

“DEEFAKE” - SOXTA NATIJALAR YARATISH UCHUN SUN’IY INTELLEKT VA BOSHQA ZAMONAVIY TEXNOLOGIYALARDAN FOYDALANISH

Mustafa Djamatov Xatamovich

O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalari va axborot xavfsizligi kafedrası katt o‘qituvchisi.

Saidaminxo‘ja Abdazimov Zoirxo‘ja o‘g‘li

O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalari va axborot xavfsizligi kafedrası o‘qituvchisi.

<https://doi.org/10.5281/zenodo.14594304>

Annotatsiya. Ushbu maqola Deepfake texnologiyasi va uning ishlash mexanizmini batafsil ko‘rib chiqadi. Deepfake – bu Generative Adversarial Networks (GAN) asosida ishlaydigan zamonaviy sun’iy intellekt yutug‘idir. Ushbu texnologiya inson ovozi, yuzi va harakatlarini soxtalashtirib, haqiqatga juda yaqin virtual materiallar yaratish imkonini beradi. Maqolada Deepfake texnologiyasining ijtimoiy, ilmiy va axloqiy jihatlari, shuningdek, uning imkoniyatlari va xavflari keng yoritilgan.

Kalit so‘zlar: Deepfake, Sun’iy intellekt, Generative Adversarial Networks (GAN), Soxta kontent, Axborot xavfsizligi, Ijtimoiy manipulyatsiya, Axloqiy masalalar, Ovoz va video modifikatsiyasi, Deepfake aniqlash texnologiyalari.

“DEEFAKE” - THE USE OF ARTIFICIAL INTELLIGENCE AND OTHER MODERN TECHNOLOGIES TO CREATE FAKE RESULTS

Abstract. This article examines in detail the Deepfake technology and its mechanism of operation. Deepfake is a modern artificial intelligence achievement based on Generative Adversarial Networks (GAN). This technology allows you to create virtual materials that are very close to reality by forging human voices, faces and movements. The article extensively covers the social, scientific and ethical aspects of Deepfake technology, as well as its opportunities and risks.

Keywords: Deepfake, Artificial Intelligence, Generative Adversarial Networks (GAN), Fake content, Information security, Social manipulation, Ethical issues, Audio and video modification, Deepfake detection technologies.

«ДИПФЕЙК» — ЭТО ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ДРУГИХ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДЛЯ СОЗДАНИЯ ФЕЙКОВЫХ РЕЗУЛЬТАТОВ.

Аннотация. В этой статье подробно рассматривается технология Deepfake и то, как она работает. Deepfake — это прорыв в современном искусственном интеллекте на основе генеративно-состязательных сетей (GAN). Эта технология позволяет создавать виртуальные материалы, максимально приближенные к реальности, путем

фальсификации человеческого голоса, лица и движений. В статье рассматриваются социальные, научные и этические аспекты технологии Deepfake, а также ее возможности и риски.

Ключевые слова: Deepfake, Искусственный интеллект, Генеративно-состязательные сети (GAN), Фейковый контент, Информационная безопасность, Социальные манипуляции, Этические проблемы, Модификация аудио и видео, Технологии обнаружения Deepfake.

Sun'iy intellekt (SI) — bu kompyuter tizimlariga inson aql-idrokini taqlid qilish qobiliyatini beruvchi texnologiyalar majmuasidir. SI algoritmlari ma'lumotlarni qayta ishlash, o'rganish va murakkab masalalarni mustaqil hal qilish imkoniyatiga ega. Sun'iy intellektning asosiy yo'nalishlari quyidagilardan iborat:

Mashina o'qitish (Machine Learning): Kompyuter tizimlari dasturlashtirilmagan holda tajribalar orqali o'z-o'zini rivojlantiradi. Masalan, yuzni tanib olish tizimlari.

Chuqur o'rganish (Deep Learning): Ko'p qatlamli neyron tarmoqlar orqali ma'lumotlarni qayta ishlash va tushunish. Bu Deepfake texnologiyasining ham asosini tashkil qiladi.

Tabiiy tilni qayta ishlash (Natural Language Processing, NLP): Inson tillarini tushunish va ularni qayta ishlash texnologiyasi, misol qilib ushbu tizimga suhbat botlarini olishimiz mumkin.

Kompyuter ko'rish (Computer Vision): Tasvir va videolarni tahlil qilish va ulardan ma'lumot olish texnologiyasi.

Zamonaviy texnologiyalar esa SI asosida ishlaydigan turli innovatsion yechimlar va qurilmalarni o'z ichiga oladi. Bunga quyidagilar kiradi:

Raqamli ma'lumotlar tahlili: Big Data va IoT (Internet of Things) yordamida real vaqtda katta hajmdagi ma'lumotlarni tahlil qilish.

Avtomatlashtirilgan tizimlar: Aqlli robotlar, dronlar va o'zini boshqaruvchi avtomobillar.

Virtual va kengaytirilgan haqiqat (VR/AR): Reallikni sun'iy ravishda yaratish yoki haqiqiy tasvirlarni kengaytirish imkoniyatlari.

Sun'iy intellekt va zamonaviy texnologiyalarning uyg'unligi Deepfake kabi murakkab va samarali tizimlarni yaratishga imkon berdi. Bu texnologiyalar yordamida insoniyat ko'plab sohalarda yutuqlarga erishmoqda, lekin ular bilan bog'liq xavflarni boshqarish zarurati ham ortib bormoqda.

Hozirgi davrda texnologiya va sun'iy intellekt sohalaridagi yutuqlar jamiyat hayotining barcha jabhalariga ta'sir ko'rsatmoqda.

Shunday texnologiyalardan biri bo'lgan "Deepfake", ya'ni sun'iy intellekt yordamida soxta natijalar yaratish, raqamli sohada yangi imkoniyatlar eshigini ochmoqda. Ushbu texnologiya inson ovozi, yuzi va harakatlarini sun'iy ravishda o'zgartirib, ular orqali mavjud bo'lmagan natijalarni yaratish imkoniyatini beradi.

Deepfake atamasi "deep learning" (chuqur o'rganish) va "fake" (soxta) so'zlarining qo'shilishidan hosil bo'lgan. Ushbu texnologiya sun'iy intellektning ilg'or turi bo'lgan Generative Adversarial Networks (GAN) asosida ishlaydi. GAN'lar haqiqiyga juda yaqin bo'lgan tasvirlar va ovozlarni yaratishda ishlatiladi. Natijada, inson ko'zini alday oladigan videolar, tasvirlar va hatto ovozli xabarlar yaratish mumkin bo'lmoqda.

Hozirgi kunda Deepfake texnologiyasi sun'iy intellekt sohasidagi eng muhim va bahsli mavzulardan biriga aylangan. Uning dolzarbligi texnologiyaning ijtimoiy, ilmiy va axloqiy jihatlari bilan bog'liq bo'lib, bu texnologiya bir vaqtning o'zida yuksak imkoniyatlarni taqdim etishi va jiddiy xavf-xatarlarni keltirib chiqarishi bilan ajralib turadi.

Ijtimoiy jihatlari

Deepfake texnologiyasi ijtimoiy hayotning turli sohalariga sezilarli ta'sir ko'rsatmoqda.

Bu ta'sir ikki tomonlama bo'lib, texnologiyaning ijobiy imkoniyatlari va salbiy oqibatlarini o'z ichiga oladi:

Ijobiy jihatlari:

Deepfake orqali realistik o'quv materiallari va ta'lim dasturlari yaratilmoqda. Bu texnologiya interaktiv va qiziqarli bilim olish jarayonini ta'minlaydi.

Kino va san'at sohalarida yaratuvchanlikni oshirish imkoniyatlarini beradi. Masalan, tarixiy shaxslarni "jonlantirish" yoki murakkab vizual effektlarni yaratish imkoniyatlari mavjud.

Salbiy jihatlari:

Soxta xabarlar va noto'g'ri axborot tarqatish orqali ijtimoiy manipulyatsiyalarni amalga oshirish. Mashhur shaxslar yoki oddiy insonlar yuz ifodalarini soxtalashtirib, obro'siga putur yetkazish, shaxsiy hayot daxlsizligini buzish. Ijtimoiy tarmoqlarda soxta kontent orqali yolg'on axborotning tarqalishi keng miqyosdagi jamiyatda ishonchsizlik muhitini yuzaga keltirish.

Ilmiy jihatlari

Deepfake texnologiyasi sun'iy intellekt va kompyuter texnologiyalari rivojlanishida muhim ilmiy yutuqlarni taqdim etmoqda:

Tadqiqot imkoniyatlari:

GAN kabi ilg'or algoritmlarni rivojlantirish orqali sun'iy intellekt sohasida chuqur o'rganish uchun yangi imkoniyatlar ochilmoqda. Ovoz va tasvirlarni o'zgartirish texnologiyalari tibbiyot, masalan, nutq terapiyasi yoki yuz rekonstruksiyasi kabi sohalarda foydalanilmoqda.

Xavfli jihatlari esa:

Texnologiyani nazorat qilish muammosi. Deepfake shunchalik tez rivojlanmoqdaki, undan noqonuniy yoki axloqiy bo'lmagan maqsadlarda foydalanishni oldini olish qiyinlashmoqda. Soxta kontentni aniqlash uchun texnik vositalar hali yetarlicha rivojlanmagan, bu esa ilmiy hamjamiyat uchun yangi muammolarni keltirib chiqarmoqda.

Shaxsiy hayot daxlsizligi:

Deepfake orqali odamlarning ruxsatisiz tasvir yoki ovozdan foydalanish axloqiy jihatdan qabul qilinmaydi. Bu shaxsiy hayot huquqlarini buzadi. Texnologiya odamlarning qiyofasini soxtalashtirish orqali ularga bo'lgan ishonchni yo'qotishga olib kelishi mumkin.

Axloqiy chegaralar:

Deepfake texnologiyasi soxta materiallar yaratish orqali insoniyatning axloqiy qadriyatlariga putur yetkazadi. Masalan, noto'g'ri ma'lumot tarqatish yoki biror insonni sharmanda qilish maqsadida foydalanish.

Texnologiyani nazorat qilishda jamoatchilik va hukumatning roli yetarli bo'lmay, axloqiy muammolar chuqurlashishi mumkin.

Deepfake texnologiyasining ishlash prinsipi

Deepfake texnologiyasi zamonaviy sun'iy intellekt yutuqlaridan biri bo'lib, raqamli tasvir, video va ovozli ma'lumotlarni soxtalashtirish orqali yangi virtual natijalarni yaratishga imkon beradi. Ushbu texnologiya Generative Adversarial Networks (GANs) arxitekturasiga asoslangan va murakkab matematik algoritmlar orqali o'z natijalarini haqiqatga yanada yaqinlashtiradi. Ushbu texnologiya inson yuzini, ovozini va boshqa xususiyatlarini shunchalik aniq takrorlaydiki, bu natijani haqiqatdan farqlash qiyin bo'ladi. Quyida Deepfake'ning texnik asoslari va ishlash jarayonlari keltirilgan.

1. GAN arxitekturasini – asosiy mexanizm

Deepfake texnologiyasi Generative Adversarial Network (GAN) deb nomlangan neyron tarmog'iga tayanadi. GAN ikkita asosiy qismdan iborat:

- **Generativ model (generator):** Soxta tasvir yoki ovoz yaratadi. Masalan, u mavjud bo'lmagan insonning yuzi yoki boshqa ma'lumotlarni yaratishi mumkin.
- **Discriminator (farqlovchi):** Yaratilgan ma'lumotning haqiqiyligini aniqlashga harakat qiladi. Bu tizim generatorning natijalarini haqiqatdan ajratishga urinadi.

Bu tizimning mohiyati raqobatga asoslanadi. Generator yangi tasvir yaratadi, farqlovchi esa bu tasvirning haqiqiy yoki soxta ekanligini aniqlaydi. Har bir marta farqlovchi generator natijasini rad etsa, generator o'z algoritmini yaxshilaydi. Natijada, ikki tizim bir-biriga qarshi ishlash orqali yanada mukammal va haqiqatga yaqin soxta ma'lumotlar yaratadi.

2. Ma'lumotlarni qayta ishlash jarayoni

Deepfake yaratish uchun quyidagi bosqichlar amalga oshiriladi:

1. **Dastlabki ma'lumotlar yig'ilishi:** Dastur uchun asosiy material bo'lib xizmat qiladigan tasvir yoki videolar to'planadi. Masalan, biror mashhur shaxsning yuz ifodalari turli burchaklardan olingan bo'lishi kerak.
2. **Ma'lumotlarni tahlil qilish:** Neyron tarmoq bu ma'lumotlarni o'rganib, inson yuzidagi har bir ifoda va detallarni aniqlaydi.
3. **Yaratish jarayoni:** GAN orqali sun'iy tasvir yoki ovoz yaratiladi.
4. **Post-protsessing:** Yaratilgan materialni tahrirlash va asl material bilan sinxronlash ishlari olib boriladi.

Neyron tarmoqni o'rgatish:

Yig'ilgan ma'lumotlar GAN modeliga kiritiladi. Model inson yuz ifodalarini, ovoz o'zgarishlarini yoki boshqa xususiyatlarini o'rganadi.

- **Tasniflash:** Model insonning har bir yuz muskullarini va harakatlarini tahlil qiladi.
- **Rekonstruksiya:** Olingan natijalar sun'iy ma'lumot yaratishda ishlatiladi.

GAN modeli tomonidan olingan bilimlar asosida yangi, soxta tasvir yoki video yaratiladi. Masalan, bir insonning yuz ifodalari boshqa insonning yuziga sinxronlashtiriladi.

3. Deepfake'ning rivojlanishi va murakkabligi

Deepfake texnologiyasi dastlab oddiy modifikatsiyalarni amalga oshirgan bo'lsa, bugungi kunda u quyidagilarni amalga oshira oladi:

- Haqiqiy videodagi ovozni soxtalashtirib, boshqa bir shaxsning ovozi bilan almashtirish.
- Tasvirlardagi yuzlarni boshqa yuzlar bilan mukammal darajada o'zgartirish.
- Jonli videolarni real vaqt rejimida soxtalashtirish (Live Deepfake).

4. Texnologiyaning mukammallashishi sabablari

- **Kompyuter quvvatlarining oshishi:** Sun'iy intellekt algoritmlari tobora ko'proq ma'lumotni qayta ishlay oladi.
- **Katta ma'lumot bazalarining mavjudligi:** Internetda ochiq ma'lumotlar ko'pligi (jumladan, ijtimoiy tarmoqlardagi tasvir va videolar).
- **Algoritmlarning takomillashuvi:** GAN tizimlari nafaqat tasvirlarni, balki vaqt o'tishi bilan ovoz va harakatlarni ham ko'chira oladi.

Deepfake texnologiyasining ishlash prinsipi yuqoridagi murakkab jarayonlar orqali amalga oshadi va uning imkoniyatlari kundan-kunga kengayib bormoqda.

Deepfake texnologiyasining xavf va muammolarini yechish yo'llari

Deepfake texnologiyasining rivojlanishi bir qator yangi xavf-xatarlarni keltirib chiqarmoqda. Ushbu texnologiyaning salbiy oqibatlarini kamaytirish uchun bir nechta samarali

yechimlarni ko'rib chiqish zarur. Quyidagi yo'llar bu muammolarni hal qilishda muhim rol o'ynashi mumkin:

1. Qonunchilikni kuchaytirish va tartibga solish

Deepfake texnologiyasidan noto'g'ri foydalanishning oldini olish uchun samarali huquqiy mexanizmlar yaratish zarur. Bu quyidagi qadamlarni o'z ichiga oladi:

Maxsus qonunlar va normativ hujjatlar:

Deepfake texnologiyasiga qarshi maxsus qonunlar ishlab chiqilishi kerak. Shu bilan birga, soxta kontent yaratish va tarqatish uchun javobgarlikni aniq belgilash lozim. Masalan, soxta video yoki audio materiallar orqali obro'ni so'ndirish, firibgarlik qilish yoki axborot manipulyatsiyalarini amalga oshirish uchun jinoiy javobgarlikni joriy etish zarur. Deepfake'ni aniqlash, monitoring qilish va axborot xavfsizligi sohasida yagona standartlar ishlab chiqish muhim.

2. Deepfake'ni aniqlash va monitoring qilish texnologiyalarini rivojlantirish

Deepfake texnologiyasini aniqlash va uning salbiy oqibatlarini kamaytirish uchun maxsus dasturlar va texnologiyalarni takomillashtirish kerak:

Deepfake'ni aniqlash uchun ilg'or sun'iy intellekt tizimlaridan foydalanish zarur. Masalan, yuz ifodalari va ovoz o'zgarishlarini aniqlash uchun yangi metodlar va algoritmlar ishlab chiqilishi kerak. Buning uchun sun'iy intellekt tizimlarining o'rganish imkoniyatlarini kengaytirish kerak.

Real vaqt rejimida monitoring:

Deepfake'larni tezkor ravishda aniqlash va ularni tarqatishdan oldin bloklash uchun real vaqt monitoring tizimlari ishlab chiqilishi lozim. Bu texnologiya ijtimoiy tarmoqlarda, ommaviy axborot vositalarida va onlayn platformalarda tarqatilayotgan soxta kontentni tezda aniqlashga yordam beradi.

3. Ommaviy axborot vositalarida ta'lim va axborot savodxonligini oshirish

Ommaviy axborot vositalarida keng qamrovli ta'lim va axborot savodxonligini oshirish muhim: Jamiyatni deepfake texnologiyasi va uning xavflari haqida xabardor qilish, soxta axborotlarni aniqlash uchun zarur bilim va ko'nikmalarni shakllantirish zarur. Axborot iste'molchilari soxta materiallarni haqiqiylardan farqlashga o'rgatish kerak.

Jamoatchilikni ogoh qilish:

Deepfake texnologiyasining xavf-xatarlarini tushuntirish va odamlarni soxta kontentlarga qarshi ogoh qilish muhim. Bu jarayonda ta'lim muassasalari, ijtimoiy tashkilotlar va davlat idoralari birgalikda ishlashi kerak.

4. Texnik yondashuvlar va muhandislik yechimlari

Deepfake texnologiyasini boshqarish uchun ilg'or texnik yondashuvlar va innovatsion muhandislik yechimlari joriy etilishi lozim:

“Watermark” texnologiyasi:

Deepfake video yoki tasvirlariga raqamli izlar (watermark) qo'yish, ularni mualliflik huquqi bilan bog'lash orqali soxta kontentlarni aniqlashni osonlashtirish mumkin. Bu usul orqali, ma'lum bir video yoki tasvirni soxta bo'lganligini aniqlashda yordam berishi mumkin.

Blokcheyn texnologiyasi:

Raqamli tasvir va video materiallarni autentifikatsiya qilish uchun blokcheyn texnologiyasidan foydalanish mumkin. Blokcheyn orqali, materialning haqiqiyligi tasdiqlanadi va soxta kontentlar tarqalishi oldi olinadi.

5. Ijtimoiy mas'uliyat va axloqiy me'yorlar

Deepfake texnologiyasidan foydalanishda axloqiy me'yorlar va ijtimoiy mas'uliyatni saqlab qolish kerak:

Deepfake texnologiyasining xavf-xatarlarini kamaytirish va ularni boshqarish uchun kompleks yondashuv zarur. Bu faqat texnik yechimlar bilan cheklanmay, balki huquqiy, axloqiy va ijtimoiy choralarni ham o'z ichiga olishi kerak. Yangi qonunlarni ishlab chiqish, soxta kontentlarni aniqlash texnologiyalarini takomillashtirish, axborot savodxonligini oshirish va jamiyatni ogohlantirish kabi qadamlar yordamida Deepfake texnologiyasining salbiy oqibatlari oldini olish mumkin. Yaxshi boshqarilgan Deepfake texnologiyasi, o'zining ijobiy salohiyati bilan jamiyatga foyda keltirishi mumkin.

REFERENCES

1. **Goodfellow I., Bengio Y., Courville A.** (2016). *Deep Learning*. MIT Press.
2. **Krizhevsky A., Sutskever I., Hinton G. E.** (2012). *ImageNet Classification with Deep Convolutional Neural Networks*. Advances in Neural Information Processing Systems (NIPS).
3. **Redmon J., Divvala S., Girshick R., Farhadi A.** (2016). *You Only Look Once: Unified, Real-Time Object Detection*. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
4. **He K., Zhang X., Ren S., Sun J.** (2016). *Deep Residual Learning for Image Recognition*. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
5. **Deng J., Dong W., Socher R., Li L.-J., Li K., Fei-Fei L.** (2009). *ImageNet: A Large-Scale Hierarchical Image Database*. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
6. **Zeiler M. D., Fergus R.** (2014). *Visualizing and Understanding Convolutional Networks*. European Conference on Computer Vision (ECCV).

7. **Ren S., He K., Girshick R., Sun J.** (2015). *Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks*. IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI).
8. **LeCun Y., Bengio Y., Hinton G.** (2015). *Deep Learning*. Nature, 521(7553), 436–444.
9. **Russakovsky O., Deng J., Su H., et al.** (2015). *ImageNet Large Scale Visual Recognition Challenge*. International Journal of Computer Vision (IJCV), 115(3), 211-252.
10. **Huang G., Liu Z., Van Der Maaten L., Weinberger K. Q.** (2017). *Densely Connected Convolutional Networks (DenseNet)*. IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
11. Филин С. А. «Информационная безопасность», М.: Альфа – Пресс, 2006 г.