

Universitatea Tehnică din Cluj-Napoca
Universitatea “Politehnica” din Timișoara

Contribuții la marcarea
transparentă a imaginilor în
domeniul transformatei wavelet

Corina NAFORNITA

Conducători științifici:

Prof. Dr. Ing. Monica BORDA

Prof. Dr. Ing. Alexandru ISAR

2008

Cuprins

1. Introducere	1
1.1 Cheia criptografică publică sau secretă	2
1.2 Autentificarea	3
1.3 Concepte de bază ale marcării transparente	7
1.4 Aplicații posibile ale marcării transparente	11
1.5 Etapele marcării	13
1.5.1 Generarea marcajului	14
1.5.2 Înglobarea marcajului	14
1.5.3 Căutare pe <i>Web</i>	16
1.5.4 Detecția marcajului	16
1.5.5 Căutarea în baze de date	17
1.6 Proprietățile principale ale metodei de marcarea	18
1.6.1 Condiții generale impuse marcării	18
1.6.2 Condiții specifice impuse marcării	21
1.7 Marcarea și înregistrare pentru o protecție eficientă	22
1.8 Modele de bază pentru watermarking	23
1.9 Evaluarea performanțelor unei metode de marcarea	25
1.10 Marcarea robustă	26
1.10.1 Problema detecției optime	26
1.10.2 Soluții pentru asigurarea robusteții	30
1.10.3 Marcarea informată	31
1.10.4 Codarea informată	33
2. Tehnici de marcarea	36
2.1 Clasificarea tehnicilor de marcarea	36
2.1.1 Alegerea locațiilor unde se înserează marcajul	38
2.1.2 Domeniul de marcarea	39
2.1.2.1 Domeniul spațial	39
2.1.2.2 Domeniul unei transformate	40
2.1.2.2.a Metode bazate pe transformata Fourier discretă	42
2.1.2.2.b Metode bazate pe transformata cosinus discretă	44
2.1.2.2.c Metode bazate pe transformata wavelet	46
2.1.2.2.d Metode bazate pe transformata Fourier-Mellin	48
2.1.3 Codarea marcajului	48
2.1.4 Formarea semnalului marcat	52
2.1.5 Extragerea marcajului	54
2.2 Tehnici de marcarea transparentă	56
2.2.1 Algoritmi în domeniul spațial	57
2.2.2 Algoritmi în domeniul unei transformate	64
2.2.2.1.a Metode bazate pe DCT	65
2.2.2.1.b Metode bazate pe transformata DFT	70
2.2.2.1.c Metode care aplică transformata Fourier-Mellin	70
2.2.2.1.d Domeniul wavelet	71
2.2.2.1.e Metode care aplică fractalele	78
2.2.2.1.f Marcarea transparentă cu transformata SVD	79
2.2.2.1.g Marcarea transparentă cu transformata Ridgelet	80

2.2.2.1.h Marcare transparentă cu cuaternioni	81
2.2.2.1.i Marcare transparentă cu transformata LOT	81
2.3 Concluzii	81
3. Atacuri asupra sistemelor de marcarea	82
3.1. Problema marcării transparente	82
3.2. Constrângeri asupra atacatorului	82
3.3. Clasificarea atacurilor	84
3.4 Atacuri ce folosesc o copie marcată	86
3.4.1 Compresia.....	86
3.4.2 Filtrarea	88
3.4.3 Atacul prin adăugare de zgomot.....	89
3.4.4 Atacurile geometrice	89
3.4.5 Atacurile de tip protocol.....	92
3.4.6 Atacurile de tip criptografic	93
3.4.7 Atacurile de estimare.....	94
3.4.8 Atacul de remodulare	95
3.4.9 Atacul de estimare în desincronizare	96
3.4.10 Măsuri împotriva atacurilor prin estimare.....	97
3.4.11 Atacurile dependente de statistica locală a semnalului	100
3.4.12 Atacurile optimizate	100
3.4.13 Atacurile ce folosesc mai multe cadre din secvența video.....	101
3.5 Atacurile ce folosesc mai multe copii marcate (multiple-copy).....	103
3.5.1 Coliziunea liniară	104
3.5.2 Coliziunea neliniară.....	105
3.6 Concluzii.....	105
4. Aplicarea transformatei wavelet în marcarea informată a imaginilor	106
4.1 Introducere.....	106
4.2 Înglobarea și extragerea marcajului.....	106
4.2.1 Înglobarea marcajului.....	106
4.2.2 Detecția și extragerea marcajului	109
4.3 Prima metodă de marcarea informată.....	111
4.4 A doua metodă de marcarea informată.....	114
4.5 Detecție îmbunătățită prin metoda max-correlation	133
4.6 A treia metodă de marcarea informată. O abordare statistică	137
4.7 Concluzii.....	142
5. Aplicarea transformării wavelet în marcarea perceptuală neinformată a imaginilor	144
5.1 Introducere.....	144
5.2 Marcarea perceptuală	144
5.3 Marcarea perceptuală propusă de Barni, Bartolini și Piva	145
5.4 Masca perceptuală îmbunătățită	147
5.5 Testarea noii măști perceptuale	153
5.6 Înserare în subbenzile de frecvență mai joasă	157
5.7 Evaluarea robusteții marcajelor perceptuale.....	164
5.8 Înserare în toate subnivelele de rezoluție	183

5.9 Concluzii.....	196
6. Concluzii și contribuții personale.....	198
6.1 Concluzii.....	198
6.2 Contribuții personale	202
Publicații proprii.....	207
Bibliografie	209

Capitolul 1

Introducere

În ultimul deceniu, am asistat la o explozie în folosirea și distribuirea datelor multimedia digitale. Conectarea la Internet a calculatoarelor personale a facilitat și accelerat distribuirea aplicațiilor și datelor multimedia. Astfel, s-au dezvoltat rapid aplicațiile de comerț electronic și de servicii on-line. Echipamentele audio și video analogice sunt înlocuite progresiv cu echipamente digitale. Rezultatul a fost apariția unor dispozitive de înregistrare de masă, de capacități mari și foarte mari, pentru datele multimedia, care au pătruns masiv pe piață.

Astfel, o dată cu dezvoltarea pe scară largă a comunicațiilor prin intermediul Internet-ului, a apărut nevoia de protejare a informației digitale împotriva copierii și manipulării ilegale. Dezvoltarea rapidă a tehnologiei digitale face necesară dezvoltarea metodelor pentru protejarea produselor multimedia împotriva pirateriei. Atacurile pirat includ accesul ilegal al datelor pe Internet, modificări ale conținutului făcute cu rea-voință, retransmisia copiilor neautorizate. Impactul acestui gen de atacuri ar putea fi foarte mare atât pe plan financiar, pierderi financiare cauzate de accesarea și folosirea neautorizată a datelor, cât și în planul securității.

Când este vorba de semnale analogice, problema se rezolvă de la sine, deoarece copiile sunt de o calitate mai redusă decât originalele (casete audio și video). În schimb, informația digitală poate fi copiată perfect și distincția între original și copii este dificil, dacă nu imposibil de făcut. În plus, nu există nici un mecanism pentru a depista copierea ilegală sau modificarea conținutului.

Datele digitale sau numerice au multe avantaje față de cele analogice, dar producătorii de servicii au rețineri când oferă servicii sub formă digitală, din cauza ușurinței cu care se pot realiza duplicate care se pot distribui neautorizat. Din această cauză, se impun măsuri pentru protejarea proprietății intelectuale și a drepturilor de autor pentru materialele memorate digital [LSL00]. Absența unor sisteme de protecție adecvate a dus la întârzierea introducerii DVD-urilor (Digital Video Disc); unele companii media au refuzat inițial să producă și să comercializeze materiale pe DVD-uri, înainte de a se rezolva aceste probleme de protejare a informației [LSL00]. Astfel, în octombrie 1998 în SUA a fost adoptată o lege de protecție intelectuală, „*Digital Millennium Copyright Act*” [DMCA98], iar în Uniunea Europeană în mai 2001, respectiv aprilie 2004, au fost adoptate directive pentru protejarea copyright-ului și a drepturilor de proprietate intelectuală, inclusiv pentru produse multimedia digitale, cum ar fi CD-uri și DVD-uri [Dir01, Dir04].

Pentru a asigura protecția la copiere și protecția drepturilor de autor pentru date digitale audio sau video, au fost dezvoltate două categorii de tehnici complementare și anume: *criptarea* și *marcarea transparentă (watermarking)*.

Tehnicile de *criptare* pot fi folosite pentru protejarea datelor digitale în timpul transmiterii între emițător și receptor [CMB02]. Dar după recepția și decriptarea de la receptor, când se obține varianta originală a datelor, acestea nu mai sunt protejate. Folosind tehnica complementară *criptării*, de *marcare transparentă*, datelor li se adaugă un semnal secret imperceptibil, marcaj sau watermark. Acest marcaj se introduce direct în datele originale, într-un mod care-l face să rămână permanent prezent.

Asigurarea unui canal sigur de informație se referă la restricționarea accesului, criptarea și/sau autentificarea informației. Aceasta este o problemă rezolvată, pentru care există protocoale de securizare. Ea este însă o problemă diferită de cea a protejării dreptului de autor.

În cele ce urmează, se explică trei noțiuni importante: cheia criptografică, autentificarea și protecția dreptului de autor.

1.1 Cheia criptografică publică sau secretă

“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter.”

Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C

Datele transmise prin comunicațiile în rețele pot fi protejate împotriva utilizatorilor neautorizați prin aplicarea tehnicilor bazate pe criptare.

Criptografia este *știința secretizării datelor*. Ea stă la baza multor servicii și mecanisme de securitate folosite în rețele și mai ales în Internet, utilizând metode matematice pentru transformarea datelor, în intenția de a ascunde conținutul lor sau de a le proteja împotriva modificării. Deși are o istorie îndelungată, criptografia s-a dezvoltat în ultimii ani mai ales datorită dezvoltării rețelelor de calculatoare.

Datele originale sunt criptate de proprietar folosind o cheie privată. Utilizatorii pot decripta datele primite folosind un algoritm implementat hard sau soft. Condiția necesară pentru o decriptare cu succes este ca utilizatorul să dețină cheia privată a furnizorului, sau o cheie asociată publică sau parțial publică. Un deziderat este implementarea rapidă a algoritmului de criptare-decriptare. În plus creșterea volumului de date datorată criptării ar trebui să fie în limite rezonabile. De asemenea, lungimea cheii ar trebui să fie suficientă pentru a preveni decriptarea neautorizată prin proceduri iterative de tip *trial and error*.

Datele care pot fi citite și înțelese fără măsuri speciale se numesc *text clar*. Metoda prin care datele clare sunt mascate, ca să ascundă esența, se numește *criptare*, rezultând *textul cifrat*. Procesul invers de transformare a datelor cifrate în date clare se numește *decriptare* [PGP99, Isa02].

Criptarea convențională, numită și criptare cu cheie secretă sau cheie simetrică, folosește o cheie atât pentru criptare cât și pentru decriptare. Cheia este cunoscută doar de către destinatarul mesajului. Pentru toți ceilalți utilizatori ai rețelei cheia este secretă. În anul 1975 a fost adoptat primul standard de criptare a datelor propus de IBM, numit DES (Data Encryption Standard). Acesta descrie un algoritm de criptare simetrică.

Witfield Diffie și Martin Hellman, cercetători la universitatea Stanford au pus, în anul 1976, [DH76], bazele *criptografiei asimetrice cu chei publice*. Se utilizează două chei, una secretă (cunoscută doar de destinatarul mesajului) și una publică care poate fi cunoscută de orice utilizator al rețelei. Pe baza cheii publice se poate face identificarea sursei de unde sosește un anumit mesaj. Folosind acest algoritm se poate face și autentificarea mesajului, adică destinatarul poate să verifice și dacă expeditorul este cel declarat în cadrul mesajului și dacă mesajul a fost cumva falsificat de către un alt utilizator. Funcționarea acestei metode de criptare este descrisă în continuare.

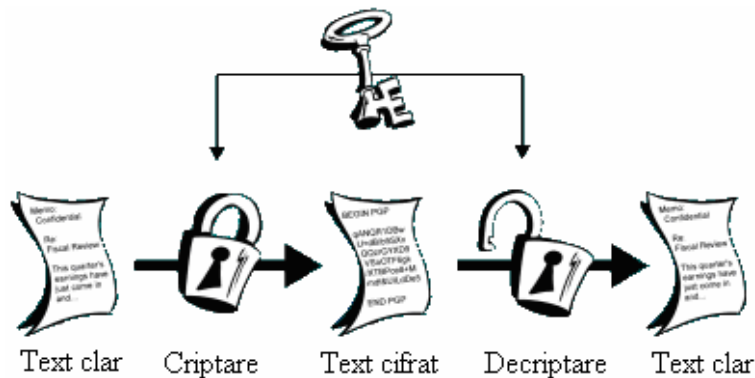


Fig. 1.1: Criptarea cu cheie privată (simetrică).

Bob și Alice au câte o copie a softului, distribuit liber, de criptare cu cheie publică. Fiecare folosește copia proprie pentru a crea o pereche de chei. Un mesaj criptat cu una dintre cheile din această pereche de chei poate fi decriptat doar cu cealaltă cheie din aceeași pereche. Cea de-a doua cheie nu poate fi generată matematic folosind doar prima cheie.

Bob face cunoscută una dintre cheile din perechea sa, aceasta devenind cheia sa publică. Alice face același lucru. Fiecare păstrează secretă cealaltă cheie din pereche, care devine cheia sa privată. Dacă Bob vrea să cripteze un mesaj, pe care să-l poată citi doar Alice, atunci el folosește cheia publică a lui Alice, care este disponibilă tuturor; acest mesaj va putea fi decodat doar cu ajutorul cheii secrete a lui Alice. Procesul invers, trimiterea unui mesaj criptat de la Alice la Bob este asemănător. De fapt, Bob și Alice pot acum schimba între ei fișiere criptate, fără a avea vreun canal sigur pentru transmiterea cheilor, acesta fiind un avantaj major asupra comunicațiilor bazate pe criptarea simetrică.

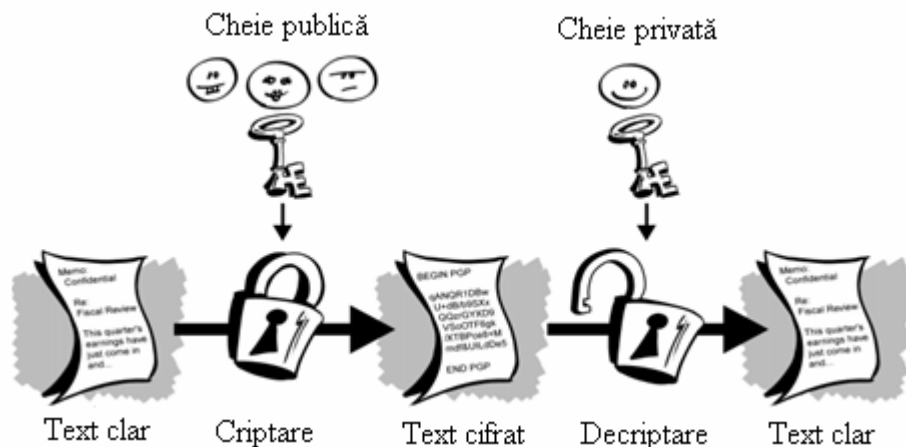


Fig. 1.2: Criptarea cu cheie publică (asimetrică).

1.2 Autentificarea

Autentificarea (în limba greacă, *αυθεντικός* înseamnă real sau original, iar în limba latină *authentēs* înseamnă autor) este stabilirea sau confirmarea că ceva, sau cineva este autentic, adică este ceea ce pretinde. Autentificarea unui obiect înseamnă

confirmarea originii sale, în timp ce autentificarea unei persoane presupune de obicei verificarea identității sale.

În securitatea calculatoarelor și rețelelor de calculatoare, autentificarea este încercarea de a verifica identitatea utilizatorului într-o comunicație, cum ar fi o cerere de login. Utilizatorul ce se dorește a fi autentificat, poate fi o persoană ce folosește un calculator sau un program. Autentificarea exprimă ideea că unele resurse au fost puse la dispoziție pentru a garanta că entitățile sunt ceea ce susțin că sunt, sau că informația nu a fost manipulată de părți neautorizate, acesta fiind una dintre obiectivele securității. Exemple de astfel de obiective includ controlul accesului, autentificarea entităților, autentificarea mesajelor, integritatea datelor, nerepudierea și autentificarea cheilor.

Până la mijlocul anilor '70 se credea că *autentificarea* și *confidențialitatea* sunt conectate intrinsec. Odată cu descoperirea funcțiilor *hash* și a semnăturilor digitale, s-a observat că autentificarea și confidențialitatea sunt obiective separate și independente ale securității informației. Separarea lor nu este doar folositoare, ci și esențială. De exemplu dacă Alice, aflată într-o țară, comunică cu Bob, aflat în altă țară, statele gazdă s-ar putea să permită sau nu confidențialitatea canalului; una dintre țări, sau ambele, ar putea dori să monitorizeze toate comunicațiile. Însă Alice și Bob vor să fie siguri de identitatea celuilalt, de integritatea și originea informațiilor pe care le trimit și pe care le primesc.

Scenariul anterior relevă câteva aspecte independente ale autentificării. Dacă Alice și Bob vor asigurări despre identitatea celuilalt sunt două posibilități:

- Alice și Bob comunică *în timp real*, adică fără întârzieri apreciabile. Alice și Bob vor dori să-și verifice identitatea în timp real. Acest lucru se poate realiza dacă Alice îl provoacă pe Bob să răspundă la o întrebare la care numai el știe răspunsul corect. Același lucru îl poate face și Bob pentru a o identifica pe Alice. Aceasta este o autentificare a entităților sau, mai simplu, o *identificare*.

- Alice și Bob *nu comunică în timp real*, adică schimbă mesaje *cu o anumită întârziere*, adică mesajele sunt rutate prin numeroase rețele, stocate și apoi redirijate după o perioadă. În acest caz nu este indicată o întrebare și așteptarea unui răspuns și, în plus, comunicarea s-ar putea să se desfășoare într-o singură direcție. Sunt necesare alte tehnici pentru autentificarea originii mesajului. Aceasta este o nouă formă de autentificare numită *autentificarea originii datelor*.

Autentificarea expeditorului este operația de verificare a identității dintre expeditor și persoana care, pe baza mesajului, pare să fie expeditorul. Să presupunem că Bob trimite tuturor utilizatorilor rețelei un mesaj, după ce l-a criptat cu cheia sa secretă. Oricare dintre utilizatori poate folosi cheia publică a lui Bob pentru a decripta acest mesaj, adevărind că acesta este un mesaj care ar putea veni numai de la Bob.

Autentificarea mesajului, reprezintă operația de validare a faptului că mesajul recepționat este o copie neatinsă a mesajului trimis. Și această operație poate fi realizată folosind criptarea cu cheie publică. Să presupunem că înainte de a expedia un mesaj, Bob efectuează o operație criptografică asupra acestuia, de exemplu îl transformă cu ajutorul unei funcții „hash”, ale cărei valori sunt dificil de calculat cu metode numerice. Cel mai simplu exemplu de astfel de funcție este cea care asociază o sumă de control textului clar. Este foarte dificil să se modifice textul clar fără a modifica valoarea obținută prin aplicarea funcției amintite mai sus.

Unul din avantajele criptării cu cheie publică este că oferă o metodă pentru implementarea semnăturilor digitale. De aceea Guvernul S.U.A a decis elaborarea unui standard de semnătură digitală, bazat pe utilizarea cheilor publice și secrete, standardul DSS (*Digital Signature Standard*) publicat în 1991.

Semnătura digitală oferă posibilitatea de verificare a autenticității informației și a integrității ei. O semnătură digitală este un mesaj codat care se potrivește cu conținutul unui document digital autentic. În loc să criptăm informația folosind cheia publică a altei persoane, o criptăm cu cheia privată personală. Dacă informația poate fi decriptată cu cheia publică personală, atunci informația provine de la tine.

Metoda cea mai simplă de înserare a semnăturii digitale este arătată în figura de mai jos:

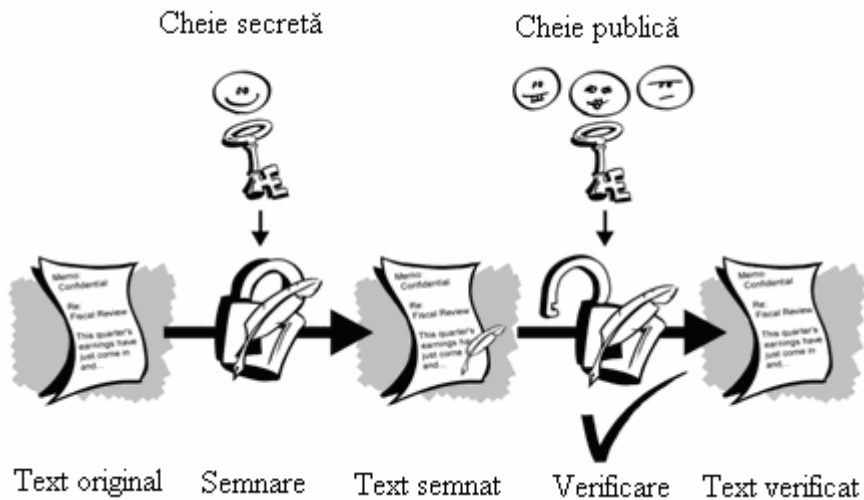


Fig. 1.3: Inserarea unei semnături digitale.

Acest standard se bazează pe un algoritm de semnătură digitală, DSA (Digital Signature Algorithm) folosit în aplicațiile în care este mai potrivită utilizarea unei semnături digitale în locul unei semnături scrise. DSA asigură posibilitatea de a genera și de a verifica semnături digitale. Generarea semnăturilor se bazează pe utilizarea unei chei secrete. Verificarea semnăturii se bazează pe folosirea unei chei publice care corespunde cheii secrete. Fiecare utilizator posedă o pereche de chei, formată din cheia sa publică și cheia sa secretă. Cheile publice pot fi cunoscute de către orice utilizator al rețelei. Oricine poate verifica semnătura unui utilizator folosind cheia sa publică.

Generarea semnăturii unui utilizator poate fi realizată numai de către acesta, deoarece în procesul de generare se folosește cheia sa secretă. În procesul de generare a semnăturii se utilizează o funcție hash, pentru a obține o variantă condensată (rezumat al mesajului) a datelor care trebuie transmise (figura 1.4, 1.5).

Funcțiile *hash* sunt funcții de compresie, contracție sau de rezumat al mesajului, fiind niște amprente digitale; ele au la intrare un șir de date de lungime variabilă n , numit *preimage* și la ieșire generează un șir de lungime fixă m (uzual 128 sau 160 biți) numit *valoarea funcției hash*. Acestui rezumat i se aplică algoritmul DSA pentru a se genera *semnătura digitală*. Semnătura digitală împreună cu mesajul semnat sunt transmise celui care trebuie să o verifice, cu ajutorul cheii publice a expeditorului. În procesul de verificare trebuie folosită aceeași funcție hash.

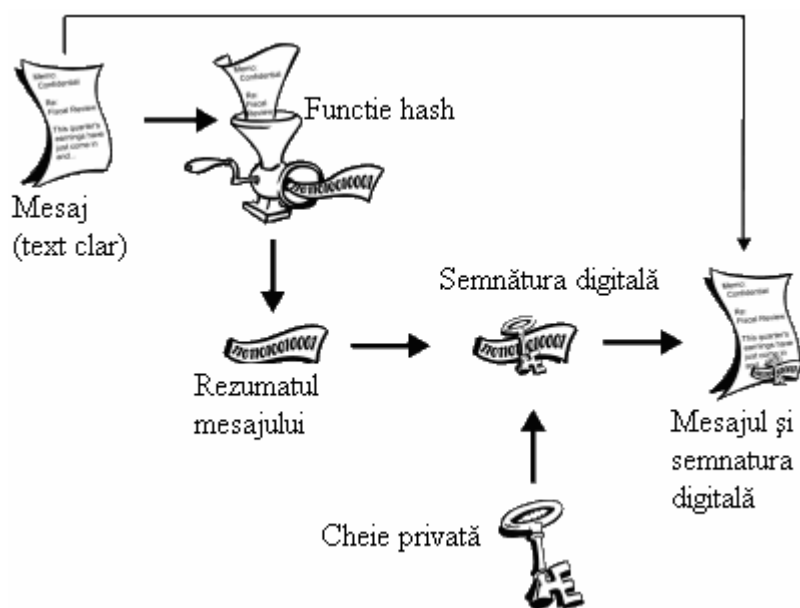


Fig. 1.4: Semnarea folosind o cheie privată.

Proceduri similare trebuie folosite și pentru generarea și verificarea semnăturilor digitale pentru date stocate (nu transmise). O semnătură digitală are același scop ca și o semnătură scrisă de mână. Diferența este că cea scrisă de mână este ușor de falsificat, pe când cea digitală este aproape imposibil de falsificat.

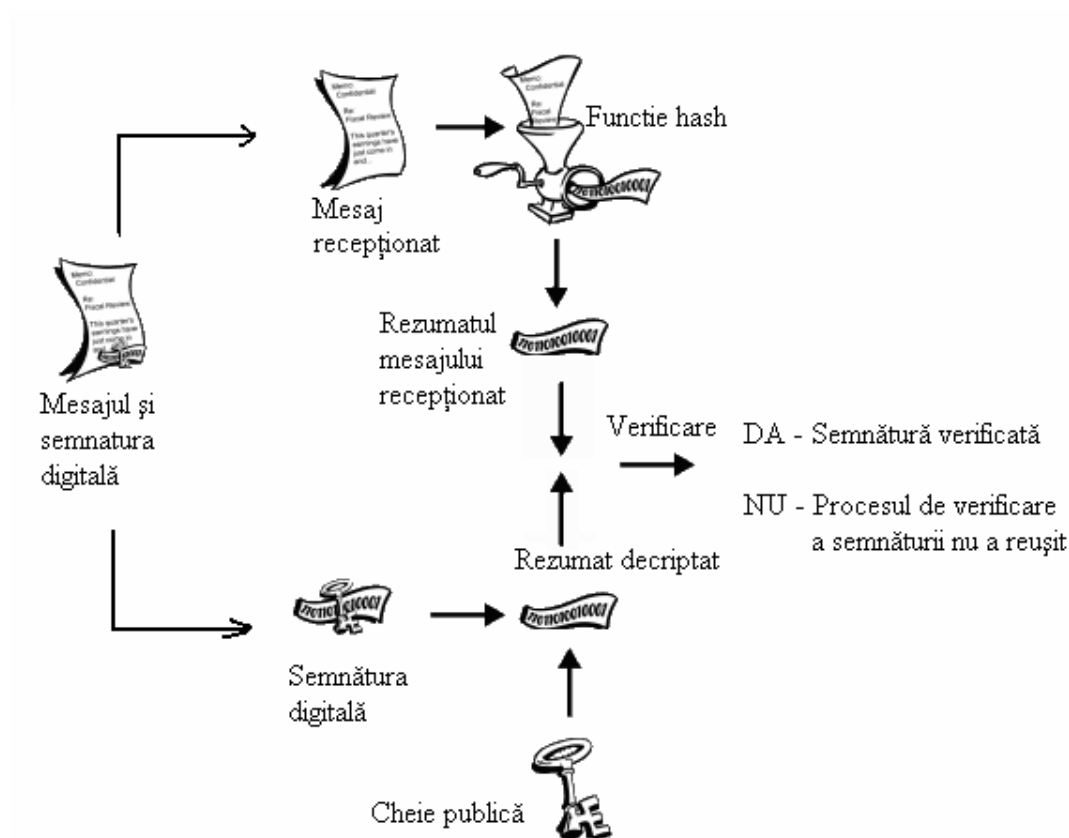


Fig. 1.5: Verificarea cu cheie publică.

În cazul datelor multimedia, manipularea conținutului poate fi făcută în diferite scopuri, legale sau ilegale, prin compresie, filtrare, modificare cu rea intenție. Produsul modificat nu este autentic. De aceea, utilizatorii ar trebui să poată verifica originalitatea conținutului unui produs digital. Verificarea conținutului poate fi făcută adăugând semnături digitale în datele transmise. Procedurile de verificare a autenticității se bazează pe algoritmi publici și pe chei publice. Orice modificare ne semnificativă adusă produsului sau semnăturii ar trebui să ducă la neautentificare. Lungimea semnăturii este proporțională cu cantitatea de date „semnate”, astfel că semnăturile sigure și eficiente nu sunt fezabile pentru produse multimedia (care de obicei au o cantitate mare de date).

1.3 Concepte de bază ale marcării transparente

“A distinguishing mark or device impressed in the substance of a sheet of paper during manufacture, usually barely noticeable except when the sheet is held against strong light” - Oxford English Dictionary

Manipularea datelor în format digital și transmiterea lor spre utilizatori poate fi făcută prin serviciile web. Utilizatorul poate avea acces la un produs interesant, fie direct de pe pagina *web* a proprietarului de drept, fie printr-o bibliotecă digitală, fie printr-un intermediar. Un produs digital poate să fie prezentat în forma sa originală sau ca parte dintr-o aplicație multimedia mai mare. Considerăm un sistem elementar de distribuție a produselor digitale prezentat în Figura 1.6.

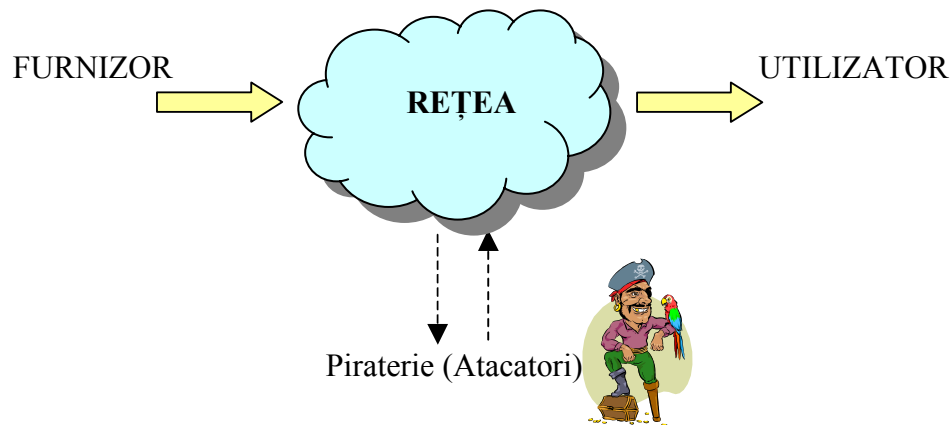


Fig. 1.6: Sistem elementar de distribuție a produselor digitale. Sunt posibile atacurile pentru violarea dreptului de autor sau modificări făcute cu rea intenție.

Utilizatorul primește un produs digital de la un editor care are drept de autor, și care poate fi și autorul original. Accesul și transmiterea produsului au loc într-un mediu de comunicații. Atacatorii pot aduce daune proprietarului de *copyright*, prin reproducerea și retransmiterea ilegală a produselor digitale. Mai mult, ei pot face modificări asupra produselor, furnizând utilizatorilor produse neautentice (false). De aceea, editorul și utilizatorul au nevoie de protecție:

- proprietarul dreptului de autor necesită o metodă de protejare eficientă în tot domeniul accesibil de adrese,
- utilizatorii cer produse autentice atunci când le achiziționează legal.

Utilizatorii nu aduc daune altora pentru că nu retransmit sau expun produse pe pagini *web* publice, dar atacatorii sunt editori neautorizați.

Considerăm pirateria în primul rând ca activitatea de copiere ilegală și/sau revânzarea produselor multimedia digitale. Ușurința cu care se pot face copii identice face pirateria o problemă majoră în securitatea informațională. Se prezintă trei situații considerate în aplicațiile obișnuite de securitate și deficiențele tehnicilor de securitate în protejarea produselor multimedia [Kun99].

În prima situație (Figura 1.7), Alice vinde un produs multimedia lui Peter. Deși informația poate fi protejată în timpul transmisiei către Peter, folosind algoritmi stabiliți de criptare, produsul va fi neprotejat o dată ce este decriptat de Peter. Nu există nici un mecanism care să îl împiedice pe Peter să facă copii ilegale ale produsului cumpărat de la Alice. De aceea, este nevoie de un nivel de securitate suplimentar pentru protejarea proprietății intelectuale.

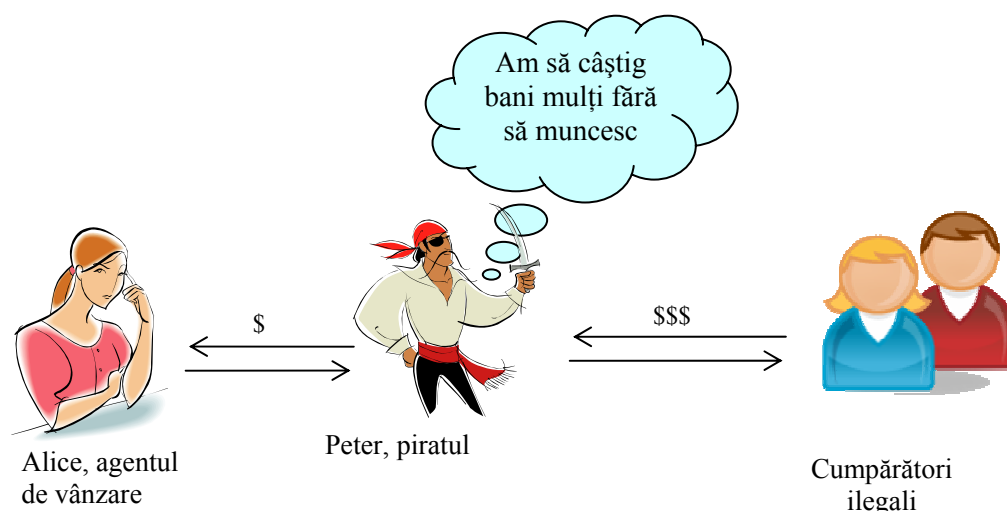


Fig. 1.7: Limitările tehnicilor obișnuite de securizare în piraterie.

Alice îi vinde lui Peter un produs multimedia. Deși informația poate fi protejată în timpul transmisiei către Peter, prin proceduri obișnuite de securizare, aceasta va fi neprotejată atunci când este decriptată de Peter.

Abordările obișnuite de autentificare nu sunt nici ele potrivite pentru protejarea conținutului produsului multimedia împotriva falsificării. Falsificarea (*tampering*) se referă la orice fel de modificare sau contrafacere a unui semnal dat. În Figura 1.8, prezentăm o astfel de situație posibilă. Alice îi trimite informații lui Bob. Înainte de a ajunge la acesta, semnalul poate suferi distorsiuni întâmplătoare, cum ar fi eronarea aleatoare a biților, sau pierderi de pachete. Aceste distorsiuni întâmplătoare nu afectează integritatea semnalului.

În plus, este posibil ca Tom, care are acces la date, să modifice cu rea-credință semnalul pentru a ascunde informații false. Procedurile obișnuite de autentificare trec datele care trebuie să fie autentificate printr-o funcție *hash one-way* pentru a produce o secvență de biți, semnătura digitală. Semnalul și semnătura digitală sunt transmise către Bob. La recepție, Bob trece semnalul primit prin aceeași funcție *hash one-way*, și poate compara secvența obținută de biți cu semnătura digitală primită. Dacă cele

două secvențe se potrivesc, atunci semnalul este considerat autentic sau credibil, altfel se consideră că a avut loc o falsificare.

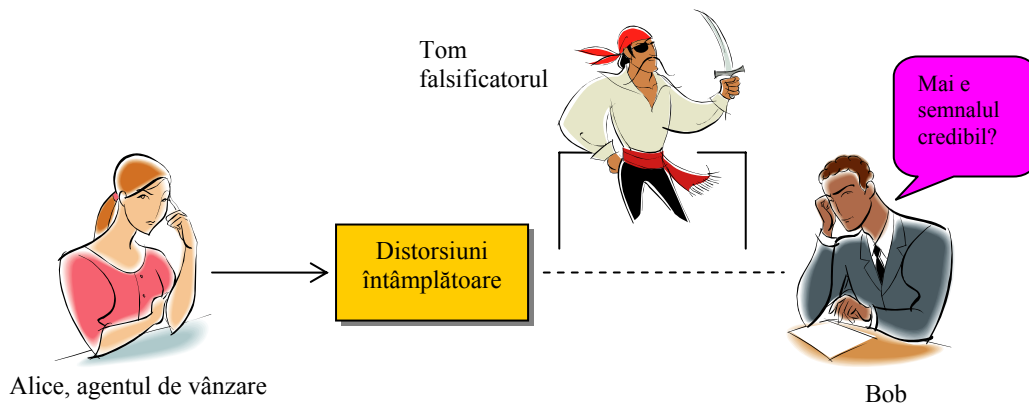


Fig. 1.8: Limitările securizării obișnuite în problema falsificării. Bob nu poate să facă diferența între distorsiuni întâmplătoare, care nu afectează integritatea semnalului, și distorsiunile făcute cu rea voință de către Tom, pentru a-l induce în eroare pe Bob.

Deși procedura de autentificare specificată este eficientă pentru unele tipuri de date, ea nu este eficientă pentru semnalele multimedia, deoarece nu se poate face deosebirea între cele două tipuri de distorsiuni, datorate marcării respectiv transmisiei. În ambele situații, semnalul este modificat. Când distorsiunile au caracter aleator, semnalul mai este încă perceptual credibil. De multe ori deciziile cu privire la integritatea conținutului se impun pe baza aprecierii gradului de distorsiuni al semnalului recepționat.

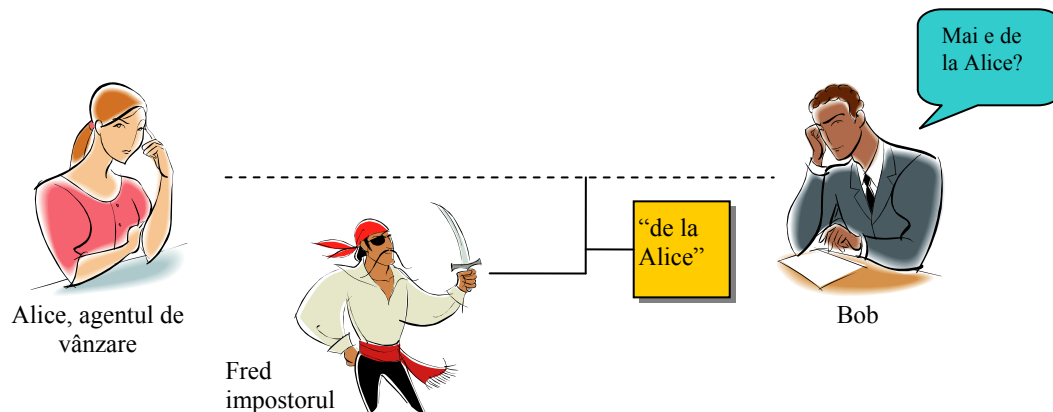


Fig. 1.9: Limitările securizării obișnuite în problema fraudei. Deoarece informația de autentificare este deseori transmisă ca informație adițională semnalului, ea poate fi eliminată în timpul conversației în alt format sau în timpul compresiei. Ca urmare, Bob va fi incapabil să afle dacă semnalul primit este sau nu de la Alice.

Figura 1.9 prezintă procesul de fraudă care se referă la orice fel de înșelătorie sau impostură. Fred trimite informații lui Bob, dar Fred ar vrea să pară că expeditorul a fost Alice. Pentru a preveni acest tip de atacuri, pot fi trimise mesaje criptate care să conțină informația separată de autentificare a expeditorului real. Cu toate acestea, semnalele multimedia suferă deseori schimbări în timpul tranzitului. Aceste schimbări

pot elimina întâmplător informația de autentificare, în așa fel încât Bob nu va putea identifica cu ușurință proprietarul de drept al produsului multimedia.

Pentru a trata neajunsurile metodelor de securizare tradiționale discutate mai sus, a fost propusă metoda de înglobare a unei informații invizibile în produse multimedia, numită *digital watermarking* (marcare transparentă). Denumirea de watermark provine de la cuvintele din limba engleză water-apă și mark-marcaj și desemnează un marcaj transparent, invizibil, asemănător transparenței apei. Termenul de watermarking este utilizat la modul general, pentru înserarea de biți de informație, unul sau câțiva biți, dar pentru cazurile în care se înserează mai mulți biți se mai folosește și termenul de *data embedding*.

Marcarea este mai potrivită pentru semnale multimedia, cum ar fi imagini, audio și video, deoarece conținutul lor este protejat, în opoziție cu formatul digital, care poate suferi conversii. În acest fel, informația de autentificare este înglobată în semnalul multimedia, chiar și după conversii ale formatului sau alte prelucrări.

Marcajele sunt generate în mod privat și apoi ar trebui să fie detectate folosind chei private sau publice în funcție de întrebuințarea lor. Marcajul conține, în general, informații despre originea și/sau destinația informației gazdă. Deși nu este folosit direct în protecția proprietății intelectuale, el ajută la identificarea sursei și destinatarului, fiind util în cazul disputelor privind dreptul de autor sau distribuitor al informației.

Teoretic, marcajul trebuie să protejeze informația permanent, deci trebuie să aibă calitatea de a fi robust, astfel încât să nu poată fi înlăturat din informația gazdă, fără degradarea esențială a calității acesteia. Acest marcaj este asemănător unei semnături, cu observația că trebuie să fie transparent.

Procedeul de marcarea transparentă pentru a putea realiza protejarea informației, constă din două operații: introducerea marcajului în datele gazdă, înainte de transmisie sau stocare, precum și extragerea marcajului din datele recepționate și compararea marcajului adăugat la emisie cu cel extras la recepție, pentru autentificare, în caz de dispută. În Figura 1.10, se prezintă schematic un sistem de protejare a datelor în format digital. Acestea sunt reprezentate prin simbolul D; se mai notează cu D' datele criptate, cu S semnătura, iar W reprezintă marcajul.

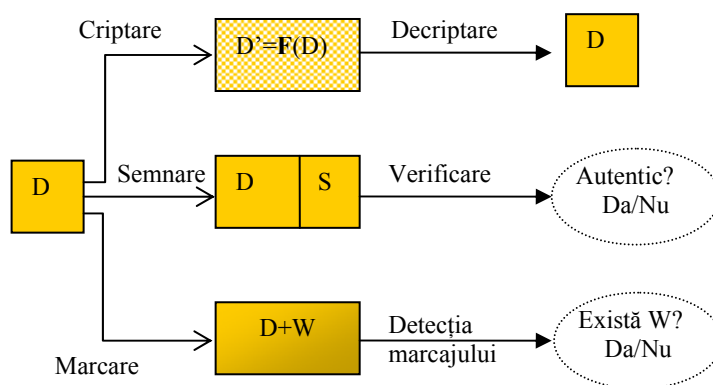


Fig.1.10: Reprezentare schematică a criptării datelor, verificarea autenticității și marcarea datelor.

A. *Marcare pentru protejarea dreptului de autor.* Marcajul (numit și etichetă pentru *copyright* sau ștampilă invizibilă în acest caz) conține informație specifică

proprietarului legal (de exemplu un *logo*) sau este un semnal aleator unic pentru respectivul proprietar. Protejarea se face în felul următor:

- Fiecare proprietar de *copyright* deține un număr unic (sau un set de numere) care constituie cheia privată a marcajului K_{pr} .
- Folosind cheia privată și un algoritm public sau privat, proprietarul dreptului de autor modifică datele digitale care sunt astfel marcate (este exclusă adăugarea de informații cum ar fi un antet sau altele).
- Folosind un algoritm de detecție, proprietarul de *copyright* poate verifica sau decoda modificările făcute de el însuși și poate folosi această informație ca un indicator al proprietății legale asupra respectivului produs.

B. Marcare pentru autentificare. Așa cum s-a spus în introducere, problema verificării autenticității produselor digitale se rezolvă cu ajutorul semnăturilor digitale. Autenticitatea este legată de un produs original de referință și de obicei are de-a face cu originalitatea conținutului, numele autorului, data la care produsul a fost creat, proprietarul dreptului de autor, etc. Marcajele se referă în principal la partea de autenticitate asociată cu originalitatea conținutului (termenii de integritate a datelor, verificarea conținutului sau dovada modificării datelor sunt de asemenea folosiți). Se schițează următoarea schemă de bază:

- Autorul original deține o cheie privată unică K_{pr} .
- Cu ajutorul unui algoritm ce folosește cheia privată, datele sunt modificate cu scopul de a îngloba informația de autenticitate. Algoritmul ar trebui să furnizeze și o cheie publică K_{pub} .

Receptorul poate să verifice autenticitatea produsului. El poate să-și folosească cheia publică K_{pub} și un algoritm public care furnizează un răspuns binar ce indică autenticitatea sau nu.

1.4 Aplicații posibile ale marcării transparente

Marcarea transparentă prezintă interes și pentru aplicații care nu țin de securizarea informațională [CMB02, LSL00, Bar03a, Bar03b].

1. *Monitorizarea transmisiilor TV:* dacă o firmă care își face publicitate, dorește să afle câte din reclamele plătite au fost efectiv transmise, poate să monitorizeze transmisiile TV cu ajutorul observatorilor umani. Desigur, acest lucru se poate dovedi extrem de costisitor și în plus nefiabil. Există de asemenea sisteme de monitorizare, care nu apelează la observatori umani. Acestea se împart în două categorii: pasive și active. Sistemele de monitorizare *pasive*, încearcă să recunoască direct conținutul difuzat, la fel ca și observatorii umani. Aceste sisteme sunt calculatoare care compară semnalul difuzat cu semnalele pe care le au în baza de date (și anume, semnalele care reprezintă spoturile publicitare). Aceste sisteme se pot dovedi nepractice, din cauza mărimii bazelor de date. În practică, aceste sisteme nu sunt folosite pentru a verifica dacă, de exemplu, o reclamă a fost difuzată. Ele sunt folosite mai ales pentru a obține date despre competitori.

Pentru a obține acuratețea cerută de procesul de verificare, ar trebui folosite sisteme de monitorizare *active*, care se bazează pe informații asociate difuzate o dată cu conținutul propriu-zis al reclamelor. Marcarea poate fi o soluție pentru monitorizarea activă a transmisiilor TV. Prin înserarea marcajelor în reclamele

comerciale, un sistem automat de monitorizare poate verifica dacă aceste reclame au fost difuzate conform contractului. Prin monitorizare pot fi protejate și alte produse TV valoroase, ca de exemplu cele mai recente știri. Sistemele de monitorizare a difuzării pot verifica toate canalele de difuzare și să taxeze stațiile TV conform constatărilor.

2. *Identificarea proprietarului*: acest lucru se poate face printr-o inscripționare vizibilă a autorului. Acest tip de „marcare” a proprietății poate însă fi ușor eliminat din semnalul multimedia respectiv. Cel mai bun exemplu în acest sens este decuparea unei porțiuni dintr-o imagine, care să nu conțină „marca” autorului. Deoarece marcajele pot fi imperceptibile și inseparabile de semnalul original, pot reprezenta o soluție ideală pentru identificarea autorului.

3. *Dovada proprietății*: ar fi de dorit ca marcajele să servească nu numai pentru a „marca” proprietatea, dar chiar să o dovedească. Dacă Alice creează o imagine și o marchează cu marca „© 2008 Alice”, atunci Bob poate fura imaginea respectivă, și folosind un program de procesare a imaginilor, poate înlocui marca cu „© 2008 Bob”. Dacă Alice nu a înregistrat imaginea la o autoritate centrală, ea va trebui să demonstreze că imaginea îi aparține. Dacă atacatorul nu dispune de un detector al marcajului, eliminarea acestuia poate fi greu de făcut. Pe de altă parte, chiar dacă marcajul nu poate fi eliminat, folosind propriul sistem de marcare, Bob poate să arate că marcajul lui ar exista în originalul lui Alice [CMYY98]. Astfel, o terță parte nu ar putea să își dea seama cui aparține imaginea.

Această problemă ar putea fi rezolvată dacă, în loc de a demonstra proprietatea prin marcare, s-ar demonstra că o imagine derivă din alta.

4. *Înregistrarea operațiilor efectuate* (transaction tracking) sau *amprentarea* (fingerprinting): pentru a urmări sursa copiilor ilegale, proprietarul poate folosi această tehnică, prin care se înserează marcaje diferite, în copiile livrate la clienți diferiți. Acest număr serial este de fapt asociat cu identitatea clientului și pot fi identificați acei clienți care încalcă convenția de licență, permițând copierea datelor de către o terță parte. Marcajul înregistrează una sau mai multe operații care au fost făcute asupra copiei unui produs multimedia. De exemplu, marcajul poate „memora” o identitate a cumpărătorului (se presupune că fiecare cumpărător are o copie diferită a originalului, marcajele nefiind aceleași).

5. *Autentificarea conținutului*: acest lucru poate fi realizat prin înglobarea *semnăturii digitale* în semnalul multimedia. Această semnătură mai este cunoscută și sub numele de marcă de autentificare. Dacă un semnal ce conține o astfel de marcă este modificat, se poate afla cum a fost distorsionat. Pentru verificarea autenticității datelor pot fi folosite marcaje fragile, care indică faptul că datele au fost sau nu alterate și localizarea alterării în caz că există.

6. *Controlul copierii* (copy control): prevenirea apariției copiilor ilegale poate fi făcută prin criptare. Există trei posibilități prin care un adversar poate obține acces neautorizat la produse multimedia: dacă decriptează datele fără a avea o cheie; dacă obține o cheie prin *reverse-engineering*; sau cel mai simplu dacă obține o cheie în mod legal, făcând copii ilegale ale datelor decriptate. Marcajele însă pot rămâne în conținut și după decriptare. Cu toate acestea, protejarea DVD-urilor împotriva copierii nu a fost făcută încă cu succes, deoarece nu orice DVD-player conține un detector al marcajului. Informația conținută în watermark poate controla direct dispozitivele de înregistrare, deoarece watermark-ul reprezintă un bit de interdicție a copierii; astfel, detectorul din dispozitiv stabilește automat dacă datele pot fi memorate sau nu.

Tehnicile de marcare sunt folosite și în alte scopuri [LSL00, AM05]:

7. *Indexarea* video-mail-urilor, a filmelor și a știrilor, în care pot fi introduse marcaje și comentarii care pot fi folosite de motoarele de căutare.

8. *Siguranța medicală*: înserarea în imaginile medicale a numelui și datelor personale ale pacientului.

9. *Ascunderea datelor* (data hiding): watermarking-ul poate fi folosit la transmiterea unor mesaje private secrete, deoarece unele guverne restricționează accesul la serviciile de criptare; astfel unele persoane pot să-și ascundă mesajele în alte date.

10. *Corectarea erorilor din transmisii video (tehnici ECDH)*: în comunicațiile video, algoritmi de detecție/corectare a erorii cu *data hiding* se axează pe recuperarea datelor pierdute în transmisii sau înlăturarea/ascunderea erorilor într-o manieră eficientă. La recepția semnalului video, informația înserată este folosită ca referință pentru a recupera mai bine pierderile.

1.5 Etapele marcării

După cum am văzut, principial marcarea transparentă constă din două prelucrări de bază desfășurate la emisie, respectiv la recepție:

-*introducerea marcajului*, cu respectarea cerințelor de *transparență perceptuală* și *robustețe*, în datele gazdă ce urmează a fi marcate;

-*extragerea marcajului* din semnalele marcate recepționate (posibil modificate) și compararea acestuia cu valoarea introdusă la emisie, în caz de dispută.

Pentru a îndeplini cerința de robustețe, marcajul introdus la emisie va depinde de una sau mai multe chei criptografice sigure (secrete sau publice), chei necesare și în procesul de detecție de la recepție.

Prima întrebare care se pune în legătură cu un sistem de marcarea transparentă sau unul steganografic este *ce marcaj alegem*, adică ce formă va lua mesajul ce va fi integrat. Cea mai simplă metodă ar fi de a integra un text într-o imagine, permițând imaginii să fie purtătorul direct al unor informații ca autor, titlu, dată, ș.a.m.d. Dezavantajul acestei abordări este însă că textul ASCII se poate considera într-un fel ca fiind o compresie LZW, în care fiecare literă este reprezentată de un anumit șablon de biți. Prin compresia marcajului înainte de integrare, robustețea are de suferit. Având în vedere natura codului ASCII, o eroare de un singur bit, în urma unui atac, poate schimba înțelesul aceluia caracter, și prin urmare și a mesajului. Ar fi simplu chiar și pentru o simplă compresie JPEG ca să reducă textul de copyright la o colecție aleatoare de caractere. De aceea informația se poate integra, în loc de caractere, într-o formă deja foarte redundantă, ca o imagine. Este de menționat faptul că în ciuda numărului mai mare de erori apărute la recuperarea marcajului, marcajul este încă de recunoscut.

Watermark

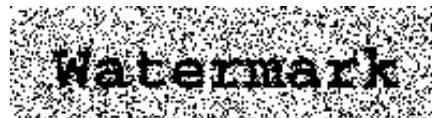


Fig. 1.11: Marcaj original, respectiv marcaj extras, cu 25% zgomot gaussian aditiv

În literatura de specialitate se pot întâlni diferite *definiții pentru marcaj* [VP99, CMB02, SK01]. Marcajele pentru imagini sunt tratate ca:

- i) manipulări ale biților celor mai puțin semnificativi, LSB, sau ai pixelilor;
- ii) rezultate ale aplicării unor coduri ascunse de marcare;
- iii) texturi invizibile;
- iv) rezultatele aplicării unor constrângeri secrete unor transformate ale imaginilor, etc.

Putem defini marcajul ca un semnal numeric W , care este suprapus pe produsele digitale printr-un proces de înglobare. Se poate descrie W ca un semnal cu componente binare sau, mai general, ternare [VP99]:

$$W = \left\{ w(\vec{k}); \left| w(\vec{k}) \in \{-1, 0, 1\}, \vec{k} \in \hat{W}^d \right. \right\} \quad (1.1)$$

unde \hat{W}^d este spațiul de date digital (matrice) al marcajului de dimensiune $d=1, 2, 3$ pentru audio, imagini fixe, respectiv video. Vectorul \vec{k} indică pozițiile elementelor matricii (coordonatele în spațiul \hat{W}^d).

1.5.1 Generarea marcajului. Fie W setul de semnale de marcare posibile. În conformitate cu teorema de existență a unei chei asociate, considerăm spațiul finit de chei K [VP99]. Dacă I este informația marcajului (*payload*), X este setul de imagini digitale fixe, atunci o metodă de generare a marcajului W ar trebui să fie definită de următoarea funcție:

$$G : I \times X \times K \rightarrow W, \quad W = G(I, X_0, K) \quad (1.2)$$

unde $K \in K$ este cheia de marcare și $X \in X$ este semnalul în care este înglobat marcajul. Pentru un anumit produs X și un semnal de marcare W , extragerea cheii ar trebui să fie imposibilă.

1.5.2. Înglobarea marcajului. Considerând semnalul de marcare $W = \{w(\vec{k})\}$, produs de G , procesul de înglobare a marcajului este definit ca o suprapunere a lui W peste produsul original $X_0 = \{x(\vec{k})\}$. Notăm procedura de înglobare prin \mathcal{E} și o definim după cum urmează:

$$\mathcal{E} : X \times W \times R \rightarrow X, \quad X_w = \mathcal{E}(X_0, W; l) \quad (1.3)$$

Parametrul l , care este o valoare reală, este asociat energiei de înglobare a marcajului sau, echivalent, vizibilității marcajului. În practică, în locul unui singur parametru l , este nevoie și de o mască de înglobare L pentru a atinge o înglobare satisfăcătoare. L este formată luând în considerare caracteristicile sistemelor vizual sau auditiv uman.

Figura 1.12 ilustrează procesul general de marcare descris de ecuația (1.3). Un marcaj, care de multe ori este alcătuit dintr-o secvență de biți, este inserat într-un semnal gazdă cu ajutorul unei chei [CMB02]. Procedul de înglobare impune

schimbări mici în semnal, determinate de cheie și de marcaj, pentru a genera semnalul marcat.

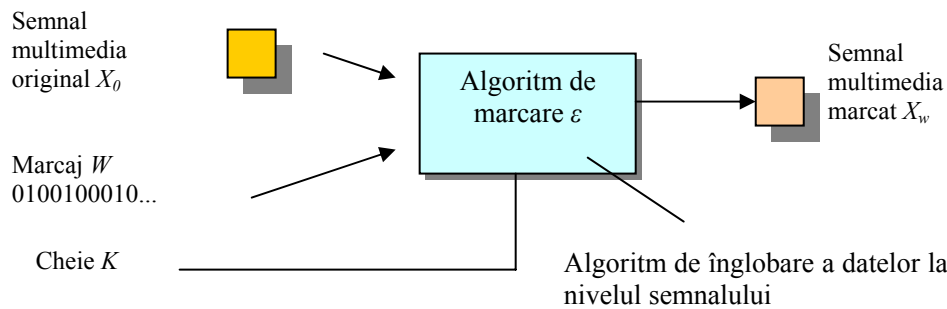


Fig. 1.12: Procesul de înglobare a marcajului. Marcajul este înglobat cu ajutorul unei chei, făcând schimbări imperceptibile în semnalul multimedia original.

Transparența perceptuală se realizează în concordanță cu un anumit criteriu de perceptibilitate care poate fi implicit sau explicit. Astfel, eșantioanele individuale ale semnalului gazdă, folosite pentru înserarea informației de marcaj, vor putea fi modificate numai între anumite limite situate sub pragurile de sensibilitate ale simțurilor umane (auz, văz). În cazul prelucrării imaginilor se obține o mască perceptuală care ne va spune cât de mult pot fi alterați anumiți pixeli, și care sunt aceștia, fără a afecta calitatea imaginii.

Un exemplu de mască perceptuală îl putem vedea în Figura 1.13 [PH99].

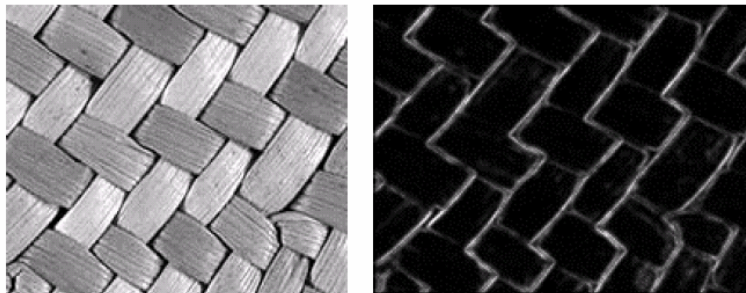


Fig. 1.13: a) imagine originală a unei țesături; b)masca perceptuală a țesăturii.

Insertia transparentă a marcajului în semnalul digital gazdă este posibilă numai datorită faptului că destinatarul final este omul. Simțurile sale sunt detectoare imperfecte caracterizate de praguri de sensibilitate (intensitate sonoră, respectiv nivel de contrast) minime precum și de fenomenul de *mascare*. Mascarea se referă la faptul că o componentă, dintr-un semnal dat, audio sau video, poate deveni imperceptibilă în prezența unui alt semnal, numit semnal de mascare. Majoritatea tehnicilor de codare ale semnalelor audio și video folosesc caracteristicile sistemului auditiv uman, HAS (Human Audio System) și ale sistemului vizual uman HVS (Human Visual System), direct sau indirect. Pentru ca semnalul de marcaj să fie robust (în ciuda amplitudinii mici a acestuia cerută de condiția de transparență), el este împrăștiat pe mai multe eșantioane în conformitate cu cerințele de granularitate, ceea ce conduce la detecția lui și din date marcate afectate de distorsiuni. Tehnica de împrăștiere este similară cu cea de întrețesere și este folosită pentru a preveni distrugerea semnificativă, sau chiar

înlăturarea marcajului în urma unor atacuri de *cropping*. Modul în care împrăștierea este efectuată depinde de cheia secretă, unică pentru fiecare marcaj în parte.

1.5.3 Căutarea pe Web. Copii ilegale ale produselor digitale sunt căutate pe paginile *web* accesibile și suspecte. De aceea, marcarea transparentă ar trebui combinată și cu o procedură automată de căutare pe *web*, notată cu S , care furnizează procedurii de detecție a marcajului produsele găsite pe un anumit domeniu.

$$X = S(\text{domeniu de retea}), \quad X \in \mathbf{X} \quad (1.4)$$

1.5.4. Detecția marcajului. Detectorul are la intrare un produs multimedia marcat sau nu și posibil distorsionat, precum și marcajul original. Răspunsul detectorului poate fi estimatul marcajului înglobat în semnalul multimedia \hat{W} , sau o valoare numerică care evidențiază prezența sau absența marcajului [CMYY98]. În al doilea caz, algoritmul de detecție este notat cu \mathcal{D} și definit după cum urmează [VP99]:

$$\mathcal{D}: \mathbf{X} \times \mathbf{K} \times \mathbf{W} \rightarrow \{0,1\}$$

$$\mathcal{D}(X, K, W) = \begin{cases} 1, & \text{daca } W \text{ exista in } X \\ 0, & \text{altfel} \end{cases} \quad (1.5)$$

Detecția marcajului ar trebui să fie făcută fără a recurge la produsele originale. Folosirea originalelor poate genera un volum mare de calcul. Se generează mai întâi marcajul folosind \mathcal{G} , bazat pe produsul X , care urmează a fi verificat și pe cheia K . Procesul de detecție și extragere al marcajului este ilustrat în Figura 1.14.

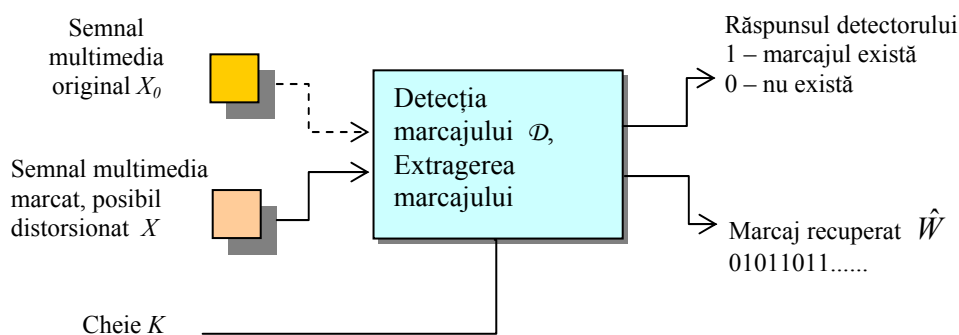


Fig. 1.14: *Detecția marcajului, fără, sau cu semnalul multimedia original.*

Detectorul informat este cel care recurge la semnalul multimedia original pentru a verifica existența marcajului într-un semnal multimedia primit, care poate fi o versiune distorsionată a semnalului multimedia marcat [CMB02]. Dacă el nu are nevoie de semnalul original, detectorul este neinformați (*blind*). Cele două sisteme se numesc sistem de marcarea *privat*, respectiv *public*.

În practică, realizarea lui \mathcal{D} implică următoarele erori:

- tipul I de eroare: marcajul este detectat, deși nu există (*fals pozitiv*).
- tipul II de eroare: marcajul nu este detectat, deși există (*fals negativ*).

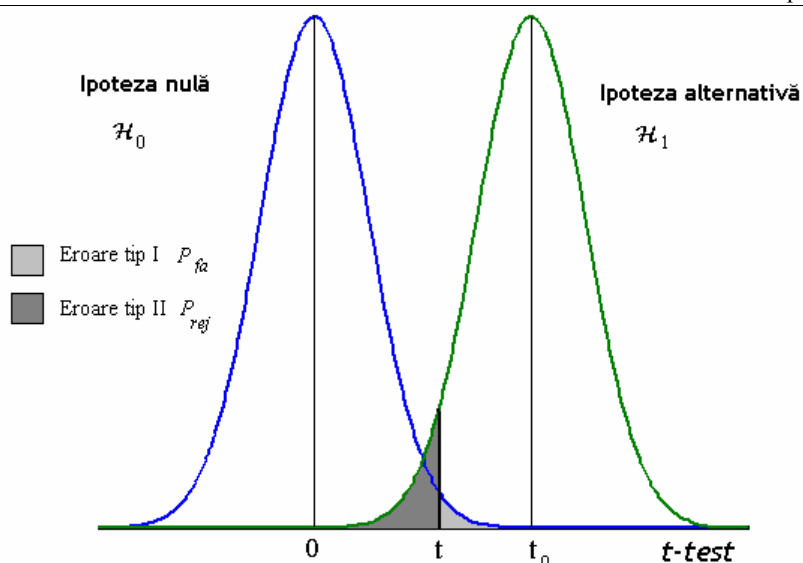


Fig. 1.15: Detecția marcatului prin statistica t-test.

Ipotezele nulă și alternativă reprezintă probabilitățile de inexistență sau de existență a marcatului. Erorile de tip I și II sunt diferite de zero pentru orice valoare a lui t , derivată din t-test [Kay93].

Erorile enunțate mai sus apar cu probabilitățile de alarmă falsă, P_{fa} , respectiv de rejecție, P_{rej} . Ideea este de a minimiza P_{fa} . Pentru a avea un detector optimal, trebuie minimizată cealaltă eroare P_{rej} , sau echivalent de a maximiza $1 - P_{rej}$. Dar aceasta este chiar probabilitatea detecției, P_D , și este criteriul Neyman-Pearson de testare a ipotezelor, adică în acest caz de detecție a semnalelor. Dacă:

$$P_D = 1 - P_{rej} \quad (1.6)$$

este probabilitatea detecției corecte, atunci intenția este de a maximiza P_D , pentru un prag P_{fa} impus [Kay93]. Testarea ipotezelor poate fi folosită pentru estimarea statistică a certitudinii și a manipulării erorii. În general, când probabilitatea unui fals pozitiv devine nesemnificativă ($P_{fa} \rightarrow 0$), probabilitatea de a rejecta un marcaj crește ($P_{rej} \rightarrow 1$) și invers. Această situație este ilustrată în Figura 1.15 unde este considerată statistica t-test.

1.5.5 Căutarea în baze de date. Furnizorii și creatorii își memorează produsele într-o bibliotecă personală notată cu \mathcal{L} . Dându-se un produs X , furnizorul ar trebui să fie capabil să găsească o metodă de potrivire/căutare \hat{m} cu scopul de a verifica dacă X este sau nu inclus în biblioteca sa \mathcal{L} .

$$\hat{m}(X, \mathcal{L}) = \begin{cases} 1, & \text{dacă } X \in \mathcal{L} \\ 0, & \text{în rest} \end{cases} \quad (1.7)$$

O procedură de *matching* (identificare) este bazată, în general, pe algoritmi foarte complecși. De aceea, nu este nici convenabil și nici fezabil să se aplice procedura \hat{m} tuturor produselor de pe domeniile web din sfera de interes. Procedura

\hat{m} este folosită pentru a confirma proprietatea asupra unui produs, atunci când detecția marcajului se face cu un nivel de certitudine mic, dar nu neglijabil.

1.6 Proprietățile principale ale metodei de marcare

Așa cum am văzut, marcajele sunt structuri invizibile înglobate în *semnalul gazdă* pentru a „marca” proprietatea [KH98]. Din cadrul marcajelor fac parte codurile de *copyright* sau de autentificare, sau „legende”, care sunt absolut necesare pentru interpretarea semnalului. Aceste marcaje, existente în semnalul multimedia, trec neobservate de obicei și pot fi depistate doar cu un detector adecvat. Cele mai răspândite tipuri de semnale care se marchează sunt imaginile statice, semnalele audio și semnalele video numerice. În cele ce urmează, ne vom referi mai ales la *imagini statice*, aceleași principii putându-se aplica și celorlalte tipuri de date.

1.6.1 Condiții generale impuse marcării.

Fiecare aplicație de marcare transparentă își are cerințele ei specifice. De aceea, nu există un set anume de cerințe care să satisfacă toate tehnicile de marcare transparentă. Totuși, pentru majoritatea aplicațiilor menționate mai sus, pot fi date niște cerințe generale [VP99, CKLS97, NP98, LSL00]:

- *Transparența perceptuală (imperceptibilitatea)*: în majoritatea aplicațiilor, algoritmul de marcare transparentă trebuie să plaseze marcajul transparent în așa fel încât acesta să nu afecteze calitatea datelor gazdă. Un marcaj transparent este într-adevăr imperceptibil, dacă observatorii umani nu pot distinge datele originale de datele marcate transparent. Totuși, chiar și cea mai ne semnificativă modificare în datele gazdă poate deveni vizibilă atunci când datele originale sunt comparate direct cu datele marcate transparent. În mod normal, utilizatorii nu au acces la datele originale și nu pot efectua această comparație. De aceea poate fi suficient ca modificările din imaginea marcată transparent să treacă neobservate, atâta timp cât datele nu sunt comparate cu cele originale.
- *Încărcătura marcajului transparent*: cantitatea de informație care poate fi stocată într-un marcaj transparent depinde de aplicație. În scopul protejării la copiere, încărcătura de un singur bit este de obicei suficientă. Pentru protejarea drepturilor proprietății intelectuale, pare rezonabil să presupunem că se dorește plasarea unei cantități de informație similară cu cea folosită pentru ISBN, International Standard Book Numbering, (10 cifre) sau ISRC, International Standard Recording Code (12 caractere alfanumerice). La toate acestea, trebuie adăugat și anul copyrightului, modificările permise asupra materialului, și clasificarea acestor modificări. Aceasta înseamnă că aproximativ 60 de biți de informație ar trebui să fie plasați în datele gazdă, imaginea, materialul video, sau fragmentul audio.
- *Granularitatea marcajului transparent* este un alt concept important cu privire la încărcătura marcajului transparent pentru date audio-video digitale. Fărămițarea marcajului transparent reprezintă cantitatea de informație necesară pentru plasarea unei unități de informație de marcaj. Folosind exemplul de mai sus, o unitate de informație de marcaj constă din 60 sau 70 de biți. Aceștia ar putea fi plasați într-un singur cadru video, sau împrăștiați, de exemplu, asupra a 100 de cadre video.

- *Robustețea*: un marcaj transparent fragil care trebuie să demonstreze autenticitatea datelor gazdă, nu trebuie să fie robust împotriva tehnicilor de procesare sau alterărilor intenționate asupra datelor gazdă, deoarece eșecul detecției marcajului transparent demonstrează că datele gazdă au fost modificate și nu mai sunt autentice. Totuși, dacă un marcaj transparent este folosit pentru altă aplicație, este de dorit ca marcajul transparent să rămână întotdeauna în datele gazdă, chiar și atunci când calitatea datelor gazdă a fost degradată, intenționat sau neintenționat. Exemple pentru degradări neintenționate sunt aplicațiile care implică transmisia sau stocarea de date, unde sunt folosite tehnici de compresie cu pierderi de date, pentru a reduce rata de bit și a crește eficiența. Alte tehnici de prelucrare care degradează calitatea datelor în mod neintenționat, includ filtrarea, re-eșantionarea, conversia analog-digitală și digital-analogică. Pe de altă parte, marcajul transparent poate fi subiectul unor procesări cu intenția de a-l elimina. Când există multe copii al aceluiași conținut, cu marcaje transparente diferite, ca în cazul amprentării, este posibilă eliminarea marcajului transparent datorită coliziunii dintre mai multe copii diferite. În general, nu ar trebui să existe nici o cale prin care marcajul transparent să fie eliminat sau modificat, fără degradarea suficientă a calității percepțuale a datelor gazdă.
- *Securitatea* tehnicilor de marcare transparentă poate fi interpretată în același mod ca și securitatea tehnicilor de criptare. O tehnică de marcare transparentă este sigură, dacă cunoașterea exactă a algoritmului de plasare și extragere a marcajului transparent nu ajută o persoană neautorizată în detectarea prezenței marcajului și eliminarea ei.
- *Marcare publică și marcare privată (oblivious/blind versus nonoblivious/non-blind)*: în unele aplicații, ca protecția copyright și monitorizarea datelor, algoritmi de extragere a datelor pot folosi imaginea originală nemarcată pentru a găsi marcajul transparent. Acest procedeu este numit marcare transparentă privată (nonoblivious watermarking). În majoritatea aplicațiilor, cum ar fi protecția la copiere și indexarea, algoritmi de extragere a marcajului transparent nu au acces la imaginea originală, nemarcată. Acest lucru îngreunează extragerea marcajului transparent. Algoritmi de marcare transparentă de acest fel sunt publici (oblivious).
- *Universalitatea*: același algoritm de marcare transparentă ar trebui să fie aplicabil pentru toate cele trei tipuri de date considerate. Acest lucru servește în marcarea produselor multimedia. De asemenea, această caracteristică este favorabilă pentru implementarea de algoritmi de marcare a imaginilor și semnalelor video pe suport hardware comun.
- *Neambiguitatea*: recuperarea marcajului ar trebui să identifice fără îndoială proprietarul. De asemenea, acuratețea identificării proprietarului ar trebui să se degradeze progresiv cu creșterea forței atacurilor.

Alte proprietăți pe care marcajele ar trebui să le aibă sunt [VP99]:

- *Complexitatea*: semnalele de marcare ar trebui să fie foarte complexe. Acest lucru este necesar pentru a se putea produce un set suficient de marcaje sesizabile. Un set foarte mare de marcaje previne refacerea unui marcaj anumit, prin proceduri iterative de tip *trial and error*. În majoritatea cazurilor, complexitatea unei marcaje este direct legată de mărimea produsului în care trebuie să fie înglobată.

- *Cheia asociată*: marcajele ar trebui să fie asociate cu un număr de identificare numit cheia marcajului. Cheia este folosită pentru a forma, detecta și înlătura marca. Prin urmare, cheia ar trebui să fie privată și să caracterizeze exclusiv proprietarul legal. Orice semnal digital extras dintr-un produs digital se presupune că este marcajul dacă și numai dacă el este asociat cu o cheie printr-un algoritm bine stabilit. Această condiție previne crearea unor marcaje contrafăcute, discutate de Craver pe larg în [CMYY98].
- *Deteția/căutarea automată*: marcajele ar trebui să combine în mod facil o metodă de căutare care scanează automat orice domeniu accesibil în rețea.
- *Deteția de încredere*: marcajele ar trebui să constituie o dovadă suficientă și de încredere a proprietății asupra unui anumit produs. Alarmerile false ar trebui să apară foarte rar, de preferință niciodată. Un anumit marcaj este o dovadă credibilă pentru a demonstra posesia dreptului de autor atunci când probabilitatea de eroare la deteție este nesemnificativă. Totuși, deteția cu un nivel de certitudine scăzut poate fi făcută cu scopul de a reduce probabilitatea de refuz P_{rej} în timpul monitorizării pe web.
- *Invizibilitatea statistică*: marcajele nu ar trebui să poată să fie refăcute folosind metode statistice. De exemplu, proprietatea unui număr mare de produse digitale, marcate cu aceeași cheie, nu ar trebui să permită extragerea marcajului aplicând metode statistice. De aceea, marcajele ar trebui să depindă de conținutul produsului.
- *Marcajele multiple*: ar trebui să fim capabili să înglobăm un număr suficient de marcaje în aceeași imagine. Fiecare marcaj ar trebui să fie detectabil folosind cheia unică corespunzătoare. Această caracteristică pare să fie necesară, deoarece nu putem preveni ca cineva să marcheze un produs deja marcat. Este de asemenea avantajos în cazurile în care dreptul de autor este transferat de la un proprietar la altul (un proces asemănător celui de amprentare). Menționăm că proprietarul legal al imaginii este singurul care poate dispune de o copie a imaginii care conține doar marcajul său.

Cerințele de mai sus sunt legate una de alta. De exemplu, poate fi obținut un marcaj transparent foarte robust prin modificări mari asupra datelor gazdă, pentru fiecare bit al marcajului transparent. Totuși, modificările mari în datele gazdă sunt observabile, și multe modificări la biții de marcaj, vor limita cantitatea maximă de biți ai marcajului transparent care pot fi stocați în obiectul gazdă. Deci, trebuie considerat un compromis între diferitele cerințe, astfel putând fi dezvoltat un marcaj transparent optim pentru fiecare aplicație.

Dependențele mutuale dintre cerințele de bază sunt arătate în figura 1.16. Relația dintre cerințele de bază pentru un marcaj transparent sigur, bine proiectat, sunt prezentate în figura 1.17.

Axa de impact perceptual reprezintă degradarea calității datelor din cauza marcării transparente. Cu cât este mai mare impactul perceptual, cu atât este mai gravă degradarea calității. Axa încărcăturii reprezintă cantitatea de date care poate fi plasată în date. Axa robusteții reprezintă capacitatea sistemului de marcarea transparentă de a rezista la atacuri. Securitatea unui marcaj transparent influențează enorm robustețea. Dacă un marcaj transparent nu este sigur, nu poate fi foarte robust.

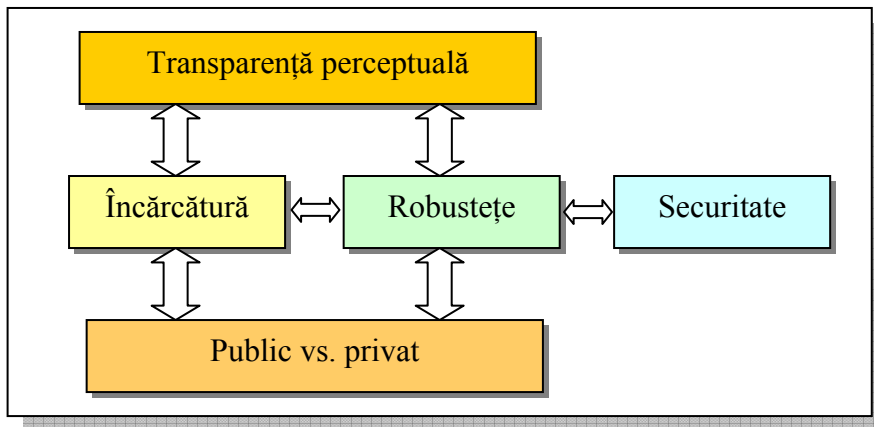


Fig. 1.16: Interdependențele dintre cerințele de bază pentru un marcaj eficient

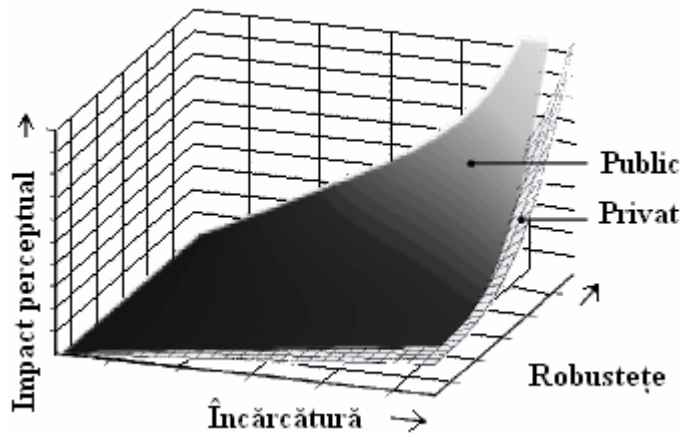


Fig. 1.17: Relația dintre cerințele de bază pentru un marcaj sigur

1.6.2 Condiții specifice impuse marcării

A. *Protecția dreptului de autor.* Pentru a fi eficient, marcajul trebuie să fie dificil, teoretic imposibil de înlăturat. Dacă se dispune doar de o informație parțială despre marcaj (de exemplu, nu se cunoaște cu exactitate localizarea marcajului în imagine), atunci încercările de înlăturare sau de distrugere a marcajului ar trebui să conducă la degradarea severă a calității imaginii. Evident, un marcaj folosit cu scopul de protejare a dreptului de autor ar trebui să fie detectabil, până în punctul în care calitatea produsului rămâne în limite acceptabile pentru orice tip de modificare. În particular, un marcaj ar trebui să fie robust la:

- a. *Prelucrări obișnuite ale semnalului:* marcajul ar trebui să poată fi încă extras, chiar dacă imaginii i se aplică procesări obișnuite. Acestea pot fi conversii D/A, A/D, reșantionare, compresie cu pierderi, precum și îmbunătățiri obișnuite aplicate unei imagini cum ar fi îmbunătățirea contrastului, corecția culorilor, egalizarea histogramei etc.

- b. *Distorsiuni geometrice obișnuite (pentru imagini și video)*: marcajele din imagini și video ar trebui să fie rezistente și la operații geometrice cum ar fi rotire, translație, decupare, scalare.
- c. *Atacuri de subterfugiu (prin înțelegere secretă/complot și falsificare)*: marcajul ar trebui să fie robust împotriva atacului combinat, lansat de mai mulți indivizi care posedă fiecare o copie marcată. Cu alte cuvinte, marcarea ar trebui să fie robustă împotriva combinării copiilor aceluiași original. De asemenea, dacă un marcaj urmează să fie folosit ca probă juridică, trebuie să fie imposibil pentru atacatori să combine imaginile lor pentru a genera un marcaj diferit, valid, cu intenția de a înșela o terță parte.

B. Verificarea conținutului. Protecția originalității conținutului cere o invizibilitate perceptuală, complexitate a marcajului, validitate a cheii, detecție de încredere și invizibilitate statistică. În aplicațiile în care trebuie detectate cele mai neînsemnate modificări făcute asupra produselor în care au fost înglobate sunt cerute marcaje *fragile*. În cazurile în care modificările nu afectează autenticitatea este dorită *robustețea*, adică:

1. *Compresia mare*
2. *Înlăturarea părților neinteresante*
3. *Alte modificări ne semnificative*, făcute pentru a introduce produsul într-un mediu multimedia.

1.7 Marcare și înregistrare pentru o protecție eficientă

Tehnicile de marcarea dezvoltate până astăzi, prezintă diferite dezavantaje care împiedică formarea unui sistem de protecție universal, de încredere, bazat exclusiv pe marcarea. Principalele dezavantaje sunt [VP99]:

1-Instabilitatea în raport cu pierderea/furtul cheii : marcarea se bazează pe o cheie privată constantă. Când un atacator află sau găsește o cheie privată, el are posibilitatea să înlătore marcajele corespondente cheii respective din toate produsele în mod direct. Ulterior, violarea dreptului de autor pentru toate produsele furnizorului respectiv devine o sarcină ușoară. De asemenea, pot fi distribuite produse falsificate.

2-Robustețe/fragilitate eficientă: marcajele folosite pentru protecția dreptului de autor ar trebui să fie robuste la toate modificările posibile. De asemenea, verificarea conținutului necesită marcaje cu o fragilitate adecvată față de o varietate de procesări. Cererile de mai sus nu se ating cu ușurință.

3-Eficiența marcajului împotriva tehnicilor noi de procesare sau atacuri: este testată robustețea marcajului, securitatea și rezistența lui la atacuri pentru tehnicile de procesare cunoscute până în prezent. Marcarea nu poate să își garanteze eficiența. În viitor ar putea fi dezvoltate noi tehnici de compresie sau de filtrare, care să înlătore cu ușurință marcajele din produsele deja distribuite.

4-Detecția publică nesigură: detecția marcajului folosind chei publice este esențială pentru verificarea conținutului. Totuși, detecția publică poate crea dificultăți în dezvoltarea tehnicilor de marcarea sigure și eficiente împotriva atacurilor pirat. Din cauza problemelor menționate anterior, marcarea nu poate asigura singură o protecție eficientă. Totuși, ea poate constitui o parte importantă a unei metode de ansamblu de protecție.

Înregistrarea produselor la o autoritate de încredere este o cale bine cunoscută pentru protejarea drepturilor de proprietate intelectuală (pentru cărți, software, etc). Informațiile de înregistrare pot fi folosite ca o dovadă inatacabilă a proprietății și drepturilor legale. Un sistem de protecție bazat pe înregistrarea produsului necesită următoarele acțiuni:

1. Furnizorul este o autoritate de încredere, care furnizează o cheie de marcare unică.
2. Înglobarea marcajului se face folosind cheia înregistrată.
3. Produsul marcat este înregistrat la autoritatea de încredere înainte de a fi distribuit.

Copia înregistrată este datată, fiind marcate atât originalitatea cât și proprietatea legală. Înregistrarea după marcare poate contribui la o protecție eficientă în diferite moduri. Se pot observa următoarele:

- Furnizorul face o căutare automată a marcajului în rețea. Când se folosește un nivel de certitudine scăzut, siguranța unui rezultat pozitiv este refăcută căutând în biblioteca \mathcal{L} . Deținerea unei copii înregistrate este dovada proprietății dreptului de autor, în fața justiției.
- Verificarea conținutului poate fi făcută de autoritatea de înregistrare și de un server public destinat acestui scop. Utilizatorul care dorește să își verifice conținutul unui produs, ar trebui să acceseze acel server particular, la care produsul a fost înregistrat. Serverul poate verifica integritatea conținutului făcând o marcare privată și apoi trimițând rezultatul către utilizator.

1.8 Modele de bază pentru watermarking

Dezvoltarea unei tehnici de marcare ia în considerare mai multe aspecte. Multe dintre tehnicile existente „împrumută” concepte din alte domenii de cercetare.

Figura 1.18 prezintă câteva din elementele avute în vedere de o tehnică de marcare. Alegerea acestor elemente pentru o metodă de marcare, pentru o aplicație dată, este încă neclară, deoarece pentru anumite aplicații, trebuie făcut un compromis între imperceptibilitate, robustețe și complexitate.

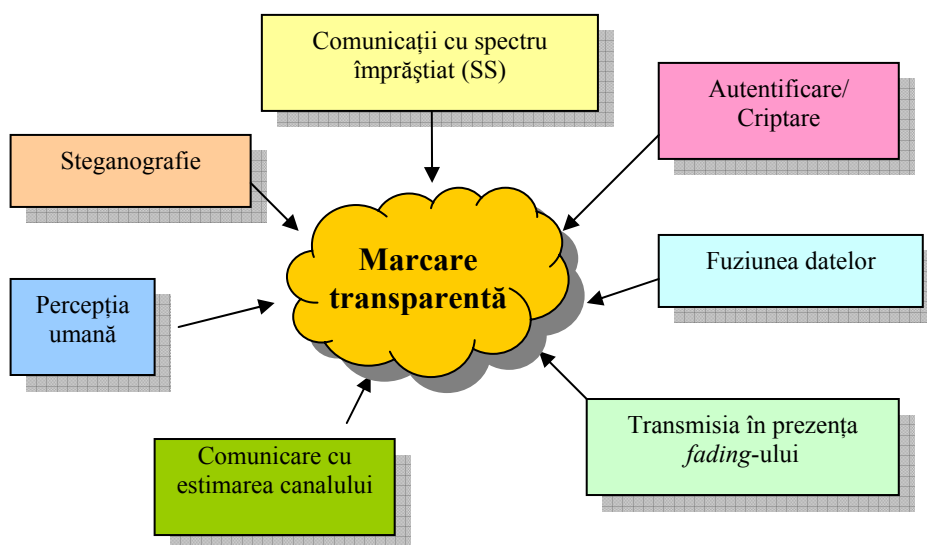


Fig. 1.18: Domeniile de cercetare care sunt în strânsă legătură cu marcarea semnalelor multimedia.

În cele ce urmează, se enumeră câteva domenii care au contact cu marcarea transparentă [Kun99].

1. *Steganografia* se referă la modul de comunicare ascunsă (*data hiding*). Problema principală este mascarea unui mesaj secret în orice tip de semnal gazdă (nu numai multimedia). Marcarea numerică și steganografia se aseamănă foarte mult, exceptând faptul că în tehnicile de marcare, se pune accent pe robustețea sau fragilitatea marcajului [CMB02].
2. *Comunicațiile cu spectru împrăștiat* (*Spread Spectrum - SS*) sunt extrem de asemănătoare cu marcarea transparentă. Procedura de înglobare a marcajului se aseamănă cu transmiterea unui semnal SS (marcaj) printr-un mediu zgomotos (semnalul gazdă). Extragerea marcajului este echivalentă cu detecția semnalului SS dintr-un mediu cu interferențe [CKLS97].
3. *Modelele perceptuale umane* sunt des folosite pentru codarea perceptuală a semnalelor multimedia. Se exploatează proprietatea de mascare a percepției umane, permițându-se astfel o introducere mai eficientă a marcajului. Astfel, se îmbunătățește robustețea marcajului sau estimarea modificărilor făcute asupra semnalului [CMB02].
4. *Autentificarea și criptarea* se folosesc în strânsă legătură cu tehnicile de marcare, într-un sistem de protecție universal. De altfel, sistemele de marcare împrumută deseori modelele folosite în criptare, realizând o înglobare elegantă [VP99, CMB02, BB01].
5. *Fuziunea datelor* este o problemă fundamentală de compresie a informației, în care mai multe semnale sunt „adunate” pentru a forma unul singur, conținând informația cea mai relevantă de la fiecare din semnalele respective. Această problemă se aseamănă cu problema marcării, în care semnalul original și semnalul de marcaj formează semnalul marcat, care trebuie să rețină proprietățile perceptuale ale semnalului gazdă, dar și informația marcajului [ZWL03, CM98].
6. *Transmisia semnalului în prezența fading-ului* este o problemă care se referă la comunicații fără fir, ce implică folosirea unor strategii pentru a combate atenuarea semnalului în timp [KH01]. În acest context, robustețea marcajului poate fi considerată capacitatea lui de a rezista interferențelor într-un canal cu *fading*.
7. *Estimarea canalului* este necesară în orice sistem de comunicații. Combaterea efectelor distorsiunilor canalelor este cu atât mai eficientă, cu cât sunt mai corecte și exacte modelele de canale propuse, conform unor estimări prealabile. Caracterizarea atacurilor înainte de extragerea marcajului poate îmbunătăți simțitor performanța unui sistem de marcare [KH01]. Pentru sistemele de marcare fragile, caracterizarea atacurilor se folosește pentru a evalua credibilitatea semnalului modificat; pentru

sisteme de marcare robuste, caracterizarea atacurilor se folosește pentru a crește credibilitatea estimării marcajului.

1.9 Evaluarea performanțelor unei metode de marcare

Un algoritm de marcare este evaluat printr-o serie de măsurări. Din cauza aspectului subiectiv al problemei, nu toate criteriile de evaluare sunt cantitative. Se prezintă în cele ce urmează cele mai folosite criterii de evaluare pentru imagini.

1. *Imperceptibilitatea*. Marcajul nu ar trebui să fie vizibil, respectiv supărător [CKLS97]. Cu alte cuvinte, un utilizator nu ar trebui să fie capabil să facă distincția între semnalul marcat și cel original.
2. *Raportul dintre puterea maximă a semnalului și puterea zgomotului (Peak Signal-To-Noise Ratio PSNR)*. Pentru a stabili un criteriu mai obiectiv al imperceptibilității, este folosit și PSNR pentru a măsura „zgomotul” adăugat imaginii originale, ca rezultat al înglobării marcajului. Deși această măsură nu este totdeauna cea mai potrivită, ea poate fi folositoare pentru a indica echilibrul între invizibilitatea marcajului și eficiența procesului de „ascundere” a datelor. PSNR se definește astfel:

$$PSNR(f, w) = 10 \log_{10} \left[\frac{\max_{\forall(m,n)} f^2(m, n)}{\frac{1}{N} \sum_{\forall(m,n)} (f_w(m, n) - f(m, n))^2} \right] \quad (1.8)$$

unde f este semnalul gazdă, f_w este semnalul marcat, w este marcajul, (m, n) reprezintă localizarea unui anumit pixel, iar N este numărul de pixeli din f sau f_w . PSNR se măsoară în dB.

3. *Coeficientul de intercorelație*. Pentru a măsura similaritatea între marcajele original și extras, se calculează coeficientul normalizat de intercorelație [CMB02, ZWL03, CMYY98]:

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^{N_w} w(i) \hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w} w^2(i)} \sqrt{\sum_{i=1}^{N_w} \hat{w}^2(i)}} \quad (1.9)$$

unde $w(i)$ și $\hat{w}(i)$ reprezintă semnalele de marcare original și, respectiv extras; N_w este lungimea marcajului. O metodă de marcare robustă încearcă să maximizeze acest coeficient de intercorelație, atunci când semnalul este distorsionat, iar o metodă de marcare fragilă încearcă să îl minimizeze, în cazul unor modificări majore.

4. *Distanța Hamming normalizată*. Dacă marcajul este alcătuit din elemente binare, pentru a măsura similaritatea dintre cele două marcaje, se poate calcula

distanța Hamming normalizată dintre marcajele original și extras [CMB02], în loc de coeficientul de intercorelație. Aceasta este dată de următoarea relație:

$$\rho_{\text{HD}}(w, \hat{w}) = \frac{1}{N_w} \sum_{i=1}^{N_w} w(i) \oplus \hat{w}(i) \quad (1.10)$$

unde w , \hat{w} și N_w sunt definite la fel ca și în ecuația (1.2), iar operatorul \oplus este SAU-EXCLUSIV (XOR).

5. *Probabilitatea unui fals pozitiv sau negativ.* În aplicațiile de securitate informațională, este necesară detecția marcajului sau detecția oricărui tip de modificare făcută cu scopul de a-l înlătura. Probabilitatea ca marcajul sau modificarea semnalului marcat să nu fie detectate se numește *probabilitatea unui fals negativ*. Asemănător, probabilitatea ca un marcaj să fie detectat, când el nu există se numește *probabilitatea unui fals pozitiv* [VP99, CMB02].
6. *Complexitatea de calcul.* În funcție de aplicația cerută, complexitatea de calcul poate fi un factor semnificativ în estimarea performanțelor unui algoritm de marcarea [CMB02]. De exemplu, extragerea marcajului la un DVD-player trebuie realizată în timp real, dar în marcarea imaginilor pentru protejarea proprietății intelectuale, acest fapt poate să nu aibă o importanță foarte mare.

1.10 Marcarea robustă

Robustețea se referă la capacitatea marcajului de a fi recuperat după procesări de semnal obișnuite și depinde de aplicație. Astfel de procesări pot fi: compresia cu pierderi, conversia numerică, atacul de imprimare și scanare (*printing and scanning*), înregistrarea analogică (casete VHS), reducerea zgomotului, conversia dintr-un format în altul (exemplu trecerea de la NTSC la PAL). Robustețea este limitată de o serie de parametri, dintre care cei mai importanți sunt costul de calcul al algoritmului de marcarea, încărcătura marcajului (*payload*) și fidelitatea impusă semnalului marcat față de cel original.

Spre exemplu în aplicația de monitorizare a transmisiilor TV (*broadcast monitoring*) marcajul trebuie să fie robust la conversii D-A și A-D, compresie cu pierderi, jitter, dar nu este necesar să fie robust la rotație, înregistrare analogică, conversie dintr-un format în altul. De asemenea costul erorilor diferă în aplicații: costul de fals negativ este mare pentru broadcast monitoring, în timp ce costul de fals pozitiv este mare pentru controlul copierii (copy control).

1.10.1 Problema detecției optime

Dacă se ia un exemplu simplu, de sistem de marcarea [CMB02], în care c_0 este imaginea originală, w - marcajul, α - intensitatea marcajului, imaginea marcată va fi:

$$\mathbf{c}_w = \mathbf{c}_0 + \alpha \mathbf{w} . \quad (1.11)$$

Fiind dată imaginea posibil marcată \mathbf{c} , și \mathbf{c}_0 imaginea originală, se extrage marcajul

$$\mathbf{w}_n = \mathbf{c} - \mathbf{c}_0 \approx \alpha \mathbf{w} \text{ dacă marcajul este prezent .}$$

Se poate folosi corelația liniară pentru a determina dacă $\mathbf{w}_n \cong \alpha \mathbf{w}$:

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) = \frac{1}{N} \mathbf{w}_n \cdot \mathbf{w} = \frac{1}{N} \sum_{x,y} \mathbf{w}_n[x,y] \cdot \mathbf{w}[x,y], \quad (1.12)$$

unde N este numărul de pixeli din imagine.

Imaginea originală, posibil afectată de zgomot AWGN, este:

$$\mathbf{c} = \mathbf{c}_0 + \mathbf{n} \quad (1.13)$$

Dacă marcajul nu este prezent în imaginea originală, atunci valoarea corelației liniare devine:

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) \cong 0 ,$$

iar dacă marcajul este prezent, și imaginea marcată a fost afectată de zgomot:

$$\mathbf{c}_w = \mathbf{c}_0 + \alpha \mathbf{w} + \mathbf{n} .$$

Atunci

$$z_{lc}(\mathbf{w}_n, \mathbf{w}) = \alpha z_{lc}(\mathbf{w}, \mathbf{w}) \text{ (marcajul este prezent).}$$

Dacă \mathbf{w} este ales astfel încât corelația între \mathbf{c}_0 și \mathbf{w} este apropiată de 0 (\mathbf{w} este zgomot alb), atunci $z_{lc}(\mathbf{c}, \mathbf{w}) \cong z_{lc}(\mathbf{w}_n, \mathbf{w})$. Prin urmare detecția se poate face și *neinformată* (fără a cunoaște imaginea originală).

Fie spațiul media un spațiu multidimensional, în care fiecare imagine are asociat un punct, iar pentru simplitate se poate considera că acesta are doar două dimensiuni. Corelația liniară este produsul scalar între \mathbf{c} și \mathbf{w} scalat cu $1/N$, adică:

$$z_{lc}(\mathbf{c}, \mathbf{w}) = \frac{1}{N} \mathbf{c} \cdot \mathbf{w} = \frac{1}{N} |\mathbf{c}| \cdot |\mathbf{w}| \cos \angle(\mathbf{c}, \mathbf{w}) \quad (1.14)$$

Dacă $|\mathbf{w}| = 1$, atunci corelația liniară este chiar proiecția lui \mathbf{c} pe direcția lui \mathbf{w} .

Prin urmare, dacă se compară $z_{lc}(\mathbf{c}, \mathbf{w})$ cu un prag, se ajunge la o regiune de detecție de tip plan [CMB02, Cox05].

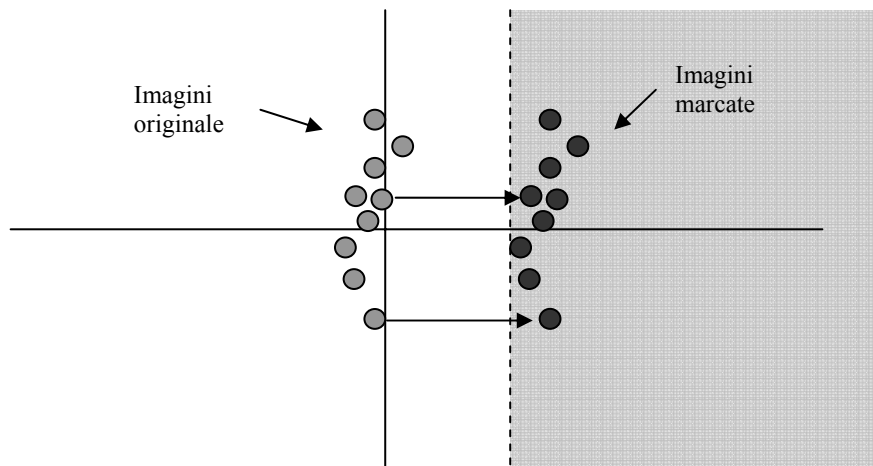


Fig. 1.19: Interpretarea geometrică a corelației liniare.

Zgomotul AWGN. Dacă imaginea este coruptă de zgomot AWGN,

$$\mathbf{c}_{wn} = \mathbf{c}_w + \mathbf{n}$$

atunci corelația liniară (filtrare adaptată) este optimală după criteriul Neyman-Pearson [Kay93]:

$$z_{lc}(\mathbf{w}, \mathbf{c}_{wn}) = \frac{1}{N}(\mathbf{w} \cdot \mathbf{c}_w + \mathbf{w} \cdot \mathbf{n}) \quad (1.15)$$

Contrastul imaginii. Dacă se schimbă contrastul imaginii, atunci imaginea devine $\mathbf{c}_{wn} = v\mathbf{c}_w$, unde v este o valoare reală. Rezultă corelația liniară :

$$z_{lc}(\mathbf{c}_{wn}, \mathbf{w}) = v z_{lc}(\mathbf{c}_w, \mathbf{w}) \quad (1.16)$$

Dacă $v < 1$ valoarea corelației poate scădea sub valoarea de prag. Pentru creșterea probabilității de detecție, se poate recurge la corelația normalizată:

$$z_{nc}(\mathbf{c}, \mathbf{w}) = \frac{\mathbf{c} \cdot \mathbf{w}}{|\mathbf{c}| \cdot |\mathbf{w}|} \quad (1.17)$$

Atunci, ajustarea contrastului nu are efect asupra detectorului [Cox05]:

$$z_{nc}(v\mathbf{c}, \mathbf{w}) = \frac{v\mathbf{c} \cdot \mathbf{w}}{v|\mathbf{c}| \cdot |\mathbf{w}|} = z_{nc}(\mathbf{c}, \mathbf{w})$$

Interpretarea geometrică a detectorului cu corelație normalizată. Corelația normalizată este cosinusul unghiului dintre cei doi vectori. Prin urmare, compararea lui $z_{nc}(\mathbf{c}, \mathbf{w})$ cu un prag este echivalentă cu compararea unui unghi cu un prag, ceea ce duce la o regiune de detecție de formă conică [CMB02, Cox05].

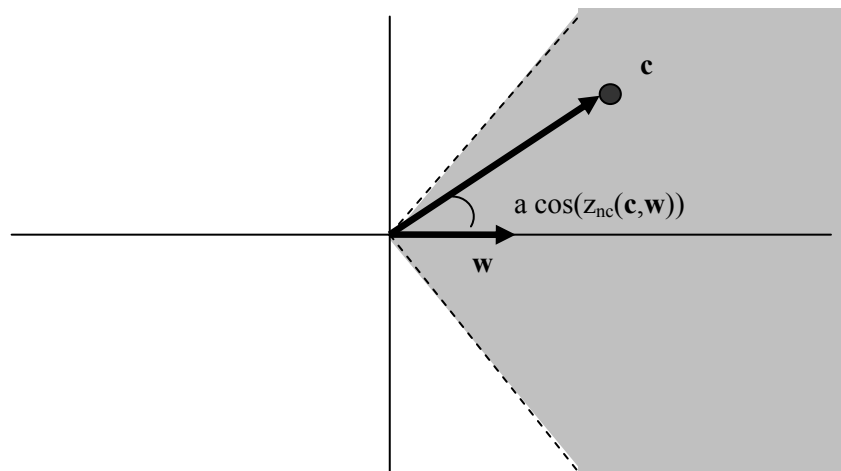


Fig. 1.20: Interpretarea geometrică a corelației normalizate.

Cuantizarea, care are loc în timpul compresiei semnalului multimedia, nu poate fi modelată ca un zgomot alb aditiv AWGN; în prezent se fac eforturi pentru modelarea zgomotului de cuantizare [CMB02].

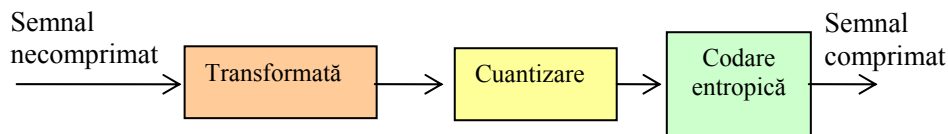


Fig. 1.21: Reprezentarea canonică a compresiei folosind o transformată.

Desincronizarea marcajului extras față de cel original, care poate fi produsă de distorsiuni geometrice pentru imagini, respectiv de distorsiuni temporale pentru semnale audio și video, nu poate fi nici ea modelată ca zgomot AWGN. Există metode pentru a compensa efectul desincronizării marcajului.

Un *marcaj de referință* este înglobat în plus față de cel care poartă efectiv informația. Înainte de detecția marcajului propriu-zis, trebuie „căutat” marcajul de referință; este posibilă detecția prin autocorelație. Această abordare are un impact negativ asupra fidelității și securității.

O altă modalitate este *sincronizarea implicită*, sau *folosirea proprietății de invarianță*. De exemplu, modulul transformatei Fourier este invariant la translație. Dacă imaginea este translata, valoarea de detecție depinde de autocorelația marcajului, care, pentru zgomotul alb este aproape de zero. De aceea, marca este puțin probabil să fie detectată. Astfel, în loc de domeniul spațial, o soluție ar fi folosirea unei transformate invariante la translație.

Sistemul de marcarea poate fi privit ca fiind compus din două părți [CMB02]:

- procesul de *extragere* a marcajului care proiectează elementele din domeniul media, în domeniul marcajului,
- un sistem de *marcare* simplu în domeniul marcajului, așa cum este descris mai sus.

Domeniul marcajului poate fi această transformată \mathcal{T} . Procesul de extragere a marcajului crește robustețea pentru că se trece într-un spațiu invariant la distorsiuni, care le inversează și care reduce zgomotul; de asemenea, dacă se folosește o cheie, se

reduce complexitatea de calcul și crește gradul de securitate. Dacă transformata \mathcal{T} este liniară și conservă energia atunci corelația liniară va fi:

$$z_{lc}(\mathcal{T}(\mathbf{c}), \mathbf{w}) = z_{lc}(\mathbf{c}, \mathcal{T}^{-1}(\mathbf{w})). \quad (1.18)$$

Rezultă că un sistem de marcare în domeniul transformatei \mathcal{T} este echivalent cu un sistem în domeniul spațial, care folosește un model diferit de marcare. Sistemul este diferit tocmai prin *neliniaritatea procesului de extragere* a marcajului.

Un exemplu simplu de *neliniaritate a sistemului* este *maskarea perceptuală*, care amplifică marcajul în zone în care zgomotul este mai puțin vizibil [CMB02].

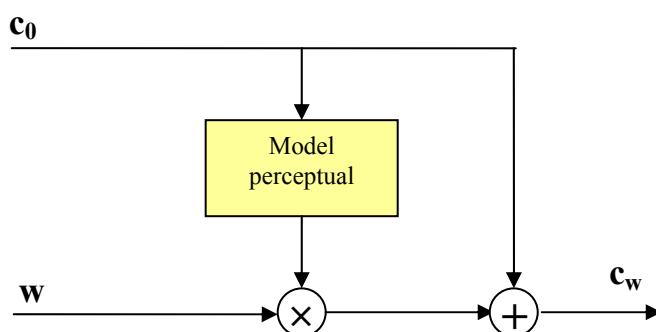


Fig. 1.22: Mascare perceptuală în înglobarea marcajului.

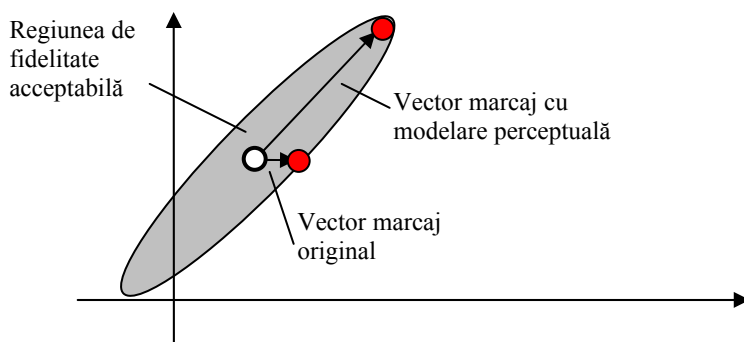


Fig. 1.23: Interpretarea geometrică a modelării perceptuale.

Marcajul obținut prin modelare perceptuală poate fi multiplicat cu o valoare mai mare a intensității, fără depășirea nivelului de distorsiune acceptabilă, ceea ce duce la o valoare de detecție mai mare.

Detecția se poate face inversând modelarea (maskarea) perceptuală la detector. Cu toate acestea, s-a constatat mai târziu că acest pas nu este necesar: distorsiunea modelului de marcaj degradează și valoarea de detecție, pentru un parametru α dat; dar se pot folosi valori mai mari ale intensității de marcare α , dat fiind faptul că marcajul este mai puțin vizibil [Cox05].

1.10.2 Soluții pentru asigurarea robusteții

Există mai multe soluții pentru a asigura robustețea:

- *Folosirea unor proprietăți invariante* la înserare, pentru ca marcajul să rămână neschimbat. Marcarea invariantă asigură că marcajul nu va fi schimbat de prelucrări de semnal folosind proprietăți invariante (cum ar fi o

transformată); se folosește câteodată pentru distorsiunile geometrice, dar este mai potrivită pentru alte tipuri de distorsiuni, cum ar fi filtrarea trece-jos. Soluția este înglobarea marcajului în coeficienții de joasă frecvență.

- *Inversarea distorsiunii la detector.* Distorsiunile pot fi inversate la detector, fiindcă multe din acestea sunt inversabile: rotirea, translația, redimensionarea. O altă soluție este distorsionarea marcajului original înainte de corelație, dar dificultatea majoră este găsirea parametrilor de distorsiune.
- *Pre-inversarea distorsiunii la înglobare.* În unele aplicații se cunoaște tipul de distorsiuni ce pot interveni. Se poate îngloba un marcaj “anti-distorsionant”, astfel încât după distorsiune marcajul este similar cu cel original. Spre exemplu, raportul de aspect se schimbă din 16:9 în 4:3 dacă se trece din format DVD sau HDTV la SDTV (în cazul video).
- *Înglobarea marcajului în mod redundant.* Înglobarea redundantă a marcajului se poate face în domeniul spațial, combinând repetițiile apoi testând, sau invers, testând fiecare parte redundantă apoi combinând rezultatele [KH01]. Alte posibilități de înglobare redundantă sunt codurile corectoare de erori, marcarea folosind comunicațiile cu spectru împrăștiat, etc.
- *Înglobarea marcajului în coeficienții de robustețe cunoscută.* Înglobarea se poate face în coeficienți mai robusți; această sensibilitate se poate modela sau se poate obține experimental [CKLS97, NB05, NC05b, NC05a, NIB05].
- *Înglobarea marcajului în regiuni semnificative perceptual.* O altă abordare este înglobarea marcajului în zone semnificative perceptual deși, în mod logic, acest lucru duce la scăderea valorii comerciale a produsului respectiv. În acest scop, se pot folosi tehnicile de tip *spread-spectrum* [CKLS97]. Rezultatul este că marcajul nu va fi distrus în urma compresiei, care înlătură părțile perceptual ne semnificative.

1.10.3 Marcarea informată

În Figurile 1.24-1.26 se prezintă procesul de *înglobare a marcajului*, funcție de tipul de *codare* și de *formare* a acestuia: *informat* respectiv *neinformat* [Cox05]. Marcarea informată folosește informații despre imaginea originală în codarea marcajului, și pentru formarea marcajului (Figura 1.26).

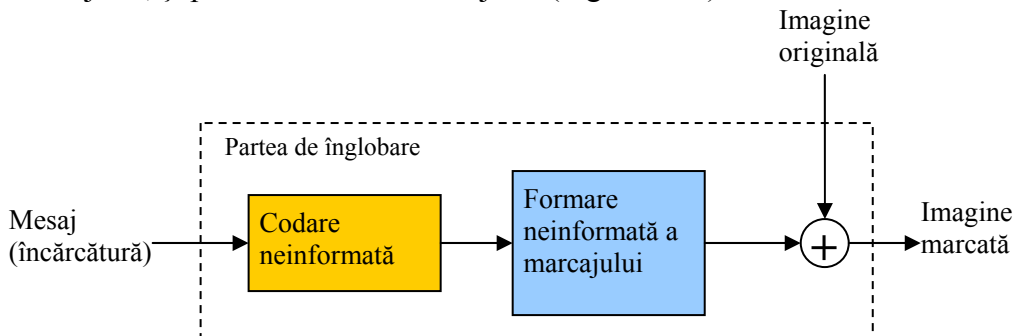


Fig. 1.24: Codare neinformată și formare neinformată a marcajului.

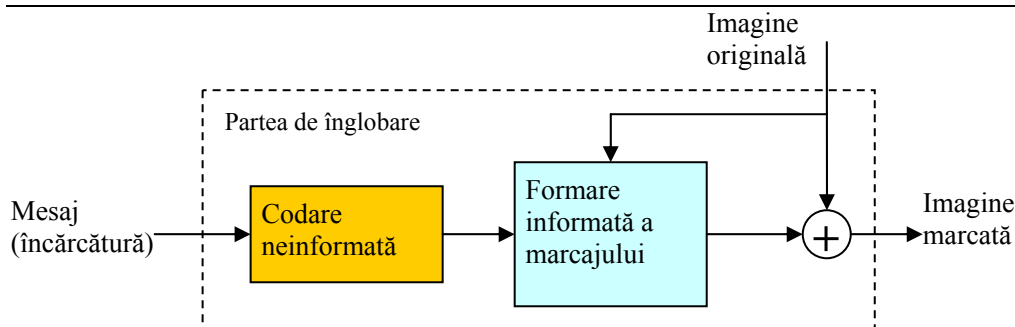


Fig. 1.25: Codare neinformată și formare informată a marcajului (mascare perceptuală).

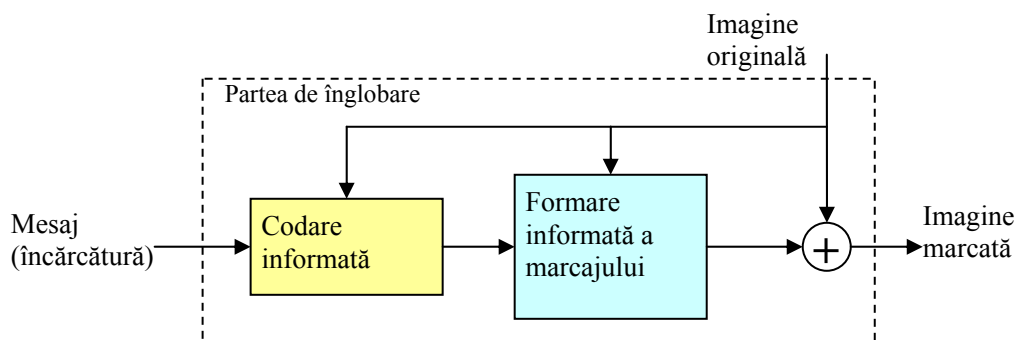


Fig. 1.26: Codare informată și formare informată a marcajului (mascare perceptuală).

Marcarea cu înglobare informată și detector neinformată poate fi privită ca și o formă de *comunicare cu informație ascunsă la transmițător* [CMB02]. În modelul lui Shannon, transmițătorul cunoaște modelul de canal. În marcarea transparentă, imaginea originală este considerată ca o sursă de zgomot, deci rezultatele teoretice ale acestui model ar trebui să fie aplicabile în acest caz.

În consecință *mascarea perceptuală* permite controlul raportului fidelitate/robustețe. Pe de altă parte, *codarea informată și mascarea perceptuală* permit creșterea încărcăturii (*payload*) pentru un raport fidelitate/robustețe dat, respectiv îmbunătățesc acest raport pentru o încărcătură dată.

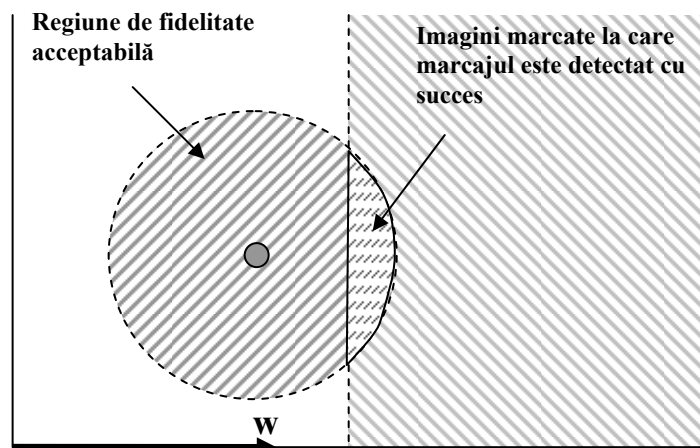


Fig. 1.27: Intersecția regiunii de detecție cu cea de fidelitate acceptabilă.

Obiectivul este producerea unei imagini care se află la intersecția regiunii de fidelitate acceptabilă și a regiunii de detecție. Problema care apare în cazul folosirii mascării perceptuale este că imaginea marcată rezultată poate fi în afara regiunii de detecție.

Există două posibilități pentru a soluționa această problemă: fie se maximizează robustețea pentru o fidelitate dată, fie se maximizează fidelitatea pentru o robustețe dată. Ambele variante necesită estimarea fidelității sau a robusteții.

În condițiile în care se presupune că eroarea medie pătratică, MSE, este un bun estimator al fidelității, și că robustețea este o funcție monotonă de corelația liniară, prin înglobare neinformată se ajunge la o robustețe maximă pentru o fidelitate dată. Pe de altă parte impactul negativ asupra fidelității poate fi minimizat pentru o robustețe dată.

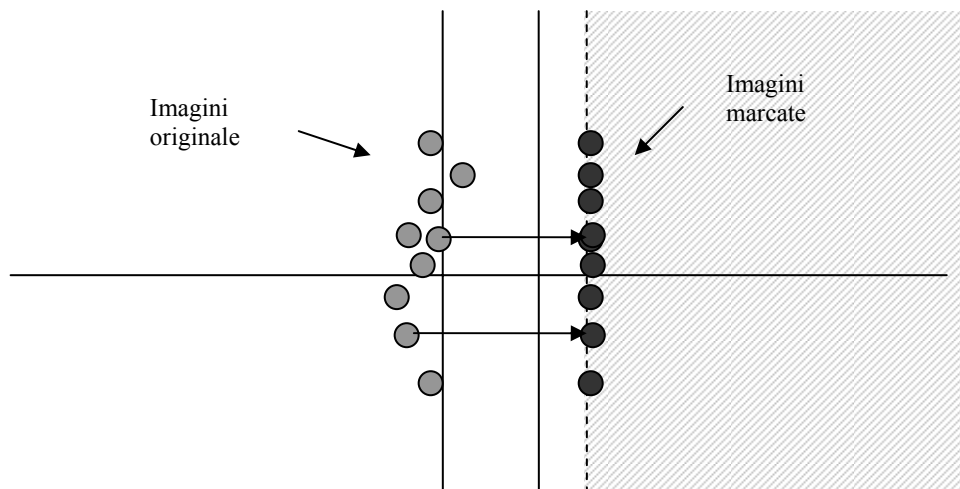


Fig. 1.28: Maximum de fidelitate pentru o robustețe dată

O altă problemă este estimarea robusteții în cazul mascării perceptuale (informate). Se poate pleca de la o premiză simplă, și anume că robustețea este o funcție monotonă de valoarea de detecție, lucru adevărat în cazul corelației liniare, dar neadevărat pentru corelația normalizată [Cox05]. În cazul corelației normalizate, rezultatele obținute la detecție sunt îmbunătățite, dacă robustețea se estimează ca fiind puterea zgomotului alb care poate fi adăugat la imaginea marcată, înainte ca marcajul să fie nedetectabil [CMB02].

1.10.4 Codarea informată

Încărcătura (*payload*-ul) marcajului poate fi crescută semnificativ în cazul în care codarea mesajului se face funcție de imaginea originală. Acest lucru este în conformitate cu teoria lui Costa, descrisă în lucrarea sa *Writing on dirty paper* [Cos83], aplicabilă și în marcarea transparentă.

Costa a studiat canalul *dirty-paper* [Cos83]. Informația se transmite printr-un canal zgomotos cu două surse de zgomot, prima fiind cunoscută la transmițător. El a demonstrat că prima sursă de zgomot, fiind cunoscută, nu afectează comunicația.

Această problemă poate fi asemănată cu transmiterea unui mesaj scris cu cerneală pe o hârtie care este afectată de praf distribuit normal. “Puterea” cernelii este limitată. Mesajul este transmis, și astfel se mai acumulează praf pe traseu. Problema

este că receptorul nu poate distinge între praf și cerneală, deci câtă informație poate fi transmisă?

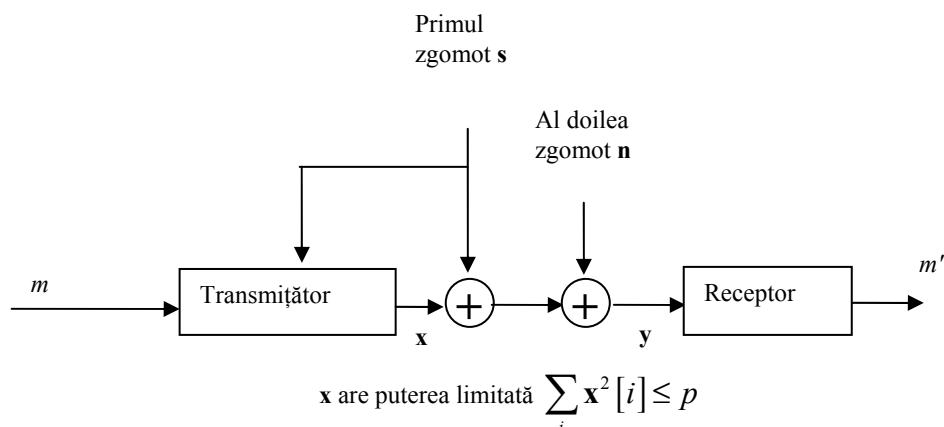


Fig. 1.29: Schema lui Costa pentru canalul dirty-paper [CM83].

Rezultatele obținute de Costa demonstrează faptul că prima sursă de zgomot nu are efect asupra capacității canalului. Această analogie este aproape similară cu marcarea transparentă cu detecție neinformată. Hârtia „murdară” s este echivalentă cu semnalul original, semnalul transmis x cu marcajul adăugat, iar limitarea puterii lui x este echivalentă cu conservarea fidelității. A doua sursă de zgomot este echivalentă cu distorsiunile suferite de semnalul multimedia. Deoarece canalul *dirty-paper* este atât de asemănător cu marcarea transparentă, rezultatele lui Costa sunt foarte interesante, în sensul că, dacă un sistem de marcarea are o comportare apropiată cu cea a canalului *dirty-paper*, atunci încărcarea maximă nu ar trebui să depindă de semnalul gazdă (original). Dar există o mare diferență între canalul *dirty-paper* și un sistem adevărat de marcarea transparentă, în sensul că cele două surse de zgomot sunt foarte rar gaussiene. Funcția densității de probabilitate a semnalelor multimedia nu e gaussiană, iar zgomotul depinde de semnalul original. În plus, controlul distorsiunii, ca o limitare a puterii, implică folosirea erorii medii pătratice, care nu este cel mai potrivit estimator al distanței perceptuale. Moulin și O’Sullivan [MOS03] au studiat modele de canale mai potrivite pentru marcarea transparentă. Ei au înlocuit a doua sursă de zgomot cu semnalul furnizat de un adversar care încearcă să elimine intenționat marcajul. S-a demonstrat că dacă semnalul gazdă are o distribuție gaussiană și constrângerea de fidelitate este exprimată funcție de constrângerea de putere, rezultatele obținute de Costa sunt valabile: capacitatea canalului este independentă de dispersia semnalului nemarcat. Dacă distribuția semnalului original nu este gaussiană, rezultatele sunt adevărate doar dacă maximul puterii p este mic în comparație cu dispersia semnalului original.

Bazându-se pe aceasta concluzie obținută de Costa, s-au construit pentru codarea informată a mesajului, *codurile dirty-paper* [CMB02]. Acestea sunt coduri în care fiecare mesaj este reprezentat prin vectori de cod alternativi. Din setul de vectori care reprezintă mesajul dorit se alege unul, \mathbf{u} , cel mai aproape de primul zgomot, adică în acest caz, de imaginea originală. Codul lui Costa este generat aleator și cere o căutare exhaustivă pentru codare și decodare, fiind convenabil numai pentru secvențe de intrare scurte.

Cele mai studiate în practică sunt *codurile latice* [CW98, EBTG02], unde fiecare cuvânt de cod este un punct al unei latice regulate. Punctele într-o latice N -dimensională pot fi construite prin însumarea multiplilor întregi a N vectori distincți.

Astfel mesajul \mathbf{w}_m , fiind un punct în această latice, poate fi descris ca suma unuia sau a mai multor marcaje de referință $\mathbf{w}_{r0}, \dots, \mathbf{w}_{rN}$, înmulțite cu niște întregi, $\mathbf{z}[0], \mathbf{z}[1], \dots, \mathbf{z}[N]$:

$$\mathbf{w}_m = \sum_i \mathbf{z}[i] \mathbf{w}_{r_i}$$

Fiecare dimensiune în spațiul de marcarea codează un simbol, de obicei un bit. Acesta este codat alegând între două puncte de cuantizare.

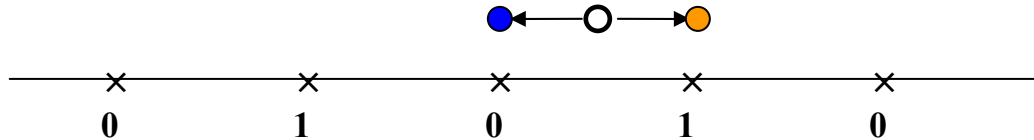


Fig. 1.30: Codare latice, pentru $N=1$.

Aceste sisteme sunt cunoscute sub denumirea de sisteme de *marcare QIM* bazate pe modulația prin cuantizarea indexată. Cea mai simplă formă de marcarea QIM cuantizează semnalul gazdă, folosind un cuantizor indexat de mesajul de marcare. Dacă se notează cu s semnalul marcat, cu m mesajul și cu x semnalul gazdă, atunci $s(x, m) = q_m(x)$. Semnalul rezultat va fi compus numai din valori din setul posibil al ieșirilor cuantizorului. Acest tip de marcarea este adecvat mai ales în cazul în care semnalul rezultat va fi ulterior cuantizat, de exemplu prin compresie. Modulația de *dither* poate produce un semnal care conține toate valorile din semnalul gazdă. Din valorile cuantizate sunt translatate cu un nivel variabil de *dither*, d , de exemplu cu relația $s(x, m) = q_m(x + d) - d$.

Sistemele de marcarea care folosesc *coduri latice* au o capacitate mult mai mare decât sistemele bazate pe corelație (de obicei peste 1000 de biți), dar nu sunt atât de robuste ca cele din urmă. Sistemele bazate pe corelație au raport mai bun încărcare/robustețe atunci când zgomotul este mare, pe când cele care folosesc coduri latice sunt susceptibile la schimbarea contrastului. *Codurile convoluționale* sunt o alternativă la codurile latice, fiind construite să fie robuste la ajustarea contrastului.

Capitolul 2

Tehnici de marcare

2.1 Clasificarea tehnicilor de marcare

În Figura 2.1 este dată o clasificare a tehnicilor de marcare existente:

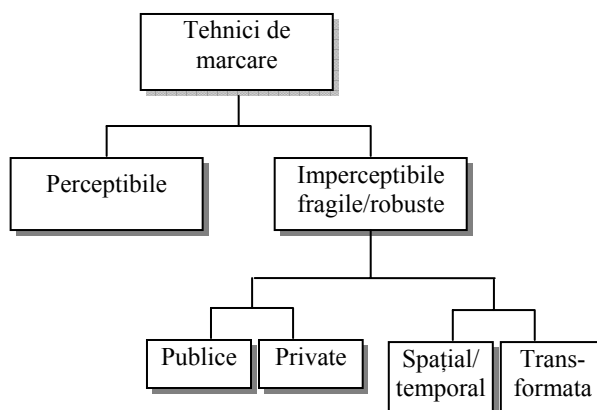


Fig. 2.1: Clasificarea tehnicilor de marcare.

Marcajele pot fi:

- *perceptibile*
- *imperceptibile*

Marcajele perceptibile creează schimbări sesizabile în semnalul original, atunci când sunt înglobate, dar nu împiedică semnalul marcat să comunice mesajul original. Deși marcarea perceptibilă nu este atât de răspândită, deoarece poate fi supărătoare pentru sistemul vizual uman, ea a fost implementată cu succes pentru imagini în [BMM96], prin înglobarea unui *logo* vizibil, care permite ca toate detaliile semnificative ale imaginii să fie văzute.

Marcajele imperceptibile au fost prezentate sumar în capitolul 1, dar *subiectul acestei teze fiind marcarea transparentă adică imperceptibilă a imaginilor statice*, acest subiect va fi tratat în continuare. Marcajele imperceptibile pot fi, în funcție de aplicație:

- *fragile*
- *robuste*.

Marcajele fragile sunt înglobate în semnalul multimedia astfel încât aproape orice transformare nedorită a semnalului marcat va duce la alterarea acestuia, oferind în acest fel informații despre modificări ale semnalului făcute cu rea voință [PW02].

Marcajele robuste sunt înglobate în semnalul gazdă astfel încât eliminarea lor să fie dificil de făcut, în contrast cu marcajele fragile. Acestea trebuie să fie rezistente împotriva *atacurilor* intenționate. Un *atac* este orice fel de modificare a semnalului multimedia marcat care poate afecta calitatea marcajului extras.

În cadrul tehnicilor de marcare robuste, se pot defini două tipuri de marcare [CM97], după modul în care se utilizează sau nu semnalul original la detecția marcajului:

- *marcarea publică* [AP98, KH98, NP98] folosește semnalul multimedia marcat și o cheie de marcare pentru detecția respectiv extragerea marcajului, fără să fie nevoie de semnalul multimedia original. Estimarea marcajului este mai puțin robustă, dar volumul de calcul este mult mai redus.

- *marcarea privată* [ZWL03, CKLS97, KM99, CM98] folosește atât semnalul multimedia marcat, cât și cel original, pentru detecția și extragerea marcajului. Estimarea marcajului este mai robustă, dar mai lentă. Nu este potrivită în aplicațiile unde se cere viteză și eficiență, cum sunt căutările automate, în baze de date, ale produselor multimedia furate [CMB02].

Tehnicile de marcare robuste se pot clasifica în funcție de locul de înserare a marcajului, astfel:

- tehnici în *domeniul spațial/temporal* unde marcajul este înglobat în domeniul spațial pentru imagini, respectiv, în domeniul temporal pentru semnale audio [NP98],
- tehnici în *domeniul transformatorilor*, unde se lucrează asupra transformatorilor cosinus, Fourier sau wavelet ale semnalului gazdă [SK01, ZWL03, CKLS97, CMYY98, KH98, NP98, KM99, CM98, PW02, NI03, NBK04, NC04b, NB05, NC05b, NC05a, NIB05].

Multe dintre aceste metode sunt asemănătoare și diferă în anumite aspecte cum sunt formarea semnalului de marcaj, înserarea și detecția.

Semnalul de marcaj. De obicei, informația înserată nu este importantă în sine, dar există metode care nu folosesc o secvență de informație aleatoare, ci înserează, respectiv extrag, cuvinte de cod din dicționare [CKLS95], [KH98]. În alte scheme se modulează codurile din dicționar, cu biți de informație aleatori. Deși unii autori fac distincție între cele două tipuri de metode, ele sunt foarte apropiate conceptual.

Semnalul de marcare tipic este un semnal pseudoaleator, cu amplitudine mică în comparație cu cea a imaginii; de obicei se distribuie spațial 1 bit pe mai multi pixeli. Semnalul de marcaj este construit adesea ca fiind un zgomot pseudo-aleator alb [TRSH93], [STO94] sau colorat, cu o distribuție gaussiană [CKLS95], uniformă sau bipolară [KH98], [Kut98], [NP96], [TRSH93]. Pentru a face marcajul imperceptibil, se poate aplica mascarea implicită sau explicită în domeniul spațial, [BMYY97], [KRR98], [WPD99], sau spectral pentru a atenua marcajul în zonele unde acesta ar putea deveni vizibil. Semnalul de marcaj rezultat este uneori împrăștiat și lasă pixeli din imagine neschimbați [KJB98], dar de cele mai multe ori este dens și alterează totii pixelii din imagine.

Inserarea semnalului de marcaj. Semnalul de marcaj este deseori înserat în domeniul spațial, dar și în domeniul unei transformate, precum transformata cosinus discretă, DCT [CKLS95], sau transformata DCT pe blocuri [KZ95].

Înserarea marcajului poate fi făcută prin adunare [LLL97, NP96, STO94] sau printr-o adunare adaptivă după forma semnalului [BBPC98a]; de cele mai multe ori, este afectat numai canalul de luminanță, sau numai canalele de culoare [KJB97]. Adunarea poate avea loc în domeniul spațial sau în domeniul unei transformate: transformata Fourier discretă DFT [RDB96], DCT pe imagine, [BBPC98c, CKLS95, PBBC97], DCT pe blocuri [BMYY97, HG96, KZ95, LLL97, PZ98, XBA97], în domeniul wavelet [Kun99, KH98], fractal [DS96, CBD98, PJ96], Hadamard [RAA99a], Fourier Mellin [RP97, RP98], Radon [WMBC99], Ridgelet [CKN04].

De multe ori se argumentează că înserarea în domeniul unei transformate (de cele mai multe ori DCT sau wavelet) poate fi avantajoasă din punctul de vedere atât al imperceptibilității cât și al securității [BBPC98c].

Unii autori sugerează ca marcajul să fie plasat în zonele de frecvență joasă ale imaginii [CKLS95, RP97], alții susțin că trebuie înserat în frecvențele medii [BBPC98c] sau înalte. De fapt, s-a demonstrat [SG99] că pentru o robustețe maximă dorită, marcajul ar trebui să fie înserat adaptiv, în componentele spectrale pe care le are semnalul gazdă. Pentru imagini și video, acestea sunt în general, frecvențele joase.

Detecția semnalului de marcaj. Așa cum am menționat mai înainte, generarea semnalului de marcaj precum și înserarea acestuia sunt tratate de obicei împreună. În unele metode, acestea nu pot fi privite separat, în special dacă marcajul este adaptat la forma semnalului [BBPC98c, CW98, CW01a, CW01b, LLL97].

Recuperarea marcajului este de obicei făcută cu o metodă bazată pe corelație, un corelator sau un filtru adaptat. Deoarece semnalul de marcaj este de obicei construit fără cunoștințe despre semnalul gazdă, interferența dintre semnalul de marcaj și semnalul gazdă este obișnuită în marcarea transparentă. Pentru a elimina interferența cauzată de semnalul gazdă, multe metode cer ca acesta să fie cunoscut la detecție, pentru a-l scădea înainte de extragerea marcajului. Alte metode aplică o prefiltrare [DKL98, KJB97, LLL97, STO94] în loc să scadă semnalul original nemarcat. În alte cazuri, această interferență nu se elimină [PBBC97]. Unii cercetători propun folosirea unor detectoare mai sofisticate în locul detectoarelor bazate pe corelație, de exemplu un detector MAP, maximum a-posteriori [BBPC98c]. Pentru extragerea marcajului au fost propuse mai multe domenii, de multe ori aceleași de la înserarea sau formarea marcajului. Există mai puține publicații în care marcarea și extragerea au loc în domenii diferite.

Tehnicile de marcare transparentă pot fi clasificate conform câtorva criterii, după cum urmează:

- Selecția locațiilor unde va fi înserat marcajul, folosind modelul vizual uman, sau o cheie generată aleator respectiv pseudo-aleator,
- Domeniul în care este înserat marcajul: spațial/temporal sau al unei transformate (DCT, DWT, DFT, etc),
- Codarea mesajului de marcaj, folosind coduri corectoare de erori (ECC), transmisia spread spectrum (SS), multiplexarea cu diviziune în timp/spațiu, multiplexarea în cod,
- Formarea semnalului marcat: prin adunare sau cuantizare,
- Detectarea/decodarea marcajului: cu corelatoare, etc.

2.1.1 Alegerea locațiilor unde se înserează marcajul

Cox, ș.a. [CKLS97] argumentează că marcajul ar trebui înserat în regiuni perceptuale semnificative, care vor supraviețui compresiei. Pe această idee au fost propuse numeroase metode.

Pe de altă parte, dacă se consideră un algoritm de marcare public, eliminarea marcajului ar trebui prevenită doar prin secretizarea cheii. Aceasta este o implicație directă a principiului lui Kerckhoff. De exemplu, o cheie secretă poate inițializa un generator de numere pseudo-aleatoare pentru selecția locațiilor marcajului [BGM95]. Câțiva algoritmi au propus recuperarea publică a marcajului [HG97], unde doar o parte din cheia secretă este cunoscută în partea de decodare (S^{pub}).

2.1.2 Domeniul de marcare

2.1.2.1 Domeniul spațial

Multe tehnici în domeniul spațial sunt bazate pe adunarea la o imagine a unei secvențe de zgomot pseudo-aleator. În acest caz, operatorii din capitolul 1, \mathcal{E} și \mathcal{D} sunt pur și simplu adunarea și scăderea. Considerăm o imagine de mărime $N \times M$, în care fiecare pixel este reprezentat de un număr zecimal, în domeniul determinat de numărul de biți folosiți. Într-o imagine cu nivele de gri, cu 8 biți per pixel, fiecare pixel poate avea o valoare între $[0, 255]$ și fiecare pixel D poate fi reprezentat ca fiind:

$$D = \sum_{i=0}^7 b_i \cdot 2^i .$$

Această proprietate permite descompunerea unei imagini într-o colecție de imagini binare, separând valorile b_i în $n=8$ planuri de biți.

Metodele de marcare în domeniul spațial înglobează marcajul modificând în mod direct valorile pixelilor din imaginea originală. De obicei, se modifică biții cei mai puțin semnificativi ai imaginii gazdă LSB. Mesajul secret este înserat în planul de biți cel mai puțin semnificativ al imaginii gazdă, fie prin înlocuirea directă a biților, fie modificând acești biți LSB conform unei funcții inverse. Strategia de înserare poate fi bazată pe înserarea secvențială sau selectivă a mesajului, în ariile mai „zgomotoase” ale imaginii, sau prin împrăștiere aleatoare prin imagine.

Data fiind capacitatea extraordinar de mare a canalului LSB prin metoda folosirii întregii imagini purtătoare pentru transmisie, un obiect mai mic poate fi integrat de mai multe ori. Chiar dacă majoritatea acestor obiecte se pierd din cauza atacurilor, un singur marcaj supraviețuitor poate fi considerat un succes.

Imperceptibilitatea este atinsă fiindcă planul LSB este nesemnificativ din punct de vedere vizual. Astfel, principalul avantaj al unei astfel de tehnici este că modificarea planului LSB nu afectează calitatea imaginii, din cauză că variația amplitudinii pixelilor este limitată la ± 1 . Proprietățile de mascare a sistemului vizual uman permit înserarea unor cantități semnificative de informație care vor fi imperceptibile unui observator uman, în condiții de vizualizare normale. Mascarea se referă la fenomenul la care un semnal este imperceptibil unui observator în prezența altui semnal. O expunere detaliată a acestor tehnici poate fi găsită în [LD99b], [YM97], [MW98].

Alte avantaje ale tehnicilor de marcare bazate pe LSB includ capacitatea mare și complexitatea de calcul mică. De aceea, este de așteptat ca ele să fie puse în practică mai ușor, atunci când este vorba de marcare în timp real. Principalul dezavantaj este lipsa de robustețe la falsificare, atacuri geometrice, filtrare și compresie.

Metoda substituirii LSB-urilor prezintă o serie de neajunsuri, în ciuda simplității ei. Deși poate supraviețui transformărilor ca decuparea, orice adăugare de zgomot sau compresie cu pierderi cauzează, mai mult ca sigur, pierderea marcajului. Un atac chiar mai bun este substituirea bitului LSB al fiecărui punct din imagine cu „1”, pierzându-se în totalitate posibilitatea recuperării marcării, cu un impact neglijabil asupra imaginii gazdă. Mai departe, odată descoperit algoritmul, marcajul poate fi modificat ușor.

Dacă se dorește un marcaj fragil, astfel de tehnici nu pot localiza modificări ale semnalului decât spațial, nu și spectral.

O îmbunătățire a tehnicii substituirii LSB-ului, ar fi folosirea unui generator de numere pseudo-aleatoare, pentru a determina pixelii din imagine care urmează să fie folosiți pentru integrarea marcajului, pe baza unei „chei” date. Securitatea marcării este îmbunătățită din moment ce marcajul nu poate fi găsit cu ușurință de persoane intermediare. În schimb algoritmul rămâne în continuare vulnerabil la atacul prin substituția LSB-ului cu o constantă. Chiar și în locurile care nu s-au folosit pentru biți de marcare, efectul substituirii este neglijabil asupra imaginii purtătoare. Modificarea LSB-ului se dovedește a fi o metodă simplă și puternică pentru steganografie, totuși lipsește robustețea de bază cerută de aplicațiile de marcare transparentă.

Aceste tehnici presupun uneori transformarea mesajului de marcaj într-o secvență PN, care este apoi inserată în imagine, o singură dată, sau de mai multe ori dacă marcajul este mult mai mic decât imaginea gazdă. Detecția se face prin obținerea imaginii de marcare și compararea ei cu cea originală, sau folosind un corelator.

2.1.2.2 Domeniul unei transformate

Tehnicile descrise anterior pot fi aplicate și în domeniul unor transformate ale imaginii, unde se poate ține cont de criteriile perceptuale în procesul de inserare a marcajului, și în construirea unor tehnici de marcare robuste la tehnici de prelucrare obișnuite. Fiecare domeniu de transformare are avantajele și dezavantajele sale.

Pentru a înțelege avantajele unei metode de marcare în domeniul transformatelor, în cele ce urmează se analizează etapele prin care trece un semnal multimedia (imagine sau semnal audio) în timpul copierii. În Figura 2.3, prin „transmisia” semnalului înțelegem codarea sursei sau a canalului, și/sau criptarea datelor. Majoritatea prelucrărilor sunt fără pierderi, dar multe din metodele de compresie ale datelor sunt cu pierderi. Acestea din urmă (JPEG, MPEG, etc.) pot degrada calitatea datelor, printr-o pierdere iremediabilă a informației. O schemă de marcare ar trebui să fie rezistentă la distorsiunile introduse de aceste prelucrări.

Compresia cu pierderi este o operație care elimină de obicei componentele mai puțin semnificative ale unei imagini sau ale unui sunet. Majoritatea procesărilor de acest tip au loc în domeniul frecvență. De fapt, pierderile de date au loc în componentele cu frecvențe înalte.

După recepție, o imagine suferă o serie de transformări obișnuite care pot fi clasificate în distorsiuni geometrice, sau distorsiuni ale semnalului. Distorsiunile geometrice sunt specifice imaginilor și semnalelor video, și se referă la operații cum ar fi rotirea, translația, scalarea și decuparea. Prin determinarea manuală a minim patru sau nouă puncte corespondente dintre marcajul original și cel distorsionat, este posibilă îndepărtarea oricărei transformări afine, bi- sau tri-dimensionale [CKLS97]. O scalare afină, sau micșorare a imaginii duce la o pierdere a datelor în componentele de frecvențe înalte ale imaginii. Decuparea sau tăierea porțiunilor din imagine duc la pierderi irecuperabile ale datelor, care pot degrada serios orice marcaj aplicat în domeniul spațial. Dar o metodă bazată pe o transformare în frecvență, ca DCT, împărțește marcajul în întreg domeniul spațial al imaginii, și este mai puțin probabil ca el să fie afectat de decupare.

Distorsiuni obișnuite ale semnalului sunt conversiile D/A, A/D, reeșantionarea, recuantizarea, precum și îmbunătățirile aduse semnalului cum ar fi

creșterea contrastului sau a intensității culorilor pentru imagini, sau egalizarea în frecvență pentru semnale audio.

Multe dintre aceste distorsiuni sunt neliniare, deci este dificil de analizat efectul lor asupra metodelor de marcare în domeniul spațial sau al transformatei. Dar cunoșterea imaginii originale permite ca multe transformări să fie reversibile, cel puțin aproximativ.

Nu în ultimul rând, imaginea copiată poate să nu rămână în formatul digital original. Este foarte probabil ca imaginea să fie imprimată pe hârtie, sau în cazul semnalelor audio și video, ele pot fi copiate pe casete audio, respectiv video. Aceste reproduceri pot introduce degradări adiționale asupra imaginii, la care metoda de marcare trebuie să fie robustă.

Din motivele enumerate mai sus, se poate deduce că marcajul nu ar trebui să fie plasat în regiunile sau componentele spectrale *nesemnificative* ale imaginii, deoarece multe prelucrări și distorsionări obișnuite ale semnalului pot afecta aceste componente. De exemplu, un marcaj plasat în frecvențele mai înalte ale imaginii poate fi foarte ușor eliminat printr-o filtrare trece-jos. Evident că poate fi afectată orice componentă spectrală, cu condiția ca modificările făcute să fie mici. Dar schimbările mici pot fi foarte sensibile la zgomot.

Problema care se pune este cum să se introducă marcajul în regiunile de percepție maximă ale spectrului, păstrând fidelitatea semnalului original.

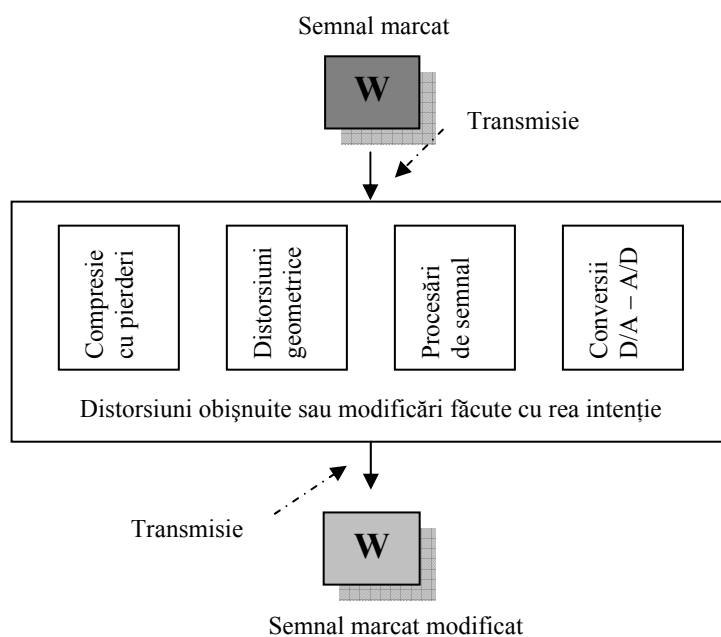


Fig. 2.2: Prelucrări obișnuite ale unui produs multimedia

Există multe lucrări care abordează problema marcării, prin analogie cu problema comunicațiilor cu spectru împrăștiat, SS (Spread Spectrum). În [CKLS97], autorii tratează domeniul transformatei DCT a imaginii ca un *canal de comunicații* și corespunzător, marcajul este văzut ca un semnal care trebuie transmis prin acest canal de comunicații. Atacurile și distorsiunile neintenționate ale semnalului sunt tratate ca un zgomot la care semnalul trebuie să fie imun.

În comunicațiile cu SS, se transmite un semnal de bandă îngustă într-o bandă mult mai largă de frecvență, astfel încât energia oricărei componente spectrale a

semnalului să fie foarte mică și aproape nedetectabilă. Marca este împrăștiată în multe componente spectrale, astfel încât energia ei din fiecare componentă să nu fie detectabilă. Deoarece în procesul de detecție a marcajului se cunoaște localizarea și conținutul marcajului, este posibil ca la recepție să se concentreze aceste semnale numeroase cu energie scăzută într-un singur semnal, al cărui raport semnal pe zgomot să fie mare. Pentru a distruge un astfel de marcaj, ar trebui adăugat zgomot cu amplitudine mare în *toate* componentele spectrale.

Împrăștierea marcajului în tot spectrul imaginii asigură o robustețe mare față de atacuri, intenționate sau nu, deoarece nu se cunoaște localizarea marcajului. În plus, pot fi selectate anumite zone de frecvență, a căror atacare ar conduce la degradări severe ale imaginii.

Un marcaj bine plasat în componentele spectrale ale semnalului va fi imposibil de văzut la imagini, respectiv de auzit la sunete. Afirmatia este adevărată dacă energia marcajului este suficient de mică în oricare componentă spectrală. În plus, energia marcajului prezentă în unele componente spectrale poate fi mărită, folosind cunoștințele despre *fenomenul de mascare* al simțului auditiv, respectiv vizual al omului.

Este cunoscut faptul că HAS și HVS disting cu o rezoluție mai mare zonele cu energie mai mare și frecvențe mai joase, din imagine sau sunet. Mai mult, majoritatea informației este localizată în regiunile cu frecvențe mai joase [CKLS97].

Mascarea perceptuală se referă la situația în care anumite informații care ar putea fi distinse de observatorul uman când sunt prezentate izolat, vor fi observate cu dificultate sau deloc, când se adaugă alte informații (o imagine puternic texturată, sau un sunet învecinat mai puternic). Astfel, prezența unui semnal poate fi ascunsă sau mascată de prezența altui semnal. Mascarea este o măsură a răspunsului la un stimul a unui observator, când este prezent un al doilea stimul, cel de mascare [CMB02, CKLS97].

2.1.2.2.a Metode bazate pe transformata Fourier discretă

În [RDB96], este folosită faza valorilor transformării Fourier discrete, DFT, pentru plasarea marcajului, deoarece, pentru inteligibilitatea imaginii, este mai importantă faza decât amplitudinea valorilor DFT. Plasarea marcajului în cele mai importante componente ale imaginii, îmbunătățește robustețea marcajului, deoarece modificarea acestor componente importante de imagine, cu scopul eliminării marcajului, ar degrada calitatea imaginii. Al doilea motiv pentru folosirea fazei valorilor DFT este că modulația de fază prezintă imunitate superioară la zgomot în comparație cu modulația de amplitudine.

Multe tehnici de marcare folosesc modulația de amplitudine în DFT, din cauza proprietății de invarianță la translații sau deplasări [LWBC01, RP98]. Deoarece translația ciclică a imaginii în domeniul spațial nu afectează amplitudinile coeficienților DFT, marcarea plasată în acest domeniu va fi invariantă la translații.

În cazul folosirii unui marcaj CDMA (Code Division Multiple Access), metoda poate fi rezistentă la decupare. Marcajul poate fi plasat direct în frecvențele medii cele mai importante, deoarece modulația coeficienților de frecvență joasă generează efecte vizibile, iar coeficienții frecvențelor înalte sunt foarte vulnerabili la zgomot, filtrare și compresie cu pierderi. În final, marcajul poate fi făcut dependent de conținutul imaginii, prin modularea coeficienților de amplitudine DFT, $|I(u,v)|$ în modul următor [CKLS95]:

$$|I_w(u, v)| = |I(u, v)|(1 + k \cdot W(u, v)). \quad (2.1)$$

Aici, $W(u, v)$ reprezintă un marcaj CDMA, un model pseudo-aleator bidimensional (2D) și k reprezintă factorul de câștig. Modificarea coeficienților DFT nu este fixă, ci proporțională cu amplitudinea coeficienților DFT. Coeficienții DFT mici sunt foarte puțin afectați, dar coeficienții DFT mai mari sunt modificați mai mult. Acest lucru este în conformitate cu legea lui Weber [Jai81]. Sistemul vizual uman (HVS) nu percepe modificările egale în imagini egale, dar sensibilitatea vizuală este aproape constantă în privința schimbărilor relative dintr-o imagine. Dacă ΔI este o diferență ușor vizibilă, atunci $\Delta I/I = \text{constant}$. Rescrierea relației (2.1) conduce la:

$$\frac{|I_w(u, v)| - |I(u, v)|}{|I(u, v)|} = \frac{\Delta I(u, v)}{|I(u, v)|} = k \cdot W(u, v) \cong \text{constant} \quad (2.2)$$

Deoarece în acest caz marcajul este plasat în majoritate în coeficienții DFT mai mari, adică în componentele cele mai semnificative ale imaginii din punct de vedere perceptual, robustețea marcajului este îmbunătățită. Este de menționat că simetria coeficienților Fourier trebuie păstrată, pentru a asigura ca datele de imagine să fie de valoare reală după transformarea inversă la domeniul spațial. Dacă coeficientul $|I(u, v)|$ într-o imagine cu $N \times M$ pixeli este modificat conform relației (2.1), corespondentul lui, $|I(N-u, M-v)|$, trebuie modificat și el în același mod.



Fig. 2.3: Marcajul inserat în amplitudinea coeficienților Fourier
 (a) Imaginea originală, (b) Imaginea marcată, (c) Diferența $W(x, y) = I - I_w$, scalată pentru a fi vizibilă, (d) Imagine puternic marcată

În figura 2.3(b) este prezentată, ca exemplu, o imagine în care marcajul este plasat folosind toți coeficienții de amplitudine DFT, în conformitate cu relația (2.2) și folosind un factor de câștig k relativ mic. Figura 2.3(c) prezintă diferența, puternic amplificată, dintre imaginea originală și cea marcată, iar figura 2.3(d) arată o imagine marcată, folosindu-se o valoare mare pentru factorul de câștig k .

Transformata DFT este mai adesea folosită în formele ei derivate, cum ar fi transformata cosinus discretă, DCT sau transformata Fourier-Mellin.

2.1.2.2.b Metode bazate pe transformata cosinus discretă

Domeniul transformării cosinus discrete, DCT, este deseori folosit pentru plasarea marcajului. DCT este o transformată reală, care reprezintă imaginea prin coeficienți ai unor semnale cosinusoidale, de diferite frecvențe (care constituie baza acestei transformate). Transformata DCT a imaginii este calculată pe blocuri de dimensiune 8x8 ale imaginii, care apoi sunt transformate individual. Transformata 2D-DCT, a unei imagini, este matricea rezultată astfel încât, colțul din stânga sus reprezintă frecvența joasă, iar colțul din dreapta jos reprezintă frecvența înaltă. DCT stă la baza algoritmului de compresie JPEG, care este unul dintre cele mai răspândite formate de memorare a datelor la ora actuală. Marcajele înserate, în domeniul transformatei DCT, sunt capabile să supraviețuiască unor forme de prelucrări precum filtrarea trece-jos, trece-sus, filtrarea mediană, etc.

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

Fig. 2.4: Valori de cuantizare folosite la compresia JPEG.

Folosind DCT, o imagine poate fi împărțită cu ușurință în benzi de pseudo-frecvență, în așa fel încât marcajul să poată fi plasat convenabil în cele mai importante frecvențe medii. În plus, a fost intens studiată sensibilitatea sistemului vizual uman la imaginile de bază DCT, rezultând tabela de cuantizare JPEG (figura 2.4) [PM93].

Aceste rezultate pot fi folosite pentru predicția și minimizarea impactului vizual la distorsiunile cauzate de marcaj. În final, pentru compresia imaginilor și materialelor video este folosită pe scară largă DCT pe bază de blocuri.

Prin plasarea marcajului în același domeniu cu al schemei de compresie utilizată pentru procesarea imaginii, domeniul DCT în acest caz, se poate anticipa compresia cu pierderi, pentru că se pot anticipa coeficienții DCT care vor fi eliminați de către algoritmul de compresie. Descompunerea DCT se poate exploata și pentru a crea aplicații de marcare în timp real.

În figura 2.5(a) este dat un exemplu pentru o imagine în care este plasat un marcaj CDMA bidimensional, W , în frecvențele medii a blocurilor DCT de dimensiune 8x8. Coeficienții DCT de 8x8, $F(u,v)$, sunt modulați conform:

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + k \cdot W_{x,y}(u,v), & u,v \in F_M, \quad x,y = 1,8,16,\dots \\ I_{x,y}(u,v), & u,v \notin F_M \end{cases} \quad (2.3)$$

Aici F_M înseamnă frecvențele medii, k factorul de câștig, (x,y) locația spațială a unui bloc de dimensiune 8×8 de pixeli în imaginea I , și (u,v) coeficientul DCT, în blocul DCT de 8×8 corespunzător (figura 2.6).

În figura 2.5(c) este prezentată diferența, puternic amplificată, dintre imaginea originală și imaginea marcată. Figura 2.5(d) arată spectrul Fourier al marcajului. Se poate vedea că marcajul afectează doar frecvențele medii (regiunile albe), lăsând componentele de frecvență joasă și înaltă relativ neafectate (regiunile întunecate).

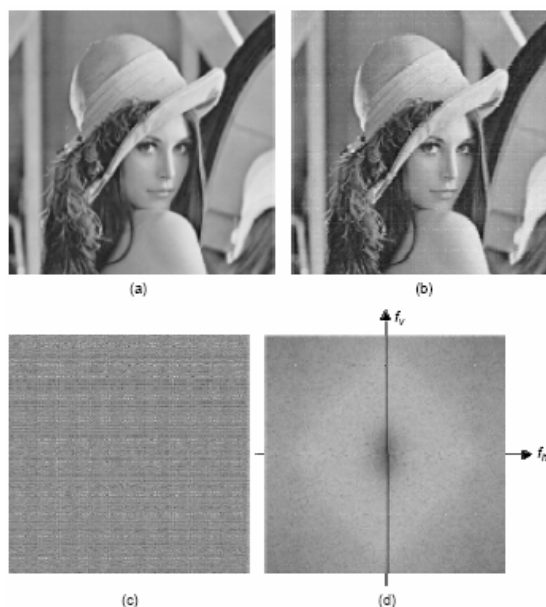


Fig. 2.5: Un marcaj DCT de 8×8 , de bandă medie, independent de conținutul imaginii. (a) Imaginea marcată, (b) Imaginea puternic marcată, (c) Diferența $W(x,y) = I(x,y) - I_w(x,y)$, și (d) Spectrul Fourier $W(u,v)$

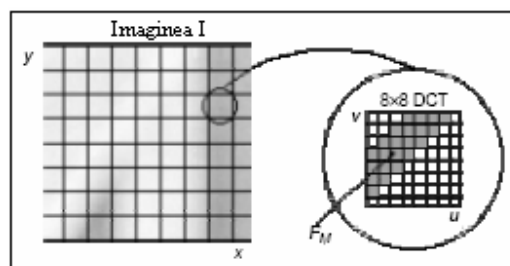


Fig. 2.6: Definierea benzii de frecvențe medii într-un bloc DCT

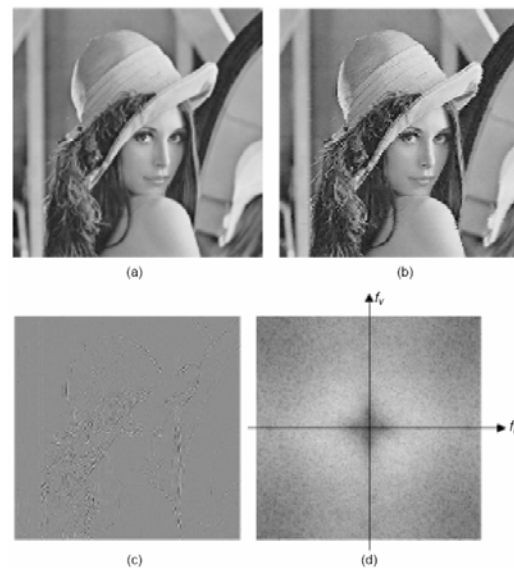


Fig. 2.7: Un marcaj DCT de 8×8 , de bandă medie, dependent de conținutul imaginii. (a) Imaginea marcată, (b) Imaginea puternic marcată, (c) Diferența $W(x,y) = I(x,y) - I_w(x,y)$, și (d) Spectrul Fourier $W(u,v)$

Marcajul poate fi făcut dependent de imagine prin schimbarea funcției de modulație cu:

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v)(1+k \cdot W_{x,y}(u,v)), & u,v \in F_M, x,y=1,8,16\dots \\ I_{x,y}(u,v), & u,v \notin F_M \end{cases} \quad (2.4)$$

Dacă este aplicată această funcție de modulație, rezultatele din figura 2.5 se vor schimba în rezultatele prezentate în figura 2.7. Din figura 2.7(b) și (c) reiese că majoritatea distorsiunilor introduse de marcaj sunt localizate în jurul marginilor și în porțiunile cu „textură”.

Îmbunătățiri suplimentare pentru performanțele sistemelor de marcare în domeniul DCT, pe bază de corelație, pot fi obținute prin folosirea detectoarelor de marcaj pe baza modelelor gaussiene generalizate și nu pur gaussiene [HAPG00].

2.1.2.2.c Metode bazate pe transformata wavelet

Aceste tehnici implică inserarea informației în benzile LH și HH ale transformatei wavelet a imaginii. Schimbările în aceste regiuni nu sunt sesizabile de către observatorii umani, din cauza caracteristicilor sistemului vizual uman [HW00, KH98, KH03, NI03, NBK04, KM99, KKK02, CM98, CN04]. Dacă tehnicile de marcare pot exploata caracteristicile HVS, este posibilă ascunderea marcajelor într-o imagine cu mai multă energie, lucru care crește robustețea marcajelor. Din acest punct de vedere transformarea wavelet discretă, DWT, este foarte atractivă, deoarece este mai eficientă din punctul de vedere al calculului. Se pare că ochiul uman este mai puțin sensibil la zgomot în benzile DWT de rezoluție înaltă și în benzile DWT cu orientare de 45° (banda HH). În plus, codarea DWT a imaginilor și a materialelor video, cum ar fi codarea EZW (Embedded Zero-tree Wavelet), este inclusă în

standardele de compresie video și de imagine, ca JPEG2000. Prin plasarea marcajului în același domeniu (domeniul DWT) se poate anticipa compresia EZW cu pierderi, deoarece se pot anticipa care benzi DWT vor fi afectate de schema de compresie. Mai departe, se poate exploata descompunerea DWT pentru a crea aplicații de marcare în timp real.

În figura 2.8(a) este dat un exemplu pentru o imagine în care este plasat un marcaj CDMA bidimensional, W , în benzile DWT: LH_1 , HH_1 , și HL_1 , folosind un factor de câștig k mare. Figura 2.8(b) arată diferența puternic amplificată, dintre imaginea originală și cea marcată. Coeficienții DWT din cele trei benzi DWT sunt modulați folosind relația:

$$I_W(u, v) = I(u, v) + k \cdot W(u, v) \quad (2.5)$$

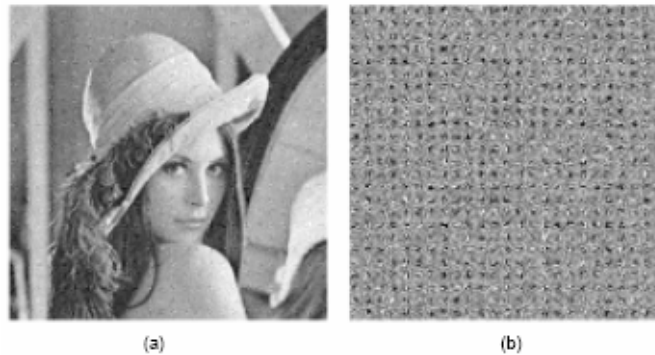


Fig. 2.8: Marcaj DWT independent de conținutul imaginii.
(a) Imagine puternic marcată, și (b) Diferența $W(x,y)=I(x,y)-I_W(x,y)$

Marcajul DWT poate fi făcut dependent de imagine, prin modularea coeficienților DWT în fiecare dintre cele trei benzi DWT conform ecuației de mai jos:

$$I_W(u, v) = I(u, v)(1 + k \cdot W(u, v)). \quad (2.6)$$

În figura 2.9(a) este dat un exemplu pentru o imagine în care este plasat același marcaj CDMA, W , în benzile DWT: LH_1 , HH_1 , și HL_1 , conform relației (2.6), cu un factor de câștig k mare.

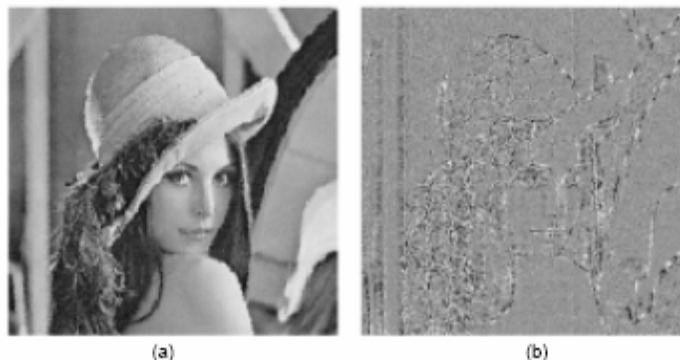


Fig. 2.9: Marcaj DWT dependent de conținutul imaginii.
(a) Imagine puternic marcată, și (b) Diferența $W(x,y)=I(x,y)-I_W(x,y)$

2.1.2.2.d Metode bazate pe transformata Fourier-Mellin

Aceste metode, relativ noi, au apărut din nevoia ca marcajul să fie invariant la atacuri geometrice (rotații, scalări și translații, sau altfel spus invariant RST). Ele presupun crearea unei coordonate polare logaritmice a amplitudinii transformării DFT pentru imaginea originală, unde are loc înserarea. Acest tip de metode este extrem de rezistent, adică invariant, la atacurile de tip RST [LWBC01, RP98].

2.1.3 Codarea marcajului

Transmisia cu spectru împrăștiat SS este des folosită în domeniul marcării transparente, majoritatea tehnicilor bazându-se pe acest principiu. Avantajele de bază ale transmisiunilor cu SS sunt: reducerea efectelor interferențelor și prevenirea interceptării semnalului. Principial, comunicațiile cu SS constă din transmiterea unui semnal de bandă îngustă, pe un canal de bandă largă, cu interferențe. În acest caz semnalul de bandă îngustă este marcajul I, iar canalul de bandă largă este semnalul X, audio sau video.

Având în vedere că marcajele trebuie să aibă o putere mică pentru a atinge imperceptibilitatea, marcarea poate fi văzută ca o comunicație printr-un canal foarte zgomotos. Aproape toate schemele de marcare reprezintă încărcătura utilă (payload) sub forma unei secvențe pseudo-aleatoare (PN). Numărul aleator folosit la generarea secvenței devine cheia marcajului. Aceste scheme sunt private, deoarece pentru a detecta marcajul, decodorul trebuie să cunoască cheia [CKLS97, RP98].

Cele două etape ale marcării sunt:

-*Înserarea marcajului*: informația de marcaj, I, se împrăștie prin modulare cu un zgomot pseudo-aleator PN (Pseudo-Noise) care constituie cheia K, asigurând astfel mascarea zonelor din semnalul original afectate de marcaj. Folosirea tehnicii cu SS protejează eficient marcajul, mai ales împotriva manipulărilor neintenționate, proprii procesărilor uzuale (compresie, scalare), de la transmiterea și stocarea datelor.

-*Deteția marcajului*: în cazul marcării bazate pe SS, deția autorizată (se cunoaște K) este ușor de făcut și fără originalul X, utilizând un receptor cu corelator. Desincronizările care pot să apară vor putea fi compensate prin utilizarea unui corelator cu fereastră glisantă, care va găsi prin alunecare, valoarea maximă a funcției de corelație și deci va detecta valoarea adevărată a informației I de marcaj. Deția marcajului conduce la decizia dacă datele au fost marcate folosind o anumită cheie sau nu.

Detectorul produce o anumită ieșire binară. Pentru a analiza corectitudinea funcționării unui detector, avem doi parametri importanți:

P_D = probabilitatea deției corecte și

P_{fa} = probabilitatea de alarmă falsă.

Pentru ca o metodă să fie cât mai bună, ea trebuie să aibă P_D cât mai mare și P_{fa} cât mai mic. Acești parametri se pot folosi de asemenea și pentru compararea diverselor metode de marcare transparentă.

În general pentru deție este folosită o versiune a marcajului, generată local. Acest marcaj este corelat cu datele recepționate. Dacă la receptor, cheia folosită este cea corectă, atunci valoarea corelației este mare. După deția corectă a prezenței marcajului este posibilă extragerea acestuia cu ajutorul intercorelației. În acest caz se ia o decizie independentă asupra fiecărui bit în parte.

O metodă îmbunătățită de marcare, ISS, folosind SS, este propusă de Malvar și Florencio [MF03]; ea înlătură semnalul ca sursă de interferență. Câștigul este similar cu cel obținut de QIM, dar ISS nu suferă de aceeași sensibilitate la scalare. Înserarea marcajului se face cu relația:

$$\mathbf{s} = \mathbf{x} + \mu(x, b)\mathbf{u},$$

unde funcția $\mu(x, b)$ modulează secvența de marcaj, \mathbf{u} . Parametrul b este intensitatea din algoritmul SS clasic, iar x este dat de $x \triangleq \langle \mathbf{x}, \mathbf{u} \rangle / \|\mathbf{u}\|$. Autorii analizează cazul liniar:

$$\mathbf{s} = \mathbf{x} + (\alpha b - \lambda x)\mathbf{u},$$

spre deosebire de abordarea tradițională SS:

$$\mathbf{s} = \mathbf{x} + b\mathbf{u}$$

Parametrii α și λ controlează nivelul de distorsiune și înlăturarea semnalului gazdă din statistica de detecție. Tehnica SS tradițională este obținută pentru $\alpha = 1$ și $\lambda = 0$.

Creșterea încărcăturii marcajului. Din punctul de vedere al detectorului marcajului, o imagine I poate fi privită ca un zgomot gaussian, care distorsionează informația de marcaj W . Mai departe, imaginea marcată I_w poate fi privită ca ieșirea unui canal de comunicație afectat de zgomot gaussian, prin care se transmite informația de marcaj. Transmisia sigură a marcajului este teoretic posibilă, dacă rata de informație a marcajului nu depășește capacitatea canalului [SW49]:

$$C = W_b \log_2 \left(1 + \frac{\sigma_w^2}{\sigma_I^2} \right) \text{bit / pixel} . \quad (2.7)$$

Aici C este dată în biți (ai informației de marcaj) per pixel de imagine, și lățimea de bandă disponibilă W_b egală cu un Hertz per pixel. Pentru sistemele reale, totuși, poate fi determinată empiric o limită mai redusă:

$$C = W_b \log_2 \left(1 + \frac{\sigma_w^2}{\alpha \cdot \sigma_I^2} \right) \text{bit / pixel} . \quad (2.8)$$

Aici, α este un factor de scală tipic mai mare ca 1, în jurul valorii trei. Deoarece raportul semnal-pe-zgomot σ_w^2 / σ_I^2 este mult mai mic decât unu, relația de mai sus poate fi aproximată cu:

$$C \approx \frac{1}{\ln 2} \left(\frac{\sigma_w^2}{\alpha \cdot \sigma_I^2} \right) \text{bit / pixel} . \quad (2.9)$$

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

Cea mai simplă metodă, de a plasa un șir de l biți de marcaj $b_0b_1\dots b_{l-1}$ într-o imagine, este împărțirea imaginii I în l subimagini $I_0I_1\dots I_{l-1}$, și adăugarea unui marcaj la fiecare subimagine, unde fiecare marcaj reprezintă un bit al șirului [LLL97], [SC96], [HLR00]. Acest procedeu este descris în figura 2.10.

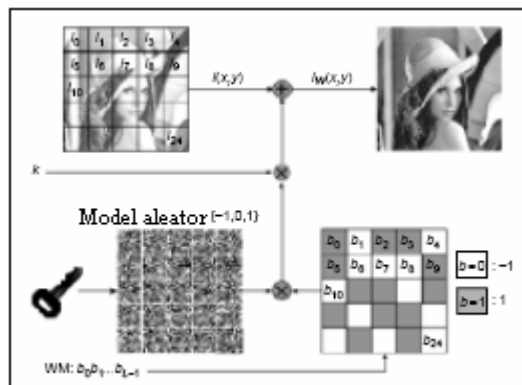


Fig. 2.10: Procedura de plasare a șirului biților de marcaj

Folosind relația (2.9) se pot calcula numărul de pixeli P , necesari per subimagine, pentru detecția sigură a unui singur bit într-o subimagine:

$$P \approx \frac{\alpha \sigma_I^2 \ln 2}{\sigma_W^2} \text{ pixeli} . \quad (2.10)$$

Biții de marcaj pot fi reprezentați în mai multe moduri. Dacă bitul de marcaj este 1, se adaugă o secvență pseudo-aleatoare, iar dacă este 0, subimaginea se lasă neatinsă. În acest caz detectorul calculează corelația dintre subimagine și secvența pseudo-aleatoare și atribuie valoarea 1 bitului de marcaj, când corelația depășește un anumit prag T , în caz contrar bitul de marcaj se consideră zero. Folosirea unui prag poate fi ocolită, prin adăugarea a două secvențe pseudo-aleatoare diferite, RP_0 și RP_1 , pentru biții de marcaj 0 și 1. În acest caz detectorul calculează corelația dintre subimagine și cele două modele. Bitului de marcaj 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 [SC96]. În acest caz, detectorul trebuie să calculeze doar o corelație dintre subimagine și una dintre secvențe; semnul corelației determină valoarea bitului de marcaj.

Altă modalitate de a crește încărcătura marcajului de bază este folosirea tehnicilor DS-CDMA (Direct Sequence-CDMA) [RP98a,b]. Pentru fiecare bit b_j din șirul biților de marcaj b_0, b_1, \dots, b_{l-1} este generată o secvență pseudo-aleatoare diferită, stohastic independentă, RP_i , cu aceeași dimensiune ca imaginea. Acest model este independent de valoarea bitului b_j . Aici se folosește modelul $+RP_i$ dacă b_j reprezintă un 0, și $-RP_i$ dacă b_j reprezintă un 1. Suma tuturor celor l secvențe aleatoare $\pm RP_i$ formează marcajul. Înaintea adăugării la imagine, marcajul se poate scala cu un factor, sau se poate limita la un anumit domeniu. Un exemplu pentru generarea unui marcaj unidimensional este prezentat în figura 2.11. Sunt folosite șapte secvențe pseudo-aleatoare diferite, pentru plasarea celor șapte biți de marcaj 0011010.

RP_0 : -1 1 1-1-1 1-1-1 1 1-1	b_0 : 0	\rightarrow	$+RP_0$: -1 1 1-1-1 1-1-1 1 1-1
RP_1 : 1 1-1-1 1-1-1 1 1-1 1	b_1 : 0	\rightarrow	$+RP_1$: 1 1-1-1 1-1-1 1 1-1 1
RP_2 : 1-1-1 1-1-1 1 1-1 1-1	b_2 : 1	\rightarrow	$-RP_2$: -1 1 1-1 1 1-1-1 1-1 1
RP_3 : -1-1 1-1-1 1 1-1 1-1-1	b_3 : 1	\rightarrow	$-RP_3$: 1 1-1 1 1-1-1 1-1 1 1
RP_4 : -1 1-1-1 1 1-1 1-1-1 1	b_4 : 0	\rightarrow	$+RP_4$: -1 1-1-1 1 1-1 1-1-1 1
RP_5 : 1-1-1 1 1-1 1-1-1 1 1	b_5 : 1	\rightarrow	$-RP_5$: -1 1 1-1-1 1-1 1 1-1-1
RP_6 : -1-1 1 1-1 1-1-1 1 1 1	b_6 : 0	\rightarrow	$+RP_6$: -1-1 1 1-1 1-1-1 1 1 1 +
			W : -3 5 1-3 1 3-7 1 3-1 3

Fig. 2.11: Exemplu pentru generarea unui marcaj CDMA pentru 7 biți b_0, b_1, \dots, b_6

W : -3 5 1 -3 1 3 -7 1 3 -1 3	
I : 98 98 97 98 97 96 97 96 95 94 94 +	
I_W : 95 103 98 95 98 99 90 97 98 93 97	
	$E[(RP_0 - E[RP_0]) \cdot (I_W - E[I_W])] = +15.6 \rightarrow b_0 = 0$
	$E[(RP_1 - E[RP_1]) \cdot (I_W - E[I_W])] = +16.4 \rightarrow b_1 = 0$
	$E[(RP_2 - E[RP_2]) \cdot (I_W - E[I_W])] = -26.4 \rightarrow b_2 = 1$
	$E[(RP_3 - E[RP_3]) \cdot (I_W - E[I_W])] = -3.1 \rightarrow b_3 = 1$
	$E[(RP_4 - E[RP_4]) \cdot (I_W - E[I_W])] = +21.6 \rightarrow b_4 = 0$
	$E[(RP_5 - E[RP_5]) \cdot (I_W - E[I_W])] = -23.6 \rightarrow b_5 = 1$
	$E[(RP_6 - E[RP_6]) \cdot (I_W - E[I_W])] = +0.4 \rightarrow b_6 = 0$

Fig. 2.12: Exemplu pentru extragerea marcajului CDMA

Fiecare bit b_j din șirul biților de marcaj 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_i . Când corelația este pozitivă, este asignată bitului de marcaj valoarea 0, altfel se presupune că bitul de marcaj este 1. Figura 2.12 arată, extragerea biților de marcaj plasați în figura 2.11.

Metodele pentru creșterea încărcăturii marcajului descrise mai sus, și anume, folosirea de porțiuni de imagine individuale pentru fiecare bit de marcaj și folosirea CDMA, au avantajele și dezavantajele lor. Dacă fiecare bit de marcaj are propria porțiune de imagine, nu există interferență între biți, și este necesar doar un număr mic de înmulțiri pentru calculul corelației. Dar dacă se decupează o porțiune de imagine se pierde biții de marcaj de la margine. Dacă se folosește tehnica CDMA, probabilitatea ca toți biții să fie recuperați după decuparea imaginii este mare. Totuși, biții de marcaj pot interfera între ei, și este necesară efectuarea multor înmulțiri pentru calcularea corelațiilor, deoarece fiecare bit este complet împrăștiat pe suprafața imaginii.

Biții de marcaj plasați, folosind metodele menționate, pot reprezenta orice: mesaje copyright, numere de serie, text simplu, semnale de control, etc. Conținutul reprezentat de acești biți poate fi comprimat, criptat și protejat prin coduri corectoare de erori. În unele cazuri poate fi util un logo ca marcaj, în locul unui șir de biți. Dacă imaginea marcată este distorsionată, logo-ul va fi afectat și el. Pentru detectarea lui pot fi exploatate capacitățile HVS de recunoaștere a modelelor [Bra97], [HW96], [VP96].

Creșterea încărcăturii marcajului poate fi făcută, [CBM02], folosind multiplexarea cu diviziune în: timp/spațiu (TDM/SDM), în frecvență (FDM), sau în cod (CDM). În primele două cazuri, imaginea este împărțită în componente spațiale sau spectrale și fiecare bit al marcajului este inserat în părți separate ale imaginii, în spațiu sau frecvență. În al treilea caz se folosește comunicația cu spectru împrăștiat cu diviziune prin cod și secvență directă, DS-CDMA. Este generat pentru fiecare bit, câte un model diferit pseudo-aleator independent și stohastic, RP_i depinzând de

valoarea acestuia (de exemplu $+RP_i$ dacă b_j reprezintă un 0 și $-RP_i$ dacă b_j reprezintă un 1). Suma celor l modele aleatoare $\pm RP_i$ reprezintă marcajul.

Codurile corectoare de erori sunt folosite pentru a crește robustețea unui marcaj. De obicei, încărcătura marcajului este codată, înainte de înserare [MDC02, AWS01, AP00, AGP02, BPGS01].

2.1.4 Formarea semnalului marcat

Cea mai simplă cale de marcare este *modulația* de amplitudine [LWBC01, RP98] sau de fază [RDB96] a imaginii originale și a marcajului (ne referim la modulația de fază numai pentru domeniul unei transformate). Energia marcajului poate fi crescută dacă este folosită mascarea perceptuală. HVS este mai puțin sensibil la schimbări în zone cu luminanță mare, contururi și texturi într-o imagine. În tehnicile aditive, cea mai simplă formă de a crește energia marcajului, fără a degrada calitatea imaginii marcate, este folosirea unui factor de câștig adaptat local [KM99, KKK02].

Un alt tip de înserare a marcajului este bazat pe *cuantizare* [CW01a, b], unde eşantioanele semnalului gazdă sunt cuantizate în funcție de bitul de marcaj, rezultând astfel semnalul marcat. Decodorul cuantizează eşantioanele primite și decide cărei cuante îi corespunde fiecare eşantion. Astfel, semnalul gazdă nu se mai comportă ca o interferență, spre deosebire de tehnicile spread spectrum.

Modulația prin cuantizare indexată QIM [CW99] este diferită de tehnicile LSB și SS. Cea mai simplă formă de marcare QIM cuantizează semnalul gazdă folosind un cuantizor indexat de mesajul de marcaj. Dacă se notează cu s semnalul marcat, cu m mesajul și cu x semnalul gazdă, atunci $s(x, m) = q_m(x)$. Semnalul rezultat va fi compus numai din valori din setul posibil al ieșirilor cuantizorului. Acest tip de marcare este adecvat mai ales în cazul în care semnalul rezultat va fi cuantizat, de exemplu prin compresie. Modulația de dither (o schemă ordonată de corecție) poate produce un semnal care conține toate valorile din semnalul gazdă. Valorile cuantizate sunt translatate, cu un nivel variabil de dither, de exemplu cu relația $s(x, m) = q_m(x + d) - d$.

Aceste tehnici sunt mai robuste, și optime din punct de vedere al transmiterii informației, decât metodele clasice de tip LSB sau SS. Dar metodele clasice QIM nu sunt robuste la scalare; o soluție este utilizarea unui pas variabil de cuantizare, folosind un model perceptual [LC05].

Tehnicile SS de marcare, care folosesc pentru detecția marcajului semnalul original, au în general performanțe mai bune decât cele care nu folosesc semnalul original. În majoritatea sistemelor SS de marcare private, secvența de zgomot pseudo-aleator alb este adăugată la semnalul original, și detectată prin corelația cu semnalul marcat. Aceasta înseamnă că marcajul este înglobat în domeniul spațial sau al transformatei semnalului printr-o adunare (operație liniară). De exemplu, dacă marcajul este adăugat în domeniul spațial, atunci imaginea marcată este dată de relația:

$$f_w = f + w. \quad (2.11)$$

unde f și f_w sunt semnalele original și, respectiv, marcat, iar w este marcajul generat pseudo-aleator. Pentru a testa existența unui marcaj w_0 într-un semnal dat f_w , se calculează intercorelația dintre f_w și w_0 . Mai precis,

$$\rho(f_w, w_0) = \rho(f, w_0) + \rho(w, w_0) \quad (2.12)$$

unde $\rho(\cdot, \cdot)$ reprezintă coeficientul de intercorelație, așa cum s-a definit în relația (2.2). Rezultatul are doi termeni: intercorelația dintre semnalul gazdă și marcajul cunoscut și intercorelația dintre marcajul extras și cel cunoscut.

Dacă $\rho(f, w_0)$ are o valoare relativ mare, detectorul poate să nu fie de încredere. Dacă este cunoscut semnalul original, prima estimare a marcajului înglobat se poate face prin scăderea semnalului original din cel marcat. Apoi rezultatul este comparat cu marcajul cunoscut, cu ajutorul coeficientului de intercorelație, îmbunătățindu-se astfel detecția.

Dezavantajele marcării [KH01], prin analogie cu comunicațiile cu SS, sunt:

- SS permite detecția unui marcaj cunoscut, dar banda largă de frecvențe cerută nu permite introducerea unei secvențe lungi de biți sau a unui *logo*, într-un semnal audio sau într-o imagine.
- Abordările SS sunt vulnerabile la problema „*near-far*”. Efectul „*near-far*” apare atunci când sursa de perturbații este mai aproape de receptor decât sursa de informații. În consecință, puterea zgomotului este mai mare decât cea a semnalului purtător de informație. Aceasta înseamnă pentru marcare că, dacă puterea marcajului scade datorită distorsiunilor cauzate de *fading*, rezultatul detecției prezintă un grad de încredere redus.
- Cele mai multe abordări SS nu sunt adaptive. Aceasta înseamnă că ele nu țin cont nici de nestaționaritatea spațială a imaginii originale, cauzată de interferențe, și nici nu includ tehnici adaptive pentru a estima variațiile statistice.
- Structura corelatorului, folosit pentru detecția marcajului, nu este eficientă în prezența *fading*-ului. Deși sistemele SS încearcă să exploateze împrăștierea marcajului pentru a media *fading*-ul, acestea nu sunt gândite pentru a maximiza performanța. În mediile în care predomină *fading*-ul, se folosește diversitatea spațio-temporală pentru a elimina efectele acestuia.

În [KH01], autorii consideră că SS nu este cel mai adecvat pentru modelarea transmisiei marcajului printr-un canal de comunicație. Transmiterea marcajului poate fi asemănătoare cu transmisia semnalului printr-un canal asociat (Figura 2.4). Se presupune că distorsiunile obișnuite ale semnalului, decuparea, filtrarea, și codarea perceptuală, nu sunt modelate adecvat, ca un zgomot de interferență de bandă îngustă, ci au un efect de *fading* asupra marcajului. Deci, folosind diversitatea și caracterizările atacurilor, marcajul poate fi făcut mai robust [KH01].

Din cauza importanței robusteții pentru cazul distorsiunilor spațiale și spectrale, marcajul se înglobează în domeniul wavelet, care localizează astfel de degradări. Acest domeniu permite o marcare robustă mai eficientă și, în cazul marcării fragile, este mai potrivit pentru a caracteriza modificările făcute cu rea intenție.

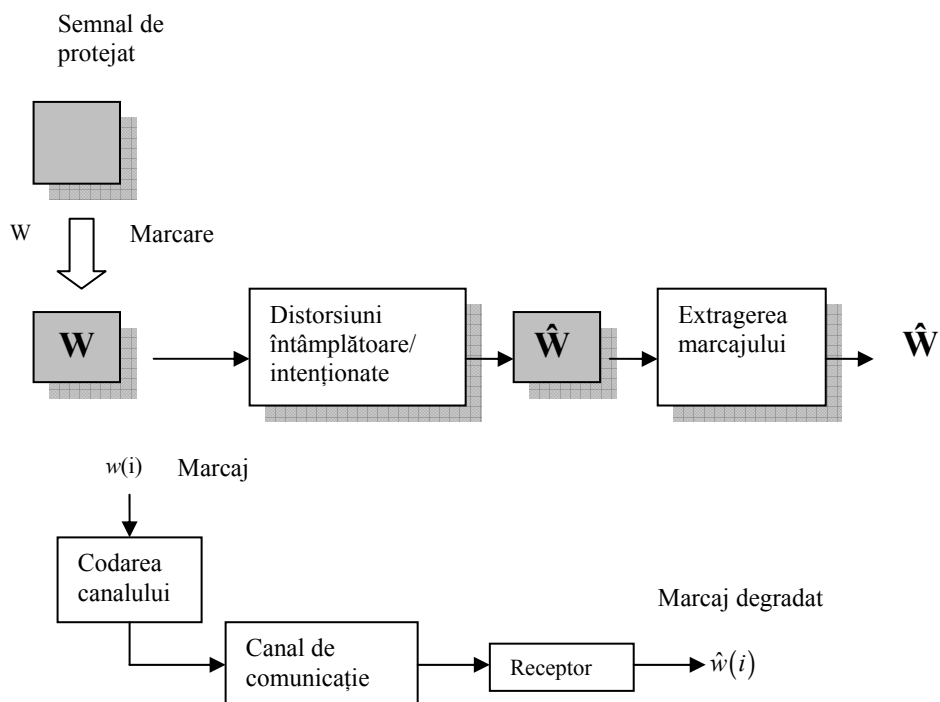


Fig. 2.13: Marcarea ca o problemă de comunicații. Înglobarea marcajului și procesul de extragere pot fi interpretate ca o transmisie într-un mediu zgomotos cu fading.

2.1.5 Extragerea marcajului

Cea mai simplă metodă de a plasa un marcaj într-o imagine, este adăugarea unui zgomot pseudo-aleator la luminozitatea pixelilor imaginii. Multe metode se bazează pe acest principiu [BGM95], [STO94], [HG96], [Pit96], [WD96].

În general zgomotul pseudo-aleator constă din numerele întregi $\{-1,0,1\}$; dar pot fi folosite și numere care nu sunt întregi. Zgomotul este generat pe baza unei chei folosind stări ale generatorului (*seeds*). Singurele constrângeri sunt ca energia lui să fie uniform distribuită, mai mult sau mai puțin, și să nu fie corelat cu conținutul imaginii gazdă. Pentru a crea imaginea marcată $I_w(x,y)$, modelul pseudo-aleator $W(x,y)$ este multiplicat cu un mic factor de câștig k și adunat la imaginea gazdă $I(x,y)$:

$$I_w(x,y) = I(x,y) + k \cdot W(x,y). \quad (2.13)$$

Pentru a detecta un marcaj într-o imagine $I_w(x,y)$, posibil marcată, se calculează corelația dintre imaginea $I_w(x,y)$ și zgomotul pseudo-aleator $W(x,y)$. În general, $W(x,y)$ este normalizat înainte de corelație, la o medie nulă. Modelele pseudo-aleatoare, generate folosind diferite chei, au o corelație foarte redusă între ele. De aceea, pe durata procesului de detecție, valoarea corelației va fi foarte mare pentru un model pseudo-aleator generat cu cheia corectă, și va fi foarte mică în caz contrar.

Pe durata procesului de detecție, se alege de obicei un prag T , pentru a decide dacă marcajul este detectat sau nu. Când corelația depășește pragul T , detectorul de marcaj stabilește că imaginea $I_w(x,y)$ conține marcajul $W(x,y)$:

$$\begin{aligned}
 R_{I_W(x,y)W(x,y)} > T &\rightarrow W(x,y) \text{ detectat} \\
 < T &\rightarrow \text{nu este detectat } W(x,y)
 \end{aligned}
 \quad (2.14)$$

Dacă $W(x,y)$ este alcătuit doar din numerele întregi $\{-1,1\}$, și dacă numărul de „-1” este egal cu numărul de „1”, corelația se poate estima ca fiind [LSL00]:

$$\begin{aligned}
 R_{I_W(x,y)W(x,y)} &= \frac{1}{N} \sum_{i=1}^N I_{W_i}^+(x,y) W_i^+(x,y) = \frac{1}{N} \sum_{i=1}^{N/2} I_{W_i}^+ W_i^+ + \frac{1}{N} \sum_{i=1}^{N/2} I_{W_i}^- W_i^- \\
 &= \frac{1}{2} \{ \mu[I_{W^+}^+(x,y)] - \mu[I_{W^-}^-(x,y)] \}
 \end{aligned}
 \quad (2.15)$$

Aici N este numărul punctelor de imagine din imaginea I_W , iar $+,-$ indică setul de puncte unde zgomotul corespunzător este pozitiv sau negativ, și $\mu[I_{W^+}^+(x,y)]$ reprezintă valoarea medie a setului de puncte în $I_W^+(x,y)$. Din relația (2.15) rezultă că problema detecției marcajului corespunde cu testarea ipotezei că două seturi de puncte de imagine, alese aleator dintr-o imagine marcată, au aceeași medie.

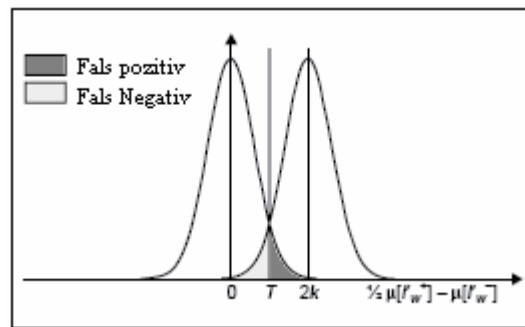


Fig. 2.14: Procedura de detecție a marcajului

Pe durata procesului de detecție, detectorul de marcaj poate comite două tipuri de erori (vezi cap. 1). Poate detecta existența marcajului, deși acesta nu există (*fals pozitiv*), sau respinge existența marcajului, deși marcajul este prezent (*fals negativ*). Funcția densității de probabilitate pentru procesul de detecție este prezentată în figura 2.14. Probabilitățile acestor două tipuri de erori rezultă pe baza modelului autoregresiv de ordin întâi a imaginii [LSL00]:

$$\begin{aligned}
 P_{fp} &= \frac{1}{2} \operatorname{erfc} \left(\frac{T\sqrt{N}}{\sigma_w \sigma_1 \sqrt{2}} \right) \quad \text{și} \\
 P_{fn} &= \frac{1}{2} \operatorname{erfc} \left(\frac{(\sigma_w^2 - T)\sqrt{N}}{\sigma_w \sigma_1 \sqrt{2}} \right)
 \end{aligned}
 \quad (2.16)$$

unde

$$\operatorname{erfc}(c) = \frac{1}{\sqrt{2\pi}} \cdot \int_c^{\infty} e^{-t^2/2} dt$$

Aici P_{fp} reprezintă probabilitatea de fals pozitiv, iar P_{fn} reprezintă probabilitatea de fals negativ (P_{fp} a fost notată în capitolul 1 cu P_{fa} , iar P_{fn} a fost notată în capitolul 1 cu P_{rej}), σ_W^2 reprezintă dispersia pixelilor marcajului și σ_I^2 reprezintă dispersia pixelilor din imagine. Dacă marcajul $W(x,y)$ constă doar din numerele întregi $\{-1,1\}$, și numărul de „-1” este egal cu numărul de „1”, dispersia marcajului, σ_W^2 , este egală cu k^2 . Erorile P_{fp} și P_{fn} pot fi minimizează crescând factorul de câștig k . Totuși, folosind valori mai mari pentru factorul de câștig, scade calitatea vizuală a imaginii marcate.

Întrucât conținutul imaginii poate interfera cu marcajul, în special în componentele de joasă frecvență, fiabilitatea detectorului poate fi îmbunătățită prin aplicarea unei filtrări adecvate înainte de corelație [DKL98, STO94]. Acest lucru scade contribuția imaginii originale la corelație. De exemplu, poate fi folosit, un filtru simplu, cu răspuns finit la impuls (FIR), de intensificare a marginilor, F_{edge} :

$$F_{edge} = \frac{1}{2} \cdot \begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}. \quad (2.17)$$

Rezultatele experimentale arată că filtrarea înainte de corelație reduce semnificativ probabilitatea de eroare, chiar dacă a fost serios afectată calitatea vizuală a imaginii marcate, înainte de corelație [HLR00], [LLL97]. În [LR00] pentru creșterea robusteții marcajului este propusă egalizarea spectrală înaintea plasării marcajului.

Cele mai multe tehnici bazate pe SS folosesc corelația pentru detecția marcajului. Acest tip de detector presupune implicit că interferența este gaussiană. Cu toate acestea, imaginile nu au o distribuție gaussiană și mulți autori sugerează prefiltrarea imaginii înainte de detecție, pentru a îmbunătăți performanța detectorului, din cauză că cea mai mare energie se află în frecvențele joase ale acesteia. Filtrarea trece-sus face ca imaginea să aibă o distribuție mai apropiată de cea gaussiană. În schemele private de marcare transparentă, extragerea imaginii originale din cea marcată, este tot o formă de prefiltrare.

În abordările bazate pe SS, se presupune că există o sincronizare perfectă între transmițător și receptor. Dacă imaginea este decupată, scalată sau transformată geometric, apare desincronizarea. Unele lucrări propun marcaje invariante la astfel de atacuri geometrice, RST, bazate pe transformarea Fourier-Mellin [RP98].

În [CM03] se propune *detecția secvențială a marcajului*, care duce la o creștere în viteză față de detectoarele cu mărime fixă. Sunt discutate optimizarea codării asociată cu detecția marcajului și autorii constată creșterea în viteză cu 70%. Metoda poate avea succes în multe aplicații practice. Detecția secvențială permite controlarea simultană a probabilităților de alarmă falsă și de eroare (*miss*). Se fixează aceste probabilități și apoi se variază numărul eşantioanelor încât să se obțină aceste probabilități. Lungimea marcajului este aleasă ad-hoc, dar autorii propun o cale de calculare a lungimii pentru o metodă dată.

2.2 Tehnici de marcare transparentă

Tehnicile de marcare transparentă din literatură pot fi grupate în trei mari clase:

-Prima include metodele din *domeniul transformatelor*, care înserează informația de marcaj prin modularea coeficienților transformatei imaginii originale.

-A doua clasă include tehnicile din *domeniul spațial*, care înserează marcajul modificând direct valorile pixelilor imaginii originale. Tehnicile care înserează marcajul în domeniul unei transformate se dovedesc a fi mai robuste la prelucrări obișnuite de semnal.

-A treia clasă sunt tehnicile care folosesc *domenii cu caracteristici speciale (feature domain)*. Aceste tehnici țin cont de regiuni, granițe și caracteristicile unui obiect. Astfel de tehnici pot prezenta avantaje în plus față de celelalte abordări, în detecția și recuperarea marcajului după atacuri geometrice.

Se face o trecere în revistă a principalelor tehnici de marcare conform cu domeniul de inserare. Sunt de asemenea considerate și exemple de tehnici din domeniul spațial și domeniul fractal. Dintre numeroasele tehnici existente, ne vom axa în principal asupra tehnicilor ce folosesc domeniul wavelet. Deși acesta pare să fie cel mai eficient până acum, vom considera în cele ce urmează și celelalte tehnici existente, pentru a avea o imagine de ansamblu asupra principalilor algoritmi.

2.2.1 Algoritmi în domeniul spațial

Multe tehnici din domeniul spațial sunt bazate pe adunarea la o imagine, a unei secvențe de zgomot pseudo-aleator. Operatorii din capitolul 1, ε și \mathcal{D} sunt adunarea și scăderea. De obicei, marcajul modifică direct valorile pixelilor din imaginea originală, și anume biții cei mai puțin semnificativi, LSB, ai imaginii gazdă. Avantajele tehnicilor de marcare bazate pe LSB includ capacitatea mare și complexitatea de calcul redusă. De aceea, este de așteptat ca ele să fie puse în practică mai ușor atunci când este vorba de marcarea în timp real. Principalul lor dezavantaj este lipsa de robustețe la falsificare, atacuri geometrice, filtrare și compresie.

Tanaka ș. a. [TNM90] au introdus ideea etichetării (tagging) imaginilor pentru ascunderea informației secrete și asigurarea drepturilor de autor. Pentru inserarea marcajului algoritmul folosește o schemă de codare cu predicție. Marcajul este inserat prin dither-area imaginii, bazată pe proprietățile statistice ale imaginii.

Caronni [Car95] descrie un sistem de urmărire a distribuției neautorizate a imaginilor. El propune marcarea imaginilor folosind modularea spațială și numește acest proces etichetare. Eticheta este un pătrat de mărime $N \times N$ cu valoarea constantă, proporțională cu luminanța locală maximă a imaginii. În primul pas, sunt identificate toate locațiile posibile din imagine unde ar putea fi inserată o etichetă, prin calcularea dispersiei locale și compararea ei cu niște limite inferioare și superioare, determinate empiric. Pentru inserare sunt folosiți numai pixelii cu dispersia minimă. Aria selectată este marcată prin adunarea/scăderea etichetei și a unei structuri aleatoare, de medie nulă. Locația etichetei și secvența de zgomot sunt generate cu o cheie. Pentru a recupera bitul inserat, se calculează diferența dintre imaginea etichetată și cea originală. Media locației, presupusă marcată, este comparată cu media locației vecine, pentru a determina valoarea bitului. Ca măsură a degradării imaginii etichetate, Caronni propune coeficientul de corelație dintre imaginea originală și cea etichetată. Coeficientul de corelație 1 arată că cele două sunt identice, dar pentru imaginile puternic afectate de procesul de marcare, acesta va fi apropiat de zero.

Primele tehnici de marcare fragilă, ca cele descrise de Walton [Wal95] și Van Schyndel [STO94], inserau marcajul direct în domeniul spațial al unei imagini. În tehnica de marcare fragilă de semnare a lui Walton, se calculează o sumă de control

pentru cei mai semnificativi 7 biți din planul de biți ai imaginii, ascunsă apoi în biți LSB aleși aleator.

Alte tehnici [STO94], [SO93], [WD96] înserează în planul de biți LSB, secvențe- m , pentru că prezintă corelații foarte bune, și se poate folosi un detector corelativ. O astfel de schemă a fost propusă în [STO94] și extinsă la 2D în [SO93].

Tirkel ș.a. [TRSH93] recunosc importanța marcării transparente și propun ca aplicații etichetarea, protejarea drepturilor de autor, protejarea împotriva falsificării și accesul controlat la imagini. Pentru imaginile alb-negru sunt propuse două metode. În prima, marcajul, sub forma unui cod PN generat dintr-o secvență- m , este înserat în planul biților LSB, a imaginii originale. Pentru acces nelimitat la planul de biți LSB, fără introducerea unor distorsiuni vizibile, imaginea este mai întâi comprimată la 7 biți, prin manipulări adaptive ale histogramei. Metoda este o extensie a metodei simple de codare LSB, prin care biții LSB sunt înlocuiți cu o informație codată. Decodarea este directă, deoarece planul LSB conține marcajul fără distorsiuni. În a doua, marcajul, generat la fel, este adunat la planul de biți LSB. Decodarea se face folosind proprietatea de autocorelație unică și optimală a secvențelor m .

Prima lucrare care menționează explicit și definește noțiunea de marcare transparentă digitală (watermarking) este lucrarea lui Schyndel ș.a. [STO94]. Sunt descrise două tehnici: în prima se înlocuiesc biții LSB ai imaginii, iar în a doua se adună o secvență PN la planul de biți LSB al imaginii originale, folosind pentru detecție autocorelația. Aceasta este de fapt și ideea folosirii secvențelor- m ; adunarea LSB este extinsă, îmbunătățită și conduce la o schemă mai robustă, folosind secvențe- m bidimensionale, 2D [TSO93].

Wolfgang și Delp [WD96] au continuat munca lui van Schyndel pentru a îmbunătăți robustețea și localizarea marcajelor, cu tehnica VW2D. Marcajul este înserat prin adăugarea unei secvențe- m bipolare, în domeniul spațial. Detecția se face printr-un detector corelator modificat. O secvență aleatoare este transformată din $\{0,1\}$ în $\{1,-1\}$, aranjată într-un bloc și adunată la imagine. Pentru a localiza falsificarea în domeniul spațial, algoritmul suprapune imaginea cu blocul de marcaj, calculează produsul scalar și îl compară cu valoarea ideală. Fie funcția de intercorelație $R_{XY}(\alpha, \beta)$ a două blocuri X și Y :

$$R_{XY}(\alpha, \beta) = \sum_i \sum_j X(i, j)Y(i - \alpha, j - \beta). \quad (2.17)$$

Fiind dată imaginea originală X , blocul de marcaj W , imaginea marcată Y și imaginea probabil falsificată Z , atunci statistica test δ pentru un bloc, e definită ca:

$$\delta = R_{YW}(0, 0) - R_{ZW}(0, 0). \quad (2.18)$$

Dacă marcajul este neschimbat, $\delta = 0$, iar dacă δ depășește un anumit prag, imaginea se consideră falsificată. Metoda detectează orice tip de filtrare și autorii susțin că o variantă îmbunătățită a acesteia detectează și compresia JPEG.

Matsui și Tanaka [MT94] propun mai multe tehnici de marcare a imaginilor. Prima metodă este bazată pe o schemă de codare cu predicție, pentru imagini cu nivele de gri, care folosește corelația dintre pixelii vecini, prin codarea erorii de predicție, în loc să codeze valorile pixelilor individuali. Imaginea digitală este scanată într-o ordine predefinită, parcurgându-se toți pixelii. Setul de pixeli este apoi codat,

folosind o schemă de codare cu predicție, păstrând prima valoare și înlocuind valorile următoare cu diferența între pixelii vecini:

$$e_i = x_i - x_{i-1}. \quad (2.19)$$

Tab. 2.1 Tabela de cifrare (sample cipher key)

Δ_i	...	-4	-3	-2	-1	0	1	2	3	4	...
c_i	...	0	0	1	1	0	1	0	0	1	...

Pentru a însera un marcaj sub forma unui șir binar, Matsui și Tanaka introduc o tabelă de cifrare cu cheie, care asignează un bit c_i fiecărei diferențe Δ_i posibile (în tabelul 2.1 este dat un exemplu). Corespondența dintre valorile biților și diferențe este ținută secretă. Pentru a însera un bit b , se selectează un pixel x_i , cu diferența corespunzătoare e_i . Se verifică în tabel dacă valoarea bitului c_i , corespunzând lui $\Delta_i = e_i$, are aceeași valoare ca și bitul b . Dacă da, se trece la înserarea următorului bit. Dacă nu, se selectează cea mai apropiată valoare de e_i în tabela de cifrare care are bitul corespunzător. Marcajul poate fi recuperat prin căutarea bitului în tabela de cifrare.

În a doua metodă se modifică schema ordonată de corecție (dither), pentru imagini binare. O schemă de corecție este formată prin compararea nivelelor monotone ale pixelilor dintr-un bloc, cu un prag dependent de poziție, și punerea pe 1 a pixelilor care depășesc pragul. Pragurile dependente de poziție sunt date într-o matrice pătrată, $N \times N$, matricea de corecție, cu elementele $d_{pq}^{(n)}$, unde n indică numărul de ordine, între zero și $N^2 - 1$, iar p și q sunt linia și coloana (vezi Fig. 2.15).

6	7	8	9
5	0	1	10
4	3	2	11
15	14	13	12

Fig. 2.15 Matrice dither concentrată pe un punct

Fiind dată o matrice de corecție, valorile de prag corespunzătoare sunt:

$$T = \left(d_{pq}^{(n)} + \frac{1}{2} \right) \times \frac{R}{N^2}. \quad (2.20)$$

unde R este gama luminanței dinamice a imaginii. Pentru a corecta o imagine, ea este împărțită în blocuri adiacente, de aceeași mărime cu matricea de corecție. Fiecare valoare dintr-o matrice este apoi comparată cu valoarea de prag corespunzătoare și modificată în consecință. Fie mulțimea perechilor de praguri:

$$S_k = \left\{ (x_i, x_j)_k \mid x_i - x_j = k; i, j = 0, 1, \dots, N; i \neq j \right\}. \quad (2.21)$$

unde x_i, x_j sunt pragurile din matricea dither. Fie $(y_i, y_j)_k$ semnalul de ieșire al lui x_i, x_j și presupunem că valorile sunt $(0,0)_k$, $(0,1)_k$, $(1,0)_k$ și $(1,1)_k$; doar două perechi $(0,1)$ și $(1,0)$ sunt considerate pentru înserarea datelor. Pentru a însera un bit b este selectată o pereche de ieșire $(y_i, y_j)_k$ și y_i este comparat cu valoarea bitului b . La valori egale perechea rămâne neschimbată, altfel y_i și y_j sunt schimbate între ele. Pentru a decoda semnătura înserată, procedura descrisă mai sus este inversată. Din nou perechile $(0,0)_k$, $(1,1)_k$ nu sunt luate în considerare.

A treia schemă este propusă pentru marcarea documentelor facsimil. Documentele facsimil sunt scanate, cu o rezoluție orizontală de aproximativ 8.22 pixeli/mm și apoi sunt comprimate folosind o codare cu pas variabil (Run Length Encoding), urmată de o codare Huffman modificată. Procesul de înserare modifică pasul variabil dintre două secvențe, schimbând pixelii. Dacă trebuie înserat un 1, pasul variabil este forțat să fie par, iar dacă trebuie introdus un 0, pasul este forțat să fie impar. Pentru o înserare validă, pasul variabil original trebuie să fie mai mare decât 1. Decodarea unui bit se face inspectând lungimea pasului variabil decodat.

Se constată că marcarea digitală, modulația digitală și mai ales modulația cu spectru împrăștiat cu secvență directă (DS-SS) au concepte similare. Astfel, s-a propus marcarea transparentă ca o comunicație afectată de zgomot negausian. Prima abordare teoretică a fost propusă de Smith [SC96]. Hernandez ș.a. [HPGR98] au făcut o analiză mai aprofundată a modulației în amplitudine a impulsurilor multiple 2D.

Bender ș.a. [BGM95, BGML96] propun două tehnici de marcare. Una din acestea, o metodă statistică de marcare, cunoscută și ca metoda *patchwork* [BGM95], împarte imaginea în 2 subseturi, A și B, unde luminanța unui subset este crescută cu o cantitate mică, iar luminozitatea celuilalt subset B este scăzută cu aceeași cantitate. Perechea de pixeli (a_i, b_i) este folosită pentru a ascunde un bit 1; se crește valoarea lui a_i cu 1, și se descrește valoarea lui b_i cu 1. Presupunând că imaginea gazdă are anumite proprietăți statistice, marcajul poate fi regăsit foarte ușor, prin medierea diferenței dintre valorile celor două subseturi. Se presupune că, dacă nu există marcaj, diferența medie este apropiată de zero. Numărul de pixeli din fiecare set fiind n : dacă pixelii din A sunt incrementați cu 1, iar cei setul B sunt decrementați cu 1, suma diferențelor între cele două seturi este egală cu $2n$:

$$\sum_n (a_i - b_i) = \begin{cases} 2n, & \text{perechi marcate} \\ 0, & \text{perechi nemarcate} \end{cases} \quad (2.22)$$

A doua metodă, numită codarea blocurilor cu textură, înserează marcajul prin copierea unui bloc de textură, într-o altă zonă a imaginii cu textură similară. Pentru recuperarea marcajului, este folosită autocorelația. Proprietatea interesantă a tehnicii este robustețea la orice fel de distorsiune, deoarece ambele zone din imagine sunt la fel distorsionate, deci recuperarea marcajului prin autocorelație încă funcționează.

Pitas și Kaskalis [NP96, Pit96, PK95] propun o metodă de înserare a semnăturii, bazată pe ideea algoritmului patchwork, folosit de Bender ș.a. [BGM95]. Marcajul $S = \{s_{m,n}\}$ este format dintr-un model binar, de aceeași mărime ca imaginea originală, având același număr de 1 ca și de 0 (distribuție uniformă). Imaginea originală I , împărțită aleator în două subseturi A și B de aceeași mărime este:

$$\begin{aligned} A &= \{x_{mn} \in I, s_{mn} = 1\} \\ B &= \{x_{mn} \in I, s_{mn} = 0\} \end{aligned} \quad (2.23)$$

Cu $x_{m,n}$ s-au notat valorile luminanței, iar m și n indică poziția pixelului. Marcajul este adăugat la imagine, prin incrementarea subsetului A cu un factor k pozitiv, de exemplu $A' = \{x_{mn} + k, x_{mn} \in A\}$. Imaginea marcată este dată de unificarea celor două subseturi, A' și B . De fapt, se adună un zgomot de frecvență înaltă la imaginea originală. Pentru a verifica prezența marcajului, este folosită testarea ipotezelor. Statistica test q este definită ca fiind diferența normalizată dintre media \bar{a}' a setului A' și media \bar{b} a setului B :

$$q = \frac{\bar{b} - \bar{a}'}{\sqrt{\sigma_{A'}^2 + \sigma_B^2}} \quad (2.24)$$

unde $\sigma_{A'}^2$ și σ_B^2 sunt variantele setului A' respectiv B . Rezultatul este comparat cu un prag pentru a determina existența marcajului. Metoda este imună la subeșantionare urmată de supraeșantionare și rezistă la compresia JPEG până la o compresie de 1:4.

O variantă îmbunătățită a acestei tehnici este propusă de Langelaar ș.a. [LLL97]. Imaginea este împărțită în pătrate cu mărimea multiplu de 8. Un singur bit este înserat prin modificarea iterativă a unui bloc selectat pseudoaleator. Fiecare bloc selectat are asignat un model pseudoaleator P , cu distribuție uniformă de 1 și 0. Pentru a însera un bit de valoare 1, modelul scalat $k \times P$ este adunat la bloc, unde k este un factor predefinit. Pentru un bit 0, modelul scalat este scăzut din bloc. Fie I_0 media tuturor valorilor pixelilor din bloc pentru care valoarea modelului corespunzător este zero, și I_1 media celorlalti pixeli. Fie diferența între cele două medii, $D_{high} = I_1 - I_0$, iar $D_{low} = \hat{I}_1 - \hat{I}_0$ diferența dintre medii, după compresia JPEG cu un factor predefinit Q . Dacă este înserat un 0 (sau 1), modelul P este scăzut iterativ din bloc, până când ambele diferențe sunt mai mici (sau mai mari) decât un prag predefinit T , sau este atins numărul maxim de iterații. Bitul poate fi extras prin calcularea diferenței D_{high} dintre cele două medii, I_1 și I_0 . Semnul diferenței este folosit pentru a determina valoarea bitului. Testele efectuate au folosit ca parametri: mărimea blocului 32x32, pragul $T=1$, factorul de scalare inițial $k=4$, și numărul maxim de iterații 6, indicând că metoda este destul de robustă la compresie JPEG, cu eroare de bit de aproximativ 5% pentru calitate JPEG 85%, și respectiv BER=20% pentru calitate JPEG 60%.

În a doua metodă, autorii propun o metodă bazată pe transformata DCT. Coeficienții DCT sunt ordonați prin scanare, iar cei de la capăt sunt puși pe zero.

Pentru a crește performanța metodelor spațiale bazate pe împărțirea imaginii în blocuri, Bruyndonckx ș.a. [BQM95] folosesc clasificarea pixelilor. Marcajul este generat modificând luminanța în blocuri 8x8 ale imaginii, adunând câte un bit de informație la fiecare bloc. Codorul alege locația secretă a blocului care va fi modificat. Pixelii, din blocuri selectate pseudoaleator, sunt clasificați în zone (1 și 2) cu valori omogene ale luminanței. Clasificarea se bazează pe trei tipuri de contrast între zone: mare, progresiv și cu zgomot. Fiecare zonă este și ea împărțită în două

categorii A și B, bazată pe un model (*grid*) definit de codor. Fiecare pixel este apoi clasificat într-una din cele patru combinații de categorii, 1/A, 1/B, 2/A și 2/B. Un bit b este înserat prin modificarea mediei categoriei pentru a satisface condițiile:

$$\begin{aligned} \text{dacă } b = 0: \quad & m_{1B}^* - m_{1A}^* = S \\ & m_{2B}^* - m_{2A}^* = S \\ \text{dacă } b = 1: \quad & m_{1A}^* - m_{1B}^* = S \\ & m_{2A}^* - m_{2B}^* = S \end{aligned} \quad (2.24)$$

unde m_{1A}^* , m_{1B}^* , m_{2A}^* și m_{2B}^* sunt mediile categoriei modificate, iar S este intensitatea de marcare. Modificarea valorilor mediilor se face prin uniformizarea dispersiei luminanței pentru toți pixelii din aceeași zonă. Pentru creșterea robusteții, autorii folosesc înserarea redundantă a biților de marcaj și coduri corectoare de erori. Autorii raportează o robustețe bună la compresia JPEG.

În [Hir96] se propune o metodă pentru autentificare și stabilirea dreptului de copyright. Se construiește un graf derivat din imagine, care conține semnătura digitală și un graf izomorf. Ambele grafuri sunt ascunse în imagine, în planul LSB. Pentru stabilirea izomorfismului grafului la receptor se aplică algoritmul ZKIP (Zero Knowledge Interactive Proof) pentru a afirma dreptul de copyright asupra imaginii. În consecință, informația secretă nu este dezvăluită în timpul autentificării.

Pentru a crește performanța marcării transparente bazată pe comunicațiile SS, în domeniul spațial, Kutter ș.a. [KJB97, KJB98] propun o metodă care înserează marcajul exclusiv în canalul pentru culoarea albastră (Blue din RGB), pentru maximizarea intensității marcajului, păstrând imperceptibilitatea. Ei propun și preprocesarea imaginii înainte de detectarea marcajului. Această operație îmbunătățește semnificativ robustețea și este aplicabilă oricărei tehnici de tip SS în domeniul spațial. Marcajul este înserat sub forma unui număr binar, printr-o modulație de amplitudine în domeniul spațial. Într-o poziție (i, j) aleasă aleatoriu, este înserat un singur bit b ; în funcție de valoarea bitului, se adună sau se scade o cantitate proporțională cu luminanța din acea locație:

$$B_{i,j} \leftarrow B_{i,j} + \alpha(-1)^b L_{i,j} \quad (2.25)$$

unde $B_{i,j}$ este valoarea din poziția (i, j) a canalului albastru, $L_{i,j}$, luminanța din acea locație, iar α , intensitatea de marcare. Pentru a recupera bitul de marcaj, se calculează un estimat al valorii imaginii nemarcate, folosind o combinație liniară a pixelilor adiacenți, în formă de cruce:

$$\hat{B}_{i,j} = \frac{1}{4c} \left(\sum_{k=-c}^c B_{i+k,j} + \sum_{k=-c}^c B_{i,j+k} - 2B_{j,k} \right) \quad (2.26)$$

unde c este mărimea ferestrei în formă de cruce. Valoarea bitului este dată de semnul diferenței $\delta_{i,j}$ dintre pixelul posibil marcat și cel estimat original. Pentru a crește robustețea, fiecare bit este înserat de mai multe ori, iar la extragere, se folosește o logică majoritară. Având cheile potrivite, ambele marcaje originale pot fi recuperate.

Extensiile acestei metode au îmbunătățit robustețea și chiar recuperarea marcajului după atacuri geometrice [Kut98] sau atacurile de tip print și scan.

Macq ș.a. [MQ95] au introdus marcarea transparentă adaptivă funcție de HVS, folosind mascarea și modularea. Marcajul, o structură binară, este filtrat trece-jos, modulat în frecvență, mascat și apoi adunat la imaginea gazdă. Este folosită o cheie secretă pentru a determina frecvențele de modulație și localizarea marcajului. Pentru mascare, este folosit rastrul (grating) o extensie a fenomenului de mascare pentru semnale monocromatice. Pentru a adapta și mai bine marcajul la imagine, este folosită o masca perceptuală, bazată pe zone morfologice omogene de frecvență înaltă. Recuperarea marcajului se face prin demodulare, urmată de o corelație.

P. Wong [WPW98] descrie o tehnică de marcarea fragilă, care obține un rezumat al imaginii utilizând o funcție *hash*. Imaginea, dimensiunile ei și cheia de marcarea sunt modificate de funcția *hash* în timpul inserției și sunt folosite pentru a schimba bitul LSB al imaginii originale. Astfel că, atunci când informația suplimentară corectă și imaginea marcată nealterată sunt furnizate detectorului, se obține o imagine binară aleasă de proprietar (de exemplu un *logo* al unei companii). Metoda are proprietăți de localizare și poate identifica regiuni de pixeli modificați în imaginea marcată.

Tehnica lui Yeung și Mintzer [YM97] este mai complicată, nu doar de înserare a unei valori binare în cel mai puțin semnificativ bit. Cheia de marcarea este folosită pentru a genera secvențe pseudo-aleatoare (una pentru fiecare canal sau componentă a culorii) care controlează modificările ulterioare ale pixelilor. După inserție, este folosit un proces de difuzie a erorilor pentru răspândirea efectelor pixelilor alterați, făcând ca marcajul să fie mai greu de văzut

Metodele recente [STHW04] aplică marcajul în planul LSB, și în alte planuri, sau într-o combinație a acestora. Cantitatea de date înserată poate fi fixă sau variabilă, depinzând de numărul de pixeli selectați, de luminanță și de contrast.

Într-o manieră diferită, Voyatzis și Pitas [VP96a, VP96b] marchează imaginile prin înserarea unui logo, folosind automorfisme toroidale. Un automorfism toroidal poate fi considerat ca o transformare spațială a regiunilor plane care aparțin unei arii pătratice 2D, fiind definit în subsetul $U = [0,1) \times [0,1) \in R^2$ prin:

$$\mathbf{r}' = \mathbf{A}\mathbf{r}, \quad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{1}. \quad (2.27)$$

Acțiunile iterative ale lui \mathbf{A} asupra unui punct \mathbf{r}_0 formează un sistem dinamic, care poate fi exprimat ca o hartă (map):

$$\mathbf{r}_{n+1} = \mathbf{A}^n \mathbf{r}_0 \pmod{1} \quad \text{sau} \quad \mathbf{r}_{n+1} = \mathbf{A}\mathbf{r}_n \quad (2.28)$$

Un exemplu de automorfism în dinamică este “cat map”, definit ca:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{1}.$$

Setul de puncte $\{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \dots\}$ este numit orbita sistemului. Un astfel de sistem “amestecă” sau mixează haotic punctele. În anumite circumstanțe, automorfismul

poate avea orbite periodice, adică după T iterații punctul curent este același cu cel initial, $\mathbf{A}^T \mathbf{r}_0 = \mathbf{r}_0$.

Pentru marcarea unei imagini, un marcaj pătratic, sub forma unei imagini binare mai mică decât imaginea gazdă, este mai întâi mixat cu automorfismul \mathbf{A}_N . Marcajul mixat este suprapus peste un bloc selectat din imaginea originală, folosind o funcție de înserare, ca modificarea LSB. Recuperarea marcajului se face prin extragerea marcajului mixat din imaginea semnată, urmată apoi de reconstrucția marcajului folosind automorfismul \mathbf{A}_{N-T} , unde T este perioada automorfismului în sistemul dat. Robustețea poate crește prin proceduri sofisticate de suprapunere/înserare.

Înserarea marcajului nu este bazată numai pe principiul modulării SS. Chen și Wornell [CW01a,b] au propus cuantizarea. Metoda lor numită QIM (Quantized Index Modulation), modulația prin cuantizare indexată folosește un set de cuantizoare N -dimensionale, care satisfac o condiție de distorsiune. Sunt construite astfel încât valorile de reconstrucție dintr-un cuantizor să fie „depărtate” de punctele de reconstrucție ale altui cuantizor. Mesajul de transmis este folosit ca index pentru selectarea cuantizoarelor. Cuantizorul selectat este folosit apoi pentru înserarea informației, prin cuantizarea pixelilor în domeniul spațial sau DCT. La decodare este folosită o metrică de evaluare a tuturor cuantizoarelor, iar indexul cuantizorului cu distanța minimă identifică informația înserată. Autorii arată că performanța schemei propuse este superioară celei standard cu modulație SS.

Pe lângă tehnicile care folosesc modulația din domeniul spațial, Maes ș.a. [MO98] propun modificarea proprietăților geometrice ale imaginii. Metoda se bazează pe un model de linii dense generat pseudoaleator, care reprezintă marcajul. Se calculează un set de puncte reprezentative, cu un filtru detector de muchii. Punctele detectate sunt apoi deviate, astfel ca multe puncte să fie în vecinătatea liniilor. La detecție, se verifică dacă un număr semnificativ de puncte sunt în vecinătatea liniilor din model.

În [CB01], marcajul se înserează cu ajutorul a două chei. Prima codează bitul într-un bloc de pixeli, iar a doua generează secvența de marcaj. Înserarea marcajului se face prin adunarea sau scăderea modelului pseudo-aleator în domeniul spațial; intensitatea de înserare este dată de distribuția densității spectrale a coeficienților DCT și tabela de cuantizare JPEG, pentru a crește robustețea la compresia JPEG. Modelul este un șir de biți înserați într-un set pătratic de blocuri și repetat pe toată imaginea. La detecție, se verifică marcajul cu operația XOR. Metoda este rezistentă la filtrare, decupare, zgomot aditiv (marcaj detectat cu BER 3.17% respectiv BER 22.2% pentru 15% respectiv 20% zgomot uniform) și alte atacuri.

2.2.2 Algoritmi în domeniul unei transformate

Au fost propuse multe tehnici care se folosesc o transformată. Pentru înserarea marcajului, este aplicată semnalului gazdă o transformare și apoi sunt modificate coeficienții transformatei. Transformatele au fost studiate mai ales în contextul codării și compresiei imaginii, dar multe rezultate sunt aplicabile și pentru marcarea transparentă. În cele mai multe imagini culorile pixelilor adiacenți sunt corelate. Trecerea imaginii într-un domeniu al unei transformate, ca DCT sau DWT, ar trebui să decoreleze eșantioanele originale și să concentreze energia semnalului original în câțiva coeficienți. O imagine codată în frecvență are energia concentrată în

coeficienții cu index mic, deci conține mai ales componente de joasă frecvență. Ele reprezintă forma și caracteristicile globale ale imaginii, luminanța și contrastul. Frecvențele înalte reprezintă muchiile imaginii, dar contribuie puțin la energia din domeniul spațial-spectral. O imagine ar putea conține 95% din energia sa în 5% din frecvențele cele mai joase ale transformatei DCT bidimensionale. Obiectivul creării unei tabele de cuantizare adecvate pentru compresia JPEG este reținerea acestor coeficienți DCT, și componente de frecvență înaltă suficiente pentru a avea destule muchii, ca să fie acceptabilă vizual.

Metodele din [RDB96], [RDB96b], [BP96a], [BP96b], [NP96], [PI96], [BRD95], [CKLS95], [CKLS96], [HG96] sunt primele în domeniu și reprezintă un cadru de cercetare fundamental pentru marcarea. În [FKK01], [FKK04] se determină domeniul în care este maximizată capacitatea marcajului. Autorii se concentrează asupra compresiei cu pierderi, care implică cuantizarea într-un anumit domeniu. Folosind o cuantizare liniară, se estimează capacitatea de marcarea pentru diferite domenii. Se precizează cele mai adecvate transformate pentru marcarea la compresia JPEG. Autorii constată că un cod de repetiție și marcarea într-alt domeniu decât al compresiei cresc capacitatea de marcarea.

2.2.2.1.a Metode bazate pe DCT

Există o multitudine de metode care folosesc transformata DCT a întregii imagini, sau pe blocuri de 8x8. Dintre cele mai cunoscute sunt metodele propuse de Cox ș.a. [CKLS95], [CKLS96] și Koch și Zhao [KZ95].

Matsui și Tanaka [MT94] propun o metodă bazată pe modificarea coeficienților DCT, într-o schemă de transmisie progresivă. Biții de marcaj sunt înserați modificând regula de rotunjire a coeficienților cuantizați, astfel încât coeficienții rezultati, să fie pari sau impari, în funcție de biții marcajului.

Marcarea eficientă în domeniul DCT a fost introdusă de Koch ș.a. [KZ95, BKZ98]. Imaginea este împărțită în blocuri 8x8, ca la compresia JPEG și apoi se calculează transformata DCT a fiecărui bloc. Dintr-un bloc selectat pseudoaleator, se alege o pereche de coeficienți de frecvență medie, din 12 perechi predeterminate. Pentru înserarea unui bit, coeficienții sunt astfel modificați (cuantizați) încât diferența lor să fie ori pozitivă ori negativă, funcție de valoarea bitului. Pentru a fi rezistentă la compresia JPEG, este luată în considerare matricea de cuantizare JPEG, când se alterează coeficienții DCT. Metoda are o robustețe bună la compresii JPEG cu un factor de calitate de până la 50%.

De fapt se modifică diferența dintre coeficienții de frecvență medie, selectați aleator în blocuri DCT ale imaginii originale, alese tot aleator. Se folosește ca marcaj o secvență binară, $w \in \{0,1\}$. Din fiecare bloc b_i , sunt selectați doi coeficienți de frecvență medie $f_b(m_1, n_1)$ și $f_b(m_2, n_2)$; apoi fiecare bloc este cuantizat cu un factor de cuantizare Q , conform matricii de cuantizare JPEG. Diferența absolută dintre coeficienții selectați este:

$$\Delta_b = \left| f_b(m_1, n_1) \right| - \left| f_b(m_2, n_2) \right|. \quad (2.29)$$

Un bit de informație w_i este înserat într-un bloc b_i , modificând perechea $f_b(m_1, n_1)$ și $f_b(m_2, n_2)$, astfel încât distanța dintre cei doi să devină:

$$\Delta_b = \begin{cases} \geq q, & \text{daca } w_i = 1 \\ \leq -q, & \text{daca } w_i = 0 \end{cases} \quad (2.30)$$

unde q este un parametru ce controlează intensitatea de marcare. Algoritmul nu este foarte robust, din cauză că doi coeficienți per bloc sunt marcați. Algoritmul nu este robust nici la scalare, decupare, fiindcă dimensiunile imaginii sunt folosite pentru a genera o secvență de marcaj adecvată. Efectele introduse sunt vizibile, din cauză că marcajul este inserat în domeniul DCT 8x8. Ele pot fi văzute mai ușor în zonele omogene, nu în contururi. Se schimbă coeficienții de frecvență medie, din blocurile cu nivele de cuantizare identice, cu tabela de cuantizare JPEG color; astfel un coeficient $B(u_1, v_1)$ va fi mai mare decât celălalt $B(u_2, v_2)$, dacă bitul este "1", și mai mic dacă bitul este "0". O altă posibilitate este schimbarea ușoară a unor tripleți de coeficienți de frecvență medie.

Bors și Pitas [BP96a, BP96b, BP98] propun modificarea coeficienților DCT care satisfac o condiție de selecție a poziției blocului. Imaginea este împărțită în blocuri 8x8, selectate cu un clasificator gaussian cu rețele. Coeficienții DCT de frecvență medie sunt modificați folosind o constrângere DCT liniară sau o regiune DCT de detecție circulară, pentru a ascunde informația de marcaj. În prima abordare, constrângerea liniară este dată de:

$$Y = \mathbf{FQ} \quad (2.31)$$

unde \mathbf{F} este vectorul de coeficienți DCT modificat, iar \mathbf{Q} este vectorul ponderilor format de către marcaj. Constrângerea este impusă prin schimbarea coeficienților DCT bazată pe criteriul minimizării pătratelor. Al doilea algoritm definește regiunile circulare din jurul coeficienților DCT selectați, coeficienții care sunt apoi cuantizați:

$$\|\mathbf{F} - \mathbf{Q}_k\|^2 = \min_{i=1}^H \|\mathbf{F} - \mathbf{Q}_i\|^2 \quad \text{atunci } \mathbf{F} = \mathbf{Q}_k \quad (2.32)$$

unde $\mathbf{Q}_i, i=1, \dots, H$ este setul vectorilor cu coeficienți formați din marcaj. În recuperarea marcajului, algoritmul verifică mai întâi constrângerea asupra coeficienților DCT din toate blocurile, urmată de constrângerea asupra localizării. Algoritmul rezistă la compresia JPEG pentru o rată de compresie de 13:1, respectiv 18:1, folosind constrângerea DCT liniară sau regiunea de detecție circulară DCT.

Swanson ș.a. [SZT96] propun o metodă de marcare în domeniul DCT, bazată pe mascarea spectrală a blocurilor DCT, similară cu cea propusă de Smith și Comiskey [SC96]. Imaginea gazdă este împărțită în blocuri pătrate, și se calculează transformata DCT pentru fiecare. Pentru fiecare bloc DCT, este calculată o mască spectrală, știind că mascarea de tip grilă crește pragul vizual în jurul frecvenței de mascare pentru aceste semnale de tip grilaj. Maska perceptuală rezultantă este adăugată la blocul DCT, prin scalare și înmulțire cu o secvență PN de lungime maximă. Procesul de inserare prevede și post-procesarea de mascare spațială pentru a face marcajul invizibil și pentru a controla factorul de scalare. Detecția necesită imaginea originală și marcajul original; ea se face prin testarea ipotezelor. Autorii raportează o robustețe bună la compresia JPEG, zgomot colorat și decupare.

Tao și Dickinson [TD97] introduc o tehnică adaptivă de marcare, în domeniul DCT, bazată pe un clasificator perceptual regional, cu indecși de sensibilitate.

Marcajul este înserat în N coeficienți DCT, tip AC. Aceștia sunt selectați să aibă pașii de cuantizare cei mai mici, conform tabelii de cuantizare JPEG. Coeficienții x_i selectați sunt modificați după cum urmează:

$$\hat{x}_i = x_i + \max \left[x_i \alpha_m, \text{sign}(x_i) \frac{D_i}{k} \right]. \quad (2.33)$$

unde α_m definește indexul sensibilității la zgomot pentru blocul curent, D_i este pasul de cuantizare pentru X_i , iar k satisface condiția $5 \leq k \leq 6$. Aici, marcajul nu este generat aleator. Există mai multe căi de determinare a sensibilității la zgomot, folosind mascarea HVS. Algoritmul folosește efectele de mascare a luminanței, a muchiiilor, precum și a texturilor. Autorii propun un algoritm de clasificare în regiuni, care clasifică blocurile în șase clase perceptuale: muchie, sensibilitate uniformă joasă, moderat ocupată, ocupată, foarte ocupată, în ordinea descrescătoare a sensibilității la zgomot. Fiecare clasă perceptuală are asociat un index de sensibilitate la zgomot. Recuperarea marcajului se face cu ajutorul imaginii originale, a marcajului și a testării ipotezelor. Metoda este robustă la compresia JPEG până la un factor de calitate de 5% și zgomot aleator cu raportul semnal-pe-zgomot maxim PSNR de 22.1 dB.

Podilchuk [PZ98] propune marcarea perceptuală, folosind diferența abia sesizabilă JND (Just Noticeable Difference), pentru a determina masca de modulare a marcajului, dependentă de imagine. Modularea marcajului cu coeficienții selectați se face în domeniul DCT sau wavelet:

$$I_{u,v}^* = \begin{cases} I_{u,v} + JND_{u,v} \times w_{u,v}, & \text{dacă } I_{u,v} > JND_{u,v} \\ I_{u,v}, & \text{altfel} \end{cases}. \quad (2.34)$$

unde $I_{u,v}$ sunt coeficienții transformatei imaginii originale, $w_{u,v}$ sunt biții marcajului, iar $JND_{u,v}$ sunt valorile JND calculate cu modele vizuale. Pentru transformata DCT, autorii folosesc modelul perceptual al lui Watson, care folosește sensibilitatea în frecvență și luminozitate, precum și mascarea de contrast locală. Acest model calculează pragurile de mascare dependente de imagine, pentru fiecare bloc în parte. Detecția se face prin corelația dintre diferența imaginii originale și marcate și secvența de marcaj. Corelația maximă este comparată cu un prag, pentru a determina existența marcajului. Metoda este foarte robustă la compresia JPEG, decupare, scalare, zgomot aditiv, corecția de gamă și atacuri de tip imprimare-copiere-scanare. Pentru atacuri care implică transformări geometrice, înainte de detecție trebuie aplicate operațiile inverse.

În [PBBC97] și [BBCP98a] se descrie o metodă bazată pe transformata DCT, care folosește caracteristicile HVS. Marcajul este o secvență pseudoaleatoare de M numere reale, cu distribuție normală $\mathbf{X} = \{x_1, x_2, \dots, x_M\}$. Coeficienții transformatei DCT, a imaginii originale de dimensiune $N \times N$, sunt reordonați într-un vector, prin scanare în zig-zag (la fel ca la JPEG). Din vector, se aleg coeficienții cu indexul $(L+1)$ până la $(L+M)$, M fiind lungimea aleasă a marcajului (16000 aici) și L poziția de unde începe înserarea, pentru a genera vectorul $\mathbf{T} = \{t_{L+1}, t_{L+2}, \dots, t_{L+M}\}$. Detecția se

face fără imaginea originală. Pentru reducerea probabilității de eroare, înserarea se face folosind valoarea absolută a coeficienților:

$$t'_{L+i} = t_{L+i} + \alpha |t_{L+i}| x_i \quad (2.35)$$

unde α este intensitatea de înserare. Coeficienții modificați înlocuiesc pe cei originali înainte de reconstrucția imaginii marcate I' .

Deși formula de înserare a marcajului este construită să țină cont de HVS, marcajul este vizibil în unele regiuni ale imaginii. De aceea, după înserare, sunt folosite caracteristicile de mascare spațială ale HVS; imaginea originală I și cea marcată I' sunt adunate pixel cu pixel, conform unui factor local adaptiv $\beta_{i,j}$, rezultând o nouă imagine marcată I'' :

$$y''_{i,j} = y_{i,j} (1 - \beta_{i,j}) + \beta_{i,j} y'_{i,j}. \quad (2.36)$$

Parametrul $\beta_{i,j}$ este dispersia, calculată pe un bloc 9x9, centrat pe pixelul $y_{i,j}$, și normalizată la maximul dispersiilor tuturor blocurilor.

Detecția se face astfel neinformată, folosind corelația dintre marcajul original și coeficienții posibil marcați:

$$z = \frac{\mathbf{Y} \cdot \mathbf{T}^*}{M} = \frac{1}{M} \sum_{i=1}^M y_i t_{L+i}^* \quad (2.37)$$

Pragul de decizie este estimat, cu metode statistice, folosind imaginea recepționată:

$$T'_z = \frac{\alpha}{3M} \sum_{i=1}^M |t_i^*| \quad (2.38)$$

Rezultatele experimentale sunt foarte bune, metoda fiind robustă la mai multe tipuri de atacuri, compresie JPEG, filtrare mediană, marcare multiplă, dar și distorsiuni geometrice (după aplicarea transformării geometrice inverse).

Tehnicile de marcare în domeniul spectral au fost introduse prima oară de Boland ș.a. [BRD95] și Cox ș.a. [CKLS95], care au dezvoltat independent metode perceptuale adaptive bazate pe modulare. Cox ș.a. propun o metodă bazată pe SS [CKLS95]. Autorii susțin că marcajul trebuie plasat în componentele perceptuale cele mai semnificative, rezistente la compresie și la prelucrările obișnuite. Marcajul este o secvență $X = x_1, \dots, x_n$ de 1000 de numere reale aleatoare, alese dintr-o distribuție gaussiană $\mathcal{N}(0,1)$, care crește invizibilitatea și robustețea. Marcajul X este înserat în imaginea V pentru a produce secvența de coeficienți V' modificați.

Când se înserează X în V , pentru a obține V' , se specifică un parametru de scalare α , care determină măsura în care X modifică pe V . Pentru calcularea lui V' se poate folosi una din cele trei formule:

$$v'_i = v_i + \alpha x_i. \quad (2.39)$$

$$v'_i = v_i (1 + \alpha x_i). \quad (2.40)$$

$$v'_i = v_i e^{\alpha x_i}. \quad (2.41)$$

unde x_i este bitul de marcaj, α este intensitatea de marcare, iar v_i sunt coeficienții perceptual semnificativi. Fiind dat V^* , se poate calcula funcția inversă pentru a obține X^* din V^* și V . Ecuația (2.39) este totdeauna inversabilă, iar ecuațiile (2.40) și (2.41) sunt inversabile dacă $v_i \neq 0$.

Ecuația (2.39) nu e potrivită dacă valorile lui v_i variază mult. Dacă $v_i = 10^6$, adăugând 100 s-ar putea să fie insuficient pentru recuperarea marcajului, dar dacă $v_i = 10$ adăugând 100 va distorsiona această valoare într-o măsură inacceptabilă. Inserția bazată pe ecuația (2.40) sau (2.41) este mai rezistentă împotriva acestor variații mari. Este de menționat că (2.40) și (2.41) dau rezultate similare dacă αx_i este mic. De asemenea dacă v_i este pozitiv, atunci (2.41) este echivalent cu $\log(v_i) = \log(v_i) + \alpha x_i$, și poate fi privit ca o aplicație a lui (2.39) pentru cazul în care sunt folosiți logaritmi valorilor originale.

Autorii [CKLS97] sugerează că nu este suficient un singur parametru de scalare α , pentru perturbarea tuturor valorilor lui v_i , deoarece diferitele componente spectrale ar putea avea toleranța la modificări diferită. În relația $v_i' = v_i (1 + \alpha_i x_i)$, se pot folosi parametri de scalare multipli $\alpha_1, \alpha_2, \dots, \alpha_n$. Un α_i mare înseamnă că v_i se modifică cu un factor mare, fără să se modifice calitatea perceptuală a documentului. Parametrul α_i poate fi privit ca măsura relativă a modificării lui v_i .

Detecția se face pe baza similarității dintre marcajul original X și marcajul X^* extras din imaginea marcată și atacată:

$$\text{sim}(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X^*}}. \quad (2.42)$$

Algoritmul este robust la manipulări de tip compresie JPEG (calitate 5%), dithering, transmisie fax, imprimare-copiere-scanare, marcare multiplă, atacul de coliziune. În experimente, marcajul a avut o lungime de 1000 de numere cu distribuția $N(0,1)$, $\alpha = 0.1$, iar coeficienții selectați sunt cei maximi, cu excepția componentei continue. Robustețea se datorează selecției coeficienților importanți din punct de vedere perceptual. Algoritmul nu este robust la atacul de inversiune propus de Craver ș.a. [CMYY97], iar efectuarea transformatei DCT pe toată imaginea face ca algoritmul să fie lent. Boland ș.a. propun o tehnică similară bazată pe modulația de amplitudine și modulația de frecvență de tip FSK (Frequency Shift Keying); ei sugerează folosirea unor transformate cum ar fi: DCT, wavelet, Walsh-Hadamard, și transformata Fourier rapidă, FFT.

Cuantizarea pară-impară este o tehnică simplă care înserează un bit “0” sau “1” folosind operatorii de cuantizare pară sau impară [WL02a], [WL02b]. Marcarea diferențiată alterează energia a două grupuri de blocuri DCT, A și B, încât $E_A < E_B$ dacă bitul de marcaj este “1”. Înainte de a schimba energia acestor blocuri, blocurile DCT sunt schimbate aleator astfel încât aceste perechi de blocuri A-B să fie selectate tot aleator în imagine, crescând astfel securitatea metodei de marcare [LL01].

În [BTS05] se consideră mai adecvată modelarea coeficienților DCT cu “cozi lungi” (familia alpha-stable), decât funcțiile exponențiale precum modelul gaussian generalizat [HPGA98]. Pentru detecția oarbă, se folosește distribuția Cauchy din familia alfa-stabilă. Distribuția este singura cu formă compactă, din familia alfa-stabilă simetrică negaussiană, și conduce la un detector aproape optimal.

2.2.2.1.b Metode bazate pe transformata DFT

Ruanaidh ș.a. [RDB96, RDB96b] propun marcarea folosind faza DFT. Pentru a însera un bit, este modificată faza unui coeficient selectat $F(k_1, k_2)$ prin adunarea unei valori mici δ :

$$\angle F(k_1, k_2) \leftarrow F(k_1, k_2) + \delta \quad (2.43)$$

Pentru ca imaginea marcată să fie reală, faza trebuie să satisfacă simetria impară, ceea ce conduce la o modificare suplimentară:

$$\angle F(N_1 - k_1, N_2 - k_2) \leftarrow \angle F(N_1 - k_1, N_2 - k_2) + \delta \quad (2.44)$$

unde $0 \leq k_1 < N_1$ și $0 \leq k_2 < N_2$. Coeficienții sunt modificați numai dacă puterea lor relativă este mai mare decât un prag dat. Dacă imaginea originală este cunoscută, marcajul poate fi recuperat cu ușurință comparând faza. Atunci când aceasta nu este cunoscută la detector, Ruanaidh sugerează folosirea cuantizării fazei originale înainte de modificarea ei. Deviațiile dintre stările cuantizate sunt apoi folosite pentru a ascunde marcajul.

2.2.2.1.c Metode care aplică transformata Fourier-Mellin

Ruanaidh ș.a. [HPRP98] propun o metodă care plasează marcajul într-un domeniu invariant la rotire, scalare și translație, folosind o combinație dintre transformata Fourier discretă, DFT, și reprezentarea polară logaritmică, LPM (log polar map). Figura 2.16 prezintă o schemă a acestei metode de marcare transparentă.

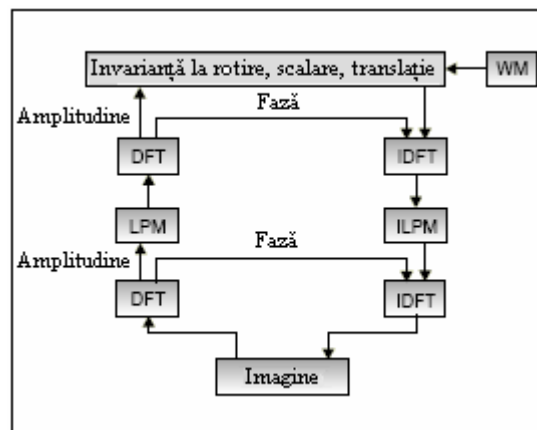


Fig. 2.16: Schemă de marcaj transparent invariantă la rotire, scalare, și translație

În primul pas, este calculată transformata DFT a imaginii originale. Una din proprietățile transformatei DFT este că o translație în domeniul spațial este echivalentă cu o deplasare de fază în domeniul DFT. Astfel, dacă se păstrează numai amplitudinea coeficienților DFT, se obține un domeniu invariant la translații. În pasul următor, pentru fiecare coordonată carteziană (u, v) a amplitudinilor DFT este determinat un punct corespunzător (μ, θ) în LPM:

$$u = e^{\mu} \cos \theta \quad v = e^{\mu} \sin \theta \quad (2.45)$$

unde $\mu \in R$ și $0 < \theta < 2\pi$.

Sistemul de coordonate polar logaritmice transformă rotirea și scalarea din domeniul cartezian, în translații de-a lungul axei orizontale și verticale. În continuare, prin folosirea amplitudinii DFT a coordonatelor LPM, se obține un domeniu invariant la rotire, scalare și translație. Transformata Fourier pentru LPM este echivalentă cu transformarea Fourier-Mellin. Combinând cei doi pași se obține o transformare invariantă la rotire, scalare și translație. Marcajul ia forma unui semnal SS bidimensional. În teste, marcajul are 104 biți, imaginea marcată este rotită cu 143° și scalată la 75% pe fiecare axă. Marcajul este recuperat cu succes din imaginea astfel atacată. Metoda este rezistentă la compresie JPEG până la calitatea de 75% și decupare la 50% din imaginea originală. Această metodă a fost prima construită special pentru a rezista atacurilor RST.

În Figura 2.17 se pot vedea proprietățile LPM. Partea (b) arată LPM al imaginii Lena (a). Partea (c) ne arată o versiune rotită și scalată a imaginii Lena, și (d) ne arată LPM corespunzătoare lui (c). Se poate vedea clar că rotirea și scalarea în domeniul spațial, original sunt convertite în translații în domeniul LPM.

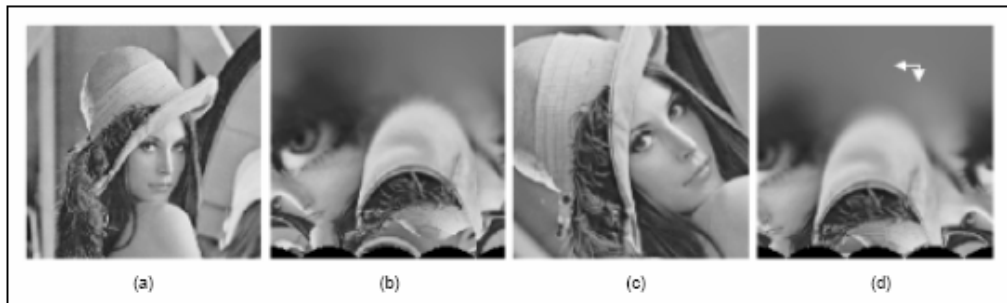


Fig. 2.17: Exemplu al proprietăților LPM. (a) Imaginea originală, (b) LPM lui (a), (c) Scalat și rotit, și (d) LPM lui (c)

Implementarea practică a schemei anterioare s-a dovedit a fi dificilă. De aceea autorii au propus o abordare diferită, unde un marcaj transparent CDMA este plasat în domeniul amplitudinii DFT invariante la translații. Pentru a face marcajul transparent invariant la scalare și rotire, se plasează un al doilea marcaj transparent ca șablon, în acest domeniu [HRPP98], [RPHP99]. Pentru a extrage marcajul transparent, mai întâi se determină scara și orientarea imaginii marcate, folosind șablonul, astfel:

- se calculează transformata DFT a imaginii marcate,
- se calculează coordonatele LPM ale amplitudinilor coeficienților DFT și ale modelului șablonului
- se calculează diferențele (offset) orizontale și verticale dintre cele două LPM, cu tehnici de căutare și intercorelație, rezultând un factor de scalare și rotire.

În final, imaginea este transformată înapoi la mărimea și orientarea originală, și este extras marcajul purtător de informație. O variantă a acestei metode a fost propusă de Lin ș.a. [LWBC01], folosind transformata Radon.

2.2.2.1.d Domeniul wavelet

Boland ș.a. [BRD95] au propus prima dată înserarea marcajului folosind o descompunere multirezoluție. Marcajul este un model pseudoaleator bidimensional. Imaginea și marcajul sunt descompuse folosind transformata wavelet discretă 2D, și marcajul este adăugat în fiecare subbandă a imaginii prin ponderare. Decodarea se face prin corelație normalizată între estimarea marcajului și marcajul original. Au fost

propușe mai multe scheme folosind transformata wavelet [IMK99, Kun99, XBA97, ZXZ98], diferența fiind modul de ponderare pentru a diminua efectele vizibile. Majoritatea înserează marcajul în subbenzi de detaliu, cu mici excepții [JSSK02].

O tehnica perceptuală [WQF98] înserează marcajul astfel încât zgomotul să nu depășească diferența abia sesizabilă, JND, pentru fiecare coeficient. Ordinea de însereare este ca cea a semnificației vizuale. Este garantată invizibilitatea și robustețea, dar nu și securitatea, ceea ce este un dezavantaj major.

Zhu ș.a. [ZXZ98] implementează o tehnică de marcare în domeniul wavelet, cu 4 nivele de descompunere, folosind ca marcaj o secvență gaussiană de numere pseudo-aleatoare. Sunt marcate numai benzile de detaliu. Dacă W_j este secvența de marcaj w_j de la nivelul de rezoluție j , este satisfăcută relația:

$$\dots \subset W_3 \subset W_2 \subset W_1$$

Lungimea marcajului W_j pentru o imagine de mărimea $M \times M$ este dată de:

$$N_j = 3 \frac{M^2}{2^{2j}} \quad (2.46)$$

Acest algoritm poate fi ușor adaptat pentru tehnici de marcare video, bazat pe transformata wavelet 3D, datorat tocmai simplității. Natura ierarhică a dezvoltării wavelet permite detecția multirezoluție a marcajului, care este un vector gaussian aleator adunat la toți coeficienții din benzile de frecvență înaltă, în domeniul wavelet. S-a arătat că atunci când imaginea este comprimată, marcajul poate fi identificat corect la fiecare nivel de rezoluție. Marcajul nu este sigur deoarece, când se cunoaște algoritmul, poate fi extras statistic de atacatori.

Podilchuk [PZ98] propune marcarea perceptuală folosind diferența abia sesizabilă, JND, pentru a determina masca de modulare a marcajului, dependentă de imagine. Modularea marcajului cu coeficienții selectați se face în domeniul DCT sau wavelet, așa cum s-a văzut în ecuația (2.34). Sunt folosite filtre biortogonale 7/9. Modelul vizual pentru a determina factorii JND în domeniul wavelet este cel al lui Watson ș.a. [WYSV96]. Ei compară robustețea marcajului înserat în domeniul DCT cu cel în domeniul DWT, respectiv cu algoritmul SS-DCT din [CKLS97]; ambele sunt mai bune decât metoda SS, iar marcajul din domeniul wavelet rezistă mai bine la compresie, decupare, scalare decât cel din domeniul DCT. Dar selecția coeficienților în domeniul wavelet nu include părțile semnificativ vizuale și deci există posibilitatea ștergerii marcajului înserat în coeficienții nesemnificativi. Filtrarea trece-jos va afecta marcajul înserat în coeficienții de frecvență înaltă. Aici autorii propun un detector modificat, la care este calculată media corelației pentru fiecare nivel:

$$\rho_{ww^*}(l) = \frac{1}{N_f} \sum_{f=1}^{N_f} \rho_{ww^*}(l, f) \quad (2.47)$$

unde N_f este numărul de orientări, $N_f = 3$. Prin evaluarea corelațiilor separat pe nivelul de rezoluție, detectorul este mai robust la operații precum decuparea, care afectează componentele spectrale de frecvență înaltă, din cauză că marcajul are un suport spațial mai mic în nivele de rezoluție joasă ($l = 1$). De asemenea este mai robust la filtrarea trece-jos. Prin eliminarea nivelelor care au valori de corelație mici, detecția devine mai robustă. De asemenea, se consideră corelația medie per orientare în frecvență:

$$\rho_{ww^*}(f) = \frac{1}{N_l} \sum_{l=1}^{N_l} \rho_{ww^*}(l, f), \quad (2.48)$$

unde N_l este numărul de nivele, care aici este 4. Prin evaluarea corelațiilor separat pe orientare, se profită de orice structură asociată cu imaginea originală, unde marcajul este mai puternic. Examinând corelațiile separat per subbandă, se alege valoarea maximă per nivel și per locațiile în frecvență:

$$\rho_{ww^*}(f) = \max_{l,f} \{ \rho_{ww^*}(l), \rho_{ww^*}(f) \} \quad (2.49)$$

ceea ce duce la o robustețe crescută.

Dugad ș.a. [DRA98] folosesc ca marcaj o secvență gaussiană de numere reale pseudo-aleatoare. Marcajul este inserat în câțiva coeficienți selectați. Transformata wavelet este pe 3 nivele de rezoluție, cu filtre Daubechies-8. Algoritmul selectează coeficienții din toate subbenzile de detaliu cu amplitudinea peste un prag dat T_1 și îi modifică, folosind relația:

$$f^l(m, n) = f(m, n) + \alpha |f(m, n)| w_i \quad (2.50)$$

La partea de extragere, sunt luați în considerare numai coeficienții peste un prag $T_1 > T_2$. Mascarea vizuală este implicită, prin proprietățile de localizare în timp-frecvență ale transformatei DWT. Din cauză că subbenzile de detaliu la care se adaugă marcajul conțin mai mult muchii, energia semnăturii este concentrată în jurul acestora. Aceasta face ca marcajul să fie invizibil, deoarece observatorii umani sunt mai puțin sensibili în zonele cu texturi și muchii. Dar robustețea algoritmului este redusă, fiindcă aceste locații sunt cel mai ușor de modificat prin compresie sau alte atacuri obișnuite.

Inoue ș.a. [IMK99], propun folosirea unei descompuneri multirezoluție cu filtre simetrice 5/3, sau Daubechies-16. Cu algoritmul EZW coeficienții sunt clasificați ca semnificativi sau nu, folosind arborele-zero [LK92], [PK95], [STO94], [Sha93]. Coeficientul $f(m, n)$ este nesemnificativ dacă $|f(m, n)| < T$, T fiind pragul. Dacă un coeficient și toți descendenții lui sunt nesemnificativi față de pragul T , atunci setul format din acești coeficienți este numit arbore-zero pentru pragul T .

Se consideră două grupuri. Unul este cel al coeficienților semnificativi unde sunt aleși toți arborii zero, Z pentru pragul T . Acest grup nu consideră subbanda de aproximare LL. Toți coeficienții din arborele-zero Z_i sunt setați după cum urmează:

$$f'(m, n) = \begin{cases} -m & \text{dacă } w_i = 0 \\ +m & \text{dacă } w_i = 1 \end{cases} \quad (2.51)$$

Al doilea grup manipulează coeficienții semnificativi de la nivelul cu rezoluție joasă, adică subbenzile de detaliu LH_3 , HL_3 și HH_3 . Selecția coeficienților se face cu relația:

$$T_1 < |f(m, n)| < T_2; \text{ unde } T_2 > T_1 > T \quad (2.52)$$

Marcajul înlocuiește un coeficient selectat prin cuantizare.

$$f'(m, n) = \begin{cases} T_2 & w_i = 1 \text{ și } f(m, n) > 0 \\ T_1 & w_i = 0 \text{ și } f(m, n) > 0 \\ -T_2 & w_i = 1 \text{ și } f(m, n) < 0 \\ -T_1 & w_i = 0 \text{ și } f(m, n) < 0 \end{cases} \quad (2.53)$$

Pentru a extrage marcajul din primul grup de coeficienți, este calculată M valoarea medie a coeficienților aparținând arborelui-zero Z_i și apoi se aplică relația:

$$w_i = \begin{cases} 0 & \text{dacă } Mi < 0 \\ 1 & \text{dacă } Mi \geq 0 \end{cases} \quad (2.54)$$

Pentru al doilea grup marcajul w_i este detectat dintr-un coeficient semnificativ:

$$w_i = \begin{cases} 0 & \text{dacă } |f^*(m, n)| < (T_1 + T_2)/2 \\ 1 & \text{dacă } |f^*(m, n)| \geq (T_1 + T_2)/2 \end{cases} \quad (2.55)$$

Se folosesc pozițiile rădăcinilor pentru a „ghida” procesul de detecție. Rezultatele experimentale arată că metoda propusă dă o imagine marcată de o calitate mai bună decât tehnicile existente la momentul respectiv și că este robustă la compresia JPEG. Pe de altă parte, detectorul este sensibil la atacuri de desincronizare deoarece depinde de coeficienții ne semnificativi.

În [WSK98], marcajul este adăugat la coeficienții semnificativi în subbenzi semnificative. Mai întâi este folosită codarea wavelet multiprag MTWC, pentru a selecta coeficienții semnificativi. Spre deosebire de alte codoare, care folosesc un singur prag inițial în cuantizarea prin aproximații succesive, SAQ (Successive Approximate Quantization), MTWC are praguri diferite în subbenzi diferite. Formula de înserare este:

$$f'_{s,i}(m, n) = f_s(m, n) + \alpha_s \beta_s T_s w_i \quad (2.56)$$

unde f' este coeficientul marcat, f este coeficientul original, α_s este ponderea pentru subbanda s , β_s este ponderea pentru subbenzi, T_s este pragul curent pentru subbanda s în planul de biți j , iar w_i este al i -lea element din secvența de marcaj de lungime N_w . Selectarea coeficienților semnificativi se desfășoară astfel:

1) Se pune pragul $T = f_{\max,s} / 2$, jumătate din maximul valorii absolute a coeficienților wavelet din subbanda respectivă; totii coeficienții sunt neselectați.

2) Se selectează subbanda, în afară de termenul DC, cu valoarea maximă $\beta_s T_s$, unde β_s este ponderea pentru subbanda s . Pentru subbanda selectată, se examinează coeficienții neselectați $f_s(m, n)$ și se aleg ca semnificativi coeficienții mai mari decât valoarea curentă a pragului T_s . Marcajul este înserat în aceștia.

3) Se actualizează pragul cu noua valoare $T_s^{new} = T_s / 2$;

4) Se repetă pașii 2 și 3 până când tot marcajul este înserat.

Detecția se face fără a recurge la imaginea originală.

Xie și Arce [XA98] descompun imaginea folosind transformata wavelet pentru a obține o reprezentare a imaginii de frecvență joasă. Marcajul care este o secvență binară, este înserat în imaginea de aproximare (subbanda LL) a imaginii originale. De fiecare dată sunt selectați coeficienții nesuprapuși dintr-o fereastră alunecătoare, de dimensiune 3×1 . Mai întâi, sunt ordonate crescător elementele b_1, b_2, b_3 ale acestei ferestre. Apoi gama între $\min|b_j|$ și $\max|b_j|$ cu $j = 1, \dots, 3$, este împărțită în intervale de lungime

$$\Delta = \alpha \cdot \frac{\max|b_j| - \min|b_j|}{2} \quad (2.57)$$

Medianul acestor coeficienți este cuantizat la un multiplu de D . Coeficientul median este modificat pentru a îngloba un bit de marcaj și înlocuit în subbanda respectivă. Procesul de extragere nu recurge la imaginea originală. Acest algoritm este construit

atât pentru aplicații de autentificare, cât și protejarea drepturilor de autor. Numărul nivelelor de rezoluție determină robustețea algoritmului. Cu 5 niveluri de rezoluție se poate obține o robustețe bună. Metoda presupune însă un efort mare de calcul.

Xia ș.a. [XBA97], [XBA98] propun un algoritm de marcarea cu filtre wavelet Haar, folosind două nivele de descompunere. Sunt adăugate coduri pseudo-aleatoare la coeficienții mari, în benzile de frecvență mare și medie din DWT. Înserarea se face conform relației:

$$f'(m, n) = f(m, n) + \alpha \cdot f(m, n)^\beta w_i$$

în care α este un factor de ponderare sau intensitatea de marcarea, iar β este amplificarea pentru coeficienții mari. În subbanda de aproximare nu este înserat marcaj. De aceea, acest algoritm concentrează cea mai mare energie în muchii și texturi, care reprezintă cei mai mulți coeficienți în subbenzile de detaliu. Aceasta sporește invizibilitatea procesului de marcarea, deoarece observatorii umani sunt mai puțin sensibili la schimbarea de informație în muchii și texturi, comparativ cu schimbările în componentele spectrale de joasă frecvență din subbanda LL. Practic se înserează mai multe marcaje în domeniul DWT în fiecare imagine de detaliu, cu excepția subbenzii de aproximare, sugerând că detecția poate fi făcută ierarhic, calculând intercorelațiile marcajului original cu diferența dintre cele două imagini pentru fiecare nivel de rezoluție. Metoda este robustă la o serie de distorsiuni, dar filtrarea trece-jos și mediană afectează robustețea marcajului deoarece coeficienții marcați sunt în frecvențele înalte.

Kundur și Hatzinakos, [KH98], propun aplicarea familiei de filtre ortogonale Daubechies pentru descompunerea imaginii originale cu DWT pe trei nivele de rezoluție. Algoritm selectează pseudo-aleator locațiile în care se înserează marcajul în subbenzile de detaliu. Coeficientul median este cuantizat la cel mai apropiat punct de reconstrucție care reprezintă informația de marcaj. Pasul de cuantizare este controlat de parametrul Δ . Cuantizarea mai grosieră crește robustețea, dar astfel crește și distorsiunea introdusă de procesul de marcarea. Robustețea algoritmului nu este suficientă. De aceea, autorii sugerează o îmbunătățire în [KH01], unde se folosește un marcaj de referință pentru a estima dacă un marcaj a fost înserat sau nu. Tot Kundur și Hatzinakos [KH98b], [KH99] propun o tehnică de marcarea fragilă, numită metodă de dovedire a autenticității. Marcajul binar se înserează în domeniul wavelet prin cuantizare, cu chei specificate de utilizator. Metoda de cuantizare este aceeași din [KH98]. Este introdusă o transformată wavelet, care produce pixeli întregi în domeniul spațial, pentru a evita erorile de rotunjire în timpul transformării inverse, deoarece acestea pot fi considerate ca falsificare. Algoritm este o extensie a metodei din [KH98], fiind folosit pentru a dovedi falsificarea.

Ei dezvoltă un algoritm pentru imagini statice în care se folosesc tehnicile de fuziune a imaginilor de detaliu și incorporează un model al HVS [KH97]. Marcajul este o imagine logo, descompusă cu DWT. Imaginea e descompusă cu L pași unde $L \leq M$. Marcajul este înserat în toate subbenzile de detaliu. Kundur prezintă și setul de reguli pentru selectarea parametrilor pentru modelul HVS și a parametrilor de scalare. Simulările arată robustețea algoritmului la distorsiuni obișnuite, dar algoritmul nu este robust la rotație.

Chae ș.a. [CM98] folosesc ca marcaj o imagine cu nivele de gri, care poate fi 25% din imaginea originală, și transformata DWT cu un nivel de descompunere pentru ambele imagini, cea originală și cea de marcaj. Coeficienții sunt “expandați” deoarece imaginea de marcaj este un sfert din cea originală. Pentru imaginea logo, A ,

B, C desemnează cei mai semnificativi biți MSB, octetul mijlociu și cei mai puțin semnificativi biți, LSB. Astfel A, B, C dau 24 biți per coeficient. Sunt obținute trei numere A', B', C' reprezentate pe 24 biți, considerând A, B, C ca fiind cel mai semnificativ octet al acestora. Planele de biți mijlociu și LSB sunt puse pe zero. Se construiește un bloc de mărime 2x2. Imaginea logo este adăugată după cum urmează:

$$f'(m, n) = \alpha f(m, n) + w(m, n) \quad (2.58)$$

unde $w(m, n)$ este coeficientul DWT al imaginii originale, iar coeficienții DWT ai imaginii logo sunt dați de $w(m, n)$. Acest algoritm este limitat la imagini logo de marcaj de mărime cel mult 25% din imaginea originală. Este dificil de folosit nivele de descompunere mai mari din cauza că marcajul este un logo. Rezultatele experimentale arată că procesul de marcare nu afectează vizibil imaginea, iar calitatea marcajului extras este bună chiar și după compresia JPEG. Dar atacurile geometrice nu au fost studiate. Apare un compromis între capacitate (cantitatea de date ascunse) și calitatea imaginii marcate.

Murkherjee [MCM98] și Chae ș.a. [CMM98] introduc o secvență de marcaj w_i de simboluri cu p biți (structura laticice). Este calculată o descompunere de un nivel DWT a imaginii originale și a imaginii marcate, iar coeficienții sunt cuantizați în p-nivele. Patru coeficienți sunt aranjați pentru a forma un vector de dimensiune n. Coeficienții corespunzători din banda de aproximare a imaginii logo de marcaj sunt înserați în coeficienții corespunzători din banda LL a imaginii originale. Aceeași metodă este aplicată și pentru benzile de detaliu. Înserarea se face conform relației:

$$v' = v + \alpha C(w_i) \quad (2.59)$$

unde $C(w_i)$ este cuvântul de cod pentru coeficienții de marcaj w_i . Pentru a detecta marcajul, este cerută imaginea originală. Vectorul eroare:

$$e = \frac{v^* - v}{\alpha} \quad (2.60)$$

este folosit pentru căutarea vecinului cel mai apropiat din dicționarul cuvintelor de cod, pentru a recupera informația de marcaj:

$$w_i = \min_{w_j} \|C(w_j) - e\|$$

Robustețea poate fi controlată cu factorul de intensitate α și calitatea imaginii de marcaj poate fi reglată prin nivelul de cuantizare p. Căutarea în dicționar face metoda lentă dacă acesta este mare.

O metodă de marcare pentru decizie multi-index (metoda maximizării deviației) este propusă de Zhihui și Liang [ZL00]. Tehnica este aplicată în domeniul DCT și wavelet, folosind modele vizuale umane. Rezultatele experimentale arată că metoda bazată pe transformata DWT se apropie de capacitatea de marcare maximă, comparativ cu alte domenii de marcare.

Tsekeridou și Pitas [TP00] folosesc marcaje cu autocorelație mare într-o rețea carteziană, cvasi-invariante la scalare. Schema este implementată în domeniul wavelet. Este de așteptat ca aceste marcaje să fie robuste la scalare dar nu și la alte transformări geometrice.

În [HTC00] se prezintă o arhitectură VLSI, pentru algoritmul EZW, care face o codare a imaginii în timp real. Pentru scanarea coeficienților wavelet se face o căutare pe nivel, începând de sus, pentru a localiza relațiile părinte-copil și pentru a crește viteza. Simbolurile generate în procesul de creare a hărții de semnificații (SMAP) și cuantizarea prin aproximații succesive (SAQ) sunt codate independent.

Aceasta permite transmisia a mai puțini biți și ușurează comunicația fără sacrificarea PSNR-ului. Împreună cu codorul EZW este prezentată o schemă progresivă de marcarea, pentru protejarea drepturilor de autor.

Loo și Kingsbury [LK00] propun un algoritm de marcarea în domeniul transformării wavelet complexe; ei modelează marcarea ca o comunicație. Ei arată că CWT are o capacitate relativ mare de înserare. Se concluzionează că CWT este un domeniu potrivit pentru a însera un marcaj.

Hsu și Wu [HW00] descompun marcajul și imaginea gazdă printr-o reprezentare multirezoluție, marcajul fiind o imagine logo. Imaginea de marcaj este 50% din cea originală care se descompune cu DWT Daubechies-6, iar imaginea de marcaj cu o funcție de reducere în rezoluție RR, din standardul de compresie JBIG. Această descompunere este potrivită pentru imagini alb-negru, dar nu e practică pentru imagini normale. Un nivel de diferență este obținut prin scăderea unei versiuni mărite a reziduuului din marcajul original. Coloanele pare ale marcajului sunt ascute în subbenzile HL_i , iar cele impare în subbenzile LH_i . Marcajul nu se înserează în subbanda de aproximare pentru a menține imperceptibilitatea, și nici în subbenzile HH_i pentru că marcajul este mai ușor de distrus în frecvențele înalte. Masca reziduală este folosită pentru a modifica relația dintre coeficienții vecini din imaginea gazdă. Imaginea originală se presupune cunoscută la detector. Algoritmul este sensibil la orice fel de compresie, din cauză că informația de marcaj este înserată în subbenzile de detaliu.

Ejima și Miyazaki [EM00] folosesc pachetele wavelet pentru marcarea de imagini și video. Este calculată energia fiecărei subbenzi $B_{i,j}$, iar anumite subbenzi sunt selectate pseudo-aleator conform energiei. Media valorii absolute a coeficienților pentru fiecare subbandă selectată este cuantizată și folosită pentru înserarea unui bit de informație. Coeficienții din subbanda respectivă, selectați pseudo-aleator, sunt modificați pentru a reflecta această medie cuantizată. Algoritmul generează informație redundantă, fiindcă pachetele wavelet au subbenzi de detaliu și aproximare pentru fiecare nivel de rezoluție, ceea ce duce la creșterea complexității metodei.

Kim ș.a. [KSLR99] înserează marcajul în coeficienții mari ai fiecărei subbenzi DWT, cu $L=3$ nivele de rezoluție, în afară de primul nivel. Numărul de biți de marcaj w_i este proporțional cu energia subbenzii respective. Energia este definită ca fiind:

$$e_s = \frac{1}{M \cdot N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f^2(m, n) \quad (2.61)$$

unde M, N sunt dimensiunile subbenzii ; marcajul w_i este generat dintr-o secvență pseudo-aleatoare de numere reale cu distribuție gaussiană. În subbenzile de detaliu, sunt modificați 4500 de coeficienți, dar numai 500 în subbanda de aproximare. Înainte de înserare, coeficienții sunt sortați după amplitudine. Metoda este robustă la compresie JPEG, netezire, decupare. Nu se fac referiri la robustețea împotriva atacurilor geometrice (redimensionare, rotație).

În [KM99] sunt selectați coeficienții semnificativi perceptual cu ajutorul pragurilor dependente de nivel. Imaginea este descompusă în trei nivele $L=3$, cu filtre biortogonale. Marcajul este o secvență gaussiană, de 1000 de numere pseudo-aleatoare reale. Detecția se face folosind pragurile cunoscute din procesul de înserare. Metoda este robustă la diverse atacuri, dar nu și la cele geometrice. Lucrarea nu se referă la posibilitatea înserării marcajului cu repetiție, sau ponderarea marcajului pentru a crește robustețea. O metodă similară, propusă în [KKK02], înserează

marcajul în coeficienții semnificativi perceptual pentru fiecare subbandă, folosind proprietățile statistice ale HVS și ale imaginii originale.

În [BBP01], autorii înserează marcajul în toți coeficienții subbenzilor de detaliu de la nivelul de rezoluție cel mai fin, dar folosind un factor de ponderare care împiedică sesizarea marcajului. Masca perceptuală ține cont de sensibilitatea la zgomot, textura și luminața tuturor subbenzilor.

$$\tilde{I}_i^\theta(i, j) = I_i^\theta(i, j) + \alpha w_i^\theta(i, j) x_i^\theta(i, j) \quad (2.62)$$

unde α este intensitatea de marcare iar $w_i^\theta(i, j)$ este o funcție de ponderare, a cărei valoare este egală cu jumătate din pasul de cuantizare, $q_i^\theta(i, j)$. Pasul de cuantizare este calculat ca produsul ponderat a trei factori. Metoda nu se folosește de imaginea originală la detecție și este extrem de robustă la diverse tipuri de atacuri. O extensie a acestei metode în domeniul transformării wavelet redundante este propusă în [HF02].

Tehnicile de marcare în domeniul wavelet sunt de asemenea folosite pentru marcarea fragilă, care este o componentă semnificativă în autentificarea conținutului [PW03, KH99].

2.2.2.1.e Metode care aplică fractalele

Ideea folosirii fractalelor a apărut în [PJ96]. Tehnicile de marcare bazate pe compresia imaginii cu fractale sunt strâns legate de tehnicile de marcare în domeniul spațial. În compresia cu fractale a imaginii, aceasta este codată folosind principiile sistemelor cu funcții iterative și auto-similaritate (self-similarity). Codorul folosește auto-similaritatea imaginii la diferite rezoluții, asociind, printr-o serie de comprimări, blocurile mai mari ale imaginii unor blocuri similare mai mici. Decodorul aplică oricărei imagini transformările inverse pentru a găsi originalul. Modificând dimensiunea blocurilor, pragul de eroare și distanța de căutare, se modifică timpul de codare, PSNR și rata de bit. Comparativ cu codarea JPEG și JPEG-2000, folosirea fractalelor duce la un timp de codare mult mai mare, dar decodarea este mult mai rapidă.

Imaginea originală este împărțită în blocuri pătrate R_k numite blocuri de gamă (range block). F este setul de funcțiilor de asociere f_k , compuse dintr-o transformare geometrică g_k și o transformare masică m_k (massic transform). Funcțiile de asociere sunt aplicate pe blocuri de domeniu D_k , mai mari decât blocurile de gamă.

Transformarea geometrică implică mutarea blocului de domeniu D_k la locația unui bloc de gamă R_k și reducerea mărimii acestuia la mărimea blocului de gamă.

Transformarea masică implică ajustarea intensității și orientării pixelilor în blocul de domeniu, după transformarea geometrică, rotații cu 90, 180 și -90° , reflecția la jumătatea orizontalei și a axelor diagonale, precum și asocierea identității.

Pentru a comprima o imagine pentru toate blocurile de gamă R_k , trebuie găsită cea mai bună funcție de asociere, astfel încât diferența dintre blocul de domeniu R_k și blocul domeniu asociat $F_k(D_k)$ să fie minimă. Deci codarea include o căutare spațială pe toate blocurile de domeniu posibile. Decodarea se face prin iterarea funcțiilor de asociere codate folosind orice imagine inițială. Pentru a însera un bit cu această schemă, e selectat pseudoaleator un bloc de gamă. Spațiul de căutare corespunzător S_k pentru blocurile de gamă este apoi divizat în două subspații de căutare, S_k^1 și S_k^2 , de dimensiune egală. Fiecare subspațiu este asignat unui bit, și

blocul de gamă curent e codat printr-o căutare doar în subspațiul corespunzător valorii bitului curent. Pentru a regăsi bitul înserat, imaginea e comprimată din nou, de data aceasta folosind întregul spațiu de căutare, a blocurilor de domeniu. Pentru blocul de gamă marcat, locația blocului de domeniu corespunzător indică valoarea bitului înserat. Algoritmul a fost testat pentru compresie JPEG și a indicat o robustețe bună, până la o compresie cu o calitate de aproximativ 50%. Dezavantajul tehnicii este viteza redusă datorată schemei de compresie cu fractale.

O abordare foarte asemănătoare a fost propusă de Davern și Scott [DS96]. Singura diferență este că ei nu codează întreaga imagine, ci doar o regiune de gamă definită de utilizator, bazată pe regiunea de domeniu definită tot de utilizator. Fiind date două regiuni, codarea marcajului este echivalentă cu sistemul propus de Puate și Jordan [PJ96] în care regiunea e împărțită în două și, depinzând de valoarea bitului, este folosită una din cele două părți pentru codarea unui bloc de gamă. Ideea folosirii fractalelor în domeniul spațial pentru marcarea a fost extinsă pentru transformata DCT pe blocuri de către Bas ș.a. [BCD98].

În [FS00] se propune pentru marcarea transparentă o metodă bazată pe transformata DCT în subbenzi, compusă dintr-o transformată wavelet și apoi una DCT aplicată pe fiecare subbandă. Marcajul este distribuit într-un număr mare de coeficienți selectați din toate patru subbenzile unei descompuneri cu un nivel. Fiecare subbandă dă o altă ieșire a detectorului. Rezultatul este mediat. Rezultatul final este îmbunătățit față de ieșirea per subbandă, iar schema de marcarea este foarte robustă. Autorii folosesc același detector ca cel propus de Piva în [BBCP98a].

În [KAS05] autorii înserează marcajul în domeniul transformatei discrete multiwavelet; pentru a găsi parametri, ca pragurile de detecție și intensitatea de înserare, se folosesc algoritmi genetici.

2.2.2.1.f Marcarea transparentă cu transformata SVD.

Există metode care înserează marcajul în domeniul spațial sau al unei transformate, ca DCT sau DWT, dar numai după ce este aplicată și transformarea SVD (Singular Value Decomposition), de descompunere în valori singulare, care are proprietatea de a concentra energia în câțiva coeficienți [LT02], [Cha02], [Cha03], [GZE03], [GE04]. Transformarea SVD este o tehnică liniară în algebră, cu aplicații ca: problema celor mai mici pătrate, calcularea matricii pseudo-inverse și analiza cu variabile multiple. În plus, SVD a fost folosită pentru codarea imaginii, estimarea zgomotului și mai recent marcarea imaginilor. O imagine X de mărime $M \times N$, cu $M \geq N$, poate fi reprezentată cu SVD astfel:

$$X = U \Sigma V^T = \sum_{i=1}^N \sigma_i u_i v_i^T \quad (2.63)$$

unde U și V sunt matrici ortogonale de mărime $M \times M$, respectiv $N \times N$, iar Σ este o matrice $M \times N$ cu elementele diagonale reprezentând valorile singulare, σ_i a lui X . Coloanele matricii ortogonale U sunt vectorii singulari din stânga, iar cele ale matricii V – vectorii singulari din dreapta. Vectorii singulari din stânga lui X sunt vectorii proprii a lui XX^T ; vectorii singulari din dreapta sunt vectorii proprii pentru $X^T X$. Matricea Σ are structura de forma:

$$\Sigma = \begin{bmatrix} \sigma_1 & & & 0 \\ 0 & \sigma_2 & & \\ & & \dots & \\ 0 & & & \sigma_N \\ \hline & & & 0 \end{bmatrix} \quad (2.64)$$

Transformarea SVD este o descompunere matricială care, în sensul celor mai mici pătrate, compactează maximum de energie a semnalului în cât mai puțini coeficienți posibili. Are posibilitatea de a se adapta la variațiile statistice locale ale imaginii; cu toate acestea, transformarea SVD a imaginii este necesară pentru a recupera marcajul. În [Cha02], atât marcajul cât și imaginea gazdă se descompun cu SVD. Marcajul este o imagine mai mică decât imaginea originală.

$$X = U \Sigma_x V^T \quad (2.65)$$

$$W = U_w \Sigma_w V_w^T \quad (2.66)$$

Inserarea valorilor singulare ale marcajului se face folosind valorile singulare ale imaginii originale, precum și o intensitate de marcare. Dacă imaginea de marcaj este mai mică, se folosesc numai primele valori singulare:

$$\sigma_{y_i} = \sigma_{x_i} + \alpha_i \sigma_{w_i} \quad (2.67)$$

Imaginea marcată se obține tot cu transformata SVD, folosind matricile U și V:

$$Y = U \Sigma_y V^T \quad (2.68)$$

Estimarea marcajului se face informat, cunoscând imaginea originală, și marcajul original, mai precis matricile Σ_x , U_w și V_w ; detecția presupune următorii pași:

$$\hat{Y} = \hat{U} \hat{\Sigma}_y \hat{V}^T \quad (2.69)$$

$$\hat{\Sigma}_w = \frac{\hat{\Sigma}_y - \Sigma_x}{\alpha} \quad (2.70)$$

$$\hat{W} = U_w \hat{\Sigma}_w V_w^T \quad (2.71)$$

Gradul de asemănare este dat de similaritatea dintre W și \hat{W} . Pentru a însera mai mulți biți, imaginea se descompune în blocuri. Rezultatele arată că metoda neadaptivă este mai robustă decât cea adaptivă, pentru ambele abordări, pe toată imaginea, sau pe blocuri.

O metodă similară, bazată pe transformarea SVD pe blocuri 8x8 pentru inserarea unei imagini logo este descrisă în [Cha03]. În [GZE03] se folosește marcare dublă în domeniul SVD, iar în [GE04] marcajul este inserat domeniul DWT-SVD.

2.2.2.1.g Marcare transparentă cu transformata Ridgelet. O schemă multiplicativă în domeniul transformatei Ridgelet (RT) este propusă în [CKN04]. Sensibilitatea direcțională și anizotropia transformatei RT sunt folosite pentru a obține o reprezentare rară (sparse) a imaginii, în care coeficienții semnificativi sunt direcțiile cu energie mare asociate muchiilor drepte. Pentru o imagine naturală, imaginea de muchii asociată este obținută cu un banc de filtre, construite cu funcții circulare armonice CHF; apoi această imagine de muchii este împărțită în blocuri mai mici pentru a obține muchii drepte. Transformata RT este aplicată fiecărui bloc, iar marcajul este inserat în anumiți coeficienți.

2.2.2.1.h Marcare transparentă cu cuaternioni. Imaginile color pot fi marcate separat per canal, sau în domeniul transformatei cuaternionice, [BBC03].

Pixelii RGB sunt asociați cu un număr unic în domeniul QFT, care are trei părți imaginare. Transformata QFT depinde de un cuaternion pur μ ; valoarea acestuia este selectată pentru o robustețe și/sau imperceptibilitate dată, funcție de valoarea medie a culorii per bloc și a unei componente perceptuale. Una din schemele implementate este bazată pe QIM. Metoda este robustă la tehnici de filtrare de luminanță.

2.2.2.1.i Marcare transparentă cu transformata LOT. În [PRP99] autorii propun o metodă de marcăre de tip SS în domeniul transformatei LOT (Lapped Orthogonal Transforms), folosită în locul transformatei DCT pentru a nu produce artefacte vizibile atunci când puterea marcajului crește. Se sugerează folosirea unui model în domeniul DFT pentru a compensa dezavantajul că transformata LOT nu este robustă la decupare, rotație sau schimbare de scală. O dată detectate aceste transformări, marcajul este detectat în domeniul LOT, fără a folosi imaginea originală. Alte tehnici folosesc segmentarea Voronoi și apoi o transformată, cum ar fi DCT [SO03].

2.3 Concluzii

Cele mai multe scheme se bazează pe același principiu simplu, schimbarea redusă a valorii unor coeficienți aleși pseudoaleator în domeniul spațial sau al unei transformate. Aceste schimbări sunt apoi identificate folosind un corelator sau alte tehnici asemănătoare corelației. În mod normal, numărul de coeficienți modificați este mult mai mare decât numărul de biți de înserat. Aceasta poate fi considerată ca o marcăre redundantă și duce implicit la creșterea robusteții.

Domeniul de înserare al marcajului poate influența semnificativ robustețea marcajului. Metodele de marcăre în domeniul spațial sunt mai puțin robuste la atacuri de tip adăugare de zgomot, compresie JPEG. Dar marcajul poate fi recuperat ușor dacă imaginea a fost decupată sau translatată. Acest avantaj este mai puțin evident în frecvență. Decuparea în domeniul spațial produce distorsiuni mari în domeniul spectral ceea ce duce de obicei la distrugerea marcajului. Același lucru este valabil și pentru transformata DCT aplicată pe toată imaginea. Dacă sunt marcate blocuri DCT, pentru o detecție cu succes este important să se cunoască poziția blocurilor în care a fost înserat marcajul. Domeniul wavelet are dezavantaje asemănătoare, deoarece transformarea nu este invariantă la translație sau rotație. Cele mai multe metode plasează marcajul în domeniul spațial, dar și numărul metodelor în domeniul DCT este mare.

Capitolul 3

Atacuri asupra sistemelor de marcare

3.1. Problema marcării transparente

Canalul de distribuție a documentelor multimedia de la producător la utilizatori, poate fi considerat ca un *canal de atac* asupra marcajului înserat, astfel că abordarea acestei probleme face apel la metodele din teoria transmisiunii informației. Atacurile pot genera distorsiuni întâmplătoare sau intenționate. Atacurile pot avea loc în timpul transmisiei sau asupra mediului de memorare. Atacurile pot fi clasificate și în funcție de obiectivele pe care încearcă să le împiedice.

Obiectivele marcării transparente sunt: *imperceptibilitatea, robustețea, capacitatea și securitatea criptografică*.

Imperceptibilitatea se referă la faptul că marcajul ar trebui să nu poată fi perceput și în plus să nu interfereze cu datele ce trebuie protejate. Deși diferențele abia vizibile se accentuează dacă produsul original este comparat direct cu cel marcat, ele rămân practic neobservate, deoarece produsul original este accesibil doar proprietarului legal.

Robustețea se referă la posibilitatea de înlăturare a marcajului: cu cât acesta este mai greu de înlăturat, cu atât marcajul este mai robust. Atacurile asupra robusteții sunt cele care încearcă să elimine sau să estimeze marcajul prin prelucrarea semnalului primit.

Capacitatea se referă la cantitatea de informație conținută de marcajul înglobat. Atacurile asupra capacității vizează reducerea capacității marcajului. Astfel, într-o aplicație de *fingerprinting*, fiecare utilizator primește o copie a originalului, în care este înserat un marcaj diferit. Prin formarea unei coaliții de atacatori, în urma acțiunii lor comune, se reduce capacitatea marcajului.

Securitatea criptografică se referă la integritatea semanticii marcajului și la identificarea sursei în aplicația de autentificare, respectiv la asigurarea confidențialității marcajului în marcarea robustă. Atacurile asupra securității criptografice sunt atacuri de falsificare ilegală. Un exemplu grăitor este fotografia lui Bill Clinton alături de soția sa Hillary, care în varianta falsă pare că este alături de Monica Levinsky [BCHL05, C.-Y. Lin]. Sistemul propus de C.-Y. Lin poate reconstitui imaginea originală; acesta este cunoscut sub denumirea de *Self-Authentication and Recovery Image*, SARI [LYC00].

Ultimele trei obiective – robustețea, capacitatea, și securitatea criptografică – reprezintă și punctele vulnerabile ale sistemului de marcare în fața unui atacator.

3.2. Constrângeri asupra atacatorului

Obiectivul atacatorului este *reducerea securității sistemului de marcare*, adică reducerea probabilității de detecție/extragere a marcajului original, respectiv creșterea probabilității de detecție/extragere a unui marcaj care nu a fost înserat în semnalul marcat (extragere falsă). În atingerea obiectivelor sale, atacatorul este supus și el unor constrângeri [Kun05].

O primă constrângere este *imperceptibilitatea*. Un atacator trebuie să păstreze valoarea comercială a produsului multimedia în cauză, neputând induce decât *distorsiuni imperceptibile*, distorsiuni care se apreciază prin:

- variația energiei imaginii: eroarea medie pătratică MSE, raportul semnal-pe-zgomot, SNR, sau raportul semnal pe zgomot de vârf, PSNR; dar acestea nu sunt cele mai bune măsuri pentru evaluarea degradării calității unei imagini.
- factorul JND (*Just Noticeable Difference*), diferența abia sesizabilă, când marcajul este considerat încă imperceptibil; se folosește în modelele perceptuale. Un JND este acel nivel de distorsiune introdus care poate fi perceput în 50% din cazuri [CMB02]. Modelul propus de Watson în [Wat93] încearcă să estimeze JND comparând imaginea originală și cea degradată. El definește unitatea de măsură a JND cu ajutorul unui zgomot alb, care produce o distorsiune unitară.

A doua condiționare se referă tot la *considerații de ordin perceptual*, cum ar fi tipul de document multimedia care este marcat, agresivitatea codării perceptuale aplicate, respectiv procesări sau atacuri anterioare.

A treia constrângere se referă la *ipoteza marcării transparente (marking assumption)*, când se presupune că există o schemă de marcăre ce satisface în același timp cerințele de fidelitate și robustețe. Acest principiu este folosit în construirea codurilor rezistente la coliziune pentru amprentarea (*fingerprinting*) datelor [BS95], [BS98]. Amprenta este compusă dintr-un set de mărci, fiecare fiind modelată ca poziție în semnalul digital și poate lua un număr finit de stări. O *marcă* este considerată *detectabilă* dacă membrii unei coaliții de utilizatori nu au mărcile identice pe fiecare poziție.

Spre exemplu, pentru mai multe copii marcate ale aceluiași document original, marcajul poate fi identificat prin localizarea pixelilor de valoare diferită de pe aceleași poziții (umbrite în Figura 3.1). Ipoteza marcării transparente presupune că mărcile nedetectabile nu pot fi schimbate arbitrar fără a face semnalul digital inutilizabil; dar se consideră perfect posibil ca o marcă detectabilă să fie schimbată în orice stare de către coaliția de atacatori. Conținutul redistribuit de atacator va include părți din amprenta originală, permițând astfel identificarea copiilor ilegale (*traitor tracing*). Astfel, un posibil atac este interschimbarea pixelilor sau coeficienților unei transformate a imaginii de valoare diferită în copiile respective.

$$\begin{array}{l}
 m_1 = \\
 m_2 = \\
 m_3 =
 \end{array}
 \begin{array}{|c|c|c|c|c|c|}
 \hline
 0 & 1 & 1 & 1 & 0 & 1 \\
 \hline
 0 & 1 & 1 & 0 & 1 & 1 \\
 \hline
 0 & 0 & 1 & 1 & 1 & 1 \\
 \hline
 \end{array}$$

Fig. 3.1: Într-o coaliție de atacatori, aceștia nu cunosc localizarea marcajului, decât prin compararea coeficienților de valoare diferită în copii marcate diferite.

Atacatorul este limitat de *informația de care dispune pentru a estima/elimina marcajul* și anume: algoritmi de inserare/extragere a marcajului; modelele perceptuale pentru semnalele multimedia; numărul necesar de copii ale aceleiași imagini, marcate cu marcaje diferite, pentru atacul de coliziune tip I cu succes;

numărul necesar de copii ale imaginilor diferite marcate cu același marcaj, pentru atacul de coliziune tip II cu succes.

În fine, atacatorul este condiționat de *resursele disponibile*: puterea de calcul, documentul original, decodorul, respectiv codorul.

3.3. Clasificarea atacurilor

Atacurile pot folosi *o singură copie marcată* a unui original (caz în care atacurile pot fi *neintenționate* sau *intenționate*), sau *mai multe copii* ale documentului original (caz în care ele sunt intenționate).

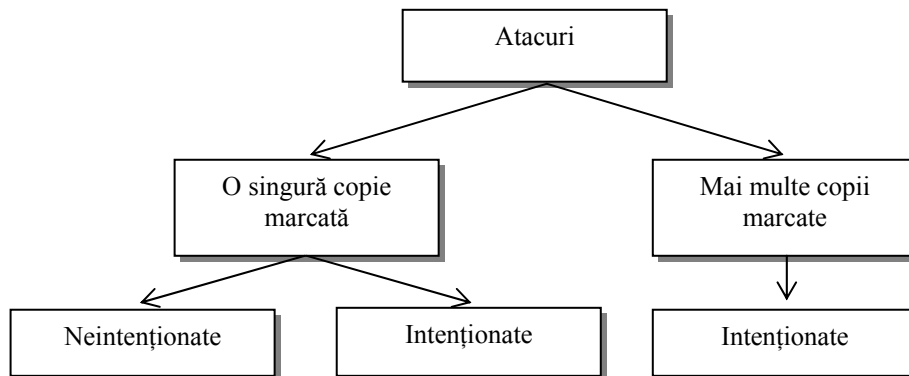


Fig. 3.2: Clasificarea atacurilor, funcție de numărul de copii marcate.

Atacurile asupra unei copii marcate, pot fi clasificate după cum urmează:

- *neintenționate*: conversiile în alt format, care rezultă din
 - compresie,
 - modificarea ratei de bit,
 - compensarea raportului de aspect, sau
 - conversia tipului de fișier.
- *intenționate*, care se pot clasifica în două mari categorii:
 - atacuri asupra unui *singur cadru (single-frame)*:
 - filtrare,
 - transformări geometrice,
 - atacuri criptografice,
 - de protocol,
 - de estimare a semnalului gazdă sau a marcajului,
 - zgomot aleator;
 - atacuri asupra *mai multor cadre (multiple-frames)*:
 - medierea mai multor cadre;
 - estimarea mai multor cadre (de exemplu prin mediere ponderată).

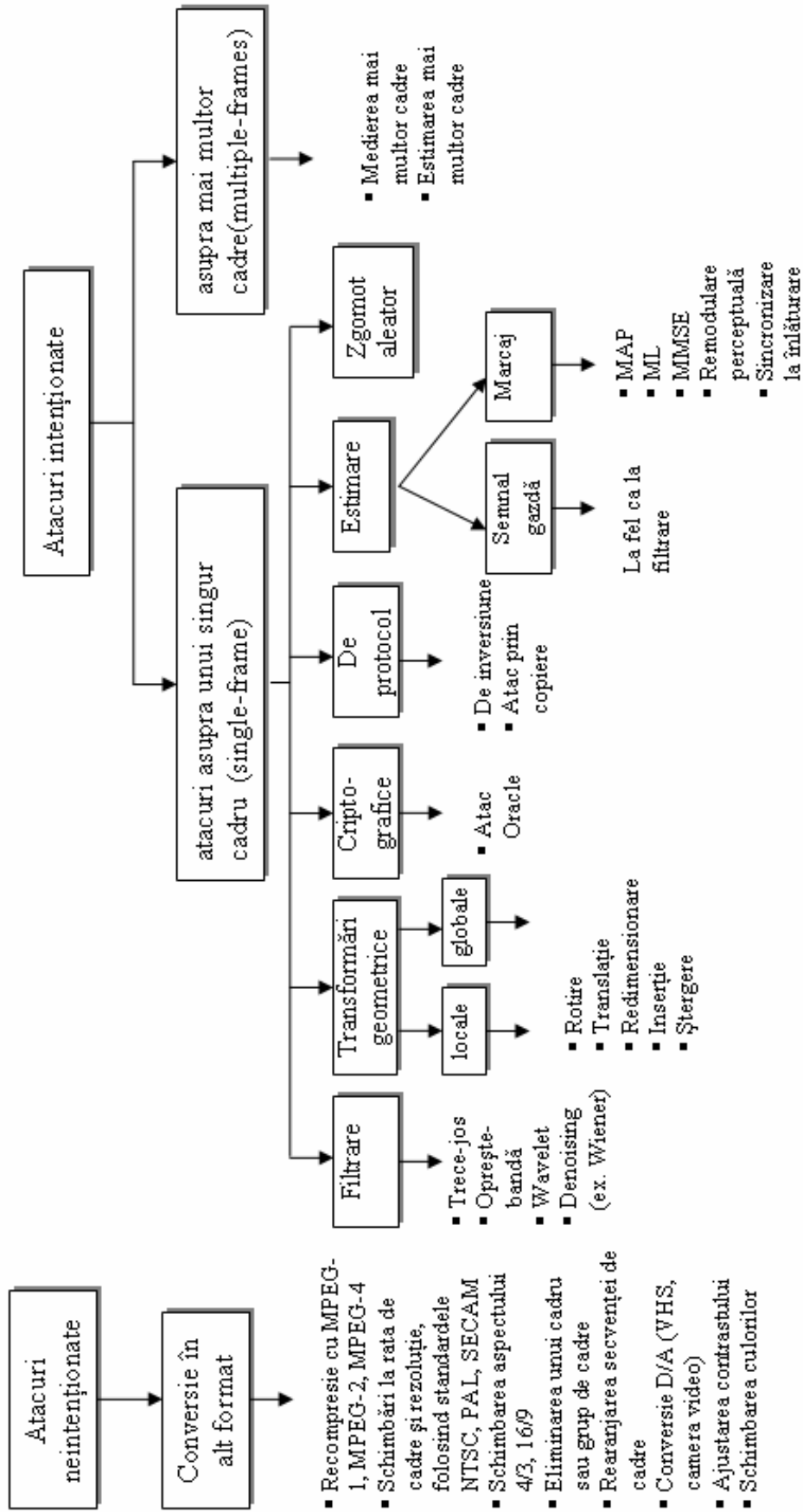


Fig. 3.3: Atacuri ce acționează asupra unei copii marcate

3.4 Atacuri care folosesc o copie marcată

Aceste atacuri folosesc o singură copie a documentului marcat, putând fi intenționate sau nu. Atacurile *intenționate* asupra unui singur cadru exploatează informația spațială și/sau spectrală a unei imagini, în timp ce atacurile intenționate ce operează asupra mai multor cadre folosesc informația temporală de la cadru la cadru.

3.4.1 Compresia

În categoria atacurilor *neintenționate*, cel mai întâlnit atac este compresia. Aceasta înlătură părțile ne semnificative din punct de vedere perceptual, dintr-un semnal multimedia. Astfel, prin compresie, semnale perceptual asemănătoare, ajung să fie identice. Pe de altă parte, marcarea înserează mesaje diferite într-un semnal multimedia original, astfel că se ajunge la o mulțime de semnale diferite, dar perceptual asemănătoare. Prin urmare, cele două operațiuni sunt complementare.

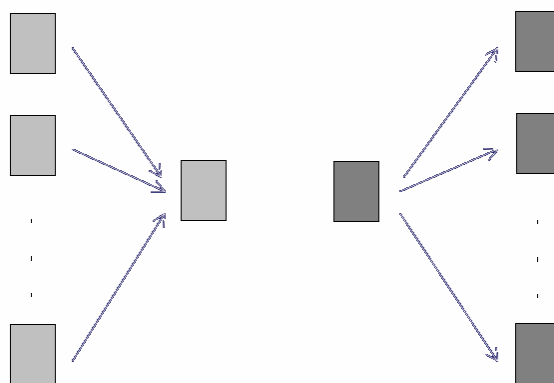


Fig. 3.4: Compresia și marcarea transparentă, ca operații complementare.

Robuștețea la compresia JPEG poate fi îmbunătățită în mai multe moduri. O metodă constă în comprimarea și apoi decompimarea unui model pseudo-aleator W , cu ajutorul algoritmului JPEG [SC96]. Energia modelului rezultat este crescută pentru a compensa pierderea de energie datorită compresiei. În final, acest model este adăugat la imagine pentru generarea imaginii marcate. Aici, ideea este de a folosi algoritmul de compresie pentru a elimina în avans, prin filtrare, toată energia care s-ar pierde mai târziu pe parcursul compresiei. Se presupune că un marcaj alcătuit în acest fel, este invariant la compresii JPEG ulterioare, cu același factor de calitate, cu excepția unor mici artefacte numerice. Pot fi aplicate alte distorsiuni preliminare ale modelului de marcaj, precum filtrarea, pentru a preveni alte degradări anticipate ale imaginii marcate.

În [NP96] energia modelului de marcaj este concentrată în componentele spectrale de frecvențe mai joase, prin calcularea unui factor de câștig individual $k_{x,y}$ pentru fiecare pixel al modelului de marcaj, în locul folosirii aceluiași factor de câștig k pentru toți pixelii. Mai întâi este generat un model pseudo-aleator $W(x,y)$, care constă din numerele 0 și k . Apoi modelul este despărțit în blocuri 8×8 , și este calculată transformata DCT $W(u,v)$ a fiecărui bloc 8×8 . Elementele nenule din blocurile 8×8 , sunt acum privite ca factori de câștig $k_{x,y}$, și adaptate în așa fel încât energia Φ din coeficienții DCT de frecvență înaltă F_H să fie minimizată (Figura 3.5):

$$\Phi = \sum_{u,v \in F_H} W(u,v)^2 \quad F_H = \{u,v \mid 5 < u \leq 8, 5 < v \leq 8\}$$

Energia Φ este minimizată ținând cont de următoarea condiție:

$$\sum_{x=1}^8 \sum_{y=1}^8 W(x,y) \cdot k = \sum_{x=1}^8 \sum_{y=1}^8 W(x,y) \cdot k_{x,y}, \quad k_{\min} \leq k_{x,y} \leq k_{\max}$$

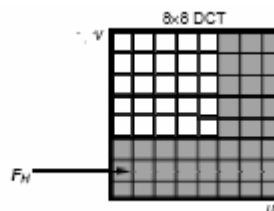


Fig. 3.5: Banda DCT F_H în care energia Φ a marcajului este minimizată

Efectul minimizării energiei de frecvențe înalte asupra modelului marcajului este ilustrat în Figura 3.6. Figura 3.6 (a) arată modelul marcajului în interiorul unui bloc 8x8, unde este folosit un factor de câștig constant $k=3$. După minimizarea energiei pentru $k_{\min}=0$ și $k_{\max}=6$, modelul marcajului descrește spre zero (Fig. 3.6 (b)), deși suma pixelilor nenuli încă este egală cu suma pixelilor nenuli din marcajul original.

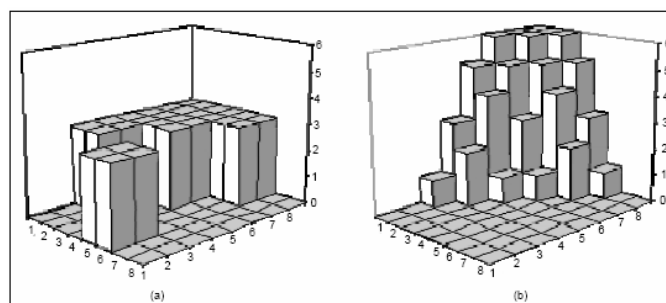


Fig. 3.6: (a) Marcaj original și (b) Marcaj de frecvență joasă

În [HLR00] și în [LLL97], imunitatea la compresia JPEG se asigură prin obținerea unui factor de câștig k pentru fiecare bloc de 32x32 de pixeli, pe baza unei imagini comprimate JPEG de calitate mai scăzută. La fiecare bloc de imagine de 32x32 pixeli este adăugat un model pseudo-aleator de 32x32 pixeli reprezentând un bit de marcaj. O copie a acestui bloc de imagine marcată, este degradată în conformitate cu standardul JPEG, pentru care se folosește un factor de calitate relativ scăzut. Dacă bitul de marcaj nu se poate extrage corect din această copie degradată, modelul de marcaj este adăugat la imagine cu ajutorul unui factor de câștig mai mare, și este alcătuită o nouă copie degradată pentru a verifica bitul. Această procedură este repetată iterativ pentru fiecare bit, până când toți biții pot fi extrași cu un grad de certitudine mare din copiile degradate. Un marcaj format în acest mod este rezistent la

compresia JPEG, folosind un factor de calitate mai mare sau egal cu factorul de calitate folosit pentru degradarea copiilor. În figura 3.7 este dat un exemplu pentru un asemenea marcaj, amplificat pentru a fi vizibil.

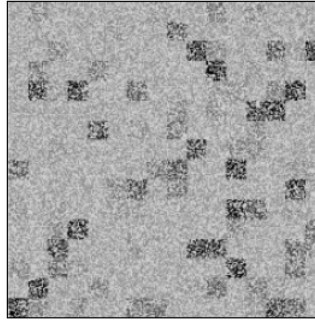


Fig. 3.7: Marcaj unde factorul de câștig local la un bloc este bazat pe o imagine comprimată JPEG cu calitate mai scăzută

3.4.2 Filtrarea

Filtrarea modelează *marcajul ca un zgomot aditiv*, care este o presupunere rezonabilă în cazul marcării transparente de tip *spread spectrum*. Înlăturarea marcajului este echivalentă cu o problemă de eliminare a zgomotului din imagine (*denoising*), rezultatul fiind estimarea imaginii originale.

Pentru *denoising* se pot folosi metode simple de filtrare medie și mediană în domeniul spațial, respectiv filtrarea trece-jos, oprește-bandă, folosirea filtrelor wavelet în domeniul unei transformate. O abordare îmbunătățită este filtrarea trece-bandă a unei anumite game de frecvență, în cazul în care marcajul a fost înserat într-o gamă cunoscută de frecvență.

Filtrarea de tip trece-jos este un atac eficient dacă marcajul a fost înserat în coeficienții de înaltă frecvență, iar filtrarea oprește-bandă este eficientă dacă marcarea a fost făcută folosind coeficienții de frecvență medie.

O altă metodă de *denoising* este filtrarea Wiener, care nu necesită informație apriori, fiind bazată pe modelarea stohastică a imaginilor cu modelul gaussian staționar generalizat [VHBP99]. Considerând o secvență video cu N_f cadre marcate y_t , din care x_t sunt cadrele originale, respectiv n_t sunt marcajele înserate, se calculează estimatul cadrului original \hat{x}_t după cum urmează:

$$\hat{x}_t(i, j) = \left(\frac{\hat{\sigma}_{x_t}^2(i, j)}{\hat{\sigma}_{x_t}^2(i, j) - \sigma_{n_t}^2} \right) y_t(i, j) \quad t = 1 \dots N_f \quad (3.1)$$

unde $\hat{\sigma}_{n_t}^2$ este estimatul dispersiei globale a marcajului și $\hat{\sigma}_{x_t}^2$ este estimatul dispersiei *locale* a semnalului original. Dispersia globală a marcajului este dată de relația:

$$\hat{\sigma}_{n_t}^2 = \left(\frac{\text{med}_{i,j} \left[\left| y_t(i, j) - \hat{x}_t(i, j) \right| \right]}{0.6745} \right)^2 \quad t = 1 \dots N_f \quad (3.2)$$

unde $med_{i,j}$ este valoarea mediană globală; valoarea 0.6745 a fost calculată în conformitate cu modelul gaussian staționar generalizat, iar \hat{x}_t este pre-estimatul mediei locale pentru imaginea originală.

Dispersia locală a imaginii originale poate fi aproximată ca fiind:

$$\hat{\sigma}_x^2(i, j) = \max\left[0, \overline{y_t^2}(i, j) - \hat{\sigma}_n^2\right] \quad (3.3)$$

unde pătratul mediei locale a imaginii marcate este dat de un estimat de plauzibilitate maximă, ML (Maximum-Likelihood). Toți parametrii locali de mai sus pot fi estimați folosind o fereastră locală de dimensiuni 5×5 .

Această metodă de *denoising* poate fi aplicată asupra cadrelor în domeniul spațial sau într-un context multirezoluție, bazat pe transformata wavelet. În acest caz, filtrarea Wiener adaptivă se aplică la fiecare subbandă wavelet și imaginea atacată este reconstruită din descompunerea wavelet.

Ca o măsură posibilă împotriva atacurilor de filtrare este folosirea eficiență a redundanței și a diversității. Marcajul poate fi trimis prin mai multe canale de transmisie, iar la detecție se face o combinație optimală, astfel încât rata erorilor să scadă [KH01], așa cum se vede în Figura 3.5.

3.4.3 Atacul prin adăugare de zgomot

Zgomotul adăugat introduce distorsiuni imperceptibile, chiar la un raport semnal pe zgomot mic, de 20 dB, iar impactul negativ asupra detecției marcajului este nesemnificativ.

Soluțiile posibile împotriva atacului prin zgomot AWGN sunt codurile corectoare de erori precum și folosirea diversității și a combinării repetițiilor marcajului în mod optim.

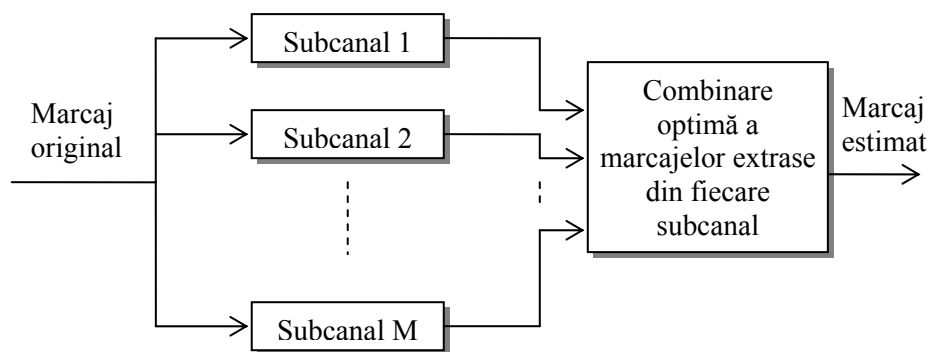


Fig 3.8: Folosirea diversității și a combinării repetițiilor marcajului în mod optim.

3.4.4 Atacurile geometrice

Atacurile geometrice au ca obiectiv desincronizarea detectorului, pentru ca acesta să nu găsească marcajul. Atacurile geometrice posibile sunt: translația, rotația,

redimensionare (scaling), respectiv combinații ale acestora; curbarea neliniară a imaginii; ștergere și înserare de cadre (în cazul semnalelor video).

Atacurile geometrice se împart în două categorii: globale sau staționare, respectiv locale.

În cazul atacurilor geometrice *globale* noile valori ale pixelilor se obțin astfel:

$$\hat{Y}_n(i, j) = Y_n(T(i, j)), \quad (3.4)$$

unde T este transformarea (atacul) respectiv. În continuare se prezintă câteva astfel de atacuri și transformările care le corespund.

- atac RST ,

$$T(i, j) = \begin{bmatrix} k \cos \theta & k \sin \theta & t_x \\ -k \sin \theta & k \cos \theta & t_y \end{bmatrix} \begin{bmatrix} i \\ j \\ 1 \end{bmatrix} \quad (3.5)$$

- atac de tip translație ciclică (cyclic shift),

$$\hat{Y}_n(i, j) = Y_n(i + \Delta_x \bmod M, j + \Delta_y \bmod N) \quad (3.6)$$

Atacurile *locale* (de tip Stirmark [PAK98]) profită de faptul că sistemul vizual uman nu este sensibil la translații și modificări afine locale. Pixelii sunt translați și redimensionați local, fără a introduce distorsiuni vizibile.

Robustețea împotriva transformărilor afine *globale* este asigurată prin folosirea unui domeniu invariant la acestea (cum este transformata Fourier-Mellin), folosirea unui marcaj de referință, sau folosirea marcajelor periodice, a căror funcție de autocovarianță, ACF, permite estimarea distorsiunilor. Asigurarea robusteții împotriva atacurilor *locale* introduse de programe ca și Stirmark este încă nesoluționată. Un exemplu de atac de acest tip este prezentat în Figura 3.9.

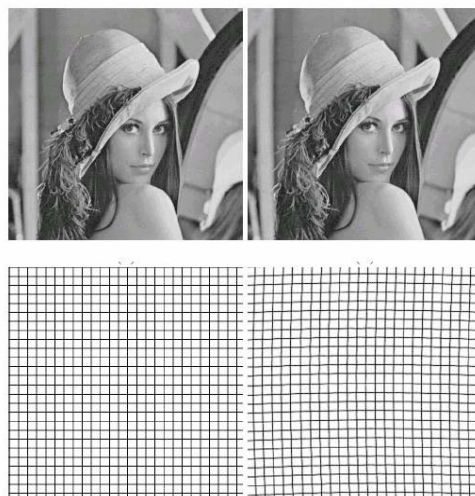


Fig. 3.9: Atac jitter, Stirmark. Stânga: imaginea originală (sus), matricea asociată (jos). Dreapta: imaginea după atac (sus), „matricea” asociată (jos). Efectul atacului este vizibil numai asupra matricii asociate.

În cazul marcării neinformate, folosirea unor metode eficiente de înregistrare poate asigura robustețea la atacurile geometrice.

Un marcaj trebuie să fie robust nu numai la tehnicile de compresie cu pierderi, dar și la transformările geometrice ca scalare, decupare, rotire, etc. Transformările geometrice afectează în mică măsură calitatea imaginii, dar afectează în mare măsură marcajele plasate cu ajutorul metodelor descrise anterior. Deoarece transformările geometrice afectează în mod tipic sincronizarea dintre modelul pseudo-aleator al marcajului și imaginea marcată, sincronizarea trebuie redobândită înainte ca detectorul să înceapă calculul corelațiilor.

Cea mai la îndemână metodă de a obține invarianța la translație (shift), este modulația de amplitudine a coeficienților DFT. Dacă, dintr-o anumită cauză, este preferat un alt domeniu pentru plasarea marcajului și este nevoie și de invarianță la schimbări de poziție, se poate adăuga un marcaj (semn) în domeniul spațial pentru a determina translația. Acest semn poate fi un model pseudo-aleator, ca și marcajul transparent însuși. Detectorul determină prima oară poziția spațială a acestui marcaj, prin mișcarea lui peste toate locațiile posibile din imagine, și apoi calculând corelația dintre aceasta și porțiunea de imagine corespunzătoare. Translația cu corelația cea mai mare definește poziția spațială a semnelui. În final, imaginea este mișcată înapoi în poziția sa originală, și aplicată procedura normală de detecție a marcajului.

O căutare completă a acestui marcaj (semn), este foarte anevoioasă din punct de vedere al calculelor. De aceea, în [KDHM99], este propusă o altă metodă: adăugarea unui model pseudo-aleator în imagine de două ori, dar în diferite locuri. Aici conținutul marcajului transparent, adică biții marcajului sunt plasați în poziții relative a două modele de marcaj. Pentru a detecta marcajul transparent, detectorul calculează corelația de fază dintre imagine și modelul de marcaj, folosind transformarea Fourier rapidă (FFT), și detectează cele două vârfuri de corelație a celor două modele. Conținutul marcajului transparent derivă din pozițiile relative ale vârfurilor. Dacă toată imaginea e deplasată înainte de detecție, pozițiile absolute ale vârfurilor de corelație se schimbă, dar pozițiile relative rămân neschimbate, lăsând biții marcajului detectabili.

În [FH97], este propusă o metodă în care se adaugă o grilă la o imagine, care poate fi folosită pentru a scala, roti, și translați înapoi imaginea în poziția și mărimea originală. Grila este reprezentată de o sumă de semnale sinusoidale, care apar ca maxime în domeniul de frecvență FFT. Aceste vârfuri sunt folosite pentru a determina distorsiunile geometrice.

În [KP99], este propusă o metodă care plasează un model pseudo-aleator de mai multe ori, la diferite locații, în domeniul spațial al unei imagini. Detectorul estimează marcajul W' , prin aplicarea unui filtru trece sus F_{HP} asupra imaginii marcate:

$$W' = I_w \otimes F_{HP}$$

$$F_{HP} = \frac{1}{12} \cdot \begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

În final, este calculată funcția de autocorelație a marcajului estimat \hat{W} . Această funcție va avea valori maxime în centru și în pozițiile marcajelor înserate de mai multe ori. Dacă imaginea a fost supusă unei transformări geometrice, vârfurile din funcția de autocorelație vor reflecta aceeași transformare și deci, vor furniza o grilă care poate fi folosită pentru a transforma înapoi imaginea, la mărimea și orientarea originală.

În [HPRP98] și în [HRPP98], se propune o metodă care plasează marcajul într-un domeniu invariant la rotire, scalare, și translație, folosind o combinație dintre transformata Fourier discretă, DFT, și reprezentarea polară logaritmică, LPM, așa cum s-a văzut în capitolul 2. Mai întâi este calculată amplitudinea coeficienților DFT pentru a obține un domeniu invariant la translații. În pasul următor, pentru fiecare coordonată (u,v) al amplitudinilor DFT este determinat un punct corespunzător (μ,θ) în LPM:

$$u = e^{\mu} \cos(\theta); v = e^{\mu} \sin(\theta).$$

Acest sistem de coordonate polar logaritmice (LPM) transformă rotirea și scalarea, în translații de-a lungul axei orizontale și verticale. În continuare, prin folosirea amplitudinii DFT a coordonatelor LPM, se obține un domeniu invariant la rotire, scalare și translație. În acest domeniu se poate adăuga un marcaj transparent CDMA, de exemplu prin modularea coeficienților, folosind relația:

$$|I_w(u,v)| = |I(u,v)|(1+kW(u,v)).$$

În practică, implementarea schemei s-a dovedit a fi dificilă. De aceea autorii propun o abordare diferită, unde un marcaj transparent CDMA este plasat în domeniul amplitudinii DFT invariante la translații. Pentru a face marcajul transparent invariant la scalare și rotire, se plasează un al doilea marcaj transparent ca șablon, în acest domeniu. Pentru a extrage marcajul transparent, mai întâi se determină scara și orientarea imaginii marcate prin folosirea șablonului după cum urmează:

- Este calculată transformata DFT a imaginii marcate
- Sunt calculate coordonatele LPM ale amplitudinilor coeficienților DFT și ale modelului șablonului
- Sunt calculate „offset”-urile orizontale și verticale dintre cele două LPM, folosind tehnici de căutare și intercorelație, rezultând un factor de scalare și rotire.

În final, imaginea este transformată înapoi la mărimea și orientarea originală, și este extras marcajul purtător de informație.

Pentru a combate efectele atacurilor StirMark, pentru imaginile color, în metoda *canalelor duale*, imaginea este împărțită în două canale, unul pentru sincronizare și unul pentru înserare [Ker01]. Transformata wavelet complexă a fost propusă ca domeniu de înserare [LK00] pentru a crește robustetea la transformări geometrice.

3.4.5 Atacurile de tip protocol

Atacurile de tip protocol periclitizează întregul concept al sistemului de marcare transparentă. Exemple sunt:

- *atacul de ambiguitate sau inversiune*. Atacatorul extrage un marcaj propriu din semnalul marcat, rezultând un semnal pseudo-gază, care atunci când este folosit

în detecția informată, va permite atacatorului detecția marcajului. Astfel apare incertitudinea cu privire la identitatea deținătorului drepturilor de autor [CMYY98]. Pentru protejarea copyright-ului, marcajele trebuie să fie neinvertibile. Cu alte cuvinte un atacator nu ar trebui să poată extrage o marcă din semnalul multimedia marcat. O soluție la această problemă este ca marcajul să fie dependent de semnalul original printr-o funcție *one-way*, neinvertibilă.

- *atacul de copiere*, care estimează marcajul dintr-un semnal marcat și îl inserează într-un alt semnal, numit semnal *țintă*. Acest tip de atac este aplicabil dacă poate fi produs în semnalul țintă un marcaj valid fără cunoașterea sistemului de marcarea sau a cheii. Din nou, marcajele dependente de semnalul original pot fi rezistente la atacul de copiere. Atacul este gândit împotriva autentificării.
- *atacul mozaic* împarte semnalul astfel încât el este afișat ca o entitate, dar detecția marcajului nu este posibilă. Acest atac este de tip Stirmark. În Figura 3.10 se dă un exemplu pentru funcționarea acestui tip de atac.
- *atacul de re-marcare*, în care o imagine marcată va fi re-marcată cu un alt sistem, creând confuzie asupra primului marcaj înserat. O posibilă contramăsură ar fi ca generarea marcajelor să depindă de momentul de timp (*time-stamping*).



Fig. 3.10: *Atacul Mozaic. Imagine originală și cea segmentată în subimagini cu programul 2Mosaic [PAK98].*

Soluțiile posibile împotriva acestor tipuri de atacuri presupun stabilirea unor reguli de construire a sistemului de marcarea, pentru a le combate pe cele cunoscute, cum ar fi folosirea marcajelor non-invertibile, în cazul atacului de ambiguitate [CMYY98]. O altă posibilitate este folosirea unui detector flexibil.

3.4.6 Atacurile de tip criptografic

Atacurile de tip criptografic au ca țintă elemente criptografice din sistemul de marcarea transparentă. Ele folosesc metode standard de criptanaliză pentru atacarea sistemului:

- căutarea prin „forță brută” a mesajului înserat;
- estimarea cheii;
- atacul Oracle: pentru marcaje rezistente la falsificare, detectorul este disponibil, astfel că se poate deduce modul de înlăturare a marcajului. Oracolul produce un răspuns DA sau NU la întrebarea „este imaginea marcată ?” și eventual dă și informații suplimentare, ca de exemplu coeficientul de intercorelație.

Într-un sistem criptografic, există diferite nivele de securitate:

- *Securitatea necondiționată* – sistemul nu poate fi spart, chiar și cu putere de calcul nelimitată, deoarece adversarul nu deține destule informații. Aceasta presupune o măsură teoretică informațională numită secret perfect,
- *Securitatea cu complexitate teoretică*: modelul atacatorului (puterea de calcul polinomială) este folosit pentru a dovedi ineficiența atacului; în cel mai rău caz această analiză are o valoare practică aproape nulă,
- *Securitatea practică (demonstrabilă)* se referă la o situație în care complexitatea spargerii sistemului poate fi redusă prin rezolvarea unei probleme matematice presupuse dificile,
- *Securitatea computațională* presupune că un atac asupra sistemului nu este fezabil din cauza puterii de calcul; cel mai bun atac trebuie perceput ca acela care depășește puterea de calcul a atacatorului,
- *Securitatea ad-hoc*: argumentele despre resursele insuficiente ale unui atacator de a sparge mecanismele existente de securitate sunt expuse într-un mod convingător. Aceasta este cea mai răspândită abordare pentru studiul securității unui protocol.

O măsură posibilă împotriva acestui tip de atacuri este folosirea unor primitive de criptare bine construite.

3.4.7 Atacurile de estimare

O altă categorie de atacuri sunt cele de estimare. În aceste cazuri, se estimează *marcajul* sau *semnalul gazdă*, fără a cunoaște cheia secretă, folosind informații despre statistica marcajului, respectiv a semnalului gazdă. Aceste atacuri sunt aplicabile când marcajul a fost înserat în mod redundant, sau când avem la dispoziție mai multe copii marcate. În Figura 3.11 este prezentat atacul prin estimarea marcajului.

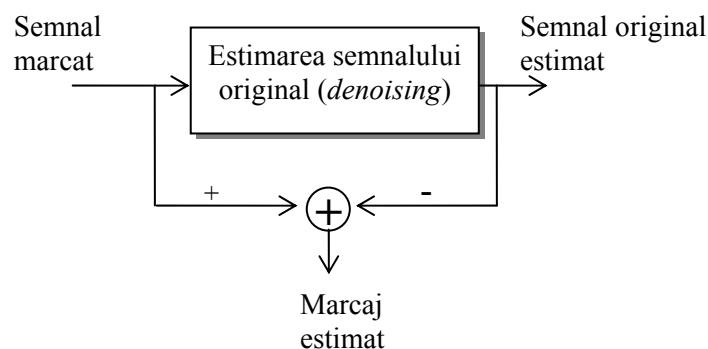


Fig. 3.11: Atac prin estimarea marcajului

Depinzând de scopul final al atacului, atacatorul poate estima marcajul sau semnalul gazdă folosind algoritmi ML (Maximum-Likelihood), MAP (Maximum A Posteriori), sau MMSE (Minimum Mean Square Error). Atacurile de estimare pot fi considerate de eliminare, de protocol, sau de desincronizare, funcție de scopul în care este folosit semnalul estimat.

La *estimarea semnalului gazdă*, marcajul este considerat ca zgomot în semnalul marcat. Acest atac este echivalent cu proiectarea unei scheme de *denoising* optimal. Dacă se ia în considerare legătura strânsă între *denoising* și compresie, atunci atacatorul poate folosi un codor bazat pe transformata wavelet cu un raport rată-distorsiune optim.

Cu alte cuvinte, estimarea gazdei se face prin *denoising* optimal, sau compresie perfectă. Aceste două operații sunt considerate atacuri de eliminare.

Estimarea marcajului se face folosind algoritmi de estimare ML, MAP, MMSE. În urma estimării, se extrage semnalul gazdă estimat din semnalul marcat.

3.4.8 Atacul de remodulare

Cu marcajul estimat, un atacator poate să *remoduleze o imagine*: se extrage marca estimată din imaginea marcată (modulare negativă). Un exemplu de atac de remodulare este prezentat în Figura 3.12. În cazul unui detector cu corelație, prin aceste acțiuni se anulează corelația pozitivă, cu condiția ca marcajul estimat să fie asemănător cu cel original. Pe de altă parte, prin extragerea unei versiuni amplificate a marcajului estimat, detectorul prin corelație nu va reuși să găsească marcajul în imaginea atacată. Pentru acest motiv, se introduce un câștig $\gamma \geq 1$ care reprezintă compromisul între distorsiunea structurii de date atacată, respectiv succesul atacului [VPPE01].

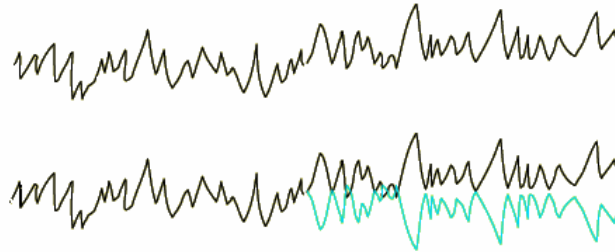


Fig. 3.12: Atac prin remodulare.

Există patru variante ale atacului de remodulare. Pentru câștigul $\gamma = 1$ se obține un estimat MMSE/MAP și atacul se reduce la *denoising*. Pentru câștigul $\gamma > 1$ deși calitatea documentului atacat este redusă, performanța detecției prin corelație scade sensibil. Detectorul poate decide chiar că imaginea nu a fost marcată dacă corelația ajunge la 0. A treia variantă este folosirea unei măști perceptuale în loc de un câștig fix, pentru a controla vizibilitatea distorsiunilor introduse.

Ultima variantă a atacului de remodulare este ca atacatorul să scadă estimatul marcajului ponderat de masca perceptuală, dar și să adauge puncte dispersate (*outliers*), pentru a obține distribuția unui zgomot non-gaussian, fapt care, din nou, scade performanța detecției prin corelație [VPPE01].

În plus, folosind proprietățile sistemului vizual uman, acest zgomot poate fi introdus în părți mai puțin semnificative perceptual. Această tehnică se numește *remodulare perceptuală* [VSA00]. Ea este exemplificată în Figura 3.13.

Atacul de estimare poate fi folosit pentru implementarea atacului de copiere, menționat mai sus. Desigur, marcajul copiat trebuie să fie adaptat la semnalul țintă pentru a păstra calitatea semnalului marcat în mod fals. Pentru imagini, se poate exploata sensibilitatea la contrast și fenomenul de mascare a texturilor specifice sistemului vizual uman. Atacul de copiere bazat pe estimare are succes dacă este folosit același model perceptual ca pentru algoritmul original de marcarea. Atacul descris este potrivit unei scheme de marcarea aditivă. În cazul sistemelor bazate pe cuantizare, chiar și un estimat perfect al marcajului nu poate fi copiat, deoarece este

foarte puțin probabil ca semnalul copiat să fie un marcaj valid pentru semnalul țintă. În Figura 3.14. este prezentat un sistem de implementare a atacului prin copiere.

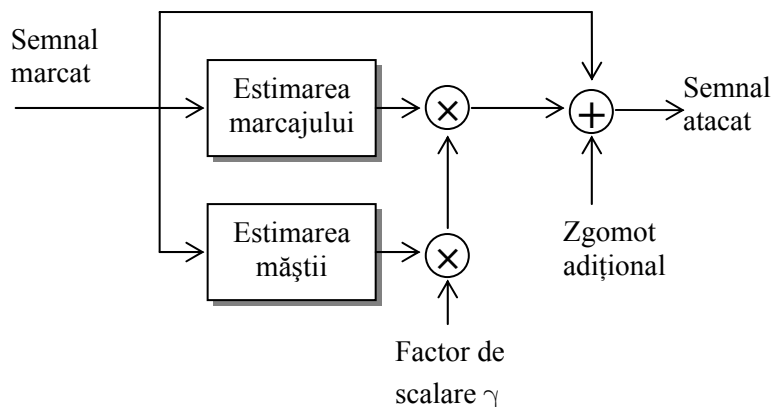


Fig. 3.13: Atac prin estimarea marcajului, remodulare perceptuală.

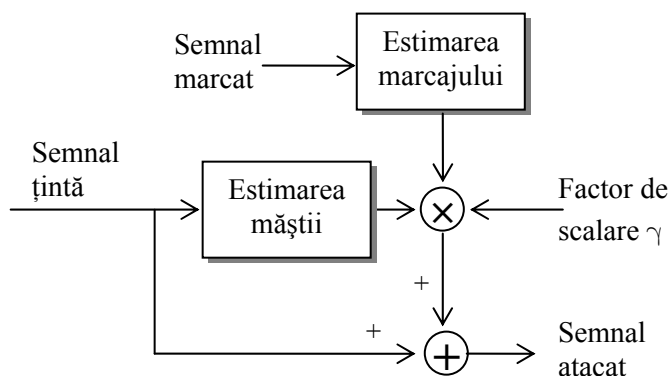


Fig. 3.14: Atac prin copiere

3.4.9 Atacul de estimare în desincronizare

Atacul prin estimarea marcajului poate fi eficient și în desincronizare. Ideea de bază este căutarea marcajelor care asigură sincronizarea, eliminarea acestora, și apoi aplicarea unor tehnici de desincronizare, cum sunt transformările globale afine, pentru imagini.

Ne referim în continuare la atacul metodelor de sincronizare prin înserarea unui marcaj de referință în spectrul de amplitudini al imaginii, sau prin generarea unor marcaje periodice, care pot fi detectate prin autocovarianță. În ambele cazuri, maximele sunt generate în domeniul transformatei Fourier [VSA00, VSA01], după cum se vede în Figura 3.15. Aceste vârfuri pot fi detectate, următorul pas fiind interpolarea spectrului imaginii marcate.

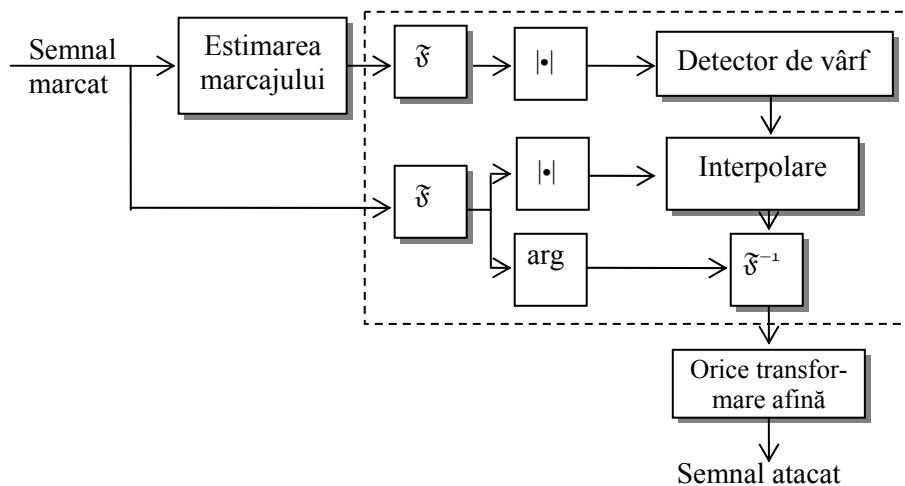


Fig. 3.15: Estimarea marcajului folosită în atacul de desincronizare.

3.4.10 Măsură împotriva atacurilor prin estimare

Pentru a fi robust în fața acestor atacuri, marcajul trebuie să fie dificil de estimat. Există două abordări.

În prima abordare [SG99], marcajul trebuie să îndeplinească *condiția densității spectrale de putere PSD* (Power spectral Density). Se are în vedere situația ideală din punct de vedere teoretic, când semnalul original și marcajul sunt tratate ca procese aleatoare, gaussiene colorate, staționare, independente, de medie nulă. Deoarece semnalul original este dat, se presupune că are o PSD fixă, în timp ce PSD a marcajului poate fi variabilă. Întrebarea este ce formă trebuie să aibă aceasta din urmă pentru ca marcajul să fie rezistent la atacurile prin estimare? În acest prim caz, estimatul optimal este obținut prin filtrare Wiener.

Eroarea medie pătratică E , între marcajul original și cel estimat, este o măsură bună pentru rezistența marcajului la atacul de estimare. Se poate arăta că E este maximă dacă și numai dacă densitatea spectrală de putere a marcajului este direct proporțională cu cea a semnalului.

Această cerință se numește *condiția densității spectrale de putere*. Pentru orice ieșire a filtrului adaptat, un marcaj care îndeplinește această condiție face ca atacul de estimare să inducă cea mai mare distorsiune.

Pentru ca valoarea corelației să ajungă la zero, atacul ar trebui să introducă distorsiuni cu puterea egală cu a semnalului original; prin urmare semnalul atacat nu va avea valoare comercială.

A doua abordare folosește *funcția de vizibilitate a zgomotului*. În marcarea imaginii, eliminarea zgomotului (*denoising*) este o cale naturală de a dezvolta atacuri bazate pe estimare, optimizate pentru modelul statistic al imaginilor [SVA99]. Imaginea marcată este văzută ca o versiune zgomotoasă a imaginii originale, iar marcajul reprezintă zgomotul care ar trebui estimat. Astfel, marcajul estimat este același cu zgomotul estimat.

După eliminarea zgomotului, se consideră un anumit model statistic pentru imaginea originală. Rezultă o *funcție de mascare a texturilor*, TMF (Texture Masking Function), dependentă de imagine, cu valori între 0 și 1. Pentru a înscrie un marcaj dificil de estimat, procesul de înglobare ar trebui să folosească funcția inversă acesteia, numită funcția de vizibilitate a zgomotului: $NVF = 1 - TMF$. Valorile de 1

ale funcției NVF indică regiuni plate, unde marcajul ar trebui atenuat, iar valorile de 0 ale NVF indică texturi și muchii, unde marcajul trebuie amplificat.

Prima abordare poate da rezultate mai slabe, deoarece modelul statistic folosit nu este potrivit imaginilor. Cu toate acestea, rezultatele obținute cu prima abordare sunt asemănătoare cu cele obținute cu a doua abordare. Aceasta este în concordanță cu argumentarea euristică a lui Cox ș.a. [CKLS97], care susține că marcajul trebuie plasat în “componentele perceptual semnificative” ale unei imagini.

Robustețea marcajului poate fi îmbunătățită prin creșterea energiei marcajului. Totuși, creșterea energiei conduce la degradarea calității imaginii. Prin exploatarea proprietăților HVS, energia poate fi crescută local în locurile unde marcajul nu este remarcat de ochiul uman. Deci, prin exploatarea HVS, se pot plasa marcaje invizibile perceptual, care au energie mai mare ca în cazul distribuției uniforme a acestei energii asupra imaginii.

Aprecierea calității imaginilor, pentru compresia măsurată relativ la imaginea originală necomprimată, conține aspecte subiective [BA99]:

1 Vizibilitatea erorilor în imaginea comprimată depinde foarte mult de localizare, de exemplu dacă sunt în arii foarte netede sau foarte texturate.

2 Importanța vizuală a erorilor depinde de localizarea în imaginea originală, de exemplu, erorile pe contururile sau pe fața unui portret vor afecta recunoașterea, mai mult decât erorile în fundal.

Aceste aspecte pot fi exploatate și în procesul de marcare transparentă.

Pentru ca un semnal vizual să fie perceput, trebuie să aibă o cantitate minimă de contrast, care depinde de luminozitatea și frecvența medie. Pe deasupra, un semnal de anumită frecvență poate masca un semnal perturbator de frecvență similară [Wan95], [BBCP98a]. Efectul de mascare este deja folosit în marcajul DCT dependent de imagine, descris în capitolul 2, unde coeficienții DCT sunt modulați cu ajutorul formulei (2.4). Aici, la fiecare sinusoidă din imagine (semnal de mascare), este adăugată o altă sinusoidă (marcajul), având amplitudinea proporțională cu semnalul de mascare. Dacă factorul de câștig k este ales corespunzător, se produce mascarea de frecvență.

Sistemul vizual uman este mai puțin sensibil la schimbări în regiunile cu luminozitate mare. Acest lucru poate fi exploatat prin alegerea factorului de câștig a marcajului dependent de luminozitate. Deoarece ochiul uman este cel mai puțin sensibil la culoarea albastră, un marcaj perceptual invizibil, plasat în canalul albastru, poate conține mai multă energie ca un marcaj perceptual invizibil plasat în canalul de luminozitate a unei imagini color [KJB97].

În jurul marginilor și porțiunilor cu texturi ale unei imagini, sistemul vizual uman este mai puțin sensibil la distorsiuni, decât în porțiunile netede. Acest efect se numește mascare spațială, și poate fi folosit pentru marcare, prin creșterea locală a energiei marcajului în aceste porțiuni mascate ale imaginii [MQ95]. Tehnicile de bază pentru marcarea spațială descrise anterior, pot fi extinse prin mascare spațială, de exemplu, folosind următoarea funcție de modulație:

$$I_w(x, y) = I(x, y) + Msk(x, y) \cdot k \cdot W(x, y)$$

Aici, $W(x, y)$ reprezintă marcajul pseudo-aleator bidimensional, k reprezintă factorul de câștig fix, și $Msk(x, y)$ reprezintă imaginea mască. Valorile măștii se întind de la 0 la k'_{max} și dau o măsură a insensibilității la distorsiuni pentru fiecare punct corespunzător în imaginea originală $I(x, y)$. O metodă de a genera imaginea mască

Msk , este filtrarea imaginii originale cu un filtru Laplace trece-sus și reținerea valorilor absolute a imaginii filtrate rezultate [KDHM99].

În figura 3.16(a) este arătată o mască pentru imaginea Lena, care este generată de un simplu detector de muchii Prewitt. Figura 3.16(b) arată marcajul puternic amplificat modulat cu această mască.

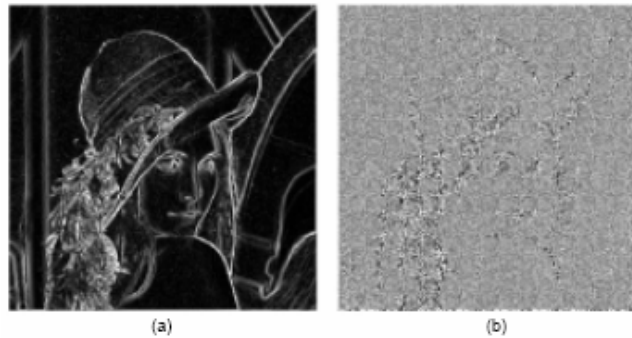


Fig. 3.16: Marcare folosind masca bazată pe operatori Prewitt. (a) Mască, și (b) Diferența $W(x,y)=I(x,y)-I_W(x,y)$

O altă metodă pentru generarea imaginii mască este folosirea sumei pătratelor coeficienților DCT-AC de dimensiune 8x8 [NCH99]. Figura 3.17 (a) arată o mască generată folosind această energie DCT-AC, pentru imaginea Lena. Figura 3.17(b) prezintă marcajul puternic amplificat modulat cu această mască. Experimentele arată că un marcaj invizibil, modulat cu un factor de câștig adaptat local la o asemenea mască, poate conține de două ori mai multă energie ca un marcaj invizibil, modulat cu un factor de câștig fix.

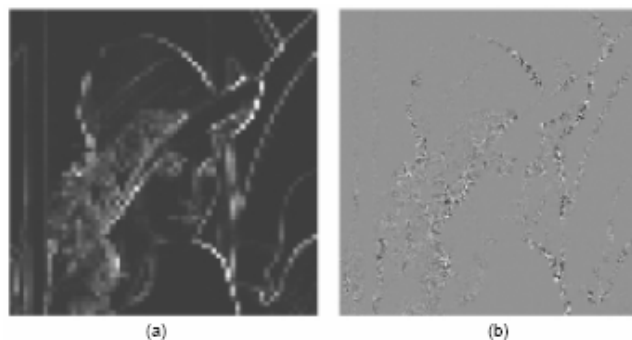


Fig. 3.17: Marcare folosind o imagine mască pe baza energiei DCT-AC. (a) Imaginea mască, și (b) Diferența $W(x,y)=I(x,y)-I_W(x,y)$

Mascarea spațială poate fi aplicată și atunci când marcajul e plasat în alt domeniu, cum ar fi DFT, DCT [BBCP98b], sau DWT. În acest caz, mai întâi este plasat marcajul nespațial într-o imagine I , rezultatul fiind o imagine temporară notată cu I_{Wt} . Imaginea marcată I_W este acum construită prin mixarea imaginii originale I și a acestei imagini temporare I_{Wt} , cu ajutorul unei imagini mască Msk :

$$I_W(x,y) = (1 - Msk(x,y)) \cdot I(x,y) + Msk(x,y) \cdot I_{Wt}(x,y)$$

Aici imaginea mască trebuie scalată la valori în domeniul 0 la 1.

3.4.11 Atacurile dependente de statistica locală a semnalului

Mai multe atacuri de estimare pot fi combinate cu succes în funcție de statistica locală a semnalului. Atacatorul poate estima marcajul folosind proprietăți ale sistemului vizual uman și diferite modele statistice ale imaginilor. Marcajul poate fi estimat și eliminat cu ușurință din regiunile plate ale imaginii, mai degrabă decât din texturi și muchii. Modelul stohastic pentru texturi și muchii este nestaționar și deci relativ complicat de folosit în cazul în care se dorește o estimare precisă. De aceea, atacatorul va încerca să folosească pe cât posibil avantajele *denoising*-ului, eliminând marcajul din regiunile plate fără a introduce distorsiuni vizibile, și chiar îmbunătățind raportul PSNR. Pe de altă parte, atacatorul va folosi remodularea cu putere crescută în regiunile de texturi și de muchii, care sunt mascate de sistemul vizual uman. În același timp, atacatorul poate folosi funcția de vizibilitate a zgomotului NVF (Noise Visibility Function), pentru a determina automat aceste regiuni [VSA00, VSA01]. Atacul este prezentat în Figura 3.18.

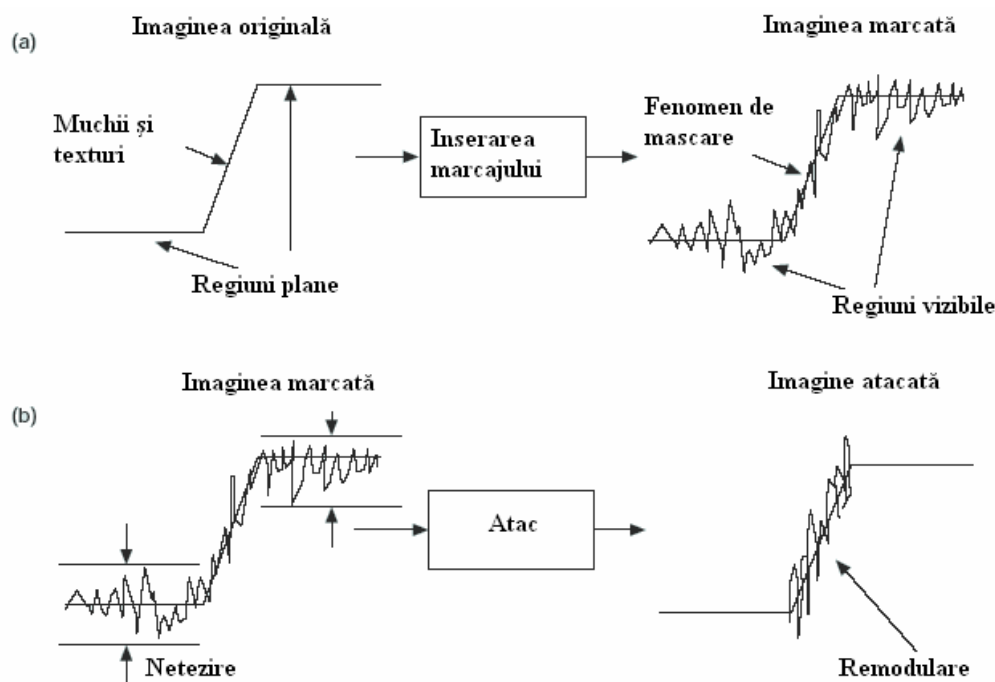


Fig. 3.18: a) Strategia folosită la marcare, prin exploatarea funcției de mascare a sistemului vizual uman; b) Strategia atacatorului folosind *denoising* și remodulare perceptuală.

3.4.12 Atacurile optimizate

Până acum, am enumerat atacurile bazate pe estimare, și soluțiile posibile pentru a le combate. Cu toate acestea, mai există și alte moduri în care sistemul de marcare poate să reacționeze la atacurile bazate pe estimare, în special la remodulare.

Detectorul poate estima marcajul remodulat și să încerce să inverseze remodularea, obținând astfel o detecție sigură a marcajului. De exemplu, când

estimarea marcajului se face prin filtrare Wiener, detectorul poate aplica o filtrare Wiener inversă. Evident, acest lucru nu este dorit de atacator. De aceea, el trebuie să adauge zgomot la semnalul atacat, care ar fi amplificat de filtrarea Wiener inversă, și astfel performanța detectorului scade.

Atacatorul trebuie să găsească o combinație bună între folosirea marcajului estimat și a zgomotului care trebuie adăugat. Sistemul de marcarea nu numai că trebuie să facă estimarea marcajului dificilă, dar și puterea marcajului să fie mai mare decât cea a zgomotului aditiv pe care un atacator l-ar putea introduce.

Problema poate fi formulată într-un mod și mai general: atacatorul încearcă să minimizeze capacitatea marcajului sub constrângerea distorsiunilor introduse de atac, în timp ce sistemul de marcarea încearcă să maximizeze capacitatea marcajului, sub constrângerea distorsiunilor introduse de marcarea. Această situație poate fi privită ca un “joc” între atacator și sistemul de marcarea. Pentru a rezolva această problemă, se folosește o abordare din teoria informației, care presupune că adversarii își cunosc comportarea [SEG01, MOS03].

Din punctul de vedere al teoriei informației, marcarea este un joc dintre atacator și marcator. Funcția de cost este informația mutuală între intrarea și ieșirea canalului de atac, atacatorul încearcă să o minimizeze în timp ce marcatorul încearcă să o maximizeze. Limita superioară a acestei informații mutuale este capacitatea marcajului. Cu alte cuvinte, cel mai bun atac este echivalent cu cea mai eficientă compresie posibilă, cu constrângerea dată de distorsiunile introduse, iar strategia optimă de marcarea este codarea optimă a canalului când atacatorul cunoaște caracteristica canalului.

Considerând cazul în care semnalul original și marcajul sunt procese aleatoare gaussiene colorate, staționare, independente și de medie nulă, densitatea spectrală de putere a marcajului este independentă de câtă distorsiune poate fi introdusă de atacator. La nivele scăzute de distorsiune, marcajele de tip zgomot alb se comportă aproape optimal, în timp ce la distorsiuni mari, marcajele care îndeplinesc condiția densității spectrale de putere sunt mai potrivite. Marcajele înserate în componente ale semnalului cu dispersie mare sunt eliminate mai eficient de zgomotul aditiv. Pentru a aplica aceste rezultate în marcarea transparentă, ar trebui folosite descompuneri bune ale semnalului, care-l separă în componente cu statistică diferită. În cazul imaginilor, descompunerea wavelet ar putea fi o alegere bună.

3.4.13 Atacurile ce folosesc mai multe cadre din secvența video (multiple-frames)

Aceste atacuri sunt specifice secvențelor video, și exploatează informația temporală disponibilă de la cadru la cadru într-o secvență video. Cele mai multe cadre sunt puternic corelate între ele, în special în scene statice sau cvasi-stactice. Această corelare se manifestă și între marcajele înserate în cadrele respective, ceea ce rezultă într-o redundanță temporală a secvenței video, precum și a secvenței marcajelor. Ideea care stă la baza atacurilor statistice este exploatarea acestei redundanțe pentru a elimina marcajul. În comparație cu atacurile asupra imaginilor marcate, atacurile asupra secvențelor video au nevoie de multe cadre pentru a fi eficiente. Aceste atacuri se pot face prin medierea mai multor cadre pentru a estima semnalul gazdă sau marcajul. Există două cazuri posibile:

1. marca înserată este diferită la fiecare cadru (atac de *mediere*), sau dimpotrivă,
2. marca înserată este aceeași pentru fiecare cadru (atac de *coliziune*).

Prin urmare, medierea va amplifica una dintre componente, semnalul gazdă original în primul caz, sau marcajul original în al doilea caz, și va atenua cealaltă componentă [Kun05, DCP00].

- **Atacul de mediere**

Acesta este un atac foarte simplu, bazat pe faptul că niște cadre consecutive din secvența video sunt asemănătoare, mai ales pentru scenele statice. Se presupune că marcajele în cadre diferite sunt *necorelate*. Medierea poate fi văzută ca o filtrare temporală trece-jos a semnalului video marcat, folosind o fereastră alunecătoare de L cadre, care calculează estimatul semnalului video original:

$$\hat{x}_t = \frac{1}{L} \sum_{k=t}^{t+L-1} y_k = \frac{1}{L} \sum_{k=t}^{t+L-1} x_k + \frac{1}{L} \sum_{k=t}^{t+L-1} n_k \quad t = 1 \dots N_f \quad (3.7)$$

unde \hat{x}_t este cadrul estimat t din semnalul video original, iar y_k este cadrul k din semnalul video marcat. Dacă L nu este prea mare, cadrele sunt asemănătoare și $\sum x_k$ tinde către un cadru mediu, în timp ce $\sum n_k$ scade spre 0 dacă marcajele sunt independente de la un cadru la altul. În Figura 3.19 este prezentat un atac de mediere. Aceste atacuri păstrează calitatea în scenele statice. Distorsiuni vizibile apar în scenele în mișcare, unde ar trebui folosit un L mai mic.

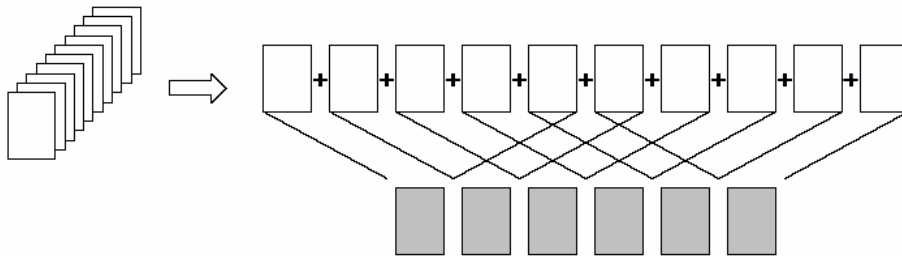


Fig 3.19: Atac de mediere într-o secvență video [Kun05].

- **Atacul de coliziune (estimare)**

Problema care apare la medierea printr-o fereastră alunecătoare a cadrelor este că nu funcționează bine când marcajele sunt corelate în cadre consecutive. Cel mai defavorabil caz apare când același marcaj este înserat în toate cadrele. În acest caz, un atac mai potrivit este cel de coliziune, care folosește redundanța marcajului în loc de cea a semnalului video. Presupunând că toate cadrele sunt independente, dar au înserate aceeași marcă în ele, se estimează marcajul din aceste cadre diferite din *toată* secvența video, cu scopul de a-l elimina.

Totuși, energia cadrelor este mult mai mare decât energia marcajului, și o simplă mediere nu va da un estimat bun al marcajului. Soluția este estimare marcajului din fiecare cadru, ca \hat{n}_t , de exemplu, dintr-un cadru \hat{x}_t din care zgomotul

a fost eliminat, folosind un filtru Wiener, calculând diferența $\hat{n}_t = y_t - \hat{x}_t$. Aceste estimări sunt apoi mediate pentru a obține o aproximare mai bună a marcajului original:

$$\hat{n} = \frac{1}{N_f} \sum_{t=1}^{N_f} \frac{1}{\sigma_{\hat{n}_t}} \hat{n}_t \quad (3.8)$$

unde $\sigma_{\hat{n}_t}$ este deviația standard a lui \hat{n}_t . Estimatul final al marcajului, \hat{n} poate fi eliminat printr-o scădere din fiecare cadru:

$$\hat{x}'_t = y_t - s \cdot p_t \cdot \hat{\sigma}_{n_t} \cdot \hat{n} \quad t = 1 \dots N_f \quad (3.9)$$

unde $\hat{\sigma}_{n_t}$ este deviația standard globală a zgomotului, estimată din fiecare cadru, iar s este un coeficient ales experimental. Scopul acestor factori este de a adapta semnalul, care va fi extras, la energia marcajului care trebuie eliminat, ținând cont de adaptabilitatea conținutului. p_t este o variabilă aleatoare cu valori posibile 1 sau 0, cu probabilitățile respective p și $1-p$. Aceasta provine din faptul că un zgomot va fi similar cu un marcaj ales pentru jumătate din pixelii considerați. De aceea, extrăgând toți biții marcajului estimat din cadrul marcat va crește probabilitatea ca marcajul original înserat să fie doar inversat, deci încă detectabil. Cea mai bună metodă de eliminare a marcajului este scăderea a jumătate din pixelii acestuia, punând $p = 0.5$ care duce la anularea autocorelației folosite în general pentru detecția marcajului.

O soluție la acest atac a fost propusă în [KMY04]: un sistem de distribuție multimedia în care toate copiile sunt marcate cu același marcaj, dar fiecare utilizator are o cheie secretă distinctă, ce diferă de cea de înserare. Un atacator cu acces la o cheie de detecție poate „păcăli” detectorul corespondent, dar nu și celelalte detectoare.

3.5 Atacurile ce folosesc mai multe copii marcate (multiple-copy)

Aceste atacuri intervin când semnalul gazdă este același, iar marcajul este diferit. În esență, aceste atacuri sunt de coliziune. Există două mari abordări ale acestui caz: prin prisma prelucrării semnalelor, respectiv prin prisma codării informației. Tipurile de coliziune pot fi clasificate după cum urmează [Kun05, EKK99, SEG00, ZWL03, WTWL04]:

- de estimare: liniară (prin mediere, ponderată sau nu; prin filtrare; zgomot alb) respectiv neliniară,
- de tip statistic: min, max, median, minmax, negativ modificat, negativ aleator.
- ipoteza marcării transparente (*marking assumption*): coliziune prin copiere-și-lipire, aleatoare, vot majoritar, atacuri binare (and, or, xor).

Într-un atac de coliziune, o coalitie de pirați care au versiuni diferite ale aceluiasi produs multimedia, examinează copiile diferite în speranța creării unui nou semnal care să nu fie legat de nici unul dintre ei. Există mai multe tipuri de coliziune. O metodă de coliziune liniară este sincronizarea copiilor marcate diferit și medierea lor. Un alt atac de coliziune, numit „copiere-și-lipire”, constă în asamblarea de către atacatori a unor porțiuni tăiate din propriile copii, rezultând un semnal nou. Alte

atacuri folosesc operații neliniare, cum ar fi luarea valorii maxime sau mediane a componentelor din semnale. Trebuie menționat că acest atac diferă de coliziunea asupra mai multor cadre dintr-o singură secvență video, așa cum s-a specificat în subparagraful 3.4.13.

3.5.1 Coliziunea liniară

Este unul dintre cele mai fezabile atacuri de coliziune împotriva *fingerprinting*-ului. Dacă sunt K utilizatori, fiecare deținând o copie marcată diferit, și se coalizează, ei pot să combine liniar aceste K semnale pentru a produce o versiune fără marcaj. Fiindcă, în mod normal, nici unul dintre atacatori nu este dispus să riște mai mult decât celălalt, semnalele ce conțin amprente diferite se mediază cu ponderi egale, ca în Figura 3.20. Medierea reduce puterea marcajelor. Cu cât numărul de atacatori este mai mare, cu atât fiecare marcaj este mai greu de detectat. Semnalul obținut poate avea o calitate perceptuală chiar mai bună, în sensul că e mai asemănător cu semnalul original, decât cele marcate. Atacul descris în [EKK99] completează schema din Figura 3.20 prin adăugarea unui zgomot de putere mică, semnalul original fiind afectat de procesul de marcare cu o distorsiune limitată. S-a arătat că $O(\sqrt{N/\log N})$ este ordinul de mărime al numărului de adversari suficienți pentru a învinge sistemul de marcare-amprentare, unde N este lungimea totală a marcajului.

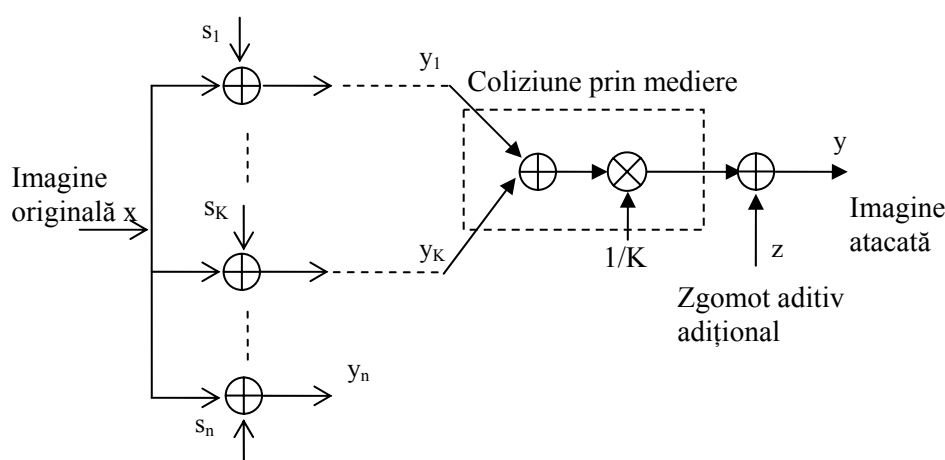


Fig.3.20: Coliziune liniară.

În [SEG00], este expus un atac mai general, în care atacatorii folosesc filtre invariante la translația liniară (LSI) plus zgomot alb pentru a elimina marcaje (amprente) bazate pe coduri ortogonale. Presupunând că toate amprente sunt independente și au caracteristici statistice identice, s-a arătat că atacul LSI optim este cel pentru care ponderile sunt egale înaintea adăugării zgomotului aditiv. Atunci când marcajul este împrăștiat în tot semnalul gazdă și detecția se face printr-o corelație, atacul de coliziune „copiere-și-lipire” are un efect similar cu cel de mediere. În ambele cazuri, energia fiecărei amprente este redusă cu un factor corespunzând la numărul de copii care se utilizează.

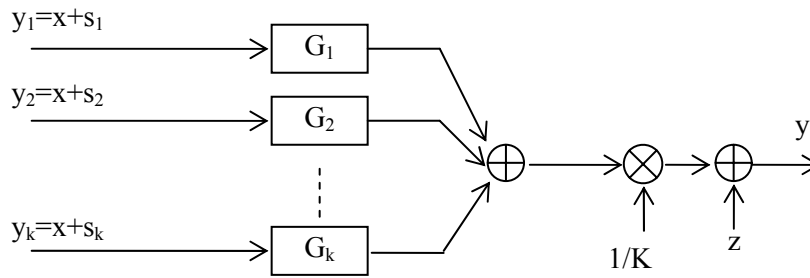


Fig.3.21: Coliziune liniară cu filtre LSI.

3.5.2 Coliziunea neliniară

Pentru fiecare componentă a semnalului multimedia, atacatorii pot alege orice valoare dintre cele observate, cuprinsă între cea minimă și cea maximă, cu grad mare de încredere că produsul obținut va avea o calitate perceptuală nealterată (valorile obținute fiind în gama JND). O clasă importantă de atacuri prin coliziune neliniară sunt cele bazate pe operații cum ar fi luarea valorii maxime, minime, sau mediana a componentelor corespundente din cele K copii marcate diferit [ZWL03]. Se poate presupune pentru simplitate, ca aceste atacuri au loc în același domeniu ca și cel al marcării. Diferența abia vizibilă (JND) din modelul vizual uman este folosită pentru a controla energia marcajelor înserate, pentru garantarea imperceptibilității. Câteva atacuri posibile sunt următoarele, [WTWL04]:

- *Minim, maxim, sau median*, semnalul are valoarea minimă, maximă, respectiv mediană a componentelor corespunzătoare a celor K semnale marcate;
- *Atacul minmax*: fiecare componentă din semnalul atacat este media între minimul și maximul componentelor corespunzătoare;
- *Atacul negativ modificat*: fiecare componentă din semnalul atacat este diferența dintre mediană și suma dintre maxim și minim a componentelor corespunzătoare;
- *Atacul negativ aleator*: fiecare componentă din semnalul atacat ia cu probabilitatea p , valoarea maximă a celor K componente ale semnalelor marcate, și valoarea minimă cu probabilitatea $(1 - p)$.

Atacurile de coliziune mediană sau minmax sunt similare ca performanță cu coliziunea liniară. Pe de altă parte, eficiența atacului se îmbunătățește prin coliziune minim, maxim sau negativ modificat. Atacul de coliziune negativ modificat are cea mai bună performanță, dar distorsiunile introduse sunt mult mai vizibile. După combinarea neliniară, atacatorii pot introduce zgomot aditiv [WTWL04].

Măsuri posibile împotriva atacurilor folosind copii multiple, sunt codurile anti-coliziune și construirea marcajelor astfel încât coliziunea să ducă la distorsiuni perceptuale pentru atacator (Joint Source Fingerprinting) [LK05].

3.6 Concluzii

În analiza performanțelor tehnicilor de marcarea transparentă, sunt folosite benchmark-urile (Stirmark, UnZign, Certimark, etc). În paralel cu dezvoltarea tehnicilor de marcarea transparentă, are loc și dezvoltarea unor noi atacuri. Este probabilă o cooperare a criptografiei cu tehnici moderne de prelucrarea semnalelor, domenii legate de obstrucționarea marcării transparente. Poate fi întrevăzută apariția unor atacuri noi care să îmbine tehnici de steganaliză cu atacuri din marcarea.

Capitolul 4

Aplicarea transformării wavelet în marcarea informată a imaginilor

4.1 Introducere

În acest capitol, se prezintă algoritmi de marcarea transparentă a semnalelor multimedia, în care s-a dorit ca marcajul să fie nu numai detectabil, ci să poată fi și extras [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. De aceea, pentru simplitate, s-a folosit un marcaj binar. Ne concentrăm asupra marcării imaginilor statice, având în vedere faptul că se poate face o generalizare a metodei și pentru alte tipuri de semnale multimedia.

În cele ce urmează, vom aborda o metodă de marcarea care lucrează în domeniul transformării wavelet. Cercetările făcute asupra ochiului uman indică faptul că retina împarte o imagine în mai multe componente, care se transmit de la ochi înspre cortex pe benzi diferite de frecvență. Aceste canale pot fi excitate doar de componente ale unor semnale cu caracteristici asemănătoare. Prelucrarea semnalelor din diferitele benzi de frecvență este independentă. Studiile au arătat că fiecare dintre aceste canale are o bandă de lățime de aproximativ o octavă. În mod asemănător, într-o descompunere multirezoluție, imaginea este separată în benzi de frecvență cu lățimi aproximativ egale pe o scară logaritmică. De aceea, este de așteptat ca folosirea transformării wavelet discrete să permită prelucrarea independentă a componentelor rezultate, fără o interacțiune perceptibilă/vizibilă între ele.

În plus, metodele prezentate [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] plasează marca atât în spațiu, cât și în frecvență; acest lucru permite în principiu detecția schimbărilor imaginii, localizate spațial și spectral.

Pentru a nu schimba imaginea în mod vizibil, nu înglobăm marcajul în componentele de frecvență joasă (subimaginea LL a transformatei). Procesul de înglobare are loc selectiv, în funcție de o cheie de marcarea, în subimaginea de detaliu ale transformatei imaginii. Schimbarea coeficienților selectați trebuie făcută în așa fel încât imaginea gazdă să nu fie perceptibil afectată.

4.2 Înglobarea și extragerea marcajului

4.2.1 Înglobarea marcajului

Presupunem, pentru simplitate, că marcajul binar are lungimea N_w și este compus din elementele $\{-1,1\}$. Imaginea originală f , în care înglobăm marca, este imaginea gazdă. Marcajul este înglobat în coeficienții wavelet de detaliu ai imaginii gazdă, cu ajutorul unei chei de marcarea. Această cheie este generată în funcție de imaginea originală și este folosită pentru a selecta pozițiile exacte în domeniul wavelet în care se înglobează marca. Pentru fiecare coeficient din domeniul wavelet, cheia are valoarea 1 sau 0, indicând dacă coeficientul este sau nu marcat. Numărul valorilor de „1” din cheie trebuie să fie mai mare sau egal cu lungimea marcajului.

Valorile marcajului sunt înglobate repetat în coeficienți diferiți selectați de cheie, dacă lungimea marcajului este mai mică decât numărul valorilor de „1” din cheie. Tehnica constă în trei etape descrise mai jos:

Etapa 1. Se calculează transformata wavelet discretă la nivelul de rezoluție L a imaginii gazdă, pentru a produce o secvență de $3L$ sub-imagini de detaliu, corespunzătoare detaliilor pe orizontală, verticală, respectiv pe diagonală pentru fiecare nivel de rezoluție și o aproximație grosieră a imaginii la cel mai mic nivel de rezoluție. Notăm cel de-al s -lea coeficient de detaliu din componenta imaginii la nivelul de rezoluție l a imaginii gazdă cu $f_{s,l}(m,n)$, unde $s \in \{h, v, d\}$ (coeficienții de detaliu pe orizontală, verticală, respectiv diagonală) și $l = 1, \dots, L$. Aproximarea imaginii este reprezentată de $f_{a,L}(m,n)$. Indicele a provine de la aproximare. În Figura 4.1 se prezintă un exemplu de calcul al transformării wavelet.

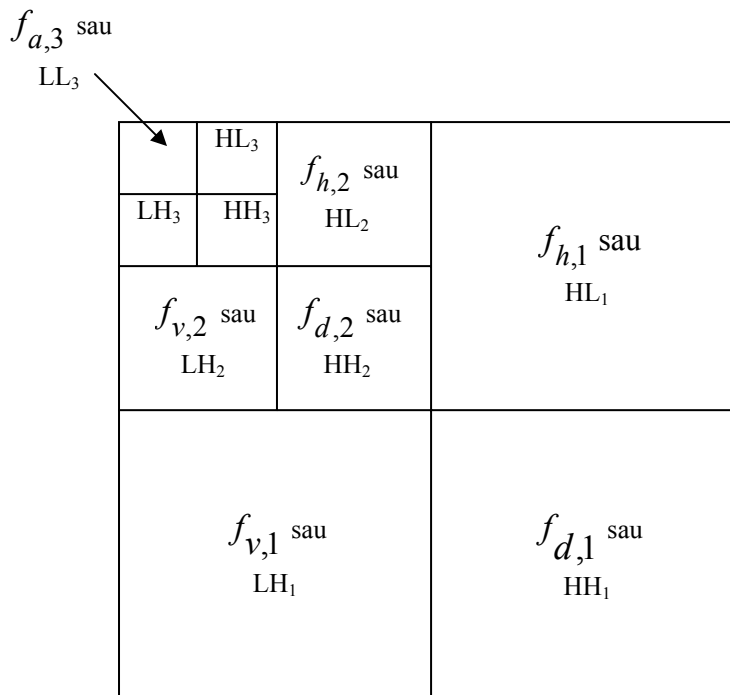


Fig. 4.1: Reprezentare ierarhică a coeficienților wavelet pe trei nivele de rezoluție. Imaginea de aproximare LL și imaginile de detaliu LH, HL și HH conțin informația necesară pentru refacerea imaginii de aproximare pentru următorul nivel de rezoluție.

În funcție de imaginile de detaliu, se generează cheia de marcare k , conform relației [NI03, NBK04, Naf04b, NB05]:

$$k_{s,l}(m,n) = \begin{cases} 1, & \text{dacă } f_{s,l}(m,n) > T_{s,l} \\ 0, & \text{altfel} \end{cases} \quad (4.1a)$$

$$k_{s,l}(m,n) = \begin{cases} 1, & \text{dacă } |f_{s,l}(m,n)| > T_{s,l} \\ 0, & \text{altfel} \end{cases} \quad (4.1b)$$

unde $k_{s,l}$ reprezintă cheia asociată fiecărei imagini de detaliu iar $T_{s,l}$ reprezintă un prag dependent de subbandă. Cheia se calculează pentru $l=1,\dots,L$ și pentru $s \in \{h,v,d\}$.

Dacă lungimea cheii N_k , o considerăm ca fiind numărul de cifre de „1” din cheie, atunci generarea cheii se va face astfel încât marca originală să fie înserată de un număr impar de ori, adică $\frac{N_k}{N_w} = M = 2p + 1$ (aici M specifică numărul de repetiții). De aceea, pentru fiecare nivel, dacă lungimea cheii $k_{s,l}$ este $N_{s,l}$, atunci generarea cheii respective se face astfel încât să se îndeplinească condiția din relația:

$$\frac{N_{s,l}}{N_w} = 2p + 1 \quad (4.2)$$

unde lungimea cheii k se poate defini astfel [NBK04]:

$$N_k = \sum_{\substack{l=1..L \\ s=h,v,d}} N_{s,l} \quad (4.3)$$

Etapa 2. Considerăm fiecare nivel de rezoluție l și localizarea coeficienților (m, n) . Dacă valoarea asociată cheii k este unu se procedează după cum urmează, altfel nu se înglobează marcajul:

$$f_{s,l}^w(m,n) = f_{s,l}(m,n) \oplus w(m,n) \quad (4.4)$$

unde $s \in \{h,v,d\}$, $f_{s,l}^w$ este coeficientul wavelet de detaliu al imaginii marcate, iar $f_{s,l}$ este coeficientul wavelet de detaliu al imaginii originale, pentru imaginea de detaliu k , și respectiv pentru nivelul de rezoluție l . Operatorul \oplus reprezintă operația de înglobare a bitului marcajului în coeficientul wavelet de detaliu corespunzător.

Etapa 3. Se aplică transformata wavelet inversă imaginilor de detaliu și de aproximare obținute, pentru a forma imaginea marcată. Procesul de înglobare a marcajului este prezentat în Figura 4.2.

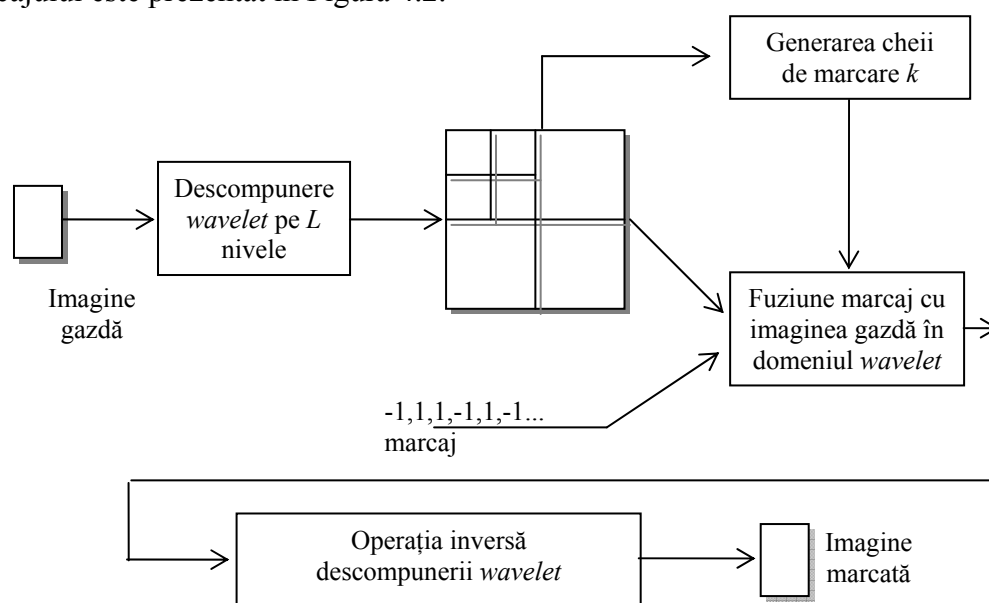


Fig. 4.2: Metodele de marcare propuse [NI03, NBK04, Naf04b, NB05, NIB05]. Se prezintă pașii care trebuie efectuați în general pentru a obține imaginea marcată.

4.2.2 Detecția și extragerea marcajului

Pentru a detecta și extrage marca, imaginea originală trebuie să fie cunoscută. Prin urmare, sistemul de marcare prezentat este *privat*. Imaginea recepționată este o versiune posibil distorsionată a imaginii marcate. Scopul procesului de extragere este obținerea unei estimări de încredere a marcajului original. Procesul de detecție cere cunoștințe și despre marcaj $w(m,n)$.

Reprezentăm imaginea căreia vrem să-i aplicăm procesul de extracție prin $r(m,n)$. Imaginea originală este $f(m,n)$. Pentru detecția și extragerea marcajului, se parcurg următoarele etape:

Etapa 1. Primul pas implică aplicarea unei descompuneri wavelet cu L nivele asupra imaginii $r(m,n)$, precum și asupra imaginii originale $f(m,n)$. Fie $r_{s,l}(m,n)$ a-s-a imagine de detaliu din nivelul de rezoluție l a imaginii $r(m,n)$.

Etapa 2. Cheia k se generează folosind imaginea originală, așa cum s-a văzut în faza înglobării marcajului. Această cheie furnizează locațiile unde a fost înglobat un bit al marcajului binar. Extragem marcajul din acești coeficienți după cum urmează:

$$\hat{w}(m,n) = r_{s,l}(m,n) \Theta_{f_{x,l}}(m,n) \quad (4.5)$$

unde $\hat{w}(m,n)$ reprezintă bitul recuperat, iar operatorul Θ reprezintă operația inversă celei efectuate în procesul de înglobare.

Etapa 3. Dacă marcajul a fost înglobat în locații diferite de mai multe ori, atunci este atașată marcajului estimat valoarea bitului extras cea mai des întâlnită. Dacă au fost extrași un număr egal de „1”, respectiv de „-1”, atunci se face o alegere aleatoare pentru valoarea bitului de marcaj. În [NI03], inserarea dar și detectarea marcajului se face respectiv în/din: **(a)** subbanda de detalii diagonale a primului nivel de rezoluție, **(b)** toate subbenzile de detalii ale acestui nivel. În afară de [NI03], în restul capitoului ne vom referi la trei tipuri de detectoare: **(1)** din toate nivelele, **(2)** din ultimul nivel, care este cel mai puțin afectat de operații precum compresia [NBK04, Naf04b, NB05], **(3)** detecție cu corelație maximă cu marcajul original (*max-correlation*) [Naf05b].

Un marcaj dat este detectat, dacă intercorelația dintre marcajul extras și marcajul dat este mai mare decât un prag cunoscut dinainte. Mai precis, condiția de detecție a marcajului este dată de:

$$\rho(w, \hat{w}) = \frac{\sum w(n) \cdot \hat{w}(n)}{\sqrt{\sum w^2(n)} \sqrt{\sum \hat{w}^2(n)}} \geq T, \quad (4.6)$$

unde w este marcajul dat, \hat{w} este marcajul extras, iar T este pragul cunoscut dinainte. $\rho(w, \hat{w})$ este cunoscut ca și coeficientul de intercorelație dintre marcajul dat și marcajul extras. Dacă nu se menționează alte condiții, toate sumele din ecuația (4.6) și din următoarea secțiune au indexul n și domeniul de la 1 la N_w . Dacă coeficientul de intercorelație este mai mare sau egal cu T , marcajul dat este detectat în imaginea recepționată. Dacă imaginea de la recepție este aceeași cu imaginea marcată, atunci coeficientul de intercorelație ar trebui să fie 1. Dacă imaginea recepționată este o versiune modificată a imaginii marcate, fără schimbări vizibile, atunci coeficientul de intercorelație ar trebui să aibă o valoare mare (subunitară, dar apropiată de 1). Detecția și extragerea este prezentată în Figura 4.3.

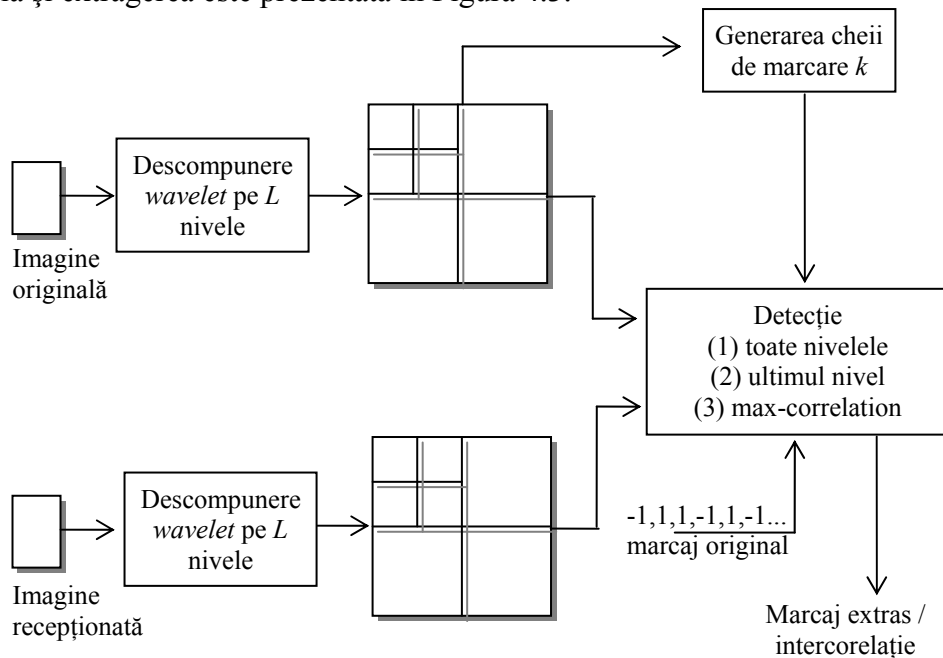


Fig. 4.3: Detecția și extragerea marcajului pentru metodele propuse [NBK04, Naf04b, NB05, NIB05]. În [NI03] detecția se face din (a) subbanda de detalii diagonale a primului nivel de rezoluție, (b) toate subbenzile de detalii ale acestui nivel

Cele trei variante ale metodei propuse în [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05], diferă prin modul de înglobare al bitului marcajului, așa cum s-a definit în ecuația (4.4), precum și în modul de generare a cheii de marcarea (diferă valorile $T_{s,l}$). Pentru a treia variantă, alegerea acestor praguri se face pe baza unei *analize statistice* a coeficienților wavelet [NIB05].

4.3 Prima metodă de marcarea informată

În [NI03], am experimentat inserarea marcajului în **primul nivel de rezoluție**. Detecția a fost făcută din toate subbenzile, sau numai din subbanda de detalii diagonale. Imaginea originală se descompune într-o imagine de aproximație și trei imagini de detaliu, cu alte cuvinte L este 1. Prin urmare, generarea cheii se face doar pentru primul nivel, folosindu-se un singur parametru q_1 . Operația definită de operatorul \oplus din relația (4.4) este în acest caz:

$$f_{s,1}^w(m,n) = f_{s,1}(m,n) + \alpha w(m,n) \quad (4.7)$$

unde $s \in \{h, v, d\}$, iar α este o variabilă pozitivă, definită de utilizator. Este ușor de dedus că operația definită de \ominus din relația (4.5) este în acest caz:

$$\hat{w}(m,n) = \frac{r_{s,1}(m,n) - f_{s,1}(m,n)}{\alpha} \quad (4.8)$$

Dacă $r_{s,1}(m,n) = f_{s,1}(m,n)$, se face o alegere aleatoare pentru bitul de marcaj binar.

Pentru simulări, am folosit următoarele valori pentru parametri: $q_1 = 0.06$, iar $\alpha = 10$, transformata wavelet cu funcție mother wavelet Daubechies 5. Am înglobat marcajul în două moduri:

- numai în coeficienții wavelet de **detaliu pe diagonală** ai primului nivel de rezoluție, respectiv,
- în **toate imaginile de detaliu ai primului nivel** de rezoluție.

Imaginea originală, precum și cele două imagini marcate sunt prezentate în Fig. 4.4.



Fig.4.4(a) Imaginea originală “Lena”, (b) Versiunea marcată în subimaginea de detalii diagonale la primul nivel, PSNR=43.76 dB, (c) Versiunea marcată “Lena”, în toate imaginile de detaliu ai primului nivel de rezoluție, PSNR=39.14 dB.

Cele două imagini marcate au $PSNR = 43.76$ dB, respectiv $PSNR = 39.14$ dB. Se poate observa că a doua imagine este perceptual mai afectată decât prima. Marcajul extras din a doua imagine este mai robust împotriva atacurilor decât cel extras din prima imagine.

Am studiat efectul distorsiunilor obișnuite ale semnalului (compresie JPEG, filtrare mediană, zgomot aditiv alb gaussian) asupra coeficientului de intercorelație între marcajul cunoscut și cel extras din imaginea atacată. Comparăm performanțele acestei prime variante a metodei propuse cu o metodă propusă de Kundur și Hatzinakos în [KH98]. Cheia de marcarea folosită pentru a îngloba marcajul este $k_{d,l}(m,n)$. Parametrul definit de utilizator este $Q = 4$, așa cum au indicat autorii în [KH98]. În acest caz, imaginea marcată are $PSNR = 57.33$ dB.

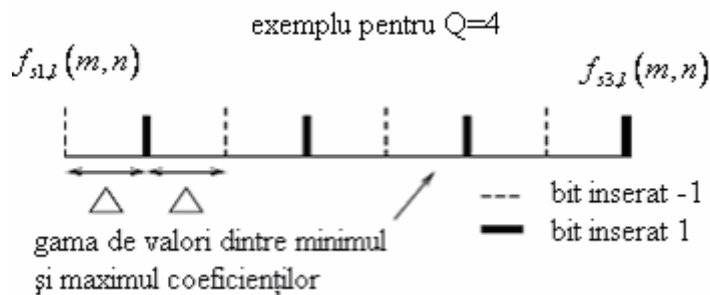
În [KH98], marcajul se inserează după cum urmează:

a. se sortează coeficienții în ordine crescătoare astfel încât $f_{s1,l}(m,n)$, $f_{s2,l}(m,n)$ și $f_{s3,l}(m,n)$ sunt coeficienți $f_{s1,l}(m,n) \leq f_{s2,l}(m,n) \leq f_{s3,l}(m,n)$, unde $s1, s2, s3 \in \{h, v, d\}$ și $s1, s2, s3$ sunt diferite.

b. Se cuantizează $f_{s2,l}(m,n)$ ca în figura de mai jos. Gama de valori între $f_{s1,l}(m,n)$ și $f_{s3,l}(m,n)$ este împărțită în cuante de lățimea

$$\Delta = \frac{f_{s3,l}(m,n) - f_{s1,l}(m,n)}{2Q - 1},$$

unde Q este o variabilă definită de utilizator. Pentru a insera un bit 1, $f_{s2,l}(m,n)$ este cuantizat la cea mai apropiată valoare cu linie continuă din figură, respectiv pentru -1, la cea mai apropiată valoare punctată.



Procedeeul de inserare a marcajului în [KH98]

Detecția se face într-o manieră similară, prin ordonarea coeficienților wavelet, și estimarea bitului care a fost inserat, din poziția coeficientului de mijloc.

În Fig. 4.5, se prezintă coeficientul de intercorelație $\rho(w, \hat{w})$ în funcție de dimensiunea filtrului $M \times M$, pentru filtrarea mediană, în funcție de rata de compresie, pentru compresia JPEG, respectiv în funcție de raportul semnal/zgomot (SNR). Graficele marcate cu simbolul „o” sunt rezultatele pentru prima abordare (a fost marcată numai imaginea de detalii pe diagonală). Graficele marcate cu simbolul „x” sunt rezultatele pentru a doua abordare (au fost marcate toate imaginile de detalii). Celelalte grafice sunt rezultatele pentru metoda propusă în [KH98].

Coeficientul de intercorelație pentru metoda propusă în această secțiune este, în mod evident, mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG și zgomot alb gaussian aditiv.

Metoda propusă nu arată robustețe împotriva filtrării mediane, comparativ cu metoda din [KH98].

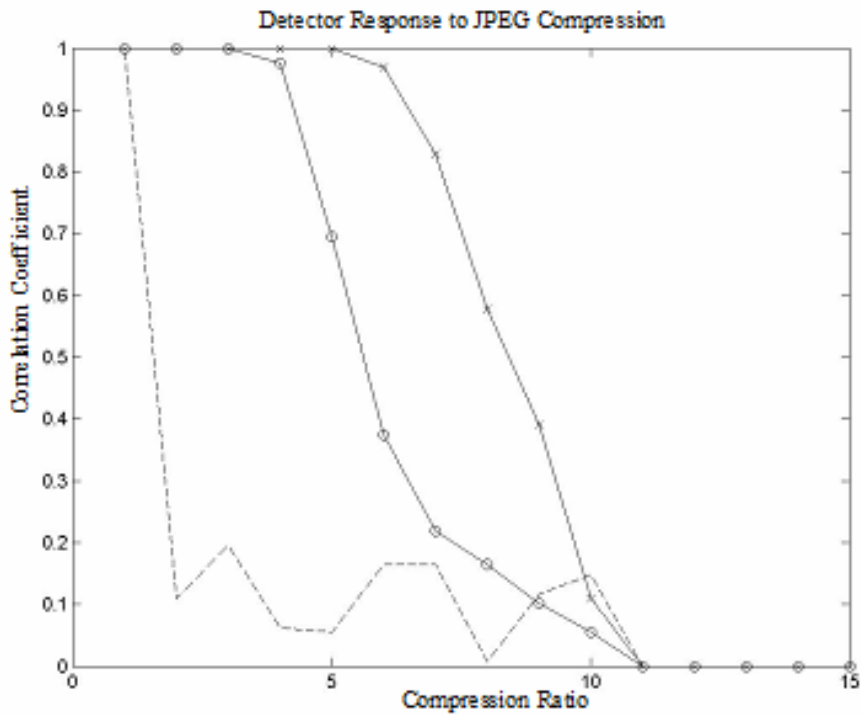


Fig. 4.5 (a) Răspunsul detectorului la compresia JPEG.

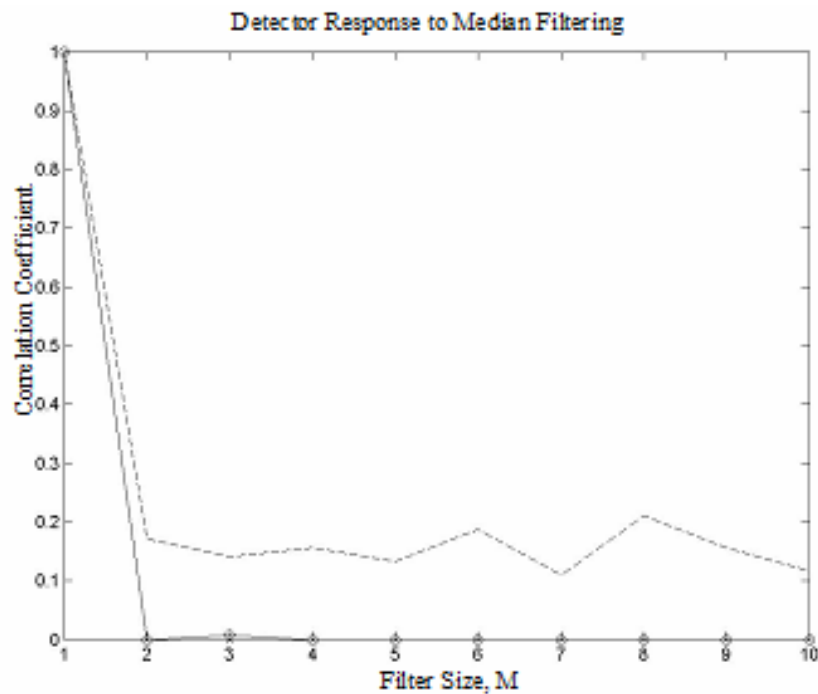


Fig. 4.5 (b) Răspunsul detectorului la filtrarea mediană.

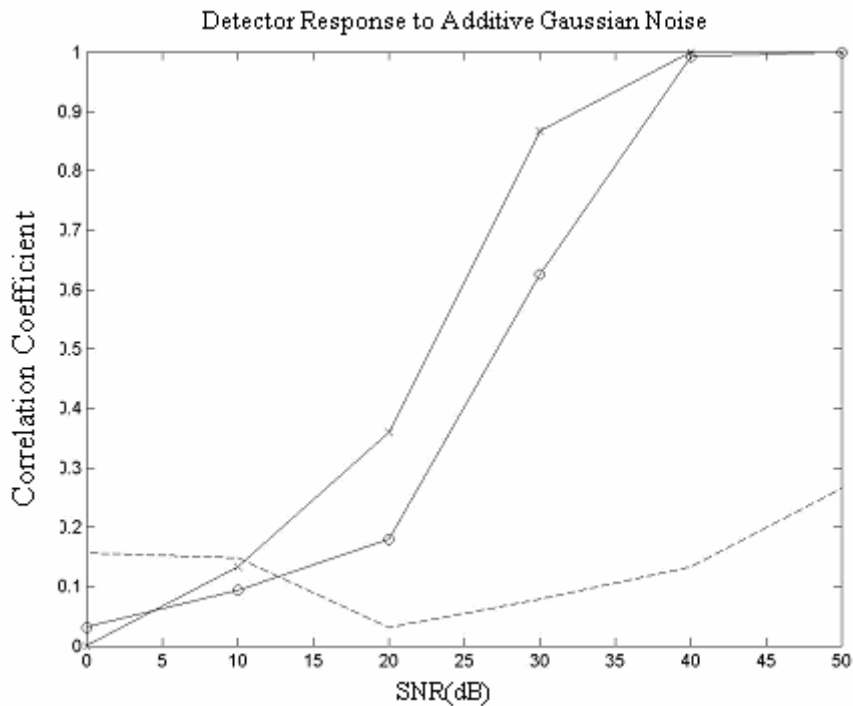


Fig. 4.5 (c) Răspunsul detectorului la zgomot alb gaussian aditiv. Graficele marcate cu simbolul „o” sunt rezultatele pentru prima abordare, cele marcate cu „x” sunt rezultatele pentru a doua abordare. Restul graficelor sunt rezultatele pentru metoda din [KH98].

4.4 A doua metodă de marcarea informată

Imaginea originală se descompune pe trei nivele de rezoluție, adică într-o imagine de aproximație $f_{a,3}$ și câte trei imagini de detaliu pentru fiecare nivel de rezoluție.

Generarea cheii se face pentru trei nivele de rezoluție, cu ajutorul parametrilor q_1, q_2, q_3 , folosind relația (4.1a). Aceștia sunt pozitivi și pot fi definiți de utilizator:

$$T_{s,l} = q_l \max_{m,n} \{ f_{s,l}(m,n) \} \quad (4.9)$$

În acest caz operația \oplus din relația (4.4) este:

$$f_{s,l}^w(m,n) = f_{s,l}(m,n) + \alpha \cdot f_{s,l}(m,n) w(m,n) \quad (4.10)$$

unde $s \in \{h, v, d\}$, $l = 1, \dots, L$ iar $\alpha \in (0,1)$ este o variabilă definită de utilizator, respectiv operația \ominus din relația (4.5) este:

$$\hat{w}(m,n) = \frac{r_{s,l}(m,n) - f_{s,l}(m,n)}{\alpha \cdot f_{s,l}(m,n)} \quad (4.11)$$

Dacă $r_{s,l}(m,n) = f_{s,l}(m,n)$ și/sau dacă $f_{s,l}(m,n) = 0$, se face o alegere aleatoare pentru $w(m,n)$.

Un set preliminar de experimente [Naf04a] a fost efectuat pe imaginea Lena. Ca parametri s-au folosit, marcajul binar de lungime $N_w = 256$, transformata wavelet cu funcția mother wavelet Daubechies 5 ca domeniu de marcare, numărul de nivele de rezoluție $L = 3$, intensitatea de marcare $\alpha = 0.1$ precum și variabilele dependente de nivel $q_1 = 0.06$, $q_2 = 0.04$, $q_3 = 0.02$.

Imaginea originală, imaginea marcată cu metoda propusă, precum și imaginea marcată cu metoda descrisă în [KH98] sunt prezentate în Fig. 4.6. Pentru a îngloba marcajul folosind metoda din [KH98], cheile de marcare folosite pentru fiecare nivel de rezoluție sunt $k_{d,1}$, $k_{d,2}$, respectiv $k_{d,3}$ (care indică selectarea pozițiilor în care se inserează marcajul). Aici înglobarea marcajului se face în mai multe nivele de rezoluție, față de experimentul anterior.



Fig. 4.6: (a) Imaginea originală "Lena", (b) Versiunea marcată "Lena", folosind a doua variantă a metodei propuse, PSNR=45.39 dB, (c) Versiunea marcată "Lena", folosind metoda din [KH98], PSNR=45 dB

Cele două imagini marcate au PSNR foarte apropiat: 45.39 dB, respectiv 45 dB. Nici una nu este afectată în mod vizibil de procesul de marcare.

În Fig. 4.7, se prezintă coeficientul de intercorelație $\rho(w, \hat{w})$ în funcție de dimensiunea filtrului, $M \times M$, pentru filtrarea mediană, în funcție de rata de compresie, pentru compresia JPEG, respectiv în funcție de raportul semnal/zgomot (SNR). Graficele marcate cu simbolul „+” sunt rezultatele pentru metoda propusă, cele cu linii întrerupte fiind graficele pentru extragerea marcajului din ultimul nivel de rezoluție. Graficele nemarcate sunt rezultatele pentru metoda propusă în [KH98], iar cele cu linii întrerupte reprezintă graficele pentru care marcajul a fost extras din ultimul nivel de rezoluție.

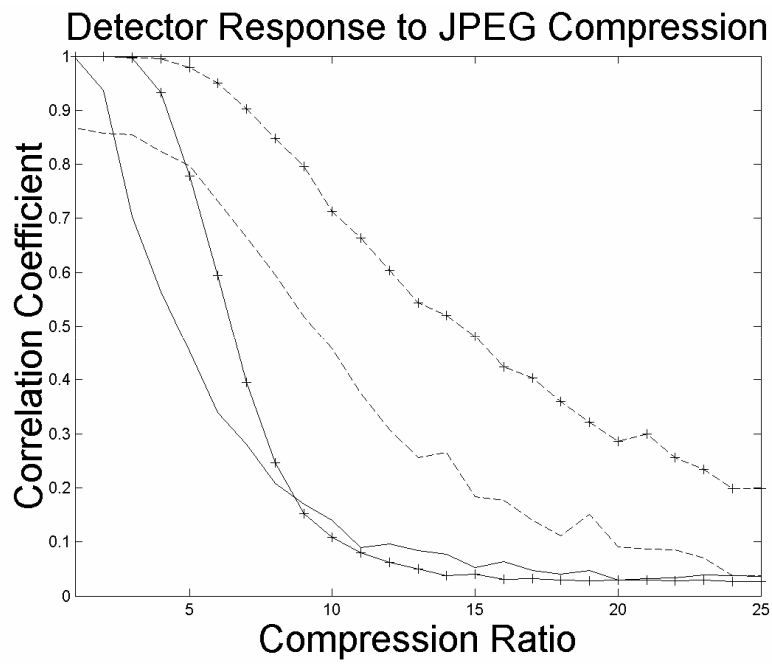


Fig. 4.7(a): Răspunsul detectorului la compresie JPEG

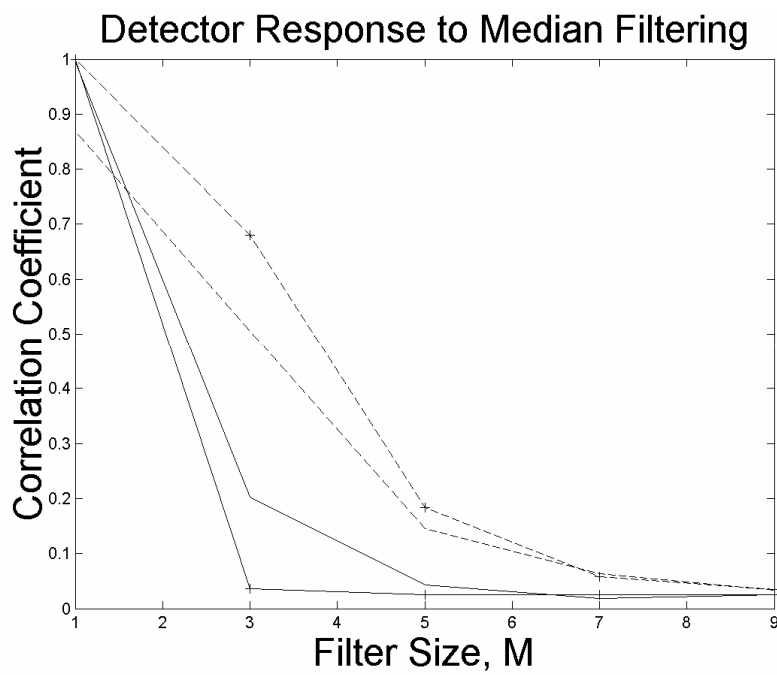


Fig. 4.7(b): Răspunsul detectorului la filtrare mediană

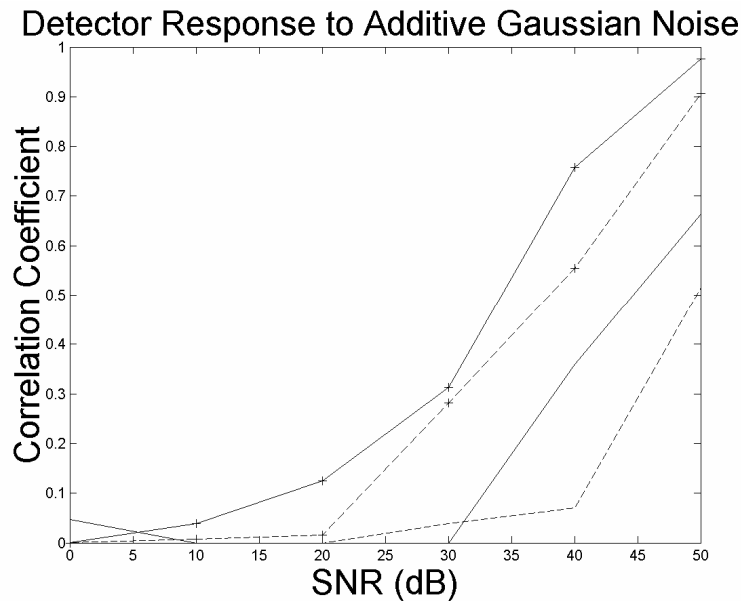


Fig. 4.7(a): Răspunsul detectorului la zgomot AWGN.

Fig. 4.7: Răspunsul detectorului la distorsiuni obișnuite. Graficele marcate cu “+” sunt pentru metoda propusă, cele nemarkate sunt pentru metoda din [KH98].

Graficele cu linie întreruptă sunt obținute pentru extragerea marcajului din ultimul nivel de rezoluție.

Rezultate. Se observă că performanțele metodei propuse în [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelație este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluție. Acest lucru se datorează faptului că distorsiunile obișnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un al doilea set de experimente [Naf04b] a fost efectuat folosind patru imagini de mărime 256x256, și anume Lenna, Boat, Barbara și Peppers, prezentate în Figura 4.8. Ca parametri s-au folosit, marcajul binar de lungime $N_w = 256$, transformata wavelet cu funcția mother wavelet Daubechies 5 ca domeniu de marcarea, numărul de nivele de rezoluție $L = 3$, intensitatea de marcarea $\alpha = 0.1$ precum și variabilele dependente de nivel $q_1 = 0.06$, $q_2 = 0.04$, $q_3 = 0.02$.

Performanțele metodei propuse în [Naf04b] sunt comparate cu tehnica spread-spectrum în domeniul DCT propusă de Cox ș.a. [CKLS97]. Aceștia înglobează o secvență pseudo-aleatoare în cei mai mari coeficienți DCT, fără a afecta coeficientul DC, astfel împrăștiind marca în mai multe componente spectrale:

$$v'(i) = v(i)(1 + \beta w(i))$$

unde $v(i)$ reprezintă coeficientul DCT de marcat, $w(i)$ este bitul de marcaj, β este puterea de marcarea, iar $v'(i)$ este coeficientul marcat. În lucrarea originală [CKLS97], marcajul era o secvență pseudo-aleatoare de tip $\mathcal{N}(0,1)$ cu lungimea 1000 și puterea de marcarea era de valoarea $\beta = 0.1$.

Pentru o mai bună comparație, marcajul folosit este bipolar, cu aceeași lungime, ca la metodele mele, 256 biți. De asemenea, numărul de repetiții a fost același în ambele cazuri (spre exemplu 33 repetiții pentru Peppers).



Fig.4.8: Imagini originale folosite în primul set de experimente: Lenna, Boat, Barbara și Peppers. Coloana din mijloc reprezintă imaginile marcate cu metoda propusă [Naf04b]. Coloana din dreapta reprezintă imaginile marcate cu metoda din [CKLS97]

Diferența între imaginea marcată și cea originală este evaluată în două moduri, folosind PSNR precum și observatori umani. Imaginile marcate cu metoda propusă nu au fost distorsionate semnificativ față de originale, în timp ce cele marcate cu metoda lui Cox ș.a. au distorsiuni vizibile, chiar supărătoare. Imaginile originale și cele marcate cu ambele metode sunt prezentate în Fig. 4.8. Tabelul 4.1 conține valorile PSNR pentru fiecare imagine.

Tab. 4.1: Valori PSNR [dB] ca măsură a zgomotului introdus de procesul de marcare

Imagine \ PSNR	Lenna	Boat	Barbara	Peppers
Metoda propusă	45.39 dB	44.35 dB	44.18 dB	45.55 dB
Metoda lui Cox și alții	27.19 dB	25.35 dB	26.44 dB	25.75 dB

În metoda propusă, diferența între imagini este prezentată în Fig. 4.9. Este evident că marcajul este inserat în texturi și contururi. De exemplu, la imaginea Lenna, marcajul afectează detaliile precum penele de la pălărie.

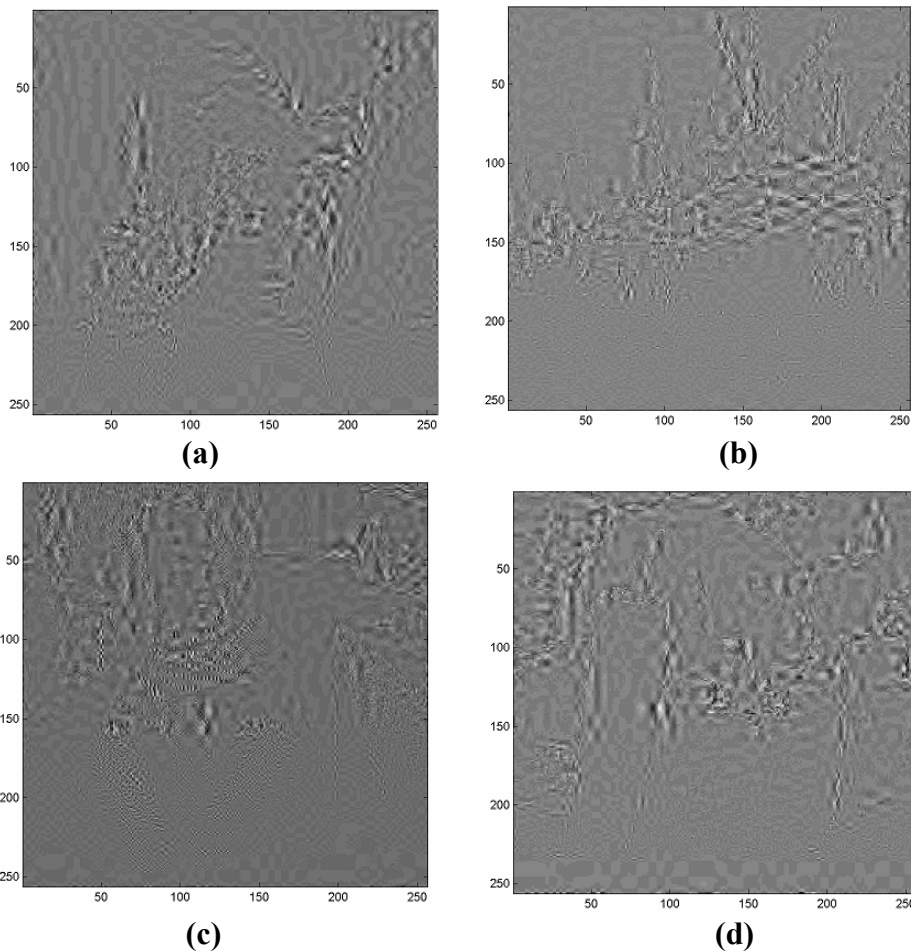


Fig. 4.9: Imagini diferență între imaginea marcată și cea originală pentru cele patru cazuri, Lenna (a), Boat (b), Barbara (c), și respectiv, Peppers (d).

Rezultate. Am arătat că cele patru imagini nu au fost afectate de procesul de marcare. Se analizează robustețea sistemului propus cu parametrii prezentați.

Extragerea marcajului se face în două feluri, folosind regula majoritară (detector tip 1, notat NC1 în următoarele figuri), și din ultimul nivel, aici $l=3$, cel cu rezoluție brută (detector tip 2 notat aici NC2).

Efectul prelucrărilor semnalelor obișnuite (filtrare mediană, zgomot AWGN, compresie JPEG) este prezentat prin coeficientul de corelație între original și marcajul recuperat. Performanțele pentru [Naf04b] sunt comparate cu rezultatele metodei din [CKLS97]. Pentru fiecare imagine, răspunsul detectorului este prezentat ca funcție de lungimea ferestrei filtrului M , rata de compresie CR și raportul semnal-pe-zgomot SNR pentru cazul filtrării mediane, compresiei JPEG și respectiv zgomot AWGN (Fig. 4.10 - 4.21). Răspunsul detectorului a fost calculat ca o medie de 32 răspunsuri pentru 32 marcaje necorelate. Graficele marcate cu simbolurile "o" și "+" sunt rezultatele pentru metoda propusă [Naf04b], detector 1 și 2 (sau NC1 și NC2) respectiv, în timp ce graficele nemarcate reprezintă rezultatele pentru metoda propusă în [CKLS97].

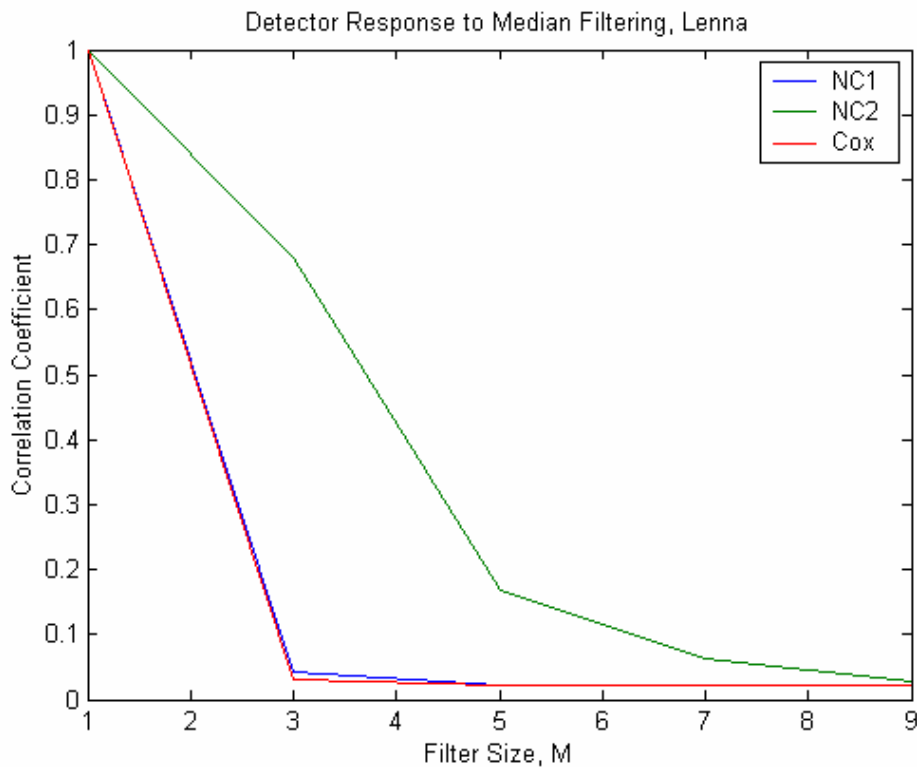


Fig. 4.10: Răspunsul detectorului la filtrarea mediană, imagine test "Lenna" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

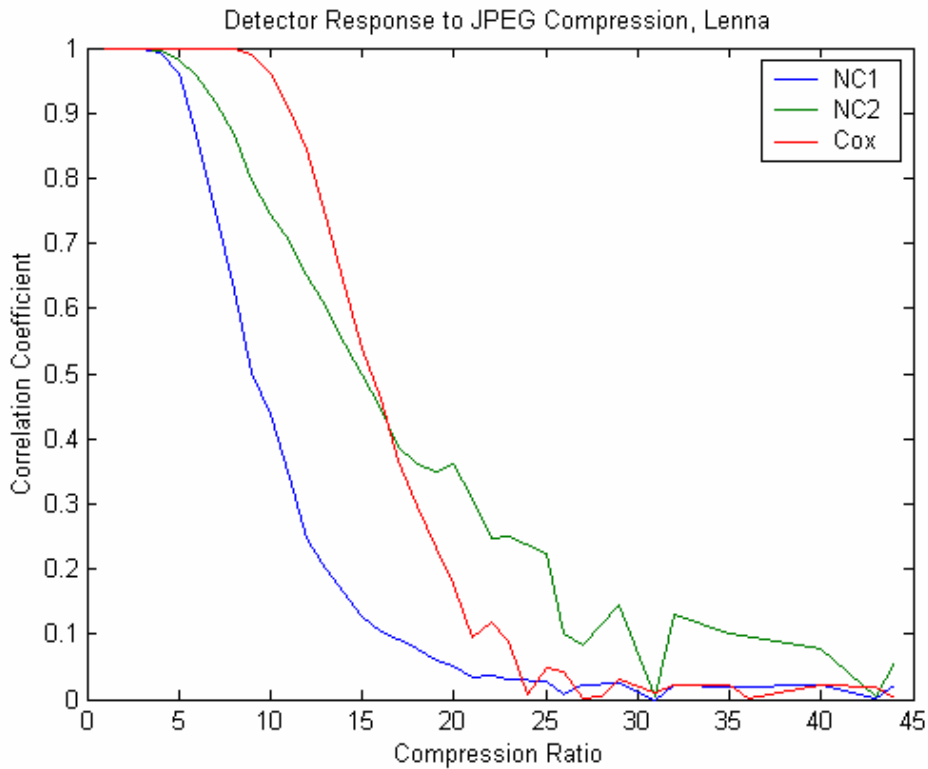


Fig. 4.11: Răspunsul detectorului la compresie JPEG, imagine test "Lenna" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

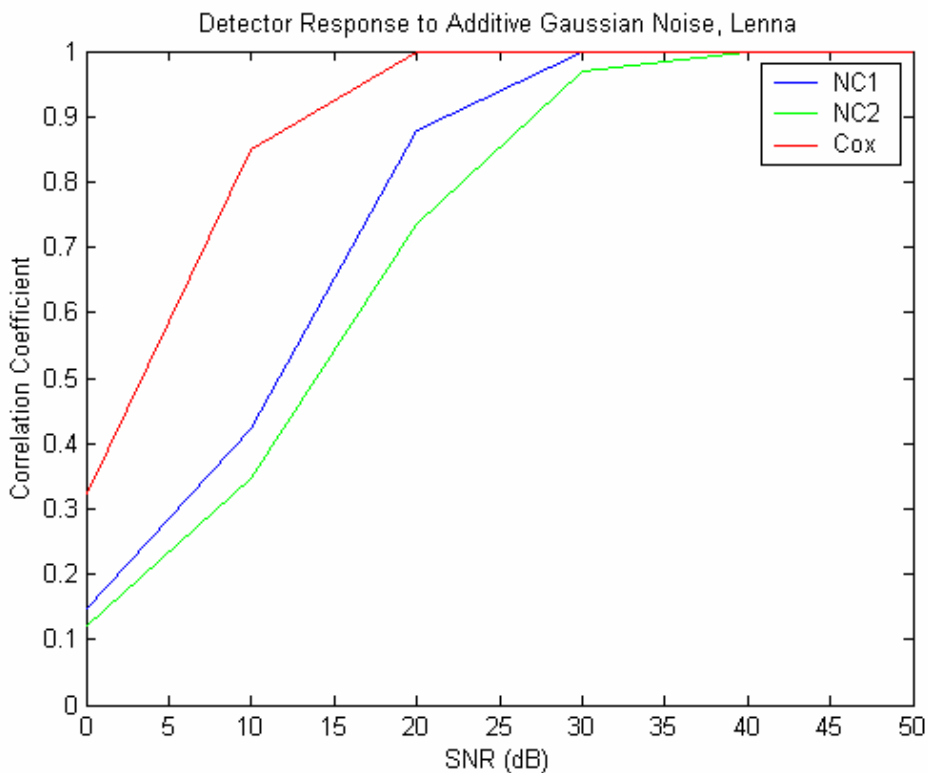


Fig. 4.12: Răspunsul detectorului la AWGN, imagine test "Lenna" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

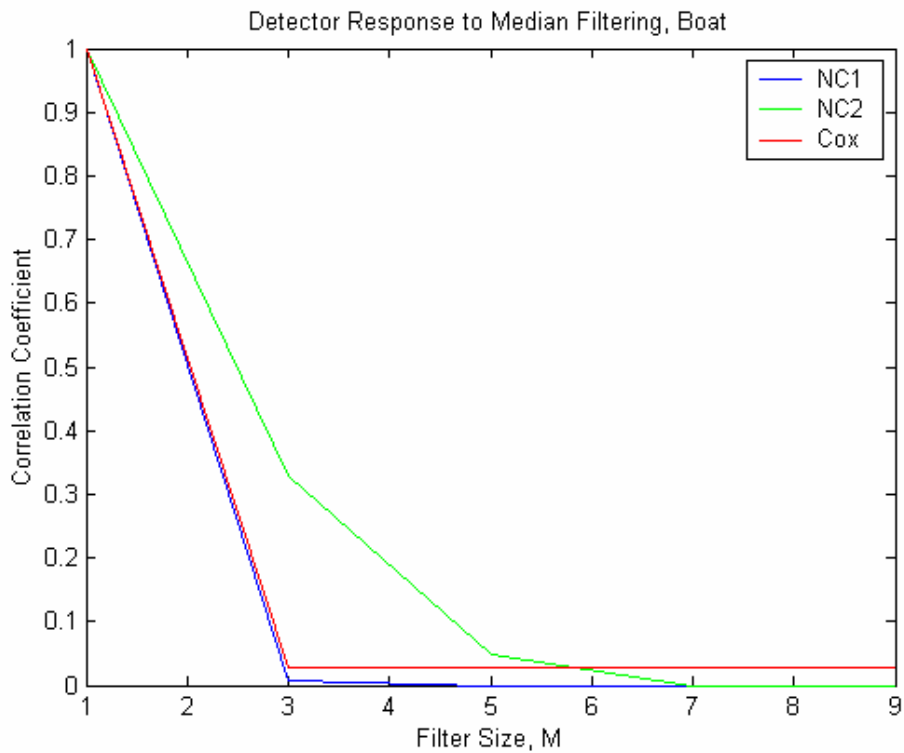


Fig. 4.13: Răspunsul detectorului la filtrarea mediană, imagine test "Boat" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

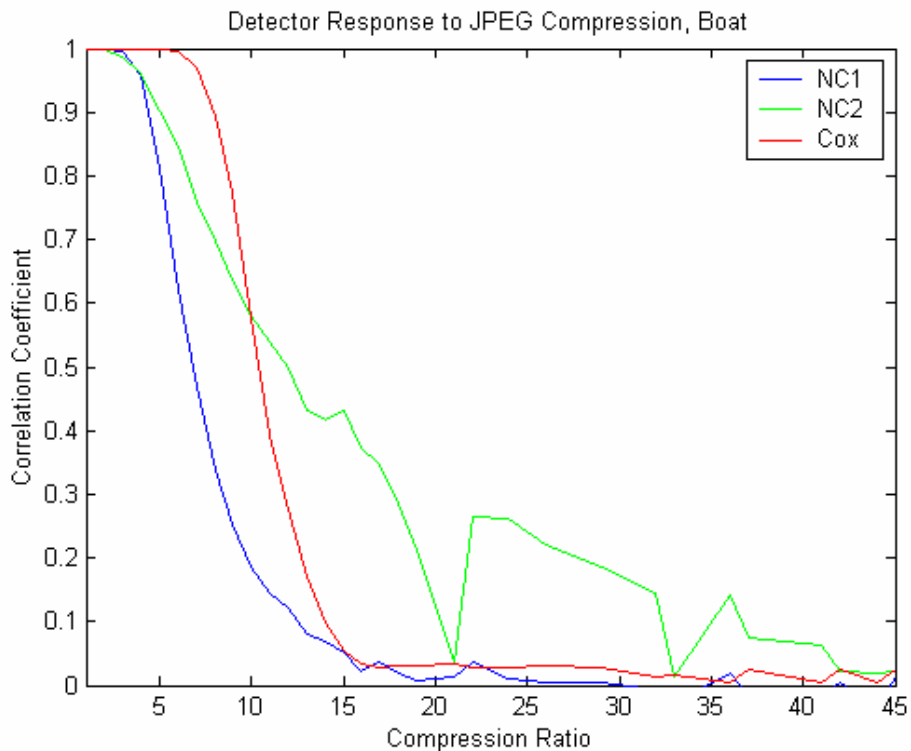


Fig. 4.14: Răspunsul detectorului la compresie JPEG, imagine test "Boat" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde)

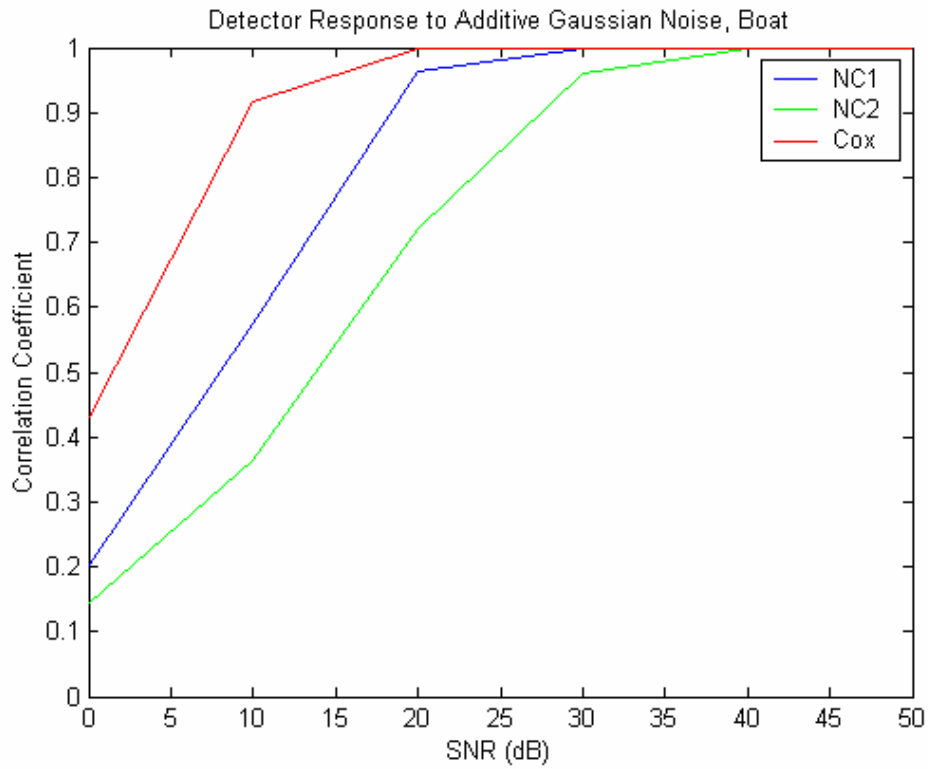


Fig. 4.15: Răspunsul detectorului la AWGN, imagine test "Boat" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

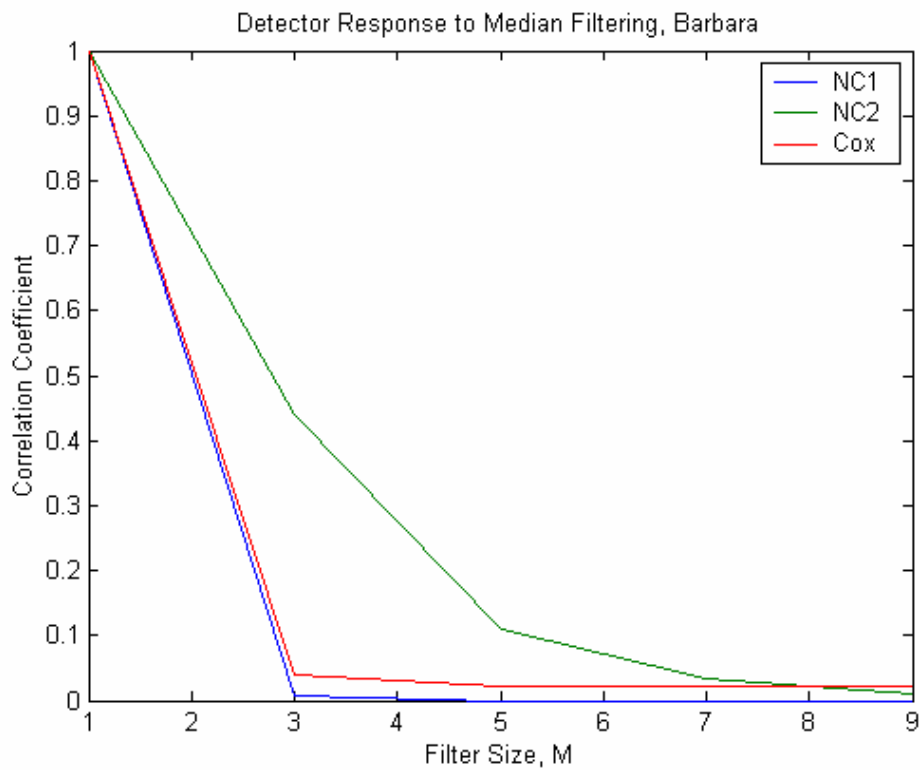


Fig. 4.16: Răspunsul detectorului la filtrarea mediană, imagine test "Barbara" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

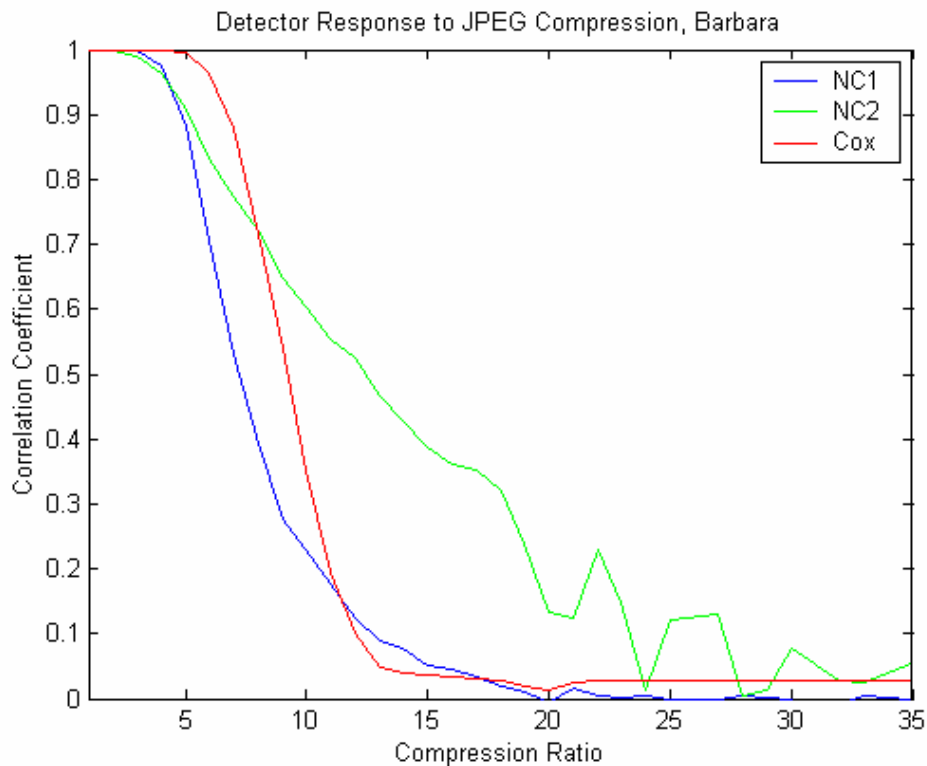


Fig. 4.17: Răspunsul detectorului la compresie JPEG, imagine test "Barbara" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

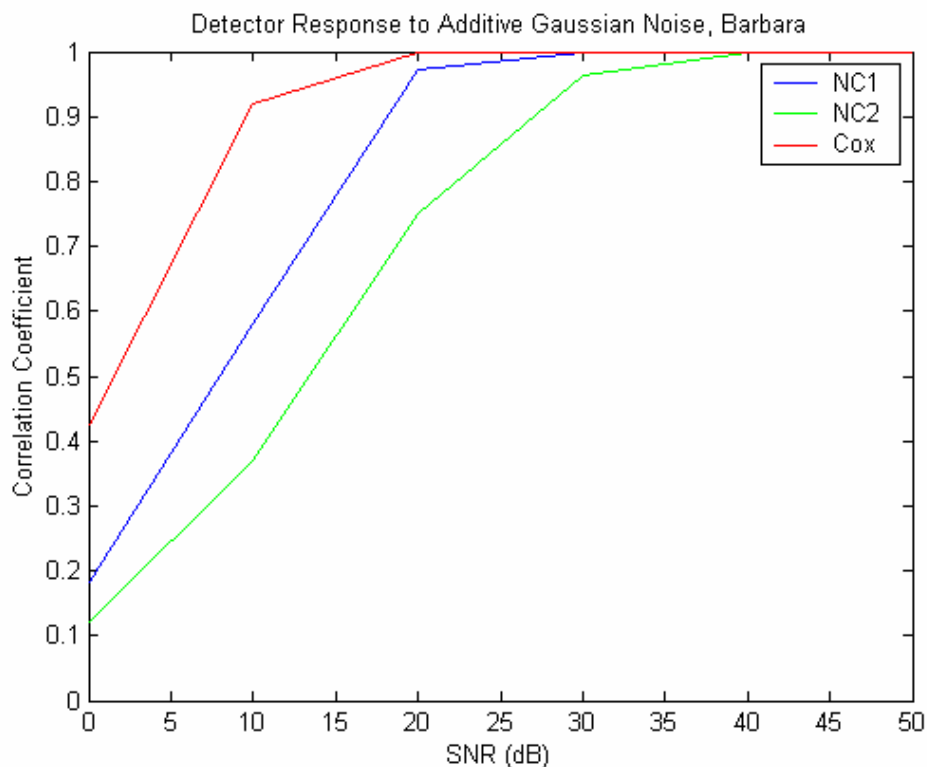


Fig. 4.18: Răspunsul detectorului la AWGN, imagine test "Barbara" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde)

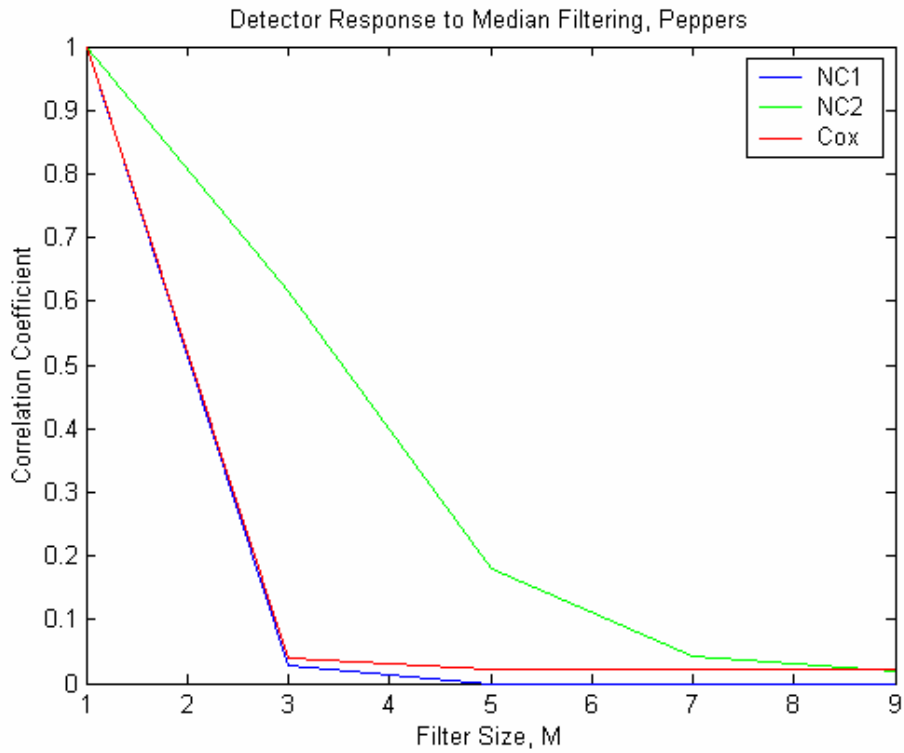


Fig. 4.19: Răspunsul detectorului la filtrarea mediană, imagine test "Peppers" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde)

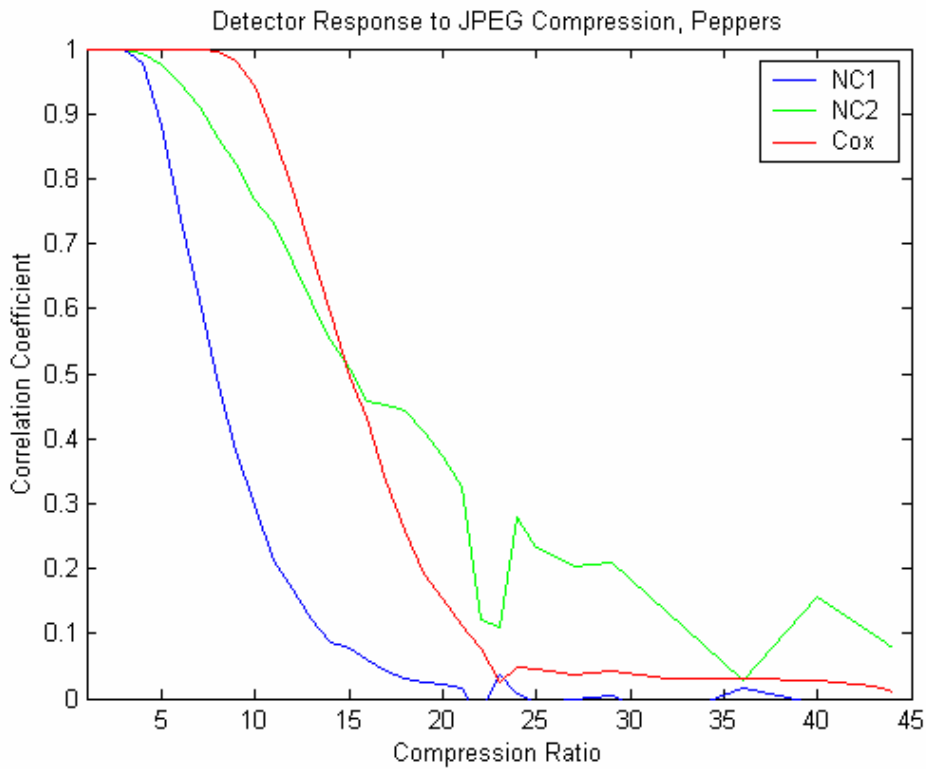


Fig. 4.20: Răspunsul detectorului la compresie JPEG, imagine test "Peppers" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

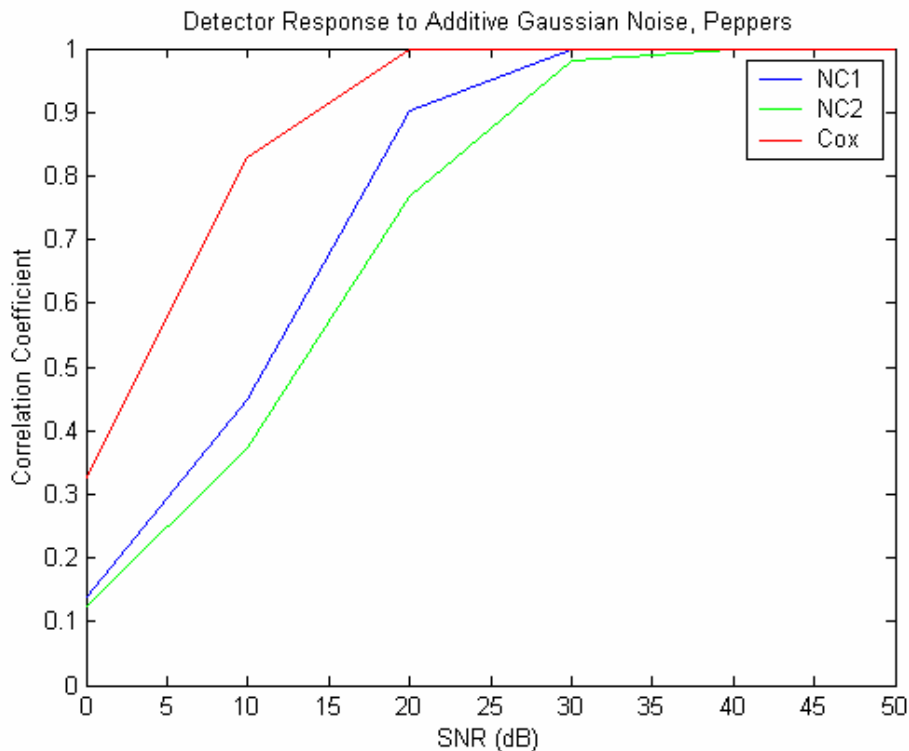


Fig. 4.21: Răspunsul detectorului la AWGN, imagine test "Peppers" pentru metoda din [CKLS97] (roșu), metoda propusă, detectorul 1 (albastru), detectorul 2 (verde).

Punând valoarea pragului la 0.5 în procesul de detecție avem următoarele rezultate.

Atac prin filtrare mediană: Pentru imaginile marcate Lenna, Barbara și Peppers, atacul prin filtrare mediană cu mărimea filtrului mai mare sau egal decât $M=3$ duce la o corelație mai mică decât 0.5.

De fapt numai detectorul NC2 detectează marcajul cu succes în urma filtrării cu $M=3$. Pentru imaginea Boat nici măcar detectorul NC2 nu reușește să detecteze marcajul.

Compresie JPEG: Pentru Lenna, corelația este mai mică decât 0.5 la o rată de compresie 16 (pentru detectorul NC2 și Cox) și respectiv CR 10 (NC1). Pentru Boat și Barbara, corelația este mai mică decât 0.5 la o rată de compresie de 13 pentru NC2, 10 pentru Cox și 7 pentru NC1. Pentru imaginea Peppers, valorile ratei de compresie pentru care corelația este mai mică decât 0.5 este 15 (NC2, Cox) și respectiv 8 (NC1).

Atac AWGN: Pentru Lenna și Peppers, răspunsul detectorului pentru metoda lui Cox ș.a. este peste 0.5 la un raport semnal-pe-zgomot de 5 dB, având o performanță considerabil mai bună decât detectoarele NC1 (12 dB) și NC2 (15 dB).

Pentru Boat și Barbara, valorile detectorului sunt aproximativ egale pentru fiecare metodă: 3 dB (Cox), în jur de 14 dB (NC2) și 7 dB (NC1).

O metodă robustă de marcarea transparentă a fost prezentată în [Naf04b] ce înserează marcajul în coeficienți selectați în așa manieră încât schimbările să nu fie

vizibile în imagine. Marcajul este inserat în texturi și muchii ale imaginii folosind sistemul vizual uman. Ambele metode sunt dependente de imagine. Aparent metoda lui Cox și alții este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, și inferioară pentru filtrarea mediană. Aceste teste au fost efectuate însă pentru imagini marcate puternic în cazul metodei [CKLS97]. Metoda prezentată de mine este comparabilă sau mai bună decât metoda lui Cox ș.a. În cele ce urmează prezint **al treilea set de experimente**, care ia în considerare acest aspect.

Pentru toate simulările, care vor fi prezentate în continuare s-a folosit imaginea „Peppers” (256x256) și o marcă binară având lungimea $N_w = 256$. S-a utilizat transformata wavelet cu funcția mother wavelet Daubechies 5, cu 3 nivele de rezoluție. Marcajul a fost generat aleator.

În toate testele s-au folosit următorii parametri: $q_1 = 0.06$, $q_2 = 0.04$, $q_3 = 0.02$. Mai exact, au fost afectați 8448 de coeficienți din totalul de 65536 (incluzând subbanda LL), prin urmare numărul de repetiții al marcajului original a fost pentru această imagine $M=33$. Intensitatea de marcare α a avut una dintre valorile 0.1, 0.2 și 0.3.

Extragerea marcajului a fost realizată în două moduri [Naf05a]:

- din toate nivelele de rezoluție, prin mediere, respectiv,
- din ultimul nivel de rezoluție al transformatei, care poate fi afectat mai puțin de distorsiuni obișnuite ale semnalului.

S-a comparat metoda propusă [NBK04, Naf04b, NB05, Naf05b] cu tehnica spread-spectrum în domeniul DCT propusă de Cox ș.a.[CKLS97]. Pentru a face posibilă compararea cu metoda propusă, se inserează același marcaj binar și același număr de repetiții a marcajului ca în [NB05]. Imaginile rezultate pentru tehnica propusă de Cox ș.a. [CKLS97] sunt vizibil distorsionate față de cele originale, având raportul maxim semnal-pe-zgomot (PSNR) în jur de 25 dB, ceea ce este inacceptabil. Fixând valoarea $\beta = 0,01, 0,02$ și $0,03$, imaginile marcate cu tehnica SS au PSNR comparabil cu cele marcate cu tehnica propusă. Sunt considerate separat trei cazuri: a) $\alpha = 0.1$ și $\beta = 0.01$; b) $\alpha = 0.2$ și $\beta = 0.02$; c) $\alpha = 0.3$ și $\beta = 0.03$.

Imaginea originală Peppers, precum și imaginile marcate cu cele două metode sunt prezentate în Figurile 4.22, 4.23 și 4.24. Observatorii umani nu pot face distincție între imaginea originală și imaginile marcate.

În Tabelul 4.2 se prezintă valorile PSNR pentru fiecare imagine marcată (Peppers, Lena, Boat și Barbara) ca o măsură a distorsiunilor introduse de marcaj.

Tab. 4.2: Valori PSNR [dB] pentru imaginile marcate, tabel din [NB05]

Metodă \ Imagine	Metoda propusă [NB05]			Metoda lui Cox [CKLS97]		
	$\alpha=0.1$	$\alpha=0.2$	$\alpha=0.3$	$\beta=0.01$	$\beta=0.02$	$\beta=0.03$
Peppers	45.54	40.28	36.94	45.75	39.73	36.21
Lena	45.39	40.12	36.77	47.19	41.17	37.65
Boat	44.35	38.86	35.45	45.35	39.33	35.81
Barbara	44.18	38.7	35.27	46.44	40.42	36.90

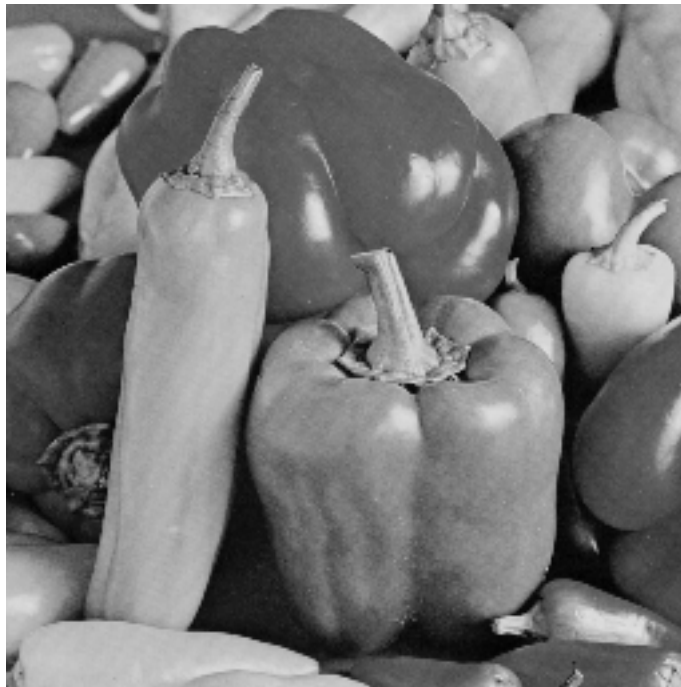


Fig. 4.22: Imagine originală Peppers

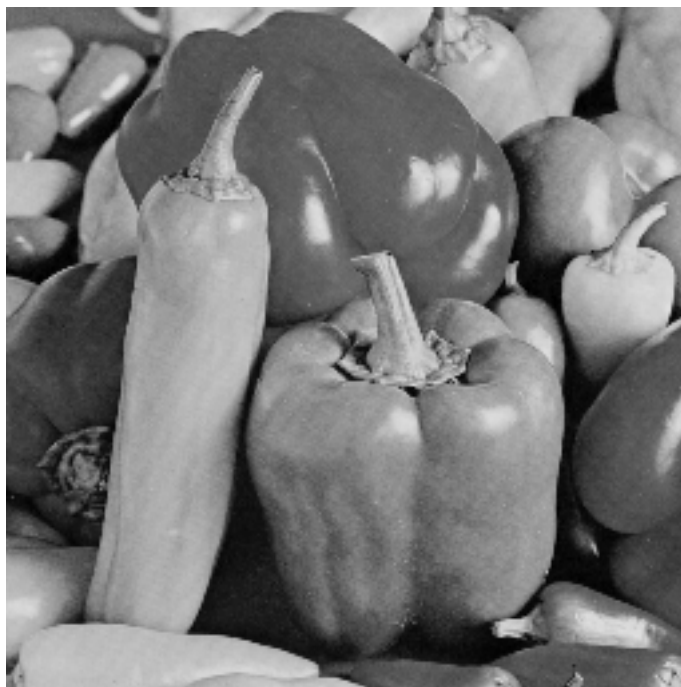


Fig. 4.23 (a): Imagine marcată [NB05], pentru $\alpha = 0.1$, PSNR=45.54 dB.

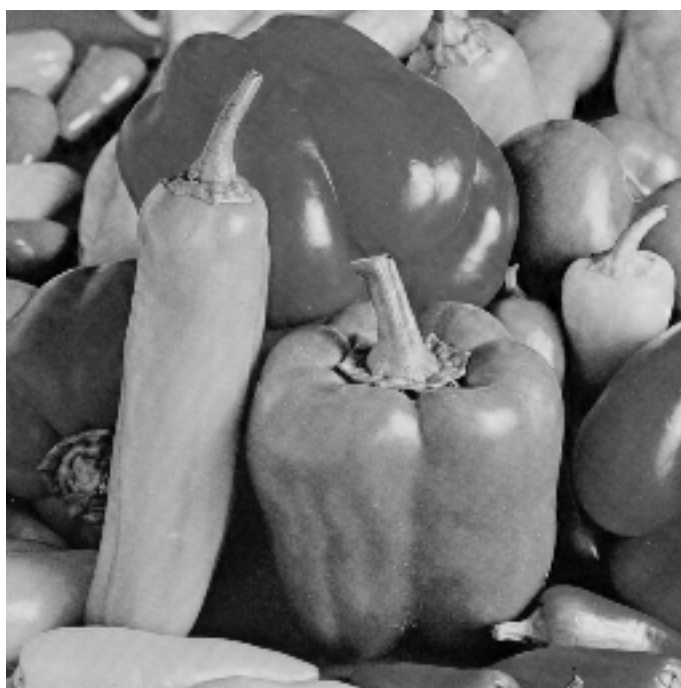


Fig. 4.23(b): Imagine marcată [NB05], pentru $\alpha = 0.2$, PSNR=40.28 dB

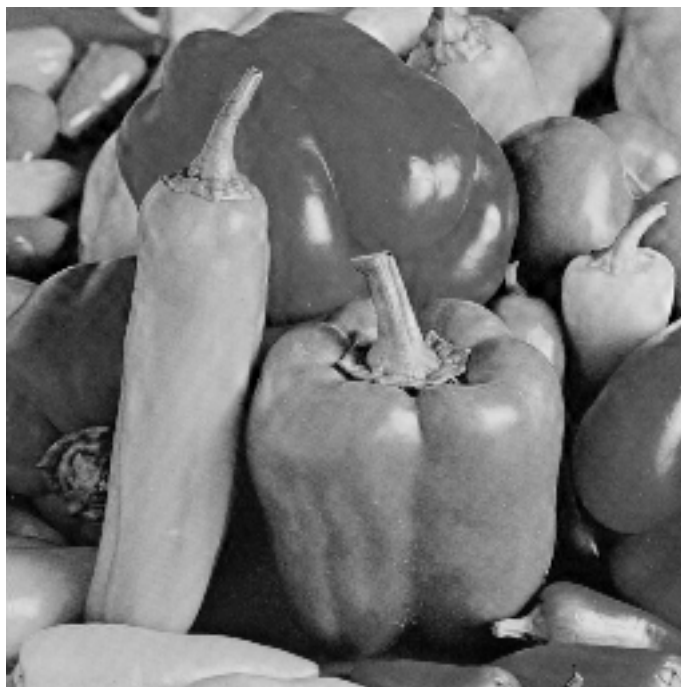


Fig. 4.23(c): Imagine marcată [NB05], pentru $\alpha = 0.3$, PSNR=36.94 dB



Fig. 4.24(a): Imagine marcată folosind metoda SS din [CKLS97], pentru $\beta=0.01$, PSNR=45.75 dB

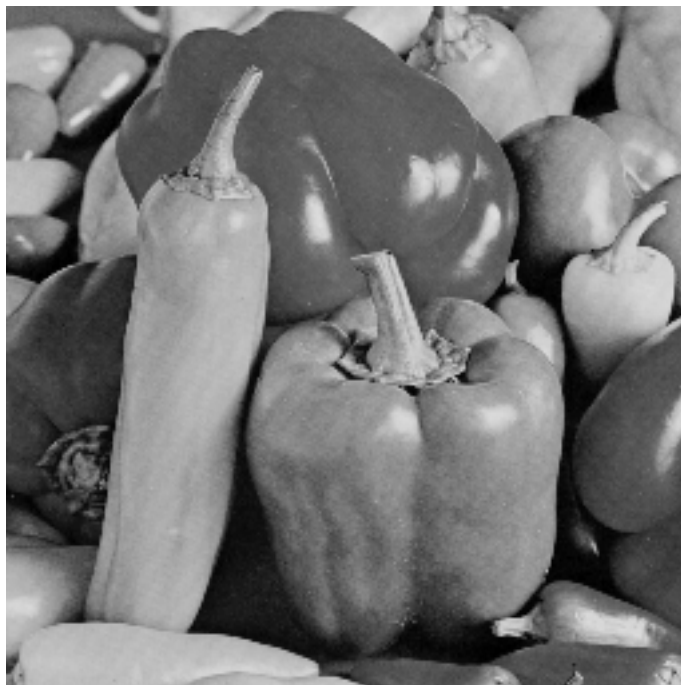


Fig. 4.24(b): Imagine marcată folosind metoda SS din [CKLS97], pentru $\beta=0.02$, PSNR = 39.73dB



Fig. 4.24(c): Imagine marcată folosind metoda SS din [CKLS97], pentru $\beta=0.03$, $PSNR = 36.21dB$

Pentru a demonstra robustețea noii metode [NB05], se investighează efectul distorsiunilor obișnuite asupra coeficientului de corelație între marcajul original și cel recuperat. Se compară performanțele acestei metode cu cele ale metodei propuse de Cox ș.a. [CKLS97]. Imaginile marcate au fost atacate prin filtrare mediană, compresie JPEG, zgomot aditiv alb Gaussian, AWGN, compresie JPEG2000, redimensionare, ajustarea contrastului, decupare. În Tabelele 4.3, 4.4 și 4.5 se prezintă răspunsul detectorului pentru cele două metode, atunci când imaginile marcate sunt distorsionate prin compresie cu pierderi (JPEG și JPEG2000) cu rate de compresie diferite, atac AWGN cu raportul semnal-pe-zgomot 11.4 dB, redimensionare la jumătate, filtrare mediană cu dimensiunea filtrului 3x3, ajustarea contrastului și decupare. Din valorile din tabele se observă că metoda propusă funcționează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepții, când oricum, marca nu este detectabilă în ambele cazuri (de exemplu, în Tabelul 4.3, $\alpha=0.1$ și $\beta=0.01$ la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe și nu detectează marca în prezența celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10, decupare, redimensionare, filtrare mediană, ajustarea contrastului, compresie JPEG2000 cu rata de compresie mai mare de 10).

În ceea ce privește rezultatele obținute cu metoda originală, detectorul 2 are performanțe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN. În cazul decupării, cele două tipuri de detectoare au aceleași rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru $\alpha = 0.3$. Răspunsurile detectoarelor, obținute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obținute pentru imaginile comprimate cu JPEG, evidențiindu-se astfel robustețea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α , cu atât sunt mai bune performanțele metodei [NB05]. Cu toate acestea există un *compromis între robustețe și invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la $\alpha=0.2$.

Tab. 4.3: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Metodă \ Atac	Metoda propusă [NB05], $\alpha=0.1$		Metoda Cox ș.a. $\beta=0.01$
	Detector 1	Detector 2	
JPEG, Q=75 (CR=5.5)	0.78	0.98	0.59
JPEG, Q=50 (CR=8.3)	0.50	0.92	0.35
JPEG, Q=25 (CR=12.8)	0.16	0.65	0.04
JPEG, Q=20 (CR=15)	0.09	0.54	0
Decupare, 1/2	0.30	0.34	0
AWGN, SNR=11.4dB	0.55	0.36	0.12
Redimensionare 256->128->256	0	0.14	0
Filtrare mediană, 3*3	0.02	0.60	0
Ajustarea contrastului	0	0.03	0
JPEG2000, CR = 5	0.96	0.89	0.47
JPEG2000, CR = 10	0.20	0.66	0.14
JPEG2000, CR = 15	0.03	0.43	0.03
JPEG2000, CR = 20	0	0.32	0
JPEG2000, CR = 25	0	0.27	0

Tab. 4.4: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Metodă \ Atac	Metoda propusă [NB05], $\alpha=0.2$		Metoda Cox ș.a., $\beta=0.02$
	detector 1	detector 2	
JPEG, Q=75 (CR=5.5)	0.97	0.99	0.89
JPEG, Q=50 (CR=8.3)	0.71	0.97	0.56
JPEG, Q=25 (CR=12.8)	0.32	0.80	0.11
JPEG, Q=20 (CR=15)	0.21	0.78	0.03
Decupare, 1/2	0.42	0.40	0.007
AWGN, SNR=11.4dB	0.86	0.78	0.38
Redimensionare 256->128->256	0.08	0.52	0
Filtrare mediană, 3*3	0.13	0.82	0
Ajustarea contrastului	0	0.22	0
JPEG2000, CR = 5	0.99	0.98	0.85
JPEG2000, CR = 10	0.56	0.93	0.24
JPEG2000, CR = 15	0.24	0.78	0.04
JPEG2000, CR = 20	0	0.59	0.01
JPEG2000, CR = 25	0	0.51	0

Tab. 4.5: Răspunsul detectorului pentru imagini marcate distorsionate [NB05]

Atac \ Metodă	Metoda propusă [NB05], $\alpha=0.3$		Metoda Cox et al., $\beta=0.03$
	detector 1	detector 2	
JPEG, Q=75 (CR=5.5)	0.99	1	0.99
JPEG, Q=50 (CR=8.3)	0.85	1	0.67
JPEG, Q=25 (CR=12.8)	0.40	0.89	0.18
JPEG, Q=20 (CR=15)	0.25	0.89	0.09
Decupare, 1/2	0.44	0.45	0
AWGN, SNR=11.4dB	0.89	0.78	0.39
Redimensionare 256->128->256	0.015	0.53	0
Filtrare mediană, 3*3	0.25	0.96	0
Ajustarea contrastului	1	0.95	0
JPEG2000, CR = 5	1	0.99	0.92
JPEG2000, CR = 10	0.67	0.97	0.34
JPEG2000, CR = 15	0.35	0.84	0.10
JPEG2000, CR = 20	0.12	0.71	0.01
JPEG2000, CR = 25	0.07	0.66	0

4.5 Detecție îmbunătățită prin metoda max-correlation

Al treilea detector extrage fiecare estimată, \hat{w}_r , a marcajului original, și calculează coeficientul de corelație dintre \hat{w}_r și w [Naf05b]. Marcajul pentru care se înregistrează valoarea maximă a corelației cu marcajul original se consideră rezultatul aplicării detectorului 3. Se face o comparație cu celelalte două detectoare, pentru cazul $\alpha = 0.2$, pentru diverse atacuri (Tabelul 4.6). Al treilea detector are performanțe mai bune față de primul, iar detectorul 2 are performanțe mai bune sau similare decât detectorul 3, cu excepția atacului prin decupare sau ajustare a contrastului.

Tab. 4.6: Comparație între cele trei detectoare pentru diverse atacuri [Naf05b]

Atac vs. răspunsul detectorului	Tip detecție		
	1	2	3
JPEG, CR = 14.85	0.21	0.78	0.69
Filtrare mediană, 3*3	0.13	0.82	0.81
Redimensionare, 256->128->256	0.03	0.45	0.31
AWGN, SNR = 11.4 dB	0.82	0.57	0.49
Decupare 1/2	0.42	0.44	0.64
Ajustarea contrastului	0	0.22	0.31
JPEG 2000, CR=10	0.56	0.93	0.85
JPEG 2000, CR=15	0.24	0.78	0.64

În Tabelul 4.7 se prezintă răspunsul celor trei tipuri de detectoare pentru atacul de coliziune, prin medierea a patru imagini marcate. Este evident că al treilea detector

este mai bun decât primele două, deoarece estimarea marcajului se face în funcție de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

Tab. 4. 7: Comparație între cele trei detectoare pentru atacul de coliziune (mediere a patru imagini marcate) [Naf05b]

Tip detecție vs. răspunsul detectorului	Marca originală			
	W ₁	W ₂	W ₃	W ₄
Tip 1	0.35	0.25	0.41	0.49
Tip 2	0.36	0.30	0.39	0.44
Tip 3, W = W ₁	0.47	0.35	0.30	0.38
Tip 3, W = W ₂	0.37	0.40	0.29	0.42
Tip 3, W = W ₃	0.39	0.30	0.42	0.38
Tip 3, W = W ₄	0.28	0.35	0.36	0.49

În Figurile 4.25-4.32 se prezintă valorile coeficienților de corelație pentru 1000 de marcaje generate aleator. Pentru majoritatea atacurilor (cu excepția celui de coliziune) numai marca numărul 500 ar trebui să fie pozitiv detectată. În cazul atacului de coliziune, ar trebui detectate marcajele cu numerele 200, 400, 600 și 800, deoarece acestea au fost mediate. De asemenea se dau valorile PSNR dintre imaginile marcate distorsionate și cele marcate nedistorsionate.

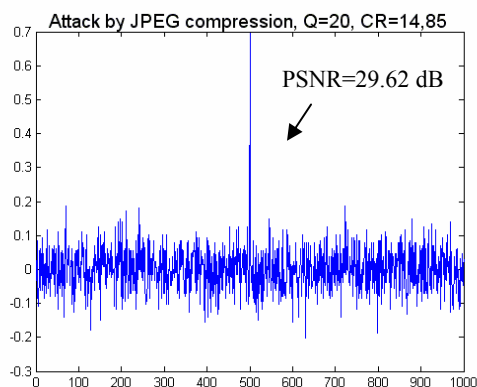


Fig. 4.25: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de compresie JPEG [Naf05b].

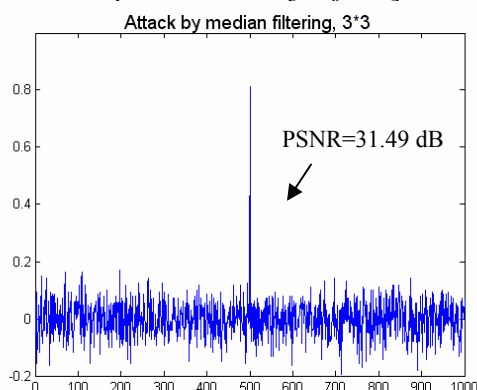


Fig. 4.26: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de filtrare mediană [Naf05b].

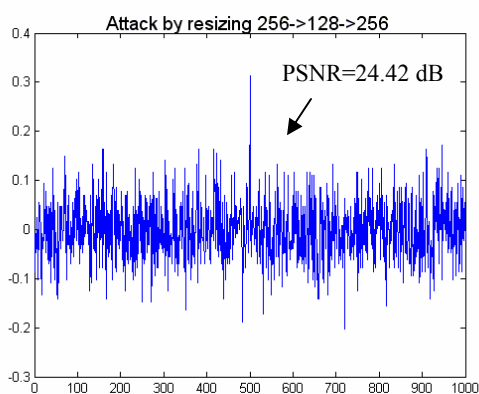


Fig. 4.27: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de redimensionare [Naf05b].

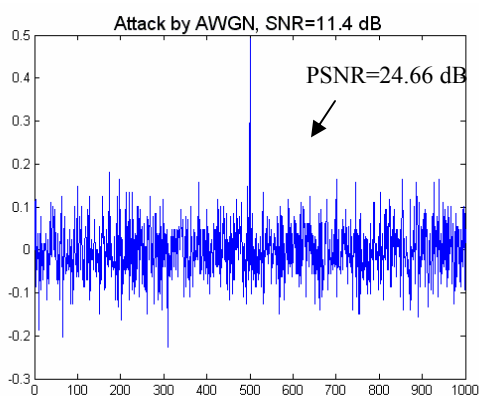


Fig. 4.28: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul AWGN [Naf05b].

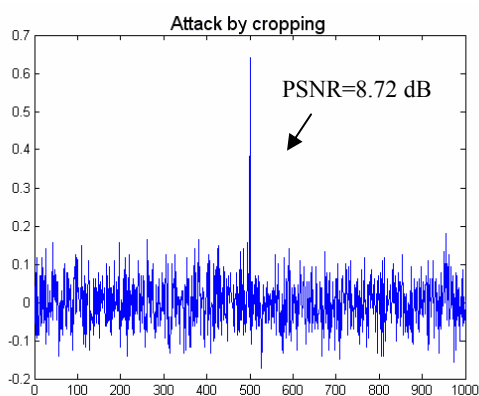


Fig. 4.29: Răspunsul detectorului 3 la 1000 marcaje generate aleator după atacul de decupare [Naf05b].

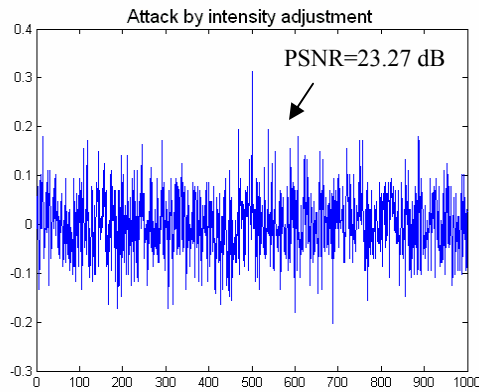


Fig. 4.30: Răspunsul detectorului 3 la 1000 marcaje generate aleator, după modificarea contrastului [Naf05b].

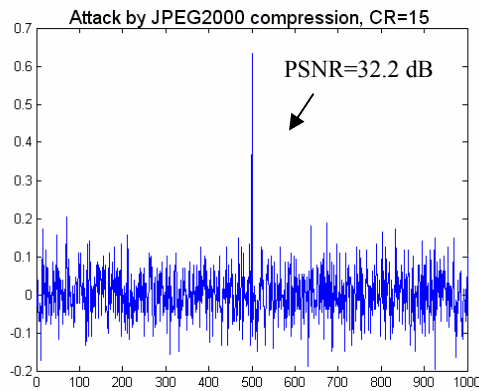


Fig. 4.31: Răspunsul detectorului 3 la 1000 marcaje generate aleator, după compresie JPEG 2000 [Naf05b].

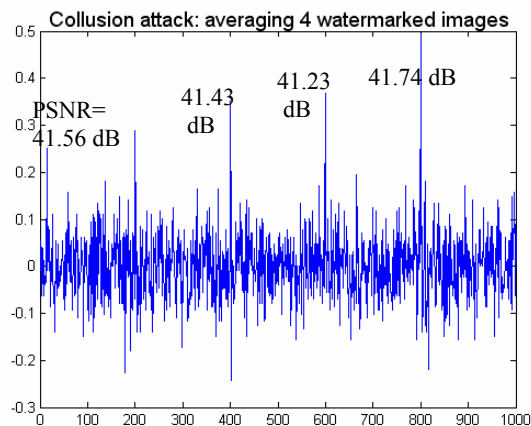


Fig. 4.32: Răspunsul detectorului 3 la 1000 marcaje generate aleator ($W_{orig}=W_4$), după coliziune [Naf05b].

4.6 A treia metodă de marcarea informată. O abordare statistică

La fel ca mai înainte, imaginea originală se descompune pe trei nivele de rezoluție, adică într-o imagine de aproximație $f_{a,3}$ și câte trei imagini de detaliu pentru fiecare nivel de rezoluție. Operația definită de \oplus din relația (4.4) este de această dată:

$$f_{s,l}^w(m,n) = f_{s,l}(m,n) + \alpha \cdot |f_{s,l}(m,n)| w(m,n) \quad (4.12)$$

unde $s \in \{h, v, d\}$, $l = 1, \dots, L$ iar α este o variabilă definită de utilizator, astfel încât $\alpha \in (0,1)$. Prin urmare, operația definită de \ominus din relația (4.5) este în acest caz:

$$\hat{w}(m,n) = \frac{r_{s,l}(m,n) - f_{s,l}(m,n)}{\alpha \cdot |f_{s,l}(m,n)|} \quad (4.13)$$

Dacă $r_{s,l}(m,n) = f_{s,l}(m,n)$ și/sau dacă $f_{s,l}(m,n) = 0$, se face o alegere aleatoare pentru $w(m,n)$.

Generarea cheii se face pentru trei nivele de rezoluție, cu relația (4.1b), folosind caracteristici statistice ale coeficienților wavelet [NIB05]. Pragurile $T_{s,l}$ sunt definite după cum urmează:

$$T_{s,l} = m_{s,l} \sigma_{s,l} \quad (4.14)$$

unde $\sigma_{s,l}$ reprezintă abaterea standard a coeficienților wavelet pentru subbanda s , din nivelul de rezoluție l , iar parametrii $m_{s,l}$ sunt selectați pe baza unei *analize statistice* a transformatei DWT [IML05].

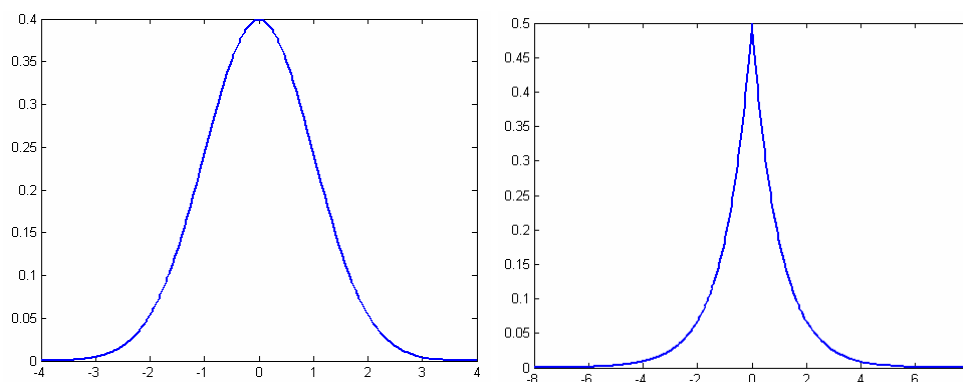


Fig. 4.33: Distribuția normală, respectiv distribuția Laplace folosită pentru modelarea caracteristicilor statistice ale coeficienților wavelet.

Funcția de densitate de probabilitate, pdf, a coeficienților de detaliu wavelet scade mai repede decât pdf gaussiană (fiind o distribuție "heavy tailed"), de aceea am ales ca model de repartiție a coeficienților de detaliu distribuția Laplace [SS02], reprezentată în Figura 4.33 :

$$f_{f_{s,l}}(y) = \frac{1}{2\sqrt{2}\sigma_{s,l}} \cdot \exp\left(-\frac{|y|}{\sqrt{2}\sigma_{s,l}}\right) \quad (4.15)$$

Probabilitatea de a selecta un coeficient wavelet de detaliu cu valoarea absolută mai mare decât pragul $T_{s,l}$ este dată de:

$$P_{T_{s,l}} = P\left(|f_{s,l}| > T_{s,l}\right) = 2 \cdot \exp\left(-\frac{T_{s,l}}{\sqrt{2}\sigma_{s,l}}\right) - 1 \quad (4.16)$$

Astfel, pragurile pot fi calculate după cum urmează:

$$T_{s,l} = \sqrt{2} \cdot \sigma_{s,l} \cdot \ln\left(\frac{2}{P_{T_{s,l}} + 1}\right) \quad (4.17)$$

Dacă se alege $P_{T_{s,l}} = 0,5$ și dacă se ține seama de relația dată în [IML05]:

$$\sigma_{s,l}^2 = 2^{2l-2} \cdot \sigma_{s,1}^2, \quad (4.18)$$

valorile de prag devin [NIB05]:

$$T_{s,l} = 0.2 \cdot 2^l \cdot \sigma_{s,1} \quad (4.19a)$$

Deci jumătate din coeficienții wavelet de detaliu $f_{s,l}$ dintr-o anumită subbandă și nivel de rezoluție (s,l) sunt mai mari în valoare absolută decât pragurile $T_{s,l}$.

Dupa experimente s-a constatat că inserarea marcajului în mai puțini coeficienți duce la o robustețe crescută; astfel am folosit următoarele praguri:

$$T_{s,l} = 2^l \cdot \sigma_{s,1} \quad (4.19b)$$

Pe de altă parte, fiindcă se cere inserarea aceluiași marcaj original de mai multe ori, este nevoie de mai mulți coeficienți în fiecare subbandă (măcar N_w coeficienți sau cu alte cuvinte, cel puțin o repetiție a marcajului, mai ales pentru valori mari ale lui l). De aceea selecția pragurilor se face adaptiv, cu inițializarea la valorile indicate în relația (4.17b). La fiecare iterație, valorile pragurilor descresc:

$$\begin{aligned}
 T_{s,l}(0) &= T_{s,l} \\
 T_{s,l}(p) &= T_{s,l}(p-1) - 0.25
 \end{aligned}
 \tag{4.18}$$

până când este satisfăcută condiția ca măcar un marcaj să fie inserat într-o subbandă.

S-au efectuat simulări [NIB05] folosind tot imaginea Peppers, 256 x 256, și o marcă de 256 de biți. De asemenea, s-a folosit funcția mother wavelet Daubechies 5 pentru a produce coeficienții wavelet, cu un număr de nivele de rezoluție $L = 3$.

Intensitatea de marcarea a fost fixată la $\alpha = 0.1$. Prin alegerea noilor praguri, s-au afectat numai 2816 coeficienți din 65536, astfel că numărul de repetiții al marcajului original este în final $M=11$. Imaginea nu este afectată de procesul de marcarea care este transparent, valoarea PSNR fiind în acest caz de 44.95 dB.

Din nou se analizează robustețea metodei la aceleași tipuri de atacuri, și se face o comparație cu metoda propusă de Cox ș.a. [CKLS97]. De data aceasta, marcajul binar de 256 de biți este înserat o singură dată în coeficienții DCT cei mai mari, așa cum am descris mai sus.

În Tabelul 4.8 este prezentat răspunsul detectorului pentru cele două metode comparate, atunci când imaginea marcată este atacată prin compresie cu pierderi JPEG, cu factor de calitate 75, 50, 25, 20 și JPEG2000, cu rata de compresie 5, 10 și 15, cu AWGN cu raportul semnal-pe-zgomot $SNR = 11.4$ dB, prin redimensionare la jumătate, prin filtrare mediană cu dimensiunea filtrului 3 și 5, prin ajustarea contrastului și prin decupare. Din valorile din tabel de observă că metoda este mai performantă decât cea din [CKLS97] pentru toate atacurile.

Tab. 4.8: Comparație între metoda propusă în [NIB05] și metoda lui Cox [CKLS97].

Atac vs. Răspunsul detectorului	Metoda propusă [NIB05]			Metoda Cox et al.
	Detector 1	Detector 2	Detector 3	
JPEG, Q=75	0.9688	1	0.9922	0.8984
JPEG, Q=50	0.8281	0.9531	0.9063	0.7031
JPEG, Q=25	0.4219	0.7813	0.6875	0.4531
JPEG, Q=20	0.3281	0.6797	0.6641	0.3047
Filtrare mediană, 3*3	0.2891	0.7500	0.7734	0.4375
Filtrare mediană, 5*5	0.0234	0.2344	0.3672	0.1563
Redimensionare, 256->128->256	0.0703	0.2422	0.2422	0.0469
AWGN, SNR = 11.4 dB	0.6484	0.6094	0.5469	0.2734
Decupare $\frac{1}{2}$	0.4219	0.3906	0.5703	-0.0156
Ajustarea contrastului	0.0234	0.0859	0.1641	0.0547
JPEG 2000, CR=15	0.5859	0.6563	0.6016	0.4844
JPEG 2000, CR=10	0.9766	0.8984	0.7891	0.6484
JPEG 2000, CR=5	1	0.9922	0.9922	0.8750

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare și ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN și la compresia JPEG2000.

Detectorul 3 are performanțe mai bune decât detectorul 1, în cazul majorității atacurilor, și performanțe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, și a ajustării contrastului.

În Tabelul 4.9 se prezintă răspunsurile detectoarelor 1 și 2 pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite. Se observă că toate cele 4 marcaje sunt detectate.

Figura 4.34 arată imaginea marcată, folosind metoda propusă, marcajul ca imagine diferență. precum și cheia de marcarea care indică coeficienții selectați pentru fiecare subbandă. Evident, aceștia se concentrează mai ales în zona conturilor și a texturilor, (deoarece au fost selecționați coeficienții de detaliu cu cele mai mari valori), ceea ce face marcajul imperceptibil.

Tab. 4.9: Rezultate pentru atacul de coliziune, prin medierea a patru imagini marcate [NIB05]

Tip de detecție	Marca originală			
	W ₁	W ₂	W ₃	W ₄
Tip 1	0.37	0.34	0.39	0.40
Tip 2	0.38	0.36	0.39	0.36



Fig.4.34(a): Imaginea marcată, PSNR=44.95 dB [NIB05]

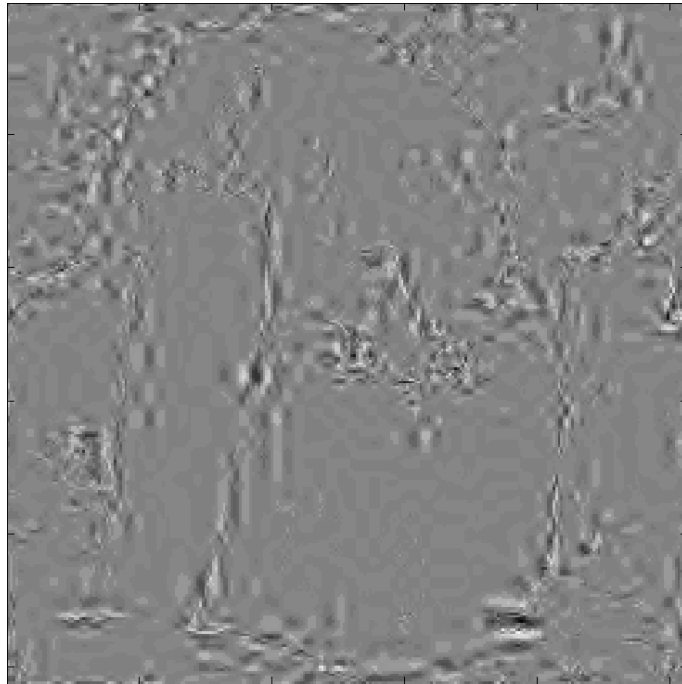


Fig. 4.34(b): Marcaj ca diferență între imaginea originală Peppers și cea din Figura 4. 34(a). Se observă că marcajul este concentrat în jurul conturilor și texturilor [NIB05].

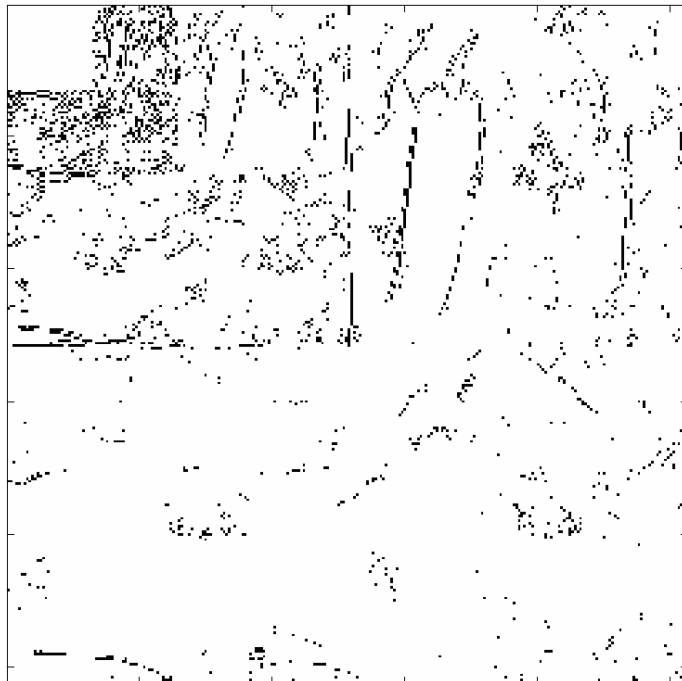


Fig.4.34(c): Cheia de marcarea K, care indică coeficienții selectați din fiecare subbandă pentru imaginea originală Peppers [NIB05].

4.7 Concluzii

S-au prezentat trei metode de marcarea informată [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. Metodele se bazează pe descompunerea multirezoluție a imaginii cu transformata wavelet discretă. Se fac schimbări asupra unor coeficienți wavelet, care nu vor avea un impact vizual asupra unui observator uman.

Coeficienții au fost selectați folosind o detecție cu logică de prag [NI03, NBK04, Naf04b, NB05, Naf05b]. Pragul depinde de coeficienții wavelet ai fiecărei imagini de detaliu. Marcajul este înserat în texturi și muchii ale imaginii folosind sistemul vizual uman.

Prima metodă [NI03] înserează și detectează marcajul în/din subbanda de detalii diagonale al primului nivel de rezoluție, respectiv în toate subbenzile primului nivel; evident, deși a doua abordare afectează mai mult imaginea, marcajul se dovedește a fi mai robust la prelucrări obișnuite de semnal (compresie JPEG, filtrare mediana, zgomot AWGN). Metoda este comparată cu cea din [KH98]. Coeficientul de intercorelație pentru metoda propusă este mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG și zgomot alb gaussian aditiv. Cu toate acestea, metoda propusă nu prezintă robustețe împotriva filtrării mediane, comparativ cu metoda din [KH98].

A doua metodă înserează marcajul în cele trei nivele de rezoluție, exceptând imaginea de aproximare, folosind același mod de selecție a coeficienților wavelet. Detecția se face din **(1)** toate nivele mediat, prin decizie majoritară, sau **(2)** din ultimul nivel de rezoluție, mai puțin afectat de diverse prelucrări de semnal.

Un **set preliminar de experimente** [Naf04a] face o comparație a metodei cu metoda de tip cuantizare prezentată în [KH98], se dovedește că metoda mea este mai robustă. Se observă că performanțele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelație este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluție. Acest lucru se datorește faptului că distorsiunile obișnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un al doilea set de experimente a fost efectuat folosind patru imagini; s-a făcut o comparație a metodei propuse [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox și alții este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, și inferioară pentru filtrarea mediană. Aceste teste au fost efectuate pentru imagini marcate puternic în cazul metodei [CKLS97].

Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcarea mai mică astfel încât imaginile să nu fie vizibil afectate de procesul de marcarea pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensități și apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG și JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului și decupare. Metoda propusă funcționează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepții, când, oricum, marca nu este detectabilă în ambele cazuri

(de exemplu, pentru, $\alpha=0.1$ și $\beta=0.01$ la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe și nu detectează marca în prezența celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10; decupare; redimensionare; filtrare mediană; ajustarea contrastului; compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanțe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleași rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru $\alpha=0.3$.

Răspunsurile detectoarelor, obținute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obținute pentru imaginile comprimate cu JPEG, evidențiindu-se astfel robustețea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α , cu atât sunt mai bune performanțele metodei [NB05]. Cu toate acestea există un *compromis între robustețe și invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la valoarea $\alpha=0.2$.

S-au analizat **trei tipuri de detectoare** [NB05, Naf05b], care pot da rezultate diferite în funcție de atacul la care a fost supusă imaginea:

- din toate nivelele de rezoluție, prin mediere, respectiv,
- din ultimul nivel de rezoluție al transformatei, care poate fi afectat mai puțin de distorsiuni obișnuite ale semnalului,
- prin **corelație maximă** cu marcajul căutat [Naf05b].

Este evident că al treilea detector este mai bun decât primele două, deoarece estimarea marcajului se face în funcție de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

A treia metodă de marcare informată propune o **abordare statistică** [NIB05], unde se selectează *mai puțini coeficienți wavelet* în care se înserează marcajul, deci numărul de repetiții este mai mic, față de metoda 2. Răspunsul detectorului este mai bun față de metoda a doua, deoarece coeficienții mari nu sunt atât de afectați de atacurile obișnuite (compresie, filtrare, etc.). Selecția pragurilor este bazată pe proprietățile statistice ale coeficienților wavelet. Detectoarele sunt la fel cu cele menționate anterior.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare și ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN și la compresia JPEG2000.

Detectorul 3 are performanțe mai bune decât detectorul 1, în cazul majorității atacurilor, și performanțe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, și a ajustării contrastului. Pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 și 2, toate cele 4 marcaje sunt detectate.

Performanțele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox și alții în [CKLS97] respectiv cu metoda propusă de Kundur și Hatzinakos [KH98]. Metoda a demonstrat o performanță mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT și a analizei statistice a coeficienților wavelet.

Capitolul 5.

Aplicarea transformării wavelet în marcarea perceptuală neinformată a imaginilor

5.1 Introducere

Se studiază o metodă de marcarea perceptuală [BBP01], care operează în domeniul wavelet. Aceasta se bazează pe tehnica de tip *spread spectrum* propusă de Cox ș.a. [CKLS97]. Detecția nu folosește semnalul original, deci sistemul este public.

Masca perceptuală ține cont de sensibilitatea la zgomot, textura și luminața tuturor subbenzilor. Prezentăm o mască perceptuală îmbunătățită, unde conținutul texturii este estimat folosind deviația standard locală a imaginii originale, comprimată în domeniul DWT, pentru a avea aceeași mărime ca și marcajul de inserat. Eficiența noii măști este comparată cu cea propusă de Barni ș.a. [BBP01].

Capitolul de față are următoarea structură. În paragraful 5.2 se explică și se exemplifică conceptul de marcarea perceptuală. Scopul paragrafului 5.3 este descrierea metodei din [BBP01]. În paragrafele 5.4 și 5.5 se prezintă construcția noii măști, [NIB06a], precum și rezultate obținute în urma simulărilor. Următorul paragraf prezintă o mască perceptuală și mai generală, propusă în [NIB06b], care permite ascunderea datelor și în subbenzile de frecvență mai joasă, ceea ce duce la o robustețe crescută. Concluziile sunt enunțate în ultimul paragraf.

5.2 Marcarea perceptuală

O cerință impusă unui sistem de marcarea este imperceptibilitatea. Aceasta se poate îndeplini utilizând diverse metode.

O metodă este folosirea caracteristicilor statistice ale coeficienților wavelet a imaginii originale. Variația coeficienților wavelet poate fi estimată la orice nivel de rezoluție, și se pot detecta, folosind această estimare, coeficienții cu valoare absolută mare, cu ajutorul unui detector de prag. Dacă se inserează marcajul în acești coeficienți, corespunzând primelor trei nivele de rezoluție, se obține un marcaj robust. Robustețea este proporțională cu valoarea pragului. Aceasta soluție a fost propusă în [NIB05], unde robustețea este crescută prin inserări multiple ale marcajului în subbenzile respective. Toți biții marcajului sunt inserați cu aceeași intensitate. Coeficienții cu valoare absolută mare corespund contururilor, coeficienții cu valoare absolută medie corespund texturilor, iar cei cu valoare absolută mică corespund zonelor omogene din imaginea originală. Totuși, această tehnică are dezavantaje: este dificil de inserat întregul mesaj în contururi, în special când mesajul este lung, deoarece numai o parte din pixeli se află pe contururile imaginii originale. Pentru mesaje mai lungi (care produc o încărcătură mai mare), valoarea pragurilor trebuie scăzută, ajungându-se astfel ca marcajul să fie inserat și în texturile imaginii originale. Se poate spune deci că metoda enunțată folosește o mascare perceptuală. Dar analiza robusteții acestei metode nu este deloc simplă, în special când numărul de repetiții ale marcajului este mare. Robustețea se îmbunătățește cu creșterea numărului de repetiții,

dar descrește odată cu scăderea pragurilor. De fapt, există unii coeficienți care nici nu sunt folosiți pentru inserare. Acesta este motivul pentru care în [BBP01] este propusă o abordare diferită pentru înglobarea marcajului. Se preferă să se insereze marcajul în toți coeficienții wavelet de detaliu dar se folosesc intensități diferite. Pentru coeficienții din contururi se folosește o intensitate mai mare, pentru coeficienții corespunzători texturilor se folosește o intensitate medie, iar pentru cei corespunzători zonelor omogene se folosește o intensitate mică. Aceasta este în concordanță cu analogia între *water-filling* și *watermarking* propusă de Deepa Kundur în [Kun00].

5.3 Marcarea perceptuală propusă de Barni, Bartolini și Piva

În continuare se prezintă mai întâi soluția propusă în [BBP01] de Barni, Bartolini și Piva.

A. Însurarea marcajului

Imaginea I , de marime $2M \times 2N$ este descompusă pe 4 nivele de rezoluție, folosind transformata wavelet discretă, Daubechies-6, unde I_l^θ este subbanda din nivelul $l \in \{0,1,2,3\}$ și orientarea $\theta \in \{0,1,2,3\}$. Un marcaj binar $x_l^\theta(i, j)$ de lungime $3MN/2^l$ este inserat în toți coeficienții subbenzilor de detaliu de la nivelul $l=0$ (de frecvență înaltă/rezoluție mare), prin adunare :

$$\tilde{I}_l^\theta(i, j) = I_l^\theta(i, j) + \alpha w_l^\theta(i, j) x_l^\theta(i, j) \quad (5.1)$$

unde α este intensitatea de marcare iar $w_l^\theta(i, j)$ este o funcție de ponderare, a cărei valoare este egală cu jumătate din pasul de cuantizare, $q_l^\theta(i, j)$. Pasul de cuantizare este calculat în [BBP01] ca produsul ponderat a trei factori:

$$q_l^\theta(i, j) = \Theta(l, \theta) \Lambda(l, i, j) \Xi(l, i, j)^{0.2} \quad (5.2)$$

iar însurarea are loc doar în primul nivel de descompunere, $l=0$ (frecvență înaltă).

Primul factor reprezintă sensibilitatea la zgomot, depinzând de orientare și de nivelul de rezoluție:

$$\Theta(l, \theta) = \begin{cases} \sqrt{2}, & \theta = 1 \\ 1, & \text{altfel} \end{cases} \cdot \begin{cases} 1.00, & l = 0 \\ 0.32, & l = 1 \\ 0.16, & l = 2 \\ 0.10, & l = 3 \end{cases} \quad (5.3)$$

Al doilea factor ține cont de luminozitatea locală, bazată pe nivelele de gri ale versiunii trece-jos a imaginii (adică sub-imaginea de aproximare de nivel 4 obținută în urma calculului transformării wavelet):

$$\Lambda(l, i, j) = 1 + L'(l, i, j) \quad (5.4)$$

unde:

$$L'(l, i, j) = \begin{cases} 1 - L(l, i, j), & L(l, i, j) < 0.5 \\ L(l, i, j), & \text{altfel} \end{cases} \quad (5.5)$$

și

$$L(l, i, j) = \frac{1}{256} I_3^3 \left(1 + \left\lfloor \frac{i}{2^{3-l}} \right\rfloor, 1 + \left\lfloor \frac{j}{2^{3-l}} \right\rfloor \right)$$

Al treilea factor este calculat după cum urmează:

$$\begin{aligned} \Xi(l, i, j) &= \sum_{k=0}^{3-l} \frac{1}{16^k} \sum_{\theta=0}^2 \sum_{x=0}^1 \sum_{y=0}^1 \left[I_{k+l}^{\theta} \left(y + \frac{i}{2^k}, x + \frac{j}{2^k} \right) \right]^2 \\ &\cdot \text{Var} \left\{ I_3^3 \left(1 + y + \frac{i}{2^{3-l}}, 1 + x + \frac{j}{2^{3-l}} \right) \right\}_{\substack{x=0,1 \\ y=0,1}} \end{aligned} \quad (5.6)$$

Acesta reprezintă textura în vecinătatea unui pixel. El este compus din produsul a doi factori, primul fiind media locală pătratică a coeficienților wavelet din toate subimaginele de detaliu, în timp ce al doilea este dispersia locală a subbenzii de aproximare. Ambii factori sunt calculați într-o fereastră de 2×2 corespunzând pixelului localizat în (i, j) . Primul factor poate reprezenta distanța față de muchii în timp ce al doilea factor, textura.

Această estimare a dispersiei locale nu este prea de precisă, deoarece este calculată cu o rezoluție joasă.

De aceea se prezintă o nouă metodă de estimare a texturii, dar și a luminanței [NIB06a, NIB06b].

B. Detecția marcajului

Detecția se face folosind coeficientul de corelație între coeficienții wavelet marcați și biții de marcaj:

$$\rho_l = \frac{4^l}{3MN} \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \tilde{I}_l^{\theta}(i, j) x_l^{\theta}(i, j) \quad (5.7)$$

Corelația este comparată cu pragul T_l , calculat astfel încât probabilitatea de fals pozitiv să aibă o anumită valoare, folosind criteriul Neyman-Pearson. De exemplu, dacă $P_f \leq 10^{-8}$, pragul este $T_l = 3.97 \sqrt{2\sigma_{\rho_l}^2}$, unde $\sigma_{\rho_l}^2$ este dispersia coeficienților wavelet, dacă imaginea a fost marcată cu un marcaj Y altul decât X:

$$\sigma_{\rho_l}^2 \approx \frac{16^l}{(3MN)^2} \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \left(\tilde{I}_l^\theta(i,j) \right)^2. \quad (5.8)$$

5.4 Masca perceptuală îmbunătățită

Un alt mod de a genera al treilea factor din pasul de cuantizare, este prin segmentarea imaginii originale, găsindu-i contururile, texturile și regiunile omogene, așa după cum se poate observa în Figurile 5.1-5.6.

Criteriul folosit pentru această segmentare este valoarea deviației standard locale a fiecărui pixel din imaginea originală [NIB06a]. Într-o fereastră glisantă pătratică $W(i,j)$, conținând $W_S \cdot W_S$ pixeli, centrată pe fiecare pixel $I(m,n)$ din imaginea gazdă, media locală este calculată cu:

$$\hat{\mu}(i,j) = \frac{1}{W_S \cdot W_S} \sum_{I(m,n) \in W(i,j)} I(m,n) \quad (5.9)$$

iar dispersia locală este:

$$\hat{\sigma}^2(i,j) = \frac{1}{W_S \cdot W_S} \sum_{I(m,n) \in W(i,j)} \left(I(m,n) - \hat{\mu}(i,j) \right)^2 \quad (5.10)$$

Deviația standard locală estimată este radical din dispersia locală.



Fig. 5.1: Barbara

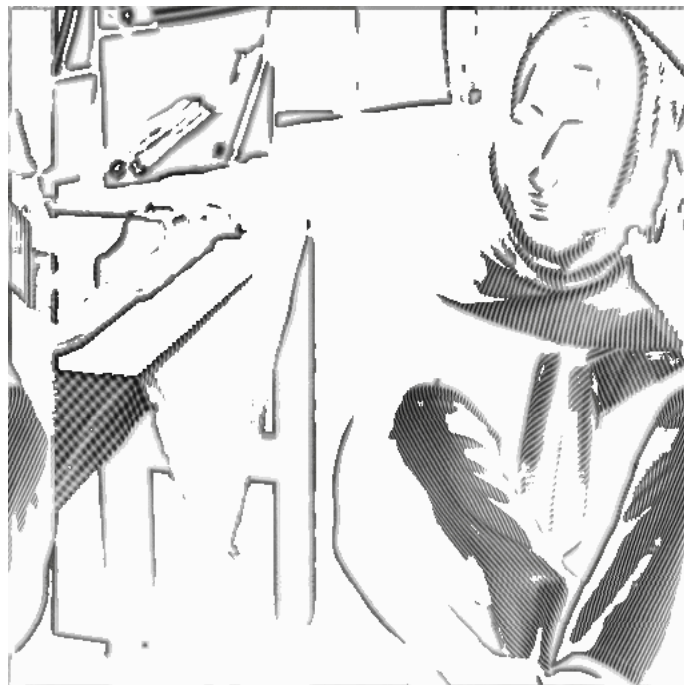
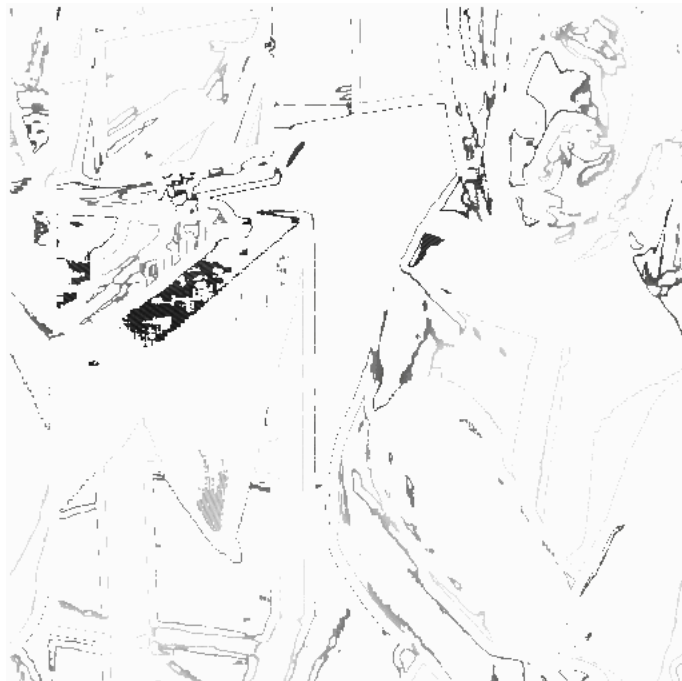


Fig. 5.2: Clasa corespunzătoare intervalului I_6 conține contururi și texturi grosiere [NIB06a]. Imaginea este complementara imaginii reale, adică zonele nesemnificative sunt reprezentate cu alb.



*Fig. 5.3: Clasa corespunzătoare intervalului I_5 conține contururi și texturi [NIB06a].
Imaginea este complementara imaginii reale, adică zonele ne semnificative sunt reprezentate cu alb.*



*Fig. 5.4: Clasa corespunzătoare intervalului I_4 conține texturi [NIB06a].
Imaginea este complementara imaginii reale, adică zonele ne semnificative sunt reprezentate cu alb.*



*Fig. 5.5: Clasa corespunzătoare intervalului I_3 conține texturi [NIB06a].
Imaginea este complementara imaginii reale, adică zonele ne semnificative sunt reprezentate cu alb.*



*Fig. 5.6: Clasa corespunzătoare intervalului I_2 conține texturi [NIB06a].
Imaginea este complementara imaginii reale, adică zonele ne semnificative sunt reprezentate cu alb.*



Fig. 5.7: Clasa corespunzătoare intervalului I_1 conține zone omogene [NIB06a]. Imaginea este complementara imaginii reale, adică zonele ne semnificative sunt reprezentate cu alb.

De exemplu, imaginea Barbara (Figura 5.1) poate fi segmentată în clase a căror elemente au ca valoare deviația standard normalizată [NIB06a], aparținând unor intervale posibile $I_p = (\alpha_p, \alpha_{p+1})$, unde p ia valorile $1, \dots, 6$, iar $\alpha_1=0, \alpha_2=0.025, \alpha_3=0.05, \alpha_4=0.075, \alpha_5=0.1, \alpha_6=0.25, \alpha_7=1$ (Fig. 5.2-5.7).

Această imagine a fost aleasă pentru conținutul bogat în contururi, texturi, dar și zone omogene. În fiecare din Figurile 5.2-5.7 este reprezentată clasa corespunzând intervalului $I_p, p = 1, \dots, 6$, celelalte elemente fiind ignorate (reprezentate cu alb). Trebuie menționat că nivelele de gri reprezintă contururi și texturi iar culoarea albă reprezintă zonele ne semnificative.

Aceste imagini demonstrează calitatea bună a segmentării bazate pe valorile deviației locale standard. Astfel de imagini pot fi folosite pentru mascarea perceptuală în procesul de inserare a marcajului. Pasul de cuantizare pentru un coeficient wavelet este dat de o valoare direct proporțională cu deviația standard locală corespunzătoare pixelului din imaginea originală.

Pentru a asigura o mascare perceptuală, dimensiunile diferitelor subimagini de detalii trebuie să fie egale cu dimensiunile măștilor corespunzătoare. De aceea, imaginea de deviație standard locală este comprimată. Factorul de compresie cerut pentru o mască corespunzătoare nivelului de rezoluție l este $4(l+1)$, pentru $l = 0, \dots, 3$. Această compresie poate fi realizată în domeniul DWT.

Pentru generarea măștii folosite la inserarea marcajului în nivelul de rezoluție l , se calculează transformata wavelet discretă a imaginii de deviație standard locală, făcând $l + 1$ iterații. Imaginea de aproximare obținută reprezintă rezultatul compresiei, sau cu alte cuvinte, masca cerută. Acest tip de compresie este ilustrat în Figura 5.8.



*Fig. 5.8(a): Deviația standard locală a imaginii Barbara.
Imaginea este complementara imaginii reale.*



*Fig. 5.8(b): Deviația standard locală a imaginii Barbara, comprimată cu CR = 4.
Imaginea este complementara imaginii reale.*



*Fig. 5.8(c): Deviația standard locală a imaginii Barbara, comprimată cu CR=16.
Imaginea este complementara imaginii reale.*

Diferența principală între sistemul de marcarea propus în [BBP01] și sistemul prezentat în [NIB06a], este dată de calculul dispersiei locale – al doilea factor – în

relația (5.6). Pentru a obține noile valori ale texturii, varianța locală a imaginii este calculată, folosind relațiile (5.9)-(5.10), cu dimensiunea ferestrei glisante $W_s = 7$.

Deviația standard locală este descompusă în domeniul wavelet și este păstrată doar imaginea de aproximare a acesteia, normată cu media ei. Pentru obținerea texturii este prezentată în Figura 5.9 o schemă generală.

Relația (5.6) este înlocuită cu:

$$\Xi(l, i, j) = \sum_{k=0}^{3-l} \frac{1}{16^k} \sum_{\theta=0}^2 \sum_{x=0}^1 \sum_{y=0}^1 \left[I_{k+l}^{\theta} \left(y + \frac{i}{2^k}, x + \frac{j}{2^k} \right) \right]^2 \cdot \text{DWT}_l^3 \left\{ \text{Std}(I)_{x,y=0,7} \right\} \quad (5.11)$$

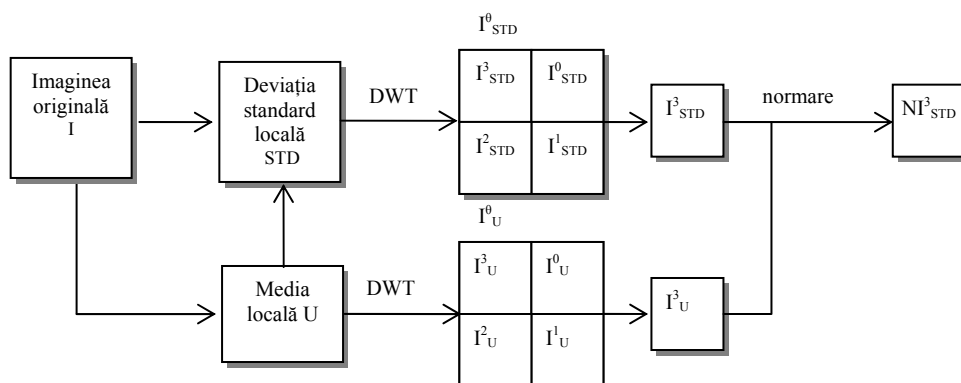


Fig. 5.9: O schemă generală pentru obținerea texturii [NIB06a].

5.5 Testarea noii măști perceptuale

Marcajul binar este înglobat în toate subimaginele de detaliu de la primul nivel de rezoluție wavelet, folosind relațiile (5.1)-(5.5). Imaginea Barbara a fost marcată cu diferite intensități de marcăre α , între 0.1 și 1.5.

Imaginea Barbara marcată pentru $\alpha=1.5$ este prezentată în Figura 5.10. După cum se observă, nu există o diferență perceptibilă între imaginea originală și cea marcată, valoarea raportului PSNR pentru această a doua imagine fiind de 45 dB.

Fiecare imagine marcată este comprimată JPEG folosind diverși factori de calitate 5, 10, 15, 20, 25, 50.

Pentru a testa performanța algoritmului, se prezintă în Figurile 5.11-5.14 rezultatele pentru compresie JPEG.

În Figurile 5.11 și 5.12 se arată numai raportul ρ/T , ca funcție de PSNR între imaginea marcată (neatacată) și cea originală, respectiv ca funcție de α . Pentru fiecare PSNR și fiecare factor de calitate Q , sunt calculate corelația ρ și pragul T . Probabilitatea de fals pozitiv este 10^{-8} .

Eficiența sistemului de marcăre propus poate fi măsurată folosind raportul ρ/T . Dacă $\rho/T > 1$, marcajul este detectat.



Fig. 5.10: Imaginea Barbara marcată cu $\alpha = 1.5$, folosind metoda din [NIB06a].

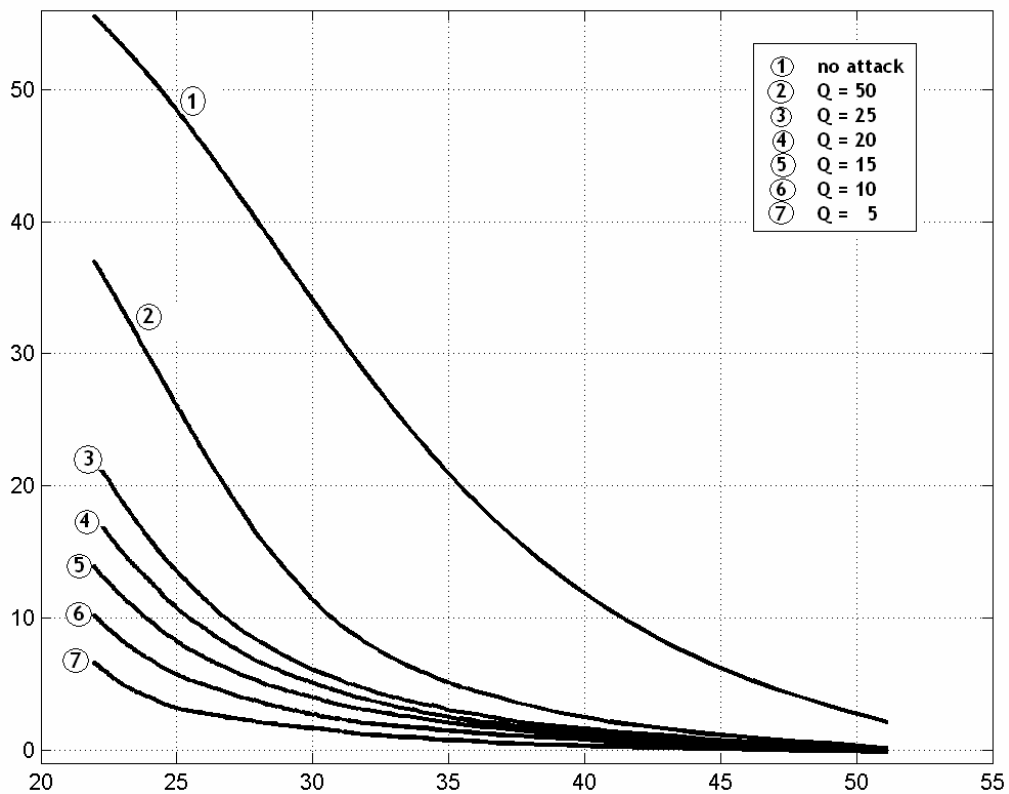


Fig. 5.11: Raportul ρ/T ca funcție de valorile PSNR dintre imaginile marcate și originală, pentru compresie JPEG, la diverși factori de calitate. P_f este 10^{-8} [NIB06a].

Analizând Figura 5.11, se observă că marcajul poate fi detectat pentru un interval mare de valori PSNR, și de factori de calitate Q . Pentru valori PSNR mai mari decât 30 dB, marcajul este invizibil. Pentru factori $Q \geq 25$, distorsiunea introdusă de compresia JPEG este tolerabilă.

Pentru valorile PSNR de la 30 dB la 35 dB, valori de interes practic, marcajul poate fi extras pentru toate valorile semnificative ale factorilor de calitate ($Q \geq 25$). De aceea, sistemul propus este viabil.

Figura 5.12 arată dependența raportului ρ/T funcție de puterea de marcarea, α , în cazul compresiei JPEG. Dacă puterea de marcarea crește, valorile PSNR ale imaginilor marcate descresc, iar raportul ρ/T crește.

Raportul ρ/T variază invers proporțional cu α , direct proporțional cu PSNR, și invers proporțional cu rata de compresie.

Marcajul este detectabil pentru valori foarte mici ale lui α . Pentru factorul de calitate $Q=5$ (sau o rata de compresie $CR=32$), marcajul este detectabil chiar pentru valori mici ale lui α , adică 0.5.

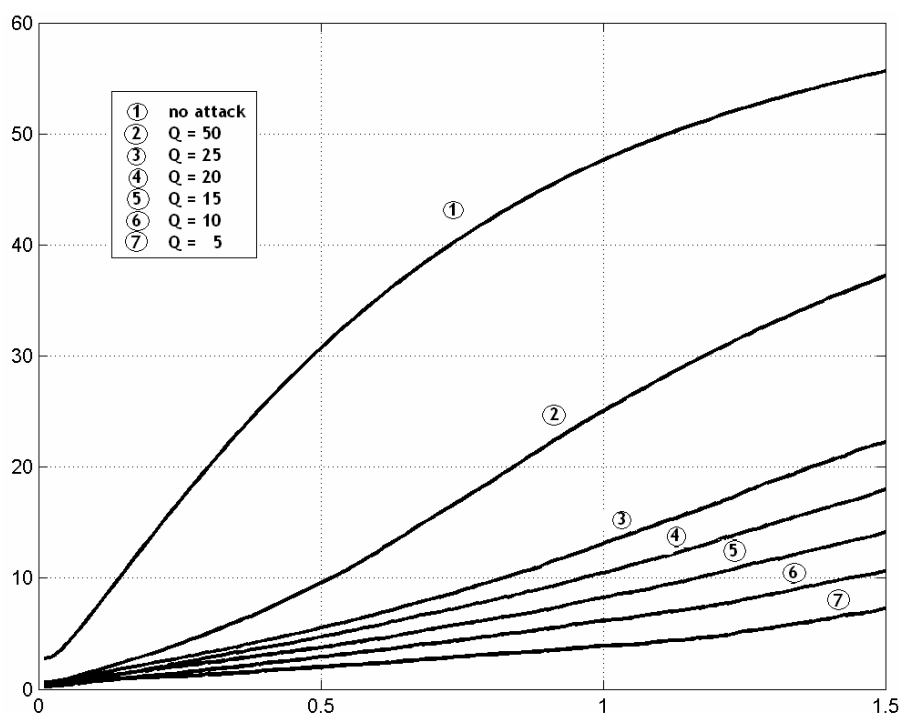


Fig. 5.12: Raportul ρ/T ca funcție de puterea de marcarea, pentru compresie JPEG, la diverși factori de calitate. P_f este 10^{-8} , [NIB06a].

Figura 5.13 prezintă detecția unui marcaj adevărat pentru cazul compresiei JPEG cu diverse valori Q , pentru marcarea cu $\alpha=1.5$; pragul este mult mai mic decât răspunsul detectorului.

În fine, selectivitatea detectorului este ilustrată în Figura 5.14, când sunt testate 1000 de marcaje diferite (999 false și unul adevărat). Al doilea răspuns al detectorului ca mărime (corespunzând unui fals) este arătat împreună cu valoarea de prag, pentru fiecare imagine atacată. Se observă că sunt rejectate falsurile pozitive.

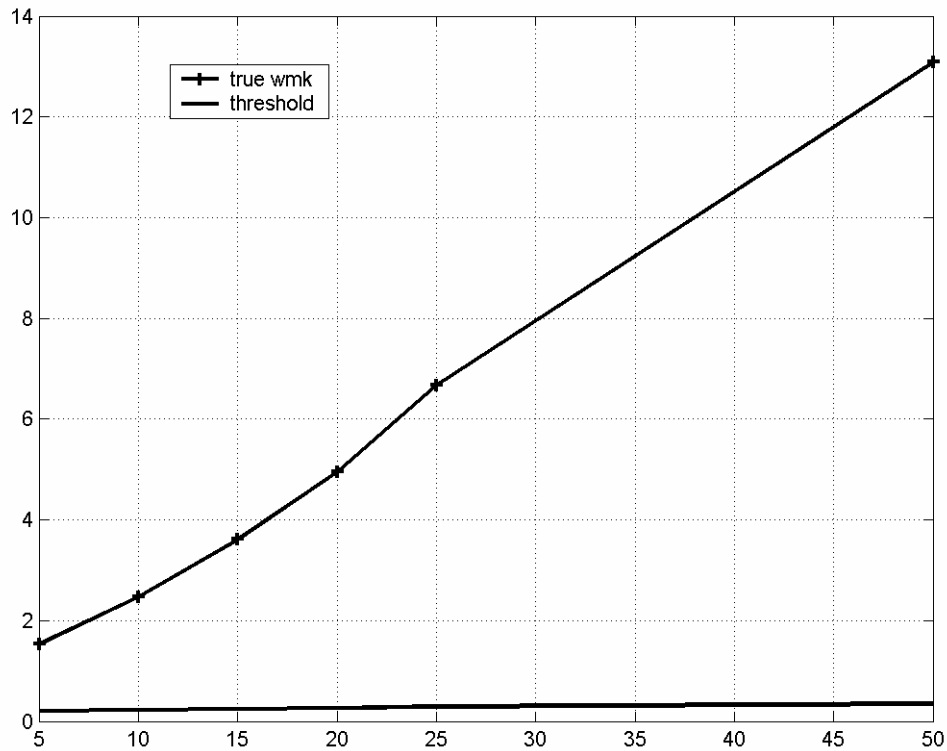


Fig. 5.13: Răspunsul detectorului ρ , pragul de detecție T , ca funcție de Q , factor de calitate în compresia JPEG. Marcajul este detectat cu succes. P_f este 10^{-8} , [NIB06a].

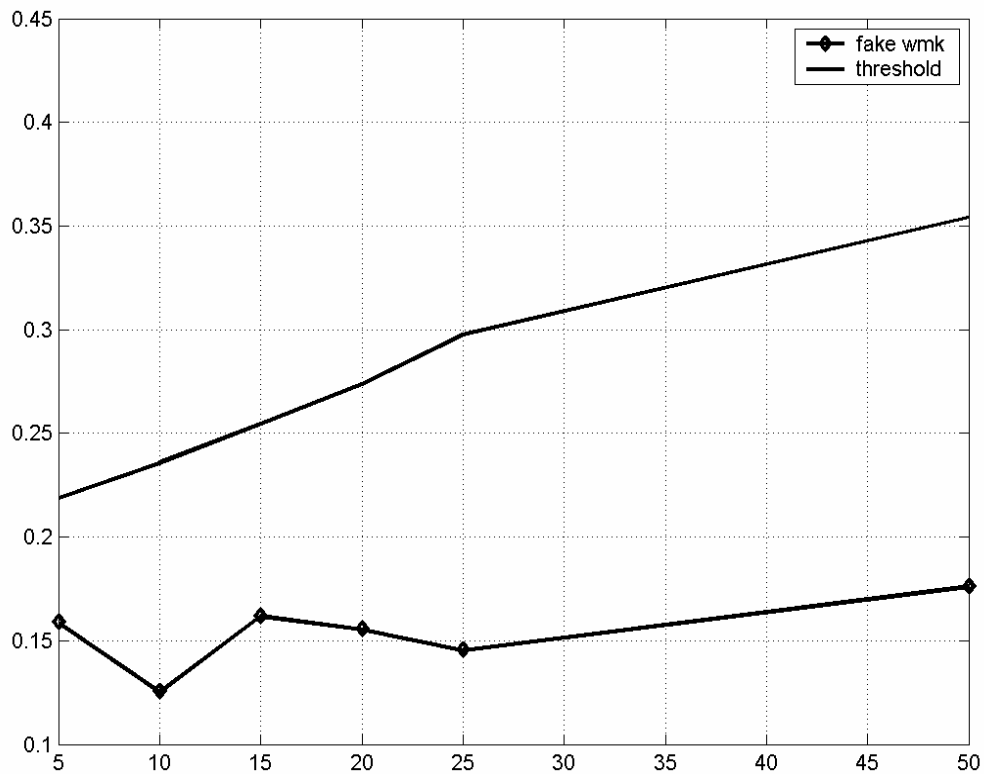


Fig. 5.14: Al doilea răspuns al detectorului ca mărime, ρ_2 , corespunzând unui marcaj fals, și pragul T . Pragul este deasupra lui ρ_2 , [NIB06a].

În Tabelul 5.1 se prezintă o comparație între metoda propusă de mine și prezentată în [NIB06a] și cea din [BBP01]. De această dată, algoritmul a fost testat pe imaginea Lena, pentru $\alpha=1.5$ și un factor de calitate $Q = 5$, corespunzând unei rate de compresie JPEG de 46. Valoarea lui P_f este 10^{-8} și se testează răspunsul detectorului la 1000 de marcaje decorelate. Tabelul arată răspunsul detectorului pentru marcajul original, ρ , pragul de detecție T , precum și al doilea răspuns ca mărime, ρ_2 . Răspunsul detectorului este mai mare decât în cazul metodei din [BBP01].

Noul tip de mască perceptuală reușește să ascundă datele mai bine, datorită estimării mai precise a texturii, cu ajutorul deviației standard locale a imaginii comprimate în domeniul wavelet.

Tab. 5.1. Comparație între metoda prezentată în [BBP01] și cea propusă [NIB06a].

CR = 46, compresie JPEG	Noua metodă [NIB06b]	Metoda lui Barni ș.a. [BBP01]
ρ	0.3199	0.038
T	0.0844	0.036
ρ_2	0.0516	0.01

În continuare se prezintă o extensie a acestei metode [NIB06b], prin care marcajul se poate ascunde imperceptibil și în subbenzile de frecvență mai joasă. Acest lucru aduce un nivel crescut de robustețe.

5.6 Înserare în subbenzile de frecvență mai joasă

Din moment ce imaginea de aproximare a ultimului nivel de rezoluție (4 în cazul prezentat în paragrafele anterioare), conține prea puțină informație, imaginea de luminanță poate fi estimată mai bine pornind de la o imagine de aproximare wavelet de rezoluție mai bună.

De aceea, în continuare masca de luminanță se va calcula diferențiat, pe subimaginea de aproximare de la nivelul l , unde urmează să fie înserat marcajul [NIB06b].

Prin urmare, relația (5.6) este înlocuită cu:

$$L(l, i, j) = \frac{1}{256} I_l^3(i, j) \quad (5.12)$$

unde I_l^3 reprezintă imaginea de aproximare de la nivelul l . Deoarece masca de luminanță este mai dependentă de nivelul de rezoluție, funcția de sensibilitate la zgomot devine:

$$\Theta(l, \theta) = \begin{cases} \sqrt{2}, & \text{dacă } \theta = 1 \\ 1, & \text{altfel} \end{cases} \quad (5.13)$$

Imaginea originală, precum și cele două măști obținute folosind metodele din [NIB06b] și din [BBP01] sunt prezentate în Figura 5.15. Îmbunătățirea este vizibilă în jurul muchiilor și conturilor.



Fig. 5.15(a): Imaginea originală Lena



*Fig. 5.15(b): Masca obținută folosind metoda propusă de Barni ș.a. în [BBP01].
Imaginea este complementară imaginii reale, imagine reprodusă din [NIB06b].*



*Fig. 5.15(c): Masca de nivel 0, obținută folosind metoda din [NIB06b].
Imaginea este complementară imaginii reale.*



*Fig. 5. 16(a): Imagine marcată pentru metoda prezentată [NIB06b], cu $\alpha = 1.5$,
nivelul 0 (PSNR = 38 dB).*



Fig. 5. 16(b): Imagine marcată pentru metoda prezentată în [NIB06b], cu $\alpha = 1.5$, nivelul 1 (PSNR = 43 dB).



Fig. 5.16(c): Imagine marcată folosind masca din [BBP01], cu $\alpha = 1.5$, nivelul 0 (PSNR = 20 dB).

În cele ce urmează se prezintă testele făcute asupra metodei de înserare derivată pe baza relațiilor (5.12) și (5.13), pentru două cazuri diferite [NIB06a]:

- 1) marcajul este înserat numai în nivelul 0, respectiv,
- 2) marcajul este înserat exclusiv în nivelul 1.

Pentru evaluarea performanței, se consideră atacul prin compresie JPEG. Imaginea Lena este marcată în toate subbenzile de detaliu de la nivelul 0 și respectiv în toate subbenzile de detaliu de la nivelul 1, cu diferite intensități de marcăre, începând de la 1.5 la 5. Marcajul binar este înserat așa cum s-a descris mai sus. Pentru $\alpha=1.5$, imaginile marcate, la nivelul 0 respectiv 1, precum și imaginea marcată folosind masca din [BBP01], sunt prezentate în Figura 5.16.

În mod evident, calitatea imaginilor marcate este păstrată folosind această mască. Valorile PSNR sunt 38 dB (nivelul 0), respectiv 43 dB (nivelul 1), comparativ cu cea din [BBP01], cu un PSNR de 20 dB.

Valorile PSNR sunt date în Figura 5.17 ca funcție de intensitatea de marcăre α . Marcajul este încă imperceptibil, chiar și pentru valori mari ale lui α .

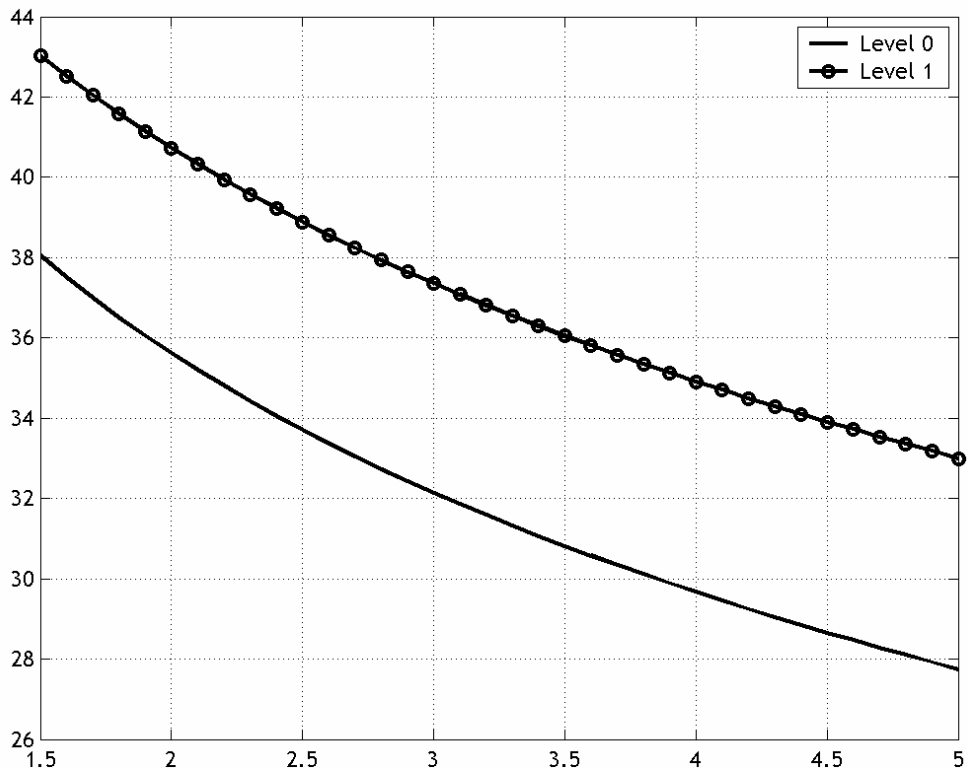


Fig. 5.17: Valorile PSNR ca funcție de α . Inserarea marcajului a fost făcută în nivelul 0, respectiv 1 [NIB06b].

Pentru verificarea algoritmului folosind această mască, se prezintă în Figurile 5.18-19 rezultatele pentru compresia JPEG. Fiecare imagine marcată este comprimată folosind standardul JPEG, pentru șase factori de calitate diferiți, $Q \in \{5, 10, 15, 20, 25, 50\}$. Pentru fiecare imagine atacată, se calculează corelația ρ și pragul T . În toate experimentele, probabilitatea de fals pozitiv este 10^{-8} . Eficiența noului sistem de

marcare poate fi măsurată, la fel ca și înainte, folosind raportul ρ/T . Dacă raportul este mai mare decât 1, atunci marcajul este detectat.

Figurile 5.18-5.19 prezintă dependența acestui raport funcție de α . Se observă că marcajul este detectat cu succes pentru un interval mare de factori de compresie. Pentru valori PSNR mai mari decât 30 dB, marcajul este invizibil. Pentru factori de calitate $Q \geq 10$, distorsiunea introdusă de compresia JPEG este acceptabilă. Pentru toate valorile lui α , marcajul este detectat pentru toți factorii de calitate semnificativi ($Q \geq 10$).

Dacă puterea de marcarea crește, valoarea PSNR a imaginii marcate scade, iar raportul ρ/T crește. Pentru $Q = 10$ (sau o rată de compresie $CR = 32$), marcajul este încă detectabil chiar pentru valori mici ale lui α .

Figura 5.20 prezintă detecția unui marcaj adevărat de la nivelul 0, pentru diferiți factori de calitate, în cazul $\alpha=1.5$; pragul este sub răspunsul detectorului.

Selectivitatea detectorului este de asemenea ilustrată, în cazul testării a 999 de marcaje false: al doilea răspuns ca mărime este arătat, pentru fiecare factor de calitate. Se observă și de această dată că deciziile de fals pozitiv sunt rejectate.

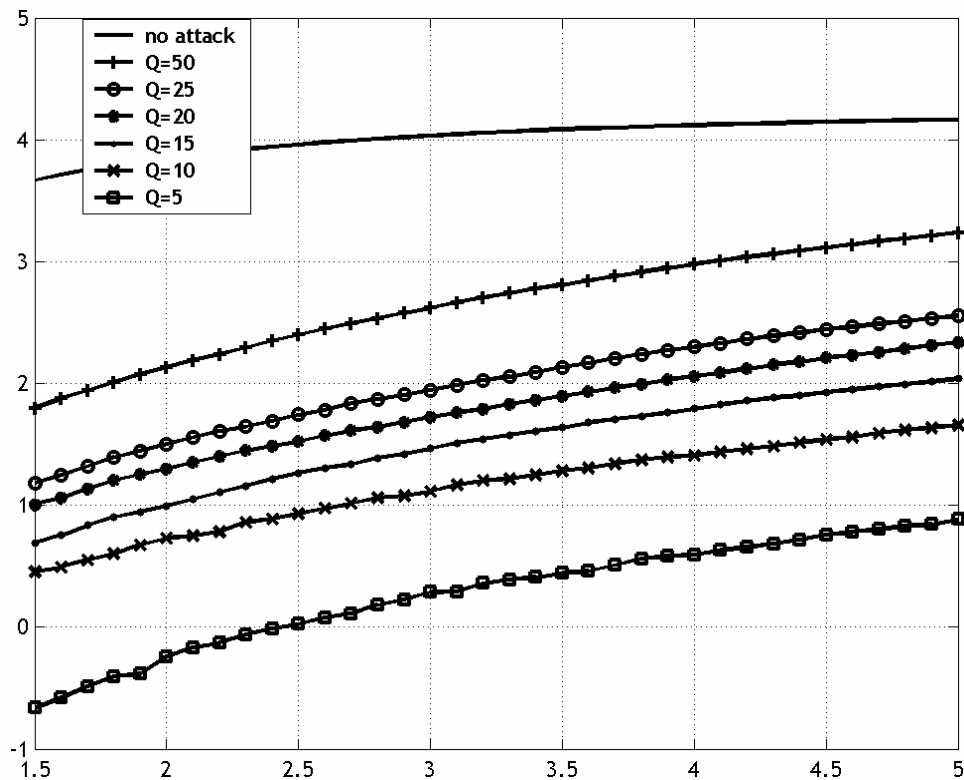


Fig. 5.18: $\log(\rho/T)$ ca funcție de α , pentru compresie JPEG (marcaj inserat la nivelul 0) [NIB06b].

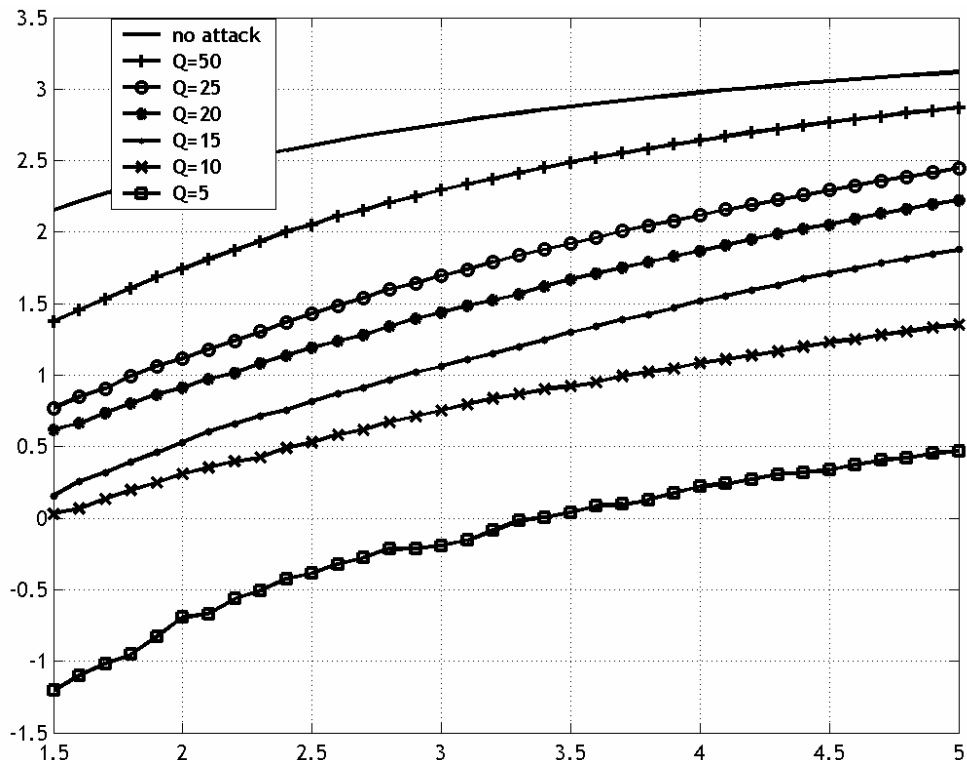


Fig. 5.19: $\log(p/T)$ ca funcție de α , pentru compresie JPEG (marcaj înserat la nivelul 1) [NIB06b].

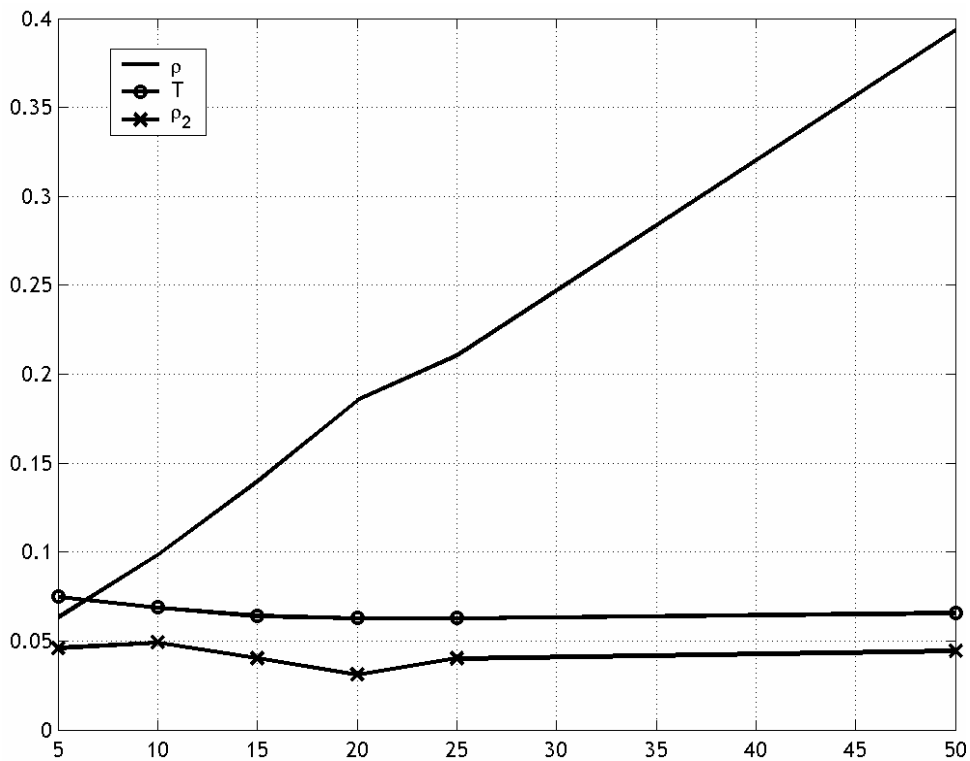


Fig. 5.20: Răspunsul detectorului ρ , pragul de detecție T , al doilea răspuns ca mărime ρ_2 , corespunzând unui marcaj fals, ca funcție de diferiți factori de calitate JPEG. Marcajul este detectat. Au fost testate 999 de marcaje false [NIB06a].

În Tabelul 5.2 se dă o comparație între această mască [NIB06a] și cea prezentată în [BBP01], pentru compresie JPEG, cu $Q = 10$, echivalent unei rate de compresie de 32 pentru imaginea Lena. Se dau răspunsul detectorului, pentru marcajul original, ρ , pragul de decizie, T , precum și al doilea răspuns ca mărime al detectorului, corespunzând unui marcaj fals, ρ_2 , atunci când marcajul a fost inserat în nivelul 0. Răspunsul detectorului este mai mare decât pentru metoda din [BBP01].

Tab. 5.2: Comparație între metoda prezentată în [NIB06a] și cea propusă de Barni ș.a. [BBP01].

Compresie JPEG, CR=32	Noua metodă [NIB06a]	Metoda lui Barni ș.a. [BBP01]
ρ	0.0750	0.062
T	0.0636	0.036
ρ_2	0.0461	0.011

5.7 Evaluarea robusteții marcajelor perceptuale

Într-un sistem de marcarea, evaluarea robusteții ar trebui făcută numai atunci când criteriile de invizibilitate sunt satisfăcute. În acest scop, propunem măsurarea impactului perceptual al marcajului asupra imaginii folosind bine cunoscutul criteriu al raportului maxim (de vârf) semnal-pe-zgomot, PSNR și, în plus, un model spațial care indică pixelii modificați vizibil față de imaginea originală. În aceasta secțiune, studiem sistemul propus de Barni și alții [BBP01] precum și metoda propusă în [NIB06a] ambele bazate pe mascare pixel cu pixel în domeniul wavelet. Limităm intensitatea de marcaj astfel încât PSNR să fie în jur de 35 dB, iar media pixelilor afectați vizibil mai mică decât 25%. Sunt testate mai multe imagini cu mai multe tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare și corecție de gamma) pentru a evidenția efectele acestor atacuri asupra rezultatelor detectorului. Rezultatele arată limitările acestor tehnici atunci când se impune constrângerea de invizibilitate.

Marcajele perceptuale sunt folosite pentru a satisface cele două cerințe de transparență precum și invizibilitate în același timp. Studiem două tehnici de marcarea perceptuală care înserează marcajul în domeniul wavelet. În [BBP01] marcajul este mascat conform caracteristicilor sistemului vizual uman, (HVS), ținând cont de textura și luminanța tuturor subbenzilor de detaliu ale transformatei wavelet. În [NIB06a] o altă mască perceptuală este folosită, bazată pe deviația standard locală a imaginii (a se vedea paragraful anterior).

Aceste tehnici sunt perceptuale, dar nu trebuie testată robustețea unei metode decât dacă sunt satisfăcute unele criterii de invizibilitate. Așa cum a sugerat Fridrich și alții în [FG99], un model spațial care indică numărul și localizarea pixelilor afectați de marcarea [Gir89] poate fi folosit pentru a cuantifica invizibilitatea procesului de marcarea. Acest model a fost folosit și pentru “corectarea” marcajului în domeniul spațial în [SZT96].

Mai mult, un estimat al robusteții [FG99] este folosit pentru a demonstra validitatea algoritmilor atunci când criteriile de invizibilitate sunt satisfăcute.

Cele două tehnici de marcarea au fost descrise anterior. Ca și până acum, la detecție vom considera raportul între corelația ρ din relația (5.7) și pragul dependent

de imagine, T_ρ , astfel încât detectorul este o funcție neliniară cu prag fix. În cele ce urmează vom nota metoda din [BBP01] cu “metoda 1” iar cea descrisă în [NIB06a] cu “metoda 2”.

Rezultate obținute în urma simulării. Mai multe imagini din baza de date din [USC] au fost marcate la nivelul $l=0$ cu diferite intensități de marcare α . Un marcaj binar este inserat în toate subimaginele de detaliu, ale primului nivel de rezoluție, $l=0$, așa cum s-a văzut în paragraful 5.4.

Pentru $\alpha=0.2$ (metoda 1) și $\alpha=0.4$ (metoda 2), imaginile sunt neafectate de procesul de marcare. Această afirmație se bazează atât pe valorile PSNR obținute, cât și pe modelul spațial de mascare care indică numărul și localizarea pixelilor afectați din imagine [Gir89, Fri99b]. Imaginea Lena originală și marcată cu cele două metode este prezentată în fig. 5.23, împreună cu pixelii afectați din imagine, conform modelului lui Girod.

Media intensității de marcare $\bar{\alpha}$, valorile PSNR precum și procentajul de pixeli afectați sunt prezentați în tabelul 5.3. Aceste valori sunt prezentate și în Figura 5.21 (a)-(c).

Tab. 5.3: Comparație a invizibilității între imaginile marcate cu cei doi algoritmi, tabel din [Naf07a].

Imagine	Intensitate medie		PSNR (dB)		Pixeli modificați (%)	
	1	2	1	2	1	2
IM1	2.95	5.19	33.33	34.33	40.39	22.95
IM2	3.00	3.98	32.83	35.76	36.87	14.92
IM3	1.97	3.76	35.90	36.19	8.71	6.75
IM4	2.36	3.21	35.28	38.38	25.30	2.59
IM5	3.84	5.91	30.97	32.90	58.20	31.36
IM6	1.99	3.06	36.39	38.40	11.84	4.55
IM7	2.48	4.35	34.38	34.86	18.25	13.14
IM8	3.23	3.56	32.60	37.12	48.29	7.58
IM9	2.55	3.14	34.40	37.89	28.79	4.96
IM10	2.34	3.79	35.05	36.72	18.48	6.73
IM11	2.48	3.47	34.98	37.78	26.65	4.66
IM12	2.13	3.60	35.94	37.16	13.80	3.82
IM13	2.80	5.96	33.61	33.08	16.04	19.90
IM14	3.21	4.51	32.66	35.52	53.26	10.69
IM15	1.79	2.86	37.61	39.56	4.25	1.17
IM16	0.96	2.54	41.75	39.82	0.21	2.21
IM17	1.72	3.25	38.03	38.62	2.80	0.99
IM18	1.76	2.95	37.90	39.42	2.37	0.38
IM19	2.60	3.54	34.61	37.79	38.90	1.76
IM20	2.57	3.19	34.74	38.71	42.05	0.64
IM21	2.08	3.35	36.56	38.49	6.87	0.40
IM22	1.24	2.73	40.40	40.05	1.09	0.43
IM23	1.97	3.58	36.91	37.84	9.76	1.55
IM24	1.76	2.96	37.92	39.52	1.31	0.13

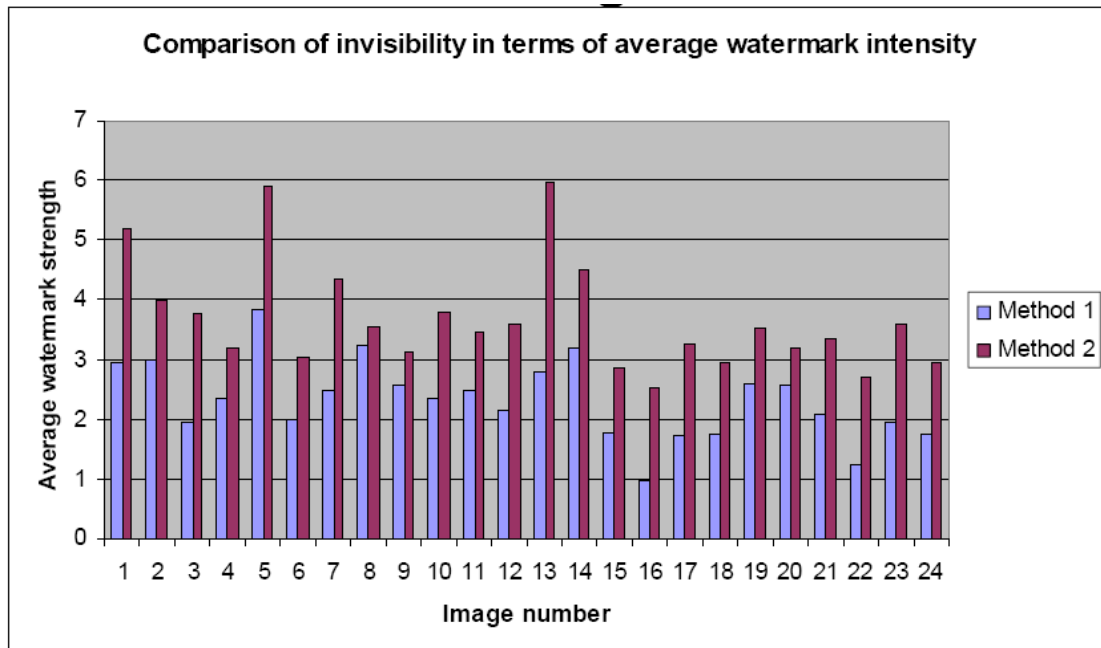


Fig. 5.21(a): Comparație a invizibilității între imaginile marcate cu cei doi algoritmi funcție de intensitatea de marcă medie

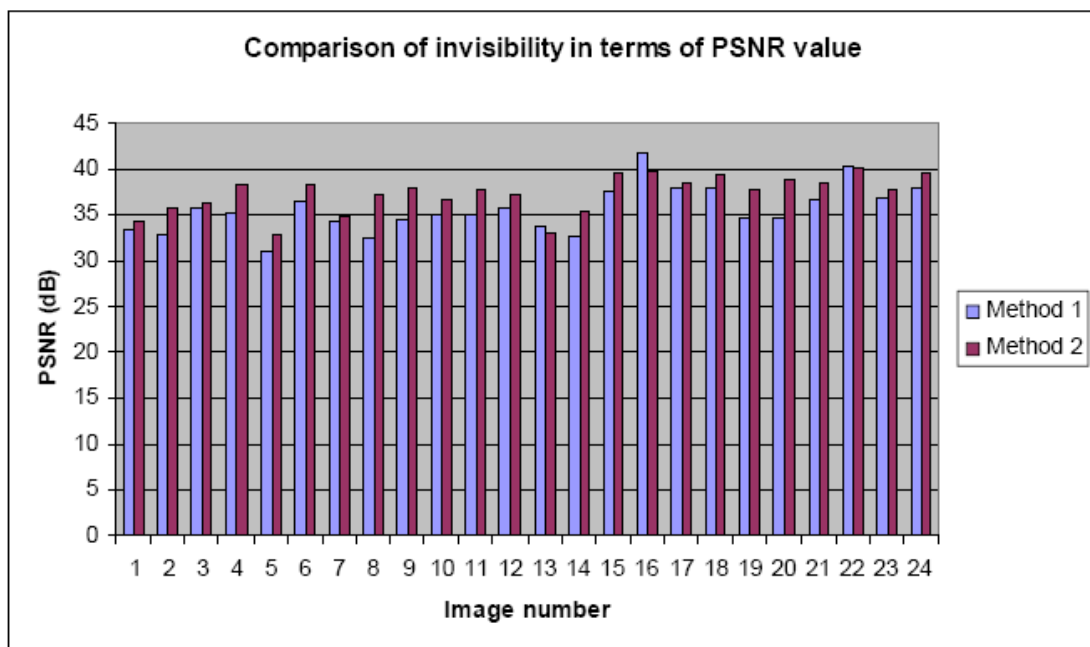


Fig. 5.21(b): Comparație a invizibilității între imaginile marcate cu cei doi algoritmi funcție de valoarea PSNR dintre imaginea marcată și originală

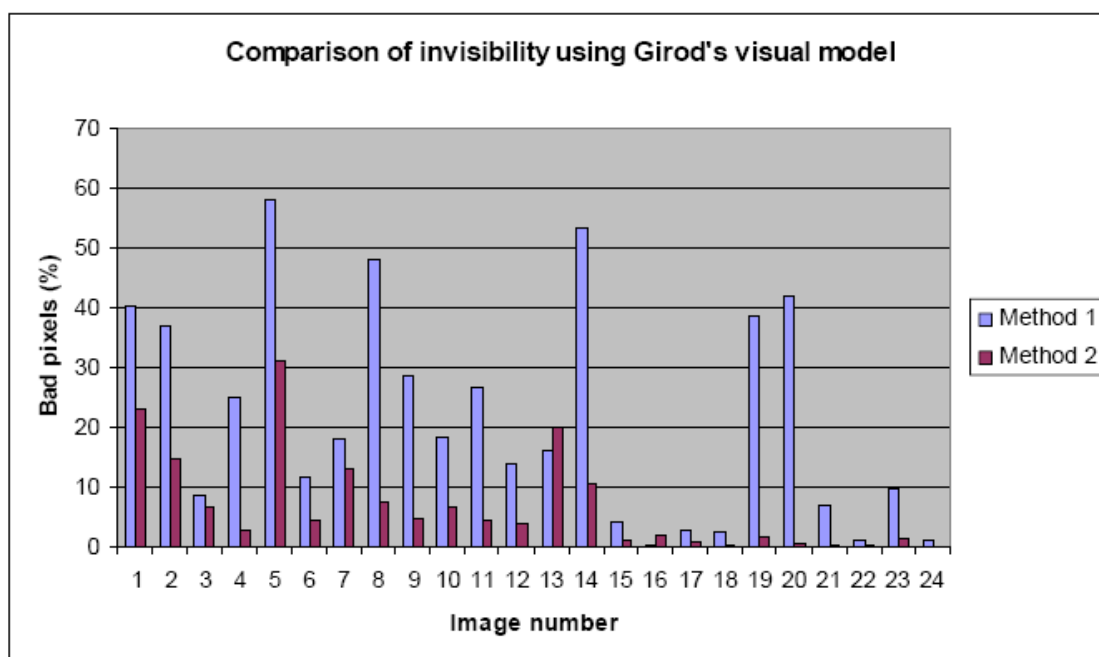


Fig. 5.21(c): Comparație a invizibilității între imaginile marcate cu cei doi algoritmi funcție de procentajul de pixeli afectați folosind modelul lui Girod

Tab. 5.4: Comparație a robusteții [Naf07a].

Imagine	Raport p/T		Robustețe	
	1	2	1	2
IM1	33.22	22.78	0.80	0.72
IM2	37.25	20.00	0.91	0.65
IM3	39.40	31.33	0.59	0.57
IM4	59.00	29.18	0.79	0.56
IM5	37.70	23.95	0.81	0.65
IM6	66.33	38.25	0.66	0.53
IM7	30.75	21.95	0.68	0.65
IM8	44.14	21.62	0.63	0.37
IM9	51.20	28.63	0.76	0.51
IM10	46.60	29.23	0.71	0.59
IM11	62.00	34.70	0.82	0.60
IM12	35.16	23.33	0.40	0.34
IM13	40.28	35.11	0.69	0.73
IM14	39.50	23.73	0.86	0.62
IM15	59.66	31.77	0.67	0.54
IM16	47.50	36.28	0.35	0.43
IM17	57.33	36.00	0.61	0.57
IM18	58.00	32.11	0.56	0.47
IM19	52.20	29.66	0.90	0.62
IM20	51.60	26.33	0.88	0.56
IM21	51.75	30.54	0.75	0.60
IM22	41.66	34.00	0.48	0.50
IM23	49.25	32.45	0.69	0.62
IM24	58.66	36.87	0.65	0.54

Tabelul 5.4 prezintă raportul dintre corelație și prag dar și estimatul robusteții așa cum este definit în [FG99], *raportul dintre puterea marcajului și puterea modificării acceptabile, folosind modelul lui Girod*:

$$\frac{\sum_{i,j} w^2(i,j)}{\sum_{i,j} m^2(i,j)} \quad (5.14)$$

unde $w(i,j)$ este marcajul, estimat ca diferența dintre doi pixeli ai imaginii, iar $m(i,j)$ este modificarea maximă acceptabilă pentru imaginea originală.

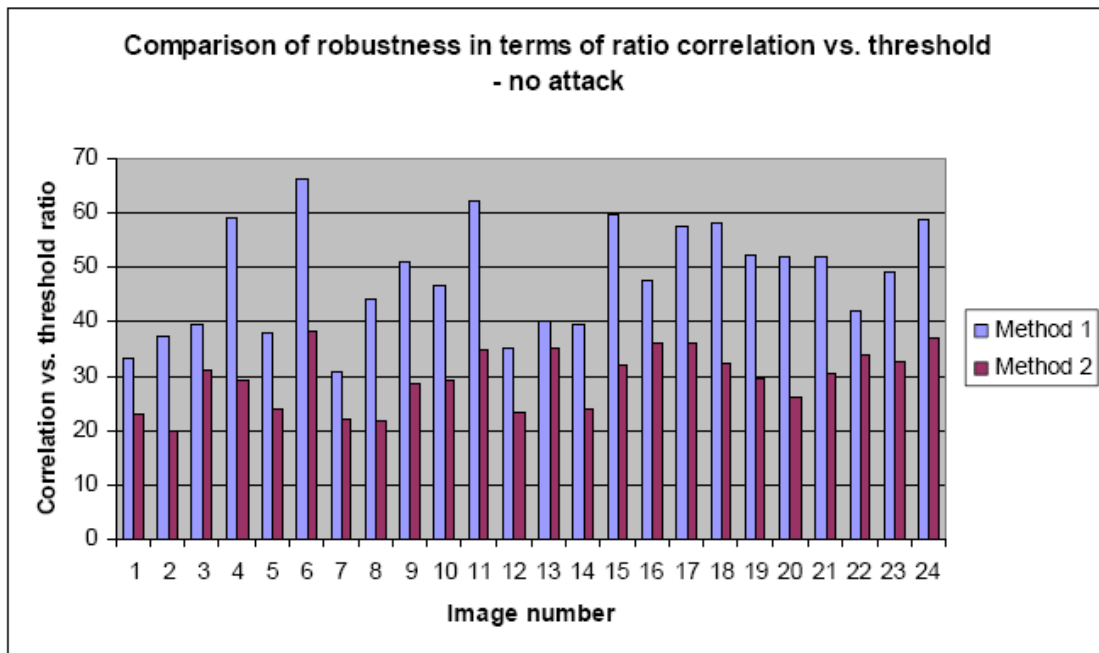


Fig. 5.22(a): Comparația robusteții funcție de raportul corelație per prag

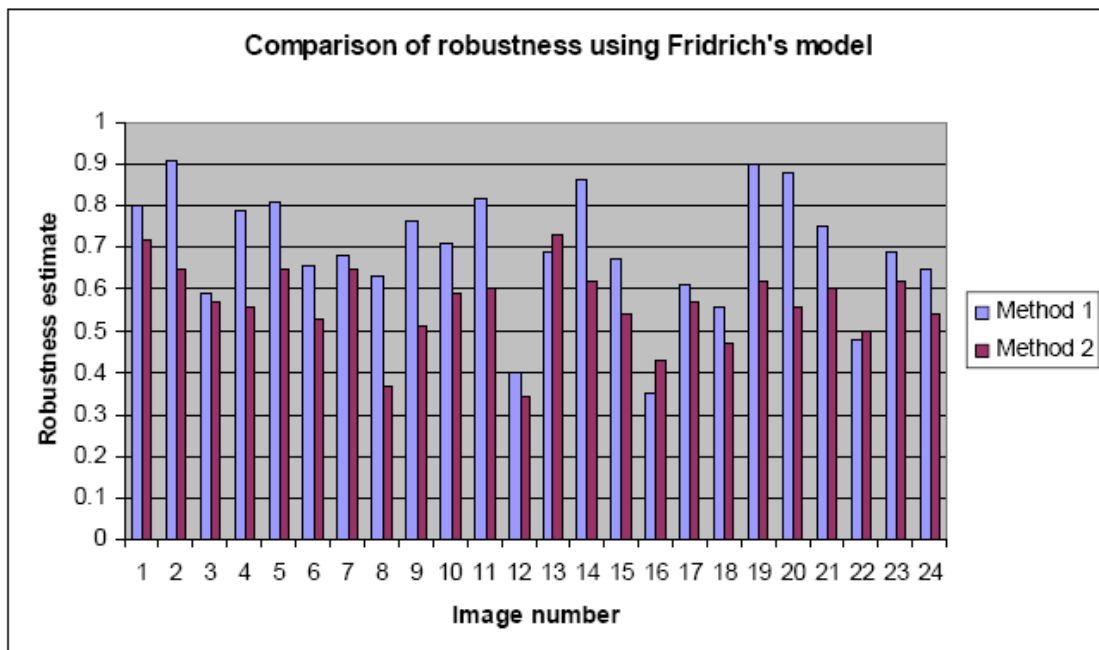


Fig. 5.22(b): Comparația robusteții folosind modelul lui Fridrich



Fig. 5.23: Imaginea originală Lena (sus), imaginile marcate cu $\alpha=0.2$ (metoda 1) [BBP01], PSNR=36.39 dB, 11.84% pixeli afectați, respectiv cu $\alpha=0.4$ (metoda 2), [Naf07a], PSNR=35.92dB, 15.71% pixeli afectați. Pixelii afectați din imagini, conform modelului lui Girod sunt reprezentați cu negru [Naf07a].

Pentru a verifica validitatea algoritmilor prezentați anterior pentru aceste intensități de marcarea, de exemplu $\alpha=0.2$ (metoda 1) și $\alpha=0.4$ (metoda 2), am efectuat teste pentru compresie JPEG, filtrare mediană, decupare, redimensionare și corecție de gamma. Pentru fiecare imagine atacată, corelația ρ și pragul T_p sunt calculate. Probabilitatea de fals pozitiv este fixată la valoarea 10^{-8} .

Tabelele 5.5, 5.6, 5.7, 5.8 prezintă raportul corelație/prag pentru fiecare imagine și atac. Pentru o mai bună vizualizare a rezultatelor, prezentăm și grafice cu valorile corelațiilor în funcție de imagini pentru fiecare atac.

Rezistența la compresia JPEG: marcajul este încă detectabil chiar la factori de calitate 10, în ambele cazuri. Metoda 2 are evident rezultate mai bune în fiecare caz; detectează marcajul pentru $Q=5$ pentru jumătate din imagini. Metoda 1 nu reușește să detecteze marcajul în cazul compresiei cu $Q=5$.

Rezistența la filtrarea mediană: marcajul de la metoda 2 a supraviețuit în aproape toate imaginile pentru filtrare mediană cu lungimea ferestrei filtrului până la 3. Pentru filtru cu dimensiune 5, marcajul inserat cu metoda 2 nu este detectabil. Metoda 1 nu a supraviețuit în nici unul dintre cazuri.

Rezistența la redimensionare: marcajul este detectat cu succes în ambele cazuri, atât pentru metoda 1 cât și pentru metoda 2.

Rezistența la corecția de gamma: așa cum era de așteptat pentru corelație normalizată, ambele metode sunt practic insensibile la ajustarea contrastului [Cox05].

Rezistența la decupare: marcajul inserat cu metoda 1 este detectat în imaginea decupată de 32×32 în cele mai multe cazuri, în timp ce marcajul inserat cu metoda 2 este detectat numai la unele imagini. Metoda 2 detectează marcajul până la imaginea decupată de mărime 64×64 , inclusiv.

Performanțele metodei 1, ușor mai bune decât ale metodei 2 în cazul corecției gamma și decupării, pot fi explicate prin faptul că *puterea marcajului* este mai mare în cazul metodei 1 decât în cazul metodei 2, așa cum se vede din valorile estimate ale robusteții din tabelul 5.4.

Concluzii. Am argumentat că nu ar trebui testată robustețea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute. Ca și constrângere de invizibilitate, am folosit raportul maxim semnal-pe-zgomot, precum și modelul de mascare spațială din [Gir89]. Au fost testate două măști perceptuale, pe un număr mare de imagini. Intensitatea de marcarea a fost fixată astfel încât procentajul de pixeli degradați din imaginea marcată să nu depășească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Aceasta a indicat că imaginile nu sunt vizibil afectate de procesul de marcarea.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare și corecție de gamma).

Rezultatele simulării au arătat că la impunerea constrângerii de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode au fost comparabile și au detectat cu succes marcajul numai în cazul atacurilor ușoare. Aceste rezultate au fost prezentate în [Naf07a].

Tab. 5.5: Raport corelație/prag, comparația robusteții în cazul compresiei JPEG pentru diverși factori de calitate. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

<i>Imagine</i>	<i>JPEG</i> <i>Q=20</i>		<i>JPEG</i> <i>Q=15</i>		<i>JPEG</i> <i>Q=10</i>		<i>JPEG</i> <i>Q=5</i>	
	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>
IM1	4.79	6.09	3.76	5.04	2.58	3.90	0.17	2.41
IM2	2.92	3.45	2.34	3.02	1.71	2.37	0.32	1.60
IM3	2.55	3.74	1.88	2.99	1.27	2.01	0.27	1.23
IM4	3.18	3.84	2.28	3.01	1.45	2.07	0.24	1.06
IM5	4.52	5.36	3.66	4.36	2.49	3.16	0.29	1.83
IM6	2.38	3.46	1.52	2.70	0.97	2.03	0.56	0.91
IM7	2.37	4.15	1.82	3.28	1.13	2.08	0.12	1.31
IM8	4.67	4.12	3.69	3.39	2.66	2.40	0.12	1.38
IM9	2.29	2.45	1.72	1.91	1.20	1.29	0.13	0.50
IM10	2.88	4.04	2.40	3.40	1.74	2.75	0.35	1.42
IM11	2.89	3.60	2.06	2.66	1.31	1.64	0.16	0.83
IM12	2.14	2.83	1.61	2.05	1.16	1.41	0.35	0.73
IM13	4.55	7.22	3.74	6.00	2.60	4.19	0.14	2.52
IM14	5.11	5.19	3.88	4.32	2.51	2.97	0.33	1.55
IM15	3.18	3.82	2.40	2.86	1.54	1.82	0.24	0.75
IM16	1.76	2.61	1.29	2.01	0.96	1.26	0.19	0.50
IM17	2.82	4.43	2.14	3.09	1.22	1.80	0.23	0.17
IM18	2.49	3.59	1.72	2.57	0.94	1.28	0.27	0.30
IM19	4.81	5.49	3.60	4.11	2.29	2.77	0.39	1.36
IM20	4.79	4.42	3.55	3.59	2.00	2.34	0.20	0.62
IM21	3.74	5.05	2.80	4.00	1.58	2.54	0.22	0.82
IM22	2.40	3.49	1.79	2.19	1.28	1.29	0.43	0.58
IM23	3.39	4.97	2.60	3.42	1.73	2.22	0.18	0.90
IM24	3.21	4.37	2.15	3.30	1.29	1.63	0.13	0.47

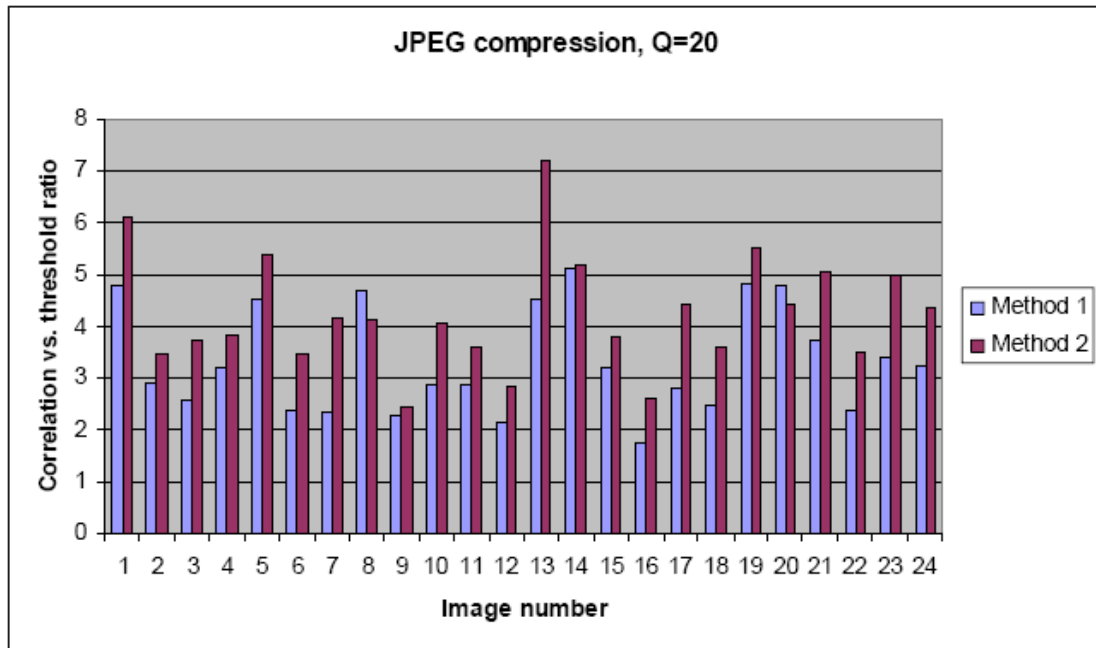


Fig. 5.24(a): Raport corelație/prag, comparația robusteții în cazul compresiei JPEG, factor de calitate 20

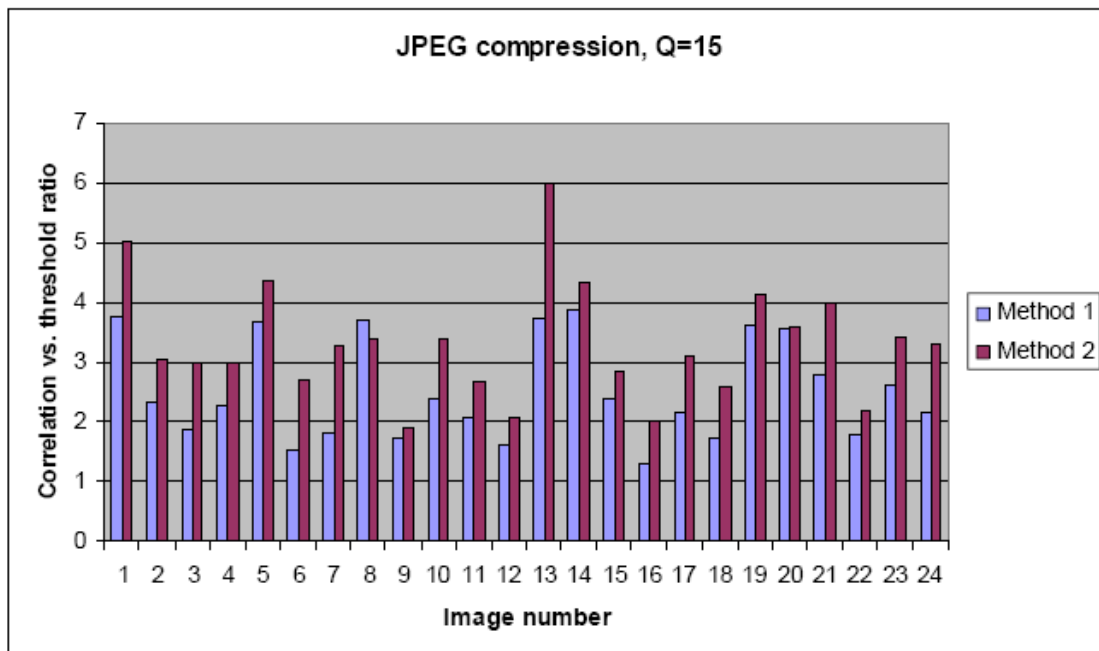


Fig. 5.24(b): Raport corelație/prag, comparația robusteții în cazul compresiei JPEG, factor de calitate 15

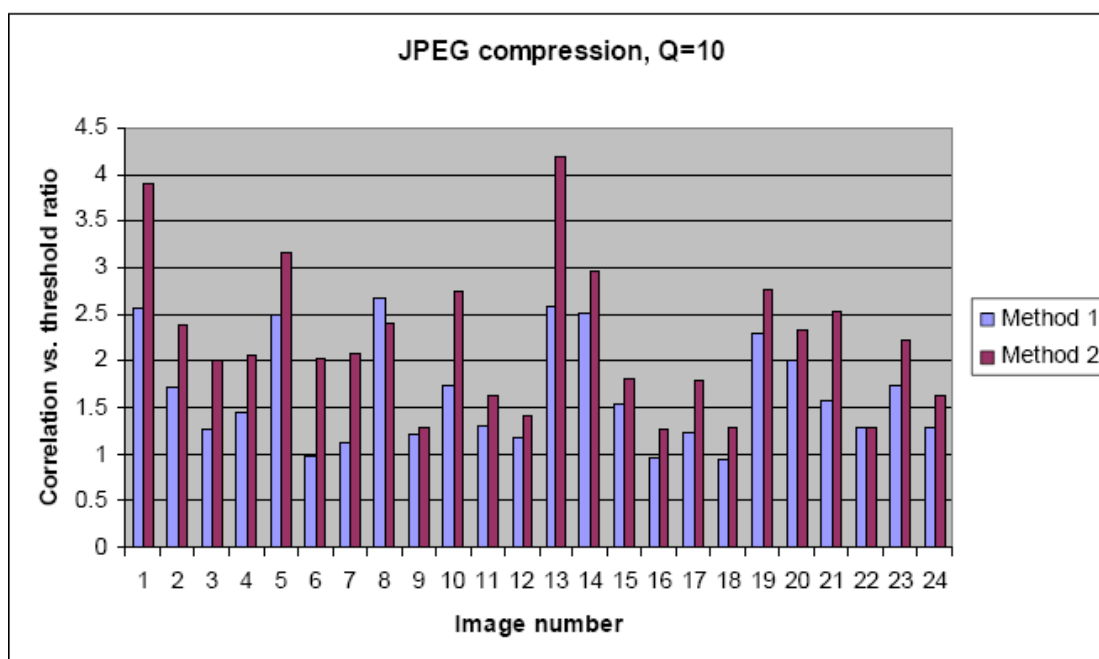


Fig. 5.24(c): Raport corelație/prag, comparația robusteții în cazul compresiei JPEG, factor de calitate 10

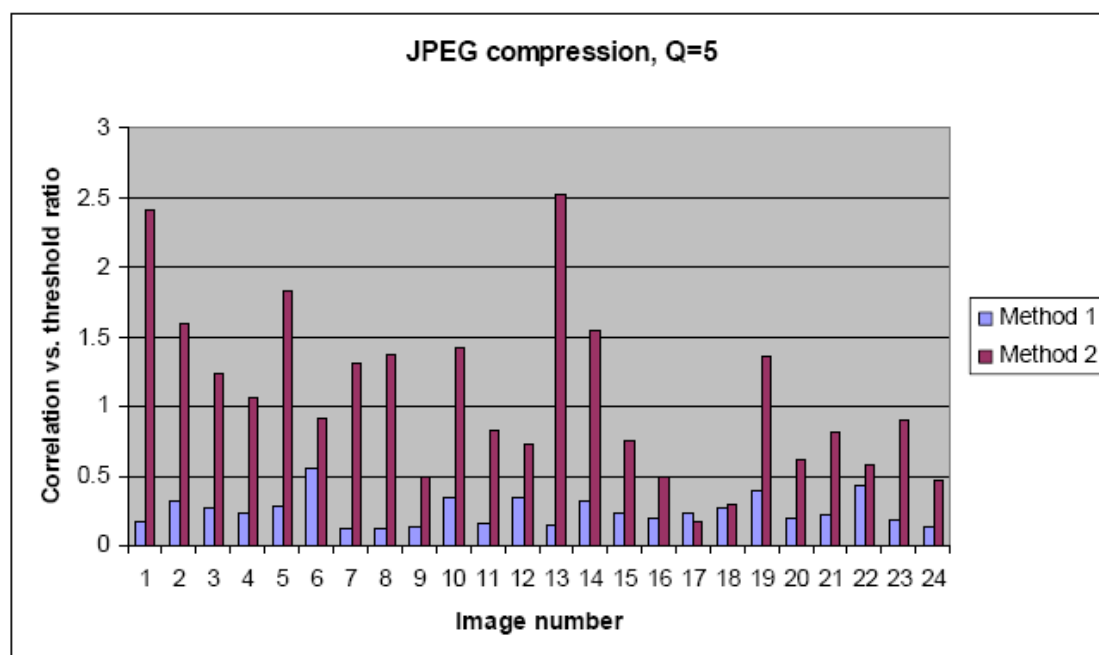


Fig. 5.24(d): Raport corelație/prag, comparația robusteții în cazul compresiei JPEG, factor de calitate 5

Tab. 5.6: Raport corelație/prag, comparația robusteții în cazul filtrării mediane și a redimensionării. Intensitatea maximă de marcăre este dată de constrângerea de invizibilitate [Naf07a].

<i>Imagine</i>	<i>Filtrare mediană M=3</i>		<i>Filtrare mediană M=5</i>		<i>Redimensionare 75%</i>		<i>Redimensionare 50%</i>	
	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>
IM1	0.47	1.21	0.29	-0.46	8.95	12.33	2.13	0.85
IM2	1.22	2.53	0.38	0.69	10.21	11.37	2.11	1.02
IM3	0.34	1.65	0.13	0.41	8.49	14.22	1.59	1.27
IM4	0.68	1.41	0.05	0.52	11.52	14.09	1.34	1.32
IM5	0.68	1.74	0.23	0.59	9.15	12.48	1.84	1.07
IM6	1.57	2.83	0.59	1.39	14.09	17.55	2.31	1.40
IM7	0.62	1.29	0.24	0.27	7.02	11.93	1.29	1.27
IM8	0.54	1.52	0.00	0.42	12.10	11.18	1.85	0.83
IM9	1.02	1.33	0.55	0.66	11.96	12.42	2.14	1.47
IM10	0.73	2.40	0.27	0.92	10.88	15.37	1.98	1.35
IM11	0.92	0.54	0.36	0.46	16.97	17.33	1.99	1.76
IM12	0.50	0.97	0.13	-0.14	9.04	12.67	1.46	0.62
IM13	0.47	3.59	0.20	0.66	9.55	17.28	1.95	1.41
IM14	0.24	1.21	-0.02	0.02	10.20	12.57	1.66	1.30
IM15	0.67	1.61	0.15	-0.10	12.86	16.83	2.32	1.26
IM16	0.56	-1.04	0.22	-0.33	10.22	18.94	2.07	1.55
IM17	0.80	-0.08	0.50	-0.68	13.49	18.63	2.91	1.40
IM18	0.53	1.31	0.18	0.10	10.25	15.03	1.16	1.20
IM19	0.50	1.12	0.06	-0.20	14.19	15.42	2.83	1.09
IM20	0.29	1.54	-0.07	-0.27	14.10	14.14	2.70	1.06
IM21	0.24	1.27	0.00	-0.50	13.31	16.40	2.48	1.30
IM22	0.29	-0.63	0.24	-0.69	11.69	17.99	2.35	1.64
IM23	0.58	0.87	0.34	-0.60	11.64	16.74	2.48	1.05
IM24	0.75	1.98	0.30	-0.26	15.28	19.79	2.82	1.54

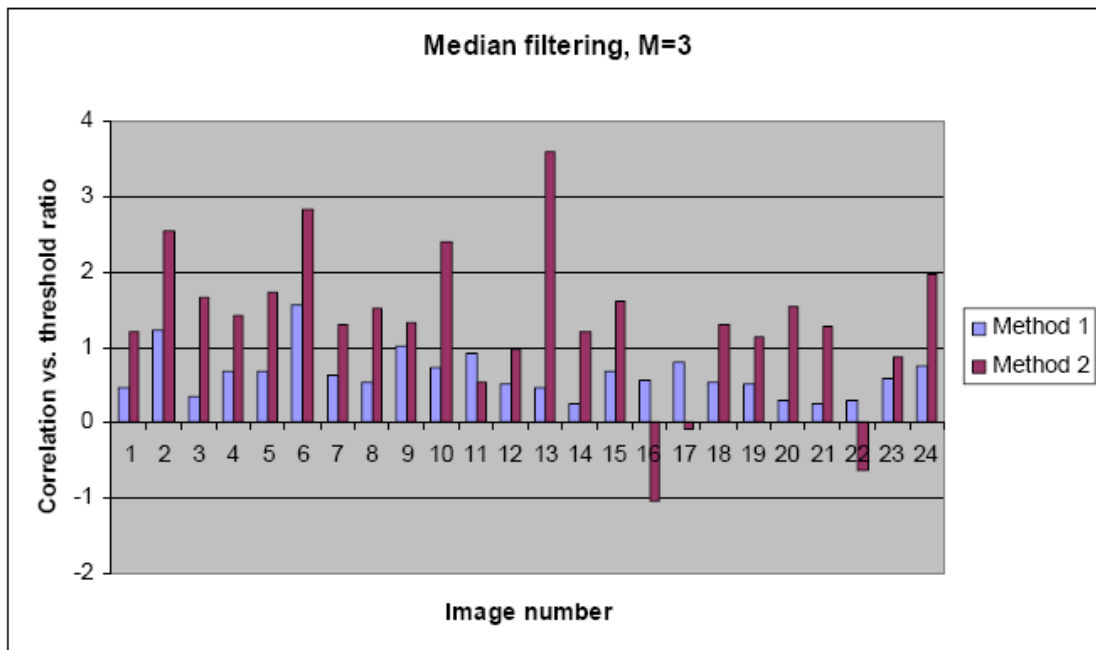


Fig. 5.25(a): Raport corelație/prag, comparația robusteții în cazul filtrării mediene, dimensiune filtru 3

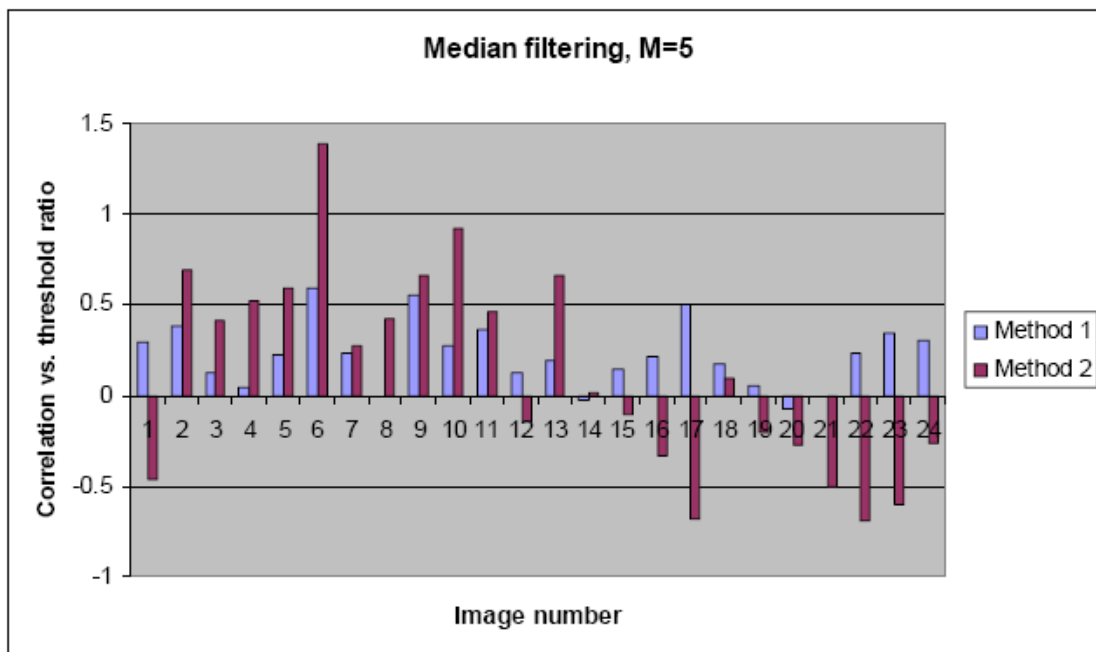


Fig. 5.25(b): Raport corelație/prag, comparația robusteții în cazul filtrării mediene, dimensiune filtru 5

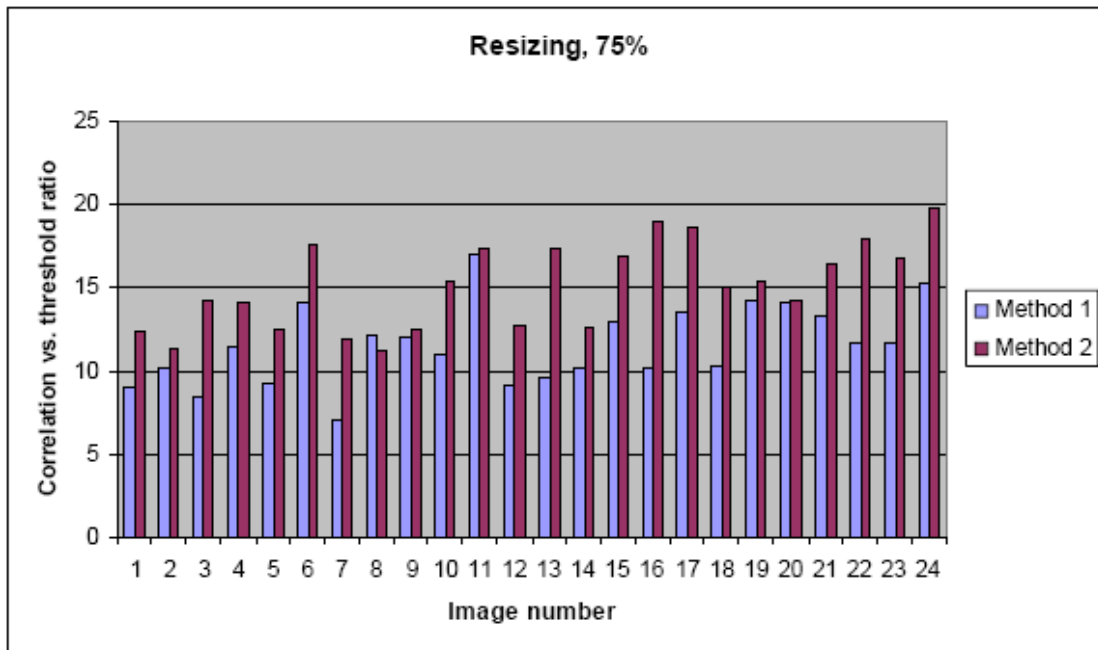


Fig. 5.26(a): Raport corelație/prag, comparația robusteții în cazul redimensionare, 75%

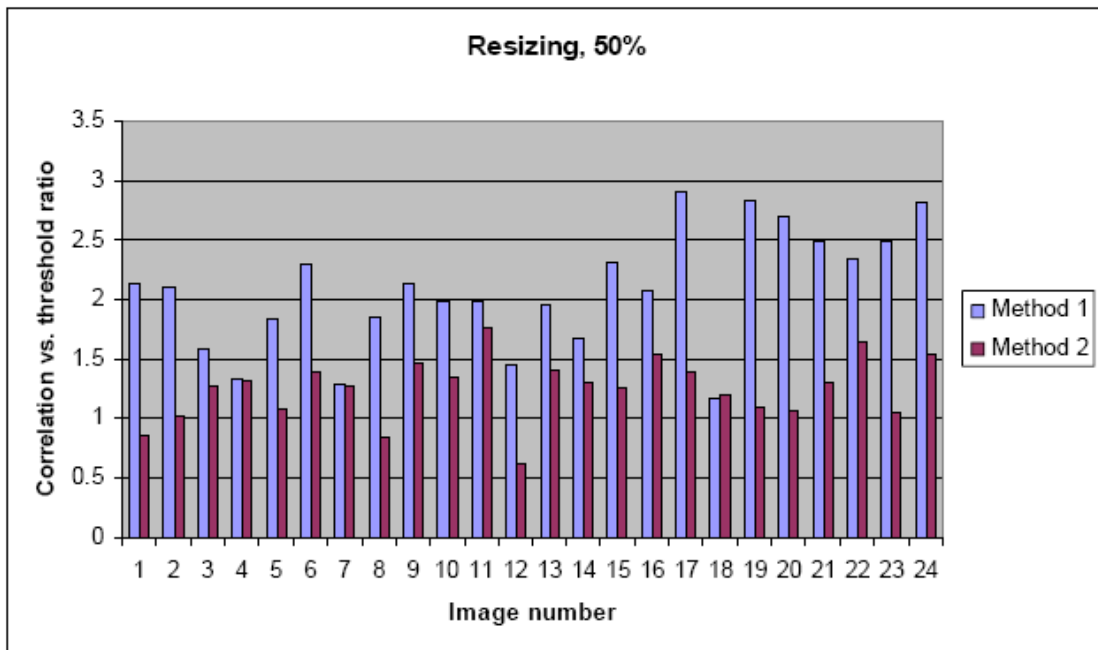


Fig. 5.26(b): Raport corelație/prag, comparația robusteții în cazul redimensionării, 50%

Tab. 5.7: Raport corelație/prag, comparația robusteții în cazul corecției de gamma. Intensitatea maximă de marcare este dată de constrângerea de invizibilitate [Naf07a].

<i>Imagine</i>	$\gamma=0.5$		$\gamma=1$		$\gamma=1.5$		$\gamma=2$	
	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>	<i>1</i>	<i>2</i>
IM1	25.04	28.43	25.33	28.97	25.22	28.99	25.04	28.80
IM2	24.82	27.14	28.49	25.51	30.00	23.95	30.74	22.67
IM3	35.31	37.03	32.92	39.32	32.02	40.83	31.52	42.03
IM4	37.06	36.11	39.86	35.56	40.28	34.30	40.34	32.65
IM5	26.72	31.09	29.97	30.10	30.83	28.48	31.05	26.78
IM6	44.23	43.13	44.07	44.87	43.04	45.31	42.43	44.81
IM7	21.24	29.81	25.33	28.61	26.54	26.68	26.95	24.81
IM8	29.36	31.00	35.25	27.39	38.20	25.21	38.88	23.76
IM9	40.40	32.61	40.89	34.89	39.91	34.98	38.30	34.86
IM10	33.47	36.60	35.60	37.46	35.80	36.91	35.41	35.95
IM11	47.55	40.51	46.41	42.86	44.90	43.89	43.87	44.00
IM12	25.88	26.75	27.19	29.89	26.23	30.09	24.96	29.10
IM13	34.77	39.77	32.89	42.47	31.70	43.80	30.96	44.49
IM14	30.58	30.21	32.94	31.06	32.98	30.50	32.59	29.44
IM15	40.14	39.06	39.46	40.75	38.61	41.56	37.98	41.72
IM16	34.03	40.35	30.03	44.97	27.73	47.71	27.34	49.59
IM17	37.80	41.75	37.00	43.79	36.13	44.65	35.57	45.02
IM18	41.87	33.93	40.00	40.45	37.93	42.48	35.31	43.47
IM19	37.46	36.81	39.57	36.66	39.95	35.96	39.99	35.04
IM20	37.30	34.34	39.98	34.17	40.48	33.36	40.44	32.36
IM21	37.38	37.21	36.73	38.91	35.88	39.54	35.11	39.66
IM22	33.01	39.61	31.85	42.41	30.86	43.72	30.01	44.83
IM23	34.89	38.47	34.68	40.17	34.06	40.98	33.67	41.19
IM24	44.30	46.28	44.34	47.56	43.73	47.85	43.22	47.77

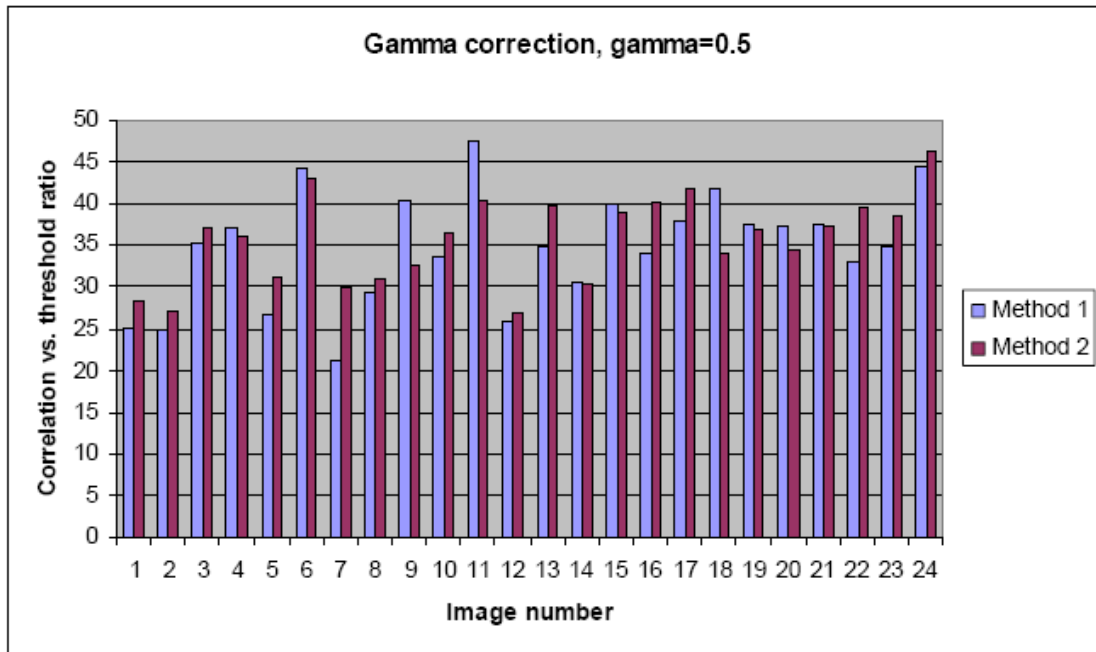


Fig. 5.27(a): Raport corelație/prag, comparația robusteții în cazul corecției de gamma, $\gamma=0.5$

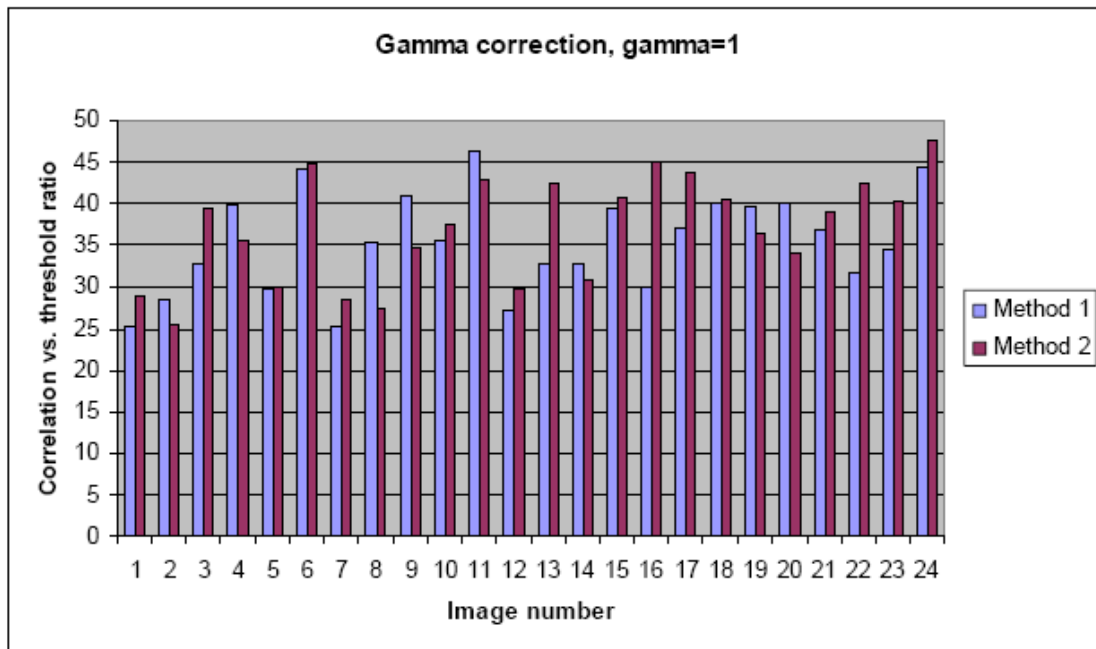


Fig. 5.27(b): Raport corelație/prag, comparația robusteții în cazul corecției de gamma, $\gamma=1$

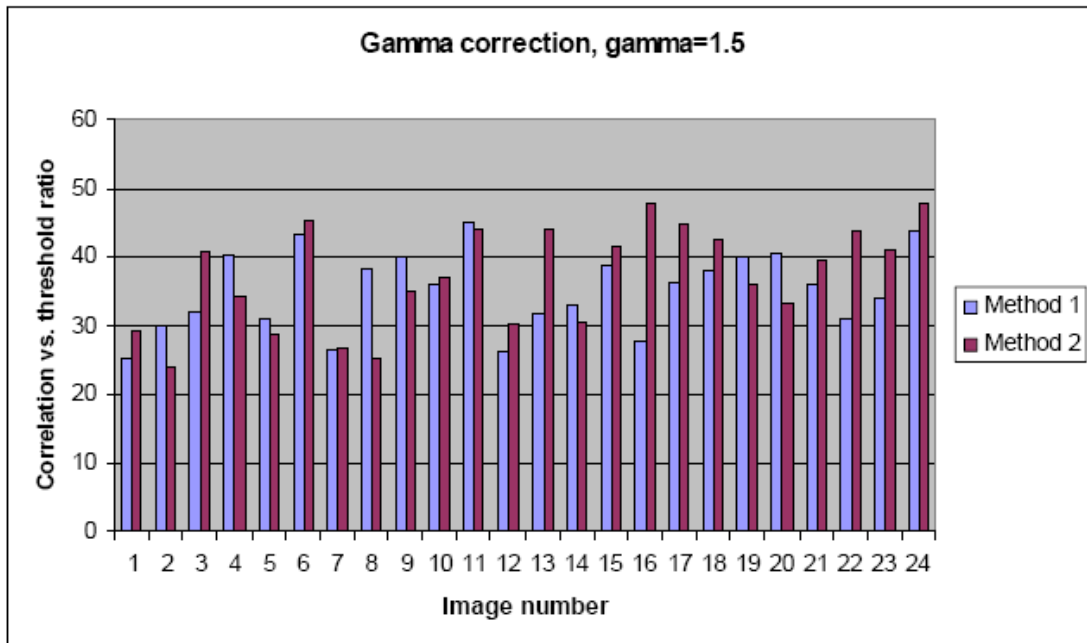


Fig. 5.27(c): Raport corelație/prag, comparația robusteții în cazul corecției de gamma, $\gamma=1.5$

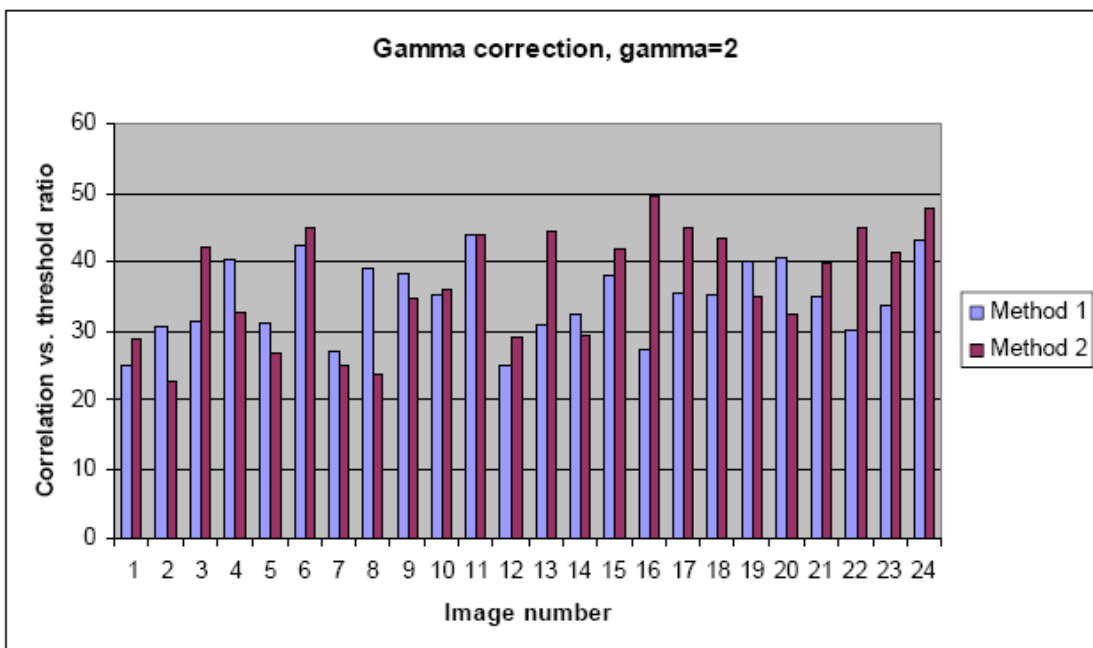


Fig. 5.27(d): Raport corelație/prag, comparația robusteții în cazul corecției de gamma, $\gamma=2$

Tab. 5.8: Raport corelație/prag, comparația robusteții în cazul decupării. Intensitatea maximă de marcarea este dată de constrângerea de invizibilitate [Naf07a].

<i>Imagine</i>	256x256		128x128		64x64		32x32	
	1	2	1	2	1	2	1	2
IM1	14.11	15.62	8.61	5.15	3.19	2.39	1.61	0.90
IM2	12.86	11.94	5.46	4.79	2.46	1.61	1.29	0.50
IM3	17.68	14.82	8.23	6.71	3.67	2.75	1.61	1.16
IM4	15.82	13.64	7.42	5.79	2.62	2.62	1.21	1.04
IM5	14.14	13.92	7.38	6.23	3.40	2.69	1.60	1.36
IM6	18.08	14.60	8.01	5.11	3.92	2.13	1.85	0.79
IM7	10.56	13.98	4.74	7.38	1.99	3.56	0.83	1.51
IM8	15.17	10.56	6.68	3.21	2.18	2.26	1.05	1.33
IM9	18.32	13.72	8.23	6.01	3.53	2.42	1.80	0.97
IM10	15.66	15.44	8.21	7.04	3.48	2.78	2.13	0.83
IM11	18.59	13.82	8.48	6.15	3.38	2.63	1.52	1.04
IM12	16.15	13.81	6.97	6.09	2.50	2.79	1.08	1.00
IM13	16.32	16.41	7.30	6.64	2.84	2.90	1.48	1.26
IM14	15.72	15.02	7.53	5.72	2.45	2.46	1.30	1.18
IM15	14.64	13.37	5.57	6.02	1.62	2.19	0.76	0.81
IM16	13.33	11.24	6.59	5.35	2.65	2.50	1.02	1.07
IM17	14.95	13.34	6.22	5.96	2.18	2.96	0.93	1.21
IM18	13.97	14.48	6.57	5.43	2.23	2.29	1.00	0.80
IM19	15.41	14.52	6.95	6.45	2.44	2.60	1.04	0.87
IM20	15.46	14.18	6.51	6.13	2.62	2.63	1.05	1.00
IM21	14.15	13.54	6.09	5.13	2.68	2.03	1.06	0.99
IM22	11.87	11.54	5.52	4.87	1.78	3.17	0.79	1.00
IM23	14.55	13.52	6.19	6.64	3.17	2.31	1.09	0.96
IM24	15.69	14.18	6.63	6.32	2.01	2.64	0.94	0.78

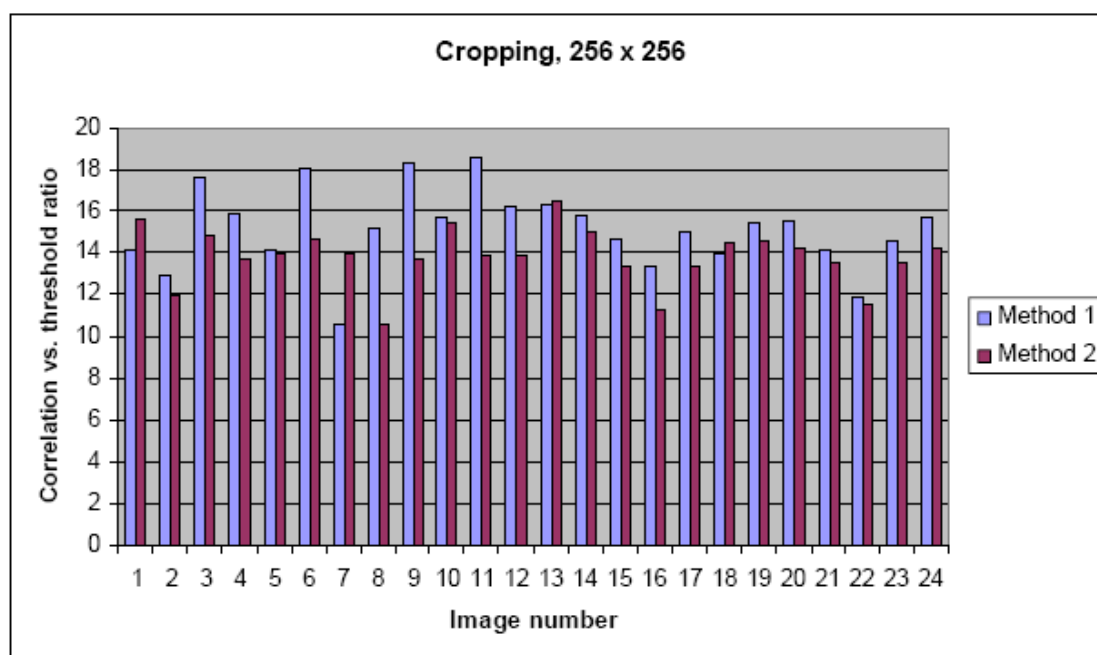


Fig. 5.28(a): Raport corelație/prag, comparația robusteții în cazul decupării 256x256

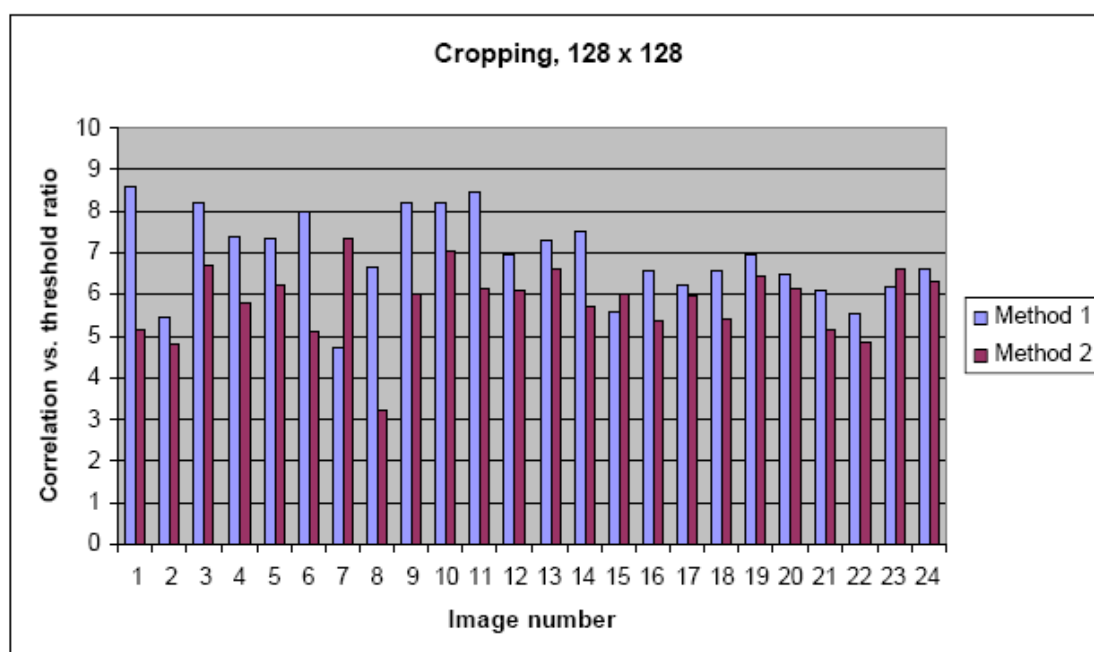


Fig. 5.28(b): Raport corelație/prag, comparația robusteții în cazul decupării 128x128

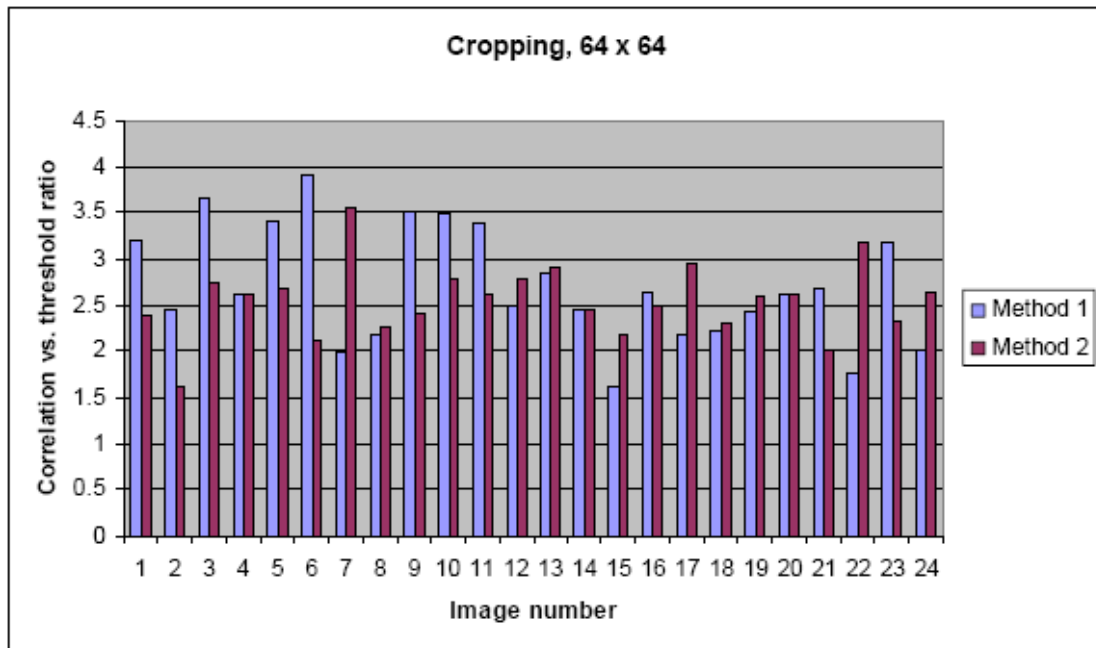


Fig. 5.28(c): Raport corelație/prag, comparația robusteții în cazul decupării 64x64

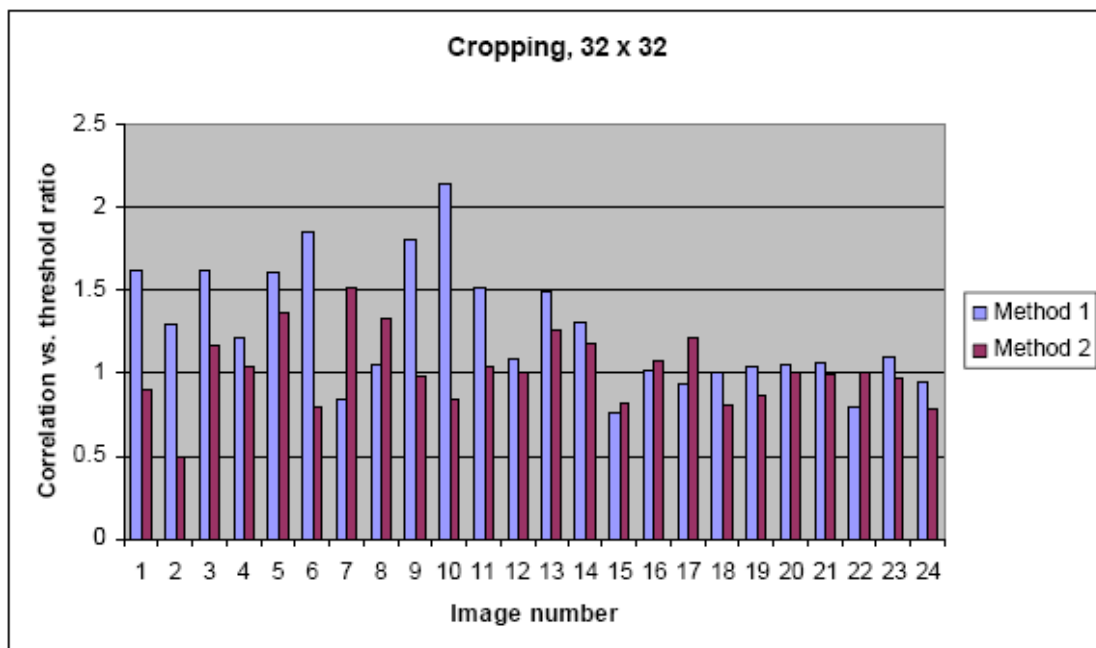


Fig. 5.28(d): Raport corelație/prag, comparația robusteții în cazul decupării 32x32

5.8 Înserare în toate subnivelele de rezoluție

În acest paragraf, se investighează folosirea mascării perceptuale prezentată mai sus pentru înserarea marcajului în **toate subnivelele** de rezoluție [Naf07b]. Sunt folosite trei detectoare care folosesc avantajele descompunerii multirezoluție a transformării wavelet. Marcajul este detectat din: 1) toate nivelele de rezoluție, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, și 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Evaluarea corelațiilor pe nivele de rezoluție, respectiv subbandă, este câteodată avantajoasă. De exemplu pentru decupare, marcajul este mai greu de detectat în frecvențe joase decât înalte, pe când filtrarea trece-jos afectează frecvențele înalte. Astfel, se elimină nivelele sau subbenzile de rezoluție cu corelație mică similar cu abordarea din [PZ98]. Acest tip de înserare combinat cu noile detectoare face algoritmul mai rezistent la atacuri gen ștergerea tuturor celor trei subbenzi care conțineau marcajul în nivelul zero. În [BBP01] detecția este făcută așa cum am văzut în paragrafele anterioare, folosind coeficientul de corelație pentru nivelul $l = 0$:

$$\rho(l) = \frac{4^l}{3MN} \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \tilde{w}_l^\theta(i, j) x_l^\theta(i, j) \quad (5.15)$$

Autorii au făcut presupuneri simplificatoare asupra variabilelor aleatoare. Valorile marcajului $x_l^\theta(i, j)$ sunt variabile aleatoare binare, de medie nulă. Este făcută o presupunere realistă privind coeficienții wavelet, aceea că sunt variabile aleatoare gaussiene, statistic independente, de medie nulă. Conform teoremei limită centrală, $\rho(l)$ este de asemenea presupusă a fi distribuită normal. Fiind dată o imagine și un marcaj, sunt posibile numai trei cazuri:

- A. Imaginea nu este marcată
- B. Imaginea este marcată cu o secvență Y alta decât X.
- C. Imaginea este marcată cu secvența căutată, și anume X.

Astfel există două ipoteze:

- H₀**: Marcajul căutat nu este înserat în imaginea recepționată, incluzând cazul A și B,
- H₁**: Marcajul adevărat este inserat în imaginea recepționată, deci cazul C.

Printr-o analiză simplă autorii [BBP01] arată că în ambele ipoteze, H₀ și H₁, corelațiile sunt normal distribuite și mediile lor sunt:

$$\mathbf{H}_0: \mu_{\rho(l)_0} = 0.$$

$$\mathbf{H}_1: \mu_{\rho(l)_1} = \frac{4^l}{3MN} \alpha \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E[w_l^\theta(i, j)].$$

Un marcaj X este prezent dacă $\rho(l) > T_{\rho(l)}$. Probabilitatea de fals pozitiv (de detecție

a marcajului când nu există) este $P_{fp} = \text{Prob} \left\{ \rho(l) > T_{\rho(l)} \middle| H_0 \right\}$. Pentru a estima

această probabilitate, în [BBP01] sunt calculate dispersiile pentru corelațiile din cazul A și B:

$$\begin{aligned} \sigma_{\rho(l)_A}^2 &= \left(\frac{4^l}{3MN} \right)^2 \sigma_x^2 \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E \left[\left(I_l^\theta(i,j) \right)^2 \right] \\ \sigma_{\rho(l)_B}^2 &= \left(\frac{4^l}{3MN} \right)^2 \sigma_x^2 \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} E \left[\left(I_l^\theta(i,j) \right)^2 \right] \\ &\quad + \alpha^2 \sigma_x^2 E \left[\left(w_l^\theta(i,j) \right)^2 \right] \end{aligned}$$

Cazul B este cazul cel mai nefavorabil, cu cât este mai mare varianța cu atât mai mare este probabilitatea de eroare. Corelația este comparată cu pragul $T_{\rho(l)}$, calculat pentru a da o probabilitate de detecție falsă (fals pozitiv), folosind criteriul Neyman-Pearson [Kay03]:

$$P_{fp} \leq \frac{1}{2} \text{erfc} \left(\frac{T_{\rho(l)}}{\sqrt{2\sigma_{\rho(l)_B}^2}} \right)$$

Spre exemplu, dacă $P_{fp} \leq 10^{-8}$, pragul este:

$$T_{\rho(l)} = 3.97 \sqrt{\sigma_{\rho(l)}^2},$$

cu $\sigma_{\rho(l)}^2$ dispersia coeficienților wavelet, dacă imaginea a fost marcată cu un marcaj

Y altul decât X:

$$\sigma_{\rho(l)}^2 \approx \left(\frac{4^l}{3MN} \right)^2 \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \left(\tilde{I}_l^\theta(i,j) \right)^2 \quad (5.16)$$

Considerăm raportul dintre corelație $\rho(l)$ din relația (5.15) și pragul dependent de imagine $T_{\rho(l)}$, ca și în cazurile precedente. Urmărind același raționament din [BBP01], primul detector evaluează prezența marcajului în toate nivelele de rezoluție:

$$d_1 = \frac{\rho_{d1}}{T_{d1}} \quad (5.17)$$

unde corelația este:

$$\rho_{d1} = \frac{1}{3MN \sum_{l=0}^2 4^{-l}} \sum_{l=0}^2 \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \tilde{I}_l^\theta(i,j) x_l^\theta(i,j) \quad (5.18)$$

și pragul este determinat pentru $P_{fp} \leq 10^{-8}$:

$$T_{d1} = 3.97 \sqrt{\sigma_{\rho_{d1}}^2} \quad (5.19)$$

$$\sigma_{\rho_{d1}}^2 \approx \frac{1}{\left(3MN \sum_{l=0}^2 4^{-l}\right)^2} \sum_{l=0}^2 \sum_{\theta=0}^2 \sum_{i=0}^{M/2^l-1} \sum_{j=0}^{N/2^l-1} \left(\tilde{I}_l^\theta(i,j)\right)^2 \quad (5.20)$$

În general, coeficienții wavelet sunt considerați a fi variabile aleatoare cu anumite densități de probabilitate, cum ar fi cea gaussiană. Astfel de modele statistice simple sunt necorespunzătoare pentru coeficienții wavelet dintr-o imagine naturală, deoarece nu sunt luate în considerare dependențele între coeficienți inter-scală și intra-scală [SS02]. Există interdependențe puternice între coeficienți vecini cum ar fi un coeficient, părintele (localizat adiacent la un nivel de rezoluție mai brut) și frați (localizați adiacent în spațiu).

Ignorând acest fapt, presupunem că există independența statistică a coeficienților wavelet de la nivele de rezoluție diferite și subbenzi diferite. Am trasat în acest scop histograma corelațiilor pentru imaginea Lena, și pentru imaginea marcată (Figura 5.29). Am efectuat testul Pearson chi-square pe ambele distribuții empirice; ipoteza gaussiană a fost acceptată la un prag de semnificație 0.05, nivel de încredere de 95% și am considerat că primul detector propus este valid [Naf07b].

Al doilea detector consideră răspunsurile detectoarelor de la diferite nivele, adică $d(l) = \rho(l)/T(l)$, cu $l \in \{0,1,2\}$, și le elimină pe cele cu valoare de detecție mai mică:

$$d_2 = \max_l \{d(l)\} \quad (5.21)$$

Al treilea detector consideră răspunsurile de la subbenzi și nivele diferite, ca fiind $d(l, \theta) = \rho(l, \theta) / T(l, \theta)$, cu $l, \theta \in \{0,1,2\}$, și le elimină pe cele cu valoare de detecție mai mică:

$$d_3 = \max_{l,\theta} \{d(l,\theta)\} \quad (5.22)$$

Corelațiile și pragul sunt calculate folosind același raționament per subbandă, indicându-i orientarea și nivelul.

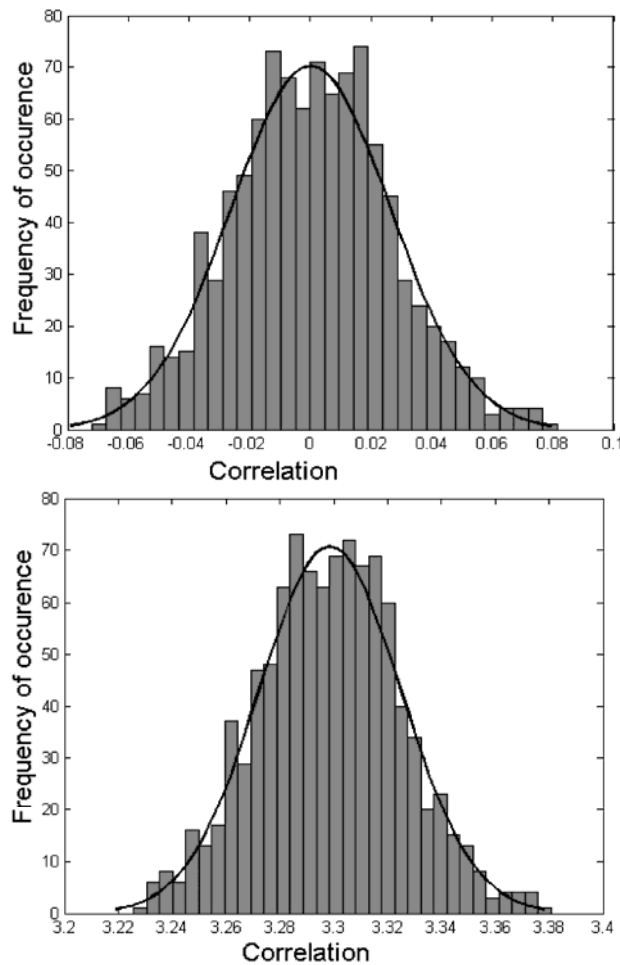


Fig.5.29: Distribuții empirice ale corelațiilor pentru primul detector, sus, imaginea originală și jos, imaginea marcată cu $\alpha=1.5$, [Naf07b].

Rezultate obținute în urma simulărilor. Au fost marcate mai multe imagini de mărime 512×512 , de această dată la toate nivelele $l \in \{0,1,2\}$, folosind masca perceptuală prezentată. Intensitatea de marcare α a fost fixată la 1.5 în toate experimentele privind metoda propusă. Imaginile marcate sunt neafectate de procesul de marcare față de originale.

Pentru metoda din [BBP01] am inserat un marcaj în toți coeficienții de detaliu de la primul nivel de rezoluție, $l=0$, pentru $\alpha=0.2$, așa cum s-a discutat și în paragraful anterior. Aceasta rezultă într-adevăr într-o calitate similară a imaginilor, conform Fig. 5.30.

Ceea ce rămâne constant pentru comparare, sunt marcajele bidimensionale inserate în primul nivel, respectiv $x_0^\theta(i, j)$, precum și calitatea imaginii. Nu comparăm metoda din [Naf07b] cu cea din [BBP01] atunci când marcajul este inserat în toate nivelele de rezoluție, fiindcă masca lor nu este potrivită pentru inserare în alte nivele decât cel de rezoluție înaltă.



Fig.5.30: Imaginea originală Lena, precum și imaginile marcate pentru (stânga) metoda propusă [Naf07b], $\alpha=1.5$, PSNR=36.86 dB, (dreapta) metoda lui Barni și alții [BBP01], $\alpha=0.2$, PSNR=36.39 dB

Se prezintă rezultatele pentru unele imagini standard din baza de date USC-SIPI Image Database [USC], folosite și anterior. Tabelul 5.9 prezintă valorile PSNR pentru ambele cazuri. În fig. 5.31, se prezintă un grafic cu valorile PSNR pentru fiecare imagine, precum și o valoare medie per metodă.

Pentru primul detector, prezentăm de asemenea un estimat al probabilității de detecție falsă pentru imaginea Lena, înainte și după compresia JPEG cu factor de calitate $Q=10$, ca și funcție de pragurile de detecție, T_{ρ_1} . Valorile de prag au fost calculate folosind estimata dispersiei lui ρ_1 obținute în urma experimentelor.

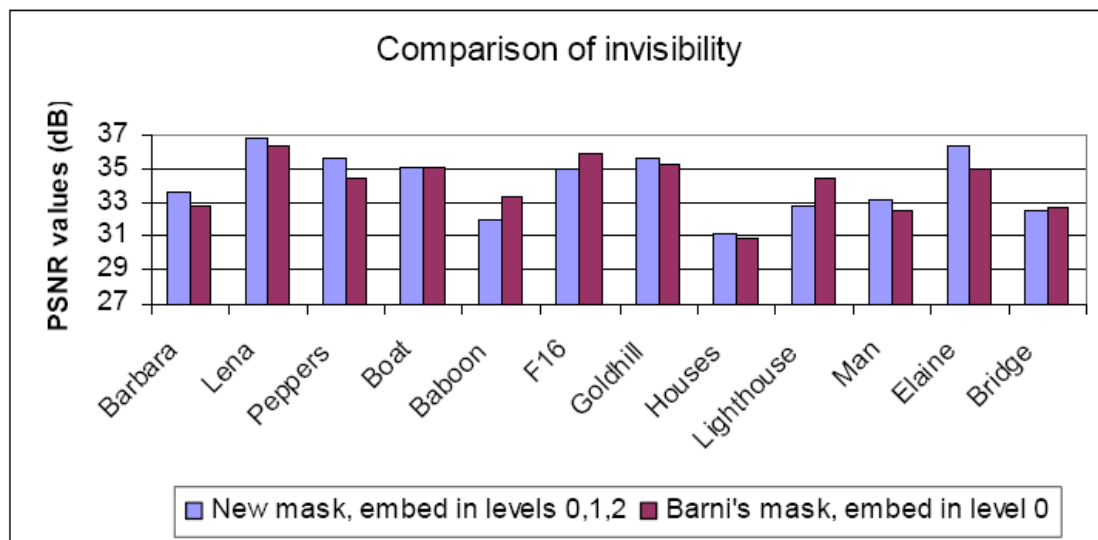
S-au efectuat teste folosind prelucrări de semnal obișnuite, compresie JPEG, filtrare mediană, decupare, redimensionare, corecție gamma și blurring. Pentru fiecare imagine atacată, și fiecare detector, sunt calculate valorile, d_i , pentru $i \in \{1,2,3\}$, raportul între corelație și pragul dependent de imagine. Probabilitatea de fals pozitiv este fixată la 10^{-8} . Tabelele 5.10 – 5.15 prezintă răspunsul detectoarelor pentru fiecare imagine, atac și metodă. Pentru o mai bună vizualizare a rezultatelor, prezentăm și grafice cu valorile corelațiilor în funcție de imagini pentru fiecare atac, precum și o valoare medie per detector.

Am ales parametrul atacului pentru care marcajul este încă detectabil cu cel puțin o metodă. La compresia JPEG, metoda propusă a detectat cu succes marcajul până la factorul de calitate 10. Primul detector este mai bun în toate cazurile.

Metoda propusă în [Naf07b] are rezultate mai bune decât tehnica lui Barni [BBP01].

Tab. 5.9. Comparație a invizibilității

<i>Image vs. PSNR (dB)</i>	<i>Metoda propusă</i>	<i>Metoda lui Barni și alții</i>
Barbara	33.68	32.83
Lena	36.86	36.39
Peppers	35.61	34.40
Boat	35.05	35.05
Baboon	32.01	33.33
F16	34.92	35.90
Goldhill	35.64	35.28
Houses	31.17	30.97
Lighthouse	32.79	34.38
Man	33.28	32.60
Elaine	36.35	34.98
Bridge	32.58	32.66

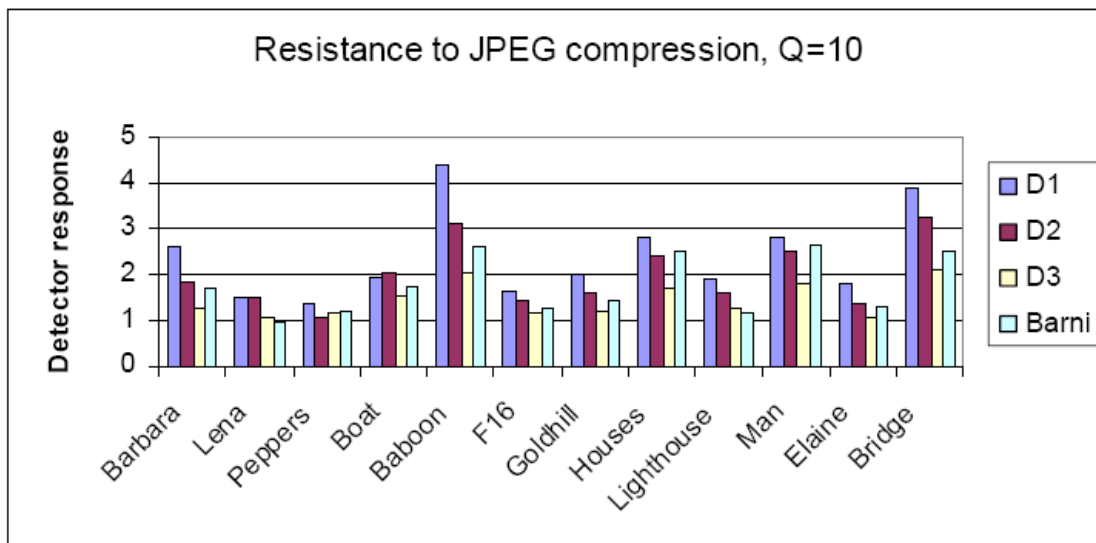


Metoda propusă	Metoda lui Barni
34,16 dB	34,06 dB

Fig. 5.31: Valori PSNR, comparația invizibilității, împreună cu valorile medii pentru cele două metode.

Tab. 5.10. Rezistența la compresia JPEG, $Q=10$

<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	2.61	1.87	1.27	1.71
Lena	1.50	1.51	1.04	0.97
Peppers	1.34	1.04	1.13	1.20
Boat	1.93	2.04	1.53	1.74
Baboon	4.39	3.11	2.06	2.58
F16	1.64	1.47	1.17	1.27
Goldhill	2.01	1.60	1.18	1.45
Houses	2.79	2.38	1.71	2.49
Lighthouse	1.89	1.62	1.24	1.13
Man	2.81	2.50	1.82	2.66
Elaine	1.78	1.37	1.06	1.31
Bridge	3.91	3.25	2.08	2.51



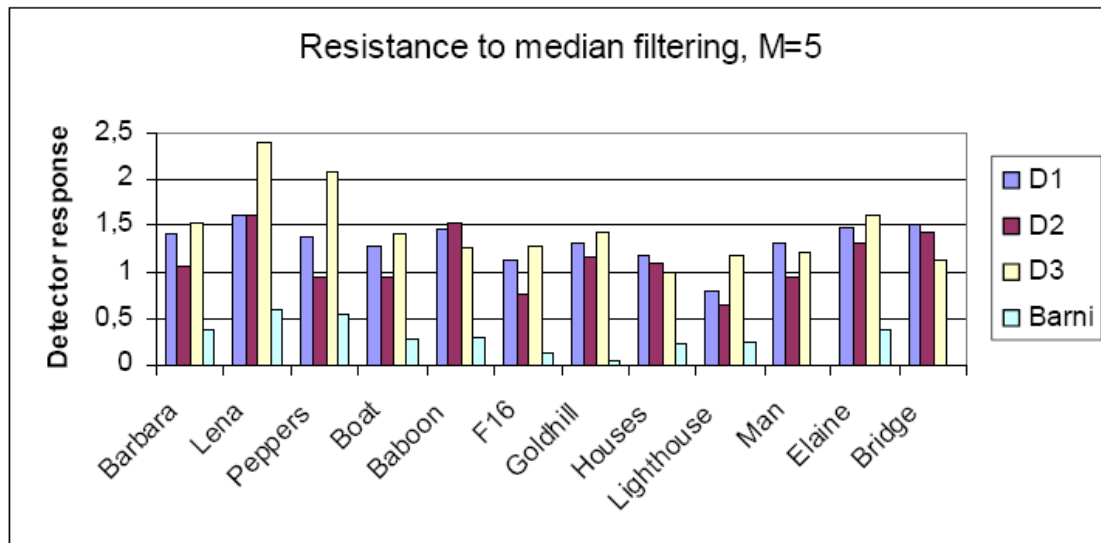
D1	D2	D3	Barni
2,38	1,98	1,44	1,75

Fig. 5.32: Raport corelație/prag, comparația robusteții în cazul compresiei JPEG, $Q=10$, împreună cu valorile medii pentru detectoare.

Pentru ambele metode, marcajul a supraviețuit în toate imaginile pentru filtrare mediană cu lungimea ferestrei filtrului până la 3. Pentru $M=5$, marcajul înserat cu metoda propusă în [Naf07b] folosind primul și al treilea detector poate fi recuperat, dar metoda lui Barni nu reușește să găsească marcajul.

Tab. 5.11. Rezistența la filtrare mediană, $M=5$

<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	1.41	1.06	1.53	0.38
Lena	1.60	1.60	2.40	0.59
Peppers	1.38	0.95	2.09	0.55
Boat	1.29	0.94	1.40	0.27
Baboon	1.45	1.53	1.27	0.29
F16	1.13	0.77	1.29	0.13
Goldhill	1.31	1.16	1.44	0.05
Houses	1.20	1.08	0.98	0.23
Lighthouse	0.78	0.65	1.19	0.24
Man	1.32	0.95	1.21	0.01
Elaine	1.49	1.32	1.60	0.36
Bridge	1.52	1.43	1.15	-0.02



D1	D2	D3	Barni
1,32	1,12	1,46	0,25

Fig. 5.33: Raport corelație/prag, comparația robusteții în cazul filtrării mediene, $M=5$, împreună cu valorile medii pentru detectoare.

În cazul redimensionării la 50%, marcajul a fost detectat cu succes în ambele cazuri, cu rezultate mai bune pentru metoda propusă [Naf07b]. Al treilea detector are o performanță mai bună.

Tab. 5.12. Rezistența la redimensionare, 50%

<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	3.94	4.50	3.26	2.11
Lena	4.13	5.86	6.01	2.31
Peppers	4.42	6.20	7.09	2.14
Boat	3.23	4.20	5.45	1.98
Baboon	4.74	4.89	4.73	2.13
F16	3.85	4.97	6.63	1.59
Goldhill	4.48	6.12	6.98	1.34
Houses	3.50	4.49	5.93	1.84
Lighthouse	3.15	3.87	6.00	1.29
Man	3.96	5.11	4.88	1.85
Elaine	4.78	6.53	6.62	1.99
Bridge	4.59	5.77	5.64	1.66

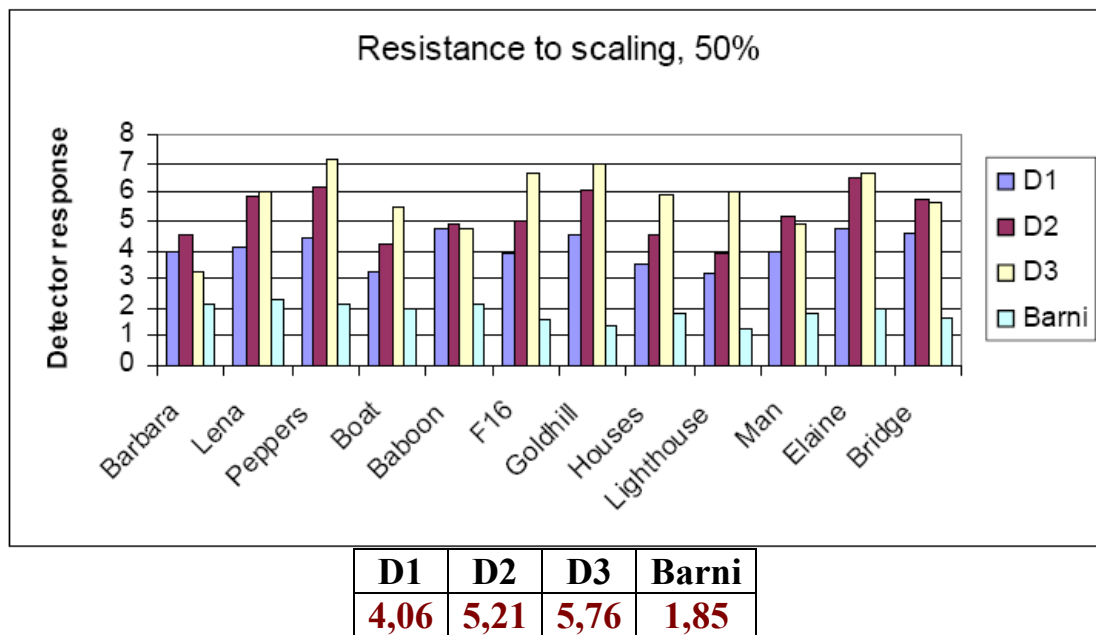


Fig. 5.34: Raport corelație/prag, comparația robusteții în cazul redimensionării, 50%, împreună cu valorile medii pentru detectoare.

Marcajul inserat cu metoda propusă a fost detectat cu succes până la imaginea decupată de mărime 32x32, numai cu al treilea detector, care îi dovedește eficiența. Metoda lui Barni detectează marcajul cu răspuns apropiat ca valoare ca și al treilea detector.

Tab. 5.13. Rezistența la decupare, 32x32

<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	0.36	0.44	1.48	1.29
Lena	0.85	1.06	1.87	1.85
Peppers	0.85	1.02	1.82	1.80
Boat	0.45	0.89	1.91	2.13
Baboon	0.87	0.98	1.90	1.61
F16	0.29	0.69	1.90	1.61
Goldhill	0.45	0.75	1.66	1.21
Houses	0.68	1.14	1.76	1.60
Lighthouse	0.54	1.06	2.32	0.83
Man	1.29	1.52	1.25	1.05
Elaine	0.51	0.95	1.57	1.52
Bridge	1.03	1.30	1.37	1.30

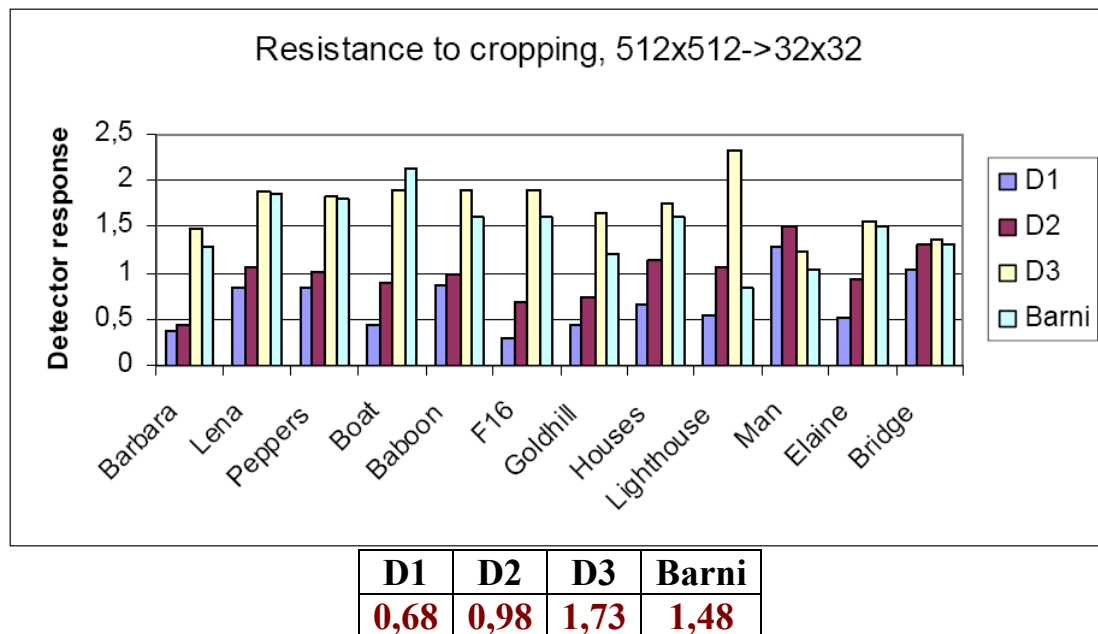
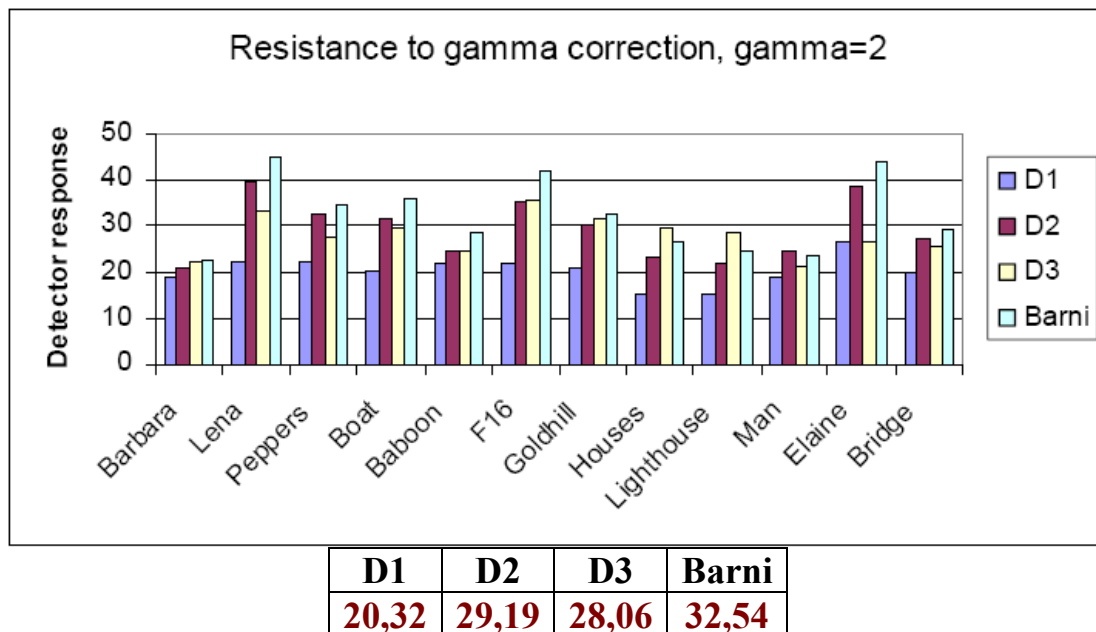


Fig. 5.35: Raport corelație/prag, comparația robusteții în cazul decupării, 32x32, împreună cu valorile medii pentru detectoare.

Așa cum era de așteptat pentru detectorul cu corelație normalizată, ambele metode sunt practic insensibile la corecția de gamma [Cox05].

Tab. 5.14. Rezistența la corecția de gamma, $\gamma=2$

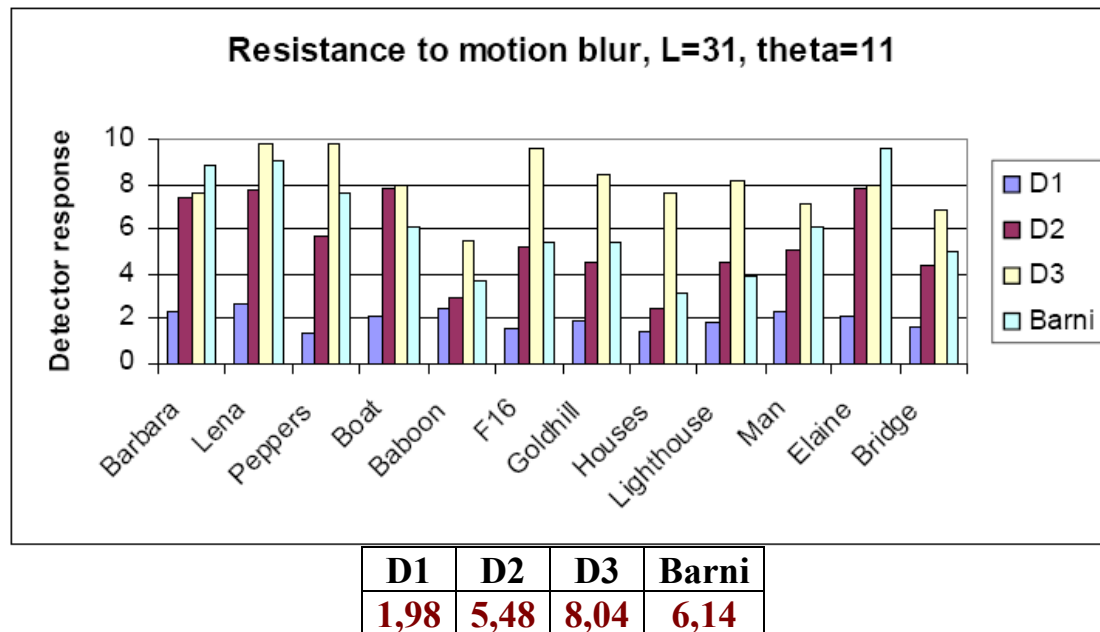
<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	18.72	20.57	22.11	22.67
Lena	22.41	39.62	32.97	44.81
Peppers	22.52	32.48	27.58	34.86
Boat	20.15	31.91	29.89	35.95
Baboon	21.76	24.92	24.67	28.80
F16	21.63	35.00	35.85	42.03
Goldhill	20.90	30.03	31.74	32.65
Houses	15.35	23.45	29.76	26.78
Lighthouse	15.37	21.65	28.47	24.81
Man	18.68	24.67	21.30	23.76
Elaine	26.77	38.83	26.70	44.00
Bridge	19.58	27.16	25.73	29.44

Fig. 5.36: Raport corelație/prag, comparația robusteții în cazul corecției de gamma, $\gamma=2$, împreună cu valorile medii pentru detectoare.

Pentru atacul de blur (încețoșare) de mișcare, ambele metode au detectat cu succes marcajul. Al treilea detector are rezultate ușor mai bune decât celelalte.

Tab. 5.15. Rezistența la blur de mișcare, $L=31$, $\theta=11$

<i>Imagine vs. Răspunsul detectorului</i>	<i>Metoda propusă</i>			<i>Metoda lui Barni</i>
	<i>d1</i>	<i>d2</i>	<i>d3</i>	
Barbara	2.33	7.47	7.62	8.86
Lena	2.69	7.78	9.77	9.05
Peppers	1.35	5.74	9.80	7.62
Boat	2.12	7.83	7.94	6.14
Baboon	2.40	2.92	5.56	3.66
F16	1.56	5.23	9.62	5.42
Goldhill	1.95	4.52	8.46	5.37
Houses	1.45	2.48	7.70	3.17
Lighthouse	1.88	4.53	8.17	3.86
Man	2.37	5.07	7.11	6.11
Elaine	2.12	7.84	7.94	9.55
Bridge	1.61	4.36	6.82	4.97

Fig. 5.37: Raport corelație/prag, comparația robusteții în cazul blur, $L=31$, $\theta=11$, împreună cu valorile medii pentru detectoare.

Pentru primul detector, am estimat probabilitatea de fals pozitiv căutând multe marcaje diferite într-o imagine marcată, Lena. Fiecare prag T_{p1} a fost calculat astfel încât P_{fp} să aibă o anumită valoare. Procedura a fost repetată pentru valori ale lui P_{fp} începând de la 10^{-1} până la 10^{-4} . În total am testat 5×10^4 marcaje per imagine. Estimarea a fost făcută înainte de orice tip de manipulare și după compresia JPEG, cu factor de calitate 10.

Valoarea estimată a probabilității de fals pozitiv, P_{fp} este prezentată în figura 5.38 în funcție de raportul $T_{\rho 1} / \sigma_{\rho 1B}$ dintre pragurile de detecție și deviația standard a corelațiilor din cazul B, corespunzătoare unui anumite valori teoretice a probabilității de fals pozitiv.

Surprinzător, valoarea estimată a acestei probabilități P_{fp} , este mai mică după compresie decât înainte de orice atac pentru același prag de detecție. Acest lucru poate fi explicat prin faptul că înainte de compresie, distribuția empirică a corelațiilor în cazul B (un alt marcaj este inserat în imagine), nu este gaussiană. Deși cele două distribuții sunt mai apropiate după atac, sunt foarte bine separate și distribuția empirică pentru un marcaj incorect are media sub zero, comparativ cu cazul anterior, unde era centrată pe zero (fig. 5.39 și 5.40). Astfel pentru un prag fix, aceasta duce într-adevăr la o probabilitate de fals pozitiv mai mică după atac. Rezultate similare au fost obținute pentru imaginea Barbara, la același atac.

Pentru primul detector, probabilitatea de fals pozitiv este apropiată de cea teoretică. Presupunerea anterioră, aceea că coeficienții wavelet de la diverse niveluri și subbenzi sunt variabile aleatoare statistic independente și distribuite identic este rezonabilă și deci detectorul va avea performanțe bune.

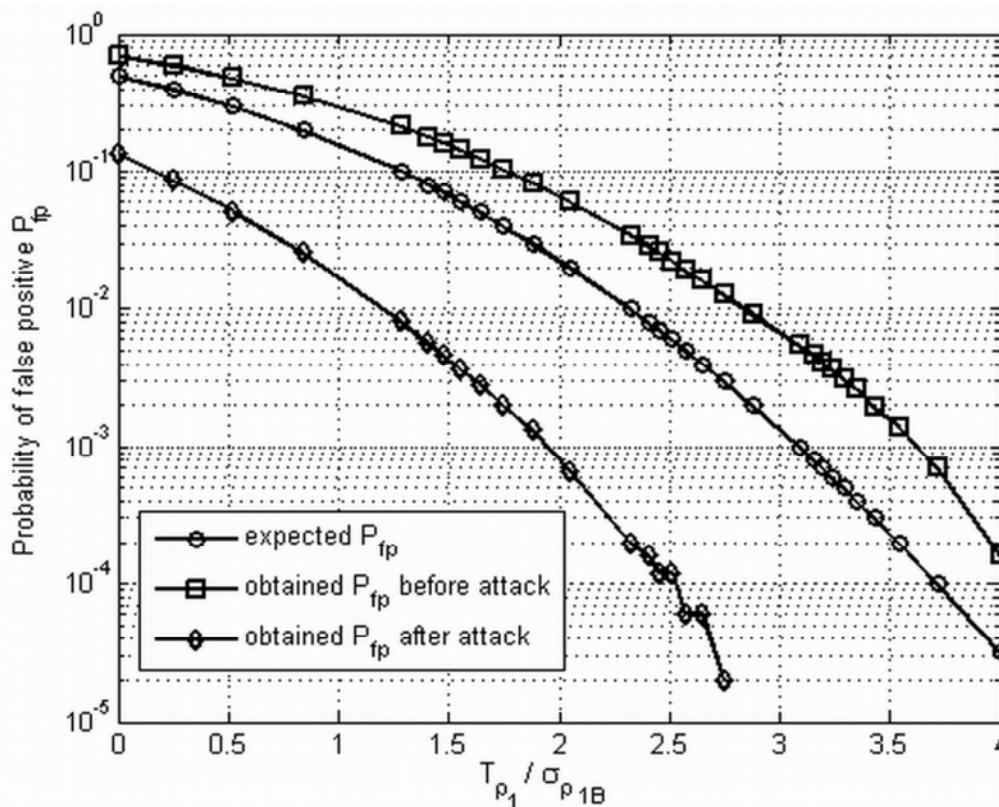


Fig. 5.38: Probabilitatea de fals pozitiv în funcție de raportul $T_{\rho 1} / \sigma_{\rho 1B}$ dintre pragurile de detecție și deviația standard a corelațiilor din cazul B (un alt marcaj este inserat în imagine). Valoarea teoretică este trasată cu simbolul „o”. Testele au fost efectuate pe imaginea Lena, înainte și după compresia JPEG cu factor de calitate 10, precum și 5×10^4 marcaje diferite.

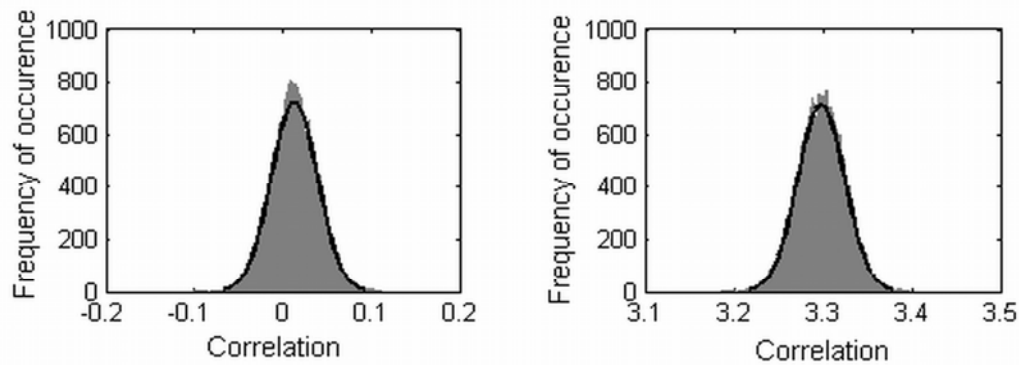


Fig. 5.39: Histogramele pentru corelațiile din cazul B (un alt marcaj este inserat în imagine), și cazul C (marcajul căutat este inserat în imagine), pentru imaginea Lena, înainte de atac. Au fost testate 5×10^4 marcaje diferite.

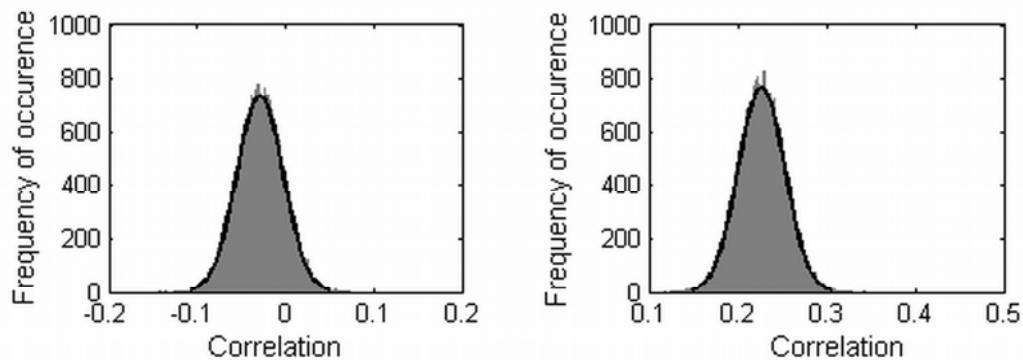


Fig. 5.40: Histogramele pentru corelațiile din cazul B (un alt marcaj este inserat în imagine), și cazul C (marcajul căutat este inserat în imagine), pentru imaginea Lena, după atacul prin compresie JPEG, factor de calitate 10. Au fost testate 5×10^4 marcaje diferite.

Concluzie. Am propus inserarea marcajului în toate nivelele de rezoluție a imaginii; acest lucru poate fi util spre exemplu în cazul ștergerii tuturor subbenzilor de frecvență înaltă care conțin marcajul în sistemul propus de Barni ș.a.[BBP01]. Detectorul nelinier cu prag fix ca raport între corelație și pragul dependent de imagine este din nou folosit. Propunem și evaluăm performanțele a trei detectoare a marcajului 1) din toate nivelele de rezoluție, 2) separat din fiecare nivel, considerând maximum răspunsurilor de pe nivele, și 3) separat din fiecare subbandă, considerând maximum răspunsurilor de pe subbenzi. Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare și filtrare mediană unde al treilea detector a arătat o performanță mai bună. Am testat metoda la diverse atacuri, și am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măștii perceptuale, și am folosit diversitatea transformării wavelet.

5.9 Concluzii

Am prezentat un tip nou de mascare perceptuală, construită pornind de la o metodă propusă de Barni ș.a.[BBP01]. Aceasta ascunde datele în toți coeficienții wavelet de detaliu, folosind o intensitate de marcarea variabilă, conform unei măști perceptuale.

Deși tehnica propusă în [BBP01] este una performantă, îmbunătățiri ale ei au fost propuse de mine în [NIB06a, NIB06b] exploatând superior caracteristicile sistemul vizual uman.

Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluție mai bună. Noul tip de mască perceptuală reușește să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviația standard locală a imaginii. Compresia wavelet a fost folosită pentru a obține imaginea de textură de aceeași mărime ca și marcajul.

O extensie a acestei metode este prezentată în [NIB06b]. În cadrul ei, marcajul se poate ascunde imperceptibil și în subbenzile de frecvență mai joasă.

Acest lucru aduce un nivel crescut de robustețe. Imaginea de luminanță este și ea estimată folosind o rezoluție mai bună, pe imaginea de aproximare de frecvență mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor și în nivele de rezoluție scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obținute sunt de interes practic, în special datorită faptului că marcajul poate fi inserat în frecvențe joase, de aici crescând și robustețea sistemului de marcare.

Am argumentat că nu ar trebui testată robustețea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute [Naf07a]. Ca și constrângere de invizibilitate, am folosit raportul maximal semnal-pe-zgomot, precum și modelul de mascare spațială din [Gir89]. Au fost testate două măști perceptuale pe un număr mare de imagini, respectiv cele prezentate anterior, [BBP01] și [NIB06a]. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradați din imaginea marcată să nu depășească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Acestea ne asigură că imaginile nu au fost vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare și corecție gamma).

Rezultatele simulării au arătat că impunând constrângerea de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode au fost comparabile și au detectat cu succes marcajul numai în cazul atacurile ușoare. Aceste rezultate au fost prezentate în [Naf07a].

În [Naf07b], am propus inserarea marcajului în toate nivelele de rezoluție ale imaginii; acest lucru poate fi util spre exemplu în cazul ștergerii tuturor subbenzilor de frecvență înaltă care conțin marcajul în sistemul propus de Barni și alții [BBP01]. Detectorul neliniar cu prag fix ca raport între corelație și pragul dependent de imagine este din nou folosit. Propunem și evaluăm performanțele a trei detectoare ale marcajului 1) din toate nivelele de rezoluție, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, și 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare și filtrare mediană unde al treilea detector a arătat o performanță mai bună. Am testat metoda la diverse atacuri, și am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măștii perceptuale, și am folosit diversitatea transformării wavelet. Trebuie menționat că rezultatele metodei [BBP01] au fost obținute folosind codul sursă oferit de unul dintre autori, Alessandro Piva.

Capitolul 6

Concluzii și contribuții personale

6.1 Concluzii

În **capitolul unu** am prezentat conceptele de bază ale marcării transparente și aplicațiile posibile. Am descris apoi etapele marcării: generarea marcajului, înglobarea și detecția marcajului. Au fost enumerate proprietățile metodelor de marcarea, precum și condițiile generale și specifice impuse. Dezvoltarea unei tehnici de marcarea ia în considerare mai multe aspecte, ce „împrumută” concepte din alte domenii de cercetare: steganografia, comunicațiile cu spectru împrăștiat (Spread Spectrum - SS), modelele perceptuale umane, autentificarea și criptarea, fuziunea datelor, transmisia semnalului în prezența fading-ului, estimarea canalului. Alegerea acestor elemente pentru o metodă de marcarea, pentru o aplicație dată, este încă o problemă nerezolvată, deoarece pentru anumite aplicații, trebuie făcut un compromis între imperceptibilitate, robustețe și complexitate. În continuare, am prezentat evaluarea performanțelor unei metode de marcarea, folosind diverse criterii imperceptibilitatea, raportul dintre puterea maximă a semnalului și puterea zgomotului PSNR, coeficientul de intercorelație, distanța Hamming normalizată, probabilitatea unui fals pozitiv sau negativ, complexitatea de calcul. Am tratat problema marcării robuste și soluțiile pentru asigurarea robusteții.

Capitolul 2 începe cu o clasificare a tehnicilor de marcarea, în funcție de diferite criterii și continuă cu stadiul actual al tehnicilor în funcție de domeniul de marcarea. Această a doua parte este mult mai vastă, tocmai din cauza multitudinilor abordărilor existente în literatură, care provin din domenii fundamentale ca prelucrarea semnalelor, teoria informației, etc.

Astfel, cele mai multe scheme de marcarea transparentă se bazează pe același principiu simplu, schimbarea redusă a valorii unor coeficienți aleși pseudoaleator în domeniul spațial sau al unei transformate. Aceste schimbări sunt apoi identificate folosind un corelator sau alte tehnici asemănătoare corelației. În mod normal, numărul de coeficienți modificați este mult mai mare decât numărul de biți de înserat. Aceasta poate fi considerată ca o marcarea redundantă și duce implicit la creșterea robusteții.

Domeniul de înserare al marcajului poate influența semnificativ robustețea marcajului. Metodele de marcarea în domeniul spațial sunt mai puțin robuste la atacuri de tip adăugare de zgomot sau compresie JPEG. Dar marcajul poate fi recuperat ușor dacă imaginea a fost decupată sau translatată. Acest avantaj este mai puțin evident în frecvență. Decuparea în domeniul spațial produce distorsiuni mari în domeniul spectral ceea ce duce de obicei la distrugerea marcajului. Același lucru este valabil și pentru transformata DCT aplicată pe toată imaginea. Dacă sunt marcate blocuri DCT, pentru o detecție cu succes este important să se cunoască poziția blocurilor în care a fost înserat marcajul. Domeniul wavelet are dezavantaje asemănătoare, deoarece transformarea nu este invariantă la translație sau rotație. Cele mai multe metode plasează marcajul în domeniul spațial, dar și numărul metodelor în domeniul DCT este mare.

În **capitolul 3**, am făcut o prezentare a celor mai cunoscute atacuri asupra sistemelor de marcarea transparentă, precum și a soluțiilor posibile pentru diminuarea efectelor acestora. În analiza performanțelor tehnicilor de marcarea transparentă, sunt folosite benchmark-urile (Stirmark, UnZign, Certimark, etc). În paralel cu dezvoltarea tehnicilor de marcarea transparentă, are loc și dezvoltarea unor noi atacuri. Este probabilă o cooperare a criptografiei cu tehnici moderne de prelucrarea semnalelor, domenii legate de obstrucționarea marcării transparente. Poate fi întrevăzută apariția unor atacuri noi care să îmbine tehnici de steganaliză cu atacuri din marcarea.

În **capitolul 4** am prezentat trei metode de marcarea informată [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05]. Acestea se bazează pe descompunerea multirezoluție a imaginii cu transformata wavelet discretă. Se fac schimbări asupra unor coeficienți wavelet, care nu vor avea un impact vizual asupra unui observator uman.

Coeficienții au fost selectați folosind o detecție cu logică de prag [NI03, NBK04, Naf04b, NB05, Naf05b]. Pragul depinde de coeficienții wavelet ai fiecărei imagini de detaliu. Marcajul este înserat în texturi și muchii ale imaginii folosind proprietățile sistemului vizual uman.

Prima metodă [NI03] înserează marcajul în subbanda de detalii diagonale al primului nivel de rezoluție, respectiv în toate subbenzile primului nivel; evident, deși a doua abordare afectează mai mult imaginea, marcajul se dovedește a fi mai robust la prelucrări obișnuite de semnal (compresie JPEG, filtrare mediană, zgomot AWGN). Metoda este comparată cu cea din [KH98]. Coeficientul de intercorelație pentru metoda propusă este mai mare decât pentru metoda propusă în [KH98], în cazul compresiei JPEG și zgomot alb gaussian aditiv. Cu toate acestea, metoda propusă nu prezintă robustețe împotriva filtrării mediane, comparativ cu metoda din [KH98].

A doua metodă înserează marcajul în cele trei nivele de rezoluție, exceptând imaginea de aproximare, folosind același fel de selecție a coeficienților wavelet. Detecția se face din **(1)** toate nivelele mediat, prin decizie majoritară, sau **(2)** din ultimul nivel de rezoluție, mai puțin afectat de diverse prelucrări de semnal.

Un **set preliminar de experimente** [Naf04a] face o comparație a metodei cu metoda de tip cuantizare prezentată în [KH98], și dovedește că metoda este mai robustă. Se observă că performanțele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelație este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluție. Acest lucru se datorează faptului că distorsiunile obișnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

Un **al doilea set de experimente** a fost efectuat folosind patru imagini; s-a făcut o comparație a metodei propuse [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox și alții este superioară în cazul atacului AWGN, comparabilă cu detectorul NC2 pentru compresia JPEG, și inferioară pentru filtrarea mediană. Aceste teste au fost efectuate, în cazul metodei [CKLS97], pentru imagini marcate puternic, imagini ce nu mai sunt, oricum, utile.

Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcare mai mică astfel încât imaginile să nu fie vizibil afectate de procesul de marcare pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensități și apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG și JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului și decupare. Metoda propusă funcționează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepții, când, oricum, marca nu este detectabilă în ambele cazuri (de exemplu, pentru, $\alpha=0.1$ și $\beta=0.01$ la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe și nu detectează marca în prezența celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10, decupare, redimensionare, filtrare mediană, ajustarea contrastului, compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanțe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleași rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru $\alpha=0.3$.

Răspunsurile detectoarelor, obținute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obținute pentru imaginile comprimate cu JPEG, evidențiindu-se astfel robustețea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α , cu atât sunt mai bune performanțele metodei [NB05]. Cu toate acestea există un *compromis între robustețe și invizibilitate*, pe baza căruia intensitatea de inserare ar trebui limitată la valoarea $\alpha=0.2$.

Pentru a doua metodă, s-au analizat **trei tipuri de detectoare** [NB05, Naf05b], care pot da rezultate diferite în funcție de atacul la care a fost supusă imaginea:

- 1. din toate nivelele de rezoluție, prin mediere, respectiv,
- 2. din ultimul nivel de rezoluție al transformatei, care poate fi afectat mai puțin de distorsiuni obișnuite ale semnalului,
- 3. prin **corelație maximă** cu marcajul căutat [Naf05b].

Este evident că al treilea detector este mai bun decât primele două, deoarece estimarea marcajului se face în funcție de marcajul original care este posibil inserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

A treia metodă propune o **abordare statistică** [NIB05], unde se selectează *mai puțini coeficienți wavelet* în care se înserează marcajul, deci numărul de repetiții este mai mic, față de metoda 2. Răspunsul detectorului este mai bun față de metoda a doua, deoarece coeficienții mari nu sunt atât de afectați de atacurile obișnuite (compresie, filtrare, etc.). Selecția pragurilor este bazată pe proprietățile statistice ale coeficienților wavelet. Aceleași detectoare sunt folosite ca și mai înainte.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare și ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN și la compresia JPEG2000.

Detectorul 3 are performanțe mai bune decât detectorul 1, în cazul majorității atacurilor, și performanțe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, și a ajustării contrastului. Pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 și 2, sunt detectate toate cele patru marcaje.

Performanțele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox și alții în [CKLS97] respectiv cu metoda propusă de Kundur și Hatzinakos [KH98]. Metoda a demonstrat o performanță mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT și a analizei statistice a coeficienților wavelet.

În **capitolul cinci**, am prezentat un tip nou de mascare perceptuală, pornind de la o metodă propusă de Barni ș.a.[BBP01]. Aceasta ascunde datele în toți coeficienții wavelet de detaliu, folosind o intensitate de mascare variabilă, conform unei măști perceptuale.

Deși tehnica propusă de aceștia este performantă, au fost propuse îmbunătățiri ale ei în [NIB06a, NIB06b], care țin seama mai bine de sistemul vizual uman. Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluție mai bună.

Noul tip de mască perceptuală reușește să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviația standard locală a imaginii. Compresia wavelet a fost folosită pentru a obține imaginea de textură de aceeași mărime ca și marcajul.

În continuare am prezentat o extensie a acestei metode [NIB06b], prin care marcajul se poate ascunde imperceptibil și în subbenzile de frecvență mai joasă. Acest lucru aduce un nivel crescut de robustețe. Imaginea de luminanță este și ea estimată folosind o rezoluție mai bună, pe imaginea de aproximare de frecvență mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor și în nivele de rezoluție scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obținute sunt de interes practic, în special datorită faptului că marcajul poate fi inserat în frecvențe joase, de aici rezultând și creșterea robusteții sistemului de mascare.

Am argumentat că nu ar trebui testată robustețea unei metode, atâta timp cât criteriul (criteriile) de invizibilitate nu sunt satisfăcute [Naf07a]. Ca și constrângere de invizibilitate, am folosit raportul maximal semnal-pe-zgomot, precum și modelul de mascare spațială din [Gir89]. Au fost testate două măști perceptuale pe un număr mare de imagini, respectiv cele prezentate anterior, [BBP01] și [NIB06a]. Intensitatea de mascare a fost fixată astfel încât procentajul de pixeli degradați din imaginea marcată să nu depășească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Aceasta a indicat că imaginile nu au fost vizibil afectate de procesul de mascare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare și corecție gamma).

Rezultatele simulării au arătat că impunând constrângerea de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode au fost comparabile și au detectat cu succes marcajul numai în cazul atacurile ușoare. Aceste rezultate au fost prezentate în [Naf07a].

În [Naf07b], am propus inserarea marcajului în toate nivelele de rezoluție a imaginii; acest lucru poate fi util spre exemplu în cazul ștergerii tuturor subbenzilor de frecvență înaltă care conțin marcajul în sistemul propus de Barni și alții [BBP01]. Detectorul neliniar cu prag fix ca raport între corelație și pragul dependent de imagine este folosit din nou. Propunem și evaluăm performanțele a trei detectoare ale marcajului:

- 1) din toate nivelele de rezoluție,
- 2) separat din fiecare nivel, considerând maximum răspunsurilor de pe nivele, și

3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi.

Aceasta a fost avantajos pentru atacuri precum decupare, redimensionare și filtrare mediană unde al treilea detector a arătat o performanță mai bună. Am testat metoda la diverse atacuri, și am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măștii perceptuale, și am folosit diversitatea transformării wavelet.

Trebuie menționat că rezultatele metodei [BBP01] au fost obținute folosind codul sursă oferit de unul dintre autori, Alessandro Piva.

6.2 Contribuții personale

1. O primă contribuție personală este legată de clasificarea și aprecierea critică a metodelor de marcarea transparentă și a atacurilor și este prezentată în capitolele doi și trei. Marea diversitate a materialelor publicate în literatura de specialitate, numărul foarte mare de metode de marcarea și atac raportate în literatură au făcut analiza deosebit de dificilă. Ea se întinde pe 70 de pagini și volumul ei este justificat de afirmațiile precedente. Am organizat în așa fel capitolele doi și trei încât, în varianta electronică a tezei, cititorul poate consulta fiecare titlu bibliografic citat, pentru a-și face o părere proprie despre cele scrise de mine. Consider că trebuie depuse în continuare eforturi, pentru “a face ordine” printre multitudinea de metode de marcarea și atac care provin din teoria semnalelor, teoria informației, criptare, ș.a.

O concluzie personală, rezultată în urma analizei efectuate este faptul că marcarea în domeniul transformatei wavelet este o cale promițătoare mai ales dacă îmbracă o formă adaptivă. Acesta este motivul pentru care în activitatea mea în domeniu am investigat mai ales o astfel de cale.

În capitolele 4 și 5 am prezentat aproape exclusiv contribuțiile mele personale, pe care le pot numi originale. Acestea își propun să răspundă la câteva întrebări de interes practic pentru domeniu, cum ar fi:

(A) Unde este de preferat să se însereze marcajul (în domeniul spațial sau în domeniul unei transformate) pentru a obține o marcarea cât mai robustă ? ;

(B) În care dintre nivelurile de descompunere ale DWT este mai bine să se însereze marcajul (în toate, în cele de rezoluție inferioară sau în cele de rezoluție superioară) pentru a obține o marcarea cât mai robustă ? ;

(C) În care dintre subbenzile DWT este mai bine să se însereze marcajul pentru a obține o marcarea cât mai robustă ?;

(D) Ce arhitectură de detector asigură cea mai bună extragere a marcajului ?

(E) Cum să se facă marcarea perceptuală ?

Aceste contribuții sunt prezentate în continuare dintr-o perspectivă istorică, care coincide în general și cu creșterea robusteții inserării marcajului. Ele se bazează pe simularea metodelor corespunzătoare în Matlab și pe compararea rezultatelor obținute astfel cu cele ale celor mai bune metode raportate în literatură.

2. Oferă răspunsuri pentru întrebările (B), (C). Am elaborat o primă metodă de marcarea informată (capitolul 4) prezentată în [NI03] care înserează marcajul în

subbanda de detalii diagonale al primului nivel de rezoluție, respectiv în toate subbenzile primului nivel; evident, deși a doua abordare afectează mai mult imaginea, marcajul se dovedește a fi mai robust la prelucrări obișnuite de semnal (compresie JPEG, filtrare mediană, zgomot AWGN). Metoda este comparată cu cea din [KH98]. Coeficientul de intercorelație pentru metoda propusă de mine este mai mare decât pentru metoda propusă în [KH98], în cazul atacului de tip compresie JPEG și de tip zgomot alb gaussian aditiv. Cu toate acestea, metoda propusă de mine nu prezintă robustețe împotriva filtrării mediane, comparativ cu metoda din [KH98].

3. Oferă răspunsuri la întrebările (A), (B), (C), (D). Am elaborat o a doua metoda de marcarea informată (capitolul 4) care înserează marcajul în cele trei nivele de rezoluție, exceptând imaginea de aproximare, folosind același fel de selecție a coeficienților wavelet. Detecția se face din (1) toate nivele prin decizie majoritară, sau (2) din ultimul nivel de rezoluție, mai puțin afectat de diverse prelucrări de semnal.

3a. Oferă răspunsuri la întrebările (B), (C) și (D). Un set de experimente [Naf04a] face o comparație a metodei propuse de mine, cu metoda de tip cuantizare prezentată în [KH98], se dovedește că metoda mea este mai robustă. Se observă că, în general, performanțele metodei propuse [Naf04a] sunt superioare metodei din [KH98]. De asemenea, coeficientul de intercorelație este mai mare dacă extragerea marcajului se face numai din ultimul nivel de rezoluție. Acest lucru se datorează faptului că distorsiunile obișnuite ale semnalului sunt mai semnificative pentru componentele spectrale mai înalte ale imaginii.

3b. Oferă răspunsuri la întrebarea (A). Un al doilea set de experimente a fost efectuat folosind patru imagini; s-a făcut o comparație a metodei propuse de mine [Naf04b] cu cea de tip spread-spectrum prezentată în [CKLS97]. Aparent metoda lui Cox și alții este superioară în cazul atacului AWGN, comparabilă cu detectorul meu NC2 pentru compresia JPEG, și inferioară pentru filtrarea mediană. Dar aceste teste au fost efectuate în cazul metodei [CKLS97] pe imagini marcate puternic.

3c. Oferă răspunsuri la întrebările (A), (B), (C) și (D). Al treilea set de experimente [NB05] ia în considerare acest aspect, selectând intensitatea de marcarea mai redusă, astfel încât imaginile să nu fie vizibil afectate de procesul de marcarea pentru metoda din [CKLS97]. Imaginea Peppers este marcată cu diverse intensități și apoi prelucrată cu diverse atacuri, compresie cu pierderi (JPEG și JPEG2000), zgomot AWGN, redimensionare, filtrare mediană, ajustarea contrastului și decupare. Metoda propusă de mine funcționează mai bine decât cea a lui Cox, pentru toate atacurile, cu mici excepții, când, oricum, marca nu este detectabilă în ambele cazuri (de exemplu, pentru, $\alpha=0.1$ și $\beta=0.01$ la ajustarea contrastului). De fapt, rezultatele pentru metoda lui Cox sunt mult mai slabe și nu detectează marca în prezența celor mai multe atacuri (compresie JPEG cu rata de compresie mai mare decât 10, decupare, redimensionare, filtrare mediană, ajustarea contrastului, compresie JPEG2000 cu rata de compresie mai mare de 10). Detectorul 2 are performanțe mai bune în cazul compresiei cu pierderi, filtrare mediană, rescalare, în timp ce detectorul 1 are rezultate mai bune pentru atacul AWGN.

În cazul decupării, cele două tipuri de detectoare au aceleași rezultate. În cazul ajustării contrastului, marcajul este detectat de ambele detectoare numai pentru $\alpha=0.3$.

Răspunsurile detectoarelor, obținute pentru imaginile comprimate cu JPEG2000, sunt mult mai mari decât cele obținute pentru imaginile comprimate cu JPEG, evidențiindu-se astfel robustețea marcajului inserat în domeniul DWT.

Cu cât este mai mare intensitatea de marcare α , cu atât sunt mai bune performanțele metodei mele [NB05]. Cu toate acestea există un *compromis între robustețe și invizibilitate*, pe baza căruia intensitatea de înserare ar trebui limitată la valoarea $\alpha=0.2$.

4. Răspunde la întrebările (A) și (D). Pentru detecția marcajului la metoda a doua (capitolul 4) am analizat trei tipuri de detectoare, dintre care al treilea este original [NB05, Naf05b]. Aceste detectoare dau rezultate diferite în funcție de atacul la care a fost supusă imaginea. Ele decid în funcție de informația:

- 1. din toate nivelurile de rezoluție, prin mediere,
- 2. din ultimul nivel de rezoluție al transformatei, care poate fi afectat mai puțin de distorsiunile obișnuite ale semnalului,
- 3. obținută prin corelația maximă cu marcajul căutat [Naf05b]. Acest detector este original.

Este evident că al treilea detector este îmbunătățit față de primele două, deoarece estimarea marcajului se face în funcție de marcajul original care este posibil înserat în imagine. Cu alte cuvinte, marcajul rezultat este cel mai asemănător cu cel original.

5. Răspunde la întrebările (B), (C), (D) și (E). În [NIB05], (capitolul 4), am propus o abordare statistică în cadrul căreia se selectează *mai puțini coeficienți wavelet* în care se înserează marcajul, deci numărul de repetiții este mai mic, dar răspunsul detectorului este mai bun în al doilea caz, deoarece coeficienții mari nu sunt atât de afectați de atacurile obișnuite (compresie, filtrare, etc.). Selecția pragurilor este bazată pe proprietățile statistice ale coeficienților wavelet. Se folosesc aceleași detectoare menționate la contribuția anterioară.

Se observă că detectorul 2 are rezultate mai bune pentru compresia cu pierderi, filtrare mediană, redimensionare și ajustarea contrastului, în timp ce detectorul 1 are rezultate mai bune la atacul AWGN și la compresia JPEG2000.

Detectorul 3 are performanțe mai bune decât detectorul 1, în cazul majorității atacurilor, și performanțe comparabile cu detectorul 2, sau chiar mai bune în cazul filtrării, redimensionării, decupării, și a ajustării contrastului. Pentru atacul de coliziune, cu medierea a patru imagini marcate cu marcaje diferite, în cazul detectoarelor 1 și 2, sunt detectate toate cele 4 marcaje.

Performanțele metodelor propuse [NI03, NBK04, Naf04b, NB05, Naf05b, Naf05a, NIB05] au fost comparate cu cele ale metodei propuse de Cox și alții în [CKLS97], respectiv cu metoda propusă de Kundur și Hatzinakos [KH98]. Metoda mea a demonstrat o performanță mai bună în cazul tuturor atacurilor, în special din cauza utilizării transformatei DWT și a analizei statistice a coeficienților wavelet.

6. Răspunde la întrebările (B), (C), (D) și (E). Am prezentat (capitolul 5), un tip nou de mascare perceptuală, pornind de la o metodă propusă de Barni și alții [BBP01]. Aceasta ascunde datele în toți coeficienții wavelet de detaliu, folosind o intensitate de marcare variabilă, conform unei măști perceptuale.

Deși tehnica propusă de aceștia este performantă, au fost propuse de mine îmbunătățiri ale ei în [NIB06a, NIB06b] ținând seama mai bine de caracteristicile

sistemului vizual uman. Într-o primă fază, tehnica din [NIB06a] estimează textura folosind o rezoluție mai bună.

Noul tip de mască perceptuală reușește să ascundă datele mai bine, datorită estimării mai precise a texturii. Imaginea de textură este calculată folosind deviația standard locală a imaginii. În acest sens metoda este una adaptivă. Compresia wavelet a fost folosită pentru a obține imaginea de textură de aceeași mărime ca și marcajul.

7. Răspunde la întrebările (B), (C), (D) și (E). O extensie a acestei metode (capitolul 5), este cea din [NIB06] în care marcajul se poate ascunde imperceptibil și în subbenzile de joasă frecvență. Acest lucru aduce un nivel crescut de robustețe. Imaginea de luminanță este și ea estimată folosind o rezoluție mai bună, pe imaginea de aproximare de frecvență mai înaltă. De asemenea sensibilitatea la zgomot este mărită. Această mască perceptuală permite inserarea imperceptibilă a datelor și în nivele de rezoluție scăzută, cum ar fi nivelul 1.

Imaginile marcate folosind masca propusă de mine în [NIB06a, NIB06b] au fost testate la compresia JPEG. Rezultatele obținute sunt de interes practic, în special datorită faptului că marcajul poate fi inserat în frecvențele joase, crescând astfel și robustețea sistemului de marcare.

Lucrarea citată, [NIB06b] a fost publicată în Springer-Verlag. Ca urmare a recunoașterii faptului că am adus o contribuție în domeniu, am fost nominalizată ca recenzor la *IEEE Transaction on Information Forensics and Security*, la *IEEE Transaction on Multimedia*, precum și la *EURASIP Journal on Information Security*.

8. Răspunde la întrebările (B), (C), (D) și (E). Am argumentat (capitolul 5), că nu ar trebui testată robustețea unei metode, atâta timp cât nu sunt satisfăcute criteriile de invizibilitate. Ca și constrângere de invizibilitate, am folosit raportul maxim semnal-pe-zgomot, precum și modelul de mascare spațială din [Gir89]. Au fost testate pe un număr mare de imagini două măști perceptuale, respectiv cele prezentate anterior, [BBP01] și [NIB06a]. Intensitatea de marcare a fost fixată astfel încât procentajul de pixeli degradați din imaginea marcată să nu depășească în medie 25%, iar valorile PSNR au fost în jur de 35 dB. Astfel am asigurat ca imaginile să nu fie vizibil afectate de procesul de marcare.

Cele două seturi de imagini marcate au fost supuse la diferite tipuri de atacuri (compresie JPEG, filtrare mediană, redimensionare, decupare și corecție gamma).

Rezultatele simulării au arătat că impunând constrângerea de invizibilitate bazată pe modelul lui Girod [Gir89], cele două metode dau rezultate comparabile și au detectat cu succes marcajul numai în cazul atacurile ușoare. Aceste rezultate au fost prezentate în [Naf07a].

9. Răspunde la întrebările (B), (C), (D) și (E). În [Naf07b], (capitolul 5), am propus inserarea marcajului în toate nivelele de rezoluție ale imaginii; acest lucru poate fi util spre exemplu în cazul ștergerii tuturor subbenzilor de frecvență înaltă care conțin marcajul în sistemul propus de Barni și alții [BBP01]. Este din nou folosit detectorul neliniar cu prag fix, ca raport între corelație și pragul dependent de imagine. Am propus și evaluat performanțele a trei detectoare ale marcajului: 1) din toate nivelele de rezoluție, 2) separat din fiecare nivel, considerând maximul răspunsurilor de pe nivele, și 3) separat din fiecare subbandă, considerând maximul răspunsurilor de pe subbenzi. Aceste detectoare au fost avantajoase pentru atacuri precum decupare, redimensionare și filtrare mediană unde al treilea detector a arătat o

performanță mai bună. Am testat metoda la diverse atacuri, și am arătat că este mai bună decât cea prezentată în [BBP01]. Comportarea metodei [Naf07b] poate fi explicată prin faptul că am folosit un estimat mai bun al măștii perceptuale și am folosit diversitatea transformării wavelet. Rezultatele celor trei detectoare pot fi fuzionate ameliorându-se în continuare procesul de extragere a marcajului.

Lucrarea citată, [Naf07b] a fost apreciată. Ea compară rezultatele mele cu cele ale echipei Barni, Bartolini și Piva și arăt în ea că rezultatele mele sunt superioare. În consecință această metodă reprezintă rezultatul final al tezei de doctorat. O recunoaștere indirectă a venit chiar de la Mauro Barni, la recomandarea căruia am devenit recenzor și la *Institution of Engineering and Technology Information Security, IET IFS*.

Lucrarea [NBK04] a fost citată de către Bao Zheng, Zhang Jian-wei, Xia De-Shen, Dong Bing, Gao Shang-bin, în lucrarea *Image adaptive Watermarking Algorithm based on Zero Tree Structure of Wavelet Transform*, în *Computer Engineering and Applications*, 2006, Vol. 42, No. 32, p.72-76, Wanfang Data, China.

Dizertația mea de master, *Filigranage dans le domaine des ondelettes*, din 2004, [Naf04e] a fost citată în *Proceedings of World Academy of Science, Engineering and Technology*, vol. 17, Dec. 2006, ISSN 1307-6884, în lucrarea *A Watermarking System Using the Wavelet Technique for Satellite Images*, I. R. Farah, I. B. Ismail, M. B. Ahmed.

Lucrarea [Naf05b] a fost citată în Springer Verlag de către Xue-Quan Xu, Xian-Bin Wen, Yue-Qing Li, Jin-Juan Quan, în lucrarea *A New Watermarking Approach Based on Neural Network in Wavelet Domain*, *Advanced Intelligent Computing Theories and Applications with Aspects of Artificial Intelligence*, 2007, LNCS.

Mai amintesc că raportul meu “Studiul comportării la atacuri a imaginilor marcate transparent” a fost citat de revista care apare la adresa www.resursejuridice.ro care a dat și link-ul către acesta în octombrie 2007, mai precis <http://www.resursejuridice.ro/content/view/714/77/>.

De altfel, ca o concluzie, în viitor, eforturile pentru rezolvarea problemei de marcare cred că trebuie dirijate mai puțin spre domeniul tehnic și mai mult spre rezolvarea unor aspecte juridice ale folosirii mărcării. Fără o legislație adecvată, rezultatele obținute de cercetătorii din domeniile tehnice nu se pot aplica în practică.

Publicații proprii

*2007

- [[Naf07a](#)] **C. Nafornta**, “Robustness Evaluation of Perceptual Watermarks”, IEEE Int. Symposium on Signal, Circuits and Systems ISSCS 2007, 12-13 July 2007, Iasi, Romania.
- [[Naf07b](#)] **C. Nafornta**, “Atacuri asupra imaginilor marcate transparent”, Politehnica Publishing House, 2007, ISBN 978-973-625-414-7, 130 pag.
- [ANBI07a] I. Adam, **C. Nafornta**, J.M. Boucher, A. Isar, “A New Implementation of the Hyperanalytic Wavelet Transform”, IEEE Int. Symposium on Signal, Circuits and Systems ISSCS 2007, 12-13 July 2007, Iasi, Romania, in press.
- [ANBI07b] I. Adam, **C. Nafornta**, J.M. Boucher, A. Isar, “A Bayesian Approach of Hyperanalytic Denoising”, IEEE Int. Symposium on Intelligent Signal Processing WISP 2007, 3-5 Oct. 2007, Madrid, Spain.

*2006

- [[NIB06a](#)] **C. Nafornta**, A. Isar, M. Borda, “Pixel-wise masking for watermarking using local standard deviation and wavelet compression”, Scientific Bulletin of Politehnica Univ. of Timisoara, Trans. on Electronics and Communications, tom 51(65), fasc.2, pp. 146-151, ISSN 1583-3380.
- [[NIB06b](#)] **C. Nafornta**, A. Isar, M. Borda, “Improved Pixel-Wise Masking for Image Watermarking”, in Multimedia Content Representation, Classification and Security, September 11-13, 2006, Istanbul, Turkey, Lecture Notes in Computer Science, Springer-Verlag, 2006, pp. 90-97.
- [[Naf06](#)] **C. Nafornta**, “Cresterea securitatii retelelor de comunicatii de date prin autentificare bazata pe watermarking”, Research report for CNCSIS grant, type TD, code 47 no. 2930/2006.
- [IMNO06] A. Isar, S. Moga, **C. Nafornta**, M. Oltean, I. Adam, “Image Denoising Using Wavelet Transforms With Enhanced Diversity”, Proc. International Conference Communications 2006, Bucharest, June, 3-4, 2006, ISBN(10) 973-718-496-3, ISBN(13) 978-973-718-496-2, pp.161-164.

*2005

- [[Naf05a](#)] **C. Nafornta**, “Digital Watermarking in the Wavelet Domain”, Politehnica Publishing House, ISBN 973-625-236-1. 2005
- [[Naf05b](#)] **C. Nafornta**, “Improved Detection for Robust Image Watermarking”, Proc. of International Symposium on Signal, Circuits and Systems, ISSCS2005, Iasi, Romania, 14-15 July 2005, vol. 2, pp.473-476.
- [[Naf05c](#)] **C. Nafornta**, “Stadiul actual al tehnicilor de marcare transparentă a imaginilor”, Research report for CNCSIS grant, type TD, code 47 no. 34702/24.06.05

- [[Naf05d](#)] **C. Nafornita**, “Studiul comportarii la atacuri a imaginilor marcate transparent”, (Image Watermarking Attacks) Research Report for CNCSIS Grant, Type TD, Code 47, No. 34702/24.06.05.
- [[NB05](#)] **C. Nafornita**, M. Borda, “Multiple Embedding in Wavelet Subbands for Robust Image Watermarking”, Proc. of International Workshop on Spectral Methods and Multirate Signal Processing, SMMSP 2005, 200-22 June, Riga, Latvia.
- [[NIB05](#)] **C. Nafornita**, A. Isar, M. Borda, “Image Watermarking Based on the Discrete Wavelet Transform Statistical Characteristics”, IEEE EUROCON 2005 - The International Conference on “Computer as a Tool”, Nov. 21-24, 2005, Belgrade, Serbia & Montenegro.

***2004**

- [[NBK04](#)] **C. Nafornita**, M. Borda, A. Kane, “A Wavelet-Based Digital Watermarking using Subband Adaptive Thresholding for Still Images”, microCAD 2004, Miskolc, Hungary, 18 – 19 March 2004, pp. 87 - 92.
- [[Naf04a](#)] **C. Nafornita**, “Balizarea imaginilor Statice Folosind Transformata Wavelet Discreta”, Raport de Cercetare din Cadrul Grantului CNCSIS, de tip D, cod 47, numar 33385/29.06.04.
- [[Naf04b](#)] **C. Nafornita**, “A Wavelet-Based Watermarking for Still Images”, Buletinul Științific al UPT tom 49(63) Electronică și Telecomunicații, fascicula 2, 2004, pp. 126-131.
- [[Naf04c](#)] **C. Nafornita**, “Watermarking in the wavelet domain”, Research report for CNCSIS grant, type TD, code 47 no. 33385/29.06.04.
- [[Naf04d](#)] **C. Nafornita**, “Algoritmi robusti de marcare transparenta a imaginilor cu turbocoduri”, Research report for CNCSIS grant, type TD, code 47 no. 33385/29.06.04.
- [[Naf04e](#)] **Nafornita Corina**. “Filigranage dans le domaine des ondelettes”. Mémoire de diplôme pour obtenir le degré de M.Sc. Université Politechnica Timisoara, Faculté d’Electronique et Télécommunication. TIMISOARA-2004.

***2003**

- [[NI03](#)] **C. Nafornita**, A. Isar, “Digital Watermarking of Still Images Using the Discrete Wavelet Transform,” Scientific Bulletin of Politehnica University of Timisoara, Electronics and Telecommunications Trans., Tom 48(62), Fascicula 1, 2003, pp. 73-78.

Bibliografie

- [[AGP02](#)] N. Abdulaziz, A. Glass, K.K.Pang, "Embedding Data in Images Using Turbo-Coding", 6th Symposium on DSP for Communication Systems, 28-31 Jan. 2002, Univ. Of Wollongong, Australia.
- [AM03] F. Arnia, K. Munadi, "Improving Invisibility in DCT Domain Watermarking System Using Wavelet Based Image Fusion", Proc. of IECI Japan Workshop 2003, ISSN 1344-7491.
- [AM05] C. Adsumilli, S. K. Mitra, "Error Concealment in Video Communications Using DPCM Bit Stream Embedding", ICASSP 2005.
- [AP00] N.K.Abdulaziz, K.K. Pang, "Robust Data Hiding for Images", Proc. IEEE Communication Technology, ICCT 2000.
- [AP98] R. J. Anderson and F. Petitcolas, "On the limits of steganography," IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection), vol. 16, pp. 474-481, May 1998.
- [ASS02] I. Avcibas, B. Sankur, K. Sayood, "Statistical evaluation of image quality measures", Journal of Electronic Imaging / April 2002 / Vol. 11(2).
- [AWS01] A. Ambroze, G. Wade, C. Serdean, M. Tomlinson, Y. Stander, M. Borda, "Turbo Code Protection of Video Watermark Channel", IEE Proceedings Vision Image, *Signal Processing*, Vol. 148, No. 1, Feb. 2001, pp. 54-58.
- [BA99] A.P.Bradley, "A Wavelet Visible Difference Predictor", IEEE, Trans. On Image Processing, Vol.8, No.5, May 1999.
- [Bar03a] M.Barni et al., "What is the Future for Watermarking? (Part I)", IEEE Signal Processing Magazine, Sept. 2003, pp. 55-60.
- [Bar03b] M.Barni et al., "What is the Future for Watermarking? (Part II)", IEEE Signal Processing Magazine, Nov. 2003, pp. 53-57.
- [BB01] T. Băjenescu, M. Borda, "Securitatea în Informatică și Telecomunicații", editura Dacia, Cluj-Napoca, 2001.
- [BBC03] P. Bas, N. Le Bihan, J.-M. Chassery, "Color Image Watermarking Using Quaternion Fourier Transform", ICASSP 2003, April 2003, pp.III - 521-4, vol.3.
- [BBCL99] M. Barni, F. Bartolini, V.Capellini, A. Lippi, A. Piva, "A DWT-based Technique for Spatio-Frequency Masking of Digital Signatures", Security and Watermarking of Multimedia Contents, SPIE, Vol. 3657, pp. 31-39, San Jose, California, 23-29 Jan. 1999.
- [BBCP98a] M Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT Domain System for Robust Image Watermarking", Signal Processing (Special Issue on Watermarking), vol. 66, no.3, 1998.
- [BBCP98b] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. 5th IEEE Int. Conf. Image Processing ICIP'98, vol. I, Chicago, IL, Oct. 4-7, 1998, pp. 450-454.

- [BBCP98c] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci, "A M.A.P. identification criterion for DCT-based watermarking," in Proc. Europ. Signal Processing Conf. (EUSIPCO '98), Rhodes, Greece, Sept. 1998.
- [BBGH00] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, "Applications for Data Hiding", IBM Systems Journal, 39, 3&4, 2000, pp. 547-568.
- [BBP01] M. Barni, F. Bartolini, A.Piva; "Improved Wavelet-Based Watermarking through Pixel-Wise Masking," IEEE Transactions on Image Processing, Volume 10, Issue 5, May 2001, pp.783 – 791.
- [BBPS02] M. Barni, F. Bartolini, A.Piva, F. Salucco, "Robust Watermarking for Cartographic Images", EURASIP Journal on Applied Signal Processing, 2002:2, pp.197-208.
- [BCD98] P. Bas, J.-M. Chassery, F. Davoine, "Using fractal code to watermark images," in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998.
- [BCHL05] Poza Bill Clinton & Hillary, înlocuită cu Monica Levinsky, în varianta falsificată, autor C.-Y. Lin (originalul a apărut în ziarul Newsweek).
- [BGM95] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", Proc. SPIE, Storage and Retrieval for Image and Video Databases III, vol. 2420, San Jose, CA, Feb. 9-10, 1995, pp. 165-173.
- [BGML96] W. Bender, D. Gruhl, and N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, 35, 3&4, 1996, pp. 313-336.
- [BKZ98] Burgett, S.; Koch, E.; Zhao, J., "Copyright labeling of digitized image data", IEEE Communications Magazine, Vol. 36, Issue 3, March 1998, pp. 94 – 100.
- [BMM96] G.W. Braudaway, K.A. Magerlein, F. Mintzer, "Protecting publicly available images with a visible watermark," Proc. SPIE – Int. Soc.Opt. Eng., vol. 2659, pp.126 – 133, 1996.
- [BMM96b] G. W. Braudaway, K. A. Magerlein, and F. C. Mintzer, "Color correct digital watermarking of images," U.S. Patent 5 530 759, June 1996.
- [BMYY97] D. Benham, N. Memon, B.-L. Yeo, and M. Yeung, "Fast watermarking of DCT-based compressed images," in Proc. Int. Conf. Image Science, Systems, and Technology (CISST '97), Las Vegas, NV, June 1997, pp. 243–253
- [BN04] M.Borda, I. Naornita, "Digital Watermarking – Principles and Applications", Proc. of Int. Conf. Communications 2004, Bucharest, pp.41-54.
- [BP96a] A. Bors and I. Pitas, "Embedding parametric digital signatures in images," in EUSIPCO-96, Trieste, Italy, Sept. 1996.
- [BP96b] A.G. Bors, I. Pitas, "Image Watermarking Using DCT Domain Constraints", International Conference on Image Processing, ICIP 96.
- [BP98] A.G. Bors, I. Pitas, "Image Watermarking Using Block Site Selection and DCT Domain Constraints", Optics Express, Vol. 3, No. 12, pp. 512-522, Dec. 1998
- [BPGS01] F. Balado, F. Pérez-González, and S. Scalise, "Turbo Coding for Sample-Level Watermarking in the DCT Domain", Proc. of the IEEE Int. Conf. on Image Processing (ICIP), pp. 1003-1006, Thessaloniki, Greece, Oct. 2001.

- [BQM95] O. Bruyndonckx, J.-J. Quisquater, B. Macq, "Spatial method for copyright labeling of digital images", Proc. IEEE Nonlinear Signal Processing Workshop, 1995, pp.456-459
- [Bra97] G.W. Braudaway, "Protecting Publicly-Available Images with an Invisible Watermark," in Proc. ICIP 97, IEEE Int. Conf. on Image Processing, Santa Barbara, CA, Oct. 1997, pp. 524-531.
- [BRD95] F. Boland, J. O'Ruanaidh, C. Dautzenberg, "Watermarking digital images for copyright protection", Proc. of IEE Int. Conf. on Image Proc. and Its Applications, Edinburgh, 1995
- [BS95] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in Advances in Cryptology—Proc. CRYPTO '95 (Lecture Notes in Computer Science), vol. 963, Don Coppersmith, Ed. Berlin, Germany: Springer, 1995, pp. 452–465
- [BS98] Boneh, Dan and James Shaw, "Collusion-Secure Fingerprinting for Digital Data", IEEE Trans. on Information Theory, vol. 44, no. 5, pp. 1897-1905, Sept. 1998.
- [BTS05] A. Briassouli, P. Tsakalides, A. Stouraitis, "Hidden Messages in Heavy-Tails: DCT-Domain Watermark Detection Using Alpha-Stable Models", IEEE Trans. on Multimedia, Vol. 7, No. 4, August 2005, pp.700-715.
- [Car95] G. Caronni, "Assuring ownership rights for digital images," in Proc. VIS 95, Session "Reliable IT Systems," Vieweg, Germany, 1995.
- [CB01] D. Coltman, A.G. Bors, "Hierarchical Watermarking Depending on Local Constraints", IEEE, Int. Conf. on Image Processing, Thessaloniki, Greece,7-10, Oct. 2001.
- [CBD98] J.-M. Chassery, P. Bas, and F. Davoine, "Self-similarity based image watermarking," in Proc. Europ. Signal Processing Conf.(EUSIPCO '98), Rhodes, Greece, Sept. 1998
- [Cha02] D.V.S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," Proc. of 45th IEEE Midwest Symposium on Circuits and Systems, Tulsa, OK, August 2002, pp. 264-267.
- [Cha03] D.V.S. Chandra, On Block-based Image Watermarking, Proceeding (399) Signal and Image Processing – 2003.
- [CHOS98] T.-Y. Chung, M.-S. Hong, Y.-N. Oh, D.-H. Shin, S.-H. Park, "Digital Watermarking for Copyright Protection of MPEG2 Compressed Video", IEEE, 1998, pp.895-901.
- [CKLS95] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia", NEC Res. Institut., Princeton, NJ, Tech. Rep. 95-10, 1995.
- [CKLS96] I.J. Cox, J. Killian, T. Leighton and T. Shamoan, "Secure Spread Spectrum Watermarking for Images, Audio and Video", Proc. of ICIP, vol. 3, pp.243-246, 1996.
- [CKLS97] I. Cox, J. Killian, T. Leighton, T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, pp.1673-1687, 1997.
- [CKN04] P. Campisi, D. Kundur, A.Neri, "Robust Digital Watermarking in the Ridgelet Domain", IEEE, Signal Processing Letters, Vol. 11, No. 10, Oct. 2004, pp. 826-830.

- [CL02] A. Cohen, A. Lapidoth, "The Gaussian Watermarking Game", IEEE Trans. on Information Theory, Vol.48, No.6, 2002, pp. 1639-1667.
- [CL97] I. Cox, J.-P. M.G. Linnartz, "Public watermarks and Resistance to Tampering", Proc. IEEE, Int. Conf. on Image Processing, 1997.
- [CM02] I. Cox, M. Miller, "The first 50 years of electronic watermarking", Journal of Applied Signal Processing, 2002, 2, 126-132, 2002.
- [CM03] R. Chandramouli, N. Memon, "On Sequential Watermark Detection", Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery, IEEE Trans. on Signal Processing, 2003.
- [CM97] I. Cox, M. Miller, "A Review of Watermarking and the Importance of Perceptual Modeling", Proc. SPIE Human Vision and Elect. Imaging II, vol. SPIE, vol. 3016, Feb. 1997.
- [CM98] J.J. Chae, B.S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", Proceedings of the SPIE EI'98, vol. 3312, pp.308-317, San Jose, Feb. 1998.
- [CMB02] I. Cox, M. Miller, J. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.
- [CMM98] J. J. Chae, D. Mukherjee, and B. S. Manjunath, "A robust data hiding technique using multidimensional lattices," Proc. Forum on Advances in Digital Libraries, Santa Barbara, California, pp. 319-26, 1998.
- [CMM99] I.J.Cox, M.L.Miller, A.L.MCKellips, "Watermarking as Communications with Side Information", Proc. of IEEE, vol. 87, No. 7, July 1999, pp. 1127-1141
- [CMYY98] S. Craver, N. Memon, B. Yeo, M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications", IEEE Journal On Selected Areas In Communications, Vol. 16, No. 4, May 1998.
- [Cos83] M. Costa, "Writing on Dirty-Paper" (Corresp.), IEEE Trans. on Information Theory, vol.29, no.3, May 1983, pp. 439- 441.
- [Cox05] I. Cox, "Robust Watermarking", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.
- [CPR01] J.Chou, S.S.Pradhan, K.Ramchandran, "Turbo Coded Trellis Based Constructions for Data Embedding: Channel Coding with Side Information", In Proc. of Asilomar Conf. on Signals, Systems and Computers, Pacific Grove (USA), Oct. 2001
- [CW01a] B. Chen, G. W. Wornell, "Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia", Journal of VLSI Signal Processing 27, 7-33, 2001.
- [CW01b] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans. on Information Theory, Vol. 47, No. 4, May 2001.
- [CW98] B. Chen and G. W. Wornell, "Digital Watermarking and Information Embedding Using Dither Modulation", IEEE Second Workshop on Multimedia Signal Processing, pp. 273-278, 1998.
- [CW99] B. Chen, G. W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", 1999, ISIT: Proceedings IEEE Int. Symposium on Information Theory.

- [DCP00] F. Deguillaume, G. Csurka and T. Pun, "Countermeasures for Unintentional and Intentional Video Watermarking Attacks", SPIE Electronic Imaging, San Jose, CA, January 2000.
- [Del04] E. Delp, "Multimedia security: the 22nd century approach", invited talk at ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, Sept.20-21, 2004.
- [DH76] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans. On Information Theory, vol. IT-22, No.6, November 1976.
- [Dir01] European Parliament, "Directive on the harmonisation of certain aspects of copyright and related rights in the information society", <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>, <http://europa.eu/scadplus/leg/en/lvb/l26021.htm>, 2001/29/EC, 22 May 2001
- [Dir04] European Parliament, "The Directive on the enforcement of intellectual and industrial property rights such as copyright and related rights, trademarks, designs or patents", http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_157/l_15720040430en00450086.pdf, 2004/48/EC, April 2004
- [DKL98] G. Depovere, T. Kalker, and J.-P. Linnartz, "Improved Watermark Detection Using Filtering Before Correlation", Proc. 5th IEEE Int. Conf. Image Processing ICIP'98, vol. I, Chicago, IL, Oct. 4-7, 1998, pp. 430-434.
- [DMCA98] U.S. Copyright Office Summary, "The Digital Millennium Copyright Act of 1998," Dec. 1998: <http://lcweb.loc.gov/copyright/legislation/dmca.pdf>
- [DRA98] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", ICIP 1998.
- [DS96] P. Davern and M. Scott, "Fractal based image steganography," in Lecture Notes in Computer Science: Information Hiding, vol.1174. Berlin, Germany: Springer, 1996, pp. 279-294.
- [EBTG02] J.J. Eggers, R. Bäuml, R. Tzschoppe and B. Girod, "Scalar Costa Scheme for Information Embedding", IEEE Transactions on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery, Vol. 51, No. 4, p. 1003-1019, 2002.
- [EKK99] F. Ergun, J. Killian, R. Kumar, "A Note on the Limits of Collusion-Resistant Watermarks", Eurocrypt'99, pp. 140-149, 1999.
- [EM00] Ejima, M., Miyazaki, A., "A wavelet-based watermarking for digital images and video", Proc. IEEE Int. Conf. Image Processing, 2000.
- [Fau93] O. Faugeras, "Three Dimensional Computer Vision: A Geometric Viewpoint", Cambridge, MA: MIT Press, 1993
- [FG99] J. Fridrich, M. Goljan, "Comparing Robustness of Watermarking Techniques", Proc. of SPIE, Vol. 3657, Security and Watermarking of Multimedia Content, San Jose, California, Jan. 25-27, 1999, pp. 214-225.
- [FH97] D.J. Fleet and D.J. Heeger, "Embedding Invisible Information in Color Images", Proc. ICIP 97, IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997.

- [FKK01] C. Fei, D. Kundur, R. Kwong, "The Choice of Watermarking Domain in the Presence of Compression", Proc. IEEE Int. Conf. on Information Technology: Coding and Computing, pp. 79-84, Las Vegas, Nevada, April 2001.
- [FKK04] C. Fei, D. Kundur, R. Kwong, "Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression", IEEE Trans. on Image Processing, Vol. 13, No. 2, Feb. 2004, pp. 126 – 144.
- [Fri99] J. Fridrich, "Key-Dependent Random Image Transform and Their applications in Image Watermarking", 1999 Int. Conf. on Imaging Science, Systems and Technology, CISST'99, Las Vegas, June 28-July 1, 1999, pp. 237-243.
- [Fri99b] Matlab implementation of Girod's model
<http://www.ws.binghamton.edu/fridrich/masking.html>
- [FS00] V. Fotopoulos, A.N. Skodras, "A Subband DCT Approach to Image Watermarking", X European Signal Processing Conference, Tampere, Finland, Sept.4-8, 2000.
- [GE04] E. Ganic, A. M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", ACM MM&SEC'04, September 20–21, 2004, Magdeburg, Germany.
- [Gir89] B. Girod, "The information theoretical significance of spatial and temporal masking in video signals", Proc. SPIE Human Vision, Visual Processing, and Digital Display, vol. 1077, pp. 178–187, 1989.
- [GZE03] E. Ganic, N. Zubair, A.M. Eskicioglu, "An Optimal Watermarking Scheme Based on Singular Value Decomposition", Proc. of the IASTED International Conference on Communication, Network, and Information Security (CNIS 2003), pp. 85-90, Uniondale, NY, December 10-12, 2003.
- [HAPG00] J.R. Hernández, M. Amado, F. Pérez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE Trans. on Image Processing, vol. 9, pp. 55-68, Jan. 2000.
- [HF02] L. Hua, J.E. Fowler, "A Performance Analysis of Spread-Spectrum Watermarking Based on Redundant Transform", Proc. of IEEE Int. Conf. on Multimedia and Expo, Lausanne, Switzerland, Aug. 2002, Vol. 2, pp. 553-556.
- [HG96] F. Hartung, B. Girod, "Digital Watermarking of Raw and Compressed Video", Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communications, Oct. 1996, pp. 205-213.
- [HG97] F. Hartung, B. Girod, "Fast Public-Key Watermarking of Compressed Video", Int. Conf. on Image Processing ICIP'97, Oct. 1997, Santa Barbara, California.
- [HG97b] F. Hartung, B. Girod, "Digital Watermarking of MPEG-2 Coded Video in the Bitstream Domain", Proc. ICASSP'97, Vol. 4, pp. 2621-2624.
- [HG98] F. Hartung, B. Girod, "Watermarking of Uncompressed and Compressed Video", Signal Processing 66 (1998) 283 – 301.
- [Hir96] K. Hirotsugu, "An image digital signature system with zkip for the graph isomorphism", Int. Conf. Image Processing, ICIP 1996, vol.3, pp.247-250.

- [[HK99](#)] F. Hartung, M. Kutter, "Multimedia Watermarking Techniques", Proc. IEEE, 87, 7, 1999, pp. 1079-1106.
- [[HLR00](#)] A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, and R.L. Lagendijk, "Image and Video Databases: Restoration, Watermarking and Retrieval", Advances in Image Communications, vol. 8, New York: Elsevier Science, 2000.
- [[HPG99](#)] J.R. Hernández, F. Pérez-Gonzalez, "Statistical Analysis of Watermarking Schemes for Copyright Protection of Images", Proceedings of the IEEE, 87(7):1142-1166, July 1999. Special Issue on Identification and Protection of Multimedia Information.
- [[HPGA98](#)] J.R. Hernández, F. Pérez-Gonzalez, M. Amado, "DCT-Domain Image Watermarking and Generalized Gaussian Models", Proc. of the COST #254 Int. Workshop on Intelligent Communications and Multimedia Terminals, pp. 23-26, Ljubljana, Slovenia, November 1998.
- [[HPGR98](#)] J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez, and G.Nieto, "Performance analysis of a 2-d multipulse amplitude modulation scheme for data hiding and watermarking still images," IEEE J. Select. Areas Commun., vol. 16, pp. 510-524, 1998.
- [[HPRP98](#)] A. Herrigel, H. Petersen, J. O Ruanaidh, T. Pun, and P. Shelby, "Copyright Techniques for Digital Images Based on Asymmetric Cryptographic Techniques", Workshop on Information Hiding, Portland, Oregon, USA, Apr. 1998.
- [[HRPP98](#)] A. Herrigel, J.J.K. Ó Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure Copyright Protection Techniques for Digital Images", Information Hiding, Lecture Notes in Computer Science, vol. 1525, D. Aucsmith, Ed. Berlin, Germany: Springer, 1998, pp. 169-190.
- [[HSG99](#)] F. Hartung, J.K. Su, B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks", Proc. SPIE, 3657, Security and Watermarking of Multimedia Contents, Jan. 1999.
- [[HTC00](#)] Shen-Fu Hsiao, Yor-Chin Tai, and Kai-Hsiang Chang, "VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking", IEEE Trans. Consumer Electronics, Vol. 46, No. 3, pp. 628-636, Aug. 2000.
- [[HW00](#)] C. Hsu, J. Wu, "Image Watermarking by Wavelet Decomposition", Academy of Information and Management Sciences Journal, Vol. 3, No.1, pp. 70-86, 2000.
- [[HW96](#)] C.-T. Hsu and J.-L. Wu, "Hidden Signatures in Images", Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 223-226.
- [[ICN02](#)] A. Isar, A. Cubitchi, M. Nafornta, "Algorithmes et techniques de compression", ed. Orizonturi Universitare, Timisoara, Romania, 2002, 181, 973-8391-38-5.
- [[IMK99](#)] H. Inoue, A. Miyazaki, T. Katsura, "An image Watermarking Method Based on the Wavelet-Transform", Proc. of ICIP, vol. 3, pp. 296-300, 1999.
- [[IML05](#)] A. Isar, S. Moga, X. Lurton, "A Statistical Analysis of the 2D Discrete Wavelet Transform", Proc. of the International Conference AMSDA 2005, May 17-20, 2005, Brest, France, pp. 1275-1281.

- [IN98] A. Isar, I. Nafornta, "Reprezentari Timp – Frecventa", Editura Politehnica, Timisoara, 1998.
- [Isa02] A. Isar, "Securitatea Transmiterii Informației pe INTERNET", 2002.
- [Jai81] A.K. Jain, "Image Data Compression: A Review", Proc. IEEE, vol. 69, pp. 349-389, Mar. 1981,
- [JSSK02] S. Joo, Y. Suh, J. Shin, H. Kikuchi, "A New Robust Watermarking Embedding into Wavelet DC Components", ETRI Journal, 24-25 Oct., 2002, pp. 401-404.
- [Kal01] T. Kalker, "Considerations on Watermarking Security", IEEE 4th Workshop on Multimedia Signal Processing, Cannes, France, 2001, pp.201-206.
- [Kal05] T. Kalker, "Digital Rights Management", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.
- [KAS05] P. Kumsawat, K. Attakitmongcol, A. Srikaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", IEEE Trans. Signal Processing, Vol. 53, No. 12, Dec. 2005, pp. 4707-4719.
- [Kay93] Steven M. Kay, "Fundamentals of Statistical Signal Processing: Detection Theory", Prentice Hall, 1993.
- [KD00] D. Kundur, "Water-Filling for Watermarking", Proc. IEEE Int. Conf. On Multimedia and Expo, New York, pp. 1287-1290, August 2000.
- [KD00b] D. Kundur, "Implications for High Capacity Data Hiding in the Presence of Lossy Compression", Proc. IEEE Int. Conf. On Info. Tech.: Coding & Comp, 2000.
- [KD05] D. Kundur, "Attacks Against Watermarking Schemes", (joint work with William Luh), ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 23, 2005.
- [KD05b] D. Kundur, "Authentication Watermarking", (joint work with Chuhong Fei and Raymond Kwong), ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 22, 2005.
- [KDHM99] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, "A Video Watermarking System for Broadcast Monitoring", Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, CA, Jan. 1999, pp. 103-112.
- [Ker01] Andrew D. Ker, "An Idea for Blind Watermarking Scheme Resistant to Stirmark", Programming Research Group Technical Report RR-01-14, Oxford University Computing Laboratory, 2001.
- [KH01] D. Kundur, D. Hatzinakos, "Diversity and Attack Characterization for Improved Robust Watermarking", IEEE Transactions on Signal Processing, Vol. 49, No. 10, 2001, pp. 2383-2396.
- [KH97] D. Kundur, D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," In International Conference on Image Processing, pp. 544-547, Santa Barbara, California, USA, Oct. 1997.
- [KH98] D. Kundur, D. Hatzinakos, "Digital Watermarking using Multiresolution Wavelet Decomposition", Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, Vol. 5, pp. 2969-2972, May 1998.

- [KH98b] D. Kundur, D. Hatzinakos, "Towards a Telltale Watermarking Technique for Tamper-Proofing", ICIP 1998.
- [KH99] D. Kundur, D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", Proc. IEEE, 87, 7, July 1999.
- [KH99b] D. Kundur, D. Hatzinakos, "Mismatching perceptual models for effective watermarking in the presence of compression", Proc. SPIE, Multimedia Systems and Applications II, September 1999.
- [KI01] S. Kay, E. Izquierdo, "Robust Content Based Image Watermarking", Proc. of Workshop on Image Analysis For Multimedia Interactive Services, WIAMIS 2001, Tampere, Finland, May 2001.
- [KJB97] M. Kutter, F. Jordan, F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation", Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, Feb. 1997, pp. 518-526.
- [KJB98] M. Kutter, F. Jordan, F. Bossen, "Digital signature of color images using amplitude modulation," J. Electron. Imaging, vol. 7, no. 2, pp. 326-332, Apr. 1998
- [KK04] D. Kundur, K. Kannan, "Video Fingerprinting and Encryption Principles for Digital Rights Management", Proceedings of the IEEE, Vol. 92, No. 6, June 2004, pp. 918-932.
- [KKK02] B. S. Kim, K. K. Kwon, S. G. Kwon, K. N. Park, K. N. Park, K. I. Song, K. I. Lee, "A Robust Wavelet-Based Digital Watermarking Using Statistical Characteristic of Image and Human Visual System", Proc. of ITC-CSCC 2002, vol 2. pp. 1019-1022.
- [KLD98] T. Kalker, J.P. Linnartz and M. van Dijk, "Watermark Estimation Through Detector Analysis", ICIP-98, October 1998.
- [KM99] J.R. Kim and Y.S. Moon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding", Proc. of IEEE ICIP, Vol. 2, Kobe, Japan, Oct. 1999, pp. 226-230.
- [KMKM00] M. Kesal, M. K. Mihcak, R. Koetter, and P. Moulin, "Iteratively Decodable Codes for Watermarking Applications", Proc. 2nd Int. Symp. on Turbo Codes and Related Topics, Sept. 2000, Brest, France
- [KMY04] D. Kirovski, H. Malvar, Y. Yacobi, "A Dual Watermark-Fingerprint System", IEEE Multimedia, 2004, pp.59-73
- [KP99] M. Kutter and F.A.P. Petitcolas, "A Fair Benchmark for Image Watermarking Systems", Proc. Electronic Imaging '99, Security and Watermarking of Multimedia Contents, vol 3657, San Jose, CA, Jan. 25-27, 1999, pp. 226-239.
- [KRR98] M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Content-based watermarking of images," in Proc. ACM Multimedia '98, Bristol, U.K., Sept. 1998.
- [KSLR99] S.W.Kim, S.Suthaharan, H.K. Lee, K.R.Rao, "Image Watermarking Scheme Using Visual Model and BN Distribution", Electronics Letters, 4th Feb. 1999, Vol. 35, N0. 3, pp. 212-214
- [Kun99] D. Kundur, "Multiresolution Digital Watermarking: Algorithms and Implications for Multimedia Signals", Ph.D. Thesis, Dept. of Electrical & Computer Engineering, University of Toronto, August 1999.

- [[Kut98](#)] M. Kutter, "Watermarking resisting to translation, rotation, and scaling," in Proc. SPIE Int. Symp. on Voice, Video, and Data Communication, Nov. 1998
- [[KZ95](#)] E. Koch, J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing (Neos Marmaras, Greece, June 20-22, 1995).
- [[LC05](#)] Q. Li, I. Cox, "Using Perceptual Models to Improve Fidelity and Provide Invariance to Valumetric Scaling For Quantization Index Modulation Watermarking", ICASSP 2005.
- [LD98] P. Linnartz and M. van Dijk, "Analysis of the sensitivity attack against electronic watermarks in images", in Proceedings of the 2nd Workshop on Information Hiding, Portland OR, April 15–17, 1998.
- [[LD99](#)] E.T. Lin, E.J. Delp, "A Review of Fragile Image Watermarks", Proc. of the Multimedia and Security Workshop (ACM Multimedia '99), Orlando, pp.25-29, 1999.
- [[LD99b](#)] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS '99), Savannah, GA, April 25-28, 1999, pp. 274-278.
- [LHL03] W-N Lie, T-L Hsu, G-S Lin, "Verification of Image Content Integrity by Using Dual Watermarking on Wavelets Domain", ICIP'2003, pp. 487-490.
- [[LK00](#)] P. Loo, N.G. Kingsbury, "Watermarking Using Complex Wavelets with Resistance to Geometric Distortion", The 10th European Signal Processing Conference (Eusipco2000), 5-8 Sept. 2000, Tampere, Finland.
- [[LK05](#)] W. Luh, D. Kundur, "New Paradigms for Effective Multicasting and Fingerprinting of Entertainment Media", IEEE Communications Magazine, June 2005, Vol. 43, No. 6, pp.77-84.
- [[LK92](#)] A.S. Lewis, G. Knowles, "Image Compression Using the 2-D Wavelett Transform", IEEE, Trans. on Image Processing, 1,2, April, 1992, pp. 244-250.
- [[LL01](#)] G.C. Langelaar, R.L. Lagendijk, "Optimal Differential Energy Watermarking of DCT Encoded Images and Video", IEEE Trans. On Image Processing, 10, 1, Jan. 2001.
- [[LLL97](#)] G.C. Langelaar, J.C.A. van der Lubbe, and R.L. Lagendijk, "Robust Labeling Methods for Copy Protection of Images", Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, Feb. 1997, pp. 298-309.
- [[LMT00](#)] T.-H. Lan, M. F. Mansour, A. H. Tewfik, "Robust High Capacity Data Embedding", ICIP 2000, pp. 581-584
- [[LOBL99](#)] C.H. Lee, H.S. Oh, Y. Baek, H.K. Lee, "Adaptive Digital Image Watermarking Using Variable Size of Blocks in Frequency Domain", 1999 IEEE TENCON, pp. 702-705.
- [LR00] T. Liang and J. Rodriguez, "Improved Watermarking Robustness Via Spectrum Equalization", Proc. IEEE ICASSP 2000, Istanbul, Turkey, June 5-9, 2000.

- [LSL00] G. C. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State-of-the-Art Overview", *IEEE Signal Processing Mag.*, vol. 17, no. 5, pp. 20–46, Sept. 2000.
- [LSL04] D.C. Lou, C.H. Sung, "Robust Watermarking Scheme for Digital Images Using Significant Coefficients and the De-Correlating Principle", *Journal of CCIT*, 32,2, May 2004.
- [LT02] R. Liu, T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", *IEEE, Trans. On Multimedia*, 4, 121-128, 2002
- [LWBC01] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, Y. M. Lui, "Rotation, Scale, and Translation Resilient Watermarking for Images", *IEEE Trans. On Image Processing*, 10, 5, May 2001.
- [LYC00] C.-Y. Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection", Ph.D. Thesis, Columbia University, 2000.
- [LYKM06] Z.Liu, H. Yu, D. Kundur, M. Merabdi, "On Peer-To-Peer Multimedia Content Acces and Distribution", *Proc. IEEE International Conference on Multimedia and Expo, Toronto, Canada, July 2006*.
- [Mal99] S. Mallat, "A Wavelet Tour of Signal Processing", Academic Press, 1999.
- [MB99] M.L. Miller, J.A. Bloom, "Computing the Probability of False Watermark Detection", *Proc. of Workshop in Information Hiding, Dresden, Germany, Sept. 29-Oct.1, 1999*.
- [MBM02] P.Moulin, A. Briassouli, H. Malvar, "Detection-Theoretic Analysis of Desynchronization Attacks in Watermarking", *Proc. DSP'02, Santorini, Greece, July 2002*.
- [MCB00] M.L. Miller, I.J. Cox, J.A. Bloom, "Informed Embedding: Exploiting Image and Detector Information during Watermark Insertion", *Int. Conf. on Image Proc., ICIP, 2000*.
- [MCM98] D. Mukherjee, J.J. Chae, and S.K. Mitra, "A source and channel coding approach to data hiding with application in hiding speech in video", *Proceedings of the IEEE International Conference on Image Processing, Chicago, IL, October 1998*.
- [MDC02] M.L. Miller, G.J. Doerr, I.J. Cox, "Dirty-Paper Trellis Codes for Watermarking", *IEEE Int. Conf. on Image Processing*, 2, pp. 129-132, 2002.
- [MF03] H. Malvar, D. Florencio, "Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking", *IEEE Trans. on Signal Processing*, Vol. 51, No. 4, April 2003, pp. 898-905.
- [MI03] P. Moulin, A. Ivanovic, "The Zero Rate Spread-Spectrum Watermarking Game", *IEEE Trans. on Signal Processing*, Vol. 51, No. 4, pp. 1098-1117, April 2003.
- [MK03] P. Moulin, R. Koetter, "Data Hiding—Theory and Algorithms", National University of Singapore, Institute for Mathematical Sciences, Tutorial lecture notes, Dec. 1, 2003.
- [MK05] P. Moulin, R. Koetter, "Data Hiding Codes", (tutorial paper), *Proceedings IEEE*, Vol. 93, No. 12, pp. 2083-2127, Dec. 2005.
- [MM04] P. Moulin, M.K.Mihcak, "The Parallel-Gaussian Watermarking Game", *IEEE, Trans. On Inf. Theory*, Vol.50, No. 2, Feb. 2004.

- [MN05] N. Memon, "Multimedia Fingerprinting", ECRYPT Summer School on Multimedia Security, Salzburg, Austria, Sept. 24, 2005.
- [MO98] M. J. J. B. Maes and C. W. A. M. Overveld, "Digital watermarking by geometric warping," in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998
- [MOS03] P. Moulin, J. O'Sullivan, "Information-Theoretic Analysis of Information Hiding", IEEE Trans. on Information Theory, 49, 3, March 2003, pp.563-593.
- [MP03a] P.Moulin, "Embedded-Signal Design for Channel Parameter Estimation, Part I: Linear Filtering", Proc. IEEE Workshop on Statistical Signal Processing, St Louis, MO, Sep. 2003.
- [MP03b] P.Moulin, "Embedded-Signal Design for Channel Parameter Estimation, Part II: Quantization Embedding", Proc. IEEE Workshop on Statistical Signal Processing, St Louis, MO, Sep. 2003.
- [MQ95] B.M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting", Proc. IEEE, vol. 83, pp. 944-957, June 1995.
- [MR00] A T. Murgan, R. Radescu, "Principiile teoriei codurilor. Algoritmi si aplicatii", Ed. Tehnica, Bucuresti, 2000.
- [MS99] S. Mallat, "A Wavelet Tour of Signal Processing", Academic Press, 1999.
- [MT94] K. Matsui and K. Tanaka, "Video-steganography: How to Secretly Embed a Signature in a Picture," in Proc. IMA Intellectual Property Project, vol. 1, Jan. 1994, pp. 187–206.
- [MU01] P. Meerwald, A. Uhl, "A Survey of Wavelet-domain Watermarking Algorithms", Proc. SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, San Jose, CA, USA, January 22 - 26, 2001.
- [MW01] N. Memon, P. W. Wong, "A Buyer-Seller Watermarking Protocol", IEEE Trans. on Image Processing, 10, 4, April 2001.
- [MW04] Pierre Moulin, Ying Wang, "New Results on Steganographic Capacity", Proc. CISS Conference, Princeton, NJ, Mar. 2004.
- [MW98] N. Memon and P.W. Wong, "Protecting Digital Media Content," Comm. ACM, Vol. 41, No. 7, July 1998, pp. 35—43.
- [NCH99] K.S. Ng and L.M. Cheng, "Selective block assignment approach for robust digital image watermarking", Proc.SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 14-17.
- [NP96] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures", Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP-96), vol. 4, Atlanta, GA, May 1996, pp. 2168-2171.
- [NP98] N. Nikolaidis, I. Pitas, "Robust Image Watermarking in the Spatial Domain", Signal Processing, Elsevier Science, Vol. 66, No. 3, pp. 385-403, 1998.
- [PAK98] F. Petitcolas, R. Anderson, M. Kuhn, "Attacks on Copyright Marking Systems", 2nd workshop on Information Hiding, 1525, Lecture Notes in Computer Science, Portland, Oregon, April 1998, pp. 218-238.

- [PAK99] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding –A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7): 1062-1078, July 1999.
- [PBBC97] A. Piva, M. Barni, E. Bartoloni, and V. Cappellini, "DCT-based watermarking recovering without resorting to the uncorrupted original image," in Proc. IEEE Int. Conf. Image Processing (ICIP), vol. 1, Santa Barbara, CA, 1997, p. 520
- [PD01] C.Podilchuk, E. Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, July 2001, pp. 33-46.
- [Pee03] C.B. Peel, "On Dirty-Paper Coding", IEEE Signal Processing Magazine, May 2003, pp. 112-113.
- [PFA] F.A. Petitcolas, MATLAB implementation of a D.C.T. based watermarking algorithm by Ingemar J. Cox et al., <http://www.petitcolas.net/fabien/software/>
- [PFA00] F.A. Petitcolas, "Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, Sept.2000, pp.58-64.
- [PGP99] ***, "An Introduction to Cryptography", PGP 6.5.1 documentation, 1999, online at <ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf>
- [PH99] F. Perez–Gonzales, J.R. Hernandez, "A Tutorial on Digital Watermarking", Proc. of the 33rd IEEE Annual Carnahan Conf. on Security Technology, Madrid, Spain, October 1999.
- [Pit96] I. Pitas, "A Method for Signature Casting on Digital Images", Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 15-17, 1996, pp. 215-218.
- [PJ96] J. Puate and F. Jordan, "Using fractal compression scheme to embed a digital signature into an image," in Proc. SPIE Photonics East'96 Symp., Boston, MA, Nov. 1996,
- [PK95] I. Pitas, T. Kaskalis, "Applying signatures on digital images", Proc. IEEE Nonlinear Signal Processing workshop, 1995, pp. 460-463
- [PL02] P. Loo, "Digital Watermarking using Complex Wavelets", Ph.D. Thesis., March 2002, Univ. of Cambridge, USA
- [PM93] W.B. Pennebaker and J.L. Mitchell, "The JPEG Still Image Data Compression Standard", New York: Van Nostrand, 1993
- [PMBA05] F. Perez – Gonzales, C. Mosquera, M. Barni, A. Abrado, "Rational Dither Modulation: A High Rate Data-Hiding Method Invariant Gain Attacks", IEEE Trans. On Signal Processing, Vol. 53, No. 10, Oct. 2005.
- [PRP99] S. Pereira, J.K. O'Ruanaidh, T. Pun, "Secure Robust Digital Watermarking Using the Orthogonal Transform", In P.W.Wong and E.J.Delp eds., IS&T/SPIE 11th Annual Symposium, Electronic Imaging'99: Security and Watermarking of Multimedia Contents, Vol. 3657 of SPIE Proceedings, pp. 21-30, California, 23-29 Jan. 1999.
- [PW02] A. H. Paquet, R. K. Ward, "Wavelet-Based Digital Watermarking for Image Authentication", IEEE Canadian Conference on Acoustics Speech and Signal Processing (ICASSP) 2002.
- [PZ98] C.I. Podilchuk, W. Zeng, "Image-Adaptive Watermarking Using Visual Models", IEEE, JSAC, Vol. 16, No.4, May 1998, pp.525-539.

- [[RAA99a](#)] M. Ramkumar, A.N. Akansu, A. Alatan, On the Choice of Transforms for Data Hiding in Compressed Video, ICASSP-99
- [[RAA99b](#)] M. Ramkumar, A.N. Akansu, A.A. Alatan, "A Robust Data Hiding Schemes for Images Using DFT", IEEE, International Conference on Image Processing, II, pp. 211-215, Oc. 1999.
- [[RDA98](#)] K. Ratakonda, R. Dugad, N. Ahuja, "Digital Image Watermarking: Issues in Resolving Rightful Ownership", ICIP 1998.
- [[RDB96](#)] J.J.K. Ruanaidh, W.J. Dowling, F.M. Boland, "Phase watermarking of digital images", Proc. IEEE Int. Conf. Image Processing, 1996, pp. 239-242.
- [[RDB96b](#)] J.J.K. Ruanaidh, W.J. Dowling, F.M. Boland, "Watermarking digital images for copyright protection", IEE Proc., Vision, Image, and Signal Processing, Aug. 1996, Vol. 143, Issue 4, pp. 250-256.
- [[RP97](#)] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in Proc. IEEE Int. Conf. Image Processing 1997 (ICIP 97), Santa Barbara, CA, vol. 1, Oct. 1997, pp. 536-539.
- [[RP98](#)] J.J.K. Ó Ruanaidh, T. Pun, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking", Signal Processing, 66(1998), pp. 303-317.
- [[RPHP99](#)] J. O'Ruanaidh, H. Petersen, A. Herrigel, S. Pereira, T. Pun, Cryptographic Copyright Protection for Digital Images based on Watermarking Techniques, Elsevier Science, Theoretical Computer Science, Vol. 226, Issue 1-2 (Sept. 1999), Special issue: cryptography, pp. 117 - 142, 1999.
- [[SATW02](#)] C.V. Serdean, M.A. Ambroze, M. Tomlinson and J.G. Wade, "DWT Based Video Watermarking for Copyright Protection, Invariant to Geometrical Attacks", Proc. 3rd Int. Symp. Communication Systems, Networks and Digital Signal Processing - CSNDSP 2002, Stafford, UK, 15-17 July 2002.
- [[SC96](#)] J. R. Smith and B. O. Comiskey, "Modulation and information hiding in images," in Lecture Notes in Computer Science: Information Hiding, vol. 1174. Berlin, Germany: Springer, 1996, pp. 207-226.
- [[SEG00](#)] J.K. Su, J.J. Eggers, B. Girod, "Capacity of Digital Watermarks Subjected to an Optimal Collusion Attack", European Signal Processing Conf. (EUSIPCO 2000), 2000.
- [[SEG01](#)] J. K. Su, J. J. Eggers, and B. Girod, "Analysis of Digital Watermarks Subjected to Optimum Linear Filtering and Additive Noise", Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.
- [[SG99](#)] J. K. Su and B. Girod, "Power-Spectrum Condition for Energy-Efficient Watermarking", Proc. IEEE ICIP '99, Oct. 1999.
- [[Sha93](#)] J. M. Shapiro, Embedded Image Coding Using Zerotrees of Wavelet Coefficients, IEEE Trans. on Signal Processing, 41:3445-3662, Dec. 1993
- [[SK01](#)] A. Sequeira, D. Kundur, "Communications and Information Theory in Watermarking: A Survey", Multimedia Systems and Applications IV, A. G. Tescher, B. Vasudev, and V. M. Bove, eds., Proc. SPIE (vol. 4518), pp. 216-227, Denver, Colorado, August 2001.

- [SKH05a] K. Su, D. Kundur and D. Hatzinakos, "Statistical Invisibility for Collusion-resistant Digital Video Watermarking", IEEE Trans. on Multimedia, vol. 7, no. 1, pp. 43-51, Feb. 2005.
- [SKH05b] K. Su, D. Kundur and D. Hatzinakos, "Spatially Localized Image-Dependent Watermarking for Statistical Invisibility and Collusion Resistance", IEEE Trans. on Multimedia, vol. 7, no. 1, pp. 52-66, Feb. 2005.
- [SO03] M.A. Suhail, M.S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model", IEEE Trans. on Instrumentation & Measurement, Vol. 52, No. 5, Oct. 2003, pp. 1640-1647
- [SO93] R.G. van Schyndel, C. Osborne, "A Two-Dimensional Watermark", Proc. DICTA, 93, pp. 378-383.
- [SP01] V. Solachidis, I. Pitas, "Circularly Symmetric Watermark Embedding in 2-D DFT Domain", IEEE Trans. On Image Processing, 10, 11, Nov 2001, pp.1741-1753.
- [SS02] L. Sendur, I. W. Selesnick, "Bivariate Shrinkage Functions for Wavelet-Based Denoising Exploiting Interscale Dependency", IEEE Trans. on Signal Processing, vol. 50, No.11, Nov. 2002, pp. 2744-2756.
- [STHW04] L. Shao-Hui, C. Tian-Hang, Y. Hong-Xun, G. Wen, - "A variable depth LSB data hiding technique in images" in Proc. Int. Conf. Machine Learning and Cybernetics, 2004, 26-29 Aug. 2004, vol.7, pp. 3990 – 3994.
- [STO94] R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, "A Digital Watermark", Proc. IEEE Int. Conf. Image Processing, vol. 2, Austin, TX, Nov.1994, pp. 86-90.
- [SZT96] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," IEEE Proc. ICIP, 1996, 3, pp. 211–214.
- [SZT97] M. Swanson, B. Zhu, and A. Tewfik, "Data Hiding for Video in Video", Proceedings of ICIP97, vol. 2, 1997.
- [TD97] Bo Tao, B. Dickinson, "Adaptive Watermarking in the DCT Domain", International Conf. On Acoustics, Speech and Signal Processing, ICASSP'97, April, 1997.
- [TE04] P. Tao, A.M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", Optics East 2004 Symposium, Internet Multimedia Management System V Conference, Philadelphia, PA, Oct. 25-28,2004.
- [TN02] V. Thilak, A. Nosratinia, "Robust Bandlimited Watermarking With Trellis Coded Modulation", ICIP 2002.
- [TNM90] K. Tanaka, Y. Nakamura, K. Matsui, "Embedding secret information into a dithered multi-level image", Proc. IEEE Military Communications Conference, 1990, pp.216-220
- [TP00] S. Tsekeridou, I. Pitas, "Wavelet-Based Self-Similar Watermarking for Still Images", IEEE Int. Symp. Circuits & Systems, ISCAS 2000, pp. 220-223.
- [TRSH93] A. Z. Tirkel, G. A. Rankin, R. van Schyndel, W. J. Ho, N. Mee, C. F. Osborne, "Electronic Watermark", Digital Image Computing, Technology and Applications, Sydney Australia, 1993, pp. 666-672

- [TSO93] A. Tirkel, R. van Schyndel, and C. Osborne, "A twodimensional watermark," in Proc. DICTA 1993.
- [TSO95] A.Z. Tirkel, R. van Schyndel, C. Osborne, "A Two-Dimensional Digital Watermark", Digital Image Computing, Technology and Applications, Brisbane Australia, 1995, pp. 378-383
- [USC] USC-SIPI image database, <http://sipi.usc.edu/database/>
- [VDPP01] S. Voloshynovskiy, F. Deguillaume, S. Pereira, T. Pun, "Optimal adaptive diversity watermarking with channel state estimation", Proc. SPIE, Security Watermarking Multimedia Contents III, 2001.
- [VHBP99] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking," Intl Workshop in Information Hiding, Dresden, Germany, Oct. 1999.
- [VP96a] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," in Proc. Int. Conf. Image Processing (ICIP), vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 237-240.
- [VP96b] G. Voyatzis and I. Pitas, "Chaotic mixing of digital images and applications to watermarking," in Proc. Europ. Conf. Multimedia Applications, Services, and Techniques (ECMAST), Louvain-la-Neuve, Belgium, May 1996.
- [VP99] G.Voyatzis, I. Pitas, "Problems and Challenges in Multimedia Networking and Content Protection", TICSP Series No. 3, editor Iaakko Astola, March 1999.
- [VPPE01] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers and J. K. Su, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks", IEEE Comm. Magazine, pp.2-9, Aug.2001.
- [VSA00] S. Voloshynovskiy et al., "Generalized Watermark Attack Based on Watermark Estimation and Perceptual Remodulation", IS&T/SPIE's 12th Annual Symp., Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, P. W. Wong and E. J. Delp, Eds., SPIE Proc., vol. 3971, San Jose, CA, Jan. 2000.
- [VSA01] S. Voloshynovskiy et al., "Attack Modeling: Towards a Second Generation Watermarking Benchmark", Signal Processing, Special Issue on Information Theoretic Issues in Digital Watermarking, 2001.
- [VSA99] S. Voloshynovskiy et al., "A Stochastic Approach to Content Adaptive Digital Image Watermarking", Int'l. Wksp.Info.Hiding, vol. LNCS 1768, Lecture Notes in Comp. Sci., Springer Verlag, 29 Sept. -1 Oct. 1999, pp. 212-36.
- [Wal95] S. Walton, "Information Authentication for a Slippery New Age", Dr. Dobbs Journal, vol. 20, no. 4, pp. 18-26, Apr. 1995.
- [Wat93] A. B. Watson, "DCT Quantization Matrices Visually Optimized for Individual Images", Human Vision, Visual Processing, and Digital Display IV, Bernice E. Rogowitz, Editor, Proc. SPIE 1913-14, (1993), pp. 202-216.
- [WD96] R.B. Wolfgang and E.J. Delp, "A Watermark for Digital Images", Proc. IEEE Int. Conf. Image Processing, vol. III, Sept. 16-19, 1996, Lausanne, Switzerland, pp. 219-222.

- [[WL02a](#)] M. Wu, B.Liu, "Data Hiding in Image and Video: Part I Fundamental Issues and Solutions", *Trans. on Image Processing*, Vol. 12, No. 6, June 2003, pp. 685 – 695.
- [[WL02b](#)] M. Wu, B.Liu, "Data Hiding in Image and Video: Part II Fundamental Issues and Solutions", *Trans. on Image Processing*, Vol. 12, No. 6, June 2003, pp. 685 – 695.
- [[WL98](#)] M. Wu, B. Liu: "Watermarking for Image Authentication", *ICIP*, 1998.
- [[WMBC99](#)] M. Wu, M. L. Miller, J. A. Bloom, and I. J Cox, "A rotation, scale, and translation resilient public watermark," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999 (ICASSP '99)*, Phoenix, AZ, 1999.
- [[WPD99](#)] R.B.Wolfgang, C.I.Podilchuk, E.Delp, "Perceptual Watermark for Digital Images and Video", *Proc. of the IEEE*, Vol. 87, No. 7, July 1999, pp 1108-1155.
- [[WPW98](#)] P.W.Wong, "A Watermark for Image Integrity and Ownership Verification", *Proc IS&T PIC*, Portland, Oregon, 1998.
- [[WPW98b](#)] P.W. Wong, "A Public Key Watermark for Image Verification and Authentication", *ICIP* 1998.
- [[WQF98](#)] Wei, Z.H.; Qin, P.; Fu, Y.Q., "Perceptual digital watermark of images using wavelet transform", *IEEE Trans. Consumer Electronics*, Vol. 44, Issue 4, Nov. 1998, pp. 1267 – 1272
- [[WSAB00](#)] G. Wade, C. Serdean and A. Ambroze, M. Borda, I. Nafornita, "Watermarking uncompressed video: an overview", invited paper, *proc. Int. Symp. Electronics & Telecommunications*, Timisoara, 2000.
- [[WSB03](#)] Z. Wang, H.R. Sheikh, A.C. Bovik, "Objective Video Quality Assessment", Chapter 41 in *The Handbook of Video Databases: Design and Applications*, B. Furht and O. Marqure, ed., CRC Press, pp. 1041-1078, September 2003.
- [[WSK98](#)] H.J.M. Wang, P.C. Su, C.-C.J.Kuo, "Wavelet-Based Digital Image Watermarking", *Optics Express*, Dec. 1998, 3, 12, pp. 491-496.
- [[WTWL04](#)] M. Wu, W. Trappe, Z.J. Wang, K.J.R. Liu, "Collusion-Resistant Fingerprinting for Multimedia", *IEEE Sign. Proc. Magazine*, March 2004, pp.15-27.
- [[Wu03](#)] M. Wu, "Joint Security and Robustness Enhancement for Quantization Based Data Embedding", *IEEE, Trans. On Circuits and Systems for Video Technology*, Vol.13, No. 8, Aug. 2003
- [[WYSV96](#)] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor, "Visual thresholds for wavelet quantization error," in *Proc. SPIE Human Vision and Electronic Imaging*, 1996, vol. 2657, pp. 381–392.
- [[XA98](#)] L. Xie, G. Arce, "Joint Wavelet Compression and Authentication Watermarking", *IEEE International Conference on Image Processing*, Chicago, IL, Oct 1998.
- [[XBA97](#)] X.-G. Xia, C.G. Boncelet and G.R. Arce, "A Multiresolution Watermark for Digital Images", *Proc. of International Conference on Image Processing*, vol. 3, pp.48-51, 1997.
- [[XBA98](#)] X. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet Transform Based Watermark for Digital Images", *Optics Express*, Vol. 3, No. 12, 1998, pp. 497-505.

- [[YKL01](#)] H.H. Yu, D. Kundur, C.-Y. Lin, “Spies, Thieves, and Lies: The Battle for Multimedia in the Digital Era”, IEEE Multimedia, July-Sept. 2001.
- [[YLLS00](#)] G. Yu and C. Lu and H. Liao and J. Sheu, “Mean Quantization Blind Watermarking for Image Authentication”, Proc. IEEE Int. Conf. on Image Processing, Vancouver, Canada, Vol. III, pp. 706-709, 2000.
- [YM97] Yeung, M., Mintzer, F. “An invisible watermarking technique for image verification”, Proc. IEEE Int. Conf. Image Processing. Volume 2. (1997) 680—683.
- [[ZL00](#)] Zhihui Wei, Xiao Liang, “An Evaluation Method for Watermarking Techniques,” IEEE International Conference on Multimedia and Expo, 2000, pp. 373-376.
- [[ZL99](#)] W. Zeng, B. Liu, A Statistical Watermark Detection Technique without using Original Images for Resolving Rightful Ownerships of Digital Images, IEEE Transactions on Image Processing, Nov. 1999, Vol. 8, No. 11, pp. 1534-1548
- [[ZWWL03](#)] H. Zhao, M. Wu, Z. J. Wang, K.J.R. Liu, “Nonlinear Collusion Attacks on Independent Fingerprints for Multimedia”, Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, ICASSP 2003, Hong Kong, Apr.2003, pp.664-667.
- [[ZXZ98](#)] W. Zhu, Z. Xiong, and Y.-Q. Zhang, “Multiresolution watermarking for images and video: a unified approach,” in Proc. Int. Conf. on Image Processing (ICIP), Chicago, IL, 1998.
- [[ZXZ98](#)] W. Zhu, Z. Xiong, and Y.-Q. Zhang, “Multiresolution watermarking for images and video,” IEEE Trans. Circ. Sys. Video Tech., Vol. 9, No. 4, pp. 545-550, Jun. 1999
- [[ZZS03](#)] D. Zheng, J. Zhao, A.E. Saddik, “RST Invariant Digital Image Watermarking Based on Log-Polar Mapping and Phase Correlation”, Trans. On Circuits and Systems for Video Technology, No. 8, Aug. 2003, pp. 753-765