ОТЗЫВ

официального оппонента к.т.н. Трекина Алексея Николаевича

на диссертационную работу Ефимова Юрия Сергеевича

«Методы детектирования подделок в биометрических системах на мобильном устройстве»,

представленную на соискание ученой степени кандидата технических наук

по специальности 05.13.17 – «Теоретические основы информатики»

Диссертация посвящена разработке, реализации и внедрению алгоритмов выявления подделок в системах биометрической идентификации человека по изображению и видео радужной оболочки глаза и лица, получаемым при помощи камер мобильного устройства. Технологии биометрического распознавания уже давно содержат встроенные модули проверки живости входных данных, однако мобильные версии таких систем обладали рядом ограничений и недостатков, связанных с низким качеством используемых изображений, большим разнообразием условий их регистрации и доступностью вспомогательных сенсоров обнаружения подделок. Особенно остро эта проблема стоит для биометрических модальностей лица и радужной оболочки глаза человека, наиболее подверженных внутриклассовой изменчивости в зависимости от сценариев их получения при помощи камеры мобильного устройства.

В последние годы глубокое обучение – активно развивающаяся область машинного обучения, связанная с применением глубоких свёрточных нейронных сетей, позволило преодолеть множество барьеров в компьютерном зрении и достигнуть точности алгоритмов, сопоставимой с таковой у человека-эксперта. Среди наиболее распространённых решаемых задач – классификация и сегментация изображений, детектирование объектов на одиночном растре и в видеопотоке. Характерным ограничением таких методов является высокая вычислительная сложность, требующая применения высокопроизводительных ускорителей (графических карт, TPU) для возможности обработки входных сигналов в режиме реального времени, в то время как интеграция в мобильное устройство подразумевает использование вычислительно эффективных алгоритмов.

Работа соискателя стоит на стыке этих двух проблем, предлагая решения задачи определения живости для наиболее уязвимых к подделыванию биометрических модальностей, при сохранении низкой вычислительной сложности, и таким образом является актуальной.

Структура и содержание диссертации

Диссертация состоит из введения, обзора литературы, пяти глав, заключения и списка литературы.

Во введении обосновываются актуальность, достоверность и значимость работы. Кратко описаны научные результаты и представлены выносимые на защиту положения.

Первая глава посвящена обзору основных методов биометрической идентификации человека и подходов к обнаружению попыток подделывания для разных типов входной информации. Рассмотрены характерные особенности биометрического распознавания человека с мобильного устройства. Выделены основные требования, предъявляемые к методам обнаружения подделок в мобильных биометрических приложениях.

Во второй главе описан разработанный алгоритм определения живости лица для мобильных систем распознавания с единственной камерой видимого спектра излучения. Алгоритм учитывает особенности мобильных биометрических приложений, такие как ограничения по вычислительным ресурсам, требования по скорости работы и устойчивость к изменчивым условиям съёмки и потенциально низкому качеству входных изображений. В алгоритме присутствует многоступенчатая система оценки качества и обнаружения явных артефактов подделывания, позволяющая сократить время отклика системы путём раннего отказа от распознавания для наиболее характерных попыток взлома.

В третьей главе рассмотрена задача выявления подделок лица при помощи стереокамеры с малым стереобазисом с учётом сценариев применения мобильной

биометрической системы пользователем и значительной изменчивость условий съёмки. Собрана база данных стереоизображений, содержащая примеры распространённых способов подделывания и соответствующие примеры подлинных лиц. Разработан метод, позволяющий определять живость входного стереоизображений, основанный на применении подходов глубокого обучения и специальной новой функции потерь. Метод продемонстрировал высокие точность и обобщающую способность при тестировании на тестовом наборе данных, содержащем стереоизображения лиц, полученные при помощи мобильного устройства в крайне разнообразных условиях окружения.

Четвёртая глава посвящена выбору и реализации метода обнаружения границ радужной оболочки на изображении. В соответствии с последними тенденциями в обработке изображений и вычислительными ограничениями мобильных приложений выбран метод аппроксимации границ окружностями, параметры которых определяются при помощи классификационной нейронной сети семейства MobileNets с количеством классов, соответствующим разрешению входного изображений. Результаты проверены экспериментально на двух группах наборов данных, как высокого, так и низкого качества, а также при помощи мобильного устройства проведена оценка производительности.

В пятой главе рассмотрена задача обнаружения подделок радужки в мобильных биометрических системах. Рассмотрена устойчивость методов как к известным способам подделывания, так и к ранее не исследовавшимся методам взлома. Описана собранная база изображений, содержащая новые виды подделок. Разработан метод, позволяющий различать живой глаз и подделку, демонстрирующий лучшие результаты по сравнению с описанными в литературе аналогами.

В заключении представлены результаты работы, позволяющие сделать вывод о значимости проведённого исследования.

Автореферат соответствует тексту диссертации и отражает все основные моменты проделанной работы.

1. **Научная новизна представленных результатов**

Научная новизна диссертации состоит в том, что разработаны новые методы и алгоритмы для обнаружения границ радужки, обнаружения подделок лица при помощи единственной камеры видимого спектра излучения и стереокамеры с малым стереобазисом, обнаружения подделок радужки, превосходящие аналогичные существующие методы решения рассматриваемых задач.

Разработан оригинальный многоступенчатый алгоритм защиты от спуфинга для изображений лиц, позволяющий повысить качество решения и снизить время отклика, отбрасывая малопригодные для распознавания растры на ранних этапах анализа.

Разработан метод, позволяющий использовать фронтальную стереокамеру мобильного устройства для повышения устойчивости к наиболее распространённым видам атак при определения живости лица.

Впервые рассмотрены некоторые виды атак на системы идентификации по радужке и исследованы методы защиты от них, предложен собственный метод, показывающий высокие результаты как для ранее изученных способов атак, так и для новых видов.

2. **Достоверность представленных результатов**

Достоверность результатов подтверждена численными экспериментами, проведёнными, в том числе, с использованием открытых наборов тестовых данных. Проведён обзор литературы, а результаты исследований представлены на тематических научных и научно-практических конференциях.

3. **Значимость представленных результатов**

Значимость полученных результатов подтверждена внедрением результатов работы в практическую эксплуатацию. Разработанные методы и алгоритмы не только обеспечивают высокую точность, но и оптимизированы для работы не мобильном телефоне с точки зрения производительности, что позволяет внедрить их в эксплуатацию на широком спектре реальных устройства.

4. **Замечания**

К работе можно указать следующие замечания:

1. Не опубликованы (или не указаны как опубликованные) собранные автором наборы данных, использующихся для сравнения методов в третьей и пятой главах, которые могли бы быть использованы при оценке качества новых методов.
2. Для алгоритма обнаружения подделок радужной оболочки глаза не приведены сравнения с наиболее современными (после 2017 года) методами защиты от спуфинга.
3. В четвёртой и пятой главах при сравнении производительности предложенного метода с аналогами не указано, какая программная реализация методов использовалась, что ставит под сомнение справедливость сравнения быстродействия.
4. В четвертой главе, по сравниению с прочими, не раскрыта практическая значимость метода локализации, применимость в реальных мобильных устройствах.

5. **Заключительная оценка**

Приведённые замечания не снижают общей высокой оценки диссертационной работы.

Результаты диссертации изложены в семнадцати публикациях, пять из которых входят в перечень рекомендованных ВАК РФ. Опубликованные работы и автореферат достаточно полно отражают содержание диссертации. Результаты докладывались на Всероссийских и международных конференциях.

Диссертационная работа Ефимова Ю.С. «Методы детектирования подделок в биометрических системах на мобильном устройстве» полностью соответствует требованиям ВАК РФ (пп. 9-14 «Положения о присуждении учёных степеней», утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842), предъявляемым к диссертациям на соискание учёной степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики», а её автор, Ефимов Юрий Сергеевич, заслуживает присуждения ему учёной степени кандидата технических наук по этой специальности.

Официальный оппонент
кандидат технических наук
старший инженер-исследователь в сфере искусственного интеллекта по направлению оптимизации управленческих решений в целях снижения углеродного следа исследовательского центра «Сколковский институт науки и технологий»
Адрес: 143026, Москва, Территория Инновационного Центра «Сколково», ул. Нобеля, д. 3
Моб.: +79104948641
e-mail: alexey.trekin@yandex.ru

Трёкин Алексей Николаевич

17.08.2022 г.

Подпись Трекина А.Н. подтверждаю.
РУКОВОДИТЕЛЬ ОТДЕЛА КАДРОВОГО АДМИНИСТРИРОВАНИЯ
Гук О.С