ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Біз жаңа технологиялардан туындауы мүмкін кей қатерлерді көре аламыз. Олардың ішіндегі кейбір мәселердің бірі экзистенцианалдық, этикалық мәселелерді қамтиды. Атап айтқанда ЖИ-нің даму мен өмірімізбен интеграциясы, ЖИ-нің мінез құлқын алдын ала сараптай алмау секілді көптеген тәуекелдерге әкелуі мүмкін.

Сондықтан осы қауіптер мен тәуекелдермен күресе алатындығымызға сенімді болуымыз керек. Олардың даму құлқы біз ойлаған шеңберден асып түсуі де ғажап емес, әрі экспоненциалды дамуға тікелей әсер етеді. Бұл жаңа технологияларды адамзат игілігі үшін қызмет ететін, қоғамға зиян тигізбейтіндей етуді талап етеді. Сондықтан жаңа технологиялардың даму саласында әрдайым тығыз қарым-қатынас пен байланыс, тұрақты ынтымақтастық керек.

Тұтастай, технологиялардың дамуы мен адамзаттың мүдделерін қорғау арасындағы теңдікті сақтау қажет. Бұл жаңа технологиялардың әлеуетін тану мен жаңа ортаға бейімделуге дайын болу қажеттілігін көрсетеді.

Қолданылған әдебиеттер тізімі

1. Шваб К. Төртінші индустриялық революция. Ұлттық аударма бюросы, 2018, 184 б.
2. Knowles E. The Oxford Dictionary of Phrase and Fable – OUP Oxford, 2005, 805 p.
3. Баррат Дж.: Последнее изобретение человечества: Искусственный интеллект и конец эры Homo sapiens.– Аьпина Паблишер, 2015, 22-312 с.
4. K.Doya, A.Ema, H.Kitano, M.Sakagami, S.Russell. Social impact and governance of AI and neurotechnologies // Neural Networks. 2022 №152. P.542-554
5. Vincent C. Müller. Risks of general artificial intelligence // Journal of Experimental and Theoretical Artificial Intelligence, 2014 №26. P.297–301
6. N.Bostrom, E.Yudkowsky. The ethics of artificial // Cambridge Handbook Artificial Intelligence, 1, 2014, 316–334.

УДК 004.8

ВЛИЯНИЕ ТЕХНОЛОГИИ DEEP FAKE НА ОБРАЗОВАНИЕ И ПОДХОДЫ К ИХ ОБНАРУЖЕНИЮ

Каримжанов Амир Нуржанович
amirukz1@gmail.com
Магистрант факультета информационных технологий, кафедры информационной безопасности, ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Сатыбалдина Д.Ж.

В последние годы развитие технологий Deep Fake вызвало новые проблемы и проблемы во многих областях, включая образование. Технология Deep Fake, использующая технологии искусственного интеллекта (ИИ) для создания убедительного, но ложного медиа-контента, может оказать значительное влияние на образование различными способами [1]. В этой статье исследуется влияние технологии Deep Fake на образование, включая примеры того, как она может повлиять на онлайн-обучение, академическую честность и доверие к источникам информации, современные подходы к обнаружению Deep Fake в образовании, включая как ручные методы, так и методы обнаружения на основе ИИ, а также преимущества и недостатки каждого из них, будущее технологии Deep Fake в образовании, этические соображения и последствия. В целом, работа направлена на повышение осведомленности о проблеме технологии глубокого подделки в образовании и поощрение продолжения исследований и разработок в области методов обнаружения для решения этой проблемы.

Влияние технологии Deep Fake на образование. Технология Deep Fake может оказать значительное влияние на образование, особенно в области онлайн-обучения. В условиях растущей зависимости от онлайн-платформ для образования технология Deep Fake может использоваться для создания и распространения ложной информации, что может нанести особый ущерб в контексте обучения. Например, фальшивое видео уважаемого ученого или эксперта,

распространяющего ложную информацию, может быть опубликовано в Интернете и воспринято, ничего не подозревающими, студентами как факт. Это может привести к ряду негативных последствий, включая получение ложных знаний, плохую успеваемость и отсутствие доверия к достоверности источников информации. Технология Deep Fake также может быть использована для нарушения академической честности в образовании. Например, студент может использовать технологию Deep Fake, чтобы создать поддельные академические удостоверения или сертификаты, что позволит людям искажать свою квалификацию и полномочия. Это может привести к тому, что решения о найме и трудоустройстве будут основываться на ложной информации, что может иметь серьезные последствия, как для отдельного лица, так и для организации. Более того, использование технологии Deep Fake для создания поддельных научных статей или результатов исследований также может оказать значительное влияние на академическое сообщество.

Современные подходы к обнаружению искусственного медиа-контента в образовании. В ручном обнаружении Deep Fake контента в сфере образования люди изучают медиа контент, чтобы выявить любые признаки манипуляции. Процесс ручного обнаружения может занять много времени и сил, так как человек должен тщательно изучить информацию, чтобы обнаружить любые аномалии. Это также требует высокой степени технических знаний и опыта, что затрудняет проведение такого анализа. Однако этот метод имеет то преимущество, что он более точен, чем некоторые методы на основе ИИ, поскольку люди могут обнаруживать даже тонкие признаки манипуляции, которые могут быть пропущены автоматическими алгоритмами.

Методы обнаружения на основе ИИ. Эти методы включают использование алгоритмов машинного обучения, которые обучены обнаруживать закономерности и аномалии в медиа контенте.

В работе [2] авторы описывают процесс детектирования искусственного медиа контента как совокупность шести этапов, представленных на рисунке 1.

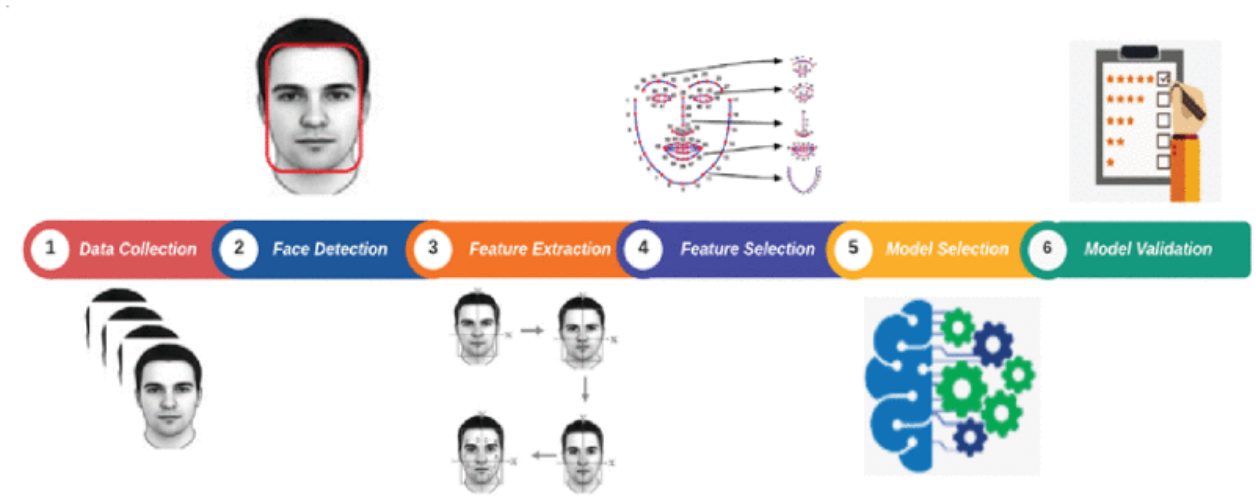

Рисунок 1. Последовательность действий для обнаружения Deep Fake [2].

На первом этапе производится сбор и систематизация оригинальных данных и поддельных данных дл анализа (файлы изображений, видео или аудио данные). Далее собранные данные анализируются с целью определения области интереса, то есть на каких частях изображения или видео необходимо сосредоточиться. В результате можно выявить некоторые характерные особенности (возраст, пол, эмоции и т.д.). Для реализации детектора необходимо провести извлечение признаков из выделенной области. На следующем этапе выбираются только признаки, наиболее полезны для детектирования поддельного контента. Далее, исходя из данных, полученных на предыдущих этапах, выбирается модель распознавания (см. рисунок 2). Конечный этап посвящен оценке производительности выбранных моделей с использованием различных показателей измерения.

Одним из примеров метода обнаружения на основе ИИ является использование сверточных нейронных сетей (CNN), которые можно обучать на больших наборах, данных реальных и поддельных данных, чтобы научиться различать их [2]. Другим примером является использование генеративно-состязательных сетей (GAN), которые включают две нейронные сети, работающие вместе для обнаружения искусственного медиа контента (см. рисунок 3) [3,4]. Одна сеть обучена генерировать реалистичные поддельные данные, а другая сеть обучена определять, являются ли данными реальными или поддельными. Еще одним примером являются автоэнкодеры. Автоэнкодеры – это нейронные сети, которые можно использовать для обучения без учителя [5]. Их можно использовать для изучения паттернов, характерных для реального медиа контента, а затем сравнивать эти паттерны с паттернами в новом медиа контенте, чтобы определить, является ли оно подделкой. ИИ имеют преимущество по сравнению с ручными методами обнаружения по скорости. Они могут быстро анализировать большие объемы данных. Однако методы, основанные на искусственном интеллекте, не являются надежными, и их все еще можно обмануть.

Как и любая другая технология, технология Deep Fake постоянно развивается и совершенствуется. Есть несколько потенциальных достижений, которые могут оказать существенное влияние на образование:

1. Улучшенные алгоритмы искусственного интеллекта. Поскольку технология искусственного интеллекта продолжает развиваться, Deep Fake контент может стать еще более сложными и трудными для обнаружения.
2. Повышенная доступность: в настоящее время создание Deep Fake требует значительных технических навыков и ресурсов. Однако по мере того, как технология становится более доступной и удобной для пользователя, людям может стать проще создавать и распространять Deep Fake.
3. Интеграция с виртуальной и дополненной реальностью. Технология Deep Fake потенциально может быть интегрирована с технологиями виртуальной и дополненной реальности, что позволит еще более убедительно моделировать людей и события.

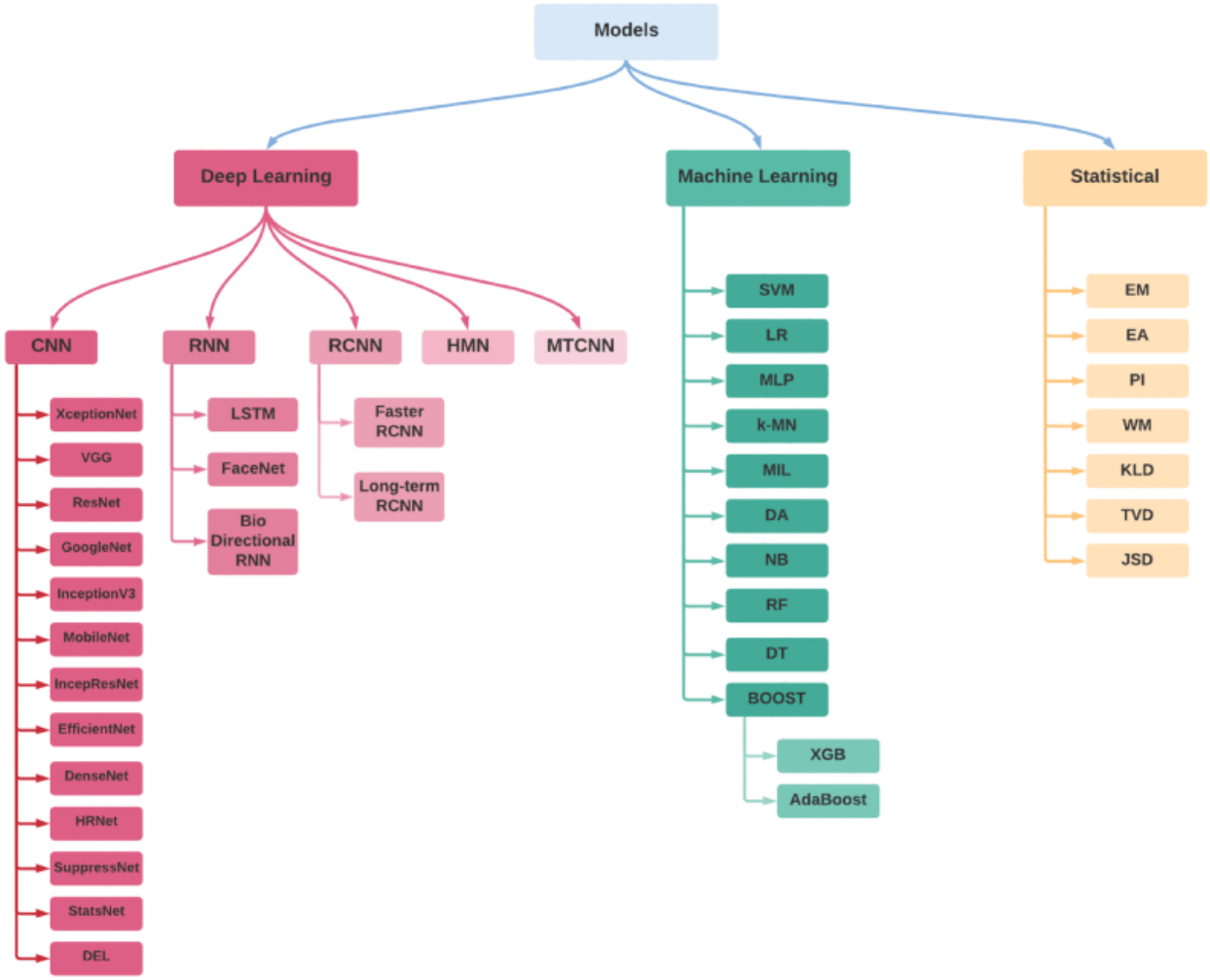

Рисунок 2. Классификация моделей, используемых для обнаружения Deepfake [2].

Поскольку технология Deep Fake продолжает развиваться, важно разработать более совершенные методы обнаружения для эффективной борьбы с ней. Непрерывные исследования и разработки в области методов обнаружения имеют решающее значение, чтобы опережать развивающиеся технологии и их потенциальное влияние на образование. Важно инвестировать в ресурсы для текущих исследований, чтобы повысить эффективность методов обнаружения. Кроме того, сотрудничество между педагогами, исследователями и технологами будет иметь важное значение для продвижения инноваций и опережения. Разработка более сложной технологии обнаружения глубокого подделки может помочь предотвратить распространение дезинформации, сохранить академическую честность и сохранить доверие к источникам информации в сфере образования.

Последствия технологии Deep Fake в образовании могут по-разному влиять на учащихся, преподавателей и учебные заведения. Для студентов создание Deep Fake контента может подорвать их академические достижения, поставить под угрозу их репутацию. Для преподавателей технология Deep Fake может использоваться для манипулирования учебными материалами и нарушения академической честности. Для учреждений использование технологии Deep Fake может нанести ущерб их репутации, подорвать доверие к ним и привести к юридическим или этическим последствиям. Важно продвигать этичное поведение в сфере образования, чтобы смягчить негативное воздействие технологий Deep Fake. Это может включать в себя информирование учащихся и преподавателей о рисках и последствиях использования технологии Deep Fake, установление четких рекомендаций по использованию цифровых медиа и внедрение надежных методов обнаружения для выявления и предотвращения Deep Fake.

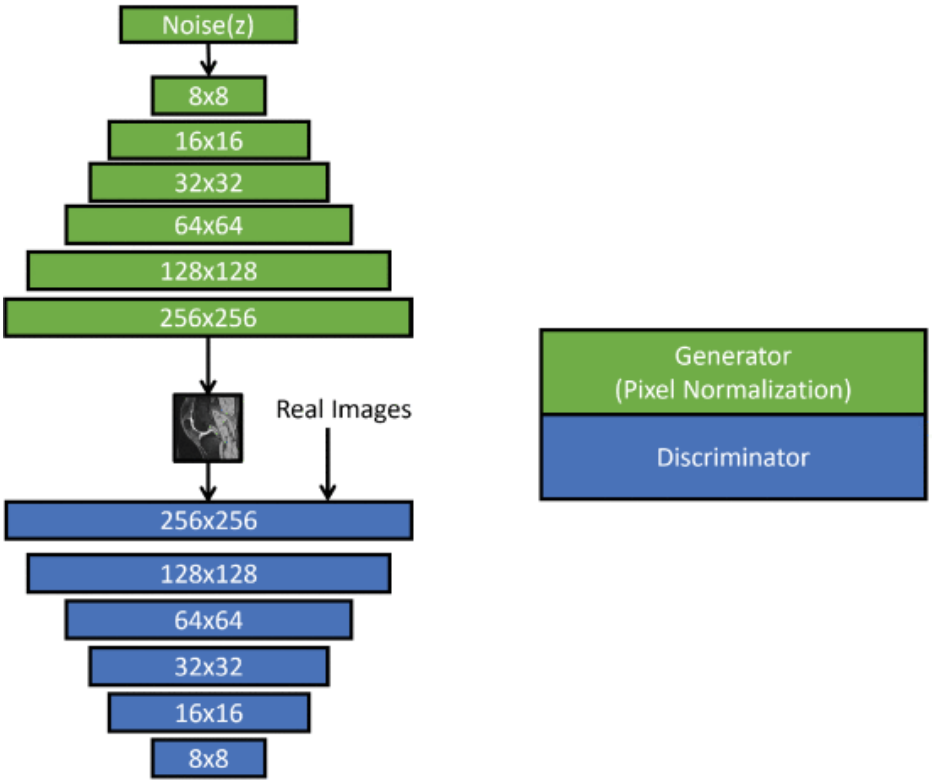

Рисунок 3. Архитектура генеративно-состязательной сети вида PGGAN (Progressive Growing Generative Adversarial Networks) [4].

Заключение

В заключение следует отметить, что технология Deep Fake представляет серьезную угрозу целостности образования. Как мы видели, это может привести к дезинформации, академической нечестности и снижению доверия к источникам информации. Обнаружение Deep Fake – постоянная проблема, но современные подходы, такие как ручное обнаружение и методы обнаружения на основе ИИ, показали некоторый успех. Педагогам и учреждениям важно сохранять бдительность и быть в курсе последних событий в этой области.

Список использованных источников:

1. Westerlund M. The emergence of deepfake technology: A review //Technology innovation management review. – 2019. – V. 9. – №. 11.
2. Rana M. S. et al. Deepfake detection: A systematic literature review //IEEE Access. – 2022.
3. Yang C. et al. Defending against gan-based deepfake attacks via transformation-aware adversarial faces //2021 international joint conference on neural networks (IJCNN). – IEEE, 2021. – P. 1-8.
4. Waqas N. et al. DEEPFAKE Image Synthesis for Data Augmentation //IEEE Access. – 2022. – V. 10. – P. 80847-80857.
5. Khalid H., Woo S. S. Oc-fakedect: Classifying deepfakes using one-class variational autoencoder //Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops. – 2020. – P. 656-657.

УДК 004.032.26

ЖҮРЕК - ТАМЫР ЖҮЙЕСІ АУРУЛАРЫН ДИАГНОСТИКАЛАУДА НЕЙРОНДЫҚ ЖЕЛІ ӘДІСТЕРІН ҚОЛДАНУ

Қартбаева Ақбота Асқаровна
Kartbayeva148@gmail.com