На правах рукописи

Ефимов Юрий Сергеевич

Методы детектирования подделок в биометрических системах на мобильном устройстве

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Москва – 2022

Работа выполнена в *Федеральном исследовательском центре «Информатика и Управление» Российской академии наук (ФИЦ ИУ РАН).*

Научный руководитель: **Матвеев Иван Алексеевич**

доктор технических наук, главный научный сотрудник отдела № 31 Федерального исследовательского центра «Информатика и управление» Российской академии наук

Официальные оппоненты: **Орлов Алексей Александрович**

доктор технических наук, доцент, заведующий кафедрой физики и прикладной математики Муромского института (филиала) ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», г. Муром, Владимирская область

Трёкин Алексей Николаевич

кандидат технических наук, старший инженер-исследователь Исследовательского центра в сфере искусственного интеллекта Сколковского института науки и технологий

Ведущая организация: ФГБОУ ВО «Московский Государственный Университет имени М.В. Ломоносова»

Защита состоится 15 сентября 2022 г. в 14 часов на заседании диссертационного совета Д 002.073.05 при Федеральном исследовательском центре «Информатика и управление» Российской академии наук (ФИЦ ИУ РАН) по адресу 119333, г. Москва, ул. Вавилова, д. 40.

С диссертацией можно ознакомиться в библиотеке и на сайте ФИЦ ИУ РАН http://frccsc.ru.

Автореферат разослан «____» _____ 2022 г.

Ученый секретарь
диссертационного совета Д 002.073.05,
кандидат технических наук *Рейер И.А.*

Актуальность темы исследования. Способы проверки подлинности разного рода информации в обществе прошли долгий путь эволюционного развития от механических замков, ключей, систем печатей и кодовых фраз до подходов автоматизированной и автоматической аутентификации. Жизнь современного человека на регулярной основе включает разного рода верификации тех или иных персональных данных: осуществление финансовых транзакций, приобретение товаров и услуг, доступ к устройствам и сервисам, процедуры идентификации личности при пересечении границ и др.

Наблюдающийся в последнее десятилетие прирост мощности вычислительных устройств, совершенствование систем регистрации и обработки цифровых изображений, параллельное накопление значительных объёмов данных и развитие систем компьютерного зрения, машинного и, в особенности, глубокого обучения позволили совершить значительный рывок технологий *биометрической идентификации*. Ключом доступа в данном случае выступает уникальная *биометрическая характеристика человека (БХЧ)* или *биометрическая модальность*. К популярным модальностям часто относят: папиллярный рисунок пальцев и ладони, изображение венозного русла кисти и ладони, особенности голоса, почерка, походки, изображения радужной оболочки и сетчатки глаза, изображения и форму лица.

Каждую из упомянутых БХЧ можно искусственно воспроизвести и предъявить биометрической системе с целью получения доступа к личной информации путем обмана. Различные модальности обладают различной сложностью подделывания, зависящей как от возможностей получения копии БХЧ, так и от сложности её воссоздания в условии ограниченных ресурсов. Процедура подделывания биометрических систем называется *спуфингом* (spoofing), а задача детектирования подлога — задачей *определения живости* или *анти-спуфингом*.

Рост точности и производительности биометрических систем приводит к расширению области применения технологий автоматического распознавания

человека. Современные мобильные устройства предоставляют пользователю широкий спектр возможностей по хранению значительных массивов данных, ведению личной и деловой переписки, осуществлению финансовых операций, доступу к защищённым цифровым ресурсам и др. В последнее десятилетие производители начали внедрять в смартфоны методы биометрической аутентификации как альтернативу паролям или цифровым кодам для ограничения доступа к персональной информации и повышения удобства использования.

Помимо рынка мобильных устройств отмечается рост спроса к цифровизации и персонификации бытовых услуг и сервисов, таких как «умные дома» (Smart Home), виртуальные помощники (Smart Assistant и др.), модель «интернета вещей» (Internet of Things). Подавляющее большинство этих приложений требуют присутствия системы автоматической идентификации/аутентификации личности.

Как следствие, расширение области применения технологий биометрической идентификации и аутентификации порождает множество актуальных задач, среди которых можно выделить проблему определения живости участника процедуры распознавания и обнаружения попыток взлома системы при помощи искусственно созданных БХЧ (т.н. подделок), поскольку именно этот компонент системы в первую очередь определяет уровень защиты, достигаемый при её использовании.

Особенно актуальной эта задача является мобильных биометрических приложений по ряду причин. Системы распознавания в мобильных устройствах и приложениях требуют удобства и быстродействия для пользователя, а также устойчивости к изменчивости окружения и самой БХЧ. В результате происходит ужесточение ограничений на средства регистрации изображений, применяемые алгоритмы распознавания и противодействия подложным попыткам входа. От мобильной биометрической системы требуется возможность работы в режиме реального времени при низком количества ошибок ложного недопуска *(False Rejection Rate — FRR)*, даже для входных данных низкого качества.

При этом сохраняется потребность в высоком уровне предоставляемой защиты, в том числе и от взлома при помощи поддельных БХЧ, что соответствует низкому количеству ошибок ложного допуска *(False Accept Rate — FAR)*. Наконец, реализация системы распознавания зачастую происходит на устройствах с сильно ограниченными вычислительными ресурсами.

Наиболее уязвимыми с точки зрения возможности спуфинга модальностями для мобильных систем являются изображения радужной оболочки глаза и видеообраза лица ввиду сравнительно небольшой сложности процедуры подделывания. Поэтому актуальными направлениями развития области определения живости в настоящее время являются: разработка высокопроизводительных методов анти-спуфинга для видеообраза лица в условиях некооперативного распознавания при помощи смартфона; разработка высокопроизводительных методов обнаружения подделок при помощи вспомогательных сенсоров, таких как мобильная стереокамера; разработка новых методов противодействия новым способам взлома мобильных систем распознавания по РОГ; разработка методов выделения границ радужки на изображениях как высокого, так и низкого качества.

Цели и задачи диссертационной работы:

В работе были поставлены следующие **цели**:

- Создать методы и алгоритмы для автоматического определения живости пользователя и обнаружения попыток взлома при помощи подделок в системах распознавания по видеообразу лица, оборудованных единственной камерой для съёмки в видимом спектре излучения, способные обрабатывать каждое изображение с частотой поступления кадров на мобильном устройстве, удовлетворяющие критериям ошибок: уровень ложных недопусков не более 3% при уровне ложного допуска не более 1%;

- Создать методы и алгоритмы выявления подделок лица при использовании пары камер с малым стереобазисом, способные обеспечивать защиту

от распространённых видов атак и имеющие достаточное для мобильных приложений быстродействие;

- Разработать методы и алгоритмы поиска границ радужной оболочки глаза для входных данных как высокого, так и низкого качества, характерного для мобильных биометрических систем;

- Создать методы и алгоритмы определения живости для мобильной системы распознавания по радужке, способные обеспечивать защиту, в том числе, от ранее не исследованных видов взлома при помощи подделок.

Для достижения поставленных целей были решены следующие **задачи**:

- Исследование и разработка методов определения живости человека по видеообразу лица, применимые в мобильном устройстве;

- Исследование и разработка методов обнаружения подделок лица человека с применением стереоинформации, извлекаемой при помощи камеры мобильного устройства с малым стереобазисом;

- Исследование и разработка методов поиска области радужки на изображении низкого качества с возможностью применения для мобильной биометрической системы;

- Исследование и разработка методов противодействия подделкам изображений радужки для мобильных систем распознавания;

- Сбор и разметка баз данных, в которых представлены изображения и последовательности изображений, реализующие приведенных выше задачи;

- Создание среды, программных средств и проведение вычислительных экспериментов по определению работоспособности перечисленных методов с опорой на собранные базы данных;

- Создание программных средств (библиотеки и тестовых приложений) для апробации реализованных методов на мобильном устройстве.

Научная новизна.

- Предложен новый метод защиты от подделывания в системах распознавания по видеообразу лица, имеющий многостадийную структуру и способный работать на мобильном устройстве с ограниченными вычислительными возможностями в режиме реального времени в сценариях изменяющихся условий окружения;

- Предложен новый метод защиты от подделывания изображения лица для мобильных систем, оборудованных стереокамерой с малым стереобазисом, обеспечивающий противодействие распространённым видам атак;

- Предложен новый высокопроизводительный метод аппроксимации границ радужки с применением методологии глубокого обучения, допускающий применение для изображений как высокого, так и низкого качества;

- Разработан новый метод определения живости радужки на изображении глаза, способный обнаруживать новые ранее не использовавшиеся виды взлома системы распознавания при помощи подделокю

Методология и методы исследования. В работе использованы методы цифровой обработки изображений, анализа данных и машинного обучения. Для предобработки и подготовки данных использовались модели детектирования лица и его ключевых точек и извлечения оптического потока. Для сбора данных и демонстрации результатов применялись методы разработки мобильных приложений для операционной системы Android.

Теоретическая и практическая значимость. Результаты, изложенные в диссертации, используются в мобильных устройствах, выпускаемых компанией Samsung Electronics Co. Ltd. Среди устройств — флагманские модели, выпускаемые компанией в период с 2018 по 2021 гг.: смартфоны Samsung

Galaxy S9/S9+, смартфон Samsung Galaxy Note9, планшет Samsung Galaxy Tab S4, смартфоны Samsung Galaxy S10e/S10/S10+, смартфоны Samsung Galaxy Note10/Note10 Ultra, смартфоны Samsung Galaxy S20/S20+/S20 Ultra, смартфоны Samsung Galaxy Note20/Note20 Ultra, смартфоны Samsung Galaxy Fold/Z Fold2/Z Fold3, смартфоны Samsung Galaxy S21/S21+/S21 Ultra.

Положения, выносимые на защиту:

- Выделены специфические качества методов определения живости видеообразов лица и радужки в системах биометрического распознавания, используемых в мобильных устройствах, описаны основные ограничения и требования, предъявляемые к алгоритмам определения живости и защиты от подделок;

- Разработан и внедрён многостадийный метод определения живости по видеообразу лица для пользователей смартфонов, оборудованных единственной фронтальной камерой; предложена методология сбора репрезентативной базы данных и с её помощью получена база изображений лиц в условиях, имитирующих применение системы распознавания человеком в повседневной жизни, осуществлена программная реализация метода;

- Описаны и исследованы виды подделок лица, которые могут быть обнаружены при использовании мобильных стереокамер с малым базисом, предложена методология сбора и с её помощью получена собрана база стереоизображений подлинных лиц и подделок, предложен метод защиты от взлома с высокой обобщающей способностью, произведено тестирование на открытой базе стереоизображений лиц;

- Выделена группа методов поиска границ радужки на изображении для мобильных биометрических приложений, разработан и программно реализован нейросетевой метод решения задачи, произведена его оценка и сравнение с описанными в литературе решениями;

- Описаны и исследованы новые способы изготовления подделок радужки, собрана база данных изображений подлинных и искусственных образцов, разработан метод распознавания живости глаза, устойчивый к новым видам подделок глаз, произведено его сравнение с аналогами из литературы по качеству решения задачи и производительности.

Степень достоверности и апробация результатов. Достоверность результатов обеспечивается обширным анализом работ в области исследования, описанием проведённых экспериментов, их воспроизводимостью, апробацией результатов на практике. Основные результаты диссертации докладывались на следующих конференциях: 64-я Всероссийская научная конференция МФТИ, Москва, 2021; 20-я Всероссийская конференция с международным участием «Математические методы распознавания образов» (ММРО-2021), Москва, 2021; International Conference on Pattern Recognition and Artificial Intelligence, Montreal, Canada, 2018; 19-я Всероссийская конференция с международным участием «Математические методы распознавания образов» (ММРО-2019), Москва, 2019; Intelligent Data Processing Conference, Gaeta, Italy 2018; Intelligent Data Processing Conference, Barcelona, Spain, 2016; XXI Международная научно-техническая конференция студентов, аспирантов и молодых учёных «Научная сессия ТУСУР», Томск, 2016.

Публикации. Материалы диссертации опубликованы в 17 печатных работах, из них 6 в журналах из списка ВАК и индексируемых в WoS, Scopus.

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причём вклад диссертанта был определяющим. Все представленные в диссертации результаты получены лично автором.

Структура и объём диссертации. Диссертация состоит из введения, 5 глав, заключения и библиографии. Общий объём диссертации 136 страниц,

из них 115 страниц текста, включая 27 рисунков. Библиография включает 156 наименований на 18 страницах.

Содержание работы

Во введении дан обзор литературы, обоснована актуальность диссертационной работы, сформулирована цели и методы исследований, поставлены основные задачи, обоснована их научная новизна, показана теоретическая и практическая значимость полученных результатов.

В первой главе приводится обзор подходов биометрической идентификации, даётся определение биометрической характеристики человека (БХЧ), приводится классификация БХЧ, описаны основные области применения и направления развития биометрических методов. Рассматриваются базовые операции, осуществляемые биометрической системой, в том числе проверка подлинности или живости для используемых данных БХЧ. Описаны группы подходов к построению подсистем детектирования подделок. Рассмотрены характерные особенности биометрического распознавания человека с мобильного устройства и специфика решения задачи определения живости для БХЧ, наиболее часто используемых в системах такого типа. Выделены основные требования, предъявляемые к методам обнаружения подделок в мобильных биометрических приложениях:

- некооперативность применяемых решений;
- переиспользование доступных аппаратных средств без внедрения дополнительных сенсоров;
- устойчивость к высокоизменчивым входным данным;
- низкая вычислительная сложность используемых алгоритмов.

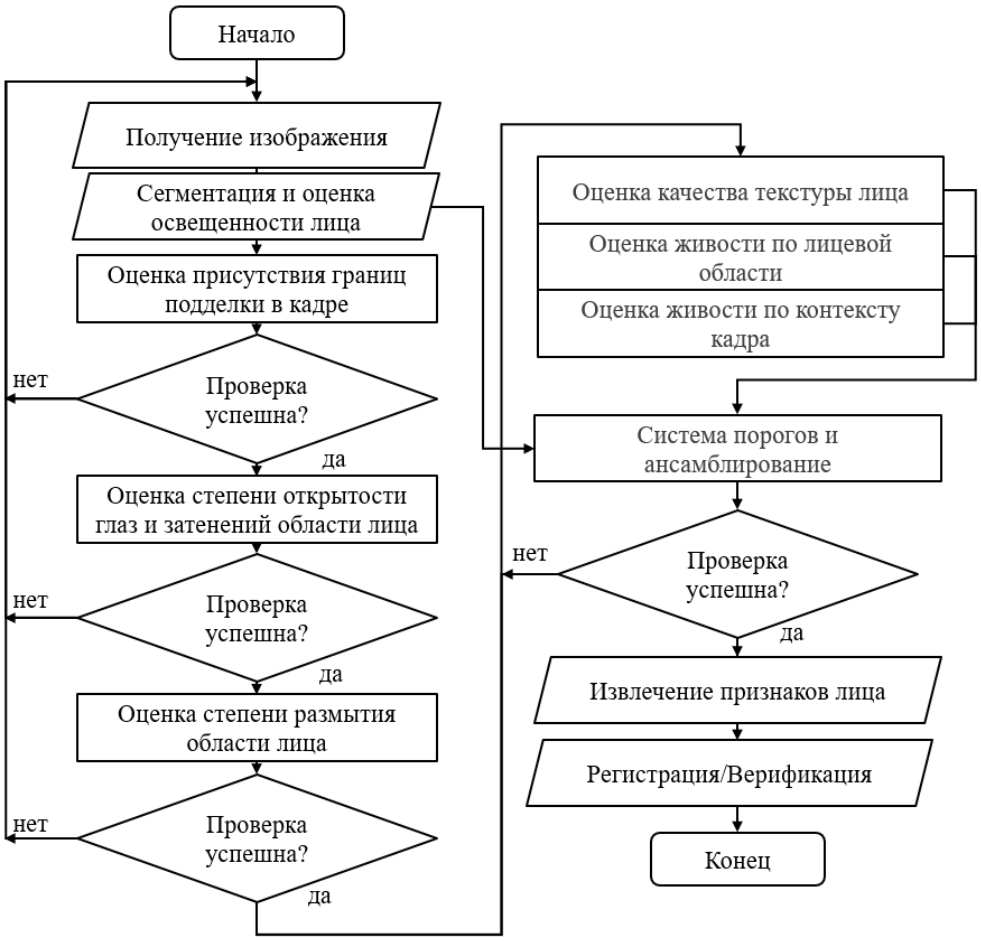


Рис. 1. Блок-схема алгоритма определения живости БХЧ.

Во второй главе предлагается метод определения подлинности лиц для мобильных биометрических систем, оборудованных фронтальной камерой. Описаны особенности и ограничения таких систем идентификации, а также возможность построения устойчивого алгоритма противодействия попыткам взлома. Произведена классификация способов подделывания по типам физических артефактов, уровню квалификации взломщика и доступности биометрической информации для создания искусственного шаблона. Дан обзор общих подходов к защите от подделывания для биометрических модальностей, использующих изображение или видеообраз лица. Вводятся основные показатели, применяемые для оценки производительности систем определения живости БХЧ.

Предложена многостадийная структура алгоритма для некооперативного детектирования попыток взлома, построенная с использованием промежуточных блоков оценки характеристик входного растра для раннего отказа от рас-

Меры качества,%		Основной алгоритм	+ Поиск границ	+ Лицевые атрибуты	+ Оценка размытия
Кадры	FAR	1.54	1.03	0.98	0.51
	FRR	4.33	4.91	5.10	5.32
Видео	FAR,	1.42	0.89	0.83	0.92
	FRR	2.04	2.55	2.64	2.84

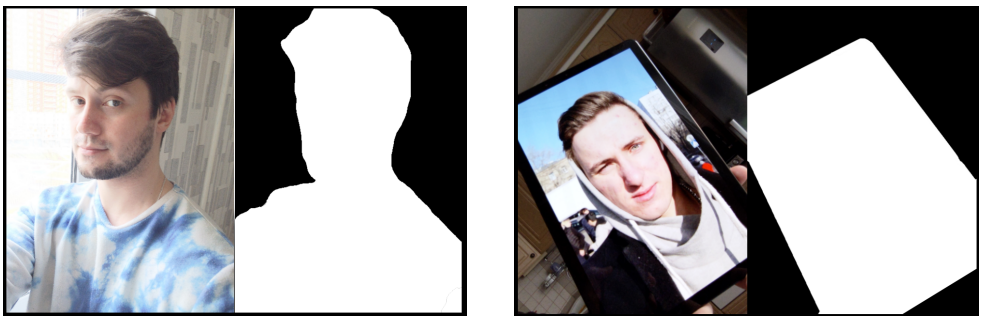
Таблица 1. Производительность многостадийного алгоритма детектирования подделок.

познавания. Составные компоненты метода (Рис. 1) можно отнести к одной из двух групп. Операции первой из них составлены из вычислительно простых проверок и оценок характеристик регионов входного растра и региона лица, реализованных в виде компактных нейросетей с низким уровнем ошибок ложного недопуска в систему. На этом этапе также извлекается дополнительная информация об окружении: оценка степени освещённости сцены с помощью встроенных датчиков освещения и информации о текущих параметрах экспозиции сенсора камеры. Методы второй группы обладают большей вычислительной сложностью и реализованы в виде свёрточных нейронных сетей для решения бинарной классификации на два класса «живое лицо» и «подделка», предсказания которых затем комбинируются с учётом результатов оценки состояния окружения и применения алгоритмов первой группы.

Описан сбор обучающей и тестовой выборок с учётом сценариев повседневного применения мобильного устройства. Приведены методы синтеза новых данных, эффективно увеличивающие размер и вариативность выборки для обучения, а также способы обучения нейросетевых моделей детектирования подделок в режиме самоконтролируемого обучения (self-supervised learning), не требующего затратной экспертной разметки данных.

Результаты представлены в Таб. 1 для двух режимов применения: покадрово и в виде видеопоследовательностей. Результаты по скорости обработки данных показали возможность использования метода на мобильном устройстве.

Третья глава посвящена особенностям построения систем обнаружения подделок для стереоизображения лица, получаемого при помощи мобильного



а б

Рис. 2. Карты принадлежности пикселей переднему плану: (а) настоящего лица; (б) подделки.

устройства и встроенной камеры с малым стереобазисом, с учётом сценариев применения биометрической системы пользователем, допускающих значительную изменчивость условий съёмки. Приведена классификация способов решения задачи определения живости лица, в том числе с использованием стереоизображений, обзор существующих методов, рассмотрены их достоинства и ограничения. Обоснована актуальность использования мобильных стереокамер для повышения уровня безопасности встроенных систем распознавания по лицу. С учётом допустимой изменчивости характеристик окружения при помощи мобильного устройства собрана и обработана база данных изображений (более 90000).

Разработан и протестирован новый алгоритм детектирования подделок для стереоизображений лиц, использующий методологию глубокого обучения. Предложена новая функция потерь для обучения классификатора на основе свёрточной нейронной сети, учитывающая информацию о глубине кадра при помощи бинарной карты принадлежности пикселей к переднему плану, Рис. 2. В процедуре обучения вводится дополнительное слагаемое помимо перекрестной кросс-энтропии для бинарных меток «живой» и «подделка», призванное обусловить внутренние представления нейронной сети на глубину сцены и тем самым повысить обобщаемость и регуляризовать нейросетевой классификатор. В архитектуру модели добавлен вспомогательная декодирующая подсеть, ис-

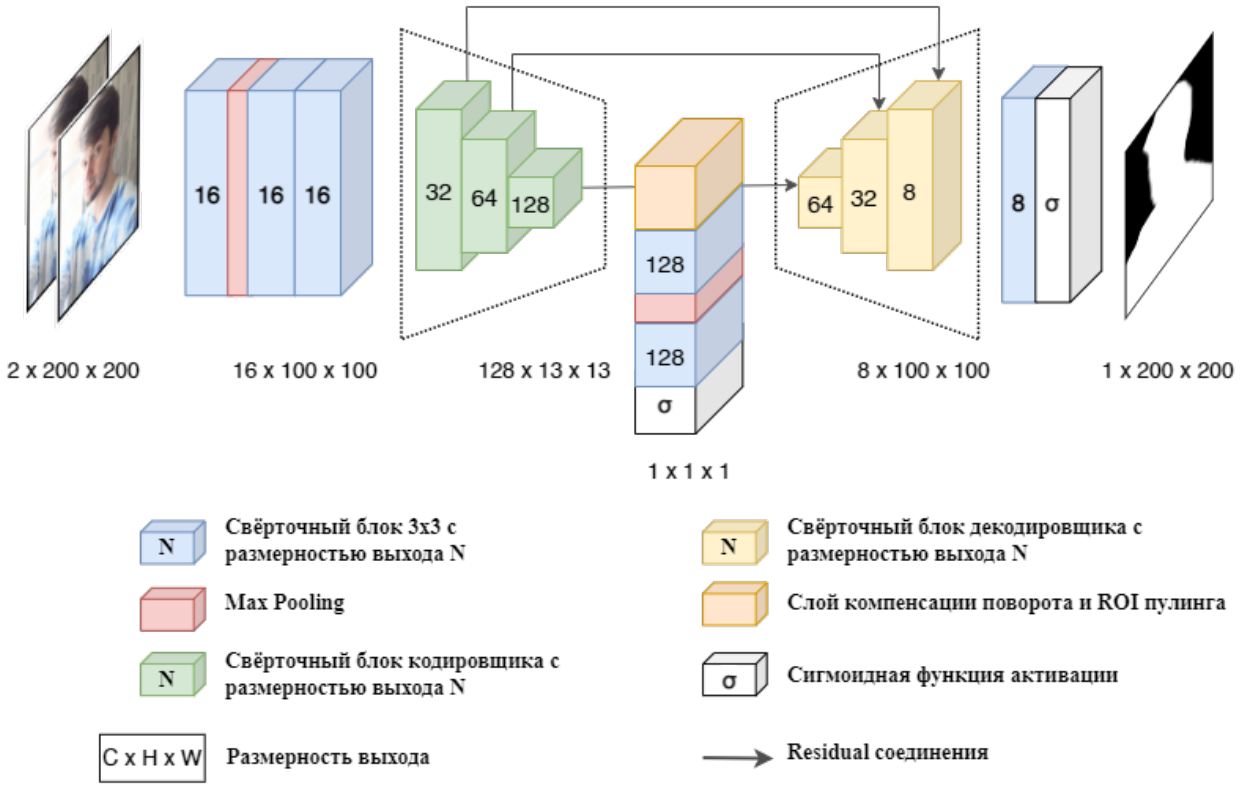


Рис. 3. Архитектура нейросетевого решения

пользующая внутренние представления основной сети и позволяющая предсказывать бинарную маску переднего плана сцены, соразмерную входному стереоизображению. Добавленный компонент используется только в процедуре обучения при помощи описанной вспомогательной функции потерь и не применяется на этапе валидации, что позволяет снизить общую вычислительную сложность прямого прохода входных данных в модели, Рис. 3. При тестировании выходными данными модели являются лишь вероятности принадлежности входной пары растров к классам «настоящее лицо» или «подделка».

При построении нейросетевого решения рассмотрены модификации модели, такие как: применение единственного изображений из пары (base); использование пары растров (stereo); использование вспомогательной подсети с предсказанием карты признаков (aux); регуляризация путём случайного добавления пар совпадающих изображений с целевой меткой класса «подделка» (zero); использование для предсказания метки класса только лицевой области путём пулинга региона интереса промежуточных представлений нейронной сети (roi).

Модель	Значения мер, %		
	APCER	BPCER	EER
base	**0.12**	41.31	12.54
base+roi	0.58	15.06	4.82
stereo	2.35	13.02	4.95
stereo+aux	0.89	**2.9**	1.89
stereo+aux+roi	0.57	3.01	1.45
stereo+aux+roi+zero	0.23	5.24	**1.24**

Таблица 2. Качество решения для модификаций модели на валидационной выборке.

Для оценки качества были выбраны следующие показатели:

- *APCER (attack presentation classification error rate)* — доля изображений подделок, ошибочно классифицированных как подлинные примеры;
- *BPCER (bona fide presentation classification error rate)* — доля изображений настоящих образцов, ошибочно классифицированных как поддельные;
- *EER (equal error rate)* — уровень равной ошибки.

В Таб. 2 приведено сравнение результатов тестирования модификаций предложенного метода, демонстрирующее необходимость применения их комбинации для повышения производительности. Для оценки обобщающей способности полученной наилучшей модели модификации *stereo+aux+roi+zero* была измерена точность определения живости для отложенной тестовой выборки стереоизображений подлинных лиц из открытой базы Holopix50k. Результат измерения составил 92.2%.

Пространственный размер входных стереоизображений был подобран с учётом ограничений вычислительной сложности модели и необходимого для решения задачи разрешения карты глубины, теоретически извлекаемой в случае

Слой	Размер входного тензора
Свертка 3×3	$1 \times 80 \times 80$
MCB(16, 2)	$16 \times 78 \times 78$
MCB(32, 1)	$16 \times 38 \times 38$
MCB(32, 2)	$32 \times 36 \times 36$
MCB(64, 1)	$32 \times 18 \times 18$
MCB(64, 2)	$64 \times 16 \times 16$
MCB(64, 1)	$64 \times 7 \times 7$
MCB(64, 1)	$64 \times 5 \times 5$
Global Average Pooling	$64 \times 3 \times 3$
Лин. классиф.для $x/y/d$	64
Softmax для $x/y/d$	80

Таблица 3. Строение нейронной сети для поиска границ радужки

малого стереобазиса и характеристик сенсоров используемой мобильной пары камер. Для предложенного метода на мобильном устройстве произведено измерение скорости обработки данных нейронной сетью. Полное медианное время для стереоизображения на одном ядре мобильного процессора Snapdragon 888 составило 23 мс.

Результаты третьей главы опубликованы в работе [1].

В четвёртой главе рассмотрена специфика поиска границ радужной оболочки глаза на изображениях при помощи нейронных сетей, с учётом применимости в мобильной биометрической системе с высокой степенью изменчивости условий окружения. Дан обзор и классификация известных алгоритмов выделения искомой, отмечены их основные достоинства и недостатки.

Описаны новые методы, построенные с использованием подходов глубокого обучения, обозначены их главные преимущества, учтены перспективы развития и практического применения [4]. Для решения задачи аппроксимации границ радужки двумя окружностями предложена, протестирована и внедрена

Слой	Размер ядра	Шаг
Depth-wise свертка	3×3	s
Batch normalization	-	-
Активация ReLu	-	-
Свертка	1×1	1
Batch normalization	-	-
Активация ReLu	-	-

Таблица 4. Строение блока $MobileConvBlock(M, s)$

архитектура, Таб. 3, свёрточной нейронной сети, основанная на применении базовых блоков семейства MobileNets, Таб. 4. Оценка параметров осуществляется последовательно при помощи двух моделей IrisNet и PupilNet: в первую очередь определяется внешняя граница радужки, затем внутренняя.

При обучении сетей предсказания параметров внешней и внутренней границ радужки задача регрессии целевых переменных сводится к задаче классификации с количеством классов, соответствующим требуемой точности решения и ограничениям разрешения входного изображения. Метод позволяет давать приблизительную оценку положений границ радужки и допускает последующее уточнение с меньшими временными затратами за счёт предсказанного первого приближения.

Результатом работы описанного метода являются параметры аппроксимирующих границы радужной оболочки окружностей:

- x_i, y_i, d_i — внешняя граница, «радужка-склера»;
- x_p, y_p, d_p — внутренняя граница, «радужка-зрачок».

Считается, что параметры окружностей были определены корректно, если абсолютная ошибка детектирования не превышает $\alpha = 5\%$ истинного диаметра

База данных	IrisNet+PupilNet		Уточнение	
	Q_p	Q_i	Q_p^r	Q_i^r
	%			
Raspberry DB	95.5	98.3	**97.9**	**98.9**
CASIA Mobile	97.9	98.5	**98.7**	**99.0**
UBIRIS v.1	85.8	95.3	**92.7**	**98.9**
ICE	97.6	95.8	**98.6**	95.8
MMU	88.3	98.5	**92.3**	**99.2**

Таблица 5. Результаты применения комбинации моделей

радужки на изображении:

$$\begin{aligned} &|x_i - X_i| < \alpha D_i, \qquad |x_p - X_p| < \alpha D_i, \\ &|y_i - Y_i| < \alpha D_i, \qquad |y_p - Y_p| < \alpha D_i, \\ &|d_i - D_i| < \alpha D_i, \qquad |d_p - D_p| < \alpha D_i. \end{aligned} \tag{1}$$

Для оценки качества применён анализ распределения относительных ошибок детектирования параметров окружности:

$$Q(\alpha) = \frac{1}{N} \left| \left\{ k : \frac{l^k}{D^k} < \alpha, k \in \overline{1, N} \right\} \right|, \tag{2}$$

где $l^k = |x^k - X^k| + |y^k - Y^k| + |d^k - D^k|$, N — размер тестовой выборки. Для простоты величина ошибки предсказания параметров внешней границы радужки обозначается как $Q_i = Q_i(0.05)$, внутренней — $Q_p = Q_p(0.05)$. Те же значения при предсказании моделью с последующим уточнением методом Даугмана приведены с дополнительным верхним индексом r (refined).

Для тестирования использованы данные открытых баз изображений радужки, полученных в ближнем инфракрасном (БИК) диапазоне излучения. С целью проверки обобщающей способности метода были выбраны растры, характерные как для полноразмерных, так и для мобильных биометрических систем. Первому сценарию соответствуют базы ICE, MMU, UBIRIS v.1, содержащие изображения глаз разных оттенков в высоком разрешении. Растры низкого

Мера качества	Метод детектирования					
	Дугман	Мазек	Ма	Ганькин	CNN	Уточнение
ε_c	2.61	4.98	3.92	0.97	1.4	1.3
ε_r	4.39	5.15	5.39	1.13	1.9	1.7
t_{c+r} (ms)	523.14	97.52	363.64	106.60	8	10

Таблица 6. Результаты сравнения с существующими методами

разрешения и качества, получаемые при помощи мобильных БИК камер, были выбраны из наборов данных CASIA Mobile и Raspberry DB. Последняя из упомянутых баз собрана вручную при помощи одноименного микрокомпьютера, оборудованного совместимой инфракрасной камерой с активной подсветкой. Результаты применения как самих нейросетевых методов к данным базам изображений, так и последующего уточнения методом Даугмана приведены в Табл. 5.

Предлагаемый подход к аппроксимации радужной оболочки также сравнён с иными методами на выборке базы изображений MMU при помощи следующих мер качества:

- относительная ошибка детектирования центров:

$$\epsilon_c = \frac{1}{N}\sum_{k=1}^{N}\sqrt{(y^k - Y^k)^2 + (x^k - X^k)^2};$$

- относительная ошибка детектирования радиусов:

$$\epsilon_r = \frac{1}{N}\sum_{k=1}^{N}|r^k - R^k|.$$

Помимо точности детектирования в сравнение было включено медианное время выполнения (t_{c+r}) на одном ядре процессора Qualcomm Snapdragon 845, Табл. 6.

Результаты четвёртой главы опубликованы в работе [2].

В пятой главе рассмотрены особенности построения систем определения живости для изображения радужной оболочки глаза при идентификации на мобильном устройстве. С учётом описанного в открытых источниках опыта групп взломщиков-экспертов воспроизведены способы подделывания для данной БХЧ. Дана классификация способов решения задачи защиты от взлома, обзор существующих методов, в контексте их достоинств и недостатков. Рассмотрены виды подделок, для которых ранее не производились исследования в области определения живости:

- распечатка изображения глаза на матовой белой бумаге с нанесённым в область радужной оболочки прозрачным клеем;
- распечатка изображения глаза на матовой белой бумаге с наложением прозрачных контактных линз на окружность радужной оболочки.

С учётом допустимой изменчивости условий окружения при помощи мобильного устройства собрана и обработана база данных изображений (более 40000), включающая новые способы подделывания. Разработан, протестирован и внедрён новый алгоритм противодействия спуфингу, использующий методологии глубокого обучения, в частности, построения свёрточных нейронных сетей. Схема исполнения дана на Рис. 4.

В качестве входных данных применяется пара растров региона глаза, полученных из общего исходного изображения: $\mathbf{I}_{\mathrm{ER}}$ — квадратная область, центрированная относительно внешней окружности радужки; $\mathbf{I}_{\mathrm{NI}}$ — нормализованное в прямоугольную область представление кольца внутренней текстуры радужной оболочки. Оба изображения обрабатываются свёрточными блоками $CNNB_{ER}$ и $CNNB_{NI}$ соответственно с последующим объединением признаковой информации путём конкатенации. Основными структурными элементами блоков являются базовые блоки архитектуры MobileNet, Табл. 4, обозначенные как MCB_I. Вероятности принадлежности входных растров к классам «живой» или «подделка» оцениваются при помощи softmax классификатора.

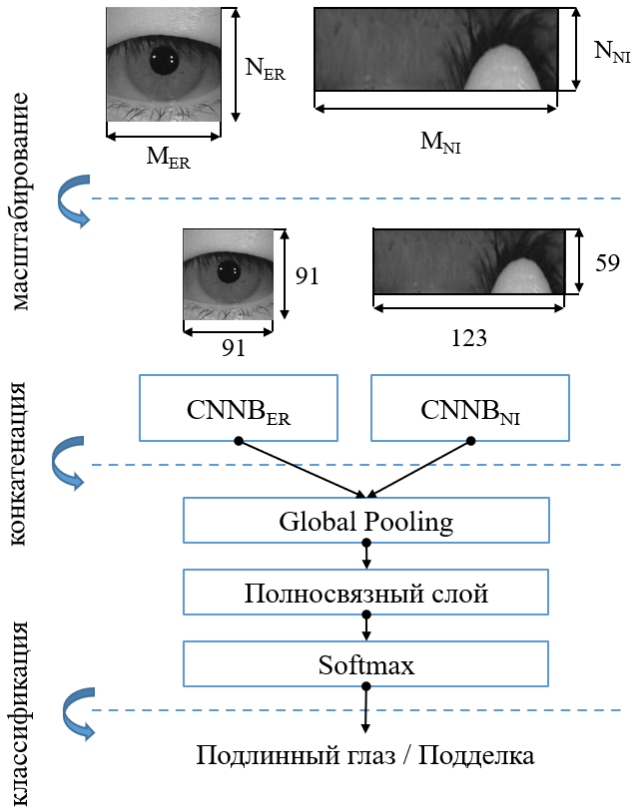


Рис. 4. Общая схема алгоритма защиты от подделывания радужки

С целью сравнения рассмотрены известные подходы к решению задачи детектирования подделок радужки, демонстрирующие наивысшую точность классификации для наборов данных изображений, полученных в ближнем инфракрасном диапазоне. Среди них: методы, основанные на применении частотного анализа (He-2008 и Czajka-2013); метод, построенные с использованием оценочных характеристик качества изображения (Sequeira-2014); методы, построенные не текстурных дескрипторах LBP (Gupta-2014) и BSIF (Raghavendra-2015).

Для оценки качества рассматриваемых решений были выбраны показатели, описанные ранее в третьей главе. В Таб. 7 приведено сравнение результатов тестирования предложенного методов и известных из литературы.

Для предложенного метода на мобильном устройстве при использовании одного ядра процессора Qualcomm Snapdragon 835 (2.45 GHz) произведено измерение производительности сети. Полное медианное время обработки пары изображений составило 5 миллисекунд.

Метод	Значения мер, %		
	BPCER	**APCER**	**Точность**
He-2008	37.0	73.9	44.2
Czajka-2013	50.5	20.7	66.1
Sequeira-2014	32.0	29.3	69.4
Gupta-2014	29.4	25.1	74.9
Raghavendra-2015	7.6	12.8	89.7
Предложенные метод	**3.8**	**3.4**	**96.9**

Таблица 7. Сравнительный анализ точности детектирования подделок радужки

Результаты пятой главы опубликованы в работе [3].

В Заключении представлены основные результаты работы:

1. Исследованы особенности построения алгоритмов противодействия взлому при помощи подделок для методов биометрического распознавания по видеообразу лица в приложениях мобильных устройств. Исследованы зависимости и причины изменения видимого образа лица с учётом специфики поведения пользователя устройства и характерных нестандартных и изменчивых условий окружения, присущих сценариям регистрации изображений объектов в мобильных приложениях. Разработан, предложен и внедрён метод детектирования подделок, допускающий применение в режиме реального времени в мобильных устройствах.

2. Исследованы методы и алгоритмы извлечения характеристик изображения лица применительно к решению задачи детектирования подделок. Разработан и внедрён метод раннего обнаружения спуфинг-атак для мобильных приложений, позволяющий до применения вычислительно сложных алгоритмов обнаруживать неестественные артефакты и атрибуты, присущие попыткам взлома, учитывать и использовать данные экспозиции камеры и вспомогательных сенсоров устройства с целью получения дополнительной информации об окружении.

3. Исследованы особенности обнаружения попыток подделывания лица при

распознавании с мобильного устройства, оборудованного стереокамерой с малым стереобазисом. Разработан и протестирован новый метод определения живости лица при помощи классификатора в виде свёрточной нейронной сети. Предложенное решение показало высокую точность и быстродействие детектирования подделок, в том числе тестировании на отложенной выборке данных открытой базы мобильных стереофотографий, содержащей изображения лиц, полученных в широком диапазоне условий окружения.

4. Разработаны, исследованы и внедрены алгоритмы аппроксимации окружностями границ радужной оболочки на изображении глаза основанные на применении методологии глубокого обучения. Предложенные подходы позволяют осуществлять оценку положений границ радужки в режиме реального времени для растров как высокого, так и низкого качества.

5. Изучена специфика построения систем обнаружения попыток взлома мобильных систем распознавания по радужке и новые способы подделывания этой БХЧ. Разработан, протестирован и внедрен новый метод определения живости в виде классификатора в виде свёрточной нейронной сети. Предложенное решение показало высокий уровень производительности и быстродействия при детектировании подделок, значительно превышающий таковой для описанных в литературе аналогичных методов.

6. Собраны, обработаны и размечены следующие базы данных: наборы изображений сниженного качества для подлинных лиц и распространенных типов подделок, содержащих более 1000 уникальных личностей и извлеченных при помощи мобильного устройства с имитацией реальных сценариев повседневного использования в изменчивых условиях окружения и применения, набор данных стереоизображений лица (более 90000), набор данных изображений подлинных и поддельных радужек, содержащий как

известные, так и новые виды атак (более 160000).

7. Созданы программные средства для проведения вычислительных экспериментов по оценке качества разработанных алгоритмов.

8. Созданы библиотека и тестовые приложения для апробации реализованных методов и алгоритмов на мобильном устройстве.

Основные публикации по теме диссертации

Публикации в журналах из списка ВАК:

1. *Ефимов Ю.С., Матвеев И.А.* Детектирование подделок в мобильных системах распознавания при помощи стереокамеры // Известия РАН. Теория и системы управления. 2022. № 2. С. 86–99.
2. *Ефимов Ю. С., Соломатин И. А., Леонов В.Ю., Одиноких Г.А.* Поиск границ радужной оболочки при помощи свёрточных нейронных сетей // Известия РАН. Теория и системы управления. 2020. № 6. С. 89–98.
3. *Efimov I., Odinokikh G., Solomatin I., Korobkin M. and Matveev I.* Iris Antispoofing Solution for Mobile Biometric Applications // Pattern Recognition and Image Analysis. 2018. № 28. P. 670–675.
4. *Odinokikh G., Korobkin M., Efimov I., Solomatin I., Matveev I.* Iris Segmentation in Challenging Conditions // Pattern Recognition and Image Analysis. 2018. № 28. P. 652–657.
5. *Ефимов Ю. С., Матвеев И. А.* Выделение точных границ радужки на изображении глаза // Информационные Технологии. 2017. Т. 23. № 4. С. 300–309.

Публикации, индексируемые в WoS, Scopus:

6. *Odinokikh G., Solomatin I, Korobkin M., Efimov I., Fartukov A.* Iris Feature Extraction and Matching Method for Mobile Biometric Applications // Proc. 2019 Intern. Conf. Biometrics (ICB), Sep. 2019. 2019. P. 1–6.

Прочие публикации:

7. *Ефимов Ю.С., Матвеев И.А.* Поиск внешней и внутренней границ радужной оболочки на изображении глаза методом парных градиентов // Машинное обучение и анализ данных. 2015. Т. 1. № 14. С. 1991–2002.
8. *Ефимов Ю.С., Матвеев И.А.* Поиск внешней и внутренней границ радужной оболочки на изображении глаза методом парных градиентов // Тезисы докладов 17-й Всероссийской конференции «Математические методы рас-

познавания образов». 2015. С. 174–175.

9. *Ефимов Ю.С., Матвеев И.А.* Сегментация радужной оболочки методом парных градиентов и уточнение границы зрачка на изображении глаза // Тезисы докладов 11-й Международной конференции «Интеллектуализация обработки информации». 2016. С. 112–113.
10. *Чигринский В.В., Ефимов Ю.С., Матвеев И.А.* Быстрый алгоритм поиска границ зрачка и радужной оболочки глаза // Машинное обучение и анализ данных. 2016. Т. 2. № 2. С. 159–172.
11. *Чигринский В.В., Ефимов Ю.С., Матвеев И.А.* Быстрый алгоритм поиска границ зрачка и радужной оболочки глаза // Тезисы докладов 11-й Международной конференции «Интеллектуализация обработки информации». 2016. С. 120–121.
12. *Efimov I., Odinokikh G., Solomatin I.* High-quality presentation attack detection in a mobile iris recognition system // Proc. Russian National Conference MMPR-18. 2018. P. 94–95.
13. *Odinokikh G., Efimov I., Solomatin I.* Iris Segmentation in Challenging Conditions // Proc. Russian National Conference MMPR-18. 2018. P. 138–139.
14. *Efimov I., Odinokikh G., Solomatin I.* Iris boundaries approximation by classifying convolutional neural network // Proc. Russian National Conference MMPR-18. 2018. P. 142–143.
15. *Efimov I., Odinokikh G., Solomatin I., Korobkin M. and Matveev I.* Iris Anti-spoofing Solution for Mobile Biometric Applications // Proc. Intern. Conf. Pattern Recognition and Artificial Intelligence. 2018. P. 666–671.
16. *Odinokikh G., Korobkin M., Efimov I., Solomatin I., Matveev I.* Iris Segmentation in Challenging Conditions // Proc. Intern. Conf. Pattern Recognition and Artificial Intelligence. 2018. P. 656–660.
17. *Efimov I., Matveev I.* Spoofing Detection in Mobile Face Recognition Using a Stereo Camera // Proc. Russian National Conference MMPR-20. 2021. P. 264.