Bevezetés a Szteganográfiába

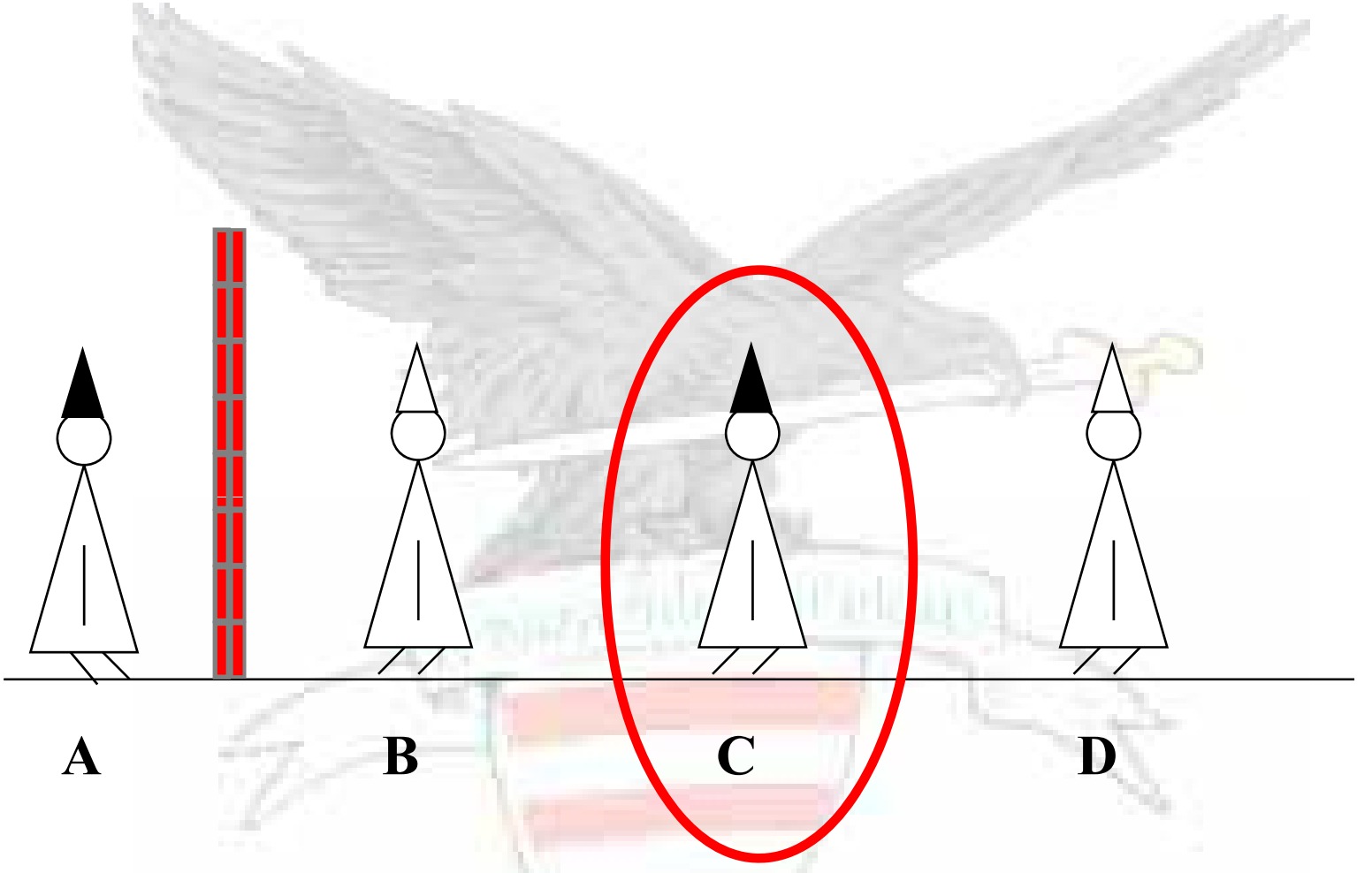
Unicsovics György

e-mail: gy.unicsovics@nbh.hu

HTE előadás, Budapest **2007. március 26**

Ki vagyok én?

- **Unicsovics György, a Nemzetbiztonsági Hivatal osztályvezetője;**
- **Híradástechnikai mérnök;**
- **Műszaki informatikai szakmérnök;**
- **ZMNE doktorandusz;**
- **Több nemzetközi IT biztonsági projekt résztvevője, illetve hazai téma veztője.**


A
B
C
D

Áttekintés:

- **Egy kis elmélet.....**
- **A szteganográfia története;**
- **Szteganográfia felosztása;**
  - **Technikai;**
  - **Nyelvészeti**
- **Szteganográfia avagy Rejtjelzés;**
- **Szteganográfia Detektálhatósága;**
- **Szteganográfiai alkalmazások;**
- **Összegzés.**

Ez talán megérne egy önálló előadást

Egy kis elmélet.....

Tények és fikciók:

- **„Közismert tény”, hogy terrorista csoportok ártalmatlannak látszó küldeményekbe ágyaznak be információkat:**

  - **Nagy forgalmú web oldalak látogatása során;**

    - eBay.com, Amazon.com

USA Today

“Terrorista csoportok Web rejtjelzés mögé rejtőzködnek”

http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

Terror groups hide behind Web encryption - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm Go

USA TODAY SPECIAL SECTIONS: USA TODAY CAREERS NETWORK

Home
News
Money
Sports
Life
Tech
Main Categories
Tech briefs
Web Guide
Tech Investor
Product reviews
More Tech
Columnists
Shareware Shelf
Talk Today
Weather

Search Go
Site Web
By LYCOS

ARCHIVES
SEARCH FOR NEWSPAPER ARTICLES
CLICK HERE

NEW E-MAIL
GET NEWS IN YOUR INBOX
Click here to get the Daily Briefing in your inbox

Tech

• E-mail this story • Subscribe to the newspaper • Sign up for e-mail news

02/05/2001 - Updated 05:17 PM ET

Terror groups hide behind Web encryption

By Jack Kelley, USA TODAY

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may be the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say.

AP

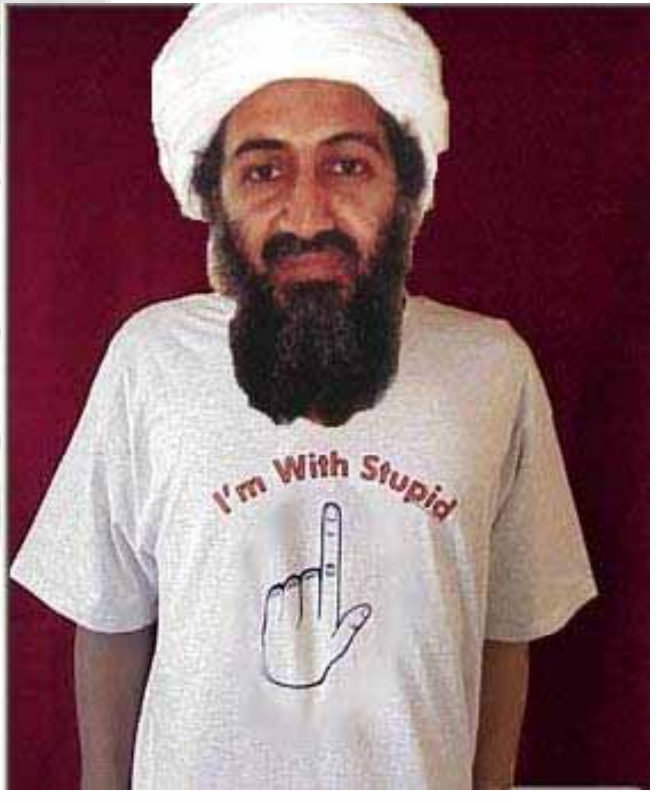
U.S. officials say Osama bin Laden is posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.

Read more

Related story • Bin Laden notes hidden in sites

"Uncrackable encryption is allowing terrorists — Hamas, Hezbollah, al-Qaida and others — to communicate about their criminal intentions without fear of outside intrusion," FBI Director Louis Freeh said last March during closed-door testimony on terrorism before a Senate panel. "They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

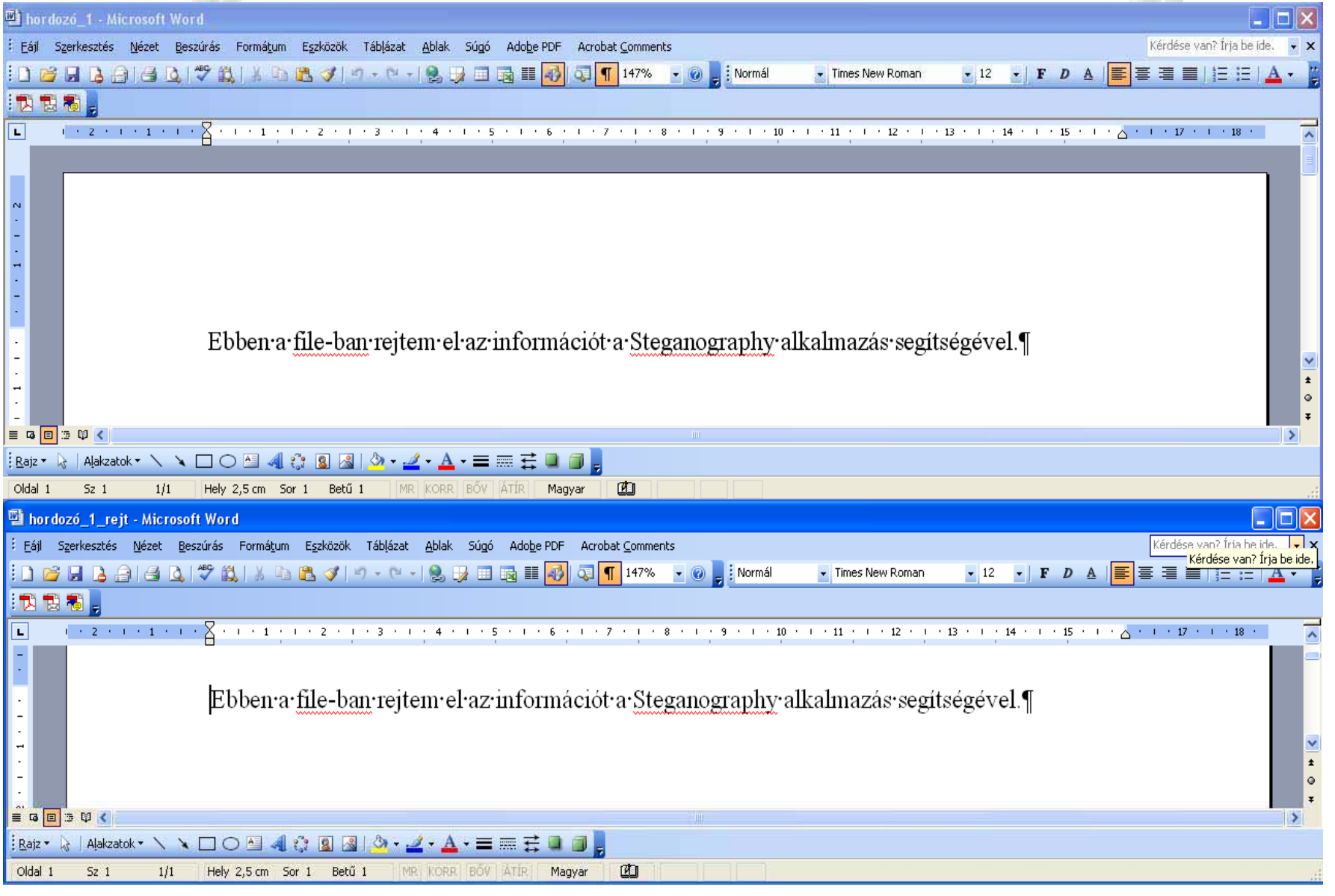
Internet



Egy kis elmélet.....folyt.

- **„Közismert tény”, hogy terrorista csoportok ártalmatlannak látszó küldeményekbe ágyaznak be információkat:**
  - **Nagy forgalmú web oldalak látogatása során;**
  - **Magánjellegű levelekbe;**

Rejtés szövegbe



Egy kis elmélet.....

- **„Közismert tény”, hogy terrorista csoportok ártalmatlannak látszó küldeményekbe ágyaznak be információkat:**
  - **Nagy forgalmú web oldalak látogatása során;**
  - **Magánjellegű levelekbe;**
  - **Publikus hírcsoportok oldalain;**

Wired

“Bin Laden: Steganography Master?”

http://www.wired.com/news/politics/0,1283,41658,00.html

A szteganográfia története

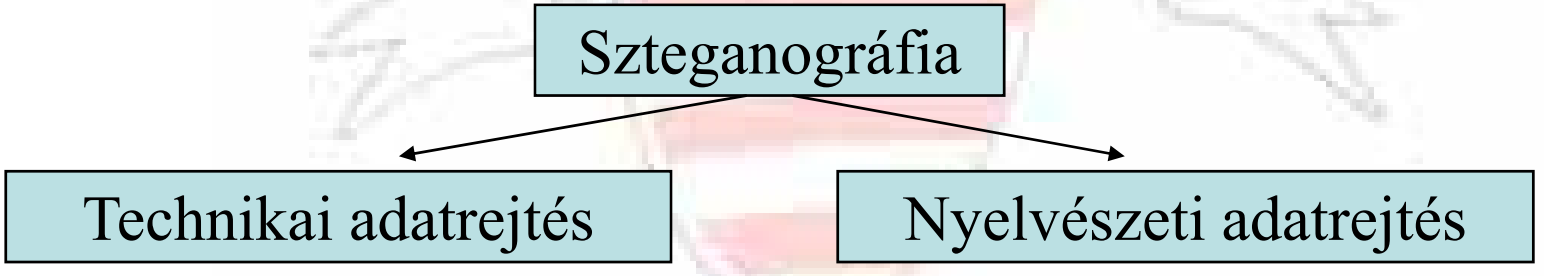
Steganography ≠ Stenography

Már az ókoriak is.....

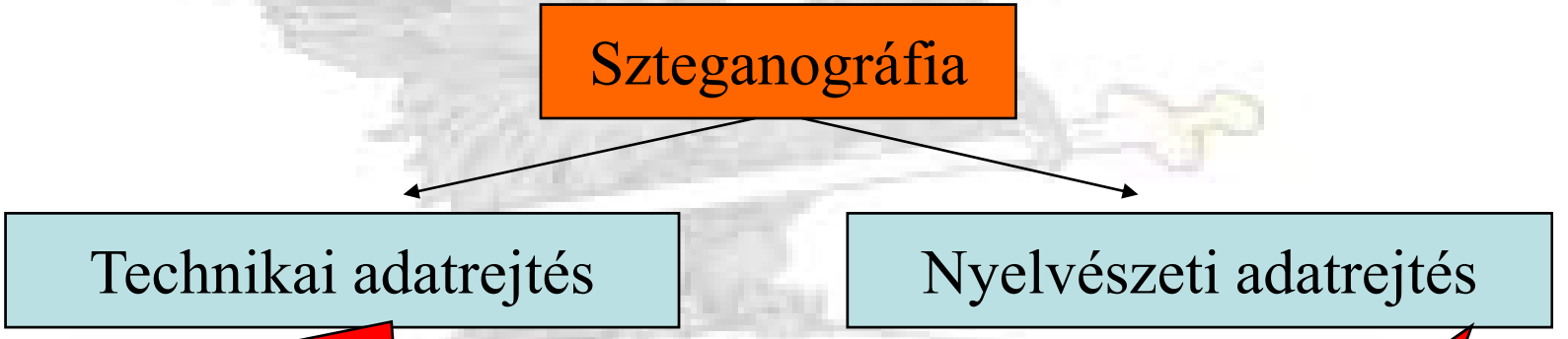
Szteganográfia jelentése és célja:

- Szteganográfia a rejtett, vagy fedett írás művészete. Célja a kommunikáció tényének elrejtése a harmadik fél elől.

Szteganográfia fő csoportjai:



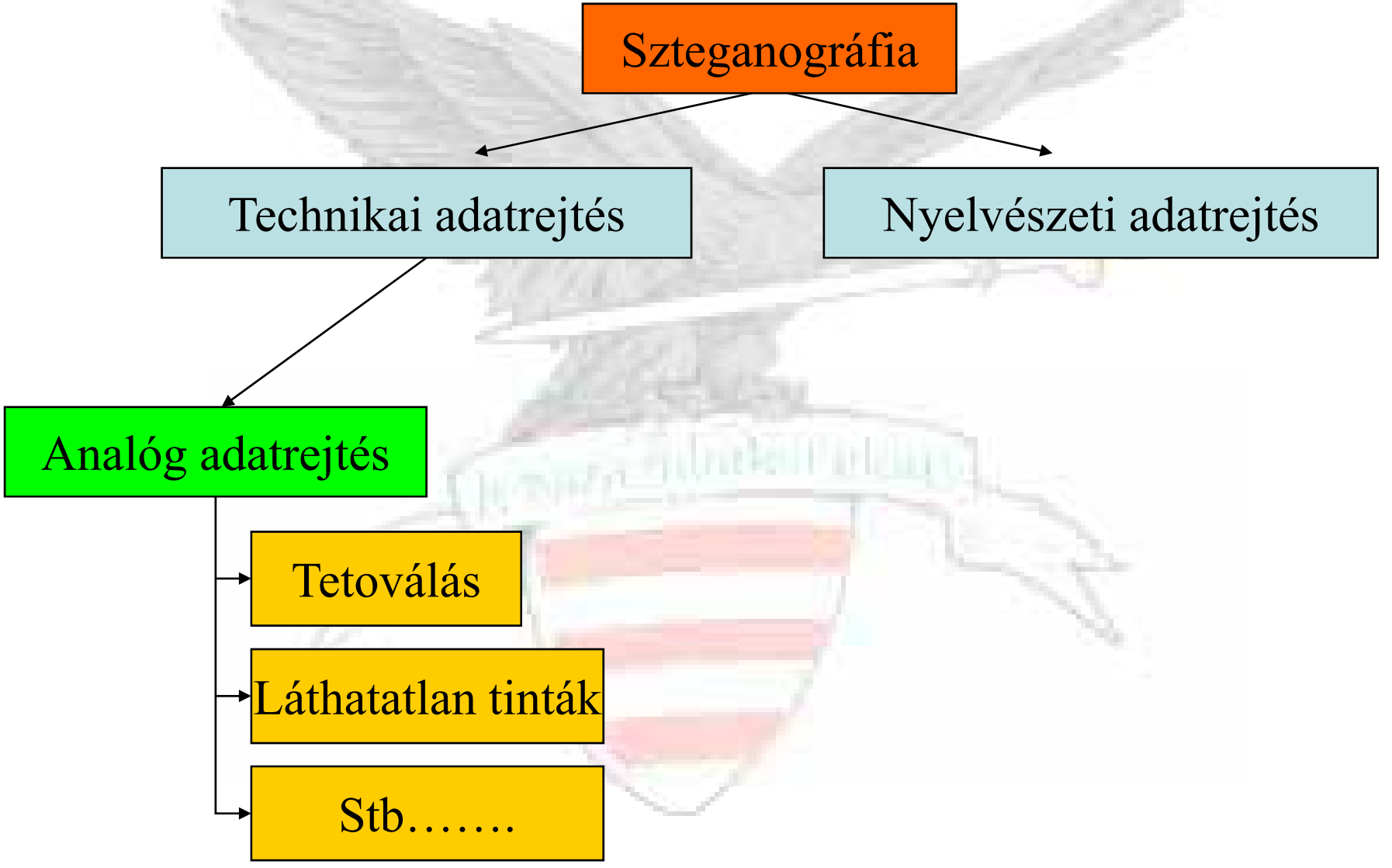
Szteganográfia felosztása



Tudományos módszereket használ az információ elrejtéséhez, amely módszerek analóg és digitális formában megjeleníthetők lehetnek.

Az üzeneteket valamely nem magától érthetődő módon rejti el a hordozóban, pl. zsargon kódként, vagy szemagrammaként.

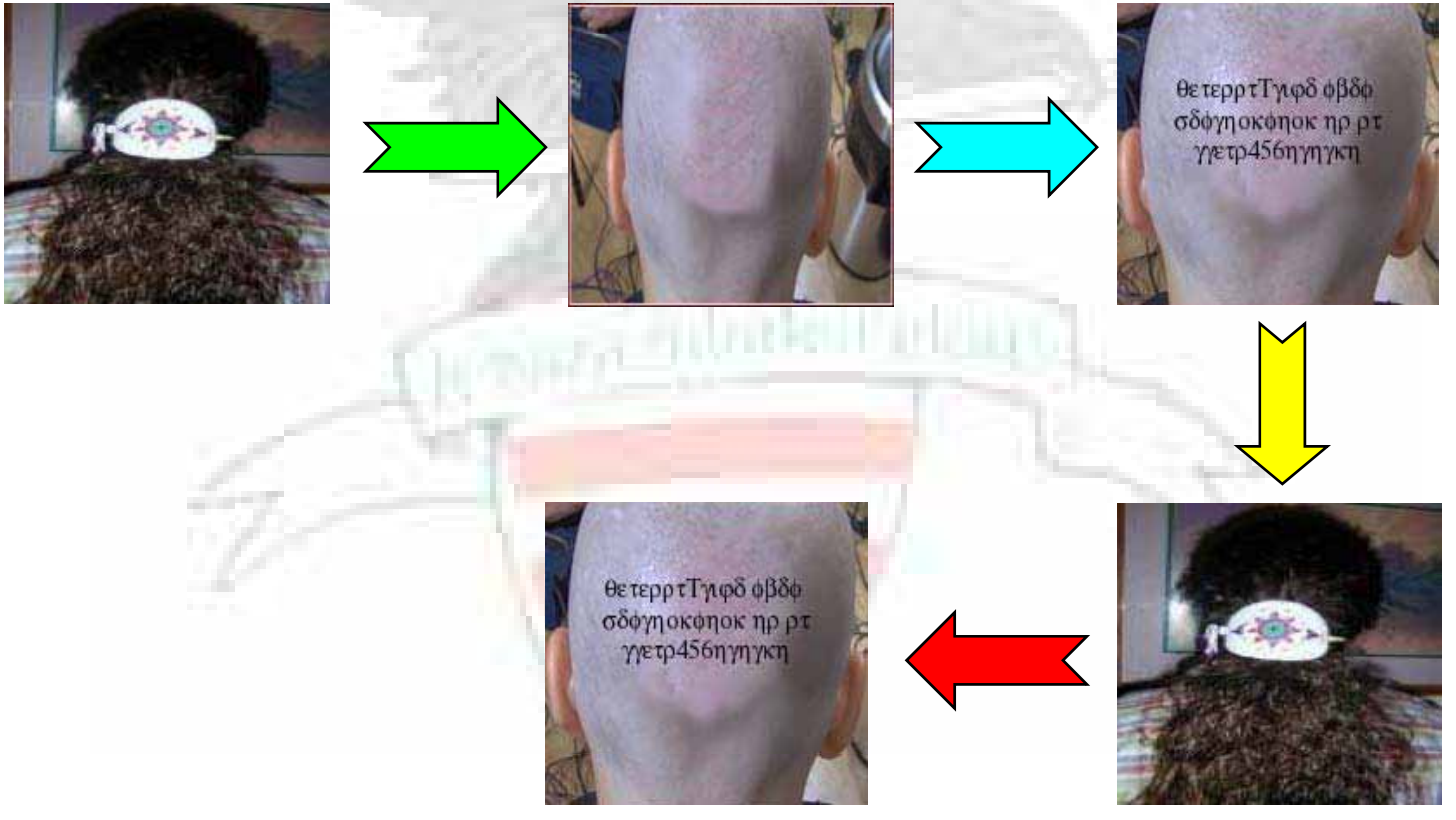
Szteganográfia felosztása folyt.



A technikai szteganográfia

Analóg adatrejtés:

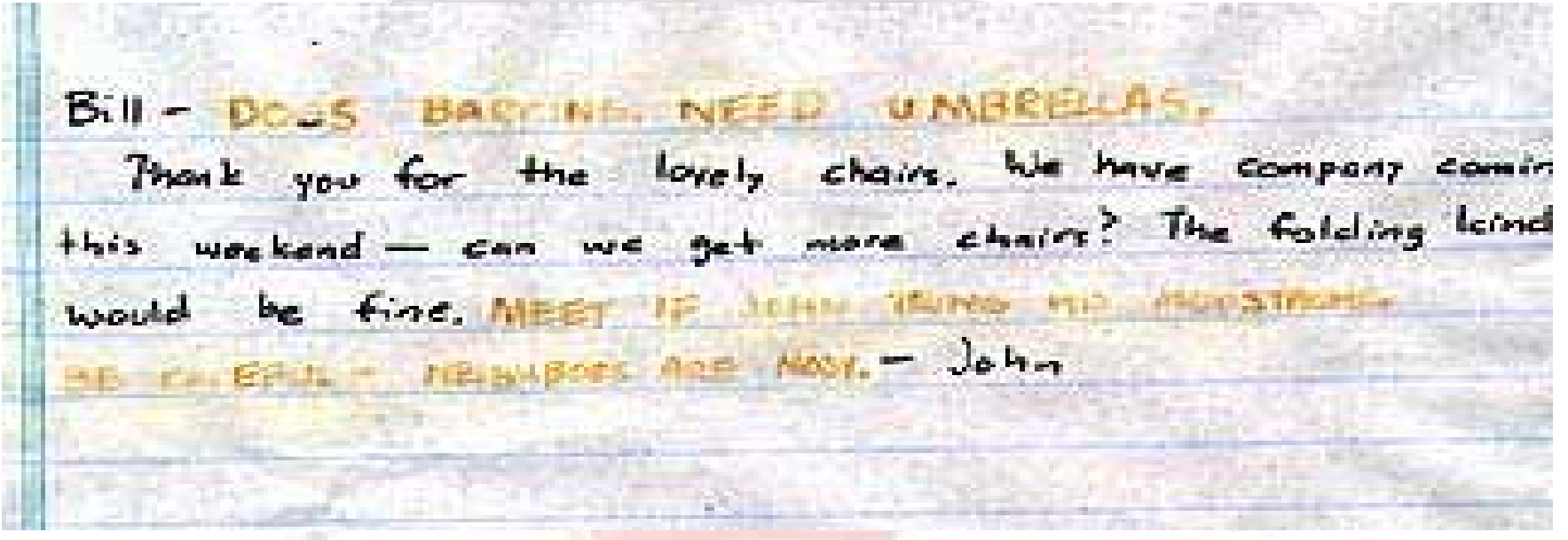
- Tetoválás:



A technikai szteganográfia folyt.

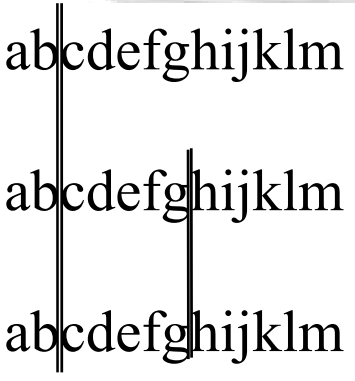
Analóg adatrejtés:

- Láthatatlan tinták:



Analóg rejtés szövegbe

Betűfont helyének vízszintes megváltoztatása



- Normál elhelyezkedés.

- A „b” betű utáni betűköz mértéke **1p ritkítva,** míg a „g” betű utáni köz **1p sürítve.**

- A „b” betű utáni betűköz mértéke **0,5p ritkítva,** míg a „g” betű utáni köz **0,5p sürítve.**

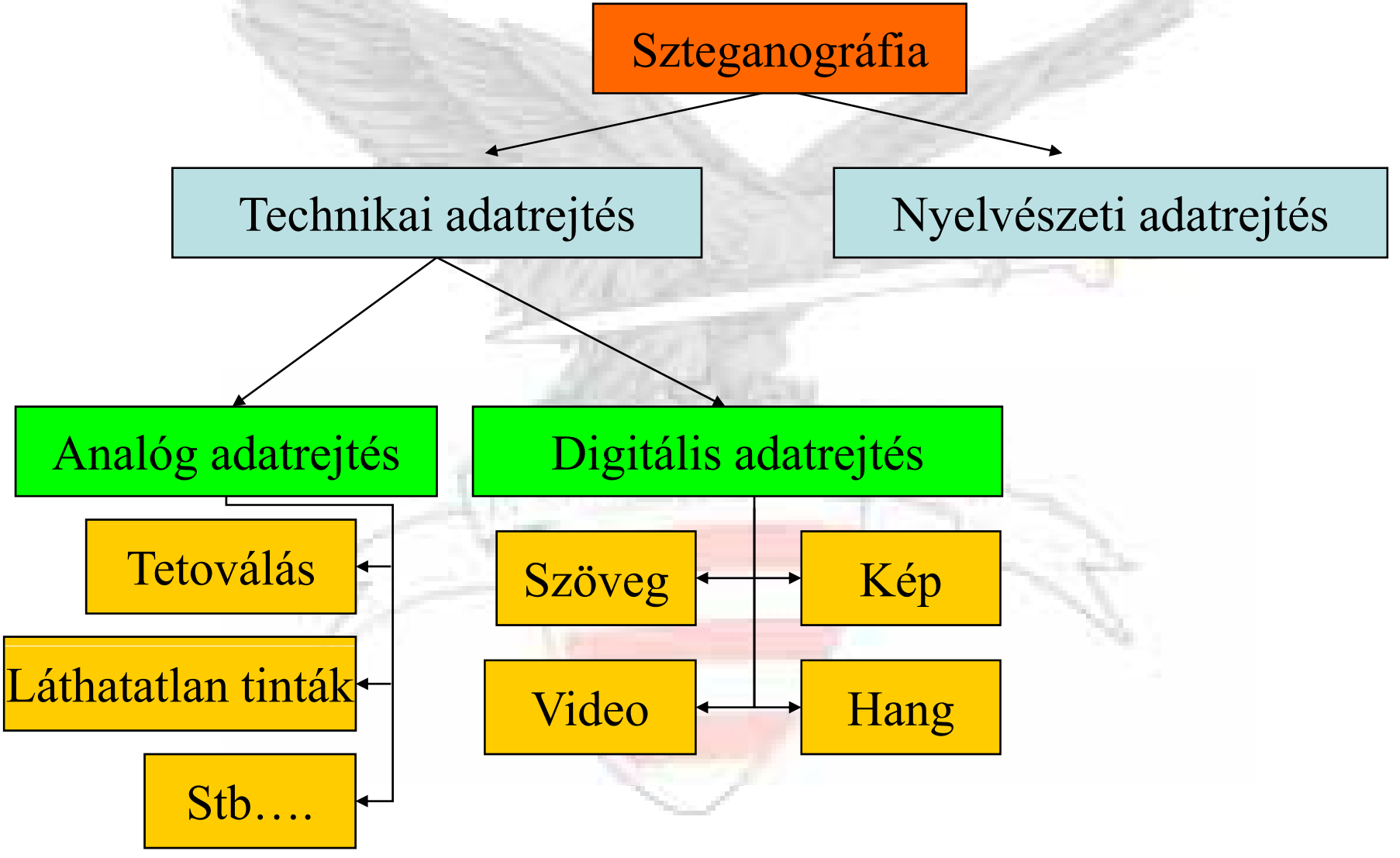
Betűfont helyének függőleges megváltoztatása

- Normál elhelyezkedés.

- Az „e” betű elhelyezése **1p emelt,** míg a „k” betű elhelyezése csak **0,5p emelt.**

- A „c” betű elhelyezése **1p süllyesztett,** míg az „m” betű csak **0,5p süllyesztett.**

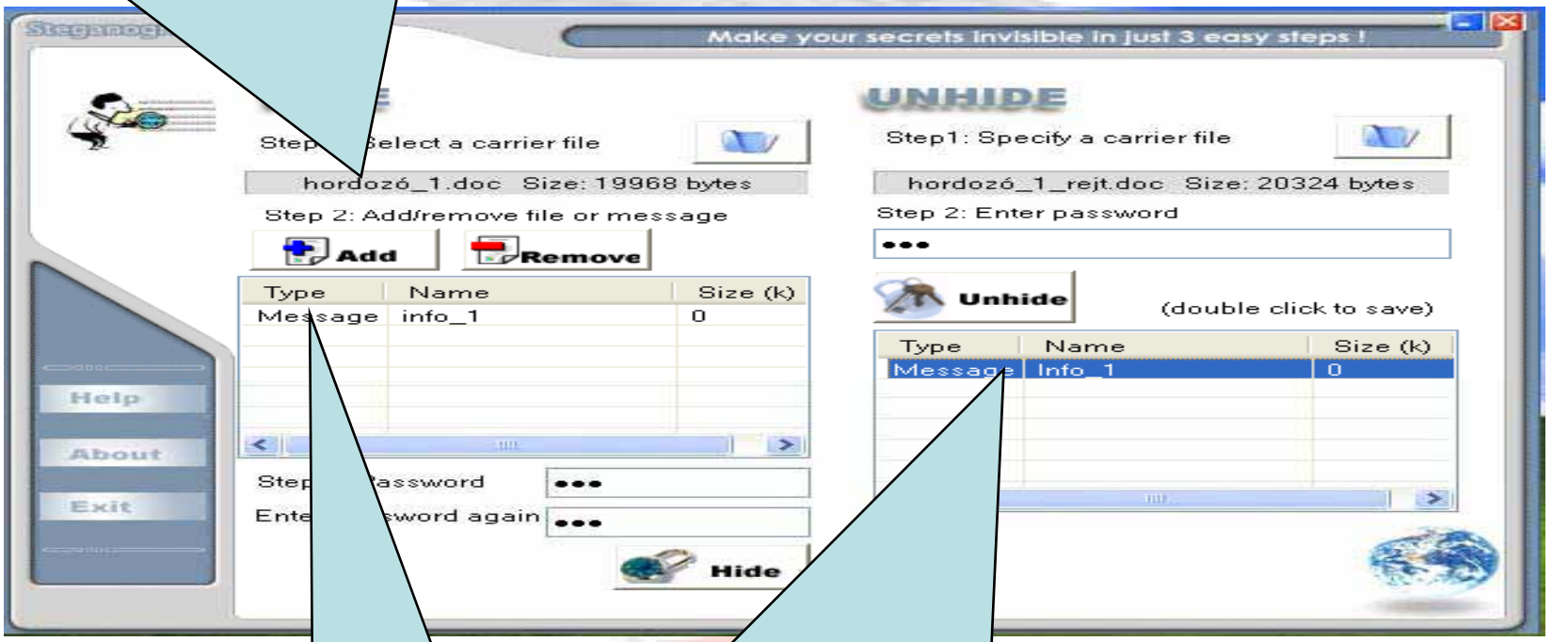
Szteganográfia felosztása folyt.



A technikai szteganográfia

Digitális adatrejtés szövegbe:

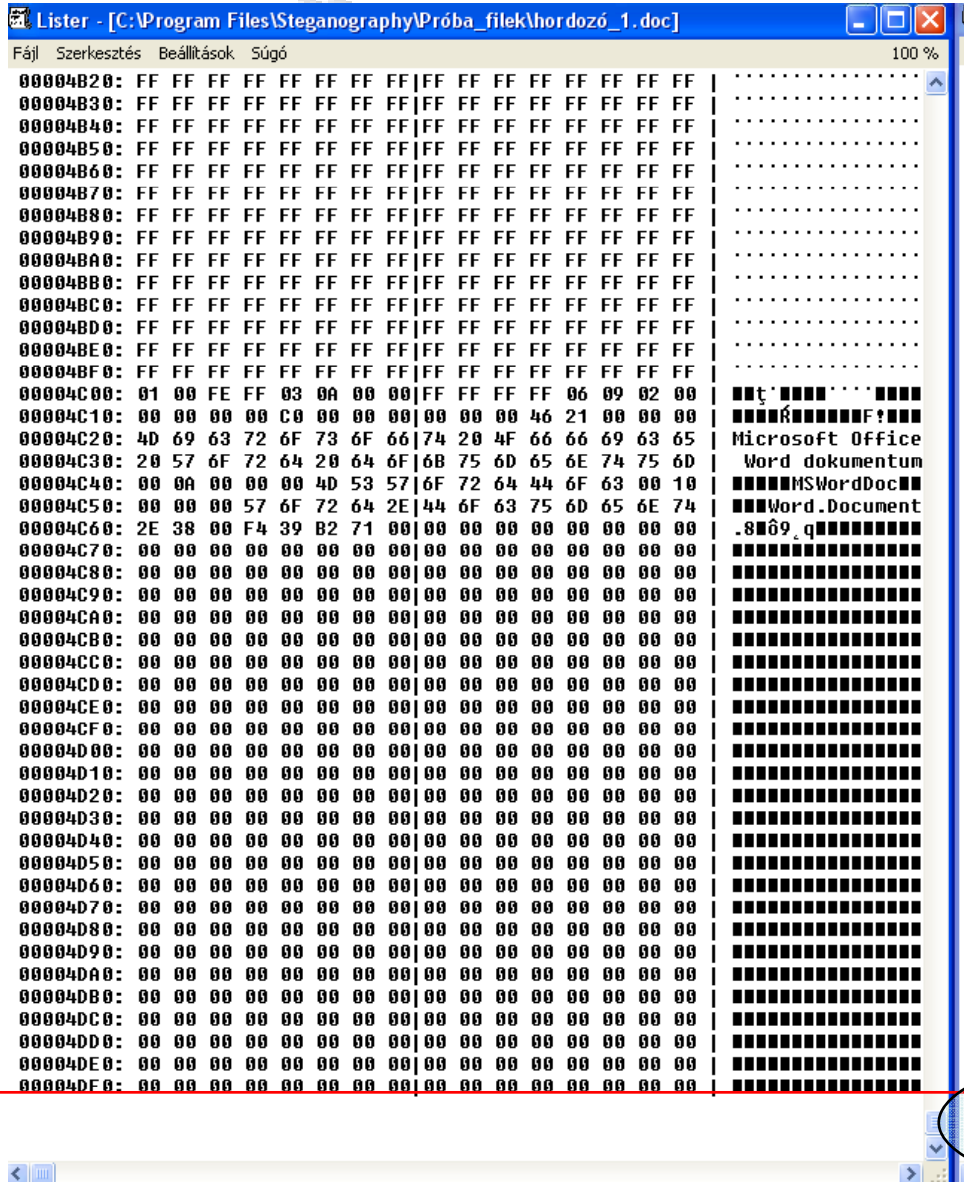
Ebben a file-ban rejtem el az információt a Steganography alkalmazás segítségével.

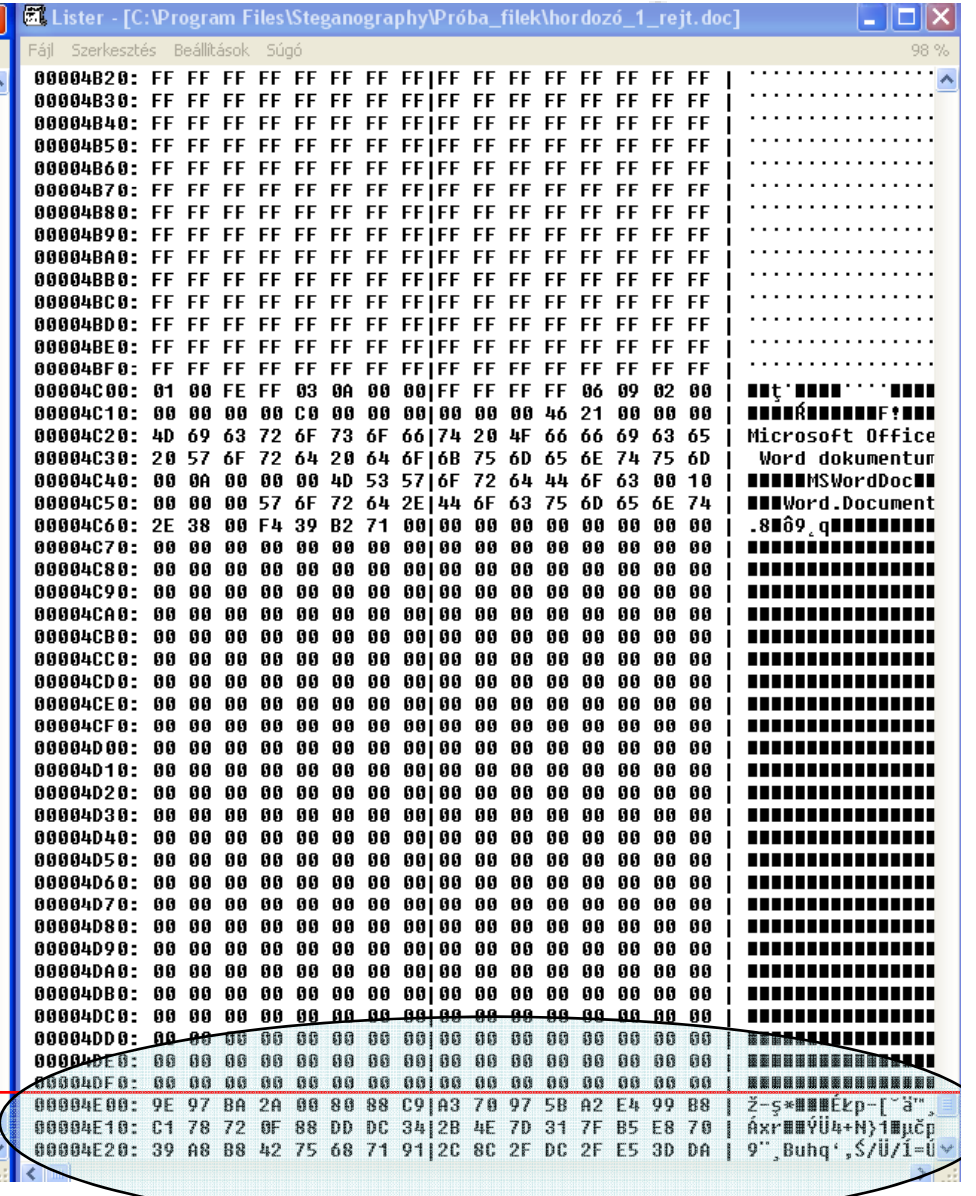


Direkt szövegbevitelt alkalmaztam

Ez itt a szöveges üzenet, amelyet igyekszem sikeresen elrejteni a beavatatlan szemlélők elől. A program meglehetős hatékonxsággal képes szöveges állományokat direkt módon beágyazni.....

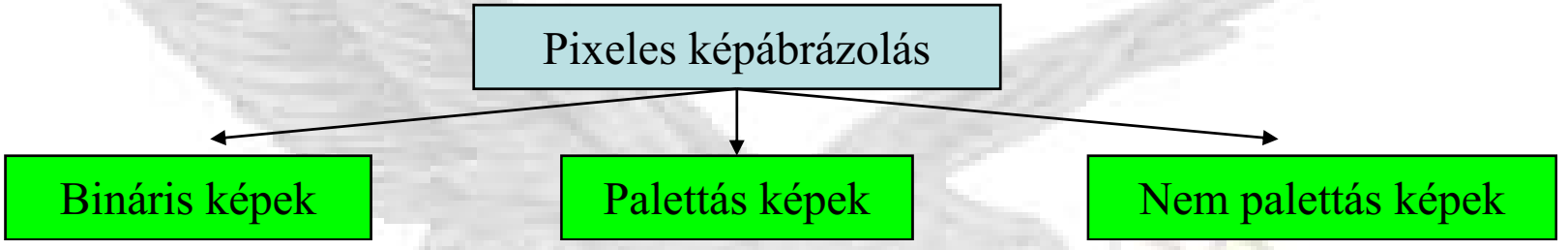
Digitális rejtés szövegbe folyt.



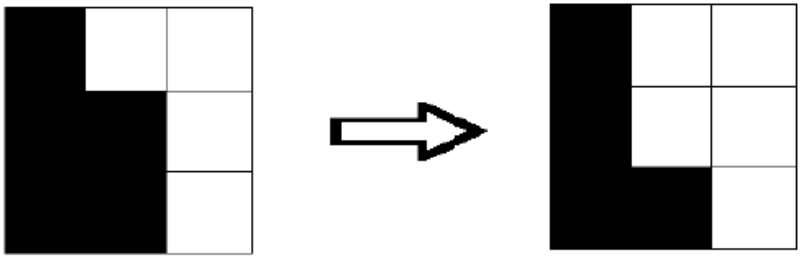


A technikai szteganográfia folyt.

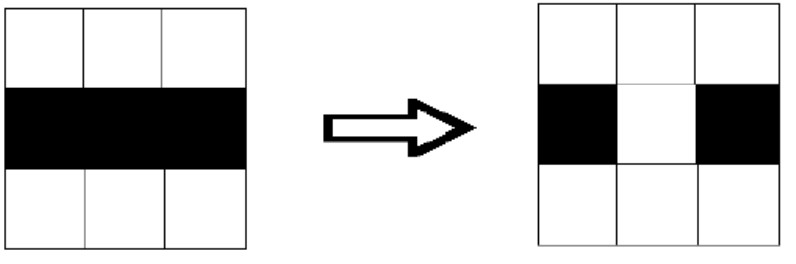
Digitális adatrejtés képekbe (elméleti háttér):



Adatrejtés bináris képekbe



Bináris kép pixelcseréje, ami alig észrevehető

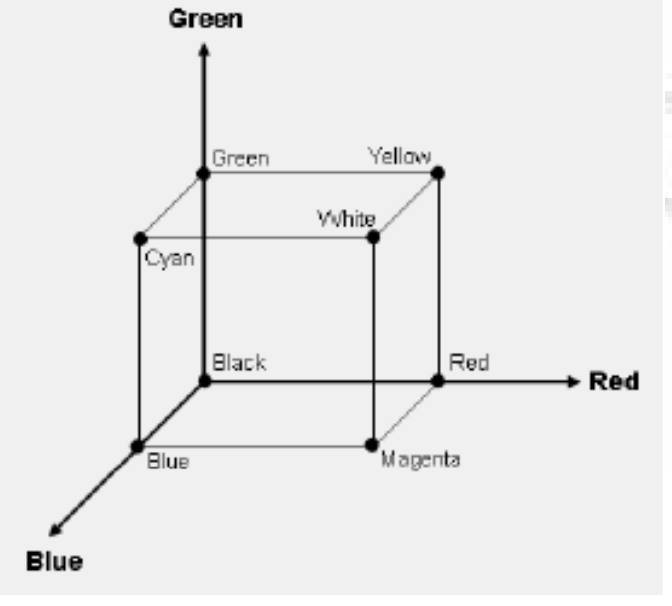


Bináris kép pixelcseréje, ami már szembetűnő

A technikai szteganográfia folyt.

Digitális adatrejtés képekbe:

- **Minden egyes képpont színét 3-3 byte határozza meg. (Többféle színábrázolás is van, ez itt csak az egyik alapelve).**
- **Egy pixel 2^(8*3) ^(8*3)=16 777 216 k =16 777 216 különböző színt vehet fel**
- **RGB színnégyzet,**

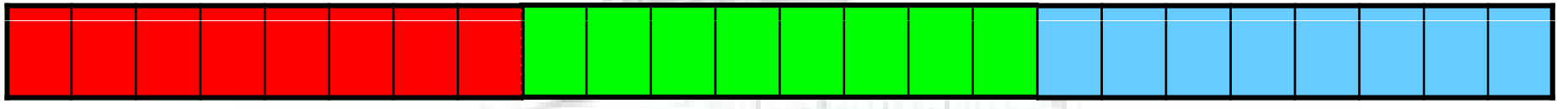


A technikai szteganográfia folyt.

Digitális adatrejtés képekbe:

- **Az adatrejtés BMP képekbe:**

  - LSB rejtés fedőképekben.



Vörös **Zöld** **Kék**

A technikai szteganográfia folyt.

Digitális adatrejtés képekbe:

Az adatrejtés palettás képekbe:

A palettás képeknél a pixelek értéke 8 bit, így a paletta 256 elemű;

Eltérések az egyes paletták színsorrendjei között

A technikai szteganográfia folyt.

Digitális adatrejtés képekbe:

Az adatrejtés JPEG képekbe:

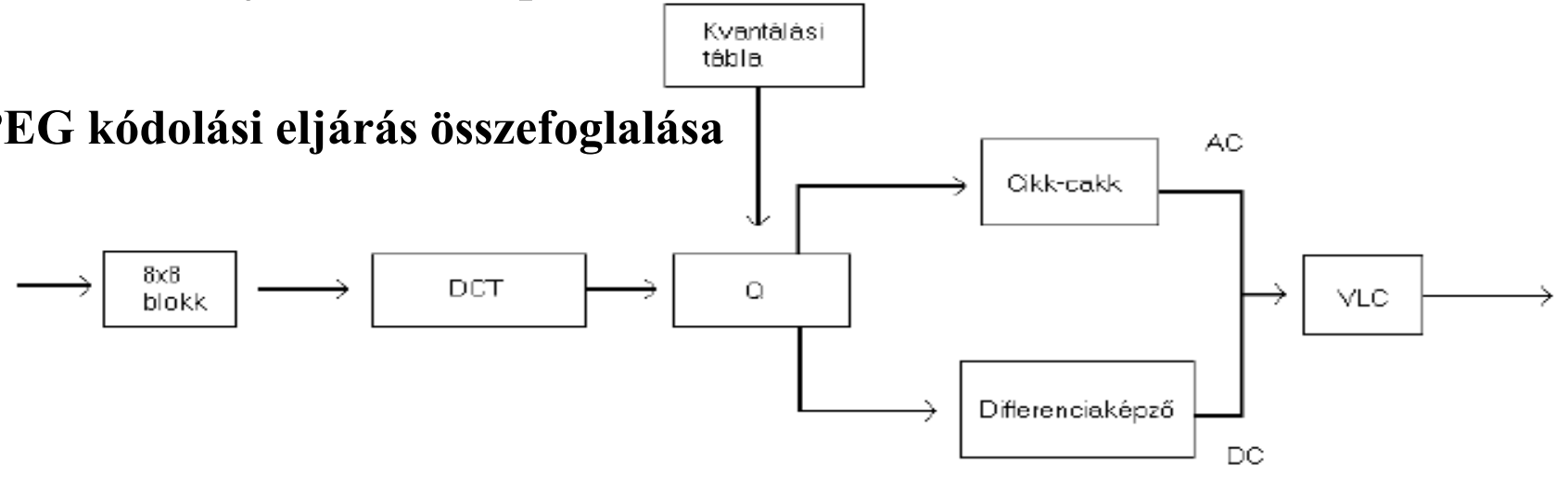
- JPEG = Joint Photographic Expert Group;
- Folytonos színtónusú állóképek digitális kódolása;
- Előnye a 65535x65535 képméret;
- Kódoló és dekódoló szimmetrikus felépítésű
- Tömörítés aránya szabadon paraméterezhető;
- Tömörítés hatásfoka és a képminőség fordított arányban áll egymással;
- Alapvetően veszteséges tömörítés, de ismert a veszteségmentes változat is, amely DPCM kódolást alkalmaz,
- A JPEG leggyakoribb tömörítési változata a DCT alapú szekvenciális kódolás;

A technikai szteganográfia folyt.

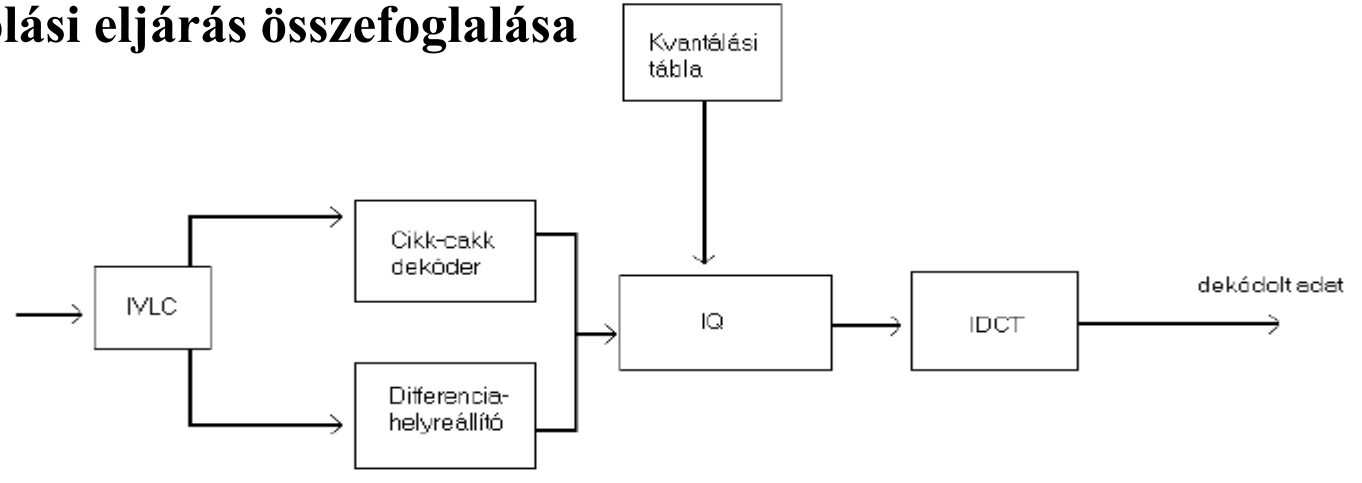
Digitális adatrejtés képekbe:

Az adatrejtés JPEG képekbe:

A JPEG kódolási eljárás összefoglalása



A JPEG dekódolási eljárás összefoglalása



A technikai szteganográfia folyt.

Digitális adatrejtés hanganyagba:

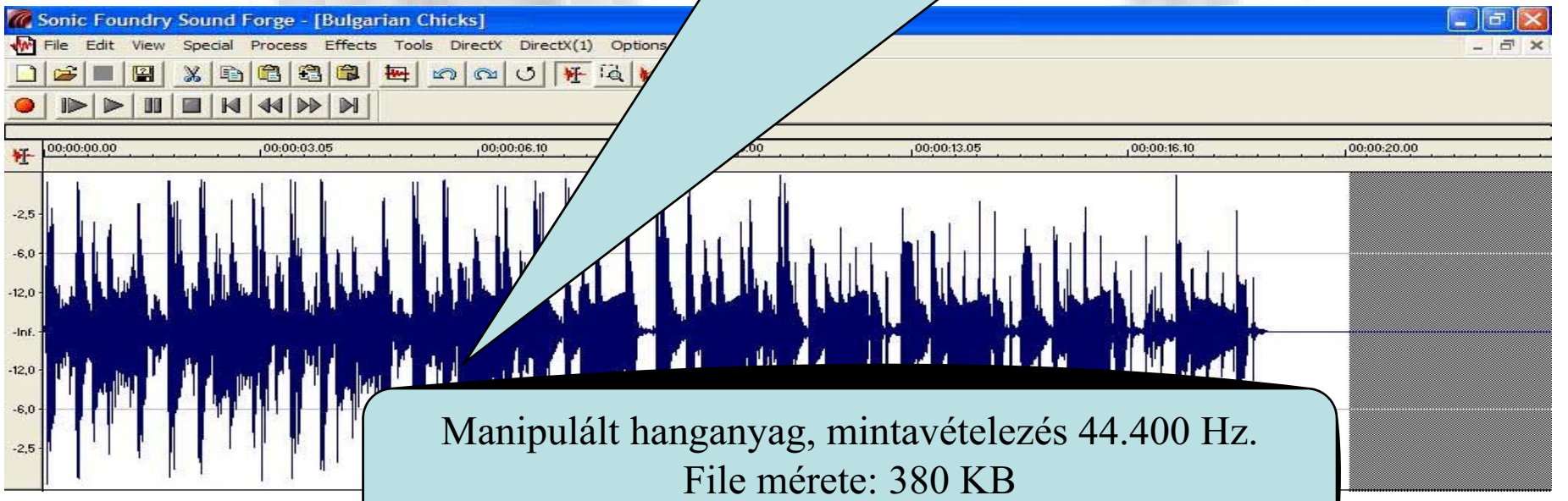
- **Ember számára hallhatatlan a változás az eredeti és a sztegomédia között;**
- **A sztegomédia statisztikai és tömörítési karakterisztikája közötti különbség minimális;**
- **Általános eljárásokat túl kell élnie (például tömörítés, kismértékű zajosítás, szűrés);**
- **A hanganyagban található a beágyazott információ, és nem az audiofájl fejlécében vagy kiterjesztésében.**

- **Az emberi hallás hallótartománya;**
- **Elfedési jelenség;**
- **Két hangot csak akkor tudunk kettőnek hallani, ha a kettő között egy minimális idő eltelik.**

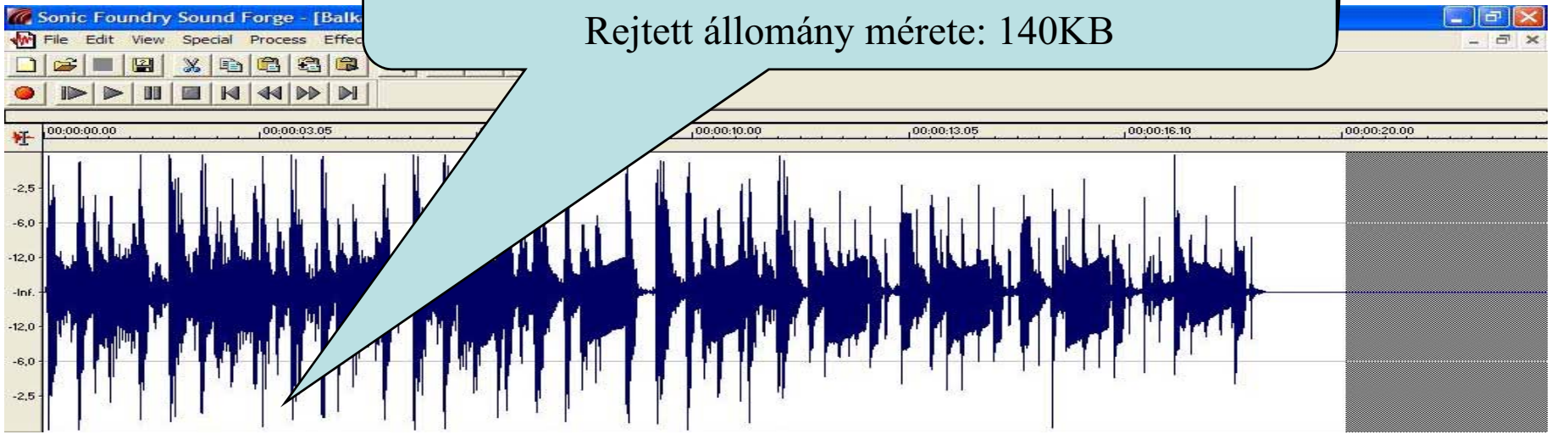
A technikai szteganográfia folyt.

Digitális adatrejtés har

Eredeti MP3 hanganyag, mintavételezés 44.400 Hz.
File mérete: 380 KB

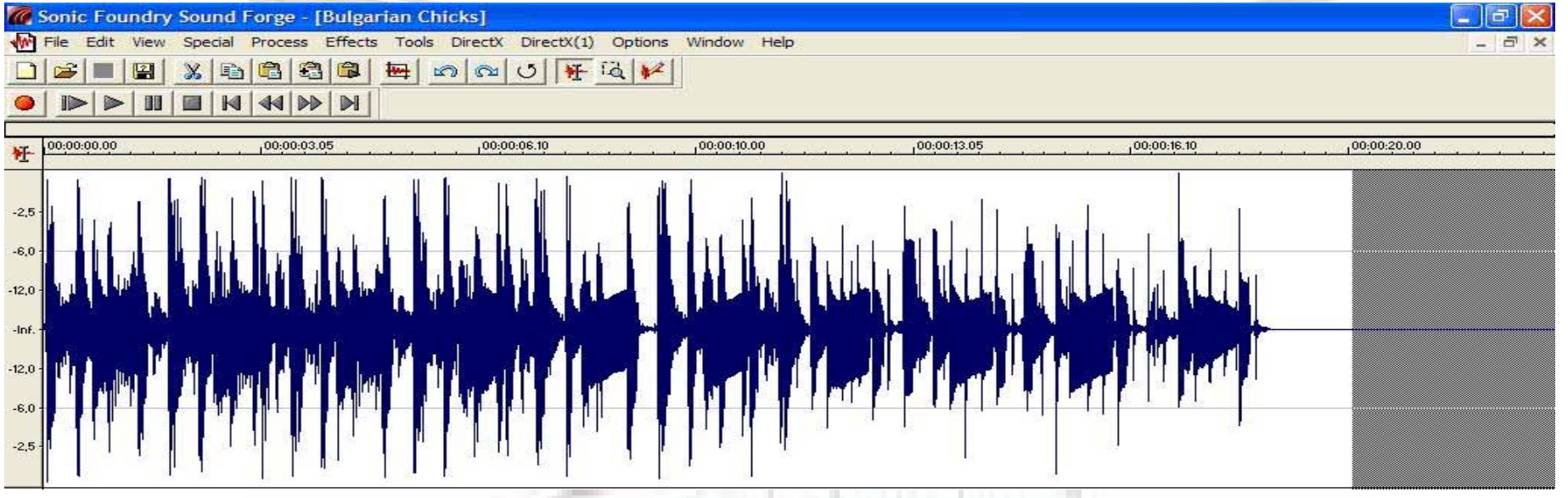


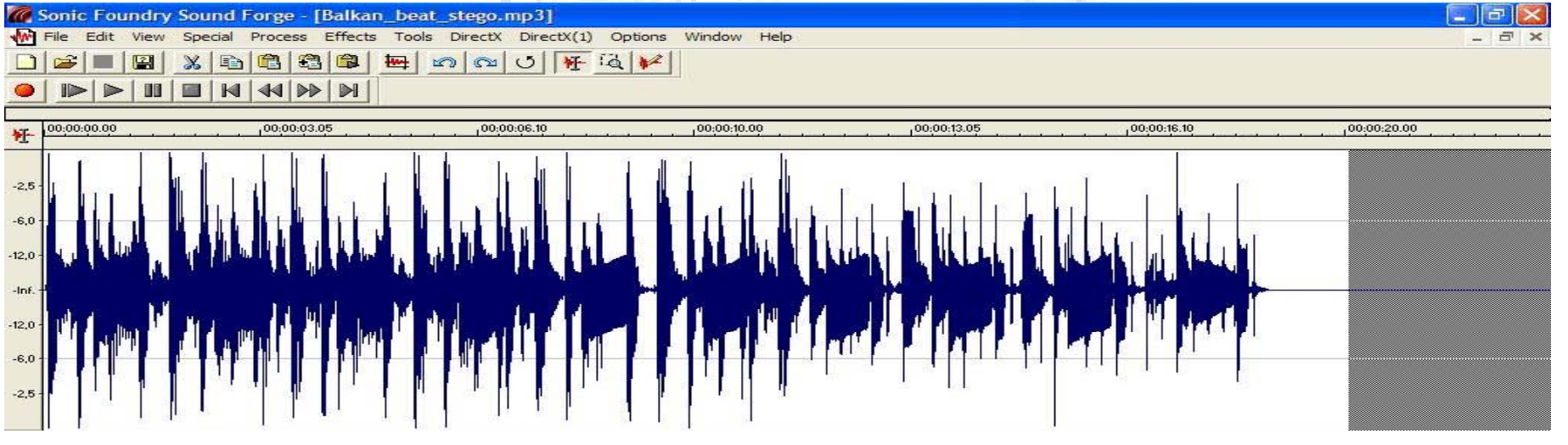
Manipulált hanganyag, mintavételezés 44.400 Hz.
File mérete: 380 KB
Rejtett állomány mérete: 140KB



A technikai szteganográfia folyt.

Digitális adatrejtés hanganyagba:





A technikai szteganográfia folyt.

Digitális adatrejtés mozgóképbe:

1. A gyorsaság és az alacsony sávszélesség miatt minél kisebb bitsebességen, de jó minőséggel, minél kisebb hibával átvinni a csatornán a videót,
2. Az illegális másolatok terjedésének a megakadályozása.

Adatrejtés tömörítetlen videóba:

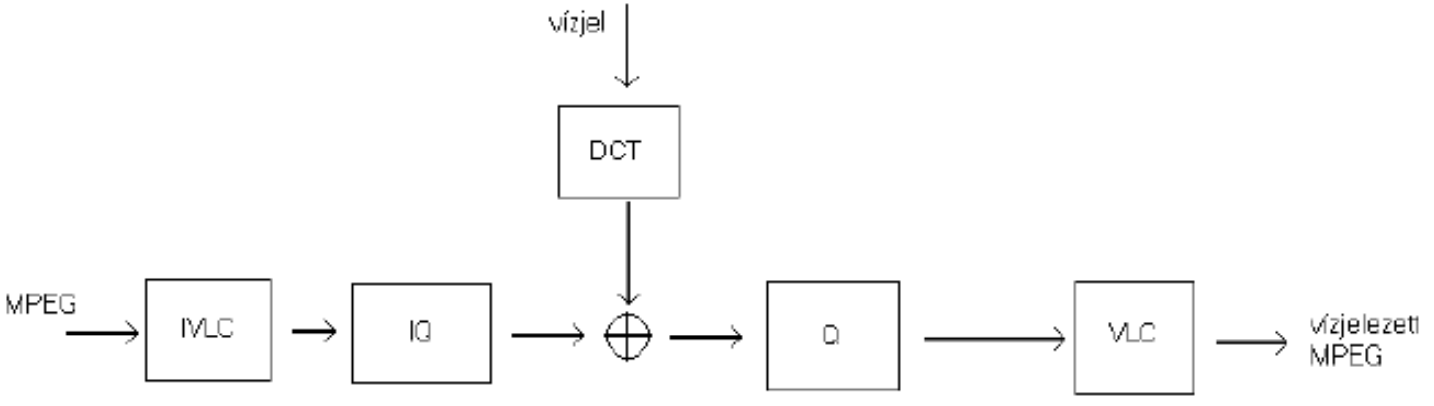
- **Szórt spektrumú vízjel;**
- **Nyilvános lulcsú vízjelzés.**

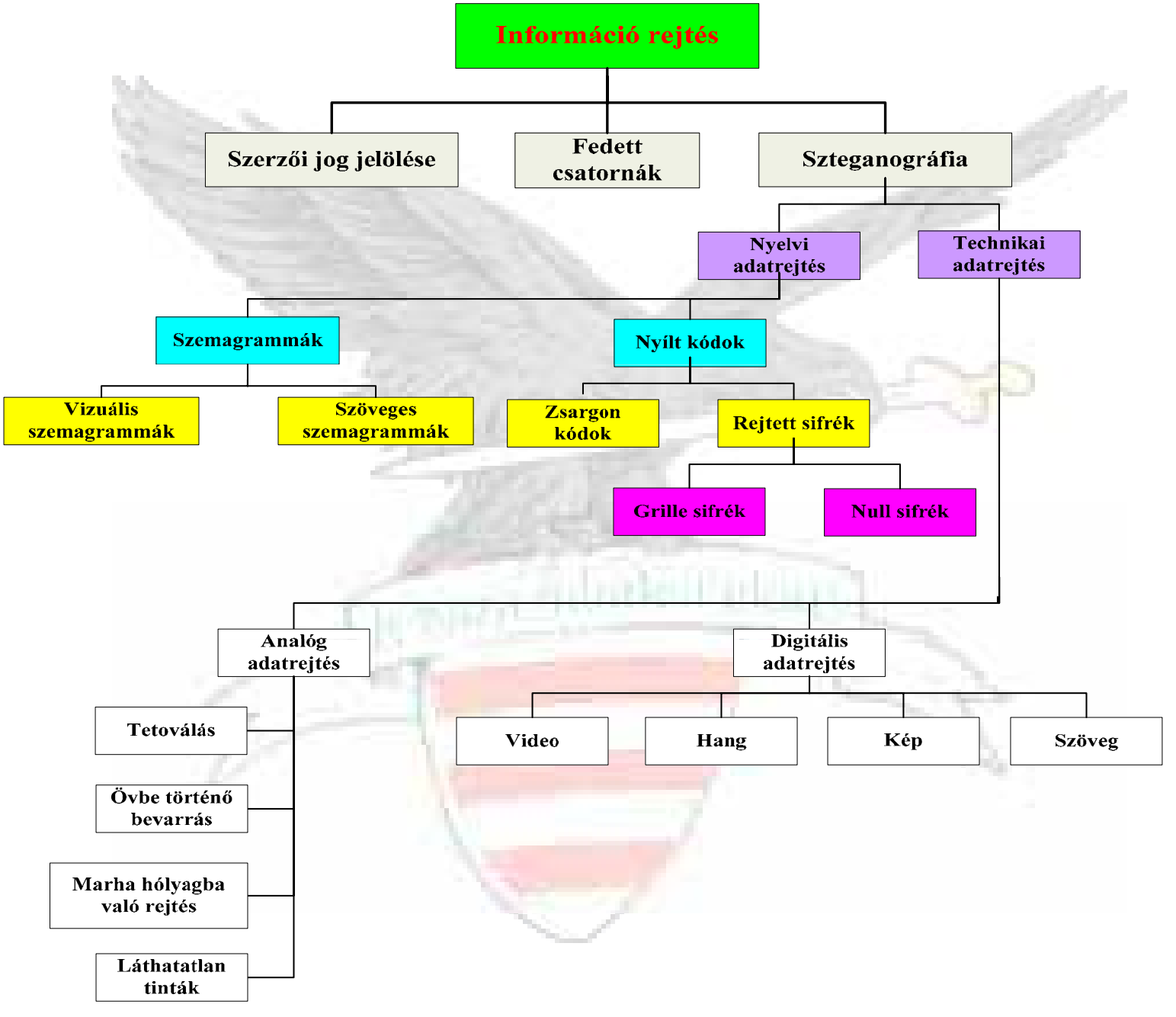
A technikai szteganográfia folyt.

Digitális adatrejtés mozgóképbe:

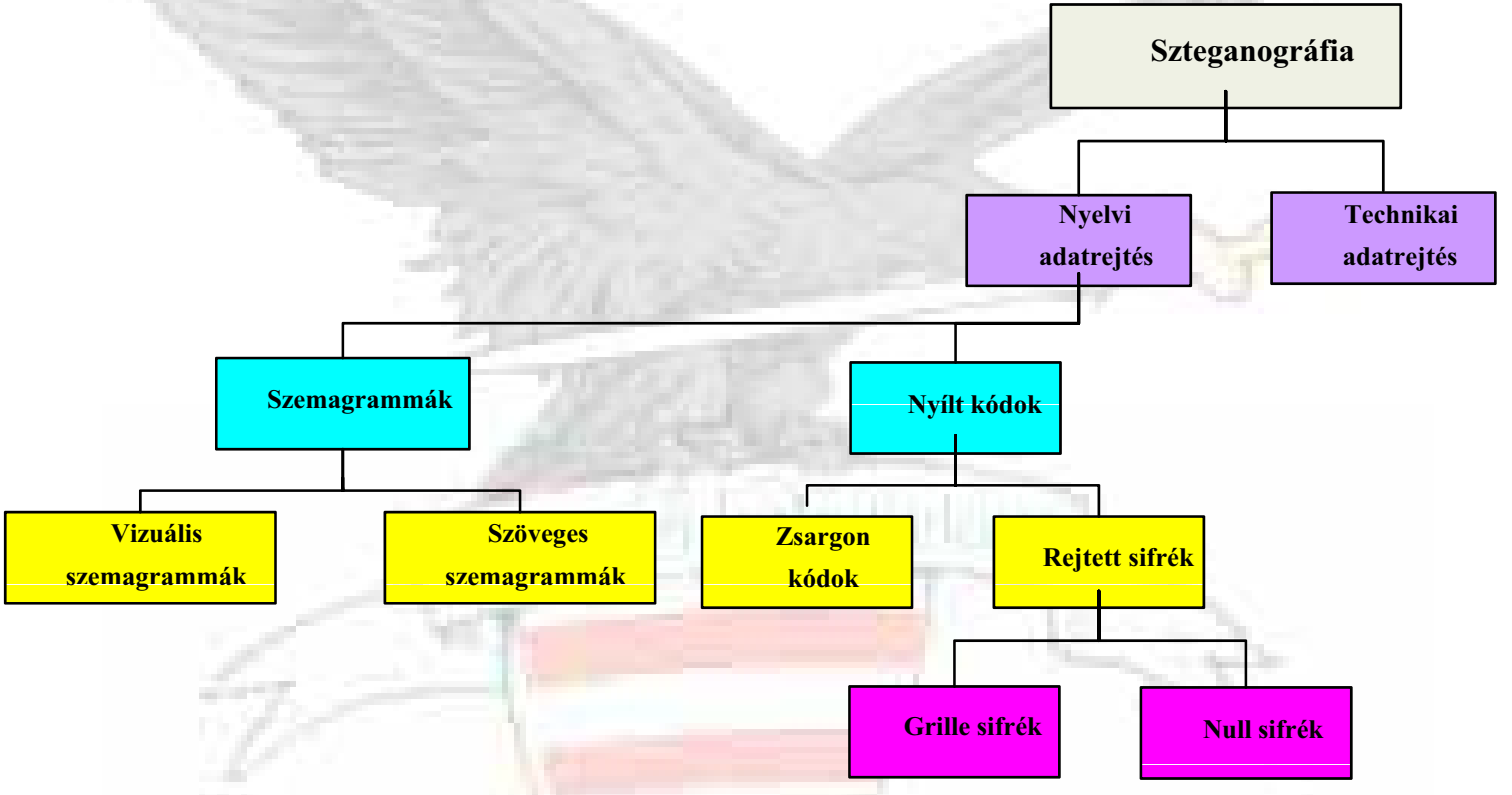
Adatrejtés tömörített videóba:

MPEG mint a leggyakoribb tömörítési eljárás




Információ rejtés
Szerzői jog jelölése
Fedett csatornák
Szteganográfia
Nyelvi adatrejtés
Technikai adatrejtés
Szemagrammák
Nyílt kódok
Vizuális szemagrammák
Szöveges szemagrammák
Zsargon kódok
Rejtett sifrék
Grille sifrék
Null sifrék
Analóg adatrejtés
Digitális adatrejtés
Tetoválás
Övbe történő bevarrás
Marha hólyagba való rejtés
Láthatatlan tinták
Video
Hang
Kép
Szöveg

A nyelvészeti szteganográfia



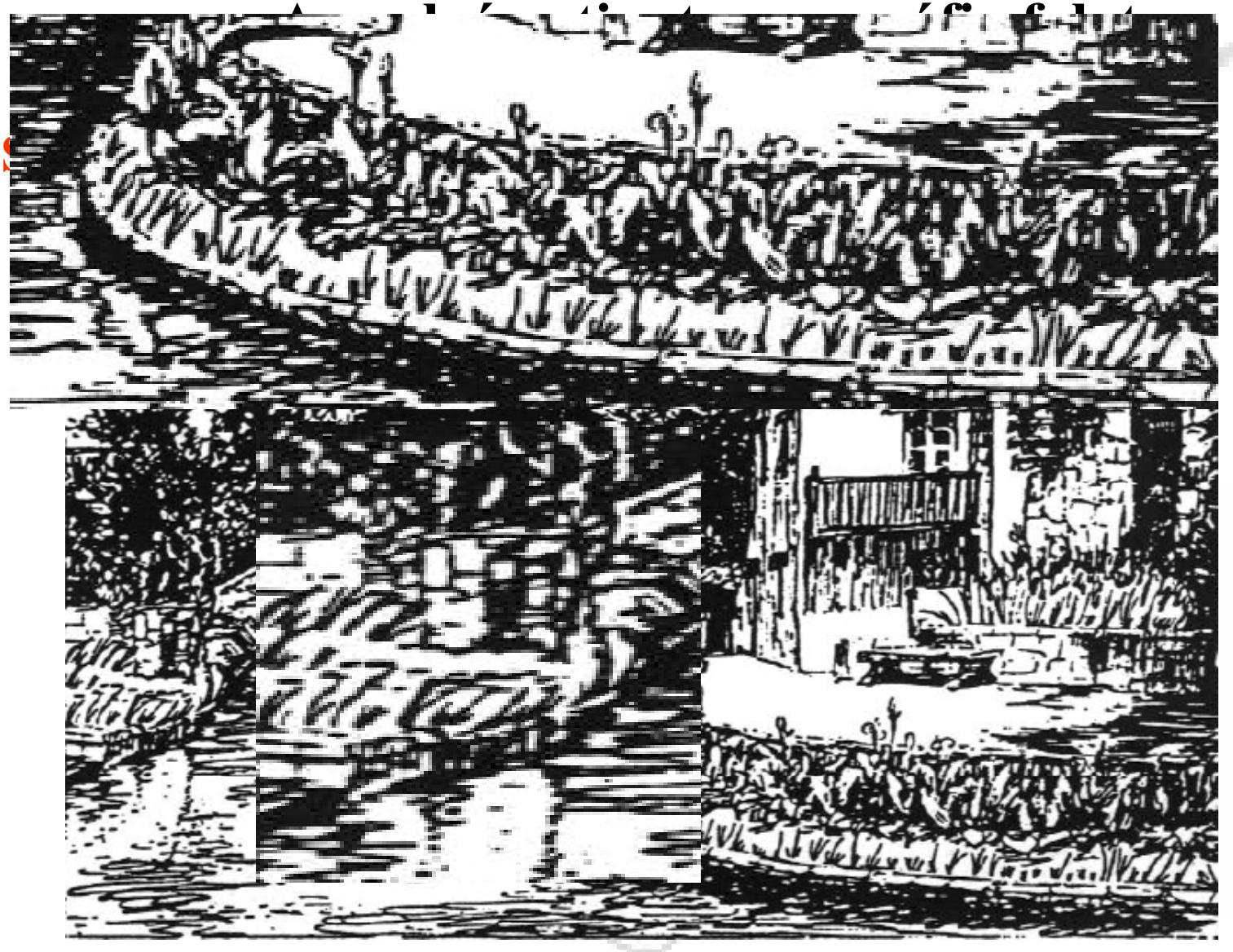
A nyelvészeti szteganográfia folyt.

Szemagrammák:

• Szimbólumok, jelek útján történő információ rejtés.

• A vizuális szemagramma nem más mint egy ártalmatlannak kinéző hordozó szimbólum, amely a mindennapi kommunikációban bármikor, bárhol előfordulhat.

• A szöveges szemagrammában a szövegnek, mint hordozónak a megjelenítését változtatjuk meg. Fontok átméretezése, különleges hatások alkalmazása, lendületes, eltérő vonások a levelekben mind gépi, mind kézírásban



A nyelvészeti szteganográfia folyt.

Nyílt kódok:

Ártalmatlannak kinéző szöveg, amely nyilvánvalóan nem kelti fel az avatatlan szemlélő gyanúját.

- **A hordozó szöveget szokás nyílt (overt) kommunikációnak nevezni;**
- **A beágyazott, rejtett információ rendszerint fedett (covert) kommunikáció.**
- **Zsargon kódok alatt nem mást értünk mint a napjainkban is használt és elterjedt szlenget, esetlegesen a szakmai zsargonként aposztrofált speciális kommunikációt.**

A nyelvészeti szteganográfia folyt.

Rejtett sifrék:

Ez a köznapi nyelvben nem mást jelent, mint a nyílt információ beágyazását egy fedő médiumba, oly módon, hogy annak megjelenítése csak azon személy részére lehetséges, akinek számára azt elrejtették.

- **Grille kód: sablon felhasználása olyan módon, hogy maga a sablon fedi el a hordozó médiumot és benne a rejtett információt. A sablon megnyitásakor, maga a beágyazott információ jelenik meg.**

A nyelvészeti szteganográfia folyt.

Rejtett sifrék:

Null kód: a nyílt szöveg, amely ártalmatlannak néz ki, valamely előre jól definiált szabályok szerinti értelmezés szerint teljesen más jelentéssel bír:

- Minden szó első és harmadik brűjének összeolvasása adja az értelmes szöveget;

- Csak minden negyedik szó értelmezendő.

„News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Newt is upset because he thinks he is President

Szteganográfia avagy Rejtjelzés

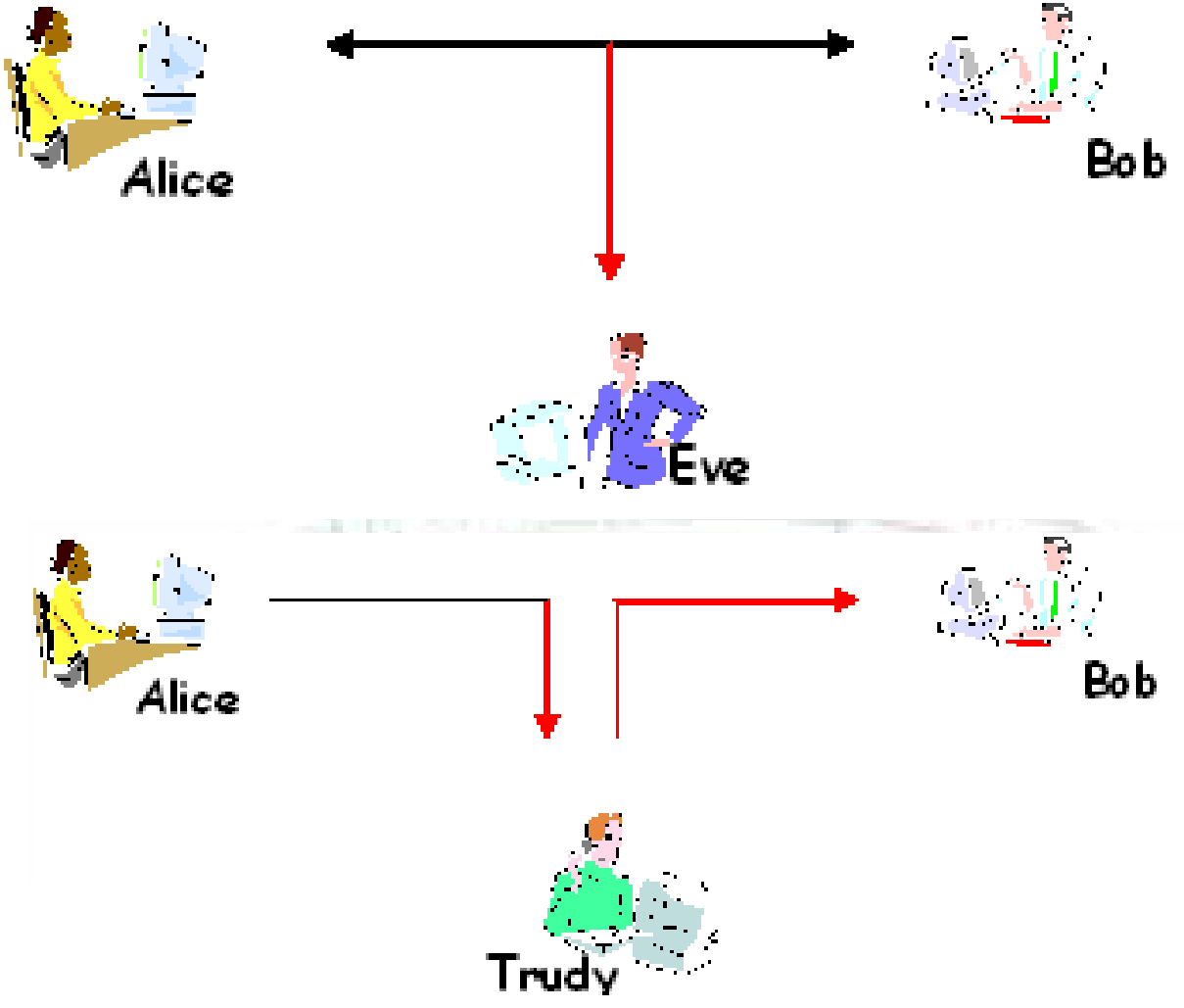
- **A titkosírással kódolt üzenetről akárki, azonnal láthatja, hogy a számára rejtett üzenetről van szó;**
- **Lehet, sőt valószínű, hogy megfejteni nem tudja, de a küldő mindenképpen gyanússá válik;**
- **Az üzenetrejtés és a rejtjelzés két különböző dolog, de együtt hatékonyabban alkalmazhatók;**
- **Az üzenet „rejtése” valami mást jelent mint a titkosítás és/vagy rejtjelzés.**

Szteganográfia avagy Rejtjelzés folyt.

- **A titkosírás is hozzáférhetetlenné teszi az üzenet tartalmát a beavatatlan számára, de.....;**
- **„rejtés alatt ma valami mást értünk;**
- **A szteganográfia nem váltja ki, nem is válthatja ki a rejtjelzést;**
- **Szteganográfia = rejtett írás;**
- **Rejtjelzés = a kriptográfia tárgykörébe tartozó tudomány;**
- **A rejtjelzés önmagában nem védelem.**

Szteganográfia Detektálhatósága

- **Börtönőrök problémája.....;**



Szteganográfia Detektálhatósága folyt.

- **Egyszerű szteganográfiai modell esetén a harmadik fél semmit nem tud az alkalmazott módszerről;**
- **Rejtjelzéssel kombinált szteganográfia esetén, a börtönőr ismeri a sztego algoritmust, azonban nem ismeri a titkos kulcsot, amelyet a kommunikáló felek használnak;**
- **Napjaink sztegoanalízise még erős fejlődésben van, az első cikkek ez irányban a késői ’90-es években láttak napvilágot;**
- **Uniformizálás szükségessége.**

Szteganográfia Detektálhatósága folyt.

- **Egyszerű szteganográfiai támadás;**
- **Ismert hordozójú támadás;**
- **Ismert információjú támadás;**
- **Választott szteganográfiai támadás;**
- **Választott információjú támadás;**
- **Ismert szteganográfiai támadás.**

Szteganográfia Detektálhatósága folyt.

Szteganalízis formái:

1. **Nagyban függenek a szteganográfiai eljárástól;**
2. **Hordozó és a sztego médium vizuális detektálása;**

   - **Egyszerű, de csak abban az esetben vezet eredményre ha alapos gyanú áll fenn.**

3. **Struktúra vizsgálat;**

   - **Statisztikai analízis, sokkal bonyolultabb, de hatásosabb, főleg az un. blind analízis esetén használatos.**

Szteganográfia Detektálhatósága folyt.

483 x 315 24 bit color Windows Bitmap

A kép mindhárom szín 1 - 1 bitjének manipulálása

A kép mindhárom szín 2 - 2 bitjének manipulálása

A kép mindhárom szín 4 - 4 bitjének manipulálása

Szteganográfiai alkalmazások

S-Tools

- GIF, BMP, WAV

JP Hide&seek

- JPEG

MP3Stego

- MP3

Steghide

- BMP, JPEG, WAV, AU

Összegezve

- **A szteganográfia nem más mint az információ elrejtésének módja egy kiválasztott hordozóba.**
- **Az interneten szabadon elérthető programok garmadája.**
- **Az adatrejtés detektálása meglehetősen bonyolult, de nem lehetetlen feladat.**
- **Sok anekdóta kering a szteganográfia különösen terroristák általi használatáról.**
- **Eddig senki nem talált erre nézve perdöntő bizonyítékot.**

Ajánlott irodalom:

Disappearing Cryptography **by Peter Wayner**
2nd edition, 2002

The Code Book **by Simon Singh, 1999**

Techniques and Applications of Digital Watermarking and Content Protection, by **Michael Arnold, Martin Schmucker, Stephen D. Wolthusen**

Information Hiding Techniques for Steganography and Digital Watermarking, by Fabien A. P. Petitcolas, Stefan Katzenbeisser

Hasznos linkek:

- http://www.stegoarchive.com/
- http://www.crazyboy.com/
- http://www.spammimic.com/
- http://www.wetstonetech.com/
- http://www.outguess.org/
- http://www.spie.org
- http://steganography.tripod.com/stego/software.html
- http://rr.sans.org/covertchannels/steganography3.php
- http://rr.sans.org/covertchannels/steganography3.php
- http://www.wired.com/news/politics/0,1283,41658,00.html
- http://www.darkside.com.au/snow
- http://www.heise.de/tp/english/inhalt/te/9751/1.html

Köszönöm, hogy meghallgattak!