Проблемы фальсификации фото- и видеоматериалов на современном этапе развития цифровизации

Владимир ИВАНОВ, д.т.н., профессор, эксперт,
Станислав ЗВЕЖИНСКИЙ, д.т.н., профессор, АО «НПК «Дедал»

ОБЩИЕ ПОЛОЖЕНИЯ

В настоящее время специальное программное обеспечение (СПО) для редактирования (подделывания) фото- и видеоизображений объектов находит широкое распространение в повседневной жизни. Качество поддельных изображений достигло такого уровня, что не только обычному потребителю, но и эксперту различить поддельные изображения субъективными методами затруднительно. При этом с точки зрения криминалистики удаление или изменение фото- и видеоматериалов (фальсификация) является нарушением целостности первичной информации и, в принципе, уголовно наказуемо.

Наиболее часто подделываются изображения с целями шантажа и ввода в заблуждение относительно произошедшего. Это реализуется путем:

- удаления или замены части видеозаписи при монтаже (линейном / нелинейном);
- кадрирования (обрезки) изображения;
- сокрытия, замены или внедрения виртуальных объектов (в т.ч. человекоподобного или полностью синтезированного) в сцену;
- анимации статических объектов и др.

Основу соответствующих методов СПО составляют математические модели и алгоритмы обработки изображений, которые позволяют сглаживать (фильтровать, маскировать, адаптировать) результаты редактирования с минимизацией внешних признаков вмешательства. Известная технология синтеза изображений, получившая название Deepfake, основанная на методах искусственного интеллекта (ИИ), в том числе, искусственных нейронных сетей (ИНС) уже широко используется для соединения и наложения существующих фото и видео на исходники. При этом выявление и использование традиционных экспертных (субъективных) признаков вмешательства (в фото- или видеоисходники) становится крайне сложным.

Экспертные методы оценивания изображений способны выявить [1]:

- «перескоки» изображений, текущего времени и даты, резкие сдвиги отдельных элементов;
- различия в характере освещения объектов (направленное, рассеянное, равномерное, локальное);
- различия в распределении теней и световых бликов объектов сцены, обусловленных различным положением источников освещения в соответствии с расчетом точек размещения источников;
- различия в расположении точек съемки объектов и сцены в целом;
- различия в цветовых оттенках и зернистости на сходных или примыкающих элементах изображений;
- перепад оптических плотностей по границе зон фрагментов частей изображений и непосредственно примыкающих к ней областей фона при наблюдаемой неоднородности границы (извилистая, истонченная, увеличенная, разорванная и пр.);
- локальные усиления насыщенности цвета деталей и локальные изменения оптической плотности по всей сцене;
- повторяющиеся мелкие элементы изображений объектов, свидетельствующие о применении инструментов графических редакторов;
- несоответствие масштаба (диспропорция размеров), отсутствие композиционного единства элементов изображений;
- различия плотности почернения одинаковых по освещению элементов изображений;
- «необоснованные» отличия по степени резкости, плотности и контраста элементов изображений;
- признаки маскировочной ретуши по границам фрагментов изображений;
- наличие внедренных искусственных структурных заполнений фона на месте удаленных или около внедренных объектов и пр.

Перечисленные признаки являются «экзогенными» или внешними для исследуемого контента. Общими недостатками таких методов являются зависимость погрешности оценки от квалификации экспертов и большие трудности, связанные с распространением новых «тонких» методов обработки изображений, преимущественно посредством СПО на основе ИНС или машинного обучения, что существенно затрудняет установление целостности (аутентичности) контента. Причем можно утверждать, что в области фото экспертные оценки дают меньшую погрешность, чем в области видео.

Проблема создания современного программно-аппаратного инструментария по выявлению признаков фальсификации фото- и видеоконтента обусловливает необходимость разработки многокритериальной оценки многомерных данных, полученных в результате исследования прямых и косвенных признаков возможных нарушений целостности. Это требует исследования существующих технологий внут-

Таблица 1. Характеристики СПО для изменения фото- и видеоконтента

Продукт / разработчик	Характеристика
FakeApp 2.1 [3] / DeepFake	Бесплатное СПО под ОС Windows (под Android нет), использует ИНС с обучением для распознавания лиц в видеофайлах и замены их на новые. Качество выходного ролика зависит от глубины обучения и объема обучающей выборки. В Google Play имеется программа с именем fakeapp, - это совершенно другое приложение. Используемые библиотеки - Keras, TensorFlow (Python).
DeepFaceLab [4-6] / iperov (псевдоним Иван Перов)	СПО с открытым кодом, с репозиторием проекта на GitHub, рассчитано одновременно и на пользователей без знаний о фрейм-ворках глубокого обучения, и на разработчиков. Используется генеративно-состязательная ИНС GAN (Generative adversarial network), библиотека Keras (Python).
FaceApp для Android/ iOS [7] / Wireless Lab, Россия	Использует ИНС GAN для генерации высокореалистичных преобразований лиц на фотографиях. Может преобразовать лицо в улыбающееся, состарить / омолодить, поменять пол и др. Доступно для бесплатного скачивания на Google Play и App Store.
Deepfakes web β [8] / VysionApps, Великобритания	Платное СПО для создания deepfake видео в интернете. Необходимо зарегистрироваться и загрузить свои видео, остальное происходит в облаке, где используются мощные графические процессоры. На изучение видеоизображений и смену лиц уходит около 4 часов. Качество выходного видео зависит от «потерь»: чем ниже эти значения (при обучении из загруженных видео), тем оно выше. Только автор получает доступ к своим видео- и учебным данным (декларируется).
FaceSwap [9]	Похожее на DeepFaceLab СПО с открытым исходным кодом, предоставляет больше возможностей, лучшие документацию и онлайн-поддержку, есть много учебников. Используются ИНС GAN, библиотеки Keras, Tensorflow, OpenCV (Python).
Deepfake Studio 1.4.10 [10] / Deep Works, США	Эволюционирование СПО FaceSwap. Не требуется мощная аппаратная часть и настройки, знания о кодировании. Устанавливается на мобильные устройства, имеет интуитивно-понятный интерфейс, необходима связь с серверами. Бесплатно распространяется на Play Market. Используется ИНС GAN.
Zao (китайский сегмент) [11] / Changsha Shenduronghe Network Tech. Ltd. (Китай)	Модулирует голоса и накладывает лицо-источник на тело актера в сцене. Позволяет пользователям обмениваться лицами с актерами в коротких клипах. Особенность алгоритма – в обучении на китайских лицах. Выборка для обучения составляет всего несколько изображений (работа с предобученными данными). Бесплатный доступ в Play Market и App Store. Пользователь загружает не свой контент, а лишь изображение, которое переносится в заданный (разработчиком) набор видео. Используются ИНС GAN, ОС iOS.
Doublicat (Reflect) [12] / RefaceAI, ранее Neocortext. Inc., Украина	ОС Android/ iOS. Свободно распространяется через Google Play. Популярен у пользователей благодаря быстрому монтажу роликов. Позволяет сделать селфи и поместить свое лицо на изображении. На средней аппаратной части обработка лица занимает около 5 с. Используется ИНС GAN, библиотека PyTorch (Python).
Dowell [13] / Everypixel Group, Россия, Челябинск	Осуществляет перенос лиц с одного видео на другое с повторением мимики, жестов и других особенностей с высокой точностью. Время обучения до 24 час. Используется ИНС GAN.
Synthesia [14] / Великобритания	Синтез видеоизображений, где вместо людей используются синтезированные человекообразные объекты.

рикадрового монтажа для синтеза поддельных изображений (фото и видео), анализа «схожих» СПО для известных видеосистем безопасности, а также исследования методов ИИ, применяемых за рубежом (в России число публикаций по исследуемой тематике на порядок меньше) на предмет выявления фальсификаций видео. В следующей работе будут описаны научно-обоснованные рекомендации по разработке перспективного отечественного СПО.

СПО ДЛЯ СИНТЕЗА ИСКУССТВЕННЫХ ФОТО- И ВИДЕОИЗОБРАЖЕНИЙ

Эталоном стандартов в области редактирования фотографий и видеоматериалов является компания Adobe [2] с продуктами Adobe Premiere, Adobe Photoshop и Adobe After Effects. В указанных или аналогичных программных продуктах ИНС используются для ускорения монтажа (линейного и нелинейного) и редактирования изображений. Под последним понимается:

- внутрикадровый монтаж, связанный с внедрением, удалением, заменой одного или нескольких объектов;
- анимация статических или внедренных объектов;
- реставрация (в т.ч. раскрашивание) старых и частично утраченных фотографий и фильмов, а также обратный процесс – «состаривание»;
- перекодирование форматов, автокадрирование;
- выбор кадров с присутствием людей, трекинг;
- удаление дымки, вуали, размытий;
- коррекция цвета, резкости, замена фона;
- поворот лица объекта, преобразование лиц в улыбающиеся, открытие глаз;
- создание уникального лица методом объединения нескольких и др.

Замена лица персонажа в видеоматериалах осуществляется, как правило, с помощью генеративно-состязательных ИНС (GAN), где совместно работают две нейросети. Алгоритм замены лица в общем виде следующий:

- на «донорском» и целевом видео размечаются границы лиц (иногда в ручном режиме);
- из обоих видеофрагментов формируются кадры (фотографии) для 2-х массивов обучающих выборок;
- изображения сжимаются (кодируются) и восстанавливаются (декодируются), каждое своей нейросетью, до требуемого значения точности (способ кодирования-декодирования одинаков для обеих ИНС);
- для замены лиц декодировщики меняются местами;
- восстановленное изображение с заменой лица предъявляется для распознавания «родной» нейросети; если она не замечает подмены, то итерационный процесс обучения останавливается.

ИНС функционирует только после обучения на «большой» репрезентативной базе прецедентов – эталонных изображений. Известные СПО используют различные типы ИНС с разным числом слоев, персептронов в одном слое

Таблица 2. Системы распознавания лиц для СКУД и обеспечения безопасности

Продукт / разработчик	Характеристика
Face++ [16] / Megvii, Китай	Распознавание лиц (вероятность 0,99 по словам разработчиков) в составе СКУД, сопоставление лиц с учетом возрастных изменений. Используются алгоритмы Megvii-000 и сверточные нейронные сети (CNN) с глубоким обучением.
Luna Platform [17] / Vision Labs, Россия	Идентификация людей по изображениям лиц в потоковом видео: обнаружение лиц; извлечение дескриптора лица; хранение дескрипторов и быстрый поиск; группировка дескрипторов лица; сопоставление дескрипторов лица; определение атрибутов лица (пол, возраст и эмоции); уведомление сторонних систем о событиях (например, о совпадении дескрипторов). Алгоритм VisionLabs-002,003.
Morpho Inc. [18] / OT-Morpho, Франция	Идентификация лиц для выпуска и управления электронными удостоверениями личности; аутентификация для доступа к различным сервисам и услугам; охрана порядка; пограничный контроль. Используется алгоритм Morpho-000.
Find Face Security [19] / Ntech Lab, Россия	Система распознавания лиц в видеопотоке реального времени на основе искусственного интеллекта. Позволяет обнаруживать людей по базе данных, применяется в системах обеспечения общественного порядка, СКУД и др. Используется алгоритм Ntechlab-003.
Facial Recognition Platform [20] / Gemalto Cogent, США	Платформа распознавания лиц, в т.ч. на некачественных изображениях, в разных положениях, с частично скрытыми лицами, а также в условиях недостаточного освещения. Используется алгоритм Cogent-000.
Vocord Tahion [21] / Vocord, Россия	Интеллектуальное видеонаблюдение для систем «Безопасный город»: контроль движения транспорта или грузов, распознавание толпы, обнаружение забытых вещей и др. Используется алгоритм Vocord-002.
Sky Biometry API [22] / Neurotechnology, Литва	Обнаруживает лица под разными углами (одновременно несколько лиц), в очках или без них, с любым выражением. Используется алгоритм Neurotechnology-003.
Face SDK [23] / Тридиви (3DiVi Inc.), Россия	Распознавание черт лица, отслеживание лиц, классификация по полу и возрасту, видеоаналитика. Используется язык C++, алгоритм GAN.
Dragonfly Eye [24] / Yitu Tech., Китай	Разработка чипов ИИ, компьютерного зрения, понимания естественного языка, распознавания голоса, робототехника. Используется алгоритм Yitu-000.
Gorilla Technology [25] / Тайвань	Видеоаналитика, включающая распознавание лиц, транспортных средств, обнаружение вторжений. Используется алгоритм Gorilla-000.
Easen Face Recognition [26] / Zhuhai Yisheng Electronics Tech., Китай	Биометрическая идентификация лиц для обеспечения общественной безопасности, в т.ч. по радужной оболочке, заявленная точность идентификации 0,998. Используется алгоритм Yisheng-001.
Интеллект [27] / ITV-Group, Россия	Нейросетевая видеоаналитика, детектор движения, сдвига камеры, закрытия и засветки объектива, изменения фона, расфокусировки, оставленных и сдвинутых вещей, трекер, поиск лиц, подсчет людей, анализ сцен.
MagicBox [28] / Компания «Агрегатор», Россия	Видеокамеры со встроенной видеоаналитикой для машинного зрения. Реализованы функции детектора движения, цифровая фильтрация изображений. Алгоритм на базе динамических текстур и точным сегментированием.

и связями между слоями. Сети сами позволяют выбирать вид решающей функции (например, линейная, логистическая, сигмоидная). В процессе обучения ИНС вычисляются коэффициенты связей между слоями и параметры разделяющей функции, которые являются коммерческой тайной разработчиков (не приводятся в публикациях).

В табл.1 кратко представлены известные СПО, работающие под различными операционными системами (ОС), предназначенные для создания и редактирования изображений с внедрением объектов и использующие технологии ИИ.

По мнению некоторых исследователей [15] неточности в работе современных ИНС в области синтеза (и фальсификации) изображений всегда остаются. Например, это заметно, когда полное лицо пытаются «натянуть» на худое и наоборот. В этих случаях может использоваться ручная дорисовка с последующим сглаживанием контуров. Существующие алгоритмы переносят только область лица от бровей до подбородка и от уха до уха, уши, волосы, лоб остаются без изменений, что может являться признаком распознавания подделки видеозаписи. Указывается, что ИНС «хорошо» меняет в видеоролике лицо анфас, однако при повороте головы «остаются» следы профиля от старого актера. Аналогично обстоят дела с положением глаз, движением губ, мимикой и эмоциями. Каждому человеку свойственны индивидуальные особенности поведения, поэтому имея такой «эталон», возможно выявить подлог. Большая часть современных СПО работает с низким разрешением перено-

симой области лица 256x256 пикселей, для качественного решения необходимо 1024x1024. Улучшение разрешения может обеспечиваться и посредством ИНС.

Изучение СПО, представленных в табл. 1, позволяет сделать следующие выводы:

- для внедрения объектов в изображение (фото, видео) чаще всего используются ИНС класса GAN, называемые «сиамские сети»;
- обработка видео осуществляется как на удаленных серверах разработчиков СПО, так и на рабочих станциях пользователей;
- для обучения ИНС требуется обучающая выборка значительного объема;
- время на создание фильма с внедренными объектами зависит от качества конечного продукта и варьируется от нескольких секунд до нескольких часов (для высокого качества требуется больше времени на обучение ИНС);
- распознавание поддельных видеоматериалов, созданных с использованием ИНС, осуществлять субъективными методами всё сложнее.

СИСТЕМЫ БЕЗОПАСНОСТИ, АНАЛИЗИРУЮЩИЕ ФОТО И ВИДЕО ПОСРЕДСТВОМ ИНС

Современные ИНС используются в различных системах контроля и управления доступом (СКУД) на объекты и к ресурсам, а также в системах безопасности (общественного порядка) крупных объектов и городов. Автоматические системы распознавания лиц активно внедряются в средства паспортного контроля. Подделка биометрических данных (фото- и видеоизображений) может сделать определенные СКУД уязвимыми.

В табл. 2 приведены характеристики известных систем распознавания лиц, применяемых в СКУД. Значения показателя правильной идентификации лиц соответствуют, по заверениям разработчиков, уровню ≥ 0,99. Чаще всего в системах применяются ИНС класса GAN, реже CNN (сверточная нейронная сеть).

Таблица 3. Характеристики зарубежных публикаций в области методов и алгоритмов поиска видеофальсификаций

Наименование источника	Математическая модель / алгоритм вычислений
1. K.Nagi Reddy, Malle Raveendra DNN Based Moth Search Optimization for Video Forgery Detection // Int. Jour. of Engineering and Advanced Technology. – 2019	Фильтрация методами Маркова и Габора с последующим распознаванием внедренных объектов нейросетью DNN. В качестве признаков используется марковская статистика для обнаружения возможной двойной компрессии. Этапы работы алгоритма: - вычисление статистик Маркова; - сегментация кадров с двойным сжатием; - извлечение объектов из кадров фильтрацией Габора; - разделение видео на исходное и отредактированное. Достоверность выявления подделок видео 0,95. Используемая ИНС DNN (Deep neural network –нейронная сеть с глубоким обучением).
2. J. Fabrizio, P. Sampaio AMR Compressed-Domain Analysis for Multimedia Forensics Double Compression Detection // Revista Brasileira de Cikncias Policiais. – 2019	Вычисление линейного коэффициента предсказания в процессе декодирования аудиодорожки. Используется модель регрессии.
3. M. Fanfani, F.Bellavia, C. Colombo, M. Iuliani A Vision-based Fully Automated Approach to Robust Image Cropping Detection // Signal Processing Image Communication. – 2019	Отредактированные файлы (подделки, закладки) в цифровых изображениях отыскиваются посредством обнаружения несоответствий тени, света, объектов перспективы и геометрии. СПО строит систему координат, выбирая началом центр камеры. На основе этой системы координат строится 3D-проекция изображения. Этот метод оценки изображений разделяется на два класса: сигнальный и кадровый.
4. M. Ramachandra, R. Cristin, K. Suresh Kumar A novel forgery detection in face images using enhanced convolutional neural network // Advances in Mathematics Scientific Jour. - 2020	Определение лиц на изображении при помощи алгоритма Виоласа Джонса и матричного алгоритма Speeded Up Robust Feature (SURF). СПО работает как с видеорядом (разбивает его на отдельные кадры), так и с изображениями. Точность и достоверность алгоритма оценивается на уровне 0,98 по сравнению с другими нейросетями и методами машинного обучения SVM, KNN, NN, FOA-SVNN. Используемая ИНС Enhanced Convolutional Neural Network (ECNN).
5. N. Kanwal, R.S. Batth. An Ontology of Digital Video Forensics: Classification, Research Gaps & Datasets // Int. Conf. on Computational Intelligence and Knowledge Economy (ICCIKE). Amity University Dubai (UAE). - 2019	Показана применимость следующих математических моделей: • DCT – дискретное косинусное преобразование; • PCA – анализ главных компонент; • SVD – сингулярное разложение; • DWT – дискретное вейвлет-преобразование; • блочный поиск по пикселям; • автокорреляция для выявления местоположения. Предлагается классификация видеокриминалистических методов. Приводятся данные по 21-му методу выявления подделки, разработанных в 2007-19 гг., с оценкой их точности к различным подделкам (30 – 99 %). Предлагаются наборы данных из поддельных видеофильмов (около 1000) разных форматов и длительности для тестирования СПО по обнаружению подделок.

Продолжение таблицы 3

Наименование источника	Математическая модель / алгоритм вычислений
6. Q. Li, R. Wang, D. Xu. An Inter-Frame Forgery Detection Algorithm for Surveillance Video // Dahongying University, Ningbo. – 2018	Корреляционный и кластерный анализ k-средних в пространстве Евклида, беспороговое обнаружение. При подделке видео уменьшается межкадровая корреляция. Алгоритм обеспечивает извлечение признаков и локализацию аномальных точек. При получении признаков выделяется 2D фазовая идентичность кадров, затем вычисляется корреляция между соседними кадрами. Аномальные точки обнаруживаются с помощью алгоритма кластеризации k-средних. Нормальные и аномальные точки группируются в две категории. Используются методы машинного обучения.
7. P. Deshpande, P. Kanikar. Pixel Based Digital Image Forgery Detection Techniques // Int. Jour. of Engineering Research and Applications. – 2012	Фазовая корреляция для вычисления пространственного смещения элементов изображения, спектральный анализ, медианная фильтрация. Обнаружение техники «копирование - перемещение», в том числе с вращением. В основе анализа изображений лежат: 1) пиксельные методы, обнаруживающие статистические аномалии; 2) методы, использующие статистические корреляции, сжатие с потерями; 3) методы, использующие артефакты, вносимые объективом видеокамеры, датчиком или постобработкой на фоточувствительной матрице; 4) методы обнаружения аномалии в 3D-изображении при взаимодействии между физическими объектами, светом и видеокамерой; 5) геометрические приемы измерения объектов и их положения относительно видеокамеры.
8. B. Van Hoorick, C. Vondrick, Dissecting Image Crops. Columbia University, New York, USA. – 2020	Нейросетевая обрезка изображения, интерполирование и экстраполирование пикселов, хроматическая аберрация. Исследуется влияние кадрирования на характеристики изображения, а также «почерк» фотографа. При кадрировании ИНС обрезает изображение для улучшения качества, обрезанная часть имеет «следы» (взаимная энтроприя) удаленного изображения. Используется сверточная нейронная сеть (CNN).
9. R.D. Singh, N. Aggarwal. Video content authentication techniques: a comprehensive survey // Springer-Verlag Berlin Heidelberg. – 2017	Когерентная межкадровая обработка. Обнаруживается факт повторного захвата видео, синтезированную структуру (при удалении объектов) и факт обрезки кадров. СПО проверяет видеоряд на внедрение отредактированных или дублированных кадров, исследует следы удаления или изменения размера кадров. Обнаруживаются изменения в видеоряде путем определения артефактов на камере / сенсоре, ошибок кодека, особенностей стабилизации и особенностей объекта съемки.
10. G. Chittapur, S. Murali, B.S. Anami. Video Forgery Detection Using Motion Extractor By Referring Block Matching Algorithm // Int. Jour. of Sientific & Technology Research. – 2019	Используются модифицированные модели Маркова с классификатором SVM, темпо-временной анализ отличий каждого набора кадров в поддельном видео. Признаки извлекаются из остаточных векторов движения, достоверность выявления 94%. Этапы работы алгоритма (на основе machine learning) следующие: 1) Загрузка видео и извлечение кадров, преобразование в оттенки серого. 2) Применение модифицированных марковских признаков для получения данных по среднему количеству пикселей по кадрам видео. 3) Вычитание каждого пикселя кадра из пикселя базового кадра, получая остаток движения для каждого кадра. 4) Вычисление 4-х направлений движения для каждого кадра остатка, на основе разницы между текущими пикселями и соседними пикселями в горизонтальном, вертикальном, диагональных направлениях. 5) Применение матрицы перехода вероятностей к каждому остатку движения. Направление для каждого кадра описывает вероятность перехода из состояния в состояние. 6) Для каждого кадра вычисляется вектор признаков в качестве входных данных для классификатора.
11. S. Mashhadani, N.L. Clarke, H. Alkawaz, S. Furnell (Univ. of Plymouth). A novel multimedia-forensic analysis tool (M-FAT) // The 12th Int. conf. for Internet Technology and Secured Transactions (ICITST). – 2017	Корреляционный анализ, вычитание фона, анализ освещенности, фильтрация Габора. Распознавание лиц на основе алгоритма с этапами: - сегментация для выделения лица; - постсегментация (очистка); - разделение изображения на части, где в одном сегменте только один элемент; - запрос во внешнее хранилище изображений (базу данных, БД); - извлечение признаков лица, обрезка, нормализация; - выделение компонент; - сохранение признаков в виде вектора, сопоставление с БД; - вычисление корреляции метаданных; - визуализация данных.

НАУЧНО-МЕТОДИЧЕСКИЙ ПОТЕНЦИАЛ ПО ВЫЯВЛЕНИЮ НАРУШЕНИЙ ЦЕЛОСТНОСТИ ВИДЕОКОНТЕНТА

Среди зарубежных публикаций в области анализа видеопотоков и выявления фейковых изображений следует отметить ряд книг и учебных пособий [29–34], а также издания представителей отдельных научных школ, представленные в табл. 3. В русскоязычном сегменте также можно отметить ряд полезных изданий [35–38]. Достоверность выявления подделок видео различными алгоритмами в среднем составляет величину 0,85–0,95.

Анализ зарубежных научных публикаций в области обнаружения подделок видео (табл. 3) позволяет сделать вывод о применяемом математическом аппарате и использовании следующих, преимущественно, «эндогенных» или внутренних характеристик и параметров изображений:

– вычисление линейного коэффициента предсказания;
– регрессионный и авторегрессионный анализ;

– фильтрация методами Маркова и Габора, медианная;
– дискретное косинусное преобразование;
– анализ главных компонент;
– сингулярное разложение;
– дискретное вейвлет-преобразование;
– корреляционный и автокорреляционный анализ амплитуд и фаз;
– кластерный анализ методом k-средних в метрике Евклида;
– спектральный анализ;
– анализ энтропии;
– интерполирование и экстраполирование.

При этом используются ИНС различных классов (CNN, ECNN, DNN), а также технологии машинного обучения (SVM-классификатор). В качестве типовых информативных признаков выбираются:

1. «Следы» RAW-данных («сырых») с аналого-цифрового преобразователя матрицы видеокамеры в конечном сжатом изображении, а также параметры межпиксельных связей.
2. Характеристики снимаемой сцены (расположение объекта относительно камеры, источника света, других объектов, расположение теней).
3. Исследование видеопотоков на повтор и обрезку кадров, многократный захват или сжатие, скорости перемещения объектов, а также пикселей (межпиксельные связи, синтезированные структуры, характер границ объектов).
4. Исследование во времени поведения синтезированного объекта на изображении – повторяемые движения (жесты руками, наклоны и повороты головы, моргание глазами) и временные интервалы повторений (как правило, период повторений равен константе, либо интервалы подчинены нормальному закону распределения).

В представленных в табл. 3 публикациях авторов разных научных школ, преимущественно из Индии и Китая, декларируются достаточно высокие оценки достоверности распознавания фактов внедрения объектов в видеоматериалы на уровне 0,87–0,99. При этом, как правило:
– не приводится информация о предподготовке изображений к извлечению признаков подделок и методах стандартизации (нормирования) вектора признаков;
– при использовании ИНС не указывается перечень признаков, с которыми работают кодировщики / декодировщики;
– не приводится количество экспериментальных тестов, объем обучающей и тестовой выборок видеоматериалов;
– не приводятся характеристики видеокамер, которые использовались для записи оригинального видео, а также камер, применявшихся для записи или создания внедряемого объекта;
– не приводятся данные о разрешении изображений (исходных и внедренных объектов), технологии создания внедряемого объекта (ИНС или оператор, квалификация автора поддельного видео) и др.

Определенная «закрытость» указанных публикаций и их относительная «свежесть» указывает не только на наличие высокого коммерческого потенциала («ноу-хау») рассмотренной области применения ИИ, но и на значимую актуальность исследований.

ЛИТЕРАТУРА

1. http://www.exp-zentr.ru/videomontag.htm.
2. https://www.adobe.com.
3. https://fakeapp.site.
4. https://github.com/chervonij/DFL-Colab.
5. https://github.com/nagadit/DeepFaceLab Linux.
6. https://github.com/iperov/DeepFaceLab.
7. https://faceapp.io.
8. https://faceswapweb.com.
9. https://github.com/deepfakes/faceswap.
10. https://apkpure.com/ru/deepfake-studio/com.deepworkings.dfstudio.
11. https://www.zaoapp.net.
12. http://reface.app.
13. https://www.dowell.ai.
14. https://www.synthesia.io/about.
15. https://vc.ru/ml/94457-kak-delayut-deepfake-video-i-pochemu-luchshe-govorit-face-swap.
16. https://www.faceplusplus.com.
17. https://visionlabs.ai/ru/products/luna-platform.
18. https://armosystems.ru/about/partners/morpho.
19. https://findface.pro/solution/biometrichesky-kompleks.
20. https://www.innovatrics.com/face-recognition-solutions.
21. https://www.vocord.ru/products/vocord-tahion.
22. https://skybiometry.com.
23. https://face.3divi.com/products/face_sdk.
24. https://www.yitutech.com.
25. https://www.gorilla-technology.com.
26. http://english.easen-electron.com.
27. https://www.itv.ru.
28. https://www.agrg.ru/videoanalytics.
29. H.T. Sencar, N. Memon. Digital image forensics. – 2013.
30. M. Kirchner. Notes on Digital Image Forensics and Counter-Forensics. – 2012.
31. G. Bradski, A. Kaehler. Learning OpenCV: Computer Vision with the OpenCV Library. O'Reilly Media, Inc., California. – 2008.
32. D.A. Forsyth, J. Ponce. Computer Vision: A Modern Approach, 2nd Edition. – 2004.
33. Компьютерное зрение [Электронный ресурс] / Л. Шапиро, Дж. Стокман. 2-е изд. (эл.). – М.: БИНОМ. Лаборатория знаний, 2013 – 752 с.
34. US6757027B1 Automatic video editing.
35. Визильтер Ю.В., Желтов С.Ю., Бондаренко А.В. и др. Обработка и анализ изображений в задачах машинного зрения. – М.: Физматкнига, 2010. – 672 с.
36. Лукьяница А.А., Шишкин А.Г. Цифровая обработка видеоизображений. – М.: «Ай-Эс-Эс Пресс», 2009. – 518 с.
37. Патент RU 2634225 Способы и системы поиска объекта в видеопотоке.
38. Патент RU 2584441 Способ определения признаков монтажа на копиях документов, выполненных электрофотографическим способом.