SOXTA TASVIR VA VIDEOLARNING ASL MOHIYATINI TUSHUNISH

Nekboyev Faxriddin Oltiboy o’g’li
Toshkent Davlat Yuridik universiteti magistratura talabasi
Email: nekboyevfaxriddin2@gmail.com
Telefon: +998 99 629 12 42

Annotatsiya: *Deepfake algoritmi foydalanuvchiga juda haqiqiy tuyuladigan, ammo aslida soxta bo‘lgan tasvirlar, audio va videolar yaratish imkonini beradigan texnologiya. Bunday darajadagi texnologiyaga chuqur o‘rganish (Deep Learning), mashina yordamida o‘rganish (Machine Learning), sun’iy intellekt (Artificial Intelligence) va neyron tarmoqlar (Neural Networks) sohalaridagi mukammallashuv orqali erishilgan. Ushbu jarayonda generativ adversarial tarmoq (GAN), avtokodlovchilar (autoencoders) kabi algoritmlar kombinatsiyasi ishlatilishi mumkin.*

Har qanday texnologiya singari, deepfake ham ijobiy va salbiy oqibatlarga ega ligi hech kimga sir emas. Ijobiy jihatdan, deepfake texnologiyasi gapirish qobiliyatini yo‘qotgan yoki gapirishda nuqsoni bo’lgan odamlarga yangi, yaxshilangan va sifatli ovoz yaratib berishda yordam berishi mumkin. Tijorat sohasida esa u animatsiya va filmlar sifatini oshirishda, ijodiy g‘oyalarni hayotga tatbiq etishda yoki yaqinlarini yo‘qotgan insonlar uchun ularni deepfake orqali tiklab, ularni jonlantirish ularga psixologik jihatdan yordam berishi mumkin.

Salbiy tomonlari esa shundaki, juda real ko‘rinadigan soxta tasvirlar, videolar yoki audio yozuvlar shaxsiy hayot daxlsizligiga, tashkilotlar faoliyatiga, demokratiyaga, hatto milliy xavfsizlikka tahdid solishi mumkin.

Ushbu maqola deepfake texnologiyasining paydo bo‘lish tarixi, uning qanday ishlashi va unda qo‘llaniladigan asosiy algoritmlar haqida ma’lumot beradi. Shuningdek, ilmiy adabiyotlarda olib borilgan muhim tadqiqotlarni tahlil qiladi hamda deepfake’ni aniqlash usullari va zararli oqibatlarni oldini olish uchun qanday samarali profilaktik choralar ko’rilganligini ko’rib chiqadi

Kalit so‘zlar: *Deepfake, GAN, avtokodlovchilar (autoencoders), soxta tasvirlar, soxta videolar, sun’iy intellekt, neyron tarmoqlar.*

Аннотация: *Алгоритм deepfake — это технология, позволяющая пользователю создавать изображения, аудио- и видеоматериалы, которые кажутся пользователю очень реалистичными, но на самом деле являются поддельными. Этот уровень технологий был достигнут благодаря достижениям в области глубокого обучения, машинного обучения, искусственного интеллекта и нейронных сетей. Этот процесс*

может использовать комбинацию таких алгоритмов, как генеративно-состязательные сети (GAN) и автокодировщики.

Как и любая технология, deepfake имеет как положительные, так и отрицательные стороны. С одной стороны, технология deepfake может помочь людям, потерявшим способность говорить или имеющим нарушения речи, создавать новые, улучшенные и высококачественные голоса. С другой стороны, она может улучшить качество анимации и фильмов, воплотить в жизнь творческие идеи или помочь людям, потерявшим близких, оживить их с помощью deepfake.

С другой стороны, поддельные изображения, видео- или аудиозаписи, которые выглядят слишком реалистично, могут поставить под угрозу конфиденциальность, функционирование организаций, демократию и даже национальную безопасность. В статье представлена информация об истории технологии дипфейков, принципах её работы и основных алгоритмах, используемых в ней. Также анализируются важные исследования в научной литературе, рассматриваются методы обнаружения дипфейков и эффективные превентивные меры для предотвращения негативных последствий.

Ключевые слова: *Дипфейк, GAN, автоэнкодеры, поддельные изображения, поддельные видео, искусственный интеллект, нейронные сети.*

Abstract: *The deepfake algorithm is a technology that allows the user to create images, audio and videos that seem very real to the user, but are actually fake. This level of technology has been achieved through improvements in the fields of deep learning, machine learning, artificial intelligence and neural networks. This process can use a combination of algorithms such as generative adversarial networks (GANs), autoencoders.*

Like any technology, deepfake has both positive and negative consequences. On the positive side, deepfake technology can help people who have lost their ability to speak or have speech impairments to create new, improved and high-quality voices. On the commercial side, it can improve the quality of animation and films, bring creative ideas to life, or help people who have lost loved ones to life by reviving them through deepfake.

On the downside, fake images, videos, or audio recordings that look too realistic can threaten privacy, the functioning of organizations, democracy, and even national security.

This article provides information about the history of deepfake technology, how it works, and the main algorithms used in it. It also analyzes important studies in the scientific literature, and considers methods for detecting deepfake and effective preventive measures to prevent harmful consequences.

Keywords: *Deepfake, GAN, autoencoders, fake images, fake videos, artificial intelligence, neural networks.*

KIRISH

“Deepfake” atamasi 2017-yil oxirida paydo bo‘lgan. U Reddit platformasi (foydalanuvchilarning ovoz berishi orqali veb-kontentni baholaydigan va saytlar muhokamasini yuritadigan Amerika ijtimoiy tarmog‘i)da faol bo‘lgan bir foydalanuvchi tomonidan kiritilgan. U “deepfake” nomli akkaunt orqali aslida unda ishtirok etmagan Gollivud aktrisalarini tasvirlagan hamda juda haqiqiy ko‘rinishga ega bo‘lgan pornografik videolarni joylashtirgan. Shu foydalanuvchi nomidan “deepfake” atamasi kelib chiqqan.[72]

Deepfake texnologiyasiga qiziqish ortib borayotganligi sababli, tobora ko'proq tadqiqotlar olib borilmoqda. So'nggi ikki yil ichida deepfakeni aniqlashning yangi usullarini ishlab chiqildi. Avvalo, “deepfake”ni aniqlash uchun yaratilgan texnologiyalar soni ortib bormoqda. Uni aniqlash uchun kichik ma'lumotlar to'plamlari (masalan, DeepFake-TIMIT)dan tortib, keng ko'lamli ma'lumotlar to'plamlari(masalan, FaceForensic++, DFDC va DeeperForensic)gacha yaratildi.[73] Bundan tashqari, bir nechta tadqiqot institutlari deepfake videolarining xavfidan xabardor bo'lib, tegishli tadqiqotlarni ilgari surishga harakat qilmoqdalar. Yaqinda Amazon, Facebook va Microsoft deepfake videolarini aniqlash uchun foydali bo'lgan innovatsion texnologiyalarni yaratish uchun deepfake detection challenge (DFDC) o'tkazish uchun birlashdilar.

Bu sohada erishilgan yutuqlarga qaramay, mavjud qalbakilashtirishni aniqlash uchun ko'plab muammolar hal qilinishi kerak. Bunday vaziyatda zamonaviy deepfake algoritmlari orqali yaratilgan soxta ma’lumotlar tarqalishining oldini olish uchun eskicha himoya choralari unchalik samara bermaydi. Buning uchun qalbakilashtirish bilan bog'liq tadqiqotlarni tahlil qilish muhimdir. Ushbu sharhda biz qalbakilashtirish videolarini aniqlashga harakat qilib, qalbakilashtirish videolari uchun mo'ljallangan mavjud aniqlash sxemasiga e'tibor qaratamiz.

ASOSIY QISM

Umuman olganda, deepfake’ni “chuqur neyron tarmoqlar yordamida yaratilgan ishonarli audio, vizual yoki multimedia kontenti” deb ta’riflash mumkin. Deepfake yoki yuzni manipulyatsiya qilish texnologiyalari to‘rtta asosiy turga bo‘linadi: shaxsni almashtirish

[72] https://www.realitydefender.com/insights/history-of-deepfakes
[73] Dolhansky, B., et al.: *The deepfake detection challenge dataset*. arXiv preprint arXiv:2006.07397. (2020)

(identity swap), yuz ifodasini qayta jonlantirish (face reenactment), atributlarni o‘zgartirish (attribute manipulation) hamda butunlay yangi yuz yaratish (entire face synthesis)[74]

Turli xil deepfake yoki yuz manipulyatsiyasi usullarini yaratish va aniqlash bo‘yicha ko‘plab ilmiy ishlar amalga oshirilgan. Biroq, quyidagi bo‘limlarda biz asosan o‘zining yangiligi, asosiy g‘oyasi va/yoki samaradorligi bilan ajralib turgan muhim tadqiqotlarni keltirdik. Shuningdek, deepfake yaratish va aniqlash sohasidagi eng so‘nggi yutuqlarni ifodalovchi zamonaviy tadqiqotlar ham ushbu tahlilga kiritilgan.

Shaxsni almashtirish (Identity Swap)

Bu bo‘limda mavjud yuzni almashtirish yoki shaxsni almashtirish texnologiyalarining (ya’ni, bir odamning yuzini boshqasining yuzi bilan almashtirish) yaratilish va aniqlash usullari haqida umumiy ma’lumot beriladi.

Shaxsni almashtirish texnologiyasini yaratish

Bu jarayon maqsadli rasm yoki videodagi odamning yuzini manba rasm yoki videodagi boshqa odamning yuzi bilan almashtirishdan iborat

Masalan:

- Korshunova va hamkorlari[75] konvolyutsion neyron tarmoqlar (CNN) asosida yuzni almashtirish usulini ishlab chiqishgan.
- Nirkin va boshqalar[76] esa tabiiy sharoitlarda ishlaydigan to‘liq konvolyutsion tarmoq yordamida yuzni almashtirish texnikasini taklif etishgan.
- Mahajan va hamkorlari[77] maxfiylikni himoya qilish maqsadida yuzni almashtirish usulini ishlab chiqqan.
- Wang va boshqalar[78] real vaqt rejimida ishlaydigan yuz almashtirish texnologiyasini taqdim etishgan.

Shaxsni almashtirishni aniqlash

Shaxsni almashtirish asosida yaratilgan deepfake videolarni aniqlash bo‘yicha ham ko‘plab tadqiqotlar olib borilgan.

Masalan:

[74] Juefei-Xu F., Wang R., Huang Y., Guo Q., Ma L., Liu Y. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. Int. J. Comput. Vis. 2022;130:1678–1734. doi: 10.1007/s11263-022-01606-8.
[75] Korshunova I., Shi W., Dambre J., Theis L. Fast Face-Swap Using Convolutional Neural Networks; Proceedings of the IEEE International Conference on Computer Vision (ICCV); Venice, Italy. 22–27 October 2017; pp. 3697–3705.
[76] Nirkin Y., Masi I., Tuan A.T., Hassner T., Medioni G. On Face Segmentation, Face Swapping, and Face Perception; Proceedings of the 13th IEEE International Conference on Automatic Face & Gesture Recognition; Xi’an, China. 15–19 May 2018; pp. 98–105.
[77] Mahajan S., Chen L., Tsai T. SwapItUp: A Face Swap Application for Privacy Protection; Proceedings of the IEEE 31st International Conference on Advanced Information Networking and Applications (AINA); Taipei, Taiwan. 27–29 March 2017; pp. 46–50.
[78] Wang H., Dongliang X., Wei L. Robust and Real-Time Face Swapping Based on Face Segmentation and CANDIDE-3; Proceedings of the PRICAI 2018: Trends in Artificial Intelligence; Nanjing, China. 28–31 August 2018; pp. 335–342.

- Koopman va hamkorlari[79] tasvirdagi rasmning nomuvofiqligi orqali aniqlash usulini taklif etishgan.

Yaqinda esa S. Liu va hamkorlari[80] bloklarni aralashtirib o‘rganish (block shuffling learning) usulini taklif etishgan. Ushbu yondashuvda tasvir bir nechta bloklarga bo‘linadi, ular tasodifiy tartibda aralashtiriladi va har bir blok ichidagi hamda bloklar orasidagi belgilarga asoslanib deepfake aniqlanadi.

Yuz ifodasini qayta jonlantirish (Face Reenactment)

Ushbu bo‘limda *yuz ifodasini o‘zgartirish* yoki *ifodani qayta jonlantirish* (ya’ni, bir odamning yuz ifodasini boshqa bir odamning ifodasi bilan almashtirish) texnologiyalarining yaratilishi va aniqlash usullari haqida umumiy ma’lumot beriladi.

Yuz ifodasini qayta jonlantirish texnologiyasini yaratish

Bu jarayon rasm yoki videodagi odamning yuz ifodasini, mo’ljallangan rasm yoki videodagi odamning yuziga ko‘chirishdan iborat.[81] Boshqacha aytganda, bu ifoda almashtirish deb ham ataladi.

Masalan:

- Thies va hamkorlari[82] real vaqt rejimida ishlaydigan yuz ifodasini qayta jonlantirish tizimini yaratishgan.
- Kim va boshqalar[83] enkoder-dekoder arxitekturasiga asoslangan modelni ishlab chiqqan.
- Nirkin va hamkorlari[84] RNN yordamida yuz ifodasini o‘zgartirish usulini taklif etishgan.
- Doukas va hamkorlari[85] GAN (Generative Adversarial Network) asosida ishlovchi tizimni ishlab chiqqan.

Yuz ifodasini qayta jonlantirishni aniqlash

Yuz ifodasini o‘zgartirish orqali yaratilgan deepfake’larni aniqlash uchun ham turli usullar ishlab chiqilgan.

---

[8]Liu S., Lian Z., Gu S., Xiao L. Block shuffling learning for Deepfake Detection. arXiv. 20222202.02819

[81] Juefei-Xu F., Wang R., Huang Y., Guo Q., Ma L., Liu Y. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. Int. J. Comput. Vis. 2022;130:1678–1734. doi: 10.1007/s11263-022-01606-8.

[82] Thies J., Zollhofer M., Stamminger M., Theobalt C., Nießner M. Face2face: Real-time face capture and reenactment of RGB videos; Proceedings of the IEEE conference on computer vision and pattern recognition; Las Vegas, NV, USA. 27–30 June 2016; pp. 2387–2395.

[83] Kim H., Garrido P., Tewari A., Xu W., Thies J., Niessner M., Pérez P., Richardt C., Zollhofer M., Theobalt C. Deep video portraits. ACM Trans. Graph. (TOG) 2018;37:1–4. doi: 10.1145/3197517.3201283.

[84] Nirkin Y., Keller Y., Hassner T. FSGAN: Subject agnostic face swapping and reenactment; Proceedings of the IEEE/CVF International Conference on Computer Vision; Seoul, Korea. 27 October–2 November 2019; pp. 7184–7193.

[85] Doukas M., Koujan M., Sharmanska V., Roussos A., Zafeiriou S. Head2Head++: Deep Facial Attributes Re-Targeting. IEEE Trans. Biom. Behav. Identity Sci. 2021;3:31–43. doi: 10.1109/TBIOM.2021.3049576.

Masalan:

- Cozzolino va hamkorlari [86] CNN asosida aniqlash modelini yaratishgan.
- Matern va boshqalar[87] tasviriy belgilar (visual features) asosida logistik regressiya usullaridan foydalangan.
- Sabir va boshqalar[88] RNN yordamida vaqt ketma-ketligidagi o‘zgarishlarni tahlil qilish orqali aniqlash usulini ishlab chiqishgan.
- Amerini va boshqalar [89] optik oqim (Optical Flow) va CNN ni birlashtirgan yondashuvni taklif etishgan.
- Wang va boshqalar[90] esa 3D CNN asosidagi modelni ishlab chiqqan.

Bundan farqli ravishda, Zhao va hamkorlari[91] fazoviy-vaqtli tarmoq (spatiotemporal network) ishlab chiqqan bo‘lib, u global va mahalliy ma’lumotlarni birgalikda tahlil qilish imkonini beradi.

Yuzdagi belgilarni o‘zgartirish (Attribute Manipulation)

Bu bo‘limda yuz atributlarini o‘zgartirish, ya’ni yuzni tahrirlash texnologiyalari haqida so‘z boradi. Bunda insonning ayrim tashqi belgilarini — masalan, teri rangi, yoshi, jinsi, yoki soch rangini o‘zgartirish orqali yangi tasvir yoki video yaratiladi.

Yuz atributlarini o‘zgartirish texnologiyasi

Ushbu usulda inson yuzining ayrim xususiyatlari, masalan soch yoki teri rangi, yosh, jins, yoki ko‘zoynak qo‘shish kabi belgilar tahrirlanadi [95,96,97]. Bunday jarayon ko‘pincha yuzni tahrirlash (face editing) deb ham ataladi.

Masalan:

- Xiao va hamkorlari [98] bir vaqtning o‘zida bir nechta atributlarni o‘zgartira oladigan ko‘p atributli GAN tizimini ishlab chiqqan.

---

[86] Cozzolino D., Thies J., Rossler A., Riess C., Niener M., Verdoliva L. Forensictransfer: Weakly-supervised domain adaptation for forgery detection. arXiv. 20181812.02510

[87] Matern F., Riess C., Stamminger M. Exploiting Visual Artifacts to Expose DeepFakes and Face Manipulations; Proceedings of the IEEE Winter Applications of Computer Vision Workshops; Waikoloa Village, HI, USA. 7–11 January 2019; pp. 1–10.

[88] Sabir E., Cheng J., Jaiswal A., AbdAlmageed W., Masi I., Natarajan P. Recurrent Convolutional Strategies for Face Manipulation Detection in Videos; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops; Long Beach, CA, USA. 16–17 June 2019; pp. 1–8.

[89] Amerini I., Galteri L., Caldelli R., Del Bimbo A. Deepfake Video Detection through Optical Flow Based CNN; Proceedings of the IEEE/CVF International Conference on Computer Vision Workshop (ICCVW); Seoul, Republic of Korea. 27–28 October 2019; pp. 1205–1207.

[90] Wang Y., Dantcheva A. A video is worth more than 1000 lies. Comparing 3DCNN approaches for detecting deepfakes; Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG); Virtual. 16–20 November 2020; pp. 515–519.

[91] Zhao X., Yu Y., Ni R., Zhao Y. Exploring Complementarity of Global and Local Spatiotemporal Information for Fake Face Video Detection; Proceedings of the 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); Singapore. 22–27 May 2022; pp. 2884–2888.

- Shuningdek, boshqa tadqiqotchilar tomonidan quyidagi yondashuvlar ham taklif etilgan:
  - VAE (variational autoencoder) va GAN kombinatsiyasi [100];
  - geometriyaga asoslangan GAN (geometry-aware GAN) [102];
  - niqob bilan bog’liq GAN (mask-guided GAN) [103];
  - 3D yuz modeli [104];

Bu texnologiyalar inson yuzidagi tabiiylikni saqlagan holda uning ko‘rinishini deyarli sezilmaydigan darajada o‘zgartirish imkonini beradi.

Atributlarni o‘zgartirishni aniqlash

Yuzdagi atributlar o‘zgartirilganini aniqlash ham so‘nggi yillarda tadqiqotchilar e’tiborida.

Masalan:

- Bharati va hamkorlari [92] Deep Boltzmann Machine asosida aniqlash modelini yaratishgan.
- Dang va boshqalar[93] CNN yordamida yuzdagi o‘zgarishlarni aniqlashgan.
- Kim va hamkorlari[94] yuz qirralariga (facial boundaries) asoslangan xususiyatlarni tahlil qilish orqali aniqlashgan.

Bunday usullar inson yuzida tabiiylikdan chetga chiqqan nozik o‘zgarishlarni aniqlab, surat yoki videoning sun’iy yaratilganini fosh etishga yordam beradi.

Butunlay yangi yuz yaratish (Entire Face Synthesis)

Ushbu bo‘limda to‘liq yuz yaratish, ya’ni mavjud bo‘lmagan inson yuzlarini sun’iy tarzda yaratish texnologiyalari hamda ularni aniqlash usullari haqida umumiy ma’lumot beriladi.

To‘liq yuz yaratish texnologiyasi

Bu yo‘nalishning maqsadi — haqiqiy bo‘lmagan, ammo juda ishonarli ko‘rinadigan inson yuzlarini yaratishdir

- Berthelot va hamkorlari[95] bu maqsadda Boundary Equilibrium GAN (BEGAN) modelini ishlab chiqishgan. Ushbu model yordamida yuqori sifatli, tabiiyga juda o‘xshash sun’iy yuzlar yaratilgan.

[92] Bharati A., Singh R., Vatsa M., Bowyer K. Detecting facial retouching using supervised deep learning. IEEE Trans. Inf. Secur. 2016;11:1903–1913. doi: 10.1109/TIFS.2016.2561898.
[93] Dang L.M., Hassan S.I., Im S., Moon H. Face image manipulation detection based on a convolutional neural network. Expert Syst. Appl. 2019;129:156–168. doi: 10.1016/j.eswa.2019.04.005.
[94] Kim D., Kim D., Kim K. Facial Manipulation Detection Based on the Color Distribution Analysis in Edge Region. arXiv. 20212102.01381
[95] Berthelot D., Schumm T., Metz L. Began: Boundary equilibrium generative adversarial networks. arXiv. 20171703.10717

- Shuningdek, yuz generatsiyasi bo‘yicha boshqa samarali yondashuvlar ham ishlab chiqilgan, jumladan:
  - ikkitalik juft GANlar (coupled GANs)[96]
  - U-Net arxitekturasi asosidagi modellar[97]
  - nutqdan yuz yaratish GAN’lari (speech-to-face GANs)[98]

Bu texnologiyalar yordamida butunlay yangi, real hayotda mavjud bo‘lmagan, ammo haqiqiy odamga juda o‘xshash yuz tasvirlarini yaratish mumkin bo‘ladi.

To‘liq yuz yaratishni aniqlash

To‘liq sun’iy yaratilgan yuzlarni aniqlash ham so‘nggi yillarda muhim tadqiqot yo‘nalishiga aylangan.

Masalan:

- McCloskey va hamkorlari [124] rangga asoslangan tahlil tizimi yordamida aniqlash usulini taklif etishgan.
- Boshqa ishlarda esa quyidagi texnikalar qo‘llanilgan:
  - GAN izlari (fingerprints) va CNN kombinatsiyasi [99]
  - PRNU (Photo Response Non-Uniformity) tahlili[100]
  - hamda o‘z-o‘ziga e’tibor mexanizmi (self-attention mechanism)[101]

Shuningdek, Guo va hamkorlari tadqiqotida shuni aniqlashgan: GAN yordamida yaratilgan yuzlarda ko‘z qorachig‘ining shakli ko‘pincha tabiiy bo‘lmaydi. Bu fiziologik cheklovlarning yo‘qligi sababli yuzaga keladi va aynan shu belgilar orqali sun’iy yaratilgan aniqlash mumkin.

XULOSA

AI yordamida yaratilgan yoki raqamli tarzda o‘zgartirilgan yuz tasvirlari, odatda DeepFake deb ataladi, va ular yuzni aniqlash tizimlarining ishonchliligiga hamda internetdagi ma’lumotlarning yaxlitligiga jiddiy tahdid soladi. Ushbu maqola deepfake va

[96] Liu M., Tuzel O. Coupled generative adversarial networks; Proceedings of the Advances in Neural Information Processing Systems 29 (NIPS 2016); Barcelona, Spain. 5–10 December 2016; pp. 469–477.
[97] Schonfeld E., Schiele B., Khoreva A. A u-net based discriminator for generative adversarial networks; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; Seattle, WA, USA. 13–19 June 2020; pp. 8207–8216.
[98] Choi H., Park C., Lee K. From inference to generation: End-to-end fully self-supervised generation of human face from speech. arXiv. 20202004.05830
[99] Yu N., Davis L., Fritz M. Attributing fake images to gans: Learning and analyzing gan fingerprints; Proceedings of the IEEE/CVF International Conference on Computer Vision; Seoul, Republic of Korea. 27 Octover–2 November 2019; pp. 7556–7566.
[100] Marra F., Gragnaniello D., Verdoliva L., Poggi G. Do GANs leave artificial fingerprints?; Proceedings of the IEEE Conference on Multimedia Information Processing and Retrieval (MIPR); San Jose, CA, USA. 28–30 March 2019; pp. 506–511.
[101] Li S., Dutta V., He X., Matsumaru T. Deep Learning Based One-Class Detection System for Fake Faces Generated by GAN Network. Sensors. 2022;22:7767. doi: 10.3390/s22207767.

yuzni manipulyatsiya qilish texnologiyalarining yaratilishi va aniqlanishi bo‘yicha so‘nggi yutuqlarni ko‘rib chiqdi.

Garchi bu sohada sezilarli yutuqlar mavjud bo‘lsa-da, yuksak samarali va keng qamrovli yaratuvchanlik hamda himoya usullarini ishlab chiqish uchun hali hal qilinishi kerak bo‘lgan bir qator muammolar mavjud. Shu bois, maqolada ochiq qolgani muammolar va tadqiqot imkoniyatlari muhokama qilingan.

Deepfake sohasida ishonchli aniqlash tizimlarini yaratish yo‘lida hali uzoq yo‘l bor va buni amalga oshirish uchun mashina o‘rganish, kompyuter ko‘rishi, inson vizual tizimi, psixofiziologiya kabi turli sohalarda tadqiqotlar zarur bo‘ladi.

Umuman olganda, ushbu maqola deepfake yaratish va aniqlash bo‘yicha yangi AI algoritmlarini ishlab chiqishda asosiy manba sifatida xizmat qilishi mumkin. Shuningdek, ushbu sharh ilmiy izlanuvchilar, amaliyotchilar, tadqiqotchilar va muhandislarni deepfake sohasini o‘rganishga ilhomlantiradi deb umid qilaman.

Foydalanilgan Adabiyotlar

1. https://www.realitydefender.com/insights/history-of-deepfakes

2.Dolhansky, B., et al.: The deepfake detection challenge dataset. arXiv preprint arXiv:2006.07397. (2020)

3.Juefei-Xu F., Wang R., Huang Y., Guo Q., Ma L., Liu Y. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. Int. J. Comput. Vis. 2022;130:1678–1734. doi: 10.1007/s11263-022-01606-8.

4.Korshunova I., Shi W., Dambre J., Theis L. Fast Face-Swap Using Convolutional Neural Networks; Proceedings of the IEEE International Conference on Computer Vision (ICCV); Venice, Italy. 22–27 October 2017; pp. 3697–3705.

5.Nirkin Y., Masi I., Tuan A.T., Hassner T., Medioni G. On Face Segmentation, Face Swapping, and Face Perception; Proceedings of the 13th IEEE International Conference on Automatic Face & Gesture Recognition; Xi’an, China. 15–19 May 2018; pp. 98–105.

6.Mahajan S., Chen L., Tsai T. SwapItUp: A Face Swap Application for Privacy Protection; Proceedings of the IEEE 31st International Conference on Advanced Information Networking and Applications (AINA); Taipei, Taiwan. 27–29 March 2017; pp. 46–50.

7.Wang H., Dongliang X., Wei L. Robust and Real-Time Face Swapping Based on Face Segmentation and CANDIDE-3; Proceedings of the PRICAI 2018: Trends in Artificial Intelligence; Nanjing, China. 28–31 August 2018; pp. 335–342.

8.Liu S., Lian Z., Gu S., Xiao L. Block shuffling learning for Deepfake Detection. arXiv. 20222202.02819

9. Juefei-Xu F., Wang R., Huang Y., Guo Q., Ma L., Liu Y. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. Int. J. Comput. Vis. 2022;130:1678–1734. doi: 10.1007/s11263-022-01606-8.

10.Thies J., Zollhofer M., Stamminger M., Theobalt C., Nießner M. Face2face: Real-time face capture and reenactment of RGB videos; Proceedings of the IEEE conference on computer vision and pattern recognition; Las Vegas, NV, USA. 27–30 June 2016; pp. 2387–2395.

11. Kim H., Garrido P., Tewari A., Xu W., Thies J., Niessner M., Pérez P., Richardt C., Zollhofer M., Theobalt C. Deep video portraits. ACM Trans. Graph. (TOG) 2018;37:1–4. doi: 10.1145/3197517.3201283.

12. Nirkin Y., Keller Y., Hassner T. FSGAN: Subject agnostic face swapping and reenactment; Proceedings of the IEEE/CVF International Conference on Computer Vision; Seoul, Korea. 27 October–2 November 2019; pp. 7184–7193.

13. Doukas M., Koujan M., Sharmanska V., Roussos A., Zafeiriou S. Head2Head++: Deep Facial Attributes Re-Targeting. IEEE Trans. Biom. Behav. Identity Sci. 2021;3:31–43. doi: 10.1109/TBIOM.2021.3049576.

14. Cozzolino D., Thies J., Rossler A., Riess C., Nienerr M., Verdoliva L. Forensictransfer: Weakly-supervised domain adaptation for forgery detection. arXiv. 20181812.02510

15. Matern F., Riess C., Stamminger M. Exploiting Visual Artifacts to Expose DeepFakes and Face Manipulations; Proceedings of the IEEE Winter Applications of Computer Vision Workshops; Waikoloa Village, HI, USA. 7–11 January 2019; pp. 1–10.

16. Sabir E., Cheng J., Jaiswal A., AbdAlmageed W., Masi I., Natarajan P. Recurrent Convolutional Strategies for Face Manipulation Detection in Videos; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops; Long Beach, CA, USA. 16–17 June 2019; pp. 1–8.

17. Amerini I., Galteri L., Caldelli R., Del Bimbo A. Deepfake Video Detection through Optical Flow Based CNN; Proceedings of the IEEE/CVF International Conference on Computer Vision Workshop (ICCVW); Seoul, Republic of Korea. 27–28 October 2019; pp. 1205–1207.

18. Wang Y., Dantcheva A. A video is worth more than 1000 lies. Comparing 3DCNN approaches for detecting deepfakes; Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG); Virtual. 16–20 November 2020; pp. 515–519.

19. Zhao X., Yu Y., Ni R., Zhao Y. Exploring Complementarity of Global and Local Spatiotemporal Information for Fake Face Video Detection; Proceedings of the 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); Singapore. 22–27 May 2022; pp. 2884–2888.

20. Bharati A., Singh R., Vatsa M., Bowyer K. Detecting facial retouching using supervised deep learning. IEEE Trans. Inf. Secur. 2016;11:1903–1913. doi: 10.1109/TIFS.2016.2561898.

21. Dang L.M., Hassan S.I., Im S., Moon H. Face image manipulation detection based on a convolutional neural network. Expert Syst. Appl. 2019;129:156–168. doi: 10.1016/j.eswa.2019.04.005.

22.Kim D., Kim D., Kim K. Facial Manipulation Detection Based on the Color Distribution Analysis in Edge Region. arXiv. 20212102.01381

23. Berthelot D., Schumm T., Metz L. Began: Boundary equilibrium generative adversarial networks. arXiv. 20171703.10717

24. Liu M., Tuzel O. Coupled generative adversarial networks; Proceedings of the Advances in Neural Information Processing Systems 29 (NIPS 2016); Barcelona, Spain. 5–10 December 2016; pp. 469–477.

25.Schonfeld E., Schiele B., Khoreva A. A u-net based discriminator for generative adversarial networks; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; Seattle, WA, USA. 13–19 June 2020; pp. 8207–8216.

26. Choi H., Park C., Lee K. From inference to generation: End-to-end fully self-supervised generation of human face from speech. arXiv. 20202004.05830

27. Yu N., Davis L., Fritz M. Attributing fake images to gans: Learning and analyzing gan fingerprints; Proceedings of the IEEE/CVF International Conference on Computer Vision; Seoul, Republic of Korea. 27 Octover–2 November 2019; pp. 7556–7566.

28. Marra F., Gragnaniello D., Verdoliva L., Poggi G. Do GANs leave artificial fingerprints?; Proceedings of the IEEE Conference on Multimedia Information Processing and Retrieval (MIPR); San Jose, CA, USA. 28–30 March 2019; pp. 506–511.