Секция «Криминалистика»

Современные возможности криминалистического исследования видеомонтажа, выполненного программным способом

Научный руководитель – Жидков Дмитрий Николаевич

Иванов Евгений Игоревич
Студент (специалист)
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, Санкт-Петербург, Россия
E-mail: ivanovjenya2000@mail.ru

В настоящее время происходит цифровизация и автоматизация различных процессов человеческой жизнедеятельности, позволившие создать информационные системы, основанные на использовании искусственного интеллекта.

Искусственный интеллект сегодня уже разрешает простейшие рутинные задачи. Машина выполняет сложнейшие операции в считанные секунды, не путается «в мыслях», не «забывает» важное, не откладывает планы на потом, именно поэтому современный рынок информационно-телекоммуникационных технологий постепенно вовлекается в развитие технологий, основанных на использовании больших данных и искусственного интеллекта. Искусственный интеллект уже производит сложнейшие вычисления, подбирает определенную последовательность фраз при общении с человеком, подбирает аудиозаписи согласно музыкальным предпочтениям пользователей и успешно монтирует видео файлы.

Ситуация в сфере производства компьютерных экспертиз и исследований сегодня крайне нестабильна, постоянно появляются новейшие объекты подобных исследований, среди прочих, к которым мы решили отнести deepfakes. С очень большой скоростью распространяются программные комплексы и приложения, с простейшим интерфейсом, основанные на технологиях искусственного интеллекта и анализа больших данных, способные заменять лица на видеозаписях, и все больше и больше людей вовлекаются в данные процессы. Ещё несколько лет назад способности по использованию подобного программного обеспечения можно было отнести к категории специальных знаний, но сегодня они, по нашему мнению, постепенно становятся не только общедоступными, но и общепонятными. В интернете имеется множество простых и удобных в использовании программ и приложений, позволяющих создавать deepfakes, среди них наиболее распространены FakeApp (Windows версия), Reface (Android и iOS версия), Avatarify (Android и iOS версия)[1].

Так при необходимости замены лица программе необходимо определенное количество кадров, с примерами мимики интересуемого субъекта, однако существуют и более сложные процессы, позволяющие создать deepfake даже при наличии фотографии. В данном случае происходит обучение генеративно-состязательной сети, в которой генератор генерирует deepfake кадр, а обученный на реальных изображениях дискриминатор подсказывает что необходимо исправить. Чем меньше поступает исправлений от дискриминатора генератору, тем больше картинка похожа на реалистичную[2]. Запущенные процессы на первый взгляд являются безобидными, пока пользователи ограничиваются накладкой движений одного человека на фотографии другого под веселую музыку, однако уже сегодня повсеместно фиксируется огромное количество фэйковых новостных сообщений, основанных на использовании видеомонтажа, поэтому мы считаем, что проникновение указанных технологий в преступную среду создаст массу проблем для раскрытия и расследования различных видов преступлений и правонарушений.

На данном этапе для раскрытия правонарушений, связанных с фейковыми видеоматериалами различными специалистами из разных стран, создаются программные обеспечения, позволяющие обнаружить фальсификацию в видеоматериалах. В список российского

программного обеспечения входят такие программы, как ЭСКИЗ-В, ВОКОРД Видеоэксперт; в список итальянского - Amped FIVE; в список США - Ikena Forensic. Эти программы имеют одинаковый принцип разоблачения deepfakes, направленный на оценку параметров шумов кадров, их отдельных участков или динамику их покадровых изменений и обнаружении аномалии в видеоряде (выявление признаков повторного сжатия, поиск областей рассогласованности параметров сигнала)[3].

Подводя итог выше сказанному хочется отметить, что искусственный интеллект в наше время является основной опорой экономики, однако в неправильных руках искусственный интеллект становится крайне опасным и сложным орудием преступлений. «На каждое действие имеется противодействие», именно поэтому любые преступления, которые совершаются с использованием IT-технологий со временем будут пресечены, а при грамотном прогнозировании условия для преступлений с использованием новых технологий условия для преступных деяний могут быть настолько неблагоприятными, что данные деяния и вовсе не найдут свою реализацию.

Источники и литература

1) 1. ООО "РБ.РУ", «Не только Deep Nostalgia: 5 приложений, оживляющих фото», 28.02.2021, https://rb.ru/news/ne-tolko-deep-nostalgia-5-prilozhenij-ozhivlyayushih-foto/
2) 2. Lloyd82, «Как делают дипфейки», 28.02.2021, https://pikabu.ru/story/kak_delayut_dipfeyki_8035001
3) 3. ДиВиЛайн, «Обзор ЭСКИЗ-В — видеотехническая экспертиза», 28.02.2021, https://diviline.ru/products/eskiz_v/review/