



Valós idejű deepfake felismerés

Dr. Forstner Bertalan

Villamosmérnöki és Informatikai Kar

Automatizálási és Alkalmazott Informatikai Tanszék



BME

A deepfake tartalmak veszélyei

- **Probléma:**

- a **deepfake** tartalmak előállítása ma már nyilvánosan elérhető eszközökkel, alacsony informatikai előképzettséggel megvalósítható
- Hitelesség rombolása, politikai manipuláció, zsarolás, személyes visszaélés
- A módszerek hónapról-hónapra változnak

- **Cél:** valós idejű multimodális (hang, kép/videó, szöveg) deepfake-detektálás és védekezési keretrendszer.

Pénzügyi kár

- **Átlagosan 450 000 USD veszteség** egy deepfake vagy AI-alapú csalás miatt [Regula: *Deepfake Trends 2024 december*)]
 - Megkérdezett cégek 92 %-a tapasztalt valamilyen pénzügyi veszteséget deepfake-kapcsolt csalás miatt.
- A pénzügyi szektorban az átlag $\approx$ **603 000 USD** [Business Wire]
- A generatív-AI és deepfake csalások globális kára
 - 2023-ban már $\approx$ **12,3 milliárd**
 - a trend alapján 2027-re $\approx$ **40 milliárd USD**

Esettanulmány: Sir Winston Churchill

Eredeti videó kicserélt hangsávval, szájra illesztve



Filmjelenet kicserélt arccal és hangsávval, szájra illesztve



Elért eredmények

- Támadási módszerek, adatbázisok feltárása (30+ hangadatbázis; nagy video/kép halmazok).
- Audio detektorok első verziói (CNN/RNN; ASVspoof-2019 LA): ~90% körüli belső pontosság.
- Kép/video detektálás: 99%+ belső mérések; kereszt-adatbázisos validáció folyamatban. (Emberi felismerés: 63%)
- Generátorokkal kísérletek: Wav2Lip, FOMM, SadTalker; Churchill-demo elkészült.
- Kodek- és tömörítés-hatás elemzése; nyers audiós modellek (RawNet2, ResNet1D).
- HPC-n futó tanítások/tesztek; CARIN-integráció előkészítése.

Megvalósíthatóság és üzleti terv

- **Konzorcium:** BME (AUT Tanszék) + TC&C Kft; integráció a CARIN hívásrögzítő ökoszisztémába.
- **Fókusz:** detektálás, DF-CAPTCHA, watermark-vizsgálat
- A fejlesztés újdonságértékének nemzetközi elismeréseként a TC&C 2025-ben elnyerte a Frost & Sullivan rangos Global New Product Innovation Recognition díját

Ipari (és egyéb) alkalmazások

- Call center és ügyfélszolgálat védelme (voice spoofing, account take-over).
- Belső vállalati kommunikáció védelme (vezetői megszemélyesítés, hamis bejelentések).
- Pénzügyi szektor: tranzakciók, jóváhagyások hitelesítése; compliance és audit.
- Kormányzati/szolgáltatói szektor: megbízható digitális csatornák, reputációvédelem.
- Oktatás és tudatosság: demonstrátorok, támadási forgatókönyvek és ellenlépések.

Csapatunk

*Audio és video deepfake támadási és -védekezési módszerek
naprakész követése*

- 4+ főállású tanszéki munkatárs

Szakmai vezető: Dr. Kővári Bence, kovari.bence@vik.bme.hu

- 5+ doktorandusz
- Tehetséges hallgatóink



KÖSZÖNÖM A FIGYELMET !



BME