Arcfelismerés adatvédelmi kérdései

BME-s hallgatóként készített diplomatervem bemutatója

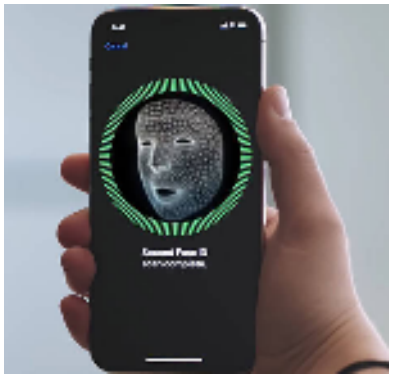
Előadó: Csarnó Tamás
Témavezető: Dr. Gulyás Gábor György

Modern arcfelismerő rendszerek

Gépi tanuláson alapszik

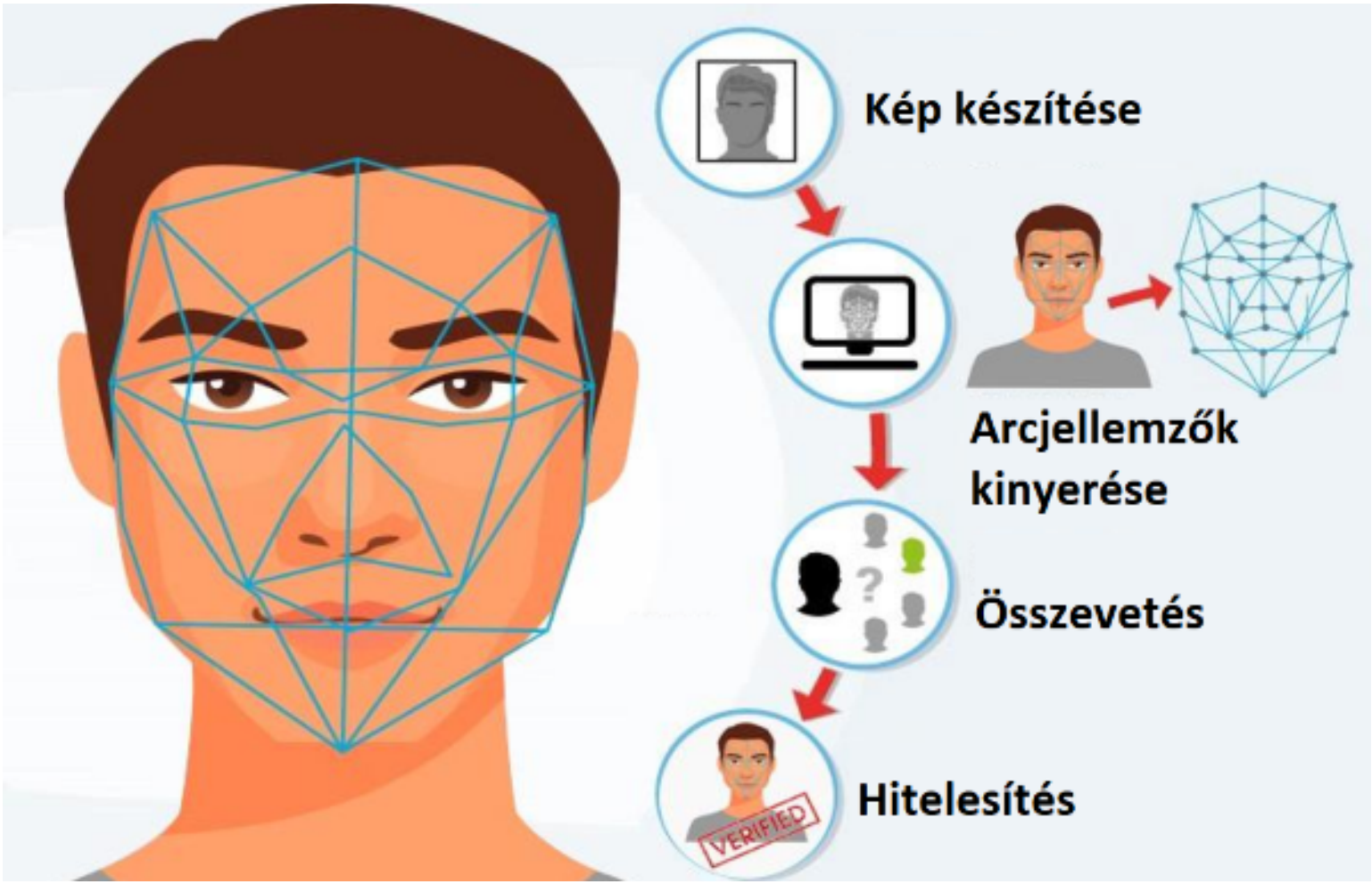
Alkalmazási példák

- Állami szektorban
  - Bűnözők megállítása
- Vállalati szektorban
  - Telefon feloldás
  - Beléptető rendszer



Kép forrás: https://tinyurl.com/49mb3y47

Mesterséges intelligencia alkalmazása



Kép forrás: https://tinyurl.com/jw8hxd44

Problémafelvetés

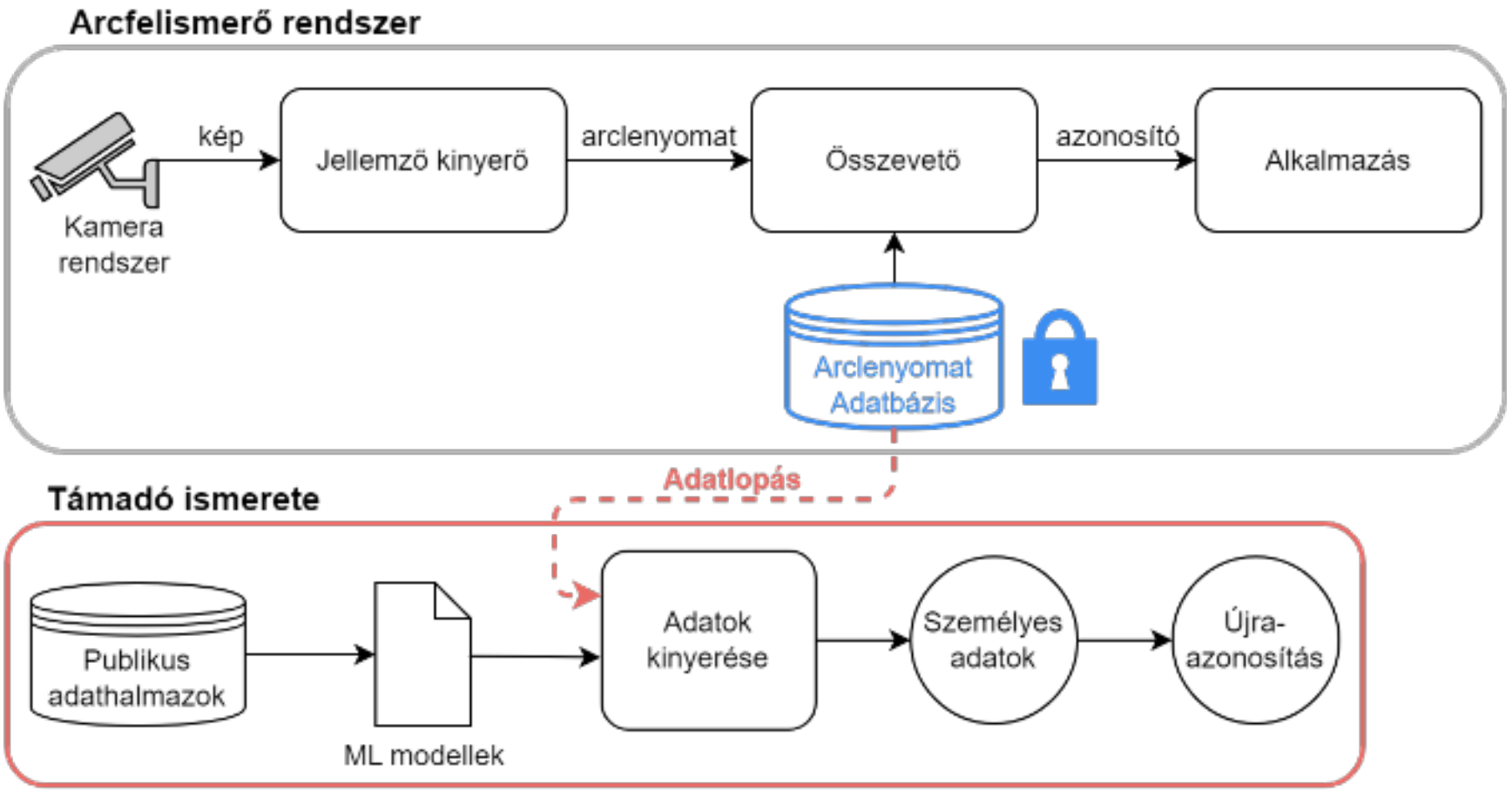
- Hipotézisem: Az arclenyomatok tárolása adatvédelmi kockázattal járnak[1].
- Arclenyomatok magukban kódolnak érzékeny információkat.

$$f\left(\text{  }\right) = \begin{pmatrix} 0.112 \\ 0.067 \\ 0.091 \\ 0.129 \\ 0.002 \\ 0.012 \\ 0.175 \\ \vdots \\ 0.023 \end{pmatrix} \begin{matrix} \\ \longrightarrow \text{Férfi} \\ \\ \\ \longrightarrow \text{20-30 év} \\ \\ \\ \longrightarrow \text{Fehér bőrszín} \\ \\ \end{matrix}$$

[1] Fábián, István, and Gábor György Gulyás. "De-anonymizing facial recognition embeddings." *Infocommunications Journal* 12.2 (2020): 50-56.

Kép forrás: https://tinyurl.com/2ydrt856

Támadó modellezése



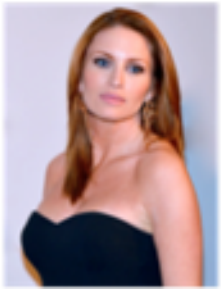
Mérés és eredmények

- Képek gyűjtése publikus adathalmazokból
- Arclenyomatok kinyerése képekből
- Neurális hálók pontossága
  - Nem: 98.8%
  - Bőrszín: 97.7%
  - Életkor: 76.9%

IMDb



Wikipedia

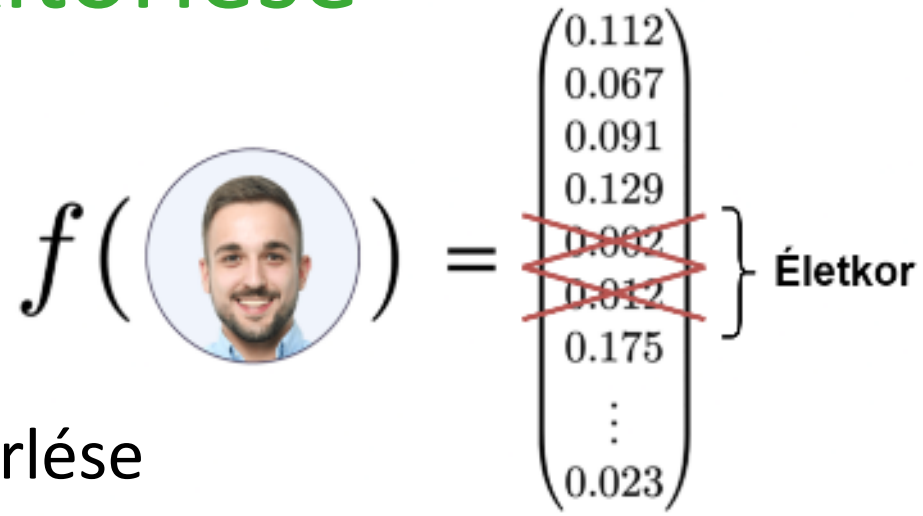


Arclenyomatok védelme

- Zaj hozzáadása az arclenyomathoz
  - El lehet fedni hozzáadott zajjal az érzékeny információkat?
- Adatok törlése az arclenyomatból
  - Meg lehet mondani, hogy az arclenyomat melyik része tárolja az érzékeny információkat?
- Kriptográfiai módszerek alkalmazása
  - Homomorfikus titkosítás
  - Lokalitás érzékeny hash

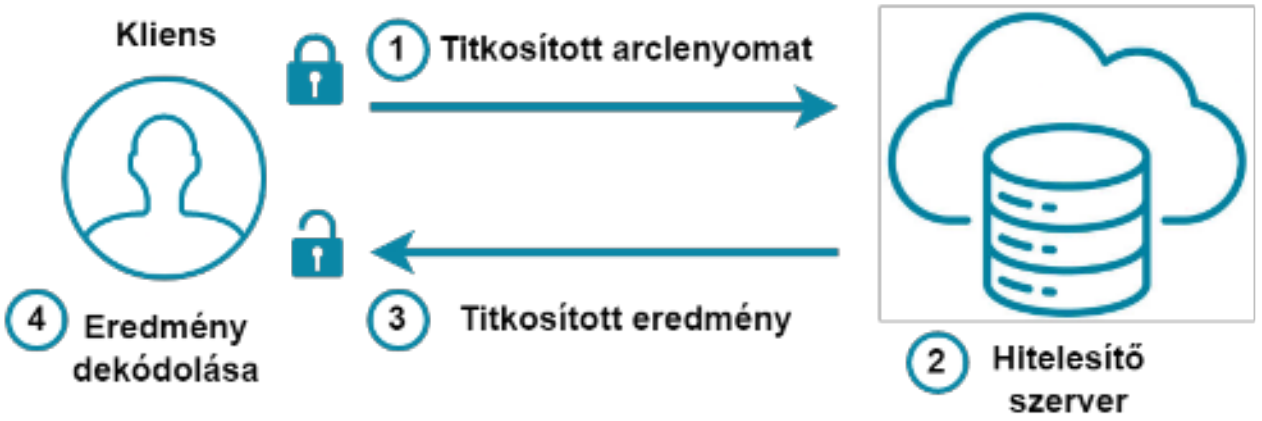
Érzékeny adatok kitörlése

- Érzékeny információk lokalizálása.
- A legfontosabb értékek törlése
- Meglepő módon törlés után is ki lehetett következtetni az érzékeny adatokat
- Az arclenyomat jellemzői kölcsönösen összefüggenek
- Redundancia



Homomorfikus titkosítás

- Az arclenyomatok titkosított formában vannak tárolva.
- Lehetővé teszi titkosított adaton matematikai műveletek végzését.
- Pl. E(1) + E(2) = E(1+2)



Köszönöm a figyelmet!

Csarnó Tamás

Szoftverfejlesztő - Vitarex Stúdió Kft.

tamas.csarno@gmail.com

+36 30 310 6311

 linkedin.com/in/tamascsarno