A Szteganográfia elemeinek bemutatása

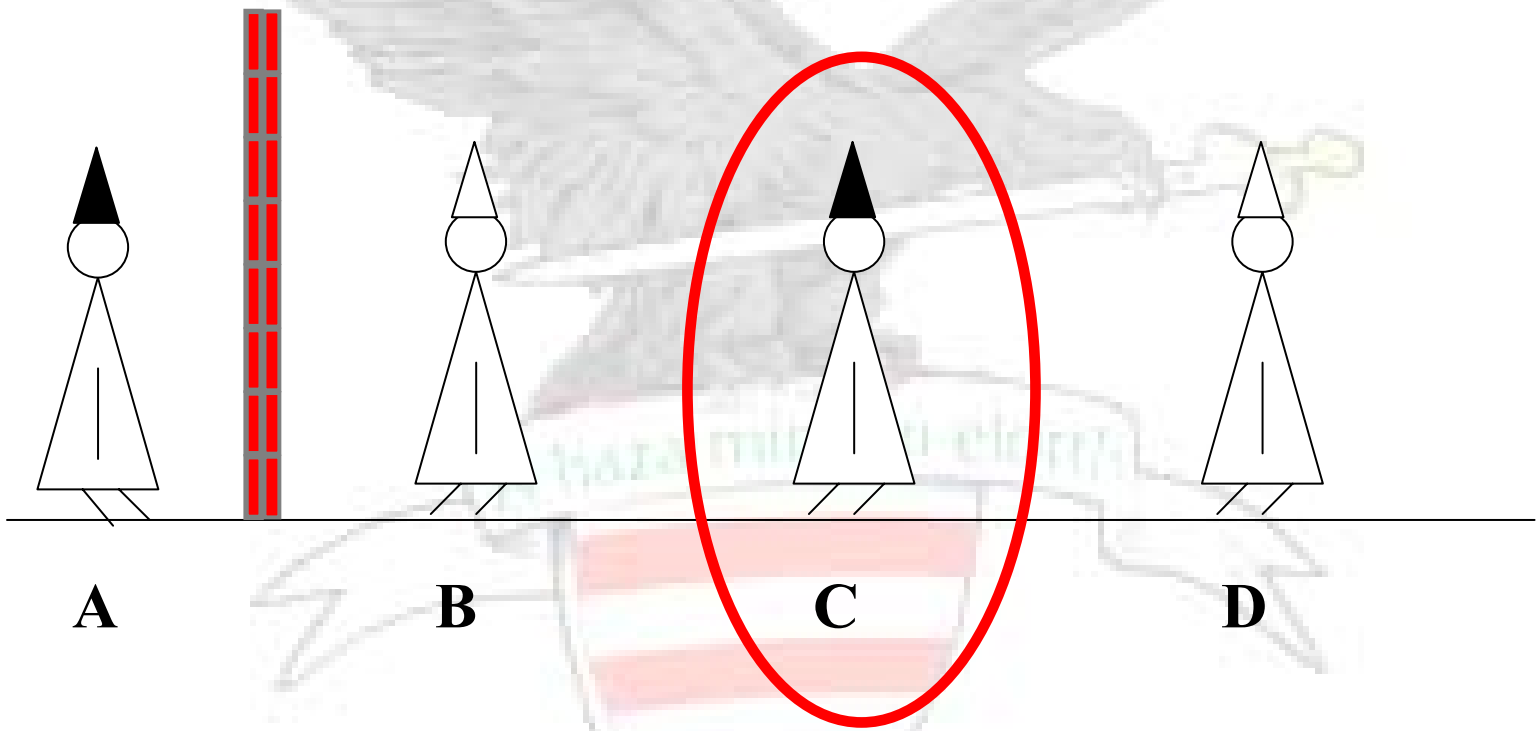
Unicsovics György

e-mail: gy.unicsovics@nbh.hu

Hétpecsét előadás, Budapest **2007. november 21.**

Ki vagyok én?

- **Unicsovics György, a Nemzetbiztonsági Hivatal vezető tanácsadója;**
- **Híradástechnikai mérnök;**
- **Műszaki informatikai szakmérnök;**
- **ZMNE doktoranduszi tanulmányaimat befejeztem;**
- **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

USA TODAY SPECIAL SECTION: 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

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.

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie 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.

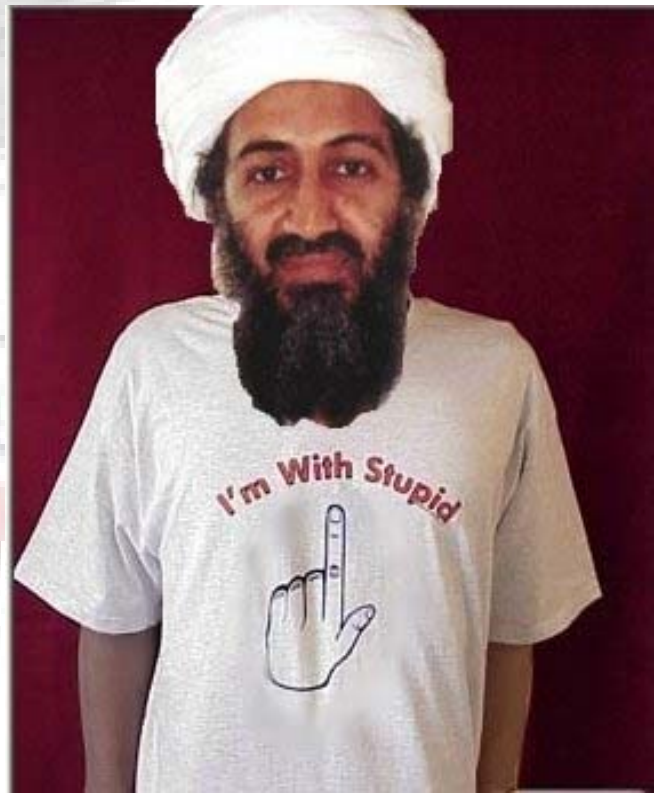
Read more

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."

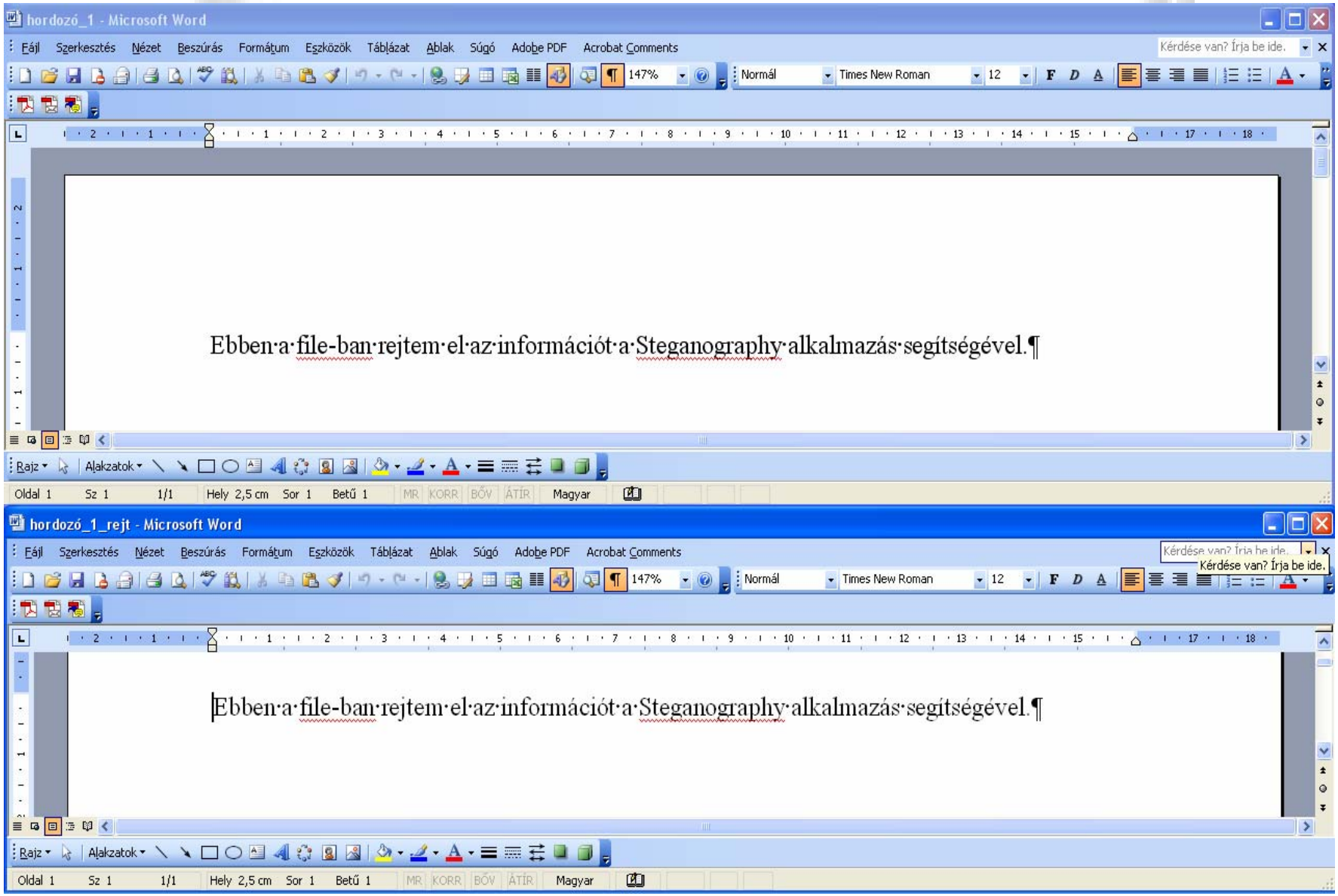
Internet



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

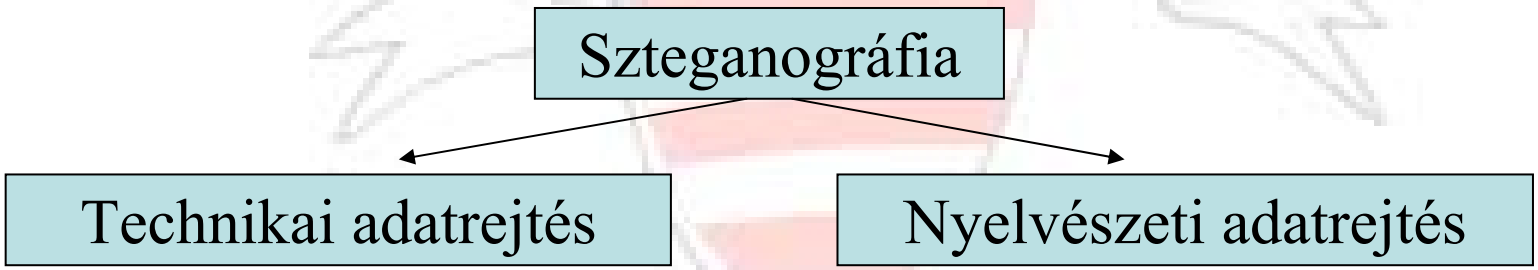
Steganography ≠ Stenography

Már az ókoriak is.....

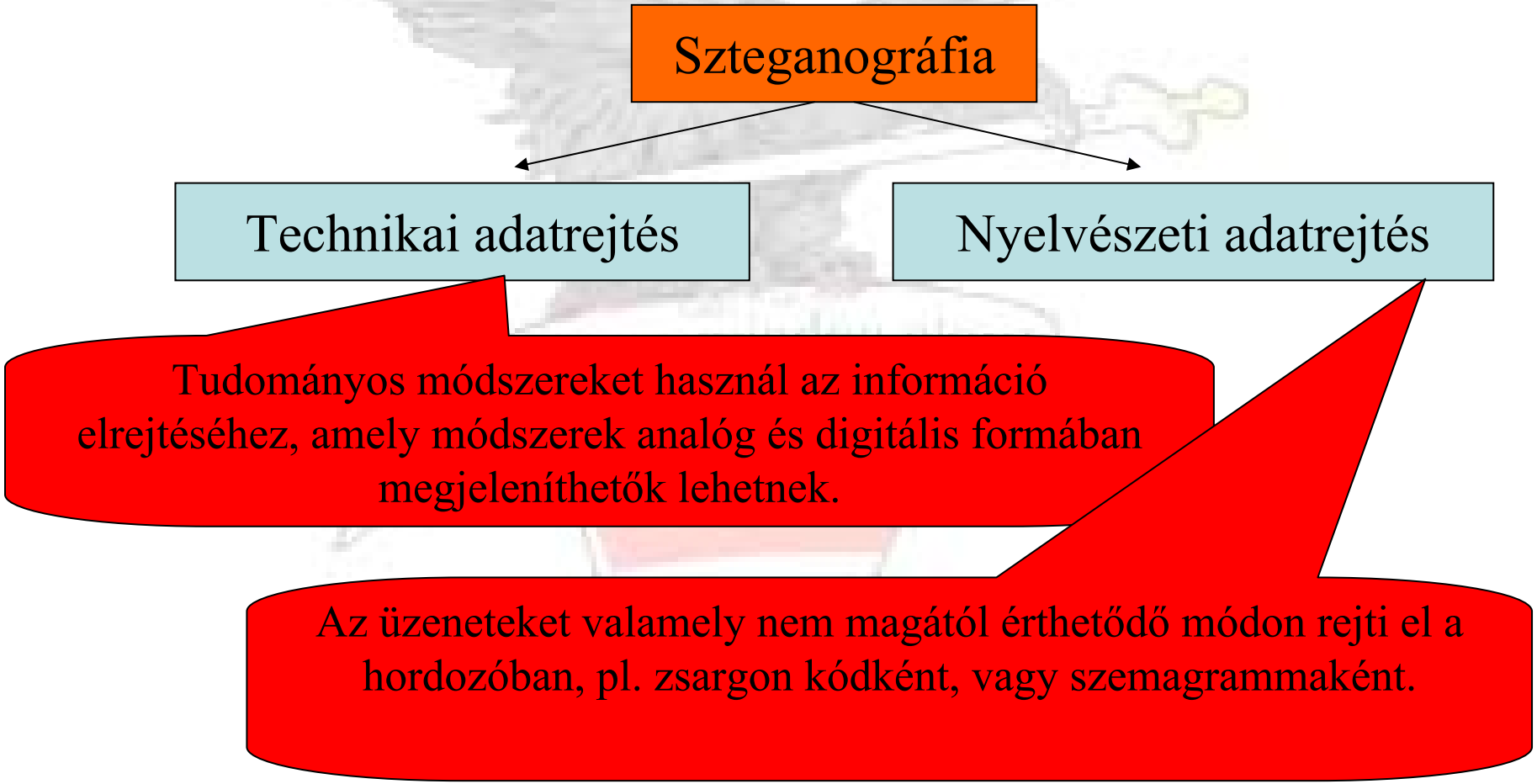
Szteganográfia jelentése és célja:

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

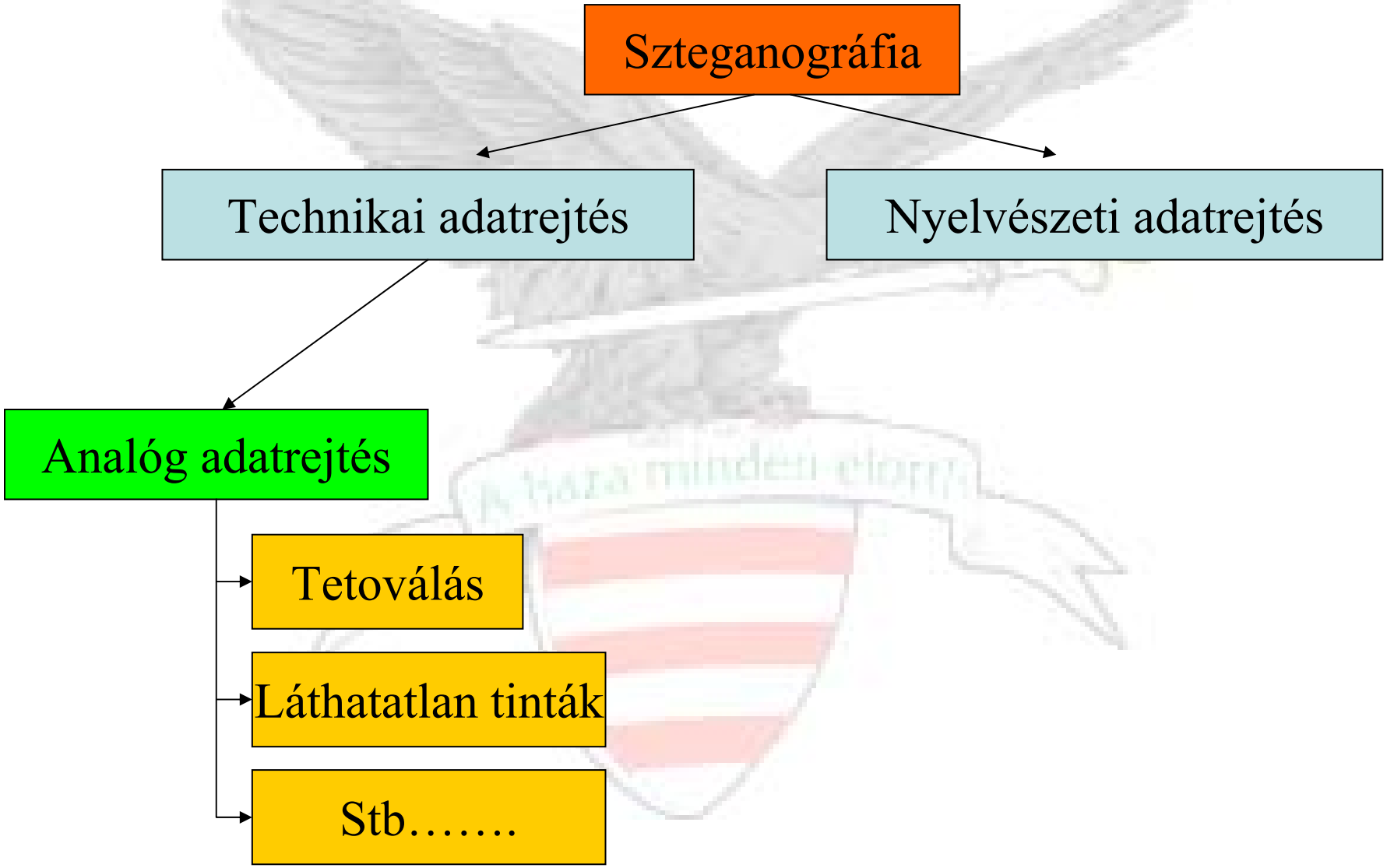
Szteganográfia fő csoportjai:



Szteganográfia felosztása



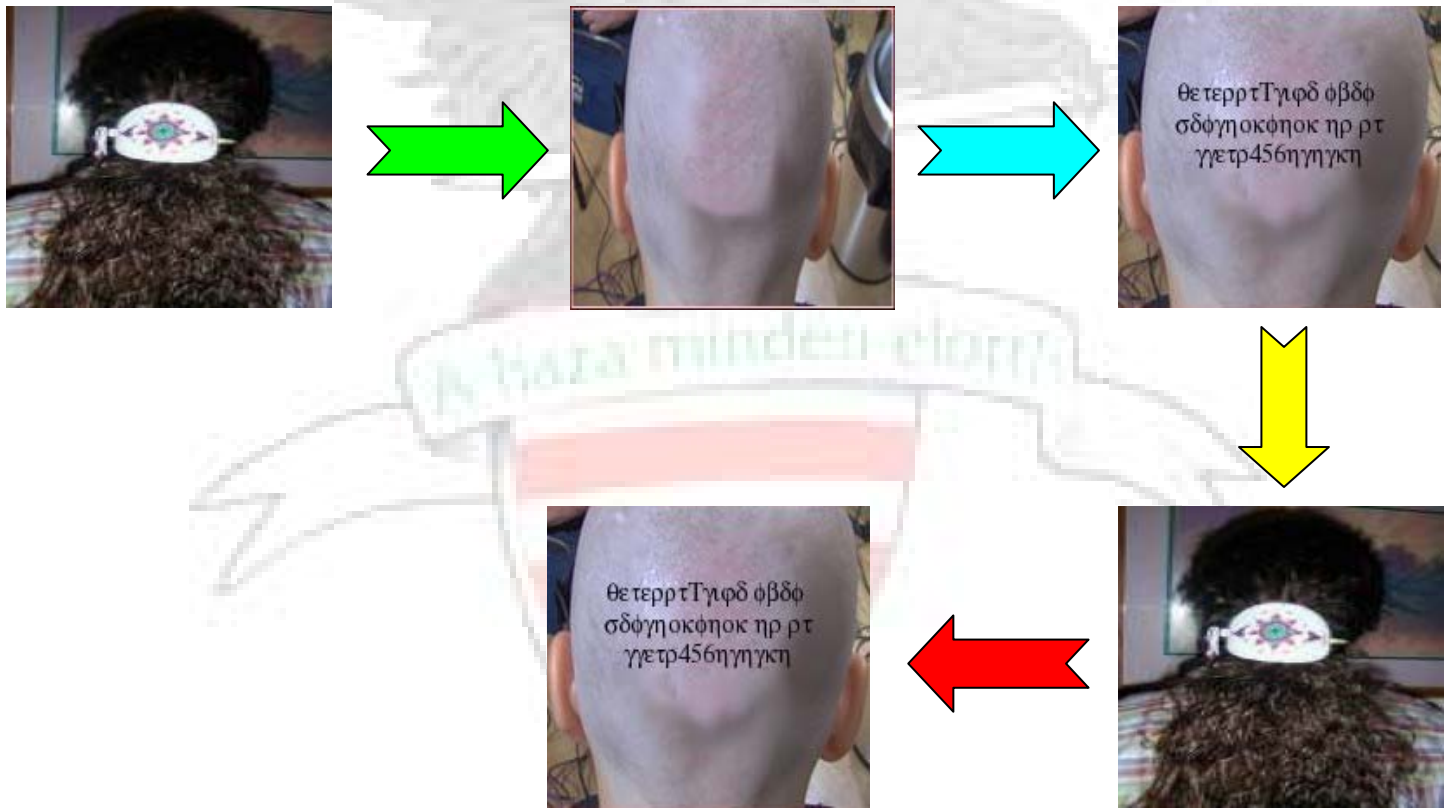
Szteganográfia felosztása folyt.



A technikai szteganográfia

Analóg adatrejtés:

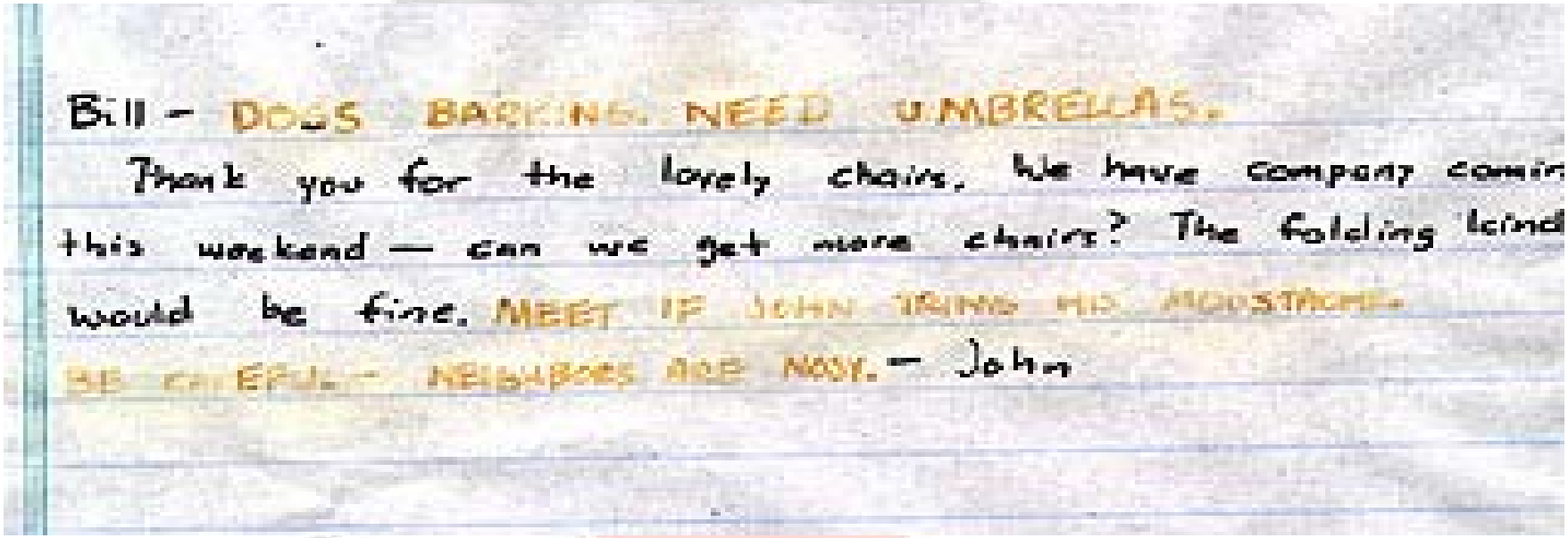
- Tetoválás:



A technikai szteganográfia folyt.

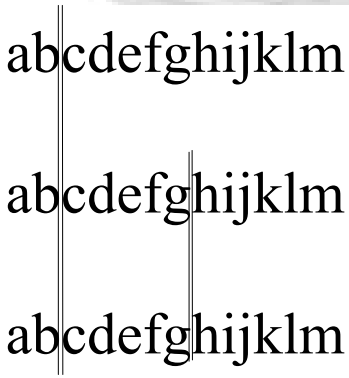
Analóg adatrejtés:

- 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.**

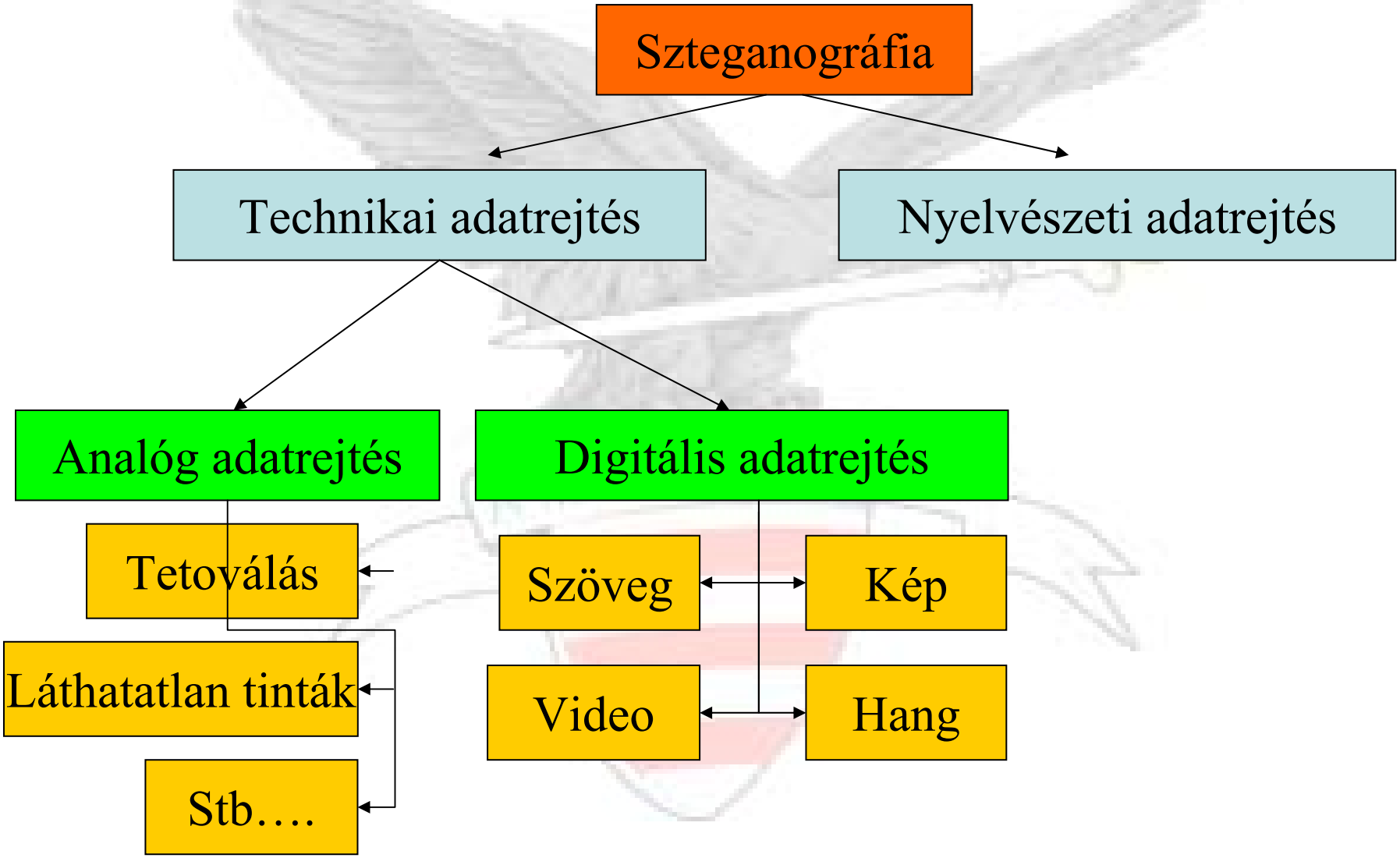
Betűfont helyének függőleges megváltoztatása

- 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.**

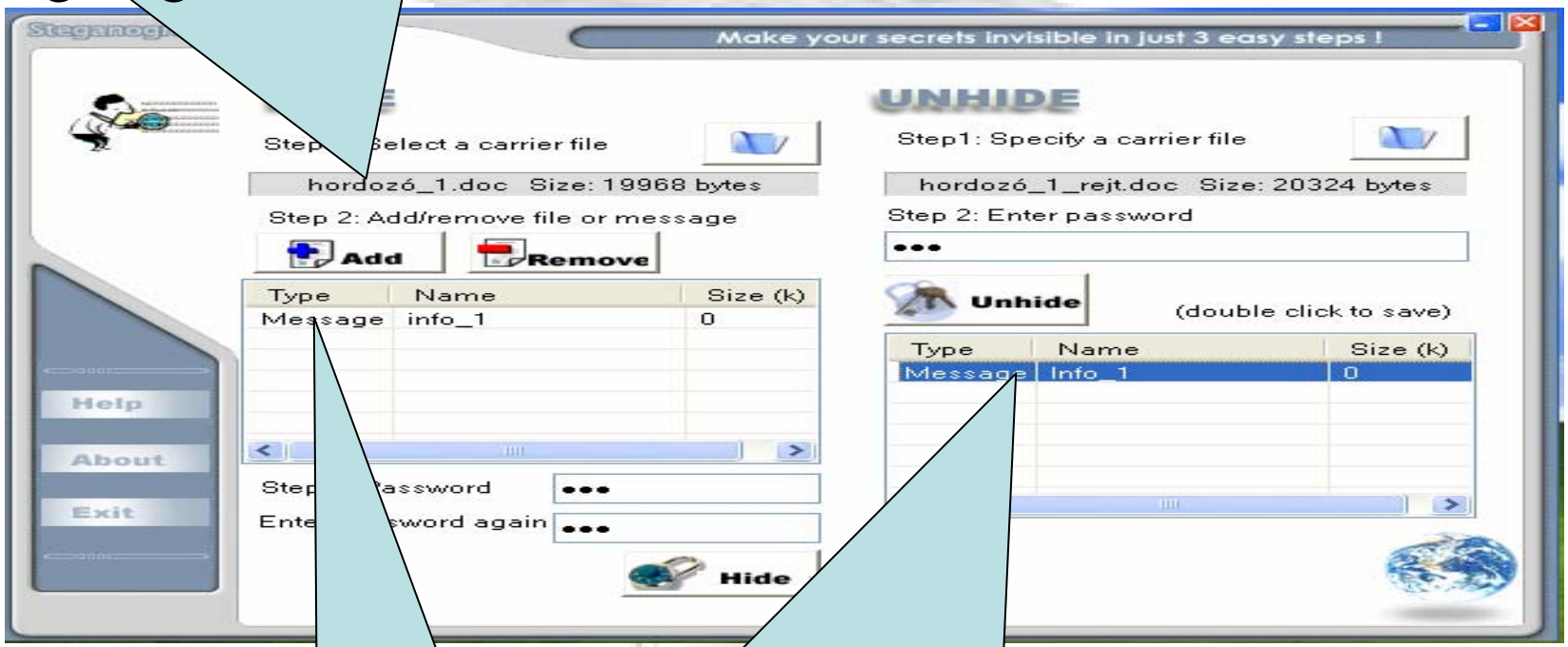
Szteganográfia felosztása folyt.



A technikai szteganográfia

Digitális adatrejtés szövegbe:

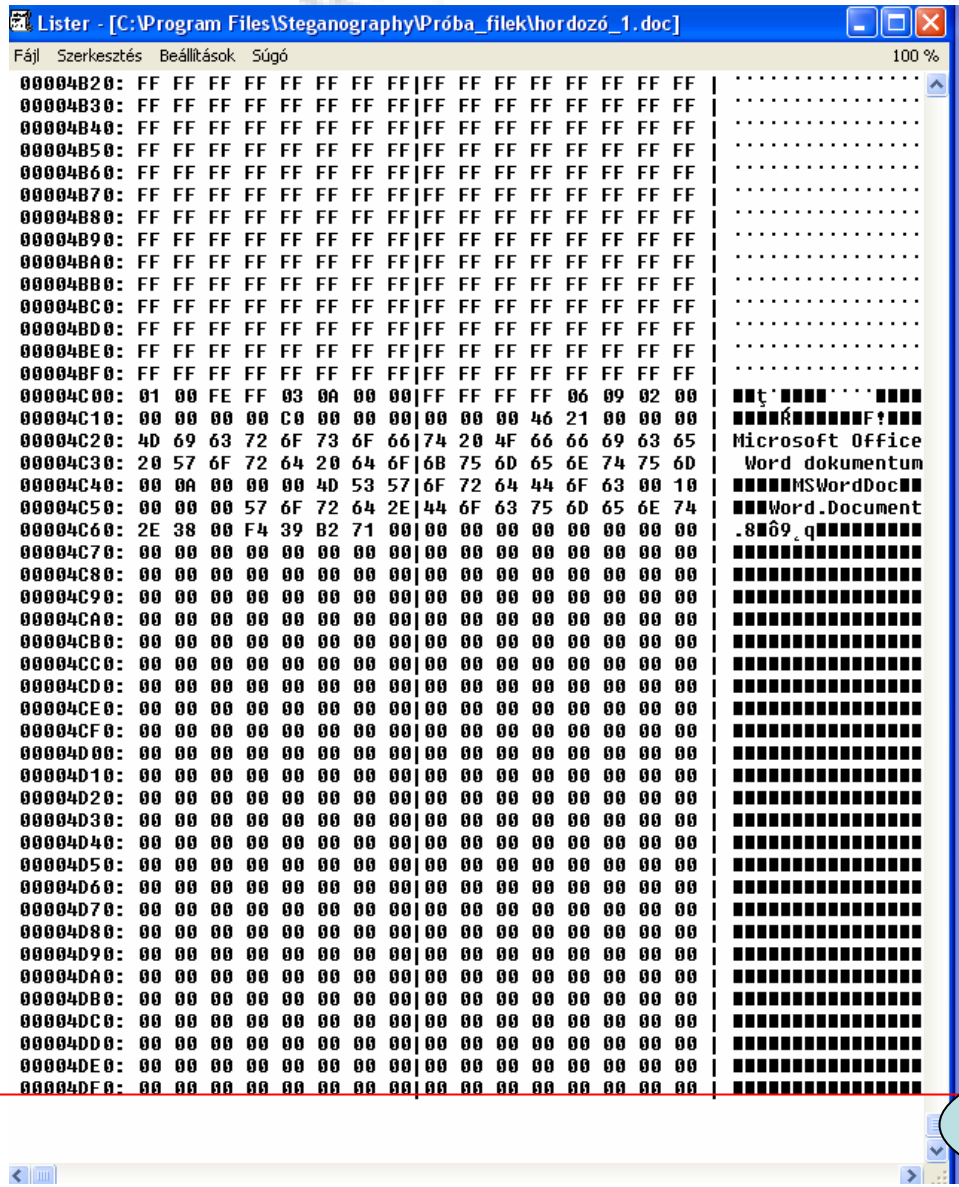
Ebben a file-ban rejtem el az információt a Steganography alkalmazás segítségével.

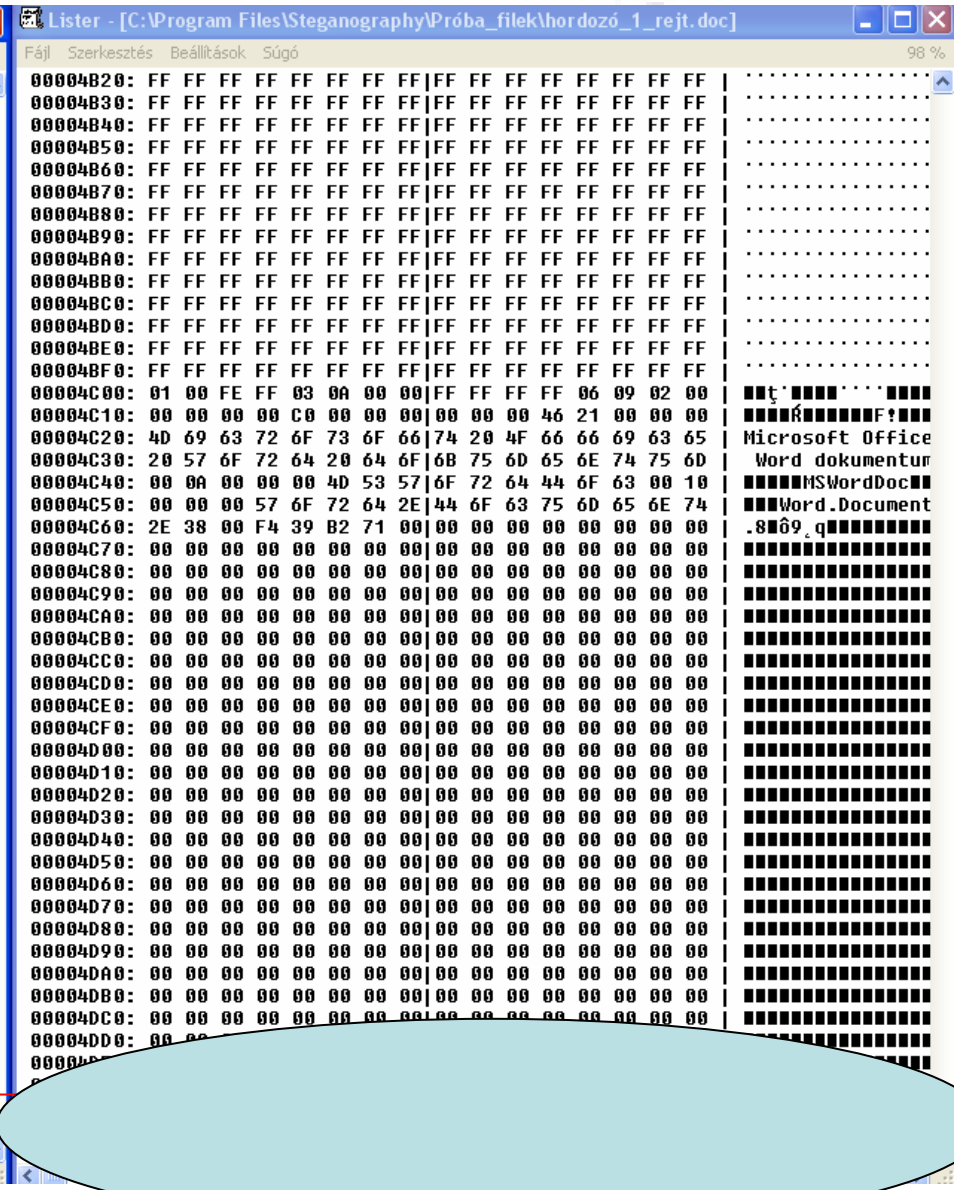


Direkt szövegbevitelt alkalmaztam

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

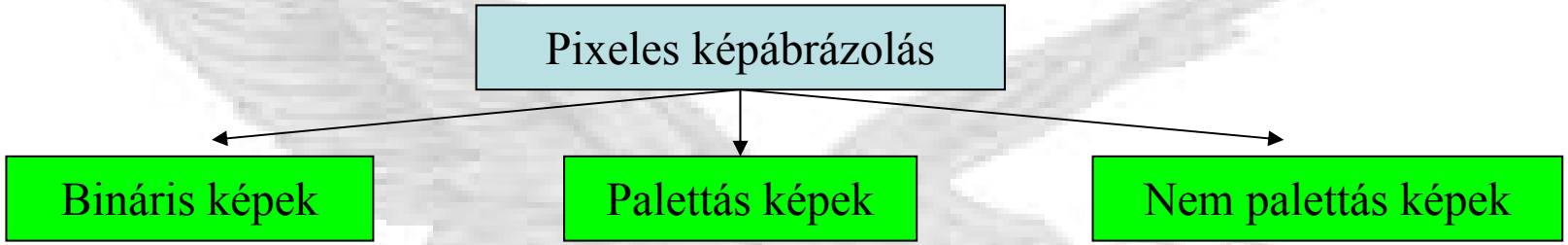
Digitális rejtés szövegbe folyt.



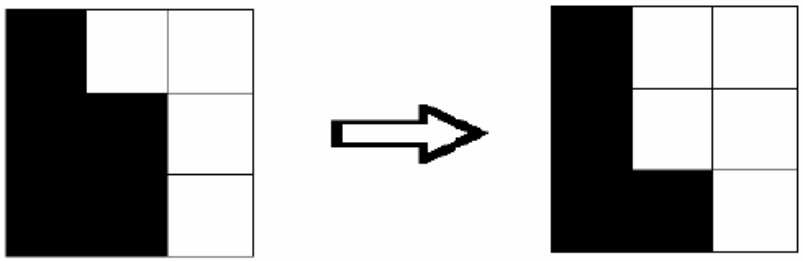


A technikai szteganográfia folyt.

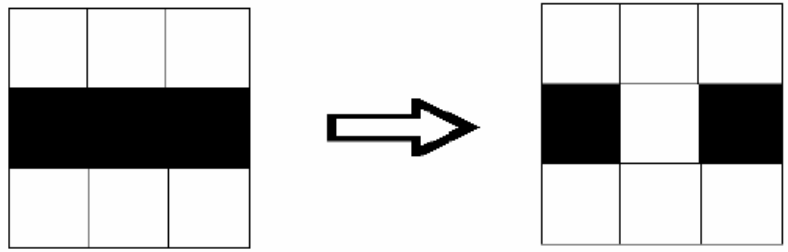
Digitális adatrejtés képekbe (elméleti háttér):



Adatrejtés bináris képekbe



Bináris kép pixelcseréje, ami alig észrevehető

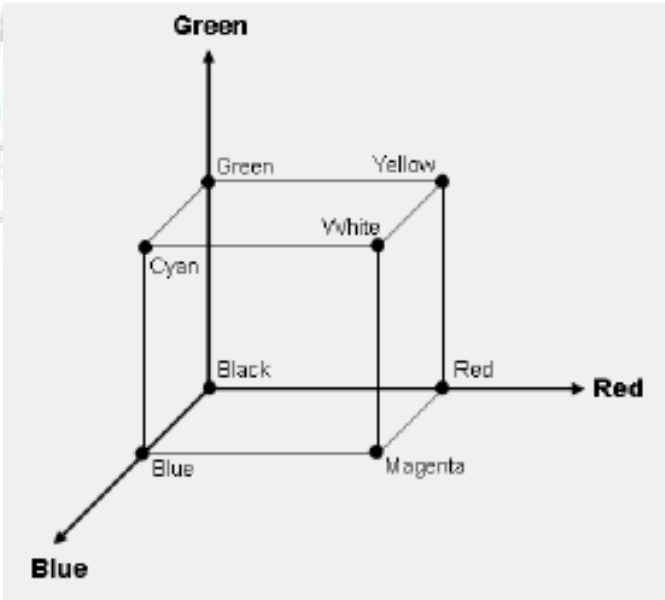


Bináris kép pixelcseréje, ami már szembetűnő

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,**

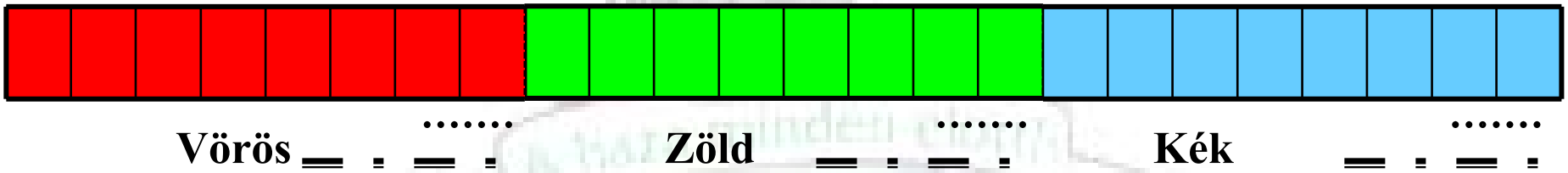


A technikai szteganográfia folyt.

Digitális adatrejtés képekbe:

- **Az adatrejtés BMP képekbe:**

- LSB rejtés fedőképekben.



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:

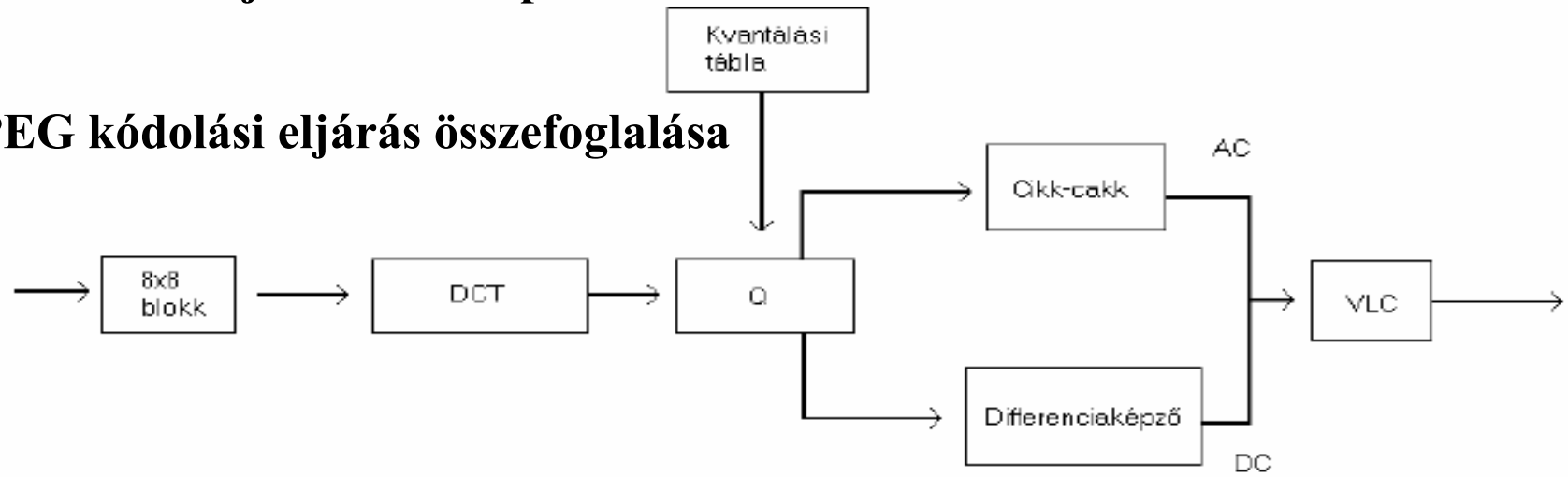
- JPEG = Joint Photographic Expert Group;
- Folytonos színtónusú állóképek digitális kódolása;
- Előnye a 65535x65535 képméret;
- Kódoló és dekódoló szimmetrikus felépítésű
- Tömörítés aránya szabadon paraméterezhető;
- Tömörítés hatásfoka és a képminőség fordított arányban áll egymással;
- Alapvetően 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.

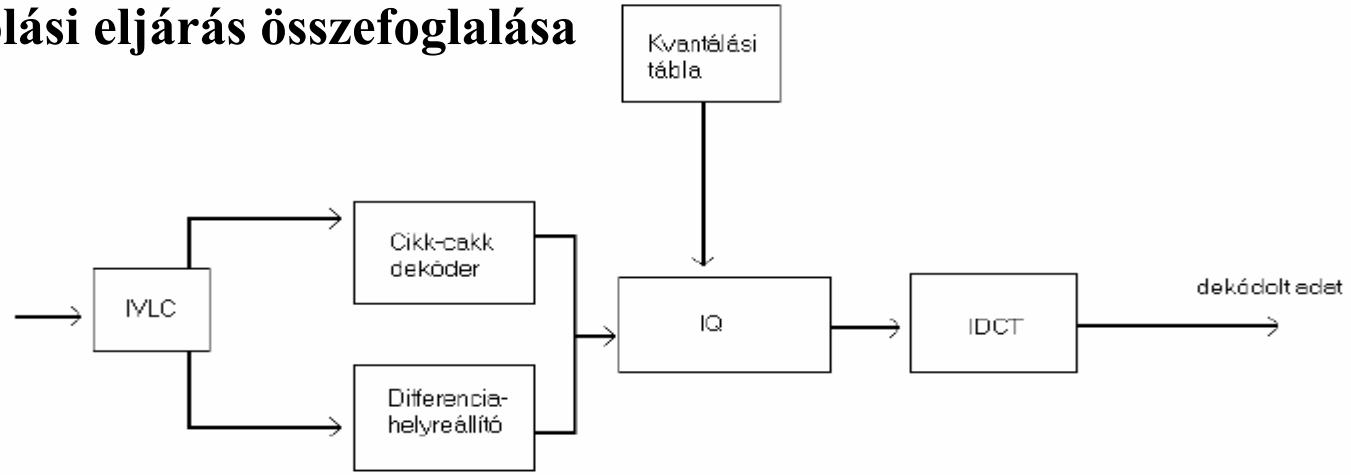
Digitális adatrejtés képekbe:

Az adatrejtés JPEG képekbe:

A JPEG kódolási eljárás összefoglalása



A JPEG dekódolási eljárás összefoglalása



A technikai szteganográfia folyt.

Digitális adatrejtés hanganyagba:

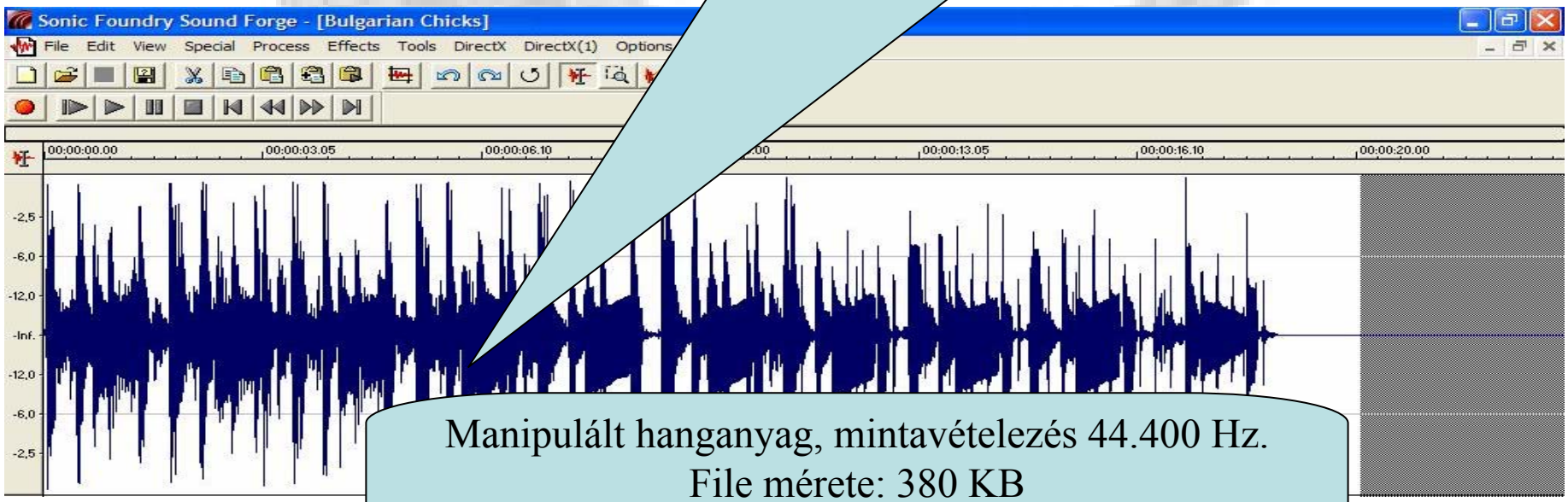
- **Ember számára hallhatatlan a változás az eredeti és a sztegomédia között;**
- **A sztegomédia statisztikai és tömörítési karakterisztikája közötti különbség minimális;**
- **Általános eljárásokat túl kell élnie (például tömörítés, kismértékű zajosítás, szűrés);**
- **A hanganyagban található a beágyazott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

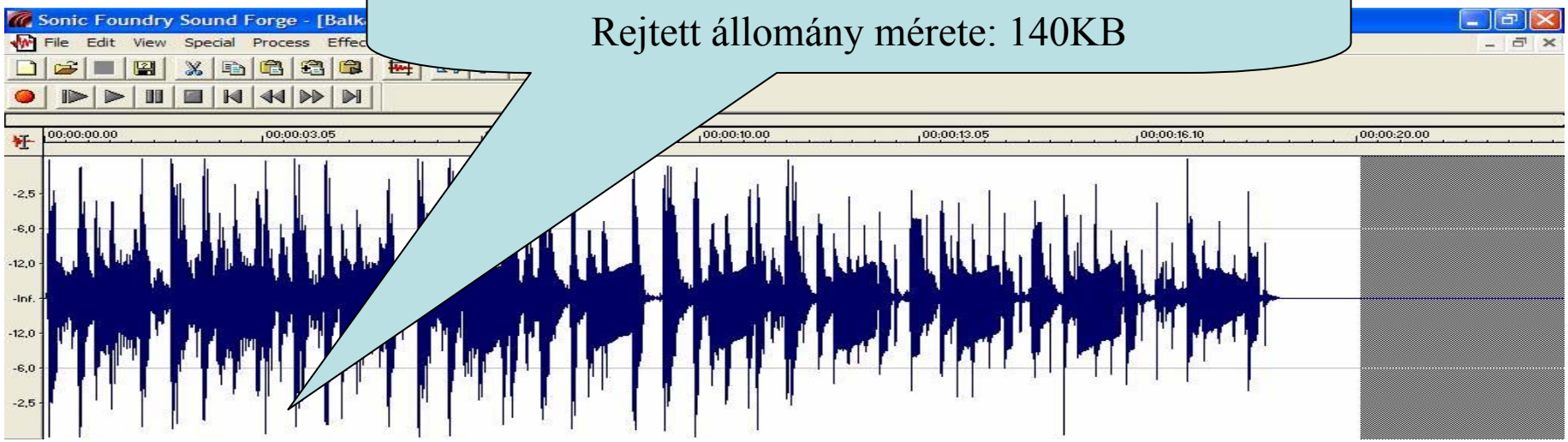
A technikai szteganográfia folyt.

Digitális adatrejtés har

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

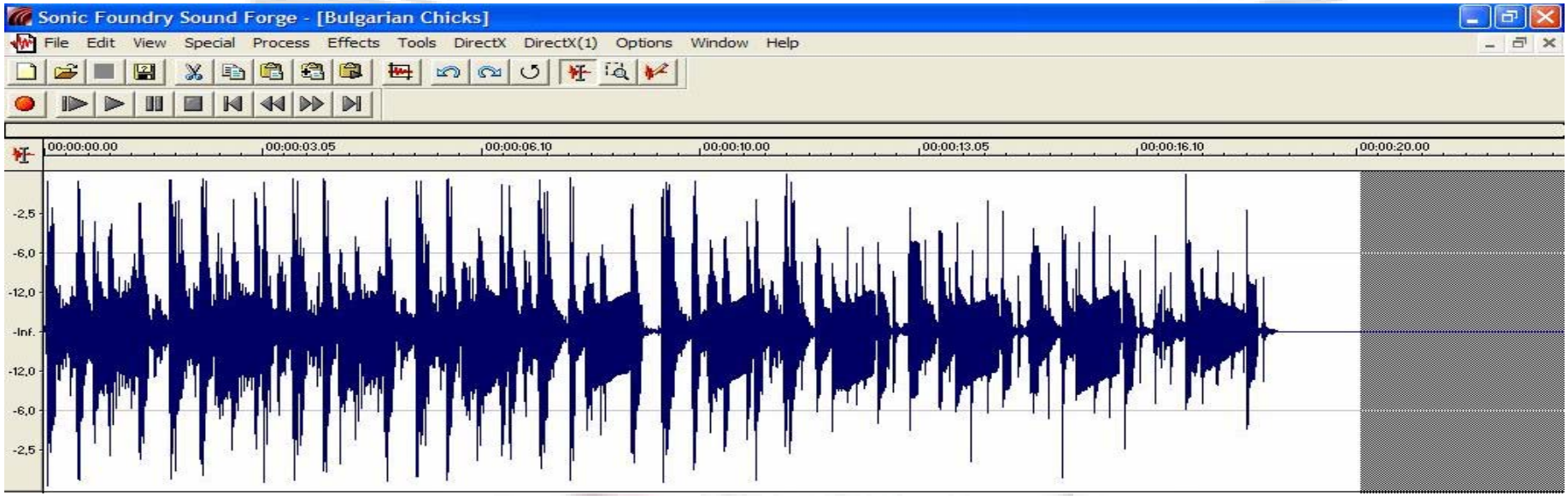


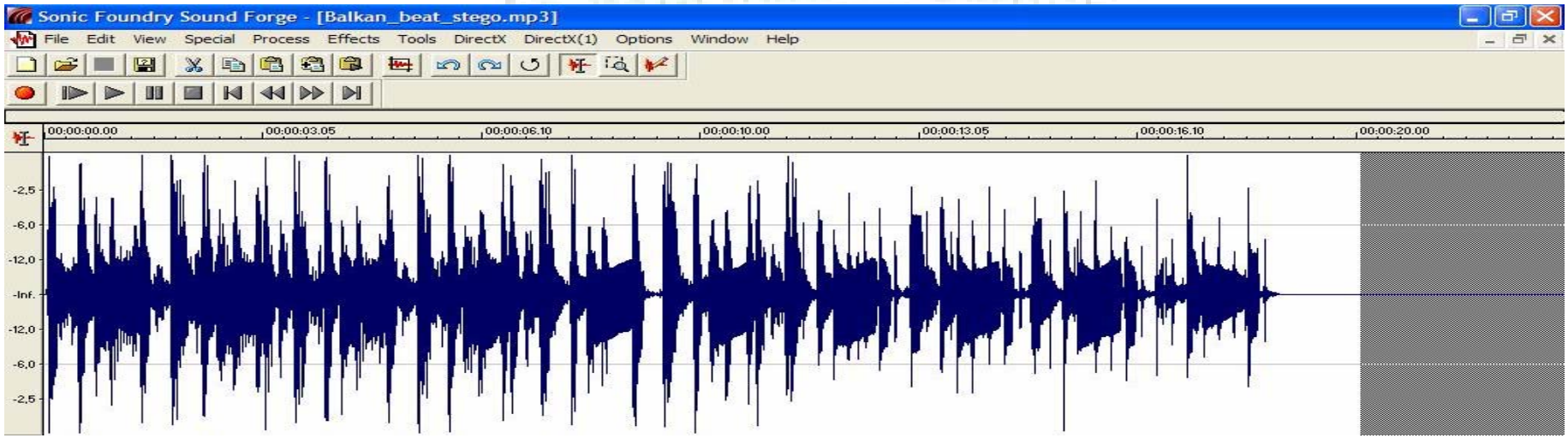
Manipulált hanganyag, mintavételezés 44.400 Hz.
File mérete: 380 KB
Rejtett állomány mérete: 140KB



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:

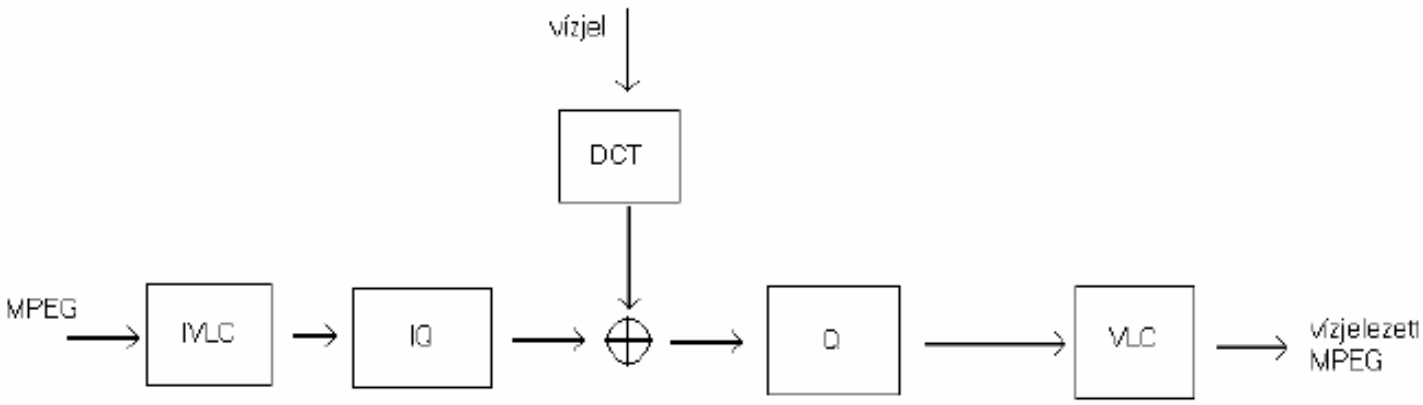
- **Szórt spektrumú vízjel;**
- **Nyilvános lulcsú vízjelzés.**

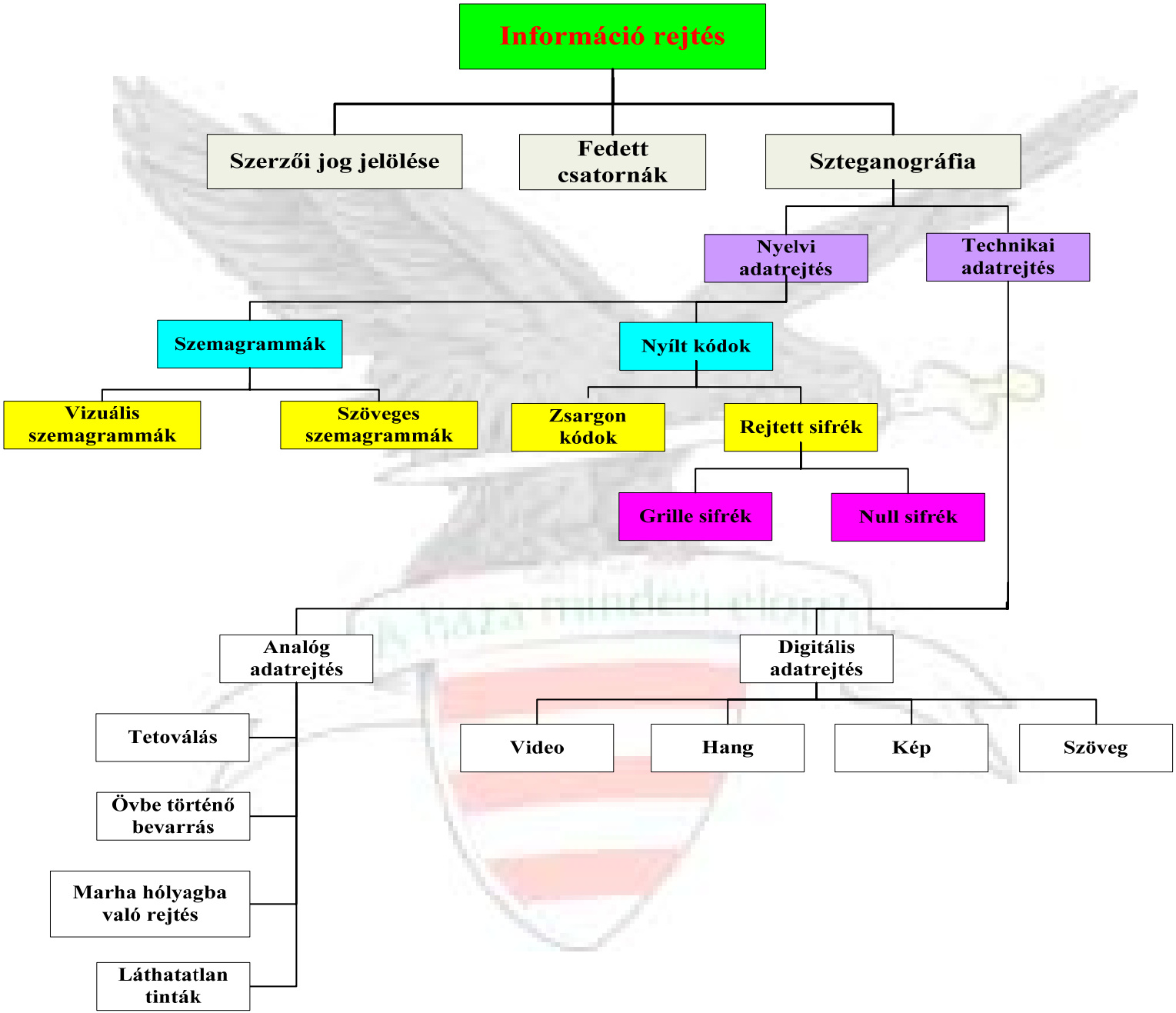
A technikai szteganográfia folyt.

Digitális adatrejtés mozgóképbe:

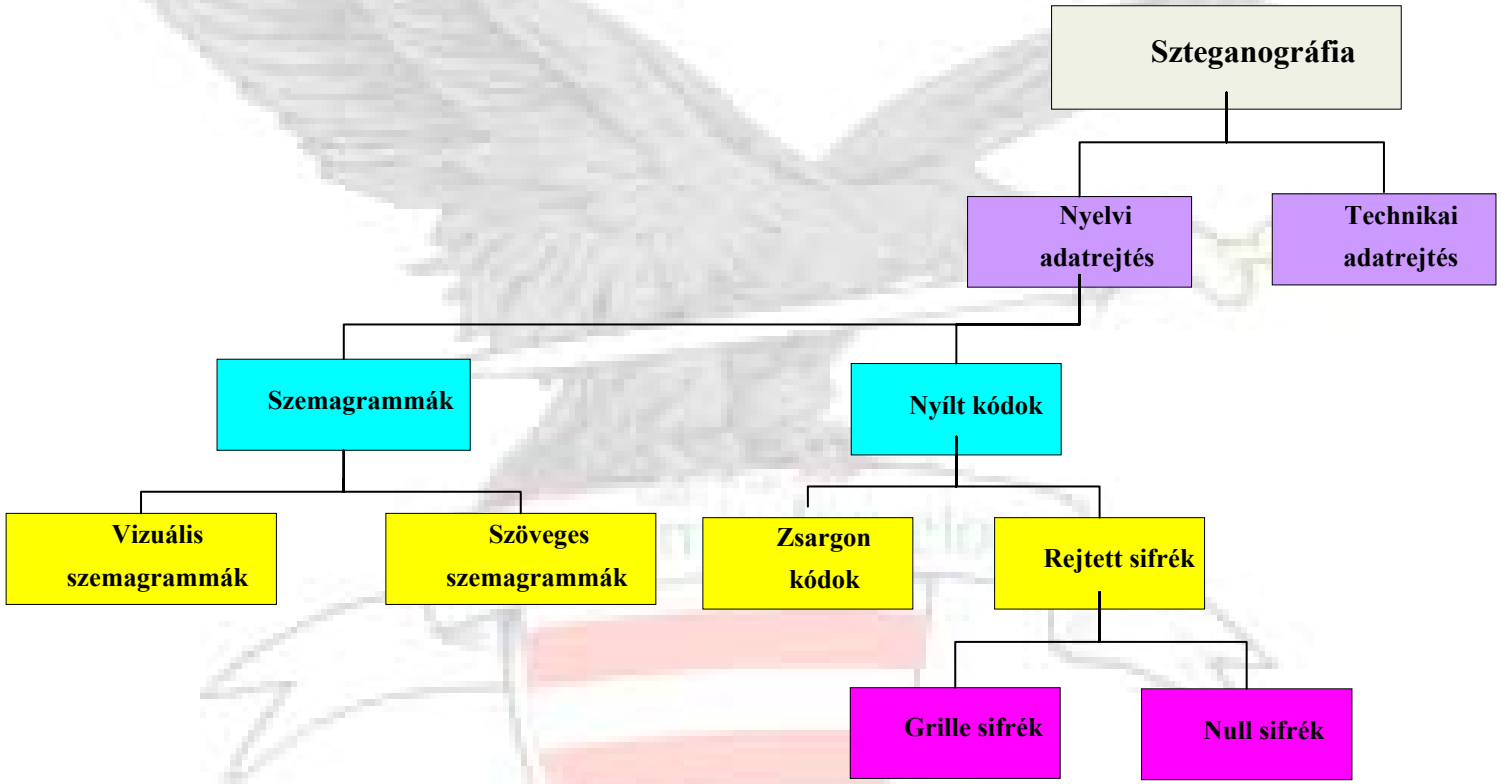
Adatrejtés tömörített videóba:

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



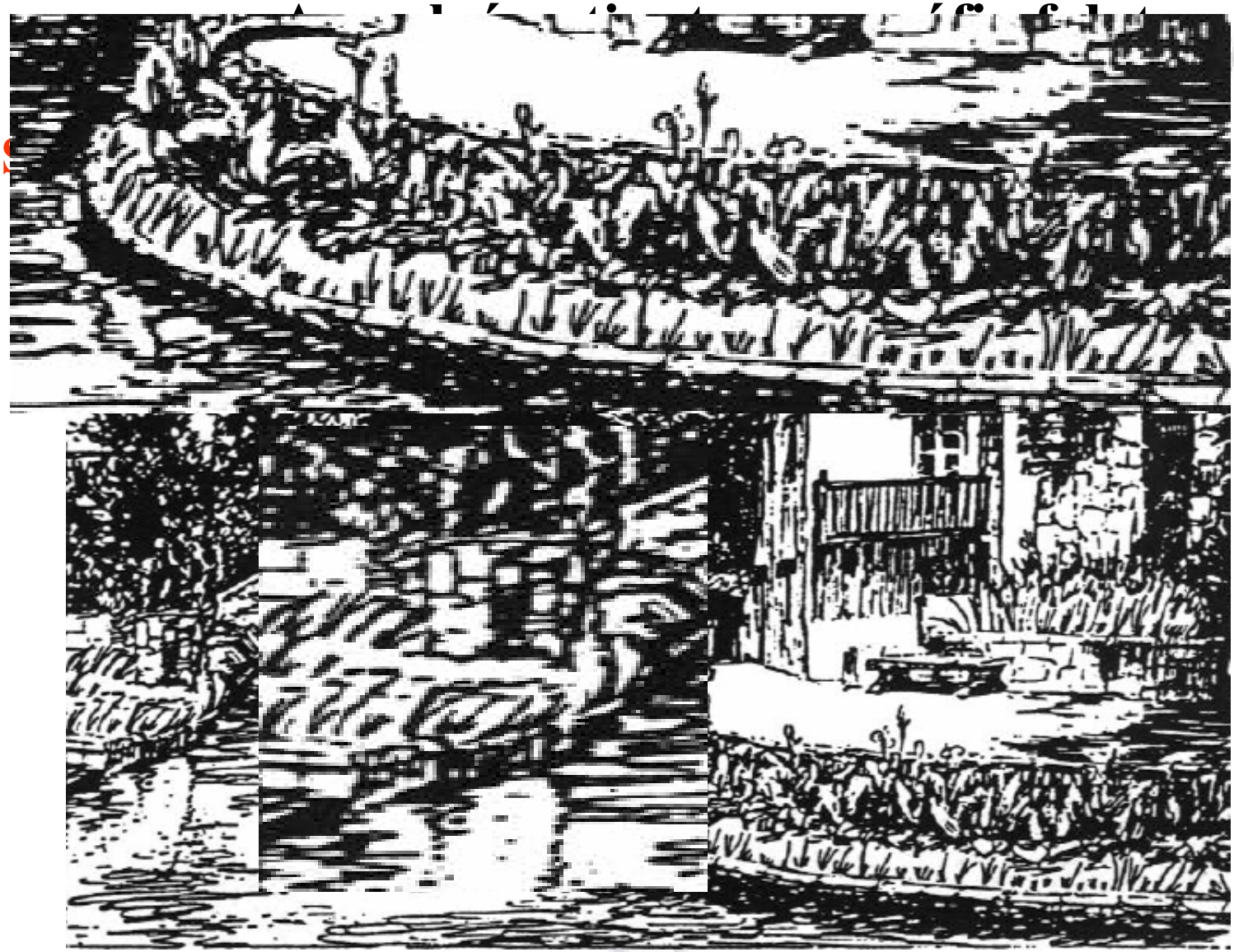
A nyelvészeti szteganográfia folyt.

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.**

Bevezetés a szteganalízisbe

Szteganalízis jelentése és célja:

- Szteganalízisnek nevezzük a rejtett információk észlelésének eljárását, melynek célja a rejtett kommunikáció felfedése.

- Nincs információ kinyerés!!!

- Nincs információ megfejtés!!!

- Védelmi szempontból az észlelés kevés!!!!

Bevezetés a szteganalízisbe folyt.

Hogyan tehetünk eleget a védelmi igényeknek?

- A szteganalízis eljárásban detektálni kell a hordozóban elrejtett üzenetet;
- A detektált üzenetet ki kell nyerni a hordozóból;
- A kinyert üzenetet meg kell fejteni.

Bevezetés a szteganalízisbe folyt.

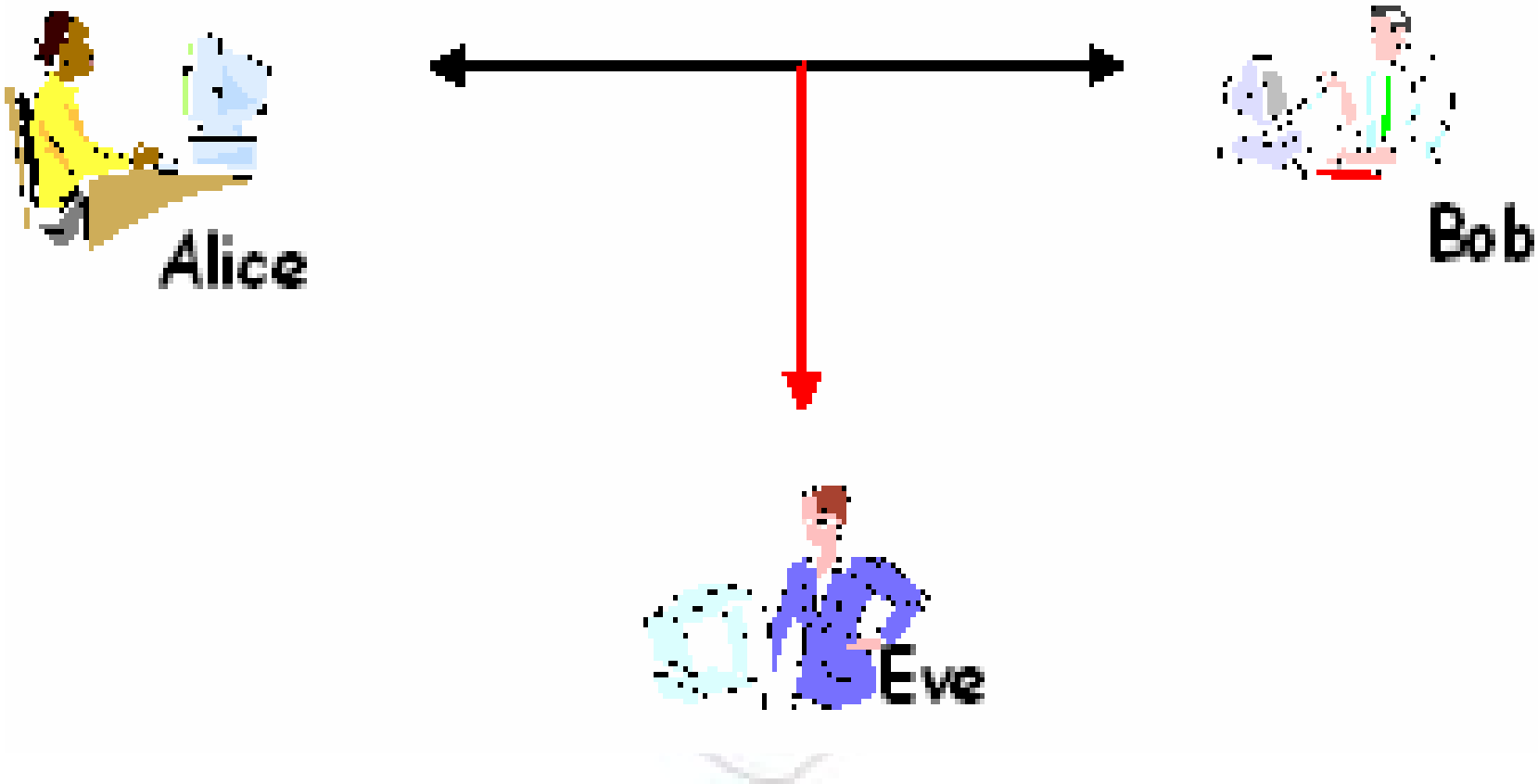
A szteganográfiai támadások célja…….

hogy a sztegomédiában felfedjük az eredeti hordozóhoz képesti változásokat, függetlenül attól, hogy ezek okoztak e szemmel érzékelhető változást az eredeti állományhoz képest.

A támadási módszerek megválasztása és a támadás kivitelezése elsődlegesen nem függvénye az alkalmazott szteganográfiai szoftvertnek.

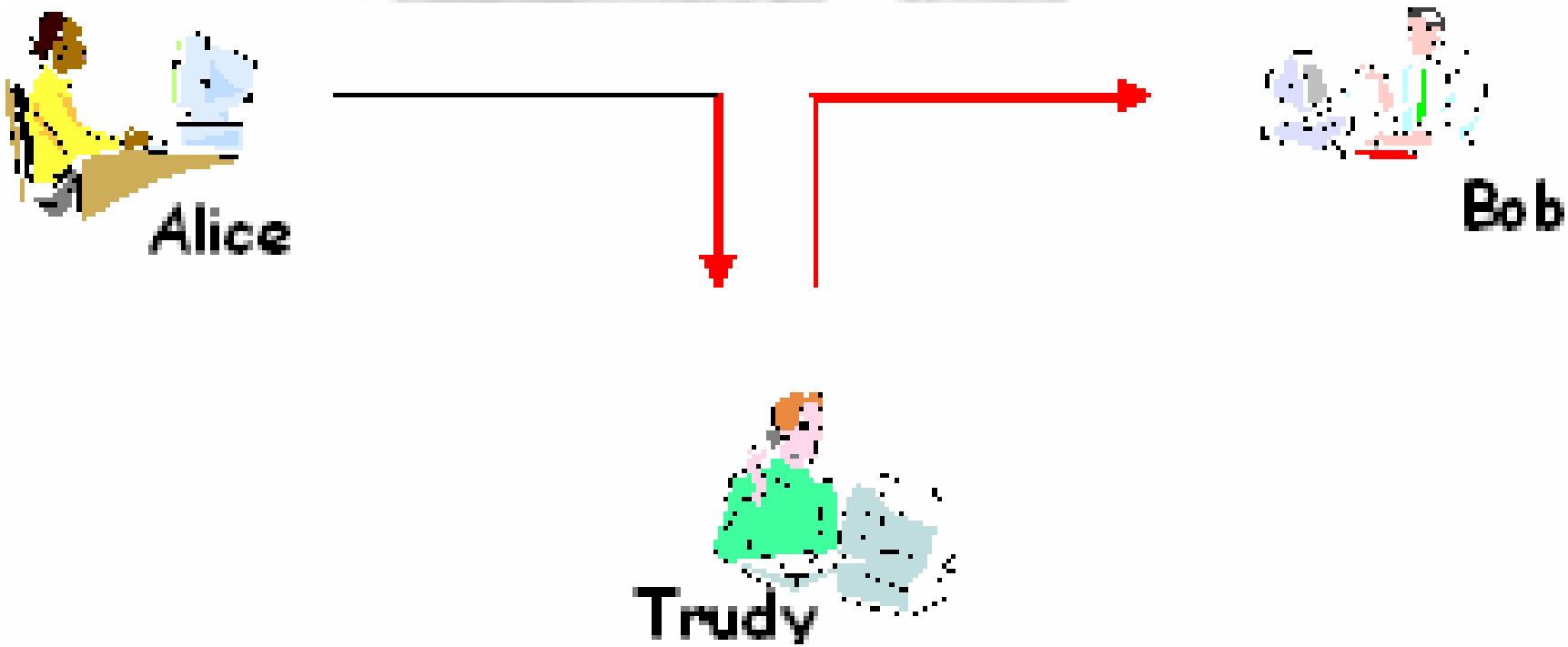
Fogvatartottak problémája.....

Passzív támadás:



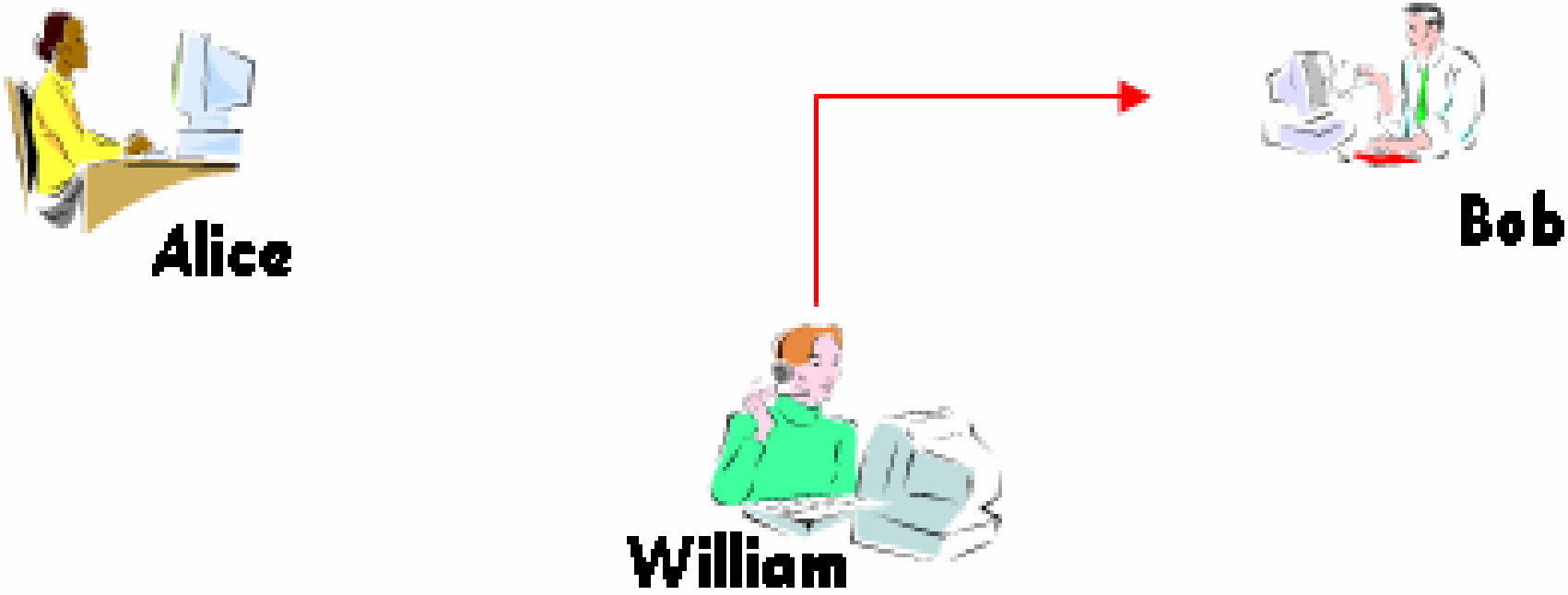
Fogvatartottak problémája.....foyt.

Aktív támadások:



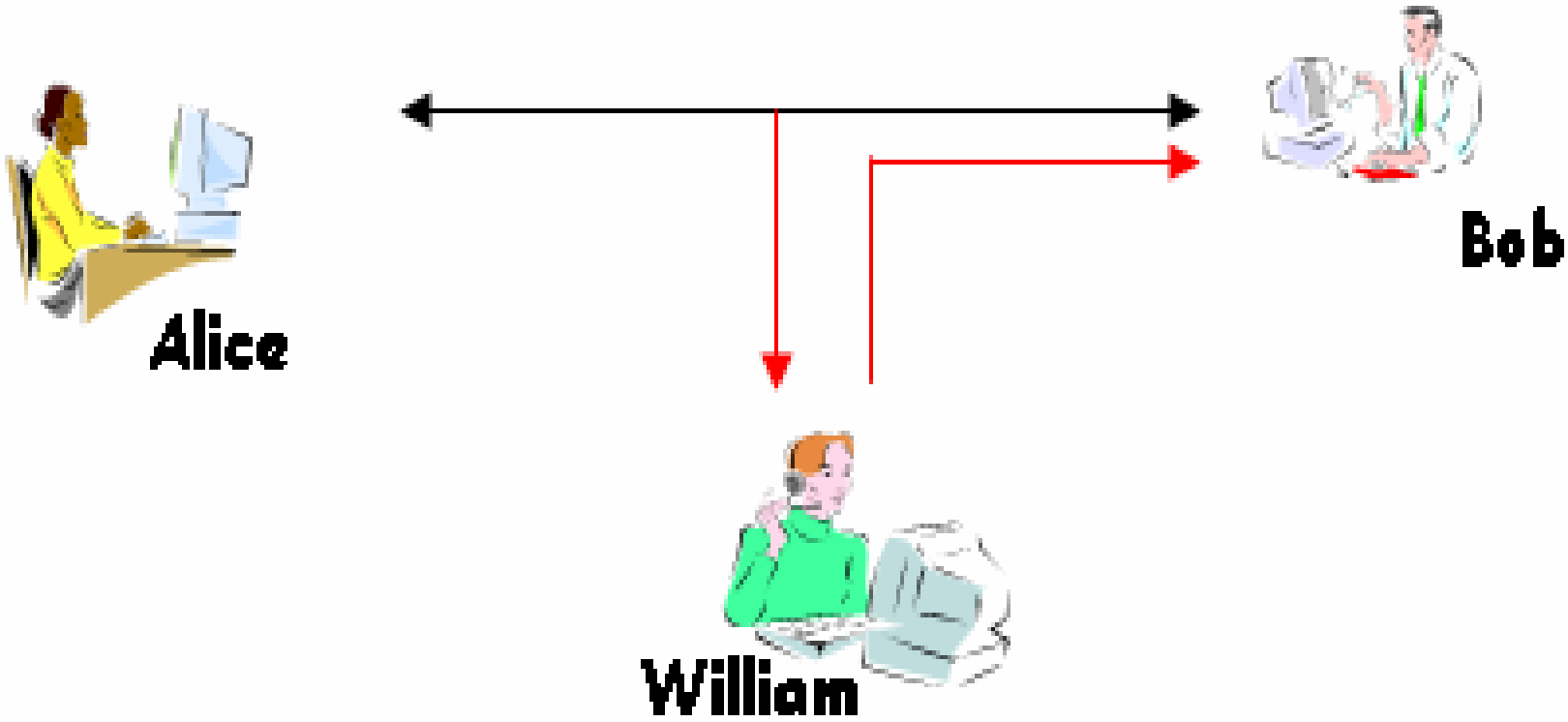
Általános szándékú aktív támadás

Fogvatartottak problémája.....foyt.



Üzenet hamisítási szándékú aktív támadás

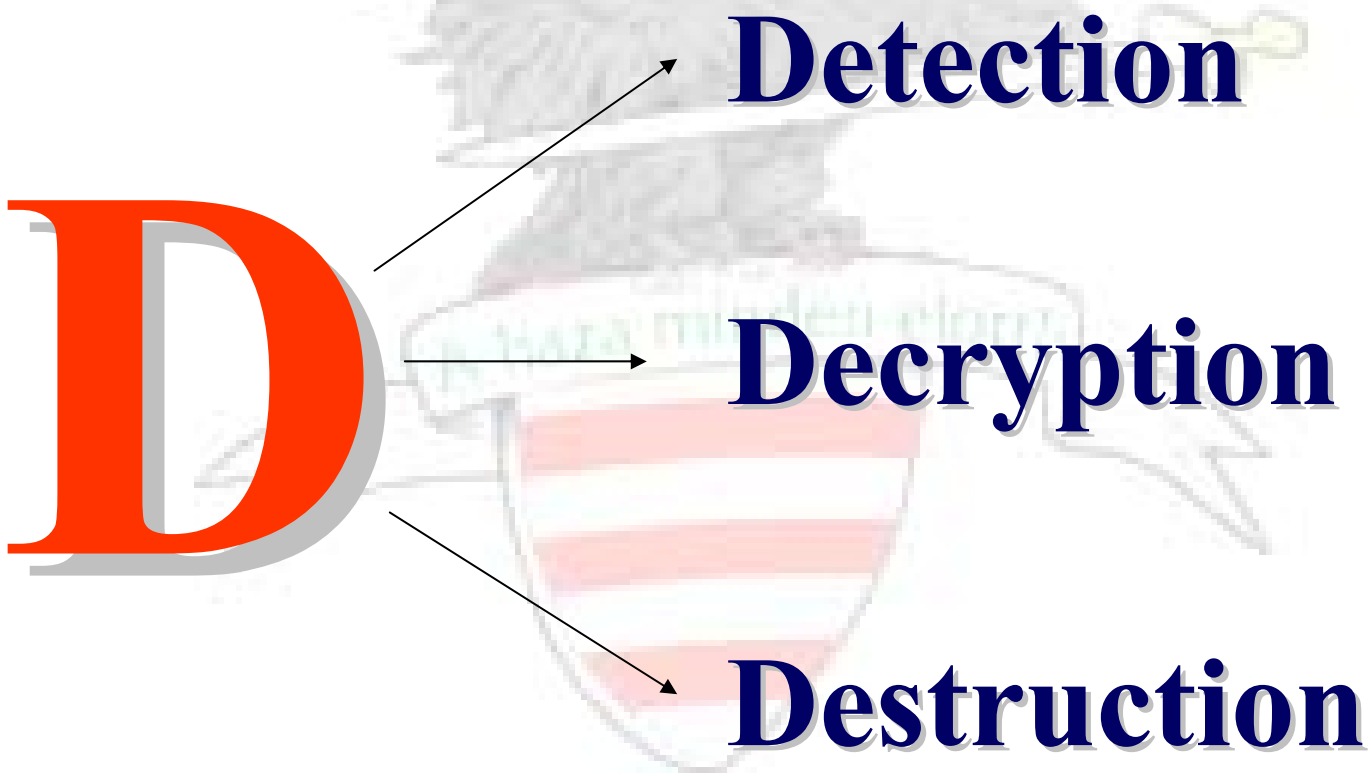
Fogvatartottak problémája.....foyt.



Aktív támadás üzenet ismételt, módosított küldésével

A szteganalízis lépései

A szteganalízist leírhatjuk mint a szteganográfiai eljárások megelőzésére irányuló tevékenységet.



A szteganográfia támadása

A következő támadási eljárásokat ismerjük:

- Csak a sztegoobjekt támadása (Stego-only attack);

- Ismert hordozó támadása *(Known cover attack);*

- Ismert üzenet támadása *(Known message attack);*

- Választott sztegoobjekt támadása *(Chosen stego attack);*

- Választott üzenet támadása *(Chosen message attack);*

- Ismert szteganográfiai támadás (*Known stego attack*);

Szteganográfia Detektálhatósága

- **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.**

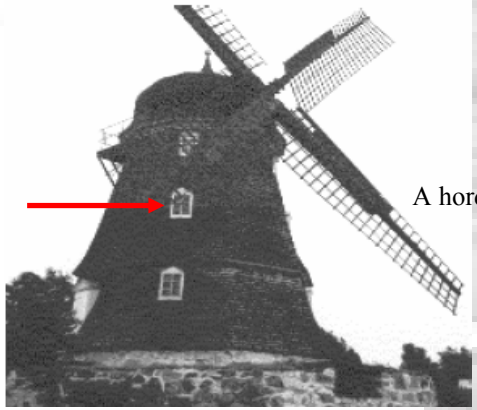
Szteganográfia Detektálhatósága folyt.

A detektálás osztályozása történhet:

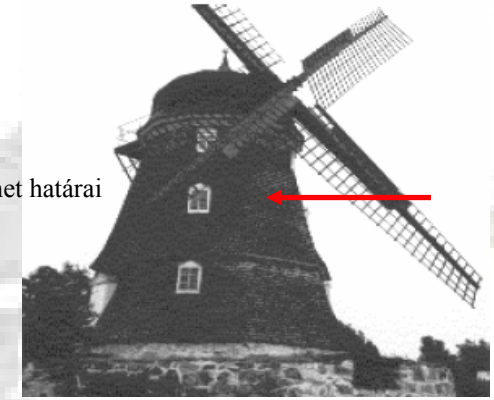
- **Fájl aláírások;**
- **Fájl anomáliák;**
- **Vizuális támadások;**
- **Statisztikai támadások;**

Szteganográfia Detektálhatósága folyt.

Vizuális támadások:

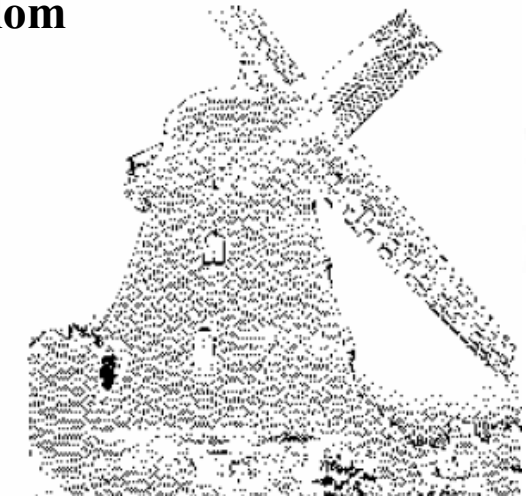


A hordozó és a rejtett üzenet határai megfigyelhetők



Eredeti hordozó **Rejtett üzenet tartalom**

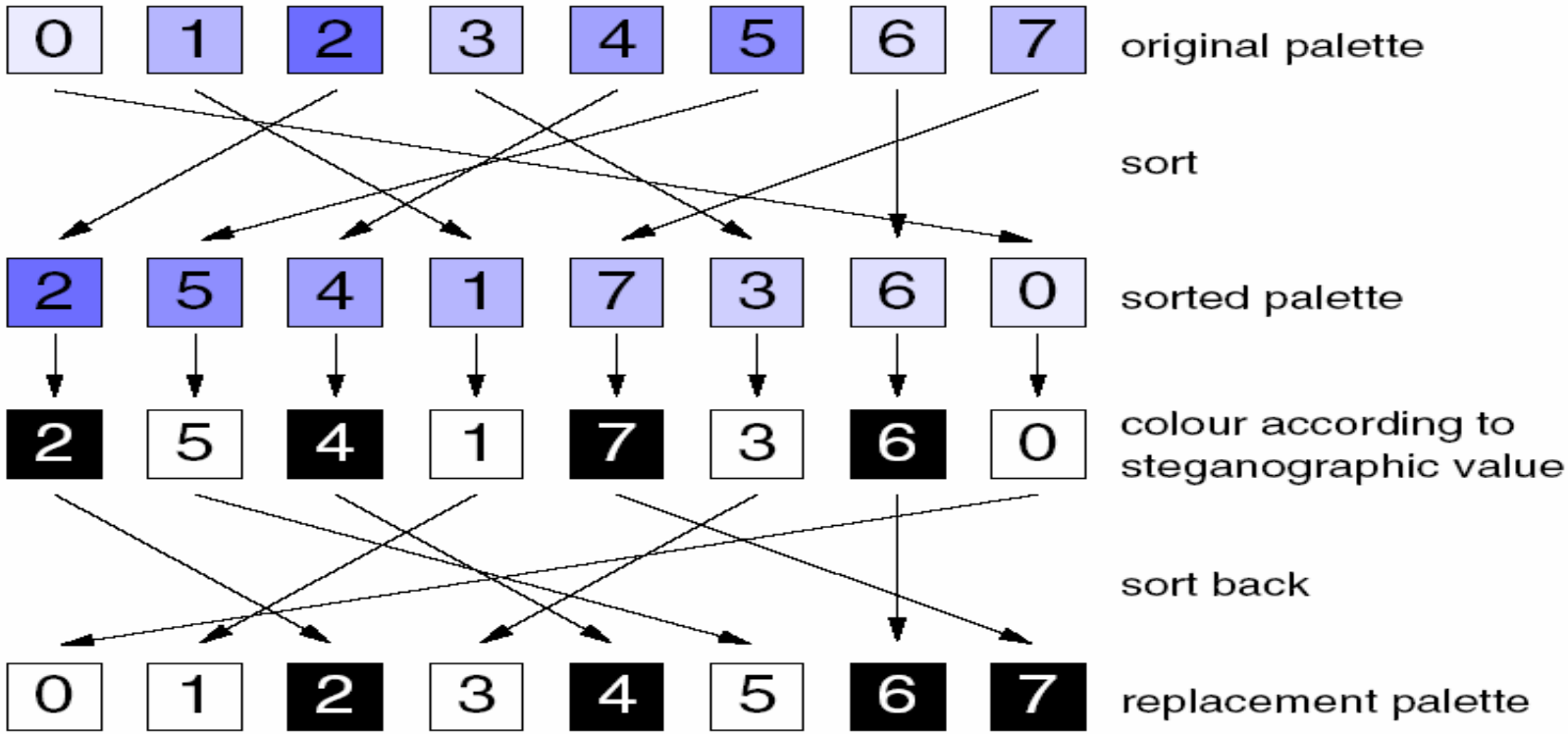
LSB=0 ha fekete



LSB=1 ha fehér

Szteganográfia Detektálhatósága folyt.

Vizuális támadások:



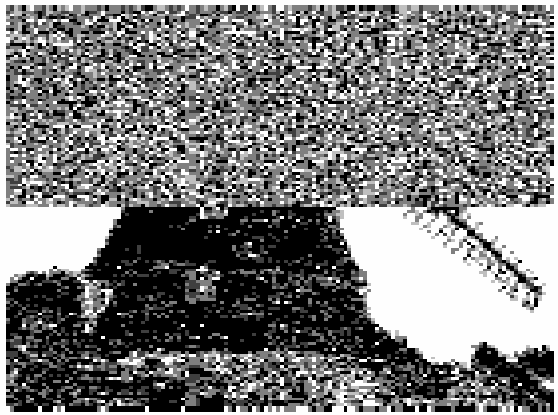
Szteganográfia Detektálhatósága folyt.

Vizuális támadások:

Eredeti hordozó

Rejtett üzenet

Szűrt A

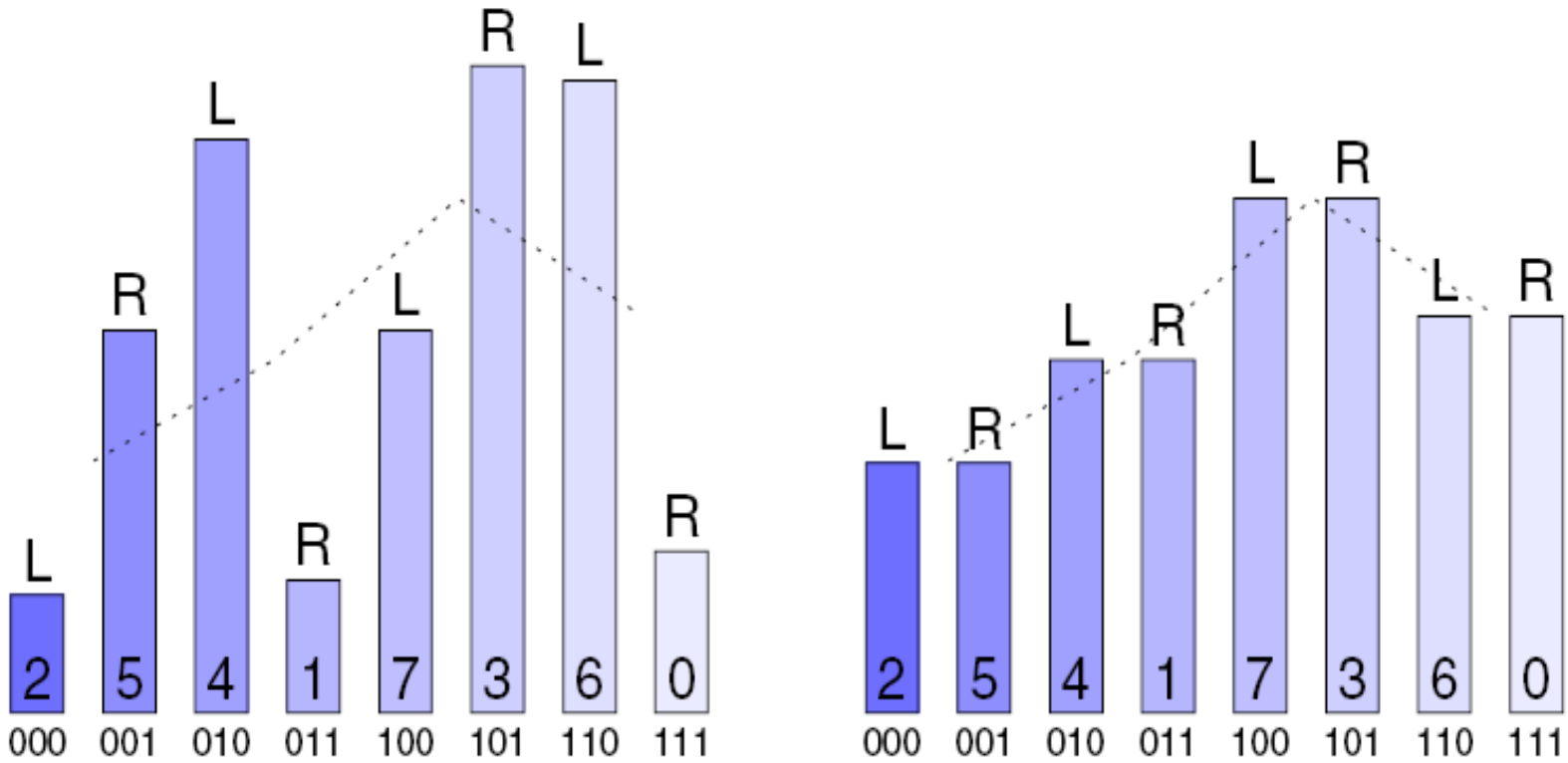


Szűrt B

Szteganográfia Detektálhatósága folyt.

Statisztikai támadások:

Chi-square Attack



A szteganalízis eszközei

A szteganográfia detektálására hivatott szoftvereket szteganalitikai eszközöknek hívjuk.

Néhány szabadon felhasználható, néhányuk fiztetős és meglehetősen drága.

A rejtett információ detektálása után a beágyazott tartalmat ki kell nyerni a hordozóból.

Néhány szteganalitikai szoftver:

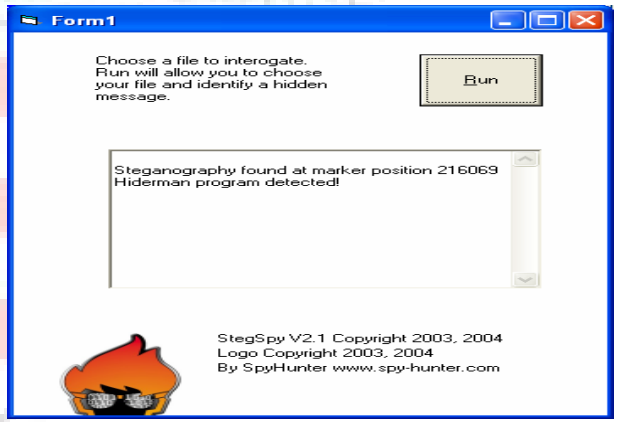
Szoftver neve	Detektált média	Licence	Fejlesztő/gyártó
StegSpy	JPEG	Szabadon felhasználható	Michael T. Raggo
Stegdetect	JPEG	Nyílt forrású	Niels Provos
StegBreak	JPEG	Nyílt forrású	Niels Provos
StegSuite		Licence díjas	Wetstone Technologies
StegAnalyzer	JPEG	Licence díjas	Wetstone Technologies

A szteganalízis eszközei folyt.

Stegspy:

25/a Eredeti hordozó (1.1 MB)

25/b StegSpy analízis eredménye

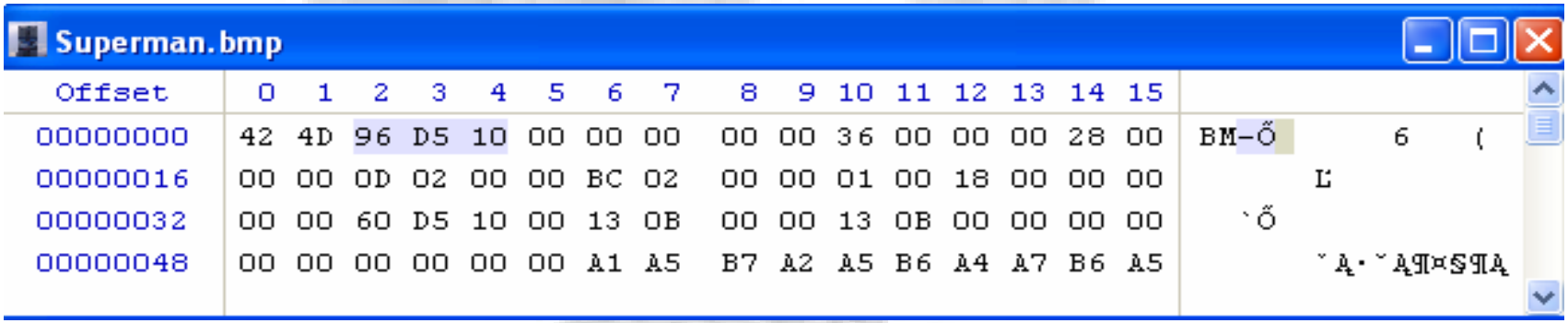


Beágyazott állományt tartalmazó hordozó (108,5 KB)

Beágyazott állomány a hordozóban, a 216069-os poziciótól kezdődően

A szteganalízis eszközei folyt.

Stegspy:

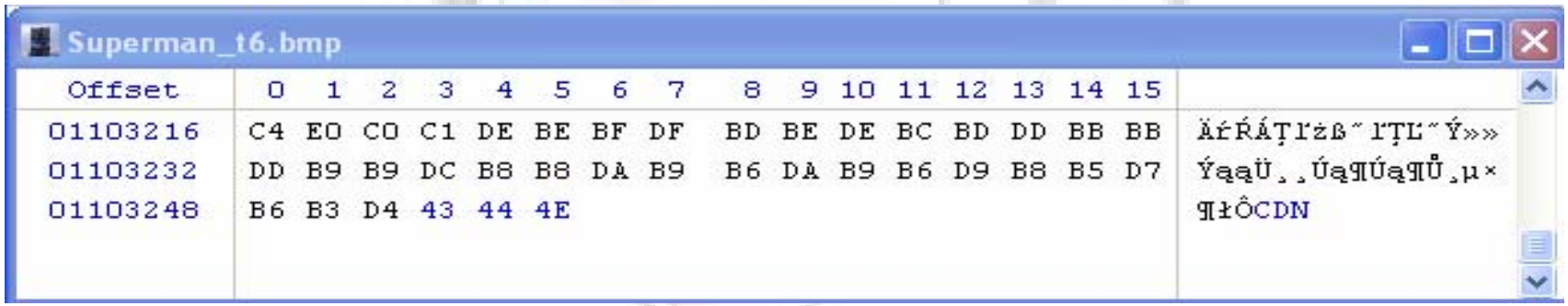


Superman.bmp

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	42	4D	96	D5	10	00	00	00	00	00	36	00	00	00	28	00
00000016	00	00	0D	02	00	00	BC	02	00	00	01	00	18	00	00	00
00000032	00	00	60	D5	10	00	13	0B	00	00	13	0B	00	00	00	00
00000048	00	00	00	00	00	00	A1	A5	B7	A2	A5	B6	A4	A7	B6	A5

BM–Ő 6 (
L
`Ő
ˇĄ·ˇĄ¶¤§¶Ą

A BMP fájl fejlécének kezdete



Superman_t6.bmp

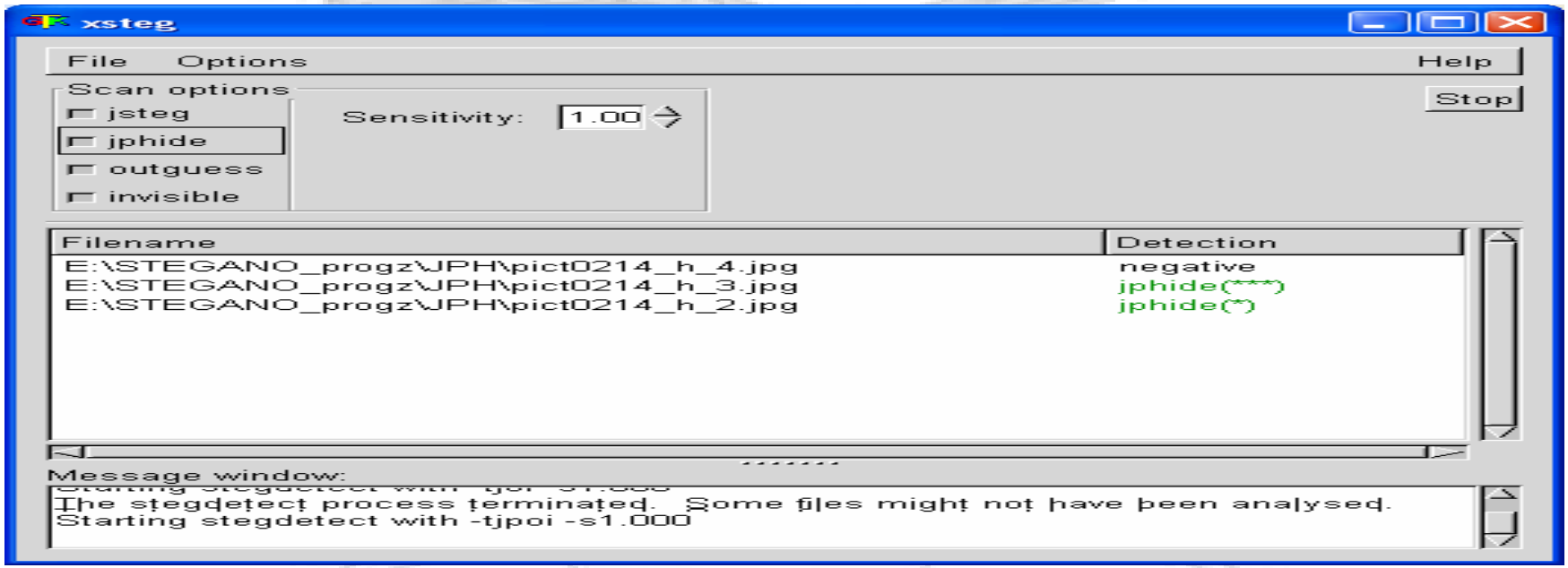
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
01103216	C4	E0	C0	C1	DE	BE	BF	DF	BD	BE	DE	BC	BD	DD	BB	BB
01103232	DD	B9	B9	DC	B8	B8	DA	B9	B6	DA	B9	B6	D9	B8	B5	D7
01103248	B6	B3	D4	43	44	4E										

ÄŕŔÁŢľžß˝ĽŢĽ˝Ý»»
Ýąą Ü¸¸Úą¶Úą¶Ů¸µ×
¶ŁÔCDN

A BMP fájl fejlécének vége

A szteganalízis eszközei folyt.

Stegdetect:



JPEG fájl detektálása a Stegdetect programmal

A szteganalízis eszközei folyt.

Stegbreak:

- **Niels Provos által kifejlesztett alkalmazás;**

- **DOS alatt futó alkalmazás, ami teljes kipróbálású szótár-támadások elvégzését teszi lehetővé JPEG formátumú képek ellen.**

- **A támadás során a beágyazásnál használt jelszó megfejtése után az elrejtett információt nyeri ki a hordozóból.**

- **A Stegbreak sikere természetesen szorosan összefügg a jelszó és a könyvtár minőségétől. A szavak könyvtárban történő változtatásának szabálya szintén szorosan összefügg a sikerrel.**

A szteganalízis eszközei folyt.

StegoSuite:

A WetStone által kifejlesztett szoftver széles körben elterjedt az igazságügyi szakértői körökben, mivel lehetővé teszi a szteganográfiai módszerek teljes tárházának felfedését.

StegoSuite moduljai:

StegoAnalyst;

StegoBreak;

StegoWatch;

A szteganalízis eszközei folyt.

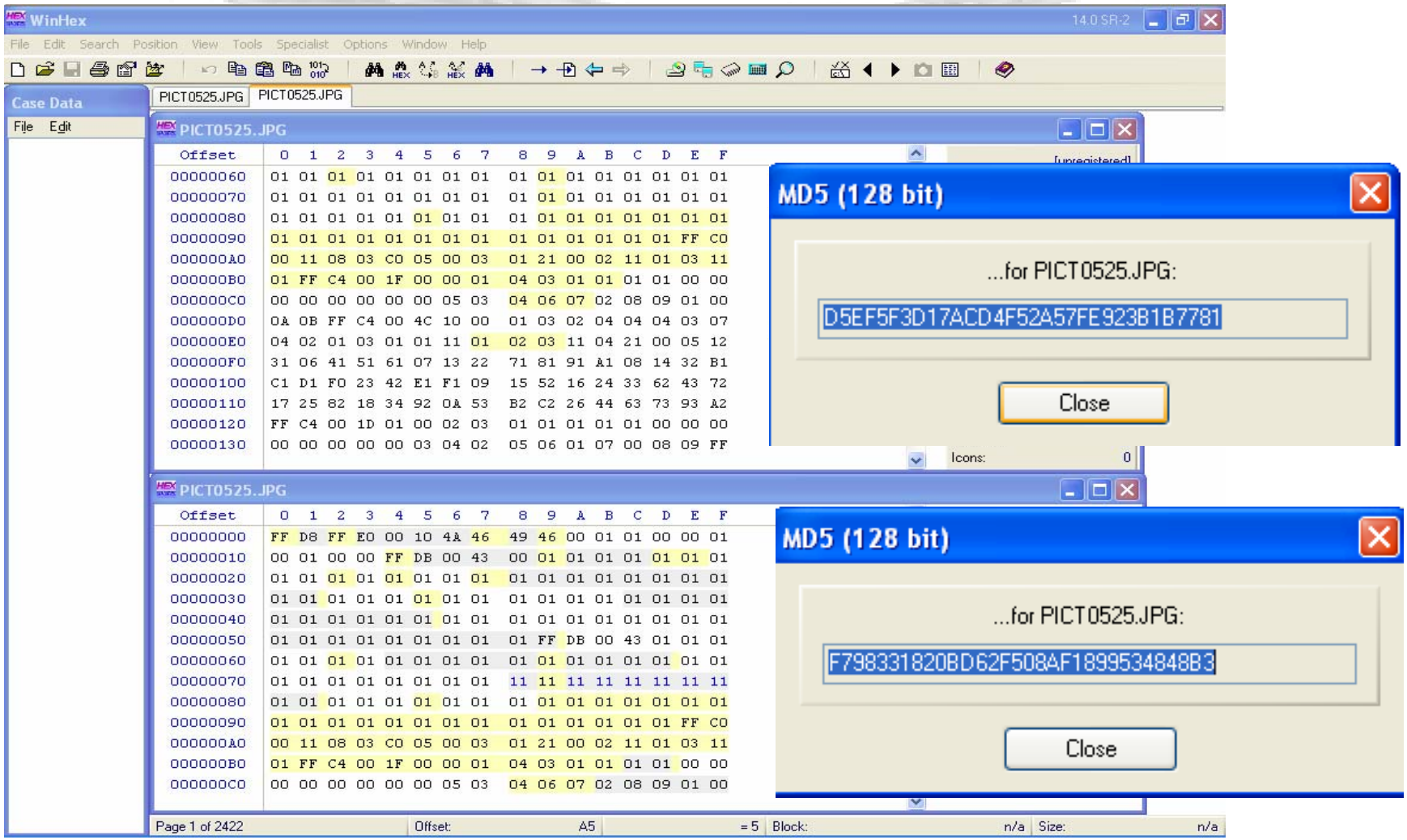
StegAnalyzer:

Jelenleg a Backbone Security két verzióban kínálja a StegAnalyzer-t:

- **A StegAnalyzer AS fájlrendszerek felderítésére szolgál, azokat képes átkutatni, ismert szteganográfiai szoftverek nyomait keresve.**
- **A StegAnalyser SS képes az ismert sztegoobjektum fájlaláírások detektálására, amellett, hogy az AS modifikáció valamennyi képességével bír.**

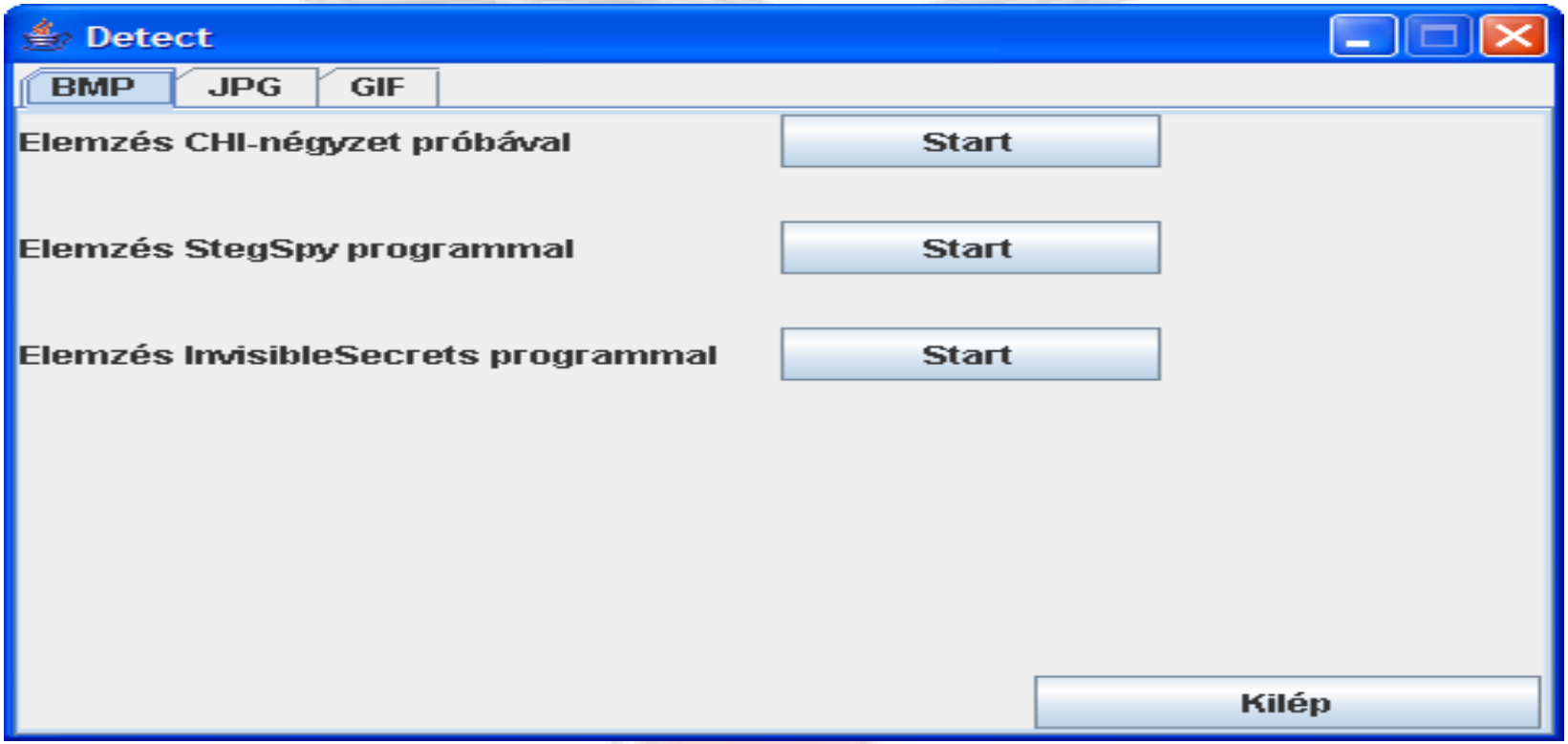
A szteganalízis eszközei folyt.

WinHex:



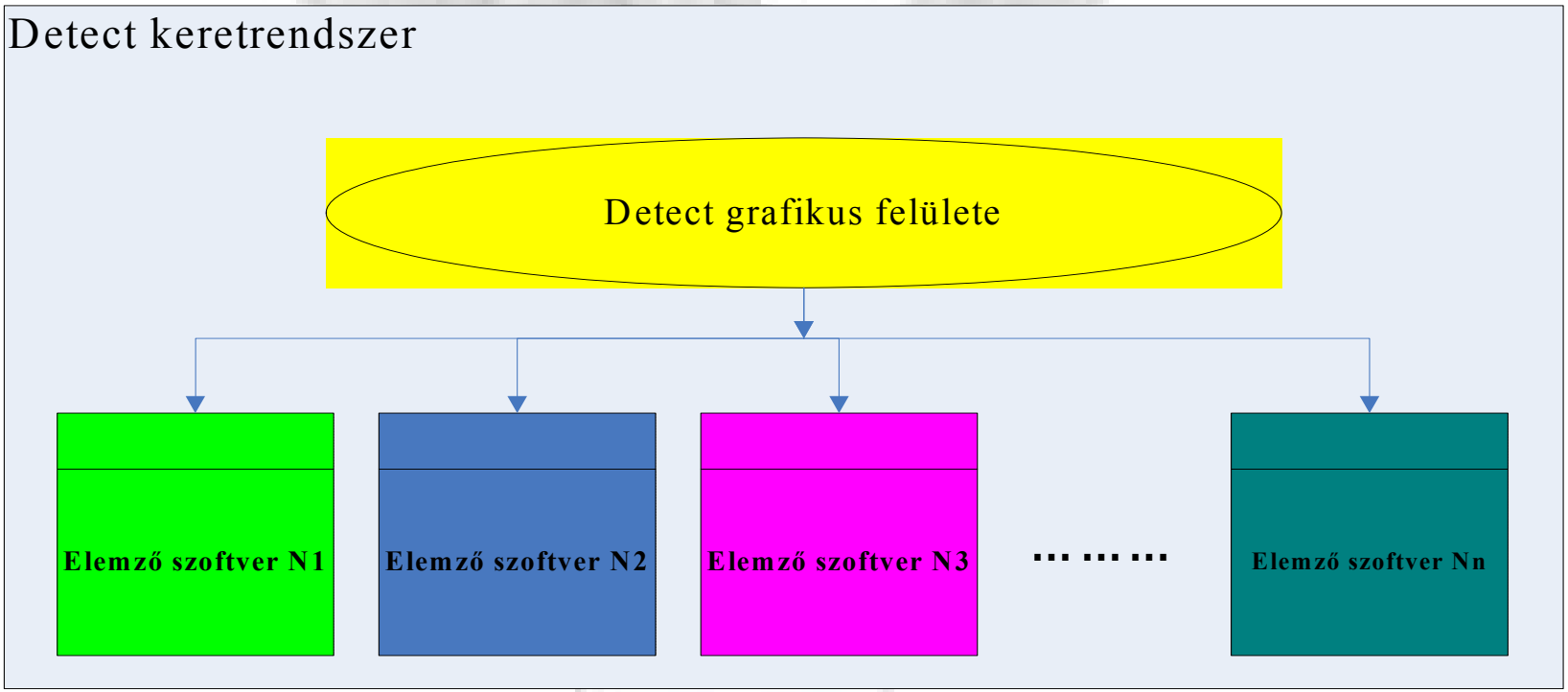
A szteganalízis eszközei folyt.

Detect:



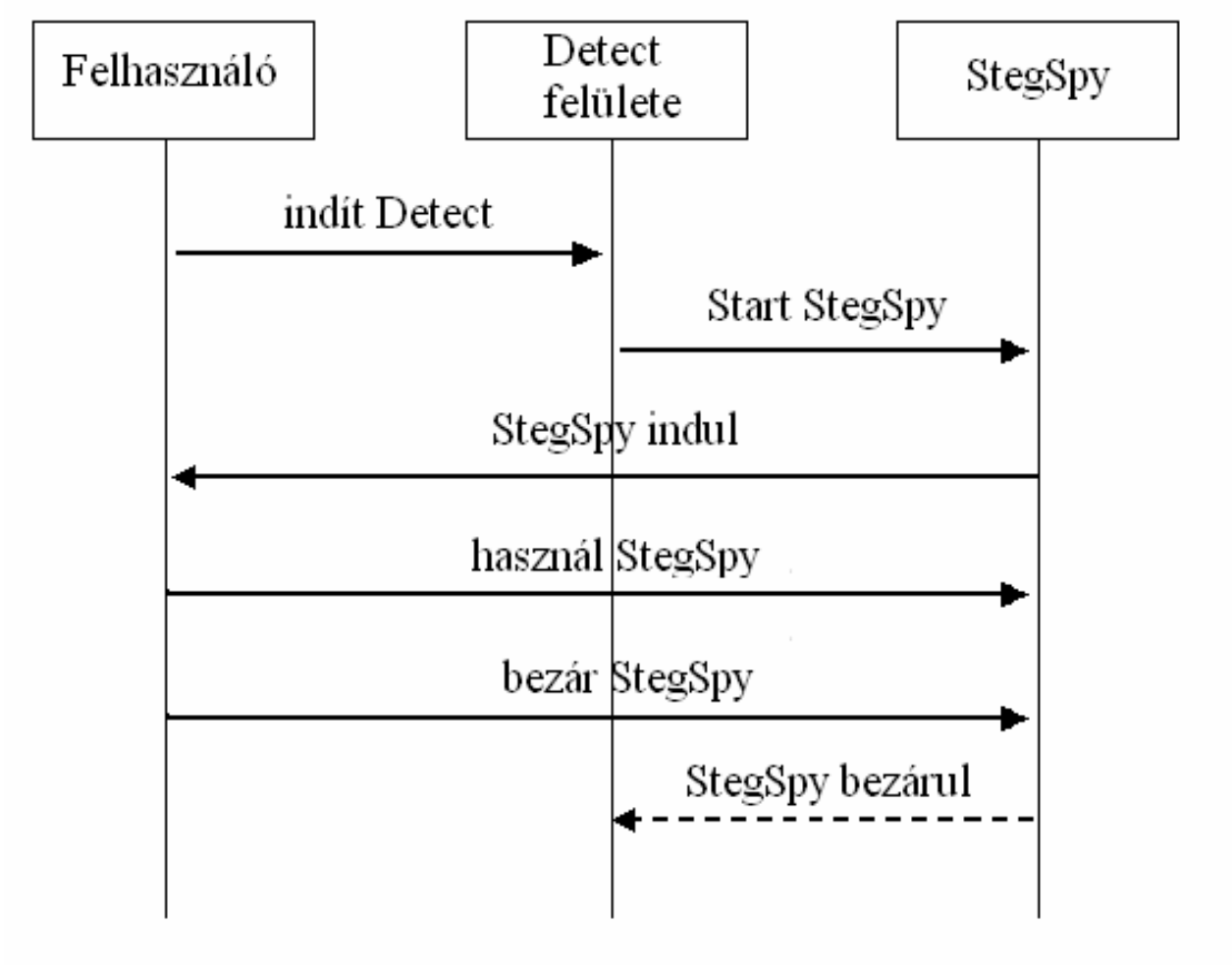
A szteganalízis eszközei folyt.

Detect:



A szteganalízis eszközei folyt.

Detect:



A szteganalízis eszközei folyt.

Detect:

Továbbfejlesztési irányok:

- a keretrendszerben a jövőben még több analizáló szoftver jelenhet meg, mely nem csak a jelenlegi hordozómédiákra biztosít több elemzési lehetőséget, hanem újabb hordozómédiát is képes vizsgálni;

- a Detect bemenetére érkező sztegoobjektum paraméterei alapján kerül automatikusan kiértékelésre, majd az eredménynek megfelelően automatikusan elindul a Detect megfelelő moduljának futása;

A szteganalízis eszközei folyt.

Detect:

Továbbfejlesztési irányok:

-a keretrendszerből indítható analizáló szoftverek bővülésével párhuzamosan merül fel az igény, hogy a Detect több szálon tudjon futni oly módon, hogy egyszerre többféle médián, több elemzés legyen végrehajtható.

A Szteganográfia észlelésének problémái

- Relatíve új és gyorsan fejlődő tudomány;
- Magas a „false positive” szám;
- hatalmas mennyiségű képi média, valamint majdnem mindegyikre létező szteganográfiai alkalmazás ;
- nagy monotonitású képek és rajzok esetében szintén magas „false positive”;
- kifejezetten problémás a kis terjedelmű üzenetek detektálása;
- titkosítás alkalmazása a szteganográfiai szoftverekben.

Igazságügy vs. Szteganográfia

- A szteganográfia természetes törekvése, hogy rejtve maradjon. Nincs kellő publicitása az igazságügyi oldalról elért eredményeknek, nincs statisztika.

- A szteganográfia hatásainak mellőzése a statisztikai hiányosságok miatt rossz alternatíva.

- Természetes azt feltételezni, hogy a szteganográfiát használják, vagy használni fogják, mivel jellegzetessége a rejtés, ami vonzó a bűnözők számára.

- Ezért, ha a bűnözők még nem is használják a szteganográfiát, a jövőben a cyberspace bűnözők által alkalmazott eszközökben biztosan felbukkannak majd a szteganográfia különböző adaptációi.

A szteganográfia legyőzése

- A szteganográfiai alkalmazások legyőzésének folyamata hasonlít a kriptoanalízishez. Az előforduló gyenge pontok feltárására koncentrál.

- Néhány megközelítés a statisztikai változásokat (fájlanomáliák, furcsa paletták, ismert fájlaláírások stb.) vizsgálja, míg mások a vizuális felderítést helyezik előtérbe.

- Mindezek ellenére az igazságügyi szakértőknek más eszközök is rendelkezésükre állnak.

A szteganográfia legyőzése folyt.

- digitális bűntény helyszínének vizsgálata;
- sztegelemzés;
- szteganográfiai szoftver detektálása;
- szteganográfiai szoftver nyomai;
- hordozó/sztegofájl párok lokalizálása;
- kulcsszó-keresés és aktivitás monitorozása;
- gyanúsított számítástechnikai ismeretei;
- valószínűtlen fájlok keresése;
- szteganográfiai kulcsok lokalizálása;
- rejtett tároló helyek;

Szteganográfiai alkalmazások

S-Tools

- GIF, BMP, WAV

JP Hide&seek

- JPEG

MP3Stego

- MP3

Steghide

- BMP, JPEG, WAV, AU

Szteganalitikai alkalmazások

StegSpy

- JPEG

StegDetect

- JPEG

Stegbreak

- JPEG

Detect

- BMP, JPEG, GIF, WAV, AU

Összegezve

- A szteganográfia nem más mint az információ elrejtésének módja egy kiválasztott hordozóba.
- A szteganalízis a rejtett információk felfedésére irányuló komplex tevékenységek összessége.
- Az interneten szabadon elérthető programok garmadája.
- Sokkal kevesebb publikált analitikai program, többségük borsos árakon.
- Az adatrejtés detektálása meglehetősen bonyolult, de nem lehetetlen feladat.
- Kombinált eljárások végrehajtása.
- Sok anekdóta kering a szteganográfia különösen terroristák általi használatáról.
- Nincs statisztikai kimutatás az analitikai szoftverek sikerességéről.
- Eddig senki nem talált erre nézve perdöntő bizonyítékot.

1997. Luisburg.....Árja Testvériség.

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!