

6. ATACURI ASUPRA SISTEMELOR DE WATERMARKING

Robustețea la atacuri este una dintre cele mai importante cerințe pentru sistemele de watermarking. O robustețe absolută la toate tipurile de atacuri și la combinațiile între ele este imposibil de obținut. Astfel, cerința practică devine următoarea: un atac de succes trebuie să deterioreze datele gazdă astfel încât să le reducă semnificativ valoarea comercială, fără ca watermark-ul să fie modificat într-o așa măsură, încât să nu mai poată fi recuperat. De fapt, printr-o proiectare corespunzătoare poate fi obținută o robustețe ridicată, dar ar trebui semnalat faptul că robustețea trebuie pusă în balanță cu cantitatea de informație a watermark-ului și imperceptibilitatea watermark-ului. Compromisul optim depinde întotdeauna de aplicație.

6.1. Clasificare în funcție de scopul atacului

În funcție de scopul atacului se poate face o clasificare generală a tipurilor de atacuri ce pot afecta sistemele de watermarking după cum urmează:

- 1. Atacuri simple** (atacuri pe forma de undă sau atacuri cu zgomot) sunt atacuri de o complexitate redusă ce încearcă să distrugă watermark-ul inserat prin manipularea tuturor datelor (date gazdă plus watermark) fără a încerca identificarea și izolarea watermark-ului. Exemple ar fi: filtrarea liniară și unele tipuri de filtrare neliniară, compresia bazată pe forma de undă (JPEG, MPEG), adăugarea de zgomot, adăugarea unui offset, decuparea, cuantizarea în domeniul timp sau spațiu, conversia digital-analog și corecția de gama.

2. **Atacuri de eliminare a detecției** (atacuri de sincronizare) sunt atacuri ce încearcă să distrugă corelația și să facă recuperarea watermark-ului imposibilă sau nefezabilă pentru un detector. Acest lucru se poate obține prin distorsiuni geometrice, ca de exemplu scalare, translatăre spațială sau temporală (video), rotație, decupare, permutarea pixelilor, subeșantionare, eliminare sau inserare de pixeli sau blocuri de pixeli sau orice altă transformare geometrică a datelor.
3. **Atacuri ambigue** (atacuri prin inversiune, atacuri cu watermark fals, atacuri cu original fals) sunt atacuri ce încearcă să inducă în eroare prin producerea de date gazdă false sau watermark-uri false [182]. Un exemplu este atacul prin inversiune [183, 184], ce încearcă să discrediteze autoritatea proprietarului drepturilor de autor prin inserarea de unul sau mai multe watermark-uri astfel încât să fie neclar care watermark a fost introdus primul.
4. **Atacuri de eliminare** sunt atacuri ce încearcă să analizeze datele cu watermark, să estimeze watermark-ul sau datele gazdă, să separe datele cu watermark în date gazdă și watermark și să elimine doar watermark-ul. Un exemplu sunt atacurile prin complotare, descrise mai pe larg în subcapitolul 3.3, extragerea zgomotului, anumite operații de filtrare neliniare sau atacuri prin comprimare folosind modelarea artificială a imaginii (de exemplu, folosind modele de texturi sau structuri 3-D). Din acest grup mai fac parte atacuri ce corespund unei scheme de watermarking specifice și o atacă prin exploatarea slăbiciunilor criptografice de proiectare a schemei, ce o fac vulnerabilă la acest tip specific de atac.

Ar trebui observat faptul că cele 4 tipuri de atacuri nu pot fi clar delimitate și unele atacuri nu aparțin clar unui grup. Atacurile prin complotare pot fi privite ca un grup în sine, deoarece au nevoie, în comparație cu alte atacuri, de mai multe copii ale datelor, cu watermark-uri diferite. Dar, deoarece încearcă să reconstruiască datele originale fără watermark și, deci, să elimine watermark-ul, încadrarea lor în categoria „atacuri de eliminare” este justificată.

6.2. Clasificare în funcție de tipul datelor gazdă

În primul rând sunt prezentate diferite tipuri de distorsiuni neagresive și atacuri deliberate specifice imaginilor. Acestea pot fi folosite și pentru a ataca sistemele de

watermarking video prin aplicarea atacului asupra fiecărui cadru al secvenței video care pot fi privită ca o succesiune de imagini de sine stătătoare. A doua categorie de metode sunt cele specifice pentru video care se folosesc și de dimensiunea temporală sau de standarde de compresie video.

6.2.1. Distorsiuni și atacuri specifice imaginilor

Există un număr destul de mare de distorsiuni și atacuri ce pot pune în pericol sistemele de watermarking pentru imagini.

O clasificare generală a distorsiunilor și atacurilor se poate face în funcție de domeniul în care au loc. Pentru a exemplifica fiecare atac în parte am folosit ca imagine originală imaginea RGB de test „Lena” de rezoluție 512x512 pixeli și adâncime de culoare de 24 biți/pixel. Pentru majoritatea atacurile, parametrii de distorsiune sunt aleși mai mari pentru ca distorsiunea să poată fi observată și cu ochiul liber. În practică aceste distorsiuni nu pot fi prea mari, deoarece imaginea sau secvența video obținută în urma distorsiunii/atacului ar fi parțial distrusă și nu ar mai avea o valoare practică pentru atacator.

A. Distorsiuni/atacuri în domeniul spațial

1) Distorsiuni fotometrice

Aceste distorsiuni operează direct asupra valorilor pixelilor imaginii și sunt de obicei periculoase pentru integritatea watermark-ului introdus în domeniul spațial. Prin inserarea watermark-ului într-un domeniu transformat efectul acestor atacuri poate fi redus. Cele mai uzuale astfel de distorsiuni sunt prezentate în cele ce urmează:

- *Iluminarea/întunecarea imaginilor* este de obicei necesară în cazul unor imagini prea întunecate sau prea luminoase, dar această operație poate fi, de asemenea, folosită pentru a ataca un sistem de watermarking. Practic iluminarea sau întunecarea se realizează prin adunarea sau scăderea unei valori l la luminanța tuturor pixelilor imaginii:

$$Y' = Y \pm l \quad (6.1)$$



Figura 6.1. Imaginea originală „Lena” și imaginile după creșterea, respectiv scăderea luminozității cu

50

- *Estomparea contururilor (blurring)* este o operație de obicei folosită pentru a uniformiza imaginea la contururi în cazul în care acestea sunt prea accentuate. În exemplul din Figura 6.2 imaginea originală este filtrată cu un filtru 2-D cu funcția pondere h care aproximează mișcarea unei camere de mână cu 5 pixeli sub un unghi de 45 de grade, unde h este:

$$h = \begin{bmatrix} 0 & 0 & 0 & 0.05 & 0.03 \\ 0 & 0 & 0.05 & 0.17 & 0.05 \\ 0 & 0.05 & 0.17 & 0.05 & 0 \\ 0.05 & 0.17 & 0.05 & 0 & 0 \\ 0.03 & 0.05 & 0 & 0 & 0 \end{bmatrix} \quad (6.2)$$

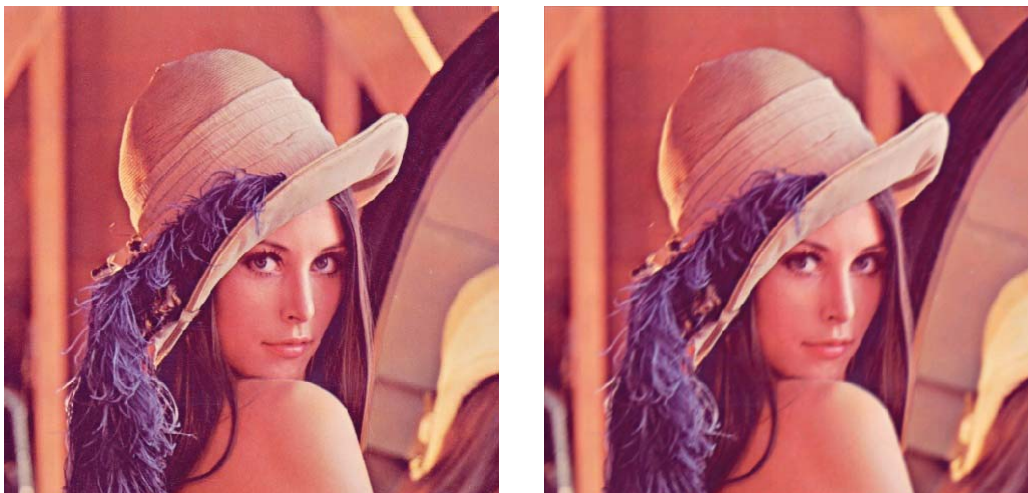


Figura 6.2. Imaginea originală „Lena” și imaginea după estomparea contururilor

- *Accentuarea contururilor (sharpening)* este o operație de obicei folosită pentru a îmbunătăți contrastul imaginilor. Practic este folosit un filtru de creștere a contrastului obținut de obicei dintr-un filtru Laplacian. În exemplul din Figura 6.3 a fost folosit filtrul 2-D cu funcția pondere:

$$h = \begin{bmatrix} 0.33 & 0.33 & 0.33 \\ 0.33 & 0.66 & 0.33 \\ 0.33 & 0.33 & 0.33 \end{bmatrix} \quad (6.3)$$

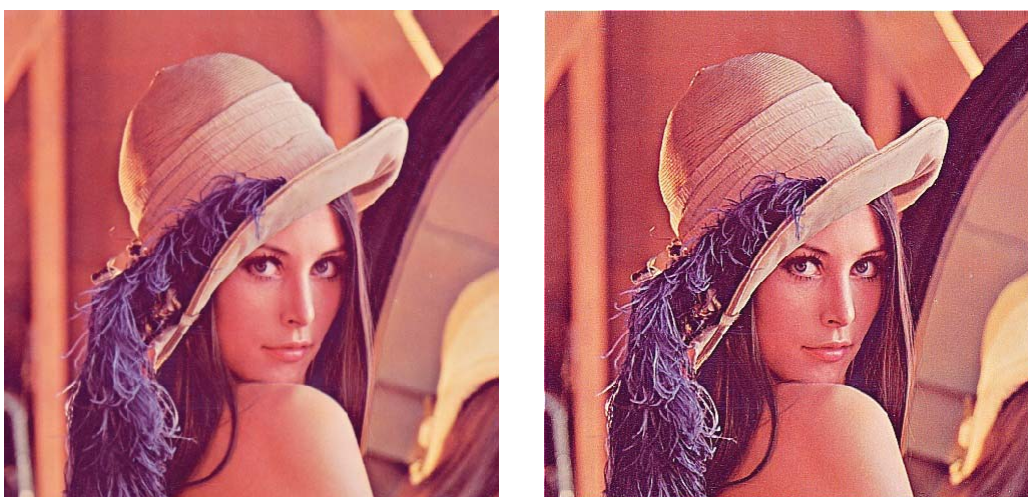


Figura 6.3. Imaginea originală „Lena” și imaginea după accentuarea contururilor (sharpening)

- *Corecția de gama*

Intensitatea luminoasă obținută în reprezentarea imaginilor sau secvențelor video folosind diferite sisteme de afișare este de cele mai multe ori neliniară. Un exemplu este monitorul cu tub catodic la care strălucirea este funcție de tensiunea aplicată după legea:

$$I = V^\gamma \quad (6.4)$$

unde I este intensitatea pixelilor și V este tensiunea aplicată. Pentru o imagine monocromă pe 8 biți, relația este:

$$y = 255 \left(\frac{x}{255} \right)^\gamma \quad (6.5)$$

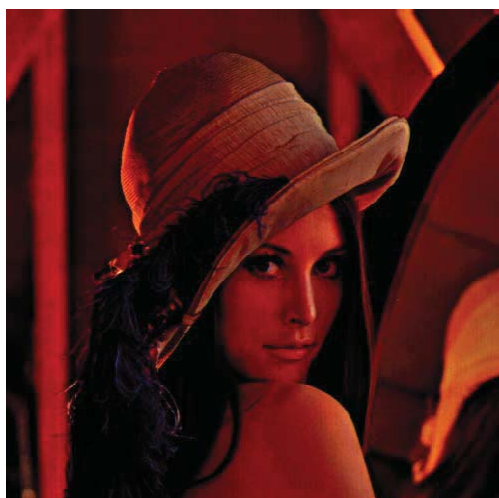
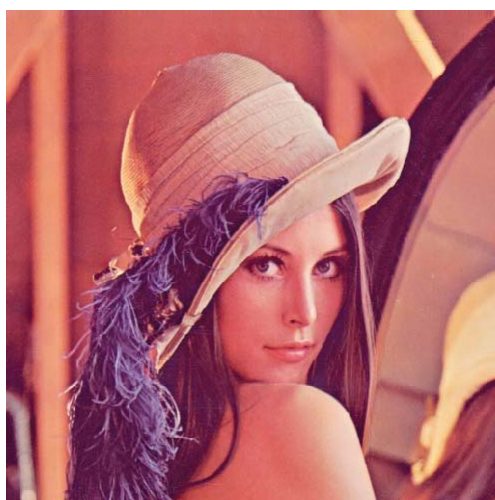


Figura 6.4. Imaginea originală „Lena” și imaginile după aplicarea corecției de gama cu factorul 5, respectiv 0.5

unde valoarea x este valoarea inițială a intensității și y este valoarea intensității așa cum apare ea pe monitor. Această neliniaritate trebuie de multe ori corectată. Dacă valoarea lui γ este cunoscută, corecția constă în aplicarea inversei relației (6.5). Două exemple de aplicare a corecției de gama, pentru $\gamma = 5$, respectiv $\gamma = 0,5$ sunt date în Figura 6.4.

- *Filtrarea mediană* înlocuiește fiecare pixel cu media pixelilor dintr-o vecinătate de $M \times N$. Acest tip de filtrare se folosește de obicei la restaurarea imaginilor în cazul degradării punctuale a imaginii, înlocuindu-se pixelii afectați de zgomot cu media pixelilor vecini. Un exemplu de filtrare mediană pe o vecinătate de 5×5 pixeli este dat în Figura 6.5.

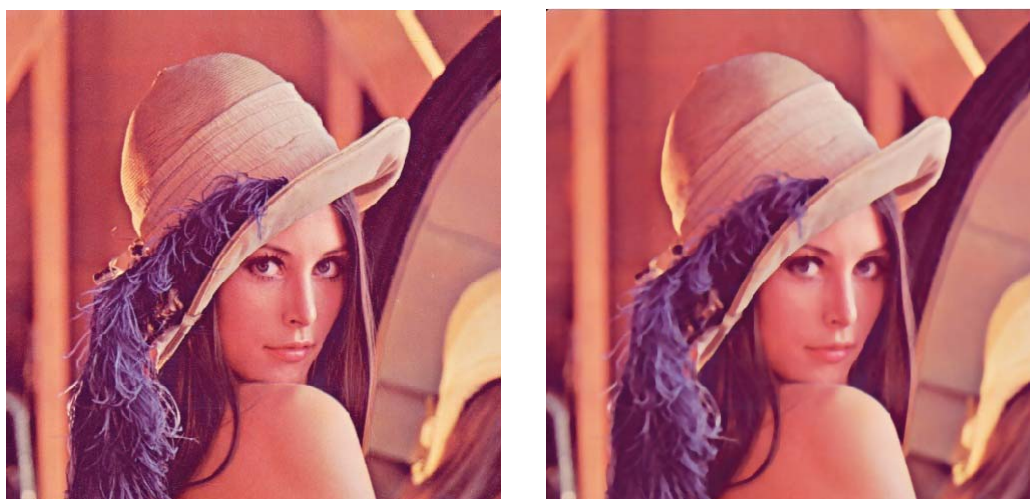


Figura 6.5. Imaginea originală „Lena” și imaginea după aplicarea unui filtru median pe o vecinătate de 5×5 pixeli

- *Adăugarea de zgomot* prin transmisiunea imaginilor și secvențelor video sau în mod intenționat poate afecta sistemele de watermarking. În Figura 6.6 sunt date două exemple de adăugare de azomot. În primul exemplu este adăugat un zgomot alb gaussian de medie 0 și varianță 0.005, iar în al doilea exemplu este adăugat un zgomot de tip „saltandpepper” (pixelii afectați au fie intensitate zero, fie intensitate maximă), numărul de pixeli afectați fiind:

$$p' = dens * p \quad (6.6)$$

unde p este numărul total de pixeli ai imaginii, iar $dens$ este densitatea zgomotului.



Figura 6.6. Imaginea originală „Lena” și imaginile cu zgomot gaussian (medie 0, varianță 0.005), respectiv zgomot de tip „saltandpepper” (de densitate 0.02)

- *Cuantizarea* la un număr mai mic de biți/pixel este folosită de majoritatea standardelor de compresie cu pierderi pentru reducerea dimensiunii imaginilor comprimate. În exemplul din Figura 6.7 am realizat o conversie a imaginii de la 24 biți/pixel la 8biți/pixel



Figura 6.7. Imaginea originală „Lena” și imaginea după o conversie de la 24 biți/pixel la 8 biți/pixel

- *Printare/scanare.* Aceste două operații consecutive pot fi, de asemenea, folosite de către un eventual atacator pentru a pune în pericol sistemul de watermarking. În exemplul din Figura 6.8 s-a realizat o printare la 300, respectiv 600 dpi și apoi o scanare.





Figura 6.8. Imaginea originală „Lena” și imaginea după printare și scanare la 300, respectiv 600 dpi

2) *Distorsiuni geometrice*

Aceste distorsiuni modifică dimensiunea sau poziția imaginii și sunt printre cele mai periculoase atacuri pentru integritatea watermark-ului introdus prin orice metodă. În literatura de specialitate au fost introduși algoritmi care sunt rezistenți la astfel de atacuri, dar cei care reușesc să rezistă la un tip de astfel de atac sunt de multe ori sensibili la alt tip de atac. Cele mai uzuale exemple sunt schimbarea rezoluției spațiale pentru reducerea dimensiunii imaginii (Figura 6.9), schimbarea ratei de aspect pentru afișarea pe display-uri de diferite mărimi (Figura 6.10), rotația imaginii sub diferite unghiuri (Figura 6.11) sau decuparea unei porțiuni din imagine (Figura 6.12).

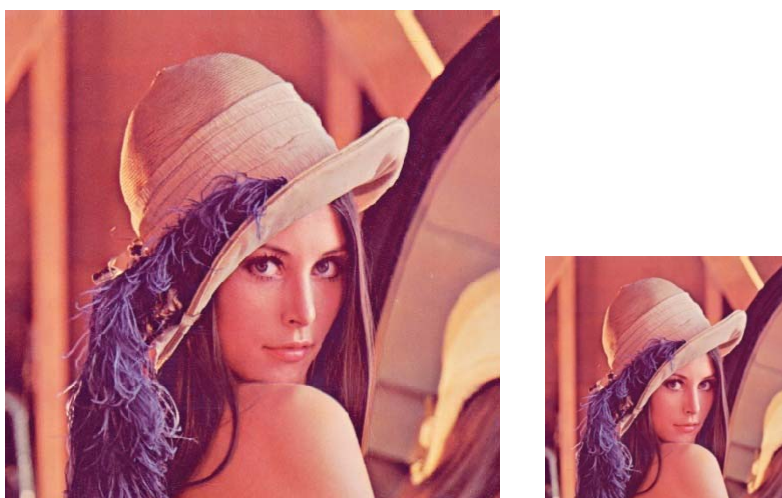


Figura 6.9. Imaginea originală „Lena” la o rezoluție de 512x512 pixeli, respectiv după schimbarea rezoluției la 256x256 pixeli



Figura 6.10. Imaginea originală „Lena” la o rată de aspect 1:1, respectiv 16:9



Figura 6.11. Imaginea originală „Lena” și imaginea după o rotație cu 45°



Figura 6.12. Imaginea originală „Lena” și imaginea după decuparea unei forme dreptunghiulare

În general, orice transformare geometrică poate fi considerată o transformare afină de coordonate. Se spune că o imagine $g(x, y)$ este o transformată afină a imaginii $f(x, y)$ dacă există un vector $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$ și două matrice $S = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ și $R = \begin{pmatrix} 1 & r_{12} \\ r_{21} & 1 \end{pmatrix}$, astfel încât $g(x, y) = f(x', y')$ și

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = S \cdot R \cdot \begin{pmatrix} x \\ y \end{pmatrix} - d \quad (6.7)$$

unde R este matricea de rotație, S este matricea de scalare și d este vectorul de translație. Astfel, o rotație a imaginii corespunde matricelor $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $R = \begin{pmatrix} 1 & r_{12} \\ r_{21} & 1 \end{pmatrix}$ și $d = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, o scalare pe direcțiile x și y corespunde lui $S = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$, $R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ și $d = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, iar o translație corespunde lui $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, și $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$. Orice transformare afină este o compunere a celor trei transformări menționate anterior.

B. Distorsiuni/atacuri în domeniul comprimat

În practică, de multe ori imaginile sunt comprimate într-un standard de compresie, ca de exemplu JPEG sau JPEG2000 pentru a reduce spațiul de stocare. Prin această conversie semnalul watermark poate suferi anumite interferențe. În Figura 6.13 imaginea „Lena” a fost comprimată folosind standardul JPEG cu factorii de calitate $Q=80$ și $Q=10$.

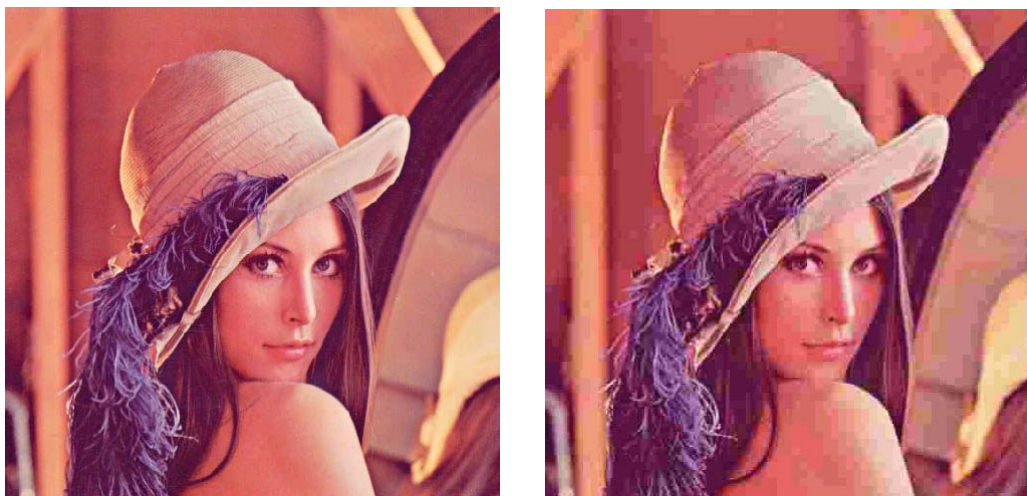


Figura 6.13. Imaginea „Lena” după compresie JPEG cu factorii de calitate $Q=80$ (stânga) și $Q=10$ (dreapta)

În Figura 6.14 aceeași imagine a fost comprimată folosind standardul JPEG2000 factorii de compresie 50:1 și 100:1.



Figura 6.14. Imaginea „Lena” după compresie JPEG2000 cu factorii de compresie 50:1(stânga) și 100:1 (dreapta)

6.2.2. Distorsiuni și atacuri specifice secvențelor video

În contextul de video există mult mai multe posibilități de atac decât pentru imagini. Cele mai uzuale sunt procesările video neagresive. Termenul neagresiv se referă la faptul că până și distribuitorii de conținut video procesează puțin datele digitale pentru o organizare mai eficientă a resurselor.

A. Distorsiuni/atacuri în domeniul spațial (desincronizare spațială)

1) Distorsiuni/atacuri fotometrice

Această categorie conține toate atacurile ce modifică valorile pixelilor din cadrele secvenței video. Deoarece fiecare cadru video poate fi privit ca o imagine de sine stătătoare, toate atacurile fotometrice prezentate pentru imagini pot fi aplicate succesiv fiecărui cadru video.

Modificările valorilor pixelilor pot apărea și datorită unei game largi de procesări video. De exemplu, transmisia datelor poate produce zgomot. Conversiile din digital în analogic și din analogic în digital produc, de asemenea, distorsiuni ale semnalelor video. Un alt tip de procesare des întâlnită este corecția de gama pentru a crește contrastul. Pentru a reduce spațiul

de stocare, proprietarii de conținut digital recodează deseori datele digitale la o rată de compresie diferită față de cea originală. O astfel de pierdere de informație ar putea altera performanțele algoritmilor de watermarking. Filtrarea spațială aplicată fiecărui cadru este deseori folosită pentru restaurarea unei secvențe video de calitate mai proastă. În cele din urmă, reeșantionarea componentelor de cromaticitate (4:4:4, 4:4:2, 4:2:0) este o procesare des folosită pentru a reduce spațiul de stocare.

2) Distorsiuni/atacuri geometrice

La fel ca și în cazul atacurilor fotometrice, atacurile geometrice prezentate în cazul imaginilor pot fi aplicate diferitelor cadre video. Pe lângă acestea, mai există unele atacuri geometrice care sunt specifice secvențelor video.

Mulți algoritmi de watermarking video se bazează pe sincronizare spațială implicită între codorul watermark și detector. Un pixel de la o anumită poziție în cadru este presupus a fi asociat cu un bit dat al watermark-ului. Multe procesări video neagresive introduc oricum desincronizare spațială ce ar putea conduce la pierdere drastică de performanță a schemei de watermarking. Cele mai cunoscute exemple sunt schimbările formatului de afișare (4/3, 16/9 și 2.11/1) și schimbările rezoluției spațiale (NTSC, PAL, SECAM și formate video comune). Pe de altă parte, poziția pixelului este amenințată de jitter. În particular, jitter-ul pozițional apare la transmisiunile analogice fără fir. În contextul camerelor digitale, distorsiunile introduse de camerele de mână pot fi considerate a fi neagresive, deoarece scopul explicit al camerei video nu este de a elimina watermark-ul inserat. S-a demonstrat că atacul prin camera de mână poate fi separat în două distorsiuni geometrice [185]: o transformare biliniară, datorată poziției camerei față de ecranul de cinema, și o transformare curbă datorată deformării lentilei. Astfel rezultă transformarea curbă – biliniară prezentată în Figura 6.15, ce poate fi modelată prin 12 parametrii.

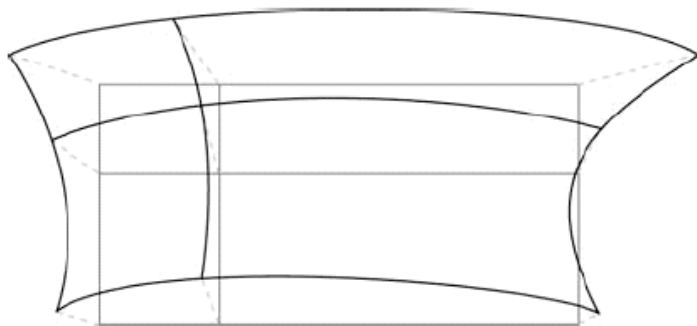


Figura 6.15. Exemplu de distorsiune creată de o cameră de mână (exagerat)

B. Distorsiuni/atacuri în domeniul timp (desincronizare temporală)

În comparație cu o imagine, o secvență video are și o a treia dimensiune, și anume timpul. Astfel, distorsiunile/atacurile din această categorie sunt specifice secvențelor video putând la rândul lor afecta semnalul watermark. De exemplu, dacă cheia secretă folosită la inserare este diferită pentru fiecare cadru, o simplă modificare a ratei cadrelor ar produce eșuarea algoritmului de detecție. Deoarece schimbarea ratei cadrelor este o procesare destul de obișnuită, watermark-urile ar trebui create astfel încât să supraviețuiască unei astfel de operații.

Un alt exemplu este prezentat în [186] unde se propune un algoritm ce permite sincronizarea temporală. Sincronizarea se realizează prin transmiterea de informație adițională împreună cu secvența video cu watermark. Cu toate că această metodă funcționează în timp real, necesitatea de a avea la decoder informația adițională face această metodă nepractică pentru majoritatea aplicațiilor.

Filtrarea inter-cadru, ca de exemplu medierea de cadre video adiacente, trebuie, de asemenea, avută în vedere.

Unul dintre cele mai periculoase atacuri este eliminarea de cadre din secvența video. Pentru ca un algoritm de watermarking să fie rezistent la acest tip de atac, el trebuie să aibă o redundanță mare de inserare a watermark-ului. O metodă pentru a detecta dacă au fost eliminate cadre din secvența video ar fi inserarea unui watermark cu numărului cadrului în fiecare cadru.

C. Distorsiuni/atacuri în domeniul comprimat

În practică de multe ori datele pot fi convertite dintr-un standard de compresie în altul, ca de exemplu din MPEG-1, MPEG-2 sau MPEG-4 într-un standard popular, ca de exemplu DivX. Prin această conversie semnalul watermark poate suferi interferențe. Diferitele cadre video pot fi alterate diferit în funcție de standardul de compresie folosit și în funcție de tipul și poziția cadrului în secvența video (ex. cadre I, P, B la compresia MPEG).

D. Editarea video

Ultimul tip de atac neagresiv conține toate operațiile ce pot fi realizate cu un editor video. Operațiile de tăiere-lipire sau tăiere-inserare-lipire sunt două procesări uzuale folosite la editarea video. Operația de tăiere-inserare-lipire este, de fapt, ceea ce se întâmplă când o reclamă este introdusă în timpul unui film. Mai mult, efecte ca estomparea și dispariția sau

ștergerea și nivelarea pot fi folosite pentru a modifica tranzițiile dintre scenele video. O astfel de editare video poate fi numită editare temporală, în contrast cu editarea spațială specifică imaginilor.

Editarea spațială se referă la adăugarea de conținut vizual în fiecare cadru al secvenței video. Conține, de exemplu, suprapunerea grafică (inserarea de embleme și subtitrări) și suprapunerea de două secvențe video (tehnologia imagine în imagine). Un astfel de atac sever produce o degradare puternică a performanțelor de detecție.

Diferitele tipuri de atacuri sunt reamintite în Tabelul 6.1. Pentru a contracara distorsiunile introduse de aceste procesări video ar trebui inserate contra-măsuri [187] în fluxul video. Pe lângă procesările neagresive trebuie avute în vedere și procesările ostile ce intervin în lumea reală. Într-adevăr, în ziua de astăzi este relativ ușor să procesezi un întreg film cu ajutorul calculatoarelor personale puternice. Orice transformare a unei secvențe video este virtual posibilă.

Tabelul 6.1. Exemple de procesări video neagresive

Distorsiuni fotometrice	➤ blurring, sharpening, ➤ creșterea/scăderea luminozității ➤ filtrare ➤ adăugare de zgomot ➤ conversie A/D sau D/A ➤ corecție de gama ➤ filtrarea intra și inter-cadru ➤ reeșantionarea componentelor de cromatică (4:4:4, 4:4:2, 4:2:0)
Distorsiuni geometrice	➤ schimbarea formatului de afișare (4/3, 16/9, 2.11/1) ➤ schimbarea rezoluției spațiale (NTSC, PAL, SECAM) ➤ jitter pozițional ➤ atac cu camera de mână
Desincronizare temporală	➤ schimbarea ratei cadrelor ➤ inserarea/eliminarea de cadre ➤ medierea de cadre
Distorsiuni în domeniul comprimat	➤ de la MPEG-1 la MPEG-2/4 ➤ de la MPEG-1/2/4 la Divx ➤ schimbarea ratei cadrelor I/P/B la standardul MPEG
Editare video	➤ tăiere-lipire și tăiere-inserare-lipire ➤ estompare și dispariție, ștergere și nivelare ➤ suprapunere grafică (subtitrări, embleme) ➤ imagine în imagine

De exemplu, pentru imagini, programul Stirmark introduce distorsiuni geometrice locale care conduc la desincronizarea detectorului. Acest program a fost optimizat pentru imagini, dar poate fi folosit pe fiecare cadru al unei secvențe video.

6.3. Atacuri prin complotare

Atacurile prin complotare sunt o problemă care a fost subliniată de ceva timp pentru imagini. Se referă la un grup de utilizatori malițioși care își unesc cunoștințele, ca de exemplu datele cu watermark-uri diferite, pentru a produce conținut ilegal, adică date fără watermark. O astfel de complotare este posibilă în două cazuri diferite:

- **Complotare de tipul I:** Același watermark este inserat în copii diferite de date diferite. Prin complotare se poate estima watermark-ul din fiecare copie cu watermark și obține un estimat mai fin a watermark-ului prin combinație lineară, ca de exemplu media estimatelor individuale. Cu un bun estimat al watermark-ului se pot obține datele fără watermark printr-o simplă scădere din cele cu watermark.
- **Complotare de tipul II:** Diferite watermark-uri sunt inserate în diferite copii ale acelorași date. Trebuie făcută doar o combinație lineară cu diferitele date cu watermark, ca de exemplu media, pentru a produce datele fără watermark. Într-adevăr, în general, medierea watermark-urilor diferite se apropie de zero.

Complotarea este o problemă foarte importantă în contextul video digital pentru că există de două ori mai multe oportunități de a dezvolta un atac prin complotare decât în domeniul imaginilor. În domeniul video, originea complotării poate fi dublă.

- **Complotare inter-video:** Aceasta este originea inițială considerată pentru imagini. O mulțime de utilizatori au o versiune cu watermark a unei secvențe video pe care o păstrează cu scopul de a produce conținut video fără watermark. În contextul protecției drepturilor de autor, același watermark este inserat în diferite secvențe video iar complotarea de tipul I este posibilă. Alternativ, într-o aplicație de amprentare, watermark-ul va fi diferit pentru fiecare utilizator și complotarea de tipul II poate fi luată în considerare. Complotarea inter-video necesită diferite secvențe video cu watermark pentru a produce conținut video fără watermark.

- **Complotare intra-video:** Acest tip de atac este specific pentru video. După cum va fi detaliat mai târziu, mulți algoritmi de watermarking consideră secvența video ca o succesiune de imagini. Inserarea watermark-ului într-o secvență video se reduce la inserarea de watermark-uri într-o serie de imagini. Din păcate, aceasta deschide noi oportunități pentru atacuri prin complotare. Dacă același watermark este inserat în fiecare cadru, complotarea de tipul I poate fi îmbunătățită, deoarece diferitele imagini pot fi obținute din scene în mișcare. Pe de altă parte, dacă sunt inserate watermark-uri diferite în fiecare cadru, atacurile prin complotare de tipul II devin un pericol în scene statice, deoarece ele produc cadre similare. Ca o concluzie, este posibilă îndepărtarea watermark-ului din fluxul video, având la dispoziție doar secvența video cu watermark.

Chiar dacă atacurile prin complotare nu sunt, de fapt, de mare interes pentru unele aplicații specifice, ca de exemplu monitorizarea emisiei, deseori ridică multe probleme în watermarking-ul video digital. Într-adevăr, se oferă posibilități pentru falsificare, dacă algoritmul de watermarking nu este rezistent la atacuri prin complotare intra-video.

Pericolul principal este complotarea intra-cadru, ca de exemplu atunci când o singură secvența video cu watermark este de ajuns pentru a elimina watermark-ul. A fost demonstrat că ambele strategii, „întotdeauna inserează același watermark în fiecare cadru” și „întotdeauna inserează watermark-uri diferite în fiecare cadru”, oferă posibilitatea atacurilor prin complotare. Datorită acestui motiv a fost găsită o strategie alternativă. O regulă de bază [188] a fost enunțată, astfel încât coliziunea intra-video să fie prevenită sau, cel puțin, făcută mai dificilă. Watermark-urile inserate în două cadre video diferite ar trebui să fie similare, în termeni de corelație, deoarece cadrele sunt asemănătoare. Altfel spus, dacă două cadre arată asemănător, watermark-urile inserate ar trebui să fie strâns corelate. Din contră, când două cadre sunt foarte diferite, watermark-urile inserate ar trebui să fie neasemănătoare. Această regulă este destul de încredere la o privire mai atentă la definiția celor două tipuri de atacuri prin complotare. Poate fi văzută ca o formă de watermarking public pentru că această regulă implică o dependență între watermark și conținutul cadrului gazdă. O implementare relativ simplă a unei astfel de abordări poate fi făcută prin inserarea unui watermark spațial localizat în funcție de conținutul fiecărui cadru video [189]. Un watermark de dimensiune mică poate fi inserat în câteva locații cheie ale fiecărui cadru, ca de exemplu în puncte proeminente. În procesul de extracție, detectorul poate descoperi cu ușurință poziția punctului proeminent și poate căuta watermark-ul.

Problema atacurilor prin complotare inter-video rămâne încă de actualitate. În ceea ce privește complotarea de tipul I, acest lucru poate fi prevenit prin inserarea unei Terțe Părți de Încredere (TPI), ce oferă mesajul de inserat. Acest mesaj este deseori o funcție a mesajului criptat pe care proprietarul dreptului de autor vrea să o ascundă. Secvențe video diferite oferă mesaje diferite pentru inserare și, astfel, watermark-uri diferite. TPI acționează, de asemenea, și ca depozit. Când este găsită o copie ilegală, proprietarul drepturilor de autor extrage mesajul inserat și îl transmite TPI-ului care îi dă în schimb mesajul original criptat asociat. Dacă proprietarul drepturilor de autor poate să îl decodeze cu succes, atunci poate să-și dovedească dreptul de proprietate. În legătură cu complotarea de tipul II, rezultatele obținute pentru imagini pot fi extinse cu ușurință și asupra domeniului video digital. Problema se pune când o complotare de utilizatori malițioși, având fiecare o copie a acelorași date, dar cu watermark-uri diferite, complotază pentru a produce ilegal datele fără watermark. Își compară datele cu watermark, observă locațiile unde diferitele versiuni diferă și modifică datele în acele locații. O contramăsura tradițională [190] constă în proiectarea unui set de watermark-uri distribuite astfel încât o coaliție de cel mult c utilizatori să reușească să elimine întreg watermark-ul. c este în general foarte mic în comparație cu numărul total de n utilizatori. Pe lângă aceasta, setul de watermark-uri este construit astfel încât nici o coaliție de utilizatori să nu poată produce un document care să păcălească un utilizator inocent, ca de exemplu unul ce nu face parte din coaliția ilegală. Cu alte cuvinte, după complotare se obține conținut video ce încă conține watermark, și watermark-ul rămas identifică clar utilizatorul malițios fără a acuza un utilizator inocent. Implementări ale unui astfel de set de watermark-uri au fost deja propuse pentru imagini și sunt bazate pe geometria proiectivă [191] sau pe teoria proiectării combinatorii [192].

