Федеральный исследовательский центр «Информатика и Управление»
Российской академии наук
ФИЦ ИУ РАН

На правах рукописи

Одиноких Глеб Андреевич

Методы и алгоритмы биометрического распознавания человека по радужной оболочке глаза на мобильном устройстве

05.13.17 – Теоретические основы информатики

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель
д. т. н.
Матвеев Иван Алексеевич

Москва – 2019

Оглавление

Введение 4

Глава 1. Биометрия радужки 14

1.1. Обзор методов биометрического распознавания 14

1.2. Применение биометрических методов 17

1.3. Структура радужки и её свойства 18

1.4. Общая модель распознавания по радужке 20

1.5. Особенности мобильной биометрии радужки 21

1.6. Выводы к первой главе 24

Глава 2. Распознавание по радужке с мобильного устройства . 25

2.1. Основные трудности при распознавании человека по радужке . . 25

2.2. Метод аутентификации по радужке с мобильного устройства . . 28

2.2.1. Структура алгоритма распознавания 29

2.2.2. Оценка качества изображения радужки 34

2.2.3. Использование дополнительных сенсоров 36

2.3. Выводы ко второй главе 41

Глава 3. Выделение области радужки на изображении 42

3.1. Особенности выделения радужки в сложных условиях 42

3.2. Методы выделения радужки на изображении 44

3.2.1. Обзор существующих методов 44

3.2.2. Выделение области радужки методами глубокого обучения 47

3.3. Выводы ко второй главе 53

Глава 4. Методы извлечения и сравнения уникальных особенностей радужки 55

4.1. Вейвлеты Габора и адаптивное квантование фазы 56

4.1.1. Извлечение вектора признаков 58
4.1.2. Квантование 61
4.2. Метод с использованием глубокого обучения 64
4.2.1. Низкоуровневое представление признаков 66
4.2.2. Высокоуровневое представление признаков 69
4.2.3. Вычисление степени схожести 70
4.2.4. Метод обучения 73
4.3. Выводы к четвертой главе 76

Глава 5. Защита от подделывания радужки 78
5.1. Обзор методов защиты от подделывания радужки 79
5.2. Обнаружение подделок радужки методами глубокого обучения . 82
5.3. Выводы к пятой главе 88

Заключение 90

Список литературы 92

Введение

Биометрические технологии распознавания (идентификации, верификации) личности широко зарекомендовали себя при решении различных задач, связанных с обеспечением повышенного уровня безопасности доступа к информации и различным материальным объектам. В основе технологий лежит свойство уникальности биометрической характеристики человека (индивидуума), используемой в качестве идентификатора. Одной из таких характеристик является изображение радужной оболочки глаза.

Радужная оболочка глаза (РОГ) имеет уникальную, сложную и слабо изменяющуюся со временем структуру, что делает её высокоинформативным и устойчивым биометрическим признаком. Несмотря на то, что свойство уникальности РОГ известно с давних времён, первые новаторские работы (в т.ч. патенты), предлагающие использование радужки в качестве биометрического признака для распознавания, приходятся на период с 1985 по 1998 годы [21, 33, 34, 46, 140, 142]. В качестве входного сигнала было предложено использование изображения РОГ, зарегистрированного цифровой камерой в ближнем инфракрасном (БИК) диапазоне частот спектра электромагнитных волн.

С развитием технических средств регистрации изображения и обработки информации, позволяющая обеспечить наиболее высокую точность распознавания, по сравнению с другими биометрическими методами [48, 98, 99], технология аутентификации личности по радужной оболочке глаза стала привлекать внимание все большего количества исследовательских групп по всему миру, о чем свидетельствуют данные обзоров технологии, приходящиеся на этот период [22, 23, 81, 101]. В то же время, одно за другим, стали появляться и первые коммерческие решения в области систем контроля и управления доступом (СКУД), использующие изображение радужки в качестве уникального идентификатора. Среди наиболее известных IriScan, Iridian, Sarnoff, Sensar, LG, Panasonic, OKI, Morpho и другие.

Среди наиболее известных на сегодняшний день биометрических систем, использующих изображение РОГ в качестве уникального идентификатора, можно выделить следующие: системы биометрического паспортного контроля в более чем 10 терминалах аэропортов Великобритании и Амстердама, на границе США и Канады, в 32 наземных, воздушных и морских портах ОАЭ (Совет Сотрудничества Арабских Государств сообщает о 62 триллионах сравнений биометрических шаблонов РОГ за последние 10 лет) [62]; в 2016 году, в рамках программы UIDAI, осуществляемой индийским правительством, изображение радужки было зарегистрировано у более чем 1 млрд жителей страны; изображение РОГ является одной из трёх биометрических модальностей (также лицо и папиллярный узор пальца и ладони), стандартизованных ICAO для применения в электронных паспортах [66].

Одной из основных причин высокого интереса к биометрическим методам аутентификации сегодня является постоянное повышение требований к безопасности, в частности, при проведении финансовых операций, защиты и персонификации пользовательских данных. Большое внимание уделяется в том числе и удобству сервисов, позволяющих отказаться от использования всевозможных паролей, ПИН-кодов, смарт-карт и иных способов защиты. Мобильные устройства, стремительно приобретающие универсальность в аспекте проведения всевозможных транзакций, становятся платформой для развёртывания на них сервисов, использующих методы биометрической аутентификации. Значительная часть смартфонов, появившихся на рынке за последние несколько лет, оборудованы компактными сенсорами для аутентификации пользователя. С каждым годом доля устройств, использующих биометрию для распознавания, увеличивается, а повышение требований к безопасности заставляет производителей прибегать к использованию более сложных средств защиты. Позволяющая обеспечить наивысшую точность и удобство в использовании, технология аутентификации по РОГ привлекает все больше внимания производителей мобильных устройств.

Актуальность темы исследования В попытках изобрести надёжные и при этом удобные способы подтверждения подлинности той или иной информации, общество проделало огромный путь от парольных фраз, сложных печатей, механических замков и ключей до методов автоматической аутентификации. Подтверждение личности при пересечении границ регионов и государств, приобретении товаров и услуг, попытках доступа к различного рода данным и устройствам, проведении всевозможных финансовых транзакций, сопровождающиеся необходимостью предоставления подтверждающей информации, становится регулярной и неотъемлемой частью жизни каждого. Более 522 млрд. безналичных платёжных транзакций было произведено в 2017 году, 282 и 389 млрд. в 2010 и 2014 годах соответственно, согласно World Payments Report 2017 (WPR2017) [138], а прогнозируемое к 2020 году значение может достигнуть 726 млрд. Количество безналичных платёжных операций стремительно увеличивается, вместе с ним растёт и доля операций, совершенная при помощи мобильных устройств. По данным WPR2017 в период с 2015-2019 гг. ожидаемый рост доли транзакций, осуществляемых с их помощью, составит 21.8% и 32% в период 2017-2022 гг. Каждая транзакция, проводимая при помощи мобильного устройства, требует предоставления подтверждающей информации (ПИН-код и др.). Помимо транзакций, требующих непосредственного участия пользователя, существует устойчивый тренд к персонификации и интеллектуализации различных сервисов и услуг, среди которых т.н. «умный дом» (Smart Home), интернет вещей (Internet of Things), роботы-помощники (Smart Assistant и др.) и многое другое. Здесь речь может идти и о т.н. некооперативном распознавании. Практически каждое из вышеперечисленных приложений подразумевает наличие системы автоматической аутентификации/идентификации пользователя.

Развитие систем компьютерного зрения, машинного (в особенности глубокого) обучения, регистрации и обработки цифровых изображений, распознавания образов в совокупности увеличением мощности вычислительных устройств,

позволили совершить значительный рывок в области *биометрической идентификации* личности. В качестве идентификатора здесь выступает уникальная *биометрическая характеристика человека (БХЧ)* или *биометрическая модальность*. К числу наиболее часто используемых для распознавания БХЧ можно отнести следующие: изображение и форма лица, изображения радужной оболочки, сетчатки и периокулярной области глаза, папиллярный узор пальцев и ладони, изображение венозного русла кисти и ладони, особенности голоса, почерка, походки. Изображение радужки, обладающей сложной структурой, индивидуальной для каждого человека, является богатым источником информации. Биометрические системы, использующие изображение РОГ в качестве биометрической модальности, на сегодняшний день показывают наивысшую точность распознавания, и поэтому привлекают внимание множества исследователей по всему миру.

Среди наиболее известных исследовательских групп: Cambridge University, Великобритания (J. Daugman); Michigan State University, США (J. Anil, A. Ross); University of Notre Dame, США (P.J. Flynn, K.W. Bowyer), University of Beira Interior, Португалия (H. Proenca), Warsaw University of Technology, Польша (A. Czajka), Institute of Automation of the Chinese Academy of Sciences, КНР (T. Tan), в том числе и несколько российских: Федеральный Исследовательский центр «Информатика и управление» РАН (д.т.н. И.А. Матвеев), МГУ им. Ломоносова (д.ф-м.н. А.С. Крылов), Институт систем обработки изображений РАН и др. Тем не менее, наибольшее внимание технологиям биометрического распознавания сейчас уделяется со стороны коммерческих компаний, создающих целые институты и направления для их реализации и доведения до рынка.

Использование биометрических технологий в мобильных устройствах и в системах некооперативного распознавания подразумевает удобство их использования, быстродействие и устойчивость к изменчивости БХЧ и окружения. Это вынуждает ужесточать требования как к алгоритмам распознавания, так и к средствам регистрации изображения. В частности, система должна осу-

ществлять устойчивое извлечение биометрического признака(-ов) из изображения низкого качества, его обработку и последующее сравнение в режиме реального времени, обеспечивая при этом низкие значения ошибки ложного недопуска *(False Rejection Rate - FRR)*. Биометрический шаблон должен быть защищен. Защита может осуществляться на системном уровне и добавлением спецальных алгоритмов хеширования биометрических данных. Кроме этого, к основным требованиям часто относят необходимость взаимодействия с пользователем и наличие системы защиты от подделки. Весь процесс обработки должен осуществляться на устройстве с сильно ограниченными вычислительными ресурсами.

Таким образом, новые сценарии использования технологий биометрического распознавания создают новые задачи, решение которых позволит существенно повысить уровень безопасности и удобства транзакций, ежедневно осущещствляемых миллионами людей по всему миру, при использовании различных сервисов и услуг.

Наиболее актуальными направлениями развития области распознавания по РОГ на сегодняшний день являются: оценка качества изображения радужки в условиях изменчивости окружения и при некооперативном распознавании; разработка методов сегментации области радужки на изображении низкого качества; разработка высокопроизводительных методов извлечения и представления особенностей радужки из изображения низкого качества; анализ информативных признаков радужки и периокулярной области глаза с целью обеспечения обратной связи с пользователем; создание устойчивых методов сравнения биометрических шаблонов радужки, получаемых в условиях значительной изменчивости окружения; разработка новых методов защиты от подделки.

Цели и задачи диссертационной работы:

В работе были поставлены следующие **цели**:

- Создать методы и алгоритмы для автоматического распознавания чело-

века по радужной оболочке глаза, способные обрабатывать изображение радужки с частотой поступления кадров на мобильном устройстве, удовлетворяющие критериям ошибок распознавания: $FRR \leq 1\%$ при $FAR < 10^{-7}$

- Разработать методы и алгоритмы оценки качества изображения радужки, определяющие её пригодность для выделения признаков и обеспечивающие обратную связь с пользователем устройства
- Разработать методы и алгоритмы выделения области радужки на изображении низкого качества
- Создать методы и алгоритмы выявления подделок радужки по изображению низкого качества, способный обеспечивать защиту от ранее не рсматриваемых видов атак

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

- Исследование и разработка методов распознавания человека по радужке, удовлетворяющих критериям, необходимым для обеспечения возможности их применения в мобильном устройстве
- Разработка метода оценки качества изображения радужки, учитывающего ограничения, особенности использования мобильного устройства и взаимодействия с пользователем
- Исследование и разработка методов выделения радужки на изображении низкого качества, получаемого в условиях постоянно изменяющегося окружения
- Исследование и разработка методов извлечения и сравнения уникальных особенностей радужки из изображения низкого качества в условиях постоянно изменяющегося окружения

- Исследование и разработка методов обнаружения попыток представления подделок радужной оболочки глаза
- Сбор и разметка баз данных изображений для проведения экспериментов в рамках решения вышеперечисленных задач
- Создание среды и программных средств для оценки производительности методов, реализованных в рамках решения вышеперечисленных задач
- Создание программных средств (библиотеки и демо-приложений) для апробации реализованных методов на мобильном устройстве

Научная новизна.

- Предложен новый высокопроизводительный метод распознавания человека по радужной оболочке глаза, способный работать на устройстве с низкой вычислительной мощностью в условиях постоянно изменяющегося окружения в режиме реального времени;
- Предложен новый высокопроизводительный метод выделения области радужки на изображении низкого качества;
- Разработан новый метод оценки качества изображения радужки, позволяющий оценить её пригодностьдля извлечения уникальных особенностей и их последующего сравнения, обеспечивающий обратную связь с пользователем в виде отображения подсказок на экране устройства;
- Разработан новый метод адаптивного квантования изображения радужки, устойчивый к искажениям текстуры радужки;
- Предложен новый метод извлечения и сравнения уникальных особенностей радужки, обеспечивающий высокую точность распознавания, устойчивый к изменению размера зрачка, условий окружения и уровню качества изображения;

- Разработан новый надежный метод защиты от подделывания радужки, обеспечивающий защиту от, в том числе, ранее не рассматриваемых видов атак;

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 2016 по 2018 гг.: смартфон Samsung Galaxy Note7, смартфоны Samsung Galaxy S8/S8+, смартфон Samsung Galaxy Note8, смартфоны Samsung Galaxy S9/S9+, смартфон Samsung Galaxy Note9, планшет Samsung Galaxy Tab S4.

Положения, выносимые на защиту:

- Исследованы особенности использования методов биометрического распознавания человека по радужной оболочке глаза в применении к мобильным устройствам, сформулированы основные требования, предъявляемые к таким методам;

- Разработан метод распознавания пользователя смартфона по изображению радужной оболочки глаза, собрана база данных изображений радужки, полученных в условиях, симулирующих реальное взаимодействие пользователя с устройством при распознавании, осуществлена программная реализация метода, произведено сравнение с аналогами, известными из литературы, по точности и скорости распознавания;

- Предложен многостадийный метод оценки качества изображения радужки, получаемого при помощи мобильного устройства, позволяющий обеспечивать обратную связь с пользователем в виде отображения подсказок на экране устройства;

- Исследованы методы выделения области радужки на изображении, получаемом в экстремальных условиях окружения, разработан и программ-

но реализован метод, основанный на глубоком обучении, произведена его оценка и сравнение с известными из литературы аналогами;

- Исследованы, разработаны и программно реализованы методы извлечения уникальных особенностей радужки по изображению, получаемому в экстремальных условиях окружения, произведено сравнение методов с существующими аналогами по скорости обработки и точности распознавания;

- 6. Исследованы новые виды подделок радужки, собрана база данных подделок, предложен метод защиты от подделок, устойчивый к новым видам подделок, произведено его сравнение с известными из литературы методами по точности детектирования и скорости обработки.

Степень достоверности и апробация результатов. Достоверность результатов обеспечивается обширным анализом работ в области исследования, описанием проведенных экспериментов, их воспроизводимостью, а так же апробацией результатов на практике. Основные результаты диссертации докладывались на следующих конференциях: The 12th IAPR International Conference On Biometrics, Crete, Greece, 2019; International Conference on Pattern Recognition and Artificial Intelligence, Montreal, Canada, 2018; International Workshop on "Photogra and computer vision techniques for video surveillance, biometrics and biomedicine Moscow Russia, 2017; Intelligent Data Processing Conference, Barcelona, Spain, 2016; Intelligent Data Processing Conference, Gaeta, Italy 2018; Samsung Mobile Developers Conference, Suwon, 2016, South Korea; Всероссийская научная конференции ЭКОМОД-2016, Киров, Россия, 2016.

Публикации. Материалы диссертации опубликованы в 10 печатных работах, из них 3 в журналах из списка ВАК.

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубли-

кованные работы. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был определяющим. Все представленные в диссертации результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения, обзора литературы, 5 глав, заключения и библиографии. Общий объем диссертации 106 страниц, из них 88 страниц текста, включая 34 рисунков. Библиография включает 154 наименований на 17 страницах.

Глава 1

Биометрия радужки

1.1. Обзор методов биометрического распознавания

Биометрия (или биометрика) - область знаний, изучающая методы и средства измерения и формализации персональных физических характеристик, поведенческих черт человека и их использование для идентификации или верификации человека. *Биометрической характеристикой человека (БХЧ)*) называются результаты измерения элемента фенотипа человека или поведенческой черты, в процессе сравнения которых с аналогичными, ранее зарегистрированными БХЧ (эталон, шаблон) реализуется процедура идентификации или верификации личности.

Биометрическая система представляет собой автоматизированную систему, решающую задачи идентификации или верификации личности и реализующую следующие операции [6]:

- регистрации выборки БХЧ от конкретного пользователя;
- формирование вектора биометрических данных из выборки БХЧ;
- формирование биометрического вектора признаков;
- сравнение биометрических векторов признаков с эталонами (шаблонами);
- принятие решения о соответствии сравниваемых БХЧ;
- формирование результата о достижении идентификации (верификации);
- принятие решения о повторении, окончании или видоизменении процесса идентификации (верификации).

Все БХЧ могут быть поделены на две группы: физиологические (статические) и поведенческие (динамические) [6]. Для каждой из груп насчитывается

множество конкретных методов, наиболее распространенные из которых перечислены ниже:

1. Физиологические биометрические характеристики человека:
    а. Видеообраз лица: овал, форма, размер отдельных деталей, геометрические параметры (расстояние между его определенными точками), узор подкожных кровеносных сосудов и др.;
    б. Структура радужной оболочки глаза;
    в. Структура кровеносных сосудов на сетчатке глаза;
    г. Особенности папиллярного узора одного или нескольких пальцев, ладони: параметры минуций (координаты, ориентация), параметры пространственно-частотного спектра и др.;
    д. Особенности папиллярного узора ладони;
    е. Особенности строения ладони: геометрия (ширина, длина, высота пальцев, расстояние между определенными точками), неровности складок кожи, рисунок вен, папиллярный рисунок ладони и др.;
    ж. Особенности уха: форма (контур, наклон, козелок, противокозелок, форма и прикрепление мочки), геометрические параметры уха (расстояние между определенными точками) и др.;
    з. Особенности губ: форма и др.;
2. Поведенческие биометрические характеристики человека:
    а. Особенности голоса: тембр, частотный спектр и др.;
    б. Особенности походки;
    в. Характер подписи: сила нажима, координата времени;
    г. Характер набора текста на клавиатуре и др.;

Источник БХЧ	Универсальность	Уникальность	Стабильность	Собираемость
Видеообраз лица	+++	+	++	+++
Термограмма лица	+++	+++	+	++
Отпечаток пальца	+++	+++	+++	++
Рука	++	++	++	+++
Радужка	++	+++	+++	++
Сетчатка	+++	+++	++	+
Подпись	+	+	+	+++
Голос	++	+	+	++
Губы	+++	+++	++	+
Ухо	++	++	++	++
Динамика письма	++	+++	+	+++
Походка	+++	++	+	+

Таблица 1.1. Экспертная оценка биометрических характеристик человека

Выбор источника БХЧ является основной задачей при создании конкретных биометрических технологий. Идеальная БХЧ должны быть универсальной, уникальной, стабильной, собираемой. Универсальность означает наличие биометрической характеристики у каждого человека. Уникальность означает, что не может быть двух человек, имеющих идентичные значения БХЧ. Стабильность – независимость БХЧ от времени. Собираемость – возможность получения биометрической характеристики от каждого индивидума.

Реальные БХЧ не идеальны и это ограничивает их применение. В результате экспертной оценки указанных свойств таких источников БХЧ установлено, что ни одна из характеристик не удовлетворяет требованиям по перечисленным свойствам (см. Таб. 1.1). Необходимым условием использования тех или иных БХЧ является их универсальность и уникальность, что косвенно может быть обосновано их взаимосвязью с генотипом человека.

1.2. Применение биометрических методов

Обращение к биометрическим технологиям идентификации личности происходит, когда речь идет о повышении требований к безопасности совместно с удобством их использования. Биометрические технологии могут быть использованы как альтернатива существующим методам аутентификации, требующих запоминания бесчисленного числа паролей, кодовых фраз, ПИН-кодов пластиковых карт, банковских счетов, ячеек и др.

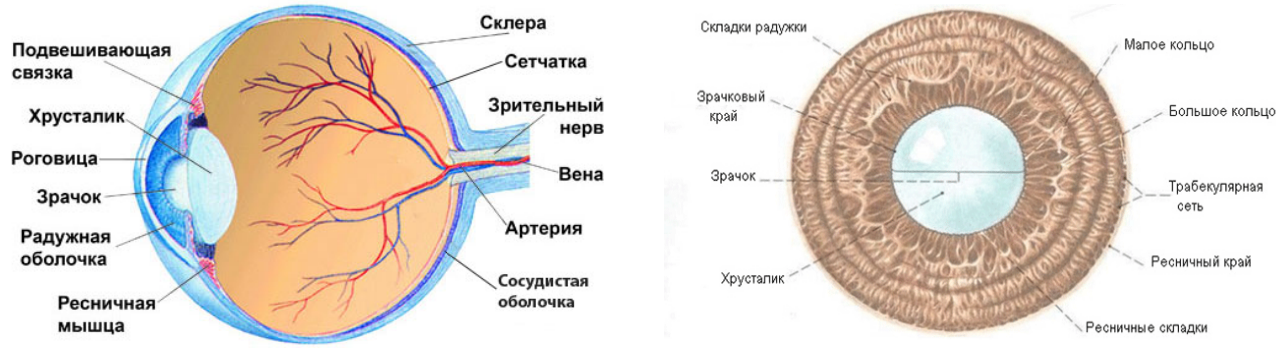
На сегодняшний день, применение таких технологий наиболее часто производится в системах безопасности для:

- Контроля и управления доступом на охраняемый объект, при пересечении государственных границ, а так же с целью ограничения доступа к электронным ресурсам, различным персональным устройствам, банковским ячейкам, депозитам и др.
- Обеспечения безопасности финансовых операций: платежные операции, снятие наличных в банкомате и др.

Рост интереса к биометрическим технологиям обусловлен повышением требований к безопасности при проведении аутентификации пользователя. На сегодняшний день биометрические технологии наиболее активно внедряются в сферах государственного контроля границ и при проведении финансовых операций. Примерами этого могут служить необходимость обязательной сдачи биометрических данных (отпечатков пальцев, изображения лица) при получении заграничного паспорта, внедрение универсальных электронных карт (ID за рубежом и УЭК на территории РФ), планы по внедрению биометрических технологий с целью аутентификации пользователя многими крупными банками, внедрение такими крупными компаниями как Samsung, Apple, Google своих платежных систем Samsung Pay, Apply Pay и Android Pay соответственно и многое другое.

1.3. Структура радужки и её свойства

Радужная оболочка глаза (радужка, лат. *iris*, из др.-греч. ἶρις «радуга») - круглая подвижная диафрагма диаметром около 12 мм, отделяющую переднюю камеру глазного яблока от задней. Расположена за роговицей между передней и задней камерами глаза, перед хрусталиком (Рис. 1.1, *а*), обеспечивает регуляцию количества света, попадающего на сетчатку. Содержит пигментные клетки (у млекопитающих — меланоциты), круговые мышцы, сужающие зрачок, и радиальные, расширяющие его.



(*а*) (*б*)

Рис. 1.1. Строение глаза (а) и радужки (б)

На передней поверхности радужки выделяют зрачковый край (margo pupillaris) шириной 1 мм и ресничный край (margo ciliaris) шириной 3—4 мм. В области зрачкового края расположен сфинктер зрачка (sphincter pupillae) — мышца, суживающая зрачок; в области ресничного края находится дилататор зрачка (dilatator pupillae) — мышца, расширяющая зрачок (Рис. 1.1, *б*). Место соединения радужки с ресничным (цилиарным) телом называется корнем радужки, остальная её часть находится в свободном взвешенном состоянии в жидкости передней и задней камер глазного яблока [3].

Структура радужки имеет вид губчатой ткани 1.2, состоящей из множества радиальных тонких перемычек (трабекул), образованных толстой адвентицией сосудов и окружающей их соединительной тканью. Между трабекулами располагаются углубления (лакуны и крипты). На границе зрачкового и реснич-

ного края определяется зубчатая линия, или круг Краузе (малое кольцо радужки) — область прикрепления эмбриональной зрачковой сосудистой мембраны. Зрачок обрамлен темно-коричневой зрачковой каймой. На передней поверхности радужки видны складки, при узком зрачке более рельефно выделяются радиальные складки, при широком зрачке — концентрические [3].

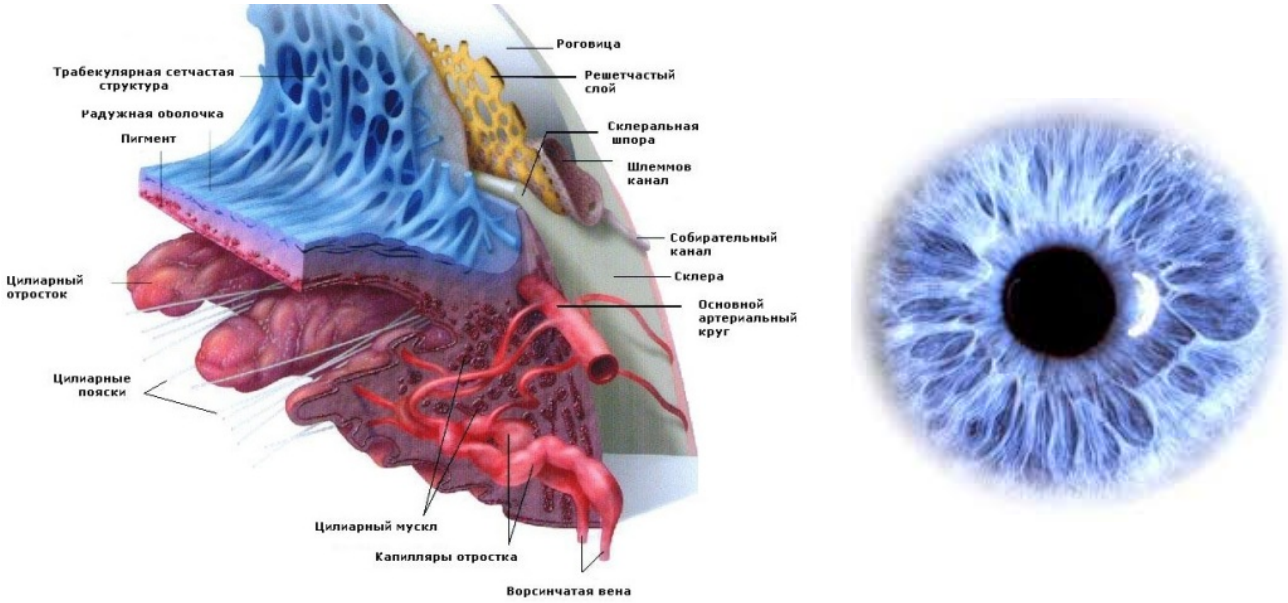


Рис. 1.2. Структура радужки

Радужка имеет генетически обусловленные рисунок и цвет. Коричневый (темный) цвет наследуется по доминантному типу, голубой (светлый) — по рецессивному. Рисунок и цвет радужки слабо изменяются в течение жизни [1]. Цвет радужки стабилизируется к 10—12 годам. В пожилом возрасте радужка становится несколько светлее вследствие дистрофических изменений. Также возможно появление пятен на поверхности радужки в связи с заболеваниями различных органов [1, 3].

Сложность и особенности текстуры радужки делают её уникальным, высоко-информативным биометрическим признаком, который может быть использован в качестве идентификатора.

1.4. Общая модель распознавания по радужке

Подавляющее большинство предложенных методов распознавания по радужной оболочке глаза используют следующую общую схему (Рис. 1.3):

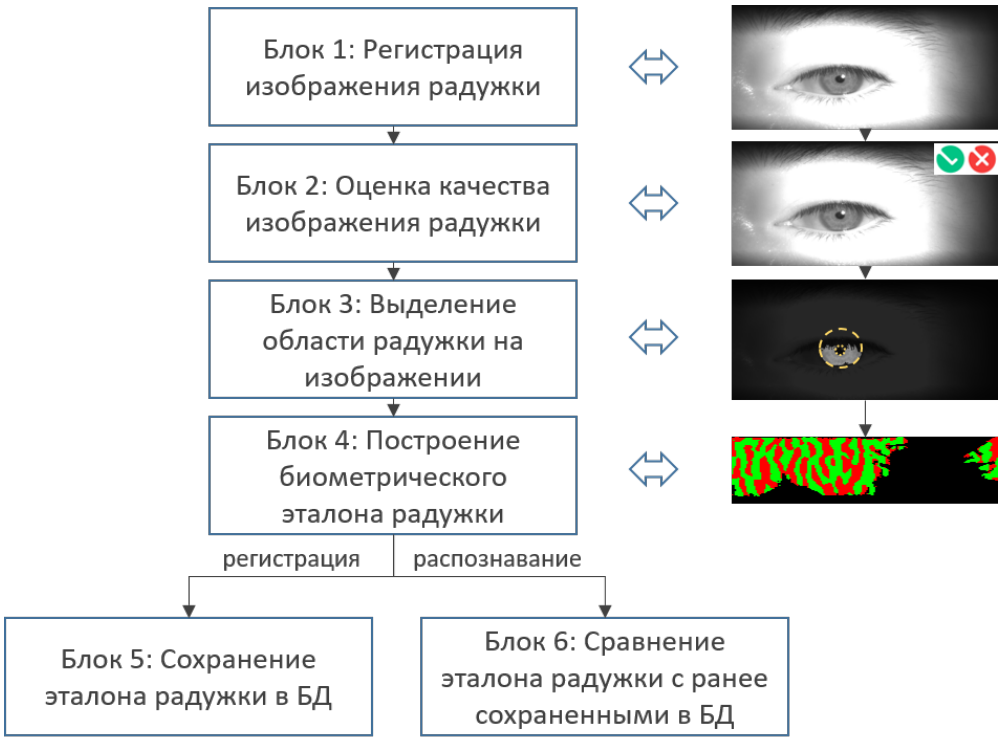


Рис. 1.3. Общая схема распознавания по радужке

Регистрация изображения радужки (блок 1) осуществляется при помощи цифровой камеры в ближнем инфракрасном (БИК, 810-950 нм), либо в видимом (380-780 нм) диапазонах длин волн. При регистрации, как правило, так же используется активная диодная подсветка. Далее (блок 2) осуществляется оценка качества полученного изображения с точки зрения его пригодности для выделения радужки и формирования биометрического эталона. К блоку оценки качества часто относят подсистему защиты от подделки. Он может быть многостадийным и распределен между остальными блоками. Следующий за ним блок 3 осуществляет выделение радужки на изображении, т.е. отделение области изображения, относящейся к радужке, от фона и шума. В качестве шума здесь выступает множество элементов: веки, ресницы, блики и т.д. После того, как область радужки выделена, осуществляется построение биометрического

эталона (блок 4).

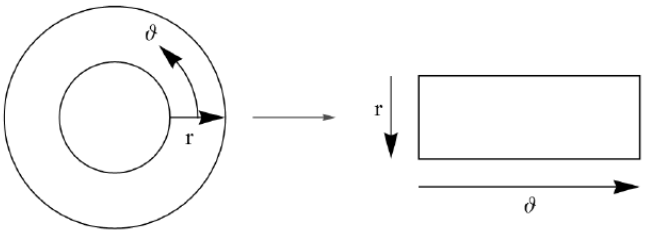


Рис. 1.4. Преобразование изображения радужки

Данный этап часто включает преобразование изображения (Рис. 1.4), путем перехода из исходной Декартовой системы координат (x, y) в полярную (r, θ) (1.1), впервые предложенную в работе [33]:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \tag{1.1}$$

где $I(x, y)$ - исходное изображение радужки, (x, y) координаты в Декартовой системе, а (r, q) - соответствующие нормализованные координаты в полярной. $x(r, \theta)$ и $y(r, \theta)$ заданы в виде линейных комбинаций наборов точек границ зрачка $(x_p(\theta), y_p(\theta))$ и радужки $(x_i(\theta), y_i(\theta))$:

$$\begin{aligned} x(r,\theta) &= (1-r)\cdot x_p(\theta) + r\cdot x_i(\theta) \\ y(r,\theta) &= (1-r)\cdot y_p(\theta) + r\cdot y_i(\theta) \end{aligned} \tag{1.2}$$

После того как биометрический шаблон радужки построен, в зависимости от текущего сценария (регистрация/распознавание) он либо сохраняется в БД (блок 5), либо сравнивается с эталонами, сохраненными в БД ранее (блок 6). При построении шаблона также часто используется процедура выбора наилучшего (-их) по заранее заданным критериям, что позволяет снизить ошибки распознавания.

1.5. Особенности мобильной биометрии радужки

Значительная доля платежных транзакций осуществляется посредством мобильных платежных систем, и эта доля стремительно растет [138]. При ра-

боте с Samsung Pay, Apply Pay и Android Pay пользователю предлагается использовать один из возможных способов аутентификации, среди которых уже сейчас присутствует биометрический шаблон отпечатков пальцев (Рис. 1.5).

Рис. 1.5. Использование отпечатков пальцев при совершении платежной транзакции с мобильного устройства

Как было упомянуто ранее, технология распознавания по радужке обладает рядом преимуществ по сравнению с распознаванием по иным биометрическим признакам, в том числе отпечаткам пальцев. Структура радужки является устойчивым, хорошо выраженным и высоко-информативным биометрическим признаком, практически не подвергающимся изменениям в течение жизни. Кроме этого, процедура распознавания по радужке является бесконтактной. Перечисленные свойства позволяют обеспечить удобство использования, более высокую точность распознавания и надежность биометрических систем идентификации, построенных на основе данного биометрического признака и, как следствие, расширение рынка мобильных устройств.

В качестве информации, используемой для построения биометрического шаблона в системах биометрической идентификации личности по радужной оболочке глаза, выступает изображение радужки.

Работа с мобильным устройством накладывает дополнительные ограничения на применения биометрической системы распознавания по радужке и, как следствие, к ней выдвигаются дополнительные требования. Система должна обеспечивать работу в условиях постоянно изменяющихся внешних условий среды. Распознавание должно производиться в помещении, на улице, в солнечную

и пасмурную погоду, учитывать возможность ношения очков, контактных линз и др. Система должна обеспечивать удобство использования, т.е. учитывать поведение пользователя, возможные моргания, тряску рук, направление взгляда и так далее. Система должна обеспечивать возможность работы в реальном времени на мобильном устройстве с ограниченным количеством потребляемой памяти и вычислительных ресурсов, обеспечивая при этом высокую точность распознавания.

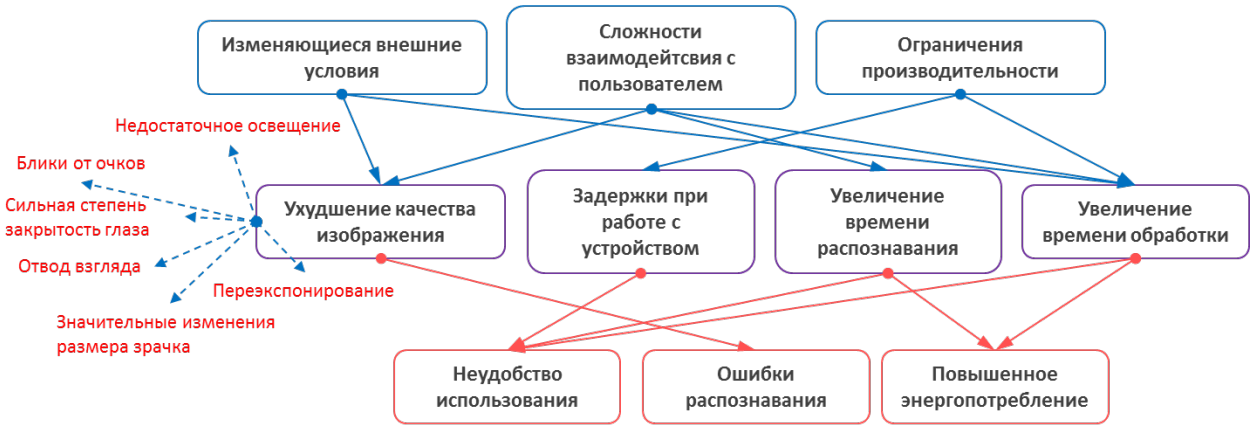
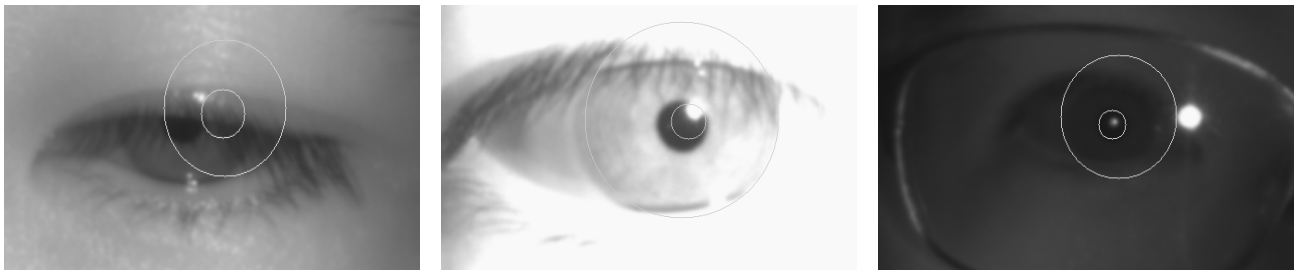


Рис. 1.6. Основные проблемы при распознавании по радужке с мобильного устройства

Неучёт вышеперечисленных требований приводит к ухудшению качества изображения (Рис. 1.6, 1.7) [40], а в некоторых случаях даже к невозможности его получения.



(*а*) (*б*) (*в*)

Рис. 1.7. Ухудшение качества изображения при распознавании по радужке с мобильного устройства, влекущее за собой ошибки сегментации радужки: а) отвод взгляда, перекрытие веками, б) пере-экспонирование, в) низкий контраст, блик от очков

Ухудшение качества изображения приводит к снижению точности распознавания, что ставит под сомнение возможность применения таких биометри-

ческих систем при осуществлении различного рода транзакций (Рис. 1.6).

1.6. Выводы к первой главе

Произведен обзор биометрических методов распознавания человека. Приведено сравнение различных биометрических характеристик человека с точки зрения их универсальности, уникальности, стабильности и собираемости. Рассмотрены основные области применения и направления развития биометрических методов. Описаны структура и свойства радужной оболочки глаза. Показаны её преимущества и недостатки как уникальной БХЧ. Приведена общая схема распознавания по радужке от процедуры регистрации изображения до вычисления степени схожести и принятия решения об идентичности/неидентичности двух радужек. Рассмотрены особенности использования радужки в качестве БХЧ при распознавании человека с мобильного устройства.

Глава 2

Распознавание по радужке с мобильного устройства

2.1. Основные трудности при распознавании человека по радужке

Биометрические технологии распознавания хорошо зарекомендовали себя и заняли нишу в решении задач, связанных с обеспечением безопасности. Говоря о мобильных устройствах, существенное количество современных персональных устройств (смартфонов, планшетов и т.д.) оснащены компактными сканерами отпечатков пальцев, предназначенных для аутентификации пользователя. Не смотря на то, что методы аутентификации по отпечаткам пальцев демонстрируют достаточно высокую точность распознавания, они все еще имеют существенные недостатки [37]. Среди всех биометрических модальностей, рассматриваемых в качестве кандидатов для замены либо объединения с отпечатками, радужная оболочка глаза остается одной из самых привлекательных [22, 30, 38, 121].

Регистрация изображения радужки обычно производится с использованием камеры высокого разрешения в ближнем инфракрасном (БИК), либо в видимом диапазоне длин волн [112] в фиксированных, практически «лабораторных» условиях окружения. Требования, предъявляемые к системе и процессу регистрации изложены в стандарте ISO/IEC 19794-6:2011 [67]. Когда речь заходит о массовом производстве, стоимость, компактность и удобство использования становятся существенными, и поэтому не все, упомянутые в стандарте [67], требования могут быть удовлетворены. В значительной степени это касается системы регистрации изображения. Не менее важным моментом является то, что рынок мобильных устройств подразумевает их использование по всему миру,

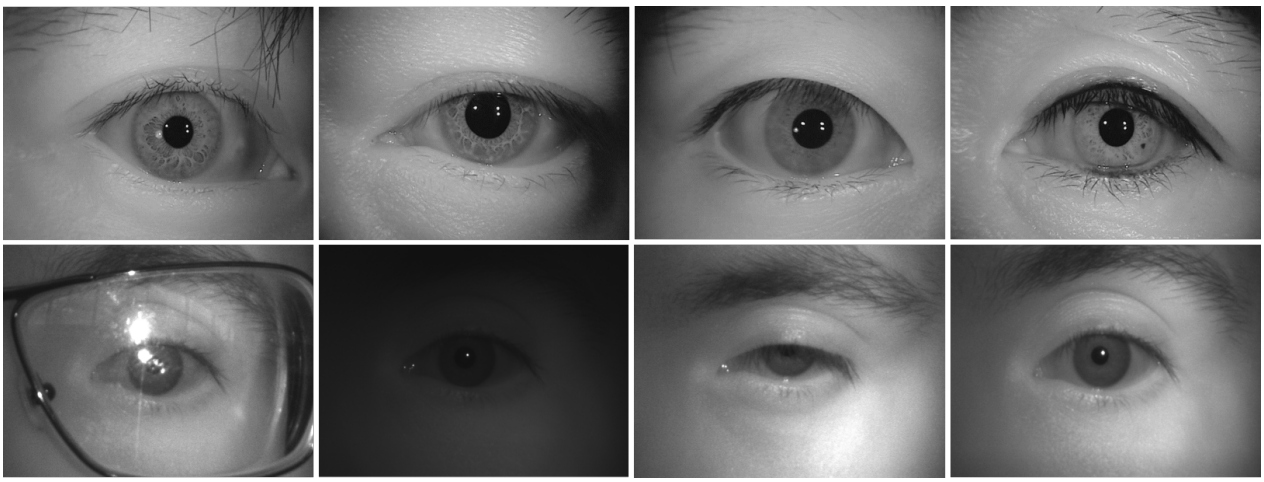


Рис. 2.1. Примеры изображений полученных при фиксированных условиях окружения (сверху), и изображений, полученных при помощи мобильного устройства (снизу)

становится важно учитывать все возможные поведенческие и расовые особенности конечных пользователей. По этой причине, в частности, не допускается использование изображений, зарегистрированных в видимом диапазоне спектра, т.к. текстура радужки темных (в основном коричневых) оттенков оказывается практически неразличимой. Более подробно о преимуществах распознавания по радужке в БИК диапазоне изложено в работах [30, 35, 38, 67], а проблемы, связанные с системами регистрации изображения радужки, подробно описаны в работах [30, 112].

Использование мобильного устройства в качестве биометрического сенсора подразумевает его способность обрабатывать биометрические данные при постоянном изменении окружения и учитывать поведение пользователя. Места использования устройства могут сильно различаться по уровням освещенности (от 10^{-4} до более 10^5 люкс под прямыми солнечными лучами), спектрам излучения источников, спектру поглощения и отражения окружающих объектов и многим другим параметрам. С другой стороны, следует учитывать и особенности пользователя: он может носить очки, контактные линзы; может произвести попытку аутентификации при ходьбе или страдать от тремора рук, тем самым вызывая дрожание устройства; пользователь может удерживать устройство слишком далеко или близко к лицу, так, что радужка оказывается вне

диапазона глубины резкости камеры, и её изображение получается размытым; зрачки пользователя могут быть сильно расширены или сужены в зависимости от уровня освещенности и по другим причинам [105, 133, 4]; область радужки может быть сильно затенена веками и ресницами, если глаз пользователя недостаточно открыт. Все упомянутые факторы влияют на качество входных биометрических данных (Рис. 2.1) и, как следствие, на точность распознавания [129].

В дополнение ко всем вышеперечисленным факторам, мобильная система должна быть простой и удобной в использовании. Для биометрической системы удобство определяется простотой взаимодействия с пользователем и высокой скоростью распознавания, где последняя обусловлена вычислительной сложностью применяемого метода (Рис. 1.6). Между сложностью и энергопотреблением существует компромисс, который важно учитывать при разработке мобильных алгоритмов. Процесс аутентификации должен осуществляться с частотой поступления кадров и, в то же время, потреблять минимальное количество энергии устройства.

При разработке мобильных биометрических систем также следует принимать во внимание важное требование, предъявляемое к системам с высоким уровнем защиты. а именно, полное отсутствие доступа извне к данным, которые они обрабатывают. К таким данным относятся пин-коды, иная персональная информация и, особенно, биометрические данные. На сегодняшний день существует технологии, предоставляющие возможность обеспечить достаточный уровень защищенности данных. Они все представляют систему на чипе (SoC, System on Chip), являющуюся защищенной частью центрального процессора устройства, с развернутой на нем отдельной операционной системой, например TrustZone от ARM или Qualcomm [12]. Такого рода системы накладывают дополнительные ограничения на приложения, с которыми они работают. Ограничения выражаются в виде еще более заниженной доступной тактовой частоте процессора, невозможности использовать многопоточность и существенно огра-

ниченном обьеме доступной оперативной памяти.

2.2. Метод аутентификации по радужке с мобильного устройства

Несмотря на успешное внедрение множества биометрических систем распознавания по радужке по всему миру, мобильные приложения этой технологии являются новой областью для исследований [84, 150]. Это связано с тем, что известные на сегодняшний день алгоритмы и решения не способны обеспечить достаточную точность распознавания на данных, полученных с мобильного устройства. В большинстве исследований в данной области используются изображения, полученные в видимом диапазоне[16, 45, 120]. В работе Thavalengal и др. [132] исследована возможность использования комбинированного решения, использующего изображения радужки, полученные одновременно в видимом и БИК диапазонах. Утверждается, что для предложенной системы и метода, распознавание на расстоянии превышающем 15 см все еще затруднено. Примером решения, использующего БИК диапазон, является работа Zhang и др. [151], в которой представлены результаты, демонстрирующие перспективность подхода с объединением для распознавания двух модальностей: радужки и лица. Апробация метода производилась на внутренней базе данных радужек и лиц. Одной из наиболее релевантных работ, предлагающих использование БИК диапазона для мобильных приложений, является [72]. Предлагается использовать дополнительные факторы, оказывающие влияние на качество изображения радужки, в частности, уровни освещенности и смазанности при оценке качества изображения и сравнении биометрических эталонов.

На сегодняшний день уже существует несколько коммерческих решений для распознавания человека по радужке с мобильного устройства. Первый смартфон с технологией распознавания по радужной оболочке глаза Delta ID Inc. [39, 82] был представлен компанией Fujitsu в 2015 году [47]. В 2016 году компания

Microsoft представила серию смартфонов Lumia 950 [93], оснащённых сканером радужки. Следом еще несколько компаний представили свои решения. Упомянутые компании использовали собственные данные, собранные для исследований и тестирования своих решений. Результаты по производительности алгоритмов не были опубликованы.

В данной главе представлено алгоритмическое решение для аутентификации человека по радужке, способное обеспечить точность и скорость распознавания достаточные для применения в мобильных приложениях. Основными особенностями метода являются: многостадийная структура алгоритма; новый подход к оценке качества изображения, позволяющий дать исчерпывающую оценку изображению радужки с учетом особенностей работы с мобильным устройством; а также новый адаптивный метод квантования вектора признаков радужной оболочки глаза. Данные особенности позволяют осуществлять распознавание в режиме реального времени в условиях сильного изменения окружения и обеспечить обратную связь с пользователем устройства. Решение детально описано в [105].

2.2.1. Структура алгоритма распознавания

Основная идея предлагаемой структуры алгоритма состоит в том, чтобы выполнять наиболее вычислительно сложные операции только с изображениями самого высокого качества. В данном случае под качеством понимается совокупность критериев, отражающих пригодность изображения радужки для извлечения особенностей и распознавания. Весь алгоритмический конвейер можно разделить на несколько частей, объединенных промежуточными этапами выбора изображений наилучшего качества. Общая схема предложенного алгоритма распознавания по радужной оболочке глаза с мобильного устройства представлена на Рис. 2.2.

На приведенной схеме (Рис. 2.2), можно выделить два основных блока обработки (до буфера изображений и после). Операции первого блока начинают-

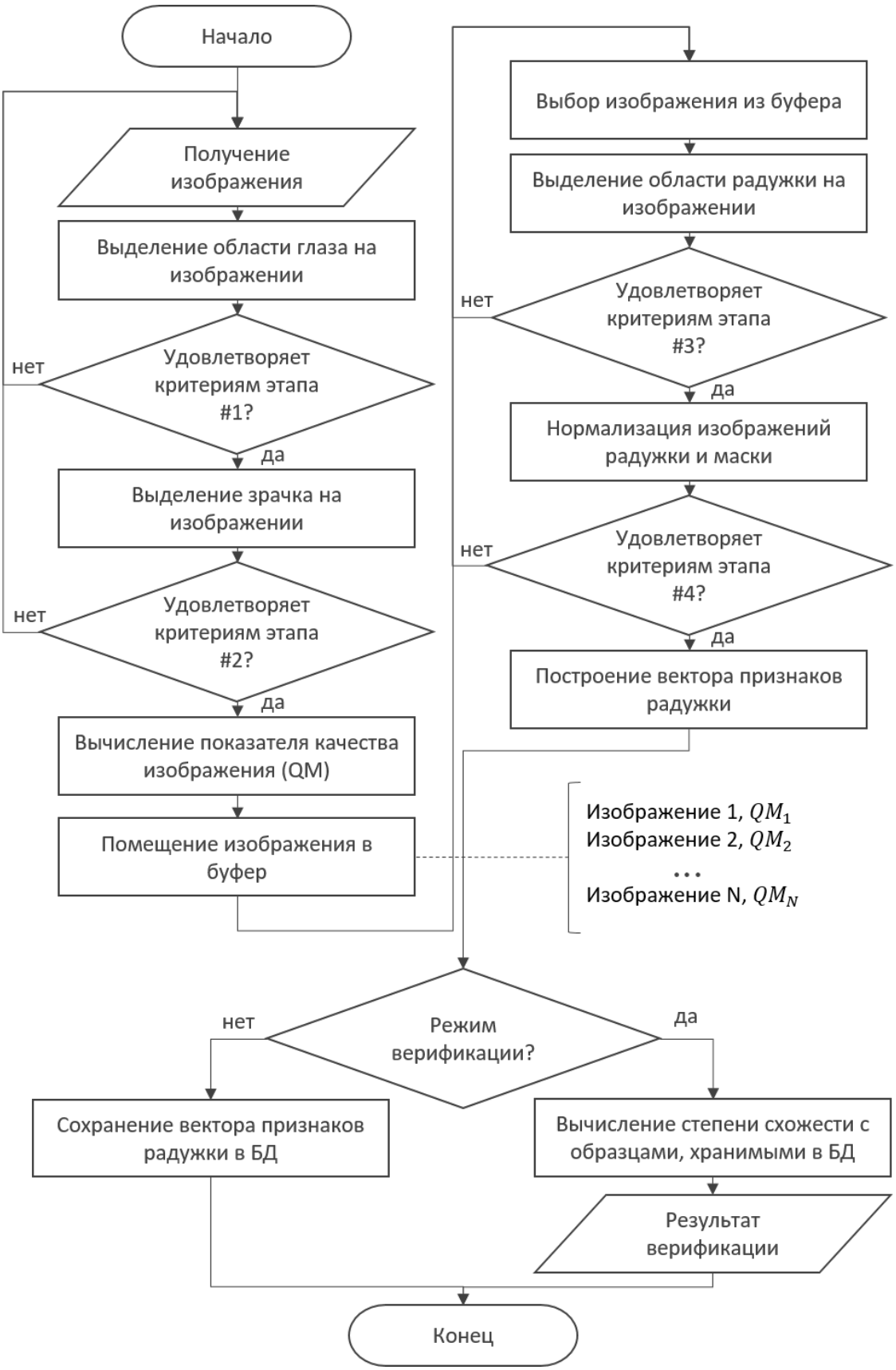


Рис. 2.2. Блок схема алгоритма распознавания по радужной оболочке глаза с мобильного устройства

ся с получения изображения и заканчиваются вычислением промежуточного показателя качества QM и помещении изображения в буфер. Операции второго блока начинаются с выбора из буфера изображения, для которого текущее значение QM является максимальным среди всех, находящихся в буфере, а заканчивается выделением уникальных особенностей и построением вектора признаков радужки.

Первый блок осуществляет обработку данных с частотой поступления кадров. На первом этапе производится выделение области глаза на входном изображении. Предложенный метод основан на применении метода MLBP, предложенного в работе [75], продемонстрировавшим наилучшие результаты для изображений с мобильного устройства. Полученные изображения проходят процедуру предобработки, включающую в себя подавление шума, а также повышения контрастности на границах зрачка и радужки. Предобработка производится с использованием оператора Шарра, представляющего из себя модификацию фильтра Собела, обладающую свойством более высокой вращательной симметрии [124]. Фильтрация производится путем свертки входного изображения с заранее подобранным набором ядер Шарра. Далее на изображении производится выделение зрачка, путем определения координат его центра и границы. различные подходы к выделению зрачка рассмотрены в [4]. Для простоты в предложенном методе зрачок параметрически представляется в виде окружности, имеющей центр (x_p, y_p) и радиус r_p. Зрачок также часто описывают эллипсом либо фигурой сложной формы. Выделение зрачка, также, обычно производится в несколько этапов. В большинстве работ, с целью ускорения вычислений, обычно можно выделить два основных этапа: грубая оценка параметров и их последующее уточнение. Методы грубой оценки зависят от условий применения. Здесь для грубой оценки предлагается метод, основанный на применении сверточных нейронных сетей, подробно описанный в главе 3.2, а для уточнения

используется интегро-дифференциальный оператор Догмана (2.1) [35].

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint\limits_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|, \tag{2.1}$$

где $I(x,y)$ — яркость изображения.

Оператор осуществляет поиск области на изображении, где достигается максимум частной производной от нормализованного интеграла по r по направлению увеличения величины радиуса. Несколько модификаций подхода Догмана рассмотрены в работах [11, 65, 73, 91]. Далее производится оценка положения век на изображении. Их положение описывается координатами точек E_u и E_l для верхнего и нижнего век соответственно, как показано на рис. 2.3. Предложенный метод определения положения век подробно описан в работе [103] и основан на применении набора разнонаправленных фильтров Габора для предобработки, и последующим уточнением границы века модификацией интегро-дифференциального оператора для параболический кривой (2.2).

$$\max_{(a,k,h)} \left| \sum_a \sum_k G_\sigma * \frac{\partial}{\partial h} \sum_a (y-k)^2 - 4a(x-h) \right|, \tag{2.2}$$

где (k,h) — вершина параболы, a — её кривизна.

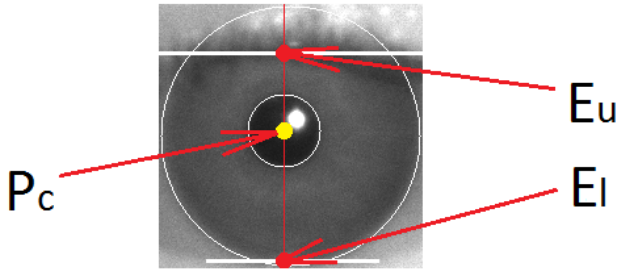


Рис. 2.3. Определение положения верхнего E_u и нижнего E_l век, P_c - центр зрачка

Вычисление промежуточного показателя качества является завершающей операцией первого блока и может производится различными способами. В данной работе в качестве оценки предлагается вычисление взвешенной суммы по

нескольким накопленным в процессе обработки параметрам качества, среди которых: средние яркости полного кадра I^f_{avg} и области глаза I^e_{avg} (Рис. 2.3), значение контраста на границе зрачок-радужка C_{pi}, степень открытости глаза NEO (2.3), выраженная по значениям E_l и E_u (Рис. 2.3). Коэффициенты регрессии между набором используемых метрик и значением математического ожидания соответствующего распределения степени схожести для пар сравнений свой со своим предложено использовать в качестве весов для вычисления финального показателя качества.

Поскольку входные данные представляют собой видеопоследовательность, а не единичный кадр, можно выбирать изображения наилучшего качества в течение заранее определенного периода времени по завершению любого этапа алгоритма. Выбор может быть выполнен с использованием показателей качества, которые были оценены до помещения изображения в буфер (Рис. 2.2). После того как буфер полностью заполнен, каждый последующий кадр вытесняет один из кадров худшего качества в течение предопределенного времени. Как только заданное время истекло, выбранные изображения переносятся на второй этап обработки. В качестве временной константы может быть выбрано время полной обработки изображения на втором этапе.

Второй этап состоит из более вычислительно сложных операций. Обрабатываются только изображения из буфера. Этап начинается с поиска центра (x_i, y_i) и радиуса r_i радужки на изображении глаза с использованием информации о параметрах зрачка. Используемый подход к поиску аналогичен тому, что использовался для поиска зрачка. Информация о расположении век используется здесь для выбора диапазона углов при обходе контура интегро-дифференциальным оператором. Информация о положении век используется для определения области поиска интегро-дифференциальным оператором. Для удаления ресниц и частично затенений используется подход, описанный в [9]. Далее над изображениями радужки полученной маски осуществляется операция нормализации (1.1). Последним этапом второго блока является извлечение уникальных

особенностей радужки и построение вектора признаков.

Извлечение особенностей радужки производится для каждого кадра, прошедшего все проверки по качеству. Заранее определенное количество векторов признаков, полученное в процессе регистрации (N_E) сохраняется в базе данных. Все они используются в дальнейшем для сравнения. Так как, возможность накапливать векторы признаков предлагается использовать и при верификации, существует несколько вариантов их использования. Метод сравнения «каждый с каждым» подразумевает $N_E \times N_V$ количество сравнений, а это не всегда оправдано (N_V - текущее количество векторов признаков в режиме верификации). Для того чтобы уменьшить количество сравнений, несколько векторов признаков могут быть отобраны в качестве наиболее репрезентативных. Правило отбора таких векторов основано на измерении для них степени схожести внутри одного класса. Пара векторов, для которых степень схожести минимальна выбираются в качестве образцов для последующего сравнения с векторами, хранящимися в базе данных. Таким образом количество сравнений уменьшается и становится равным $0.5 * N_V(N_V - 1) + 2N_E$. Если для N_E и N_V выполняется условие $N_E > N_V/2$, то количество сравнений значительно уменьшается.

2.2.2. Оценка качества изображения радужки

Оценка качества изображения является неотъемлемым этапом распознавания [4]. В литературе известно множество подходов к оценке качества изображения радужки [26, 31, 44, 49]. Однако, большинство из них не рассматривает мобильные приложения. Подход, описанный в данной работе, имеет несколько ключевых особенностей по сравнению с методами, известными ранее [58, 111].

Главной особенностью решения является предложенный набор критериев качества изображения радужки. Набор составлен из метрик, позволяющих оценивать качество с учетом большинства возможных сценариев использования устройства. Оценка по каждому из критериев производится сразу после того, как произведено соответствующее измерение.

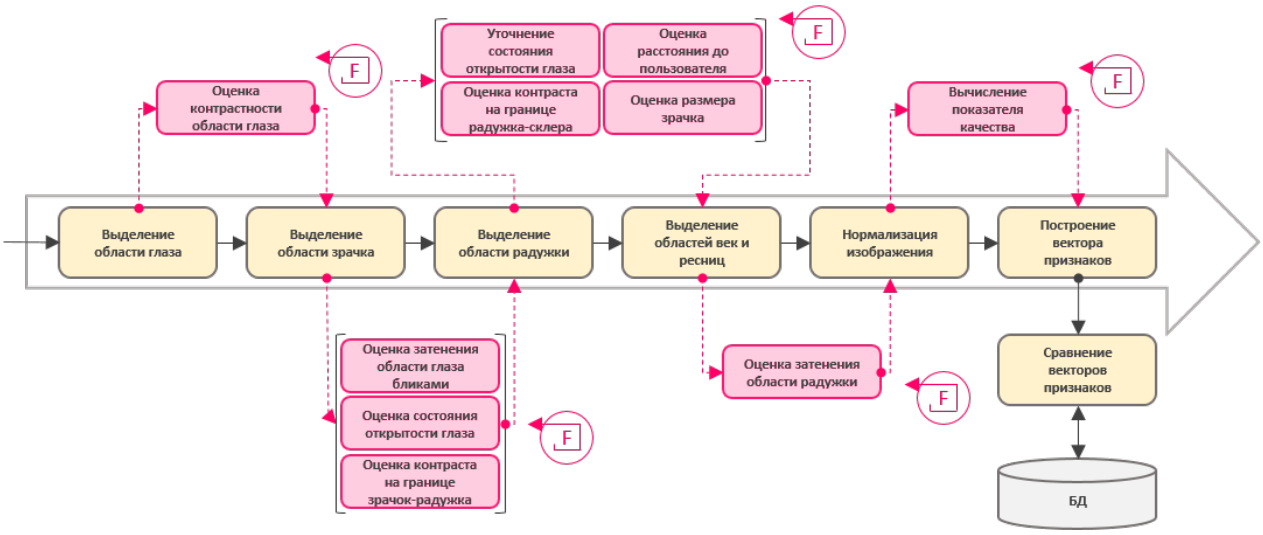


Рис. 2.4. Общая схема алгоритма оценки качества изображения

Персональное мобильное устройство подразумевает постоянное взаимодействие с пользователем. По этой причине второй особенностью предложенного решения является способность осуществлять обратную связь с пользователем устройства. В случае отсеивания кадра по какому-либо критерию качества, пользователю автоматически выводится подсказка в понятной для него форме. Например, если вычисленное расстояние до лица выходит за заранее определенный допустимый предел, то пользователю будет предложено расположить устройство ближе либо дальше.

Оценка качества также позволяет поддерживать обратную связь не только с пользователем, но и с аппаратной частью устройства, обеспечивая корректировку параметров системы регистрации изображения, с целью получения кадров наилучшего качества (подробнее в заявке на изобретение [2]). Например, изображение области глаза было классифицировано как переэкспонированное. Алгоритм автоматически корректирует значение экспозиции для регистрации последующего кадра. На схеме (Рис. 2.4) изображена структура алгоритма оценки качества изображения. Обратная связь с пользователем и аппаратной частью условно обозначена буквой $F(feedback)$ со стрелкой.

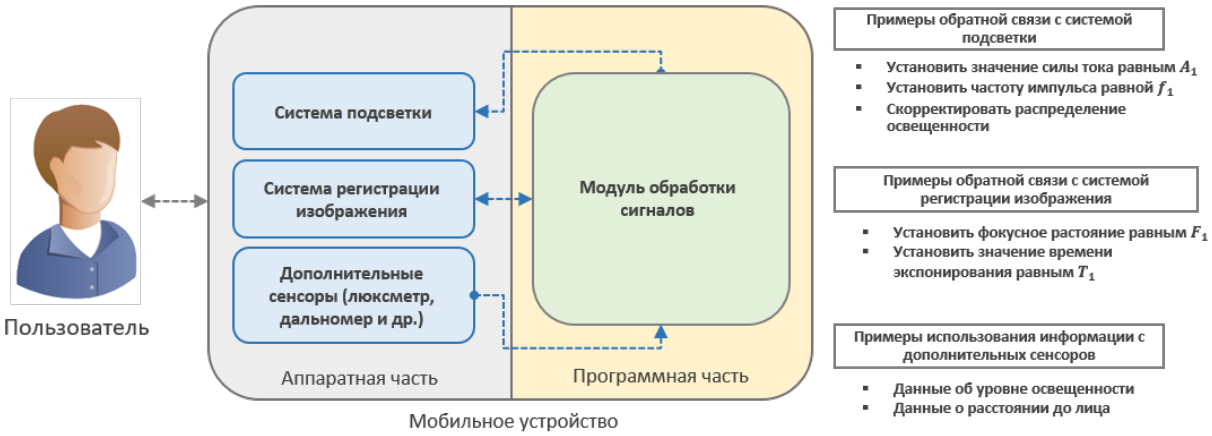


Рис. 2.5. Условная схема взаимодействия между элементами системы распознавания

2.2.3. Использование дополнительных сенсоров

Отличительной особенностью метода является использование информации с дополнительных сенсоров, доступных для использования внутри устройства. Так, например, информация об уровне освещенности, данные с дальномера и иные доступные данные могут быть использованы для подстройки как параметров аппаратной части устройства, так и алгоритма. Таким образом реализуется связь между ключевыми компонентами биометрической системы: пользователем, аппаратной и программной частями устройства (Рис. 2.5). Детальное описание предложенного метода приведено в заявке [5].

Вводятся дополнительные метрики оценки качества, позволяющие ускорить процесс обработки информации внутри алгоритма. Обе преложенные метрики (2.3, 2.4) описывают уровень открытости глаза на различных этапах алгоритма с использованием информации о положении век E_u и E_l.

$$NEO_p = \frac{|E_l - E_u|}{R_p} \tag{2.3}$$

$$NEO_i = \frac{|E_l - E_u|}{R_i} \tag{2.4}$$

Метрики NEO_p и NEO_i (NEO, сокр. - normalized eye opening) вычисляются и используются на разных этапах алгоритма, сразу, как только информация

о значения радиусов зрачка R_p и радужки R_i становится доступной. Введение пары метрик позволяет оценивать уровень открытости глаза на ранних этапах алгоритма и показало свою полезность на практике.

Заключительным этапом алгоритма является построение вектора признаков с применением фильтра Габора к нормализованному изображению радужки, а также метода адаптивного квантования, подробно описанного в главе 4.1. Параметры фильтра подобраны в результате оптимизации методом Нелдера-Мида на обучающей выборке.

Экспериментальные результаты

Экспериментальные результаты включают в себя оценку точности и скорости распознавания, а также описание данных, использованных для оценки.

Описание базы данных

На сегодняшний день не существует достаточно представительных баз данных изображений радужных оболочек глаза, полученных в БИК области частот, достаточных для того, чтобы произвести комплексную оценку метода с учетом изменений условий окружения, учитывающих особенности поведения пользователя, цвет глаз и т.д. По этой причине для проведения исследований и разработки была собрана собственная база данных. Каждый биометрический образец представлен пятисекундным видеороликом, отражающим попытку регистрации/верификации. Детальная информация о собранной БД представлена в Таб. 2.1.

База данных собрана с использованием мобильного устройства (планшета), оснащённого встроенной компактной камерой, работающей в БИК диапазоне, и активной БИК-подсветкой. Для сбора был установлен следующий сценарий: пользователь берёт устройство на начальном расстоянии около 35 см; начинается запись видеоролика и пользователь приближает устройство ближе к глазу до расстояния 15 см в течение 5 секунд. Такой подход был выбран из соображений возможных особенностей взаимодействия пользователя с устройством, таких как более удобное расстояние, возможное дрожания рук и т.д.

Параметры	Без очков	С очками
Количество пользователей	286	123
Количество радужек	566	222
Число сравнений	27 149 310	2 936 082
Расовая принадлежность	Азиаты & Европеоиды	
Количество глаз в кадре	один глаз	
Количество видеороликов на каждый глаз	$\leq$10	
Количество кадров в видеоролике	75	
Расстояние съемки	$15 - 35$ (см)	
Разрешение матрицы камеры	1280×720	

Таблица 2.1. Характеристики использованной базы данных

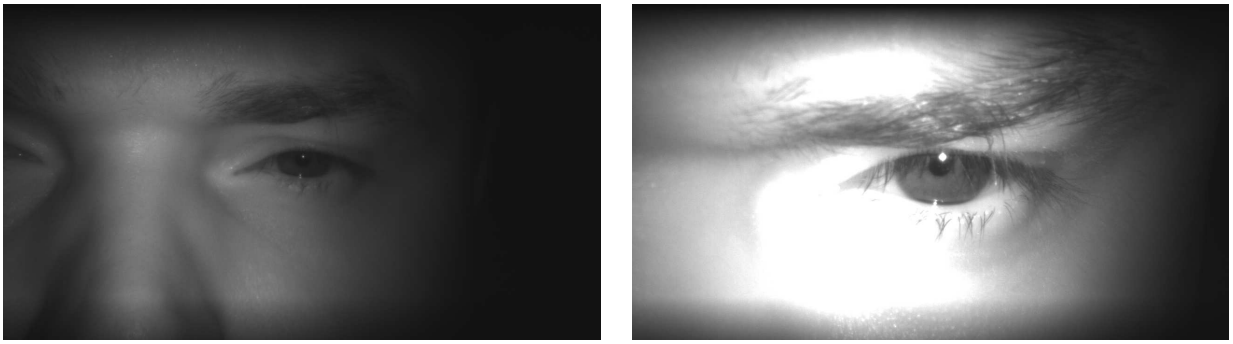


Рис. 2.6. Примеры изображений, полученных на разных расстояниях от лица до устройства: 18 и 30 (см) слева и справа соответственно

Примеры изображений, снятых камерой, представлены на Рис. 2.6. Изображения взяты из одной и той же видеопоследовательности, но соответствуют разным расстояниям (18 и 30 см). Все видеопоследовательности используются для моделирования попыток регистрации и верификации. Для обоих сценариев использовались одни и те же параметры алгоритма, поэтому значение FTE равно значению FTA (Таб. 2.2).

Результаты по точности распознавания

В соответствии с общепринятыми понятиями и определениями, подробно описанными, например, в [41], а также стандартах ISO/IEC 19795-1:2006, ISO/IEC 19794-6:2011 и ГОСТ Р ИСО/МЭК 19795-1-2007, для оценивания про-

изводительности системы распознавания были выбраны следующие (основные):

- FTE (failure to enroll) - количество транзакций регистрации, для которых не возможно завершить извлечение биометрического эталона;
- FTA (failure to acquire) - количество транзакций верификации, для которых не возможно завершить извлечение биометрического эталона;
- Степень схожести - численная мера близости двух биометрических эталонов;
- FNMR (false non-match rate) - вероятность ложного несовпадения;
- FMR (false match rate) - вероятность ложного совпадения;
- EER (equal error rate) - равный уровень ошибок, коэффициент, при котором FNMR=FMR;
- Enrollment template - биометрический шаблон, полученный в режиме регистрации, содержащий один или несколько биометрических эталонов;
- Probe template - биометрический шаблон, полученный в режиме верификации, содержащий один или несколько биометрических эталонов;

Полученные результаты по точности распознавания предложенного алгоритма представлены в таблице 2.2. Данные значения были получены с использованием системы автоматического тестирования и базы данных, описанной в таблице 2.1.

Процедура тестирования состояла из нескольких этапов:

1. Формирование биометрических эталонов из всех видеопоследовательностей в режиме регистрации;
2. Формирование биометрических эталонов из всех видеопоследовательностей в режиме верификации;
3. Формирование списка всех возможных пар сравнений шаблонов (enrollment-probe);

4. Вычисление значений степени схожести для каждой из пар биометрических шаблонов;

5. Вычисление показателей точности распознавания (Таб. 2.2);

Оценка FTA и FTE производится по результатам выполнения шагов 1 и 2. Полученные значения (Таб. 2.2) отражают возможность метода обрабатывать данные, полученные в сложных условиях.

Поскольку система аутентификации представляет собой бинарный классификатор, точность распознавания для нее оценивается с помощью ROC (receiver operating characteristic) кривой, отражающей зависимость между величинами FMR и FNMR [85]. Значения FMR и FNMR изменяются в зависимости от внутренних параметров системы распознавания, таких как порог принятия решения, с которым сравнивается полученное значение степени схожести биометрических эталонов, а также самих значений степени схожести. Более подробно о процедуре оценивания описано в работе [105].

Значение	Без очков	С очками
FTA/FTE	0.0685	0.07001
FMR	10^{-7}	10^{-6}
FNMR	0.01077	0.03912
EER	0.00128	0.00574

Таблица 2.2. Результаты по точности распознавания

Результаты по скорости распознавания

Производительность метода оценивалась при помощи вышеупомянутого планшета, оснащенного процессором Qualcomm Snapdragon 800 (2.26 GHz, Quad-core). Измерения производились на одном ядре процессора. Медианное время выполнения составило 25 и 42 (мсек) для операций первого и второго блоков (2.2.1, Рис. 2.2) соответственно.

2.3. Выводы ко второй главе

Рассмотрены основные трудности, связанные с биометрическим распознаванием человека по радужной оболочке глаза при помощи мобильного устройства. Предложены, протестированы и внедрены:

1. новая многостадийная структура алгоритма для автоматического распознавания, построенная с использованием промежуточных блоков оценки качества изображения, позволяющая осуществлять распознавание человека при помощи устройства со значительно ограниченной вычислительной мощностью в режиме реального времени ($\approx$ 15 кадров/сек.), удовлетворяющая критериями ошибок: $FNMR \leq 1\%$ при $FMR < 10^{-7}$;

2. алгоритм оценки качества, позволяющий:

   - комплексно оценивать качество входящего изображения радужки на предмет его пригодности для извлечения признаков и формирования биометрического эталона;
   - обеспечивать обратную связь с пользователем путем отображения подсказок, понятных пользователю, на экране устройства, на основании внутренних измеряемых показателей качества изображения;
   - производить управление параметрами системы регистрации изображения с целью получения изображения радужки наилучшего качества;
   - учитывать и использовать данные с иных доступных сенсоров, позволяющих получать дополнительную информацию об окружении.

Глава 3

Выделение области радужки на изображении

Выделение (сегментация) области радужки на изображении – один из основных этапов распознавания. Ошибки сегментации влекут за собой рост числа ошибок распознавания, делая систему менее надежной и удобной в использовании. Подавляющее большинство существующих подходов ориентированы на использование систем в условиях слабо изменяющегося окружения. Классические методы, основанные на эвристиках, хорошо зарекомендовали себя здесь. Широкое распространение технологий распознавания создает необходимость обеспечения полной функциональности систем в более широком диапазоне условий и, как следствие, создания более гибких и устойчивых решений.

3.1. Особенности выделения радужки в сложных условиях

Сложные условия окружения, характерные для сценария взаимодействия пользователя с мобильным устройством, оказывают значительное влияние не только на свойства самого биометрического признака, но и на качественные характеристики изображения, из которого следует предварительно извлечь информацию, описывающую его уникальные особенности.

Факторы окружения в особенной степени существенны для биометрической системы, использующей изображение объекта распознавания в качестве входных данных, в особенной при распознавании по радужке: уровень окружающего освещения варьируется в диапазоне от 10^{-4} в ночное время суток или темном помещении до 10^5 (лк) в полдень под прямыми солнечными лучами; распределение освещенности в области радужки, определяемое характеристиками и расположением источников света относительно лица и радужки. Изме-

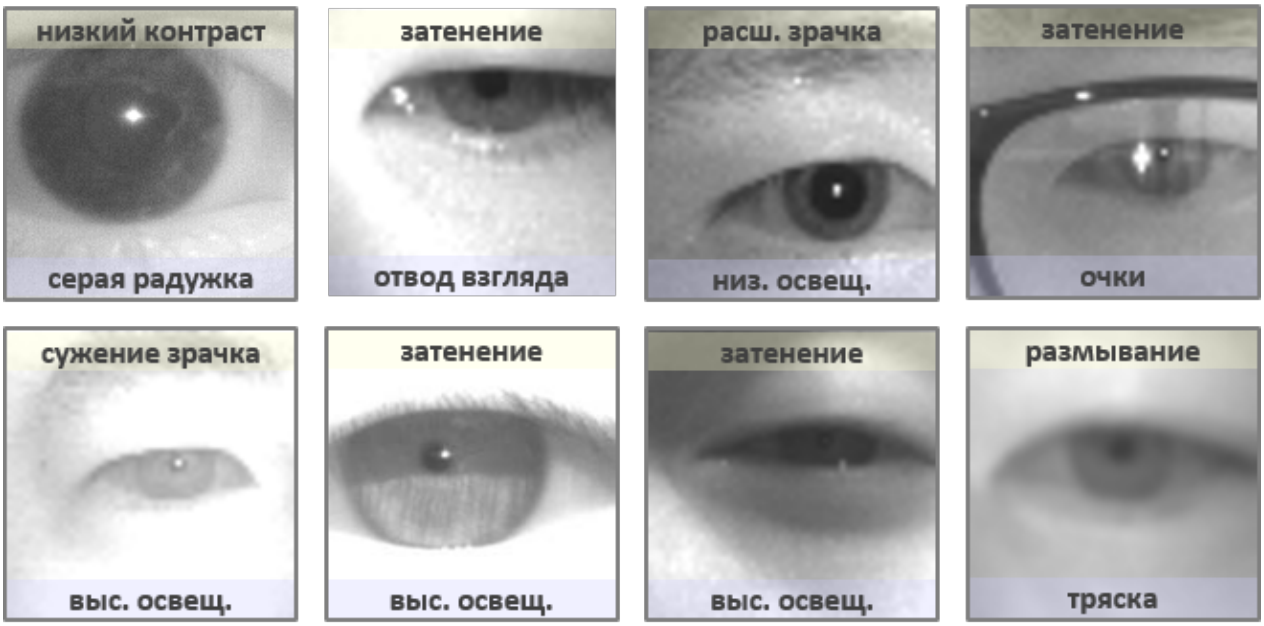


Рис. 3.1. Примеры изображений полученных при помощи мобильного устройства: причина (снизу) и следствие (сверху)

нение размеров зрачка приводят к деформации структуры радужки, различные погодные условия вынуждают пользователя устройства моргать, сильно прищуривать глаза и могут значительно снизить качество изображения в целом. Факторы окружения, влияющие на распознавание, подробно описаны в литературе [102, 119, 133, 150], а некоторые примеры изображений радужки, получаемых в сложных условиях, приведены на Рис. 3.1 и 1.7.

Важной особенностью распознавания при помощи мобильного устройства являются поведенческие характеристики пользователя, описанные в главах 1.5 и 2.1. Примеры ошибок выделения области радужки на изображении в следствие влияния факторов окружения и особенностей поведения пользователя приведены на Рис. 1.7.

3.2. Методы выделения радужки на изображении

3.2.1. Обзор существующих методов

Существует большое количество различных методов и подходов к решению задачи выделения области радужной оболочки глаза на изображении. Методы хорошо зарекомендовали себя для не мобильных приложений. Многие из них используются в коммерческих решениях и распространены настолько широко, что их по праву можно называть классическими.

Среди классических методов можно выделить основные направления:

- Применение интегро-дифференциального оператора (2.1), предложенного в работе [35]. Оператор используется для выделения радиально-симметричных структур, которыми, в данном случае, предлагается описывать зрачок и радужку. Метод имеет высокие точность и устойчивость, но обладает неприемлемой для большинства приложений вычислительной сложностью [4]. Примеры использования [8, 15, 17]. Примеры совершенствования исходного решения путем добавления различных методов предобработки представлены в работах [10, 11, 65, 73, 91];

- Анализ гистограммы изображения, бинаризации и последующее оценивание радиусов зрачка и радужки [55, 87, 108]. Методы показали свою работоспособность на качественных изображениях [28, 137], однако, в сложных условиях [109, 115] их применение сильно ограничено;

- Методология Хафа (Hough), позволяющая оценить параметры кривых заданного вида (в данном случае окружностей, описывающих зрачок и радужку) с использованием т.н. аккумуляторов. В качестве примеров использования различных подходов внутри методологии можно привести следующие [18, 24, 116, 140]. Данный подход позволяет получить выигрыш по скорости обработки, но гораздо менее устойчив к зашумлённым

данным в сравнении, например, с методами, использующими интегро-дифференциальный оператор.

Существенная часть работ, посвящённых выделению области радужки за последнее время и приходящаяся на период с 1997 по 2014 годы, сосредоточена вокруг вышеперечисленных методов [79]. В работах предлагаются различные варианты улучшения методологий путем добавления процедуры специальной предобработки изображения [108, 146], решающих правил, основанных на всевозможных эвристиках [22, 35, 90, 97, 153, 4], а также техник машинного обучения. Общая схема классического подхода изображена на Рис. 3.2 Методы хорошо разобраны и классифицированы по различным особенностям в работе [4].

Рис. 3.2. Общая схема классического подхода к выделению радужки на изображении)

С увеличением количества всевозможных данных для обучения и развитием аппаратных средств область машинного обучения в недавнем времени претерпела существенные изменения. Глубокое обучение (deep learning, DL) стало одним из подходов, позволяющих эффективно использовать данные большие объемы данных. Начиная с 2012 года глубокое обучение и, в частности, глубокие сверточные нейронные сети (deep convolutional neural networks, deep CNN) были успешно применены для решения целого ряда задач компьютерного зрения, достигнув результатов, в значительной степени превосходящих полученный ранее существующими методами и даже человека [53, 74, 80, 136].

Прошло некоторое время, пока глубокое обучение достигло области биометрического распознавания и было применено для выделения радужки на изображении. На сегодняшний день создание различных приложений, в том

числе мобильных, требует от алгоритма высокой устойчивости к сильно изменяющимся условиям окружения, упомянутым ранее (2.1). Авторы [88] впервые продемонстрировали преимущества подхода к сегментации радужки с использованием свёрточных нейронных сетей, в частности, на изображениях радужек, полученных в более сложных условиях. В работе также сравниваются два основных подхода к сегментации с использованием сверточных сетей: так называемый «patch-based» подход, при котором сеть обучают с использованием небольших фрагментов исходного изображения, принадлежащих либо не принадлежащих области объекта, который необходимо выделить, присваивая каждому из фрагментов марку класса в зависимости от принадлежности; вторым подходом является т.н. «end-to-end» способ обучения, когда на вход сети подается полноразмерное изображение, а выходом её является бинарная маска той же размерности, значение каждого пикселя в которой определяет класс объекта, например: 1 - радужка, 0 - фон.

Иным примером «patch-based» подхода является архитектура, представленная в работе [13]. Незадолго до её появления, исследователи в [127] показали, что такой подход и предложенный метод обучения в значительной степени ухудшают качество сегментации, в очередной раз закрепив преимущества «end-to-end» подхода. В работе [70] продемонстрирована возможность использования архитектуры SegNet применительно к сегментации радужки, а также предложено использование техники дропаут (dropout) обучения, впервые описанной в работе [139]. Подход позволил достигнуть достаточно высокой точности сегментации, однако, в виду вычислительной сложности, не применим на практике. Иная CNN архитектура была представлена в работе [19]. Предложено исключение пулинг (pooling) слоёв, показана высокая эффективность. Однако, в работе [80] ранее утверждалось, что такой подход не позволяет извлекать сложные особенности из изображения, что критично для задачи сегментации в сложных условиях. Известно также, что отсутствие пулинг слоёв приводит к тому, что построенная на таком подходе архитектура оказывается чувствительной к раз-

личным сдвигам объекта на изображении.

3.2.2. Выделение области радужки методами глубокого обучения

В настоящей работе предложены новые CNN архитектуры. За основу взяты две базовые архитектуры, демонстрирующие лучшие результаты в задаче сегментации различных объектов на изображении: FCN (fully-convolutional network) и SegNet. Предложена новая структура основных блоков, из которых состоят обе архитектуры.

Основные подходы с использованием глубокого обучения

Архитктура FCN, впервые предложенная для решения задач семантической сегментации объектов, подразумевает полное исключение полносвязных (fully-connected) слоев [127]. Это свойство позволяет адаптировать модель, обученную для решения задачи классификации, в модель, решающую задачу сегментации объектов без дополнительных оптимизаций. Архитектура поддерживает оба (patch-based и end-to-end) подхода к обучению и представляет собой модель т.н. «кодировщик-декодировщик» (encoder-decoder), изображенную на Рис. 3.3. Роль кодировщика заключается в построении высокоуровневого представления входных данных, в то время как декодировщик осуществляют обратную задачу. Принимая на вход представление, полученное кодировщиком, декодировщик переводит его в пространство размерности исходного изображения, используя закодированную информацию о пространственном соотношении различных элементов текстуры изображения. В архитектуре FCN декодировщик построен с использованием блоков, содержащих слои деконволюции или (deconvolution layers) или транспонированные свёрточные слои, предложенные в работе [149]. Выход каждого деконвоюционного слоя объединяется с картами признаков соответствующих симметричных слоёв кодировщика с использованием т.н. пропускных соединений (skip-connections) (Рис. 3.3) с целью восстановления структурной информации.

Другим примером архитектуры, реализующей схему кодировщик-декоди-

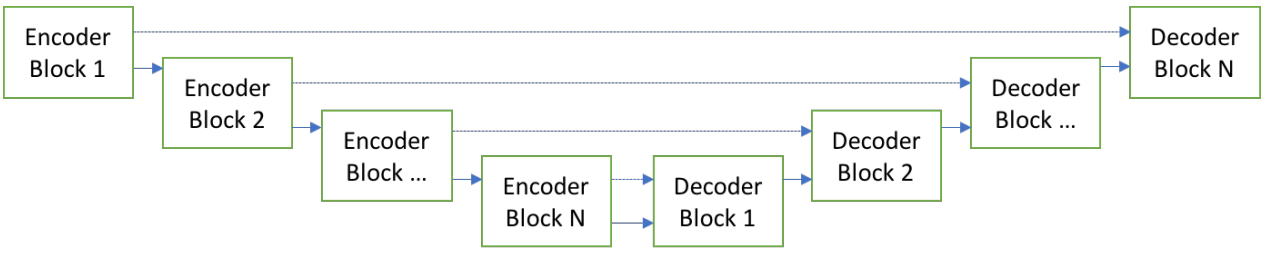


Рис. 3.3. Общая схема архитектуры кодировщик-декодировщик (encoder-decoder)

ровщик выступает SegNet [14]. Основным вкладом работы стала замена вычислительно-сложных и требовательных к памяти устройства операций деконволюции так называемыми «unpooling» слоями. Большая требовательность по объему потребляемой памяти для FCN обусловлена тем необходимостью хранить карты признаков, являющихся выходами каждого из блоков кодировщика до тех пор, пока они не будут использованы декодировщиком. Таким образом, пик потребления памяти устройства архитектурой достигается в момент, когда все карты признаков кодировщика извлечены, т.е. в момент формирования вышеупомянутого высокоуровневого представления. Архитектура SegNet позволяет на порядки снизить количество памяти, необходимой для полного прямого прохода. Несмотря на преимущества, подход SegNet с unpooling слоями снижает емкость сети, а невозможность пропускать градиенты через skip-connection при обратном распространении ошибки затрудняют обучение. Разница между структурами блоков декодировщика FCN и SegNet проиллюстрирована на Рис. 3.4.

Структура основных блоков архитектуры

Изначально идея использования остаточных (residual) связей при конструировании блоков была предложена в контексте очень глубоких сетей [60]. Далее, остаточные блоки хорошо зарекомендовали себя как эффективно использующие память и позволяющие при этом поддерживать достаточную ёмкость. Их обходные (bypass) соединения способствуют эффективной передаче градиента при обратном распространении и позволяют оптимизировать также добавочную часть в каждом соединении. Общая структура остаточного блока приведена на

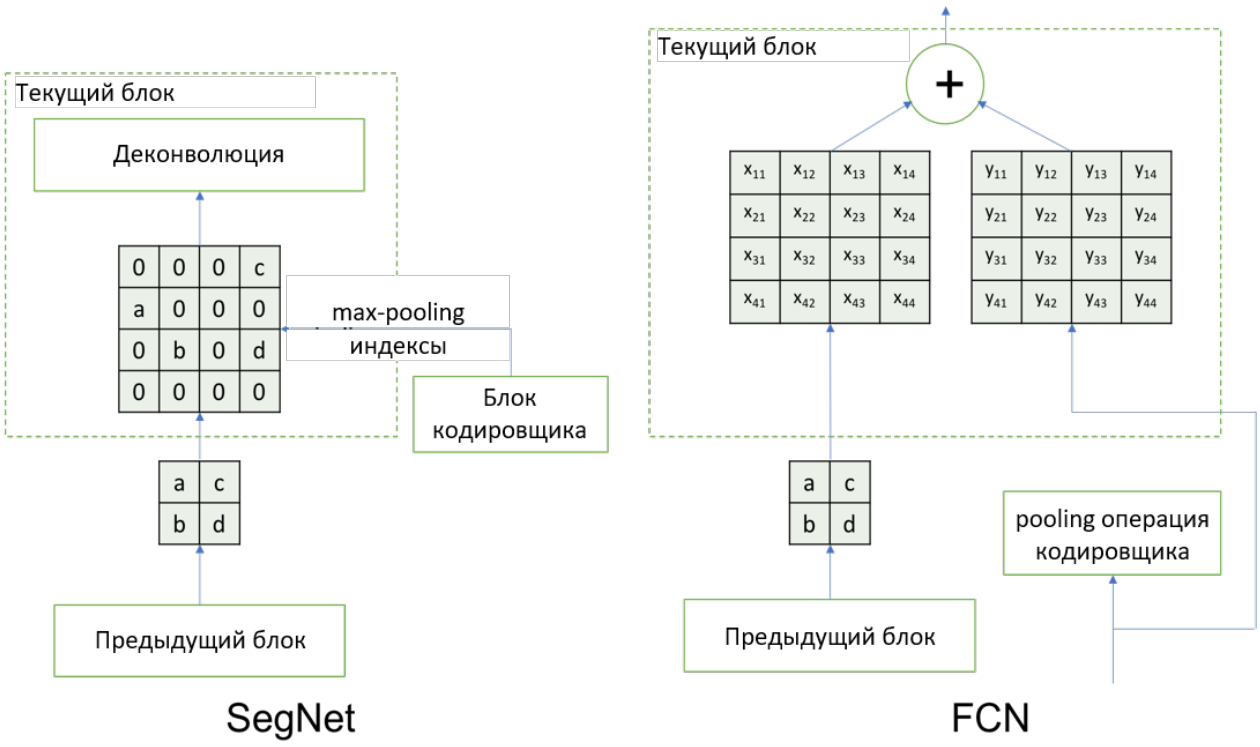


Рис. 3.4. Структуры основных блоков декодировщиков FCN (справа) и SegNet (слева)

Рис. 3.5. Авторы [60] также предложили сразу несколько модификации блока, отличающихся количеством каналов и глубиной (Рис. 3.6).

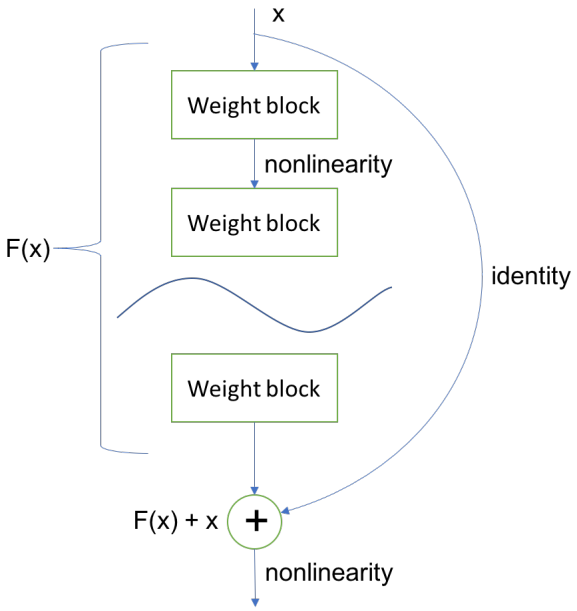


Рис. 3.5. Общая структура остаточного (residual) блока

Предложено дополнение блоков слоями нормализации (batch normalization), впервые описанными в работе [68], позволяющими ускорить сходимость модели

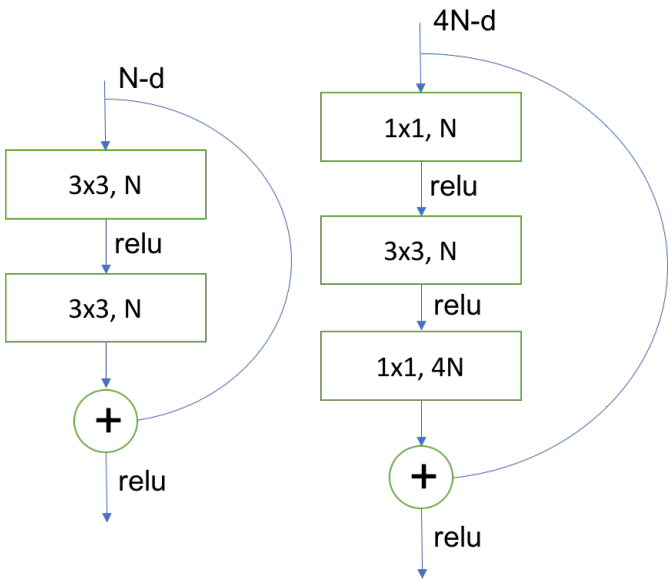


Рис. 3.6. Модификации остаточных (residual) блоков: simple - слева, bottleneck - справа

и повысить её обобщающую способность, тем самым снижать чувствительность модели к вариациям входных данных.

Предложенные архитектуры

Обе вышеупомянутые архитектуры (FCN, SegNet) были взяты за основу и модифицированы. SegNet по заявлению авторов [14] позволяет обеспечить относительно низкое потребление памяти, хотя это во многом зависит от целевой платформы и вычислительных средств. С другой стороны FCN демонстрирует лучшую показатели сходимости. Архитектура ResNet-26 с блоками типа simple была взята в качестве кодировщика и симметрично-отражённая (Рис. 3.3) как декодировщик для модифицированной FCN. Предложенная модификация SegNet представляет собой ResNet-18 кодировщик и симметрично-отражённый декодировщик (Рис. 3.3). Блоки типа bottleneck были исключены из рассмотрения для применения в FCN, т.к. требовательны к размеру карт признаков на каждом последнем слое, что является существенной проблемой для FCN. Для FCN все слои max-pooling были заменены большими значениями смещений ядра в сверточных слоях (strided convolutions). В случае с SegNet max-pooling слои были перемещены в конец каждого блока кодировщика, а смещения ядер были выбраны единичными.

Экспериментальные результаты

Экспериментальные результаты были получены на двух наборах данных: публично доступном CASIA-Iris-Lamp-V3 [29] и его модификации. Для оценки качества сегментации был выбран коэффициент Жаккара (Jaccard Index, IoU - intersection over Union, 3.1) [127]. В качестве метода для сравнения был выбран метод, демонстрирующий наилучшие результаты [88].

$$J(I_{pr}, I_{gt}) = \frac{|I_{pr} \cap I_{gt}|}{|I_{pr} \cup I_{gt}|} = \frac{|I_{pr} \cap I_{gt}|}{|I_{pr}| + |I_{gt}| - |I_{pr} \cap I_{gt}|}, \tag{3.1}$$

где I_{pr} и I_{gt} - множества пикселей, принадлежащих области радужки, предсказанных моделью и размеченными экспертом соответственно.

База данных изображений радужек CASIA-Iris-Lamp-V3 была выбрана в качестве основной для тестирования. Особенность этой БД в том, что в ней представлены изображения, полученные в осложненных, изменяющихся условиях окружения, позволяющие симулировать внутриклассовые отклонения: различные размеры зрачков, отвод взгляда, перепады яркости и др. База данных содержит 16212 изображений радужек 411 субъектов. Для оценивания методов были случайным образом выбраны 4865 изображений 124 субъектов. Разметка произведена экспертом с выполнением следующих условий: все пиксели, принадлежащие области радужки на изображении, а также ресницы, пересекающие область радужки, были приняты относящимися к классу «область радужки» (Рис. 3.7). Область ресниц, перекрывающих радужку на изображении была также отнесена к классу радужки т.к. одной из основных целей работы было показать преимущества предложенных архитектур по сравнению с существующими. Сценарий был выбран именно таким, потому что позволил существенно упростить процедуру разметки и, таким образом, увеличить количество данных. База данных была предварительно поделена на три подвыборки: обучающую (train), валидационную (validation) и тестовую (test) в соотношении 3386, 478 и 1001 изображений соответственно. Результаты, полученные на валида-

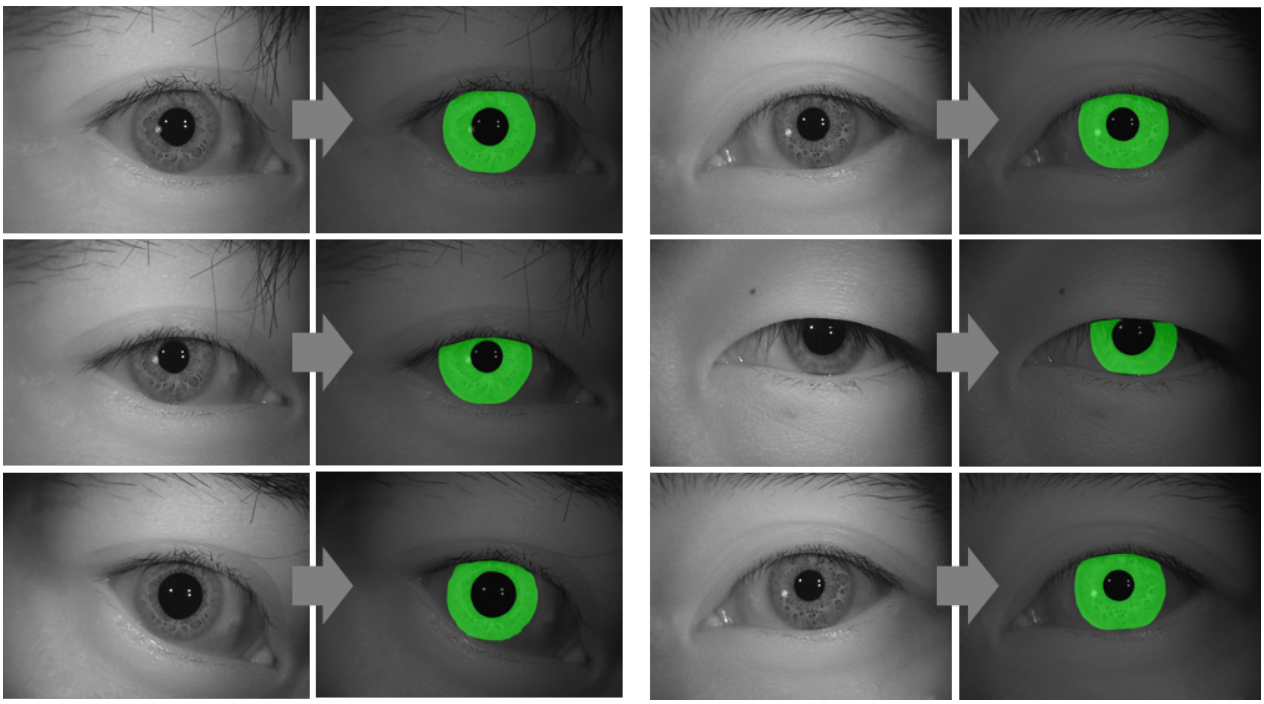


Рис. 3.7. Результаты выделения области радужки

ционной выборке, использовались для выбора лучшей модели, которая затем оценивалась на тестовой.

Исследуемые модели обучались на протяжении 200 эпох пакетами (batch) изображений по 8 штук. В качестве алгоритма оптимизации был выбран Adam [77]. Параметры обучения и тестирования были выбраны одинаковыми для всех исследуемых моделей.

Было проведено два эксперимента. В первом модели обучались на БД [29] без модификаций. Результаты представленные в Таб. 3.1, демонстрируют что обе предложенные модели показывают примерно одинаково хорошие результаты, незначительно превосходя модель [88].

$$I'(x,y) = (I(x,y) - \overline{I}) \cdot C + \overline{I}, \tag{3.2}$$

где $I(x,y)$ - исходное изображение, $\overline{I}$ - среднее значение яркости исходного изображения, C - коэффициент изменения контраста.

Целью второго эксперимента была симуляция еще более значительных изменения окружения. С этой целью над исходным набором обучающих данных

Модель	Исх. набор данных, IoU		Модиф. набор данных, IoU	
	val.	test	val.	test set
MFCN	0.918	0.919	0.668	0.676
FCN	0.930	0.930	0.884	0.894
SegNet	0.928	0.929	0.916	0.924

Таблица 3.1. Результаты по точности выделения области радужки на изображении

была произведена операция аугментации. Для этого над каждым изображением в обучающей выборке были выполнены следующие операции: значение контраста C изменялось случайным образом в диапазоне $[50\%, 150\%]$ (3.2), случайное значение в диапазоне $[-20\%, 20\%]$ также присваивалось интенсивности каждого пикселя. Финальное тестирование производилось на оригинальных изображениях из БД. Результаты показали, что предложенные модели значительное превосходят MFCN [88], демонстрируя высокую устойчивость к изменениями условий окружения, а также высокую обобщающую способность. Несколько примеров результатов сегментации радужки на изображениях из CASIA-Iris-Lamp-V3 представлены на Рис. 3.7.

Результаты по скорости распознавания

Производительность метода оценивалась на процессоре Qualcomm Snapdragon 835 (2.45 GHz). Медианное время выполнения составило 35 мсек. Алгоритмическая сложность метода, при условии фиксирования её параметров (весов и смещений) и добавления операции масштабирования на входе, линейна по размеру входных данных.

3.3. Выводы ко второй главе

Рассмотрены особенности выделения области радужной оболочки глаза на изображениях, получаемых в сложных условиях окружения, связанных с ис-

пользованием мобильного устройства и взаимодействия с пользователем. Приведен обзор и классификация существующих методов, обозначены их основные преимущества и недостатки. Рассмотрены новые методы, построенные с использованием методов глубокого обучения, выделены их основные преимущества, подчеркнуты перспективы использования и развития. Предложены, протестированы две новые архитектуры сверточных нейронных сетей, позволяющих производить устойчивое выделение области радужки на изображении низкого качества в сложных условиях окружения с частотой поступления кадров (15 кадров в секунду). Обе архитектуры позволили превзойти существующие, известные из литературы решения, основанные на глубоком обучении. Одна из предложенных архитектур успешно внедрена и используется в коммерческих продуктах.

Глава 4

Методы извлечения и сравнения уникальных особенностей радужки

Завершающими и неотъемлемыми частями алгоритма распознавания являются: извлечение уникальных особенностей (признаков) биометрического образца (-ов) и его (их) последующего сравнения, по результатам которого вычисляется степень схожести, используемая для принятия решения. Оба этапа обычно рассматриваются в едином контексте, т.к. являются смежными и сильно зависят друг от друга.

Извлекаемые признаки должны обладать следующими общими свойствами [69, 4]:

- Уникальность (информативность/значимость): признаки должны содержать в себе информацию, достаточную для того, чтобы обеспечить отличаемость биометрического образца от других;
- Стабильность (устойчивость): неизменность во времени, независимость от условий регистрации и изменчивости самого образца;
- Применимость: признаки должны быть легко извлекаемыми, сравниваемыми и храниться в компактном виде.

С точки зрения анатомии, для радужки можно выделить несколько основных источников для извлечения признаков: цвет радужки, форма зрачка, текстура радужки и др. Самыми информативным признаками радужки являются характеристики её текстуры [35]. Процедуре извлечения особенностей текстуры обычно предшествует этап нормализации (нормирования) изображения, представляющая собой конформное кольца радужки в прямоугольник, называемое

полярным преобразованием (1.1). Из литературы известно несколько вариантов такого преобразования, описанных в работе [95].

Обзоры различных методов извлечения и сравнения особенностей радужки приведены в работах [22, 23, 101, 122]. Среди модификаций можно выделить базовые подходы [4]: использование двумерных вейвлетов Габора [35], использование матриц совместной встречаемости [56, 147], использование расположения и хаарктеристик ключевых точек текстуры [113], применение дискретного косинусного преобразования [96], использование одномерный вейвлетов различных масштабов [21], различные варианты преобразования Хаара [86, 110], пирамиды Лапласа [141], метод основанный на ориентации градиентов [130]. В большинстве недавних работ предлагается использование методов глубокого обучения [51, 89, 117, 131, 152].

Специфика использования мобильного устройства (2.1, 1.5) сказывается на качестве выделения области радужки (3.1) и изменчивости текстуры радужки (1.3, 2.2). Следствием этих факторов является высокая вариативность входных данных для методов извлечения и сравнения этих особенностей. Это ограничивает возможности алгоритмов извлечения признаков, вызывая значительные внутриклассовые отклонения.

4.1. Вейвлеты Габора и адаптивное квантование фазы

Одним из наиболее распространенных подходов извлечения особенностей и представления их в виде некоторого вектора признаков (т.н. эталона) радужки является использование вейвлетов Габора. В качестве входной информации используется нормализованное изображение радужки и бинарная маска, описывающая полезную и зашумленную (ресницы, веки, блики и др.) области изображения. Базовая структура такого подхода изображена на Рис. 4.1.

Методы, основанные на применении вейвлетов Габора, являются одними из самых распространенных для не мобильных приложений, т.к. способны обеспе-

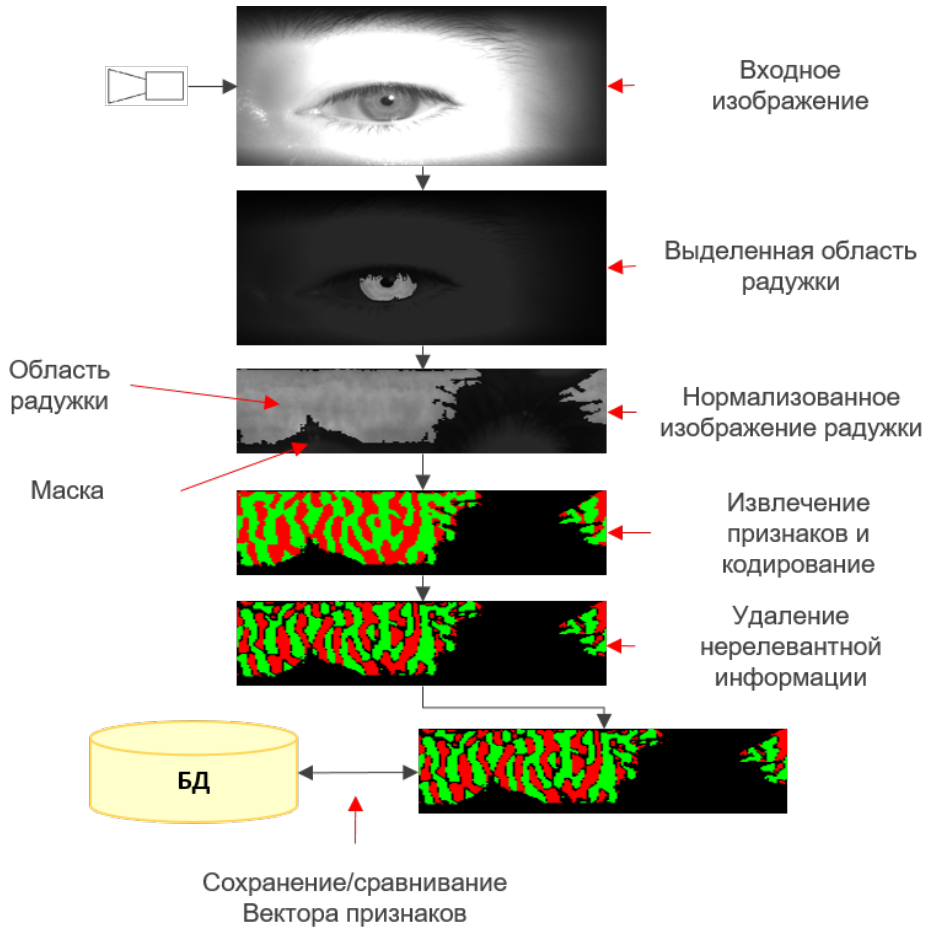


Рис. 4.1. Общая схема алгоритма извлечения и сравнения признаков радужки при помощи вейвлетов Габора

чивать достаточную точность и надежность [35]. Процедура кодирования, присущая таким методам (Рис. 4.2), необходима, в частности, для повышения стабильности представления вектора признаков и ускорения процесса сравнения. Одним из наиболее распространенных подходов к кодированию является бинарное квантование значений вектора признаков. Несмотря на то что квантование способно не учитывать нерелевантную, оно также способствует уменьшению полезной информации, дестабилизируя тем самым значения вектора признаков [63, 114]. Метод по-прежнему имеет одно важное преимущество, сделавшее его настолько популярным для использования: сравнение квантованных значений - битовая операция, а значит метод позволяет осуществлять сравнения с очень высокой скоростью. Эта особенность является очень важной, в частности,

при решении задачи идентификации, когда требуется произвести поиск максимально похожего образца по базе данных, насчитывающей большое количество примеров.

Рис. 4.2. Извлечение вектора признаков радужки вейвлетами Габора и последующее квантование

Современные модификации подхода рассматривают понятие хрупкости как неустойчивость элементов вектора без учета характера появления такой неустойчивости. В работе предлагается разделение источников нестабильности на естественные и вызванные кодированием. Предлагается новый подход к построению вектора признаков радужной оболочки. Подход состоит из двух этапов: извлечения первичных признаков с использованием фильтрации единичным вейвлетом Габора, параметра которого заранее оптимизированы, и адаптивного квантованием с предварительно оптимизированными порогами хрупкости.

4.1.1. Извлечение вектора признаков

Один из методов извлечения признаков, используемый во многих успешных коммерческих системах распознавания по радужке, основан на извлечении квантованных значений фазы после свертки нормализованного изображения с набором комплексных фильтров Габора. Этот метод был впервые предложен в

работе [34] и с тех пор подвергался различным модификациям [128, 134]. Все связанные подходы используют либо несколько фильтров с октавным увеличением частоты, либо с одним фильтром с заранее заданными параметрами. Основным преимуществом метода Габора, применяемого в этом случае, является его способность создавать полосовой фильтр с регулируемыми параметрами. Это свойство позволяет учесть априорные характеристики анализируемого объекта в частотной области. В неидеальных условиях с наличием коррелированного шума, вызванного низкочастотной разницей яркости, можно добиться более высокого качества распознавания при настройке тонкого полосового фильтра путем оптимизации его параметров.

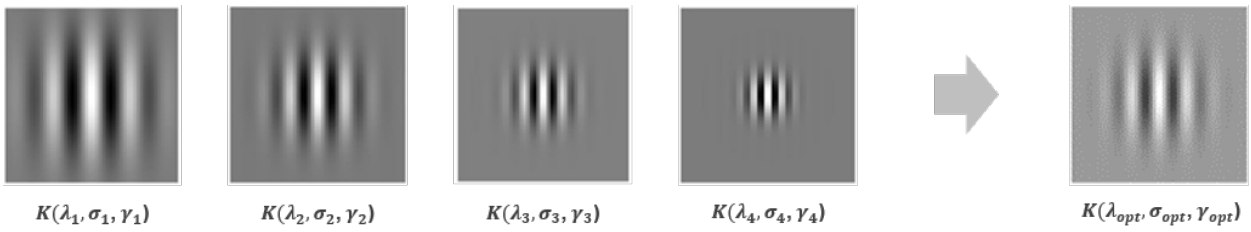


Рис. 4.3. Переход от использования нескольких ядер к одному с оптимальными параметрами

Предложен подход, использующий один фильтр с заранее оптимизированными параметрами (Рис. 4.3), различными для действительной Re и мнимой Im частей. Для оптимизации были выбраны следующие параметры ядра: длина волны λ, стандартное отклонение σ и пространственное соотношение сторон γ соответственно. Многие эксперименты, проведенные нами и другими исследователями, показали, что наиболее значимые черты радужки ортогональны ее радиальному направлению, поэтому устанавливается $\theta = 0$. В качестве целевой функции для оптимизации выбрано значение EER, отражающее частоту ошибок, соответствующую пороговому значению t, для которого FMR равна $FNMR$: $FMR(t) = FNMR(t)$. Выбор EER в качестве целевой функции позволяет оценить эффективность системы распознавания независимо от заранее определенного порога для степени схожести. Для оптимизации использовался

метод прямого поиска Нелдера-Мида [100]. Этот метод хорошо зарекомендовал себя при решении задач оптимизации, в частности, в случае наличия областей плато и седловых точек из-за его способности к нерегулярной конструкции симплекса. Оптимизация и окончательное тестирование выполнялись на наборе данных CASIA-IrisV3-Lamp [29], симулирующем изменение освещенности в процессе регистрации изображения. Весь набор данных был разделен для обучающую и тестовую выборки в пропорции 0.6/0.4.

Метод	**EER**	**d'**
OFI [34]	0.0406	3.61
Предложенный метод	0.0373	3.73

Таблица 4.1. Результаты по точности распознавания для двух алгоритмов извлечения особенностей радужки вейвлетам Габора при фиксированном алгоритме квантования

Сравнение метода производилось с базовым подходом с октавным увеличением частоты ядра (octave frequency increase, OFE), описанным в работе [34]. С целью демонстрации преимуществ обоих частей (фильтрации и квантования) предложенного метода, в качестве первого эксперимента было произведено сравнение методов фильтрации для фиксированного метода квантования. Расстояние Хэмминга (Hamming Distance, HD) выбирана в качестве меры различия пар векторов признаков радужки. Результаты представлены в таблице 4.1. Для оценки, кроме значения EER, была так еж использована метрика d', отражающая степень разделимости между полученными распределениями genuine (своих) и impostor (самозванцев). Данный показатель оказывается более чувствительным и информативным, когда выполняются условия: распределения имеют не большую площадь пересечения, распределения имеют вид Гауссового.

Результаты эксперимента (Таб. 4.1) отражают преимущества предложенного подхода. Стоит также отметить, что предлагаемый метод требует двух операций свертки (по одному для частей Re и Im соответственно), тогда как для OFI-метода требуется по крайней мере четыре (Рис. 4.3) для каждой части

(всего восемь). Т.к. размер ядра для свертки для обоих методов был выбран идентичным, можно заключить, что предложенный метод в 4 раза превосходит OFI по скорости.

4.1.2. Квантование

Квантование фазы, полученного после фильтрации сигнала, является заключительным этапом процедуры построения вектора признаков (Рис. 4.1). В оригинальной работе квантование производится в зависимости от знака фазы [34], и все элементы используются для сравнения. Кроме того, в работе [63] было показано, что не все квантованные элементы вектора признаков одинаково важны и вводится понятие хрупкости. Хрупкость в данном конкретном случае означает несогласованность информации, хранящейся в двух или более векторах одной и той же радужки. Несогласованные элементы могут быть определены из нескольких или из одного кадра. Данная работа ориентирована на однокадровый подход. Большинство современных работ [63, 83] используют константное предопределенное пороговое значение (одинаковое для Re и Im) для классификации векторных элементов на хрупкие и не-хрупкие.

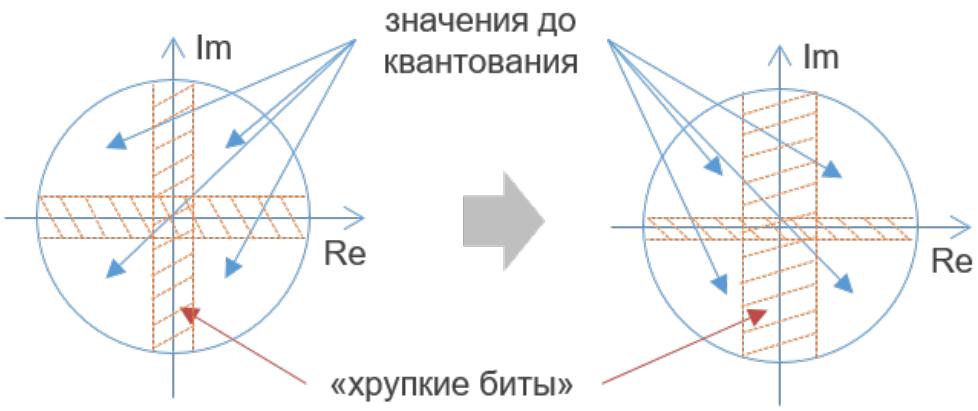


Рис. 4.4. Задание значений порогов различных для Re and Im частей

Предложенный метод подразумевает задание различных и независимых друг от друга порогов для Re and Im частей(Рис. 4.4).

Рис. 4.5. Определение порога хрупкости

Алгоритм адаптивного определения порога хрупкости использует опорное значение T_R, полученное после оптимизации и состоит из следующих этапов:

1. Значения вектора признаков упорядочиваются по возрастанию $FV = \{min..max\}$
2. Финальное значение порога хрупкости определяется как $T_F = FV[T_R * L]$, где L размерность вектора признаков (Рис. 4.5)

Опорные значения порогов $T_R(Re)$ и $T_R(Im)$ получены по результатам предварительной оптимизации на обучающей выборке полным перебором. Полученные значения $T_F(Re)$ и $T_F(Im)$ используются далее для удаления неустойчивой информации из вектора признаков после квантования.

Описание базы данных

Предложенный метод извлечение признаков проверяется на двух разных базах данных изображений радужек, полученных при помощи цифровой камеры в БИК диапазоне. Один из них CASIA-IrisV3-Lamp [29] является общедоступным и содержит изображения, снятые в условиях изменяющегося уровня освещенности (примеры изображений на Рис. 4.6). Другой набор данных был собран приватно при помощи мобильного устройства, но в сильно меняющихся условиях окружающей среды: в помещении при нормальном освещении, в темном помещении и на ярком солнце, симулируя попытки аутентификации. Описание собранной БД приведено в таблице 4.2, а примеры изображений приведены на Рис. 4.7. Параметры фильтра Габора, а также пороговые значения хрупкости (T_R) предварительно оптимизированы для каждого набора данных независимо друг от друга.

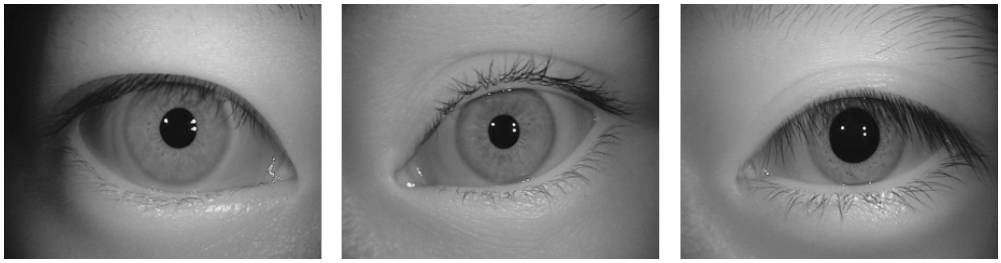


Рис. 4.6. Примеры изображений радужек из набора данных CASIA-IrisV3-Lamp

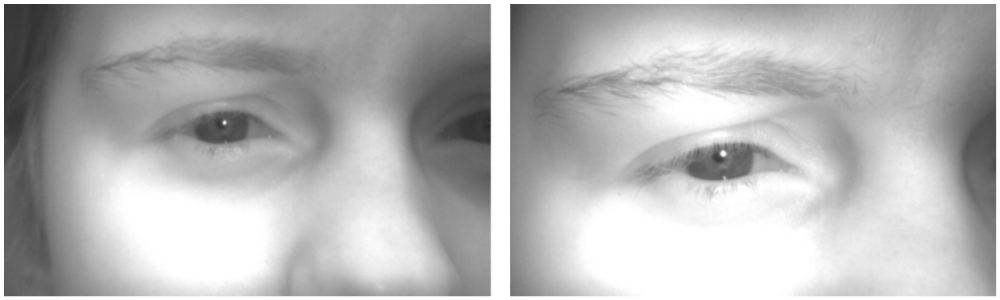


Рис. 4.7. Примеры изображений радужек из набора данных, собранных при помощи мобильного устройства

Экспериментальные результаты

Набор данных	**CASIA-IrisV3-Lamp**	**Мобильный**
Кол-во субъектов	411	286
Кол-во классов	819	566
Расы		
Кол-во радужек на изображении	1	1
Дистанция съемки	$15 \div 25$ (см)	$15 \div 35()$
Разрешение камеры (пикс.)	640×480	1280×720

Таблица 4.2. Описание баз данны тестирования

Оценивание предложенного метода адаптивного квантования производилось по значениям ERR и d'. В качестве метода для сравнения была взята работа [63]. Предложенный и описанный выше метод извлечения признаков при помощи фильтра Габора был использован в качестве основанного для извлечения признаков для обоих методов. Результаты представлены в Таб. 4.3.

Dataset	**CASIA-IrisV3-Lamp**		**Мобильный**	
	EER	d’	EER	d’
Без квантования	0.0373	3.73	0.0048	7.62
Hollingsworth [63]	0.0430	3.60	0.0043	7.77
Предложенный	0.0370	3.85	0.0040	8.01

Таблица 4.3. Результаты сравнения методов квантования

Результаты эксперимента демонстрируют превосходство метода по сравнению с [63] на обоих наборах данных.

4.2. Метод с использованием глубокого обучения

Относительно новым и одним из наиболее перспективных направлений в области биометрического распознавания, как и во многих других областях, является применение методов глубокого обучения. О преимуществах и недостат-

ках подходов, построенных на глубоком обучении, упоминалось ранее (3.2.1). Первые работы, использующие такой подход в применении к задаче извлечения и сравнения уникальных особенностей радужной оболочки глаза начали появляться в 2016 году. Отправной точкой была работа Liu и др. [89], названная DeepIris. Чуть позже Minae и др. в работе [94] провели анализ применимости подхода с извлечением признаков радужки при помощи нейронной сети, предварительно обученной на базе данных изображений ImageNet, содержащей порядка тысячи классов различных объектов. В качестве вектора признаков в таком подходе выступает вектор выходных значений, т.н. эмбеддингов (embedings), последнего полносвязного слоя сети. В работе предложено использовать данный вектор без какого-либо дополнительного обучения и подстройки параметров сети. Далее метод главных компонент (PCA) используется для понижения размерности вектора и метод опорных векторов (SVM) для классификации на genuine и impostor. В качестве базовой была использована архитектура VGG. Данную работу можно рассматривать как одну из первых попыток изучить возможности глубоких нейронных сетей в применении к задаче распознавания по радужной оболочке. Позднее Gangwar и др. [51] представили DeepIrisNet модель, объединяющую в себе перспективные методы глубокого обучения, известные на тот момент. Год спустя Tang и др. [131] представили похожу на DeepIrisNet работу, основанную на использовании эмбеддингов. В то же время Proenca и др. [117] представили метод, который они назвали IRINA. Идея работы заключалась в том, чтобы при помощи сети осуществлять поиск соответствующих патчей для пар изображений, а также Марковские случайные поля (MRF) для компенсации нелинейных искажений текстуры радужки. В качестве классификатора было предложено использовать SVM. В работе продемонстрирована высокая устойчивость к текстурным деформациям зрачка, радужки, а также к ошибкам сегментации. Однако, предлагаемая модель существенно ограничивает применимость метода для мобильных приложений в виду собственной вычислительной сложности. Подход с парой т.н. полносверточных сетей (FCN)

с модифицированной расширенной триплетной функцией потерь ETL (extended triplet loss) был предложен в работе [152]. Одна из сетей используется для извлечения признаков радужки, а вторая осуществляет построение маски. Метод нечеткого улучшения изображения в сочетании с линейной итеративной кластеризацией и нейронной сетью SOM был предложено в [7]. Несмотря на то, что метод заявлен для распознавания на мобильном устройстве, производительность в режиме реального времени не была достигнута.

Для сравнения с предложенным подходом среди вышеперечисленных были выбраны те, которые удовлетворяют следующим критериям:

- Применимость к мобильным устройствам (способность осуществлять обработку в режиме реального времени);
- Высокая точность распознавания.

Предложенный метод представляет собой сверточную нейронную сеть, спроектированную с учетом преимуществ нормализованного изображения радужки как инварианта, представления низко- и высокоуровневых признаков сравнения, а также информации об окружении. Модель состоит из двух основных частей: выделения особенностей и их последующего сравнения. Обе части обучаются совместно.

4.2.1. Низкоуровневое представление признаков

Объединение низко и высокоуровневых признаков в нейронных сетях не является новой идеей [43, 52, 71]. Известно, что первые слои в CNN отвечают за извлечение низкоуровневой текстурной информации, а представление высокого уровня достигается с глубиной [59, 148]. Методы выделения признаков радужки, основанные на различных видах вейвлет-преобразований, упомянутых ранее (вейвлеты Габора и т.д. [35, 104]), которые в течение многих лет доминировали в этой области, - это в основном попытки использовать низкоуровневое описание

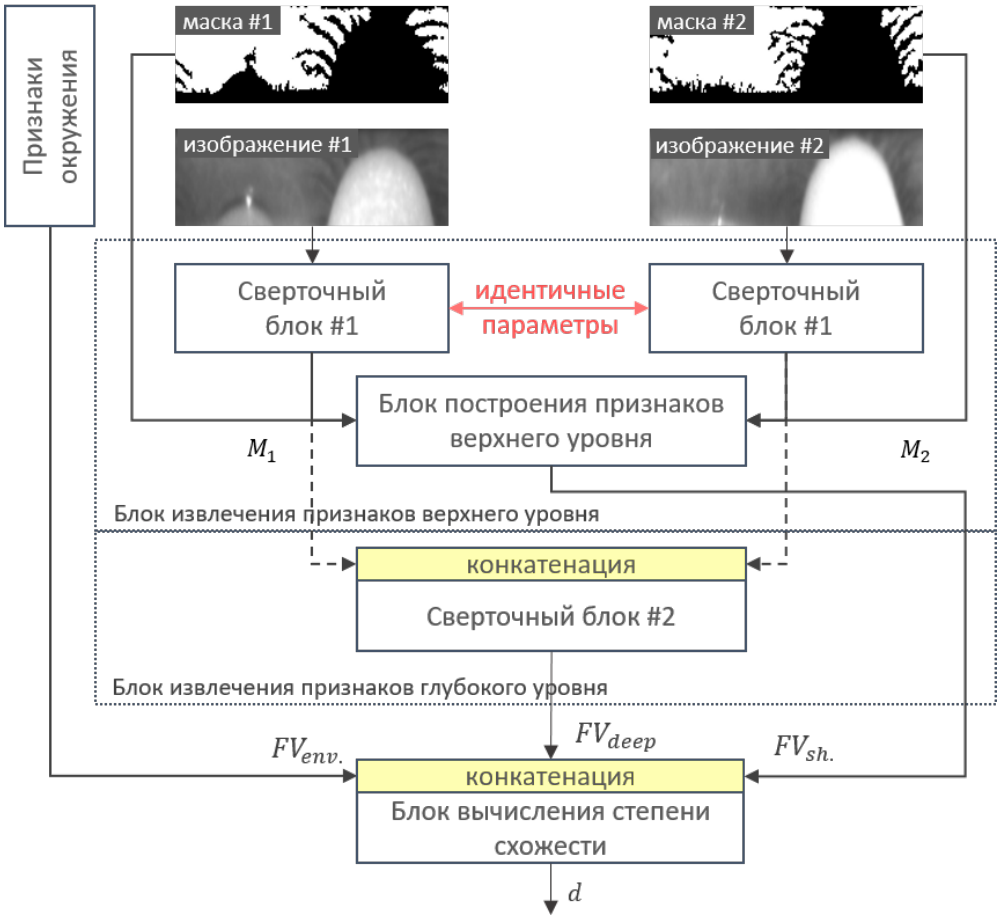


Рис. 4.8. Архитектура предложенной модели сверточной сети для извлечения и сравнения уникальных признаков радужки

текстуры. Эти методы доказали свою надежность для сценариев с практически неизменным окружением, но оказались чувствительными к ее изменениям.

Нормализованное изображение радужки представляет собой инвариант, позволяющий использовать текстурные признаки в условиях слабо изменяющейся среды, когда они остаются хорошо выровненными относительно между собой. Поэтому распознавание по радужке является хорошим примером задачи, для которой рентабельность использования низкоуровневых представлений объектов может быть исследована в контексте методов на основе CNN и сильно изменяющихся условий окружения.

В работе рассматривается влияние высокоуровневых текстурных признаков на эффективность распознавания. Взяв за основу классический подход [35]

Слой	Размер входного тензора
Сверточный 3x3 ($s' = 1, act. = tanh$)	$1 \times 49 \times 161$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 2)$	$8 \times 47 \times 159$

Таблица 4.4. Структура сверточного блока #1

к вычислению степени схожести при помощи расстояния Хэмминга (Hamming Distance, HD), вектор вида $FV_{sh} = \{x_0..x_N\}$ использовался в качестве описания высокоуровневых текстурных отличительных признаков. Каждый элемент x_i вектора FV_{sh} вычисляется следующим образом:

$$x_i = \frac{\sum |FM_{1,i}^{Sq} - FM_{2,i}^{Sq}| \times M_c}{\sum M_c} \tag{4.1}$$

где $FM_{k,i}^{Sq}$ это i-я карта признаков k-й радужки (входящей или сохраненной) после стандартизации приведением к $\mu = 0$ и $\sigma = 1$, бинаризованная по знаку; M_c - бинарная маска, используемая для выделения шума в виде ресниц, век и различных бликов, объединенная из двух: $M_c = M_1 \times M_2$.

Слой	Шаг свертки
Свертка по глубине ($k_h = k_w = 3$)	s'
Пакетная нормализация	–
ReLU	–
Свертка ($k_h = k_w = 1$)	1
Пакетная нормализация	–
ReLU	–

Таблица 4.5. Структура блока $CNNB_{MN}$

Основные элементы блока выделения высокоуровневых признаков и их взаимосвязи приведены на Рис. 4.8, а структура сверточного блока #1 представлена в Таб. 4.4. Структура основных блоков, впервые предложенная в ра-

боте [64] как вычислительно эффективная, была выбрана в качестве базового структурного элемента архитектуры (Таб. 4.5). Карты признаков $FM_{1,i}^{Sq}$ и $FM_{2,i}^{Sq}$ (4.1) являются выходом первого сверточного слоя с функцией активации $tanh()$ (Таб. 4.4).

Распределения элементов вектора FV_{sh} для genuine и impostor сравнений, полученные в процессе обучения по окончании различных эпох на валидационной выборке, представлены на Рис. 4.9. Несмотря на то, что распределения для разных фильтров для поздних эпох очень похожи, сами фильтры сильно различаются (Рис. 4.10). Форма распределений для обоих классов напоминает Гауссиан. По этой причине для оценки степени их разделимости были выбраны значения d' и EER. Изменение значений для каждого фильтра в процессе обучения представлено на Рис. 4.11. Результаты, представленные в Таб. 4.8, показывают, что добавление FV_{sh} позволяет получить несколько лучшие результаты по точности распознавания для базовой модели с ядрами 3x3 на первом сверточном слое. Также показано, что для больших ядер (9x9) разница в производительности становится более значимой (Таб. 4.8).

4.2.2. Высокоуровневое представление признаков

Представление высокоуровневых (глубоких) признаков выполняется сверточным блоком #2. Карты признаков $FM_{1,i}^{Sq}$ и $FM_{2,i}^{Sq}$, поступающие из сверточного блока #1, объединяются по каналам и поступают на вход блоку #2 (Рис. 4.8). Смысл конкатенации на данном этапе заключается в очередном использовании свойства инвариантности нормализованного изображения радужки. Эксперименты показали преимущества этого подхода по сравнению со стандартными методами [78], где векторы признаков имеют сильно пониженную размерность. Однако среди недостатков такого подхода: относительно большой размер вектора и вычислительная сложность процедуры сравнения. Структура блока представлена в Таб. 4.6. Выходной вектор $FV_{deep} \in R^{128}$ отражает высокоуровневое представление отличительных признаков и необходим для ра-

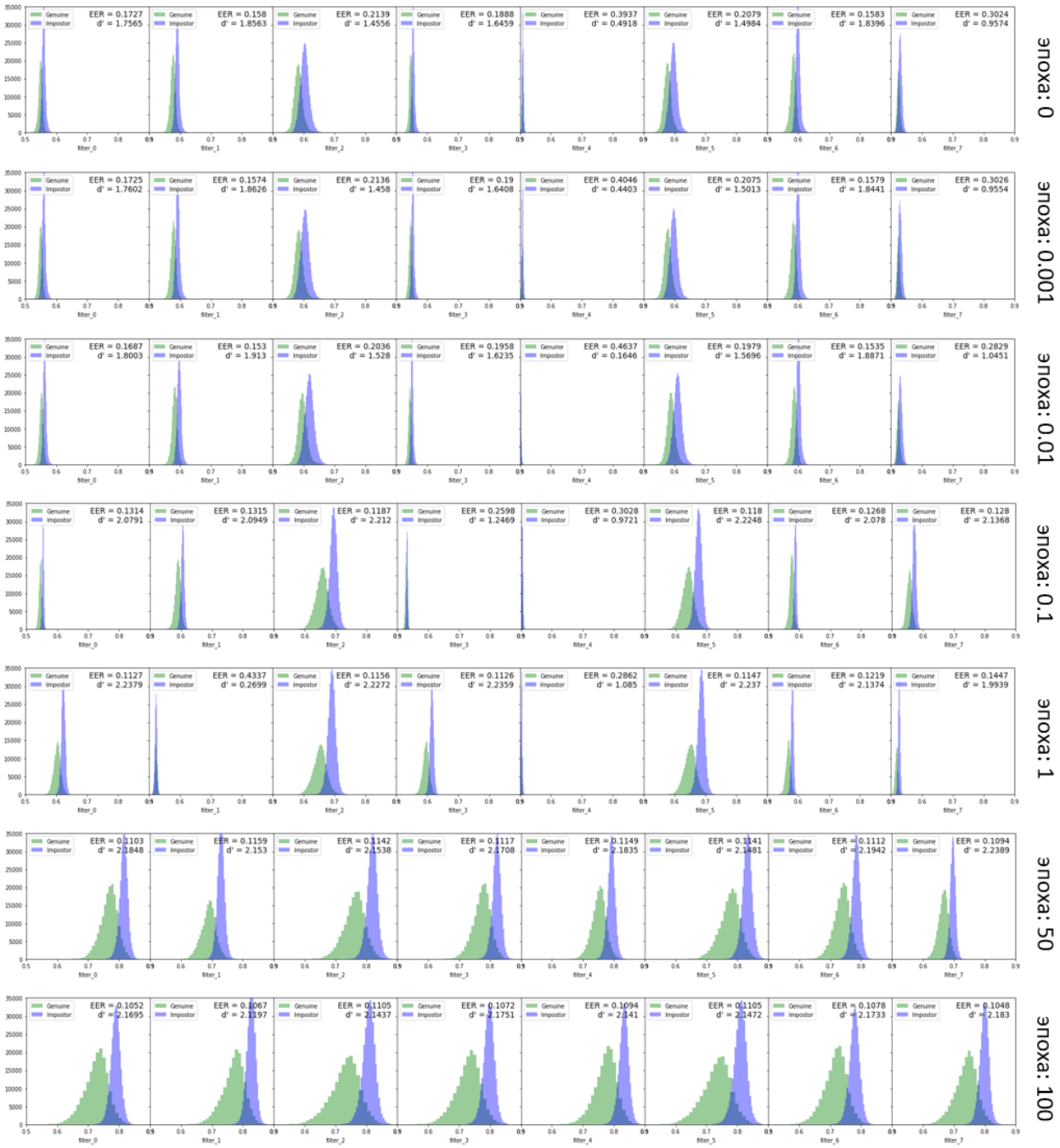


Рис. 4.9. Изменение распределений значений элементов вектора FV_{sh} в процессе обучения

боты со сложными нелинейными искажениями текстуры радужной оболочки, вызванными изменением условий окружения.

4.2.3. Вычисление степени схожести

Предварительный анализ ошибок распознавания показал, что genuine и impostor распределения хорошо разделяются. Однако, среди impostor сравне-

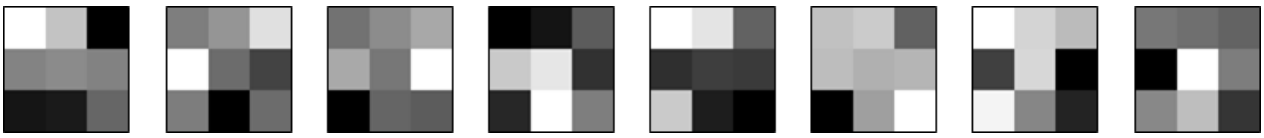
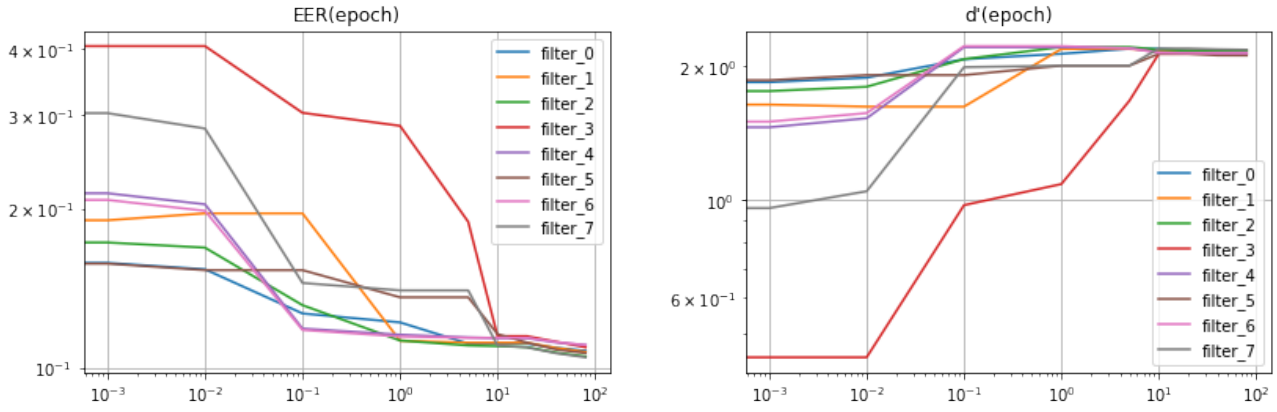


Рис. 4.10. Фильтры первого сверточного слоя, полученные после обучения (100 эпох)



(*а*) (*б*)

Рис. 4.11. Изменение значений EER (а) и d' (б) для распределений элементов вектора FV_{sh} в процессе обучения

ний существуют такие, для которых степень схожести принимает высокие значения, препятствуя фиксированию порога принятия решения на уровне, необходимом для создания устойчивой системы распознавания. Характер распределений элементов FV_{sh} (Рис. 4.9) наталкивает на идею использования методов вариационного вывода для регуляризации. Смысл метода заключается в представлении некоторого вектора в виде n-мерной случайной величины с заданным распределением. В данной работе предлагается представление векторов FV_{sh} и FV_{deep} в

Слой	**Размер входного тензора**
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 2)$	$32 \times 23 \times 79$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 2)$	$32 \times 11 \times 39$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 1)$	$32 \times 5 \times 19$
Полносвязный слой + Пакетная норм. (без акт.)	1×1632

Таблица 4.6. Структура сверточного блока #2

виде случайных величин соответствующей размерности, имеющих многомерное нормальное распределение $FV'_{sh} \sim N(\mu_{sh}, \Sigma_{sh})$ и $FV'_{deep} \sim N(\mu_{deep}, \Sigma_{deep})$ соответственно, где μ - вектор средних значений, а Σ - матрица ковариации. Вариационный вывод в нейронных сетях выполняется при помощи так называемого трюка с переопределением параметров (репараметризацией), описанного в [76]. Выбор (семплирование) значений из распределений выполняется случайным образом и только только в процессе обучения, тогда как для обученной модели выводятся только значения μ. В качества функции активации здесь предлагается использование сигмоида. Эта же процедура выполняется далее для векторов после конкатенации FV'_{sh}, FV'_{deep} и FV_{add}, где $FV_{add} = \{\Delta NPR, AOI\}$, где AOI - площадь пересечения (полезая площадь):

$$AOI = \frac{\Sigma M_c}{M_c^h \times M_c^w} \tag{4.2}$$

и ΔNPR вычисляется как:

$$\Delta NPR = \left| \frac{R_1^p}{R_1^i} - \frac{R_2^p}{R_2^i} \right| \tag{4.3}$$

где R^p и R^i соответствующие радиусы зрачка и радужки

Выходной вектор $FV'_d \in R^{128}$ является входом для последнего полносвязного слоя с двумя нейронами, представляющими два класса: свой и чужой (genuine и impostor). Для Вычисления степени схожести используется *SoftMax* классификатор.

Полученные результаты (Таб. 4.8) демонстрируют, что применение вариационного вывода (VI) повышает точность распознавания (VI=N означает замену структуры VI на простыми полносвязными слоями соответствующей размерности), но также стоит упомянуть, с увеличением объема данных для обучения, рентабельность применения такого подхода снижается.

4.2.4. Метод обучения

Еще одной особенностью предложенного метода является использование функции потерь (loss function) специального вида. Основная идея заключается в том, что некоторые изображения одной и той же радужки настолько отличаются друг от друга, что их практически невозможно отнести их к одному классу даже визуально по исходному (до нормализации) изображению. Данное свойства в значительной степени препятствует сходимости модели при обучении. Поэтому разумно взвешивать или даже полностью игнорировать такие сравнения при обучении. Предлагается следующий алгоритм:

- вычисление функции потерь (например, кросс-энтропии) для каждого сравнения в пакете;
- применение весов $weights = \{w_0..w_K\}$ для K-максимальных значений;
- суммирование значений и вывод значения для пакета;

Данный подход позволил обеспечить лучшую сходимость модели и добиться более высокой точности распознавания.

Экспериментальные результаты

Экспериментальные результаты были получены на нескольких наборах данных и сравнивались с наиболее релевантными методами среди существующих. Результаты включают оценку точности распознавания и скорости.

Экспериментальные данные

Для обучения и тестирования использовались три разных набора данных: CASIA-Iris-M1-S2 (CMS2) [27], CASIA-Iris-M1-S3 (CMS3) [27] и еще один (Iris-Mobile, IM), собранный в лаборатории при помощи мобильного устройства со встроенной камерой, работающей в БИК диапазоне. Последний собран, имитируя реальные сценарии аутентификации пользователя мобильного устройства: изображения, захваченные в сильно меняющемся освещении как в помещении,

Набор данных	**Изображений (всего)**	**Радужек (всего)**	**Изображений (на улице)**	**Субъекты**
CMS2	7723	398	0	Азиаты
CMS3	8167	720	0	Азиаты
IM	22966	750	4933	Европ. и Азиаты

Таблица 4.7. Описание базы данных тестирования

так и на открытом воздухе (под прямым солнечным светом), с очками и без очков. В нем также представлены изображения для людей различных расовых принадлежностей: азиатов и европеоидов. Более подробные спецификации наборов данных описаны в Таб. 4.7, а несколько примеров изображений области глаза представлены на Рис. 3.1. Выделение области радужки с целью получения масок было осуществлено автоматически алгоритмом, описанным в гл. 3. Примеры изображений радужек и соответствующих масок представлены на Рис. 4.8. Каждый набор данных первоначально был разделен на подвыборки: обучающую, валидационную и тестовую в пропорции 70/10/20 (%) соответственно. Разделение производилось таким образом, что для разных подвыборок не существует изображений одной и той же радужки.

Обучение

Обучение и тестирование проводились отдельно для каждого набора данных. Поскольку количество genuine сравнений N_G намного меньше, все они были использованы для обучения, а количество сравнений impostor было установлено в $N_I = 10N_G$. Модель, продемонстрировавшая лучшие результаты на валидационной выборке, выбиралась для оценки на тестовой. Все модели обучались на протяжении 150 эпох, а в качестве метода оптимизации был выбран Adam [77].

Обучение предлагаемой модели проводилось таким образом, чтобы одна эпоха была эквивалентна одному проходу по всем genuine сравнениям, тогда

$conv1 \mid VI \mid FV_{sh}$	**EER**	**FNMR**	**d'**
$8 \times 3 \times 3 \mid Y \mid Y$	0.0116	0.1925	4.3155
$8 \times 3 \times 3 \mid N \mid Y$	0.0120	0.2027	4.2048
$8 \times 3 \times 3 \mid Y \mid N$	0.0125	0.2085	4.1253
$8 \times 9 \times 9 \mid Y \mid Y$	0.0134	0.1566	4.3034
$8 \times 9 \times 9 \mid Y \mid N$	0.0172	0.1694	3.9850

Таблица 4.8. Оценка точности распознавания для различных модификаций модели

как impostor сравнения каждый раз случайным образом выбирались из всего набора для каждого пакета. Также была установлена пропорция для количества genuine и impostor сравнений в пакете $N_I^b = 10N_G^b$.

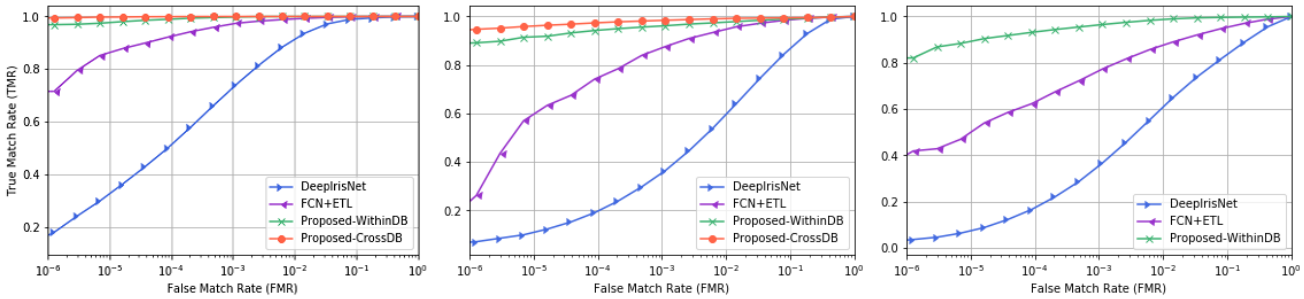
Результаты по точности распознавания

Полученные результаты по точности распознавания представлены в Таб. 4.9 и Рис. 4.12. Предложенный метод превосходит остальные на всех наборах данных. После разделения полных наборов на подмножества стало невозможно оценить FNMR для FMR=10^{-7} для наборов данных CMS2 и CMS3, поскольку количество сравнений в тестовых подмножествах не превышало 10 миллионов. По этой причине был проведен еще дополнительный эксперимент. Его суть заключалась в том, чтобы оценить эффективность предлагаемой модели на наборах данных без какого-либо обучения или дообучения на них (с переносом). Модель, прошедшая обучение на обучающей выборке IM, была протестирована на полных наборах данных (до разделения) CMS2 и CMS3, чтобы получить FNMR при FMR=10^{-7}. Модель показала результаты, превосходящей её собственные, полученные после обучения на обучающих подмножествах данных каждого из наборов, и это доказало её высокую способность к обобщению. Тем не менее, было бы справедливо отметить, что набор данных IM содержит гораздо больше изображений, чем два других.

Результаты по скорости обработки

Метод	CMS2	CMS3	IM	Testing
DeepIrisNet	0.0709	0.1199	0.1371	без переноса
FCN+ETL	0.0093	0.0301	0.0607	без переноса
Предложенный	0.0014	0.0190	0.0116	без переноса
метод	0.0003	0.0086	0.0116	с переносом

Таблица 4.9. Значения EER, полученные для сравниваемых методов на различных базах данных



(*а*) (*б*) (*в*)

Рис. 4.12. ROC-кривые построенные по результатам тестирования сравниваемых методов на базах данных: (а)CMS2, (б)CMS3, (в)IM

Тестирование предложенного метода производилось на мобильном устройстве. Полное медианное время выполнения измерено на процессоре Qualcomm Snapdragon 835 CPU (2.45 GHz) и составило 3-4 миллисекунды: 1-2 (мсек) для извлечения особенностей и столько же для из сравнения. Измерения производились на одном ядре процессора.

4.3. Выводы к четвертой главе

Рассмотрены особенности извлечения и сравнения уникальных особенностей радужки при распознавании в сложных условиях, с учетом специфики применения в мобильном устройстве. Рассмотрены два основных направления к задаче: использование вейвлетов и их всевозможных модификаций, а так-

же методов глубокого обучения. Предложены, протестированы и внедрены два разных метода: (i) основанный на применений вейвлетов Габора с последующим адаптивным квантованием фазы, позволивший достичь большей устойчивости к искажениям текстуры радужки по сравнению с существующими методами; (ii) основанный на применении глубокого обучения с учетом специфики вариативности радужки. Исследована рентабельность использования низкоуровневых текстурных особенностей радужки в объединении с высокоуровневым представлением. В рамках подхода, основанного на применении сверточной нейронной сети предложен новый метод обучения, позволивший обеспечить лучшую сходимость модели и повысить точность распознавания. Для тестирования метода была собрана и подготовлена дополнительная база данных изображений радужек, учитывающая особенности использования мобильного устройства. Оба предложенных метода позволяют обеспечивать высокую скорость распознавания, достаточную для их применения в мобильном устройстве в режиме реального времени.

Глава 5

Защита от подделывания радужки

Способность обеспечивать надежную защиту от попыток подделывания является одним из ключевых требований к системе безопасности, использующей биометрические методы. Распознавание по радужной оболочке глаза является одной из наиболее перспективных и новых биометрических технологий на рынке мобильных устройств (1.2, 1.5). О преимуществах технологии по сравнению с иными биометрическими методами упоминалось ранее (1.1). За последние годы несколько компаний представили технологию аутентификации по радужке, встроенную в свои смартфоны, среди наиболее известных: [39, 93, 123]. Предполагается, методы биометрической аутентификации станут заменой для привычных схем с паролями. В целом технология предназначена для более удобного взаимодействия с устройством и, в то же время, для повышения уровня безопасности личной информации пользователя, хранящейся на устройстве.

После выпуска устройств, оснащенных сканером радужки, стали подтверждаться факты взлома технологии путем подделывания (спуфинга, spoofing) радужной оболочки глаза и представлении её устройству в качестве оригинальной, принадлежащей пользователю. Следует отметить, что попытки взлома предпринимались группами профессионалов, специализирующимися на взломе и компрометировании технологий безопасности, в т.ч. и биометрических [20, 25]. Эксперименты проведенные в рамках данного настоящего исследования подтверждают, что идеи обоих упомянутых методов спуфинга являются выполнимыми, за исключением нескольких важных условий, которые должны быть выполнены: изображение радужной оболочки должно быть захвачено инфракрасной камерой с высоким разрешением таким образом, что диаметр радужки на изображении должен составлять не менее 250-300 точек на бумаге, напечатанной с разрешением не менее 600 dpi, что означает, что изображение должно

быть зафиксировано либо с очень короткого расстояния, либо с использованием телеобъектива с высоким разрешением; глаза должны быть открыты достаточно с прицелом, направленным к камере; изображение радужной оболочки не должно быть размытым и недооцененным; Таким образом, можно сделать вывод, что проблема анти-спуфинга радужки остается актуальной, в особенности для мобильных приложений.

5.1. Обзор методов защиты от подделывания радужки

Среди известных способов спуфинга радужки можно выделить следующие [32, 42, 49]: представление системе напечатанной на принтере с высоким разрешением изображении радужки пользователя; представление изображения либо последовательности изображений радужки с экрана другого устройства; представление системе искусственного глаза, изготовленного из стекла или пластика; представление контактной линзы с рисунком оригинальной радужки пользователя; иные возможные варианты, позволяющие обеспечить реалистичность радужки для биометрической системы.

Существующие методы борьбы с подделыванием радужки, описанные в литературе, могут быть поделены на:

- Использующие и не использующие дополнительные аппаратные средства, позволяющие обнаруживать особые физиологические свойства «живности» радужки, например глазного гиппуса, представляющего собой естественное колебание диаметра зрачка в ответ на внезапное изменение освещения (например, включение дополнительного диода) [32, 49];
- Требующие и не требующие дополнительного взаимодействия с пользователем, например посредством вывода подсказок с просьбой закрыть/открыть веки, предоставить иную дополнительную информацию в виде пин-кода и др.

Класс методов, использующих дополнительные аппаратные средства, а также требующие дополнительного взаимодействия с пользователем, рассматривается в меньшей степени, когда речь заходит о их применении на мобильном устройстве, главным образом потому, что такой подход может значительно увеличить стоимость и, в то же время, уменьшить удобство использования технологии [106]. Полностью автоматические подходы выделяются экономичностью, что делает их привлекательными для коммерческого применения, однако, требуют высокой степени универсальности и устойчивости к изменениям выходных данных.

Одной из первых работ в данной области была [36], в которой рассматривалась проблема спуфинга при помощи напечатанных на бумаге изображения радужки. В работе утверждалось, что процесс печати оставляет обнаруживаемые следы на поддельных образцах и предлагалось их обнаружение применением двумерного анализа Фурье полученного изображения. Подход показал свою эффективность против атак с использованием изображений радужки, напечатанных на бумаге. Однако, метод оказался неустойчивым к иным видам атак, описанными далее. Несколько методов анализа признаков, присущих искусственным радужкам в частотной области, были предложены в работах [61] и [31]. В работе [120] предлагается метод представления изображения радужки в виде пирамиды Лапласа для различных масштабов. Метод позволяет анализировать частотные отклики для разных ориентаций радужки и обнаруживать артефакты, присущие искусственным образцам, с использованием последовательности изображений. Методы, основанные на локальных дескрипторах, также используются для анализа и представления текстуры радужки с целью обнаружения спуфинг-атак. Например, в работах [57, 61] показана эффективность использования различных конфигураций LBP (local binary patterns, локальных бинарных шаблонов) дескрипторов против ряда известных атак (например, контактные линзы с рисунком радужки, напечатанные на бумаге, искусственные радужки из пластика или стекла т. д.). Бинарные особенности изображения,

основанные на статистиках (BSIF) также изучались в контексте обнаружения подделок и тестировались на разных базах данных подделок [118]. Комплексное решение для защиты от спуфинга на основе комбинации нескольких локальных дескрипторов (LBP, BSIF и локального квантования фазы (LPQ)) для представления текстуры представлено в комплексном исследовании [54].

В работе [49] было показано, что различные метрики качества изображения радужки могут быть использованы для обнаружение спуфинг-атак. Идея подхода исходит из предположения о том, что входные изображения подделок могут значительно отличаться по уровню качества от оригинальных для нормальных (фиксированных) условий распознавания. Несколько значимых в отношении детектирования подделок метрик качества представлены в работе [49] и протестированы на образцах подделок, напечатанных на бумаге.

Одним из наиболее многообещающих подходов к детектированию спуфинг-атак сегодня является применение методов глубокого обучения. Такие методы демонстрируют высокую надежность по сравнению с существующими. Одной из пионерских работ в применении к радужке, лицу и отпечаткам пальцев была [92]. Комплексная работа по сравнении различных подходах регулярно организовывается в рамках LivDet соревнований, где методы глубокого обучения по результатам последних лет занимают лидирующие позиции [143—145].

Все вышеупомянутые подходы к обнаружению спуфинг-атак были рассмотрены в контексте мобильных приложений, накладывающих на них дополнительные ограничения, о которых говорилось ранее (2.1, 1.5). Среди всех, для сравнения были выбраны [118, 125, 126], которые отвечали требованиям мобильных приложений, демонстрирующие при этом перспективные результаты.

5.2. Обнаружение подделок радужки методами глубокого обучения

Предложен универсальный метод обнаружения спуфинг-атак разных категорий. Метод основан на использовании моделей глубоких сверточных нейронных сетей (CNN). Входными данными метода являются два изображения: изображение радужки I_{ER}, центр которого совпадает с центром радужки, и изображение нормализованной радужки I_{NI}, получаемое преобразованием вида 1.1, 1.2. Примеры обоих изображений приведены на Рис. 5.1. Метод опирается на информацию о положении и размерах зрачка и радужки, которые, в простейшем случае, могут быть описаны параметрически окружностями.

Проверка на наличие потенциальной спуф-атаки производится сразу после этапа нормализации радужки (описан в разделе 1.4) и состоит из двух этапов: масштабирование изображения и пропускания его через сверточную нейронную сеть (Рис. 5.1). Изображение области радужки $I_{ER}(M_{ER}, N_{ER})$ вырезается с пропорцией $M_{ER} = N_{ER} = 3R_i$, где R_i - радиус радужки. Центр изображения I_{ER} совмещен с центром радужки, описываемой окружностью.

Далее обе изображения масштабируются до заранее заданного размера в пикселях (Рис. 5.1). Размер изображения выбирается заранее как оптимальный для заданной архитектуры и позволяющий обеспечивать достаточную точность и скорость обработки для полученной модели.

Архитектура сверточной сети

Предложенный метод основан на использовании основных блоков архитектуры MobileNet [64], показавшей свою эффективность и применимость для задач, связанных с мобильными приложениями. Одно из основных преимуществ архитектуры это конструкция её основных сверточных блоков. Пары слоев сверток по глубине (depth-wise convolutions) с последующими свертками с ядрами 1x1 позволяют существенно снизить количество умножений, сохраняя емкостные характеристики модели [64].

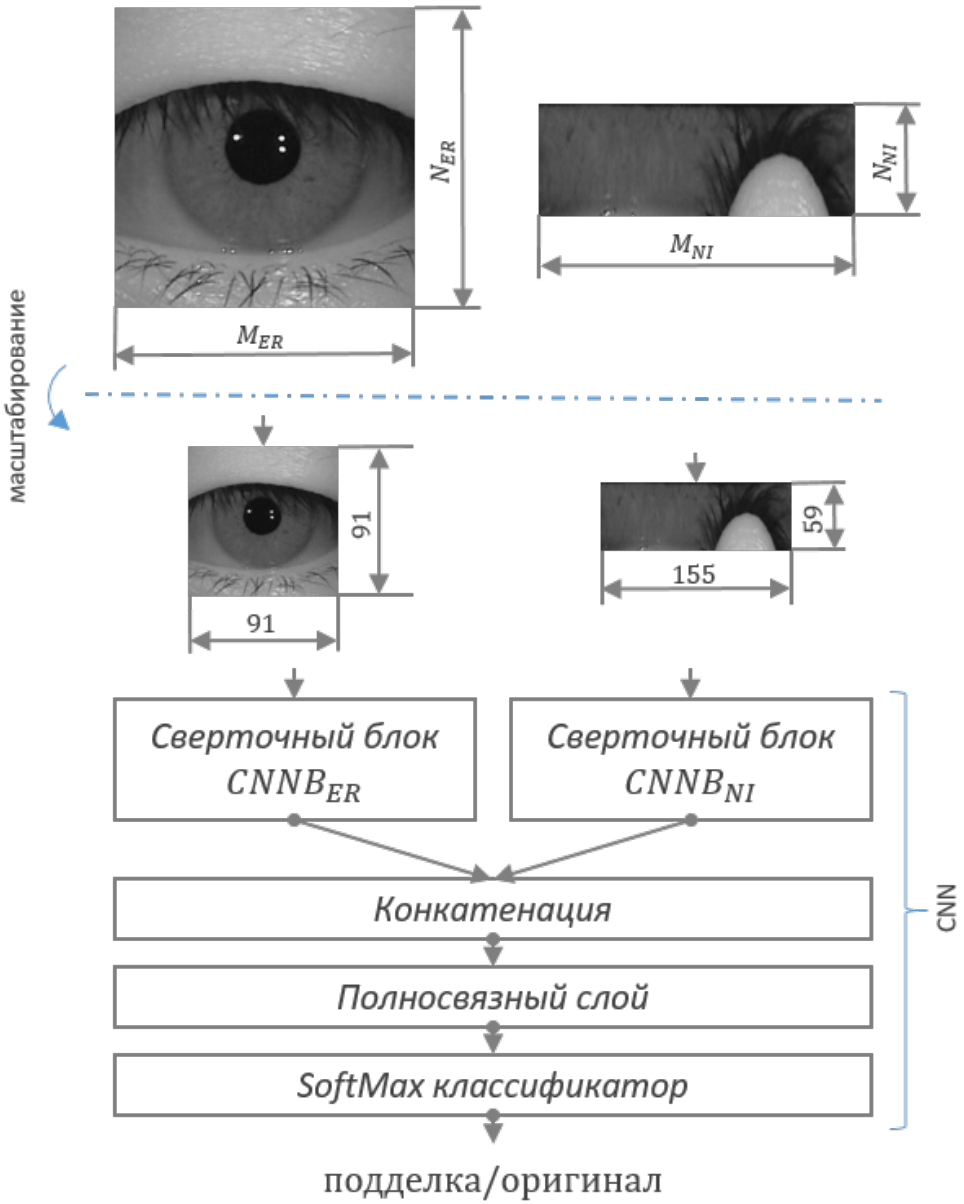


Рис. 5.1. Общая схема алгоритма защиты от подделывания радужки

Пары изображений I_{ER} и I_{NI}, полученные из одного исходного изображения подаются на вход сверточным блокам $CNNB_{ER}$ и $CNNB_{NI}$ соответственно, как показано на Рис. 5.1. Структура обоих блоков отражена в Таб. 5.1. Блоки имеют схожую структуру, основными элементами которой являются структурные единицы архитектуры MobileNet [64], обозначенные как $CNNB_{MN}$. Структура блоков $CNNB_{MN}$ описана в Таб. 4.5.

Над картами признаков, полученных для изображений I_{ER} и I_{NI} на выходе из соответствующих блоков, производится операция глобального усредняющего

Элемент архитектуры блока	**Размер входного тензора**	
	$CNNB_{ER}$	$CNNB_{NI}$
Сверточный слой ($k_h = k_w = 3, s' = 2$)	$1 \times 91 \times 91$	$1 \times 59 \times 123$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 1)$	$8 \times 45 \times 45$	$8 \times 29 \times 61$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 2)$	$16 \times 43 \times 43$	$16 \times 27 \times 59$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 1)$	$32 \times 21 \times 21$	$32 \times 13 \times 29$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 2)$	$64 \times 19 \times 19$	$64 \times 11 \times 29$
Сверточный блок $CNNB_{MN}(k_h = k_w = 3, s' = 1)$	$64 \times 9 \times 9$	$64 \times 5 \times 13$
Глобальный усредняющий пуллинг	$64 \times 7 \times 7$	$64 \times 3 \times 11$

Таблица 5.1. Структура блоков $CNNB_{ER}$ и $CNNB_{NI}$: k_h, k_w - размеры ядра свертки по вертикали и горизонтали соответственно

пулинга (global average pooling). Затем они объединяются в один вектор, являющийся входом последнего полносвязного (fully-connected) слоя. Классификатор softmax используется для оценивания вероятностей P_{spoof} and P_{live} принадлежности текущего изображения к одному из двух классов: живой или подделка.

Предложенная модификация архитектуры имеет намного меньшее количество параметров по сравнению с оригинальной [64], а также использует отступы (paddings) типа «valid», что позволяет уменьшить количество операций при прямом проходе (forward pass).

Описание базы данных подделок

На сегодняшний день доступно несколько баз данных, содержащих изображения оригинальных (живых) радужек и подделок. По аналогии с наборами данных, собранными для оценки эффективности распознавания радужки, их можно разделить на две группы: полученные в видимом и ближнем инфракрасном (БИК) спектрах. Поскольку системы, использующие БИК изображения, более распространены в виду ряда преимуществ, упомянутых ранее (1.4, 2.2), в работе рассмотрены только изображения, полученные в БИК диапазоне. В смеж-

ных работах также рассмотрено несколько распространенных типов подделок, среди которых: радужка, напечатанная на бумаге; живая радужка, покрытая текстурированными (узорчатыми) контактными линзами; живая радужка, покрытая полу-прозрачной контактной линзой, с воспроизведенным на ней рисунком радужки какого-либо человека. Случай с воспроизведением рисунка радужки пользователя устройства кажется слишком сложным в реализации, поэтому не рассматривается в данной работе. Сценарий атаки с радужкой, напечатанной на бумаге, более прост и интуитивен. В некторых из самых недавних работ в области сообщается, что такую проблему удалось решить, однако, ни в одной из них не рассматривается использование технологии в мобильном устройстве.

На сегодняшний день не существует доступных наборов данных, полученных при помощи мобильного устройства в БИК диапазоне. По этой причине такой набор данных был предварительно собран. Набор включает в себя следующие типа атак, часть из которых не была рассмотрена ранее: (i) изображение радужки, напечатанное на бумаге (PR); (ii) изображение радужки, напечатанное на бумаге с наложением прозрачных контактных линз (PWL); (iii) изображение радужки, напечатанное на бумаге с нанесением прозрачного клея (PWG). Такие типы образцов подделок были выбраны не случайно. Именно они были успешно использованы для обхода мобильной биометрической системы [20, 25]. Изображения радужной оболочки были получены с использованием NIR-камеры высокого разрешения в диапазоне расстояний от 20 до 40 (см) и далее напечатаны на белой бумаге с разрешениями 600/1200 (dpi) в равной пропорции. Полученные образцы были использованы для съемки примеров трех классов подделок. В качестве примеров живых радужек были выбраны две категории: (i) изображение радужки, полученно при нормальном освещении внутри хорошо освещенной комнаты (IN); (ii) изображение радужки, полученные в солнечную погоду вне помещения (OUT). Данные категории были выбраны из соображений рассмотрения возможности изменения условий окружения, присущих мобильным приложениям.

Таблица 5.2. Описание собранно базы данных (живой/подделка) радужек

Параметр	**Значение**
Разрешение изображения	320×240
Кол-во субъектов/глаз	23/46
Кол-во изображений подделка/живой	18548/18031
IN/OUT/PR/PWL/PWG (весь набор)	10679/7869/6233/5907/5891
IN/OUT/PR/PWL/PWG (тестовый набор)	2534/2006/1436/1452/1568

В качестве устройства для регистрации изображения было выбрано портативное вычислительное устройство Raspberry Pi с камерой (PiCamera v2.1) с дополнительно установленным полосно-пропускающим (850±20 нм) БИК фильтром, позволяющей получать изображения в БИК диапазоне частот. В качестве дополнительного источника освещения был использован светодиод с пиковой частотой излучения 850 нм. детальная информация о собранном наборе данных представлена в Таб. 5.2. Разбиение данных на обучающую и тестовую выборку производилось таким образом, чтобы наборы не пересекались по субъектам. Несколько примеров изображений I_{ER} из набора представлены на Рис. 5.2.

Экспермиентальные результаты

Для того чтобы оценить эффективность предлагаемого решения, были реализованы несколько известных литературы методов. Производительность методов оценивалась на собранном, упомянутом выше наборе данных. Среди известных подходов: методы, в основе которых лежит частотный анализ, предложенные в работах [31] и [61]; метод, построенный на LBP [57] и BSIF дескрипторах [118], а также метод, предложенный в работе [126] с использованием численных показателей качества изображения. Вышеупомянутые методы были выбраны как демонстрирующие наивысшую производительность на наборах данных изображений, полученных в БИК диапазоне согласно обзору, приведенному в

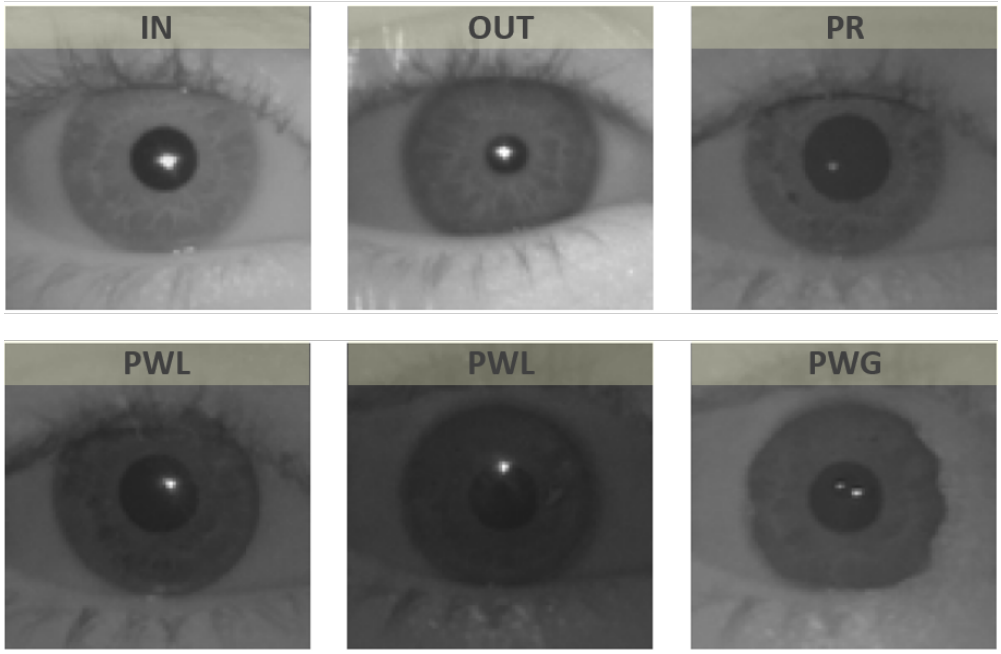


Рис. 5.2. Примеры изображений

работе [50]. По причине высокой вычислительной сложности метод, основанный на применении пары CNN в сочетании с набором решающих правил, предложенных исследователями из CASIA в работе [145], был исключен из рассмотрения как неприменимый для мобильных приложений, работающих в режиме реального времени. Время выполнения для метода в 400 раз превышает время для метода, предложенного в данной работе.

Для оценивания точности распознавания были выбраны следующие показатели: *FerrLive* - доля изображений живых образцов, ошибочно классифицированных как подделки; *FerrFake* - доля изображений подделок, ошибочно классифицированных как живые; *CCR (correct classification rate)* - доля правильно классифицированных изображений на всем наборе данных. В Таб. 5.3 приведены результаты тестирования известных из литературы и предложенного методов. Важно отметить, что только два из упомянутых решений ([118] и [126]) были изначально представлены как способные обеспечивать возможность использования в мобильном устройстве. К преимуществам метода [126] можно отвести простоту и относительное быстродействие алгоритма. Метод, предложенный в работе [118] включает в себя вычислительно сложные опе-

Таблица 5.3. Результаты по точности классификации живых радужек и подделок

Method	**FerrLive**	**FerrFake**	**CCR**
Czajka [31]	0.505	0.207	0.661
He [61]	0.370	0.739	0.442
Gupta [57]	0.294	0.251	0.749
Raghavendra [118]	0.076	0.128	0.897
Sequeira [126]	0.320	0.293	0.694
Предложенный метод	**0.048**	**0.034**	**0.959**

рации свертки с фильтрами относительно большой размерности: от 7×7 до 17×17, что делает его менее предпочтительным для развертывания на мобильном устройстве.

Тестирование предложенного метода производилось на мобильном устройстве. Полное медианное время выполнения измерено на процессоре Qualcomm Snapdragon 835 CPU (2.45 GHz) и составило 4-6 миллисекунд. Измерения производились на одном ядре процессора.

5.3. Выводы к пятой главе

Рассмотрены особенности защиты от подделывания радужек в применении к распознаванию с мобильного устройства. Воспроизведены попытки взлома при помощи методов, использованных группами профессиональных взломщиков. Произведена классификация общих подходов к защите от подделывания. Произведен обзор существующих методов, рассмотрены их преимущества и недостатки. Рассмотрены новые виды подделок, ранее не исследовавшиеся в литературе: (i) изображение радужки, напечатанное на бумаге с наложением прозрачных контактных линз; (ii) изображение радужки, напечатанное на бумаге с нанесением прозрачного клея. Собрана и обработана база данных изоб-

ражений в том числе новых видом подделок при помощи мобильного устройства с учетом возможных изменений окружения. Разработан, протестирован и внедрен новый метод защиты от спуфинг-атак, основанный на применении методов глубокого обучения, в частности, сверточных нейронный сетей. Предложенный метод продемонстрировал высокую точность обнаружения подделок, значительно превосходящую известные из литературы решения, а также скорость обработки, достаточную для запуска на мобильном устройстве в режиме реального времени.

Заключение

1. Исследованы особенности применения метода биометрического распознавания по радужной оболочке глаза в приложениях мобильных устройств. Исследованы причины и зависимости изменения радужки и пригодности её для распознавания в сложных, постоянно изменяющихся условиях окружения, а так же с учетом особенностей поведения пользователя устройства, присущих мобильным приложениям, работающих с изображениями объектов. Разработан, предложен и внедрен метод распознавания, пригодный для применения в мобильных устройствах.

2. Исследованы методы и алгоритмы оценки качества изображения радужки. Разработан и внедрен метод оценки качества для мобильных приложений, позволяющий комплексно оценивать пригодность изображения для извлечения признков, обеспечивать обратную связь с пользователем устройства, производить управление параметрами системы регистрации изображения, учитывать и использовать данные с иных сенсоров устройства, позволяющих извлекать дополнительную информацию об окружении.

3. Разработаны, исследованы и внедрены методы выделения области радужки на изображении низкого качества с использованием методов глубокого обучения, позволяющие производить устойчивое выделение области радужки на изображении низкого качества в сложных условиях окружения с частотой поступления кадров.

4. Исследованы, разработаны и внедрены методы извлечения уникальных особенностей радужки из изображения плохого качества и их последующего сравнения. Один из предложенных методов превосходит по точности существующие аналоги, в особенности, в экстремально сложных условиях. Предложенные методы обеспечивают скорость распознавания, достаточ-

ную для их применения в мобильных приложениях в режиме реального времени.

5. Исследованы особенности защиты от подделывания радужек в применении к распознаванию с мобильного устройства, а так же новые методы подделывания. Разработан, протестирован и внедрен новый метод защиты от подделывания, основанный на применении сверточных нейронный сетей. Предложенный метод продемонстрировал высокую точность и скорость обнаружения подделок, значительно превосходящую известные из литературы решения.

6. Собраны, обработаны и размечены следущие базы данных: наборы изображений радужки низкого качества, полученных при помощи мобильного устройства в условиях, симулирующих реальные сценарии его использования, содержащих максимум один (более 157000) и два (более 200000) глаза, набор данных изображений в том числе новых видов подделок радужной оболочки глаза (более 150000).

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

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

Список литературы

1. *Архангельский В.* Морфологические основы офтальмологической диагностики. — Медгиз, 1960.
2. *Гнатюк В.* [и др.]. Способ автоматической регулировки экспозиции для инфракрасной камеры и использующее этот способ вычислительное устройство пользователя: номер патента RU2667790C13. — 2018.
3. *Краснов М.* Элементы анатомии в клинической практике офтальмолога. — Государственное издательство медицинской литературы, 1952.
4. *Матвеев И.* Методы и алгоритмы автоматической обработки изображений радужной оболочки глаза. — 2014.
5. *Одиноких Г.* Способ, Система и Устройство для Биометрического Распознавания Радужной Оболочки Глаза: номер патента RU2630742. — 2017.
6. Применение биометрии. — Accessed: 2018-09-15. http://biometric.bmstu.ru/category/primenenie_biometrii.
7. *Abate A.* [et al.]. Two-Tier Image Features Clustering for Iris Recognition on Mobile // Lecture Notes in Computer Science. — 2017. — Vol. 10147. — P. 260–269.
8. *Adam M.* [et al.]. Eyelid Localization for Iris Identification // Radioengineering. — 2008. — Vol. 17, no. 4. — P. 82–85.
9. *Aligholizadeh M. J.* [et al.]. An Effective Method for Eyelashes Segmentation Using Wavelet Transform // Proc. of International Conference on Biometrics and Kansei Engineering. — 2011. — P. 185–188.
10. *Alonso-Fernandez F.* [et al.]. Iris Pupil Detection by Structure Tensor Analysis // Proc. Swedish Symposium on Image Analysis. — 2011.
11. *Alonso-Fernandez F.* [et al.]. Iris Segmentation Using the Generalized Structure Tensor // Proc. SSBA Symposium. — 2012.

12. ARM Security Technology. Building a Secure System using TrustZone Technology. — 2009. — URL: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf.

13. *Arsalan M.* [et al.]. Deep Learning-Based Iris Segmentation for Iris Recognition in Visible Light Environment // Symmetry. — 2017. — Vol. 9. — P. 263.

14. *Badrinarayanan V.* [et al.]. SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 2017. — Vol. 39. — P. 2481–2495.

15. *Bakhtiari A.* [et al.]. An Efficient Segmentation Method Based on Local Entropy Characteristics of Iris Biometrics // International Journal of Biological and Life Sciences. — 2006. — Vol. 2, no. 3. — P. 195–199.

16. *Barra S.* [et al.]. Ubiquitous Iris Recognition by Means of Mobile Devices // Pattern Recognition Lettes. — New York, NY, USA, 2015. — Vol. 57, no. C. — P. 66–73. — URL: http://dx.doi.org/10.1016/j.patrec.2014.10.011.

17. *Barzegar N.* [et al.]. A New Approach for Iris Localization in Iris Recognition Systems // Proc. IEEE/ACS Int. Conf. Computer Systems and Applications. — 2008. — P. 516–523.

18. *Basit A.* [et al.]. Localization of iris in gray scale image using intensity gradient // Optics and Lasers in Engineering. — 2007. — Vol. 45. — P. 1107–1114.

19. *Bazrafkan S.* [et al.]. An end to end Deep Neural Network for iris segmentation in unconstrained scenarios // Neural Networks. — 2018. — Vol. 106. — P. 79–95. — URL: https://doi.org/10.1016/j.neunet.2018.06.011.

20. Bkav Corporation: Galaxy S8 Iris Scanner bypassed by glue. — 2017. — URL: http://www.bkav.com/top-news/-/view_content/content/94273/galaxy-s8-iris-scanner-bypassed-by-gl-1.

21. *Boles W.* [et al.]. A human identification technique using images of the iris and wavelet transform // IEEE Trans. Signal Process. — 1998. — Vol. 46, no. 4. — P. 1185–1188.

22. *Bowyer K.* [et al.]. Image Understanding for Iris Biometrics: A Survey // Comput. Vis. Image Underst. — New York, NY, USA, 2008. — Vol. 110, no. 2. — P. 281–307. — URL: http://dx.doi.org/10.1016/j.cviu.2007.08.005.

23. *Bowyer K.* [et al.]. A Survey of Iris Biometrics Research: 2008-2010, in Handbook of Iris Recognition. — Springer, 2012.

24. *Boyd M.* [et al.]. MSc Computing Science Group Project Iris Recognition : Master's thesis / Boyd M. — Imperial College, London, 2010.

25. Chaos Computer Club (CCC): Chaos Computer Club breaks iris recognition system of the Samsung Galaxy S8. — 2017. — URL: https://www.ccc.de/en/updates/2017/iriden.

26. *Chen R.* [et al.]. Liveness detection for iris recognition using multispectral images // Pattern Recognition Letters. — 2012. — Vol. 33, issue 12. — P. 1513–1519.

27. Chinese Academy of Sciences Institute of Automation (CASIA), CASIA-Iris-Mobile-V1.0. — 2015. — URL: http://biometrics.idealtest.org/.

28. Chinese Academy of Sciences Institute of Automation. Iris image database, ver. 3. — 2005. — URL: http://www.cbsr.ia.ac.cn/IrisDatabase.htm.

29. Chinese Academy of Sciences Institute of Automation. Iris Lamp database, ver. 3. — 2018. — URL: http://biometrics.idealtest.org/dbDetailForUser.do?id=4.

30. *Corcoran P.* [et al.]. Feasibility and design considerations for an iris acquisition system for smartphones // Proc. of IEEE 4th International Conference on Consumer Electronics Berlin (ICCE-Berlin). — 2014. — P. 164–167.

31. *Czajka A.* Database of iris printouts and its application: Development of liveness detection method for iris recognition // Proc. of 18th International Conference on Methods Models in Automation Robotics (MMAR'13). — 2013. — P. 28–33.

32. *Czajka A.* [et al.]. Presentation Attack Detection for Iris Recognition: An Assessment of the State-of-the-Art // ACM Comput. Surv. — New York, NY, USA, 2018. — Vol. 51, no. 4. — 86:1–86:35. — URL: http://doi.acm.org/10.1145/3232849.

33. *Daugman J.* High confidence personal identification by rapid video analysis of iris texture // Proc. IEEE Internat. Carnahan conf. on security technology. — 1992. — P. 50–60.

34. *Daugman J.* High confidence visual recognition of persons by a test of statistical independence // Proc. IEEE TPAMI. Vol. 15. — 1993. — P. 1148–1161.

35. *Daugman J.* How iris recognition works // IEEE Transactions on Circuits and Systems for Video Technology. — 2004. — Vol. 14, no. 1. — P. 21–30.

36. *Daugman J.* Iris recognition and anti-spoofing countermeasures // Proc. of 7-th International Biometrics conference. — 2004.

37. *Daugman J.* Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons // Proceedings of the IEEE. Vol. 94. — 2006. — P. 1927–1935.

38. *Daugman J.* [et al.]. Epigenetic randomness, complexity and singularity of human iris patterns // Proceedings of the Royal Society of London B: Biological Sciences. — 2001. — Vol. 268, no. 1477. — P. 1737–1740. — eprint: http://rspb.royalsocietypublishing.org/content/268/1477/1737.full.pdf. — URL: http://rspb.royalsocietypublishing.org/content/268/1477/1737.

39. Delta ID Inc.: Fujitsu smartphone powered by Delta ID iris recognition. — 2017. — URL: http://www.deltaid.com/.

40. *Dorairaj V.* [et al.]. Performance evaluation of non-ideal iris based recognition system implementing global ICA encoding // Proc. of IEEE International Conference on Image Processing. — 2005.

41. *Dunstone T.* [et al.]. Biometric System and Data Analysis: Design, Evaluation, and Data Mining. — Springer Science+Business Media, LLC, 2009.

42. Efficient Iris Spoof Detection via Boosted Local Binary Patterns / Z. He [et al.] // Proc. of Advances in Biometrics: Third International Conference. — 2009. — P. 1080–1090.

43. *Ergun H.* [et al.]. Early and Late Level Fusion of Deep Convolutional Neural Networks for Visual Concept Recognition // International Journal of Semantic Computing. — 2016. — Vol. 10. — P. 379–397.

44. *Feddaoui N.* [et al.]. Improving Iris Recognition Performance Using Quality Measures // Advanced Biometric Technologies. — 2011. — Vol. 12. — P. 382.

45. FIRME: Face and Iris Recognition for Mobile Engagement / M. De Marsico [et al.] // Image and Vision Computing. — 2014. — Vol. 32, no. 12. — P. 1161–1172. — URL: www.sciencedirect.com/science/article/pii/S0262885614000055.

46. *Flom L.* [et al.]. Iris recognition system: patent no. US4641349A. — 1985.

47. Fujitsu Limited: Fujitsu Develops Prototype Smartphone with Iris Authentication. — 2015. — URL: http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0302-03.html.

48. Future Challenges based on the Multiple Biometric Grand Challenge // Multiple Biometric Grand Challenge. — 2010. — URL: http://www.nist.gov/itl/iad/ig/mbe.cfm.

49. *Galbally J.* [et al.]. Iris liveness detection based on quality related features // Proc. 5th IAPR Int. Conf. Biometrics. — 2012. — P. 271.

50. *Galbally J.* [et al.]. A review of iris anti-spoofing // Proc. of the 4th International Conference on Biometrics and Forensics (IWBF). — 2016. — P. 1–6.

51. *Gangwar A.* [et al.]. DeepIrisNet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition // Proc. of IEEE International Conference on Image Processing, Phoenix, AZ, USA, September 25-28, 2016. — 2016. — P. 2301–2305. — URL: https://doi.org/10.1109/ICIP.2016.7532769.

52. *Gao L.* [et al.]. Fusion of shallow and deep features for classification of high-resolution remote sensing images // Proc. of SPIE. Vol. 10607. — 2018. — P. 10607 - 10607 –6. — URL: https://doi.org/10.1117/12.2284777.

53. *Girshick R.* [et al.]. Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation // Proc. of IEEE Conference on Computer Vision and Pattern Recognition. — Washington, DC, USA : IEEE Computer Society, 2014. — P. 580–587. — (CVPR '14). — URL: https://doi.org/10.1109/CVPR.2014.81.

54. *Gragnaniello D.* [et al.]. An Investigation of Local Descriptors for Biometric Spoofing Detection // IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10, no. 4. — P. 849–863.

55. *Guang-zhu X.* [et al.]. A novel and efficient method for iris automatic location // Journal of China University of Mining and Technology. — 2007. — Vol. 17. — P. 441–446.

56. *Gupta G.* [et al.]. Iris Recognition Using Non Filter-based Technique // Proc. Biometrics Symposium. — 2005. — P. 45–47.

57. *Gupta P.* [et al.]. On Iris Spoofing Using Print Attack // Proc. of 22nd International Conference on Pattern Recognition. — 2014. — P. 1681–1686.

58. *Hamza R.* Iris recognition system: patent no. US8280119B2. — 2012.

59. *Harley A.* An Interactive Node-Link Visualization of Convolutional Neural Networks // ISVC. — 2015.

60. *He K.* [et al.]. Deep Residual Learning for Image Recognition // Proc. of IEEE Conference on Computer Vision and Pattern Recognition (CVPR). — 2016. — P. 770–778.

61. *He X.* [et al.]. A fake iris detection method based on FFT and quality assessment // Proc. of Chinese Conference on Pattern Recognition (CCPR'08). — 2008. — P. 1–4.

62. History of Iris Recognition. — 2016. — URL: https://www.cl.cam.ac.uk/~jgd1000/history.html.

63. *Hollingsworth K.* [et al.]. The best bits in an iris code // Proc. of IEEE Transactions on Pattern Analysis and Machine Intelligence. — 2009. — Vol. 31, no. 6. — P. 964–973.

64. *Howard A. and Zhu M.* [et al.]. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications // CoRR. — 2017. — Vol. abs/1704.04861. — arXiv: 1704.04861. — URL: http://arxiv.org/abs/1704.04861.

65. *Hu X.* [et al.]. Iterative Directional Ray-based Iris Segmentation for Challenging Periocular Images // Lecture Notes in Computer Science. — 2011. — Vol. 7098. — P. 91–99.

66. *ICAO.* ICAO Document 9303: Machine Readable Travel Documents, Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs. — 2015. — URL: https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf.

67. Information technology - Biometric data interchange formats - Part 6: Iris image data, Annex B : ISO. — 2011. — ISO/IEC 19794-6:2011.

68. *Ioffe S.* [et al.]. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift // Proc. of the 32nd International Conference on International Conference on Machine Learning. — 2015. — P. 448–456. — URL: http://jmlr.org/proceedings/papers/v37/ioffe15.pdf.

69. *Jain A. K.* [et al.]. An Introduction to Biometric Recognition // IEEE Trans. Cir. and Sys. for Video Technol. — 2004. — Vol. 14, no. 1. — P. 4–20.

70. *Jalilian E.* [et al.]. Iris Segmentation Using Fully Convolutional Encoder–Decode Networks // Advances in Computer Vision and Pattern Recognition. — 2017. — P. 133–155.

71. *Janani T.* [et al.]. Feature Fusion for Efficient Object Classification Using Deep and Shallow Learning // International Journal of machine Learning and Computing. — 2017. — Vol. 7, no. 5. — P. 123–127.

72. *Jeong D.* [et al.]. Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter // Proc. of Advances in Biometrics: International Conference, Hong Kong, China, January 5-7 / ed. by D. Zhang [et al.]. — Berlin,

Heidelberg : Springer Berlin Heidelberg, 2005. — P. 457–463. — URL: http://dx.doi.org/10.1007/11608288_61.

73. *Jeong D.* [et al.]. A new iris segmentation method for non-ideal iris images // Image and Vision Computing. — 2010. — Vol. 28. — P. 254–260.

74. *Karpathy A.* [et al.]. Large-scale Video Classification with Convolutional Neural Networks // Proceedings of International Computer Vision and Pattern Recognition (CVPR 2014). — 2014.

75. *Kaushik R.* [et al.]. Multibiometric System Using Level Set, Modified LBP and Random Forest // Int. J. Image Graphics. — 2014. — Vol. 14, no. 3. — URL: http://dx.doi.org/10.1142/S0219467814500132.

76. *Kingma D.* [et al.]. Variational Dropout and the Local Reparameterization Trick // Advances in Neural Information Processing Systems 28 / ed. by C. Cortes [et al.]. — Curran Associates, Inc., 2015. — P. 2575–2583. — URL: http://papers.nips.cc/paper/5666-variational-dropout-and-the-local-reparameterization-trick.pdf.

77. *Kingma D.* [et al.]. Adam: A Method for Stochastic Optimization. // CoRR. — 2014. — Vol. abs/1412.6980. — URL: http://dblp.uni-trier.de/db/journals/corr/corr1412.html.

78. *Koch G.* [et al.]. Siamese Neural Networks for One-shot Image Recognition // Proc. of the 32nd International Conference on Machine Learning. — 2015.

79. *Korobkin M.* [et al.]. Iris Segmentation in Challenging Conditions // Proceedings of International Conference on Pattern Recognition and Artificial Intelligence (ICPRAI). — Montreal, Canada, 2018. — P. 656–660.

80. *Krizhevsky A.* [et al.]. ImageNet Classification with Deep Convolutional Neural Networks // Advances in Neural Information Processing Systems 25 / ed. by F. Pereira [et al.]. — Curran Associates, Inc., 2012. — P. 1097–1105. — URL: http://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks.pdf.

81. *Labati R.* [et al.]. Iris segmentation: state of the art and innovative methods // Intelligent Systems Reference Library. — 2012. — P. 151–182.

82. *Lee J.* Fujitsu smartphone powered by Delta ID iris recognition. — 2015. — URL: http://www.biometricupdate.com/201506/ntt-docomo-fujitsu-smartphone-powered-by-delta-id-iris-recognition.

83. *Lee Y.* [et al.]. VASIR: An Open-Source Research Platform for Advanced Iris Recognition Technologies // Journal of Research of the National Institute of Standards and Technology. — 2013. — Vol. 118. — P. 244–247.

84. *Li H.* [et al.]. A Brief Survey on Recent Progress in Iris Recognition // Proceedings of 9th Chinese Conference on Biometric Recognition. — 2014. — Vol. 106. — P. 288–300. — URL: https://doi.org/10.1016/j.neunet.2018.06.011.

85. *Li Y.-H.* [et al.]. Iris Recognition, Overview // Encyclopedia of Biometrics / ed. by S. Z. Li. — Springer US, 2009. — P. 569–578. — URL: http://www.springer.com/gp/book/9780387730035.

86. *Lim S.* [et al.]. Efficient Iris Recognition through Improvement of Feature Vector and Classifier // ETRI Journal. — 2001. — Vol. 23, no. 2.

87. *Ling L.* [et al.]. Fast and efficient iris image segmentation // Journal of Medical and Biological Engineering. — 2010. — Vol. 30, no. 6. — P. 381–392.

88. *Liu N.* [et al.]. Accurate iris segmentation in non-cooperative environments using fully convolutional networks // International Conference on Biometrics (ICB). — 2016. — P. 1–8.

89. *Liu N.* [et al.]. DeepIris: Learning pairwise filter bank for heterogeneous iris verification // Pattern Recognition Letters. — 2016. — Vol. 82. — P. 154–161. — URL: https://doi.org/10.1016/j.patrec.2015.09.016.

90. *Ma L.* [et al.]. Efficient iris recognition by characterizing key local variations // IEEE Transactions on Image Processing. — 2004. — Vol. 13. — P. 739–750.

91. *Mahadeo N.* [et al.]. Model-Based Pupil and Iris Localization // Int. Joint Conf. Neural Networks. — 2012.

92. *Menotti D.* [et al.]. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection // IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10, no. 4. — P. 864–879.

93. Microsoft Corporation: Unlock your Lumia 950 or Lumia 950 XL with a look. — 2017. — URL: https://support.microsoft.com/en-us/instantanswers/4ea145a3-b98e-f8ed-a262-055ec78cdb80/unlock-your-lumia-950-or-lumia-950-xl-with-a-look.

94. *Minaee S.* [et al.]. An experimental study of deep convolutional features for iris recognition // 2016 IEEE Signal Processing in Medicine and Biology Symposium (SPMB). — 2016. — P. 1–6.

95. *Mohammadi Arvacheh, E.* A Study of Segmentation and Normalization for Iris Recognition Systems : Master's thesis / Mohammadi Arvacheh, E. — University of Waterloo, 2006. — URL: http://hdl.handle.net/10012/2846.

96. *Monro D. M.* [et al.]. DCT-Based Iris Recognition // IEEE Trans. Pattern Anal. Mach. Intell. — Washington, DC, USA, 2007. — Vol. 29, no. 4. — P. 586–595. — URL: http://dx.doi.org/10.1109/TPAMI.2007.1002.

97. *Moravcik T.* An Approach to Iris and Pupil Detection in Eye Image : Master's thesis / Moravcik T. — University of Zilina, 2010.

98. Multiple Biometric Evaluation (MBE2009). — 2009. — URL: http://www.nist.gov/itl/iad/ig/mbe.cfm.

99. Multiple Biometric Grand Challenge (MBGC - 2007). — 2007. — URL: http://www.nist.gov/itl/iad/ig/mbgc.cfm.

100. *Nelder J. A.* [et al.]. A Simplex Method for Function Minimization // Computer Journal. — 1965. — Vol. 7. — P. 308–313.

101. *Ng R.* [et al.]. A Review of Iris Recognition Algorithms // Proc. International Symposium Information Technology. Vol. 2. — 2008. — P. 1–7.

102. *Odinokikh G. A.* [et al.]. High-Performance Iris Recognition for Mobile Platforms // Pattern Recognition and Image Analysis. — 2018. — Vol. 28, no. 3. — P. 516–524. — URL: https://doi.org/10.1134/S105466181803015X.

103. *Odinokikh G.* [et al.]. Method of eyelid detection on image for mobile iris recognition // Machine Learning and Data Analysis. — 2016. — Vol. 2. — P. 442–453.

104. *Odinokikh G.* [et al.]. Feature Vector Construction Method for Iris Recognition // ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. — 2017. — Vol. XLII–2/W4. — P. 233–236. — URL: https://www.int-arch-photogramm-remote-sens-spatial-inf-sci.net/XLII-2-W4/233/2017/.

105. *Odinokikh G.* [et al.]. High-Performance Iris Recognition for Mobile Platforms // Pattern Recognition and Image Analysis. — 2018. — Vol. 28, issue 3. — P. 516–524.

106. *Odinokikh G.* [et al.]. Iris Anti-spoofing Solution for Mobile Biometric Applications // Proceedings of International Conference on Pattern Recognition and Artificial Intelligence. — 2018. — P. 666–671.

108. *Pan L.* [et al.]. Iris Localization based on Multi-resolution Analysis // Proc. 19th Intern. Conf. Pattern Recognition. — 2008. — P. 1–4.

109. *Phillips P.* [et al.]. Frvt2006 and ice2006 large-scale experimental results // IEEE PAMI. — 2010. — Vol. 5. — P. 831–846.

110. *Popescu-Bodorin N.* [et al.]. Comparing Haar-Hilbert and Log-Gabor Based Iris Encoders on Bath Iris Image Database // CoRR. — 2011. — Vol. abs/1106.2357.

111. *Prabhakar R.* Apparatuses and methods for iris based biometric recognition: patent no. US20150071503. — 2017.

112. *Prabhakar S.* [et al.]. Biometric recognition: Sensor characteristics and image quality // IEEE Instrumentation Measurement Magazine. — 2011. — Vol. 14, no. 3. — P. 10–16.

113. *Pranith A.* [et al.]. Iris recognition using corner detection // Proc of the 2nd International Conference on Information Science and Engineering. — 2010. — P. 2151–2154.

114. *Proença H.* Iris recognition: What is beyond bit fragility? // Proc. of IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10, no. 2. — P. 321–332.

115. *Proenca H.* [et al.]. A noisy iris image database // Proc. 13th Int. Conf. Image Analysis and Processing. — 2005. — P. 970–976.

116. *Proenca H.* [et al.]. Iris segmentation methodology for non-cooperative recognition // IEEE Proc. Vision, Image and Signal Processing. Vol. 153. — 2006. — P. 199–205.

117. *Proença H.* [et al.]. IRINA: Iris Recognition (Even) in Inaccurately Segmented Data // Proc. of IEEE Conference on Computer Vision and Pattern Recognition. — 2017. — P. 6747–6756. — URL: https://doi.org/10.1109/CVPR.2017.714.

118. *Raghavendra R.* [et al.]. Robust Scheme for Iris Presentation Attack Detection Using Multiscale Binarized Statistical Image Features // IEEE Transactions on Information Forensics and Security. — 2015. — Vol. 10, no. 4. — P. 703–715.

119. *Raja K. B.* [et al.]. Smartphone based robust iris recognition in visible spectrum using clustered K-means features // Proc. of 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications. — 2014. — P. 15–21.

120. *Raja K. B.* [et al.]. Multi-modal authentication system for smartphones using face, iris and periocular // Proc. of International Conference on Biometrics (ICB). — 2015. — P. 143–150.

121. *Rajput M. R.* [et al.]. IRIS biometrics survey 2010–2015 // Proc. of IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT). — 2016. — P. 2028–2033.

122. *Rathgeb C.* [et al.]. A survey on biometric cryptosystems and cancelable biometrics. // EURASIP J. Information Security. — 2011. — P. 3. — URL: http://dblp.uni-trier.de/db/journals/ejisec/ejisec2011.html.

123. Samsung Electronics Inc.: Security. — 2017. — URL: http://www.samsung.com/global/galaxy/galaxy-s8/security/.

124. *Scharr H.* Optimal second order derivative filter families for transparent motion estimation // Proc. of EUSIPCO. — 2007. — URL: http://juser.fz-juelich.de/record/58806 ; Record converted from VDB: 12.11.2012.

125. *Sequeira A. F.* [et al.]. Iris liveness detection methods in mobile applications // Proc. of International Conference on Computer Vision Theory and Applications. Vol. 3. — 2014. — P. 22–33.

126. *Sequeira A.* [et al.]. MobiLive 2014 - Mobile Iris Liveness Detection Competition // Proc. of IEEE International Joint Conference on Biometrics. — 2014. — P. 1–6.

127. *Shelhamer E.* [et al.]. Fully Convolutional Networks for Semantic Segmentation // IEEE Trans. Pattern Anal. Mach. Intell. — 2017. — Vol. 39, no. 4. — P. 640–651. — URL: https://doi.org/10.1109/TPAMI.2016.2572683.

128. *Si Y.* [et al.]. Novel Approaches to Improve Robustness, Accuracy and Rapidity of Iris Recognition Systems // Proc. of IEEE Transactions on Industrial Informatics. — 2012. — Vol. 8. — P. 110–117.

129. *Tabassi E.* Large Scale Iris Image Quality Evaluation // BIOSIG 2011 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 08.-09. September 2011 in Darmstadt, Germany. — 2011. — P. 173–183. — URL: http://subs.emis.de/LNI/Proceedings/Proceedings191/article6493.html.

130. *Takano H.* [et al.]. A system for automated iris recognition // State of the art in Biometrics. — 2011. — P. 203–218.

131. *Tang X.* [et al.]. Deep convolutional features for iris recognition // Proc. of the Chinese Conference on Biometric Recognition. — Springer. 2017. — P. 391–400.

132. *Thavalengal S.* [et al.]. Evaluation of combined visible/NIR camera for iris authentication on smartphones // Proc. of IEEE Conference on Computer Vision and Pattern Recognition Workshops. — 2015. — P. 42–49.

133. *Thavalengal S.* [et al.]. User Authentication on Smartphones: Focusing on iris biometrics // IEEE Consumer Electronics Magazine. — 2016. — Vol. 5, no. 2. — P. 87–93.

134. *Thornton J.* [et al.]. An Evaluation of Iris Pattern Representations // Proc. of IEEE International Conference on Biometrics, Theory, Applications and Systems. — 2007. — Vol. 2. — P. 1–6.

136. *Toshev A.* [et al.]. DeepPose: Human Pose Estimation via Deep Neural Networks // Proc. of the IEEE Conference on Computer Vision and Pattern Recognition. — Washington, DC, USA : IEEE Computer Society, 2014. — P. 1653–1660. — (CVPR '14). — URL: https://doi.org/10.1109/CVPR.2014.214.

137. University of Bath. Iris Image Database. (2005). — 2005. — URL: http://www.bath.ac.uk/elec-eng/research/sipg/irisweb/.

138. *Vergne C.* [et al.]. World Payments Report (WPR 2017). — 2017. — URL: https://www.worldpaymentsreport.com/reports/noncash.

139. *Wang S.* [et al.]. Fast dropout training // Proc. of the 30th International Conference on Machine Learning. Vol. 28–2 / ed. by S. Dasgupta [et al.]. — Atlanta, Georgia, USA : PMLR, 2013. — P. 118–126. — (Proceedings of Machine Learning Research). — URL: http://proceedings.mlr.press/v28/wang13a.html.

140. *Wildes R.* Iris Recognition: An Emerging Biometric Technology // Proc. IEEE. Vol. 85. — 1997. — P. 1348–1363.

141. *Wildes R.* [et al.]. A system for automated iris recognition // WACV. — 1994.

142. *Wildes R.* [et al.]. Automated, non-invasive iris recognition system and method: patent no. US5751836. — 1997.

143. *Yambay D.* [et al.]. LivDet-iris 2013 - Iris Liveness Detection Competition 2013 // Proc. of IEEE International Joint Conference on Biometrics. — 2013. — P. 1–8.

144. *Yambay D.* [et al.]. LivDet-Iris 2015 - Iris Liveness Detection Competition 2015 // Proc. of IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). — 2015. — P. 1–6.

145. *Yambay D.* [et al.]. LivDet-Iris 2017 - Iris Liveness Detection Competition 2017 // Proc. of IEEE International Joint Conference on Biometrics (IJCB). — 2017.

146. *Yuan W.* [et al.]. A rapid iris location method based on the structure of human eyes // Proc. of 27th Annual Conf. on Engineering in Medicine and Biology. Vol. 45. — 2005. — P. 3020–3023.

147. *Zaim A.* [et al.]. A New Method for Iris Recognition using Gray-Level Coccurence Matrix // Proc. IEEE Int. Conf. Electro/information Technology. — 2006. — P. 350–353.

148. *Zeiler M.* [et al.]. Visualizing and Understanding Convolutional Networks // ECCV. — 2014.

149. *Zeiler M.* [et al.]. Adaptive Deconvolutional Networks for Mid and High Level Feature Learning // Proc. of the International Conference on Computer Vision. — Washington, DC, USA : IEEE Computer Society, 2011. — P. 2018–2025. — (ICCV '11). — URL: http://dx.doi.org/10.1109/ICCV.2011.6126474.

150. *Zhang M.* [et al.]. The BTAS Competition on Mobile Iris Recognition // Proceedings of 8th International Conference on Biometrics Theory, Appli-

cations and Systems. — 2016. — URL: http://gen.lib.rus.ec/scimag/index.php?s=10.1109/BTAS.2016.7791191.

151. *Zhang Q.* [et al.]. Fusion of Face and Iris Biometrics on Mobile Devices Using Near-infrared Images // Proc. of 10th Chinese Conference on Biometric Recognition, Tianjin, China, November 13-15, 2015, Proceedings / ed. by J. Yang [et al.]. — Cham : Springer International Publishing, 2015. — P. 569–578. — URL: http://dx.doi.org/10.1007/978-3-319-25417-3_67.

152. *Zhao Z.* [et al.]. Towards More Accurate Iris Recognition Using Deeply Learned Spatially Corresponding Features // Proc. IEEE International Conference on Computer Vision. — 2017. — P. 3829–3838. — URL: https://doi.org/10.1109/ICCV.2017.411.

153. *Zhou Z.-H.* [et al.]. Projection functions for eye detection // Pattern Recognition. — 2004. — Vol. 37. — P. 1049–1056.