H.264 kódolt videófolyamok vízjelezése

OLÁH ISTVÁN

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
olah@tmit.bme.hu

Lektorált

Kulcsszavak: videó vízjelezés, H.264 vízjelezés, NCG

Cikkünkben összefoglaljuk a videó vízjelezés sajátosságait, majd bemutatunk egy olyan videó vízjelezési eljárást, ami ellenáll a H.264/AVC tömörítésnek, és a legáltalánosabb jelfeldolgozási módosításoknak.

1. Bevezetés

A digitális vízjelezés az adatrejtés (szteganográfia) egyik változata, segítségével információt rejthetünk valamilyen digitális hordozómédiába, úgy, hogy az egy laikus szemlélő számára észrevétlen marad. Legtöbbször a vízjel elhelyezése egy titkos kulcs segítségével történik, hogy csak az tudja detektálni a vízjelet, akinek birtokában van a megfelelő kulcs.

A legáltalánosabb esetben a vízjelezés első lépése a vízjel létrehozása, majd ezt a vízjelet valamilyen algoritmus segítségével elhelyezzük a hordozó médiában, és így létrejön a vízjelezett tartalom. A detektálás során feltesszük, hogy a hordozómédia időközben valamilyen módosításon esett át. Ilyen módosítás lehet a tömörítés, zajszűrés, vagy bármilyen más változtatás a tartalomban. A detektálás során a torzított vízjelezett tartalomban próbáljuk meg észlelni a vízjelet.

2. A videó vízjelezés sajátosságai

A mozgóképek vízjelezése nagyon hasonló az állóképek vízjelezéséhez, azonban van néhány speciális kérdés, amit meg kell említeni.

Az első ilyen különbség, hogy számos olyan szándékos módosítással kell számolni, amikor a tartalom terjesztője módosítja a tartalmat, hogy az megfeleljen a továbbítási csatorna sajátosságainak. Ilyen módosítás lehet például a bitráta megváltoztatása. Ezért egy jó vízjelnek jól kell tűrnie ezeket a változtatásokat.

Másik sajátossága a mozgókép-vízjelezésnek, hogy a detektálás során nem csak képkockán belüli szinkronizáció szükséges (hogy azon a helyen keresse a detektáló algoritmus a vízjelet, ahová azt elhelyezték), hanem időbeli is. Ilyenkor a vízjelet a meghatározott képkockán keresi a detektor. Időbeli szinkron elvesztését idézheti például elő, ha kihagynak néhány képkockát.

Harmadik sajátosság, hogy az egymás utáni képkockák csak egy kicsit különböznek egymástól, ami bizonyos alkalmazásoknál támadási lehetőséget kínálhat azoknak, akik el akarják tüntetni a vízjelet. Gondoljunk arra, hogy ha sok hasonló képkockát helyettesítünk az átlagukkal, akkor a néző számára a tartalom csak egy kicsit változik, viszont az átlagolás miatt esetleg eltűnik a vízjel.

Videó vízjelezésénél szükség lehet arra, hogy az algoritmus képes legyen másodpercenként 25-30 képkockát is vízjelezni. Ezért fontos az, hogy a vízjelezés amennyire csak lehet, egyszerű legyen.

Végül szempont lehet az is, hogy a beültetett vízjel ne változtassa meg a videófolyam bitsebességét és így ne következzen be esetleges torlódás a folyam hálózati továbbítása során.

3. Videóknál használt vízjelek fontos tulajdonságai

A vízjelező rendszereket sok tulajdonsággal lehet jellemezni. Ilyen tulajdonságok lehetnek a beültetés hatékonysága, a képromlás foka, a szállított adat mennyisége, a detektálás módja, a hibás detektálások aránya, a vízjel robusztussága, a biztonság tulajdonságai, a kulcsok milyensége, az ellenállás foka különböző támadások esetén, skálázhatóság és még számos egyéb tulajdonság is. Az, hogy e tulajdonságok közül melyiket tekintjük fontosnak és melyiket elhanyagolhatónak, nagyban függ attól, hogy mire akarjuk használni a vízjelet.

Az egyik legfontosabb tulajdonság, hogy mennyire rontja el a beültetett vízjel a hordozó képet. Ideális esetben a vízjel láthatatlan marad az emberi szem számára.

Egy másik fontos tulajdonság a robusztusság. Annál robusztusabb a vízjel, minél jobban ellenáll a tartalommódosításokkal szemben, legyenek azok egyszerű átkódolások, vagy rosszindulatú támadások, amik arra irányulnak, hogy eltávolítsák a vízjelet. Ezért célszerű lehet olyan részletgazdag helyekre elhelyezni vízjelet, melyek módosítása már észrevehető romlást eredményez a tartalomban.

Harmadik fontos tulajdonsága a videó vízjelezési algoritmusoknak a vak detektálás, ami azt jelenti, hogy a vízjelet az eredeti, vízjelezetlen tartalom nélkül is lehet detektálni. Ez a tulajdonság azért fontos, mert a tartalom nagyméretű és nehéz lehet eljuttatni a detektálás helyére.

A kapacitás azt jelenti, hogy mennyi adatot tud a vízjel szállítani egy képkockában. Ez lehet akár csak egy bitnyi adat, vagy akár egy egész szövegrész vagy kép is, a vízjel alkalmazási területétől függően. A vízjel kapacitása összefüggésben van annak láthatóságával és robusztusságával, ugyanis minél több információt tartalmaz a vízjel, annál jobban láthatóak a változások, vagy annál kevésbé lesz robusztus.

4. Videó vízjelezés alkalmazásai

A következőkben a digitális videó vízjelezés néhány alkalmazási módját tekintjük át.

Az első felhasználási mód a *másolásvezérlés*, amin azt értjük, hogy a médiában elhelyezett vízjel-bitek jelzik a lejátszó készülék számára, hogy az adott tartalom lejátszható vagy másolható-e.

A második elterjedt felhasználási mód a tévécsatornákon sugárzott *reklámok automatizált figyelése*. Ilyenkor a reklám tartalmaz egy vízjelet, amelynek detektálásával megállapítható, hogy mikor és hányszor sugározta a csatorna az adott reklámot.

A *nyomon követés (fingerprinting)* során egy adott tartalom (például egy film) minden példányát olyan vízjellel látják el, ami azonosítja azt a személyt, aki a filmet megvette, letöltötte. Ha a tartalom egy másolata felbukkan valamilyen illegális terjesztési hálózaton, akkor a vízjel segítségével azonosítható annak forrása.

A vízjelek használhatóak *hitelesítési feladatok* ellátására is. Ilyenkor egy olyan „törékeny” vízjelet helyeznek el a tartalomban, ami bizonyos fokú módosítások után nem detektálható többé. A tolerálható módosítás foka legtöbb esetben jól beállítható. Ezáltal megállapítható, hogy módosította-e valaki a vízjelezett tartalmat.

A *szerzői jogvédelmi alkalmazás* lényege, hogy a videóban elhelyezett vízjel olyan információt hordoz, ami azonosítja a tartalom tulajdonosát. Vitás esetekben így egyértelműen megállapítható, hogy ki a tartalom valódi tulajdonosa.

Az utolsó felhasználási mód a *tartalomhoz kapcsolódó információk szállítása*. Ilyenek lehetnek a szerzők neve, címek, feliratok és egyéb mellékinformációk.

5. A javasolt vízjelező rendszer

Az általunk tervezett vízjelező módszer célja, hogy H.264 kódolóval [1] tömörített videókat vízjelezhessünk. A vízjelezés és a tömörítés egymással ellentmondásban állnak, mert a vízjelezés során olyan apró változások keletkeznek a képen, amelyeket az emberi szem már nem vesz észre. A tömörítés célja pedig éppen az, hogy ezeket az észrevehetetlen változásokat eltüntesse és ezáltal a videó méretét csökkentse. A javasolt vízjelezési módszer felhasználási területe lehet valamilyen információszállítási feladat.

A vízjelező algoritmusok általában a tartalom kevésbé fontos részében rejtik el a vízjelet, így mérsékelve a minőség romlását. A jobb szubjektív minőség azonban a robusztusság csökkenését okozza: a különböző veszteséges tömörítési eljárások a kevésbé fontosnak tartott részeket durvábban kvantálják, így az ott elrejtett információ is nagyobb mértékben sérül.

Ezért, ahogyan az [2]-ben is láthatjuk, a vízjelet olyan helyre kell rejteni, ahol az emberi szem számára láthatatlan és mégis ellenáll a különböző kodekek általi veszteséges tömörítésnek. Ezek a helyek például a képkockán levő objektumok határai: ezeket a tömörítő algoritmusok finomabban kvantálják és kis mértékű változtatásuk nem lesz észrevehető az emberi szem számára.

A vízjelezés során megkeressük tehát azokat a blokkokat, amik alkalmasak vízjel rejtésére. Ezt a blokkok Normált Gravitációs Középpontjának (NCG) kiszámításával döntjük el. Az NCG értékek megadják, hogy melyek azok a blokk, amelyekben élek (éles átmenetek) találhatóak. Ha egy blokkhoz tartozó NCG érték egy előre meghatározott határ felett van, a blokkot vízjelezésre alkalmasnak választjuk. Bővebben a [2]-ben olvashatunk az NCG koordinátákról és azok tulajdonságairól.

Az algoritmus futása során minden egyes képkockában, a képkocka összes blokkjának kiszámítjuk az NCG értékét. Amely blokkok értéke egy előre meghatározott átlag felett van (tesztjeinkben ezt az értéket 420-nak választottuk – ennél nagyobb NCG értékű blokkokat már elegendően finoman kvantál a H.264 kódoló), alkalmasak vízjel beágyazására.

Az első képkockánál egy titkos kulcs alapján döntjük el, hogy a lehetséges blokkok közül melyek lesznek azok, amelyekben ténylegesen elhelyezzük a vízjelet. A további képkockákon megvizsgáljuk, hogy az előző képkockán használt blokkok megfelelnek-e az aktuális képkockán is. Ha igen, akkor ugyanazokat használjuk. Ez azért lehetséges, mert az egymást követő képkockák hasonlóak lehetnek egymáshoz, így az élek is ugyanott találhatóak. Így elkerülhetjük, hogy a képernyőn gyorsan ugráló mintablokkok látsszanak, ezáltal a vízjel kevésbé lesz zavaró.

Ha nem felelnek meg az előzőleg használt blokkok, akkor a bemenetként kapott kulcs segítségével a vízjelezésre alkalmas blokkok közül kiválasztjuk azokat, amikbe a tényleges rejtés fog történni.

Az egyes blokkok vízjelezésére a Dittmann-algoritmus [3] egy módosított változatát fogjuk használni. Dittmann-algoritmusa eredetileg MPEG videófájlok vízjelezésére készült, azonban alkalmas bármilyen kodekkel tömörített videófolyam vízjelezésére is. Az adatrejtést a képtartományban végzi, úgy, hogy közvetlenül a pixelek fényességértékeit módosítja. A rejtendő adatot 8x8 pixel méretű blokkokba ágyazza be, minden blokkba 1-1 bitet. Az általunk használt algoritmus 16x16-os blokkokat használ, a robosztusság növelése miatt.

A vízjel beágyazása mintablokkok segítségével történik. Ezek a mintablokkok 16x16 pixel méretűek, képzésük a következőképpen történik: egy 16x16-os blokkot feltöltünk véletlenszerűn -1 és 1 értékekkel. A blokkból eltávolítjuk a magas frekvenciákat, így egybefüggő 1 és -1 területek alakulnak ki a blokkon belül. Ezáltal a

blokk könnyebben azonosítható lesz. Az eredeti Dittmann-algoritmushoz képest változás, hogy csak olyan mintablokkok felelnek meg, ahol a sorokban és oszlopokban nagyjából egyenlő a -1 és 1 értékek száma. Erre a Dittmann- és az NCG-algoritmus ellentmondása miatt van szükség: az első azon alapul, hogy egy blokkon belül a változás nem jelentős, míg a másik eljárás az NCG értékek segítségével olyan blokkokat választ ki, amelyeken belül jelentős változás van a pixelek fényességértékében. Fontos tehát, hogy a mintablokk soraiban és oszlopaiban is nagyjából egyenlő legyen a -1 és 1 értékek száma.

Az így elkészült mintablokkokból többet is készítünk. A létrehozott mintablokkokat két csoportba osztjuk, a titkos kulcsnak megfelelően. Az első csoportban kerülnek azok a mintablokkok, amik a tényleges információt fogják hordozni, míg a második csoportba azok a mintablokkok kerülnek, amelyek célja a megtévesztés. Az alkalmazás függvényében egy képkockába mindkét csoportból választunk mintablokkot. Ha valaki szándékosan el akarja távolítani a vízjelet, akkor nem fogja tudni megkülönböztetni a ténylegesen információt hordozó és a megtévesztő blokkokat, ezért mindkettőt el kell távolítsa, ami már jelentős minőségromlást okozhat a videóban.

Az NCG koordináták alapján kiválasztott blokkokhoz az algoritmus a titkos kulcs alapján kiválaszt mintablokkokat mindkét csoportból. Beágyazáskor az algoritmus a mintablokkokat felskálázza a vízjelezés erősségével, majd az így kapott blokkokat az eredeti képkocka blokkjaihoz hozzáadja, vagy kivonja, attól függően, hogy a rejteni kívánt információ 1 vagy 0. Az információt a pixel fényesség értékébe rejtjük.

A tesztjeink során minden képkockába 4 bitnyi adatot helyeztünk el, négy 16x16-os blokkot felhasználva. Azért, hogy az esetlegesen kimaradt vagy kitörölt képkockák ne okozzanak gondot a detekciónál, a 4 bitnyi információt több egymást követő képkockában is elrejtettük, ezzel tovább növelve az algoritmus robusztusságát. A tesztjeink során 9 egymást követő képkockát használtunk. Így az algoritmus ellenállóvá tehetjük a képkocka elhagyások ellen, vagy az átlagolásos támadások ellen.

A detektálás folyamata

Detektáláskor a mintablokkokat keressük meg a vízjelezett képkockákon. A titkos kulcs alapján a detektor ugyanazokat a mintablokkokat állítja elő, mint a vízjel elhelyezés során. Minden képkockánál kiszámítjuk a blokkok NCG értékeit, majd ezek alapján kiválasztjuk az alkalmas blokkokat. Mivel itt már a módosított videót vizsgáljuk, itt nagyobb tűrést állítunk be az NCG értékek vizsgálatánál, mint a beültetés során.

A titkos kulcsból meghatározzuk, mely négy mintablokkot keressük az adott képkockában, majd az összes alkalmas blokkot megvizsgáljuk, tartalmazza-e a mintablokkok valamelyikét. Azt, hogy egy adott blokk milyen bitet tartalmaz (egyáltalán tartalmaz-e adatot) a vizsgált blokk és a hozzá tartozó mintablokk közti korreláció határozza meg: pozitív korreláció esetén a detektált bit 1, negatív korreláció esetén 0, korrelálatlanság esetén a vízjelezett blokk vagy nem tartalmaz adatot, vagy a használt mintablokk nem megfelelő.

Mivel több, egymást követő képkockát is használunk ugyanannak az információnak elrejtésére, ezért a ténylegesen kapott bitekről egyszerű többségi szavazással döntünk.

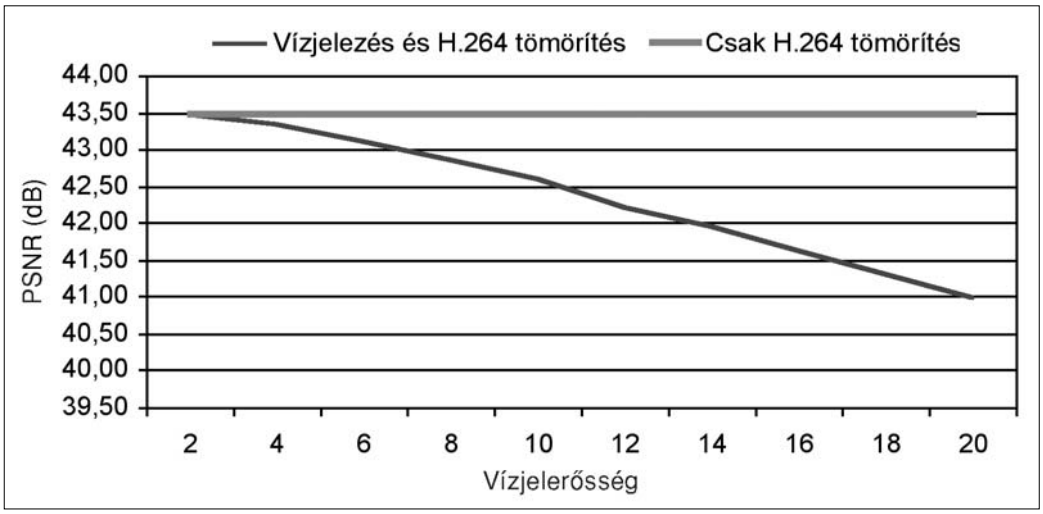
Az algoritmus a detektáláshoz nem használja az eredeti videó állományt, így vak vízjelezést valósít meg.

6. Teszteredmények

Az algoritmus működését 3 különböző videó fájlon teszteltük, melyek felbontása 720x576 pixel volt és egyenként 376 képkockából álltak. A vízjelezés erősségét 2 és 20 között állítottunk.

Az *1. ábra* bemutatja, hogy hogyan változik a videó minősége a vízjel erősségének a függvényében. Más szubjektív mérések azt az eredményt adták, hogy a 20-as erősség felé közeledve, a vízjelezett blokkok esetében már erős kockásodás figyelhető meg.

A *2. ábra* mutatja be, hogy a vízjel hogyan áll ellen a különböző módosításoknak. A tartalmakat vízjeleztük, majd a végrehajtottuk a módosítást, végül megpróbáltuk kinyerni a vízjelet a módosított tartalomból.



1. ábra
Jel-zaj viszony a vízjel erősségének függvényében

Az ábrákon látható, hogy H.264 szerinti tömörítés (1,5 Mbit/s értékkel), zajszűrés és zaj hozzáadása esetén a vízjel a beültetés erősségének a növelésével egyre jobban detektálható.

Az ábrán az is látható, hogy átméretezés, vágás és forgatás esetén a beültetés erősségének a növelése a detektort döntésképtelen állapotba hozza. Ennek az az oka, hogy a detektor elveszítette a szinkront a képkockákban található vízjellel és máshol kereste a vízjelet.

7. Összefoglalás

A bemutatott módszerrel elhelyezett vízjelek túlélik a H.264 tömörítést és azokat a támadásokat, melyek zaj hozzáadásán, vagy zajszűrésen alapulnak. A módszer fő hátránya, hogy nem ellenálló a szinkronizáció megzavarásán alapuló támadásokkal szemben.

Irodalom

[1] ISO/IEC 14496-10 and ITU-T Rec. H.264, "Advanced video coding", 2003.

[2] D. Pröfrock, M. Schlauweg, E. Müller, "A New Uncompressed-Domain Video Watermarking Approach Robust to H.264/AVC Compression", Proceedings of the IASTED International Conference on Signal Processing, Pattern Recognition and Applications (SPPRA), Austria, 2006.

[3] Jana Dittmann, Mark Stabenau, Ralf Steinmetz, "Robust MPEG Video Watermarking Technologies", Proceedings of the ACM Multimedia, 1998. pp.71–80.

2. ábra A vízjel robusztussága különböző módosítások esetén