МЕТОД ОБНАРУЖЕНИЯ СИНТЕЗИРОВАННЫХ ВИДЕО БЕЗ СПЕЦИАЛЬНОГО ОБОРУДОВАНИЯ

Богушевич О.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Саванович С.Э. – старший преподаватель каф. ЗИ

Аннотация. В работе представлена двухуровневая методика верификации аудиовизуального контента, не требующая дорогостоящего оборудования. Первый уровень включает визуальный анализ (моргание, блики в глазах, границы лица и тени). Второй уровень – проверка аудиовизуальной синхронизации в замедленном режиме. Приведены критерии выявления синтезированных видео, порядок документирования результатов и варианты решений. Методика применима при внутренних расследованиях и проверке видеозвонков с финансовыми распоряжениями. Подчёркивается, что дистанционная проверка не заменяет личного контакта для критически важных решений.

Ключевые слова. видеозапись, синтезированное видео, верификация контента, визуальный анализ, аудиовизуальная синхронизация, моргание, блики в глазах, границы лица, тени, замедленный режим, подделка, защита информации, мошеннические атаки, расследования, двухуровневая методика.

В последние годы технологии синтеза мультимедиа стали настолько качественными, что подделку трудно отличить от оригинала. Это создаёт серьёзные риски для защиты информации. Если раньше данные чаще всего похищали с помощью вирусов или взлома, то теперь злоумышленник может создать синтезированную видеозапись или аудиозапись и тем самым нарушить доверие к доказательствам или обмануть сотрудников компании.

В данной статье предлагается двухуровневая методика верификации аудиовизуального контента на основе двух уровней анализа: визуального и аудиовизуальной синхронизации. Эти методы доступны без дорогостоящего оборудования и могут быть интегрированы в типовые процедуры защиты информации в организациях и при расследованиях.

На сегодняшний день зафиксированы случаи, когда мошенники использовали синтезированное видео для имитации руководителя компании в видеозвонке, что приводило к несанкционированным финансовым переводам. Кроме того, поддельные аудио- и видеозаписи начинают появляться в судебной практике, создавая проблему «ложного алиби»: злоумышленник может объявить подлинную улику сфабрикованной, вызвав сомнение в достоверности доказательств. Традиционные средства защиты информации – антивирусы, контроль доступа, шифрование – бессильны против такого рода угроз, поскольку они работают с формой файла, а не с его содержанием. Поэтому актуальной становится задача разработки доступных методов верификации видеоконтента, не требующих дорогостоящего оборудования.

Перед началом проверки необходимо открыть видео в плеере и подготовить лист для фиксации временных меток. Сначала выполняется беглый просмотр всего видео в обычном темпе, в ходе которого отмечаются любые фрагменты, вызывающие ощущение неестественности: странные движения губ, подозрительные блики или рывки изображения.

Затем проводится детальная проверка трёх визуальных признаков. Первый – моргание. Нормой считается 10–30 морганий в минуту. Если моргание отсутствует дольше десяти секунд подряд или движения век выглядят слишком быстрыми, это подозрительный признак. Второй признак – блики в глазах. В подлинной записи блики симметричны и синхронно смещаются при повороте головы [1]. Если блики одинаковы в обоих глазах, не меняются или появляются асимметрично, это указывает на синтез. Третий признак – границы лица и тени. Размытие, ореолы на стыке лица и фона, неестественно гладкая «пластиковая» кожа или отсутствие теней также являются подозрительными. При выявлении хотя бы одного явного артефакта проверка прекращается, и проверяющий приступает к документированию нарушений.

Выбор именно этих признаков не случаен. Моргание – сложный для синтеза биомеханический процесс; современные нейросети часто либо «забывают» его вовсе, либо генерируют с неестественной частотой. Блики в глазах зависят от физики отражения света и геометрии сцены – их правдоподобная имитация требует точного моделирования источников освещения, что на практике встречается редко. Артефакты на границах лица возникают из-за несовершенства алгоритмов сведения синтезированного лица с исходным фоном.

Следует учитывать, что эффективность визуального уровня анализа зависит от качества видеозаписи. При низком разрешении, сильной зернистости или высоком сжатии такие признаки, как блики в глазах и границы лица, могут быть плохо различимы. В этих условиях основная диагностическая нагрузка перекладывается на уровень аудиовизуальной синхронизации, который сохраняет работоспособность даже на посредственных записях. Если же качество видео не позволяет надёжно различить даже движение губ, запись признаётся неверифицируемой без применения инструментальных методов.

Если визуальный анализ не выявил нарушений, выполняется проверка аудиовизуальной синхронизации. Выбирается фрагмент речи длительностью 5–10 секунд, видео переводится в замедленный режим (0,5x). Проверяющий оценивает совпадение открытия рта с началом звука на гласных, наличие микродвижений губ перед согласными «б», «п», «м» (в естественной речи они есть, в синтезированной – часто отсутствуют), а также естественность звучания. Любое несоответствие фиксируется как признак подделки.

Затем результаты документируются: в протоколе указываются дата, название файла, временные метки артефактов, скриншоты и итоговое заключение. На основании этого принимается одно из трёх решений: видео признаётся достоверным; подозрительным (исключается из использования); либо при неоднозначных признаках направляется на дополнительную экспертизу.

Для наглядности рассмотрим типовой сценарий. Сотрудник компании получает видеосообщение от лица, которое представляется руководителем, с указанием срочно перевести деньги на указанный счёт. Прежде чем выполнять распоряжение, сотрудник открывает видео в плеере и последовательно применяет описанный алгоритм. Он замечает, что руководитель ни разу не моргнул за 15 секунд разговора, а блики в глазах остаются неподвижными при повороте головы. Этого достаточно, чтобы признать видео подозрительным и не выполнять финансовую операцию до дополнительной проверки по другому каналу связи (например, личному звонку). Таким образом, алгоритм выступает в роли оперативного фильтра, предотвращающего мошеннические действия.

Другой типичный сценарий связан с внутренним расследованием. В компанию поступает видеозапись, предположительно фиксирующая нарушение сотрудником правил безопасности. Запись вызывает сомнения у службы безопасности, так как сотрудник отрицает свою причастность и заявляет, что видео является подделкой. Специалист запускает алгоритм проверки: при замедленном воспроизведении он обнаруживает, что движение губ на ключевых фразах не совпадает со звуковой дорожкой, а на границах лица заметно мерцание пикселей. Видео признаётся синтезированным и исключается из числа доказательств.

Предложенный ручной алгоритм не конкурирует с автоматизированными системами, а дополняет их. Программные решения на основе нейросетей способны анализировать видео быстрее и глубже, но требуют установки специализированного ПО, вычислительных ресурсов и квалификации для интерпретации результатов. Ручной метод, напротив, доступен любому сотруднику с минимальной подготовкой, не требует затрат и даёт результат здесь и сейчас. Оптимальной стратегией представляется комбинированный подход: ручная проверка используется для оперативного отсева очевидных подделок, а подозрительные или особо важные видео направляются на автоматизированный анализ.

Также, предложенный алгоритм решает три практические задачи в области защиты информации. Он позволяет выявлять синтезированные видео при проведении внутренних расследований. Также, данный алгоритм может быть использован для проверки видеозвонков, содержащих финансовые распоряжения, что напрямую противостоит мошенническим атакам. Кроме того, документальная фиксация результатов проверки лишает злоумышленника возможности поставить под сомнение подлинность записи – процедура проведена по формализованному алгоритму, и её результаты можно перепроверить.

Важно подчеркнуть, что ни один алгоритм дистанционной проверки не даёт абсолютной гарантии. В ситуациях, связанных с принятием критически важных решений (финансовые переводы, передача конфиденциальных данных, изменение доступа), единственным надёжным способом подтверждения личности остаётся личная встреча или многофакторная аутентификация по независимому каналу связи.

При этом важно понимать границы применимости предложенного метода. Алгоритм не даёт стопроцентной гарантии: высококачественные синтезированные видео, созданные с использованием современных нейросетей и достаточных вычислительных ресурсов, могут не содержать видимых артефактов. Кроме того, как уже отмечалось, метод чувствителен к качеству исходной записи. Поэтому его основное назначение – оперативная фильтрация заведомо поддельных материалов и выявление грубых синтезов, тогда как для окончательного заключения в спорных случаях требуется экспертиза с привлечением специализированного программного обеспечения.

Перспективным направлением дальнейших исследований является частичная автоматизация описанного алгоритма. Это позволит снизить субъективность проверки и ускорить обработку большого объёма видеоматериалов, сохранив при этом доступность метода для организаций с ограниченным бюджетом.

Список использованных источников:

1. Айтрекинг против дипфейков [Электронный ресурс] – 2026. Режим доступа: https://www.itsec.ru/articles/ajtreking-protiv-dipfejkov