

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Самарский государственный технический
университет»
ФГБОУ ВО «СамГТУ»

На правах рукописи

Ефимов Илья Николаевич

**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И КОМПЛЕКСЫ
ПРОГРАММ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА К
ИНФОРМАЦИОННЫМ РЕСУРСАМ**

Специальность 05.13.18 – Математическое моделирование, численные методы
и комплексы программ

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:

Косолапов Александр Михайлович,
д. т. н., профессор

г.Самара – 2016

Содержание

Введение.....	4
1 Анализ существующих решений и формулировка задач исследования	11
1.1 Общая характеристика и постановка задач	11
1.2 Методы автоматического распознавания изображений лиц	15
1.3 Классификация способов подтверждения подлинности объекта	20
1.4 Выводы по 1 разделу.....	26
2 Разработка технологии распознавания пользователей информационных ресурсов.....	27
2.1 Требования к формированию изображений лиц.....	27
2.2 Распознавание изображений лиц.....	29
2.2.1 Поиск координат распознаваемого объекта на изображении	31
2.2.2 Локализация информативной области на изображении	34
2.2.3 Вычисление информативных признаков	39
2.2.4 Математическая модель, метод и алгоритм численного определения информативных признаков	43
2.2.5 Функции расчёта расстояния	50
2.2.6 Технология распознавания изображений лиц и экспериментальные исследования.....	53
2.3 Подтверждение подлинности распознаваемого объекта	60
2.3.1 Модель атак на биометрическую систему.....	61
2.3.2 Постановка задачи подтверждения подлинности распознаваемого объекта.....	64
2.3.3 Математическая модель, метод и алгоритм подтверждения подлинности распознаваемого объекта	66

2.3.4 Характеристики технических устройств, используемых для подтверждения подлинности объекта.....	71
2.3.5 Экспериментальные исследования	78
2.4 Технология распознавания пользователей информационных ресурсов	80
2.5 Выводы по 2 разделу.....	82
3 Программный комплекс распознавания пользователей информационных ресурсов.....	84
3.1 Описание архитектуры БД программного комплекса.....	85
3.2 Архитектура и объектная модель программного комплекса.....	90
3.3 Основные модули программного комплекса	92
3.4 Выводы по 3 разделу.....	97
Заключение	98
Список сокращений и условных обозначений.....	100
Словарь терминов.....	102
Список цитируемой литературы.....	103
Приложение А	116
Приложение Б	124

Введение

Актуальность работы. Методы биометрической идентификации личности находят все более широкое применение в системах контроля доступа (СКД) к рабочим местам, мобильным устройствам, локальным и глобальным информационным ресурсам. Наиболее перспективными являются системы, принцип работы которых основан на распознавании лица человека, т.к. для реализации систем не требуется специализированная техника, а биометрический признак нельзя потерять, забыть или передать.

Несмотря на значительный прогресс, связанный с разработкой новых и повышением эффективности существующих алгоритмов распознавания изображений лиц, подобные системы все ещё подвержены уязвимостям в виду возможной подмены распознаваемого лица фотографией или фотомаской. Существующие способы подтверждения подлинности распознаваемого объекта можно разделить на следующие классы в зависимости от вида воздействия на распознаваемый объект: способы без воздействия на распознаваемый объект (способы, использующие анализ текстурных признаков, 3D моделей объекта, биофизических признаков и т.д.), способы с физическим воздействием (способы, применяющие видимый спектр света, ИК излучение и т.д.), способы с командным воздействием (система защиты указывает пользователю на необходимость произвести некоторые действия, например, произнести сгенерированный случайный текст, моргнуть или открыть рот и т.д.).

Актуальность исследований в этом направлении подтверждается большим числом работ учёных как в России, так и за рубежом. Наиболее известные результаты получены в следующих российских организациях: ИПИ РАН, ИСОИ РАН [5, 9, 27, 35–39], Самарский национальный исследовательский университет [2, 7, 41, 43, 51, 52, 57, 58], МГУ им. М.В. Ломоносова, НИИЦ БТ МГТУ им. Н.Э. Баумана [33, 34] и др. Наиболее значимые результаты за рубежом в этом направлении выполнены в следующих научно-исследовательских институтах и корпорациях: в

США – Массачусетский технологический институт, компания Google, компания Microsoft, компания Apple, а также корпорация Toshiba в Японии, Кембриджский университет в Великобритании [44] и др. Изучению различных аспектов проблемы распознавания человека по изображению лица посвящены труды В.В. Старовойтова, В.Н. Вапника, Ю.И. Журавлёва, Г. С. Поспелова, Э.В. Попова, В.М. Глушкова, В.А. Сойфера, В.А. Фурсова, В.В. Сергеева, Я.А. Фурмана, F. Rosenblatt, B. Widrow, J. Hopfield, M. Minsky, T. Kohonen, M. Kirby, A. Pentland, M. Turk, T. Ojala, M. Pietikainen, T. Ahonen, T. Cootes, I. Chingovska, P. Viola, M. Jones и других отечественных и зарубежных учёных. Однако задача распознавания и подтверждения подлинности распознаваемого объекта не решена в полной мере. Требуется разработать и исследовать математические модели, численные методы, алгоритмы и программный комплекс, обеспечивающие высокие показатели быстродействия и достоверности распознавания при небольших аппаратных затратах и стоимости. Решению указанной проблемы посвящена данная диссертация.

Целью диссертационной работы является разработка и исследование математических моделей, методов, алгоритмов и технологий для комплексного решения задачи распознавания пользователей информационных ресурсов, отличающегося низкой вычислительной сложностью и не требующего дополнительного специализированного оборудования. Для достижения поставленной цели в диссертации решаются нижеследующие задачи.

1. Анализ известных методов распознавания человека по изображению лица и подтверждения подлинности распознаваемого объекта. Обоснование выбора численного метода построения модели распознаваемого объекта.

2. Разработка, обоснование и исследование математической модели, метода и алгоритма численного определения информативных признаков.

3. Разработка, обоснование и исследование метода и алгоритма подтверждения подлинности распознаваемого объекта.

4. Разработка информационной технологии и комплекса проблемно-ориентированных программ для обеспечения процессов распознавания и подтверждения

подлинности распознаваемого объекта. Проведение экспериментальных исследований для анализа адекватности предложенных математических моделей, методов и алгоритмов.

Научная новизна диссертационной работы.

1. Предложены математическая модель информативного признака объекта, модифицированный численный метод построения гистограмм локальных бинарных шаблонов, основанный на использовании оригинальной комбинации формы шаблона и способа сравнения фрагментов информативного признака, и алгоритм численного определения информативных признаков, отличительной особенностью которого является более низкая вычислительная сложность и высокая эффективность использования в процессе распознавания образов, в частности, изображений лиц.

2. Разработаны, обоснованы и исследованы метод и алгоритм подтверждения подлинности распознаваемого объекта на основе многократной оценки рассеивания яркостей сопряжённых пикселей изображений лица объекта, позволяющие обнаружить подмену объекта, предъявляемого системе распознавания.

3. Предложено комплексное решение задачи распознавания пользователей информационных ресурсов на основе оригинальной технологии, в отличие от существующих обеспечивающей возможность работы в реальном времени и высокую вероятность правильного распознавания человека по изображению лица за счёт использования оригинального информативного признака и метода подтверждения подлинности распознаваемого объекта.

4. Разработанные математические модели, методы и алгоритмы реализованы в виде комплекса программ для обеспечения процессов распознавания и подтверждения подлинности распознаваемого объекта.

Методы исследований. При решении поставленных задач в диссертационной работе использовались методы численного анализа, математического моделирования, теории вероятностей и математической статистики, теория баз данных, теория цифровой обработки сигналов и изображений.

Практическая значимость работы в теоретическом плане заключается в разработке модифицированного численного метода построения информативного признака объекта, метода подтверждения подлинности распознаваемого объекта и технологии распознавания пользователей информационных систем по изображению лица.

Прикладная ценность результатов работы заключается в возможности использования их в различных отраслях промышленности и транспорта для принятия решения о предоставлении доступа к рабочим местам, технологическим процессам и информационным ресурсам.

Внедрение результатов работы. Результаты диссертации нашли применение в учебном процессе кафедры «Информационные системы и телекоммуникации» ФГБОУ ВПО «Самарский государственный университет путей сообщения». Полученные в работе теоретические положения и практические результаты частично внедрены в ООО "МИП" Электротехника СамГУПС". Результаты внедрения подтверждены соответствующими актами.

Работа поддержана грантом СамГУПС в номинации «Научная работа аспиранта» по теме "Биометрическая идентификация лиц" и выполнена при финансовой поддержке фонда содействия развитию малых форм предприятий в научно-технической сфере по теме «ИИС идентификации нарушителя по изображению лица» в номинации «Информационные технологии».

Апробация работы. Основные положения и результаты диссертационной работы докладывались и обсуждались на 10 научных конференциях:

- на Международной научно-технической конференции «Перспективные информационные технологии (ПИТ-2016)» (г. Самара, 2016);
- на Международной научно-технической конференции «Перспективные информационные технологии (ПИТ-2013)» (г. Самара, 2013);
- на XXVIII Международной научно-практической конференции «Перспективы развития информационных технологий» (г. Новосибирск, 2016 г.);
- на VIII Международной научно-практической конференции «Эффективные инструменты современных наук – 2012» (г. Прага, Чехия, 2012 г.);
- на VIII Международной научно-практической конференции «Наука и инновации – 2012» (г. Пшемьсль, Польша, 2012 г.);
- на Межуниверситетских инновационных чтениях «УМНИК 2013», (г. Самара, 2013 г.);
- на Всероссийской научно-практической конференции «Роль молодёжи в формировании и развитии инновационных кластеров» (г. Самара, 2014);
- на научно-технической конференции студентов и аспирантов ФГБОУ ВПО СамГУПС «Дни студенческой науки XXXVIII» (г. Самара, 2011г.);
- на научно-технической конференции студентов и аспирантов ФГБОУ ВПО СамГУПС «Дни студенческой науки XXXIX» (г. Самара, 2012г.);
- на научно-технической конференции студентов и аспирантов ФГБОУ ВПО СамГУПС «Дни студенческой науки XXXX» (г. Самара, 2013г.).

Публикации. Результаты диссертации опубликованы в 17 работах, из них 4 публикации в журналах, рекомендованных ВАК [13, 18, 20, 23], 5 тезисов докладов на международных научно-практических конференциях [12, 14, 21, 24, 25], 5 тезисов докладов на научно-теоретических конференциях [15–17, 19, 22]. Получены свидетельство о государственной регистрации программы для ЭВМ «Аутентификация двумерных изображений» (№ 2013611188 от 9.01.2013 г.) [3], свидетельство на базу данных «База данных двумерных изображений для аутентификации» (№ 2013620323 от 12.01.2013 г.) [4], патент на изобретение «Способ

и устройство распознавания рельефности изображения лица» (№ RU 2 518 939, 11.04.2014) [55].

Положения, выносимые на защиту.

1. Математическая модель информативного признака объекта, модифицированный численный метод построения информативных признаков и алгоритм определения гистограмм локальных бинарных шаблонов.
2. Метод и алгоритм подтверждения подлинности распознаваемого объекта.
3. Комплексное решение задачи распознавания пользователей информационных ресурсов на основе новой информационной технологии.
4. Программный комплекс для обеспечения процессов распознавания и подтверждения подлинности распознаваемого объекта, реализующий разработанные методы, математические модели, алгоритмы и технологии.

Обоснованность выносимых на защиту научных положений, выводов и рекомендаций подтверждается корректностью использования математического аппарата, основных положений теории распознавания образов; корректной постановкой экспериментов и их обработкой; качественным и количественным соответствием результатов теоретических исследований и экспериментальных данных; практическим применением результатов исследований.

Личный вклад автора. Работы [12–19, 21, 22] выполнены самостоятельно, в работах [3, 4, 20, 23–25, 55] диссертанту принадлежит совместная постановка задачи и анализ результатов, ему лично принадлежит разработка методов решений, алгоритмизация, реализация в виде программного продукта

Структура и объем диссертации. Диссертационная работа состоит из введения, трёх разделов и заключения, изложенных на 125 страницах машинописного

текста, включая 36 рисунков и 14 таблиц, список сокращений и условных обозначений, словарь терминов, список цитируемой литературы, содержащий 126 наименований и два приложения.

В приложении приведены акты о внедрении результатов диссертационной работы, а также сигнатуры реализованных методов на объектно-ориентированном языке C#.

1 Анализ существующих решений и формулировка задач исследования

В данном разделе приведена общая характеристика и постановка задач исследования. Выполнен сравнительный анализ известных методов распознавания человека по изображению лица и подтверждения подлинности распознаваемого объекта. Результаты анализа являются основой для исследования и реализации комплексного решения задачи распознавания пользователей информационных ресурсов во втором и третьем разделах диссертации.

1.1 Общая характеристика и постановка задач

Технологии автоматической идентификации человека находят применение в различных областях промышленности и железнодорожного транспорта. Идентификация человека требуется в работе контрольно-пропускных пунктов, при учёте рабочего времени сотрудников, в ограничении доступа к рабочим местам, мобильным устройствам и информационным системам и т.д. От вероятности правильного распознавания зависит сохранность конфиденциальных данных и объектов предприятия. Внедрение методов распознавания человека по изображению лица позволит решить задачу учёта рабочего времени на предприятии. Технология распознавания изображений лиц найдёт применение в операциях расчёта времени нахождения каждого сотрудника на своём рабочем месте и фиксации времени прибытия и ухода сотрудников с предприятия. Автоматическое распознавание и подтверждение подлинности распознаваемого объекта требуются и в дистанционном обучении (далее ДО). Экзамены считаются обязательным и жизненно необходимым компонентом обучения. Эффективность экзаменов в ДО зависит от вероятности правильного распознавания студентов. Низкая вероятность правильного распознавания студентов уменьшает авторитет ДО.

Существующие способы распознавания человека можно разделить на следующие [20]:

- по имени пользователя и паролю;
- с применением специализированных устройств (микропроцессорных карточек, токенов и т.д.);
- по биометрическим характеристикам человека;
- смешанный способ (например, по биометрическим характеристикам, имени пользователя и паролю).

Первые два способа не дают стопроцентной уверенности, что распознаваемый пользователь именно тот, кто является владельцем специального устройства или пароля.

Преимущество последних двух способов, по сравнению с двумя первыми, заключается в том, что распознаётся не внешний предмет, принадлежащий пользователю или запомненная им фраза, а биометрический признак, который невозможно потерять, передать или забыть.

На данный момент известен ряд биометрических технологий, которые могут быть использованы в системах распознавания человека по [20]:

- отпечаткам пальцев;
- чертам лица;
- радужной оболочке глаз;
- голосу;
- другим характеристикам.

В ходе исследования необходимо разработать технологию для обеспечения процессов идентификации (по чертам лица) и аутентификации (со смешанным способом по чертам лица, логину и паролю), а также программное обеспечение для её реализации. Преимуществами такой технологии будут:

- удобство пользователей – при идентификации объекту не нужно запоминать данные учётной записи;
- возможность осуществлять ненавязчивый контроль доступа пользователей к системе;

- отсутствие необходимости в специализированном дорогостоящем оборудовании, необходимым и достаточным устройством является видеокамера.

Далее приведём постановку задачи распознавания пользователей по изображению лица. Решение должно состоять из одного или нескольких рабочих мест, оборудованных компьютерами, устройствами ввода изображения – видеокамерой, а также требуемым сетевым оборудованием (рисунок 1.1). Рабочие места могут находиться территориально далеко друг от друга. Получение доступа к рабочему месту возможно в двух режимах: с вводом логина и пароля, а также без дополнительных действий. Для получения доступа к рабочему месту пользователю необходимо находиться в области видимости видеокамеры. На сервер отправляется запрос, включающий в себя изображение с видеокамеры, логин и пароль. Далее на изображении выделяется область, содержащая лицо пользователя. Ответом сервера является решение о выдаче доступа к рабочему месту. Решение принимается на сервере в автоматическом режиме, но в частном случае при большом количестве отказов в доступе зарегистрированному пользователю решение может быть принято с участием администратора сервера.

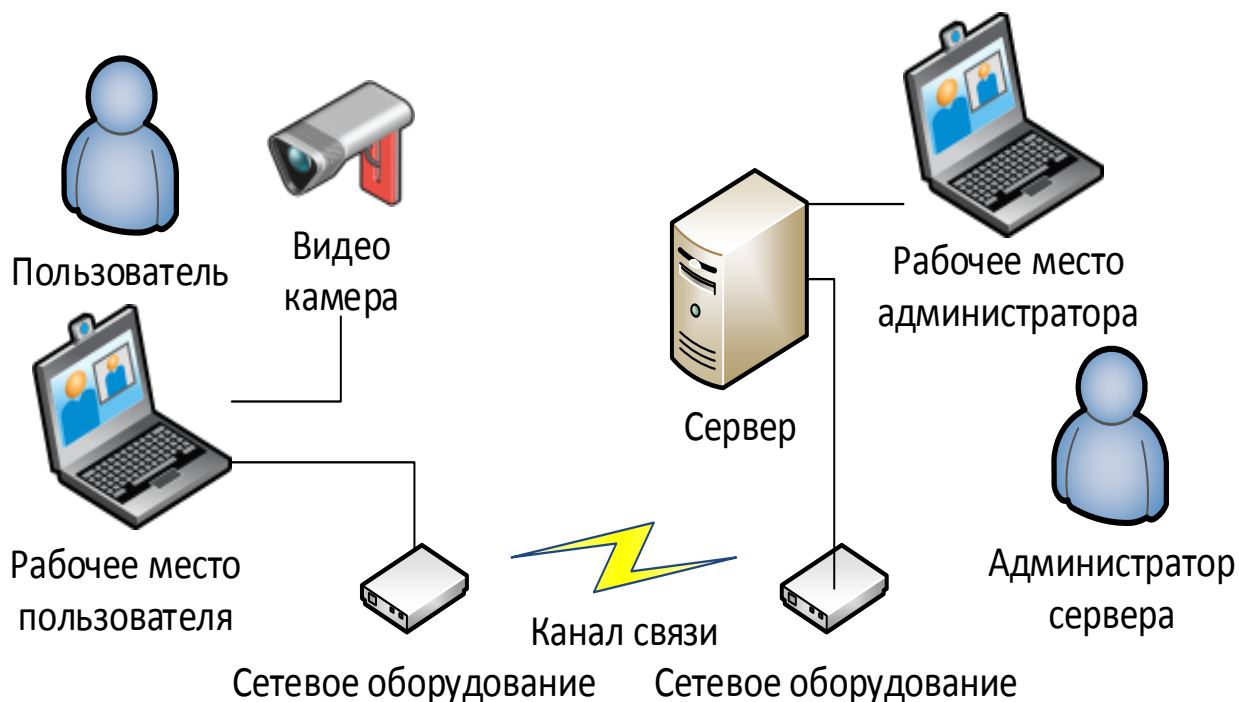


Рисунок 1.1 – Схема распознавания пользователей в системе контроля доступа

Объект распознавания представляется в виде двумерного изображения, на котором в реальных условиях могут присутствовать шумы, создаваемые устройствами первичной информации, погрешностью преобразования и источниками света. Также присутствует уязвимость подмены подлинного объекта в процессе распознавания. Таким образом, возникает задача повышения вероятности правильно распознавания человека по его двумерному изображению. На рисунке 1.2 изображены возможные пути повышения вероятности правильного распознавания изображений лица пользователя, в частности, 4-ый путь можно разделить ещё на три направления. В данной работе для решения задачи повышения вероятности правильного распознавания человека по изображению лица были выбраны третье и четвёртое направления.



Рисунок 1.2 – Пути повышения вероятности правильного распознавания

В рамках задачи повышения вероятности правильного распознавания изображений лица можно выделить следующие пути совершенствования системы: уменьшение погрешности функциональных преобразований сигналов с датчиков первичной информации, улучшение алгоритмов построения модели распознаваемого объекта, увеличение степени защиты системы от спуфинг атак, улучшение качеств применяемых алгоритмов распознавания образов.

1.2 Методы автоматического распознавания изображений лиц

При разработке систем биометрического распознавания пользователей по изображению лица необходимо понять, как распознаёт лица человек. Изучение процесса распознавания лиц человеком может помочь понять основные аспекты. Однако человек использует больше информации, чем искусственные системы. Человеческая система использует данные, полученные от различных органов чувств. Во многих случаях косвенные признаки, такие как фон, причёска, мимика и т.д., также играют важную роль в распознавании лиц. Перечисленные признаки трудно учитывать системам машинного распознавания, т.к. подобных данных и их комбинаций существует большое множество. Тем не менее, процесс распознавания доставляет некоторые трудности и для человека. Человеку затруднительно запомнить большое количество лиц. Ключевым преимуществом систем машинного обучения является её почти неограниченная память [126].

Глаза, рот, нос, контуры лица определены как наиболее важные признаки для восприятия и запоминания лиц. Кроме того, было обнаружено, что верхняя часть лица является более полезной для распознавания, чем нижняя. Так исследования по направленности освещения показали [85], что людям проще распознавать лица, освещённые сверху-вниз, чем лица, освещённые снизу-вверх. Кроме того, эстетические характеристики (например, красота, привлекательность, приятность и т.д.) играют важную роль при распознавании лиц – более привлекательные лица легче запоминаются. Указанные аспекты необходимо учитывать при создании искусственных систем распознавания лиц.

На верное распознавание влияют следующие факторы: условия съёмки, освещение, повороты головы, выражение лица. Помимо перечисленного, на работу системы сильно влияет макияж. В работе [79] показано, что макияж может существенно изменить внешний вид пользователя как на локальном уровне (контрастность и текстура кожи), так и на глобальном (форма лица). Уменьшение процента верного распознавания составляет от 2,90% до 21,47%.

Существует большое количество принципиально различных методов, позволяющих определить личность человека по изображению лица. Главными критериями оценки методов являются вычислительная сложность алгоритмов и вероятность правильного распознавания. Ниже приведены наиболее эффективные методы автоматического распознавания изображений лиц.

Геометрические характеристики лица – один из первых признаков, используемых для распознавания лиц. Впервые этот признак применялся в криминалистике. Далее была разработана компьютерная система, использующая геометрические характеристики лица. Суть метода состоит в выделении комплекта антропометрических точек и дальнейшем сравнении расстояний между точками. Комплекты точек выбираются исследователем эмпирическим путём. Ключевыми точками являются уголки глаз и рта, центры зрачков и бровей и т.п. Процесс распознавания изображений лиц заключается в сравнении признаков распознаваемого лица с эталонными признаками из БД. Вероятность правильного распознавания зависит от наиболее точного нахождения антропометрических точек. Задача точного нахождения антропометрических точек относится к трудоёмким и вычислительно затратным задачам. В данном методе важно, чтобы изображение лица человека было без помех. Поэтому процесс предобработки изображения является важнейшим из этапов в методе. В работе [95] использовали вейвлеты Габора для обнаружения антропометрических точек на изображении лица. Количество антропометрических точек равнялось 35–45. Доля верного распознавания образов составила 86%. Геометрические сопоставления характеристик лица наиболее полезно для поиска возможных совпадений в сравнительно большой БД. Для применения метода выдвигаются следующие требования к подготовке изображений: отсутствие направленного освещения, нейтральное выражение лица и отсутствие посторонних предметов, пересекающих область лица.

Метод сравнения эталонов (Template Matching) [90] основывается на сравнении регионов лица. Каждый совпавший регион увеличивает меру сходства

изображений. Один из недостатков метода сравнения эталонов является его вычислительная сложность. Другая проблема заключается в описании этих регионов. Также система распознавания должна быть инвариантна к определённым расхождениям между эталонным и распознаваемым изображением.

Метод главных компонент (МГК) описан исследователем Карлом Пирсоном в 1901 году. Также его называют методом «собственных векторов» либо «собственных лиц». МГК является методом сокращения размерности избыточных данных. МГК используется в методе Eigenface, который представлен Тюрком и Пентландом в 1991 году [115]. Для всех изображений лиц в БД производится процесс вычисления первых главных компонент. Далее запускается процесс сопоставления изображений, заключающийся в сравнении главных компонент распознаваемого изображения с главными компонентами изображений в БД. Изображение из БД считается распознанным, если имеет наименьшее расстояние от исходного изображения. Для метода Eigenface необходимо создать условия, приближенные к идеальным: единый уровень освещённости, однотипное выражение лица, отсутствие предметов, перекрывающих части лица. При несоблюдении указанных условий Eigenface не сможет корректно определять межклассовые вариации. Eigenface считается первой работоспособной технологией распознавания лиц. Тюрк и Пентланд применили Eigenface на БД из 2500 изображений лиц 16 субъектов, полученных с разными ракурсами съёмки, размерами объекта и условиями освещения. Эксперименты доказали, что система была довольно устойчивой к изменениям масштаба, но результаты резко ухудшались при изменении освещения объекта.

Далее приведены различные работы, использующие МГК. Могхаддам и Пентланд использовали МГК для распознавания и сжатия изображений. В работе [103] приведён метод кодирования, сжатия и распознавания изображений для приложений видео-телефонии. Могхаддам и Пентланд объявили о получении хороших результатов (одно неправильное определение) при экспериментах на 150

фронтальных изображениях БД FERET. Байесовский МГК, предложен Могхаддам в соавторстве [99]. Проверка и испытания систем на основе байесовского МГК проводилась на БД FERET. Могхаддам утверждал, что экспериментальные результаты демонстрируют простоту и вычислительную производительность метода. В работе [92] предложен метод с применением МГК для обнаружения и распознавания лиц на изображениях со сложным фоном. В [73] исследователи предложили использовать МГК и фильтры Габора вместе для преодоления недостатков МГК. В первой части метода, с помощью фильтров Габора, извлекаются черты лица на исходном изображении. Далее, для распознавания лиц используется МГК.

В 1996 году для распознавания лиц исследователями был предложен метод линейного дискриминантного анализа (линейный дискриминант Фишера) [81]. Цель дискриминантного анализа определяется как нахождение проекции, которая максимизирует межклассовое расстояние и минимизирует внутриклассовое в пространстве признаков, где собственные вектора рассчитываются путём анализа собственных значений. Альтернативный способ, который сочетает в себе МГК и дискриминантный анализ изучается в [126].

При увеличении угла поворота головы – вероятность верного распознавания резко уменьшается. Метод сравнения эластичных графов (Elastic Bunch Graph Matching) позволяет добиться более высокой вероятности правильного распознавания изображений лица при повороте головы на угол до 22° по сравнению с предыдущими методами. Для использования метода лицо обозначается в виде графа, вершины которого расположены на антропометрических точках: контуры лица, уголки губ, кончик носа, глаза, центры зрачков и т.д. В работе [119] доля верного распознавания составила – 86,5% для поворота на 10 градусов и 66,4% для поворота на 30 градусов. Метод сравнения эластичных графов превосходит другие методы распознавания с точки зрения инвариантности к повороту головы. Однако представленный метод имеет более высокие вычислительные затраты по сравнению аналогами.

Привлекательность использования нейронных сетей (НС) связана с их нелинейностью. Одной из первых искусственных НС, используемых для распознавания образов, была сеть под названием WISARD [35]. Для распознавания лиц применяются такие архитектуры НС, как многослойный персептрон [111] и сверточные НС. В работе [91] предложены гибридные НС, сочетающие в себе самоорганизующейся карты (SOM) и сверточную НС. Процент верного распознавания на базе из 400 изображений составил 96,2 %. В работе [66] использовались вероятностные решения на основе НС. Процент верного распознавания лиц на БД ORL достиг 96%.

Скрытые марковские модели (СММ) успешно применяются для приложений распознавания изображений лиц. Изображение лица делят на регионы глаз, носа, рта и передают на вход СММ. В работе [109] учёные, используя СММ, сообщили о 87% верного распознавания на БД, состоящей из 400 изображений. В таблице 1.1 представлены результаты работы наиболее часто применяемых методов для распознавания человека по изображению лица.

Таблица 1.1 – Результаты экспериментальных исследований методов автоматического распознавания изображений лиц

Методы автоматического распознавания изображений лиц	Процент верного результата распознавания
Расчёт геометрических характеристик лица [95]	86%
Метод главных компонент [103]	95%
Сравнение эластичных графов [78]	90%
Скрытые Марковские модели [109]	87%
Сверточные НС [91]	96.2%
Нейросетевой метод [66]	96%
Метод сравнения эластичных графов [119]	86,5%

1.3 Классификация способов подтверждения подлинности объекта

Биометрические системы уязвимы к атакам спуфинга (spoofing). Для биометрических систем спуфинг — это обман путём предоставления биометрическому сенсору копий, муляжей, фотографий, видеозаписи, заранее записанных звуков и т. п. Цель атаки спуфинга при распознавании — представление незарегистрированного пользователя в системе как зарегистрированного. Противодействие атакам спуфинга является трудоёмкой задачей, так как злоумышленник имеет непосредственный контакт с сенсором, в связи с этим невозможно использовать методы шифрования и цифрового кодирования [1]. В [80] авторы продемонстрировали успешный взлом коммерческих систем распознавания лиц, используя фотографию или видеозапись зарегистрированного пользователя с экрана устройства.

На момент написания диссертационной работы уже существовало множество систем защиты от спуфинга. Наилучшие результаты, по данным разработчиков, продемонстрировали системы, использующие специализированные сканеры или видеокамеры, позволяющие реконструировать 3D объект. Тем не менее, способы подтверждения подлинности распознаваемого объекта, не использующие специализированное оборудование и не требующие дополнительных действий, наиболее перспективны, т.к. удобнее для конечного пользователя и могут быть легко интегрированы в существующие системы распознавания лиц.

Дополнительной трудностью для разработчиков систем защиты от спуфинга является отсутствие публичных БД, содержащих полный перечень спуфинг атак (фотографии объекта на бумажном носителе, изображения фото и видео с различных экранов устройств, фотомаски, силиконовые маски, изображения объекта с нанесённым гримом, а также 3D маски и муляжи). Многие исследователи тестируют разработанные решения подтверждения подлинности объекта на собственных базах данных, которые не являются общедоступными. Отсутствие общедоступных БД препятствует справедливой оценке и сравнению предлагаемых способов подтверждения подлинности распознаваемого объекта.

Способы подтверждения подлинности распознаваемого объекта (СППРО) разделяются в зависимости от вида воздействия на распознаваемый объект: способы с физическим воздействием (СФВ), с командным (СКВ) и без воздействия (СБВ). Оригинальная классификация СППРО представлена на рисунке 1.3.

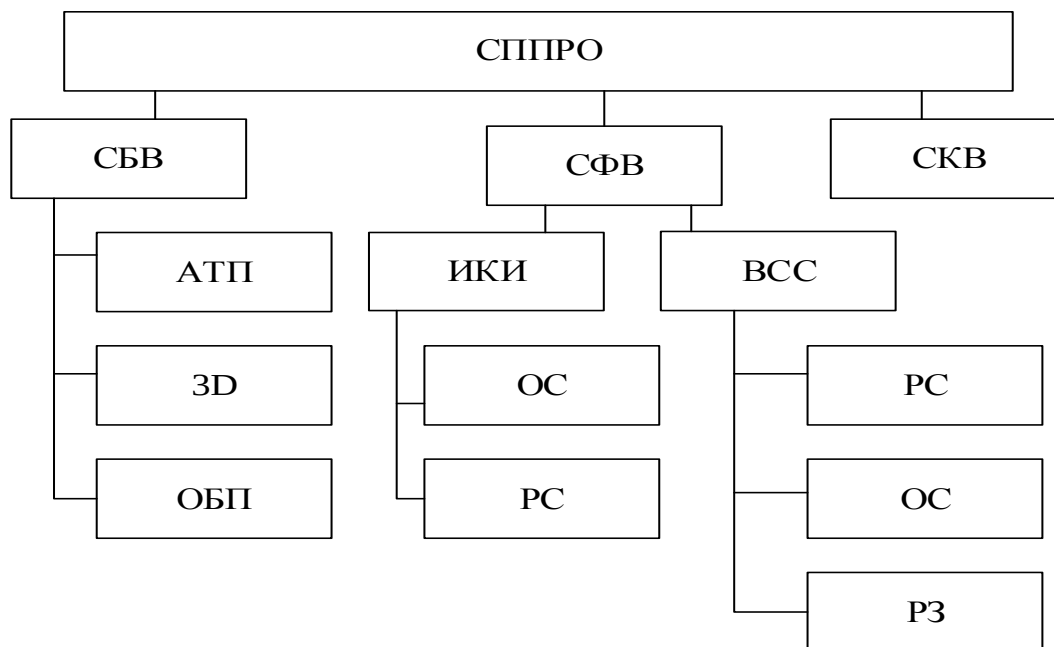


Рисунок 1.3 – Классификация способов подтверждения подлинности распознаваемого объекта

Для функционирования способов, основанных на командном воздействии, пользователю необходимо произвести некоторые действия в указанный системой защиты момент: произнести сгенерированный случайный текст, моргнуть или открыть рот, продемонстрировать различные эмоции и т.д.

Способы с физическим воздействием можно условно разделить на:

- способы, применяющие ИК излучение (ИКИ), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи и зрачков, рельефной структуры (РС) объекта и т.д.;
- способы, применяющие видимый спектр света (ВСС), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи и зрачков, реакции зрачков (РЗ), рельефной структуры (РС) объекта и т.д.

Способы без воздействия на объект разделяют на:

- способы, анализирующие текстурные признаки (АТП): локальные бинарные шаблоны (ЛБШ), гистограммы ориентированных градиентов и т.д.;
- способы, использующие построение 3D модели объекта с помощью: карт глубин, аффинного преобразования, сканера или видеокамер и т.д.;
- способы, использующие обнаруженные биофизические признаки (ОБП): движение глаз, моргание, мимика, движение головы относительно фона, кровеносные сосуды, термограмма и т.д.

Ниже представлены СППРО, не использующие воздействие на распознаваемый объект.

Существует целый ряд работ, в которых для обнаружения подмены используются различные текстурные признаки: ЛБШ и метод опорных векторов (процент правильного признания реального объекта составил не менее 91,2%, а процент пропуска злоумышленника – не более 0,2%) [71, 94], ЛБШ и искусственные нейронные сети (процент верного распознавания составил 97,5% на базе двумерных изображений) [108], вейвлеты Габора [94], гистограммы ориентированных градиентов [121], пространственно-временные дескрипторы [64, 70] и т.д. В работе [71] приведены результаты экспериментальных исследований различных СППРО, которые используют текстурные признаки. Исследования проводились на подготовленной авторами статьи БД, содержащей следующие типы атак: печатные фотографии, фото и видео, отображаемые на электронных экранах различных размеров. Доля ошибки достигла 15%, когда системы подтверждения подлинности сталкивались с широким набором типов спуфинг атак.

Другая категория методов сосредоточилась на обнаружении биофизических признаков распознаваемого объекта. В [68] представлен ряд методов, основанных на скорости моргания, анализе движения глаз, рта или головы относительно фона. Методы используют поле оптического потока для оценки движения. Ошибка распознавания составила не более 8,98%. Данный вид СППРО не устойчив к атакам, основанным на демонстрации фото и видео фрагментов с

экранов различных устройств. В [80] исследователи продемонстрировали возможность успешного взлома систем, использующих описанные СППРО.

Следующие СППРО основаны на анализе термограммы или рисунка поверхностных кровеносных сосудов распознаваемого объекта [67, 124]. Достоинство данных способов заключается в их относительной нечувствительности к изменению освещения. Подтверждение подлинности основано на том, что реальные объекты, в отличие от искусственных, излучают различный диапазон инфракрасного излучения или имеют поверхностные кровеносные сосуды.

В работе [93] выполняется восстановление 3D-модели лица с помощью аффинного преобразования, без необходимости вмешательства пользователя и дополнительных аппаратных средств. В [83] приведены результаты экспериментальных исследований существующих на рынке систем защиты, специализирующихся на противодействии спуфинг атак, с помощью построения 3D модели объекта. Исследователями была подготовлена новая БД из 26 предметов, включающая объекты 2D, 2.5D и 3D. Результаты экспериментов показали высокую уязвимость к спуфинг атак протестированных систем. Доля ошибочного принятия объекта за реальный составила не менее 8,4%.

Для функционирования представленных ниже СППРО требуется физическое воздействие на распознаваемый объект.

В работах [33, 34] представлен подход к обнаружению подмены на основе анализа спектральных характеристик отражения кожи лица человека. Представлен алгоритм защиты от спуфинг атак, в ходе которого с помощью сенсора формируют изображения распознаваемого объекта при различных длинах волн и анализируют спектральные характеристики поверхности объекта. Авторы работы говорят о результатах FAR (False Acceptance Rate) = 0,05, FRR (False Rejection Rate) = 0,09 на тестовой выборке, включающей изображения двадцати реальных человек, трёх силиконовых масок и трёх фотографий лица.

В работе [54] для подтверждения подлинности распознаваемого объекта используются изображения зрачков пользователя. В данном изобретении защита

от спуфинга основана на свойстве человеческого зрачка – сужаться при повышении интенсивности света. Чтобы узнать, получено ли изображение пользователя с глаза живого человека, а не с его муляжа, варьируют интенсивность освещения. Система защиты от спуфинга отслеживает реакцию зрачка на модуляцию освещения, поэтому время регистрации немного увеличивается.

В [98] описываются несколько различных способов защиты от спуфинга. В данном изобретении подтверждение подлинности распознаваемого объекта основано на свойстве человеческого зрачка – отражать проецируемое изображение. Представлен алгоритм подтверждения подлинности, в ходе которого одно или несколько изображений проецируются на экране компьютера. Изображения отразятся от зрачка пользователя и будут захвачены видеокамерой.

Для функционирования представленных ниже СППРО требуется командное воздействие на распознаваемый объект.

В работе [110] для подтверждения подлинности распознаваемого объекта используются изображения, полученные в обычном состоянии, и в состоянии, когда пользователю требуется выполнить предложенное системой действие. Набор действий не повторяется, действия могут быть следующими: открыть или закрыть глаза, закрыть один глаз, закрыть или открыть рот и т.д.

В [65] описан метод защиты от спуфинга с использованием изображения лица, записей голоса и жестов пользователя. В процессе защиты от спуфинга система анализирует перечисленные биометрические характеристики и формирует решение о предоставлении доступа к системе. Взаимодействие пользователя с системой осуществляется при помощи голоса и жестов, которая сопоставляет подаваемые команды с шаблонами из БД и предоставляет доступ к запрашиваемым ресурсам только при положительном результате проведенного сравнения.

В работе [60] пользователю необходимо смотреть в указанные на мониторе места, выставляемые случайным образом. Далее производится анализ траектории движения глаз. Разработчики метода пишут о 95% правильно распознанной подмены на БД, содержащей двумерные изображения распознаваемого объекта.

В работе [107] решение поставленной задачи достигается за счёт измерения движения и формы руки пользователя. В [97] для подтверждения подлинности объекта используется изображение языка. В данном изобретении подтверждение подлинности основано на свойстве человеческого языка – непроизвольно двигаться (извиваться), которое является естественным и убедительным доказательством того, что объект жив и может быть использован для распознавания.

Также возможно сочетание различных подходов, чтобы добиться более высоких результатов. В работе [89] пользователю предлагается сделать указанное системой движение, изменить мимику, открыть рот и т.д. Затем последовательность изображений с ИК камеры, после нормализации и удаления шума, анализируется. Сочетание нескольких подходов приведено и в работе [69]. Представленная система обнаружения подмены объекта использует видеокамеру, датчики движения и света. Исследователи получили следующие результаты: скорость распознавания составила 3 секунды, процент верного признания реального объекта составил 95-97%, а процент пропуска злоумышленника – 2-3%. Недостатком такого рода методов будет необходимость дополнительного оборудования или неудобство конечного пользователя (недружественный интерфейс системы подтверждения подлинности).

На данный момент отсутствуют технологии, которые способны обеспечить надёжное распознавание без использования специализированного оборудования. Для гарантии надёжного распознавания необходимо обеспечить высокую вероятность правильного распознавания изображений лиц, подтверждение подлинности распознаваемого объекта и возможность работы системы распознавания в реальном времени. Существующие технологии могут обеспечить перечисленные операции лишь по отдельности. По этой причине возникла необходимость в разработке соответствующей технологии и отдельных составляющих процесса распознавания.

Результаты анализа существующих способов подтверждения подлинности объекта являются основой для исследования во 2 и 3 разделах диссертации.

1.4 Выводы по 1 разделу

1. Приведены общая постановка и характеристика задач исследования. Обоснован выбор объекта распознавания – изображение лица (п. 1.1).

2. Определены факторы, существенно влияющие на вероятность правильного распознавания изображений лиц, такие, как поворот головы более чем на 10 градусов, макияж, изменение условий съёмки и т.д. Выполнен анализ путей повышения вероятности правильного распознавания человека по изображению лица (п. 1.1).

3. Выполнен сравнительный анализ эффективности основных подходов к распознаванию человека по изображению лица (метод главных компонент, метод сравнения эталонов, метод оптического потока, сравнение эластичных графов, скрытые марковские модели, нейросетевые методы) (п. 1.2).

4. Выполнен сравнительный анализ существующих способов подтверждения подлинности распознаваемого объекта. Анализ показал, что существующие решения для подтверждения подлинности распознаваемого объекта не отвечают современным требованиям по причине того, что имеют высокую стоимость, используют специализированное оборудование, неудобны для конечного пользователя или имеют недостаточную вероятность правильного обнаружения подмены распознаваемого объекта (п. 1.3).

5. Предложена новая классификация известных способов подтверждения подлинности распознаваемого объекта (п. 1.3). Существующие классификации не отражают все многообразие известных способов подтверждения подлинности и нуждаются в пересмотре и дополнении. Приведённая классификация позволяет выявить дальнейшие пути развития способов подтверждения подлинности распознаваемого объекта и позволяет ориентироваться в многообразии существующих технических решений.

2 Разработка технологии распознавания пользователей информационных ресурсов

Материал данного раздела посвящён разработке комплексного решения задачи распознавания пользователей информационных ресурсов на основе новой технологии и делится на четыре основные части. В первой части описаны требования к условиям формирования изображений лиц. Во второй части описана разработанная информационная технология распознавания изображений лиц, а также приведены экспериментальные исследования технологии. Для оценки результатов работы предложенной технологии используется ROC-анализ (Relative Operating Characteristic). Приведены методы, математические модели и алгоритмы преобразования, вычисления характерных признаков и распознавания исходных изображений, выбранные автором исследования с учётом достоинств и недостатков существующих методов. В третьей части решается задача создания метода, математической модели, алгоритма и устройства подтверждения подлинности распознаваемого объекта. Приведены возможные действия злоумышленников по взлому систем защиты от спуфинга и общая модель атак на биометрическую систему. Предложенное решение защиты отличается возможностью выявления случаев предъявления фотографий, видеозаписей и фотомасок, не применяя 3D-камер и алгоритмов стерео-реконструкции. Приведены результаты экспериментальных исследований. В последней части данного раздела представлена оригинальная технология распознавания пользователей информационных ресурсов.

2.1 Требования к формированию изображений лиц

В обязанности пользователя входит управление информационными системами различного назначения, зачастую имеющими биометрическую защиту. Как следствие, пользователь заинтересован в том, чтобы его распознали, избегая поворотов головы, перекрытия частей лица и т.п. Но в некоторых случаях избежать

отличий с эталонным изображением не удаётся. Такими отличиями могут быть: условия получения исходного изображения (расстояние от камеры до объекта, ракурс, условия освещения и т.д.), выражение лица (нейтральное, весёлое, грустное и т.д.), параметры исходного изображения (разрешение, гамма, контраст, степень зашумлённости и т.д.).

Учитывая перечисленные отличия, автоматическое распознавание лица пользователя может быть затруднено, если не сформулированы ограничения, налагаемые на условия подготовки изображений. Далее приведены требования к качеству изображений и условиям съёмки, разработанные в ГОСТ Р 19794-5–2006 [8]. Если на вход системы распознавания пользователей поступают изображения, не удовлетворяющие перечисленным ниже ограничениям, результат работы системы может быть некорректен.

Размер области, содержащей лицо пользователя на изображении. Требуется, чтобы длина и ширина области, содержащей лицо пользователя, была не меньше 100 пикселей, а расстояние между координатами центров зрачков должно быть больше 50 пикселей.

Требования к теням в области лица. В области лица от верхней части до нижней не должны присутствовать затемнения. Допускается наличие головного убора или шарфа, если предметы не закрывают и не затемняют область, содержащую лицо.

Положение лица. Координаты зрачков обязаны лежать на горизонтали перпендикулярно линии переносицы, лежащей на вертикали. Расстояние от нижнего края изображения до линии вертикали зрачков должно быть больше 50% и меньше 70% всей длины изображения.

Освещённость. При формировании изображения, объект необходимо равномерно освещать. Наличие какого-либо направленного освещения на изображении лица является критичным для распознавания. Необходимо избегать присутствия на изображении бликов, возникающих при использовании одного высокоинтенсивного источника освещения.

Выражение лица. Для успешного распознавания рекомендованы следующие выражения лица:

- улыбка отсутствует, глаза открыты не широко, рот закрыт;
- улыбка присутствует с сомкнутыми губами, рот закрыт, внутренняя часть рта или зубы не видны.

2.2 Распознавание изображений лиц

Разрабатываемая система распознавания должна включать представленные на рисунке 2.1 модули.

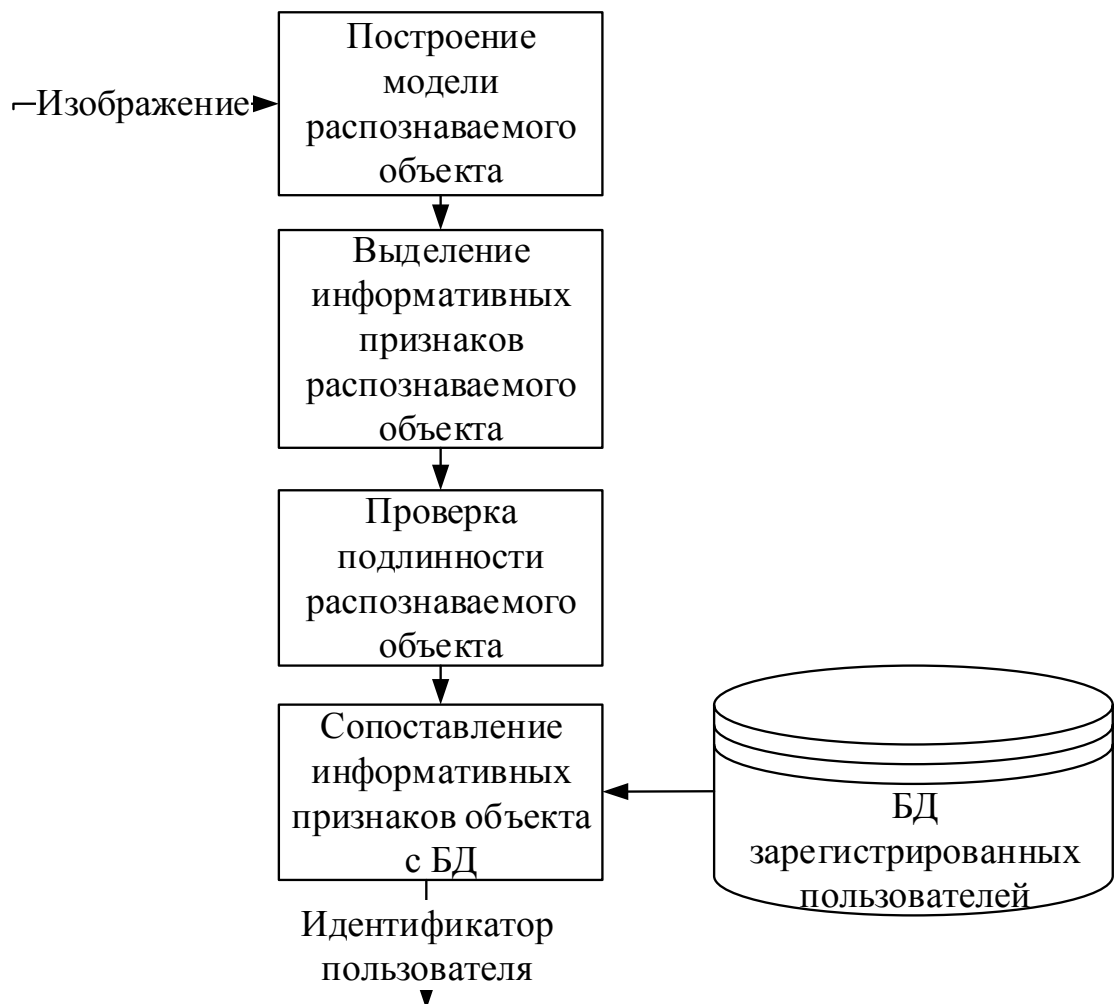


Рисунок 2.1 – Структура системы распознавания изображений лиц

Система распознавания должна включать следующие модули:

- модуль построения модели распознаваемого объекта, включающий поиск координат лица на изображении, локализацию информативной области, предобработку и нормализацию;
- модуль подтверждения подлинности распознаваемого объекта (алгоритмы подтверждения подлинности распознаваемого объекта путём отслеживания возможной подачи на вход системы распознавания фотографий или видеозаписей лица ранее зарегистрированного пользователя);
- модуль вычисления информативных признаков (главные компоненты, локальные бинарные шаблоны, градиент яркости, расстояния между антропометрическими точками и т.д.);
- модуль сопоставления информативных признаков исходного изображения с эталонным (скрытые Марковские модели, ИНС, различные метрики, такие, как хи-квадрат, коэффициенты корреляции, расстояние Бхаттачария и т.д.).

Ниже представлена формальная постановка задачи идентификации в общем виде, которая используется дальше в работе.

Пусть все множество изображений лиц $\Omega_0, \Omega_1, \dots, \Omega_{L-1}$ в БД делится на L классов, где каждый соответствует зарегистрированному человеку. Для каждого изображения вычисляется вектор признаков, состоящий из K значений:

$$\rho = (\rho_0, \rho_1, \dots, \rho_{K-1})^T, \quad (2.1)$$

где T – оператор транспонирования.

Идентификация – принятие решения о соотнесении некоторого входного вектора признаков $\bar{\rho}$ (изображения лица) определённому классу Ω_L . Входной объект считается принадлежащим классу Ω_L , если значение функции расстояния (или функции схожести) $d(\rho_l, \bar{\rho})$ для вектора признаков $\bar{\rho}$ является наибольшей:

$$d(\rho_l, \bar{\rho}) > d(\rho_j, \bar{\rho}), l \neq j, l, j = 0, 1, \dots, L - 1. \quad (2.2)$$

Дополнительно следует вычислять случаи ошибочного соотнесения входных векторов признаков $\bar{\rho}$, отсутствующих в БД, с зарегистрированными пользователями. Для этого значение функции расстояния $d(\rho_l, \bar{\rho})$ должно превышать заранее вычисленное пороговое значение τ_{ROC} :

$$d(\rho_l, \bar{\rho}) \geq \tau_{ROC}. \quad (2.3)$$

Процесс аутентификации отличается от идентификации тем, что заранее известно какому классу Ω_L соответствует входной вектор признаков $\bar{\rho}$. Задачей аутентификации является подтверждение подлинности входного объекта. Для этого значение функции расстояния $d(\rho_l, \bar{\rho})$ для класса Ω_L должна превышать заранее вычисленное пороговое значение τ_{ROC} (2.3).

Приведённая постановка задачи распознавания может быть найдена во многих публикациях, посвящённых распознаванию пользователей по изображению лица и моделированию информационных систем [29–31, 40, 53].

2.2.1 Поиск координат распознаваемого объекта на изображении

Для начала процесса распознавания необходимо определить координаты лица на изображении. Процесс обнаружения лица является первым шагом системы распознавания. Этот процесс определяет производительность системы, так как требует большего количества процессорного времени. Поиск координат распознаваемого объекта на изображении является трудоёмкой задачей из-за ряда факторов:

- детектор используется с различным освещением и положением человека;
- сложный фон создаёт дополнительные трудности для обнаружения лица;
- частичное перекрытие лица создаёт сложности для алгоритмов поиска лица, т.к. только часть объекта видна для обработки.

Для решения задачи поиска координат лица на изображении многие исследователи предложили различные подходы. Существует четыре группы методов обнаружения лица [122]. Автором был выбран метод Виолы-Джонса, обладающий высокой скоростью и достаточной эффективностью.

П. Виола и М. Джонс в 2001 году представили алгоритм поиска координат лица на изображении [116]. Разработанный метод показал результаты поиска координат лица на 15% лучше по сравнению с существующими аналогами. Досто-

инствами представленного метода являются высокая эффективность, возможность использования в реальном времени и общность, т.е. возможность детектирования разнообразных объектов. Алгоритм Виолы-Джонса осуществляется в два этапа:

- определяются признаки распознавания и вычисляются их значения;
- комбинируются наиболее информативные признаки с использованием алгоритма AdaBoost.

Для повышения скорости алгоритма Пол Виола и Майкл Джонс предложили использовать интегральное изображение, имеющее одинаковые размеры с рассматриваемым изображением, на котором производится поиск координат лица. Математическое выражение для определения интегрального изображения представлено ниже:

$$ii(x, y) = \sum_{i=0}^{x*y} i(x', y'), \quad (2.4)$$

где $ii(x, y)$ – значение i -го элемента интегрального изображения со следующими координатами (x, y) ; $i(x', y')$ – интенсивность пикселя рассматриваемого изображения с координатами (x', y') .

Интегральное изображение вычисляется независимо от размера или местоположения. В алгоритме Пола Виолы и Майкла Джонса используются признаки, подобные примитивам Хаара. Исследователи предложили использовать следующие виды признаков: двупрямоугольные, трёхпрямоугольные, диагональные. Признаки f_i помещают на изображение, сумма интенсивности пикселей, лежащих в белых областях, вычитается из суммы интенсивностей пикселей, лежащих в черных областях:

$$f_i = \sum_{i=0}^{y*x} r_{i,white} - \sum_{i=0}^{y*x} r_{i,black}, \quad (2.5)$$

где $\sum r_{i,white}$, $\sum r_{i,black}$ – суммы интенсивностей пикселей рассматриваемого признака.

В алгоритме Пола Виолы и Майкла Джонса для обучения классификатора используется алгоритм AdaBoost. AdaBoost способствует увеличению эффективности классификации, путём объединения слабых классификаторов и формирования сильнейшего классификатора. Ниже представлен алгоритм AdaBoost:

- Производится поиск «наилучшего» слабого классификатора. Выражение для этого классификатора с пороговым значением τ_c имеет вид:

$$w = \begin{cases} 1, & f_i \geq \tau_c; \\ -1, & f_i < \tau_c. \end{cases} \quad (2.6)$$

- Вычисляется «наилучший» сильный классификатор из фиксированного числа слабых классификаторов. Выражение для сильного классификатора выглядит следующим образом:

$$w = \begin{cases} 1, & \sum_{c=1}^c \alpha_c w_c \geq \frac{1}{2} \sum_{c=1}^c \alpha_c; \\ 0, & \sum_{c=1}^c \alpha_c w_c < \frac{1}{2} \sum_{c=1}^c \alpha_c, \end{cases} \quad (2.7)$$

$$\alpha_c = \log \frac{1}{\beta_c}, \quad (2.8)$$

где w_c – слабый классификатор; α_c, β_c – весовые коэффициенты слабого классификатора; c – номер текущего слабого классификатора, $c = \overline{1, C}$ C – количество слабых классификаторов.

Идея каскадов классификаторов заключается в построении меньших и более эффективных классификаторов для устранения негативных примеров и уменьшения времени вычисления. Каскады классификаторов рассчитываются для всех фрагментов изображения. В случае остановки фрагмента каким-либо классификатором фрагмент отбрасывают и последующие вычисление не производятся. Если фрагмент проходит первый этап, не требующий трудоёмких вычислений, фрагмент попадает на следующий этап, в котором выполняются более трудоёмкие вычисления. Для поиска координат лица на изображении требуется пройти все классификаторы в каскаде.

2.2.2 Локализация информативной области на изображении

В данном разделе представлен алгоритм численного метода построения модели распознаваемого объекта на основе активных моделей формы и обоснован его выбор. Метод предназначен для быстрой и точной локализации информативной области на изображениях пользователей.

Следующее действие после нахождения координат распознаваемого объекта – уточнение координат и точная локализация границ лица. Решение этой задачи предложили многие исследователи [28, 48]. Слабая контрастность, различные условия освещения и сильная деформация не позволяют использовать классические детекторы границ. Модели формы позволяют получить точное описание границ объекта при наличии приблизительных координат его положения. Первоначально модели формы применялись для работы с объектами, имеющими чётко выраженные границы (например, изображения печатных плат). С развитием методов построения моделей стало возможным применять модели для следующих задач: распознавание образов, анализа формы различных объектов на изображениях и т.д.

В 1992 году группа под руководством Тима Кутса [76] предложила метод построения статистических моделей формы (Statistical shape models). Статистическая модель формы содержит следующую информацию: взаимное расположение границ (контуров), расположение точек и информацию о форме. Статистическая модель формы невосприимчива к различиям в масштабе, изменению ракурса и смещениям. Статистическая модель формы строится по ряду размеченных изображений. Метки на изображении следует выбирать по следующим соответствиям характерных точек:

- углы;
- «Т» – образные пересечения линий;
- биологические особенности;
- точки вдоль границ объекта не столь выраженные, как предыдущие, но находящиеся на большом расстоянии между найденными точками.

В связи со сложностью поиска нужной координаты, метки на изображении наносятся в ручном (самим экспертом) или в полуавтоматическом режиме (эксперту необходимо уточнять координаты меток после использования какого-либо алгоритма поиска меток).

Прежде чем собрать статистическую модель, следует все данные привести в одну систему координат. Для компенсации несоответствия в масштабе, ракурсе и смещении между метками необходимо как можно лучше сопоставить между собой и нормализовать положения всех форм. Классическим решением выравнивания является «Прокрустов анализ» [74].

Множество меток формируется в виде матрицы $S = [s_1, s_2, \dots, s_m]$, где $s_m = [x_1, y_1, \dots, x_n, y_n]^T$ – положения точек без учета их взаимного расположения. Чтобы вычислить взаимное расположение, следует применить метод главных компонент. Для статистической модели формы воспользуемся следующим выражением:

$$s = s_0 + P_s b_s, \quad (2.9)$$

где s_0 – усреднённая по всем наборам обучающей выборки (усреднённая форма) форма; P_s – матрица главных компонент; b_s – параметры модели формы.

Выражение для статистической модели формы демонстрирует, что модель формы можно выразить как сумму усреднённой формы s_0 с совокупностью собственных форм, находящихся в матрице P_s . При изменении вектора параметров b_s производятся разного рода деформации для приведения формы к исходному изображению. Пределы возможного варьирования параметров следующие: $-3\sqrt{\lambda_s} \leq b_s \leq 3\sqrt{\lambda_s}$, где λ_s – дисперсия.

В 1995г. группа под руководством Тима Кутса предложила итеративный метод подстройки статистической модели к изображению под названием – «Активные модели формы» (Active Shape Models – ASM) [77]. Метод активно применяется для анализа изображений лиц и медицинских изображений. Для статистической модели итеративно подбираются: глобальное преобразование T (транспонирование, масштаб, поворот), положение каждой точки (локальное

уточнение) и критерии модели формы b_s . Преобразования подбираются таким образом, чтобы уменьшить ошибку сопоставления:

$$|X - T(s_0 + P_s b_s)|^2, \quad (2.10)$$

где X – профиль наилучшего сопоставления. Для определения ошибки сопоставления следует использовать расстояние Махаланобиса, в котором учитывается корреляция между переменными.

Алгоритм ASM включает следующие операции:

- **Шаг 1.** Производится поиск наилучших координат для каждой метки. Изначально ASM предложены для работы с изображениями, имеющими сильные края, поэтому наиболее простой способ – взять самый сильный край вдоль контура на изображении. Проводится расстояние фиксированной длины с центром в каждой точке, фактически берётся нормаль к контуру. Вычисляются яркости изображения на равных промежутках вдоль линии профиля. Вычисляется градиент и определяется новое положение как точка максимального градиента.
- **Шаг 2.** Производится проверка наиболее подходящего преобразования модели в новое состояние.
- **Шаг 3.** Обновляются параметры модели с использованием ошибки сопоставления между моделью и изображением (2.10).
- **Шаг 4.** Предыдущие этапы повторяются до достижения заданного значения ошибки сопоставления.

Свойства текстуры не менее важны, чем свойства формы. В 1998г. группа под руководством Тима Кутса предложила метод, учитывающий текстуру в контексте формы, под названием – «Активные Модели Внешнего Вида» (Active Appearance Models – AAM) [75].

Алгоритм ААМ включает следующие операции:

- **Шаг 1.** Строится активная модель формы.
- **Шаг 2.** Производится деление объекта на треугольники с вершинами в метках модели формы. Размеченная область извлекается из изображения.

- **Шаг 3.** Текстура трансформируется к усреднённой форме методом триангуляции.

- **Шаг 4.** Производится нормализация текстуры, компенсируя различные условия освещения.

Формируется матрица из столбцов, содержащих значения пикселей текстуры. Применяется метод МГК для матрицы текстуры. Для активной модели внешнего вида используется следующее выражение:

$$g = g_0 + P_g b_g, \quad (2.11)$$

где g_0 – текстура, усреднённая для всех реализаций обучающей выборки (усреднённая текстура); P_g – матрица главных компонент; b_g – параметры активной модели внешнего вида.

Чтобы корректно отображать деформации, требуется коррелировать модели формы и внешнего вида. В 2001г. группой под руководством Тима Кутса предложен метод объединения моделей. Алгоритм включает следующие операции:

- **Шаг 1.** Для всех моделей оцениваются b_s и b_g .
- **Шаг 2.** Производится построение вектора параметров объединённой модели:

$$v = \begin{pmatrix} W_s b_s \\ b_g \end{pmatrix}, \quad (2.12)$$

где W_s – диагональная матрица весов, уравнивающая вклад расстояний между моделью формы и моделью внешнего вида;

- **Шаг 3.** К каждому вектору s применяется метод главных компонент. Вектор объединённых параметров модели формы и модели текстуры выражается следующей формулой:

$$v = P_v b_v, \quad (2.13)$$

где

$$P_v = \begin{pmatrix} P_{vs} \\ P_{vg} \end{pmatrix} \quad (2.14)$$

– матрица главных компонент общей модели, P_{vs} соответствует длине вектора P_s , а P_{vg} соответствует длине вектора P_g .

- **Шаг 4.** Новые выражения для формы и текстуры имеют вид:

$$s = s_0 + W_s^{-1} P_s P_{vs} b_v, \quad (2.15)$$

$$g = g_0 + P_g P_{vg} b_v. \quad (2.16)$$

- **Шаг 5.** Взаимозависимые выражения для моделей формы и текстуры имеют вид:

$$s = s_0 + Q_s b_v, \quad (2.17)$$

$$g = g_0 + Q_g b_v, \quad (2.18)$$

$$Q_s = W_s^{-1} P_s P_{vs}, \quad (2.19)$$

$$Q_g = P_g P_{vg}. \quad (2.20)$$

Численный метод построения модели распознаваемого объекта (рисунок 2.2) состоит из ниже перечисленных операций. Производится построение активных моделей формы. Вычисляются координаты антропометрических точек, которые отмечены на рисунке 2.2,а. Выполняется триангуляция областей изображения с помощью вычисленных антропометрических точек. Производится отображение регионов изображения в соответствующие области формируемой текстуры (рисунок 2.2,б). На рисунке 2.2,в представлен результат описанного выше преобразования исходного изображения.

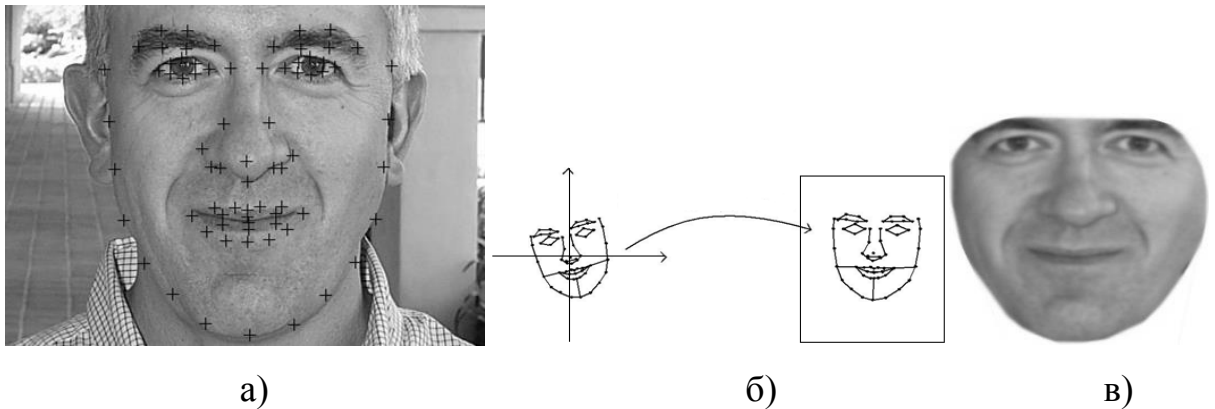


Рисунок 2.2 – Построение модели распознаваемого объекта:

- а) поиск антропометрических точек; б) перенос формируемой текстуры;
- в) результат построения модели распознаваемого объекта

2.2.3 Вычисление информативных признаков

По данным ряда исследований [61, 62] распознавание лиц с помощью ЛБШ обеспечивает требуемые результаты с точки зрения скорости работы и эффективности использования в процессе распознавания образов. ЛБШ доказали свою состоятельность в задачах детектирования и распознавания лиц, вследствие частичной инвариантности к условиям освещения, изменениям выражений лица и высокой скорости вычисления, что позволяет использовать ЛБШ в реальном масштабе времени. ЛБШ являются простыми, но очень эффективными, текстурными признаками. Указанные свойства достигаются за счёт того, что подсчёт ведётся не индивидуально для каждого пикселя, а используются окрестности.

Метод вычисления ЛБШ введён группой под руководством Т. Ojala [101]. Шаблон вычисляется в окрестности точки 3×3 , используя значение интенсивности центральной точки в качестве порогового значения. Если значение интенсивности рассматриваемого пикселя меньше центрального, то результатом сравнения будет 0, иначе – 1. В результате вычислений получается восьмиразрядный бинарный код, в общей сложности – 256 различных шаблонов.

В 2002 году группа под руководством Т. Ojala [102] представила метод ЛБШ в более общей форме. Отличием от оригинального метода, в котором использовалась окрестность точки 3×3 , является отсутствие ограничений на размер окрестности. Таким образом, количество пикселей и радиус окрестности варьировались. Для представления ЛБШ используется обозначение $LBP_{P,R}$, где P – количество рассматриваемых точек окрестности, R – радиус окрестности. Получим выражение для ЛБШ, суммируя пороговые различия интенсивностей:

$$LBP_{P,R}(x, y) = \sum_{i=0}^{P-1} s(g_i - g_c) 2^i, \quad (2.21)$$

где (x, y) – координаты центрального пикселя; i – номер рассматриваемого пикселя; g_c – значение интенсивности центральной точки; g_i – интенсивность в произвольной точке, выражение для $s(z)$ имеет вид:

$$s(z) = \begin{cases} 1, & z \geq 0; \\ 0, & z < 0. \end{cases}$$

Необходимо определить признаки, инвариантные к изменению ракурса и изменениям положения. Упомянутым требованиям отвечают равномерные коды ЛБШ [120]. Коды ЛБШ являются равномерными, если количество побитовых переходов не больше двух. Например, шаблоны 11111111 (нет переходов) и 11101111 (2 перехода) – равномерны, а шаблоны, имеющие более двух переходов, такие как шаблоны 111110100 (3 перехода) и 10101010 (7 переходов), нельзя назвать равномерными. Количество равномерных шаблонов равно $P(P - 1) + 2$, где P – количество рассматриваемых точек окрестности.

В 2008 году были предложены два новых усовершенствованных ЛБШ [62]: Three-Patch ЛБШ (рисунок 2.3,а) и Four-Patch ЛБШ (рисунок 2.3,б). Основное отличие предложенных ЛБШ от существующих в том, что сравниваются с помощью метрики (например, Хи-квадрат) фрагменты изображения, а не пиксели.

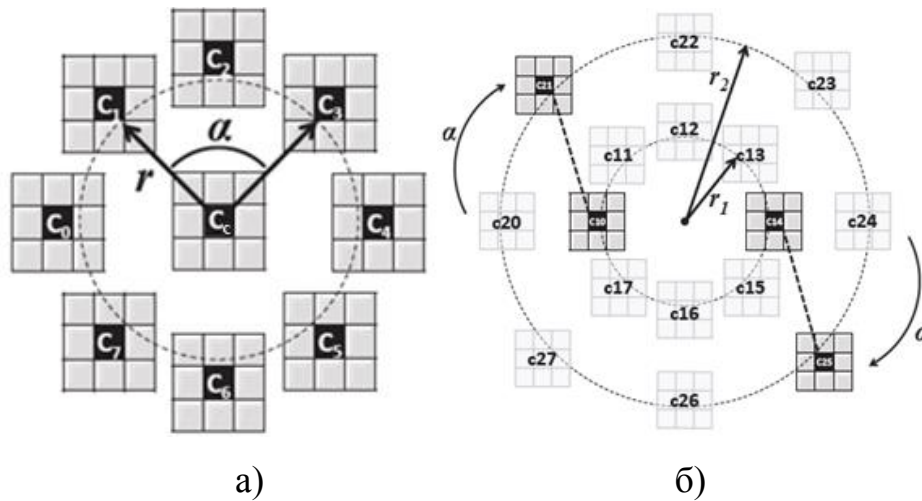


Рисунок 2.3 – Схемы построения информативных признаков: а) $TP_{8,1,2}$ для $P = 8, r = 1$ и $\alpha = 2$; б) $FP_{8,1,2,1}$ для $P = 8, r_1 = 1, r_2 = 2$ и $\alpha = 1$

Three-Patch ЛБШ вычисляется путём сравнения значений трёх фрагментов (рисунок 2.3,а). Алгоритм Three-Patch ЛБШ включает следующие шаги:

- **Шаг 1.** Фрагменты C_i и $C_{i+\alpha}$ сравниваются по некой метрике d со значением центрального фрагмента C_c , где α – число, определяющее второй фрагмент для сравнения.

- **Шаг 2.** Если окрестность C_i ближе по значениям к C_c , чем $C_{i+\alpha}$ к C_c , то $s(z) = 1$, иначе $s(z) = 0$.

- **Шаг 3.** Для каждого пикселя вычислить $TP_{P,R,\alpha}(x, y)$:

$$TP_{P,R,\alpha}(x, y) = \sum_{i=0}^{P-1} s(d(C_i, C_c) - d(C_{i+\alpha}, C_c))2^i, \quad (2.22)$$

$$s(z) = \begin{cases} 1, & z \geq \tau; \\ 0, & z < \tau. \end{cases}$$

На практике пороговое значение $\tau > 0$ (например, $\tau = 0,01$) для обеспечения стабильности в расчётах.

Шаблон Four-Patch ЛБШ вычисляется путём сравнения четырёх фрагментов (рисунок 2.3,б). Алгоритм Four-Patch ЛБШ включает следующие шаги:

- **Шаг 1.** Определяются 2 окружности фрагментов с радиусами R_1 и R_2 .
- **Шаг 2.** По некой метрике d попарно сравниваются фрагменты $C_{1,i} - C_{2,i+\alpha}$ и $C_{1,i+p/2} - C_{2,i+p/2+\alpha}$, где α – номер следующего фрагмента для сравнения.
- **Шаг 3.** Если первая пара фрагментов ближе по значениям друг к другу, чем вторая, то $s(z) = 1$, иначе $s(z) = 0$.
- **Шаг 4.** Для каждого пикселя вычислить $FP_{P,r_1,r_2,\alpha}(x, y)$:

$$FP_{P,r_1,r_2,\alpha}(x, y) = \sum_{i=0}^{P-1} s(d(C_{1,i}, C_{2,i+\alpha}) - d(C_{1,i+p/2}, C_{2,i+p/2+\alpha}))2^i. \quad (2.23)$$

Three-Patch ЛБШ и Four-Patch ЛБШ существенно улучшали результат применения признаков в распознавании и классификации изображений. По заявлению авторов [62], дальнейшие модификации и увеличение количества сравниваемых областей не принесли существенного улучшения результата.

В работе [62] описан метод применения ЛБШ для распознавания лиц. Алгоритм включает следующие операции:

- **Шаг 1.** Изображение разбивается на K регионов (рисунок 2.4,а). В каждом регионе к каждому пикселю изображения применяются ЛБШ операторы. Производится построение гистограммы, в которой каждому значению равномерного

ЛБШ соответствует свой столбец, а также один столбец для неравномерных ЛБШ. Количество столбцов гистограммы в одной области равно $P(P - 1) + 3$.

- **Шаг 2.** Гистограммы регионов изображения объекта объединяют в одну общую гистограмму. Количество столбцов в общей гистограмме равно $K(P(P - 1) + 3)$.

- **Шаг 3.** Степень сходства двух изображений I_0 и I_1 определяется сравнением их гистограмм $H_0(h, k)$ и $H_1(h, k)$ какой-либо метрикой (метрика Хи-квадрат):

$$d_{chi}(I_0, I_1) = \sum_{k=1}^K \sum_{h=1}^{P(P-1)+3} \frac{(H_0(h, k) - H_1(h, k))^2}{H_0(h, k) + H_1(h, k)}, \quad (2.24)$$

где h – рассматриваемый столбец гистограммы; k – текущий регион области лица.

Так как некоторые области лиц (например, область глаз) могут нести более важную информацию, чем другие области, к каждому региону для распознавания присваиваются веса в зависимости от важности региона. Выражение для метрики Хи-квадрат, с учётом присвоенного веса w_j области j , имеет вид:

$$d_{chi}(I_0, I_1) = \sum_{k=1}^K V_k \sum_{h=1}^{P(P-1)+3} \frac{(H_0(h, k) - H_1(h, k))^2}{H_0(h, k) + H_1(h, k)}. \quad (2.25)$$

Веса областей V_k подобранные эмпирическим путём, изображены на рисунке 2.4,б. Черные квадраты соответствуют весу 0, темно серые – 1, светло-серые – 2, белые – 4.

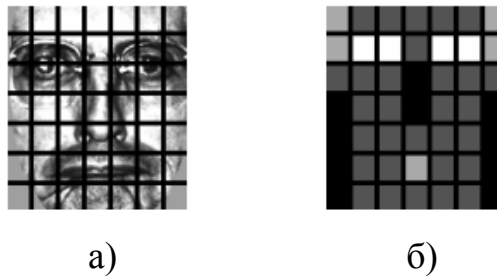


Рисунок 2.4 – Построение информативного признака: а) изображение лица, поделённое на области; б) разметка весов областей

2.2.4 Математическая модель, метод и алгоритм численного определения информативных признаков

На данный момент, помимо Three-Patch ЛБШ и Four-Patch ЛБШ, существуют альтернативные ЛБШ [100, 114]. Одним общим недостатком является вычислительная сложность алгоритмов. Автором диссертации разработан новый вид ЛБШ. Предложенный ЛБШ медианного пикселя (далее ЛБШМП, рисунок 2.5) ускоряет процесс вычисления признаков при сохранении высокой эффективности использования в процессе распознавания образов.

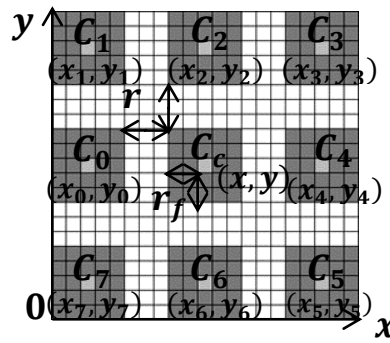


Рисунок 2.5 – Схема построения ЛБШМП: $P = 8$, $r = 3$, $P_f = 25$, $r_f = 2$

Выражение для ЛБШМП имеет вид:

$$M_{P,r,P_f,r_f}(x,y) = \sum_{i=0}^{P-1} 2^i \cdot s(z_i), \quad (2.26)$$

где i – номер фрагмента; (x, y) – координаты пикселя; $i = 0, 1, \dots, P - 1$; P – количество рассматриваемых фрагментов; r – радиус окрестности; P_f – количество пикселей во фрагменте; r_f – радиус фрагмента, а выражение s имеет вид:

$$s(z_i) = \begin{cases} 1, & z_i \geq \tau; \\ 0, & z_i < \tau, \end{cases}$$

где $z_i = \text{med}(C_i) - \text{med}(C_c)$ – разность медианных значений фрагментов C_i и C_c , схема нахождения которых изображена на рисунке 2.5; τ – пороговое значение, которое берётся больше нуля (например, $\tau = 0,01$). Каждый фрагмент состоит из значений яркостей следующих элементов:

$$C_i = \left(g(x_i - r_f, y_i - r_f), \dots g(x_i, y_i), \dots g(x_i + r_f, y_i + r_f) \right), \quad (2.27)$$

где x_i и y_i – координаты центрального пикселя фрагмента C_i :

$$x_i = \begin{cases} x - 2r_f - r - 1, i = 0, 1, 7; \\ x, i = 2, 6; \\ x + 2r_f + r + 1, i = 3, \dots, 5, \end{cases} \quad y_i = \begin{cases} y - 2r_f - r - 1, i = 1, \dots, 3; \\ y, i = 0, 4; \\ y + 2r_f + r + 1, i = 5, \dots, 7. \end{cases} \quad (2.28)$$

Чтобы найти медианное значение $med(C_i)$ фрагмента C_i , необходимо расположить элементы фрагмента в порядке возрастания значений яркости пикселей. Элемент с минимальным значением яркости будет находиться под номером 0, с максимальным значением – под номером, равным $4r_f \cdot (r_f + 1)$. Медианное значение $med(C_i)$ будет элементом под номером равным $2r_f \cdot (r_f + 1)$. Выражение для яркости пикселя, в соответствии с рекомендациями стандарта Федеральной комиссии связи (FCC) [105], имеет вид:

$$g(x, y) = 0,3 \cdot R_{x,y} + 0,59 \cdot G_{x,y} + 0,11 \cdot B_{x,y}, \quad (2.29)$$

где $R_{x,y}$, $G_{x,y}$ и $B_{x,y}$ – цветовые составляющие пикселя с координатами (x, y) .

Дальнейшим развитием ЛБШМП стало изменение формы построения шаблона и увеличение числа сравниваемых фрагментов (рисунок 2.6).

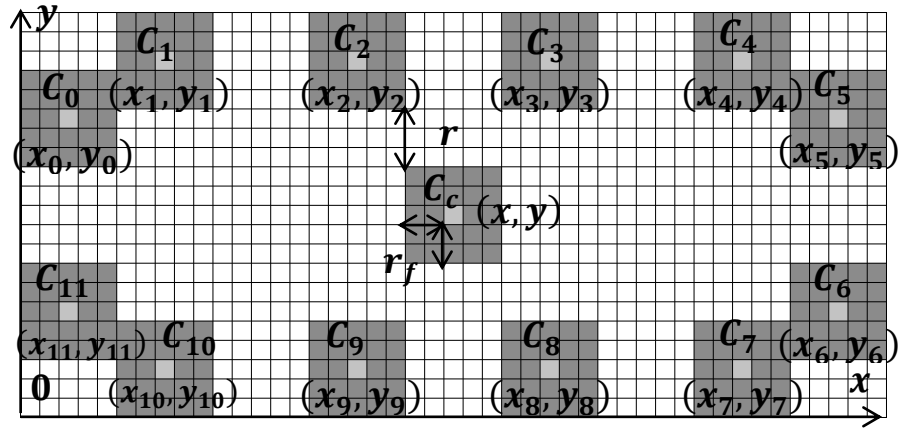


Рисунок 2.6 – Схема построения ЛБШМП, с увеличенным числом фрагментов

Тогда выражение (2.28) для координат центрального пикселя x_i и y_i фрагмента C_i будет иметь вид:

$$x_i = \begin{cases} x - 6r_f - 5 - r, i = 0, 11; \\ x - 4r_f - 4 - r, i = 1, 10; \\ x - 2r_f - 1, i = 2, 9; \\ x + 2r_f + 1, i = 3, 8; \\ x + 4r_f + 4 + r, i = 4, 7; \\ x + 6r_f + 5 + r, i = 5, 6, \end{cases} \quad y_i = \begin{cases} y + 2r_f + 1 + r, i = 1, \dots, 4; \\ y + 2r_f + 1, i = 0, 5; \\ y - 2r_f - 1, i = 6, 11; \\ y - 2r_f - 1 - r, i = 7, \dots, 10. \end{cases} \quad (2.30)$$

Для увеличения вероятности правильного распознавания добавлена внешняя структура сравнения. Подобно Four-Patch ЛБШ, изменился алгоритм сравнения – фрагменты сравниваются не с центральным фрагментом, а с внешней структурой. Результатом преобразований стала схема, представленная на рисунке 2.7. Указанная схема построения показала более высокие результаты по данным экспериментов. Количество и схема размещения фрагментов данной конструкции могут варьироваться в зависимости от требуемого результата.

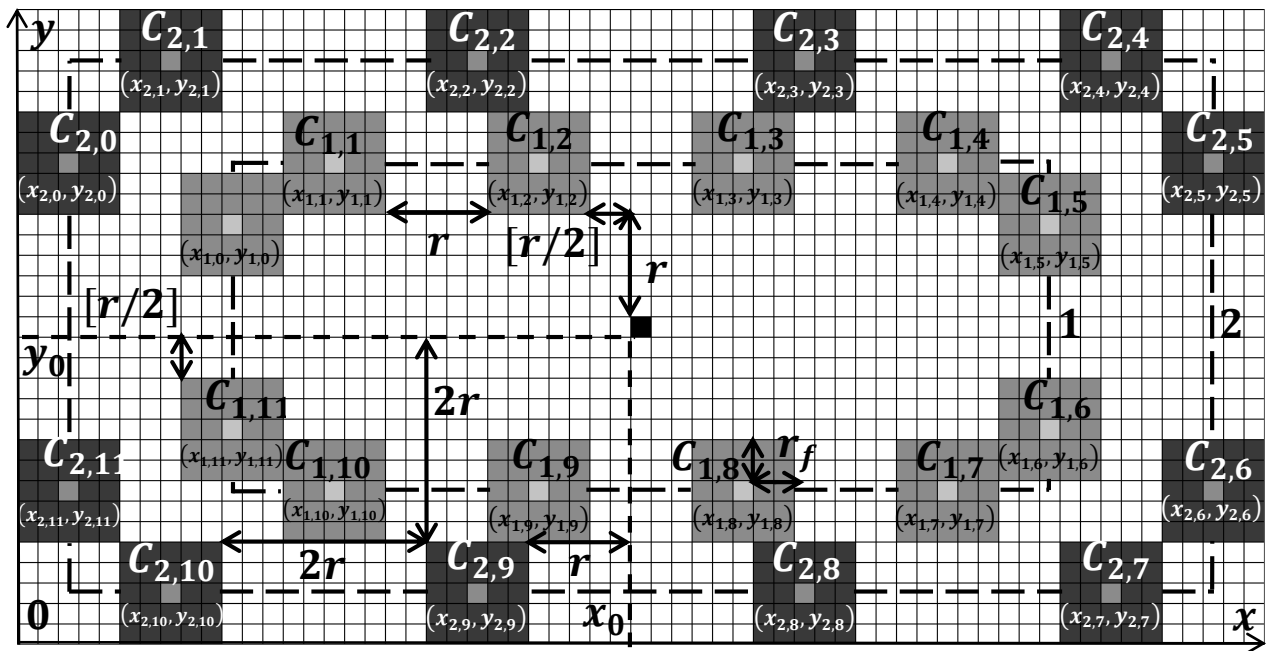


Рисунок 2.7 – Схема построения ЛБШМП: $P = 12$, $r = 5$, $P_f = 25$, $r_f = 2$

Гистограмма ЛБШ, построенная одновременно для всего изображения, содержит только текстурные особенности без информации о расположении кодов на изображении. Для учёта информации о расположении особенностей, изображение разбивается на K регионов (в первоначальном способе Т.Аhonen предлагается разделять изображение на 7×7 блоков), в каждой вычисляется гистограмма ЛБШ (рисунок 2.8,а, б, в). Вычисленные гистограммы для каждой области объединяются (рисунок 2.4) в одну общую (рисунок 2.8,г, д, е), при этом общая гистограмма содержит текстурные особенности и информацию о расположении кодовых комбинаций. Ниже приведены примеры комбинаций деления изображения лица на регионы и примеры гистограмм.

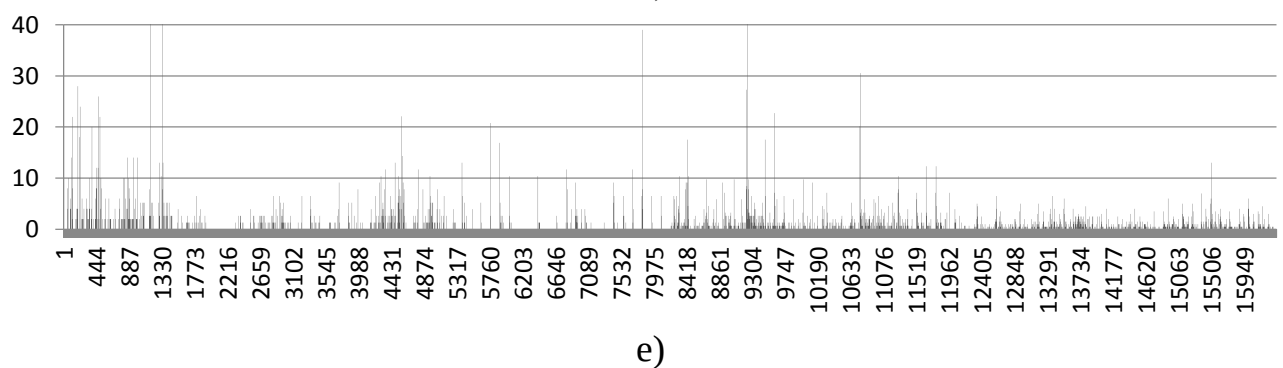
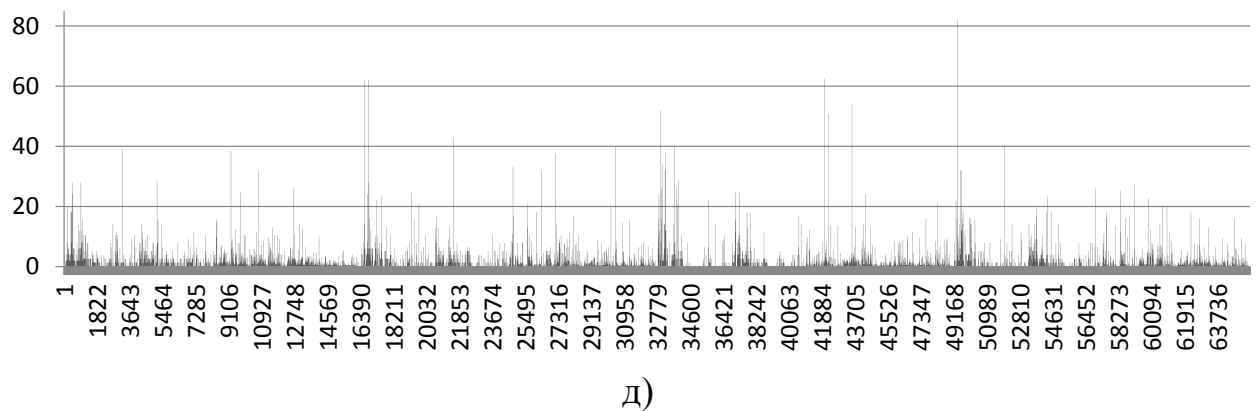
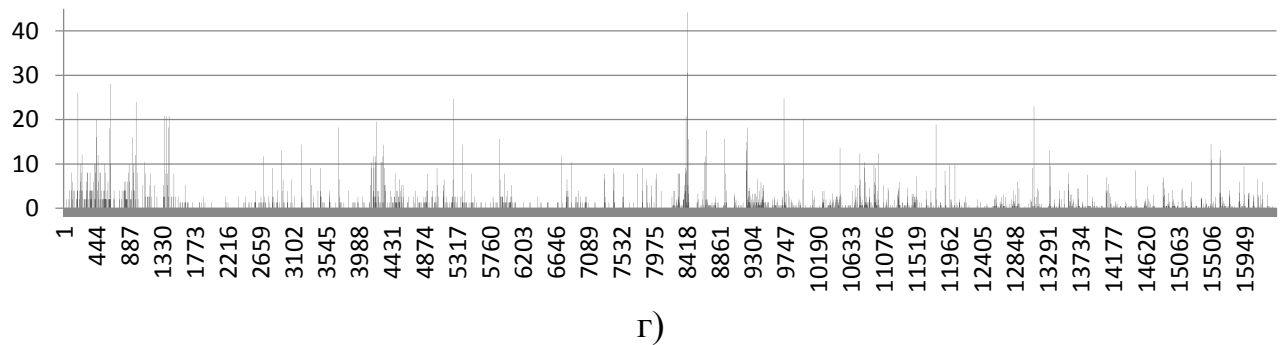
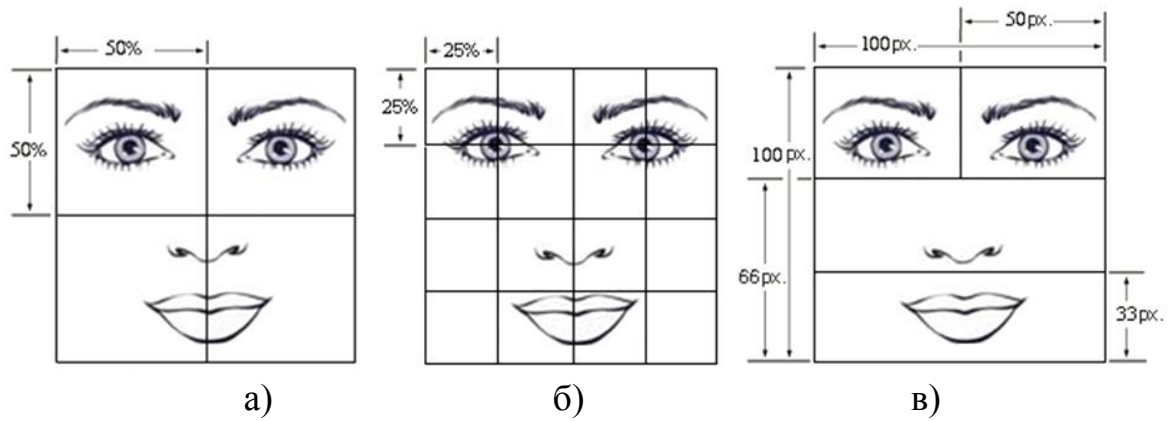


Рисунок 2.8 – Схемы деления изображения лица на регионы и гистограммы:

а) схема из 4 регионов; б) схема из 16 регионов; в) схема из 4 регионов, с регионами глаз, носа и рта; г) гистограмма из 4 регионов; д) гистограмма из 16 регионов; е) гистограмма из 4 регионов, с областями глаз, носа и рта

Таким образом, математическая модель информативного признака гистограммы кодов ЛБШМП (рисунок 2.7) будет иметь следующий вид:

$$H_{P,r,P_f,r_f}(h,k) = V_k \sum_{x=x_0}^{W_k-x_0-1} \sum_{y=y_0}^{H_k-y_0-1} f(M_{P,r,P_f,r_f}(x,y),h), \quad (2.31)$$

где P – количество рассматриваемых фрагментов; r – ближайшее расстояние от центрального пикселя с координатами x и y до первой окрестности фрагментов, $x = 0, 1, \dots, W_k - 1$, $y = 0, 1, \dots, H_k - 1$; P_f – количество рассматриваемых пикселей во фрагменте; r_f – размер фрагментов; h – номер столбца гистограммы, $h = 0, 1, \dots, 2^P - 1$; k – номер региона гистограммы, $k = 0, 1, \dots, K - 1$; K – количество регионов, разделяющих изображение; V_k – весовой коэффициент k -го региона; W_k и H_k – ширина и высота k -го региона; $x_0 = 3r + 6r_f + 3$ и $y_0 = 2r + 2r_f + 1$ – начальные координаты центрального пикселя. Функция f имеет вид:

$$f(M_{P,r,P_f,r_f}(x,y),h) = \begin{cases} 1, & M_{P,r,P_f,r_f}(x,y) = h; \\ 0, & M_{P,r,P_f,r_f}(x,y) \neq h, \end{cases} \quad (2.32)$$

где $M_{P,r,P_f,r_f}(x,y)$ – комбинация ЛБШМП, вычисляемая следующим образом:

$$M_{P,r,P_f,r_f}(x,y) = \sum_{i=0}^{P-1} s(z_i) 2^i, \quad (2.33)$$

$$s(z_i) = \begin{cases} 1, & z_i \geq \tau; \\ 0, & z_i < \tau, \end{cases}$$

где $z_i = med(C_{1,i}) - med(C_{2,i})$ – разность медианных значений фрагментов $C_{a,i} = C_{a,i}(x,y)$ (рисунок 2.7); a – порядковый номер окрестности, $a = \{1, 2\}$; i – номер фрагмента, $i = 0, 1, \dots, P - 1$; τ – пороговое значение берётся больше, чем ноль (например, $\tau = 0,01$). Элементы $C_{a,i}$ следует расположить в порядке возрастания значений яркости пикселей. Элемент с минимальным значением яркости находится под номером 0, с максимальным – под номером, равным $4r_f \cdot (r_f + 1)$. Медианным значением $med(C_{a,i})$ фрагмента $C_{a,i}$ является элемент под номером, равным $2r_f \cdot (r_f + 1)$. Фрагмент $C_{a,i}$ состоит из значений яркости $g(x,y)$:

$$C_{a,i} = (g(x_{a,i} - r_f, y_{a,i} - r_f), \dots, g(x_{a,i}, y_{a,i}), \dots, g(x_{a,i} + r_f, y_{a,i} + r_f)), \quad (2.34)$$

где $x_{a,i}$ и $y_{a,i}$ – координаты центрального пикселя фрагмента $C_{a,i}$:

$$x_{a,i} = \begin{cases} x - 5r_f - 3 - [3ra/2], i = 0, 11; \\ x - 3r_f - 2 - [3ra/2], i = 1, 10; \\ x - r_f - 1 - [ra/2], i = 2, 9; \\ x + r_f + 1 + [ra/2], i = 3, 8; \\ x + 3r_f + 2 + [3ra/2], i = 4, 7; \\ x + 5r_f + 3 + [3ra/2], i = 5, 6, \end{cases} \quad y_{a,i} = \begin{cases} y + r_f + 1 + ra, i = 1, \dots, 4; \\ y + r_f + 1 + [ra/2], i = 0, 5; \\ y - r_f - 1 - [ra/2], i = 6, 11; \\ y - r_f - 1 - ra, i = 7, \dots, 10, \end{cases} \quad (2.35)$$

где $[.]$ – оператор выделения целой части от вещественного выражения.

Алгоритм определения гистограмм ЛБШМП включает следующие шаги:

- **Шаг 1.** Изображение (рисунок 2.9,а) делится на регионы (рисунок 2.9,б). Для каждого региона, в зависимости от его ценности, устанавливаются значения веса V_k (например, для глаз $V_k = 1,2$, для носа $V_k = 1,1$, для рта $V_k = 1$).

- **Шаг 2.** Для каждого пикселя k -го региона вычисляется значение ЛБШМП. Определяется медианное значение каждого фрагмента окрестностей и вычисляется z_i . Если z_i меньше порогового значения τ , то результатом будет 0, иначе – 1. Результаты сравнения объединяются в одну кодовую комбинацию и переводятся в десятичную систему счисления.

- **Шаг 3.** Полученное значение на шаге 2 является номером столбца h гистограммы H_{P,r,P_f,r_f} , к значению которого добавляется 1.

- **Шаг 4.** Локальные гистограммы регионов (рисунок 2.9,в) объединяются в один общий информативный признак (рисунок 2.9,г) с учётом веса региона.

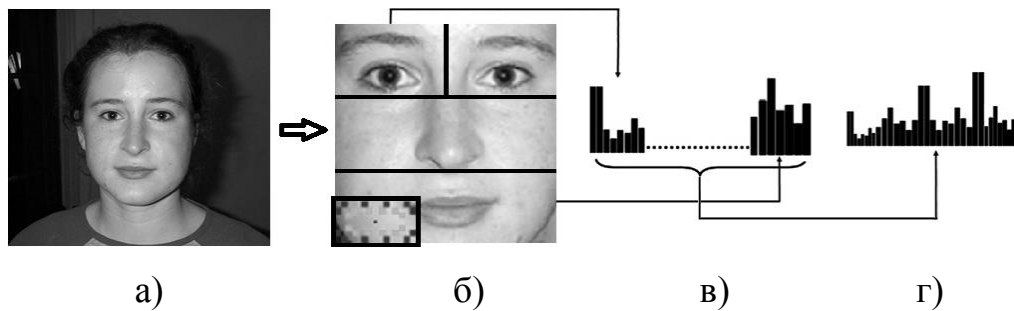


Рисунок 2.9 – Построение информативного признака: а) исходное изображение; б) изображение, разделённое на регионы; в) гистограммы регионов по отдельности; г) общая гистограмма

Для того чтобы наглядно увидеть реализацию информативных признаков, необходимо рассчитать для каждого пикселя значение ЛБШ, привести значения ЛБШ к общему множеству (0..256), установить цветовые составляющие красного, зелёного и голубого цвета пикселя равными значению ЛБШ этого пикселя. На рисунке 2.10 представлены иллюстрации к ЛБШМП.



а) б) в) г) д) е)

Рисунок 2.10 – Иллюстрации к ЛБШ: а) исходное изображение; б) представление – $LBP_{8,1}$; в) представление – $TP_{8,1,2}$; г) представление – $FP_{8,1,2,1}$; д) представление – $M_{8,1,8,1}$; е) представление – $M_{12,5,25,2}$

Использование данного информативного признака (рисунок 2.7) увеличивает долю верного распознавания на 7% на БД (таблица 2.2) и скорость работы в 2 раза по сравнению с Four-Patch ЛБШ. Ниже в таблице 2.1 приведены данные, позволяющие провести сравнительный анализ скоростных характеристик с аналогами. Алгоритмы выполнялись на изображении размером 100×100 пикселей. Сигнатуры методов вычисления гистограмм ЛБШМП приведены в приложении А – «Вычисление кодов ЛБШМП» и «Подготовка гистограммы изображения».

Таблица 2.1 – Скоростные характеристики информативных признаков

Информативный признак	Время выполнения
Three-Patch ЛБШ	107 мс
Four-Patch ЛБШ	124 мс
ЛБШМП	61 мс

В приложении А приведены результаты статистической обработки экспериментальных исследований различных комбинаций формы и размера информативного признака ЛБШМП (таблицы А1 и А2).

2.2.5 Функции расчёта расстояния

Как только для каждого изображения в БД подготовлены информативные признаки, производится процесс сопоставления входного изображения с эталонным из БД. Т. Ahonen и А. Hadid, в [63] предложили алгоритм хи-квадрат в качестве основной метрики для сравнения каждого входного изображения лица с БД. Как будет показано позже (рисунок 2.13), данная метрика не даёт удовлетворительных результатов.

Для распознавания исходного объекта применяются различные технологии, наиболее известные описаны в п. 1.2. Выбор способа сопоставления информативных признаков обусловлен используемым сценарием системы распознавания лиц. Сценарии распознавания возможны следующие:

- «1:N» – информативный признак исходного изображения сравнивается со всеми признаками в БД;
- «1:1» – информативный признак исходного изображения сравнивается с одним признаком в БД.

Сценарий «1:1» используется в процессе аутентификации для того, чтобы осуществить проверку подлинности исходного объекта. Сценарий «1:N» используется в процессе идентификации исходного изображения для присвоения идентификатора исходному объекту.

Для осуществления процессов аутентификации и идентификации в данной диссертационной работе принято использовать функции расстояния. Существует множество функций расстояния, ниже приведены некоторые из них [10]:

- расстояние Минковского;
- Евклидово расстояние;
- расстояние Манхэттена;
- расстояние Чебышева;
- расстояние Махаланобиса;
- коэффициент корреляции.

Автором диссертационной работы в роли информативного признака были выбраны гистограммы кодовых комбинаций ЛБШМП.

Ниже приведены наиболее подходящие метрики, предложенные Суэйн и Баллард в [112], для сопоставления гистограмм кодовых комбинаций.

Корреляция. Для оценки корреляции используется следующая формула:

$$d_{correl}(H_1, H_2) = \frac{\sum_{h=0}^{L_H} H'_1(h) \cdot H'_2(h)}{\sqrt{\sum_{h=0}^{L_H} H'^2_1(h) \cdot H'^2_2(h)}}, \quad (2.36)$$

где H_1, H_2 – исходная и эталонная гистограммы; h – номер столбца гистограммы; L_H – количество столбцов гистограммы; выражение для $H'(h)$ имеет вид:

$$H'(h) = H(h) - \frac{1}{L_H} \sum_{h=0}^{L_H} H(h).$$

При $d_{correl}(H_1, H_2) = 1$ можно говорить о полном совпадении сравниваемых признаков, при $d_{correl}(H_1, H_2) = -1$ – об абсолютном несовпадении.

Хи-квадрат. Выражение для расстояния хи-квадрат имеет вид:

$$d_{chi}(H_1, H_2) = \sum_{h=0}^{L_H} \frac{(H_1(h) - H_2(h))^2}{H_1(h) + H_2(h)}, \quad (2.37)$$

Для хи-квадрат при $d_{chi}(H_1, H_2) = 0$ можно говорить о полном совпадении, а абсолютное несовпадение зависит от количества столбцов в гистограммах.

Ядро пересечения гистограмм. Выражение для функции ядра пересечения гистограмм имеет вид:

$$d_{intersection}(H_1, H_2) = \sum_{h=0}^{L_H} \min(H_1(h), H_2(h)). \quad (2.38)$$

Для данной функции высокий результат указывает на совпадение с признаком эталонного объекта, а низкий – на абсолютное несовпадение. Если исходная и эталонная гистограммы нормализованы, то полное совпадение – 1, а абсолютное несовпадение – 0. Несколько изменив выражение (2.38), можно использовать нижеследующую метрику (2.39) в процессе аутентификации.

$$d_{intersection}(H_1, H_2) = 100\% \cdot \frac{\sum_{h=0}^{L_H} \min(H_1(h), H_2(h))}{\sum_{h=0}^{L_H} H_2(h)}. \quad (2.39)$$

Полное совпадение гистограмм – 100%, а абсолютное несовпадение – 0%.

Расстояние Бхаттачария. Выражение для вычисления расстояния Бхаттачария имеет вид:

$$d_{bhattacharyya}(H_1, H_2) = \sqrt{1 - \sum_{h=0}^{L_H} \frac{\sqrt{H_1(h) \cdot H_2(h)}}{\sqrt{\sum_{h=0}^{L_H} H_1(h) \cdot \sum_{h=0}^{L_H} H_2(h)}}}. \quad (2.40)$$

При использовании расстояния Бхаттачария низкие результаты означают хорошее совпадение, а высокие – плохое. Если исходная и эталонная гистограммы нормализованы, то полное совпадение – 0, а полное несовпадение – 1.

Расстояние Минковского. Для оценки расстояния Минковского используется нижеследующая формула.

$$d_{min}(H_1, H_2) = \left(\sum_{h=0}^{L_H} |H_1(h) - H_2(h)|^l \right)^{1/l}, \quad (2.41)$$

где l – порядок расстояния Минковского. Для данной метрики обязательно выполнение неравенства $l \geq 1$. Низкое значение $d_{min}(H_1, H_2)$ означает полное совпадение, а высокое – абсолютное несовпадение.

Для некоторых метрик важно, чтобы значения входных данных были нормализованы. Процесс нормализации производится по следующей формуле:

$$norm(H(h)) = \frac{H(h) - \min H}{\max H - \min H}, \quad (2.42)$$

где $norm(H(h))$ – нормализованное значение объекта гистограммы $H(h)$, а $\max H$ и $\min H$ – максимальное и минимальное значения гистограммы. Сигнатура метода нормализации и центрирования приведена в приложении А – «Нормализация и центрирование гистограммы».

Сигнатура общего метода для всех функций расстояния приведена в приложении А – «Вычисление значения функции расстояния».

2.2.6 Технология распознавания изображений лиц и экспериментальные исследования

На рисунке 2.11 изображена оригинальная информационная технология распознавания изображений лиц.



Рисунок 2.11 – Технология распознавания изображений лиц

Технология состоит из 4 модулей: выделение области, содержащей лицо, локализация информативной области на изображении, вычисление информативных признаков и сопоставление признаков с БД изображений лиц зарегистрированных пользователей. Модуль локализации информативной области (п. 2.2.2) содержит в себе такие операции, как построение активной модели внешнего вида, поиск антропометрических точек лица, перенос регионов исходного изображения в соответствующие области формируемой текстуры, применение различных фильтров к полученной текстуре. Модуль выделения информативных признаков содержит две операции: вычисление кодов ЛБШМП (п. 2.2.4), генерация и нормализация гистограммы кодов ЛБШМП. Следующий модуль включает: операцию хранения признаков в БД и операцию сопоставления признаков исходного изображения с базой лиц. Критерием распознавания изображений является превышение эмпирически установленного порога значением функции расстояния. В данной работе в качестве метрики сравнения была выбрана функция ядра пересечения гистограмм (п. 2.2.5). Для осуществления процесса идентификации используется выражение (2.38), а для аутентификации – выражение (2.39).

Чтобы эффективно оценить производительность и вероятность правильного распознавания на каждом этапе, модули тестировались на БД (таблица 2.2), полностью включающей изображения баз Калифорнийского технологического института [117], The Indian Face Database [87], The FEI Face Database [113] и выборочно FERET [104].

Таблица 2.2 – Изображения лиц, используемые для проведения экспериментальных исследований

	Тестовая выборка	В базе данных
Зарегистрированные пользователи	2000 изображений, 200 человек	400 изображений, 200 человек
Незарегистрированные пользователи	400 изображений различных лиц	

Экспериментальные исследования информативного признака выполнены на основе БД, содержащей 400 изображений лиц 200 человек, по 2 на каждого зарегистрированного пользователя, и тестовой выборки, содержащей 2400 различных изображений лиц пользователей. Изображения пользователей подбирались в соответствии с заявленными требованиями в пункте 2.1. Выборка для каждого пользователя включает изображения с разными выражениями лица и при различных условиях освещения. Ниже (рисунок 2.12) представлены примеры изображений, содержащихся в БД, используемой для получения экспериментальных результатов.



Рисунок 2.12 – Пример изображений лиц экспериментальной БД

Для оценки эффективности систем распознавания традиционно используется ROC-анализ. ROC-анализ впервые упомянут в 1966 году [84] для повышения качества классификации объектов противника. Далее ROC-анализ стал использоваться в таких направлениях, как медицина, радиолокация и т.д. ROC-анализ позволяет оценить вероятность правильного распознавания и является визуализацией компромисса между следующими характеристиками:

- результаты классификации положительные и истинные значения положительные – истинно положительные случаи, TP (True Positives);
- результаты классификации отрицательные и истинные значения отрицательные – истинно отрицательные случаи, TN (True Negatives);

- результаты классификации положительные, истинные значения отрицательные – ложно положительные случаи, FP (False Positives);
- результаты классификации отрицательные, истинные значения положительные – ложно отрицательные случаи, FN (False Negatives).

Количество истинно верных случаев $TP + TN$, а истинно ложных $FP + FN$. После проведения эксперимента, подав на вход системе тестовую выборку, необходимо рассчитать процент случаев выдачи доступа зарегистрированному пользователю (TPR (True Positives Rate) – истинно положительные случаи) и процент случаев выдачи доступа к системе незарегистрированному пользователю (FPR (False Positives Rate) – ложно положительные случаи):

$$TPR = \frac{TP}{TP + FN} \cdot 100\%, \quad (2.43)$$

$$FPR = \frac{FP}{TN + FP} \cdot 100\%. \quad (2.44)$$

Для построения ROC-кривой необходимо рассчитать TPR и FPR : по оси ординат откладывается TPR , по оси абсцисс – FPR . Первым выполняется процесс расчёта информативных признаков изображений, содержащихся в обучающей выборке. После запускается экспериментальный процесс, в ходе которого система распознавания лиц идентифицирует каждое изображение из тестовой выборки. Каждый информативный признак система распознавания сопоставляет с признаками изображений обучающей выборки. Полученные результаты являются основой для построения ROC-кривой.

На рисунках 2.13 и 2.14 представлены результаты экспериментальных исследований системы распознавания пользователей. В роли информативных признаков использовались гистограммы на основе ЛБШМП (рисунок 2.7), Four-Patch ЛБШ (п. 2.2.3), Three-Patch ЛБШ (п. 2.2.3), GLBP (Gradient local binary patterns), ЛБШ (п. 2.2.3), яркости пикселей, LGBP (Local Gabor binary pattern) и HOG (Histogram of oriented gradients). Для сопоставления информативных признаков применялась функция ядра пересечения гистограмм (п. 2.2.5).

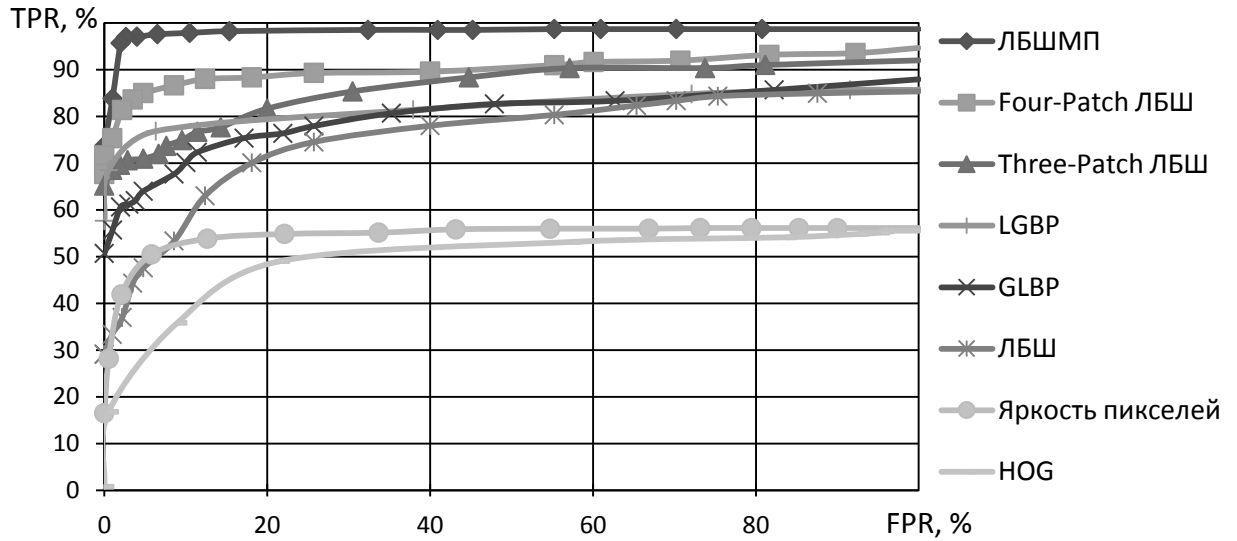


Рисунок 2.13 – Результаты экспериментальных исследований системы распознавания лиц

Визуальное сравнение ROC-кривых не является оптимальным и не всегда удаётся верно определить наилучший способ распознавания. Основным критерием для выбора наилучшего алгоритма является сравнение площади под ROC-кривыми – AUC (Area Under Curve). Выражение для AUC имеет вид:

$$AUC = \sum_{n=1}^N \left[\frac{TPR_{n+1} + TPR_n}{2} \right] \cdot (FPR_{n+1} - FPR_n), \quad (2.45)$$

где n – текущая точка на графике; N – количество аппроксимированных точек на графике, полученных с вариацией порогового значения τ_{ROC} .

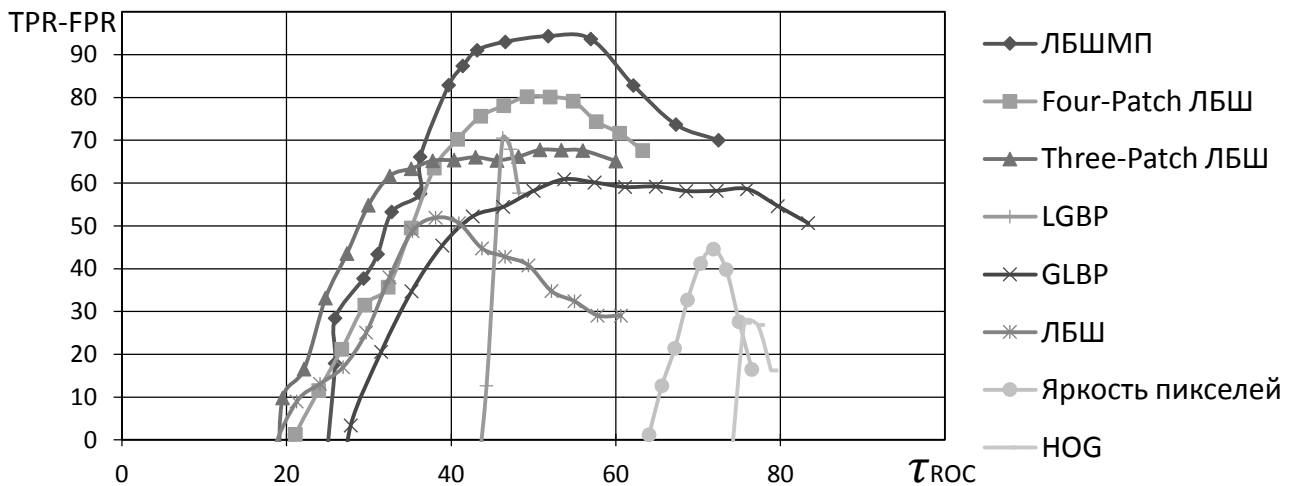


Рисунок 2.14 – Выбор порогового значения τ_{ROC} .

Наилучшим является информативный признак с наибольшим значением AUC. В таблице представлены значения площадей под кривой ROC-кривых (рисунок 2.13). Значение $AUC = 0,981$ (таблица 2.3) для кривой гистограммы кодов ЛБШМП является наибольшим среди кривых рисунка 2.13.

Таблица 2.3 – Характеристика AUC для системы распознавания лиц с различными информативными признаками

Информативный признак	AUC
ЛБШМП	0,981
Four-Patch ЛБШ	0,902
Three-Patch ЛБШ	0,861
LGBP	0,817
ЛБШ градиента	0,801
ЛБШ	0,757
Яркость пикселей	0,545
HOG	0,489

Дополнительной задачей является определение наилучшего значения порога τ_{ROC} на графике с изображением ROC-кривой (рисунки 2.13 и 2.14). Варьируя значение порога τ_{ROC} , можно управлять долей правильного распознавания. При уменьшении значения порога уменьшается количество случаев верного распознавания, а при увеличении возрастает. Значение порога τ_{ROC} выбирается таким, при котором количество случаев верного распознавания наибольшее. Для нахождения порогового значения τ_{ROC} необходимо вычислить на графике точку отсечения (optimal cut off value) и сопоставить ей пороговое значение из тестовой выборки следующим образом:

$$cut_off = \max(TPR_n - FPR_n). \quad (2.46)$$

Эффективным значением порога для признака ЛБШМП на рисунке 2.13 является значение 7450. При указанном значении процент случаев выдачи до-

стуга зарегистрированному пользователю не менее 97%, а процент выдачи доступа человеку, не имеющему допуск, не более 2%. Ниже в таблице 2.4 представлены некоторые типичные примеры нормализованных изображений лиц.

Таблица 2.4 – Примеры нормализованных изображений лиц

Параметр	Оригинал	Сильное освеще- ние	Сильное освеще- ние + улыбка	Сильный боковой дневной свет	Слабый свет	Закрытые глаза + улыбка
Изображе- ние						
Расстоя- ние до эталона	-	7568	7555	7465	7494	7480

На рисунке 2.15 представлены результаты использования технологии (рисунок 2.11) в процессе аутентификации. Для сравнения информативных признаков используется метрика (2.39). Высота столбца гистограммы равна количеству экспериментов со значением метрики равной номеру столбца. Учитывая данные экспериментов, следует выбрать порог τ_{ROC} , равный 18%.

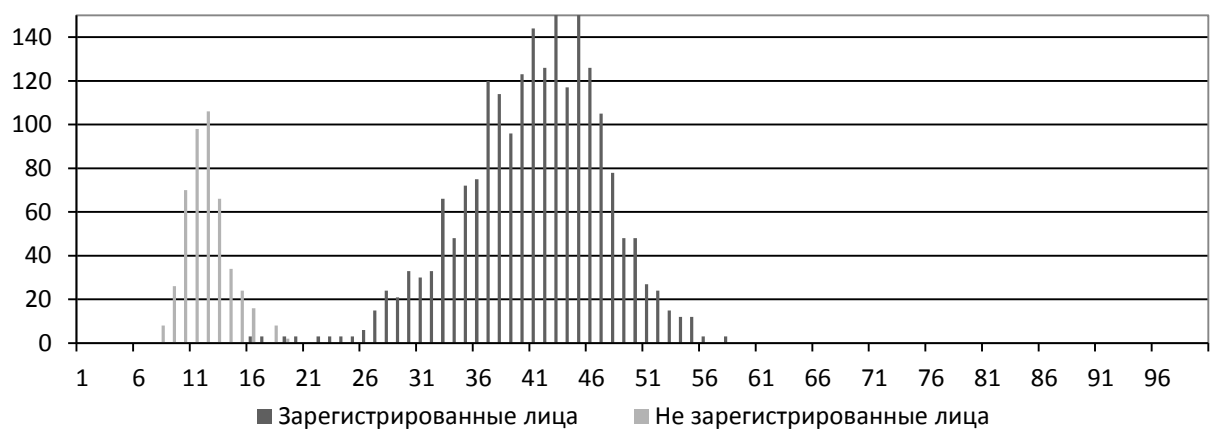


Рисунок 2.15 – Результаты аутентификации пользователей

2.3 Подтверждение подлинности распознаваемого объекта

Несмотря на значительный прогресс, связанный с разработкой новых и повышением эффективности существующих алгоритмов распознавания лиц, подобные системы все ещё подвержены уязвимостям в виду возможной подмены распознаваемого лица на фотографию или фотомаску. Системы контроля в большей степени нацелены на распознавание лица пользователя и не защищают от подмены распознаваемого объекта. В [80] авторы продемонстрировали, успешный взлом коммерческих систем распознавания лиц, используя фотографию или видеозапись зарегистрированного пользователя. Системы биометрического распознавания нуждаются во внедрении эффективных способов подтверждения подлинности распознаваемого объекта.

В публикациях [71, 72, 82, 86, 94] и пункте 1.3 описан ряд подходов, используемых исследователями для подтверждения подлинности распознаваемого объекта. Однако их существенными недостатками являются высокая вычислительная сложность, неудобство конечного пользователя, использование специализированного оборудования или отсутствие защиты перед использованием злоумышленниками фотографий, видеозаписей или фотомасок лица зарегистрированного пользователя.

В процессе исследований были разработаны оригинальные метод, математическая модель и алгоритм подтверждения подлинности распознаваемого объекта. Метод подтверждения подлинности относится к классам, использующим воздействие на пользователя (классификация представлена в пункте 1.3). Предложенное решение не использует специализированное оборудование, что является преимуществом по сравнению с аналогами из данного класса, удобнее для конечного пользователя и может быть легко интегрирован в существующие системы распознавания лиц. Метод, математическая модель и алгоритм найдут применение в системах распознавания изображений лиц человека в качестве самостоятельного решения или в виде дополнительного средства предотвращения спуфинг атак.

2.3.1 Модель атак на биометрическую систему

При разработке методов защиты биометрических систем распознавания пользователей необходимо определить все возможные виды угроз и описать модель атак. На данный момент уже составлены модели атак на различные биометрические системы [47, 106]. В данном пункте описана модель атак на системы распознавания пользователей по изображению лица. Определены девять наиболее уязвимых мест для атак злоумышленников в общей схеме биометрической системы, показанной на рисунке 2.16.

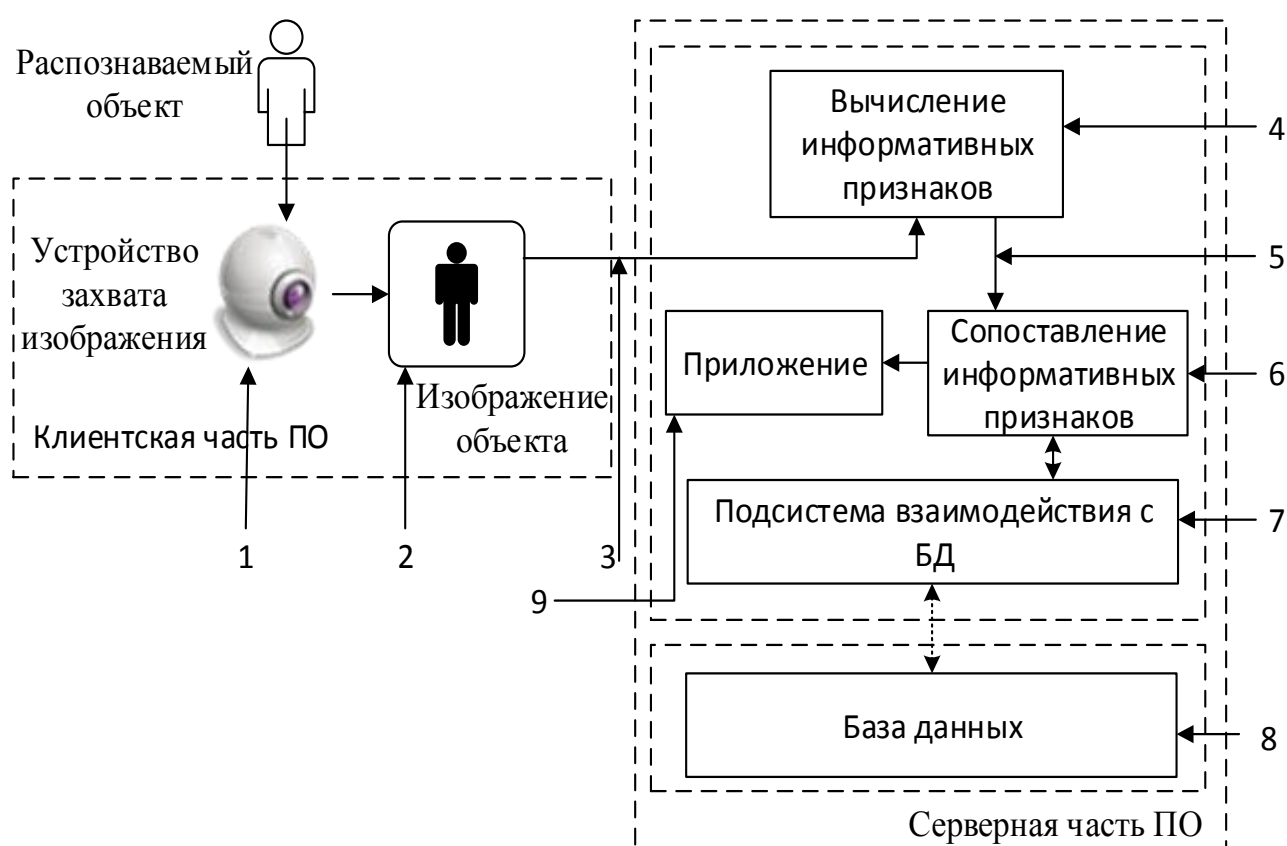


Рисунок 2.16 – Общая схема биометрической системы распознавания пользователей с обозначенными атаками

Для осуществления успешных атак на системы биометрического распознавания злоумышленник должен обладать навыками в различных специализированных областях, а также иметь информацию о изъянах в оборудовании и аппаратной реализации, структуре и способе организации базы данных, методах расчёта и сопоставления информативных признаков, о подсистеме взаимодействия

с базой данных и о других моделях и методах, заложенных в реализованную систему биометрического распознавания [47]. Возможными целями злоумышленника могут являться:

- нелегальный доступ одного или нескольких незарегистрированных пользователей к охраняемой информации или на объекты предприятия;
- запрет в доступе зарегистрированному пользователю;
- полный отказ в работе всей системы биометрического распознавания.

На рисунке 2.16 приведены места для возможных атак на систему распознавания по изображению лица, которые также могут быть применены и для других существующих биометрических систем. Цифры на рисунке 2.16 соответствуют пунктам в нижеследующем списке

1. *Устройство захвата изображения.* Представление устройству захвата поддельных биометрических данных. Для различных систем биометрического распознавания используют такие объекты, как искусственный палец, копия подписи, маска лица зарегистрированного пользователя и т.д.

2. *Канал связи между устройством захвата изображения и клиентской частью биометрической системы.* Замена сигнала, полученного с устройства захвата изображения, и передача для дальнейшей обработки в клиентскую часть биометрической системы.

3. *Канал связи между клиентской и серверной частями системы биометрического распознавания.* Для совершения атаки поддельная версия сигнала, подготовленная злоумышленником, передаётся в систему биометрического распознавания, минуя устройство захвата изображения и клиентскую часть программного обеспечения.

4. *Модуль вычисления информативных признаков.* Атака производится на модуль вычисления информативных признаков таким образом, чтобы модуль генерировал информативные признаки, предварительно выбранные злоумышленником.

5. *Канал передачи информативных признаков.* Результат работы модуля вычисления информативных признаков подменяются злоумышленником (предполагается, что метод вычисления признаков известен злоумышленнику). Данный вид атаки актуален в случае, если информативный признак передаётся удалённо.

6. *Модуль сопоставления информативных признаков.* Модуль сопоставления информативных признаков повреждается таким образом, чтобы формировать заранее выбранные злоумышленником оценки соответствия.

7. *Канал связи и подсистема взаимодействия с базой данных.* Целью данной атаки является перехват и модификация информативных признаков, полученных от базы данных через канал связи и подсистему взаимодействия.

8. *Элемент базы данных, содержащий информативные признаки.* Злоумышленником модифицируется один или несколько элементов в базе данных. Подобная модификация может привести либо к ошибочной выдаче доступа к системе злоумышленнику, либо к отказу в доступе зарегистрированному пользователю.

9. *Приложение.* Производится подмена окончательного решения о выдаче доступа пользователю к системе. Это означает, что система распознавания была полностью отключена, даже если база информативных признаков и система распознавания образов находятся в работоспособном состоянии.

Все выше перечисленные атаки, кроме атаки на устройство захвата изображения, являются общими для всех биометрических систем. Для защиты систем биометрического распознавания от подобных атак необходимо использовать методы шифрования и цифрового кодирования. Наибольшую угрозу для биометрических систем, использующих изображение лица в роли объекта распознавания, представляют атаки на устройство захвата изображений (спуфинг атаки). Злоумышленник имеет непосредственный доступ к видеокамере, а использовать методы цифрового кодирования и шифрования не представляется возможным. По этой причине необходимо более подробно остановиться на спуфинг атаках. В следующем пункте данного раздела представлены возможные виды атак на устройство захвата изображения.

2.3.2 Постановка задачи подтверждения подлинности распознаваемого объекта

В отличие от систем, где требуется дополнительное оборудование (распознавание по пальцу и др.), при распознавании человека по изображению лица очень легко создать копию распознаваемого объекта. Все, что необходимо, это фотография человека, которую легко можно обнаружить в интернете или сфотографировать пользователя на расстоянии. Одной из задач исследования является детектирование подмены представленного видеокамере объекта. Данная задача является не всегда лёгкой даже для человека. Решение должно обладать низкой вычислительной сложностью и высокой вероятностью верного обнаружения подмены распознаваемого объекта без использования дополнительного специализированного оборудования. В зависимости от направленности биометрической системы, спуфинг атаки могут иметь различные уровни сложности. В таблице 2.5 рассмотрены возможные виды угроз и меры защиты от подмены распознаваемого объекта.

В соответствии с приведёнными в таблице 2.5 угрозами и представленными мерами защиты, решение задачи подтверждения подлинности распознаваемого объекта должно содержать следующие действия:

- Формирование серии изображений объекта с различной интенсивностью освещения объекта в случайные моменты времени.
- Анализ изображений распознаваемого объекта с различной интенсивностью освещения. Анализ следует производить после проведения всех подготовительных операций по подготовке серии изображений, чтобы сократить время формирования решения о подмене. Тем самым предотвратить возможность предъявления сенсору подложных объектов.
- Оценка биометрической активности объекта, для обнаружения случаев предъявления 3D муляжа лица зарегистрированного человека.

В данном исследовании не рассматриваются такие виды атак, как грим или силиконовая маска.

Таблица 2.5 – Виды угроз и меры защиты от подмены объекта

Угроза	Описания	Мера защиты
Фото	Злоумышленник предъявляет видеокамере распечатанные фотографии высокого разрешения, либо цифровые фотографии с экрана какого-либо устройства.	Человеческое лицо – это 3D объект, поэтому различным регионам поверхности присущи различные коэффициенты отражения, рассеяния, преломления и поглощения. Бумага и экран устройства указанным свойством не обладают. Необходимо анализировать изображения объекта с различной интенсивностью освещения.
Видеозапись	Системе распознавания предъявляется видеозапись объекта, либо серия искусственно сформированных изображений.	Необходимо сформировать серию изображений объекта с различной интенсивностью освещения в случайные моменты времени, чтобы избежать возможного совпадения.
Устройство с экраном + ПО	Изображение объекта, изменённое приложением, предъявляется системе распознавания. Специализированное приложение способно изменять изображение объекта, имитируя моргание глаз, падение света как на 3D объект (подсвечиваются соответствующие регионы) и т.д.	Следует производить анализ изображений после формирования серии изображений, чтобы сократить время формирования решения о подмене. Тем самым предотвратить возможность предъявления сенсору подложных изображений.
Фото маска	Видеокамере предъявляется распечатанное изображение лица человека с прорезями для глаз и губ.	Для предотвращения атаки необходимо анализировать изображения с различной интенсивностью освещения объекта.
3D муляж	Сенсору предъявляют 3D муляж лица человека.	Следует анализировать биометрическую активность объекта.
Грим/Силиконовая маска	Изменение внешности злоумышленника с целью обмана системы защиты.	Необходимо использовать дополнительное дорогостоящее оборудование.

2.3.3 Математическая модель, метод и алгоритм подтверждения подлинности распознаваемого объекта

В данном подразделе приведены оригинальные метод, математическая модель, алгоритм и устройство защиты от спуфинга, не требующие специализированного оборудования, и, как следствие, внедрение не повлечёт за собой существенного удорожания СКД. Одним из способов всестороннего изучения и оптимизации параметров объекта, явления или процесса называют математическое моделирование. Математическая модель – это уравнение или система уравнений, связывающая параметры объекта, явления или процесса с факторами, влияющими на них. Допустимо составление разных математических моделей, различаемых по объёму охвата параметров, полные и неполные [32, 46, 50, 59]. Математическая модель, представленная в данном подразделе, является совокупностью частных моделей, описывающих процесс подтверждения подлинности объекта.

Визуальный осмотр изображений реального человека и его фотографии демонстрирует, что изображения могут быть очень похожи, даже человеческому глазу тяжело определить подмену. Ниже представлены изображения реального человека (рисунок 2.17,а, г), фотографии на бумажном носителе (рисунок 2.17,б, д) и экрана телефона (рисунок 2.17,в, е) с различной интенсивностью освещения.



Рисунок 2.17 – Примеры изображений с различной интенсивностью освещения:

а), г) реальный человек; б), д) фотография; в), е) экран телефона

Тем не менее, некоторые различия между изображениями лица человека и его фотографией могут стать очевидней, если образы перевести в надлежащее пространство признаков. Человеческое лицо – это 3D объект, поэтому различным регионам поверхности лица присущи различные коэффициенты отражения, рассеяния, преломления и поглощения. Бумага и экран устройства указанным свойством не обладают. Есть основание предполагать, что текстурные свойства изображений лица реального человека и подложного объекта будут отличаться при различной интенсивности освещения. При изменении интенсивности освещения появятся текстурные артефакты и неравномерно изменится освещённость регионов распознаваемого объекта. Текстурные артефакты будут хорошо заметны в местах однородных областей, например, на лбу или щеках, а неравномерное изменение освещённости – в областях глаз и рта. Описанные изменения освещённости будут отчётливо видны при анализе отношений яркости пикселей изображений объекта до подсветки и после:

$$q_j(x, y) = \frac{g_{0,j}(x, y)}{g_{1,j}(x, y) + 1}, \quad (2.47)$$

где j – номер текущего значения последовательности Y , $g_{b,j}(x, y)$ – значение яркости пикселя массива $I_{b,j}$, соответствующего изображению лица пользователя, b – идентификатор массива пикселей, обозначающий режим подсветки, при котором производилась подготовка массива, $b = \{0, 1\}$, x и y координаты рассматриваемого пикселя, $x = 0, 1, \dots, W - 1$, $y = 0, 1, \dots, H - 1$, W и H – количество пикселей, соответствующих ширине и высоте массива $I_{b,j}$.

Следует оценить меру рассеивания всех значений $q_j(x, y)$. Для оценки степени рассеивания относительно среднего значения (математического ожидания) вычисляют дисперсию:

$$D(I_{0,j}, I_{1,j}) = \frac{1}{WH} \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} (q_j(x, y) - \bar{q}_j)^2, \quad (2.48)$$

где $\bar{q}_j$ – среднее значение или математическое ожидание дискретной случайной величины $q_j(x, y)$, которое вычисляется по формуле:

$$\bar{q}_j = \frac{1}{WH} \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} q_j(x, y). \quad (2.49)$$

Оценка меры рассеивания $D(I_{0,j}, I_{1,j})$ величины $q_j(x, y)$ позволяет сделать вывод о поверхности распознаваемого объекта: чем больше оценка, тем больше рассеяны значения и, соответственно, тем более рельефную поверхность имеет распознаваемый объект. В приложении А приведены трёхмерные графики (рисунки А1, А2, А3, А4), построенные на основе значений $q_j(x, y)$, для оценки поверхностей различных объектов (реального лица пользователя, фотографии, фотомаски и экрана устройства).

Оценка меры рассеивания $D(I_{0,j}, I_{1,j})$ уменьшает вероятность взлома с помощью плоского объекта (фотографии, фотомаски, экрана устройства). Но остаётся опасность взлома подбором, т.е. случайного совпадения вспышки и изменения изображения на экране устройства с помощью соответствующего программного обеспечения. Чтобы исключить подобную возможность, необходимо производить подтверждение подлинности распознаваемого объекта многократно и в различные моменты времени.

В диссертации предложен метод подтверждения подлинности распознаваемого объекта, в соответствии с которым генерируется управляющая последовательность случайных чисел Y . Для каждого значения Y_j последовательности Y формируются массивы пикселей $I_{0,j}$ и $I_{1,j}$, соответствующие изображениям лица пользователя информационной системы, при этом, если следующее значение в последовательности $Y_j = 1$, то массив $I_{1,j}$ формируется при включённой подсветке, а если $Y_j = 0$, то при выключенной. Массив пикселей $I_{0,j}$ формируется без подсветки. Формируется совокупность значений оценки рельефности распознаваемого объекта $X(I_{0,j}, I_{1,j})$. Величины $X(I_{0,j}, I_{1,j})$ и Y_j могут принимать зна-

чения только из множества $\{0,1\}$. Проводится сравнительный анализ последовательности Y и совокупности значений $X(I_{0,j}, I_{1,j})$ в соответствии с пороговым значением τ_{spf} следующим образом:

$$\sum_{j=0}^{Q-1} X(I_{0,j}, I_{1,j}) \oplus Y_j \leq \tau_{spf}, \quad (2.50)$$

где j – номер текущего значения последовательности Y , $j = 0, 1, \dots, Q - 1$; Q – количество значений в последовательности Y ; $\oplus$ – сложение по модулю 2.

Выражение для оценки рельефности объекта имеет вид:

$$X(I_{0,j}, I_{1,j}) = \begin{cases} 1, D(I_{0,j}, I_{1,j}) \leq \tau_{ROC}; \\ 0, D(I_{0,j}, I_{1,j}) > \tau_{ROC}, \end{cases} \quad (2.51)$$

где τ_{ROC} – пороговое значение, при котором разница значений ($TPR - FPR$) максимальна.

Математическая модель служит исходным материалом для создания алгоритма. Алгоритм включает точное и полное описание, определяющее последовательность выполнения вычислительных действий, позволяющих получить искомый результат (в данном случае – детектирование подмены распознаваемого объекта) [11, 42, 49]. Алгоритм подтверждения подлинности распознаваемого объекта состоит из следующей последовательности действий:

- **Шаг 1.** Создаётся последовательность случайных чисел Y .
- **Шаг 2.** Формируется массив пикселей $I_{0,j}$ без подсветки.
- **Шаг 3.** Формируется массив пикселей $I_{1,j}$, при этом, если следующее значение $Y_j = 1$, то массив формируется при включённой подсветке, а если $Y_j = 0$, то при выключенной.
- **Шаг 4.** Принимается решение с учётом шага 3, если $j > Q - 1$, то следует перейти к шагу 5, иначе к шагу 2. К величине j добавляется единица.
- **Шаг 5.** Формируется совокупность значений оценки рельефности распознаваемого объекта $X(I_{0,j}, I_{1,j})$.

- **Шаг 6.** Проводится сравнительный анализ последовательности Y и совокупности значений $X(I_{0,j}, I_{1,j})$.

- **Шаг 7.** Принимается решение о подлинности объекта.

Для реализации алгоритма подтверждения подлинности распознаваемого объекта необходимо выполнить последовательность действий, представленную на рисунке 2.18.



Рисунок 2.18 – Схема, отражающая алгоритм подтверждения подлинности распознаваемого объекта

Представленный алгоритм (рисунок 2.18) можно модифицировать, в частности, добавлять новые блоки или заменять старые блоки с условием сохранения основной идеи исследования. Вместо блока подсветки возможно использование лампы накаливания или компьютерного монитора. Для данного алгоритма приемлемы небольшие изменения интенсивности освещения и как следствие, при этом происходит снижение воздействия на пользователя.

2.3.4 Характеристики технических устройств, используемых для подтверждения подлинности объекта

Далее представлены расчёты для определения основных характеристик технических устройств, используемых в системе подтверждения подлинности распознаваемого объекта.

В соответствии с методом подтверждения подлинности распознаваемый объект ориентирован нормально к видеокамере. На объект, который имеет коэффициент отражения ρ , воздействуют световым потоком Φ_b . Источник света, сопряжён с видеокамерой. Известны параметры ПЗС-матрицы, параметры оптики видеокамеры и параметры источника света.

Для расчёта яркости источника освещения V_b , взаимного расположения источника освещения и распознаваемого объекта воспользуемся законом аддитивности освещённостей [6]. При воздействии на объект несколькими источниками света, его освещённость равна сумме освещённостей от каждого источника света. Если распознаваемый объект до включения подсветки имеет освещённость E_n , то закон аддитивности освещённости для случая с пониженным уровнем освещения примет вид:

$$E_{c0} = E_0 + E_n; \quad (2.52)$$

для случая с повышенным уровнем освещения:

$$E_{c1} = E_1 + E_n, \quad (2.53)$$

где E_{c0} и E_{c1} – общая энергетическая освещённость объекта; E_0 и E_1 – энергетическая освещённость от источника света системы подтверждения подлинности распознаваемого объекта. Вычтем (2.52) из (2.53):

$$E_{c1} - E_{c0} = E_1 - E_0. \quad (2.54)$$

Соотношения для силы света J_b и энергетической освещённости объекта от точечного источника будут иметь вид [45]:

$$E_b = \frac{\Phi_b}{S_o} = \frac{\Omega \cdot J_b}{S_o} = \frac{J_b \cdot \cos \alpha}{L^2}, \quad (2.55)$$

$$\Omega = \frac{S_o \cdot \cos \alpha}{L^2}, \quad (2.56)$$

где Φ_b – световой поток, исходящий в пределах телесного угла Ω ; S_o – площадь поверхности объекта; L – расстояние от источника света до объекта; α – угол между направлением источника и перпендикуляром к освещаемой поверхности.

В случае протяжённого источника света следует говорить о силе света каждого элемента источника и площади его поверхности. Тогда под Φ_b следует понимать световой поток, излучаемый каждым элементом поверхности источника. В частности, можно разделить всю поверхность источника света на отдельные Z участков существенно меньших расстояния до облучаемого объекта и принять их за точечные источники света. Каждый участок источника освещения имеет свою площадь S_z , яркость B_{bz} , угол между направлением источника и перпендикуляром к освещаемой поверхности α_z и расстояние до объекта L_z . Полная освещённость объекта от всех отдельных участков протяжённого источника света может быть вычислена следующим образом [26]:

$$E_b = \sum_{z=1}^Z \frac{B_{bz} \cdot S_z \cdot \cos \alpha_z}{L_z^2}, \quad (2.57)$$

где z – рассматриваемый номер участка поверхности объекта.

Угол обзора источника освещения θ_z – угол, при котором сохраняется удовлетворительный уровень яркости. Яркость B_{bz} от каждого региона источника освещения будет одинакова, если α_z не превышает θ_z , а линейные размеры источника освещения не превышают значения $2 \cdot \operatorname{tg}(\theta_z) \cdot L$. При условии, что яркость B_{bz} всей поверхности источника освещения одинакова, целесообразно использовать следующую формулу для полной освещённости объекта [26]:

$$E_b = \frac{B_b \cdot S \cdot \cos \alpha}{L^2}, \quad (2.58)$$

где B_b – яркость поверхности источника освещения; S – площадь светящейся поверхности протяжённого источника освещения.

Откуда правая часть соотношения (2.54) равна:

$$E_1 - E_0 = \frac{(B_1 - B_0) \cdot S \cdot \cos \alpha}{L^2} = E_{c1} - E_{c0}. \quad (2.59)$$

Выражение для расчёта яркости источника освещения B_b , взаимного расположения источника освещения и распознаваемого объекта следующее:

$$L = \sqrt{\frac{(B_1 - B_0) \cdot S \cdot \cos \alpha}{E_{c1} - E_{c0}}}. \quad (2.60)$$

Световое излучения от распознаваемого объекта попадает через объектив на светочувствительный слой ПЗС-матрицы видеокамеры и создаёт на нем оптическое изображение распознаваемого объекта с эквивалентной освещённостью E_{eb} . Эквивалентная освещённость E_{eb} показывает степень уменьшения реальной освещённости объекта E_{cb} при прохождении света через объектив камеры (коэффициент пропускания объектива видеокамеры K_a) с учётом спектральной чувствительности видеокамеры K_λ , а также с учетом светосилы объектива и коэффициента диффузного отражения распознаваемого объекта ρ :

$$E_{eb} = E_{cb} K_\lambda K_a \rho \frac{1}{4F^2}, \quad (2.61)$$

где F – число, равное отношению фокусного расстояния объектива к диафрагме видеокамеры. Откуда выражение для реальной освещённости объекта E_{cb} с учетом эквивалентной E_{eb} будет иметь вид:

$$E_{cb} = \frac{E_{eb} 4F^2}{K_\lambda K_a \rho}. \quad (2.62)$$

Эквивалентную освещённость оптического изображения объекта E_{eb} можно рассчитать, используя массив яркостей оптического изображения объекта $I_{b,j}$ согласно рекомендациям, описанным в стандарте федеральной комиссии связи (FCC) [105]:

$$E_{eb} = K_c \bar{g}_b, \quad (2.63)$$

$$\bar{g}_b = \frac{1}{WH} \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} g_b(x, y), \quad (2.64)$$

где K_c – коэффициент расчёта энергетической освещённости объекта; $\bar{g}_b$ – средняя освещённость распознаваемого объекта в плоскости оптического изображения; (x, y) – координаты текущего пикселя, $x = 0, 1, \dots, W - 1$, $y = 0, 1, \dots, H - 1$; W и H – количество пикселей, соответствующее ширине и высоте изображения объекта; $g_b(x, y)$ – яркость пикселя, значение которой рассчитывается с помощью (2.29).

Коэффициент K_c используется для пересчёта освещённости оптического изображения объекта $\bar{g}_b$ в эквивалентную освещённость объекта E_{eb} . Для расчёта $\bar{g}_b$ выбрана область в центре лба, неприкрытая волосами и головным убором. Данная область наиболее плоская и равномерно отражающая свет. Выбор данного региона обусловлен минимизацией погрешности, связанной с неравномерностью распределения освещённости при подсветке трёхмерных объектов.

Подставим в выражение (2.60) соотношения (2.62) и (2.63). Итоговое выражение для расчёта яркости источника освещения B_b и взаимного расположения источника освещения и распознаваемого объекта примет вид:

$$L = \sqrt{\frac{(B_1 - B_0) \cdot S \cdot \cos \alpha \cdot K_\lambda \cdot K_a \cdot \rho}{(\bar{g}_1 - \bar{g}_0 + 0,001) \cdot 4F^2 \cdot K_c}}. \quad (2.65)$$

Соотношение (2.65) необходимо использовать при калибровке системы подтверждения подлинности распознаваемого объекта. Для вычисления коэффициента K_c следует на заданном расстоянии L сформировать два изображения распознаваемого объекта с заданными яркостями источника освещения B_0 и B_1 . Выражение для расчёта K_c представлено ниже:

$$K_c = \frac{(B_1 - B_0) \cdot S \cdot \cos \alpha \cdot K_\lambda \cdot K_a \cdot \rho}{(\bar{g}_1 - \bar{g}_0 + 0,001) \cdot (2FL)^2}. \quad (2.66)$$

Соотношение (2.66) используется при следующих значениях: разность яркостей источника $(B_1 - B_0) = 17 \text{ кд/м}^2$, площадь светящейся поверхности протяжённого источника освещения $S = 0,0825 \text{ м}^2$, спектральная чувствительность видеокамеры $K_\lambda = 0,6$, коэффициент пропускания объектива видеокамеры $K_a =$

0,8, коэффициент диффузного отражения кожи лица $\rho = 0,3$, средняя освещённость распознаваемого объекта в плоскости изображения $(\bar{g}_1 - \bar{g}_0) = 4,5$ лм/м², отношение фокусного расстояния объектива к диафрагме видеокамеры (F-число) $F = 0,25$, расстояние от источника света до объекта $L = 0,5$ м, значение коэффициента расчёта энергетической освещённости равно $K_c = 0,72$.

Для повышения вероятности верного детектирования подмены следует использовать максимально допустимый уровень повышения освещённости, в соответствии с коэффициентом пульсации освещённости. Коэффициент пульсации освещённости K_p – критерий оценки относительной глубины колебаний освещённости объекта источником света. Выражение для расчёта K_p имеет вид:

$$K_p = \frac{E_1 - E_0}{2E_m} 100\%, \quad (2.67)$$

где E_1 и E_0 – максимальное и минимальное значения освещённости соответственно; E_m – среднее значение освещённости.

В документе «Гигиенические требования к естественному, искусственному и совмещённому освещению жилых и общественных зданий. СанПиН 2.2.1/2.1.1.1278-03», утверждённом 6 апреля 2003 года, указаны требования к источнику освещения $K_p \leq 20\%$. Примем $E_m = E_0$. Откуда значение освещённости E_1 не должно превышать $1,4 \cdot E_0$.

Для обеспечения устойчивости выделяемых признаков к изменениям внешней обстановки и параметров, регистрирующих устройств, необходимо проводить калибровку системы по объекту с известными спектральной характеристикой, коэффициентом отражения и на заданном расстоянии между устройством освещения и объектом. С учётом коэффициента K_c , расстояния между устройством освещения и объектом L , характеристиками видеокамеры, а также ограничения $E_1 < 1,4 \cdot E_0$, необходимо в ручном или автоматическом режиме подбирать значения освещённостей E_0 и E_1 для источника света.

Общее и текущее время работы системы подтверждения подлинности объекта определяются соотношениями:

$$T = t \cdot N, \quad (2.68)$$

$$t_j = t \cdot j, \quad (2.69)$$

$$t = t_{\text{под}} + 2 \cdot t_{\text{кам}} + t_{\text{пад}}, \quad (2.70)$$

$$t_{\text{отк}} = t_{\text{под}} + t_{\text{пад}}, \quad (2.71)$$

где t – время, затрачиваемое на обработку одного разряда, $t_{\text{под}}$ – время «подъема», за которое устройство освещения переходит в режим повышенной яркости; $t_{\text{кам}}$ – время восприятия изображения видеокамерой; $t_{\text{пад}}$ – время «падения», за которое устройство освещения переходит в режим пониженной яркости; $t_{\text{отк}}$ – время отклика (black-white-black), за которое устройство освещения изменит режим яркости от минимального значения до максимального значения и обратно. Перечисленные временные рамки зависят от технических характеристик устройства освещения и видеокамеры.

На рисунке 2.19 схематично изображены временные параметры технических устройств, используемых для подтверждения подлинности объекта.

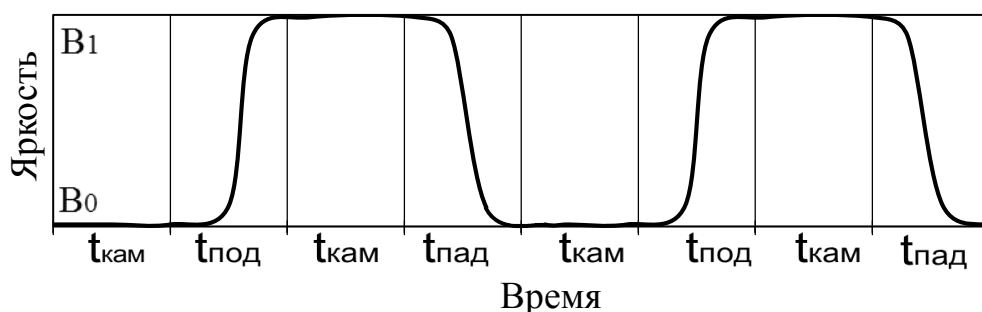


Рисунок 2.19 – Схема, отражающая временные параметры технических устройств

Тесты системы подтверждения подлинности распознаваемого объекта производились на компьютере с процессором Intel Core i3 при тактовой частоте 2,40ГГц и ОЗУ 4,00ГБ, видеокамерой SCB-0350M – 0,3 Мп при скорости работы 11 кадров/с, откуда $t_{\text{кам}} = 91\text{мс}$. Устройством освещения выбран ЖК-дисплей со следующими характеристиками: диагональ 17.3", значение яркости при максимальном режиме 224 кд/м^2 , а при минимальном – 1.34 кд/м^2 и $t_{\text{отк}} = 17\text{мс}$. Время для обработки одного разряда $t = 17 + 182 = 199\text{ мс}$. Примем $t = 0,2\text{с}$.

На графиках 2.20 видно, как с увеличением количества разрядов – Q увеличивается время работы T (формула 2.68) и уменьшается вероятность подбора последовательности Y . Минимальным значением Q выбрано 20, откуда общее время $T = 4$ с. Сгенерированная последовательность Y – это набор единиц и нулей, распределённых по нормальному закону распределения.

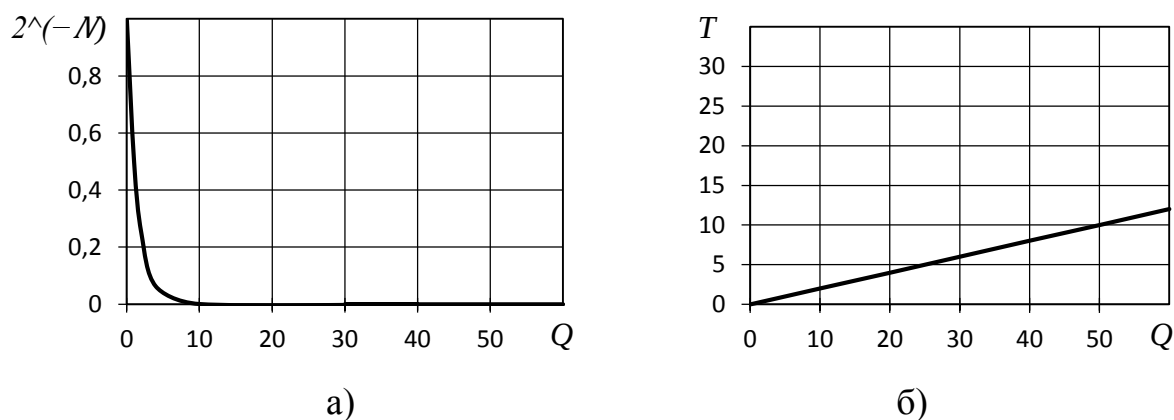


Рисунок 2.20 – Взаимосвязь количества разрядов: с вероятностью подбора последовательности Y (а) и общего времени работы T (б)

Ниже на рисунке 2.21 представлено устройство для обнаружения подмены распознаваемого объекта, состоящее из устройства регистрации изображений, устройства подсветки и процессора.

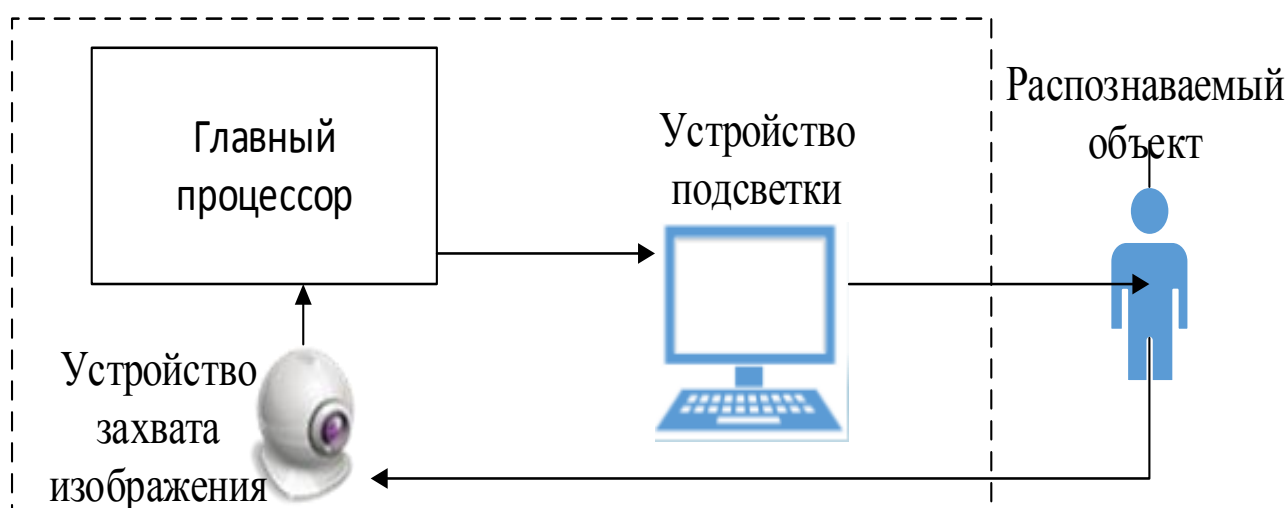


Рисунок 2.21 – Устройство обнаружения подмены распознаваемого объекта

2.3.5 Экспериментальные исследования

Для проведения опытов была подготовлена экспериментальная БД (таблица 2.6). Условия съёмки подбирались таким образом, чтобы изображения соответствовали заявленным требованиям (п. 2.1). В обучающей выборке находятся 160 случаев предоставления видеокамере лиц реальных людей, а также 400 случаев предоставления видеокамере фотографий, видеозаписей, экранов устройств и фотомасок. В тестовой выборке содержатся 320 случаев предоставления видеокамере лиц реальных людей, а также 700 случаев предоставления видеокамере фотографий, видеозаписей и фотомасок. Каждый случай предоставления объекта видеокамере дублировался при повышенной интенсивности освещения для реализации алгоритмов подтверждения подлинности объекта (п. 2.3.3).

Таблица 2.6 – Изображения лиц, используемые для проведения экспериментальных исследований

	Тестовая выборка	В базе данных
Реальные лица	320 изображений, 40 человек	160 изображений, 40 человек
Попытка обмана	700 изображений различных лиц	400 изображений, 40 человек

Примеры изображений представлены на рисунке 2.17. Существуют различные БД для экспериментальной проверки систем подтверждения подлинности [71, 125], но они не подходят ввиду специфики используемого метода подтверждения (необходимо, чтобы каждый случай предоставления объекта видеокамере дублировался при повышенной интенсивности освещения). В БД содержатся изображения лиц людей с различным возрастом, мимикой и ракурсом. Изображения подготавливались в четырёх различных условиях освещения. Распознаваемый объект предъявлялся системе подтверждения подлинности в двух режимах:

- фотографию или экран устройства фиксируют на неподвижной опоре, чтобы избежать движения во время попытки обмана;
- пользователь, используя свои собственные руки, предъявляет сенсору фотографию или экран устройства; в данном случае небольшое движение объекта относительно камеры может внести шум на изображения.

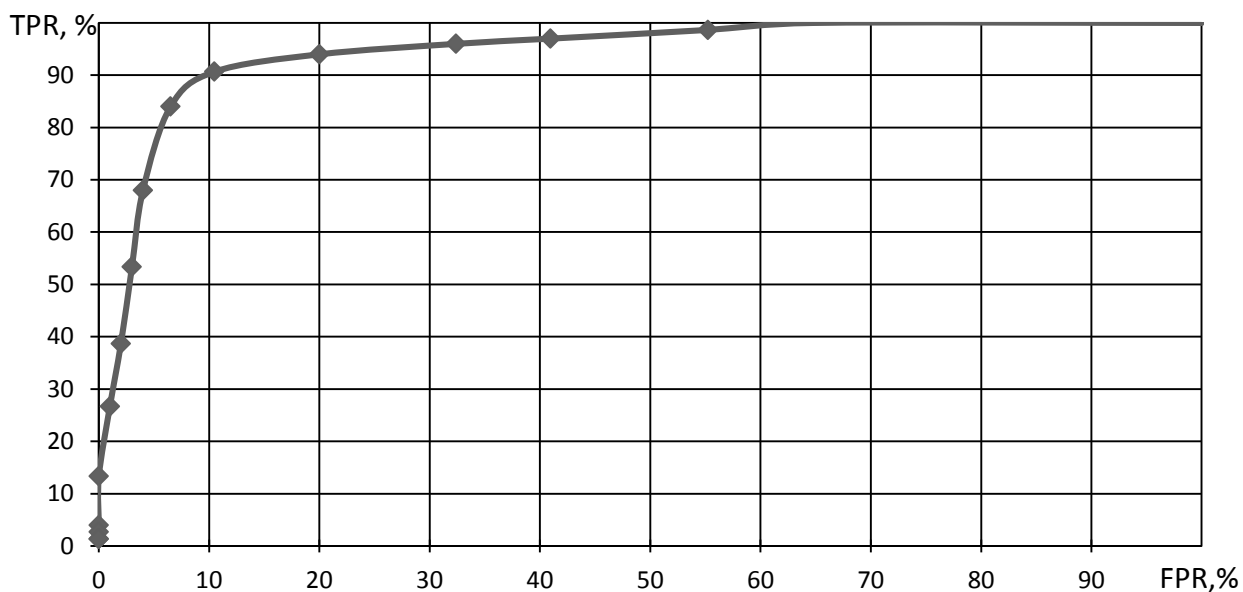


Рисунок 2.22 – Результаты экспериментальных исследований системы подтверждения подлинности распознаваемого объекта

На рисунке 2.22 представлены результаты экспериментальных исследований разработанной системы подтверждения подлинности на основе ROC анализа (п. 2.2.6). На графике 2.22 по оси ординат указан процент верного распознавания подлинности предъявляемых объектов видеокамере (True Positives Rate), а по оси абсцисс указан процент пропуска подмены распознаваемого объекта (False Positives Rate). Для кривой рисунка 2.22 значение $AUC = 0,944$. Эффективным значением порога для кривой на рисунке 2.22 является значение 0,001557. При указанном значении процент верного распознавания подлинности предъявляемых объектов видеокамере составил не менее 91%, а процент пропуска подмены распознаваемого объекта составил не более 10%.

2.4 Технология распознавания пользователей информационных ресурсов

На рисунке 2.23 представлена схема комплексного решения задачи распознавания пользователей и контроля доступа к информационным ресурсам на основе новой информационной технологии.

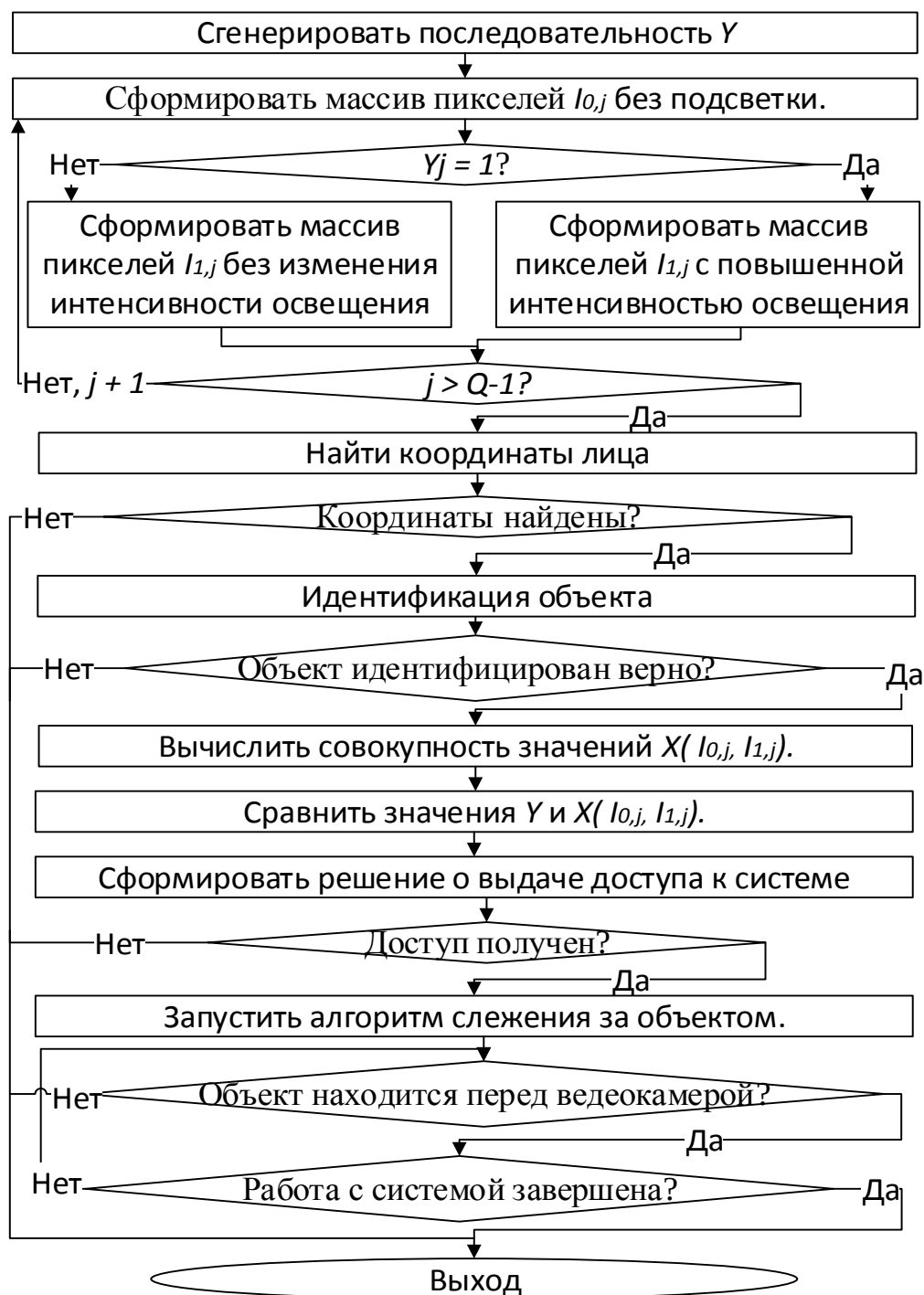


Рисунок 2.23 – Схема, отражающая технологию распознавания пользователей информационных ресурсов

Оригинальная технология распознавания пользователей информационных ресурсов (рисунок 2.23) использует следующие методы и алгоритмы:

- поиск координат лица на изображении (п. 2.2.2);
- распознавание объекта по изображению лица (п. 2.2.6);
- обнаружение подмены распознаваемого объекта на фотографию, видеозапись или фотомаску лица зарегистрированного пользователя (п. 2.3.3).

В технологии используется алгоритм слежения за распознаваемым объектом. На данный момент существует множество эффективных решений такого рода [56, 88, 96, 118, 123]. В данном случае используется алгоритм на основе каскадов Хаара (п. 2.2.2). На протяжении всего времени взаимодействия с системой работает алгоритм слежения. Как только пользователь отошёл от своего рабочего места, ему снова придётся полностью пройти процедуру распознавания.

Оригинальная информационная технология распознавания пользователей информационных ресурсов найдёт применение во многих областях промышленности и железнодорожного транспорта. Автоматическое распознавание и подтверждение подлинности распознаваемого объекта требуются и в дистанционном обучении. Экзамены считаются обязательным и жизненно необходимым компонентом обучения. Эффективность экзаменов в ДО зависит от вероятности правильного распознавания обучаемого. Низкая вероятность правильного распознавания пользователей дистанционного обучения уменьшает авторитет ДО.

Представленная технология, в отличие от существующих, обеспечивает более высокую вероятность правильного распознавания лиц пользователей за счёт использования оригинального информативного признака (п. 2.2.4), а также за счёт детектирования подмены распознаваемого объекта на фотографию, видеозапись или фотомаску лица зарегистрированного пользователя (п. 2.3.3). Технология частично инвариантна к изменениям условий освещения, наличию теней на изображении в области лица, незначительным вариациям ракурса съёмки и изменениям масштаба.

2.5 Выводы по 2 разделу

1. Представлен и обоснован выбор численного метода построения математической модели распознаваемого объекта (п. 2.2.2). Метод соответствует требованиям, выдвигаемым в ГОСТ Р 19794-5–2006 [8].
2. Предложена модификация численного метода, основанная на использовании комбинации формы и способа сравнения фрагментов информативного признака гистограмм ЛБШМП (п. 2.2.4). Предложен алгоритм численного определения информативных признаков, позволяющий добиться более высокой скорости вычисления шаблона (в 1,7 и в 2 раза по сравнению с лучшими аналогами Three-Patch ЛБШ и Four-Patch ЛБШ) при сохранении высокой эффективности использования в процессе распознавания образов.
3. Разработана информационная технология распознавания изображений лиц. Экспериментальные исследования показали следующие результаты: процент случаев выдачи доступа зарегистрированному пользователю не менее 97%, а процент ошибочной выдачи доступа человеку, не имеющему допуск, не более 2% (п. 2.2.6).
4. Представлена модель атак на биометрическую систему распознавания пользователей по изображению лица. Рассмотрены возможные действия злоумышленников по взлому систем подтверждения подлинности распознаваемого объекта, а также меры защиты от спуфинг атак. Описаны требования к разработке методов, математических моделей, алгоритмов и системы подтверждения подлинности распознаваемого объекта. Обоснован выбор методов для решения задачи подтверждения подлинности распознаваемого объекта (п. 2.3.2).
5. Разработаны и исследованы метод, математическая модель и алгоритм для решения задачи подтверждения подлинности распознаваемого объекта (п. 2.3.3). Способ на основе метода подтверждения подлинности распознаваемого объекта защищён патентом РФ [55] «Способ и устройство распознавания рельефности изображения лица». Произведена экспериментальная проверка эффективности алгоритма (п. 2.3.5). Для модуля подтверждения подлинности процент верного

распознавания реальных объектов не менее 91%, а процент пропуска подмены – не более 10%.

6. Предложено комплексное решение задачи распознавания пользователей информационных ресурсов на основе новой информационной технологии (п. 2.4), которая, в отличие от существующих, обеспечивает более высокую вероятность правильного распознавания лиц пользователей за счёт использования оригинального информативного признака, а также за счёт детектирования подмены распознаваемого объекта на фотографию, видеозапись или фотомаску лица зарегистрированного пользователя. Технология частично инвариантна к изменениям условий освещения, наличию теней на изображении в области лица, незначительным вариациям ракурса съёмки и изменениям масштаба.

3 Программный комплекс распознавания пользователей информационных ресурсов

В соответствии с заявленной постановкой задачи данного исследования (п. 1.1) реализован программный комплекс распознавания пользователей по изображению лица [3]. В данном разделе приводится детальный обзор программной реализации представленных в диссертационной работе алгоритмов и краткое руководство использования каждого компонента комплекса.

Комплекс программ реализован в режиме диалоговых окон и имеет дружелюбный графический интерфейс. Основной целью программного комплекса является оценка эффективности разработанных алгоритмов, наглядная демонстрация результатов в виде ROC-кривых (п. 2.2.6), возможность отладки и совершенствования алгоритмов. Представленный программный комплекс позволяет доказать превосходство разработанных алгоритмов над существующими при равных затратах и сложности реализации. Комплекс программ готов к коммерческому использованию в заинтересованных организациях.

Программный комплекс разбит на клиентскую и серверную части. Клиентская часть получает логин и пароль пользователя, а также производит обработку изображения, поступившего с видеокамеры. С клиентской части на сервер отправляется запрос, включающий в себя изображение, логин и пароль. Сервер на изображении выделяет область, содержащую лицо пользователя. Далее производится вычисление и сопоставление информативных признаков с БД.

Разработанный программный комплекс распознавания человека по изображению лица можно условно разделить на 5 основных компонент:

- БД для хранения изображений лиц и информативных признаков;
- модуль построения модели распознаваемого объекта (поиск области лица, вычисление антропометрических точек, предварительная обработка);
- модуль распознавания лиц (вычисление информативных признаков, запуск сравнения информативных признаков);

- модуль оценки экспериментальных исследований (отражает на графике результаты экспериментальных исследований комплекса);
- модуль подтверждения подлинности распознаваемого объекта (обнаружение подмены распознаваемого объекта на фотографию, видеозапись или фотомаску лица, зарегистрированного в системе пользователя).

Комплекс создавался в среде Microsoft Visual Studio 2015 с использованием универсальной СУБД Firebird 2.5.1. Microsoft Visual Studio 2015 является предпочтительным вариантом платформы, так как представляет собой мощную и гибкую среду разработки для Windows-приложений. Комплекс программ реализован на языке объектно-ориентированного программирования C# при помощи открытых библиотек OpenCV и Emgu CV. Библиотека OpenCV содержит эффективные функции обработки изображений и алгоритмы компьютерного зрения, написанные на языке C и C++. Emgu CV это кроссплатформенная библиотека, являющаяся оболочкой для библиотеки OpenCV. Взаимодействия с пользователем осуществляется с помощью графического интерфейса и видеокамеры. Комплекс поддерживает обработку изображений со следующими форматами: JPEG, BMP, TIFF и PGM.

3.1 Описание архитектуры БД программного комплекса

Выбор базы данных изображений является жизненно важным компонентом системы распознавания. В ходе исследования автором разработана БД [4], адаптированная к требованиям настоящего исследования.

В разработанной БД находятся такая информация, как ФИО пользователей, исходные изображения и изображения лиц пользователей, приведённые к общей форме, информативные признаки, координаты антропометрических точек, данные результатов экспериментальных исследований, характеристики используемых видеокамер и т.д. Далее на рисунке 3.1 представлена реляционная модель БД программного комплекса.

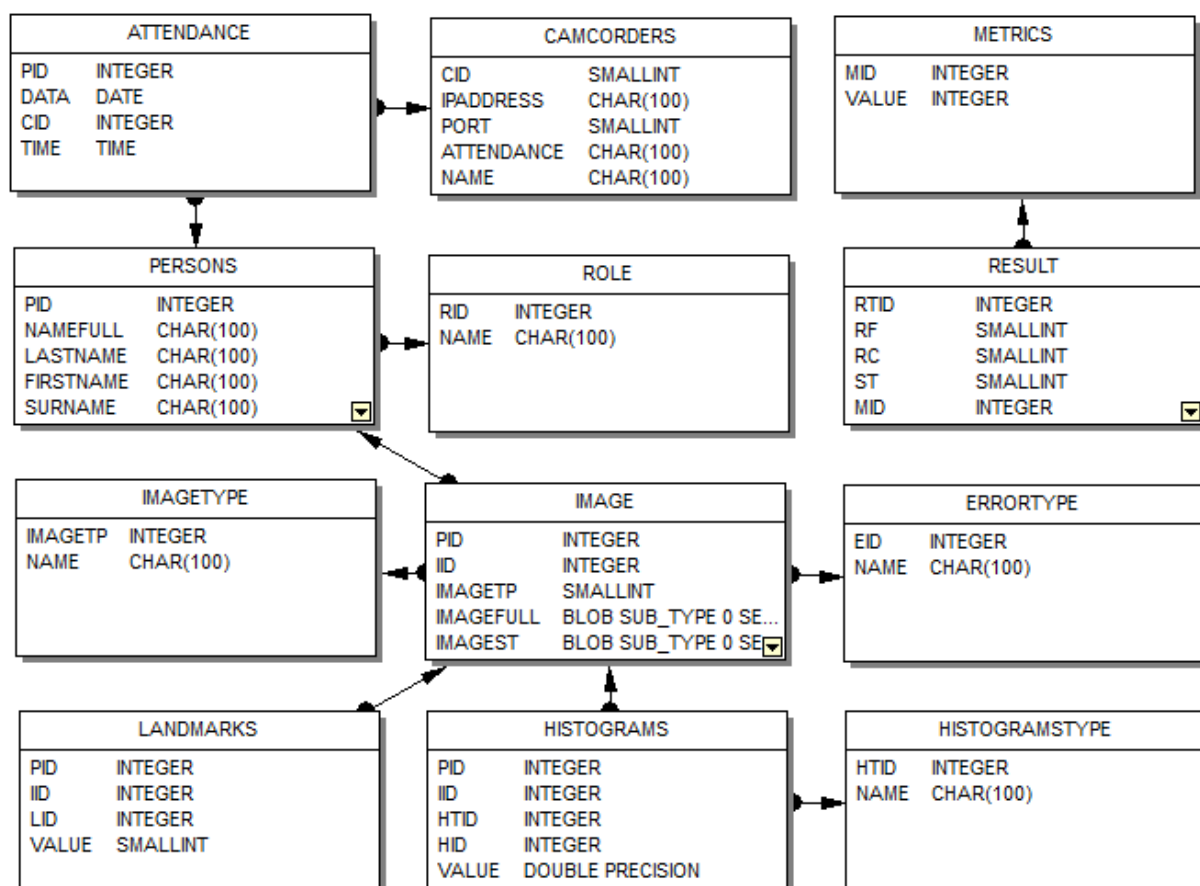


Рисунок 3.1 – Реляционная модель БД

В таблице «Histograms» хранятся информативные признаки – гистограммы кодов ЛБШ. В таблице 3.1 представлено описание таблицы «Histograms».

Таблица 3.1 – Структура таблицы «Histograms»

Название поля	Тип	Функция
PID	Число	Идентификатор пользователя
IID	Число	Идентификатор изображения
HTID	Число	Тип гистограммы
HID	Число	Идентификатор столбца гистограммы
VALUE	Число	Значение гистограммы

Основным элементом представленной структуры является таблица «Persons». Таблица «Persons» предназначена для хранения данных учётных записей пользователей. Описание «Persons» представлено в таблице 3.2.

Таблица 3.2 – Структура таблицы «Persons»

Название поля	Тип	Функция
PID	Число	Идентификатор пользователя
NAMEFULL	Строка	ФИО целиком
LASTNAME	Строка	Фамилия
FIRSTNAME	Строка	Имя
SURNAME	Строка	Отчество
RID	Число	Идентификатор полномочий
CDATE	Дата	Дата создания учётной записи
CTIME	Время	Время создания учётной записи
CPID	Строка	Идентификатор пользователя, создавшего учётную запись
UPDATE	Дата	Дата изменения учётной записи
UTIME	Время	Время изменения учётной записи
UPID	Число	Идентификатор пользователя, изменившего учётную запись
LOGIN	Строка	Логин учётной записи
PASSWORD	Строка	Пароль

В таблице «Landmarks» хранятся координаты антропометрических точек лица, рассчитанные на исходном изображении. Количество точек может варьироваться. В таблице 3.3 представлено описание полей «Landmarks».

Таблица 3.3 – Структура таблицы «Landmarks»

Название поля	Тип	Функция
PID	Число	Идентификатор пользователя
IID	Число	Идентификатор изображения
LID	Число	Идентификатор антропометрической точки
VALUE	Число	Координата антропометрической точки

Следующая таблица реляционной модели БД – «Image». «Image» содержит исходные и приведённые к общей форме изображения лиц пользователей, а также координаты антропометрических точек. Далее в таблице 3.4 представлено описание полей «Image».

Таблица 3.4 – Структура таблицы «Image»

Название поля	Тип	Функция
PID	Число	Идентификатор пользователя
IID	Число	Идентификатор изображения
IMAGETP	Число	Тип выборки, тестовая/тренировочная
IMAGEFULL	Файл	Исходное изображение
IMAGEST	Файл	Изображение, приведённое к общей форме
LXEYE	Число	Координата X левого глаза
LYEYE	Число	Координата Y левого глаза
RXEYE	Число	Координата X правого глаза
RYEYE	Число	Координата Y правого глаза
EID	Число	Идентификатор ошибки

В таблице «Camcorders» хранится информация о видеокамерах. Описание полей «Camcorders» представлено в таблице 3.5.

Таблица 3.5 – Структура таблицы «Camcorders»

Название поля	Тип	Функция
CID	Число	Идентификатор видеокамеры
IPADDRESS	Строка	IP Адрес камеры
PORT	Строка	Порт камеры
ATTENDANCE	Строка	Название аудитории
NAME	Строка	Название камеры

Таблица «Result» используется для сохранения информации о результатах проведённых экспериментов. Поля «Result» представлены в таблице 3.6.

Таблица 3.6 – Структура таблицы «Result»

Название поля	Тип	Функция
RTID	Число	Идентификатор проведённого эксперимента
RF	Число	Радиус фрагмента ЛБШ
RC	Число	Радиус окружности ЛБШ
ST	Число	Шаг сравнения последовательности ЛБШ
MID	Число	Идентификатор функции расстояния
CDATE	Дата	Дата запуска
CTIME	Время	Время запуска
CPID	Число	Идентификатор пользователя
TIMEWORK	Время	Общее время работы
TP	Число	Истинно положительные случаи
TN	Число	Истинно отрицательные случаи
FP	Число	Ложно положительные случаи
FN	Число	Ложно отрицательные случаи

В таблице «Attendance» хранится информация о времени нахождения пользователя информационного ресурса в той или иной аудитории. Описание полей «Attendance» представлено в таблице 3.7 .

Таблица 3.7 – Структура таблицы «Attendance»

Название поля	Тип	Функция
PID	Число	Идентификатор пользователя
DATA	Число	Дата
CID	Число	Идентификатор видеокамеры
TIME	Время	Проведённое время в аудитории

3.2 Архитектура и объектная модель программного комплекса

На рисунке 3.2 представлена архитектура программного комплекса распознавания пользователей по изображению лица.

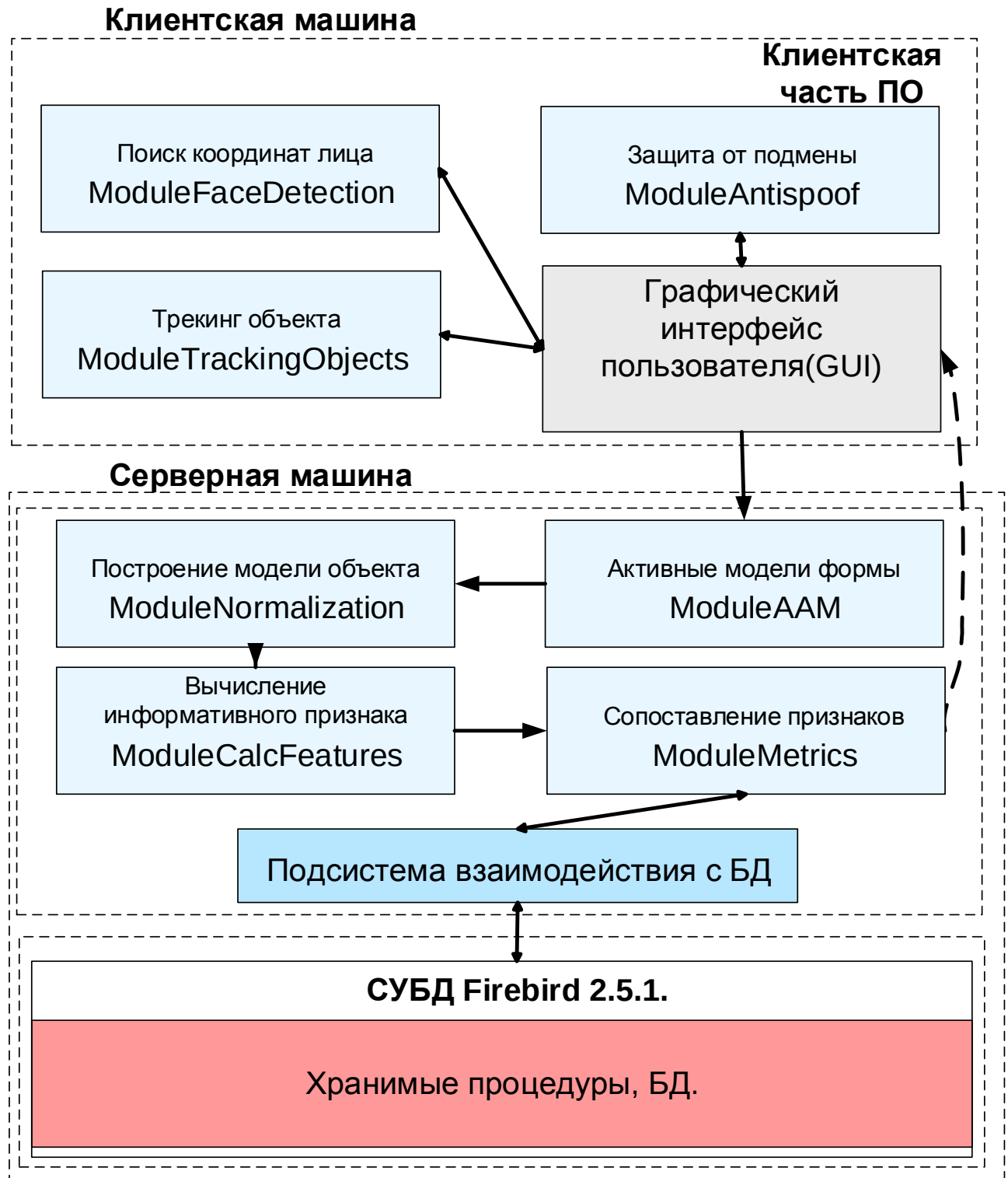


Рисунок 3.2 – Архитектура программного комплекса

Далее на рисунке 3.3 представлена объектная модель программного комплекса. Представлены основные классы объектной модели, используемые для реализации программного комплекса.

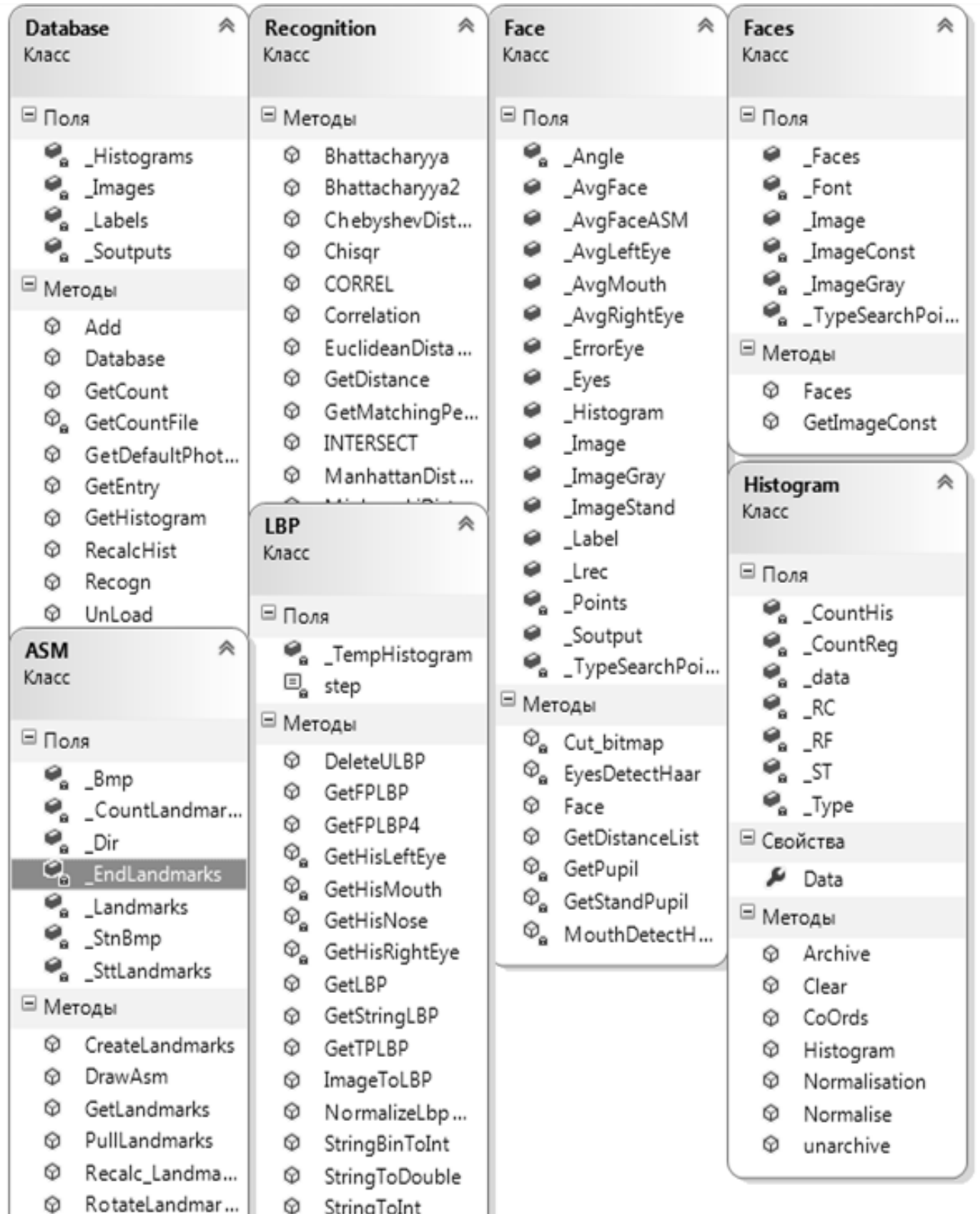


Рисунок 3.3 – Объектная модель программного комплекса

3.3 Основные модули программного комплекса

Функционирование программного комплекса возможно в двух режимах: аутентификация и идентификация. Для режима аутентификации необходимо ввести данные учётной записи в соответствующей форме (рисунок 3.4).

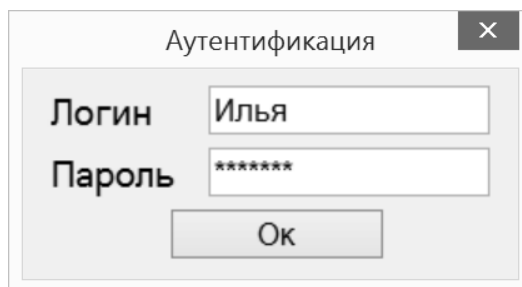


Рисунок 3.4 – Модуль аутентификации

Для запуска процесса построения модели объекта лица пользователя необходимо выбрать устройство захвата изображений. Далее производится построение модели распознаваемого объекта (п. 2.2.2), запускается поиск координат антропометрических точек. На рисунке 3.5 отмечены точки центров зрачков и другие антропометрические точки.



Рисунок 3.5 – Модуль построения модели распознаваемого объекта

С помощью антропометрических точек и процесса триангуляции производится локализация информативной области. Далее текстуру объекта подвергают

фильтрации, чтобы убрать все возможные шумы. Сигнатура метода приведена в приложении А – «Построение модели объекта лица пользователя».

Интерфейс модуля распознавания лиц представлен на рисунке 3.6.



Рисунок 3.6 – Модуль распознавания лиц

Изображение с видеокамеры приводится к общей форме и вычисляется информативный признак – гистограмма кодов ЛБШ, после чего признак сравнивается с уже существующими признаками в БД. Модуль распознавания вычисляет наиболее близкие изображения из БД к входному образу. В левом углу графического интерфейса представлены нормализованное изображение, поступившее на вход программному комплексу и три наиболее похожих на входной образ изображения из БД. Результатом работы модуля распознавания является вычисление наиболее соответствующего входному образу пользователя из БД. С помощью пороговой функции, описанной в пункте 2.2.6, вычисляется значение функции соответствия и сопоставляется с имеющейся базой для вычисления идентификатора пользователя. В нижнем левом углу интерфейса будет представлен идентификатор либо ФИО пользователя.

Внедрение методов распознавания человека на предприятии способствует решению задачи учёта рабочего времени. Модуль учёта посещаемости позволяет определить время нахождения каждого сотрудника на своём рабочем месте и зафиксировать время прибытия и ухода сотрудников с предприятий. Данный

модуль делает возможным ведение учёта посещаемости студентами лекций в ДО и консервативном обучении без «переклички» и потери времени и других возможных действий (рисунок 3.7).

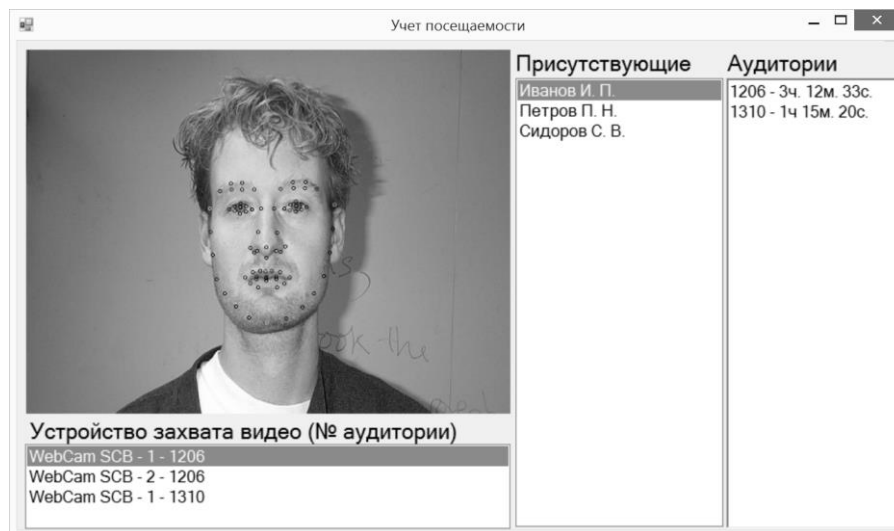


Рисунок 3.7 – Интерфейс модуля учёта посещаемости

На рисунке 3.7 представлен интерфейс модуля учёта посещаемости. Для просмотра аудитории в окне «Устройства захвата видео (№ аудитории)» необходимо выбрать ранее установленную видеокамеру, либо добавить новую (рисунок 3.8). В окне «Присутствующие» появится список пользователей, присутствующих на данный момент в выбранной аудитории. После выбора строки с ФИО в окне «Аудитории» появится список посещённых пользователем аудиторий и время, проведённое в них.



Рисунок 3.8 – Установка новой камеры

Чтобы установить новую видеокамеру, необходимо нажать правой кнопкой на окно «Устройства захвата видео (№ аудитории)» и выбрать пункт: добавить новую видеокамеру. В отрывшемся окне необходимо ввести IP адрес и № порта камеры (рисунок 3.8). Если параметры камеры указаны верно, в окне появится изображение с новой видеокамеры.

В отличие от систем, где требуется дополнительное оборудование (распознавание по пальцу и др.), при распознавании человека по изображению лица очень легко создать копию распознаваемого объекта. Все, что необходимо, это фотография человека, которую легко можно обнаружить в интернете или сфотографировать пользователя на расстоянии. Данный программный комплекс обладает автоматической защитой от несанкционированного доступа по фотографии, видеозаписи или фотомаске лица уже существующего в базе данных. При попытках спуфинга экран монитора принимает вид, показанный на рисунке 3.9. Использование модуля подтверждения подлинности возможно при непосредственном взаимодействии пользователя с системой. Для функционирования модуля подтверждения подлинности используются методы «Установка гаммы экрана» и «Установка яркости экрана», сигнатуры которых приведены в приложении А.

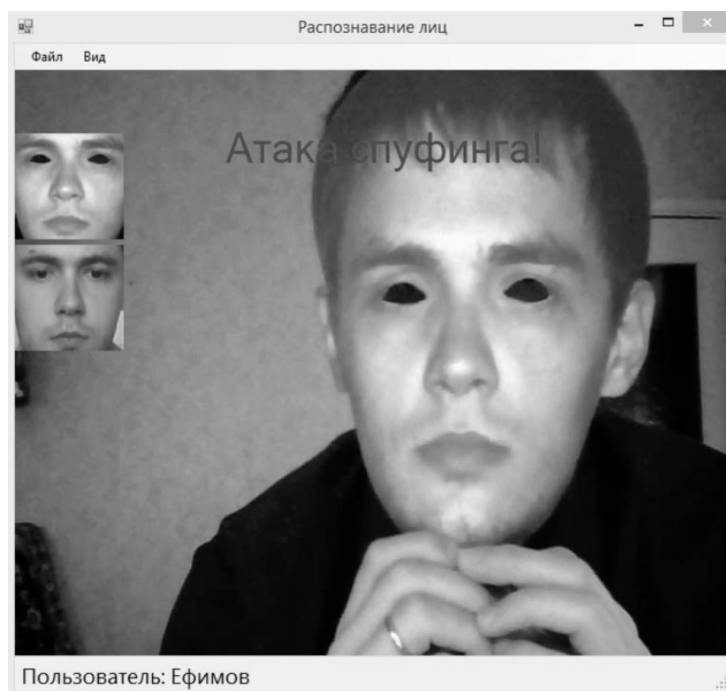


Рисунок 3.9 – Несанкционированный доступ по фотомаске

Для проведения оценки и визуализации результатов экспериментальных исследований в данной диссертационной работе используется ROC-анализ (п. 2.2.6). Каждая точка на ROC-кривой представляет собой значение вероятности распознавания на тестовой выборке при регулируемом значении пороговой функции. После проведения экспериментальных исследований, подав на вход программного комплекса тестовую выборку, необходимо рассчитать процент случаев выдачи доступа зарегистрированному пользователю (Access to Registered Person Rate, *TPR* – вертикаль графика) и процент случаев выдачи доступа к системе незарегистрированному пользователю (Access to Non-Registered Person Rate, *FPR* – горизонталь графика). Дополнительной задачей является определение площади под кривой AUC, точки отсечения и наилучшего значения пороговой функции. Для запуска экспериментальных исследований необходимо выбрать параметры информативных признаков и меру сравнения. Интерфейс модуля представлен на рисунке 3.10. Подготовленный график с ROC-кривыми и результаты исследования можно сохранить в файле с форматом XLS, XLSX и с текстовым форматом соответственно.

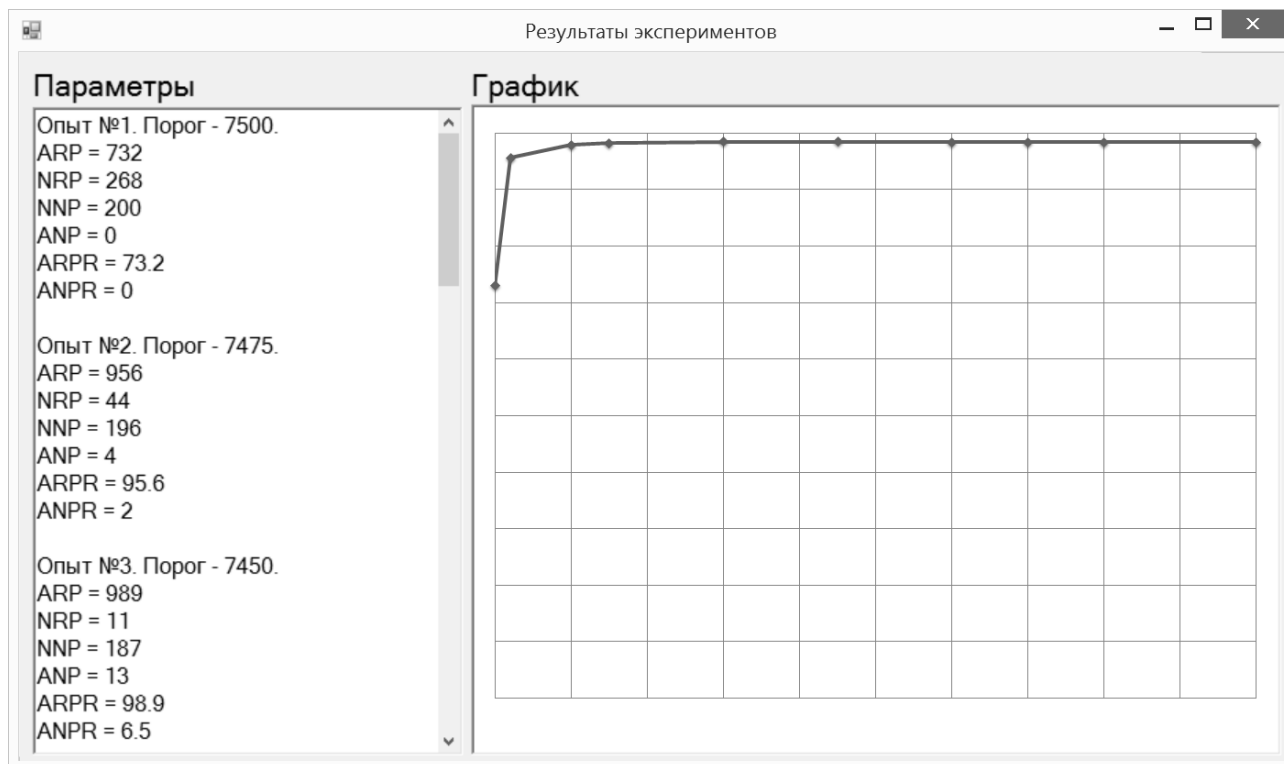


Рисунок 3.10 – Модуль оценки экспериментальных исследований

3.4 Выводы по 3 разделу

1. Реализован экспериментальный программный комплекс распознавания пользователей по изображению лица (Свидетельство о государственной регистрации программы для ЭВМ № 2013611188, 09.01.2013).

2. Представлены архитектура (п. 3.2) и объектная модель программного комплекса (п. 3.2) [3].

3. Описаны функциональные особенности клиентской и серверной частей программного комплекса (п. 3 и 3.1);

4. Приведены детальный обзор основных модулей программного комплекса и краткое руководство по применению (п.3.3).

5. Представлено описание архитектуры БД (п.3.1) (Свидетельство о государственной регистрации базы данных № 2013620323, 20.02.2013). В БД хранятся следующие данные: ФИО пользователей, исходные изображения лиц пользователей, изображения пользователей, приведённые к общей форме, информативные признаки, координаты антропометрических точек, данные результатов экспериментальных исследований и т.д.

Заключение

1. Выполнен сравнительный анализ лучших методов для распознавания пользователей по изображению лица и методов подтверждения подлинности распознаваемого объекта. Показано, что большинство существующих решений не способно комплексно решить задачу распознавания пользователей. Решения не обладают достаточной вероятностью верного распознавания образов или используют специализированное оборудование и имеют высокую стоимость реализации.

2. Предложены математическая модель информативного признака объекта, модифицированный численный метод построения гистограмм локальных бинарных шаблонов, основанный на использовании оригинальной комбинации формы шаблона и способа сравнения фрагментов информативного признака, и алгоритм численного определения информативных признаков, отличительной особенностью которого является более низкая вычислительная сложность и высокая эффективность использования в процессе распознавания образов, в частности, изображений лиц.

3. Предложена классификация известных способов подтверждения подлинности распознаваемого объекта в зависимости от воздействия на объект. Разработан, обоснован и исследован метод подтверждения подлинности распознаваемого объекта, на основе многократной оценки рассеивания яркостей сопряжённых пикселей изображений объекта. Представлен алгоритм, позволяющий обнаружить подмену объекта, предъявляемого системе контроля доступа.

4. Предложено комплексное решение задачи распознавания пользователей информационных ресурсов на основе новой информационной технологии, в отличие от существующих обеспечивающей более высокую вероятность правильного распознавания лиц пользователей за счёт использования оригинального информативного признака, а также за счёт обнаружения подмены распознаваемого объекта на фотографию, видеозапись или фотомаску лица зарегистрированного

пользователя. Технология частично инвариантна к изменениям условий освещения, наличию теней на изображении в области лица, вариациям ракурса съёмки и изменениям масштаба.

5. Разработана архитектура и выполнена реализация программного комплекса, позволяющая решить задачу распознавания пользователей информационных ресурсов по изображению лица в реальном времени.

6. Выполнены экспериментальные исследования, подтвердившие работоспособность и эффективность разработанных алгоритмов и программного комплекса распознавания пользователей по изображению лица. Для модуля распознавания изображений лиц процент случаев выдачи доступа зарегистрированному пользователю не менее 97%, а процент ошибочной выдачи доступа пользователю, не имеющему допуск, не более 2%. Для модуля подтверждения подлинности процент верного распознавания реальных объектов не менее 91%, а процент пропуска подмены – не более 10%.

Список сокращений и условных обозначений

AAM	(англ. Active appearance model) Активные модели внешнего вида.
ASM	(англ. Active shape model) Активные модели формы.
AUC	(англ. Area Under Curve) Площадь под кривой на графике.
Emgu CV	Кроссплатформенная обёртка библиотеки обработки изображений OpenCV.
FAR	(англ. False Acceptance Rate) Процент ложного совпадения биометрических характеристик двух людей.
FERET	(англ. Face Recognition Technology) База данных изображений лиц.
FPR	(англ. False Positives Rate) Ложно положительные случаи.
FRR	(англ. False Rejection Rate) Процент отказа в доступе человеку, имеющего допуск.
GLBP	(англ. Gradient local binary patterns) Локальные бинарные шаблоны градиента.
GUI	(англ. Graphical user interface) Графический пользовательский интерфейс программы.
HMM	(англ. Hidden Markov model) Скрытые марковские модели.
HOG	(англ. Histogram of oriented gradients) Гистограмма направленных градиентов.
JPEG	(англ. Joint Photographic Experts Group) Формат цифрового изображения, применяется к изображению с более 256 цветов.
LBP-TOP	(англ. Local Binary Patterns from Three Orthogonal Planes) Локальные бинарные шаблоны трёх взаимно перпендикулярных плоскостей.

LGBP	(англ. Local Gabor binary pattern) Локальные бинарные шаблоны Габора.
LPQ	(англ. Local Phase Quantization) Локальная фаза квантования.
OpenCV	(англ. Open Source Computer Vision Library) Библиотека компьютерного зрения.
ORL	(англ. Olivetti Research Laboratory) База данных изображений лиц.
PDBNN	(англ. Probabilistic Decision-Based Neural Networks) Вероятностное решение на основе нейронных сетей.
PGM	(англ. Portable Grey Map) Формат цифрового изображения, используемый как промежуточный для хранения в оттенках серого.
ROC	(англ. Receiver Operator Characteristic) Кривая, используемая для оценки результатов работы алгоритма классификации.
TPR	(англ. True Positives Rate) Истинно положительные случаи.
БД	База данных.
ЛБШ, LBP	(англ. Local binary pattern) Локальные бинарные шаблоны.
ЛБШМП, LBPMF	(англ. Local binary patterns median pixel's) Локальные бинарные шаблоны медианного пикселя.
ЛДА, LDA	(англ. Linear discriminant analysis) Линейный дискриминантный анализ.
МГК, PCA	(англ. Principal component analysis) Метод главных компонент.
ПО	Программное обеспечение.
СКД	Системы контроля доступа.
СППРО	Способ подтверждения подлинности распознаваемого объекта

Словарь терминов

АУТЕНТИФИКАЦИЯ (англ. authentication) — процедура подтверждения подлинности, например, путём сравнения введённого пользователем пароля и логина с данными, хранящимися в БД.

ИДЕНТИФИКАЦИЯ (от лат. identification — отождествлять) — процедура выявления идентификатора, однозначно идентифицирующего субъекта в информационной системе.

ИНФОРМАТИВНЫЕ ПРИЗНАКИ (англ. features) — случайные или искусственные особенности некоторого объекта.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ (от лат. modus — образ, копия, очертание) — описание объектов, процессов или явлений с помощью математических понятий.

ПОРОГ (англ. threshold) — установленное значение, в случаях, если входное значение превышает некоторый уровень (порог), входное значение считается верным.

ПРОГРАММНЫЙ КОМПЛЕКС — совокупность программ, обеспечивающая реализацию функций системы измерений и контроля процессом или измерительным экспериментом, заданное функционирование комплекса технических средств и предполагаемое развитие системы.

СПУФИНГ (англ. spoofing – подмена) — это обман биометрических систем путём предоставления биометрическому сенсору копий, муляжей, фотографий, заранее записанных звуков и т. п.

ТЕХНОЛОГИЯ (англ. technology) — совокупность методов, алгоритмов и процессов, применяемых в какой-либо отрасли.

ШУМ (англ. noise) — любая помеха, снижающая качество полезного сигнала.

Список цитируемой литературы

1. Алгулиев, Р.М. Методы обнаружения живучести в биометрических системах / Р. М. Алгулиев, Я. Н. Имамвердиев, В. Я. Мусаев // Вопросы защиты информации. – 2009. – № 3 – 86с.
2. Ананьин, М.А. Моделирование оптической обработки изображений с использованием вихревого пространственного фильтра / М. А. Ананьин, С. Н. Хонина // Компьютерная оптика. – 2009. – Т. 33. – № 4. – С. 466-473.
3. Аутентификация двухмерных изображений : свидетельство о государственной регистрации программы для ЭВМ № 2013611188 Рос. Федерация / И. Н. Ефимов, А. М. Косолапов ; ФГБОУ ВПО «Самарский государственный университет путей сообщения». – № 2012660384 ; заявл. 26.11.2012 ; опубл. 09.01.2013.
4. База данных двухмерных изображений для аутентификации : свидетельство о государственной регистрации базы данных № 2013620323 Рос. Федерация / И. Н. Ефимов, А. М. Косолапов ; заявитель и патентообладатель ФГБОУ ВПО «Самарский государственный университет путей сообщения». – № 2012621323 ; заявл. 28.11.2012 ; опубл. 20.02.2013.
5. Бибиков, С.А. Цветовая коррекция бликов на цифровых изображениях / С. А. Бибиков, Е. Ю. Минаев, А. В. Никоноров, В. А. Фурсов // Компьютерная оптика. – 2010. – Т. 34. – № 3. – С.382-391.
6. Борн, М. Основы оптики / М. Борн, Э. Вольф // М: Наука. – 1973.– 720с
7. Глумов, Н.И. Метод быстрой корреляции с использованием тернарных шаблонов при распознавании объектов на изображениях / Н. И. Глумов, Е. В. Мясников, В. Н. Копенков, М. А. Чичева // Компьютерная оптика. – 2008. – Т. 32. – № 3. – С.277-282.
8. ГОСТ Р. 19794-5–2006. Автоматическая идентификация. Идентификация биометрическая. Данные изображения лиц. – М.: Стандартинформ. – 2006. – 42с.

9. Гошин, Е.В. Метод согласованной идентификации в задаче определения соответственных точек на изображениях / Е. В. Гошин, В. А. Фурсов // Компьютерная оптика. – 2012. – Т. 36. – № 1. – С.131-135.
10. Деза, Е.И. Энциклопедический словарь расстояний / Е. И. Деза, М. М. Деза // М: Наука. – 2008. – 444с.
11. Демидович, Б.П. Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения / Б. П. Демидович, И. А. Марон, Э. З. Шувалова // Рипол Классик. – 2013. – 400с.
12. Ефимов, И. Н. Идентификация по чертам лица в системах безопасности / И.Н. Ефимов //Сборник материалов международной научно-практической конференции: Наука и инновации. г. Пшемысль, Польша. – 2012. – С. 79-80.
13. Ефимов, И.Н. Методы повышения достоверности идентификации обучаемых при дистанционном обучении / И. Н. Ефимов // Дистанционное и виртуальное обучение. – 2013. – № 8. – С. 62-73.
14. Ефимов, И.Н. Повышение точности идентификации пользователей дистанционного обучения / И. Н. Ефимов // Сборник материалов международной научно-технической конференции «Перспективные информационные технологии». – Самара: СГАУ. – 2013. – С.109-112.
15. Ефимов, И. Н. Применение нейронных сетей для распознавания лиц / И. Н. Ефимов // Дни студенческой науки: Сборник материалов XXXX научной конференции студентов и аспирантов. Самара : СамГУПС. – 2013. – №14. – С. 67-68.
16. Ефимов, И. Н. Биометрическая идентификация изображений лиц / И. Н. Ефимов // Материалы докладов конкурса программы У.М.Н.И.К. – Самара: СГАУ. – 2013. – С. 63-65.
17. Ефимов, И. Н. ИИС идентификации нарушителя по изображению лица / И. Н. Ефимов // Материалы докладов конкурса программы У.М.Н.И.К. – Самара: СГАУ. – 2014. – С. 44-46.

18. Ефимов, И.Н. Локальные бинарные шаблоны медианного пикселя – эффективные информативные признаки технологии распознавания образов / И. Н. Ефимов // Цифровая обработка сигналов. – 2015. – №1 – С. 61–65
19. Ефимов, И. Н. Анализ современных обучающих систем / И. Н. Ефимов // Дни студенческой науки: сб. материалов XXXVIII научной конференции студентов и аспирантов. - Самара : СамГУПС. – 2011. – №12. – С. 46.
20. Ефимов, И. Н. Технология идентификации обучаемых при дистанционном обучении / И. Н. Ефимов, А. М. Косолапов // Дистанционное и виртуальное обучение. – 2012. – № 12. – С. 72-78.
21. Ефимов, И. Н. Биометрическая идентификация в дистанционном обучении / И. Н. Ефимов //Сборник материалов международной научно-практической конференции: Эффективные инструменты современных наук. г. Прага, Чехия. –2012 – С. 48-49.
22. Ефимов, И. Н. Биометрическая идентификация в дистанционном обучении / И. Н. Ефимов // Дни студенческой науки: Сборник материалов XXXIX научной конференции студентов и аспирантов. – Самара : СамГУПС. – 2012. – № 13. – С. 73-74.
23. Ефимов, И. Н. Биометрическая идентификация в дистанционной подготовке кадров на ж.д. транспорте / И. Н. Ефимов, А. М. Косолапов // Вестник транспорта поволжья. – 2013. – № 1 – С. 62-66.
24. Ефимов, И.Н. Методы автоматического распознавания лиц в системах безопасности / И. Н. Ефимов, А. М. Косолапов // Перспективы развития информационных технологий: Сборник материалов XXVIII Международной научно-практической конференции. – Новосибирск.: ЦРНС. – 2016. – С.151–156.
25. Ефимов, И.Н. Классификация способов подтверждения подлинности распознаваемого объекта / И. Н. Ефимов, А. М. Косолапов // Сборник материалов международной научно-технической конференции

- «Перспективные информационные технологии». – Самара: Самарский университет. – 2016. – С.425-429.
26. Иванов, В.П. Трехмерная компьютерная графика / В. П. Иванов, А. С. Батраков, Г. М. Полищук // М.: Радио и связь. – 1995.– 224с.
 27. Козин, Н.Е. Распознавание лиц по показателям сопряженности в пространстве суммирующих инвариантов / Н. Е. Козин, В. А. Фурсов // Компьютерная оптика. – 2008. – Т. 32. – № 4. – С.400-402.
 28. Колючкин, В.Я. Алгоритмы контурной сегментации и распознавания образов объектов систем технического зрения / В. Я. Колючкин, К. М. Нгуен // Электронное научно-техническое издание «Наука и образование». Москва. – 2013. – № 4 – С. 187-201.
 29. Косолапов, А.М. Методы анализа и синтеза устройств инвариантного преобразования: Учеб.пособ. / А. М. Косолапов // Самара. СамГТУ. – 2000.– 86с.
 30. Косолапов, А.М. Автоматизация имитационного моделирования измерительного преобразователя / А. М. Косолапов, С. В. Думин // Метрология – 2008. – № 7 – С. 10-18.
 31. Косолапов, А.М. Системы управления. Методы анализа и синтеза линейных систем: Учеб.пособ. / А. М. Косолапов // Самара. СамГТУ. – 2003.– 106с.
 32. Косолапов, А.М. Параметрическая оптимизация измерителя мощности / А. М. Косолапов, С. В. Думин // Измерительная техника. – 2007. – № 10 – С. 51-53.
 33. Костылев, Н.М. Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека / Н. М. Костылев, А. В. Горевой // Инженерный журнал наука и инновации. – 2013. – № 9 – С.13.
 34. Костылев, Н.М. Обнаружение витальности человека по спектральным характеристикам кожи лица / Н. М. Костылев, Ф. А. Трушкин, В. Я. Колючкин // Вестник МГТУ им. Н.Э. Баумана. Серия “Приборостроение”. – 2012. – № 2 – С. 75-85.

35. Кузнецов, А.В. Алгоритм обнаружения дубликатов на цифровых изображениях с использованием эффективных линейных локальных признаков / А. В. Кузнецов, В. В. Мясников // Компьютерная оптика. – 2013. – Т. 37. – № 4. – С.489-495.
36. Минаев, Е.Ю. Детектирование и распознавание объектов в системах автомобильной безопасности на основе фрактального анализа / Е. Ю. Минаев, А. В. Никоноров // Компьютерная оптика. – 2012. – Т. 36. – № 1. – С.124-130.
37. Мясников, В.В. Построение эффективных линейных локальных признаков в задачах обработки и анализа изображений / В. В. Мясников // Автоматика и телемеханика. – 2010. – № 3. – С.162-177.
38. Мясников, В.В. Анализ методов построения эффективных линейных локальных признаков цифровых сигналов и изображений / В. В. Мясников, А. Ю. Баврина, О. А. Титова // Компьютерная оптика. – 2010. – Т. 34. – № 3. – С.374-382.
39. Мясников, В.В. Сравнение алгоритмов управляемой поэлементной классификации гиперспектральных изображений / В. В. Мясников, А. В. Кузнецов // Компьютерная оптика. – 2014. – Т. 38. – № 3. – С.494-502.
40. Мясников, Е.В. Численные методы и программный комплекс анализа документальных портретных изображений: дис. ... канд. техн. наук : 05.13.18 / Мясников Евгений Валерьевич. – Самара. – 2007. – 156с.
41. Попов, С.Б. Использование структурированной подсветки в системах технического зрения / С. Б. Попов // Компьютерная оптика. – 2013. – Т. 37. – № 2 – С.233-238.
42. Попов, Э.В. Алгоритмические основы интеллектуальных роботов и искусственного интеллекта / Э. В. Попов, Г. Р. Фирдман // Наука. – 1976. – 458с.
43. Прохоров, С.А. Исследование аппроксимативных возможностей радиально-базисной сети с различными функциями активации / С. А.

- Прохоров, И. А. Лёзин, И. В. Лёзина, С. К. Латыш, С. А. Саиян // Известия Самарского научного центра Российской академии наук. – 2013. – Т. 15 – № 4 – С.271–274.
44. Прудников, И.В. Исследование возможностей повышения точности идентификации информационных биометрических систем :дис. ... канд. техн. наук. : 05.25.05 / Прудников Илья Викторович. – 2012. – 163с.
 45. Пустынский, И.Н. К расчету освещенности изображения и числа сигнальных электронов в телевизионном датчике на ПЗС-матрице / И. Н. Пустынский, Е. В. Зайцева // Доклады ТУСУРа. – 2009. – № 2 – С. 5-10.
 46. Пытьев, Ю.П. Методы математического моделирования информационно-измерительных систем / Ю. П. Пытьев // М.: Физматлит. – 2004.– 400с.
 47. Ручай, А.Н. Модель атак и защиты биометрических систем распознавания диктора / А. Н. Ручай // Доклады ТУСУРа. – 2011. – № 1 – С. 96–100.
 48. Сакович, И.О. Обзор основных методов контурного анализа для выделения контуров движущихся объектов / И. О. Сакович, Ю. С. Белов // Инженерный журнал: наука и инновации. – 2014. – № 12 – С. 1-8.
 49. Самарский, А.А. Численные методы / А. А. Самарский, А. В. Гулин // М: Наука. – 1992.– 423с.
 50. Самарский, А.А. Математическое моделирование. Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов // М.: Физматлит. – 2001. – 320с.
 51. Сергеев, В.В. Применение методологии распознавания образов в задачах цифровой обработки изображений / В. В. Сергеев // Автометрия. – 1998. – № 2. – С.63–76.
 52. Сергеев, В.В. Сравнительный анализ методов нейронных сетей и иерархической аппроксимации в задачах фильтрации изображений / В. В. Сергеев, В. Н. Копенков, А. В. Чернов // Автометрия. – 2006. – Т. 42. – № 2. – С.100–106.
 53. Сойфер, В.А. Методы компьютерной обработки изображений. 2-е изд., испр / В. А. Сойфер // М.: Физматлит. – 2003. – 782с.

54. Способ идентификации личности по радужной оболочке глаза (варианты) : пат. 2407435 Рос. Федерация : МПК А 61 В 3/10 / Д. Е. Антонов ; заявитель и патентообладатель Антонов Дмитрий Евгеньевич. – № 2009128069/14 ; заявл. 22.07.2009 ; опубл. 27.12.2010.
55. Способ и устройство распознавания рельефности изображения лица : пат. 2518939 Рос. Федерация : МПК А 61 В 3/10 / И. Н. Ефимов, А. М. Косолапов; заявитель и патентообладатель ФГБОУ ВПО «Самарский государственный университет путей сообщения». – № 2013109943 ; заявл. 05.03.2013 ; опубл. 11.04.2014.
56. Тарков, М.С. Нейросетевой параллельный алгоритм слежения за объектом в реальном времени / М. С. Тарков, С. В. Дубынин // Известия Томского политехнического университета. – 2014. – № 5 – С. 78-84.
57. Фурсов, В.А. Тематическая классификация гиперспектральных изображений по показателю сопряжённости / В. А. Фурсов, О. А. Байда, С. А. Бибиков // Компьютерная оптика. – 2014. – Т. 38. – № 1. – С.154–158.
58. Фурсов, В.А. Распознавание объектов на радиолокационных изображениях с использованием показателей сопряжённости и опорных подпространств / В. А. Фурсов, Д. А. Жердев, Н. Л. Казанский // Компьютерная оптика – 2015. – Т. 39. – № 2. – С.255–264.
59. Хемминг, Р. В. Численные методы для научных сотрудников и инженеров / Р. В. Хемминг; пер. с англ., под ред. Р. Г. Гутера. М.: Наука. – 1972. – 400с.
60. Adamiak, K. Liveness detection in remote biometrics based on gaze direction estimation / K. Adamiak, D. Zurek, K. Slot // Proc. Fed. Conf. Comput. Sci. Inf. Syst. – 2015. – С. 225–230.
61. Ahonen, T. Face Recognition with Local Binary Patterns / T. Ahonen, A. Hadid, M. Pietikainen // ECCV 2004. – 2004. – С. 469-481.
62. Ahonen, T. Face description with local binary patterns: Application to face recognition / T. Ahonen, A. Hadid, M. Pietikäinen // IEEE Trans. Pattern Anal. Mach. Intell. – 2006. – № 12 – С. 2037-2041.

63. Ahonen, T. Face recognition based on the appearance of local regions / M. Pietikainen, A. Hadid, T. Maenpaa // Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on. – 2004. – С. 153-156.
64. Almaev, T.R. Local gabor binary patterns from three orthogonal planes for automatic facial expression recognition / T. R. Almaev, M. F. Valstar // IEEE Computer Society. – 2013. – С. 356-361.
65. Automatic access to an automobile via biometrics : пат. 6498970 США : A. Colmenarez, S. Gutta, M. Trajkovic ; заявитель и патентообладатель Phillips Electronics N.V. № 09/836,680 ; заявл. 17.04.2001 ; опубл. 24.12.2002.
66. Belhumeur, P.N. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection / P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman // IEEE Trans. Pattern Anal. Mach. Intell. – 1997. – Т. 19 – № 7 – С. 711-720.
67. Bhowmik, M.K. Thermal Infrared Face Recognition-A Biometric Identification Technique for Robust Security System / M. K. Bhowmik, A. N. Sarma, A. Saha, D. Bhattacharjee, D. K. Basu, G. Majumder, K. Saha, M. Nasipuri, S. Majumder // Rev. Refinements New Ideas Face Recognit. – 2011. – Т. 6 – С. 113-139.
68. Chakraborty, S. An overview of face liveness detection / S. Chakraborty, D. Das // Int. J. Inf. Theory. – 2014. – Т. 13 – № 2 – С. 11-25.
69. Chen, S. Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones / S. Chen, A. Pande, P. Mohapatra // MobiSys '14. – 2014. – С. 109-122.
70. Chingovska, I. On the Use of Client Identity Information for Face Antispoofing / I. Chingovska, A. dos Anjos // Inf. Forensics Secur. IEEE Trans. – 2015. – Т. 10 – № 4 – С. 787-796.
71. Chingovska, I. On the Effectiveness of Local Binary Patterns in Face Antispoofing / I. Chingovska, A. Anjos, S. Marcel // Biometrics Special Interest Group, 2012 BIOSIG - Proceedings of the International Conference of the. – 2012.

72. Chingovska, I. Anti-spoofing in action: Joint operation with a verification system / I. Chingovska, M. Switzerland, A. Anjos, S. Marcel // Computer Vision and Pattern Recognition Workshops (CVPRW) . – 2013. – C. 98-104.
73. Chung, K. Face recognition using principal component analysis of Gabor filter responses / K. Chung, S. Kee, S. Kim // Proc. Int. Work. Recognition, Anal. Track. Faces Gestures Real-Time Syst. ICCV'99 (Cat. No. PR00378) – 1999. – C. 11-25.
74. Cootes, T. Model-based methods in analysis of biomedical images / T. Cootes // Image Process. Oxford Univ. Press. – 2000. – C. 223-247.
75. Cootes, T.F. Active appearance models Springer / T. F. Cootes, G. J. Edwards, C. J. Taylor // Computer Vision — ECCV'98. – 1998. – C. 484-498.
76. Cootes, T.F. Training Models of Shape from Sets of Examples / T.F. Cootes, Cj. Taylor , D. H. Cooper , J. Graham // BMVC92. – 1992. – C. 1-10.
77. Cootes, T.F. Active Shape Models-Their Training and Application / T. F. Cootes, C. J. Taylor, D. H. Cooper, J. Graham // Comput. Vis. Image Underst. – 1995. – T. 61 – № 1 – C. 38-59.
78. Cox, I.J. Feature-based face recognition using mixture-distance / I. J. Cox, N.J. Princeton, J. Ghosn, P.N. Yianilos // Proceedings CVPR '96, 1996 IEEE Computer Society Conference on. – 1996. – C. 209-216.
79. Dantcheva, A. Can facial cosmetics affect the matching accuracy of face recognition systems / A. Dantcheva // Biometrics: Theory, Applications and Systems (BTAS), IEEE Fifth International Conference – 2012. – C. 391-398.
80. Duc, N.M. Your face is not your password / N.M. Duc // Black Hat Conference. – 2009. – C. 1-16.
81. Etemad, K. Face recognition using discriminant eigenvectors / K. Etemad, R. Chellappa // IEEE Int. Conf. Acoust. Speech, Signal Process. – 1996. – T. 4.
82. Freitas, P. T. LBP- TOP Based Countermeasure against Face Spoofing Attacks / F. Pereira, T. Anjos, A. Martino, J. Mario, M. Sébastien // International Workshop on Computer Vision With Local Binary Pattern Variants – ACCV. – 2013. – C. 121-132.

83. Galbally, J. Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models / J. Galbally, R. Satta // IET Biometrics – 2015. – Т. 1 – С. 1–9.
84. Green, D.M. Psychoacoustics and detection theory / D. M. Green // Journal of the Acoustical Society of America – 1960. – Т.32. – С. 1189-1203.
85. Hancock, P.J. Recognition of unfamiliar faces / P.J. Hancock // Trends Cogn. Sci. – 2000. – Т. 4. – № 9. – С. 330-337.
86. Housam, K.B. Face spoofing detection based on improved local graph structure/ K.B. Housam // Information Science and Applications (ICISA), International Conference on. IEEE. – 2014. – С. 1-4.
87. Jain, V. The Indian face database [Электронный ресурс] / V. Jain, A. Mukherjee // – 2002. Режим доступа: www.cs.umass.edu/vidit/IndianFaceDatabase.html.
88. Kalal, Z. Tracking-learning-detection / Z. Kalal, K. Mikolajczyk, J. Matas // IEEE Trans. Pattern Anal. Mach. Intell. – 2012. – Т. 34 – № 7 – С. 1409-1422.
89. Kant, C. Fake Face Recognition Using Fusion of Thermal Imaging and Skin Elasticity / C. Kant, N. Sharma // IJCSC. – 2013. – Т. 4 – С. 65-72.
90. Lades, M. Distortion invariant object recognition in the dynamic link architecture / M. Lades, J. C. Vorbrueggen, J. Buhmann, J. Lange, C. v.d Malsburg, R. P. Wuertz, W. Konen // IEEE Trans. Comput. – 1993. – Т. 42 – № 3 – С. 300-311.
91. Lawrence, S. Face recognition: a convolutional neural-network approach. / S. Lawrence, C. L. Giles, A. C. Tsoi, A. D. Back // IEEE Trans. Neural Netw. – 1997. – Т. 8 – № 1 – С. 98-113.
92. Lee, S.J. Face detection and recognition using PCA / S. Lee, I. Univ, S.Jung, J. Kwon, S. Hong // Proceedings of the IEEE Region 10. 1999. – С. 84-87.
93. Liveness detection method and apparatus of video image: пат. 8355530 США / G. Park, H. Wang, Y. Moon; заявитель и патентообладатель Samsung Electronics Co., Ltd. – № 11/889,413; заявл. 13.08.2007 ; опубл. 15.01.2013.

94. Maatta, J. Face spoofing detection from single images using micro-texture analysis / J. Maatta, A. Hadid, M. Pietikainen // Biometrics (IJCB), International Joint Conference on Biometrics, IEEE. – 2011. – С. 1-7.
95. Manjunath, B.S. A feature based approach to face recognition / B. S. Manjunath, R. Chellappa, C. von der Malsburg // Proc. 1992 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. – 1992. – С. 373-378.
96. Maresca, M.E. The Matrioska Tracking Algorithm on LTDT2014 Dataset / M.E. Maresca, A. Petrosino // Computer Vision and Pattern Recognition Workshops (CVPRW), 2014 IEEE Conference on. – 2014. – С. 720-725.
97. Method and system for identifying a person based on their tongue: пат. 8355543 США / D. Zhang, Z. Liu; заявитель и патентообладатель The Hong Kong Polytechnic University. – № 12/131,384; заявл. 02.06.2008 ; опубл. 15.01.2013
98. Methods for performing biometric recognition of a human eye and corroboration: пат. 8260008 США / J. Hanna, T. Hoyos; заявитель и патентообладатель Eyelock, Inc. – № 12/887,106; заявл. 4.09.2010 ; опубл. 21.10.2012.
99. Moghaddam, B. Bayesian face recognition / B. Moghaddam, T. Jebara, A. Pentland // Pattern Recognit. – 2000. – Т. 33 – № 11 – С. 1771-1782.
100. O'Connor, B. Facial Recognition using Modified Local Binary Pattern and Random Forest / B. O'Connor, K. Roy // International Journal of Artificial Intelligence & Applications. – 2013. – Т. 4 – № 6. – С. 1-25.
101. Ojala, T. A comparative study of texture measures with classification based on feature distributions / T. Ojala, M. Pietikäinen, D. Harwood // Pattern Recognit. – 1996. – Т. 29 – № 1 – С. 51-59.
102. Ojala, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns / T. Ojala, M. Pietikainen, T. Maenpaa // IEEE Trans. Pattern Anal. Mach. Intell. – 2002. – Т. 24 – № 7. – С. 971-987.
103. Pentland, A. View-based and modular eigenspaces for face recognition / A. Pentland, B. Moghaddam, T. Starner // Comput. Vis. Pattern Recognition, 1994. Proc. CVPR '94., 1994 IEEE Comput. Soc. Conf. – 1994. – С. 84-91.

104. Phillips, P.J. The FERET database and face-recognition algorithms / P. J. Phillips // Image and vision computing. – 1998. – Т. 16. – №. 5. – С. 295-306.
105. Plataniotis, K.N. Color image processing and applications / K. N. Plataniotis, A. N. Venetsanopoulos – Engineering Monograph: Springer Science & Business Media. – 2000. – 65с.
106. Ratha, N.K. Enhancing security and privacy in biometrics-based authentication systems / N. K. Ratha, J. H. Connell, R. M. Bolle // IBM Syst. J. – 2001. – Т. 40 – № 3 – С. 614–634.
107. Recognition method using hand biometrics with anti-counterfeiting: пат. 7983451 СИИА / B. J. Super, J. E. Crenshaw, D. A. Kuhlman; заявитель и патентообладатель Motorola Mobility, Inc.. – № 11/479,793; заявл. 30.06.2006 ; опубл. 19.06.2011
108. Rekha, P.S. Spoofing Face Recognition Using Neural Network with 3D Mask / P. S. Rekha // IJETCSE. – 2015. – Т. 14 – № 1 – С. 123-127.
109. Samaria, F.S. Parameterisation of a stochastic model for human face identification / F.S. Samaria, A.C. Harter// Applications of Computer Vision, 1994., Proceedings of the Second IEEE Workshop on. 1994. – С. 138-142.
110. Secure biometric authentication from an insecure device: пат. 20120140993 СИИА / K. L. Bruso, G. E. Newton; заявитель и патентообладатель Unisys Corp., Inc.. – № 12/960,511; заявл. 05.12.2010 ; опубл. 07.06.2012
111. Sung, K.-K. Learning human face detection in cluttered scenes / K. K. Sung, T. Poggio // Computer Analysis of Images and Patterns. –1995. – С. 432-439.
112. Swain, M.J. Color indexing / M. J. Swain, D. H. Ballard // Int. J. Comput. Vis. – 1991. – Т. 7 – № 1 – С. 11-32.
113. Thomaz, C.E. A new ranking method for principal components analysis and its application to face image analysis / C. E. Thomaz, G. A. Giralaldi // Image Vis. Comput. – 2010. – Т. 28 – № 6 – С. 902-913.
114. Trefny, J. Extended set of local binary patterns for rapid object detection / J. Trefny, J. Matas // Proc. Comput. Vis. Winter – 2010. – С. 37-43.

115. Turk, M. Eigenfaces for Recognition / M. Turk // J. Cogn. Neurosci. – 1991. – Т. 3. – № 1. – С. 71-86.
116. Viola, P. Robust real-time object detection / P. Viola, M. Jones // Int. J. Comput. Vis. – 2001. – Т. 57 – С. 137-154.
117. Weber, M. Frontal face dataset, california institute of technology [Электронный ресурс] / М. Weber, // – 1999. Режим доступа: www.vision.caltech.edu/archive.html.
118. Wei, Y. An Improved Pedestrian Detection Algorithm Integrating Haar-Like Features and HOG Descriptors / Y. Wei, Q. Tian, T. Guo // Adv. Mech. Eng. – 2013. – Т. 2013 – С. 1-8.
119. Wiskott, L. Recognizing faces by dynamic link matching. / L. Wiskott, C. von der Malsburg // Neuroimage – 1996. – Т. 4 – № 3 Pt 2 – С. 14-18.
120. Wolf, L. Descriptor based methods in the wild / L. Wolf, T. Hassner, Y. Taigman // Science (80.). – 2008. – Т. 6 – С. 1-14.
121. Yang, J. Face liveness detection with component dependent descriptor / J. Yang, Z. Lei, S. Liao // Biometrics (ICB). – 2013. – С. 1-6.
122. Yang, M.H. Detecting faces in images: A survey / M. H. Yang, D. J. Kriegman, N. Ahuja // IEEE Trans. P.A.M.I. – 2002. – Т. 24 – № 1 – С. 34-58.
123. Yu, L. A New Object Tracking Algorithm Based on the Fast Discrete Curvelet Transform. / L. Yu, X. Zhang, L. Zheng // Int. J. Signal Process. Image Process. Pattern Recognit. – 2014. – Т. 7 – № 1 – С. 1-8.
124. Zaeri, N. Thermal Face Recognition Using Moments Invariants / N. Zaeri, F. Baker, R. Dib // Int. J. Signal Process. Syst. – 2015. – Т. 3 – № 2 – С. 94–99.
125. Zhang, Z. A face antispoofing database with diverse attacks / J. Yan, S. Liu, Z. Lei // Biometrics Compendium, IEEE. – 2012. – С. 26-31.
126. Zhao, W. Discriminant analysis of principal components for face recognition / W. Zhao, R. Chellappa, A. Krishnaswamy // Proc. Third IEEE Int. Conf. Autom. Face Gesture Recognit. – 1998.

Приложение А

В таблицах А1 и А2 приведены результаты экспериментальных исследований различных комбинаций формы и размера фрагментов ЛБШМП. В тестовой выборке содержатся 2000 изображений лиц зарегистрированных пользователей и 400 изображений лиц пользователей, отсутствующих в БД. TPR (True Positives Rate) – процент случаев выдачи доступа зарегистрированному пользователю, FPR (False Positives Rate) – процент случаев выдачи доступа незарегистрированному пользователю. Значения TPR и FPR – результат ROC-анализа, полученный при точке отсечения. Комбинация формы и размера признака является наилучшей, если разница TPR и FPR максимальна.

Таблица А1 – Результаты исследований гистограмм ЛБШМП

	Радиус окрестности	Радиус фрагмента	Форма и размеры окрестности признака									
			Круг		Эллипс (Ширина/Высота)							
			TPR	FPR	4/2		3/2		2/4		2/3	
					TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
Одна окрестность	1	1	94,55	4,75	94,4	3,75	94,15	1,5	95,85	1,5	92,85	1,5
		2	90,7	2,25	95,0	4,75	93,3	1,0	95,7	2,25	92,25	1,0
		3	90,85	2,75	95,0	4,75	93,55	1,5	95,7	2,75	92,1	1,0
		4	89,95	2,25	94,85	4,75	94,7	3,25	96,55	4,25	93	2,75
	2	1	90,95	2,25	93,1	1,5	95,0	1,5	93,7	1,0	92,4	1,0
		2	95,3	7,0	93,25	2,25	95,75	2,25	95,4	3,25	91,85	0,5
		3	90,55	1,5	93,55	2,75	93,55	1,5	92,55	0,5	91,55	0,5
		4	83,5	2,25	91,95	1,5	94,0	2,25	96,3	4,25	93,7	2,75
	3	1	90,4	2,25	92,8	2,75	95,15	2,75	91,65	4,25	95,45	4,25
		2	89,95	0,5	92,65	2,75	95,15	2,75	91,25	4,25	94	3,75
		3	83,75	3,25	90,95	1,5	93,15	1,5	90,35	3,75	93,4	3,25

Таблица А2 – Результаты исследований гистограмм ЛБШМП (продолжение)

	Радиус окрестности	Радиус фрагмента	Форма и размеры окрестности признака									
			Круг		Эллипс (Ширина/Высота)							
			TPR	FPR	4/2		3/2		2/4		2/3	
					TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
Одна окрестность	3	4	89,8	13,25	90,35	1,0	93,4	3,25	89,8	3,25	91,85	2,25
	4	1	90,7	3,25	93,85	4,75	92,85	2,75	89,2	2,75	90,55	1,0
		2	88,65	0,0	90,5	1,5	91,55	1,5	89,65	3,75	93,7	4,25
		3	90,85	3,25	90,35	1,5	93,55	3,75	89,65	3,75	93,7	4,25
		4	85,95	1,5	91,1	2,25	93,0	3,25	90,5	4,75	91,7	2,25
Две окрестности	1	1	94,65	2,5	96,3	2,5	96,4	3,0	97,25	2,5	95,1	2,5
		2	98,3	6,25	96,15	2,0	96,25	3,0	95,1	0,75	94,55	2,0
		3	93,5	1,5	95,85	0,25	95,95	3,0	93,95	0,25	94,95	2,5
		4	97,15	6,25	97,1	2,0	98	5,25	94,25	0,75	96,55	7,25
	2	1	87,9	0,25	93,4	3,0	85	3,5	93,95	3,0	93,5	4,5
		2	85,75	7,25	93,95	3,0	93,25	4,0	93,65	3,5	92,65	4,0
		3	95,85	5,75	80,4	4,0	93,4	4,5	93,8	3,0	94,65	6,25
		4	96,25	6,25	94,8	5,75	96,25	7,75	90,5	3,0	85,45	2,0
	3	1	93,25	8,25	88,75	1,5	93,1	6,25	89,9	2,0	93,8	6,75
		2	90,05	5,25	90,95	4,0	95,1	9,0	89,8	4,5	83,45	3,0
		3	93,25	8,25	90,8	4,5	94,8	9,5	81,0	2,0	84,9	10,0
		4	93,1	7,25	88,75	1,5	92,65	6,25	93,4	6,25	93,25	8,25
	4	1	93,65	3,5	90,65	5,25	85,0	11,5	95,85	10,0	96,55	5,25
		2	96,0	3,0	84,3	4,0	95,7	3,5	95,7	9,0	93,5	4,5
		3	90,8	2,5	92,5	6,25	80,4	2,0	92,65	7,75	95,4	3,0
		4	95,55	2,25	95,7	9,0	96,4	4,0	82,0	2,0	93,25	1,5

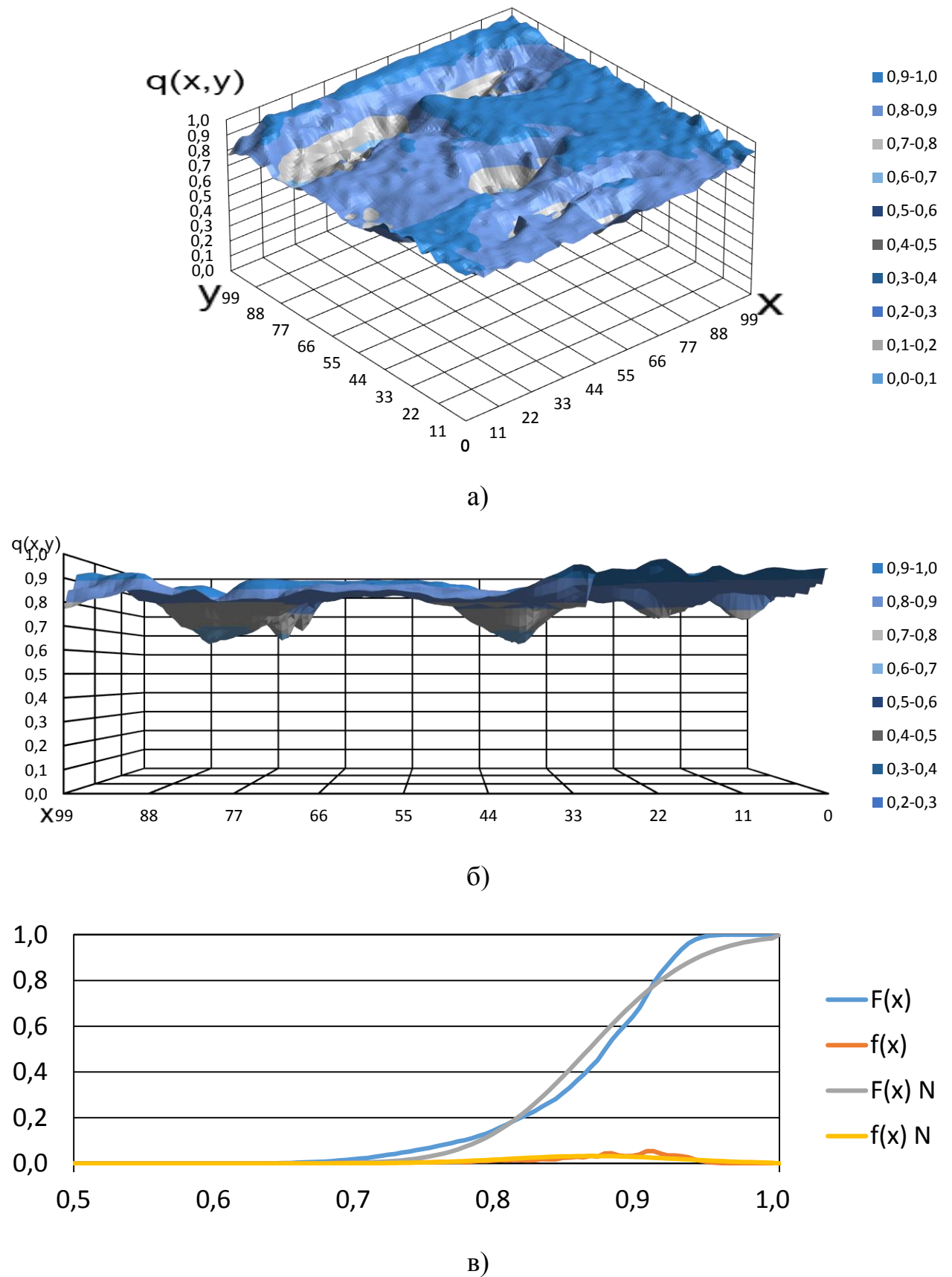


Рисунок А1 – Графики поверхности лица реального человека ($D = 0,004358$): а) вид спереди; б) вид слева; в) функция распределения и плотность вероятности

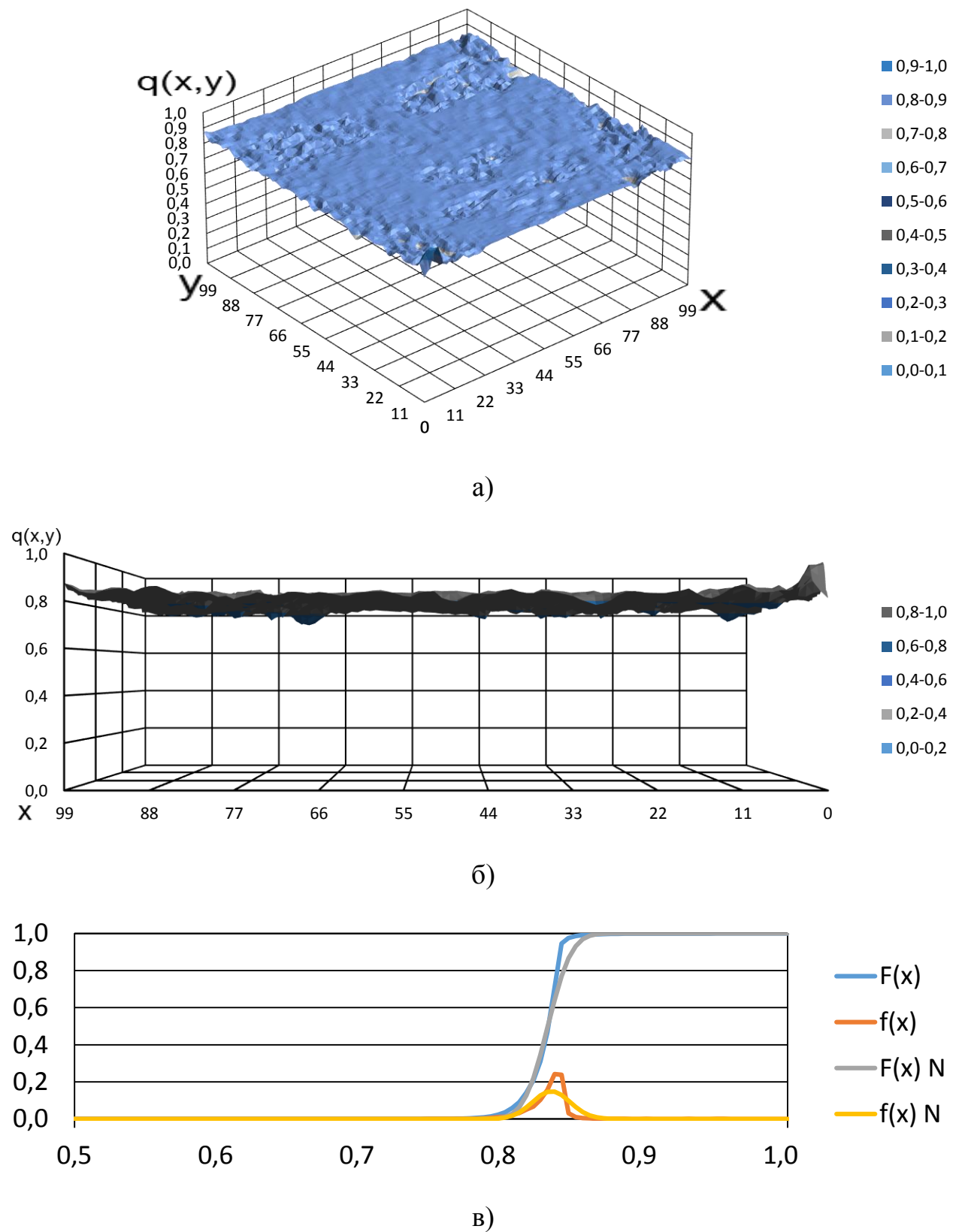


Рисунок А2 – Графики поверхности фотографии на бумажном носителе ($D = 0,000174$): а) вид спереди; б) вид слева; в) функция распределения и плотность вероятности

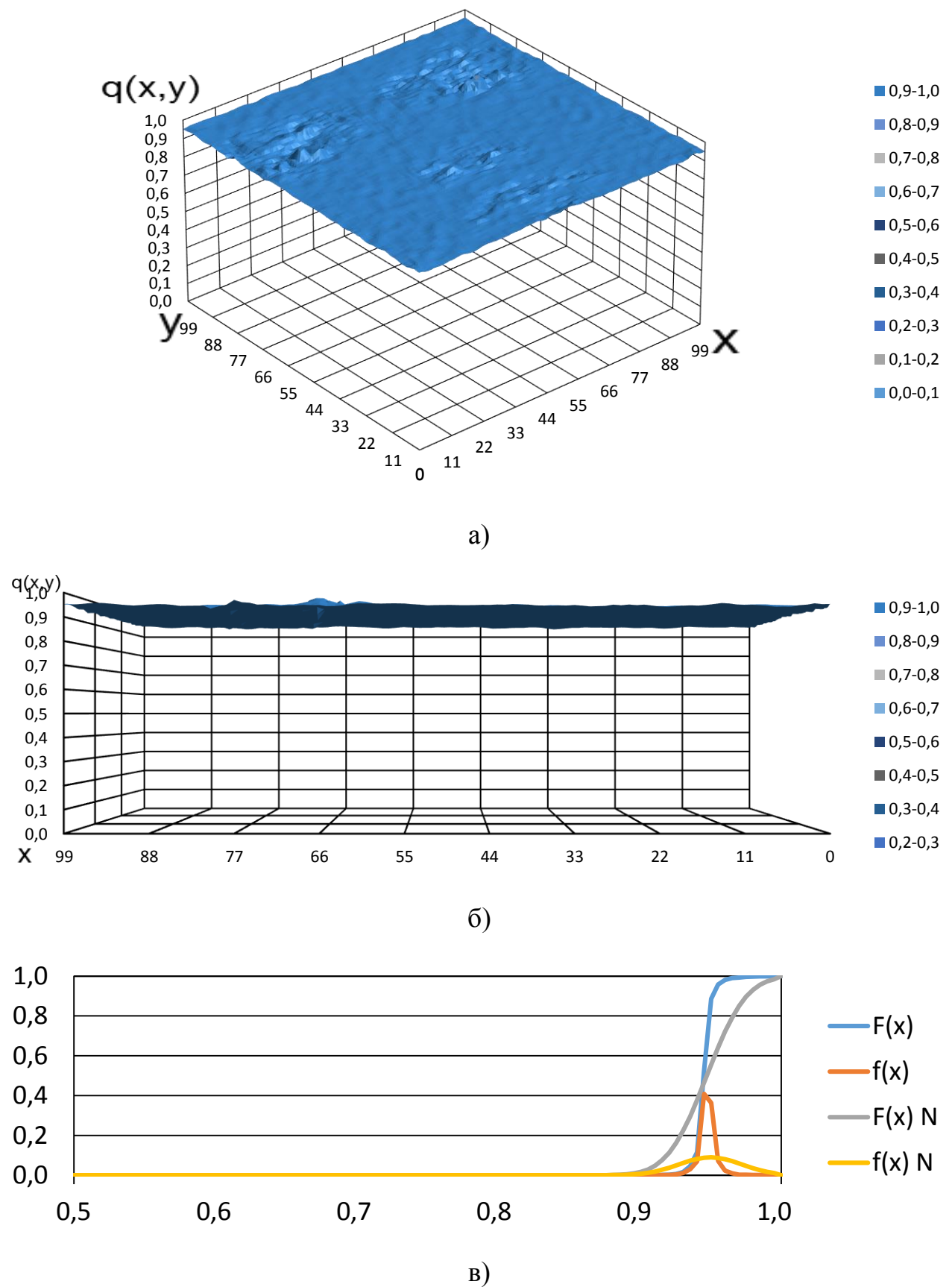


Рисунок АЗ – Графики поверхности экрана устройства ($D = 0,000039$): а) вид спереди; б) вид слева; в) функция распределения и плотность вероятности

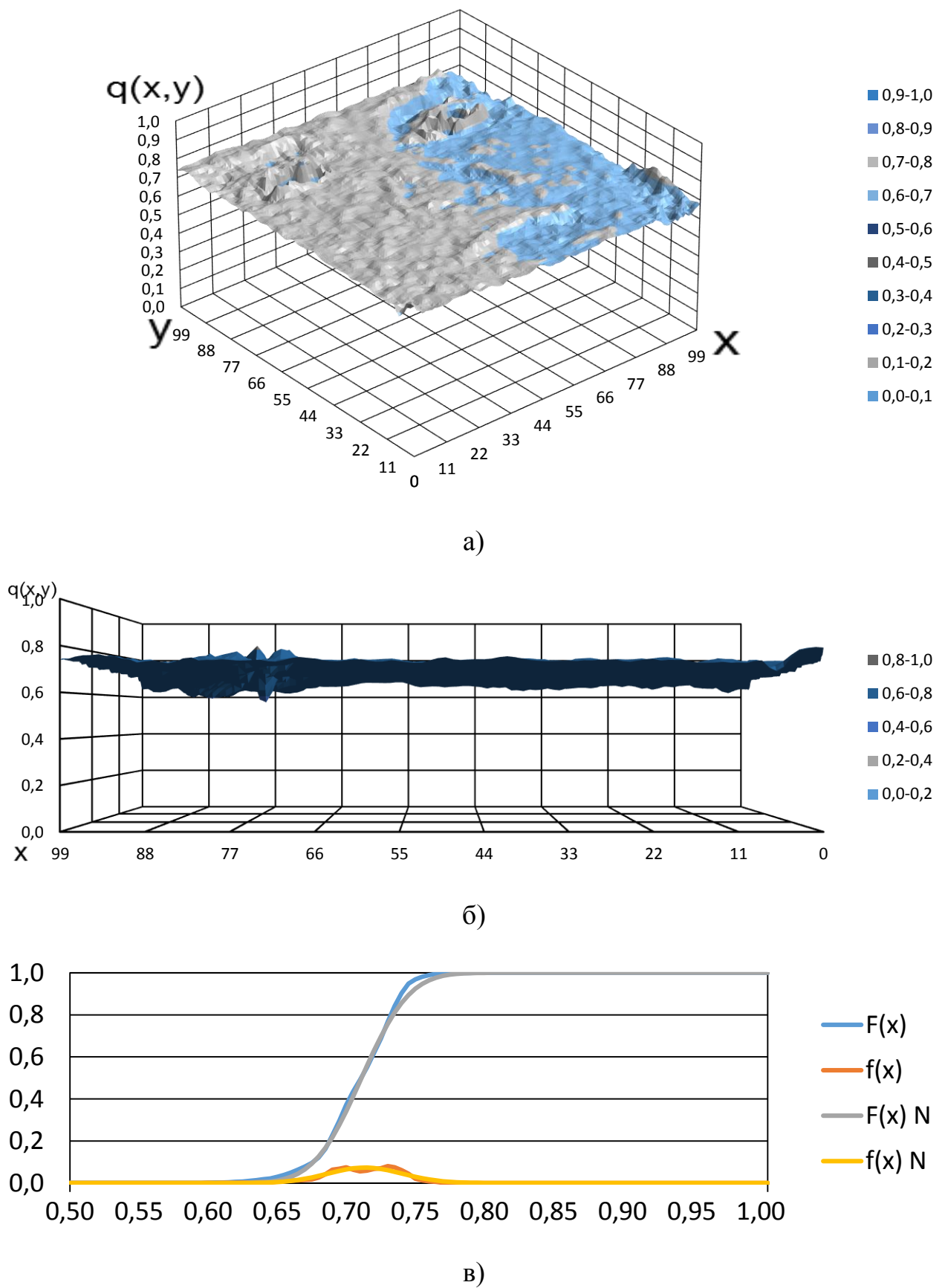


Рисунок А4 – Графики поверхности фотомаски ($D = 0,000732$): а) вид спереди; б) вид слева; в) функция распределения и плотность вероятности

Структуры и сигнатуры реализованных методов на объектно-ориентированном языке C#.

Параметры распознавания

```
namespace RecParameters
{
    public enum typeTM { Minkowski = 0, Euclidean = 1, Manhattan = 2, Che-
byshev = 3, CORREL = 4, BhattacharyyaInt = 5, Bhattacharyya = 6, Chisqr = 7, L1 =
8, INTERSECT = 9, Percentage = 10, DistanceSpoof = 11 };

    public enum typeTP { LBP = 0, ONED = 1, Brightness = 2, PatternSpf = 3 };
    public enum typeTLBP { LBPM = 0, LBPM2 = 1, FPLBP = 2, TPLBP = 3,
LBP = 4, Sobel = 5, GradientSo = 6, Shar = 7, GradientSh = 8 };

    public enum typeRec { Rec = 0, Spf = 1 };

    public struct TRecStr //Reconitin parameters
    {
        public typeRec Rec; // Тип распознавания
        public typeTM TM; // Тип метрики сравнения признаков
        public typeTP TP; // Тип информативного признака
        public typeTLBP TLBP; // Тип бинарного шаблона
        public int RF, // Радиус фрагмента
            RC, // Радиус окружности
            ST; // Номер шага сравнения
        public double THR; //Порог точки отсечения
    }
}
```

Вычисление кодов ЛБШМП

```
public static string GetLBMP(double[,] srcBmp, int i, int j, int RF, int RC, int
ST, typeTM TM, int Width, int Height)
```

Подготовка гистограммы изображения

```
public static Histogram GetHistogram(double[,] BRIGHT, TRecStr RecStr, Bit-
map bmp = null)
```

Установка гаммы экрана

```
public static void SetMonitorGamma(float Gamma)
```

Установка яркости экрана

```
public static void SetMonitorBrightness(ushort brightness)
```

Нормализация и центрирование гистограммы

```
public Histogram Normalization(Histogram Histogram)
```

Построение модели объекта лица пользователя

```
public Faces(Bitmap Bmp, HaarCascade Cascadeface, HaarCascade Cas-
cadeEye, HaarCascade CascadeMouth, int TypeSearchPoints, TRecStr RecStr = new
TRecStr(), bool OnlyOne = true)
```

Вычисление значения функции расстояния

```
public static void GetDistance (typeTM TM, ref double distance, Histogram
hist1, Histogram hist2)
```

Приложение Б

ООО "МИП "Электротехника СамГУПС"

1-й Безымянный пер., 18. г. Самара, 44306; тел. +7(987) 437-06-69 e-mail: emip@samgups.ru,
electrical.sstu@yandex.ru, ОГРН 1156318002994, ИНН 6318004079 КПП 631801001.

УТВЕРЖДАЮ:

Генеральный директор ООО
 "МИП "Электротехника СамГУПС"

В.В. Цветаев

01 2016 г.



АКТ

об использовании результатов
 кандидатской диссертационной работы
 Ефимова Ильи Николаевича

Настоящим актом подтверждается, что следующие положения и результаты диссертационной работы на соискание учёной степени кандидата технических наук Ефимова Ильи Николаевича внедрены в научную и проектную деятельность ООО "МИП "Электротехника СамГУПС":

1. Математическая модель, модификация численного метода и алгоритм численного определения информативных признаков.
2. Метод и алгоритм подтверждения подлинности распознаваемого объекта.
3. Комплексное решение задачи распознавания пользователей СКД на основе новой информационной технологии.
4. Программный комплекс распознавания пользователей по изображению лица, реализующий разработанные математические модели, методы, алгоритмы и технологии.

ООО "МИП "Электротехника СамГУПС" приобретена неисключительная лицензия на использование объектов интеллектуальной собственности, на которые получены свидетельство о государственной регистрации программы для ЭВМ № 2013611188 «Аутентификация двумерных изображений» заявка № 2012660384 от 9.01.2013, свидетельство о государственной регистрации № 2013620323 «База данных двумерных изображений для аутентификации» заявка № 2012621323 от 12.01.2013, патент РФ №2518939 «Способ и устройство распознавания рельефности изображения лица» заявка № 2013109943, в целях изготовления, применения, подготовки к продаже, продажи и иного введения в хозяйственный оборот продукта, изготовленного на основе указанных объектов интеллектуальной собственности.

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
(СамГУПС)



1-ый Безымянный пер. 18 г. Самара, 443066; тел. (846) 262-41-12, ж.д. 2-44-34, 999-52-53, факс: 262-30-76,
e-mail: rektorat@samit.ru, ИНН 6318100463 КПП 631801001, УФК по Самарской обл., (4206 СамГУПС,
л/с 20426У34880, 21426У34880) в ГРКЦ ГУ Банка России по Самарской обл. г. Самара, БИК 043601001,
р/с 40501810836012000002

УТВЕРЖДАЮ:

От _____ № _____
на № _____ от _____

Ректор Самарского государственного универ-
ситета путей сообщения



Д.В. Железнов

2014 г.

АКТ ВНЕДРЕНИЯ

Настоящим актом подтверждается, что система идентификации студентов при дистанционном обучении, разработанная Ефимовым И.Н., внедрена и используется в СамГУПС на кафедре «Информационные системы и телекоммуникации».

Система с 01.09.2013 используется в учебном процессе кафедры «Информационные системы и телекоммуникации» ФГБОУ ВПО «Самарский государственный университет путей сообщения».

Новизна основных решений реализованных в разработанной системе подтверждается свидетельствами о государственной регистрации программы для ЭВМ № 2013611188 «Аутентификация двумерных изображений» - заявка № 2012660384 от 9.01.2013 и базы данных № 2013620323 «База данных двумерных изображений для аутентификации» - заявка № 2012621323 от 12.01.2013, а также патентом № RU 2 518 939 «Способ и устройство распознавания рельефности изображения лица».

Научный руководитель работы
зав. кафедрой «ИСТ»,
д.т.н., профессор

 А.М. Косолапов

Доцент каф. ИСТ, к.т.н.

 А.П. Долгинцев

Аспирант

 И.Н. Ефимов