SUN’IY INTELLEKT ORQALI HOSIL QILINGAN OVOZLARNI ANIQLASH VA KIBERTAHDIDLARNI BARTARAF QILISH USUL VA ALGORITMLARI

Abdazimov Saidaminxo‘ja Zoirxo‘ja o‘g‘li
O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi o‘qituvchisi;
Djamatov Mustafa Xatamovich
O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi;

Annotatsiya: *Ushbu maqolada sun’iy intellekt texnologiyalari yordamida yaratilgan sintetik ovozlarni aniqlash va ularga qarshi kurashish usullari hamda algoritmlari batafsil ko‘rib chiqiladi. Maqolada akustik tahlil, mashina o‘qitish va chuqur o‘rganish metodlari asosida ishlaydigan aniqlash tizimlari tahlil qilinib, ularning afzalliklari va kamchiliklari muhokama qilinadi. Bundan tashqari, real vaqt rejimida ishlash imkoniyatlari, ma’lumotlar bazalarining ahamiyati va kelajakdagi tadqiqot yo‘nalishlari ham yoritiladi.*

Kalit so‘zlar: *Sun’iy intellekt, sintetik ovoz, deepfake, kiberxavfsizlik, ovozni aniqlash, mashina o‘qitish, chuqur o‘rganish, akustik tahlil, kibertahdid.*

Аннотация: *В данной статье подробно рассматриваются методы и алгоритмы обнаружения синтетических голосов, созданных с помощью технологий искусственного интеллекта, а также способы противодействия им. Анализируются системы обнаружения, основанные на акустическом анализе, машинном обучении и методах глубокого обучения, обсуждаются их преимущества и недостатки. Кроме того, освещаются возможности работы в режиме реального времени, значимость баз данных и перспективные направления будущих исследований.*

Ключевые слова: *Искусственный интеллект, синтетический голос, дипфейк, кибербезопасность, распознавание голоса, машинное обучение, глубокое обучение, акустический анализ, киберугроза.*

Abstract: *This article provides a detailed examination of methods and algorithms for detecting and countering synthetic voices generated through artificial intelligence technologies. Detection systems based on acoustic analysis, machine learning, and deep learning approaches are analyzed, with their advantages and limitations discussed. Furthermore, the possibilities of real-time operation, the significance of datasets, and future research directions are also explored.*

Keywords: *Artificial intelligence, synthetic voice, deepfake, cybersecurity, voice detection, machine learning, deep learning, acoustic analysis, cyber threat.*

KIRISH

Raqamli texnologiyalarning jadal rivojlanishi insoniyatga ko‘plab imkoniyatlar ochib bermoqda. Biroq, ushbu rivojlanish bilan birga yangi va murakkab xavf-xatarlar

ham paydo bo‘lmoqda. Xususan, sun’iy intellekt (SI) texnologiyalari asosidagi ovoz sintezi tizimlari — “deepfake ovoz” deb ham ataluvchi bu texnologiya — hozirgi kunda kiberjinoylarda faol qo‘llanilmoqda. Firibgarlar real insonlarning ovozini taqlid qiluvchi sintetik ovozlar yaratib, bank hisoblarini bo‘shatish, maxfiy ma’lumotlarni o‘g‘irlash va siyosiy manipulyatsiya kabi jinoyatlarni amalga oshirmoqdalar.

2024-yilda Evropa Ittifoqida amalga oshirilgan tadqiqotlar shuni ko‘rsatdiki, deepfake texnologiyalari bilan bog‘liq moliyaviy zararlar yillik 25 milliard dollardan oshib ketgan. O‘zbekistonda ham raqamlashtirish jarayoni jadallashib borayotganligi sababli, bunday tahdidlardan himoyalanish dolzarb masalaga aylanmoqda. Shu bois, sintetik ovozlarni aniqlash va kibertahdidlarni bostirish usullari va algoritmlarini chuqur o‘rganish nafaqat ilmiy, balki amaliy jihatdan ham muhim ahamiyat kasb etadi.

Mazkur maqolaning maqsadi — sintetik ovozlarni aniqlashda qo‘llaniladigan zamonaviy usullar va algoritmlarni tizimli ravishda tahlil qilish, ularning samaradorligini baholash va kiberxavfsizlikni ta’minlashda amaliy tavsiyalar ishlab chiqishdan iborat.

Sintetik ovoz texnologiyasi va uning xavflari

Sintetik ovozning yaratilish usullari

Sun’iy intellekt yordamida ovoz sintezi bir necha asosiy yo‘nalishlar bo‘yicha amalga oshiriladi. Birinchi yo‘nalish — Matn-dan-Ovozga (Text-to-Speech, TTS) texnologiyasi bo‘lib, u yozma matnni tabiiy eshitiluvchi ovozga aylantiradi. WaveNet, Tacotron, FastSpeech kabi neyron tarmoq modellari bu sohadagi eng ilg‘or yechimlardir. Ikkinchi yo‘nalish — Ovozni o‘zgartirish (Voice Conversion, VC) texnologiyasi bo‘lib, bir kishining ovozini boshqa kishining ovoziga o‘xshash tarzda o‘zgartiradi. Bu usul ayniqsa firibgarlikda keng qo‘llanilmoqda, chunki haqiqiy insonning ovozini taqlid qilish imkonini beradi.

Uchinchi yo‘nalish — Generativ- Adversarial Tarmoqlar (Generative Adversarial Networks, GAN) asosidagi ovoz sintezi hisoblanadi. GAN texnologiyasida ikkita neyron tarmoq — generator va diskriminator — bir-biri bilan raqobatlashib, tobora haqiqiyroq ovozlar yaratishga erishadi. So‘nggi yillarda diffuzion modellar (Diffusion Models) ham ovoz sintezida keng qo‘llanila boshlandi, bu esa sintetik ovozlarning sifatini yanada oshirib, ularni inson qulogi bilan farqlashni deyarli imkonsiz qildi.

Sintetik ovozlar keltirib chiqaradigan kibertahdidlar

Sintetik ovozlar asosidagi kibertahdidlar bir necha asosiy kategoriyalarga bo‘linadi. Birinchisi — moliyaviy firibgarlik bo‘lib, jinoyatchilar rahbar yoki qarindoshlarning ovozini taqlid qilib, qurbonlarni pul o‘tkazishga majbur qiladi. “Vishing” (Voice Phishing) hujumlari bu kategoriyaning eng keng tarqalgan turidir. Ikkinchisi — shaxsiy obro‘ga zarar yetkazish, ya‘ni siyosatchilar, jamoat arboblari yoki oddiy fuqarolarning deepfake ovozli yozuvlarini yaratib, ularni noqulay vaziyatga qo‘yish. Uchinchisi — korporativ josuslik bo‘lib, kompaniyalar rahbarlarining ovozini taqlid qilib, konfidensial ma’lumotlarni olish yoki noto‘g‘ri buyruqlar berish.

Sintetik ovozlarni aniqlash usullari

Akustik tahlil usullari

Akustik tahlil usullari ovozning fizik xususiyatlarini o‘rganishga asoslanadi. Mel-chastota kepstral koeffitsientlari (MFCC — Mel-Frequency Cepstral Coefficients) bu sohadagi asosiy vosita bo‘lib, ular ovozning chastota spektrini qisqa vaqt oraliqlarida tahlil qiladi. Haqiqiy inson ovozi va sintetik ovoz o‘rtasidagi tafovutlar MFCC tahlili orqali aniqlanishi mumkin, chunki sintetik ovozlarda ba’zi akustik xususiyatlar sun’iy ravishda yaratilganligi sababli noodatiy parametrlar namoyon bo‘ladi.

Linear Predictive Coding (LPC) tahlili ovoz traktining matematik modelini qurib, undagi g‘ayritabiiy ko‘rsatkichlarni aniqlashga yordam beradi. Prosodik xususiyatlar tahlili — intonatsiya, ritm, urg‘u va pauza naqshlari ham sintetik ovozlarni aniqlashda muhim rol o‘ynaydi. Sintetik ovozlarda prosodik xususiyatlar odatda bir xil va mexanik tarzda bo‘lib, tabiiy nutqdagi spontan o‘zgarishlar ularda kamroq uchraydi.

Mashina o‘qitish asosidagi usullar

Klassik mashina o‘qitish (Machine Learning, ML) algoritmlari sintetik ovozlarni aniqlashda samarali qo‘llanilmoqda. Support Vector Machine (SVM) algoritmi ikkilik klassifikatsiya muammosi sifatida haqiqiy va sintetik ovozlarni ajratishda yuqori aniqlik ko‘rsatadi. Random Forest va Gradient Boosting algoritmlari esa ko‘plab akustik xususiyatlarni birgalikda tahlil qilib, yanada ishonchli natijalar beradi. K-eng yaqin qo‘shni (K-Nearest Neighbors, KNN) algoritmi esa o‘xshash ovoz namunalari bilan solishtirish orqali aniqlash amalga oshiradi.

Gaussian Mixture Model (GMM) probabilistik modeli ovoz parametrlarining statistik taqsimotini tahlil qilib, noodatiy namunalarni aniqlaydi. Bu algoritmlar nisbatan kam hisoblash resurslari talab qilganligi sababli real vaqt tizimlarida ham qo‘llanilishi mumkin. Biroq, ular chuqur o‘rganish usullariga qaraganda yangi turlardagi sintetik ovozlarni aniqlashda kamroq samarali bo‘lishi mumkin.

Chuqur o‘rganish (Deep Learning) algoritmlari

Chuqur o‘rganish usullari zamonaviy sintetik ovozlarni aniqlashda eng yuqori samaradorlikni ko‘rsatmoqda. Konvolyutsion neyron tarmoqlar (CNN) ovozning spektrogram tasvirlarini tahlil qilib, haqiqiy va sintetik ovozlar o‘rtasidagi nozik farqlarni aniqlay oladi. Resurslar jihatidan samarali bo‘lgan ResNet va VGG arxitekturalari bu sohadagi eng keng qo‘llaniladigan modellar qatoriga kiradi.

Rekurrent neyron tarmoqlar (RNN) va uning takomillashtirilgan shakli LSTM (Long Short-Term Memory) vaqtga bog‘liq ovoz ketma-ketliklarini tahlil qilishda ustunlikka ega. Bu tarmoqlar nutqdagi uzoq muddatli bog‘liqliklarni o‘rganib, sintetik ovozlardagi noodatiy ketma-ketliklarni aniqlaydi. Transformer arxitekturasi va o‘z-o‘ziga diqqat (Self-Attention) mexanizmi so‘nggi yillarda ovozni aniqlashda inqilobiy natijalar ko‘rsatmoqda. Wav2Vec, HuBERT kabi o‘z-o‘zini o‘rgatuvchi modellar katta hajmdagi belgilangan ma’lumotlarsiz ham yuqori aniqlikka erishmoqda.

Kiberxavfsizlikda qollaniladigan algoritmlar va tizimlar

End-to-End aniqlash tizimlari

End-to-end (uchidan uchigacha) aniqlash tizimlari ovoz signalini bevosita qayta ishlab, haqiqiy yoki sintetik ekanligini aniqlaydi. RawNet2 modeli ovoz to‘lqinini to‘g‘ridan-to‘g‘ri tahlil qilib, qo‘shimcha xususiyat ajratish bosqichisiz yuqori aniqlikka erishadi. AASIST (Audio Anti-Spoofing using Integrated Spectro-Temporal Graph Attention Networks) modeli chastota va vaqt o‘lchamlarini birgalikda tahlil qiluvchi grafik diqqat mexanizmini qo‘llaydi. Bu tizim ASVspoof 2021 musobaqasida eng yuqori natijalardan birini ko‘rsatdi.

Real vaqt rejimida aniqlash algoritmlari

Telefon qo‘ng‘iroqlari va onlayn kommunikatsiyada real vaqt rejimida aniqlash tizimlari katta ahamiyat kasb etadi. Streaming qayta ishlash algoritmlari ovoz oqimini kichik bo‘laklarga bo‘lib, har birini tezkor tahlil qiladi. Kechikishni kamaytirish uchun engil tarmoq arxitekturalari (MobileNet, SqueezeNet) va model siqish texnologiyalari (Quantization, Pruning) qo‘llaniladi.

Edge Computing yondashuvi esa tahlilni markaziy serverga yubormasdan, foydalanuvchi qurilmasida amalga oshirish imkonini beradi. Bu nafaqat kechikishni kamaytiradi, balki maxfiylikni ham ta‘minlaydi. Apple, Google

va boshqa kompaniyalar o‘zlarining qurilmalariga shunday mahalliy aniqlash tizimlarini joriy etishni boshladilar.

Ko‘p modal aniqlash tizimlari

Faqat ovozni tahlil qilish bilan cheklanmasdan, ko‘p modal (multimodal) yondashuv yanada ishonchli natijalar beradi. Video qo‘ng‘iroqlarida ovoz va lab harakatlari o‘rtasidagi muvofiqlik tahlili sintetik ovozlarni aniqlashda qo‘shimcha mezon bo‘lib xizmat qiladi. Kontekst tahlili — suhbatning mohiyati, so‘ralayotgan ma’lumot yoki buyruqning g‘ayritabiiy bo‘lishi — ham shubhali holatlarni aniqlashda yordam beradi. Foydalanuvchi xulq-atvorini tahlil qilish (User Behavior Analytics) esa odatiy kommunikatsiya naqshlaridan chetlanishlarni belgilaydi.

Kibertahdidlarni bartaraf qilish strategiyalari

Texnik himoya choralari

Texnik himoya choralari bir necha darajani o‘z ichiga oladi. Birinchi daraja — ovozni autentifikatsiya qilish tizimi (Voice Authentication) bo‘lib, har bir foydalanuvchining noyob ovoz barmoq izi (voice fingerprint) ma’lumotlar bazasida saqlanadi va kiruvchi ovozlar shu baza bilan taqqoslanadi. Ikkinchi daraja — kriptografik imzolash, ya’ni ovoz yozuvlariga raqamli imzo qo‘yish orqali ularning haqiqiyligini kafolatlash. Bu usul ayniqsa yuridik ahamiyatga ega yozuvlar uchun muhimdir.

Suv belgi (Watermark) texnologiyasi ovoz fayllariga ko‘zga ko‘rinmas identifikator qo‘shib, ularning kelib chiqishini kuzatish imkonini beradi. Adobe

va Microsoft kabi kompaniyalar Content Credentials (tarkib haqiqiyligi) standartini ishlab chiqmoqda, bu esa media kontentning butun hayot tsiklini kuzatib borish imkonini beradi. Anomaliya aniqlash tizimlari (Anomaly Detection) esa tarmoq trafigi va ovoz almashinuvlarida g‘ayritabiiy naqshlarni real vaqtda aniqlaydi.

Huquqiy va me’yoriy asoslar

Texnik choralar bilan birga, huquqiy mexanizmlar ham kiberxavfsizlikni ta’minlashda muhim rol o‘ynaydi. Evropa Ittifoqining Sun’iy Intellekt Aktiga

(EU AI Act) binoan, sintetik media kontentni yaratuvchi tizimlar haqiqiy

va sintetik kontentni aniq belgilash majburiyatiga ega. Bir qator mamlakatlar deepfake yaratish va tarqatishni jinoiy javobgarlik bilan ta’minlashga qaratilgan qonunlar qabul qilmoqda.

O‘zbekiston Respublikasida ham kiberjinoyatchilikka qarshi qonunchilik bazasi takomillashtirilmoqda. Xalqaro hamkorlik, ayniqsa INTERPOL va Europol kabi tashkilotlar bilan birgalikdagi ish kiberjinoyatchilarni ta’qib qilishda samarali natijalar bermoqda.

Aholi savodxonligini oshirish

Texnik va huquqiy choralar qanchalik mukammal bo‘lmasin, aholi o‘rtasida raqamli savodxonlikni oshirmasdan turib, kibertahdidlarga to‘liq bardosh berish qiyin. Fuqarolarni deepfake texnologiyalari, ularning belgilari va o‘zini himoya qilish usullari haqida xabardor qilish zarur. Shubhali ovoz qo‘ng‘iroqlarini qanday aniqlash, bank yoki boshqa tashkilotlar nomidan kelgan g‘ayritabiiy so‘rovlarga qanday munosabat bildirish — bular haqidagi bilimlar kiberhujumlarga qarshi eng birinchi mudofaa chizig‘ini tashkil etadi.

Kelajakdagi tadqiqot yonalishlari va muammolar

Sintetik ovozlarni aniqlash sohasida bir qator dolzarb muammolar

va kelajakdagi tadqiqot yo‘nalishlari mavjud. Birinchi muammo — yangi aniqlash usuli ishlab chiqilishi bilan sintetik ovoz yaratuvchilar ham o‘z algoritmlarini yangilaydilar. Bu muammoni hal etishda generalizatsiya qobiliyati yuqori bo‘lgan, yangi turlardagi sintetik ovozlarga ham moslasha oladigan modellar yaratish talab etiladi.

Ikkinchi muammo — belgilangan ma’lumotlarning yetishmasligi. Aniqlash modellarini o‘qitish uchun katta hajmdagi real va sintetik ovoz namunalari kerak, ammo bu ma’lumotlarni yig‘ish va belgilash qimmat va vaqt talab qiladi. Few-shot va Zero-shot learning yondashuvlari bu muammoni qisman hal qilishi mumkin. Uchinchi muammo — tarjimalararo va ekologik barqarorlik, ya’ni modellarning turli til, lahjalar, shovqin sharoitlari va yozuv qurilmalarida ham yuqori aniqlikni saqlab qolishi.

Kelajakda Federated Learning (Federativ o‘rganish) texnologiyasi katta imkoniyatlar ochishi kutilmoqda. Bu yondashuv turli tashkilotlarga ma’lumotlarini ulashmagan holda birgalikda model o‘qitish imkonini beradi, bu esa maxfiylik

va xavfsizlik talablarini qondirib, ko‘proq ma’lumotdan foydalanish imkonini beradi. Shuningdek, Explainable AI (XAI) — tushuntiriladigan sun’iy intellekt — aniqlash qarorlarini shaffof qilib, foydalanuvchilar va huquq idoralariga tushunarliroq natijalar taqdim etadi.

XULOSA

Sun‘iy intellekt orqali hosil qilingan sintetik ovozlar zamonaviy kiberxavfsizlikka jiddiy va ortib borayotgan tahdid salmog‘ini tashkil etmoqda. Ushbu maqolada ko‘rib

chiqilgan tadqiqotlar shuni koʻrsatadiki, sintetik ovozlarni aniqlashda akustik tahlil, klassik mashina oʻqitish va chuqur oʻrganish usullarining kombinatsiyasi eng yuqori samaradorlikni taʻminlaydi. Ayniqsa, Transformer arxitekturasi asosidagi modellar va koʻp modal yondashuvlar bu sohadagi soʻnggi yutuqlarni ifodalaydi.

Biroq, texnik yechimlar yetarli emas. Kibertahdidlarga qarshi kurashda huquqiy mexanizmlar, xalqaro hamkorlik va aholining raqamli savodxonligi

bir-birini toʻldirib turuvchi muhim elementlardir. Oʻzbekiston sharoitida bu sohadagi milliy salohiyatni oshirish — tadqiqot markazlarini rivojlantirish, mutaxassislar tayyorlash va xalqaro standartlarga muvofiq qonunchilikni takomillashtirish — davlat kiberxavfsizligi strategiyasining ustuvor yoʻnalishi boʻlishi lozim.

Kelajakda sintetik ovoz yaratuvchi tizimlar takomillashgani sayin, aniqlash algoritmlari ham yangilanib borishi shart. Shu bois, bu sohada uzluksiz ilmiy tadqiqotlar, ochiq musobaqalar va xalqaro maʻlumotlar almashish mexanizmlarini rivojlantirish global kiberxavfsizlikning muhim sharti boʻlib qolmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. Umarov Sh.A., Abduqodirov A.. Axborot xavfsizligi tizimlarini intellektuallashtirish masalalari. Al-Farg'oniy avlodlari, 15(3), 45–60.2024

2. Kenjaboyev O. T., Allanazarov, A. Sh.. Axborot tizimi xavfsizligi. Toshkent: Uzsmart. 2013

3. Turdimatov, M.M., Sadirova X.X.. Axborotni himoyalashda chetlab oʻtishning mumkin boʻlgan ehtimollik holatini baholash usullari. Cybersecurity Journal, 27(2), 112–130.2023

4. Umarov Sh. A., Sun'iy intellekt asosida tahdidlarni aniqlash. Farg'ona: Fan va texnologiya. 2019

5. Muxtarov F. M., Toshpulatov S. M.. Sun'iy intellekt vositalarini ta'limni nazorat qilish va baholashda qoʻllash. Information Systems Review, 19(4), 78–95.2023

6. Khabibullayevich, M. R., & Khatamovich, D. M. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal Of Applied Science And Technology, 5(02), 52-55.

7. Li, Bingcheng, Dingkang Li, and Mingyuan Zhu. "Application analysis of data encryption technology". Applied and Computational Engineering 50, no. 1 (March 25, 2024): 199–205. http://dx.doi.org/10.54254/2755-2721/50/20241502.

8. Abdullayev A., Qosimova U., Axborot xavfsizligi asoslari. Uslubiy qoʻllanma. Studylib.net. 2009.

9. Toshpulatov Sh. M.. Blockchain va Zero Trust Security modeli. Samarqand: Innovatsion texnologiyalar nashriyoti. 2022

10. Abdazimov, S., & Mustafa, D. (2026). Biometric authentication: modern methods of ensuring information security. Научный Фокус, 3(34), 222-230.

11. Abdazimov, S., & Mustafa, D. (2026). Simmetrik kriptotizimlarda o‘rniga qo‘yish algoritmlarining qiyosiy tahlili va amaliy ahamiyati. Научный Фокус, 3(34), 231-237.

12. Abdazimov, S., (2022). Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2(5), 109-115.

13. Мирзаева, М. Б., & Абдазимов, С. З. (2022). Использование технологий искусственного интеллекта в сфере высшего образования.

14. Abdullayeva, B. S., Ro‘ziyev, Y. Z., & Ismoilova, K. V. (2024). Mediasavodxonlik va axborot madaniyati. Darslik. Toshkent.«Donishmand ziyosi.–2024.

15. Narzulla o‘g‘li, Q. X. (2025). Sun’iy intellekt yordamida kibertahdidlarni aniqlash va oldini olish. Global Science Review, 4(5), 147-160.