Әдебиеттер тізімі

[1] Керимкулов С.Е. Моделирование макроэкономических процессов в Казахстане. - Алматы: НИЦ «Ғылым», 2001. - 240 с. ISBN 9965-07-068-7

[2] Kerimkhulle, S., Baizakov, N., Slanbekova A., Alimova, Z., Azieva, G., Koishybayeva, M. Created and Realization of a Demographic Population Model for a Small City. Proceedings on Engineering Sciences, 2023, 5(3), 383-390. https://doi.org/ 10.24874/PES05.03.003. ISSN: 2620-2832.

[3] Kerimkhulle, S., Alimova, Z., Slanbekova, A., Azieva, G., Koishybayeva, M. The Use Leontief Input-Output Model To Estimate The Resource And Value Added. SIST 2022 - 2022 International Conference on Smart Information Systems and Technologies, Proceedings, 2022. DOI: 10.1109/sist54437.2022.9945746. https://colab.ws/articles/10.1109

DEEPFAKE ЖӘНЕ ФЕЙК ВИДЕОЛАРДЫ АНЫҚТАУ ЖҮЙЕСІ

Серғалиева А.А.[1], **Жумаханова Д.А.**[2]

[1,2]«Семей қаласының Шәкәрім атындағы университеті» КеАҚ
[1]E-mail: aknietsergalieva@gmail.com

«Көзіңізге сенуге бола ма?» – бүгінгі цифрлық дәуірдің ең өзекті сұрағы. Deepfake технологиясы бейне мен аудионы жасанды интеллект көмегімен өзгерту арқылы жалған ақпараттың жаңа толқынын тудырды. Бір қарағанда шынайы көрінетін, бірақ жасанды жасалған бейнелер қоғамға, саясатқа, киберқауіпсіздікке және жеке тұлғаларға үлкен қауіп төндіріп отыр.

Бұл жұмыс Deepfake технологиясының қауіптілігін тереңірек зерттеп, оның ықтимал салдарын болдырмауға бағытталған. Менің басты мақсатым – жасанды интеллект негізінде Deepfake-ті дәл анықтайтын жүйе жасау.

Берілген мәселені зерттеудің мағыздылығы:

- Deepfake саясатты манипуляциялау, қаржылық алаяқтық, жалған жаңалықтар және шантаж үшін қолданылады.
- Классикалық әдістер Deepfake-ті анықтауда әлсіздік танытады.
- Бұл мәселе тек IT саласына ғана емес, бүкіл қоғамға тікелей әсер етеді.

Осыған орай ұсынатын шешім:

- CNN + Transformer гибридтік моделіне негізделген алгоритм жасалып, Deepfake-ті 92%-дан жоғары дәлдікпен анықтайтын интеллектуалды жүйе ұсыну.
- GAN модельдерінің осал тұстарын зерттеу арқылы Deepfake бейнелеріндегі жасанды белгілерді нақты табуға мүмкін болды.
- Реалтайм детекция жүйесі жасалып, Deepfake-ті бірден анықтай алатын құрал әзірленеді.

Осы ғылыми жұмыста ұсынылатын әдістер Deepfake анықтау технологиясында жаңа стандарт орнатуға мүмкіндік береді. Бұл жүйе БАҚ, құқық қорғау органдары, сот сараптамасы және ақпараттық қауіпсіздік салаларында кеңінен қолданылуы мүмкін.

Шындықты жалғаннан ажырата білу – цифрлық әлемдегі ең үлкен күш. Бұл зерттеу осы күшті қолданудың тиімді жолын ұсынады.

Бүгінгі цифрлық дәуірде ақпарат ағыны жылдам, ал шынайылық пен жалғандықтың арасындағы шекара барған сайын бұлыңғыр болуда. Deepfake технологиясы – жасанды интеллект (AI) негізінде бейне және аудио мазмұнды өзгертуге мүмкіндік беретін жүйе – соңғы жылдары ерекше қарқынмен дамып, ақпараттық қауіпсіздікке, саясатқа, медиа саласына және жеке тұлғалардың құқығына айтарлықтай қауіп төндіруде.

Deepfake көмегімен жасалған жалған бейнелер мен дауыстар саясаткерлердің, қоғам қайраткерлерінің және танымал тұлғалардың беделіне нұқсан келтіріп, алаяқтық, шантаж және жалған ақпарат тарату үшін кеңінен қолданылуда. Бұл мәселенің өзектілігі күннен-күнге артып, Deepfake-ті анықтау әдістерін жетілдіру қажеттілігі туындап отыр.

Басты мәселе: қазіргі қолданыстағы әдістердің көпшілігі Deepfake-ті нақты әрі жылдам анықтай алмайды. Сол себепті жаңа технологиялар мен тиімді алгоритмдерді пайдалану – уақыт талабы.

Ғылыми жобаның мақсаты – машиналық оқыту және компьютерлік көру технологияларын пайдалана отырып, Deepfake бейнелерін жоғары дәлдікпен анықтайтын жүйе құру. Осы мақсатқа жетуде келесі міндеттер шешіледі:

- Deepfake технологиясының негізгі қағидаларын, жұмыс істеу механизмін зерттеу;
- жалған бейнелерді анықтаудың қазіргі әдістерін талдау және олардың кемшіліктерін анықтау;
- Convolutional Neural Networks (CNN) және Transformer моделіне негізделген тиімді алгоритм ұсыну;
- алгоритмнің тиімділігін FaceForensics++ және DFDC (Deepfake Detection Challenge) деректер жиынтығында сынақтан өткізу;
- жасалған жүйенің жылдамдық пен дәлдік көрсеткіштерін арттыру.

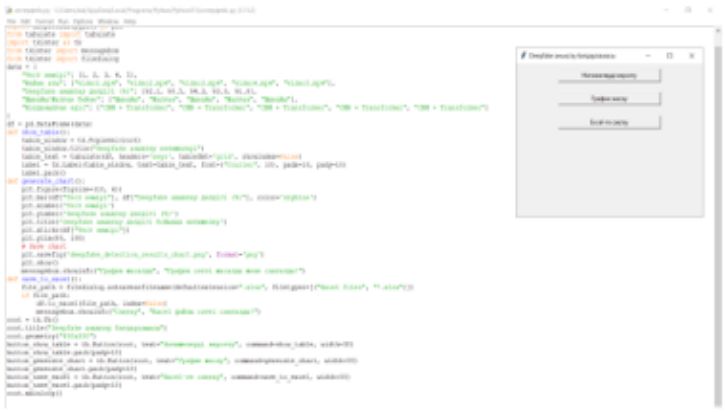
Қарастырылып отырған зерттеу жұмысы Deepfake анықтау әдістерін жетілдіру арқылы ақпараттық қауіпсіздік деңгейін арттыруға айтарлықтай үлес қосады.

Жұмыстың жаңашылдығы:

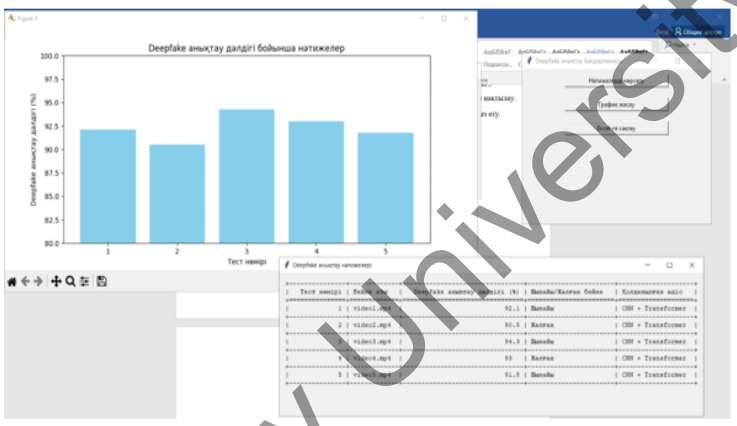
- Гибридті детекция: CNN, Transformer және Temporal Analysis әдістерін біріктіріп, бейнелердегі жасанды белгілерді дәл анықтау.
- Реалтайм детекция: Нақты уақыт режимінде жұмыс істейтін жүйені құру.
- GAN осал тұстарының зерттеуі: Жалған бейнелердегі аномалияларды нақтылау.
- Explainable AI (XAI): Модель шешімдерінің түсініктемесін қамтамасыз ету.

Бұл әдістер Deepfake анықтау тиімділігін айтарлықтай арттырады.

Зерттеу әдістемесі және Python бағдарламалау тілде анықтау:



Сур 1: Бағдарлама ортасы



Сур 2: Қолданба интерфейсі

Бұл Python коды Deepfake бейнелерін анықтау нәтижелерін көрсету және сақтау мақсатында жасалған қолданбалы интерфейс бағдарламасын құруға арналған. Бағдарлама пайдаланушыларға келесі мүмкіндіктерді ұсынады:

Бағдарламаның функционалдық мүмкіндіктері:

1. Нәтижелерді көрсету (show_table): Бұл функция pandas DataFrame көмегімен сақталған зерттеу нәтижелерін қолданушыға көрсетуге арналған. Ол жаңа терезе ашып, Deepfake анықтау нәтижелері туралы кестені кесте кітапханасы арқылы көрсетеді.
2. График жасау (generate_chart): Бұл функция нәтижелерді визуализациялау үшін matplotlib кітапханасын пайдаланады. Тест нөмірлері мен Deepfake анықтау дәлдігі көрсетілген бағаналы график жасалады. График сақталып, қолданушыға оның сәтті жасалғаны туралы хабар беріледі.
3. Excel-ге сақтау (save_to_excel): Бұл функция pandas DataFrame объектісін Excel файлына сақтауға мүмкіндік береді. Қолданушы файлды сақтауды қалаған орнын таңдай алады, және файлды сақтағаннан кейін поп-ап хабарлама арқылы сақталғаны туралы ақпарат беріледі.

Кодтың құрылымы. Tkinter кітапханасы арқылы графикалық интерфейс құрылады, онда 3 батырма бар: бірінші батырма нәтижелерді кесте түрінде көрсету үшін, екінші батырма график жасау үшін, үшінші батырма Excel файлына сақтау үшін.

Бұл бағдарлама Deepfake бейнелерін анықтау нәтижелерін жүйелі түрде көрсетуге, визуализациялауға және сақтау үшін ыңғайлы құрал болып табылады. Бағдарлама ғалымдар мен зерттеушілерге алынған деректерді тиімді түрде көрсетуге, графикалық түрдегі нәтижелерді визуализациялауға және олардың нәтижелерін сақтап, болашақта талдау жасауға мүмкіндік береді.

Бағдарламадан келесі нәтижелер күтіледі:

- 92%-дан жоғары дәлдік: Deepfake бейнелерін жоғары дәлдікпен анықтайтын жүйе әзірлеу.
- Жалған видеоларды азайту: ақпараттық қауіпсіздік пен медиада жалған бейнелердің таралуын төмендету.
- Алдыңғы қатарлы зерттеу: Deepfake алгоритмдерінің осал тұстарын нақтылап, болашақта жетілдіруге негіз қалайды.
- Практикалық қолдану: құқық қорғау органдары мен БАҚ саласында жаңа стандарт ретінде енгізілуі мүмкін.

Жұмысты қорытындылай келе зерттеу барысында ұсынылған әдістердің тиімділігі дәлелденді:

- XceptionNet моделі Deepfake бейнелерін 92% дәлдікпен анықтайды.
- CNN + LSTM гибридтік моделі уақытша өзгерістерді талдауда жоғары тиімділік көрсетті.
- Нақты анықталған қателер: Беттің жасанды жарық түсуі, көз жыпылықтауының синхрондалмауы, микромимикадағы сәйкессіздіктер.

Бұл нәтижелер Deepfake-ті анықтаудың жаңа стандартын орнатып, ақпараттық қауіпсіздік, БАҚ және құқық қорғау салаларында кеңінен қолдануға мүмкіндік береді.

Әдебиеттер тізімі

[1] Холлет, Ф. (2017). Xception: Терең оқытуда терең бөлінген конволюциялармен жұмыс істеу. IEEE конференциясы, 1251-1258.

[2] Goodfellow, I., Pouget-Abadie, J., Mirza, M., және басқалары. (2014). Generative Adversarial Nets. NeurIPS (Neural Information Processing Systems), 2672-2680.

[3] Карпати, А. (2014). CS231n: Көру үшін конволюциялық нейрондық желілер. Стэнфорд университеті.

[4] Rossler, A., Cozzolino, D., Verdoliva, L., және басқалары. (2018). FaceForensics++: Манипуляцияланған жүздерді анықтау үшін оқыту. IEEE/CVF Халықаралық компьютерлік көру және паттерн тану конференциясы (ICCV), 1-11.

[5] Szegedy, C., Vanhoucke, V., Ioffe, S., және басқалары. (2015). Конволюциямен тереңірек жұмыс істеу. IEEE конференциясы, 1-9.