Digitális vízjelzés, ujjlenyomatozás, adatrejtés és másolatvédelem

Pap Lőrinc

Bevezető – vízjelzés, ujjlenyomatozás

- Rejtett copyright vagy tulajdont jelölő üzenetek beágyazása digitális adatokba: hangba, képbe, videóba, dokumentumba, 3D modellbe, stb.
- Két fő típusa van:
  - Észlelhető
    - Megzavarja az eredeti információt, célja a tulajdonjog feltüntetése és a másolás védelme.
  - Nem észlelhető *(szteganográfia)*
    - A jelenléte nem észlelhető (= nem hallható vagy látható), speciális program segítségével azonban ez a rejtett információ visszanyerhető.

A vízjelzésről általánosan

- Nem digitális formája pl. a papírpénz másolásvédelmére szolgáló jelzések.
- 1992-ben hivatkoztak rá publikációban először, mint „*Electronic Water Mark*”.
- Mivel a digitális adatmásolás és -módosítás jelentősen egyszerűbb, szükség lett fejlettebb és robusztusabb vízjelzési technikákra.

Vízjelzések más felhasználása

- Használható **sértettség-ellenőrzés**re is:
    - Megváltoztatja a forrásanyagot, beleültetve tőle független, másodlagos információt. Ez a változtatás az eredetit észre nem vehető mértékben befolyásolja csupán.
    - Az eretedi adat módosítása a másodlagosat is megzavarja, ebből következően bizonyos mértékig visszahozható vagy megállapítható e változtatás helye.
    - ***Hátránya***, hogy az eredeti információ feltétlenül veszít minőségéből a másodlagos adat beültetése következtében.

Észlelhető vízjelzés

- Jelenléte **látható** / **hallható**.
- Célja, hogy feltüntesse a szerző adatait **másolás-védelem** céljából, illetve az ezt tartalmazó könyv / videó stb. címét, **reklám** céljából.

Nem észlelhető vízjelzés

szteganográfia

- Jelentése: ***rejtett írás.***
- A kriptográfiától abban különbözik, hogy itt még a kódolt üzenet jelenléte is rejtett, sőt, nem is kell kódolt legyen, csupán rejtett.
- Az elsődleges adatot nagyon kis mértékben módosítja (utolsó bitet „LSB” pl.  1 0 0 1 0 1 0 1).
- Fejlett rendszereknél a vízjelzés törlésével a hordozó adat is rongálódik.
- Célja, hogy *észlelhetetlen és eltávolíthatatlan* legyen, és minél több *információt* tartalmazzon.

Vízjelzési technikák és támadhatóságuk

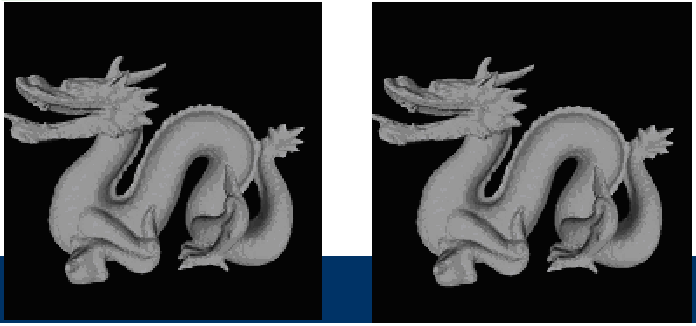
- Minden hordozó egyedi probléma, mivel a speciális változtatások ezekre való kihatása az illető médiumtól függő.
- Célja, hogy az eredeti információtól ne lehessen *(algoritmikusan)* szétválasztani:
  - az adott médiumbeli zajnak kell álcáznia magát;
  - invariáns kell legyen a tipikus transzformációkra;
  - adathordozójának veszteséges tömörítésekor is meg kell maradnia az illető háttérinformációnak.

Audió

- Az adat rejthető:
  - Gyenge minőségű audióba (alacsony bitráta) → az így megjelenő zajtól nem különböztethető meg.
  - Zajnak álcázva, mely kitölti az egész frekvencia-tartományt.
  - Megfelelően módosítva, visszhangba beültetve (ez még kellemesebben is hangzodhat mint az eredeti hanganyag (pl. kazettáról digitalizált hang)).

Videó

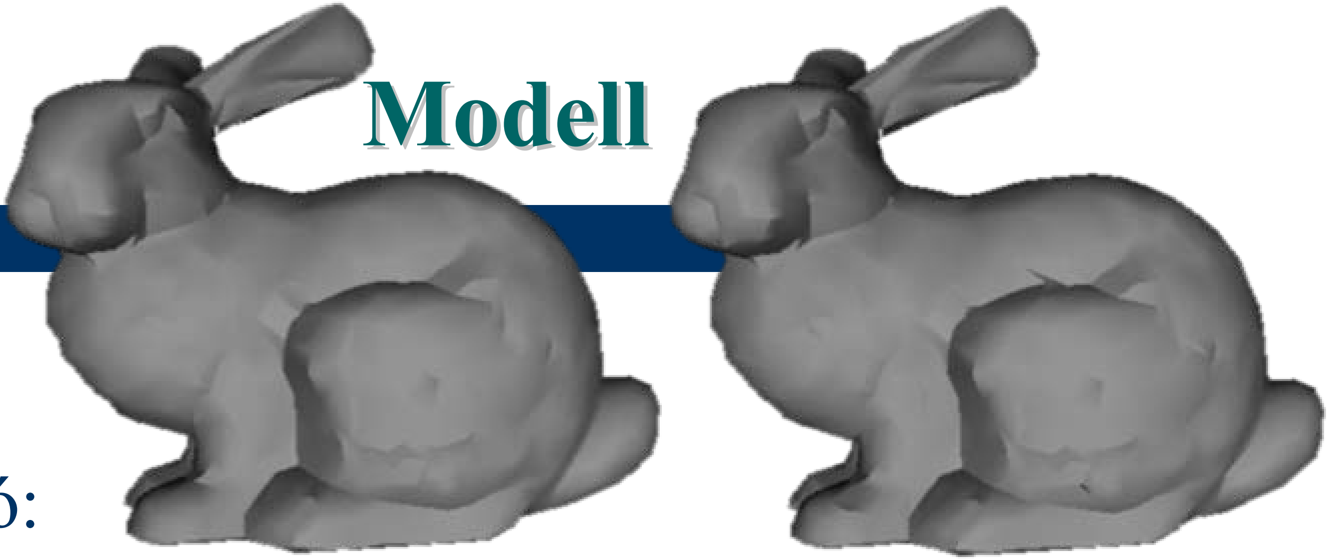
- Az adat rejthető:
  - Diszkrét Koszinusz Transzformáció *(DCT)* által, mely a videó minden képkockáját enyhén megváltoztatja. A képeket felbontja általában 8x8-as részekre, melyet DCT együtthatókká alakít át. Itt ismét kicseréljük a LSB-et, más esetben fel vagy le kerekítjük.



Modell - általánosan

- Három lépés:
  - végigmegy a modellen, kiválaszt vertexeket és ezek szomszédait úgy, hogy a későbbi módosítások minimálisak legyenek;
  - megközelíti egy zárt felülettel *(pl. elipszoid, kocka, cilinder)* vagy esetleg síkkal;
  - elmozdítja a vertexeket:
    - ami kívülre esik, az lesz a 0, ami belülre, az 1, majd ezekből a bitekből összeállítja az üzenetet.

Modell



Stanfordi nyuszi

- Strapabíró:
  - poligonegyszerűsítés;
  - poligonfelosztás;
  - zaj (egységes vagy Gauss-féle);
  - affin transzformációk;
  - fizikai 3D modell elkészítésével (~nyomtatása) majd újraszkennelésével megmaradt a vízjelzés.

Dokumentum/1

Természetes nyelv

- Természetes *(írott)* nyelv
  - A vízjel a szöveget nyelvtanilag vagy értelmileg módosítva *(ilyen nem létezik még)* egy prímszámot rejt a szövegbe:
  - **„Képpel ellentétben szövegben nincs redundancia”**

    ↓
  - **„A szövegben nincsen, a képpel ellentétben, redundancia”**

Dokumentum/2

- Beágyazható kompilálás előtt vagy után.
- Három különböző dinamikus technika van:
  - un. easter egg vízjel;
  - adatstruktúra vízjel;
  - futási nyom vízjel.
- Ujjlenyomatozás: a program beta verziójába rejtett kliens (azaz nem a tulajdonos) azonosítója.

Dokumentum/3

Programozási nyelvek – húsvéti tojás

Acrobat Forms Fill-in Plug-In Version 4.06

(c) Copyright 1999, Adobe Systems Incorporated.
All rights reserved.

The Acrobat Forms Fill-in plug-in allows users to fill in electronic forms using Acrobat.

The Widgeteers: Amer Deeba, Shawn Gaither, John MacMillan, Roberto Perelman, Scott Petersen, Jane Zhou

Management: Hitomi Kudo, Carl Orthlieb, Dina Sakahara, Rich Sutton, Lily Tran, Ada Yue

Help →
About Plug-ins →
Acrobat Forms →
Control + Alt + Shift

Az így előhozott titkos ablak a tulajdonos vagy a vevő adatait tartalmazza.

Kép - általánosan

- Az adat rejthető:
  - a fájl végéhez hozzácsatolva, így a képminőség nem romlik, de a fájlméret lényegesen megnőhet;
  - a kép ki nem használt fejlécébe;
  - szétszórva a képbe:
    - minden pixel vagy csatorna rejthet egy bitet;
    - így pl. 24 bites, 1024 x 768-as képbe 300 KB adat rejthető.
- Az adatrejtést a redundancia teszi lehetővé (ismétlődő színek).

Kép - teszt

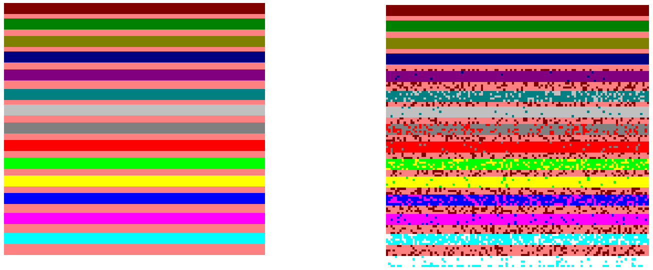
Teszt …

- Minden jelentősebb formátumot levízjelezve és manipulálva az eredeti vízjelet próbálták visszanyerni.
- Strapa-tesztek: veszteségmentes és veszteséges konverzió, bitmélység változtatása (24-bit, 8-bit, grayscale), elmosás, simítás, zaj hozzáadása és szűrése, élesítés, élerősítés, maszkolás, forgatás, nagyítás, újramintavételezés, torzítás, digitális és analóg konverzió (nyomtatás ↔ szkennelés), tükrözés stb.

Kép - konklúzió

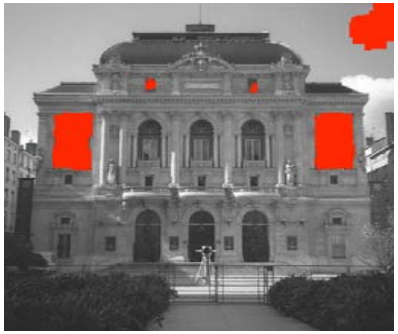
- Konklúzió:
  - Kisebb képmanipulálások, vagy veszteséges formátumba való alakítás elégséges a bit-szintű eszközök megbénítására.
  - Vannak vízjelzési technikák, melyeket csak több transzformációval, vagy azoknak az összetételével lehet kitörölni.
  - Régi Photoshoppal való vízjelzést könnyen lehetett törölni vagy lecserélni.

Kép/4



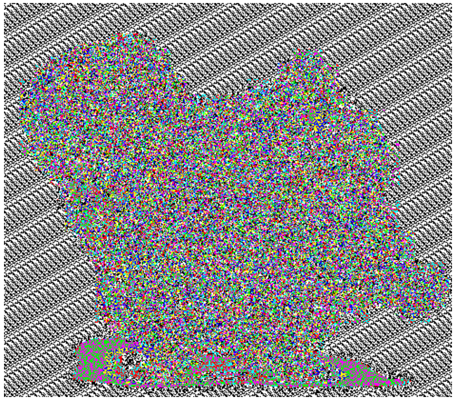
8 bites eredeti és sztegano kép *(Hide and Seek)*

Módosítások észlelése



Eredeti...

módosított…



és e kettő különbsége...

Saját program/1

- Bit szintű *(LSB)* módszer.
- A pixeleket *50%* eséllyel *1 / 256* mértékben módosítja.
- Minden pixelbe (feltételezve a 3 kanálist: R G B) elrejt a copyright üzenetből egy bitet, háromszor: hibaellenőrzésre használva.
- Sorvége jellel zárja az üzenetet.

Saját program/2

- Kiolvasásnál megnézi, hogy melyik kiolvasott üzenet szerepel leggyakrabban.
- Nem strapabíró:
    - *PNG* → *JPG* és *PNG* → *JP2* veszteségmentes tömörítésnél még működik, veszteségesnél már nem;
    - érzékeny forgatásra, elmosásra, zaj behozásra stb.
    - crop-olás során az információ részlegesen még visszanyerhető.

- **Kellett volna egy kicsit komolyabb program, mely nem ennyire egyszerű, tehát jó eséllyel „strapabíró”.**
- Ahogy elképzeltem:
  - Írsz egy első változatot, teszteled (OK)
  - Látod, hogy milyen transzformációkra NEM műkszik…
  - Definiálsz egy másik programot, mely néhányat megpróbál kivédeni,
  - Teszteled,
  - Definiálsz egy harmadik programot.

Ice age is coming!

Az egyszerű bitszintű módosítás még a crop-olásra is érzékeny.

Ý□H□+□ ;+□I›□□{kKs;□□Ai{□ □□K£Ë□q+□"□É{ingl (to a city near you ;) !)

Ice age is coming! (to a city near you ;) !)

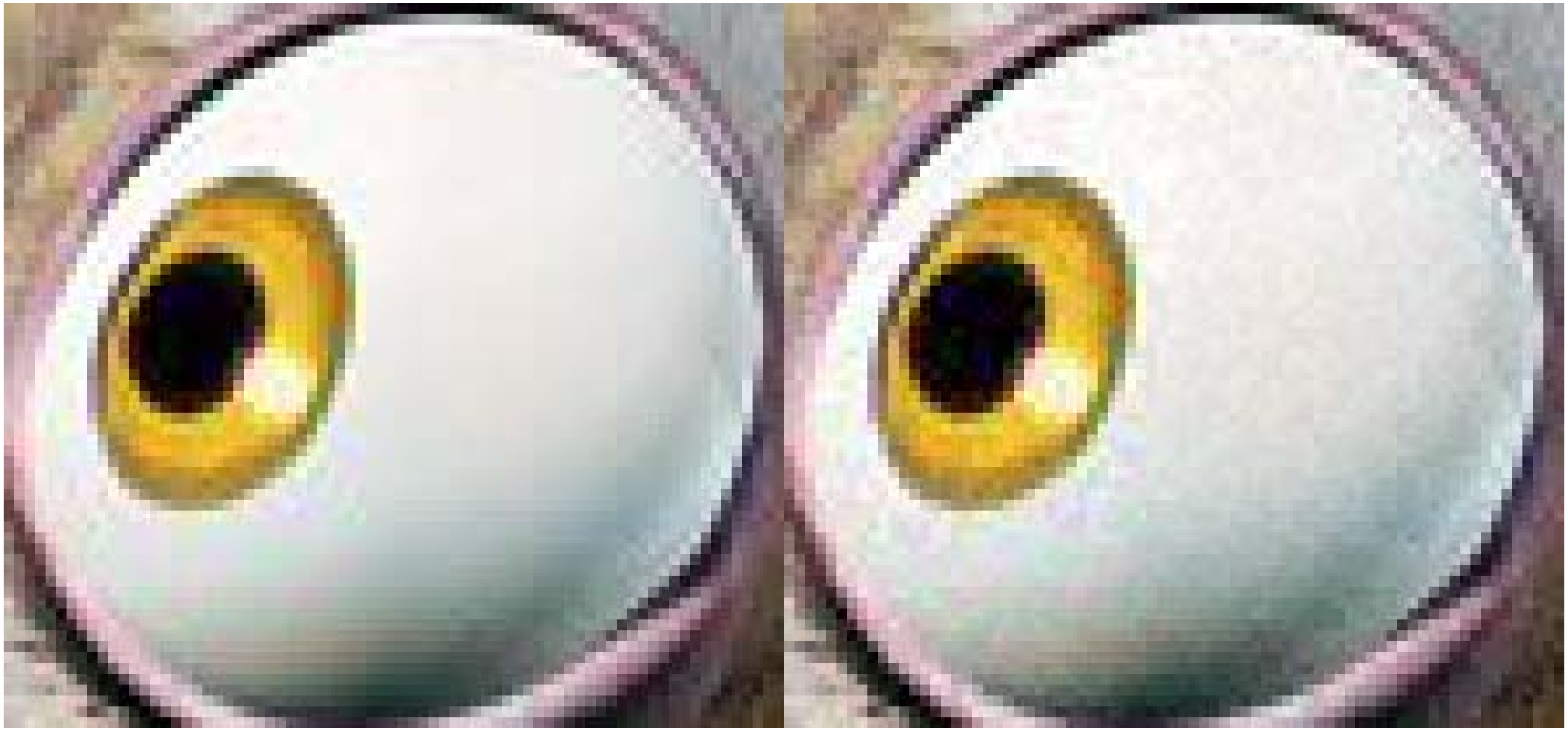
Alul az eredeti kibányászott vízjel látható, felül pedig a crop-oltból kiemelt vízjelzés.

Digimarc - általánosan

- A piac vezető kép-vízjelzéssel foglalkozó cége.
- A képbe a tulajdonos azonosítójának megfelelő ID-t, valamint a képre jellemző ún. flag-eket szór szét.
- Páronkénti, a kép pixeleiből előállított vektorok különbségén alapszik.
- A vízjelet néhány, jól megválasztott együttható utolsó bitjeibe helyezi, bitenként.

Digimarc/1

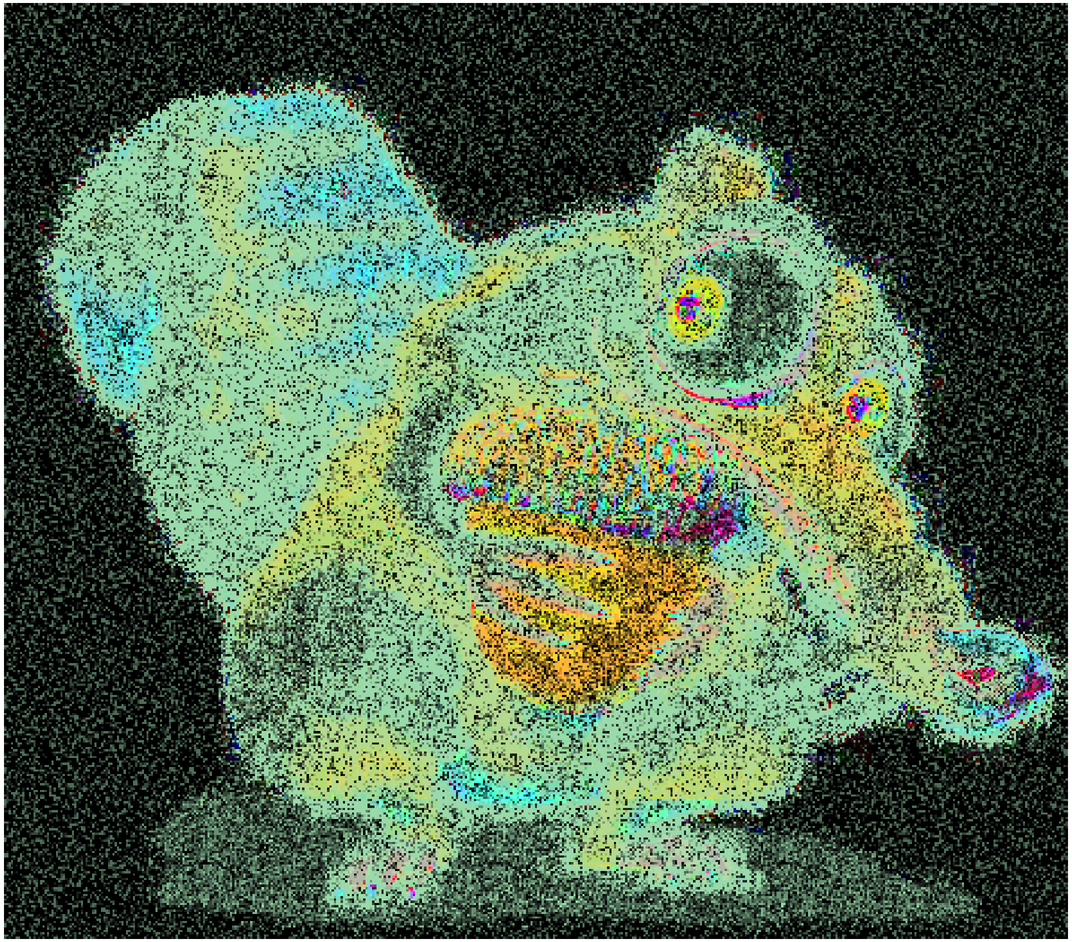
Eredeti és vízjelzett



Robusztusabb vízjel láthatóbb nyomot hagy maga után …

Digimarc/2

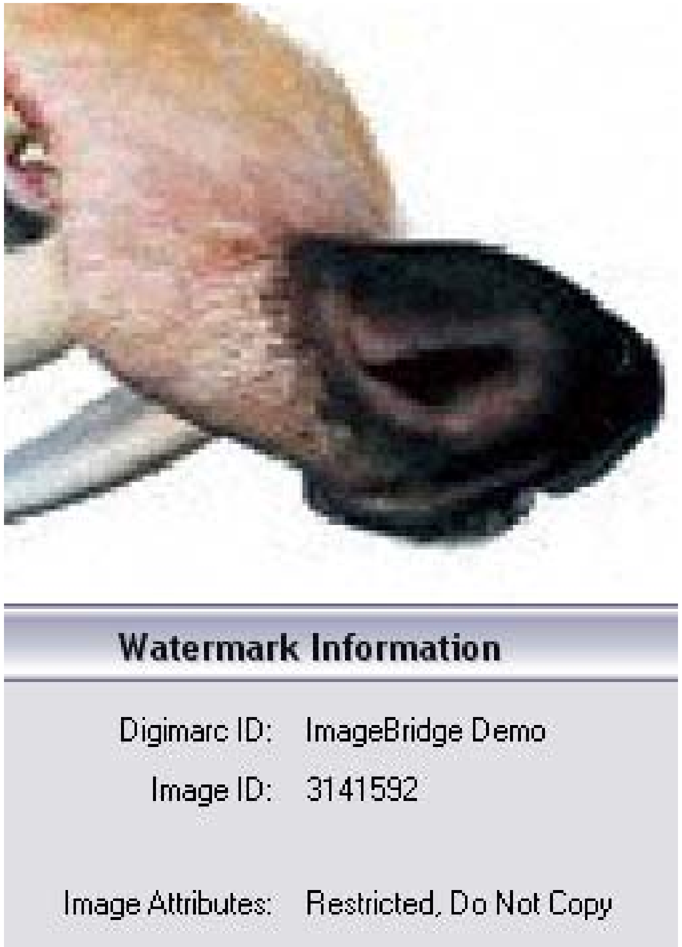
Digimark vízjelzése által behozott zaj



*= (Vizjelzett – Eredeti) * ~256*

Digimarc/3

Crop



Watermark Information

Digimarc ID: ImageBridge Demo

Image ID: 3141592

Image Attributes: Restricted, Do Not Copy

A Photoshopba beépített Digimark cég átal készített MyPictureMark nevű program vízjelző algoritmusával crop-olás után is visszanyerhető a vizjel.

Digimarc/5

Zajszűrés

Elmosás

Zajszűrésnek és elmosásnak is ellenáll.

Digimarc/6

Zaj behozása

Ha (rand() % = 0) akkor a jelenlegi pixel

= *(rand() % 256, rand() % 256, rand() % 256)*

(R,   G,   B)

Digimarc/7

Negatív

= (255 – Eredeti)

Digimarc/8

Tükrözés és forgatás

$Y = -Y$

v.

$X = -X$

$$\begin{vmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{vmatrix}, \quad a = \sim 45^\circ$$

Digimarc/9

Fekete-fehérré alakítás ill. eltolás

Elhagyjuk az egyik kanálist, vagy egyesítjük a hármat a számtani közepük szerint. (= *(R + G + B) / 3*)

A pixeleket eltoljuk (szélesség / 2)-vel x, valamint (magasság / 2)-vel y irányba.
(= *((x + width / 2) % width, (y + heigth / 2)) % heigth*)

Kép – Digimarc - konklúzió

- Konklúzió:
  - *nagyon* strapabíró:
    - többszörös veszteséges mentés (JPEG, JPEG2000);
    - nagyítást, kicsinyítést is bír, valamint több fajta harmadfokú (bicubic) újramintavételezést is (pixelek interpolálása).
  - legkisebb támogatott felbontás: 100 x 100 px.
  - Hátránya, hogy egyetlen 8 jegyű számot rendel a képhez (azonosító) + flagek, zajossá teszi a képet, ami azonban még részletnek is tűnhet nagyon gyenge minőségű kép esetén.

Amikor kérdeztem, hogy MIT CSINÁL a DIGI..., arra
gondoltam, hogy megmagyarázod, hogy MIÉRT
ENNYIREstrapabíró.

Felhasznált irodalom

- *Digital watermarking*
  http://en.wikipedia.org/wiki/Digital_watermarking

- *Digital watermark*
  http://www.webopedia.com/TERM/D/digital_watermark.html

- *Steganography - In depth explanation*
  http://www.privacycom.net/2006/05/03/steganography-in-depth-explanation/

- *Steganalysis of Images Created Using Current Steganography Software*
  http://www.jjtc.com/ihws98/jjgmu.html

- *Using Software Watermarking to Discourage Piracy*
  http://www.acm.org/crossroads/xrds10-3/watermarking.html

- *Watermarking 3D Models*
  http://www-users.cs.york.ac.uk/~adrian/Papers/Conferences/ICIP02a.pdf

- *A High-Capacity, Invertible, Data-Hiding Algorithm Using a Generalized, Reversible, Integer Transform*
  https://www.digimarc.com/tech/docs/dmrc_high_capacity.pdf