DEEPFAKE TEXNOLOGIYASI ORQALI YARATILGAN SOXTA MEDIALARNI ASLIDAN FARQLASH HAMDA ZAMONAVIY HIMOYA USULLARI

IIV Akademiyasi kursanti,

Qahorov Davronbek Rustambek o‘g‘li

Annotatsiya: Mazkur maqolada Deepfake texnologiyasining mohiyati, undan foydalanish usullari va shu orqali yaratilgan soxta medialarning haqiqiy kontentdan qanday farqlanishi bo‘yicha eng zamonaviy tahlil va texnikalar yoritiladi. Bundan tashqari, soxta media mahsulotlarga qarshi kurashish, ularni aniqlash va profilaktika qilish usullari, shuningdek, xalqaro tajribalar asosida himoya strategiyalari tahlil qilinadi.

Kalit so‘zlar: Deepfake, sun’iy intellekt, GAN, media xavfsizlik, deteksiya, akustik barmoq izi, media savodxonlik,

Kirish

Sun’iy intellekt texnologiyalarining jadal rivojlanishi natijasida yaratilayotgan Deepfake kontentlar bugungi kunda real tasvirlar va videolardan ajralmas holga kelmoqda. Bu texnologiya asosan Generative Adversarial Networks (GAN) asosida ishlab chiqilib, inson yuzini, ovozini va harakatlarini boshqasiga realistik tarzda o‘xshatib yaratadi. Mazkur texnologiyaning ijtimoiy tarmoqlarda, siyosatda va ommaviy axborot vositalarida noto‘g‘ri maqsadlarda qo‘llanishi turli tahdidlarni yuzaga keltirmoqda. Ushbu maqolada Deepfake orqali yaratilgan soxta kontentni aniqlash metodlari, texnik vositalar, xalqaro va mahalliy yondashuvlar, shuningdek, profilaktik himoya choralariga alohida e’tibor qaratiladi.

Deepfake texnologiyasi va uning ishlash prinsipi

Deepfake texnologiyasi Generative Adversarial Network (GAN) algoritmiga asoslangan bo‘lib, u ikki neyron tarmoq – generator va diskriminatordan iborat. Generator

soxta kontentni yaratadi, diskriminator esa uni haqiqatdan ajratishga harakat qiladi. Bu jarayon orqali tizim tobora mukammallashadi. Hozirda Deepfake yordamida yuz almashish (face swap), ovoz klonlash, hatto real vaqtli video manipulyatsiyalar amalga oshirilmoqda.

Soxta medialarni aniqlash usullari

- Yuz mimikalari va ko‘z harakati tahlili.

Inson yuzi — juda murakkab mushaklar tizimiga ega. Har qanday hissiy holat: quvonch, hayrat, g‘azab, hayajon yuz ifodasida o‘z aksini topadi. Deepfake modellar esa hali-hanuz bu nozik mimik harakatlarni 100% aniq takrorlay olmaydi.

Ko‘z harakati va yuz mushaklari real videolarda biologik asoslangan muvofiqlik bilan ishlaydi. Deepfake’larda esa:

Ko‘zning tabiiy miltillashi (blink rate) kam yoki umuman yo‘q.

Yuz mushaklarining harakati silliq, lekin sintetik tusda bo‘ladi.

- Lab va nutq sinxronligi ba’zida kechikkan yoki nomuvofiq bo‘ladi.

AI asosidagi detektorlar: Microsoft Video Authenticator, Sensity AI.

Sun’iy intellekt asosida ishlab chiqilgan deepfake detektorlar bugungi kunda eng samarali texnik himoya vositalaridan biri hisoblanadi. Bu vositalar video va tasvirlarda mavjud bo‘lgan sun’iylik belgilarini aniqlash, mikroanomaliyalarni tahlil qilish, va realga o‘xshatib yaratilgan anipulyatsiyalarni fosh qilish uchun mo‘ljallangan.

Microsoft tomonidan ishlab chiqilgan ushbu texnologiya sun’iy intellekt (AI) va kompyuter ko‘rish (computer vision) algoritmlariga asoslangan. U foydalanuvchiga video yoki suratning qanchalik ehtimol bilan soxta ekanligini real vaqt rejimida ko‘rsatadi.

Sensity AI — deepfake va vizual manipulyatsiyalarni aniqlashga ixtisoslashgan italiyalik kompaniya. U ommaviy axborot vositalari, ijtimoiy tarmoqlar, hukumat organlari, va korporatsiyalar bilan hamkorlikda ishlaydi.

Quyida eng mashhur va ishonchli AI asosidagi deepfake aniqlovchi texnologiyaga to‘xtalamiz:

Ovoz-fingerprint tahlili.

Ovoz-fingerprint (inglizchada audio fingerprinting) — bu har bir insonning ovoziga xos bo‘lgan noyob akustik xususiyatlarni aniqlash va raqamli imzoga aylantirish texnikasidir. Bu texnologiya biometrik ovoz tahlili asosida ishlaydi va Deepfake orqali klonlangan sun’iy ovozlarni aniqlashda keng qo‘llaniladi.

Har bir insonning ovozi balandligi (pitch), tembr (tovush rangi), so‘zlash ritmi, urg‘ular va pauzalar, nafas olish oralig‘i bo‘yicha shaxsiy va noyob hisoblanadi. Aynan shu elementlar "ovoz-fingerprint" (ya’ni, akustik barmoq izi) sifatida raqamli tizimlarda saqlanadi.

Metadata va fayl strukturasi tekshiruvi.

Metadata — bu faylning o‘zi emas, balki u haqida “ma’lumotlar haqidagi ma’lumot”. U media faylning yaratilish vaqti, muharrir dasturi, o‘lchami, o‘zgartirish tarixi, GPS koordinatalari, qurilma modeli va boshqa texnik tafsilotlarini o‘z ichiga oladi.

Blockchain asosida media verifikatsiyasi.

Deepfake texnologiyasi rivojlangani sari, foydalanuvchilar ko‘z o‘ngida real va soxta media kontentni ajratish tobora qiyinlashmoqda. Shuning uchun, kontent yaratilganidan boshlab uning kelib chiqishini, o‘zgartirilmaganligini va muallifini isbotlaydigan raqamli tizimlar zarur bo‘lib bormoqda.

Blockchain texnologiyasi — bu o‘zgartirib bo‘lmaydigan, markazlashtirilmagan, zanjirli raqamli reyestr (ledger) bo‘lib, har qanday kontent yaratilgan paytdagi holatini kripografik tarzda raqamli imzo (hash) bilan muhrlab qo‘yadi. Keyinchalik har qanday tahrir yoki manipulyatsiya aniqlanadi.

3. Zamonaviy himoya vositalari va texnologiyalari

Deepfake kontentlardan himoyalanishda quyidagi texnik vositalar qo‘llaniladi:

- AI asosidagi real vaqtli monitoring tizimlari (Deeptrace, Deepware Scanner)
- Blockchain asosida kontent manbasini tekshirish texnologiyalari
- Adobe Content Authenticity Initiative
- Google va Meta Deepfake Detection Challenge

4. Media savodxonlik va profilaktik chora-tadbirlar

- Media savodxonlik kurslarini ta’limga joriy etish
- Foydalanuvchilarni hushyorlikka o‘rgatuvchi treninglar
- OAV uchun verifikatsiya standartlari
- Kiberxavfsizlik profilaktikasi

Xulosa

Deepfake texnologiyasi — bu sun’iy intellekt yutuqlarining eng murakkab va ayni paytda xavfli ko‘rinishlaridan biridir. U orqali yaratilgan soxta media mahsulotlar jamiyat, siyosat va iqtisodiyotga salbiy ta’sir ko‘rsatishi mumkin. Shuning uchun, soxta kontentni aniqlashda texnik vositalar bilan birga, huquqiy mexanizmlar, profilaktik chora-tadbirlar va aholining axborot madaniyati darajasini oshirish muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. Goodfellow I. et al. (2014). Generative Adversarial Nets.
2. Microsoft AI & Ethics in Engineering and Research Group
3. Deeptrace Labs: The State of Deepfakes 2023
4. Adobe Content Authenticity Initiative
5. Kaspersky Lab tahlillari
6. www.deepware.ai
7. O‘zbekiston Respublikasi Axborot xavfsizligi konsepsiyasi (2022)