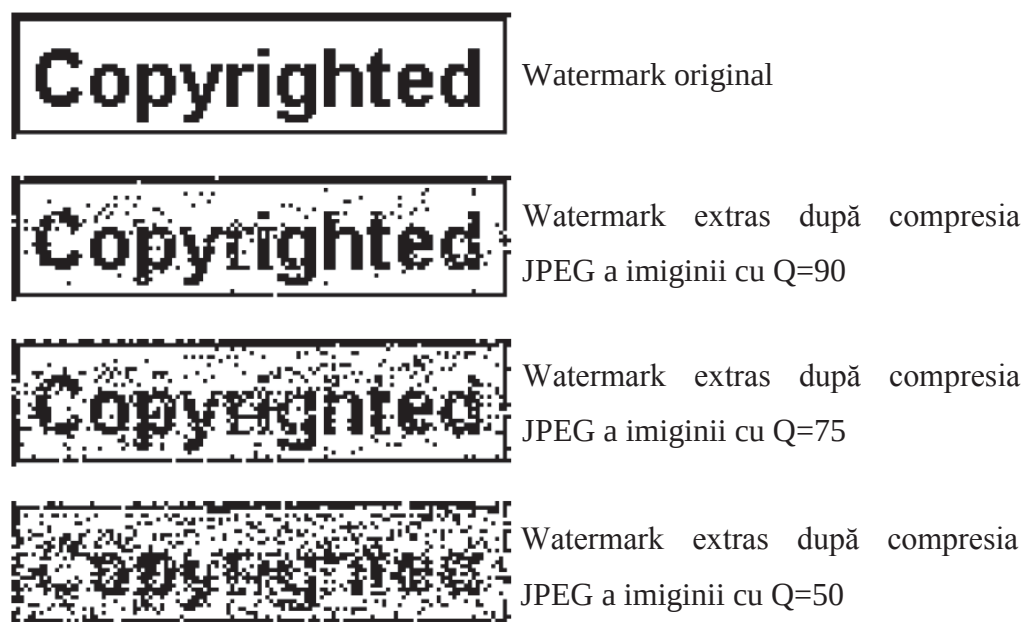


Figura 4.8. Logo-uri extrase după compresia imaginii cu diferiți factori de calitate JPEG.

D) Codare uni și bidirecțională

Tehnicile de watermarking în domeniul spațial nu sunt prea rezistente la compresie și atacuri geometrice (rotație, scalare). O metodă ce a reușit să reducă aceste dezavantaje este bazată pe modulația în amplitudine și a fost folosită în [6] pentru imagini color. Valorile pixelilor corespunzătoare canalului de albastru au fost modificate proporțional cu cele de cromaticitate astfel:

$$B_{i,j}^* = B_{i,j} + (2s-1)qL_{i,j} \quad (4.11)$$

unde B este valoarea originală a canalului de albastru, B^* este valoare modificată, L este luminanța, s este bitul ce trebui ascuns, iar q este câștigul. Câștigul este ajustat în funcție de cerințele de robustețe ale watermark-ului; o valoare mare produce un watermark vizibil iar valori mici produc un watermark cu robustețe mică. Acest algoritm s-a dovedit rezistent la

atacuri geometrice, procesare de semnal și compresie JPEG. Această tehnică a fost numită codare unidirecțională. Imaginea este împărțită în blocuri și este calculată valoarea medie a pixelilor din bloc. Fiecărui bloc îi este atribuită o valoare binară „0” sau „1”, ce formează un cod folosit pentru stocarea de informație. Dacă blocul reprezintă „1”, atunci media pixelilor din bloc este adăugată la fiecare pixel din bloc. Această metodă s-a dovedit a fi o metodă eficientă, dar a fost îmbunătățită mai departe pentru o mai mare robustețe.

Algoritmul dezvoltat din metoda anterioară, numit codare bidirecțională, era identic cu codarea unidirecțională, dar mai includea un pas în plus. În această etapă, dacă un bloc trebuia să reprezinte un „0”, valoarea medie era scăzută din fiecare pixel din bloc. Figura 4.9 (a) arată un exemplu de codare bidimensională folosind un watermark slab, deci invizibil, iar Figura 4.9 (b) arată o imagine căreia i se aplică același algoritm, dar cu un watermark mai puternic care crește robustețea, dar cu costul pierderii de calitate. Dezavantajul metodei este că, dacă cineva obține mai multe copii ale imaginii cu watermark-uri diferite, poate să elimine watermark-ul și, practic, să aibă la dispoziție imaginea originală.



a)



b)

Figura 4.9. Imagini obținute după aplicarea codării bidirecționale a) cu watermark slab, b) cu watermark puternic

E) Metode statistice

Comunitatea științifică și-a dat seama în scurt timp că watermarking-ul digital și modulația digitală, în special modulația cu spectru împrăștiat, împărtășesc concepte comune și s-a propus considerarea watermarking-ului ca o comunicație cu zgomot non-gaussian. Primele abordări teoretice au fost realizate de Smith în [98]. O analiză mai exactă a modulației în amplitudine multi-puls a fost făcută de Hernandez și al. [99].

După publicațiile mai sus menționate, interesul și activitatea de cercetare în domeniul watermarking-ului au crescut semnificativ. Producătorii și distribuitorii de materiale multimedia au fost interesați în mod deosebit de soluții funcționale. În continuare vom prezenta câteva lucrări mai recente.

Bender și al. Propun în [100] două metode pentru ascunderea de date în imagini. În prima metodă, numită „codarea perechilor”, sunt folosite perechi de pixeli (a_i, b_i) selectate aleator pentru a ascunde 1 bit de watermark prin creșterea valorii lui a_i cu o unitate și scăderea valorii lui b_i tot cu o unitate. Presupunând că imaginea satisface niște proprietăți statistice, atunci valoarea așteptată a sumei diferențelor dintre a_i și b_i pentru N perechi de pixeli este $2N$:

$$\sum_N a_i - b_i = \begin{cases} 2N, & \text{pentru perechi cu watermark} \\ 0, & \text{pentru perechi fără watermark} \end{cases} \quad (4.12)$$

A doua metodă, numită „codarea texturii blocurilor”, propune introducerea watermark-ului prin copierea texturii unui bloc din imagine într-o altă regiune a imaginii cu textură asemănătoare. Pentru recuperarea watermark-ului trebuie calculată funcția de autocorelație. O proprietate remarcabilă a acestei tehnici este robustețea ridicată la orice tip de distorsiune, dacă ambele regiuni cu textură sunt distorsionate în același mod, ceea ce înseamnă că recuperarea watermark-ului prin autocorelație funcționează.

Pitas și Kaskalis propun metoda „semnăturii” pentru imagini în [101-103] care este bazată pe algoritmul de codare a perechilor propus de Bender și al. în [104]. Watermark-ul $S = \{s_{m,n}\}$ este o matrice de numere binare de aceeași mărime ca și imaginea originală și în care numărul de „1” este egal cu numărul de „0”. Imaginea originală I , cu valorile de luminanță $x_{m,n}$ la pozițiile (m,n) este divizată în două seturi A și B de aceeași mărime în următorul mod:

$$\begin{aligned} A &= \{x_{m,n} \in I, s_{m,n} = 1\} \\ B &= \{x_{m,n} \in I, s_{m,n} = 0\} \end{aligned} \quad (4.13)$$

Watermark-ul este introdus prin modificarea elementelor subsetului A adăugând o constantă întreagă k . De exemplu, $A' = \{x_{m,n} + k, x_{m,n} \in A\}$. Imaginea cu watermark este dată de reuniunea mulțimilor A' și B . Pentru verificarea prezenței watermark-ului, este aplicat testul [105]. Statistica de test q este definită ca diferența normată dintre media $\bar{a}'$ a setului A' și media $\bar{b}$ a setului B .

$$q = \frac{\bar{b} - \bar{a}'}{\sigma_{A'}^2 + \sigma_B^2} \quad (4.14)$$

unde $\sigma_{A'}^2$ și σ_B^2 sunt varianțele setului A' , respectiv B . Parametrul q este comparat cu un prag pentru a determina dacă există un watermark sau nu. Metoda este imună la subeșantionare urmată de supraeșantionare și rezistă la compresie JPEG cu un factor de compresie 1:4.

O versiune îmbunătățită a acestei idei a fost propusă de Langelaar și al. în [106, 107]. Imaginea este împărțită în blocuri pătrate de dimensiune multiplu de 8. Un singur bit este introdus prin modificarea iterativă a unui bloc selectat pseudo-aleator. Fiecărui bloc selectat îi corespunde o secvență pseudo-aleatoare P , cu număr egal de „1” și „0”. Pentru a ascunde un bit de valoare „1”, secvența scalată $k \times P$ este adunată la bloc, unde k este un factor de scalare predefinit corespunzător nivelului de vizibilitate al watermark-ului. Fie I_0 media tuturor pixelilor din bloc pentru care valoarea corespunzătoare din secvența pseudo-aleatoare este zero și I_1 media pixelilor rămași. Fie $D_{sus} = I_1 - I_0$ diferența dintre cele două medii și $D_{jos} = \hat{I}_1 - \hat{I}_0$ diferența mediilor după compresia JPEG a blocului cu factorul de calitate Q predefinit. Dacă este ascuns un „0”, secvența P este scăzută în mod iterativ din bloc, până când ambele diferențe, D_{sus} și D_{jos} sunt mai mici decât zero sau a fost atins numărul maxim de iterații. Dacă se ascunde un „1”, secvența este însumată iterativ blocului până când D_{sus} și D_{jos} sunt mai mari decât un prag predefinit T sau a fost atins numărul maxim de iterații.

Un bit ascuns poate fi extras prin calcularea din nou a diferenței D_{sus} între cele două medii I_1 și I_0 . Semnul diferenței este apoi folosit pentru a determina valoarea bitului ascuns. Teste cu blocuri de dimensiune 32x32, prag $T=1$, factor de scalare inițial $k=4$ și număr maxim de iterații $n=6$, arată că metoda are o robustețe decentă la compresia JPEG: rată a erorii de bit de aproximativ 5% pentru o calitate JPEG de 85% și de 20% pentru o calitate de 60%.

Pentru a crește performanța metodelor de watermarking în domeniul spațial bazate pe blocuri, Bruyndonckx și al. sugerează în [108] folosirea clasificării pixelilor. Pixelii din blocuri selectate pseudo-aleator sunt clasificați în zone (1 și 2) de valoare omogenă a luminanței. Clasificarea este bazată pe 3 tipuri de contrast între zone: contrast puternic, contrast progresiv, și contrast zgomotos. Fiecare zonă este apoi împărțită în 2 categorii A și B bazate pe o grilă definită de codor. Astfel, fiecare pixel este încadrat într-una din combinațiile zonă/categorie, ca de exemplu 1/A, 1/B, 2/A și 2/B. Un bit b este ascuns prin modificarea zonei/categoriei astfel încât să fie satisfăcute următoarele constrângeri:

$$\begin{aligned}
\text{dacă } b = 0: \quad & m_{1B}^* - m_{1A}^* = k \\
& m_{2B}^* - m_{2A}^* = k \\
\text{dacă } b = 1: \quad & m_{1A}^* - m_{1B}^* = k \\
& m_{2A}^* - m_{2B}^* = k
\end{aligned} \tag{4.15}$$

unde m_{1A}^* , m_{1B}^* , m_{2A}^* și m_{2B}^* sunt valorile medii ale zonei/categoriei și k este puterea watermark-ului introdus. Modificarea valorii medii este realizată prin aplicarea de variații egale de luminanță pentru toți pixelii aparținând aceleași zone. Pentru a crește robustețea algoritmului autorii au sugerat introducerea de biți redundanți și folosirea de coduri corectoare de erori. A fost raportată o robustețe bună la compresia JPEG.

Pentru a crește performanțele metodelor de watermarking cu spectru împrăștiat în domeniul spațial, Kuter și al. [109] au propus o metodă care funcționează exclusiv pe componenta de albastru din spațiul de culori RGB, pentru a maximiza puterea watermark-ului și păstrând, în același timp, artefactele vizuale minime. Ei mai propun și o preprocesare a imaginii înainte de decodarea watermark-ului pentru a prezice watermark-ul ascuns. Acest concept îmbunătățește semnificativ robustețea și este aplicabil oricărei tehnici de watermarking în domeniul spațial. Metoda ascunde watermark-ul sub forma unui număr binar prin modulație în amplitudine în domeniul spațial. Un singur bit b este ascuns la o poziție pseudo-aleatoare (i,j) fie prin adunare, fie prin scădere, depinzând de valoarea bitului, a unei valori proporționale cu luminanța aceluși pixel:

$$B_{i,j} \leftarrow B_{i,j} + k(-1)^b L_{i,j} \tag{4.16}$$

unde $B_{i,j}$ este valoare de albastru a pixelului de la poziția (i,j) , $L_{i,j}$ este luminanța la aceeași poziție și k puterea watermark-ului. Pentru a recupera un bit ascuns este calculat un estimat al valorii originale, fără watermark folosind o combinație liniară a pixelilor învecinați în cruce:

$$\hat{B}_{i,j} = \frac{1}{4c} \left(\sum_{n=-c}^c B_{i+n,j} + \sum_{n=-c}^c B_{i,j+n} - 2B_{j,n} \right) \tag{4.17}$$

unde c definește mărimea vecinătății în formă de cruce. Valoarea bitului este determinată din semnul diferenței $\delta_{i,j}$ dintre pixelul inspectat și estimatul originalului. Pentru a crește robustețea, fiecare bit al semnăturii este ascuns de mai multe ori și, pentru extragerea bitului introdus, este folosit semnul sumei tuturor diferențelor $\delta_{i,j}$.

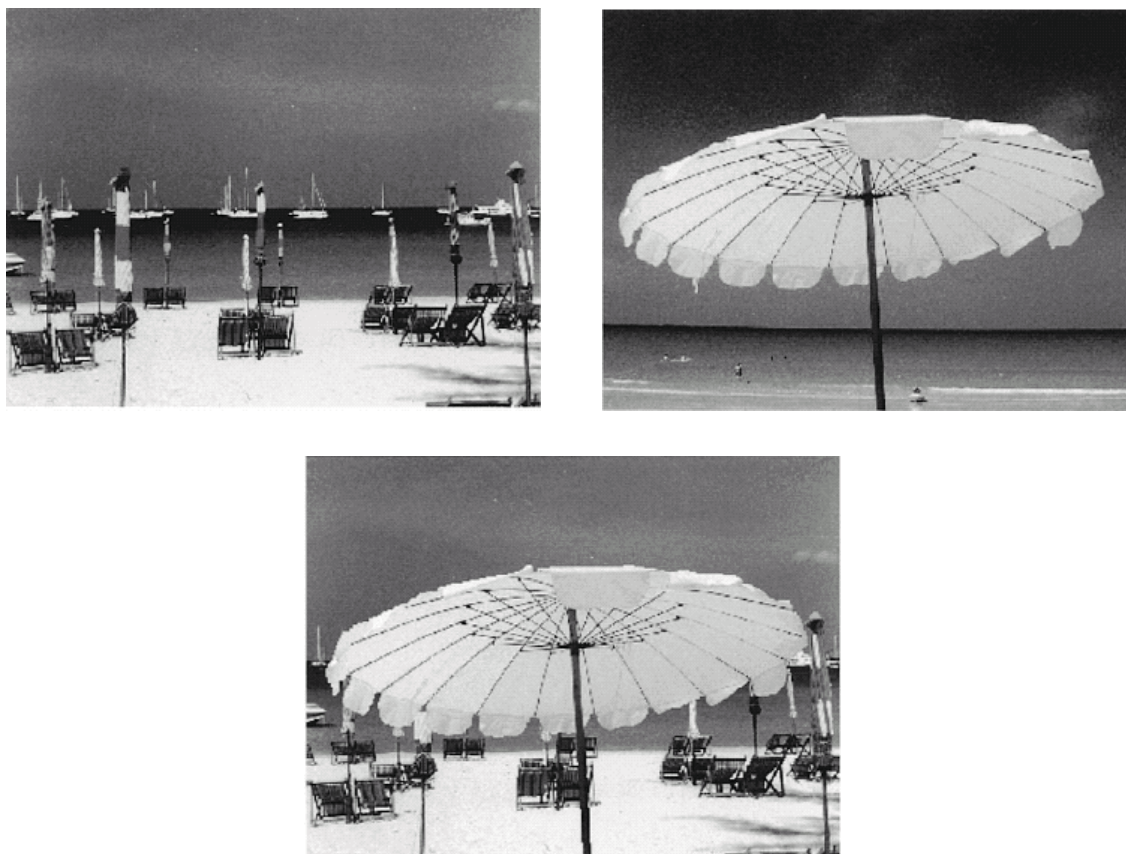


Figura 4.10. Compunerea imaginilor cu watermark. Umbrela din a doua imagine de sus este suprapusă peste plaja din prima imagine. Watermark-urile din ambele imagini pot fi recuperate din imaginea compusă.

Figura 4.10 ilustrează un exemplu de compunere a două imagini. Cele două imagini cu watermark de sus sunt folosite pentru a genera imaginea nouă, compusă de jos. Folosind cheile corespunzătoare, ambele watermark-uri originale pot fi recuperate. Extensii ale acestei metode permit creșterea robusteții și chiar recuperarea watermark-ului după atacuri geometrice și de tipul printare-scanare.

F) Metode bazate pe fractali

Tot legate de domeniul spațial sunt și metodele bazate pe compresia imaginilor folosind fractali. Ideea folosirii acestei tehnici a fost propusă prima dată în [110]. În compresia imaginilor folosind fractali, imaginea este codată utilizând principiile sistemelor de funcții iterative și similitudinea proprie [111]. Imaginea originală este divizată în blocuri pătrate R_k , numite blocuri distanță. Fie F un set de funcții de mapare f_k care sunt compuse dintr-o transformare geometrică g_k și o transformare de masă m_k . Funcțiile de mapare acționează

asupra blocurilor domeniu D_k care sunt mai mari ca dimensiune decât blocurile distanță. Transformarea geometrică constă în mișcarea blocului domeniu D_k pe poziția blocului distanță R_k și reducerea dimensiunii blocului domeniu la dimensiunea blocului distanță. Transformarea de masă ajustează intensitatea și poziția pixelilor blocului domeniu după transformarea geometrică. Transformările de masă includ rotația cu 90^0 , reflexia după axa orizontală sau diagonală. Pentru compresia unei imagini trebuie găsite pentru toate blocurile dimensiune cea mai bună combinație dintre bloc domeniu D_k și funcție de mapare f_k , astfel încât diferența dintre blocul distanță R_k și blocul domeniu mapat $f_k(D_k)$ să fie minimă. Acest lucru înseamnă că operațiunea de codare include o căutare spațială în toate blocurile domeniu posibile. Decodarea este realizată prin iterație folosind funcțiile de mapare codate. Pentru a ascunde un bit în această schemă, este selectat un bloc pseudo-aleator. Spațiul de căutare S_k corespunzător blocurilor distanță este apoi împărțit în două subspații de căutare S_k^1 și S_k^2 de aceeași mărime. Fiecărui subspațiu îi este atribuit un bit, iar blocul distanță curent este codat căutând doar în subspațiul corespunzător valorii bitului curent. Pentru recuperarea unui bit ascuns, imaginea este comprimată din nou, dar de data aceasta folosind spațiul complet de căutare. Atunci, pentru un bloc distanță marcat, blocul domeniu corespunzător denotă valoarea bitului inserat. Algoritmul a fost testat folosind compresia JPEG și a oferit rezultate bune până la un factor de calitate de 50%. Un dezavantaj al acestei scheme este viteza scăzută datorată schemei de codare cu fractali.

O abordare similară a fost propusă de Davern și Scott în [112]. Singura diferență față de metoda anterioară este faptul că nu se codează imaginea totală, ci doar o regiune distanță definită de utilizator bazată pe o regiune domeniu. Fiind date cele două regiuni, inserarea watermark-ului este echivalentă cu sistemul propus de Puarte și Jordan în care regiunea domeniu este divizată în două părți și, depinzând de valoarea bitului, una dintre subregiuni este folosită pentru a coda un bloc distanță. Această idee de watermarking în domeniul spațial, folosind codarea imaginilor cu fractali, a fost extinsă în [113] de către Bas și al. la Transformata Cosinus Discretă.

4.2.2. Watermarking în domeniul transformat

Tehnicile ce folosesc domeniul transformatelor sunt de obicei mai complexe decât metodele în domeniul spațial, necesită astfel un efort de calcul mai mare, dar oferă un grad mai ridicat de robustețe la operații uzuale de prelucrări de imagini sau video. În continuare vor fi prezentate câteva metode clasificate în funcție de transformata folosită.

A) Tehnici de watermarking în domeniul Transformatei Cosinus Discrete

Un domeniu de lucru des întâlnit în aplicațiile de watermarking este domeniul Transformatei Cosinus Discrete. Folosind DCT, o imagine poate fi ușor împărțită în benzi de pseudo-frecvență, astfel încât watermark-ul poate fi inserat în mod convenabil în cele mai importante benzi de frecvență centrală. Mai mult, a fost studiată sensibilitatea sistemului vizual uman, ceea ce a produs tabelul de cuantizare JPEG standard [114]. Aceste rezultate pot fi folosite pentru prezicerea și minimizarea impactului vizual al distorsiunilor cauzate de watermark. DCT bazată pe blocuri este folosită la scară largă pentru compresia de imagini și video. Prin inserarea unui watermark în același domeniu se poate anticipa compresia cu pierderi și exploata descompunerea DCT pentru a dezvolta aplicații de watermarking în timp real.

În Figura 4.11 (a) este dat un exemplu de imagine în care a fost inserat un watermark format dintr-un semnal 2-D pseudo-aleator în blocurile DCT de dimensiune 8 x 8 de frecvență medie. Coeficienții DCT sunt modulați conform relației (4.18):

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + k \cdot W_{x,y}(u,v) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \quad x,y = 1,8,16,\dots \quad (4.18)$$

În relația (4.18), F_M sunt benzile de frecvență medie, k este factorul de câștig, (x,y) locația spațială a unui bloc de 8x8 pixeli în imaginea I și (u,v) frecvențele coeficientului DCT din blocul DCT corespunzător (vezi Figura 4.12).

În Figura 4.11 (c) este prezentată diferența puternic amplificată dintre imaginea originală și imaginea cu watermark. Figura 4.11 (d) arată spectrul Fourier al watermark-ului. Se poate vedea clar că watermark-ul afectează doar benzile de frecvență medie.

Dacă este aplicată funcția de modulație din relația (4.19) rezultatele din Figura 4.11 se transformă în cele din Figura 4.13. Din Figura 4.13 (b) și (c) se vede că cele mai mari distorsiuni introduse de watermark sunt localizate la contururi și în zonele cu textură.

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) \cdot (1 + k \cdot W_{x,y}(u,v)) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \quad x,y = 1,8,16,\dots \quad (4.19)$$

Prima metodă eficientă de watermarking în domeniul DCT a fost introdusă de către Koch și al. în [115-117]. Ca și în schema de compresie JPEG, imaginea este, în primul rând, divizată în blocuri pătrate de dimensiune 8x8 pixeli.

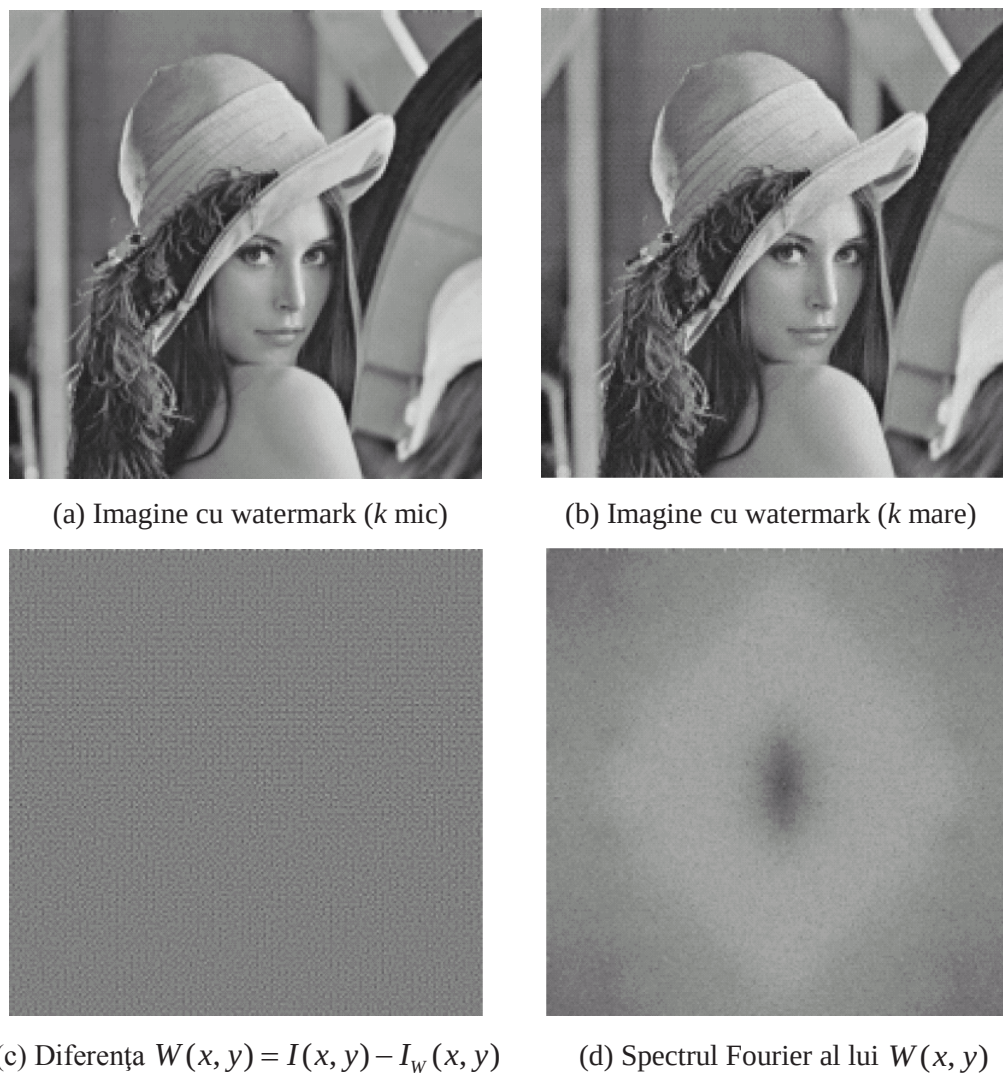


Figura 4.11. Watermark independent de conținutul imaginii inserat în benzile DCT de frecvență medie

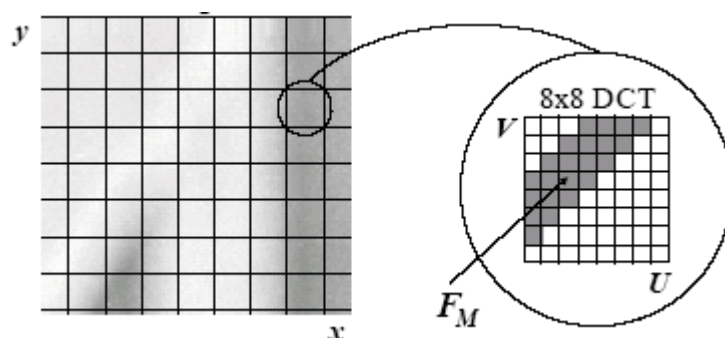


Figura 4.12. Definirea benzilor de frecvență medie într-un bloc DCT

Pentru fiecare dintre aceste blocuri este calculată Transformata Cosinus Discretă. Pentru un bloc selectat pseudo-aleator este aleasă o pereche de coeficienți de frecvență medie din 12 perechi determinate. Pentru a insera un bit de watermark coeficienții sunt modificați astfel încât diferența dintre ei să fie pozitivă, fie negativă, depinzând de valoarea bitului de inserat. Pentru ca algoritmul să fie robust la compresia JPEG cu pierderi, matricea de cuantizare JPEG este folosită la modificarea coeficienților DCT. Această metodă dovedește o robustețe bună la compresia JPEG până la un factor de calitate $Q=50$.

Bors și Pitas [118, 119] sugerează o metodă de modificare a coeficienților DCT conform unei constrângeri asupra selecției poziției blocurilor. Imaginea este întâi divizată în blocuri de 8×8 pixeli. Anumite blocuri sunt selectate conform unei decizii pe baza unui clasificator de rețea Gaussian. Coeficienții de frecvență medie sunt apoi modificați folosind fie o constrângere liniară, fie o constrângere de regiune circulară, pentru a insera informația watermark. În prima dintre abordări, constrângerea liniară este definită astfel:

$$Y = FQ \quad (4.20)$$

unde F este vectorul modificat de coeficienți DCT și Q este vectorul de ponderare dependent de watermark. Constrângerea este impusă modificând coeficienții DCT după criteriul celor mai mici pătrate. Al doilea algoritm propus definește regiuni circulare în jurul coeficienților DCT selectați. Coeficienții sunt apoi cuantizați astfel:

$$\|F - Q_k\|^2 = \min_{i=1}^H \|F - Q_i\|^2 \quad \text{atunci} \quad F = Q_k \quad (4.21)$$

unde $Q_i, i=1, \dots, H$ este setul de vectori de coeficienți dat de watermark. În procesul de recuperare a watermark-ului algoritmul verifică constrângerea asupra coeficienților DCT pentru fiecare bloc, iar apoi constrângerea asupra locației blocului. Algoritmul este robust la compresia JPEG cu un factor de compresie de 13:1 folosind constrângerea liniară și de 18:1 folosind constrângerea circulară.

Swanson și al. sugerează în [119, 120] o tehnică de watermarking bazată pe mascarea în frecvență a coeficienților DCT, metodă ce este similară cu cea propusă de Smith și Comiskey [98]. Imaginea de intrare este împărțită în blocuri și este calculată DCT. Pentru fiecare bloc de coeficienți DCT este calculată o mască de frecvență având la bază faptul că o grilă de mascare crește pragul vizual pentru componentele semnalului din jurul măștii de frecvență. Masca perceptuală rezultantă este scalată și multiplicată cu coeficientul DCT al secvenței de zgomot pseudo-aleator de lungime maximă. Acest watermark este adăugat la

blocul DCT corespunzător iar apoi se verifică prin mascare spațială dacă watermark-ul este vizibil și se controlează factorul de scalare.

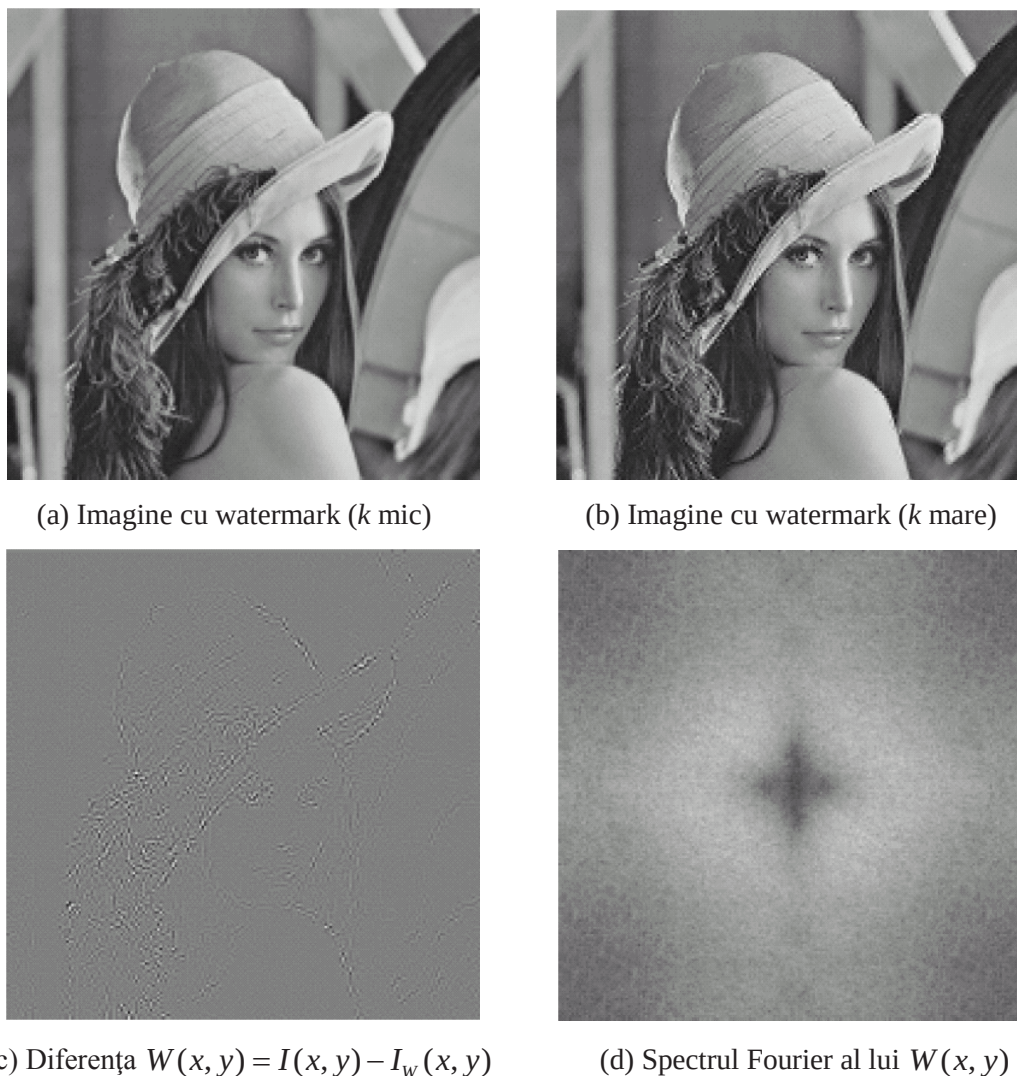


Figura 4.13. Watermark dependent de conținutul imaginii în benzile DCT de frecvență medie

Detecția watermark-ului necesită imaginea originală și watermark-ul original și este realizată prin testarea posibilităților. Autorii raportează o bună robustețe a watermark-ului la compresie JPEG, zgomot colorat și decupare a imaginii.

Tao și Dickinson [122] introduc o tehnică de watermarking adaptivă în domeniul DCT bazată pe clasificatori percepțuali de regiuni cu indice de sensibilitate asignat. Watermark-ul este inserat în N coeficienți DCT AC (de frecvență diferită de 0). Coeficienții sunt selectați astfel încât să aibă cei mai mici pași de cuantizare conform tabelului de cuantizare JPEG. Coeficienți x_i selectați sunt modificați după cum urmează:

$$\hat{x}_i = x_i + \max \left[x_i \alpha_m, \text{sign}(x_i) \frac{D_i}{k} \right] \quad (4.22)$$

unde α_m este indicele de sensibilitate la zgomot al blocului curent, D_i pasul de cuantizare pentru X_i și k satisface relația $5 \leq k \leq 6$. Trebuie observat că semnalul watermark nu este generat aleator. Există diferite abordări pentru a determina sensibilitatea la zgomot prin exploatarea eficientă a efectului de mascare al sistemului vizual uman. Autorii propun un algoritm de clasificare pe regiuni care încadrează blocul într-una din șase clase perceptuale. Algoritmul de clasificare exploatează efectele SVU de mascare a luminanței, mascare a marginilor și mascare a texturilor. Clasele perceptuale sunt definite în ordinea descrescătoare a sensibilității la zgomot astfel: la margini, uniform, de sensibilitate scăzută, texturat mediu, texturat, foarte texturat. Fiecare clasă perceptuală are asignat un indice de sensibilitate la zgomot. Recuperarea watermark-ului necesită imaginea și watermark-ul original și este bazată pe testarea posibilităților. Experimentele arată că metoda rezistă la compresia JPEG până la un factor de calitate de 5% și la zgomot aleator cu un $PSNR = 22.1dB$.

Podilchuk introduce în [123, 124] watermarking-ul perceptual folosind diferența abia observabilă (JND) pentru a determina o mască de modulație a watermark-ului dependentă de imagine. Modulația coeficienților selectați fie în domeniul DCT, fie în domeniu Wavelet poate fi descrisă astfel:

$$I_{u,v}^* = \begin{cases} I_{u,v} + JND_{u,v} \times w_{u,v}, & \text{daca } I_{u,v} > JND_{u,v} \\ I_{u,v}, & \text{in rest} \end{cases} \quad (4.23)$$

unde $I_{u,v}$ sunt coeficienții transformatei, $w_{u,v}$ sunt valorile watermark-ului și $JND_{u,v}$ este diferența abia observabilă calculată pe baza modelelor vizuale. Pentru coeficienții DCT, autorul sugerează un model perceptual definit de Watson și bazat pe folosirea sensibilității în frecvență și la luminozitate, dar și mascarea locală a contrastului. Acest model oferă pentru fiecare bloc DCT 8x8 praguri de mascare dependente de imagine. Detecția watermark-ului este bazată pe corelația dintre diferența dintre imaginea originală și imaginea inspectată și secvența de watermark. Corelația maximă este comparată cu un prag pentru a determina dacă o imagine conține watermark-ul căutat. Experimentele au arătat că schema este extrem de robustă la compresia JPEG, decupare, scalare, zgomot aditiv, corecție de gama, și scanare-xeroxare-scanare.

Piva și al. descriu în [125] altă metodă bazată pe DCT ce exploatează caracteristicile de mascare a SVU. Watermark-ul este format dintr-o secvență pseudo-aleatoare de M numere reale cu distribuție normală $\mathbf{X} = \{x_1, x_2, \dots, x_M\}$. Coeficienții unui bloc DCT de dimensiune $N \times N$ sunt rearanjați într-un vector folosind scanarea în zig-zag. Din acest vector sunt selectați M coeficienți, începând de la poziția $L+1$ ce generează vectorul $\mathbf{T} = \{t_1, t_2, \dots, t_M\}$. Watermark-ul $\mathbf{X}$ este inserat în $\mathbf{T}$ astfel:

$$t'_i = t_i + k |t_i| x_i \quad (4.24)$$

unde k este puterea watermark-ului. Coeficienții modificați înlocuiesc coeficienții nemodificați înainte ca imaginea cu watermark să fie reconstruită. Pentru a crește robustețea este aplicată mascarea vizuală după cum urmează:

$$y''_{ij} = y_{ij}(1 - \beta_{ij}) + \beta_{ij} y'_{ij} = y_{ij} + \beta_{ij}(y'_{ij} - y_{ij}) \quad (4.25)$$

unde β_{ij} este factorul de ponderare având în vedere caracteristicile SVU. Un mod simplu de a alege β_{ij} este varianța normală a eșantionului la pixelul y_{ij} definită ca raportul dintre varianța eșantionului dintr-un bloc pătrat cu centrul în y_{ij} și maximul dintre varianțele tuturor blocurilor. Ca și în majoritatea tehnicilor, detecția watermark-ului este realizată prin compararea corelației z dintre watermark și coeficienții DCT cu semn posibil corupți $\mathbf{T}^*$. Corelația z este definită conform relației (4.26).

$$z = \frac{\mathbf{X} \cdot \mathbf{T}^*}{M} = \frac{1}{M} \sum_{i=1}^M x_i t_i^* \quad (4.26)$$

Pragul S_z este adaptiv și dat de expresia:

$$S_z = \frac{k}{3M} \sum_{i=1}^M |t_i^*| \quad (4.27)$$

Rezultatele experimentale au arătat că watermark-ul este robust la diferite tehnici de procesare a imaginilor (de exemplu, compresia JPEG, filtrarea mediană și watermarking multiplu) și la distorsiuni geometrice (după aplicarea transformării geometrice inverse).

B) Tehnici de watermarking în domeniul Transformatei Fourier Discrete

Watermarking-ul în domeniul Transformatei Fourier Discrete a fost introdus prima oară de Boland și al. în [126] și Cox și al. în [127] care au dezvoltat independent metode perceptuale adaptive bazate pe modulație. Cox și al. au tras paralele între tehnologia lor și comunicațiile cu spectru împrăștiat, deoarece watermark-ul este împrăștiat printre componente de frecvență importante din punct de vedere vizual (vezi Figura 4.14).

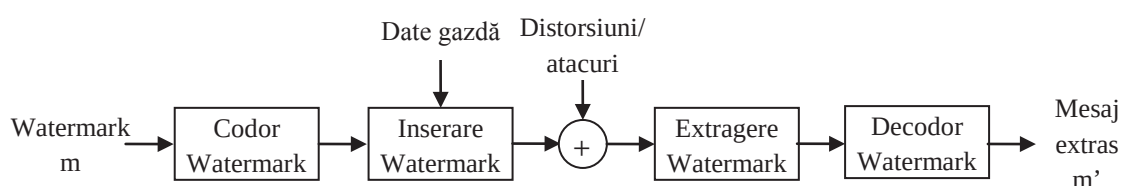


Figura 4.14. Watermarking ca sistem de comunicație

Watermark-ul conține o secvență de numere $x = x_1, \dots, x_n$ cu o distribuție statistică dată, ca de exemplu distribuția normală $N(0,1)$ cu medie zero și varianță 1. Watermark-ul este inserat în imaginea V și produce imaginea cu watermark V' . Sunt propuse trei tehnici pentru inserarea watermark-ului:

$$\begin{aligned}
 v'_i &= v_i + kx_i \\
 v'_i &= v_i(1 + kx_i) \\
 v'_i &= v_i e^{kx_i}
 \end{aligned} \tag{4.28}$$

unde k dă puterea watermark-ului și v_i sunt componente spectrale importante din punct de vedere perceptual. Prima relație este potrivită doar dacă valorile v_i nu variază prea mult.

Următoarele două relații dau rezultate similare pentru valori mici pentru kx_i și, pentru v_i pozitive, ultima relație poate fi văzută ca o aplicație a primei, dacă sunt folosiți logaritmi valorilor originale. Schema poate fi generalizată prin introducerea mai multor parametri de scalare k_i pentru a se adapta la diferitele componente spectrale și, astfel, să reducă artefactele vizuale.

În Figura 4.15 (b) este dat un exemplu de imagine în care este inserat un watermark folosind amplitudinea tuturor coeficienților DFT conform relației (4.28), forma a doua, cu o valoare relativ mică pentru factorul de câștig k . Figura 4.15 (c) arată diferența puternic

amplificată dintre imaginea originală și imaginea cu watermark. Figura 4.15 (d) arată o imagine în care watermark-ul a fost inserat folosind o valoare mare pentru factorul de câștig k .

Pentru verificarea prezenței watermark-ului, trebuie măsurată similitudinea dintre watermark-ul recuperat X^* , dat de diferența dintre imaginea originală V și imaginea posibil modificată V^* , și watermark-ul original X . Măsurarea similitudinii se face printr-un coeficient de corelație normat

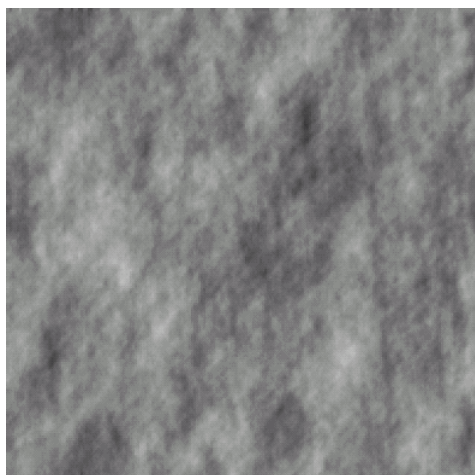
$$\text{sim}(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X}} \quad (4.29)$$



(a) Imaginea originală



(b) Imagine cu watermark (k mic)



(c) Diferența scalată pentru vizibilitate



(d) Imagine cu watermark (k mare)

Figura 4.15. Watermark ascuns în amplitudinea DFT

Testele de robustețe au arătat că metoda rezistă la compresia JPEG (cu factor de calitate de 50), dither, transmisie prin fax, printare-fotocopiere-scanare, watermarking multiplu și atacuri prin complotare (între mai mulți deținători de copii cu watermark). Pentru experimente, watermark-ul a fost de lungime 1000 cu $N(0,1)$, unde $N(\mu, \sigma)$ reprezintă o distribuție normală cu medie μ și varianță σ , k a fost setat la 0.1, iar watermark-ul a fost inserat în primii 1000 cei mai importanți coeficienți DCT folosind a doua tehnică de inserare.

Boland și al. au propus o tehnică similară bazată pe un hibrid între modulația în amplitudine și FSK (Frequency Shift Keying), și sugerează folosirea diferitelor domenii transformate ca DCT, DWT, Walsh-Hadamard și Transformata Fourier Rapidă (FFT – Fast Fourier Transform).

Ruanaidh și al. propun în [122, 128] o metodă de watermarking prin modificarea fazei în domeniul frecvență. Pentru a insera un bit este modificată faza coeficientului selectat $F(k_1, k_2)$ al Transformatei Fourier Discrete de dimensiune $N_1 \times N_2$ prin adăugarea unui factor mic δ :

$$\angle F(k_1, k_2) \leftarrow \angle F(k_1, k_2) + \delta \quad (4.30)$$

Pentru ca imaginea cu watermark să fie reală, faza trebuie să satisfacă condiția de simetrie negativă, ceea ce conduce la modificarea adițională:

$$\angle F(N_1 - k_1, N_2 - k_2) \leftarrow \angle F(N_1 - k_1, N_2 - k_2) + \delta \quad (4.31)$$

Coeficienții sunt modificați doar dacă puterea lor relativă este peste un anumit prag. Dacă imaginea originală este disponibilă, watermark-ul poate fi ușor extras prin compararea fazei. În cazul în care originalul nu este disponibil, Ruanaidh sugerează precuantizarea fazei originale înaintea modificării ei. Astfel, deviațiile între stările cuantizate pot fi folosite pentru transmiterea datelor.

În altă publicație [129], Ruanaidh și al. creează o tehnică de watermarking în special concepută pentru ca watermark-ul să fie invariant la translații, rotații și scalări. Metoda este un hibrid între DFT și mapare log-polară. Procesul este reprezentat în Figura 4.16. Într-un prim pas este calculată DFT a imaginii. Una dintre proprietățile DFT este că o deplasare în domeniul spațial rezultă într-o deplasare de fază în domeniul frecvență. Păstrând doar amplitudinea pentru procesări ulterioare face imaginea invariantă la translație. În cel de-al doilea pas, invarianța la rotație și scalare este realizată prin maparea amplitudinii din sistemul

cartezian în sistemul log-polar. Să considerăm un punct $(x, y) \in \mathbb{R}$. Atunci maparea este definită astfel:

$$\begin{aligned} x &= e^{\mu} \cos \theta \\ y &= e^{\mu} \sin \theta \end{aligned} \quad (4.32)$$

unde $\mu \in \mathbb{R}$ și $0 < \theta < 2\pi$. Se poate vedea ușor că aceasta este o mapare bijectivă și că rotația și scalarea în sistemul cartezian sunt transformate într-o translație a coordonatelor μ și θ . Calculând din nou DFT a mapării log-polare și păstrând doar amplitudinea rezultă într-o invarianță la rotație și translație. Calculând Transformata Fourier a unei hărți log-polare este echivalent cu calcularea Transformatei Fourier-Mellin. Combinând cei doi pași, se obține o transformată invariantă la rotație, scalare și translație (RST). Watermark-ul are forma unui semnal bi-dimensional cu spectru împrăștiat în domeniul transformatei invariante RST.

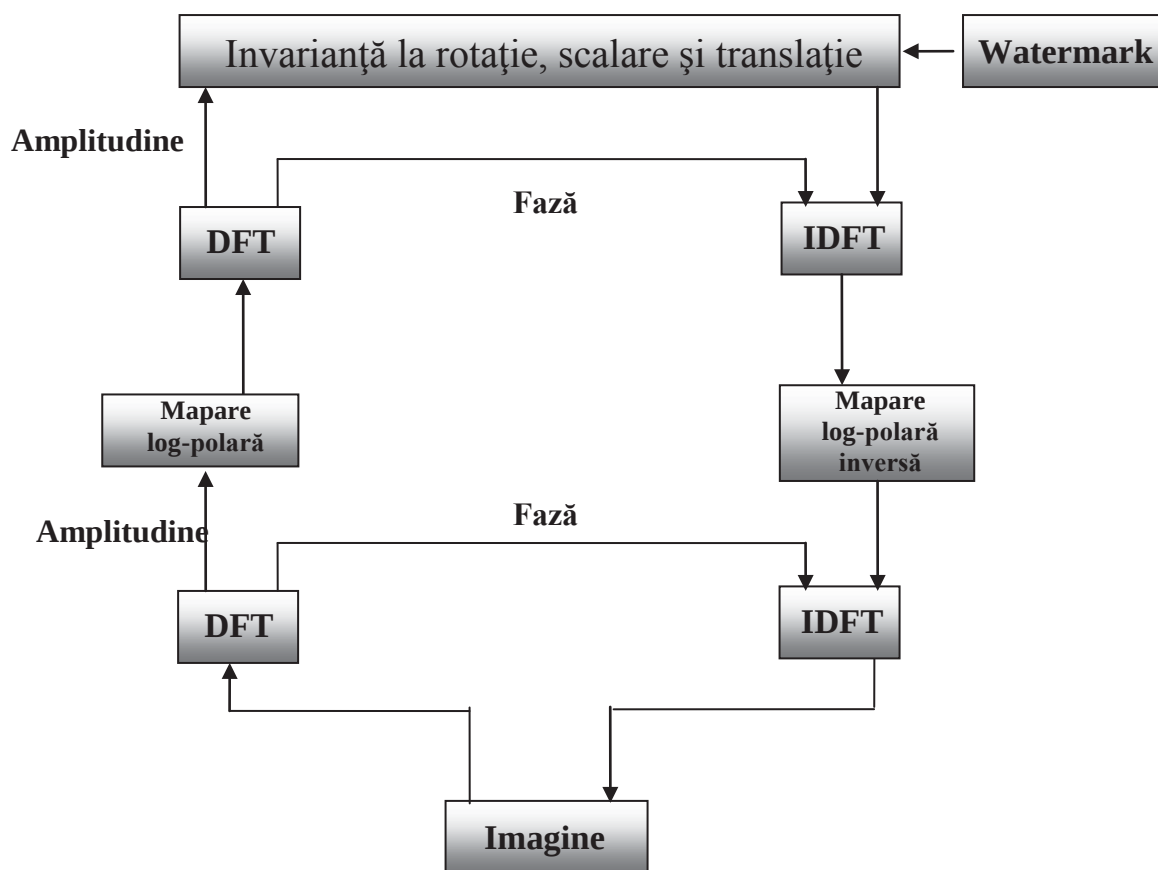


Figura 4.16. Metodă invariantă la rotații, translații și scalări

Figura 4.17 arată un exemplu al proprietăților sistemului log-polar. Figura 4.17 (b) prezintă harta log-polară a imaginii „Lena” (a). Figura 4.17 (c) reprezintă o versiune rotită și scalată a imaginii și Figura 4.17 (d) reprezintă harta log-polară (HLP) a imaginii (c). Se poate vedea clar că rotația și scalarea pot fi convertite în translație.

Într-un test, un watermark de 104 biți a fost inserat într-o imagine. Imaginea cu watermark a fost apoi rotată cu 143° și scalată cu 75% pe fiecare axă. Watermark-ul inserat a fost recuperat din această imagine. Mai mult, metoda rezistă compresiei JPEG până la un factor de calitate de 75%. Această metodă care a fost prima dezvoltată special pentru a rezista la atacuri geometrice, conține aspecte și idei interesante și ar putea fi concepută o direcție nouă de abordare a tehnicilor de watermarking. O variație a acestei idei, bazată pe Transformata Radon, a fost propusă de Wu și al. în [125].

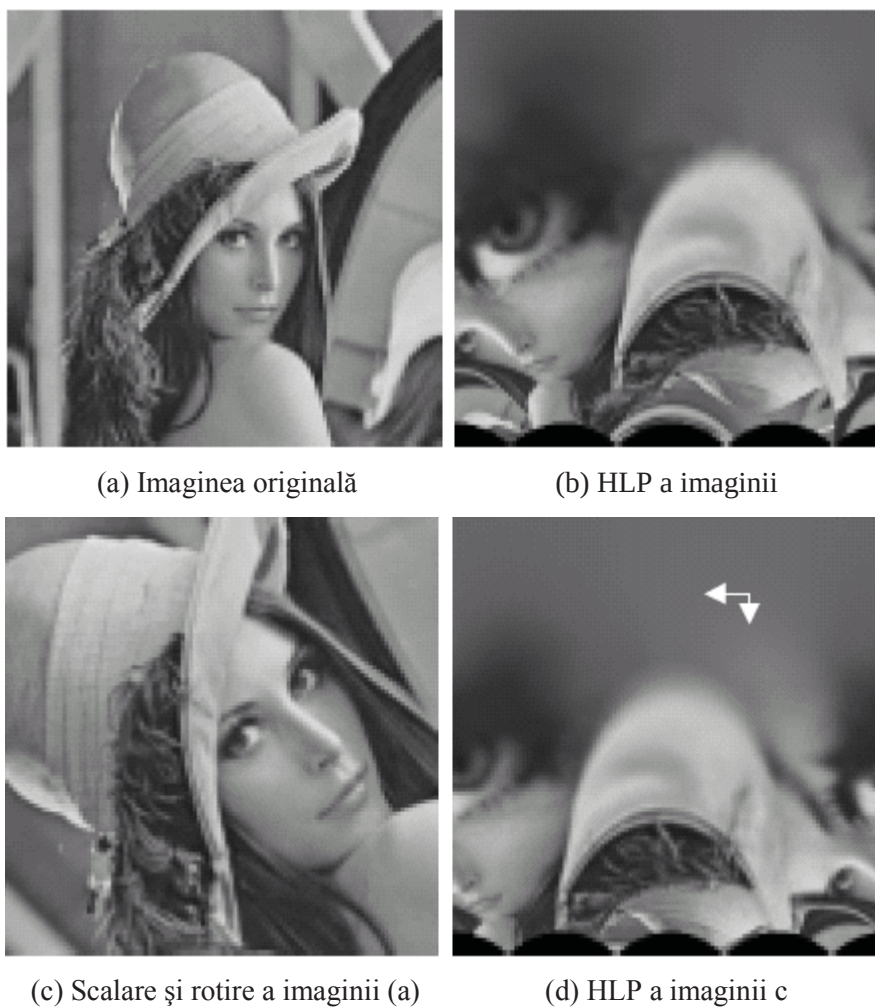


Figura 4.17. Exemplu al proprietăților hărții log-polare

C) Tehnici de watermarking în domeniul Wavelet

Deoarece tehnicile de watermarking pot exploata caracteristicile sistemului vizual uman, este posibilă ascunderea de watermark-uri cu mai multă energie în imagine, ceea ce le face mai robuste. Din acest punct de vedere, Transformata Wavelet Discretă este o unealtă foarte atractivă, pentru că poate fi folosită ca o modalitate de calcul eficientă a modelelor în frecvență a SVU [130]. De exemplu, se pare că ochiul uman este mai puțin sensibil la zgomotul din benzile DWT de rezoluție înaltă și în benzile DWT ce au o orientare de 45° (benzile HH). Mai mult, codarea de imagini și video pe baza DWT, ca de exemplu codarea EWZ (Embedded Zerotree Wavelet), sunt încadrate în standarde de compresie de ultimă generație, cum ar fi JPEG2000. Prin inserarea unui watermark în acest domeniu, putem anticipa compresia cu pierderi bazată pe DWT și exploata descompunerea DWT pentru a dezvolta aplicații de watermarking în timp real. Multe abordări aplică această tehnică în benzile DWT de rezoluție înaltă LH_1 , HH_1 , și HL_1 [130-134] (vezi Figura 4.18).

În Figura 4.19 (a) este dat un exemplu de imagine în care o secvență pseudo-aleatoare 2-D este inserată în benzile DWT LH_1 , HH_1 , și HL_1 folosind un factor de câștig k mare. Coeficienții DWT din fiecare din cele 3 benzi DWT sunt modulați după cum urmează:

$$I_w(u, v) = I(u, v) + k \cdot W(u, v) \quad (4.33)$$

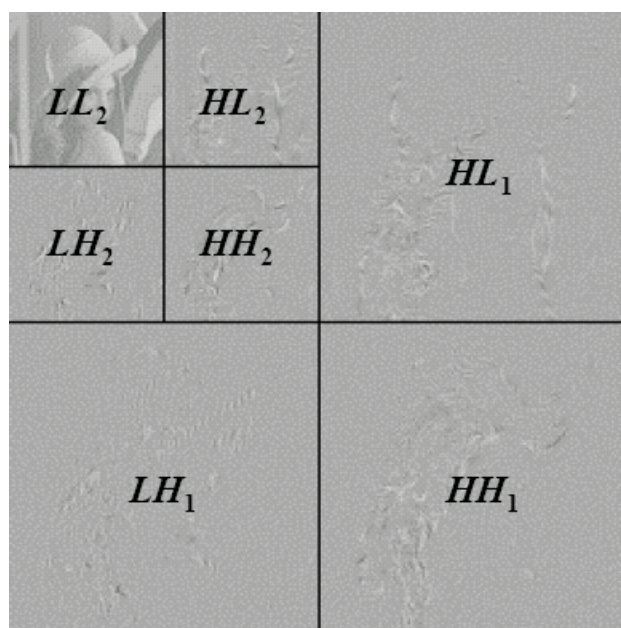


Figura 4.18. Descompunere DWT a unei imagini pe 2 nivele



(a) Imagine cu watermark (k mare) (b) Diferența $W(x, y) = I(x, y) - I_w(x, y)$

Figura 4.19. Watermark inserat în domeniul DWT independent de conținutul imaginii

Figura 4.19 (b) arată diferența puternic amplificată dintre imaginea originală și imaginea cu watermark. Watermark-ul poate fi făcut dependent de imaginea gazdă prin modulația coeficienților DWT din toate cele 3 subbenzi după cum urmează:

$$I_w(u, v) = I(u, v)(1 + k \cdot W(u, v)) \quad (4.34)$$

În Figura 4.20 (a) este dat un exemplu de imagine în care o secvența pseudo-aleatoare 2-D este inserată în benzile DWT LH_1 , HH_1 , și HL_1 folosind relația (4.34) și un factor de câștig k mare. Figura 4.20 (b) arată diferența puternic amplificată dintre imaginea originală și imaginea cu watermark.



(a) Imagine cu watermark (k mare) (b) Diferența $W(x, y) = I(x, y) - I_w(x, y)$

Figura 4.20. Watermark inserat în domeniul DWT dependent de conținutul imaginii

Inserarea watermark-ului folosind o descompunere multi-rezoluție a fost pentru prima oară propusă de Boland și al. în [126]. Ca și în schemele ce funcționează în alte domenii transformate, watermark-ul este o secvență 2-D pseudo-aleatoare. Atât imaginea, cât și watermark-ul sunt descompuse folosind Transformata Wavelet 2-D, iar în fiecare subbandă a imaginii este inserată o versiune ponderată a watermark-ului. Decodarea watermark-ului este, ca de obicei, bazată pe corelația normată dintre un estimat al watermark-ului inserat și watermark-ul original. În [135-138] au fost propuse diferite scheme bazate pe Wavelet. Diferența între diferitele metode constă, de obicei, în modul în care watermark-ul este ponderat pentru a elimina artefactele vizuale.

4.3. Codarea watermark-ului

4.3.1. Metode de watermarking cu spectru împrăștiat

Deoarece se dorește ca watermark-ul să aibă putere redusă (pentru a fi imperceptibil), procesul de watermarking poate fi privit ca un proces de comunicație printr-un canal foarte zgomotos. Tehnicile cu spectru împrăștiat sunt cunoscute pentru avantajul lor de a facilita comunicațiile în medii zgomotoase și din acest motiv sunt foarte mult folosite în watermarking. Foarte multe tehnici de watermarking reprezintă watermark-ul sub forma unei secvențe de zgomot pseudo-aleator. Starea generatorului de numere aleatoare folosit pentru generarea secvenței devine cheia watermark-ului. Deoarece decodorul trebuie să cunoască cheia pentru a decoda watermark-ul, aceste scheme sunt de regulă private. Hartung și alții propun în [139] ca o parte a secvenței să fie făcută publică pentru a permite decodarea publică a watermark-ului. De asemenea, detectorul/decodorul trebuie să se sincronizeze cu secvența pseudo-aleatoare înainte ca watermark-ul să poată fi detectat/decodat. Din păcate, acest lucru devine marele dezavantaj al multor scheme existente. O variație a principiului de baza cu spectru împrăștiat este filtrarea trece bandă/trece jos a secvenței înainte de inserarea watermark-ului [140], astfel încât watermark-ul să aibă cât mai puțină energie de înaltă frecvență care este, de regulă, eliminată de sistemele de compresie.

Metodele de watermarking cu spectru împrăștiat au fost prezentate în detaliu în subcapitolul 2.2.1 dedicat metodelor de watermarking în domeniul spațial.

4.3.2. Metode de watermarking bazate pe cuantizare

O metodă bazată pe cuantizare a fost propusă de Chen și Wornell [141]. Această metodă este denumită Modulație a Indicelui de Cuantizare (QIM) și este bazată pe un set N -dimensional de cuantizori. Cuantizorii satisfac o constrângere de distorsiune și sunt creați astfel încât valorile reconstruite folosind un cuantizor să fie „foarte departe” de punctele de reconstrucție a oricărui alt cuantizor. Mesajul de transmis este folosit ca indice pentru selectarea cuantizorului. Cuantizorul selectat este apoi folosit pentru ascunderea informației prin cuantizarea datelor imaginii în domeniul spațial sau în domeniul DCT. În procesul de codare este calculat un parametru distanță pentru toți cuantizorii și indicele cuantizorului cu cea mai mică distanță identifică informația ascunsă. Autorii arată că performanța schemei rezultate este superioară modulației cu spectru împrăștiat standard.

Takana și al. descriu în [142, 143] mai multe scheme de watermarking care se bazează pe ascunderea watermark-ului prin modificarea zgomotului de cuantizare. Ideea lor se bazează pe faptul că zgomotul de cuantizare este, în general, imperceptibil observatorilor. Prima schemă ascunde watermark-ul în imagine prin folosirea unei secvențe de date predefinite pentru a selecta nivelul într-un cuantizor predictiv. Secvența de date este astfel aleasă, încât imaginea rezultantă să arate ca și zgomotul de cuantizare. De asemenea, este prezentată și o variație a acestei scheme, unde un watermark sub forma unei matrice de dither este folosită pentru a modifica imaginea într-un anumit mod.

Există mai multe dezavantaje pentru aceste scheme. Cel mai important ar fi faptul că sunt sensibile la procesări de semnal, mai ales la recuantizare și la atacuri geometrice. Ele degradează imaginea în același mod ca și codarea predictivă sau dither-ul.

4.4. Formarea datelor cu watermark

Cea mai uzuală modalitate de formare a semnalului cu watermark este însumarea directă a watermark-ului, de obicei sub forma unei secvențe pseudo-aleatoare, la amplitudinea datelor sursă. Această operație poate fi realizată în domeniul spațial, DFT, DCT sau Wavelet, după cum s-a discutat anterior. Această metodă de formare a datelor cu watermark este de obicei folosită de tehnicile de watermarking cu spectru împrăștiat. O alternativă ar fi modificarea fazei semnalului sursă, ca de exemplu în [144]. Nu contează ce modificăm la datele sursă,

atâta timp cât nu luăm în calcul aceste date în procesul de inserare, ele vor constitui o interferență majoră la decodarea watermark-ului, limitând performanța decodatorului chiar în absența atacurilor.

În cazul metodelor de watermarking bazate pe cuantizare eșantioanele sursei sunt cuantizate pentru a reprezenta watermark-ul. Gradul de distorsiune a datelor originale depinde de cuantizorii folosiți de algoritmul de inserare.

4.5. Extragerea watermark-ului

Majoritatea schemelor de watermarking cu spectru împrăștiat folosesc corelația pentru detecția și decodarea watermark-ului, deci se presupune implicit că interferența este de tip gaussian, deoarece doar atunci corelația este optimă. Imaginile, însă nu urmăresc o distribuție gaussiană în domeniul spațial și mulți autori (de exemplu în [145, 146]) sugerează filtrarea (cu un filtru trece sus) a imaginii recepționate înainte de detecție pentru a îmbunătăți performanța. Acest lucru se realizează, deoarece majoritatea energiei imaginii se află în componentele de frecvență joasă. Prin filtrarea trece sus aceste componente sunt înlăturate și semnalul se apropie mai mult de o distribuție gaussiană. Scăderea imaginii inițiale din imaginea cu watermark înaintea detecției, ca și în cazul algoritmilor privați, este de asemenea un caz special de preprocesare. Dacă avem la dispoziție distribuția coeficienților imaginii, putem folosi un decodor de probabilitate maximă în locul blocului de corelație. De exemplu, în [147] Rosa și alții modelează coeficienții DFT folosind o distribuție Weibull și deduc decodorul optim corespunzător. Dacă inserarea watermark-ului are loc în domeniul frecvență se pot combina semnalele de la ieșirea diferitelor subbenzi într-un mod optim pentru a maximiza raportul semnal-zgomot total. Un alt aspect a detecției watermark-ului ce poate fi optimizat este alegerea pragului de detecție. Piva și alții argumentează în [148] că alegerea pragului pe baza principiului Neyman-Pearson [149] este o metodă mai bună decât minimizarea probabilității erorii în prezența atacurilor.

Sistemele de watermarking cu spectru împrăștiat se bazează pe sincronizarea perfectă dintre transmițător și receptor pentru o comunicație perfectă. Dacă imaginea este supusă unei transformări geometrice (tăiere, scalare, rotație), se pierde această sincronizare și watermark-ul trebuie resincronizat înainte de detecție. Mai mulți autori au propus folosirea unei secvențe

separate [150] sau construirea secvenței de watermark într-un mod specific [151] pentru a permite sincronizarea. Atacurile geometrice vor fi discutate în capitolul 6.

În cazul metodele bazate pe cuantizare, decodorul cuantizează eşantioanele recepționate și se uită în ce categorie intră fiecare eşantion pentru a recupera datele inserate. În acest caz, semnalul sursă nu mai acționează ca o interferență.

Se poate observa că majoritatea metodelor de watermarking pentru imagini sunt bazate pe același principiu: sunt aplicate modificări pseudo-aleatoare mici asupra unor coeficienți selectați în domeniul spațial sau al transformatei. Aceste modificări sunt apoi identificate prin corelație sau măsurări de similitudine asemănătoare corelației pentru tehnicile cu spectru împrăștiat și prin cuantizare pentru metodele bazate pe cuantizare. De obicei, numărul de coeficienți este mult mai mare decât numărul de biți de informație inserați. Rezultă astfel o inserare redundantă ce conduce la robustețe. După cum am văzut, domeniul de inserare a watermark-ului poate avea o influență substanțială asupra robusteții watermark-ului. Schemele de watermarking în domeniul spațial sunt, în general, mai puțin robuste la atacuri cu zgomot sau compresie JPEG sau MPEG cu pierderi. Oricum, un mare avantaj este, de obicei, faptul că watermark-ul poate fi ușor recuperat dacă imaginea a fost decupată sau translatată. Decuparea imaginii în domeniul spațial corespunde unei distorsiuni destul de substanțiale în domeniul frecvență, ce distruge watermark-ul inserat. Același lucru este valabil pentru domeniul DCT. Dacă watermark-ul este introdus în blocuri DCT, este important să se știe poziția blocurilor pentru o decodare cu succes. Domeniul Wavelet are dezavantaje asemănătoare, deoarece Transformata Wavelet nu este invariantă nici la translatare, nici la rotație. Majoritatea metodelor lucrează în domeniul spațial probabil datorită simplității și eficienței unor astfel de metode. Numărul de publicații bazate pe DCT este, de asemenea, mare.