

AI SUMMIT

Mesterséges Intelligencia
kutatások a Műegyetemen-
„lineárisból az
exponenciálisba”

Levendovszky János

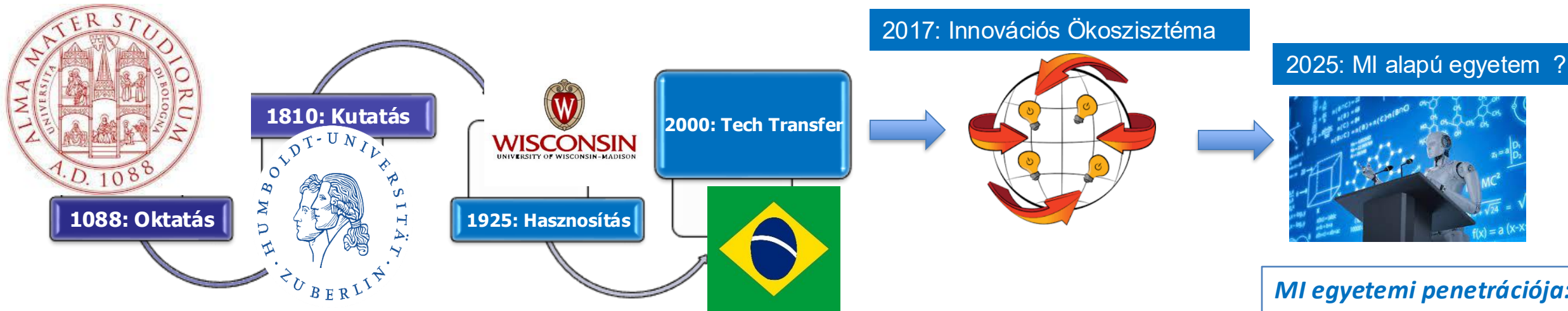


M Ű E G Y E T E M 1 7 8 2



Intézményi kihívás

Egyetemi evolúció = TUDÁS (tudásátadás - tudásvagyon felhalmozás - tudástranszfer)



Disruptív technológiák: „age of exponential”

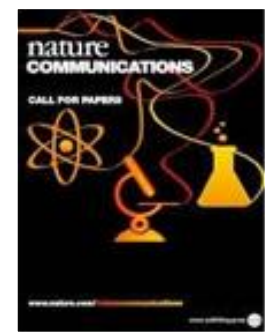
Lineáris változások

MI egyetemi penetrációja:

- Oktatás
- Nemzetközileg élvonalbeli K+F+I
- Ipari hasznosulás
- Etikai megfontolások
- Governance

Alkalmazkodás a diszruptív változásokhoz

„Adaptív” tudományos kiválóság





European Research Council
Established by the European Commission

6 professzor



EUR 76,24 million



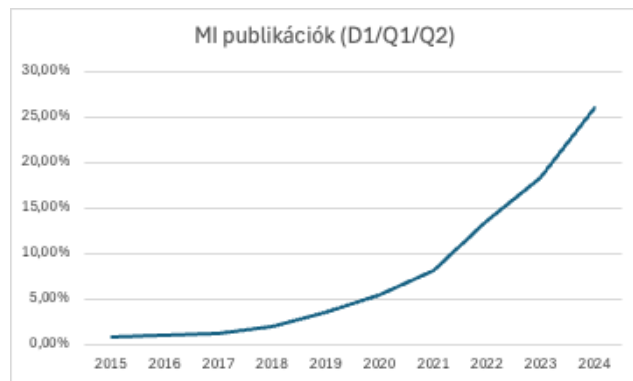
- 119 MTA doktora,
- 56 MTA rendes tag
- 7 kar MTA kiváló kutatóhely
- 47 Bólyai Ösztöndíj

HUN-REN 11 csoport
Hungarian Research Network

Lendület program 12 csoport



Innovációs teljesítmény és vállalati beágyazódás (2000+ vállalat)



Széleskörű egyetemi kompetenciák

<https://competence.bme.hu/>

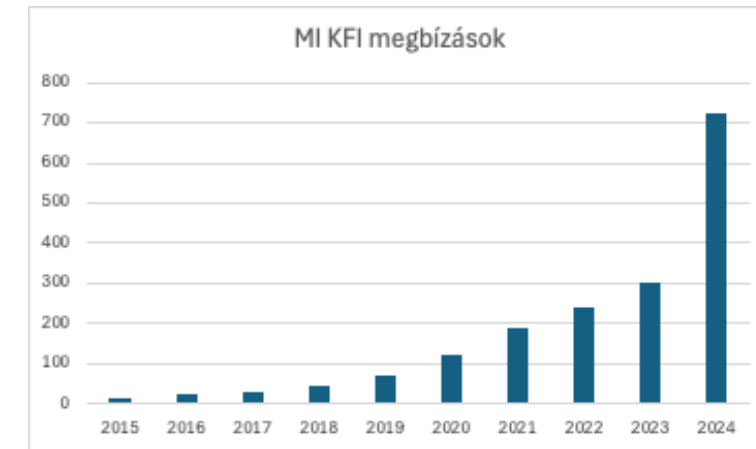


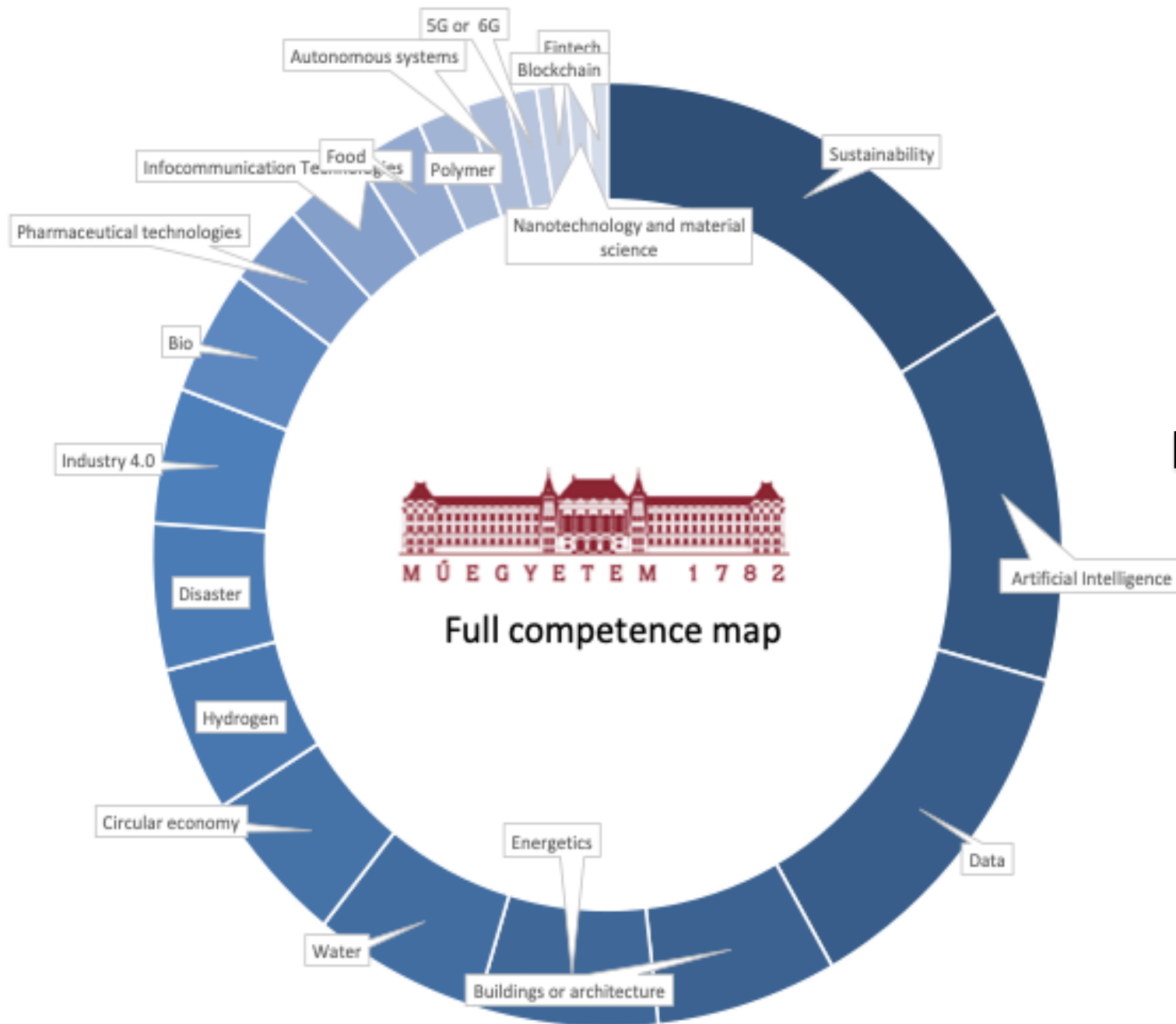


147 research groups



419 researcher profiles





Maximális társadalmi hatás !



DEEPTech INNOVÁCIÓ

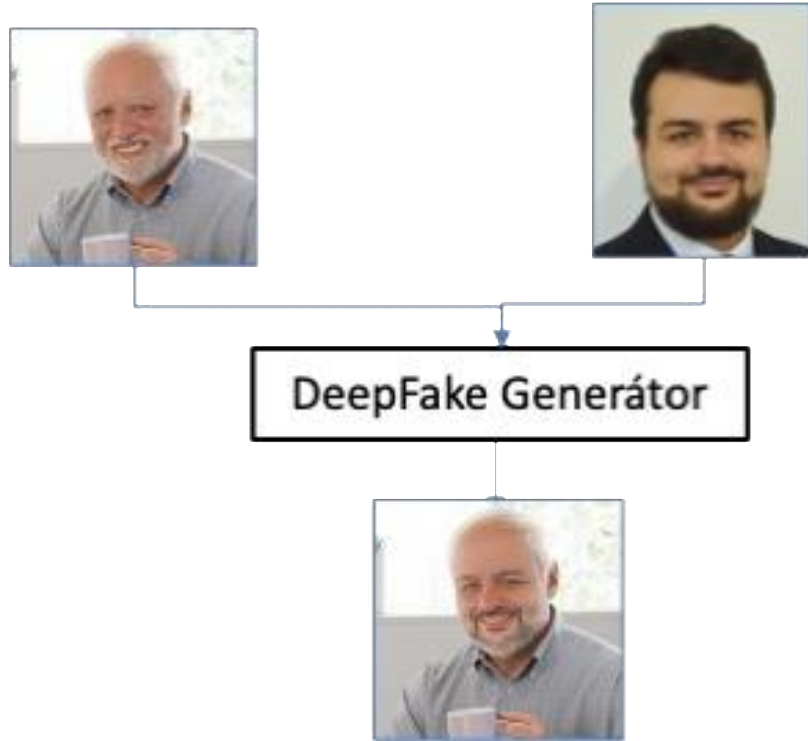
Tudomány + Innováció + Impakt

Az egyik legnagyobb MI fenyegetettség - deepfake

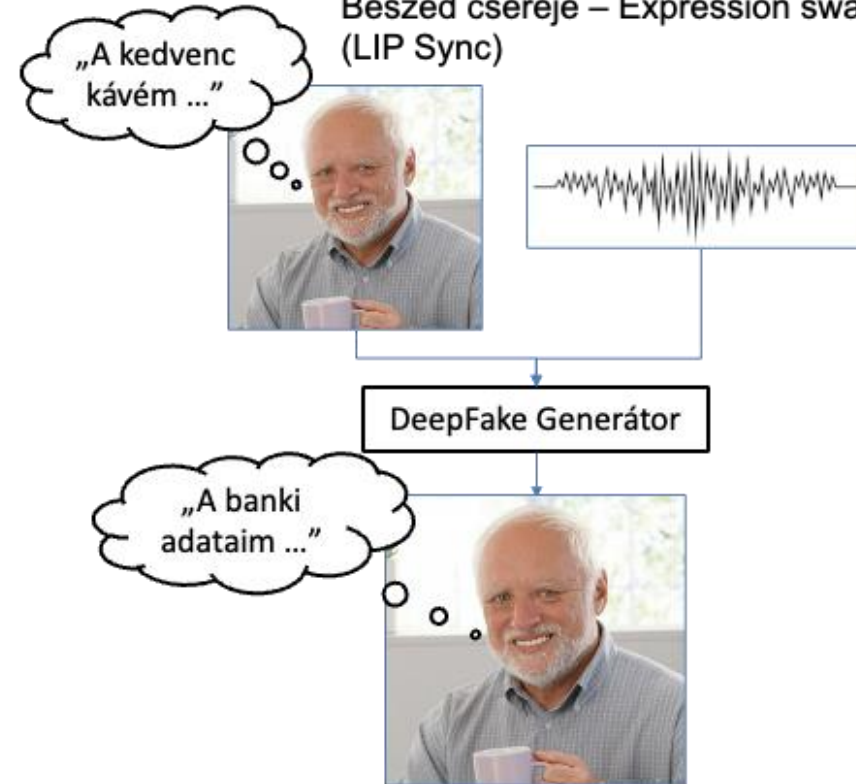


Deepfake módok és veszélyek

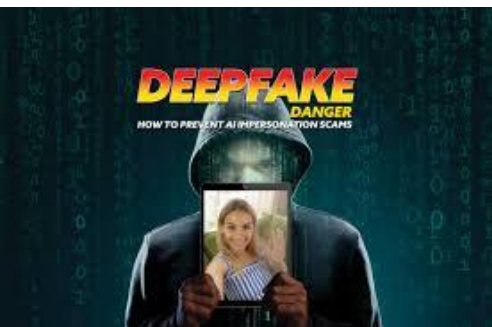
Arcok cseréje - Identity (Face) Swap



Beszéd cseréje – Expression swap (LIP Sync)



7



- Gazdasági, társadalmi és nemzetbiztonsági kockázat
- Óriási pénzügyi veszteségek
- Információk jogosulatlan megszerzése
- Politikai manipuláció (lejárattás)

FBI előrejelzés: 2030-ra 25-40 milliárd USD kárt okoz

<https://regulaforensics.com/news/deepfake-fraud-costs/>

Hatékony deepfake detekció

- Alapvető gazdasági és társadalmi érdek
- Lehetőleg on-line történjen
- Multimodalitás (kép, hang)
- Integrálható legyen hívásrendszerekbe



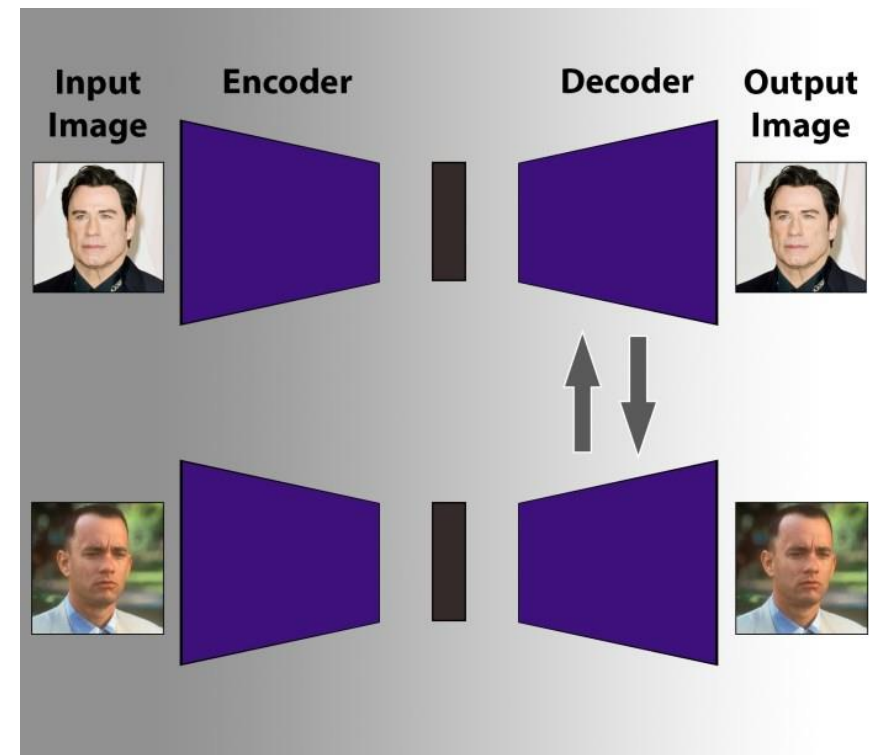
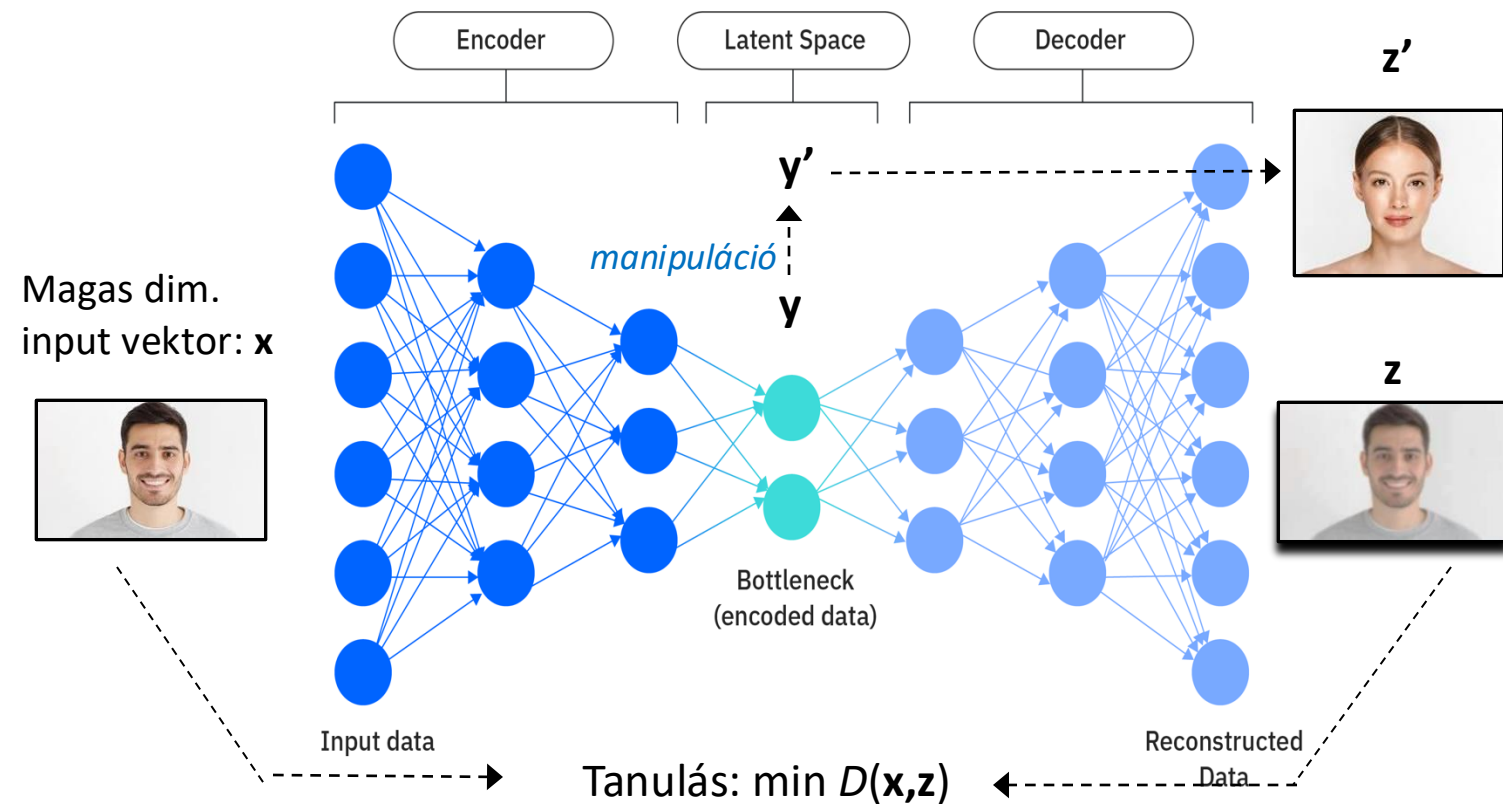
BME és TC&C



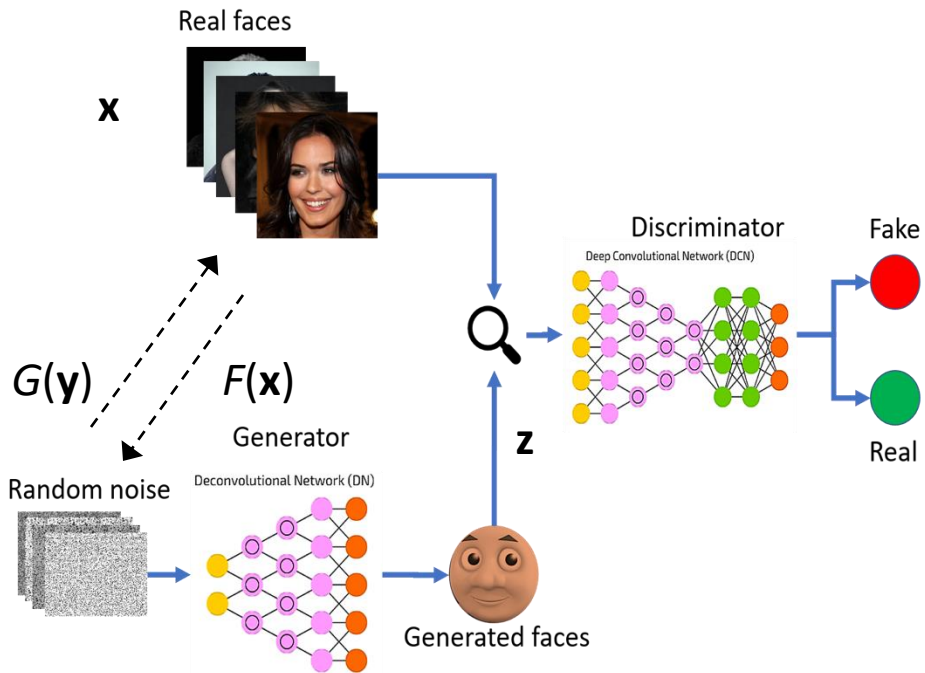
- Valós idejű multimodális (hang, kép/videó, szöveg) deepfake-detektálás és védekezési keretrendszer.
- Integráció a CARIN hívásrögzítő ökoszisztémába

Deepfake és a látens tér

Variational Autoencoder



Generative Adversarial Network (GAN)



$$E_x [\log(D(x))] + E_z [\log(1 - D(G(z)))]$$

Generator: maximalizál Discriminator: minimalizál

A dszikriminátor megtévesztése

Deepfake felismerése

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log(1 - D(G(z^{(i)})))$$

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m [\log D(x^{(i)}) + \log(1 - D(G(z^{(i)})))]$$

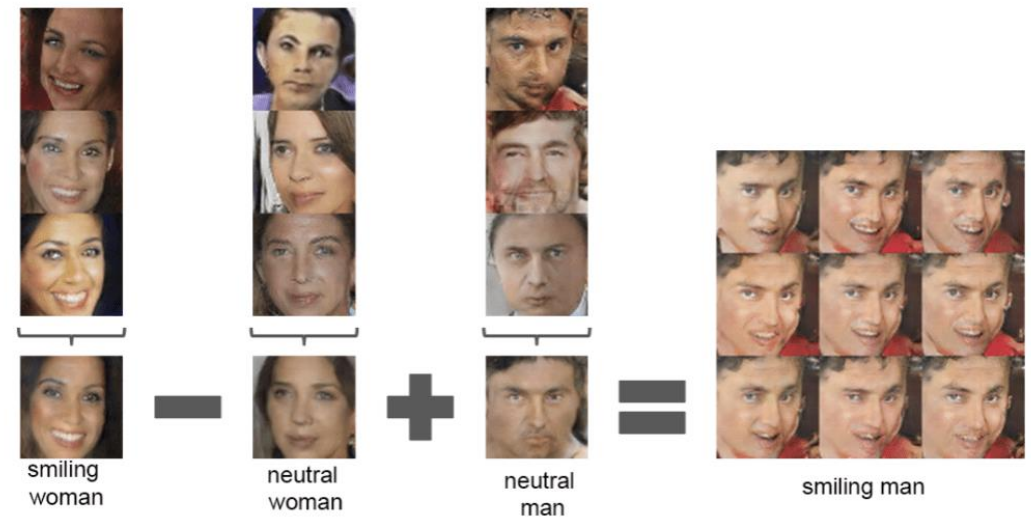
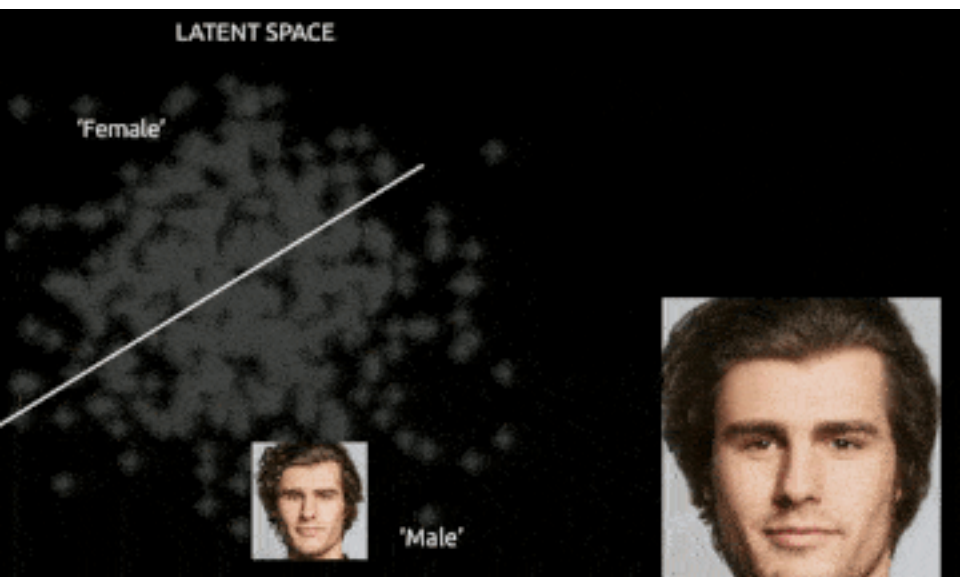
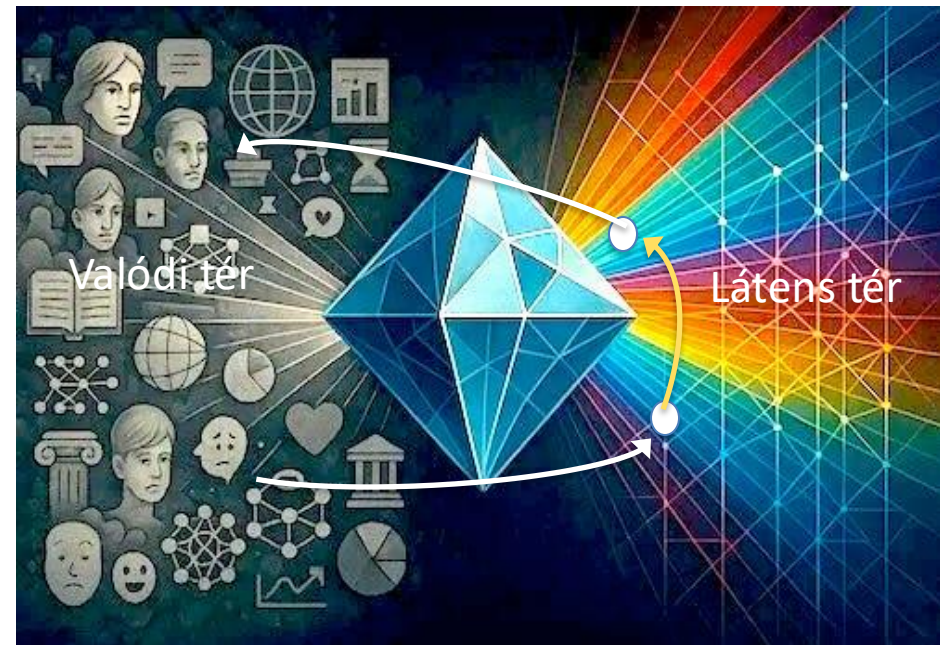
Tanulás után

Deep fake generálása

Deep fake felismerése



Manipuláció és útvonalak a „látens térben”



Denoising Diffusion Probabilistic Model (DDPM)

„Zajos” Markov lánc

$$\mathbf{x}_t = \sqrt{\bar{\alpha}_t} \mathbf{x}_0 + \sqrt{1 - \bar{\alpha}_t} \boldsymbol{\epsilon}, \quad \boldsymbol{\epsilon} \sim \mathcal{N}(0, \mathbf{I}),$$

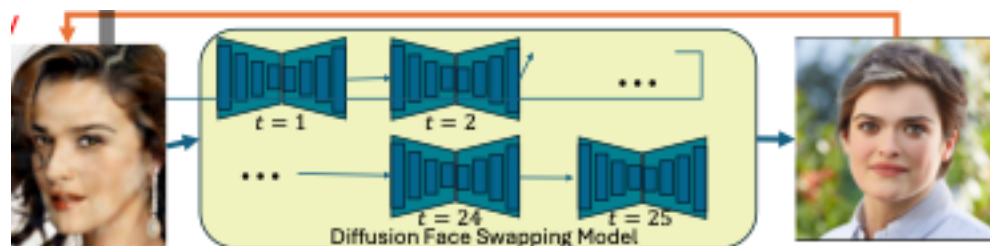
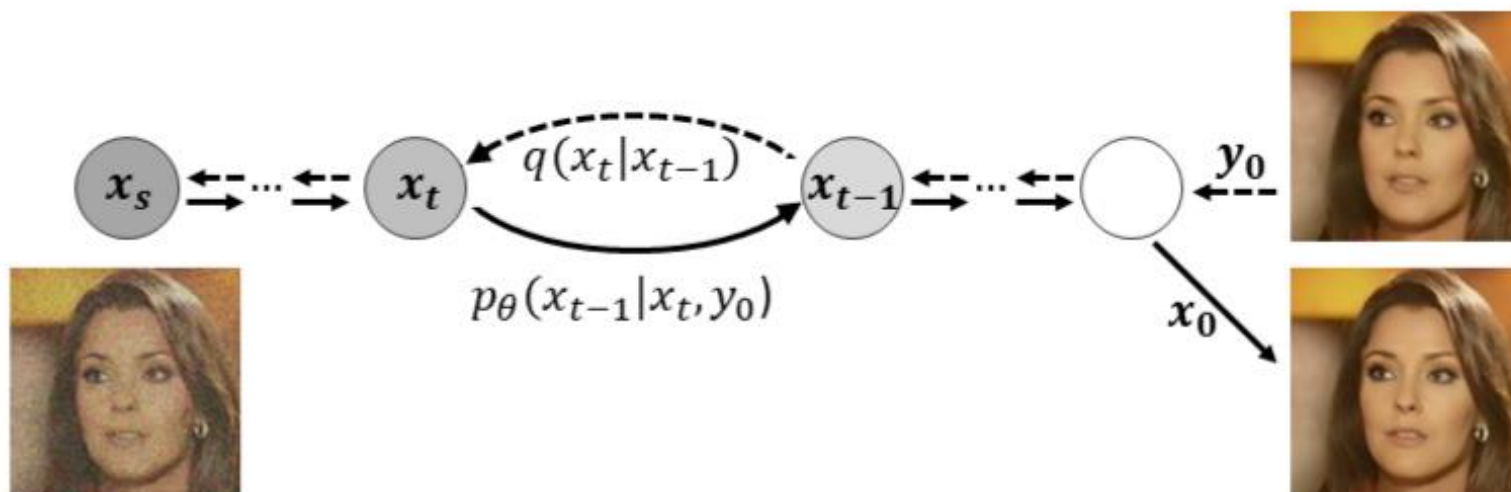
Modell paraméter optimalizálás

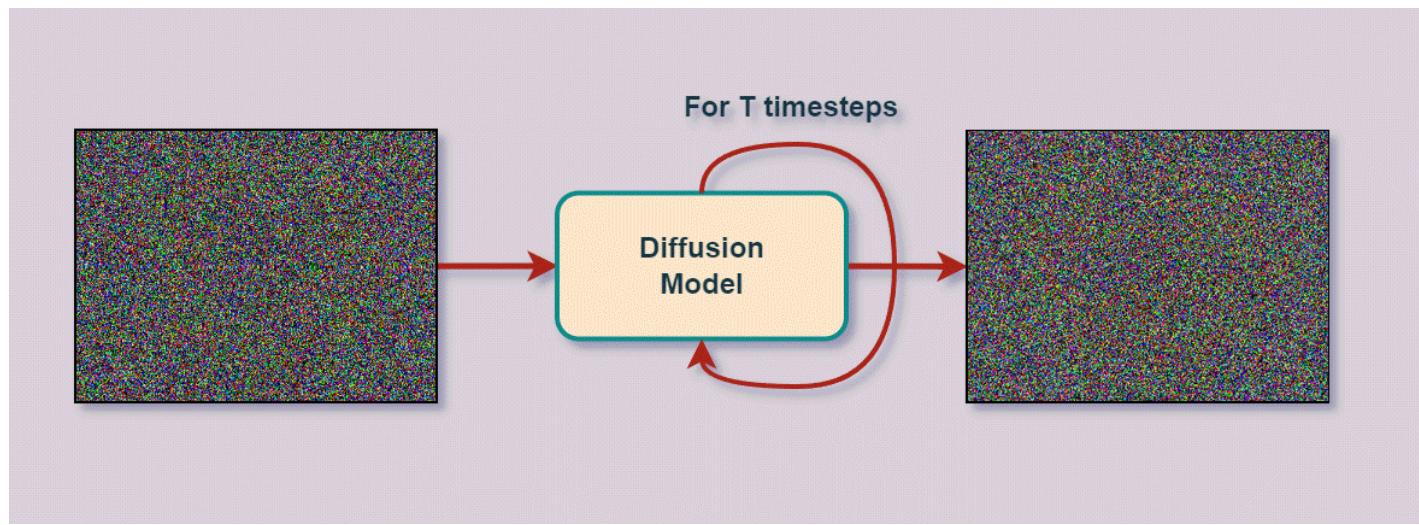
$$\boldsymbol{\theta}^* = \arg \min_{\boldsymbol{\theta}} \mathbb{E}_{\mathbf{x}_0, t, \boldsymbol{\epsilon}} [\|\boldsymbol{\epsilon} - \boldsymbol{\epsilon}_{\boldsymbol{\theta}}(\mathbf{x}_t, t)\|_2^2]$$

„Zajtalanítás”

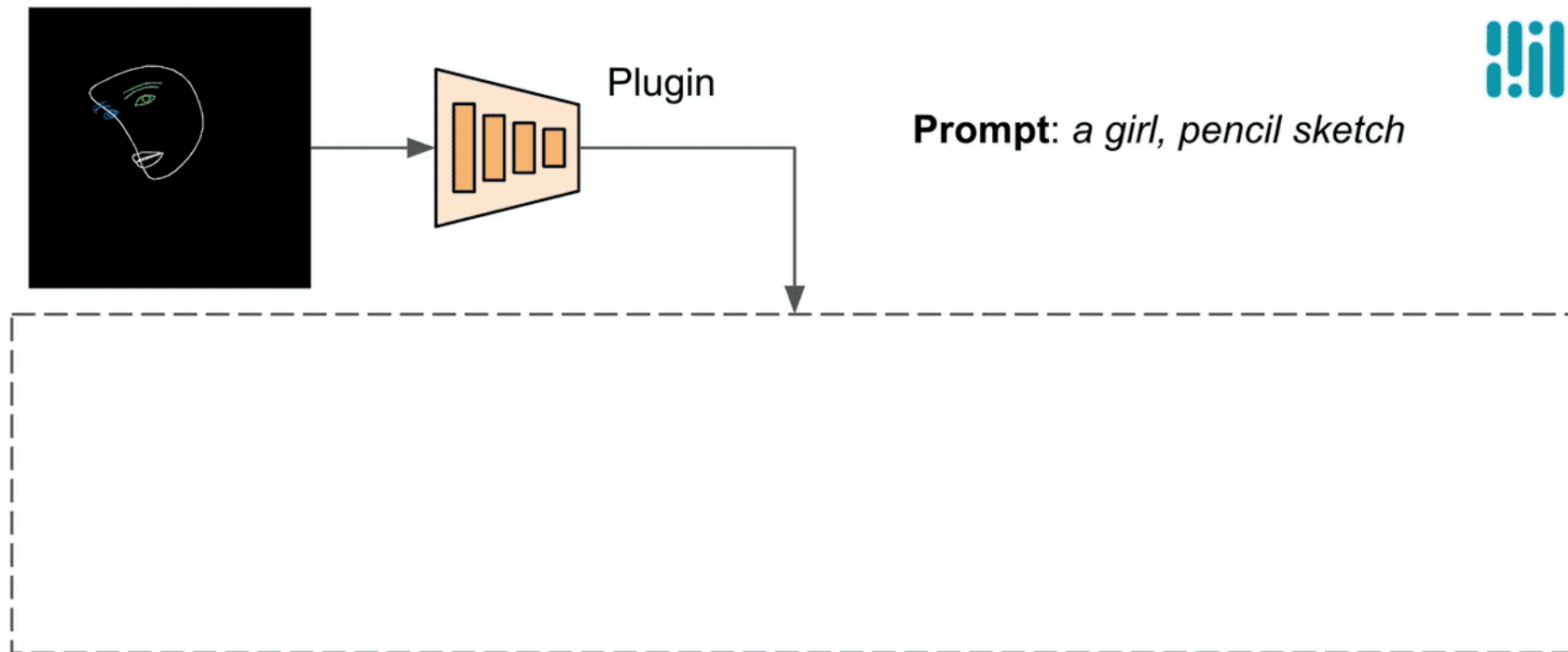
$$\hat{\mathbf{x}}_{t-1} = \frac{1}{\sqrt{\alpha_t}} \left(\mathbf{x}_t - \frac{\beta_t}{\sqrt{1 - \bar{\alpha}_t}} \boldsymbol{\epsilon}_{\boldsymbol{\theta}^*}(\mathbf{x}_t, t) \right) + \sqrt{\beta_t} \boldsymbol{\epsilon},$$

Eredeti kép: $\mathbf{x}_0$ $\longrightarrow$ Manipulált kép: $\mathbf{x}_{\infty}$

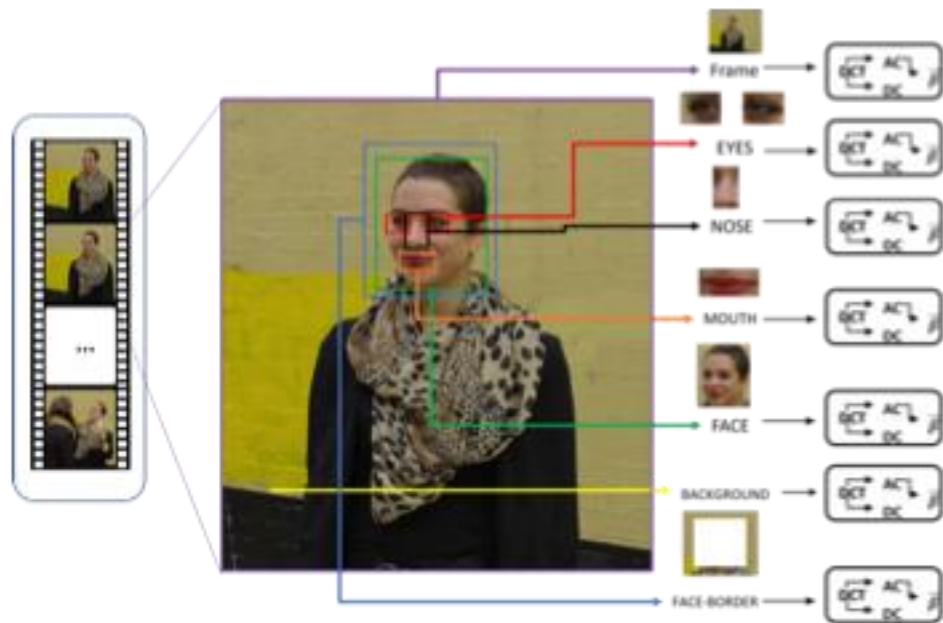




Reverse diffusion



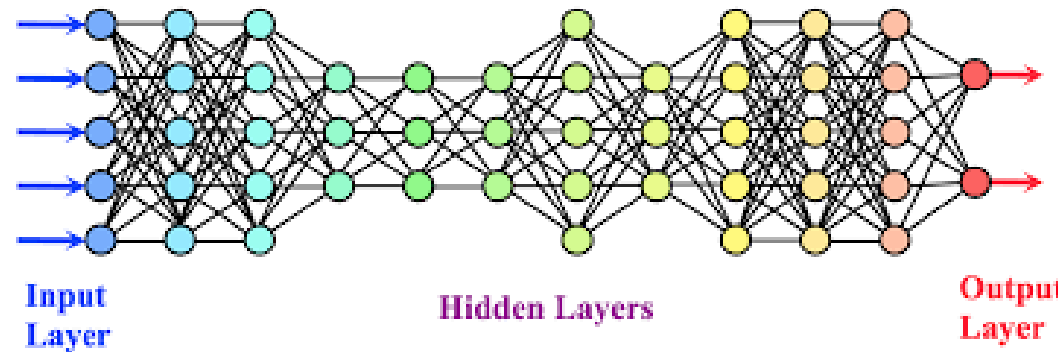
Deepfake detekció



DCT based *Luca Guarnera et al*

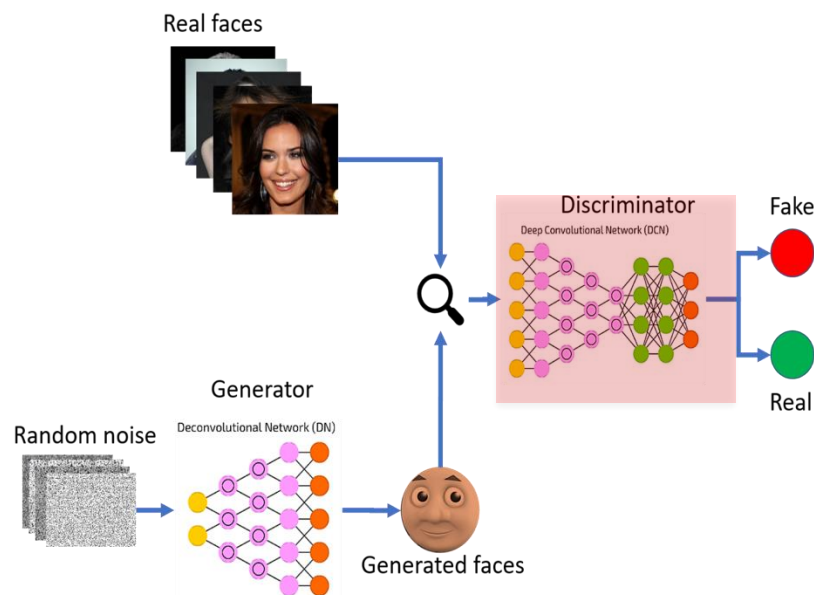
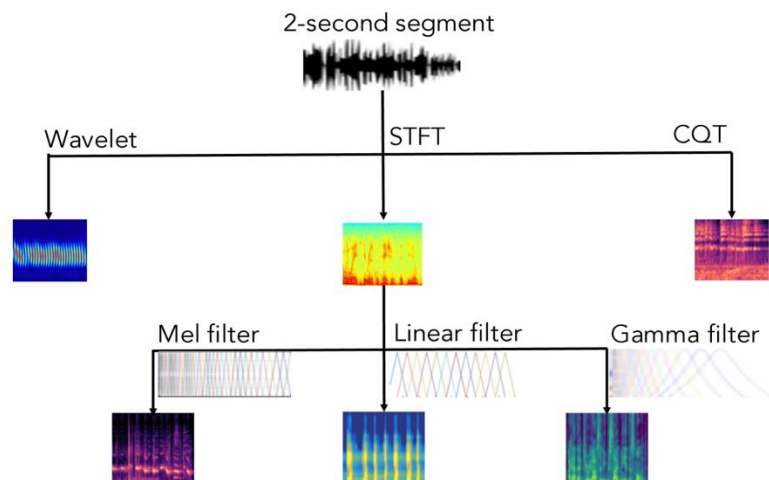
Vizsgált metrikák

- Fréchet Inception Distance (FID)
- Structured Similarity (SSIM)
- Learned Perceptual Image Patch Similarity (LPIPS)



Diszkontinuitás
és diszturbancia
jelzése,
statistikai
elemzés

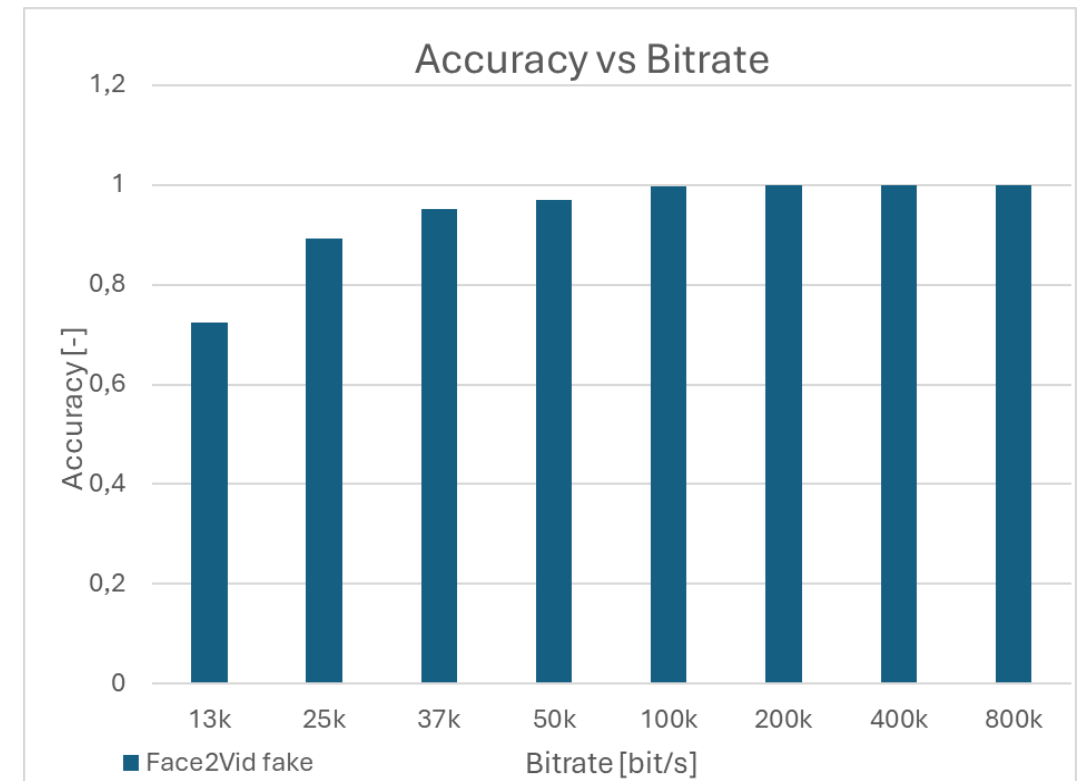
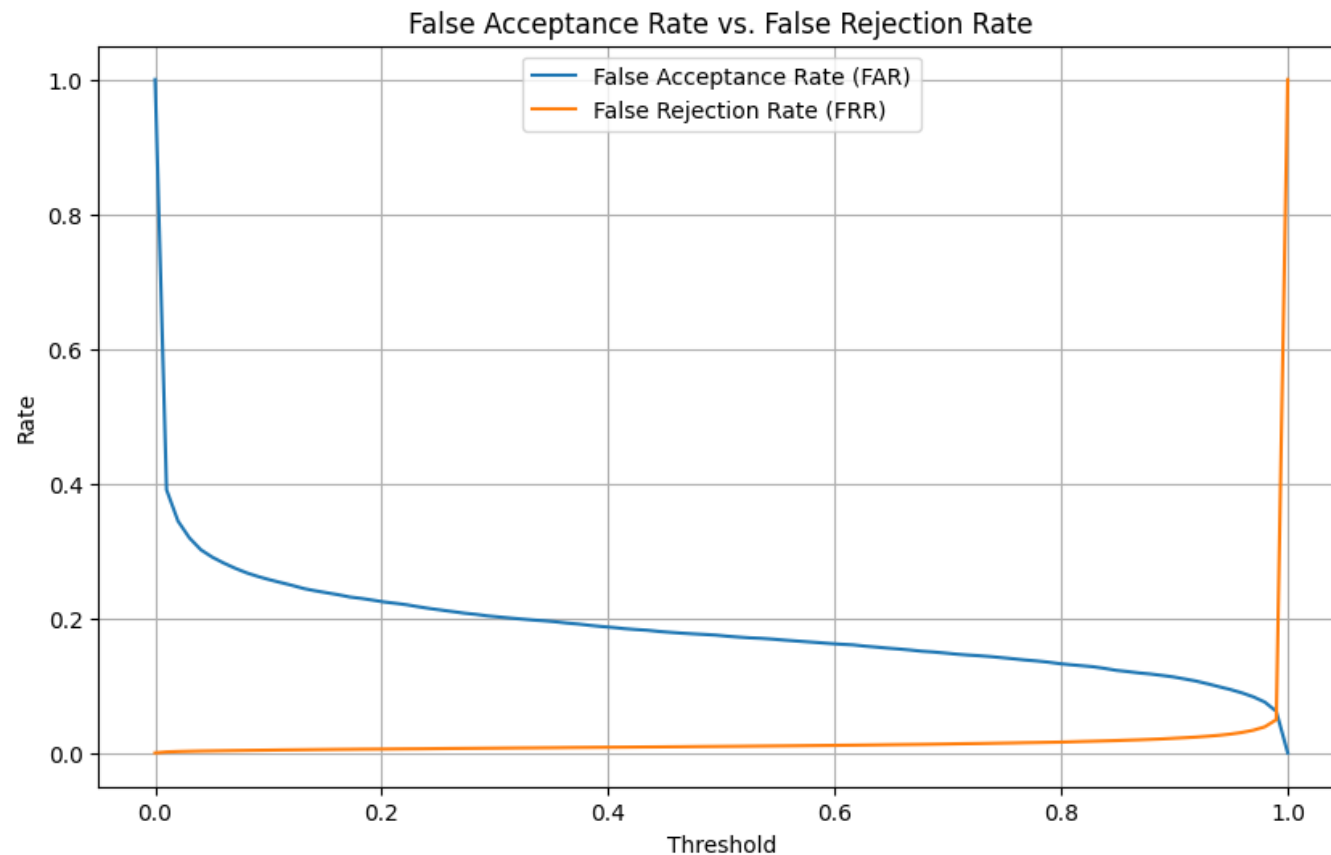
Audio: Feature Extraction-alapú modellek



BME- TC&C megoldás és teljesítőkéesség

ConvNeXt:

- A ConvNeXt modellek képesek versenyezni a legfejlettebb Transformer alapú modellekkel, például a Swin Transformer-rel. A ConvNeXt eléri a 87,8%-os ImageNet top-1 pontosságot, ami jobb, mint a Swin Transformer eredménye.
- A ConvNeXt felülmúlja a Swin Transformatort több látási feladatban (például COCO objektum detektálás, ADE20K szemantikus szegmentáció).
- A ConvNeXt modellek a hagyományos CNN-ekhez hasonlóan hatékonyan működnek. Nincs szükség bonyolult modulokra, mint például a Transformer alapú eltolásos ablakfigyelem vagy a relatív pozíciótorzítás.



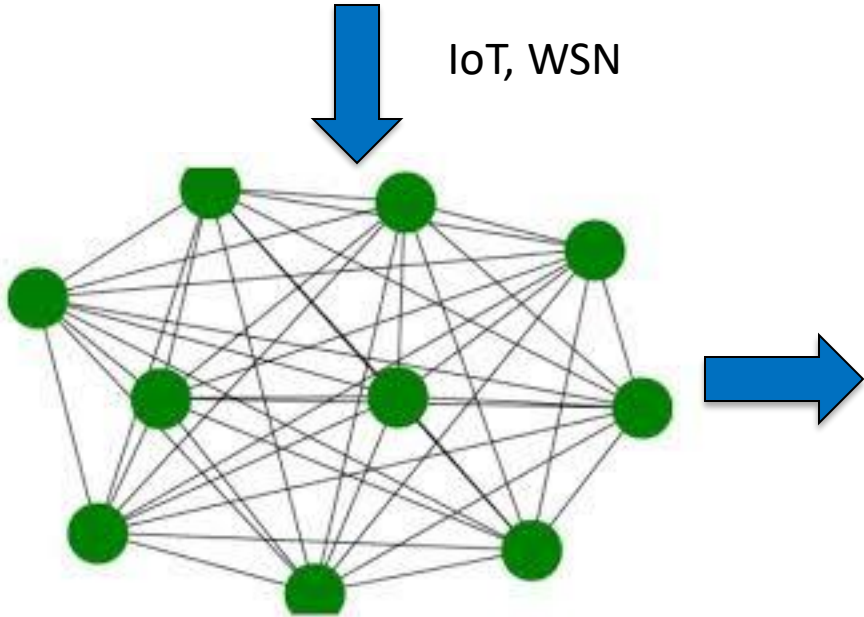
Hasznosítási terv

- Termékesítés: CARIN Deepfake Guard modul (on-prem, nagyvállalati integráció).
- DF-CAPTCHA koncepció és interaktív védelmi forgatókönyvek (valósídejű kihívások).
- Watermark-detektálás és -beágyazás vizsgálata (modalitások szerint).
- Licencelési utak: modul/licenc, integrációs szolgáltatás, pilot együttműködések.

Komplex rendszerek és MI



IoT, WSN



Computational twin

Rendszerállapotok,
anomáliák, self-healing

BME anomália detekció SW termék

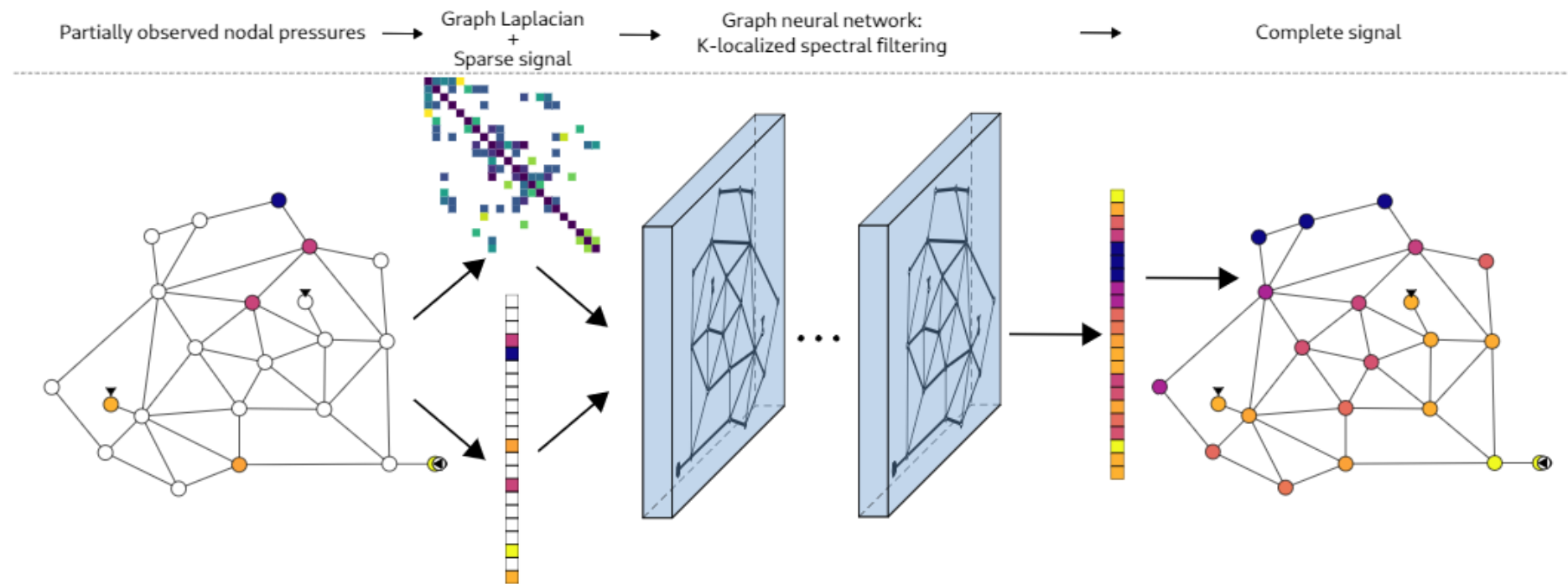
- Vodafone megvette és Európaszerte használják
- Pro progressio alapítvány innovációs nagydíja
- IT business innovációs díj



Kihívások:

- Hiányos adatok kezelése
- Bonyolult és összetett kapcsolatok (gráf modellezés)
- Anomália detekció magas dimenziós térben
-

Incomplete adat - predikció topológiai adatstruktúrákon gráfkonvolúciós hálózatokkal



Polinom

$$\Phi g(\Lambda) \Phi^T x \simeq \sum_{k=0}^K g_k \mathcal{L}^k x$$

g_k : együtthatók

Racionális

$$\Phi g(\Lambda) \Phi^T x \simeq \left(I + \sum_{l=1}^L p_l \mathcal{L}^l \right)^{-1} \left(\sum_{k=0}^K q_k \mathcal{L}^k \right) x$$

p_l : pólusok

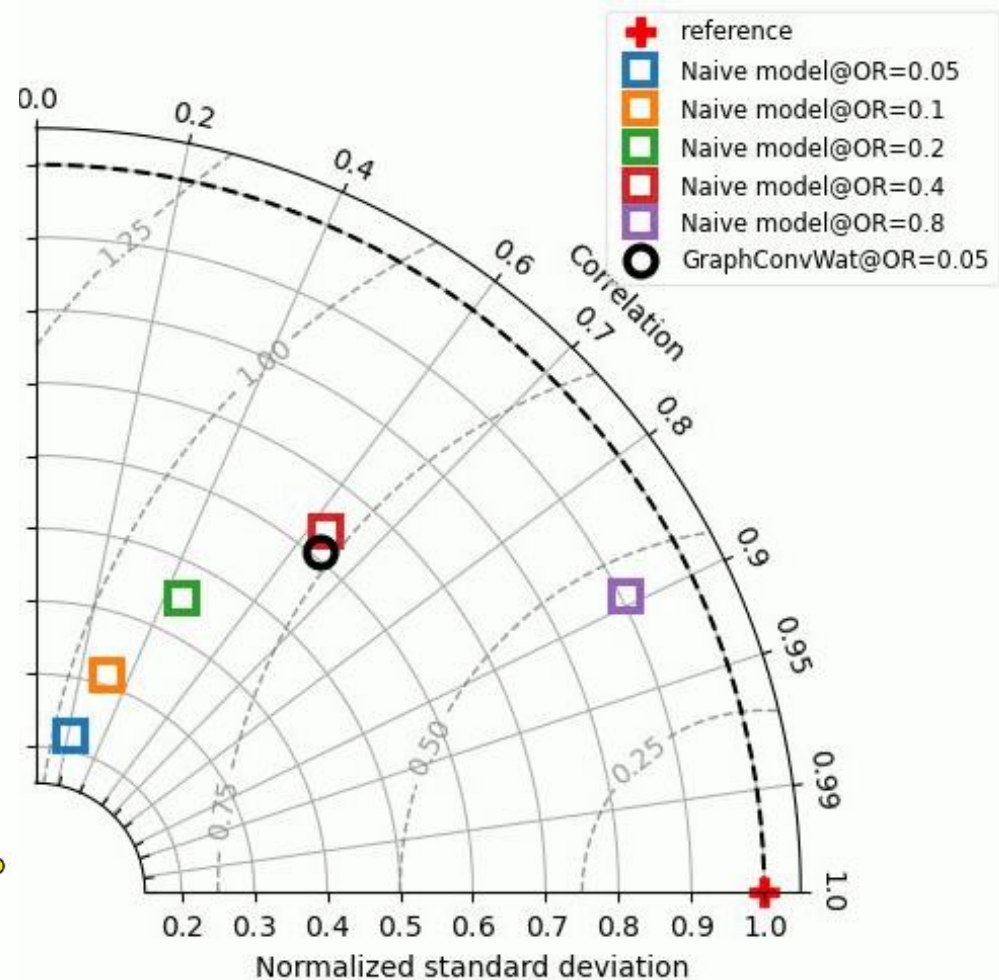
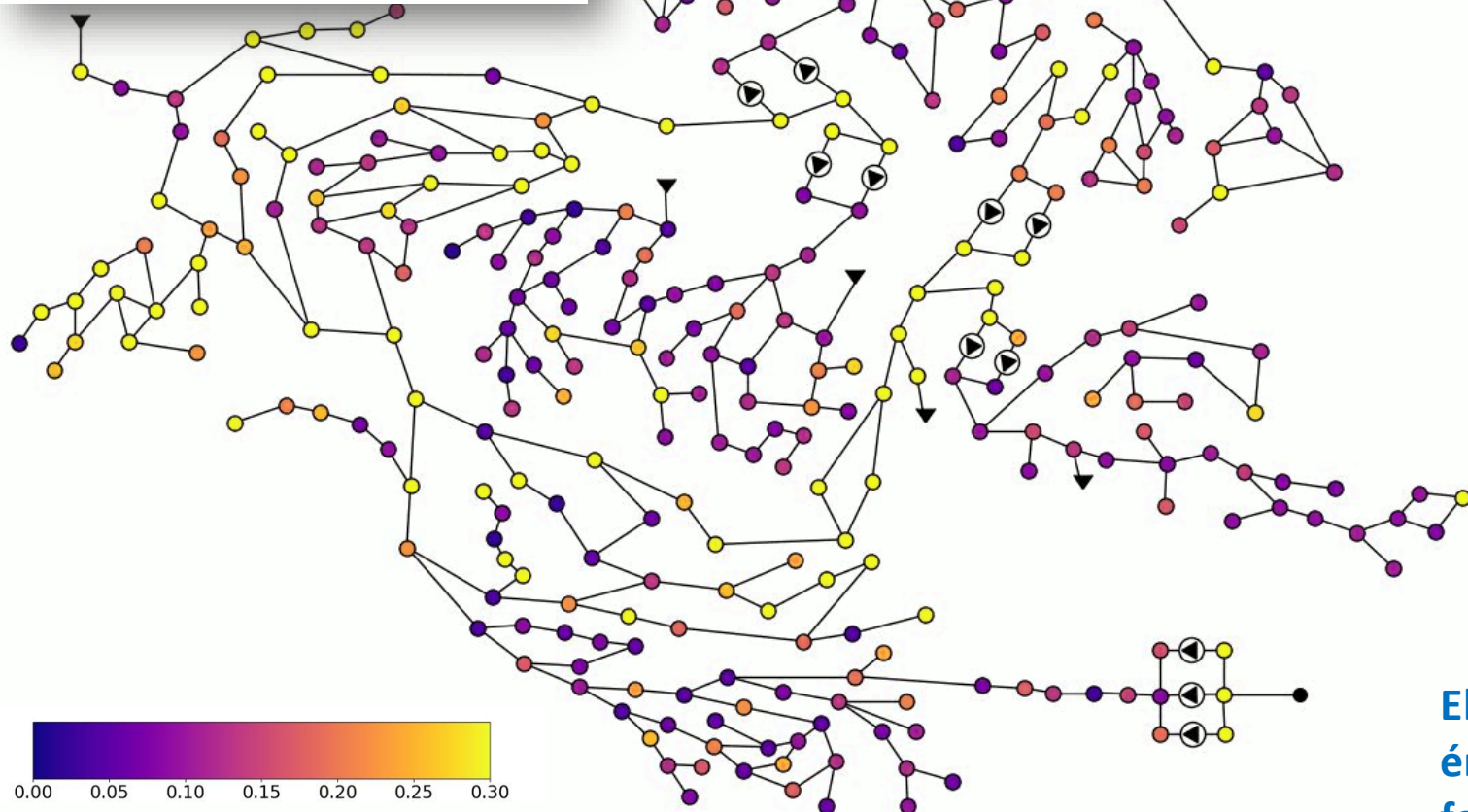
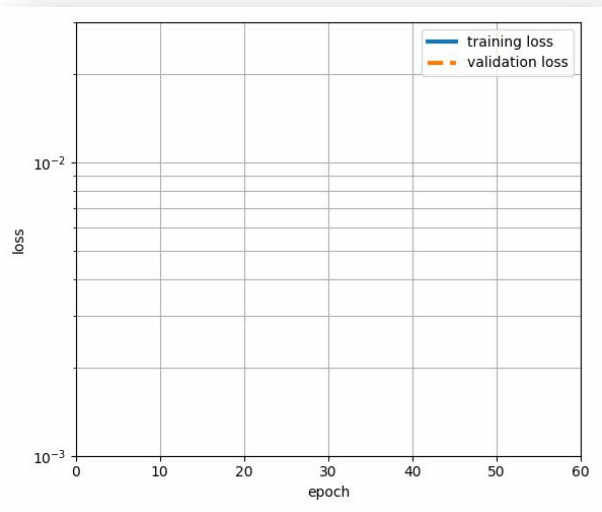
q_k : reziduumok

Lánczos

$$\Phi g(\Lambda) \Phi^T x \simeq V_K g(\mathbf{H}_K) V_K^T x$$

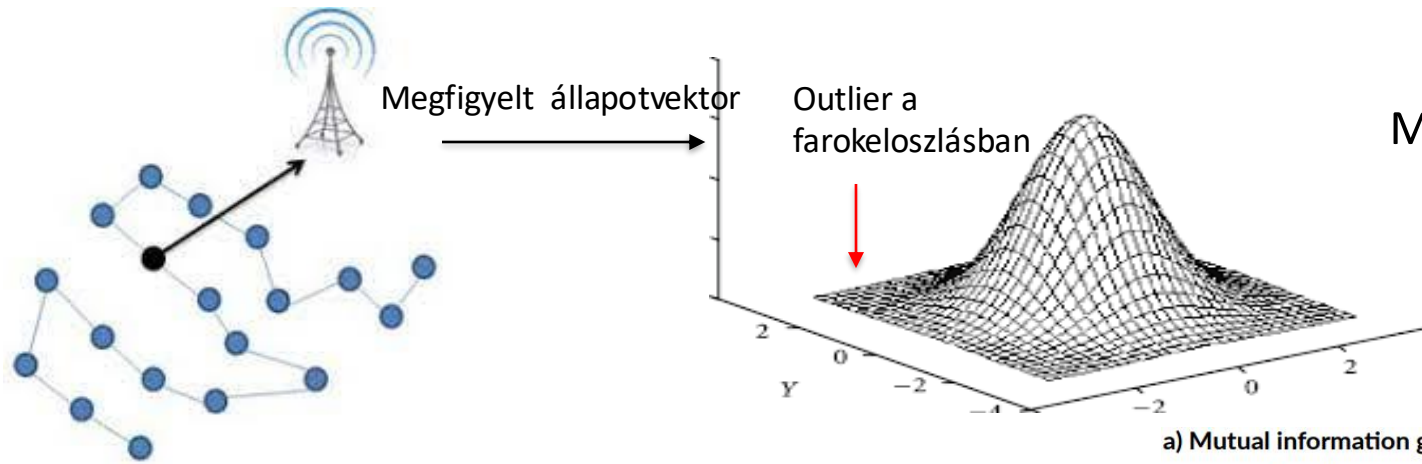
V_K : Lánczos vektorok

$\mathbf{H}_K$: Lánczos skalárok



Elegendő a csomópontok 5%-ára ismerni az értéket, a tanulás után 97%-os pontossággal tudni fogjuk az összes csomóponton !

Anomália detekció alacsony dimenziós térben



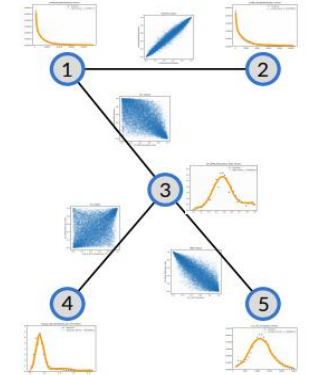
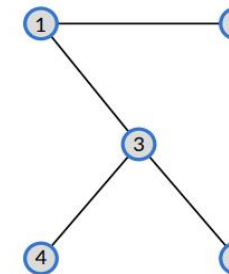
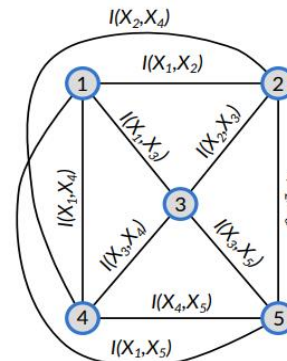
Magas dimenzióban kivitelezhetetlen



a) Mutual information graph

b) Maximum information tree

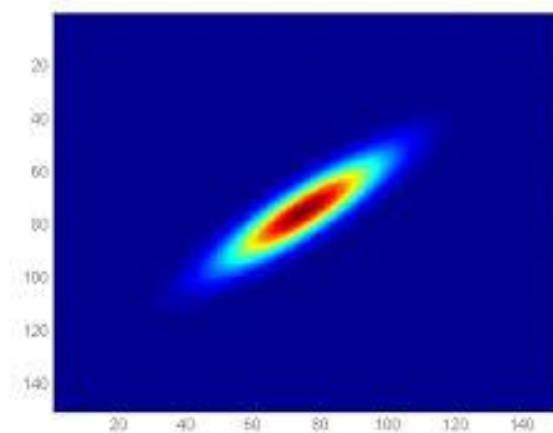
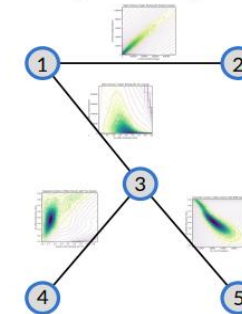
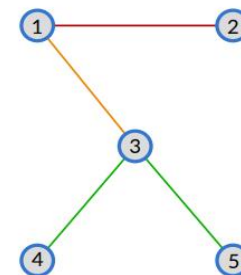
c) Fitting marginals and pair-copulas



Cho-Liu max-inf fa

e) Assigning anomaly scores to edges

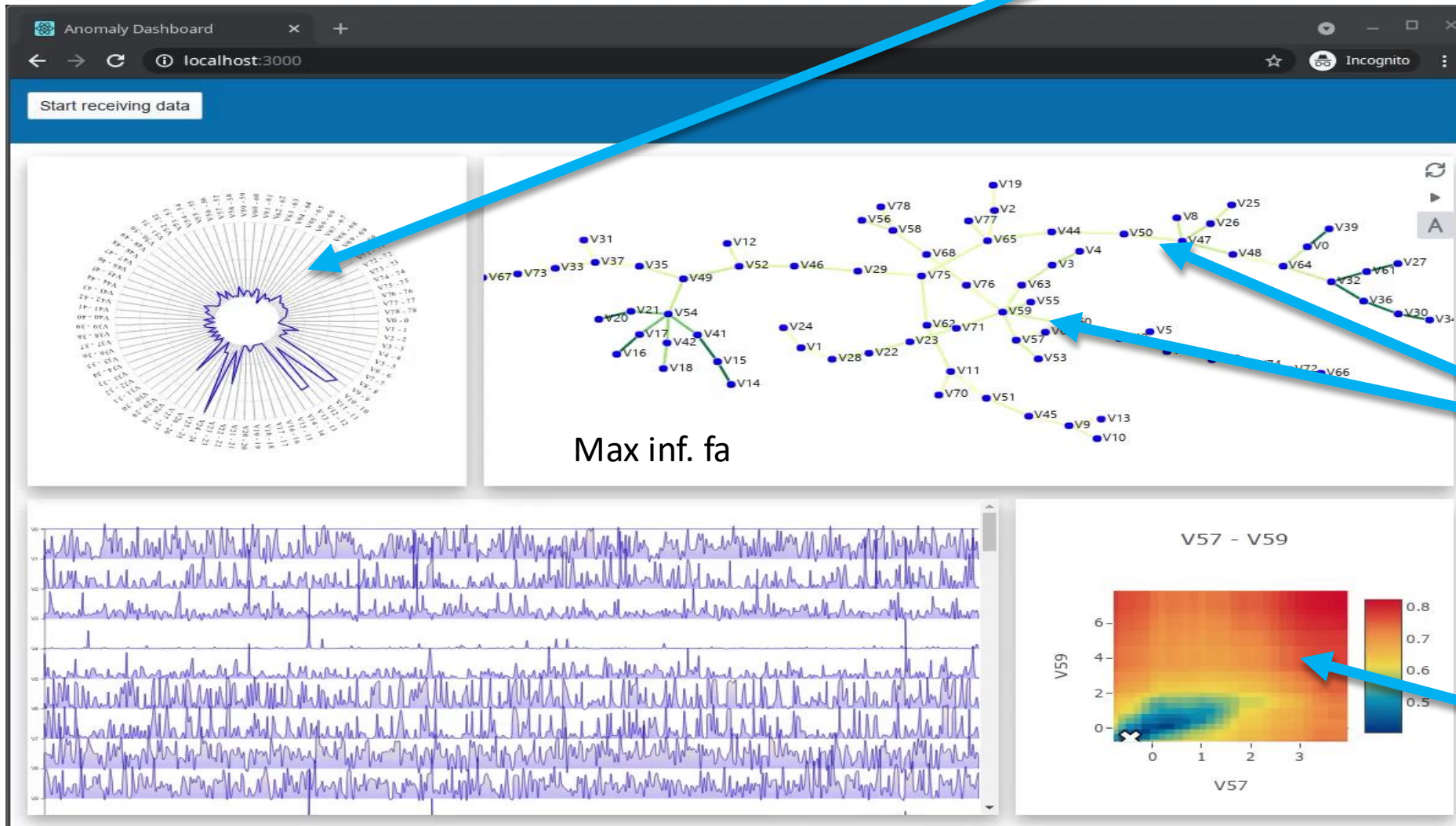
d) Reconstructing bivariate joint distributions



2D eloszlások
a fa élein

Anomaly dashboard

Radar plot – több nagyobb kiugrás



Max inf. fa

Változópárok anomália értéke – néhány változó viszonya rendellenes

A kijelölt V57-V59 változó pár anomáliatérképe – ez még mindig normális

Hasznosítás

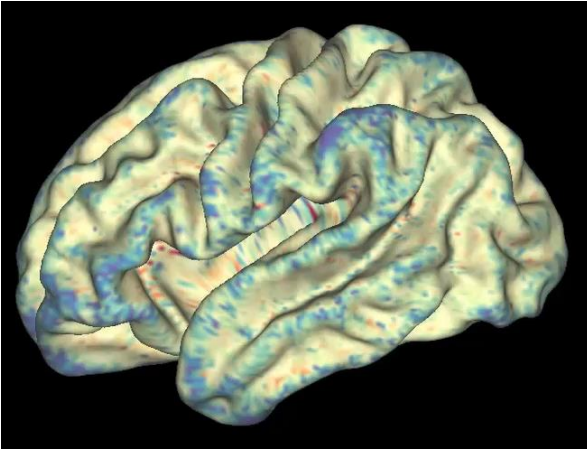
Komplex ipari rendszerek:

- Telekommunikációs hálózatok
- Városi vízvezeték-hálózatok
- Villamos energiahálózatok
- ...

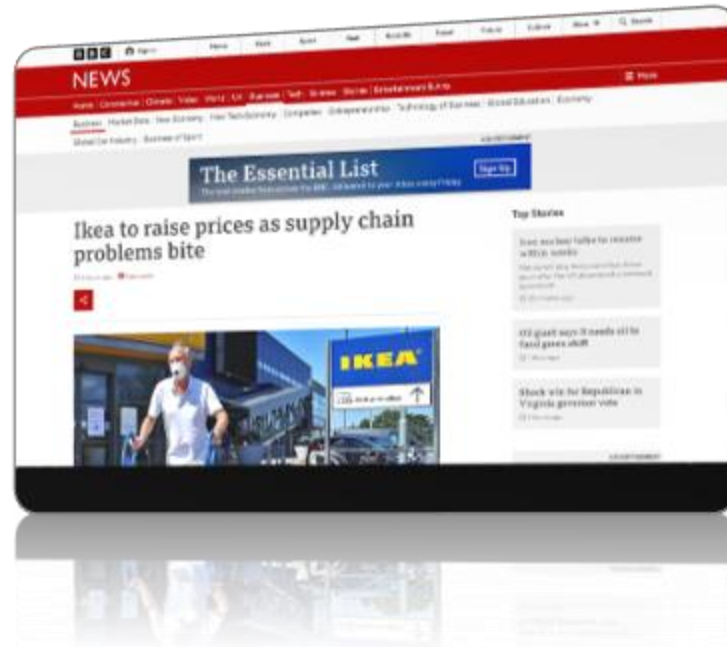


Néhány további új MI eredmény

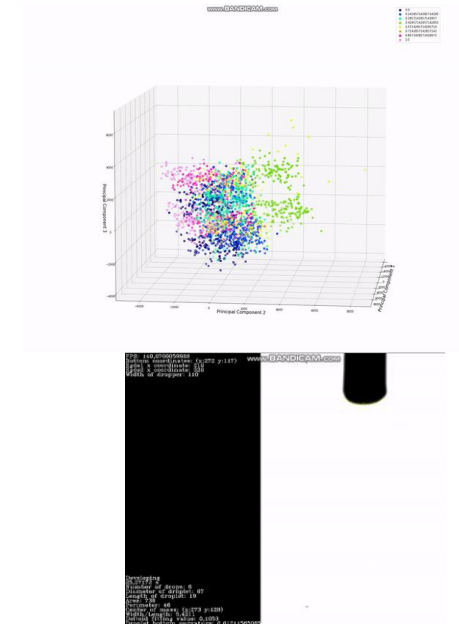
Mély neurális a korszülöttség indikálásra



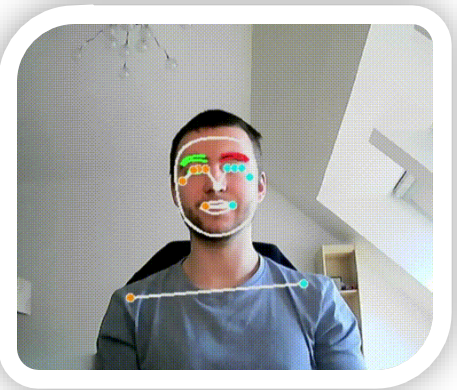
Hangulatbányászat MI-vel 14 nyelven



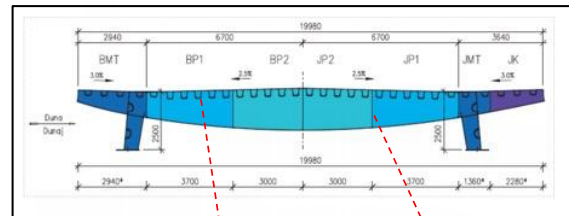
Folyadékviszkozitás gépi látással



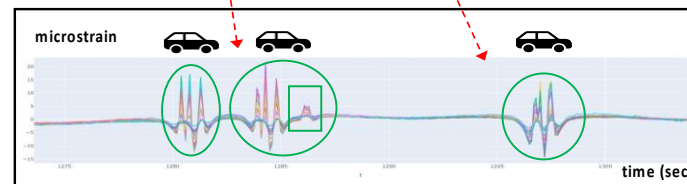
Multimodális ChatGPT



Mi alapú „okos” hidak tervezése



sensors



Autonóm járművek



BME InnoLab Zrt.: 225 darab értékesítésre váró K+F+I projekt (25 előválogatottból 16 deeptech)

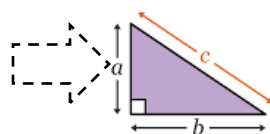


Tudományos eredményeken alapuló, élenjáró műszaki megoldások, potenciálisan diszruptív hatással.



A gazdasági és társadalmi impakt maximalizálása !

Mi az ami felett az egyetemnek őrködni kell (ember vs MI) ?

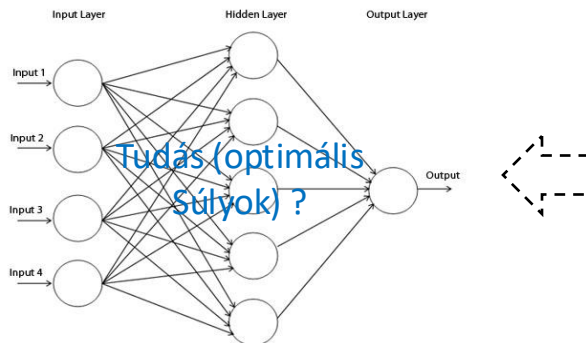


$$a^2 + b^2 = c^2$$

Pl. Tanulóhalmaz:
pitagoraszai számhár-
masok $a^2 + b^2 = c^2$

(3, 4) -> 5
(5,12) -> 13
(8,15) -> 17
(7,24) -> 25
(12,35) -> 37
(9,40) -> 41
(28,45) -> 42

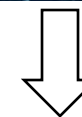
·
·
·



Promptok



Belső
reprezentáció



Válaszok

Limitált idő:

- Korlátos méretű tanulóhalmazból tudunk tanulni, ebben az esetben induktív gondolkodásra és absztrakcióra van szükségünk

Limitált számítási kapacitás:

- Részproblémákra bontás, dekompozíciók végrehajtása. Lokálisan optimalizál

A tudás nemcsak egy új adatrepresentációt (pl. optimális súlyok), hanem a megfigyelt jelenségek összekapcsolását és az ezek közötti relációk megértését jelenti !

- Hatalmas tanulóhalmazokat használhat fel. Nem kell az induktív gondolkodásra hagyatkoznia.
- Hatalmas számítási kapacitása van. Nem kell részcélokra bontás. Globálisan optimalizálhat.



Köszönöm a figyelmet !