УДК 343.98

А. А. Черкашин
слушатель факультета правоохранительной деятельности
Белгородского юридического института МВД России
имени И. Д. Путилина

Научный руководитель: ***А. М. Журбенко****,*
доцент кафедры криминалистики
Белгородского юридического института МВД России
имени И. Д. Путилина,
кандидат экономических наук

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ПРОИЗВОДСТВЕ НЕКОТОРЫХ ВИДОВ КРИМИНАЛИСТИЧЕСКИХ ЭКСПЕРТИЗ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ DEEPFAKE

В настоящее время процесс развития информационных технологий все больше проникает в различные сферы жизни общества. Так, в 2017 г. появилась технология deepfake, первоначальной целью которой была помощь в развитии творческой деятельности людей. Так, например, данная технология позволяет воссоздать образ давно умершего поэта, художника, архитектора и т. д., что может активно использоваться в различного рода культурных мероприятиях, к которым можно отнести проведение выставки работ скульпторов или художников, живших несколько столетий назад, благодаря чему посетители получат возможность увидеть, услышать или даже пообщаться с воссозданным образом человека [1].

Однако появление подобного рода технологий не могло не привлечь внимание преступной среды. Несмотря на огромный потенциал и пользу, которую она может принести для общества, рассматриваемая технология также предоставляет ряд новых возможностей для осуществления преступной деятельности. При помощи технологии deepfake преступники могут проводить различные манипуляции, которые включают в себя воздействие на общественное мнение и сознание людей, обман, дискредитацию отдельных граждан, а также осуществлять мошеннические действия, которые проявляются в замене изображения, аудио- или видеозаписей с целью получения денежных средств или иных материальных благ (совершение сделки, получение кредита и т. д.).

В связи с этим существует острая необходимость, заключающаяся в создании автоматизированных систем, способных распознать применение технологии deepfake при анализе медиаконтента. Дело в том, что без использования различного рода программного обеспечения, руководствуясь лишь органами чувств человека, довольно проблематично выявить подобные манипуляции. Среди

основных следов использования технологии deepfake можно выделить следующие: аномалии данных, порождающие неестественные движения во время проигрывания медиаконтента, несоответствие метаданных исходного файла, а именно даты или географического положения устройства, при помощи которого он был создан, и т. д.

Современные криминалистические исследования выделяют способы аутентификации, позволяющие определить погрешности в использовании технологии deepfake с помощью искусственного интеллекта, которые можно разделить на два вида — пассивная и активная аутентификация.

Под активной аутентификацией в данном случае следует понимать проверку исходного кода медиаконтента. Так, например, исходный файл получаемого изображения или видеозаписи имеет определенный код, который может быть представлен в виде водяного знака или же электронной подписи, либо же код аутентификации может быть отправлен вместе с необходимым файлом. Далее производится проверка соответствия кода и изображения или файла, с которым он связан, если программа подтверждает их соответствие, это означает, что файл или изображение являются подлинными.

Пассивная аутентификация заключается в проверке наличия признаков внесения различного рода изменений, которые в случае если и были произведены, то не могли не оставить следов. В данном случае следует отталкиваться от формата файла, в котором был получен медиаконтент. Это может быть видеозапись, изображение или же аудиозапись. Для каждого из указанных форматов существуют свои следы подделки.

Так, в случае получения файла в формате изображения необходимо обратить внимание на следы копирования и перемещения изображений, а также их сращивания. Кроме того, подделка изображения оставляет после себя следы ретуширования в виде различных артефактов, а также несоответствие условий освещенности, так как при наложении одного изображения на другое или при объединении двух различных изображений очень сложно подобрать идентичные условия освещенности для каждого из них, на первый взгляд они могут быть неразличимы, однако анализ изображения на уровне пикселей, с применением искусственного интеллекта, позволяет выявить разницу [2]. С подобной задачей очень часто справляются фототехническая экспертиза или же экспертиза цифровых изображений, которые позволяют выявить следы изменения на полученной цифровой картинке. Их применение целесообразно, когда есть подозрение, что полученное изображение человека или фотографии документов были изменены при помощи того или иного графического редактора.

При получении файла в формате видеозаписи в большинстве случаев искусственный интеллект обращает внимание на появление артефактов в виде несоответствия качества видеозаписи на определенных участках рабочей

области, неравномерной склейки двух или более слоев видео, что создает резкие переходы между кадрами, или же прерывистость наложенной аудиозаписи, появление аномалий кадров, проявляющихся в неестественном движении или появлении объектов, а также отдельных частей тела человека. Для установления данных следов изменения видеозаписи применяется видеотехническая экспертиза. С ее помощью эксперты-криминалисты могут исследовать как компьютерный файл, содержащий видеозапись, так и саму видеозапись на предмет следов изменения или применения технологии deepfake. Кроме того, в рамках данной экспертизы экспертами-криминалистами может быть проведена фоноскопическая экспертиза для установления соответствия аудиозаписи и видеозаписи, находящихся в видеофайле.

Что же касается аудиофайлов, то в данном случае искусственный интеллект позволяет проанализировать интонацию речи человека, а также частоту его голоса, чтобы установить его подлинность, кроме того, использование искусственного интеллекта позволяет определить, использовались ли при изменении файла какие-либо шумовые шаблоны, позволяющие создать уникальные идентификаторы того или иного аудиофайла [3]. Для проверки подлинности подобного рода файлов могут назначаться фоноскопические или аудиотехнические экспертизы. Данный способ особенно эффективен в случае совершения мошеннических действий при помощи телефонного звонка или получения голосовых сообщений с использованием технологии по изменению или замене голоса.

Подводя итоги проведенного исследования, можно сделать вывод, что использование искусственного интеллекта при назначении и производстве фоноскопической, аудиотехнической, видеотехнической и фототехнической экспертиз является эффективным методом расследования преступлений с использованием технологии deepfake, в частности — мошенничества. Их повсеместное внедрение позволит сократить время на определение подлинности того или иного медиафайла, а также расширит возможности при осуществлении криминалистических экспертиз, проводимых в данном направлении.

1. Дипфейки и другие поддельные видео — как защитить себя? [Электронный ресурс] // Лаборатория Касперского : [сайт]. URL: https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake (дата обращения: 14.03.2024). Перейти к источнику Вернуться к статье

2. Что такое Deepfake видео и как сделать Face Swap [Электронный ресурс] // Сравни.ру : [сайт]. URL: https://www.sravni.ru/text/deepfake-video/ (дата обращения: 14.03.2024). Перейти к источнику Вернуться к статье

3. Бессонов А. А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестн. Ун-та им. О. Е. Кутафина. 2019. № 3 (55). С. 46–52. Вернуться к статье