Adatrejtés / Adatrejtés szövegben

BME - TMIT

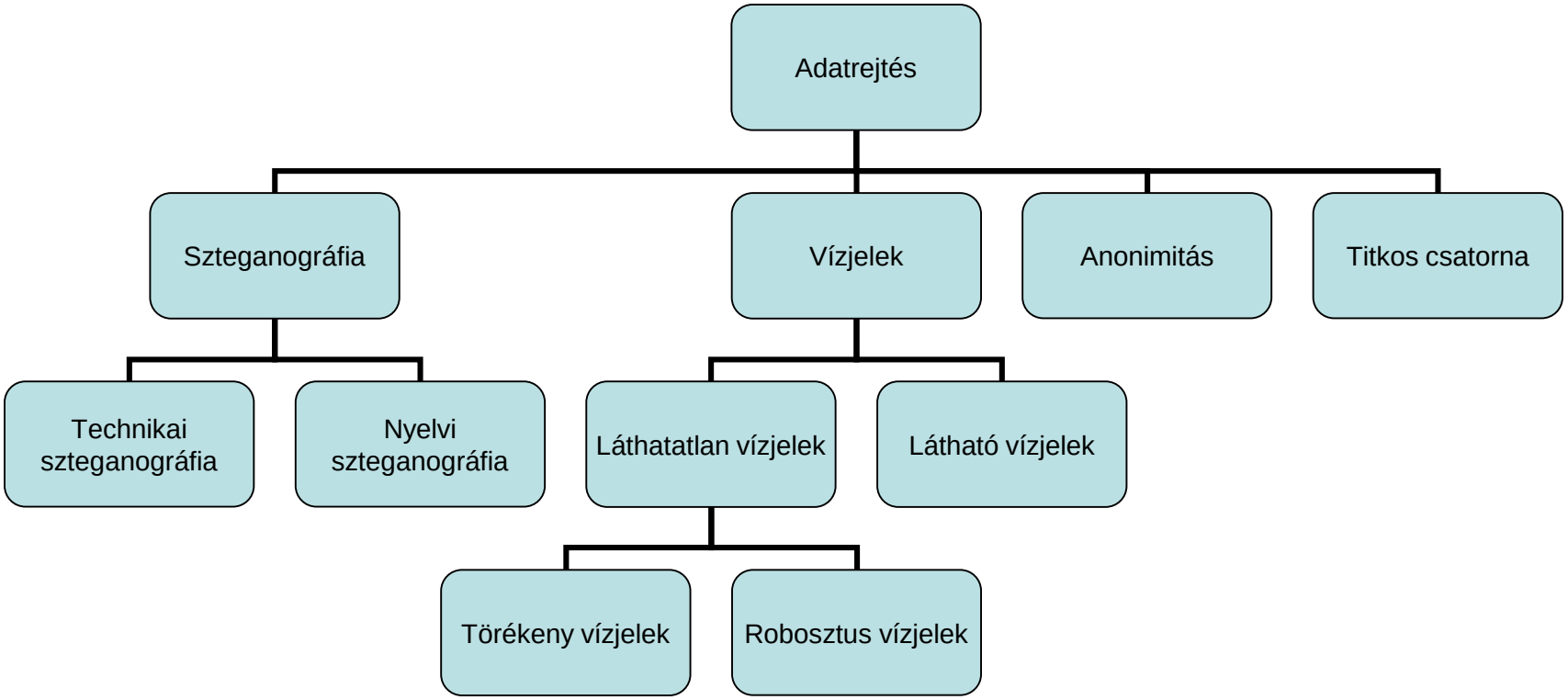
VITMA378 - Médiabiztonság

feher.gabor@tmit.bme.hu

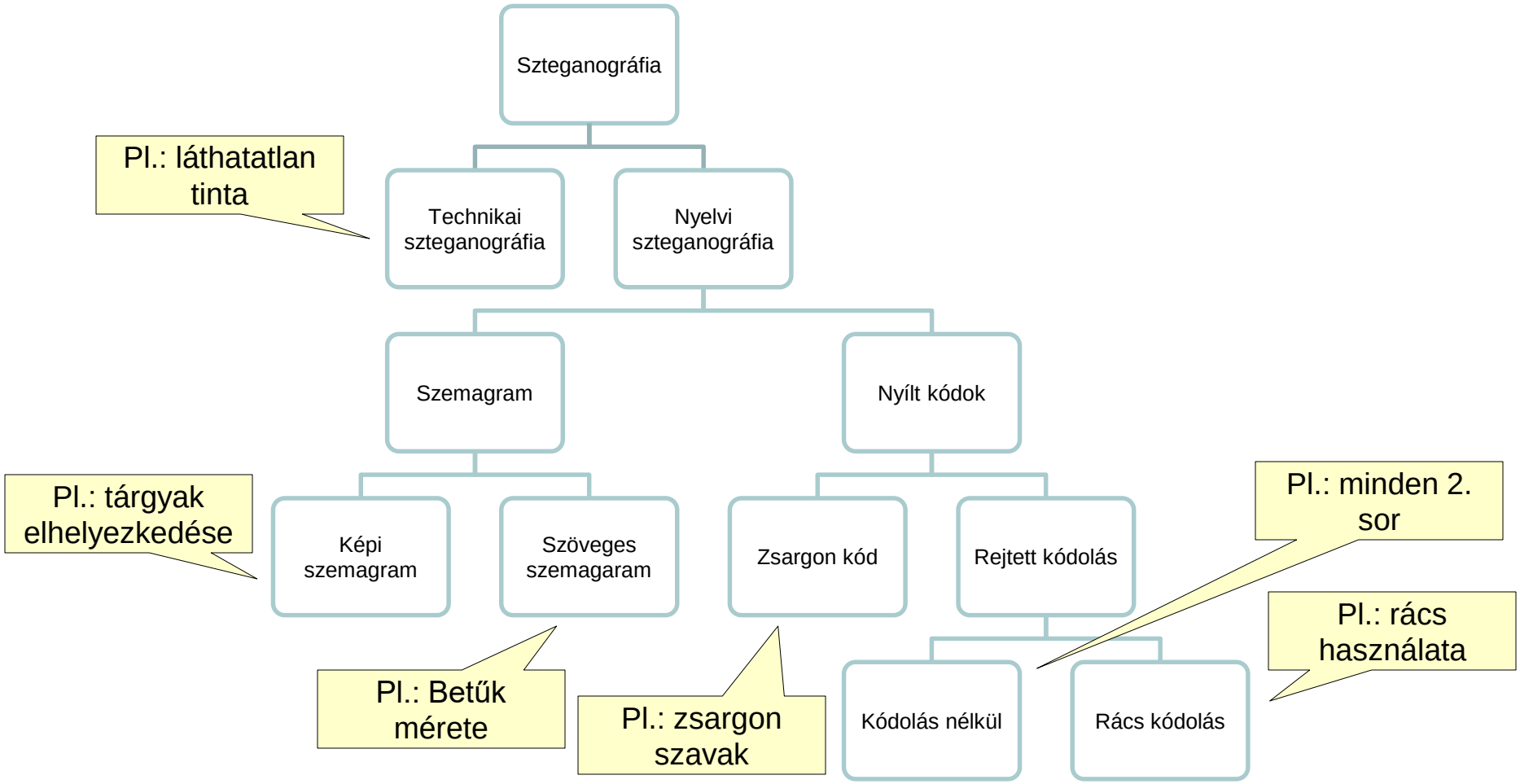
Adatrejtés régen

- Legelső írásos emlékek
  - Herodotus feljegyzései alapján (~400 BC)
    - Demeratus: Agyag táblák alá rejtett írás, értesítés a Perzsa támadásról
    - Histiaeus: leborotvált fejű szolga
  - Pliny the Elder, Láthatatlan tinta (thithymallus növény teje) az ókori római birodalomból, írás a sorok között
  - *India: Titkos kommunikáció (Kama sutra)* ~ 400 AD
  - *Ősi Kínában: selyemre írt üzenet viasz labdába gyúrva. A labda elrejtése a hírnökben…*
- Johannes Trithemius
  - Steganographia könyv (1499)

Adatrejtés típusai



Szteganográfia

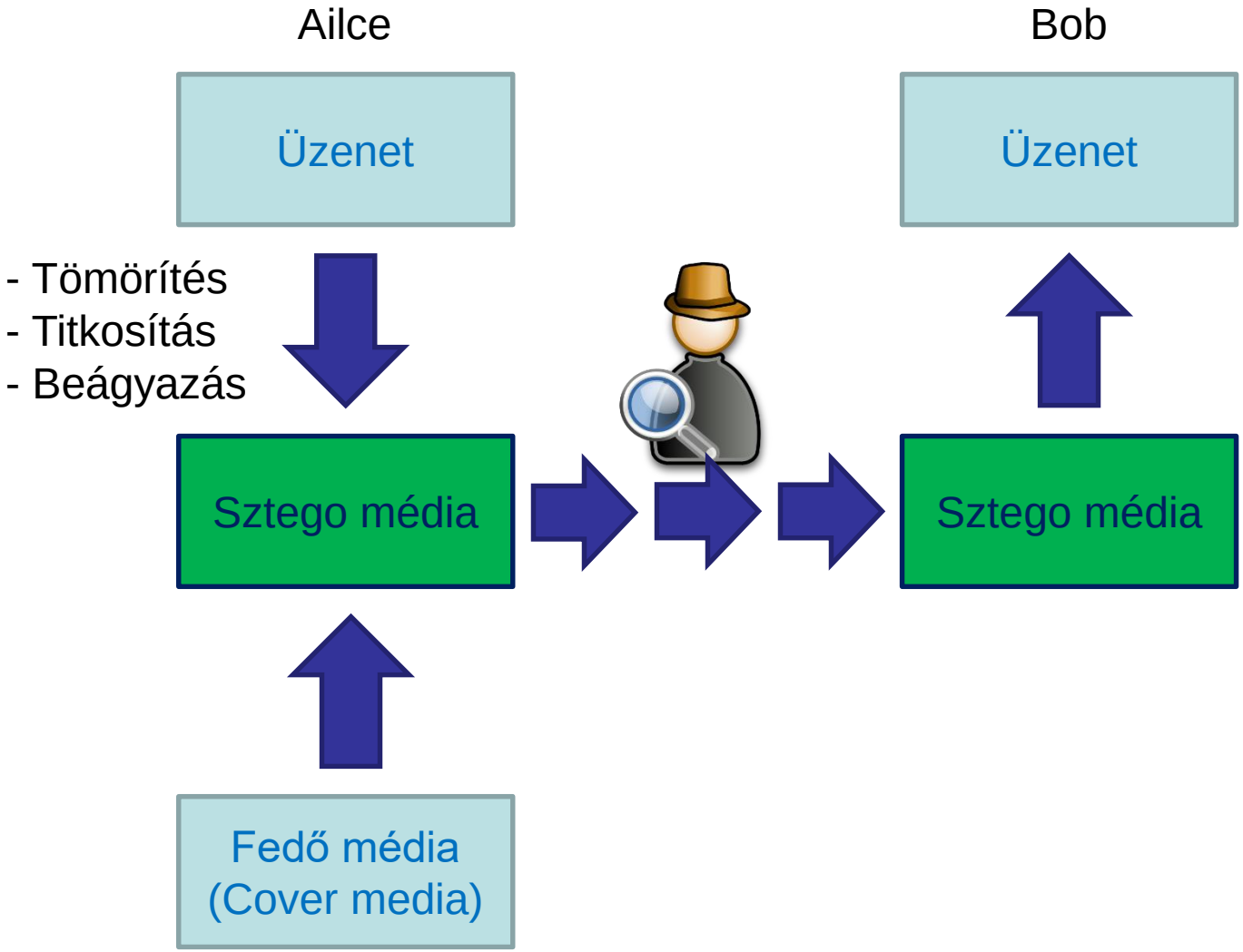


Adatrejtés fogalmak

- Fogalmak
  - Cover media: a rejtéshez használt média
  - Stego key: a rejtett adatok elhelyezése
  - Stego media: a rejtett adatot tartalmazó média

- Adatrejtés feloldásánál
  - Non-blind: Szükséges az eredeti média is
  - Blind (vak): Nem kell az eredeti média
  - Semi-blind: Nem kell az eredeti média, de kell valami más információ

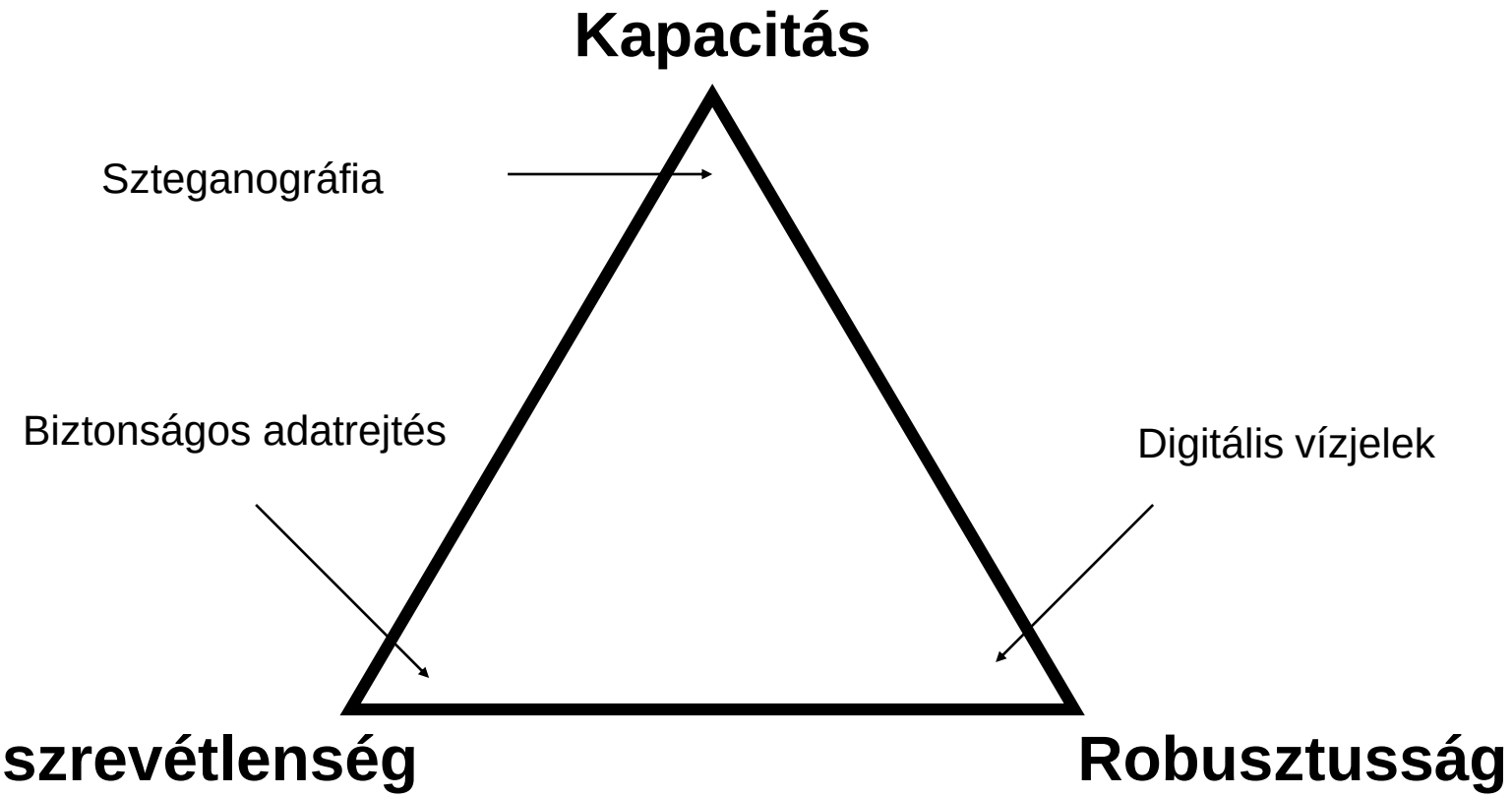
Adatrejtés és biztonság



Modern médiák adatrejtéshez

	A média mérete
• Szöveg – Levelezés, web oldalak	~ 1-2 Kbyte
• Kép – Elterjedt formátumok	~ 100KB, 1-5 MB
• Hang – CD lemezek, MP3 fájlok	~ 3-4 MB / 60-70 MB 128 – 1400 Kbps
• Videó – DVD, digitális műsorszórás	~2-5 GB 1-2-4-8 Mbps
• De lehet akár .pdf, .exe, …	

Kényszer háromszög



További tényező: **Komplexitás**

Adatrejtés szöveges anyagokban

Modern technikai szteganográfia

- Mikrofilm
- „Sárga pöttyök” – Színes lézer nyomtatók azonosítása

Mikrofilm

- John Benjamin Dancer (A mikrofilm atyja)
  - 1839: Az első kísérletek szövegek lekicsinyítésére
  - 1853: Az első eladott mikrofilmek, amit mikroszkóp segítségével lehet nézni
- Rene Dagron
  - 1859: Az első szabadalom a mikrofilmre
  - 1870-71: Frank-porosz háborúban mikrofilmes galambposta

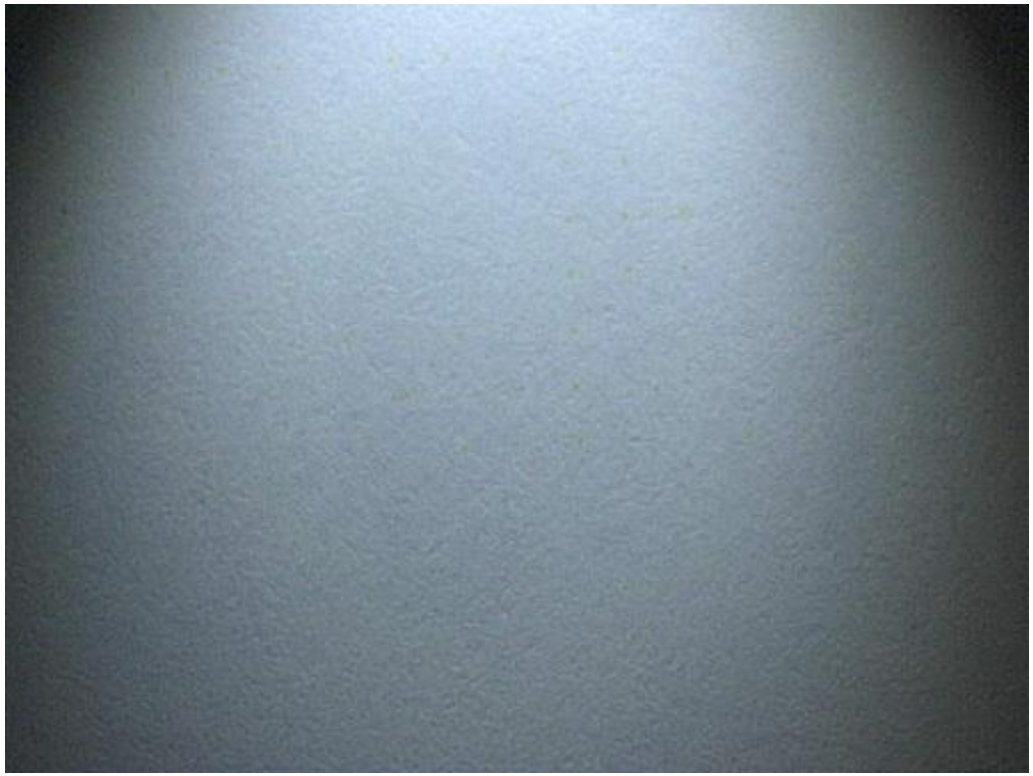
- II. világháború:
  - Kémkedés
  - Levelezés (V-mail)
  - Archiválás

Mikrofilm

- Üzenetrejtés - mikrofilm

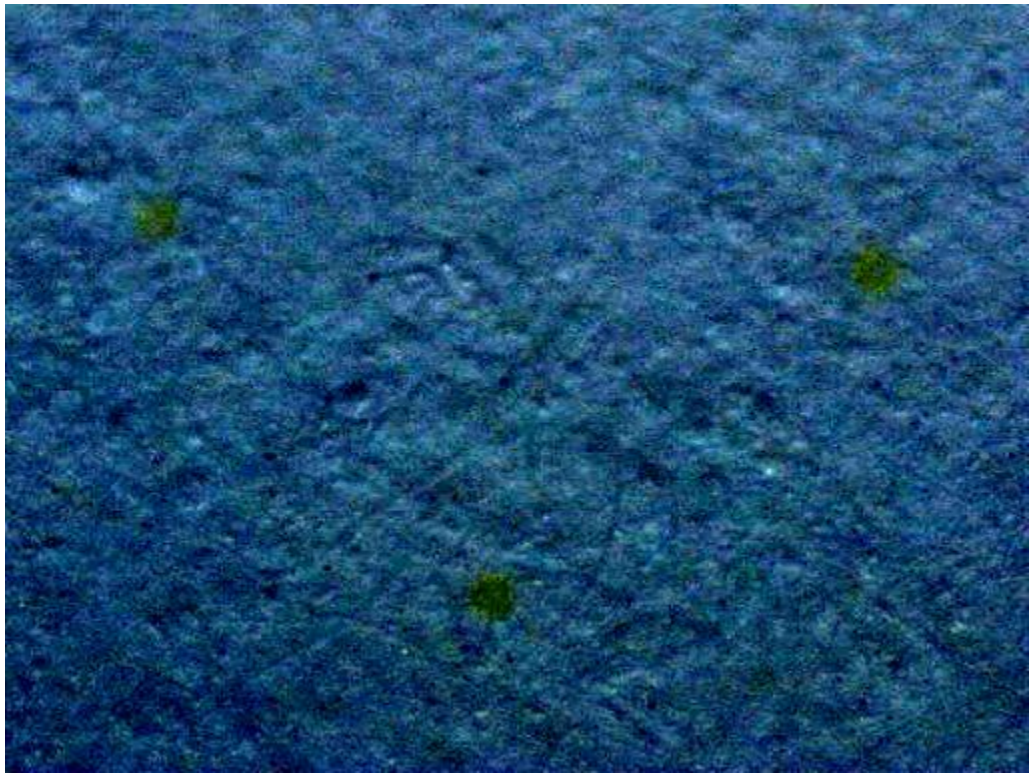
Xerox DocuColor 12

- Nyomtatott kép, 10x nagyítás:



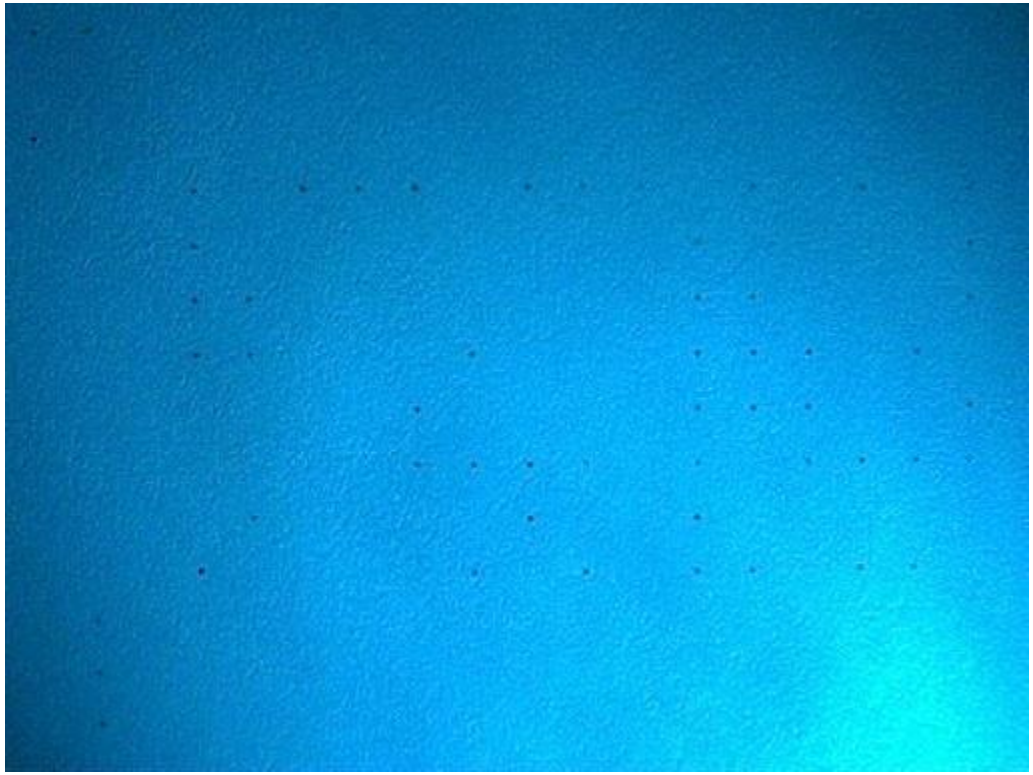
Xerox DocuColor 12

- Nyomtatott kép, 60x nagyítás + kontraszt:



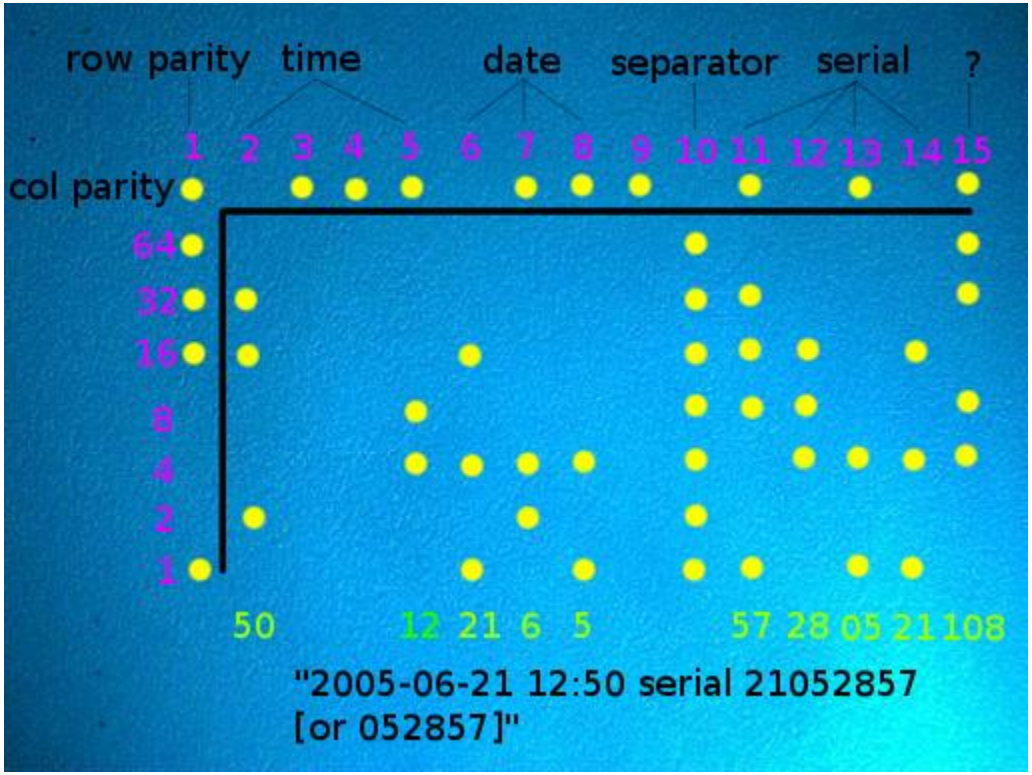
Xerox DocuColor 12

- Nyomtatott kép, 10x nagyítás, kék LED megvilágítás:



Xerox DocuColor 12

- Dekódolás:



Szöveges szemagram

Nyelvi szteganográfia

- Betű-, szó és soreltolás
  - A betűk/szavak/sorok el vannak tolva egymáshoz képest
  - Nyomtatásban is jól használható (digitálisan nehezebb)
- A karakterkészlet változtatásai
  - Rejtett szöveg

Nyílt kódok

Nyelvi szteganográfia

- Üres jelek bevitele
  - Szóköz: Sor végére, mondatok közé
  - Pl.: 1 szóköz: 0 / 2 szóköz: 1

- Karakter helyettesítése
  - Szóköz és 00h
  - CR és LF

Szintaktikus módszer

Nyílt kódok

- Szintaktikus módszer
  - Pl.: vesszők használata:
    apple, pear, and peach
    apple, pear and peach

Szemantikus módszer

Nyílt kódok

- Szemantikus módszer
  - Alma = 0, körte = 1, barack = 3, …
  - Nyelvtani szabályok (mondatszerkezet)

- Betűk elrejtése szavakban
  - Sablon használata
  - Minden kezdőbetű, minden 2. betű

Adatrejtés példa

- I. világháború
  - PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.
  - PERSHING SAILS FROM N.Y. JUNE 1