«УТВЕРЖДАЮ»
Проректор Московского государственного университета имени М.В.Ломоносова
доктор физико-математических наук, профессор
_____ Федянин А.А.
«16» 08 2022 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова»
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»

Актуальность темы диссертации

В настоящее время биометрия, то есть измерение характеристик организма человека, и основанные на ней методы быстро распространяются в различных сферах деятельности человека. Одним из основных применений является биометрическая идентификация, то есть распознавание или подтверждение личности. Здесь особенно интенсивно развиваются методы и приложения,предназначенные для мобильных устройств. Постоянно расширяется разнообразие финансовых и иных ответственных операций, производимых при помощи мобильных устройств, что требует опознавания пользователя, которое должнообладатьвысоким уровнемточности и безопасности. Существенная уязвимость биометрических технологий — возможность взлома при помощи поддельных характеристик.Мобильные системыбиометрической идентификациииимеют ряд особенностей: работа в изменчивых условиях окружения, широкий набор сценариев взаимодействия с пользователем, выполнение на устройствах с низкой вычислительной мощностью, невозможность использования дополнительных подсистем определения живости пользователя. Таким образом, существует необходимость в создании новых методов и алгоритмов, которые позволили бы обеспечить достаточную степень защиты от взлома при помощи подделок, обладая при этом малой вычислительной сложностью.

Диссертация Ю.С. Ефимова посвящена исследованию и разработке методов и алгоритмов, позволяющих осуществлять защиту от подделывания лица и радужной оболочки глаза на мобильном устройстве. Предложенные методы позволяют обеспечивать высокую

точность детектирования, сопоставимую с немобильными приложениями, при этом малая вычислительная сложность позволяет применять их в режиме реального времени на устройствах с ограниченными вычислительными ресурсами.

Структура и содержание диссертации

Диссертация состоит из введения, обзора литературы, пяти глав, заключения и списка литературы. Во введении обосновывается актуальность работы, сформулированы цели и задачи, отражена практическая значимость полученных результатов, аргументирована научная новизна, представлены выносимые на защиту научные положения.

В первой главе дан обзор биометрических методов распознавания и обнаружения попыток взлома при помощи подделок. Приводится общая схема систем распознавания по лицу и радужки и место в ней подсистемы защиты от подделок. Рассмотрены особенности мобильных приложений биометрических технологий. Сформулированы общие требования к алгоритмам обнаружения подделок для мобильных систем распознавания с учетом сценариев их применения пользователем.

Во второй главе рассматриваются основные трудности построения системы защиты от взлома для алгоритма распознавания по лицу с мобильного устройства, использующего единственную фронтальную камеру видимого спектра излучения. Приведена классификация способов подделывания по уровням квалификации взломщиков, характеристикам физических артефактов и воспроизводимости биометрической информации. Подчеркивается насколько существенно может отличаться качество изображения, полученного в сложных условиях, от изображений, полученных в условиях, регламентированных международными стандартами. Предложен метод, позволяющий обнаруживать известные на данный момент способы подделывания лица, адаптированный к сценариям применения в мобильном устройства. В основе метода лежит многостадийная структура алгоритма с расширенным набором критериев обнаружения артефактов, присущих поддельным биометрическим характеристикам. Особенностью метода является возможность повышения скорости отклика системы за счёт раннего отказа от распознавания при обнаружении явных попыток взлома, а также использование информации об окружении, получаемой из метаданных кадра и от сенсоров смартфона. Показано, что подход позволяет обеспечить защиту от подделывания в режиме реального времени и достичь уровня безопасности, требуемого современной индустрией для мобильных биометрических приложений.

Третья глава посвящена исследованию возможности повышения уровня безопасности системы обнаружения подделок лица за счёт использования стереоинформации, получаемой при помощи пары камер видимого спектра излучения с малым стереобазисом, внедряемых в мобильные устройства. Рассмотрены распространённые способы подделывания и построения нейросетевого классификатора живости с использованием информации о глубине сцены. Предложен метод детектирования подделок, использующий методологию глубокого обучения. Предложена новая функция потерь, призванная регуляризовать внутренние представления сети с целью учёта стереоинформации, содержащейся в паре входных

изображений, и повышения обобщающей способности. Даны оценки точности классификации подлинных и поддельных примеров, в том числе с помощью данных открытой базы стереоизображений лиц, содержащей сценарии съёмки, характерные для мобильных биометрических приложений. Приведена оценка производительности метода на мобильном устройства.

Четвёртая глава посвящена рассмотрению особенностей выделения области радужки на изображениях путём аппроксимации её границ окружностями. Приведён обзор существующих методов и их классификация. Рассмотрены новые подходы к выделению области радужки с применением свёрточных нейронных сетей и методологии глубокого обучения. Предложена новая архитектура на основе моделей семейства MobileNets, позволяющая решать задачу аппроксимации путём сведения к классификации на набор классов, соответствующих требуемому разрешению используемых изображений. Проведены эксперименты по оценке точности поиска границ радужки с использованием нескольких наборов данных, содержащих как примеры растров высокого качества, так и характерные для мобильных приложений низкокачественные изображения. Проведено сравнение предложенного решения с существующими по точности и производительности, демонстрирующее его применимость. Произведена оценка времени выполнения на мобильном устройстве, которая показала возможность применения методов на мобильном устройстве в режиме реального времени.

Пятая глава посвящена методам защиты от подделывания радужки. Произведен обзор и классификация существующих методов. Рассмотрены новые виды подделок. Предложена модель защиты от подделок с использованием свёрточной нейросети. Произведено сравнение метода с известными из литературы аналогами. Показана возможность применения метода на мобильном устройстве.

В заключении представлены основные результаты работы.

Основные результаты диссертации и их научная новизна

К основным результатам и особенностям диссертации Ю.С. Ефимова можно отнести:

1. Исследованы методы защиты от подделок лица для систем распознавания с единственной камерой видимого света. Предложена новая многостадийная структура алгоритма защиты от подделок, особенностью которой является система ранних отказов от распознавания для изображений, содержащих характерные для спуфинга артефакты, и возможность работы в режиме реального времени на мобильном устройстве в разнообразных сценариях применения в изменчивых условиях окружения.
2. Исследованы особенности защиты от подделывания лица с применением стереоинформации, извлекаемой при помощи пары камер мобильного устройства с малым стереобазисом. Разработана нейросетевая модель определения живости лица на стереоизображении, обучаемая при помощи новой функции потерь с целью

повышения обобщающей способности и качества решения. Предложенная модель позволяет осуществлять обработку пар изображений в режиме реального времени.

3. Разработана новая архитектура нейросетей для задачи аппроксимации границ радужки на изображении окружностями, допускающая применение в режиме реального времени для растров низкого качества, получаемых при помощи мобильного устройства.
4. Исследована специфика обнаружения подделок радужки для мобильных биометрических систем. Разработана новая архитектура нейросети, позволяющая обеспечивать устойчивую защиту от подделок в режиме реального времени, в том числе, и от ранее не рассматриваемых.

Достоверность полученных результатов

Степень достоверности результатов подтверждается проработкой литературы по теме диссертации, наличием проведенных численных экспериментов и их подробным описанием, а также внедрением результатов в практическое использование. Основные положения, сформулированные в работе Ю.С. Ефимов, получили апробацию на международных и российских конференциях. Основные результаты изложены в семнадцати работах, опубликованных в рецензируемых научных изданиях.

Значимость полученных результатов

Работа Ю.С.Ефимова носит преимущественно прикладной характер. Созданные методы, алгоритмы, программный код, а также собранные базы данных и их разметка могут быть использованы для при создании систем защиты от подделок в комплексах биометрического распознавания. Программные реализации алгоритмоввнедрены вкомпании SamsungElectronics и применяются в моделях смартфонов, выпускаемых с 2018 года.

Замечания

1. Во второй главе не рассмотрен случай работы в условиях пониженной освещённости, о котором упоминается при анализе проблем обнаружения подделок на мобильном устройстве.
2. В третьей главе не приведён подробный анализ производительности решения в зависимости от условия съёмки стереоизображения и наблюдаемой дистанции до пользователя.
3. В четвёртой главе не приведено сравнение по точности решения с иными современными нейросетевыми подходами к выделению области радужки.

Заключительная оценка

Отмеченные недостатки не оказывают влияния на положительную оценку диссертационной работы в целом.

Результаты диссертации изложены в семнадцати публикациях, пять из которых входят в перечень рекомендованных ВАК РФ. Опубликованные работы достаточно полно отражают содержание диссертации. Результаты докладывались на всероссийских и международных конференциях. В диссертации приведены все необходимые ссылки на цитируемые источники в соответствии с п. 14 «Положения о присуждении ученых степеней».

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 ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842), предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики», а её автор, Ефимов Ю.С., заслуживает присуждения ему ученой степени кандидата технических наук по данной специальности.

Диссертация и настоящий отзыв были обсуждены и одобрены на научном семинаре кафедры математических методов прогнозирования Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова», протокол №1 от 9 августа 2022 г.

Председатель семинара
доктор физико-математических наук, профессор РАН
Дьяконов Александр Геннадьевич

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова», факультет вычислительной математики и кибернетики, кафедра математических методов прогнозирования.

Почтовый адрес: 119991, г. Москва, Ленинские горы, д.1
Телефон: +7 (495) 939-10-00
Сайт: www.msu.ru
e-mail: cmc@cs.msu.ru

Подпись профессора кафедры математических методов прогнозирования
Удостоверяю: декан факультета ВМК МГУ имени М.В. Ломоносова

академик РАН И.А. Соколов