УДК 004.056.53

Вестник УрФО № 3(45) / 2022, с. 34–46

Дорофеев К.А.

DOI: 10.14529/secur220304

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ БИОМЕТРИЧЕСКИХ СИСТЕМ РАСПОЗНАВАНИЯ ЛИЦ

В статье рассматриваются современные подходы к решению задачи распознавания лиц, построению биометрических систем идентификации по лицам, а также основные проблемы и уязвимости подобных систем. Особое внимание уделено вопросам безопасности, а также проблемам, связанным с атаками на такие системы: использование подделок, распечатанных фотографий и масок, визуализированных и сгенерированных двумерных и трёхмерных изображений и видео лиц. Рассмотрены современные подходы к решению таких проблем, к противодействию подобным атакам. Также рассмотрены правовые аспекты, приведены законы, регулирующие обработку биометрических данных граждан РФ, и оценены риски атак на биометрические системы.

Основная задача исследования – провести анализ уязвимостей биометрических систем распознавания лиц и указать основные способы устранения этих уязвимостей.

Ключевые слова: *информационная безопасность, биометрия, распознавание лиц, нейронные сети, глубокое обучение, идентификация, аутентификация, правовое регулирование биометрических данных.*

Dorofeev K. A.

COMPARATIVE ANALYSIS OF VULNERABILITIES IN BIOMETRIC FACE RECOGNITION SYSTEMS

The article discusses current approaches to solving the problem of face recognition, the construction of biometric face identification systems, as well as the main problems and vulnerabilities of such systems. Particular attention is paid to security issues and problems associated with attacks on such systems: the use of fakes, printed photos and masks, visualized

and generated two- and three-dimensional images and video of faces. The modern approaches to solving such problems, to counteract such attacks are considered. It also examined the legal aspects and laws regulating the processing of biometric data of Russian federation and assesses the risks of attacks on biometric systems.

The main task of the research is to analyze the vulnerabilities of biometric face recognition systems and indicate the main ways of eliminating these vulnerabilities.

Keywords: *Information security, biometrics, face recognition, neural networks, deep learning, identification, face authentication, legal regulation of biometric data.*

1. Введение

Одной из крайне актуальных задач информационной безопасности является разработка надёжных систем биометрической идентификации, в частности систем, основанных на распознавании лиц. Обширность применения подобного рода систем тяжело переоценить. Зачастую такие системы являются частью больших, масштабных платформ, систем и решений, например, таких, как проектирование умных магазинов без касс. Существует концепция построения умных городов, где одной из важнейших частей является система распознавания лиц [1,2]. Также интерес к надёжным системам распознавания обусловлен высокими финансовыми потерями от несанкционированного доступа, от действий киберпреступников по всему миру.

Сильным фактором развития отрасли стало распространение коронавирусной инфекции (COVID). С одной стороны, общество было заинтересовано в выполнении рекомендательных мер всемирной организации здравоохранения, таких, как социальная дистанция, ношение защитных масок – и здесь помогали системы распознавания. С другой стороны, отрасль столкнулась с актуальными проблемами – распознавание лиц в масках, сильно перекрытых лиц. Это привело к появлению новых подходов, новых архитектур и методов [3,4].

Достигнуты значительные успехи в решении задачи распознавания человека по двумерному и трехмерному изображению лица благодаря применению нейронных сетей глубокого обучения с тремя и более слоями [5-13], которые объединяют в себе как выбор и расчет признаков, так и классификацию. Точность методов глубокого обучения при большом количестве слоев (от 10 до 22) и при очень большой обучающей выборке (миллионы образцов) на некоторых известных базах данных, таких как Labelled Faces in the Wild [14] (LFW) превысила точность распознавания человеком и достигла 99.6% [10-12].

Идентификация человека по лицу – одна из наиболее важных современных задач компьютерного зрения и робототехники, как с теоретической, так и с практической точек зрения. К сожалению, существующие в настоящее время системы автоматического распознавания человека по лицу в неконтролируемых условиях до сих пор имеют достаточно большую ошибку.

2. Двумерные системы распознавания

Самые ранние исследования в области распознавания лиц можно отнести к 1960-м годам [15]. Очевидно, что большинство таких систем представляли из себя реализации классических алгоритмов компьютерного зрения, обработки и поиска ключевых точек в двумерном изображении. С течением времени разрабатывались новые алгоритмы, системы распознавания лиц усложнялись и позволяли решать всё более сложные задачи [16-19].

Большинство современных систем распознавания лиц можно представить, как совокупность основных модулей (этапов обработки кадра):

- обнаружение лица;
- предобработка кадра (фильтрация, выравнивание и пр.);
- извлечение признаков, составление n-мерного шаблона;
- сопоставление или поиск в базе;
- решение дополнительных (вспомогательных) задач распознавания (определение пола, возраста, эмоций, наличие улыбки, наличие маски и пр.).

Каждый из этапов может быть представлен широким диапазоном направлений, конкретных решений и технологий.

Основные подходы к обнаружению лица в кадре:

- применение каскадов классификаторов [20];
- использование гистограмм ориентированных градиентов [21];
- применение локальных бинарных патернов [22];

• использование нейронных сетей [23-30].

Задачи, которые решают при составлении шаблона – извлечение ключевых признаков и классификация. Классические алгоритмы извлечения признаков сосредоточены на обработке постоянных черт лица, например, таких, как брови, глаза, нос, рот. Наиболее качественные дескрипторы: LBP [31], Gabor [32], SIFT [33], HOG [34]. Основная задача классификатора – получить относительные расстояния между чертами лица. К широко используемым в классификаторах алгоритмам можно отнести: метод опорных векторов, метод k – ближайших соседей, случайный лес [35-37]. Отдельно стоит отметить применение нейронных сетей различной архитектуры: свёрточные сети, множественные свёрточные сети, глубокие нейронные сети [38-45].

Остро стоит вопрос с распознаванием поддельных лиц, распечатанных фотографий и масок, визуализированных, а также сгенерированных (например нейронными сетями) двумерных изображений лиц (рис 1).

Современные возможности нейронных

Рис. 1. Примеры атак с использованием распечатанной фотографии и с помощью визуализации изображения на экране смартфона

сетей, в частности глубоких нейронных сетей, не всегда используются во благо. Иногда даже человек не способен отличить настоящую фотографию или видео от сгенерированных, с помощью современных методик синтеза (deepfake) (рис 2).

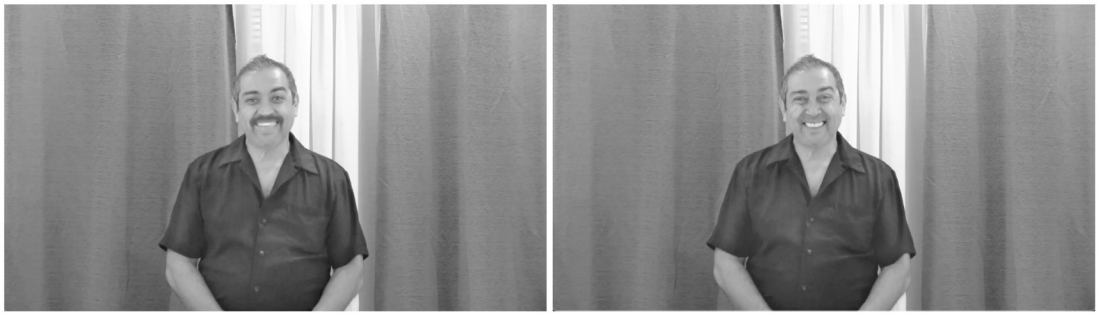

Рис. 2. Настоящее и сгенерированное с помощью deepfake изображения

Традиционные программные методы обнаружения атак с “презентацией” лица основывались на вычислениях параметров, описывающих признаки движения (моргание глаз, движение губ), текстуру лица и качество изображения [46-48]. К сожалению, точность работы подобных методов сильно зависит от тонкой настройки, от человеческого опыта

при извлечении подобного рода информации. Иногда спроектированные пространства признаков не в состоянии отличить подделку от артефактов лица. Именно поэтому внимание сообщества исследователей привлекли нейронные сети, в частности свёрточные сети и сети глубокого обучения [49].

Но несмотря на то, что были достигнуты серьёзные результаты, даже самые современные методы обнаружения атак с "презентацией" лица на основе глубокого обучения показывают неудовлетворительную точность обобщения при подаче изображений, с неизвестными заранее условиями, при работе с группами изображений, полностью отсутствующими в обучающих выборках. Таких примеров достаточно много: этнические и национальные особенности пользователей системы, использование различных датчиков, с которых приходят данные (изображения), отличающееся разрешение изображений/видео, условия окружающей среды (освещение, яркость, контрастность), расстояние между лицом и датчиком. Исследователи стараются решить возникающие проблемы обобщения, можно отметить основные тенденции – использование перекрёстных баз данных [50], применение специальных протоколов перекрёстного обучения и тестирования [51].

Несмотря на ограниченность объёмов обучающих данных есть попытки преодоления подобного рода ограничений:

• глубокое обучение для выявления внутренних различий между реальными и поддельными лицами [52];

• аугментация и искусственный синтез данных [53];

• вспомогательный надзор [53,54];

• адаптация предметной области [55];

• непрерывное обнаружение и обучение на новых типах атак [56].

Yang и другие [53] предложили метод искусственного синтеза данных для имитации спуфинговых атак на основе цифровых носителей, что привело к возможности увеличения объёмов обучающих выборок. Liu и другие [58] предложили увеличить обобщающую способность методов обнаружения "презентации" лица за счёт использования пространственного и временного вспомогательного наблюдения.

Среди последних, пожалуй, самых актуальных работ и исследований стоит отметить [57], авторы которой предложили способы решения некоторых проблем, в частности временной избыточности и межкадровых сдвигов в изображениях, а также представили метод выборки временной последовательности для кодирования и компактного представления видеопотока (рис. 3).

Эффективность такого подхода авторы

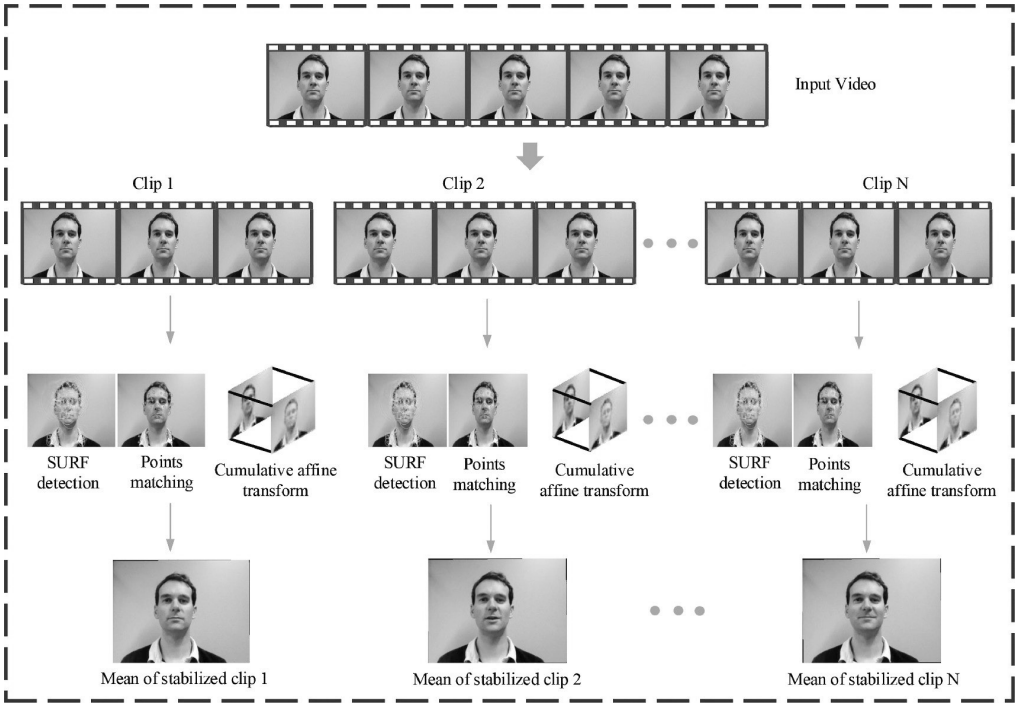

Рис. 3. Метод выборки временной последовательности

продемонстрировали с помощью использования протоколов оценки перекрёстных испытаний базы данных OULU-NPU [51] и нескольких широко используемых конфигураций перекрёстных баз данных. Отдельно стоит отметить, что авторы выложили в открытый доступ исходный код проекта.

Хотя двумерные системы распознавания и достигли серьёзных успехов, на точность распознавания таких систем до сих пор влияют многие факторы и именно поэтому многие исследователи обратились к построению трёхмерных систем распознавания лиц из-за их потенциальных возможностей преодоления присущих 2D систем ограничений и недостатков.

3. Трёхмерные системы распознавания

Для достижения высокой точности и надежности идентификации человека на динамических сценах в реальных условиях использование алгоритмов трехмерного распознавания лиц является перспективным, так как алгоритмы являются инвариантными к изменению освещения, а идентификация личности может быть проведена с разных углов обзора. Алгоритмы трехмерного распознавания используют информацию о форме лица для идентификации отличительных признаков, таких как контур глазниц, носа и подбородка, рис. 4. Однако деформации формы лица при мимических экспрессиях ухудшают качество распознавания [59]. Трехмерное изображение человеческого лица является гораздо более информативным, чем соответствующая двумерная проекция. Из-за сложной топологии формы лица при его динамическом трехмерном описании часто используется деформируемая модель лица [60-63]. С помощью данной модели можно параметрически описать мимические экспрессии человека, и, как следствие, улучшить качество идентификации человека.

Качество алгоритмов трехмерного рас-

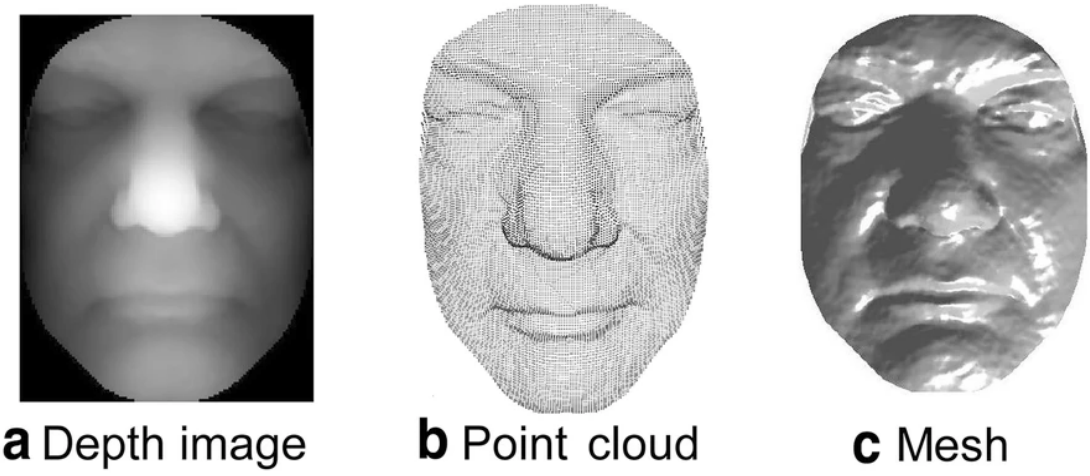

Рис. 4. Пример трёхмерной модели изображения лица

познавания напрямую зависит от точности построения трехмерной модели формы лица человека с помощью регистрации в трехмерном пространстве облаков точек, получаемых от датчиков глубины [64, 65]. Традиционный алгоритм регистрации решает вариационную задачу поиска оптимального геометрического (ортогонального или аффинного) преобразования, который наилучшим образом совмещает два облака точек с заданным соответствием между точками [66]. Выбор вида функционала в задаче оптимизации приводит к различным методам регистрации облаков точек. Наиболее используемыми являются поиск соответствия между парой облаков – точка-точка (point-to-point) и поиск соответствия – точка-плоскость (point-to-plane). Для класса ортогональных преобразований для задачи точка-точка решение в явном виде представлено в классических работах Хорна [67, 68]. Точное решение задачи точка-точка для случая произвольного аффинного преобразования приведено в работе [69]. Вариационная задача точка-плоскость в классе ортогональных преобразований решается с применением итерационного алгоритма Левенберга-Марквардта или методом линеаризации для малых углов [70]. Для вариационной задачи точка-плоскость в классе аффинных преобразований найдено точное

решение [71]. В работе [72] получено приближенное решение задачи точка-плоскость в классе ортогональных преобразований.

Стоит отметить, что метод точка-плоскость является более робастным к шуму датчиков, но для этого метода для класса ортогональных преобразований решение задачи в явном виде пока не найдено. Это усложняет применение метода в задачах, где требуется производить регистрацию в масштабе реального времени. В работе [73] представлен алгоритм динамической регистрации облаков точек, используемый для поиска соответствия между деформируемыми поверхностями. Метод предусматривает разбиение поверхностей на участки, каждый из которых обрабатывается отдельно, а способ объединения результатов регистрации основан на минимизации функционала.

Известно, что использование трехмерной карты окружающего пространства [74,75] существенно улучшает качество распознавания и локализации субъектов на динамических, контекстуально сложных сценах, особенно при частичном или полном закрытии субъектов посторонними предметами. Несмотря на то, что качество карты глубины, получаемое от RGB-D камер, таких, например, как Kinect, в целом хорошее, существуют проблемы с выходной информацией. Так в выходных данных образуются области неопределенности из-за того, что структурированный свет излучения после отражения не попадает на камеру, разрешающая способность измерения глубины сцены падает по квадратичному закону с увеличением глубины сцены [76], а также из-за того, что быстрое движение камеры приводит к потере данных.

В качестве предобработки данных применяются как двумерные, так и трехмерные подходы к задаче регуляризации полной вариации для устранения шума, возникающего при получении трехмерных данных с помощью датчиков глубины. Одним из наиболее эффективных методов фильтрации шума является применение регуляризации полной вариации [77]. В работе [78] описан способ решения задачи регуляризации анизотропной полной вариации в многомерном случае.

Для повышения точности распознавания лиц с использованием векторов признаков (дескрипторов) для предварительного обучения сверточных нейронных сетей на внешних наборах данных применяются различные методы регуляризации. Например, для того, чтобы дескрипторы каждого класса образовывали гиперсферу в многомерном пространстве, был предложен метод center loss [79]. Дескрипторы FaceNet [80] обучаются с помощью минимизации специальной функции потерь (triplet loss), которая приводит к тому, что расстояния между дескрипторами одного человека становятся меньше расстояний между дескрипторами различных людей. Кроме того, в последнее время появились функции потерь, основанные на максимизации зазора между углами, образованными извлекаемыми векторами признаками различных классов, такие, как ArcFace [81]. В то же время на практике замечено, что наиболее точные результаты распознавания лиц получаются с помощью дескрипторов CNC, обученных с помощью оптимизации традиционной функции потерь (softmax loss), если использовать высококачественную большую внешнюю базу данных лиц, такую как VGGFace-2 [82].

Получена количественная оценка точности модели, устойчивости к внешним искажающим факторам, таким как неравномерное и слабое освещение, а также к подвижности человека [83,84]. Для нежесткой математической модели лица, то есть когда лицо подвижно, и его форма может деформироваться, предложен метод построения плотной трехмерной математической модели формы лица по набору изображений и карт глубины, снятых с нескольких RGB-D камер, а также реализована система объединения данных с нескольких камер с использованием модифицированного алгоритма совмещения ICP по динамическому набору облаков точек [85].

При работе с трёхмерными моделями лиц также крайне остро стоит вопрос с распознаванием поддельных лиц, распечатанных трёхмерных масок, визуализированных изображений и видео [88-90], рис. 5. Примеры атак приведены на рис. 6. Разработанные способы обнаружения подделок можно разделить на две основные категории: обработка видимого диапазона, обработка инфракрасного диапазона [87].

Наиболее используемыми характерными чертами лица при обработке видимого диапазона являются текстура [88-90], мимика [91]. Например, совместное использование нескольких дескрипторов локальных двоичных шаблонов (LBP) позволяет обнаружить отличия текстуры между реальным лицом и трёхмерной маской достаточно эффективно

Рис. 5. Примеры напечатанных на трёхмерном принтере масок для лиц

Рис. 6. Примеры атак

[92]. Существуют методы, основанные на применении дистанционной фотоплетизмографии с использованием различных сигналов [93]. Также применяется и анализ поляризации света на коже лица [94]. Стоит отметить, что крупным потенциальным недостатком большинства существующих методов обнаружения подделок с помощью анализа видимого диапазона является чувствительность к окружению (к сцене или фону), к освещению и выражению лица.

В дополнение к видимому спектру многие исследователи рассматривают и инфракрасный спектр. Например, Wang объединил видимый и ближний инфракрасный диапазоны спектра для моделирования характеристик градиента при обнаружении масок из поливинилхлорида, силиконовых масок и фотографий лиц [95]. Такой подход доказал, что разница отражательной способности реальной кожи лица и различных подделок может быть важным фактором при принятии решения. Известны попытки применения глубоких нейронных сетей, а также свёрточных нейронных сетей для анализа мультиспектральных изображений [96-99]. Однако пока рано судить об успешности построенных моделей из-за недостаточного объёма обучающих данных.

Применение трёхмерных моделей при построении современных надёжных систем распознавания является актуальным направлением. Проводятся международные мастер-классы и соревнования по распознаванию подделок, масок [86].

4. Законодательство и правовое регулирование в области обработки и применения биометрических данных

Ключевая законодательная норма, регулирующая правовой режим биометрических данных в Российской Федерации – статья 11 Закона о персональных данных. Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» призван образовать фундамент для Единой биометрической системы, регламентировать связанные с ней процедуры (такие, например, как сбор биометрических данных) и области ее применения – пока что главным образом в финансовых сферах наподобие банковской деятельности. Единая биометрическая система – совместный проект Банка России и «Ро-

стелекома», направленный на сбор биометрической информации и её использование для идентификации пользователей финансовых услуг. Платформа была разработана по инициативе Минкомсвязи и Центрального банка, разработчик и оператор ЕБС — «Ростелеком». В конце 2021 года приобрела статус государственного информационного ресурса.

К основным стандартам отрасли можно отнести: ГОСТ Р 52633.0-2006 (Защита информации, техника защиты информации, требования к средствам высоконадежной биометрической аутентификации), ГОСТ Р 52633.4-2011 (Защита информации, техника защиты информации, интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа), ГОСТ Р 54412-2019 (Информационные технологии, биометрия, общие положения и примеры применения), ГОСТ Р 58624.3-2019 (Информационные технологии, биометрия, обнаружение атаки на биометрическое предъявление).

Самый серьёзный вопрос, возникающий при обсуждении биометрии – риск утечки биометрических данных. К сожалению, утечки происходят из самых разных баз данных, и не так важно, как они защищены от взлома снаружи, поскольку часто это делается изнутри. Компрометация биометрических данных — это самое страшное, что может произойти. Если человек доверил системе свои биометрические данные, и эта система не оправдала его доверия, то у человека в цифровом будущем сломана жизнь. Можно поменять пин-код на карточке, можно поменять паспорт, все что угодно, можно поменять фамилию, но поменять биометрические данные практически невозможно. Задача противодействия подобного рода утечкам является достаточно сложной, объёмной, многофакторной. Один из важнейших факторов - способ представления и хранения биометрических образцов. Обычно в системах хранятся «отпечатки» биометрических данных, то есть наборы зашифрованных данных. Процесс восстановления исходной биометрической информации является вычислительно сложным, зачастую практически невыполнимым.

Многие эксперты отмечают, что, к сожалению, правовое регулирование биометрии в России находится не в идеальном состоянии. Однако процесс формирования единого, структурированного подхода к вопросу регулирования биометрических данных РФ все же уже начался, многие законодательные акты, касающиеся биометрии, сейчас находятся на стадии разработки и конкретизации. Например, 6 апреля текущего года в Государственную Думу был внесён законопроект «О внесении изменений в Федеральный закон о персональных данных, предлагающий регулирование обработки биометрических данных».

5. Выводы

В компьютерном зрении и конкретно в распознавании лиц до сих пор существует много проблем и задач, которые ещё предстоит решить. Использование как двумерных, так и трёхмерных систем распознавания лиц сопряжено с известными проблемами и ошибками. Часть исследователей сосредоточила силы на применении многокомпонентных, гибридных, мультимодальных системах [100-102]. Среди основных направлений, трендов и задач для будущих исследований в отрасли можно указать следующее:

- повышение точности распознавания в сложных условиях;
- построение надёжных алгоритмов и систем обнаружения распечатанных, поддельных и сгенерированных изображений и видео;
- упрощение интерфейсной части подобного рода систем, повышение простоты развёртывания, использования и обслуживания таких систем;
- решение проблемы предвзятости и повышение релевантности систем, расширение обучающих баз в контексте использования изображений людей из различных рас и национальностей, разного цвета кожи и других особенностей;
- распознавание лиц в маске, сильно перекрытых лиц;
- решение и обсуждение этических проблем биометрии, влияние систем распознавания на личную жизнь;
- внедрение систем распознавания в повседневную жизнь, в узкие отрасли: в ритейл системы, в системы оплаты, использование распознавания при мониторинге водителя, управляющего транспортным средством и прочее.

Литература / References

1. G. Praveen, J. Dakala, Face Recognition: Challenges and Issues in Smart City/Environments, Conference: 2020 International Conference on Communication Systems and Networks, pp. 791–793, 2020.

2. M. Bansal, D. Sharma, Facial Recognition System for Security Resolutions in Smart City, International Journal of Advanced Research in Engineering and Technology, 11(10), pp. 146–151, 2020.

3. G. Jeevan, G. Zacharias, M. Nair, J. Rajan, "An empirical study of the impact of masks on face recognition", Pattern Recognition, pp. 108308, 2022.

4. N. Ullah, A. Javed, M. Ghazanfar, A. Alsufyani, S. Bourouis, "A novel DeepMaskNet model for face mask detection and masked facial recognition", Journal of King Saud University – Computer and Information Sciences, 2022.

5. I. Goodfellow, Y. Bengio, A. Courville, A. Deep learning. Cambridge, MA: MIT Press (2016).

6. Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, M.S. Lew, "Deep learning for visual understanding: A review," Neurocomputing, 187, 27–48 (2016).

7. R. He, X. Zhang, S. Ren, J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," Proc. IEEE International Conference on Computer Vision, pp. 1026–1034 (2015).

8. Y. Taigman, M. Yang, M. Ranzato, L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701–1708 (2014).

9. Y. Sun, X. Wang, X. Tang, X., "Deeply learned face representations are sparse, selective, and robust," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 2892–2900 (2015).

10. Y. Sun, D. Liang, X. Wang, X. Tang, X., "Deepid3: Face recognition with very deep neural networks," arXiv 1502.00873.

11. E. Zhou, Z. Cao, Q. Yin, "Naive-deep face recognition: Touching the limit of LFW benchmark or not?" arXiv 1501.04690.

12. F. Schroff, D. Kalenichenko, J. Philbin, J.,"Facenet: A unified embedding for face recognition and clustering," Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 815–823 (2015).

13. W. Rawat, Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," Neural Computation, June 2017. DOI: 10.1162/NECO_a_00990

14. G.B. Huang, M. Ramesh, T. Berg, E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Technical Report 07-49. Amherst: University of Massachusetts.

15. W. W., Bledsoe, "The Model Method in Facial Recognition," Technical Report, PRI 15, Panoramic Research, Inc., Palo Alto, California, 1964.

16. Pentland MT (1991) Face recognition using eigenfaces. Computer vision and pattern recognition. pp. 586–591.

17. Belhumeur PN, Hespanha DJKJP (1997) Eigenfaces vs. fisherfaces: recognition using class specific linear projection. Trans Pattern Anal Mach Intell 19:711–720.

18. Frey BJ, Colmenarez TSH A (1998) Mixtures of local linear subspaces for face recognition. In: Computer vision and pattern recognition.

19. Moghaddam B, Jebara APT (2000) Bayesian face recognition. Pattern Recognit 33:1771–1782.

20. Viola, P.; Jones, M.J. Robust Real-Time Face Detection. Int. J. Comput. Vis. 2004, 57, 137–154.

21. Dalal, N.; Triggs, B. Histograms of Oriented Gradients for Human Detection. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Diego, CA, USA, 20–25 June 2005.

22. Ahonen, T.; Hadid, A.; Pietikainen, M. Face Description with Local Binary Patterns: Application to Face Recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2006, 28, 2037–2041.

23. Deng, J.; Guo, J.; Ververas, E.; Kotsia, I.; Zafeiriou, S. RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 13–19 June 2020; pp. 5202–5211.

24. Zhang, K.; Zhang, Z.; Li, Z.; Qiao, Y. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. IEEE Signal Process. Lett. 2016, 23, 1499–1503.

25. Jiang, H.; Learned-Miller, E. Face Detection with the Faster R-CNN. In Proceedings of the 12th IEEE International Conference on Automatic Face & Gesture Recognition, Washington, DC, USA, 30 May–3 June 2017.

26. Tang, X.; Du, D.K.; He, Z.; Liu, J. PyramidBox: A Context-Assisted Single Shot Face Detector. In Computer Vision—ECCV 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 812–828.

27. Zhang, S.; Chi, C.; Lei, Z.; Li, S.Z. RefineFace: Refinement Neural Network for High Performance Face Detection. arXiv 2019, arXiv:1909.04376v1.

28. Jang, Y.; Gunes, H.; Patras, I. Registration-free Face-SSD: Single shot analysis of smiles, facial attributes, and affect in the wild. Comput. Vis. Image Underst. 2019, 182, 17–29.

29. Yashunin, D.; Baydasov, T.; Vlasov, R. MaskFace: Multi-task face and landmark detector. arXiv 2020, arXiv:2005.09412v1.

30. Chen, W.; Huang, H.; Peng, S.; Zhou, C.; Zhang, C. YOLO-face: A real-time face detector. Vis. Comput. 2020, 37, 805–813.

31. Yang, B.; Chen, S. A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image. Neurocomputing 2013, 120, 365–379.

32. Vinay, A.; Shekhar, V.; Murthy, K.B.; Natarajan, S. Face Recognition Using Gabor Wavelet Features with PCA and KPCA—A Comparative Study. Procedia Comput. Sci. 2015, 57, 650–659.

33. Bakhshi, Y.; Kaur, S.; Verma, P. Face Recognition using SIFT, SURF and PCA for Invariant Faces. Int. J. Eng. Trends Technol. 2016, 34, 39–42.

34. Dadi, H.S.; Pillutla, G.K.M. Improved Face Recognition Rate Using HOG Features and SVM Classifier. IOSR J. Electron. Commun. Eng. 2016, 11, 34–44.

35. Kremic, E.; Subasi, A. Performance of random forest and SVM in face recognition. Int. Arab J. Inf. Technol. 2016, 13, 287–293.

36. Dadi, H.S.; Pillutla, G.K.M.; Makkena, M.L. Face Recognition and Human Tracking Using GMM, HOG and SVM in Surveillance Videos. Ann. Data Sci. 2017, 5, 157–179.

37. Tee, T.X.; Khoo, H.K. Facial Recognition Using Enhanced Facial Features K-Nearest Neighbor (k-NN) for Attendance System. In Proceedings of the 2nd International Conference on Information Technology and Computer Communications, Kuala Lumpur, Malaysia, 12–14 August 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 14–18.

38. Huang, G.B.; Ramesh, M.; Berg, T.; Learned-Miller, E. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments; Technical Report 07-49; University of Massachusetts: Amherst, MA, USA, 2007.

39. Schroff, F.; Kalenichenko, D.; Philbin, J. FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7–12 June 2015.

40. Sun, Y.; Liang, D.; Wang, X.; Tang, X. DeepID3: Face Recognition with Very Deep Neural Networks. arXiv 2015, arXiv:1502.00873v1.

41. Ranjan, R.; Castillo, C.D.; Chellappa, R. L2-constrained Softmax Loss for Discriminative Face Verification. arXiv 2017, arXiv:1703.09507.

42. Wang, H.; Wang, Y.; Zhou, Z.; Ji, X.; Gong, D.; Zhou, J.; Li, Z.; Liu, W. CosFace: Large Margin Cosine Loss for Deep Face Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018.

43. Zheng, Y.; Pal, D.K.; Savvides, M. Ring loss: Convex Feature Normalization for Face Recognition. arXiv 2018, arXiv:1803.00130.

44. Deng, J.; Guo, J.; Xue, N.; Zafeiriou, S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019.

45. Alghaili, M.; Li, Z.; Ali, H.A.R. FaceFilter: Face Identification with Deep Learning and Filter Algorithm. Sci. Program. 2020, 2020, 7846264.

46. K. Kollreider, H. Fronthaler, M.I. Faraj, J. Bigun Real-time face detection and motion analysis with application in liveness assessment IEEE Trans. Inf. Forensics Secur., 2 (3) (2007), pp. 548-558.

47. Z. Boulkenafet, J. Komulainen, A. Hadid Face spoofing detection using colour texture analysis IEEE Trans. Inf. Forensics Secur., 11 (8) (2016), pp. 1818–1830.

48. D. Wen, H. Han, A.K. Jain Face spoof detection with image distortion analysis IEEE Trans. Inf. Forensics Secur., 10 (4) (2015), pp. 746–761.

49. Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, G. Zhao, Deep learning for face anti-spoofing: a survey, arXiv preprint: 2106.14948(2021b).

50. T. de Freitas Pereira, A. Anjos, J.M. De Martino, S. Marcel Can face anti-spoofing countermeasures work in a real world scenario? International Conference on Biometrics (ICB) (2013).

51. Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid OULU-NPU: a mobile face presentation attack database with real-world variations IEEE International Conference on Automatic Face & Gesture Recognition (FG) (2017), pp. 612–618.

52. A. Jourabloo, Y. Liu, X. Liu Face de-spoofing: anti-spoofing via noise modeling European Conference on Computer Vision (ECCV) (2018), pp. 290–306.

53. X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, Z. Li, W. Liu Face anti-spoofing: model matters, so does data IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2019), pp. 3507–3516.

54. Z. Yu, J. Wan, Y. Qin, X. Li, S.Z. Li, G. Zhao NAS-FAS: static-dynamic central difference network search for face anti-spoofing IEEE Trans. Pattern Anal. Mach. Intell., 43 (9) (2021), pp. 3005–3023.

55. A. Mohammadi, S. Bhattacharjee, S. Marcel Domain adaptation for generalization of face presentation attack detection in mobile settengs with minimal information IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020).

56. M. Rostami, L. Spinoulas, M. Hussein, J. Mathai, W. Abd-Almageed Detection and continual learning of novel face presentation attacks International Conference on Computer Vision (ICCV) (2021).

57. U. Muhammad, Z. Yu, J. Komulainen, Self-supervised 2D face presentation attack detection via temporal sequence sampling Pattern Recognition Letters, Volume 156, April 2022, Pages 15–22.

58. Y. Liu, A. Jourabloo, X. Liu Learning deep models for face anti-spoofing: Binary or auxiliary supervision IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2018), pp. 389–398.

59. G. Rajamanoharan, S. Zafeiriou, M. Pantic, L. Yin, "Static and dynamic 3D facial expression recognition: A comprehensive survey," Image Vis. Comput., Vol. 30 (10), pp. 683–697 (2012).

60. G. Pan, X. Zhang, Y. Wang, Z. Hu, X. Zheng, Z. Wu, "Establishing point correspondence of 3D faces via sparse facial deformable model," IEEE Trans. Image Process., Vol. 22 (11), pp. 4170–4181 (2013).

61. C. Cao, Q. Hou, K. Zhou, "Displaced dynamic expression regression for real-time facial tracking and animation," ACM Trans. Graph., Vol. 33 (4), pp. 43:1–43:10 (2014).

62. X. Zhang, L. Yin, J.F. Cohn, S. Canavan, M. Reale, A. Horowitz, P. Liu, J.M. Girard, "BP4D Spontaneous: a high-resolution spontaneous 3D dynamic facial expression database," Image Vis. Comput., Vol. 32 (10), pp. 692–706 (2014).

63. X. Li, Q. Ruan, Y. Jin, G. An, R. Zhao, "Fully automatic 3D facial expression recognition using polytypic multi-block local binary patterns," Signal Processing, Vol. 108, pp. 297–308 (2015).

64. G. Tam, Z.-Q. Cheng, Y.-K. Lai, F. Langbein, Y. Liu, D. Marshall, R. Martin, X.-F. Sun, P. Rosin, "Registration of 3D point clouds and meshes: A survey from rigid to nonrigid," IEEE Trans. Vis. Comput. Graph., Vol. 19 (7), pp. 1199–1217 (2013).

65. S. Cheng, I. Marras, S. Zafeiriou, M. Pantic, "Statistical non-rigid ICP algorithm and its application to 3D face alignment," Image Vis. Comput., Vol. 58, pp. 3–12 (2017).

66. P. Besl and N. McKay, "A method for registration of 3-D shapes," IEEE Transactions of Pattern Analysis and Machine Intelligence, Vol. 14 (2), pp. 239–256 (1992).

67. B. Horn, "Closed-Form Solution of Absolute Orientation Using Unit Quaternions," Journal of the Optical Society of America A, Vol. 4(4), pp. 629–642 (1987).

68. B. Horn B., H. Hilden and S. Negahdaripour S., "Closed-form Solution of Absolute Orientation Using Orthonormal Matrices," Journal of the Optical Society of America A, Vol. 5 (7), pp. 1127–1135 (1988).

69. S. Du, N. Zheng, S. Ying and J. Liu, "Affine iterative closest point algorithm for point set registration," Pattern Recognition Letters, Vol. 31, pp. 791–799 (2010).

70. K.L. Low, "Linear least-squares optimization for point-to-plane ICP surface registration," Technical Report TR04-004, Department of Computer Science, University of North Carolina at Chapel Hill, 2004.

71. Makovetskii A., Voronin S., Kober V. and Tihonkih D., "An efficient point-to-plane registration algorithm for affine transformations," Proc. SPIE 10396, Applications of Digital Image Processing XL, pp. 103962J (2017).

72. K. Khoshelham, "Closed-form solutions for estimating a rigid motion from plane correspondences extracted from point clouds," ISPRS Journal of Photogrammetry and Remote Sensing, Vol. 114, pp. 78–91 (2016).

73. S. Cheng, I. Marras and S. Zafeiriou, "Active nonrigid ICP algorithm," Proc. 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition, pp. 1–8 (2015).

74. J.A. Gonzalez-Fraga, V.H. Diaz-Ramirez, V. Kober, J.J. Tapia-Higuera, O. Alvarez-Xochihua, "An efficient algorithm for matching of SLAM video sequences," Proc. SPIE's 61 Annual Meeting: Applications of Digital Image Processing XXXIX, Vol. 9971, pp. 99712Z-10 (2016).

75. J.A. Gonzalez-Fraga, V. Kober, V.H. Diaz-Ramirez, "Accurate generation of the 3d map of environment with a rgb-d camera," Proc.SPIE. Vol. 10396. pp. 10396–7 (2017).

76. K. Khoshelham, S.O. Elberink, "Accuracy and resolution of kinect depth data for indoor mapping applications," Sensors. Vol. 12(2), pp. 1437–1454 (2012).

77. A. Chambolle and T. Pock, "An introduction to continuous optimization for imaging," Acta Numerica, Vol. 25, pp, 161–319 (2016).

78. S. Yang, J. Wang, W. Fan, X. Zhang, P. Wonka and J. Ye, "An efficient ADMM algorithm for multidimensional anisotropic total variation regularization problems," Proc. 19th ACM SIGKDD International conference on Knowledge discovery and data mining, pp. 641–64 (2013).

79. Wen, Y., Zhang, K., Li, Z., and Qiao, Y. A discriminative feature learning approach for deep face recognition. In European Conference on Computer Vision, pages 499–515. Springer (2016).

80. Schroff, F., Kalenichenko, D., and Philbin, J. FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 815–823 (2015).

81. Deng, J., Guo, J., Xue, N., and Zafeiriou, S. ArcFace: Additive angular margin loss for deep face recognition. arXiv preprint arXiv:1801.07698 (2018).

82. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., and Zisserman, A. (2018). VGGFace2: A dataset for recognising faces across pose and age. In Proceedings of the International Conference on Automatic Face & Gesture Recognition (FG 2018), pages 67–74. IEEE

83. Ruchay, A.N., Dorofeev, K.A., Kober, A.V. Accurate reconstruction of the 3D indoor environment map with a RGB-D camera based on multiple ICP // CEUR Workshop Proceedings, 2210, 2018. Pp. 300–308.

84. Ruchay, A.N., Dorofeev, K.A., Kober, A.V. Accuracy analysis of 3D object reconstruction using RGB-D sensor // CEUR Workshop Proceedings, 2210, 2018. pp. 82–88.

85. Ruchay, A.N., Dorofeev, K.A., Kolpakov, V.I. Fusion of information from multiple kinect sensors for 3D object reconstruction // Computer Optics, 42 (5), 2018. pp. 898–903.

86. 3rd Chalearn Face Anti-spoofing Workshop and Challenge. Workshop Schedule (11 October, 2021).

87. P. Sun, D. Zeng, X. LI, L. Yang, L. Li, Z. Chen, F. Chen. A 3D Mask Presentation Attack Detection Method Based on Polarization Medium Wave Infrared Imaging // Symmetry, 12(3), 2020.

88. Z. Boulkenafet, J. Komulainen, A. Hadid. Face spoofing detection using colour texture analysis. IEEE Trans. Inf. Forensics Secur. 2016, 11, 1818–1830.

89. D. Wen, H. Han, A. Jain. Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics. Secur. 2015, 10, 746–761.

90. A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, A. Noore. Face Presentation Attack with Latex Masks in Multispectral Videos. In Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition Workships, Honolulu, HI, USA, 21–26 July 2017; pp. 275–283.

91. S. Bharadwaj, T. Dhamecha, M. Vatsa, R. Singh. Computationally Efficient Face Spoofing Detection with Motion Magnification. In Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition Workships, Portland, OR, USA, 23–28 June 2013; pp. 105–110.

92. N. Erdogmus, S. Marcel. Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur. 2014, 9, 1084–1097.

93. S. Liu, P. Yuen, S. Zhang, G. Zhao. 3D mask face anti-spoofing with remote photoplethysmography. Lect. Notes Comput. Sci. 2016, 9911, 85–100.

94. A. Abd, H. Wei, J. Ferryman. Face Anti-Spoofing Countermeasure: Efficient 2D Materials Classification Using Polarization Imaging. In Proceedings of the IEEE International Workshop on Biometrics and Forensics, Coventry, UK, 4–5 April 2017.

95. Y. Wang, X. Hao, Y. Hou, C. Guo. A New Multispectral Method for Face Liveness Detection. In Proceedings of the Second IAPR Asian Conference on Pattern Recognition, Naha, Japan, 5–8 November 2013; pp. 922–926.

96. J. Liu, A. Kumar. Detecting Presentation Attacks from 3D Face Masks under Multispectral Imaging. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops,

Salt Lake City, UT, USA, 18–22 June 2018; pp. 47–52.

97. A. Krizhevsky, I. Sutskever, G. Hinton. ImageNet Classification with Deep Convolutional Neural Networks; NIPS. Curran Associates Inc.: New York, NY, USA, 2012; Volume 60, pp. 84–90.

98. K. Kotwal, S. Bhattacharjee, S. Marcel. Multispectral Deep Embeddings as a Countermeasure to Custom Silicone Mask Presentation Attacks. IEEE Trans. Biom. Behav. Identity Sci. 2019, 1, 238–251.

99. X. Tan, Y. Li, J. Liu, L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. Lect. Notes Comput. Sci. 2010, 6316, 504–517.

100. Elaggoune, Hocine & Belahcene, Mebarka & Bourennane, Salah. (2022). Hybrid descriptor and optimized CNN with transfer learning for face recognition. Multimedia Tools and Applications. 81. 10.1007/s11042-021-11849-1.

101. Sumegh Tharewal, Timothy Malche, Pradeep Kumar Tiwari, Mohamed Yaseen Jabarulla, Abeer Ali Alnuaim, Almetwally M. Mostafa, Mohammad Aman Ullah, "Score-Level Fusion of 3D Face and 3D Ear for

Multimodal Biometric Human Recognition", Computational Intelligence and Neuroscience, vol. 2022, Article ID 3019194, 9 pages, 2022.

102. Szczuko, P.; Harasimiuk, A.; Czyżewski, A. Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application. Sensors 2022, 22, 2356.

ДОРОФЕЕВ Константин Андреевич, старший преподаватель кафедры компьютерной безопасности и прикладной алгебры Челябинского государственного университета. 454001, г. Челябинск, ул. Бр. Кашириных, 129. E-mail: kostuan1989@mail.ru

DOROFEEV Konstantin, Senior Lecturer of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. 129 Br. Kashirinykh St., Chelyabinsk, 454001. E-mail: kostuan1989@mail.ru