pet portál

A szteganográfia és annak relevanciája a privátszféra védelmében

Földes Ádám Máté
foldesa@pet-portal.eu

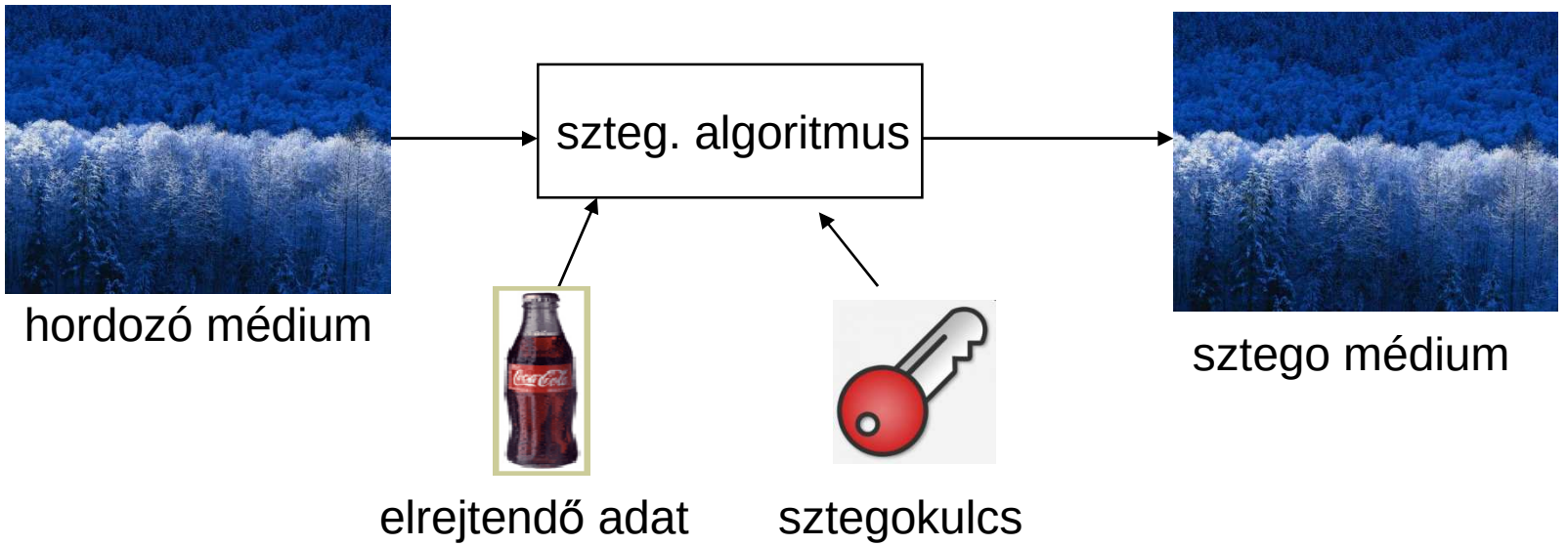
Hacktivity 2008
Budai Fonó Zeneház, 2008. szeptember 21.

Tartalom

- Bevezető
  - Alapfogalmak, rövid történeti áttekintés
  - Kapcsolat a privátszférával
  - Problémák
- Adatrejtés hordozó médiumba
- Vízjelek
- Rejtett csatornák
- Szteganalízis

Alapfogalmak

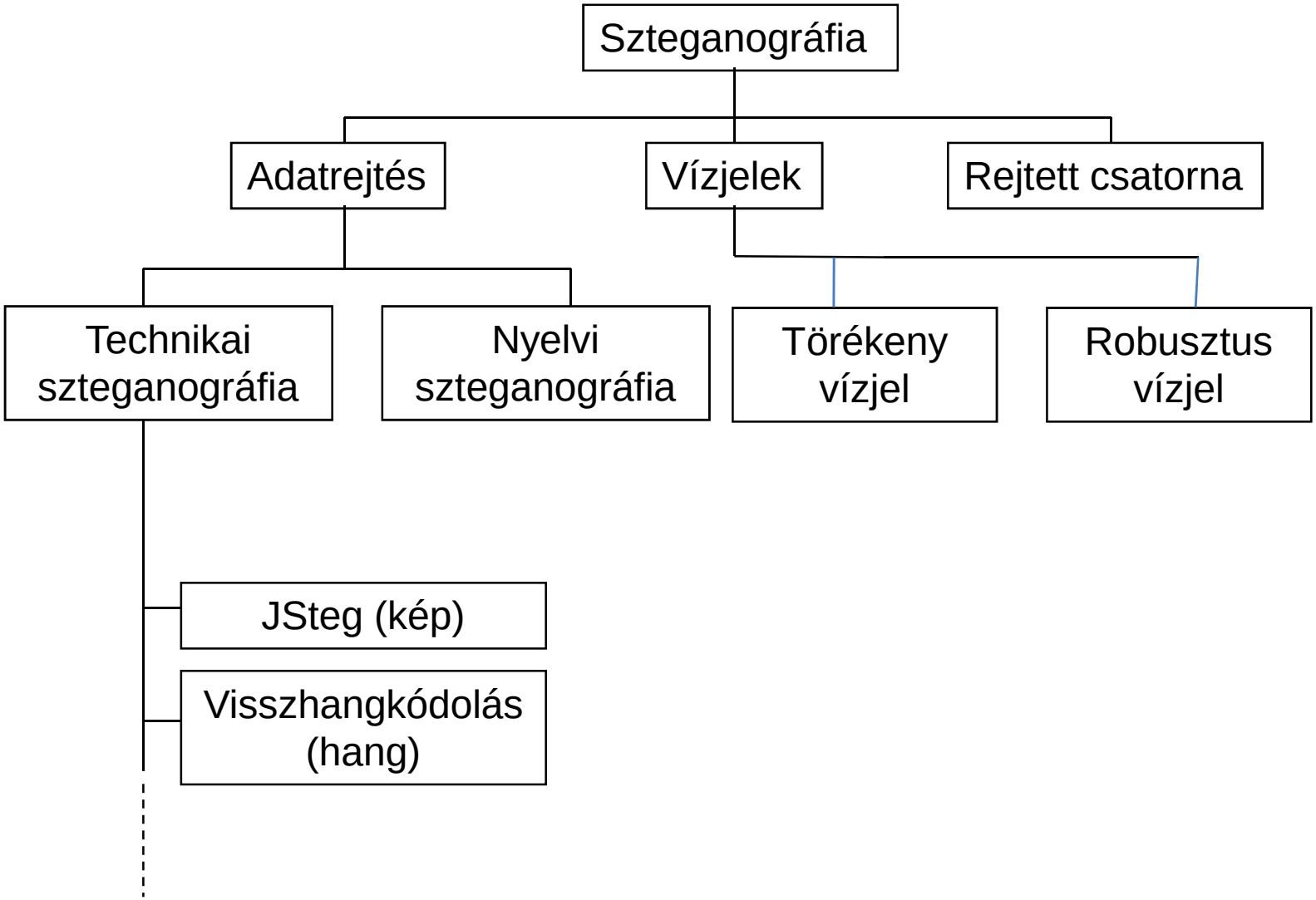
- Szteganográfia – a „rejtett írás”
- Hordozó médium (cover media)
- Sztego kulcs (stego key)
- Sztego médium (stego media)



Történeti áttekintés

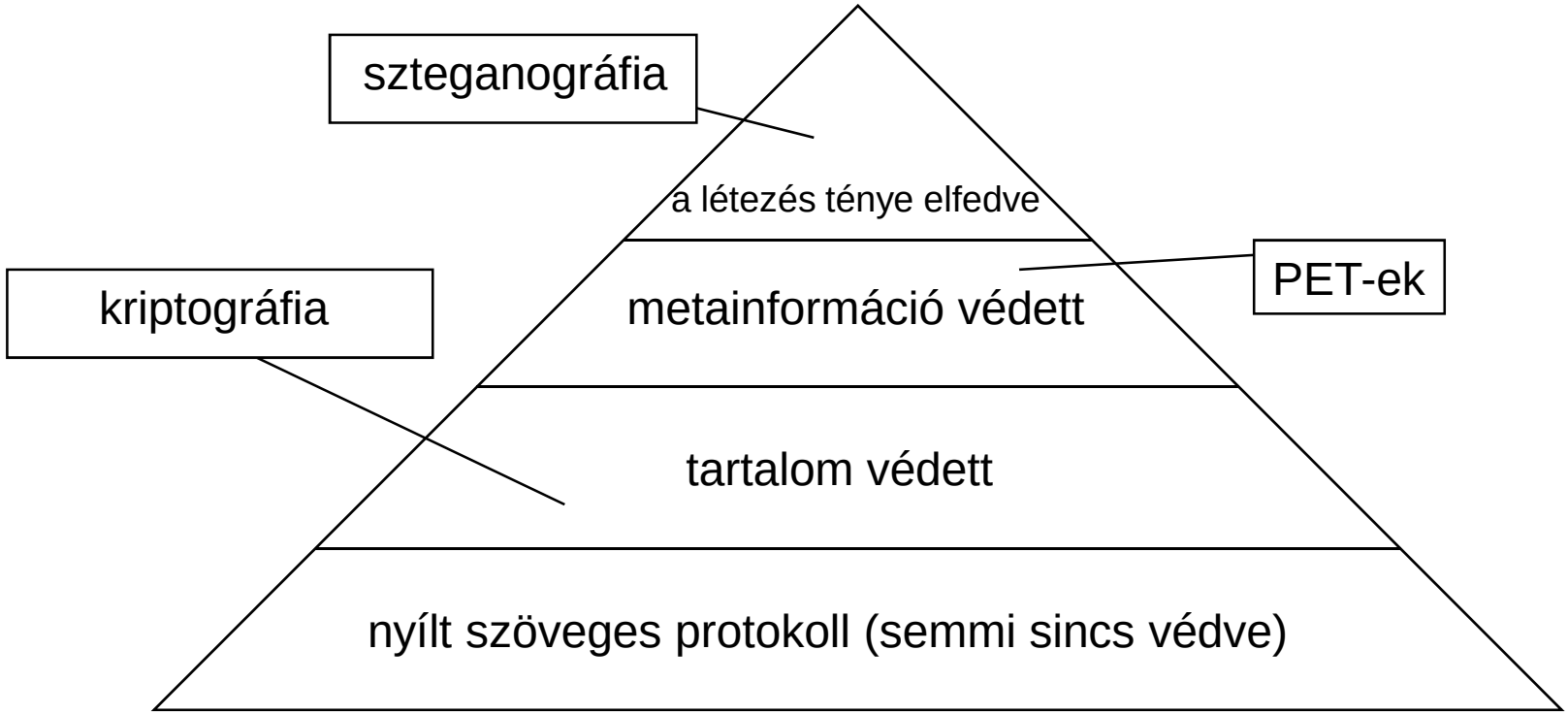
- Első feljegyzések a szteganográfia alkalmazásáról: Kr. e. 440. (hordozók: agyagtáblák, szolga feje)
- 1499: Steganographia (Trithemius)
- Egyéb technikák:
  - láthatatlan tinta
  - szöveg első betűi
  - stb.
- Probléma: Kerkchoff-elv

A szteganográfia „családfája”

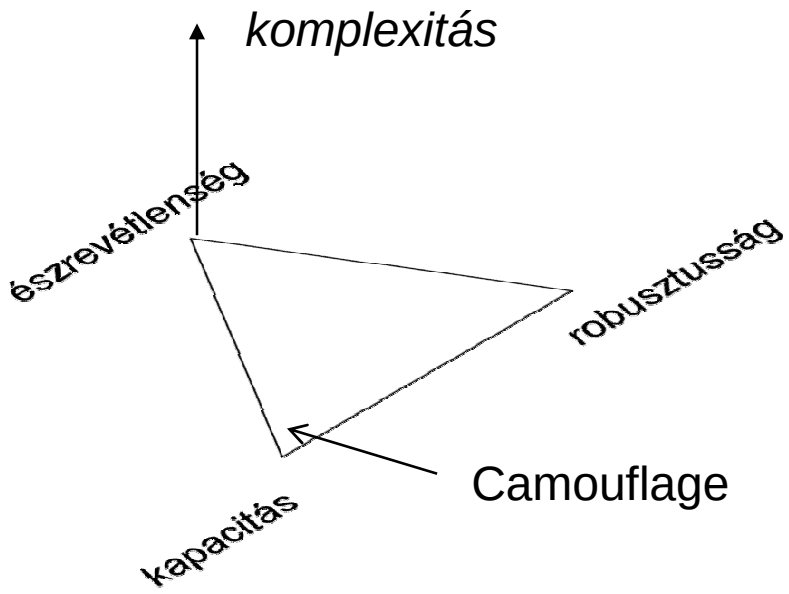


Kapcsolat a privátszférával

- Az információ védelmének szintjei



Problémák



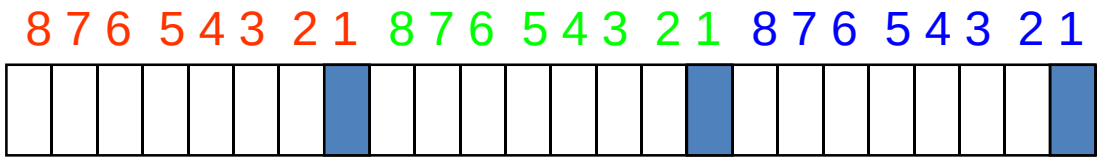
- Ismerni kell a hordozó médium típusát, és alkalmazkodni kell hozzá
  - antipélda: Camouflage

Tartalom

- Bevezető
  - Alapfogalmak, rövid történeti áttekintés
  - Kapcsolat a privátszférával
  - Problémák
- Adatrejtés hordozó médiumba
- Vízjelek
- Rejtett csatornák
- Szteganalízis

Adatrejtés tömörítetlen képekbe

- LSB
  - gyakran használt, egyszerű eljárás
  - pixelenként a legjelentéktelenebb bitekbe kódolt információ
  - szem nehezen veszi észre
  - nem robusztus az újratömörítéssel szemben



Adatrejtés tömörítetlen képekbe II.

- palettás képeknél használt módszerek
  - palettába rejtünk (pl. permutáció, paletta LSB)
    - probléma:
      - a kép méretétől független, nagyon kicsi kapacitás
      - gyanús permutáció feltűnő lehet
  - csökkentjük a paletta méretét, és a „felszabadult” helyre tesszük az információt
    - probléma: feltűnő, ha nincsenek közeli színek

Adatrejtés tömörítetlen képekbe III.

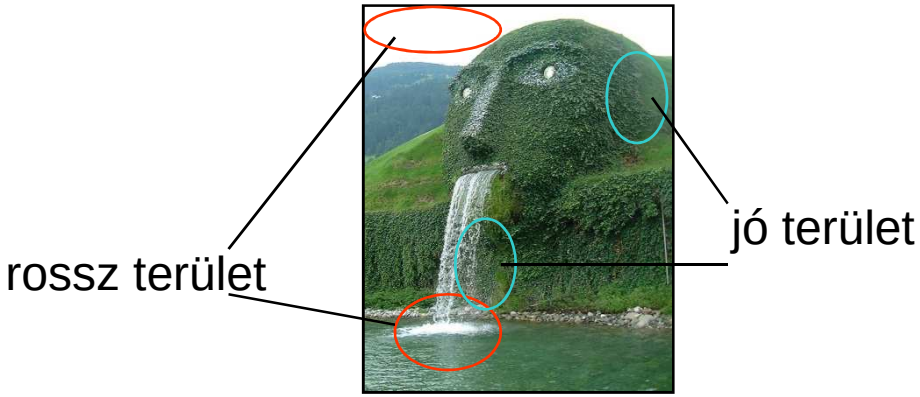
- Palettamanipulációs példa

paletta redukciója 32 színre

256 szín visszaállítása (új színek kódolják az információt)

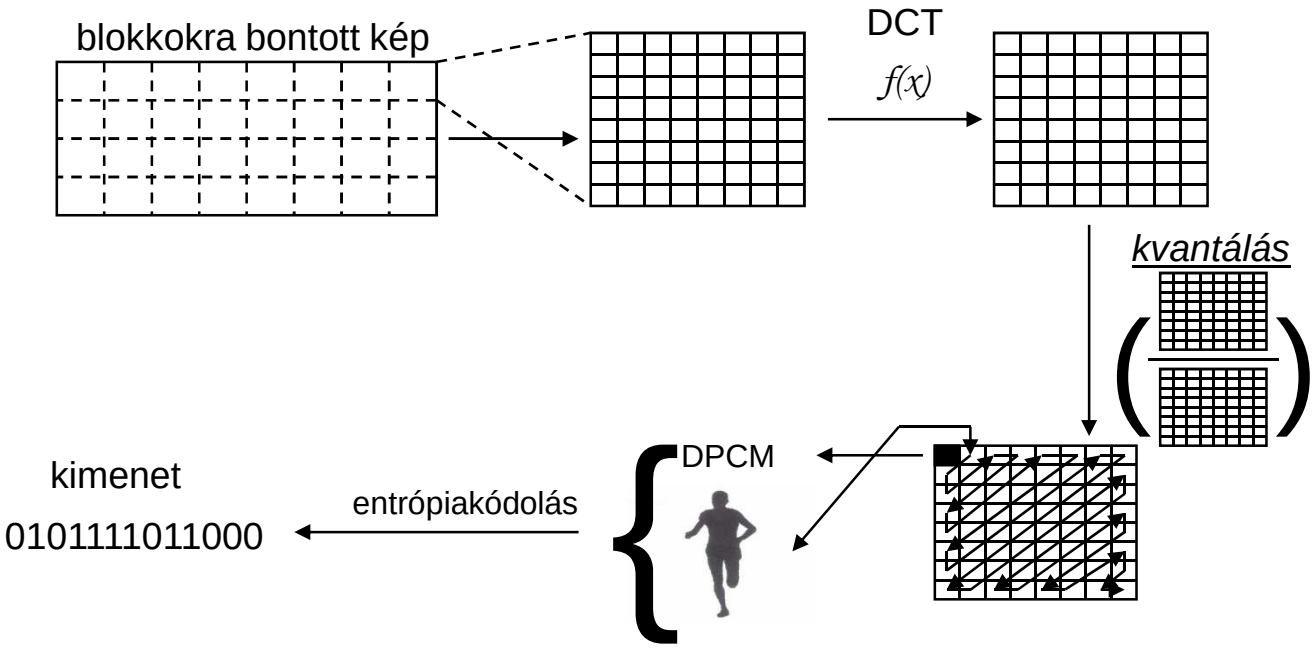
Adatrejtés tömörítetlen képekbe IV.

- Adaptív adatrejtés
  - a kép dinamikájához alkalmazkodva keressük az információrejtésre alkalmas képpontokat
  - probléma: nehéz programmal definiálni az alkalmas pixeleket



Adatrejtés tömörített képekbe

- JPEG
  - elterjedt képtömörítési módszer
  - lépései nagyvonalakban

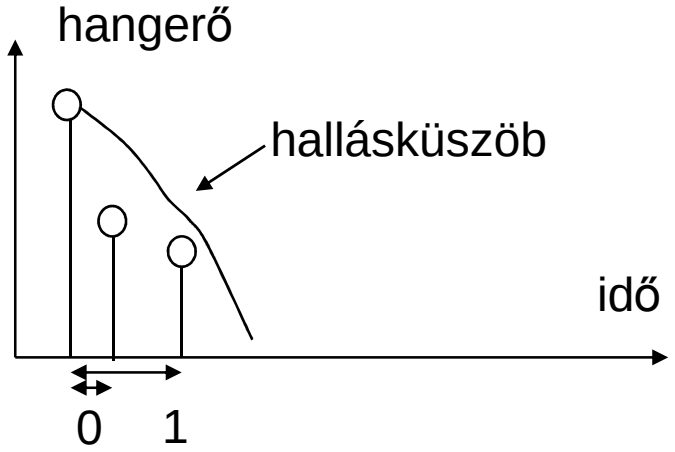


Adatrejtés tömörített képekbe II.

- együttható-kerekítéses módszer
  - kvantáláskor benyúlunk a kerekítésbe a 0,5-höz közeli törtrészű DC együtthatóknál
  - probléma: kell az eredeti kép, mert azzal összevetve találjuk meg az adatrejtési helyeket
- egyéb módszerek
  - JSteg
  - F5
  - OutGuess

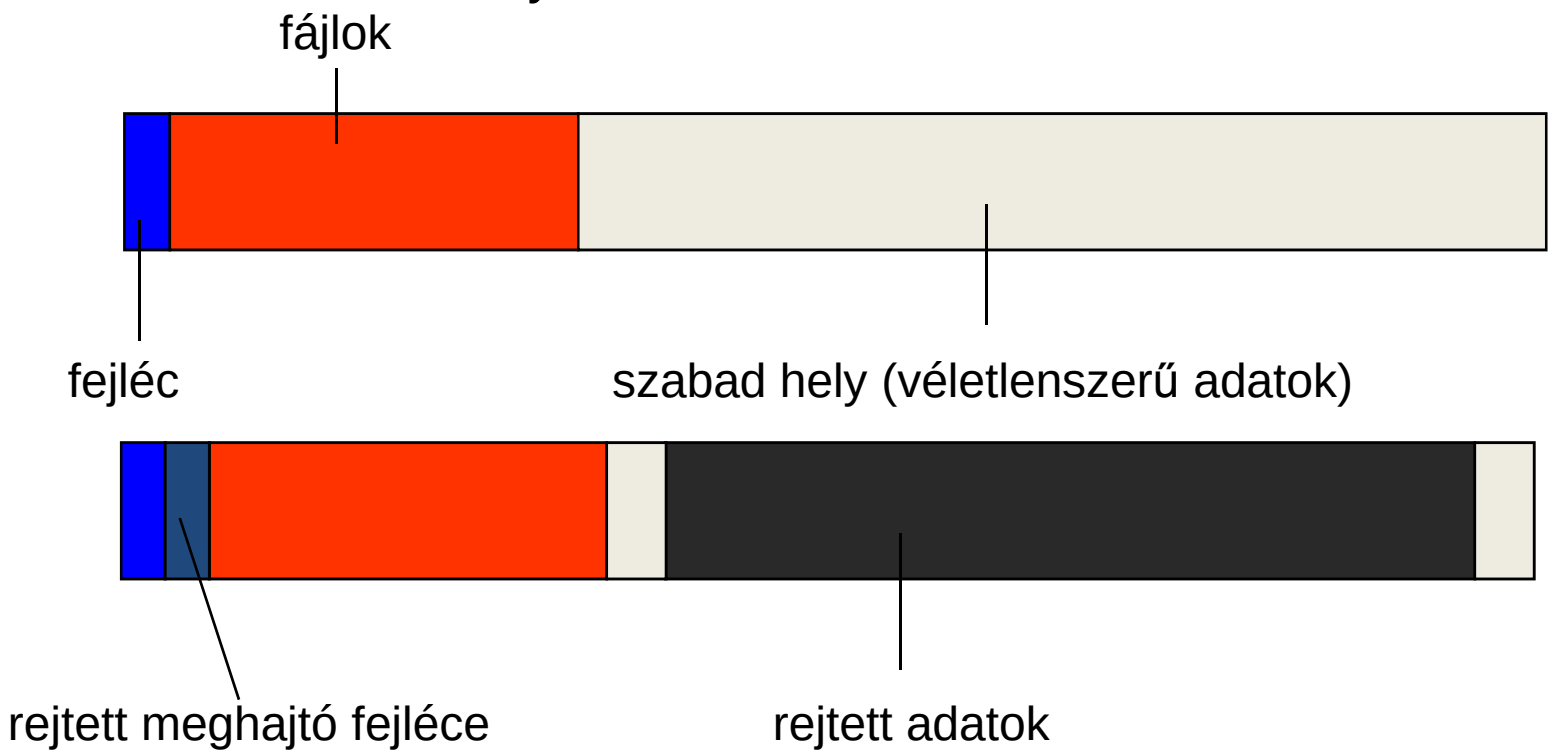
Adatrejtés hangfájlba

- LSB
  - úgy működik mint a képeknél
  - probléma: az emberi fül számára hallható lehet a bevitt zaj, különösen csendnél
- paritáskódolás
  - egy kulcs alapján LSB-csoportokat választunk, és ezek paritása adja a rejtett információt
  - előny a sima LSB-hez képest, hogy adaptívan billenthetjük át a megfelelő bitet
  - példaprogram: mp3Stego
- fáziskódolás
- visszhangkódolás



Adatrejtés titkos adatfolyamba

- A TrueCrypt módszere: hihető letagadhatóság
  - a titkosított információ statisztikailag véletlenszerűnek látszik
  - ötlet: a titkosított meghajtón véletlenszerű adatokkal töltjük ki a nem használt helyet

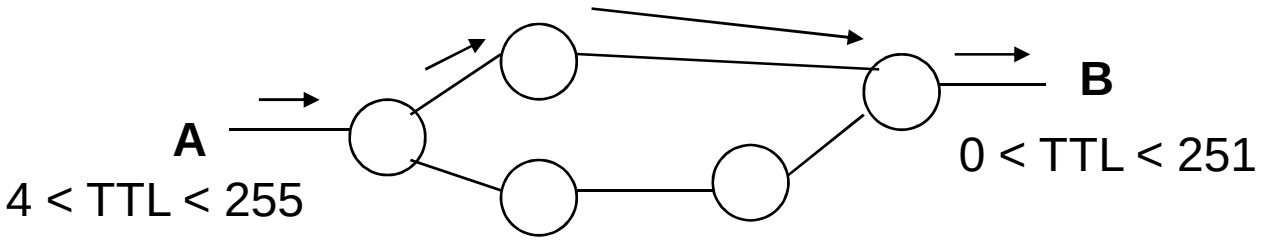


Adatrejtés binárisba

- Lehetséges futtatható programba adatot rejteni úgy, hogy a program funkcionalitása megmarad
- Megközelítés: egy feladat gyakran sokféleképpen elvégezhető
- Probléma: függés a processzorarchitektúrától
- Példaprogram: Hydan

Adatrejtés hálózati adatforgalomba

- Megközelítések
  - Hibásnak tűnő keretek injektálása WLAN-on
  - Játék az IP csomag TTL mezejével
  - HTTP üzenet manipuláció (ember észreveszi, tűzfal nem biztos)
- Példa: Loki



Tartalom

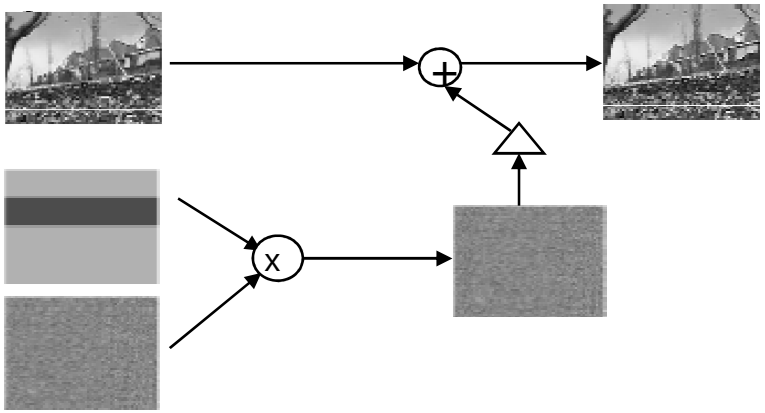
- Bevezető
  - Alapfogalmak, rövid történeti áttekintés
  - Kapcsolat a privátszférával
  - Problémák
- Adatrejtés hordozó médiumba
- Vízjelek
- Rejtett csatornák
- Szteganalízis

Vízjelezés

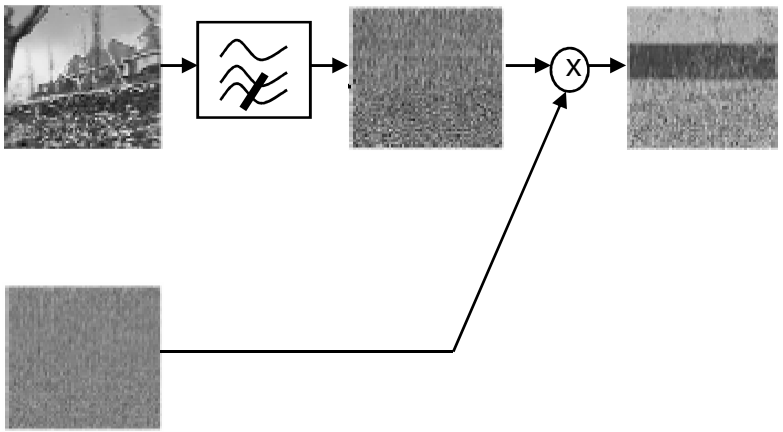
- Hordozó médium megjelölése
- Gyakori felhasználási terület: szellemi tulajdon védelme
- Kétféle vízjel
  - robusztus: BluRay lejátszó megvízjelezi a képet (ellen kell, hogy álljon sokféle átalakításnak)
  - törékeny: érvényességi „matrica” (BluRay, Loki, Hydan)
- PET-relevancia: pl. üzenet hitelesítése törékeny vízjellel

A szórt spektrum módszere

- elhelyezés
  - kiterjesztés
  - moduláció zajjal
  - eredmény összeadása az eredeti képpel



- visszaolvasás
  - felüláteresztő szűrés
  - demoduláció
  - „többségi szavazás”



A szórt spektrum módszere II.

- mindez csak az álvéletlen zaj ismeretében lehetséges
- lehetséges több vízjel elhelyezése
  - előny: nyilvános kulcsú vízjelek (speciális zajgenerátorokkal)
  - hátrány: romlik a képminőség

Vízjelek eltüntetése

- a robusztus vízjelek célja, hogy a vízjel csak a hordozó médium alapos minőségromlása árán legyen eltávolítható
- mikortól számít „jónak” egy robusztus vízjel?
- igény mutatkozott egy objektív ellenőrzőeszközre, így született a StirMark

StirMark

- nyílt forráskódú program
- célja a robusztus vízjelezési algoritmusok igazságos összehasonlítása, tesztelése
- teszttípusok: zajosítás, geometriai transzformációk, újrakódolás
- egyéb programok a szerzőtől: mp3Stego, mozaiktámadás

Tartalom

- Bevezető
  - Alapfogalmak, rövid történeti áttekintés
  - Kapcsolat a privátszférával
  - Problémák
- Adatrejtés hordozó médiumba
- Vízjelek
- Rejtett csatornák
- Szteganalízis

Rejtett csatornák

- Kapcsolat a kriptográfia és a szteganográfia közt
- Digitális aláírásokban illetve nyilvános kulcsokban lehetséges adatot szivárogtatni
  - egy speciálisan megszerkesztett DSA digitális aláírásban lehetséges információt szivárogtatni
  - RSA kulcsgenerálásnál lehetséges egy külön kulcspárral információt szivárogtatni

Rejtett csatornák II.

- Mindig jó nekünk a rejtett csatorna?
  - példa: speciálisan megszerkesztett RSA kulcsgeneráló implementáció kiszivárogtatja a kulcsot a tervezőnek
  - a szteganográfia ilyenkor pont a privátszféra védelmének rovására megy!
  - fekete dobozos implementációknál lehet ez probléma
- tanulság: bíznunk kell a titkosítónkban...

Tartalom

- Bevezető
  - Alapfogalmak, rövid történeti áttekintés
  - Kapcsolat a privátszférával
  - Problémák
- Adatrejtés hordozó médiumba
- Vízjelek
- Rejtett csatornák
- Szteganalízis

Szteganalízis

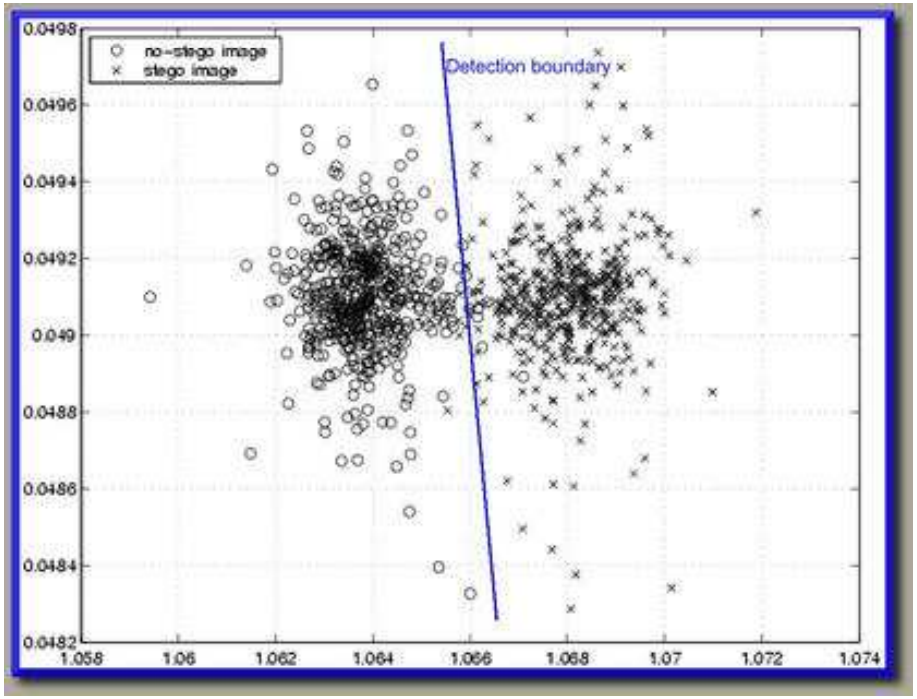
- technikák a szteganográfia alkalmazásának észrevételére
- általában az is elégséges, ha az információ jelenlétét kimutatjuk (ha „előássuk” a sztegomédiumból, az már csak hab a tortán)
- szteganalitikai programok bemutatása:
  - StegDetect
  - StegoSuite

StegDetect

- nyílt forráskódú szoftver
- felismert algoritmusok: JSteg, JPhide, OutGuess 1.3b, F5, AppendX, Camouflage
- heurisztikus keresés
- parancssoros felület (van hozzá GUI)

StegDetect heurisztika

- „nincs benne szteganográfia” és „van benne szteganográfia” adatbázisok vezetése
- az ezekben tárolt képek jellemzőiből egy ismeretlen szteganográfiai módszert is sikerrel azonosíthat



StegoSuite

- fizetős szoftver (~1500$)
- kétféle hordozó kezelése (kép, hang)
- szótáras támadás a sztegokulcsra
- next-next-finish jellegű felület

Konklúziók

- Szteganográfia = magasabb szintű titkosság mint a puszta kriptográfia
- Sok PET-szempontból releváns alkalmazás
  - de nem minden program biztonságos (Camouflage)
  - van, hogy a szteganográfia a privátszféra ellen dolgozik (rejtett csatorna)
- szteganográfia és szteganalízis ugyanolyan jellegű versenyfutása mint a kriptográfia és a kriptanalízis esetében