Adatrejtés videóban

BME - TMIT
VITMA378 - Médiabiztonság
feher.gabor@tmit.bme.hu

Vízjel

- 1282: Az első vízjelezett papír Olaszországból
  - Wassermarke (mintha víz lenne a papíron)
  - Normálisan nézve láthatatlan
- XVIII. század Európa és Amerika: vízjelzés a papíron, amely jelzi, a manufaktúrát és a méretet
- 1954: Az első elektronikus adatrejtés
  - Muzak coorporation: Egy zenemű vízjelezése egy szűrés segítségével (1 KHz körül)
- A vízjel is adatrejtés, de a rejtett adat az adott cover médiára vonatkozik!

Vízjelzés használata 1.

- A tulajdonos azonosítása
  - Szöveges formában, látható vízjel: © 2010 Fehér Gábor
  - A szöveg könnyen eltüntethető, a tartalom másolásakor nem feltétlenül megy át
  - A vízjel, mivel nem érzékelhető és nem leválasztható, ezért jobb azonosítás
- A birtoklás bizonyítéka
  - A látható jelzés hamisítható, eltüntethető
  - Létezik központi nyilvántartás, de ez költséges pl.: www.copyright.gov
  - A vízjel, mivel nem érzékelhető és nem leválasztható, ezért jobb bizonyíték

Vízjelzés használata 2.

- Műsorszórás megfigyelés
  - 1997-ben Japánban nagy botrány lett, mert a hirdetők olyan reklámokért is fizettek, amit le sem adtak!
  - Emberi hallgatás és a mintaillesztés nagyon költséges
  - A vízjelek segítségével azonosítható a reklám
- Tranzakciók nyomonkövetése
  - A tranzakciókban megjelölik a vevőt, nehogy visszaéljen az áruval
  - Pl.: pay-per-view modell esetén az adatrögzítő megjelölése.

Vízjelzés használata 3.

- Másolásvédelem
  - Digitális: A titkosításon túlmenően vízjel is jelezheti az adott eszközöknek, hogy az adott tartalom másolásvédelem alatt áll
  - Analóg: A vízjelet nehéz másolni, megakadályozza a sokszorosítást
- Eszközvezérlés
  - Tartalomhoz kapcsolódó megjelenítő eszközök irányítása (pl. zene és világítás)
  - Tartalomhoz kapcsolódó egyéb tartalmak vezérlése (pl. video és reklám)
    - 1962: Lynch Carrier Systems Inc.: Telefon irányítása
    - 1981: Dolby Labs: Vizualizáció irányítása
    - 1989: Interactive Systems Inc.: Interaktív videóeszközök irányítása

Vízjel fajták

- Látható „vízjel”
  - Cél, hogy a médiát/tulajdonost/tranzakciót jól láthatóan azonosítsa
  - Gyakran kombinálják nem látható vízjellel
- Láthatatlan vízjel
  - Törékeny vízjel
    - Általában az eredetiség azonosításra használjuk
    - Cél, hogy a vízjel a legkisebb módosításra eltűnjön
  - Robusztus vízjel
    - Leggyakoribb használat
    - Cél, hogy a vízjel a legdurvább módosításra is megmaradjon

Videó

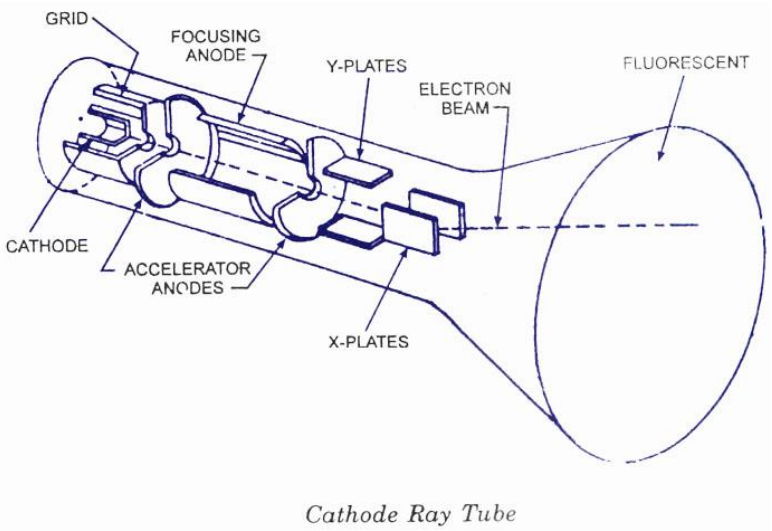
Analógtól a digitálisig

Videó tömörítés

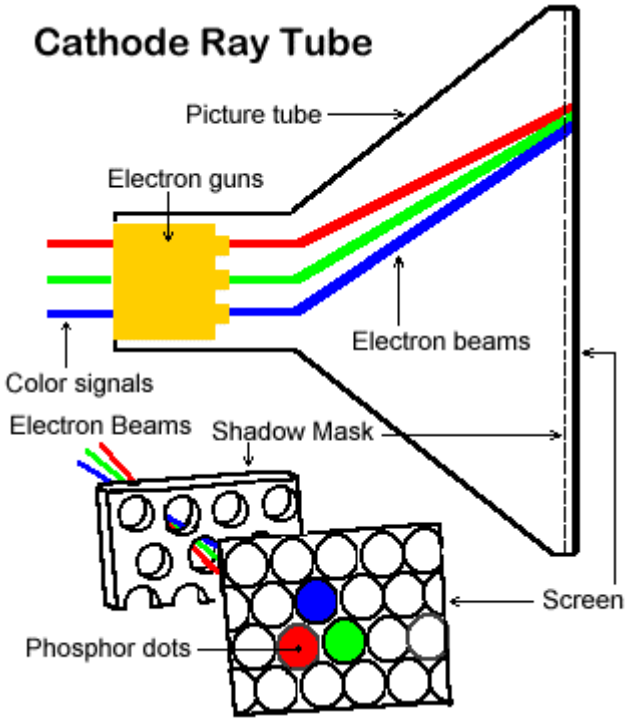
- TV adás
  - PAL (phase-alternating line)
    - Európa – SECAM (francia)
    - Perfect At Last
  - NTSC (National Television System Committee)
    - Amerika, japán
    - Never Twice the Same Colour
- Színterek
  - A fekete-fehér televíziózásból ered
  - YUV (PAL) YIQ (NTSC)
  - Lineáris leképezés

Analóg TV

- Katódsugárcső (CRT)

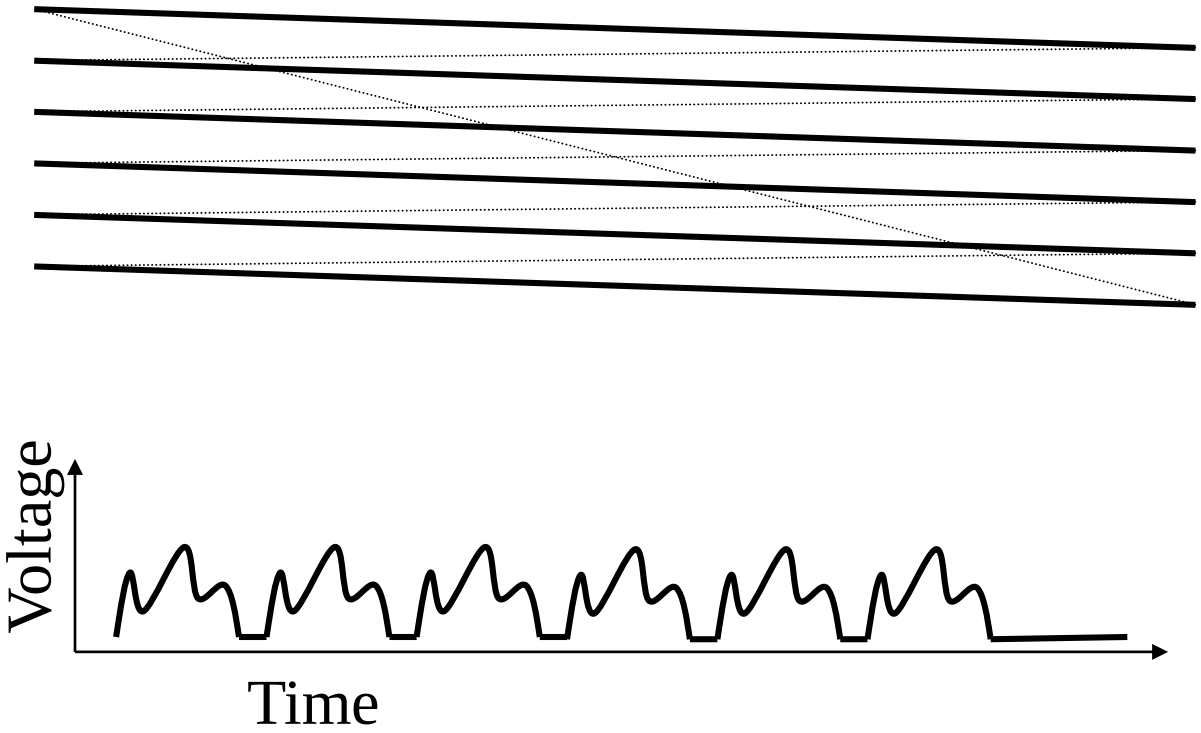


Cathode Ray Tube



Analóg pásztázás (scan)

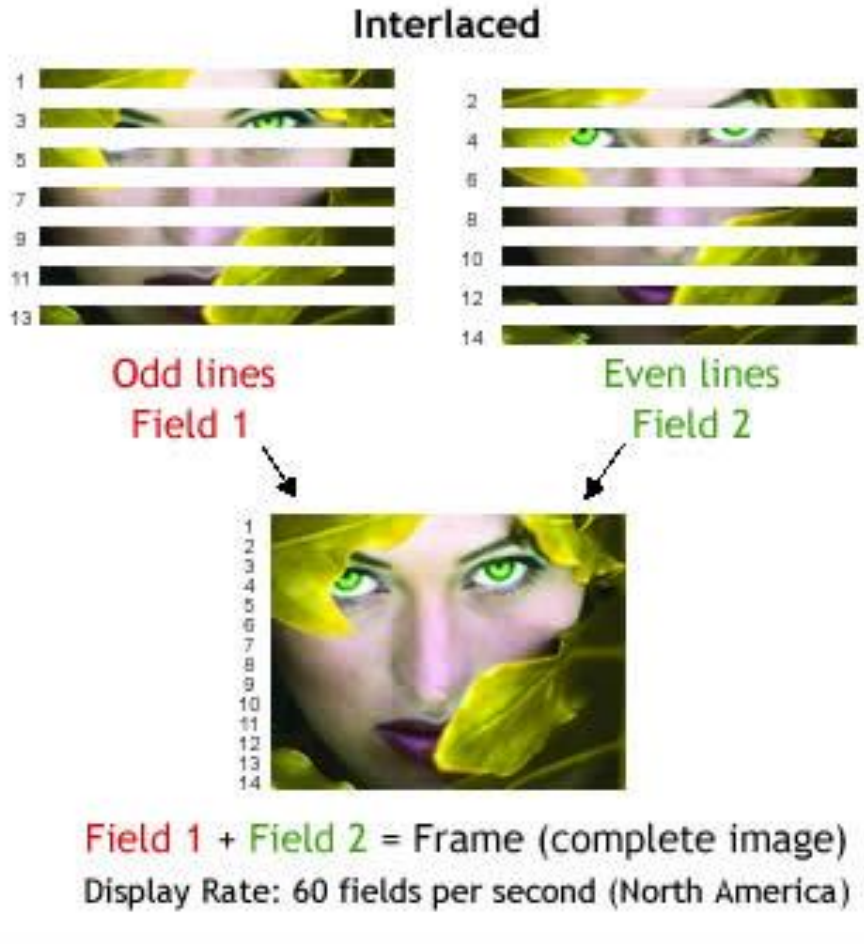
- Horizontális és vertikális



Interlacing

- Progresszív: minden sor letapogatása
  - Régebben probléma volt, hogy a sugár nem ért vissza időben, így a kép villogott
- Interlace: csak minden második sor egy félképben
  - PAL: 313 sor, 50 félkép másodpercenként
    - 288 látható sor (576i)
  - NTSC: 263 sor, 60 félkép másodpercenként
    - 240 látható sor (480i)
  - (progresszív forrás esetén zavaró lehet)

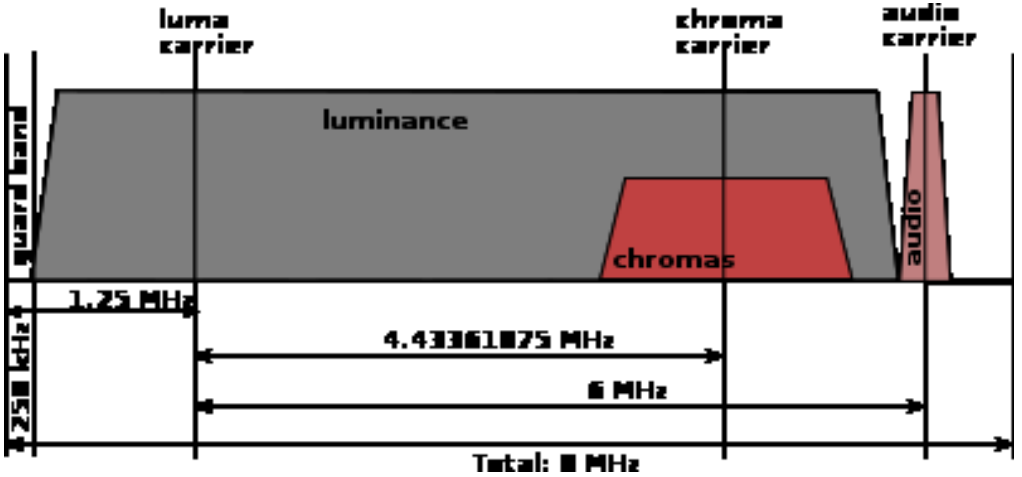
Interlacing képalkotás



Interlacing példa

Analóg sávszélesség

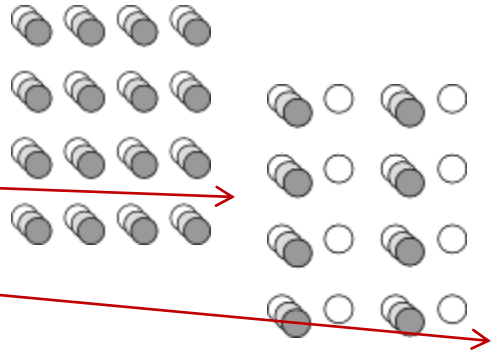
- PAL: Y: 6 MHz, U,V: 3 MHz
- NTSC: Y: 6 MHz, I: 2 MHz, Q: 1 MHz
- 6 MHz ~ 27-36 Mbps
  - 50 csatorna ~ 1.3-1.8 Gbps
  - Digitálisan többet tudunk átvinni



YUV alul-mintavételezés

- YUV 4:X:Y
  - X: U és V információ a páratlan sorokban
  - Y: U és V információ a páros sorokban

- YUV 4:4:4
- YUV 4:2:2
- YUV 4:2:0
- YUV



Digitális videó

- Képfrissítés
  - Majdnem mindig progresszív letapogatás
  - PAL: 25fps, NTSC: 29.97fps (30/1.001) (23.976fps – 3:2 pulldown mozifilmekhez)
- YUV értékek
  - U,V értékek eltérő mintavétellel
  - 4:2:2 (JPEG), 4:2:0 (MPEG), 4:1:1
  - 8 bites értékek
- Méretek
  - CIF 352x288: Common Intermediate Format, Common Interchange Format
  - QCIF 176x144
  - 4CIF 704x576 (~DVD)
- Sávszélesség:
  - PAL DVD: 25 fps * 720 * 576 * 1.5 * 8 = 120 Mb/s
  - 9:16 HDTV: 30 fps * 1920 * 1080 * 1.5 * 8 = 796Mb/s
- Tömöríteni muszáj!

Videó tömörítés

- Alapja a tér és időbeli közelség
  - Térbeli (spatial):
    - A közeli képpontok színe közel van egymáshoz
      - Az emberi szem érzékelése alapján
    - (Kivéve az éles átmeneteket)
  - Időbeli (temporal):
    - Az egymás után jövő képek nagyon hasonlítanak egymáshoz
    - (Kivéve jelenetváltás)

Tömörítés hatása

- Pozitív
  - Kisebb sávszélesség/bitrate elegendő
  - Kompaktabb tárolás
- Negatív
  - Érzékeny az adatvesztésre (redundanciával védelem a csatornakódolás során)

Intra-frame kódolás

- Csak az adott képet kódoljuk, nincs időbeli tömörítés
- Videónál szinte kizárólag transzformációs kódolás: 1-1.5 bit/pixel (mint a JPEG)
  - Csak intra-frame kódolás: M-JPEG

Inter-frame kódolás

- Az egymást követő képek hasonlósága
- Mozgáskompenzáció
  - Aktuális kép a referenciakép alapján mozgásbecsléssel
  - Nem képpontokként, nagyobb blokkokra nézzük

- Kódolás
  - Mozgásvektorok
  - A becslés hibájának kódolása (mozgáskompenzáció)

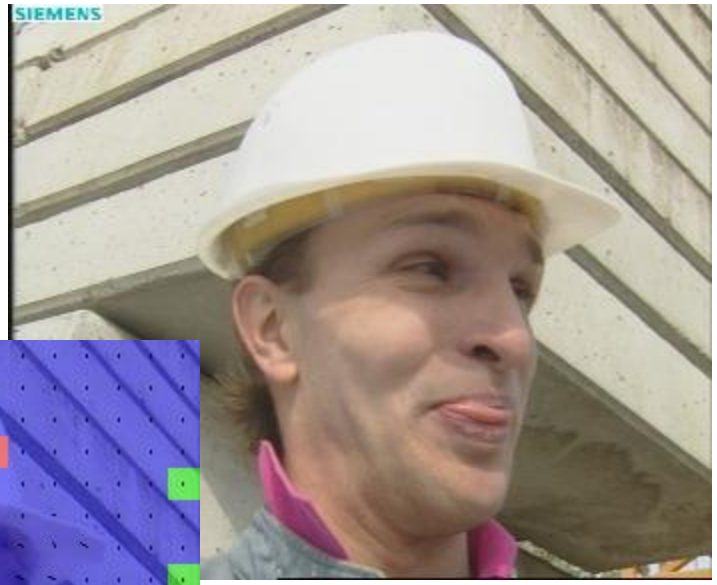
Mozgásbecslés - példa

mplayer -lavdopts vismv=1 -loop 0 -vo x11 video.avi

Mozgáskompenzáció - példa

n. keret

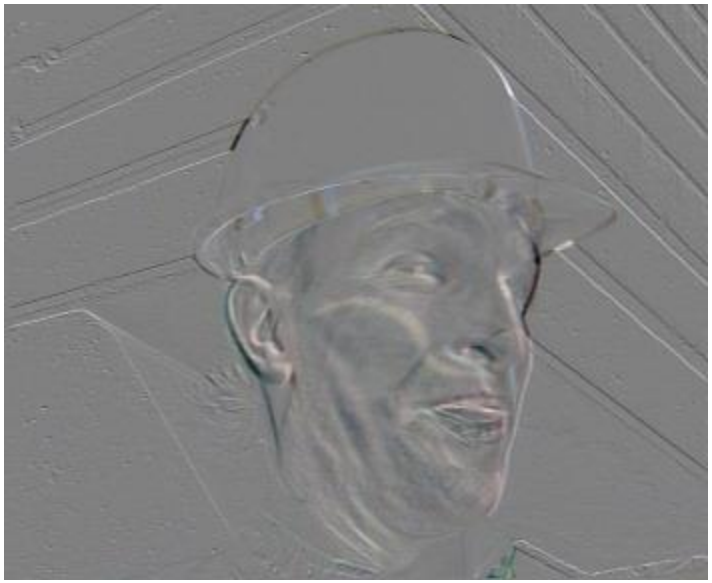
n+1. keret



n+1. keret, különbségekkel

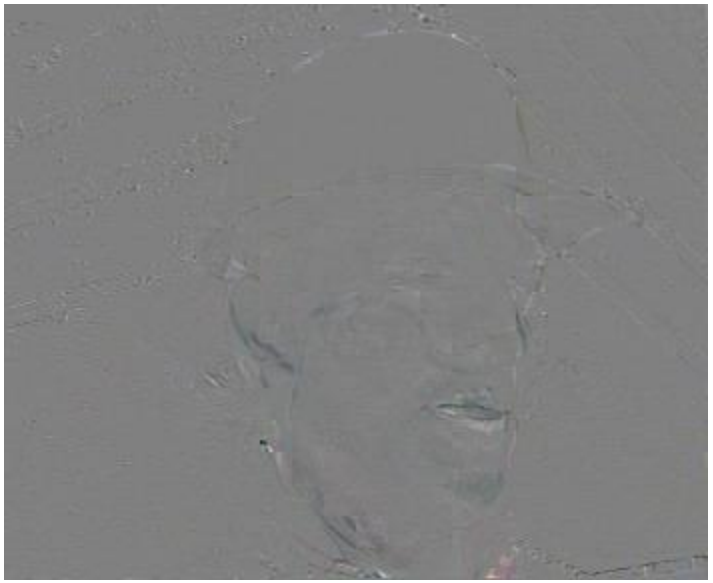
Mozgáskompenzáció - példa

Mozgáskompenzáció nélkül



Az eredeti képkocka és a mozgáskompenzáció nélküli képkocka különbsége

Mozgáskompenzációval



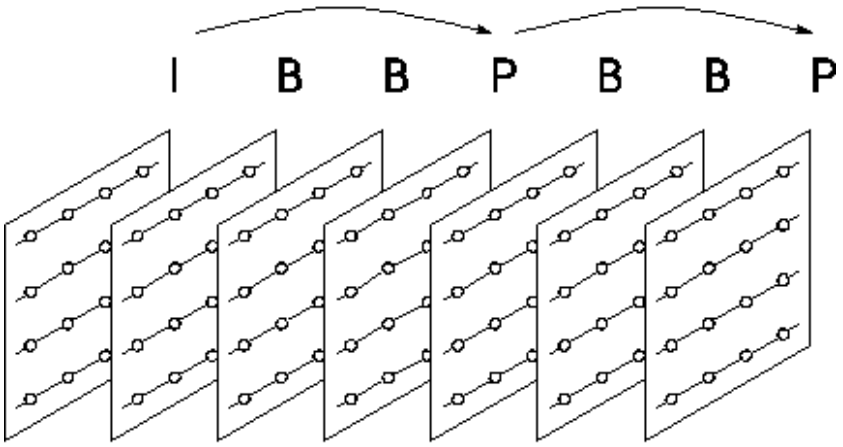
Az eredeti képkocka és a mozgáskompenzációval javított képkocka különbsége

Tömörített videó

- Szempontok
  - Kis méret (kis sávszélesség)
  - Szerkeszthetőség
  - Gyors tekerés, vissza tekerés, …
- Különböző képek
  - I: Intra-pictures – Csak térbeli tömörítés
  - P: Predicted-pictures – Mozgáskompenzáció
  - B: Bidirectional-pictures – Mozgáskompenzáció jövőbeli képekből is (Nem használható referenciaként)

Képcsoportok

- I-képek által határolt terület
  - Group of Pictures GOP - képcsoport



MPEG-1 kódolás

- MPEG-1
  - CD-n terjesztett videó (~1.5 Mbps)
  - Jelentős minőség csökkentések
    - Páros félképek elhagyása
    - X felbontás csökkentése
    - Színfelbontás csökkentése
  - Source Input Format: - SIF
    - PAL: 352 x 288, 25 kép/s
    - NTSC: 352 x 240, 29,97 kép/s

MPEG-2 kódolás

- MPEG-2
  - Digitális műsorszórás az analóg helyen (4-6 Mbps)
  - DVD formátum (4-8 Mbps)
  - HDTV, DVB
- Profilok, szintek a nagy átfedés miatt
  - MPEG-2 MP@ML (DVD, DVB)
  - 720x576, 30 kép/s, max 15 Mbps

MPEG-4 kódolás

- MPEG-4
  - Interaktív tartalom
  - “nagyon alacsony bitsebességek”
  - Objektum-orientált megközelítés
    - Szöveg, grafika, szintetikus hang, beszélő fej
- Alakkódolás
  - Tetszőleges alak
  - Mozgáskompenzáció, DCT-alapú textúra kódolás

- MPEG4:
  - MPEG-4 part 2: Advanced Simple Profile
    - Korábbi DivX, XViD, korábbi Quicktime, …
  - MPEG-4 part 3: Advanced Audio Coding (AAC)
  - MPEG-4 part 10: Advanced Video Coding (H.264)
    - Új DivX, Quicktime, Blue-ray lemezek, (mp4, mkv)

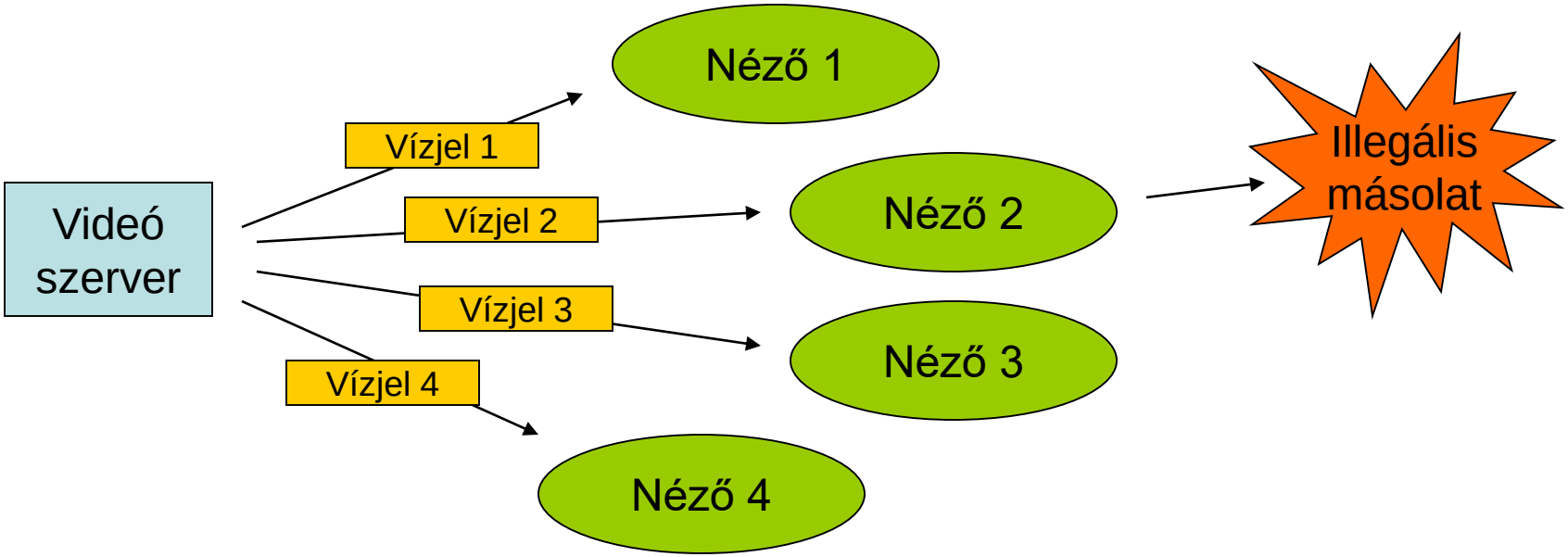
Videó vízjelezés

Vízjelek videófolyamban

- Cél az egyedi azonosítás
  - A forrás azonosítása
  - A néző azonosítása
- Látható és láthatatlan vízjelek
  - Látható vízjel: logó
  - Láthatatlan vízjel: pl. szórt spektrumú vízjel

Videó egyedi azonosítása

- Videó szerver és letölthető filmek
- Pl.: mozifilm zsűrizése a bemutató előtt



Video filmek szivárgása

Studios Sue Actor Who Allegedly Leaked "Screener" Movies Onto Internet

Authored by Mark Hefflinger on January 29, 2004 - 2:19am.

Los Angeles -- Two Hollywood film studios have filed copyright infringement claims against veteran actor Carmine Caridi ("The Godfather: Part II"), an Academy Awards voter who allegedly allowed copies of "screener" movies sent to him to be leaked onto the Internet, the Associated Press reported. Warner Bros. is seeking a minimum of $150,000 in damages for each of its two films that were leaked online, "The Last Samurai" and "Mystic River," while Columbia Pictures is asking for similar sums for infringement of its films "Something's Gotta Give" and "Big Fish." Caridi, 70, told law enforcement he sent the films to a friend and purported film buff, Russell Sprague, who was indicted last week on criminal copyright infringement charges for allegedly posting the films online. Caridi has not been charged in the incident, which highlights the Motion Picture Association of America's (MPAA) growing problem with Internet piracy. The group tried last year to ban distribution of such screeners -- sent to those who vote on film awards like the Oscars -- but the ban was later struck down by a federal judge.

http://www.salon.com/ent/wire/2004/01/29/screener/index.html

Video vízjelezési megoldások

Szórt spektrumú vízjel (Cox, 1997)

- Beillesztendő adat: a_x {-1, 1}
  - 0 és 1 elrejtendő biteknek megfelelően
- Tömörítetlen videójel
  - v_i a képpontok sorfolytonosan
  - Amennyiben nagyobb észrevétlenség szükséges, úgy csak az UV komponensek

Szórt spektrumú vízjel 2.

- Az elrejtendő információ kiterjesztése
  - $b_i = a_x$, ahol $i = x \cdot cr, \ldots, (x+1) \cdot cr - 1$
  - cr: chip-rate, az elrejtendő információ ennyi elemben ismétlődik
  - Pl.: a 0110 információ kiterjesztése

```
-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
 1  1  1  1  1  1  1  1  1  1  1
 1  1  1  1  1  1  1  1  1  1  1
-1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
```

Szórt spektrumú vízjel 3.

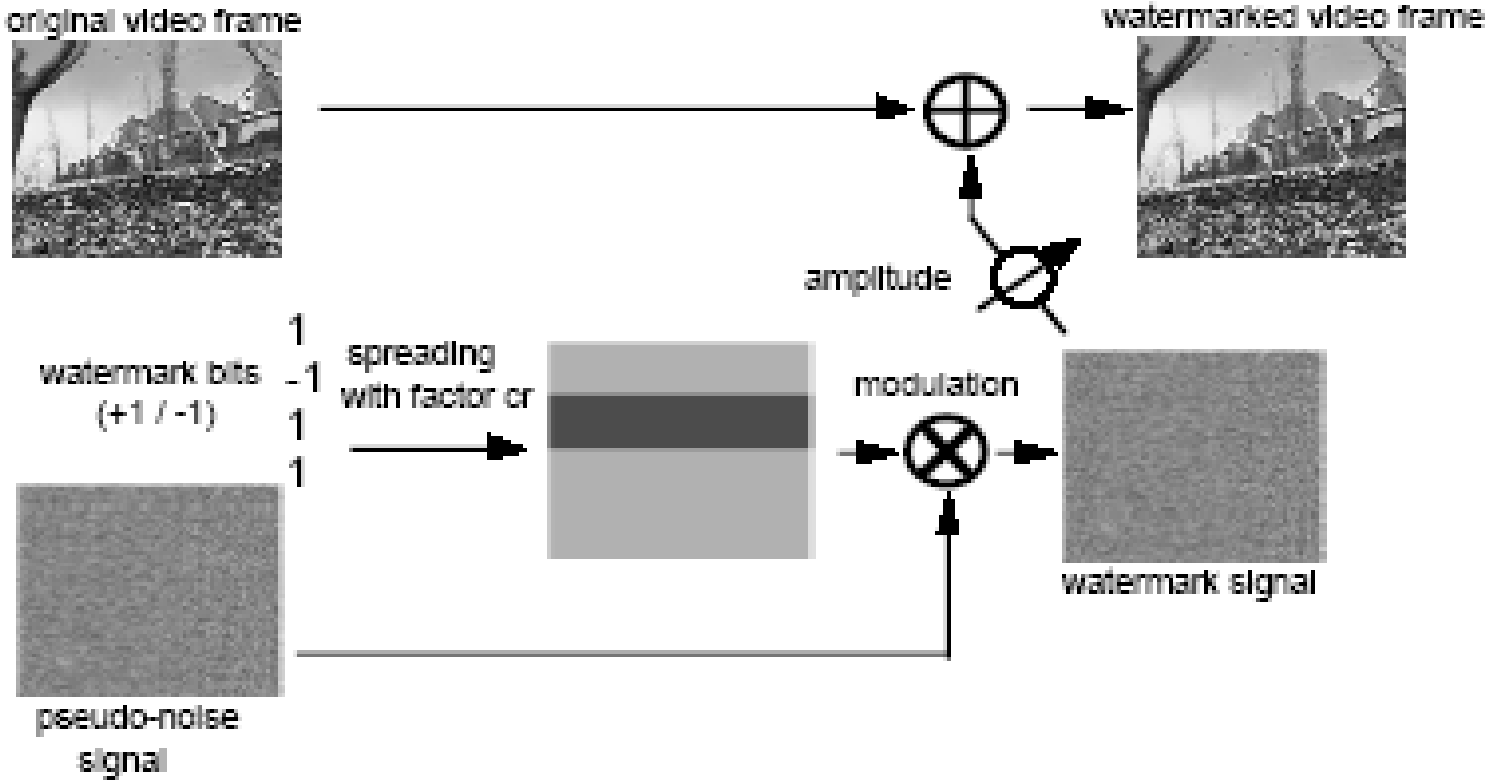
- Az információt zajba rejtjük el
  - Álvéletlen zaj: p_i {-1, 1}
  - A zaj forrása egy álvéletlen generátor. A generátor magja az adatrejtés kulcsa
- A zajt módosítjuk az elrejtendő info szerint
  - Az elrejtendő adat előállítása: $w_i = \alpha \cdot b_i \cdot p_i$
  - α: erősítés. Az adatrejtés visszafejtése során nem lesz teljesen egyértelmű mi az elrejtett adat, ezért kell erősíteni.
  - A túl erős zaj viszont rontja a képminőséget

Szórt spektrumú vízjel 4.

- Az adatrejtés során a videójelhez hozzáadjuk a „zajt”
  - $v^*_i = v_i + w_i$
- Amennyiben megfelelő erősítést használunk, úgy az adatrejtés nem feltűnő, a videó minősége nem romlik észrevehetően

Szórt spektrumú vízjel 5.

- Vízjel szórt spektrum segítségével



Adatrejtés felfedése

- A kép és a rejtett adat szétválasztása
  - $v^*_i = v_i + w_i$: nem kaphatjuk meg w_i –t, mert nem ismerjük v_i-t
  - Helyette szűréssel próbáljuk a zajt leválasztani:
    - A zajnak magas a frekvenciája
    - Nekünk most viszont a zajra van szükségünk!
    - Zajszűrés – felül-áteresztő szűrő segítségével
  - w^{**}_i : A zaj (rejtett adatunk) a szűrés után
    - Nem pontosan az, amit elrejtettünk!

Adatrejtés felfedése 2.

- A kiterjesztett információ hosszában vizsgáljuk a zajt
  - Szükségünk van az adatrejtésnél használt zajra
  - Mivel álvéletlen zajunk van, elegendő a generátor magja
  - A felfedésénél is előállítjuk p_i sorozatot

Adatrejtés felfedése 3.

$s_x = \sum p_i \cdot w^{**}_i \approx \sum p_i^2 \cdot \alpha \cdot b_i$

$i = x \cdot cr, \ldots, (x+1) \cdot cr - 1$

$s_x \approx cr \cdot \alpha \cdot b_i$, ahol b_i egyforma, mind a_x:

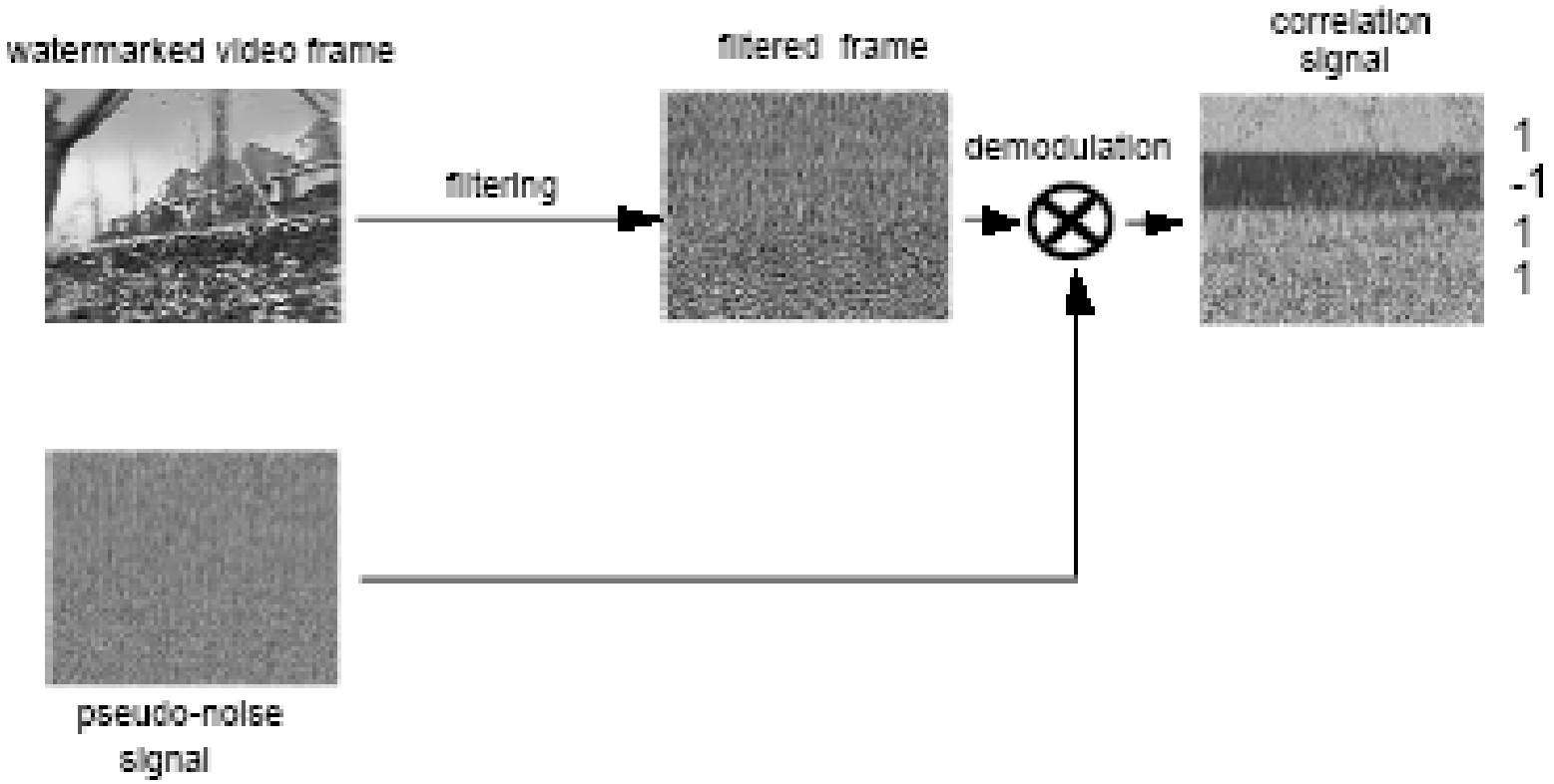
$s_x \approx cr \cdot \alpha \cdot a_x$: azaz

a_x –et becsülhetjük s_x -ből

- Minket csak az előjel érdekel
  - $a^*_x = signs(s_x)$, ahol $s_x = \sum p_i \cdot w^{**}_i$

Adatrejtés felfedése 4.

- Vízjel felfedése



Adatrejtés felfedése 5.

- Mi történik, ha nem ismerem az álvéletlen zajt?
  - $s_x = \sum q_i \cdot w^{**}_i \approx \sum p_i \cdot q_i \cdot \alpha \cdot b_i$
  - Ha q_i és p_i véletlen sorozatok, akkor körülbelül a sorozat fele eltérő, a másik fele megegyezik
  - q_i: −1 1 −1 −1 −1 1 1 −1
  - p_i: −1 −1 1 1 −1 1 −1 −1
  - s_x kinullázódik, de legalább is lehetetlen jól dönteni kis értéke miatt

$p_i \cdot q_i = -1$, ha különböznek
$p_i \cdot q_i = 1$, ha egyeznek

Ha a két mennyiség megegyezik, akkor az összeg 0

Nyilvános kulcsú vízjel

- Cél, hogy mindenki ellenőrizhesse a vízjelet
  - Szerző azonosítása
  - Másolásvédelem esetén is hasznos lehet
- Szórt spektrumú adatrejtés használata
  - Az álvéletlen zaj generátora nem lehet a nyilvános kulcs!
    - Veszélybe kerülhet a vízjel: kiszűrhető és megváltoztatható lesz
  - Rejtéshez szükséges egy privát kulcs. A publikus kulcs nem fedi fel teljesen a rejtett adatot, de ellenőrzésre még jó

Vízjel nyilvános kulccsal

- Két álvéletlen generátorom van:
  - $g^{privát}$ és $g^{nyilvános}$
  - A $g^{nyilvános}$ mag segítségével előállított p_i zaj csak n bitből egyben egyezik meg pontosan a $g^{privát}$ mag segítségével előállított zajjal, a többi pozícióban fele-fele arányban egyezik/eltér.
  - Léteznek ilyen álvéletlen generátorok

Vízjel nyilvános kulccsal 2.

- A dekódolás folyamata:

$$s_x^{\text{nyilvános}} \approx \sum p_i \cdot p_i^{\text{nyilvános}} \cdot \alpha \cdot b_i \,,$$
$$i = x \cdot cr, \ldots, (x+1) \cdot cr - 1$$

$p_i \cdot p_i^{\text{nyilvános}} = -1$, ha különböznek
$p_i \cdot p_i^{\text{nyilvános}} = 1$, ha egyeznek

- A korrelálatlan rész kinullázza egymást, marad az egyező rész:

$$s_x^{\text{nyilvános}} \approx cr/n \cdot \alpha \cdot a_x$$
$$a_x^{\text{nyilvános}} = \text{signs}(s_x^{\text{nyilvános}})$$

Minden n értékből 1 egyezik, ezért cr érték vizsgálata esetén cr/n a biztos egyezések száma

Vízjel nyilvános kulccsal 3.

- A vízjelet gyengébben érzékelem csak
  - Nehezebb döntés (de cr növelésével javítható)

- A vízjelet nem tudják kitörölni!
  - A publikus kulcsú rész azonban törölhető
  - Ha ki is törlik a nyilvános vízjelet, az privát kulccsal még mindig detektálható a vízjel

$$s_x = \sum p_i \cdot w^{**}_i \approx \sum p_i^2 \cdot \alpha \cdot b_i + \sum p_i \cdot p_i^{\text{nyilvános}} \cdot \alpha \cdot c_i$$

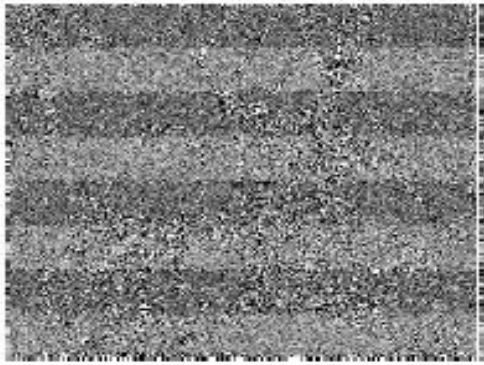
cr · (n-1/n) helyen egyezik

cr · (1/n) helyen különbözik

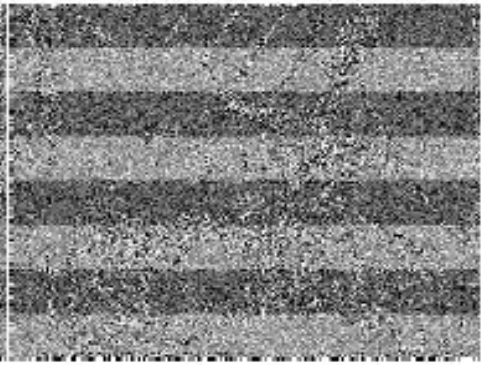
Vízjel nyilvános kulccsal 4.

watermarked frame

watermark extracted with secret pseudo-noise key



watermark extracted with public pseudo-noise key



watermark extracted with secret pseudo-noise key after attack using the public key

Vízjel nyilvános kulccsal 5.

- Beilleszthetünk több vízjelet is
  - A szórt spektrumú vízjel ezt lehetővé teszi, ha más az álvéletlen zaj sorozat (más generátor)
  - A két vízjel kiolvasható

$$s_x = \sum p_i \cdot w^{**}_i \approx \sum p_i^2 \cdot \alpha \cdot b_i + \underbrace{\sum_{i = x \cdot cr, \ldots, (x+1) \cdot cr - 1} p_i \cdot q_i \cdot \alpha \cdot c_i}$$

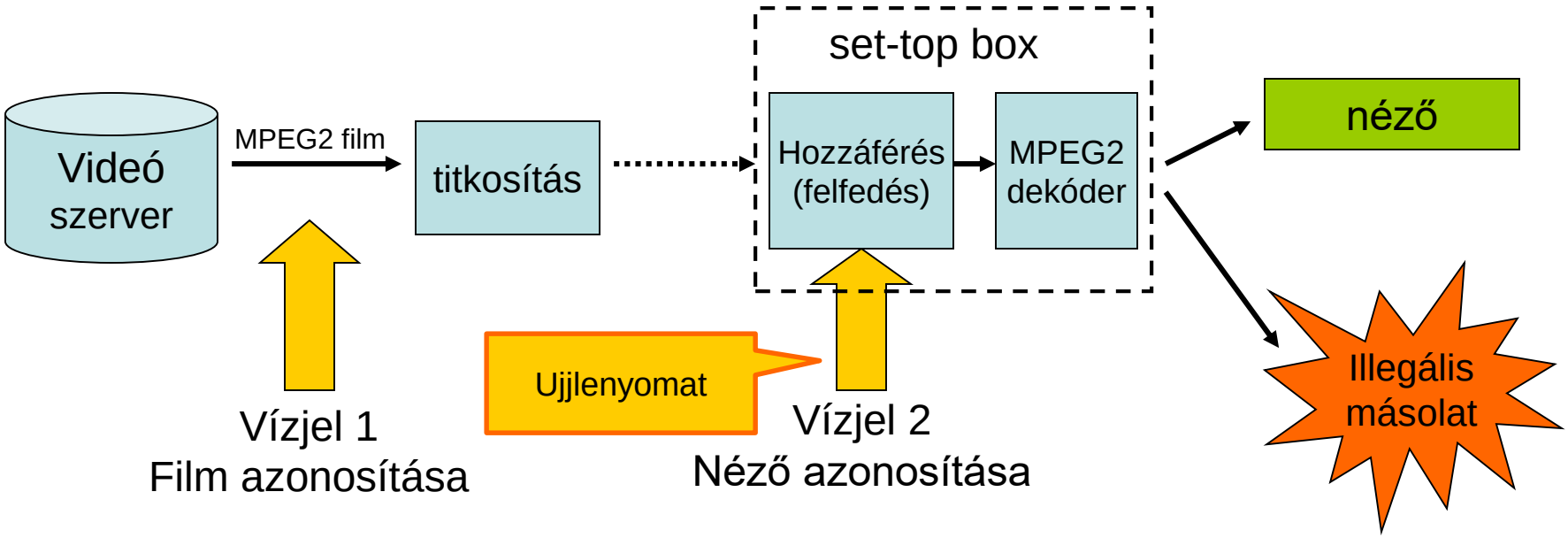
Kinullázódik. Nagyjából a vizsgált tartomány fele ilyen.

  - Időben költséges lehet
  - Tovább romlik a minőség: még több zaj
  - A vízjel olvashatósága romlik, hiszen fele annyi helyen van már csak adat

Vízjelezés használata

Videó szerver – vízjelezés

- Digitális TV adás fizetős ügyfelek számára másolásvédelemmel és ujjlenyomattal



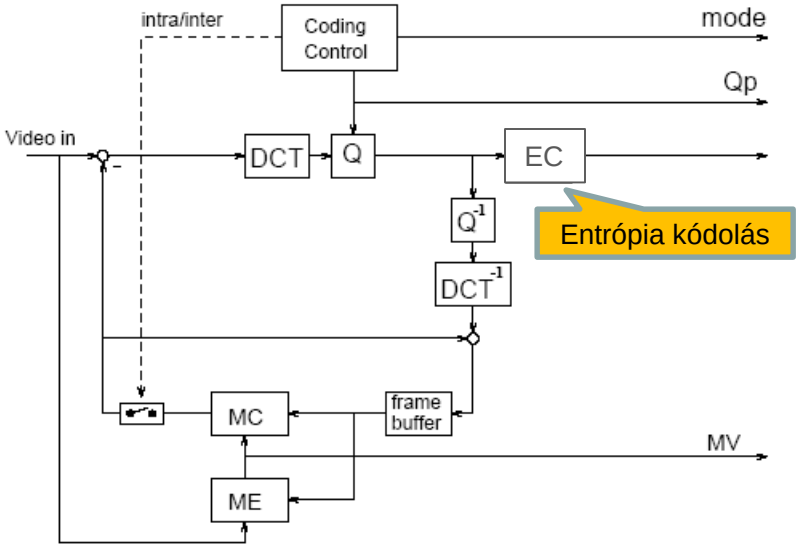
Adatrejtés tömörített videóban

- Az anyag tömörítetten áll rendelkezésre
  - Gyakori eset, pl. videó-szerver
  - Kitömöríteni nem érdemes
    - Minőségromlás (kitömörítés, újratömörítés)
    - Költséges (komplex műveletek: mozgás becslés, kvantálás megállapítása)
- Adatrejtéshez csak részben csomagoljuk ki, majd a meglévő kódok szerint visszacsomagoljuk
  - Mivel meglévő kódokat használunk, kevésbé költséges
  - Azonban az optimálistól eltérő kódolás miatti bitsebesség növekedés nem mindig engedhető meg

MPEG kódolás (ism.)

- A legtöbb videó kódolás hibrid kódolás
  - MPEG-1,2,4; H.261, H.263, H.264, …
  - Blokk alapú transzformációs kódolás (DCT)
  - Mozgásbecslés, mozgáskompenzáció (ME+MC)

- Intra- (I) keretek
- Inter- (P, B) keretek



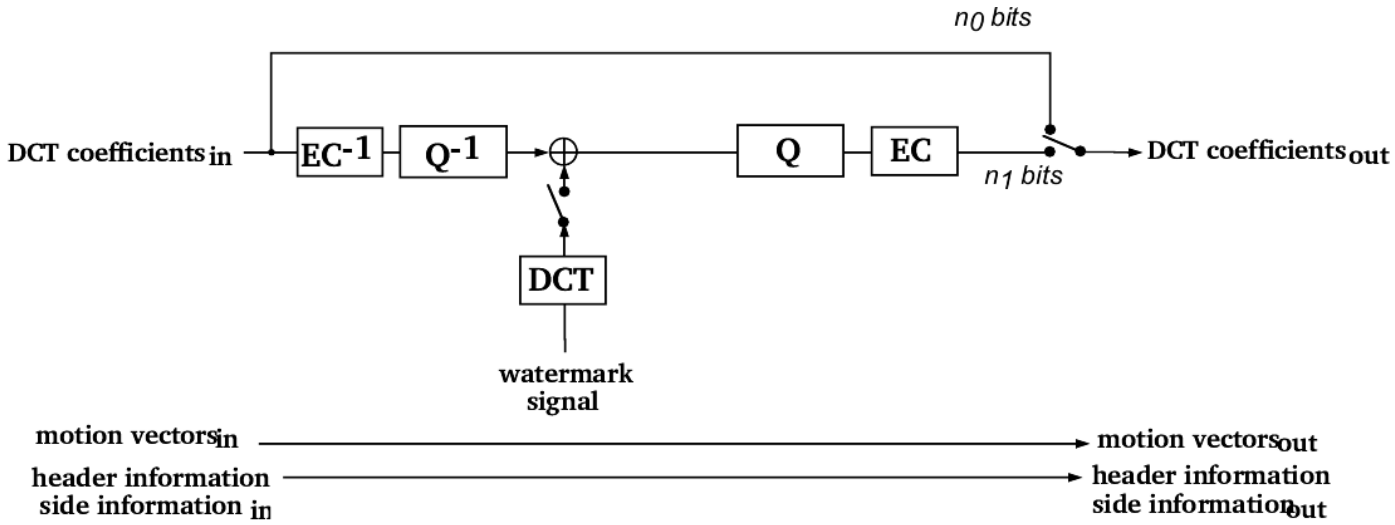
MPEG vízjel

- Vízjel elhelyezése
  - Mozgásvektorok
  - DCT együtthatók

- A vízjel előállítása hasonlóan a tömörítetlen esethez
- DCT együtthatók módosítása (additív)

MPEG vízjel 2.

1. Vízjel előállítása
2. DCT komponensek kicsomagolása (EC^{-1} és Q^{-1})
   - Inverz entrópia kódolás és kvantálás
3. Vízjel DCT felbontása
4. A videó és a vízjel együtthatók összeadása
5. Újracsomagolás
   - Entrópia kódolás és kvantálás



MPEG vízjel 3.

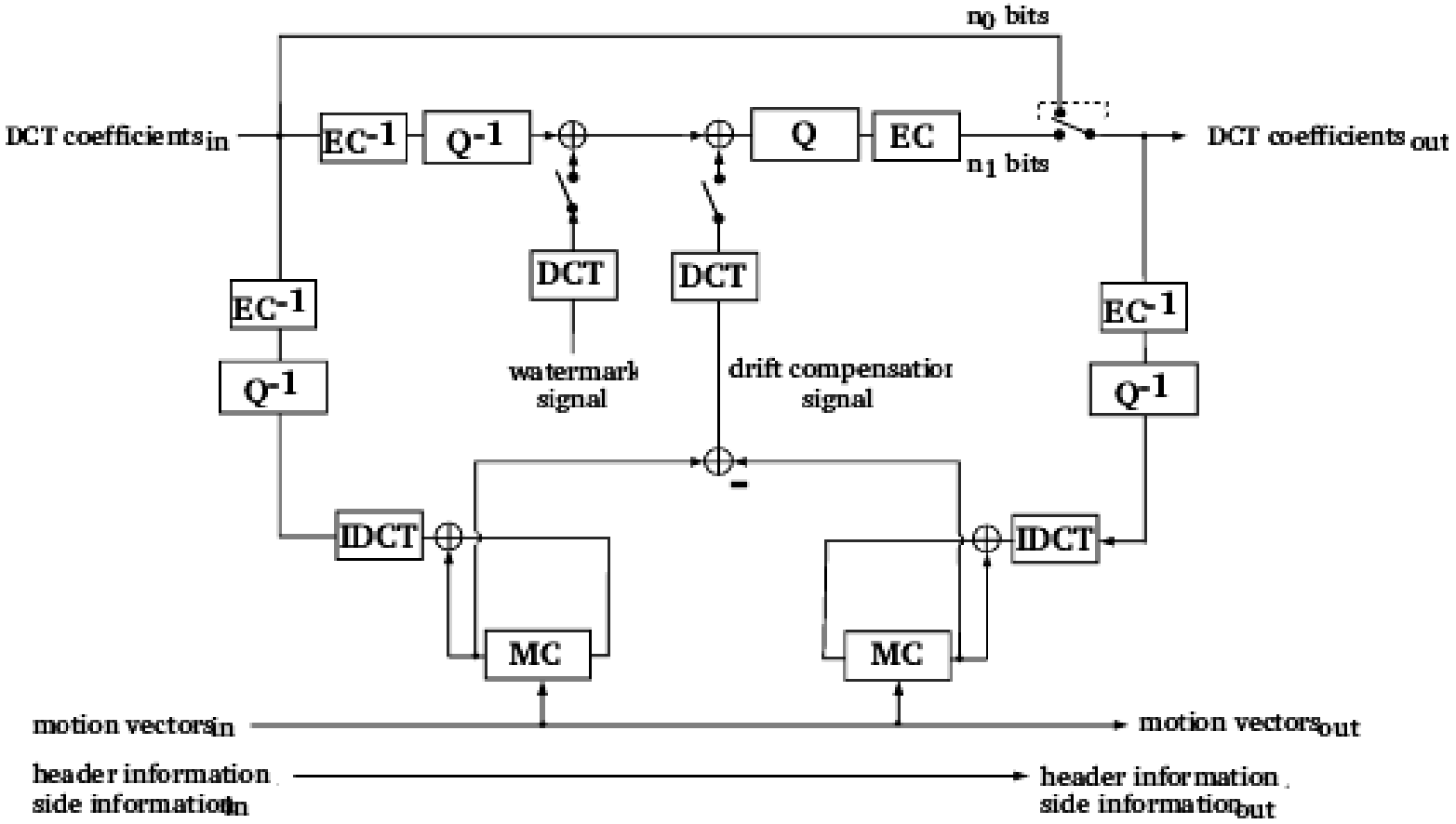
- Ha nő a 8x8 blokk tömörített hossza ($n_0 > n_1$), akkor nem lesz vízjel ebben a blokkban
  - Nem igazán gond, egy párat kihagyhatunk, az információnk úgy is redundáns
  - Az DC komponensbe azért mindig beletehetjük

- Tipikusan a folyam 10-20 százaléka lesz csak vízjelezve
  - Nagyon függ a videó tulajdonságaitól
  - Pl.: I képek gyakorisága

MPEG vízjel 4.

- Gond lehet viszont a P és B keretekkel
  - A vízjel rontja a videó minőségét
  - A mozgáskompenzáció még az eredeti jelhez lett kitalálva (sőt, még zajosítjuk is)
  - Halmozott hibák keletkeznek
- Megoldás *drift* kompenzáció
  - Ha kódoltunk egy blokkot a k keretben, akkor annak hatását a k+1 keretben visszaállítjuk (itt kivonjuk az előző vízjelet)

Drift kompenzáció



Egyszerűsített Drift kompenzáció