

Содержание

Введение.....	4
1 Методы биометрической идентификации.....	5
1.1. Сравнительный обзор методов биометрической идентификации.....	5
1.1.1. Идентификация личности по рисунку сосудов глазного дна.....	6
1.1.2. Идентификация личности по отпечатку пальца.....	7
1.1.3. Идентификация личности по 3D распознаванию лица.....	8
1.2. Перспективные методы биометрической идентификации.....	9
1.2.1. Идентификация по рисунку вен ладони.....	9
1.3. Сравнение современных методов биометрической идентификации.....	10
1.4. Формулировка цели работы.....	12
1.5. Обзор разработок в области идентификации по рисунку вен.....	13
1.5.1. Сканер Fujitsu Palmsecure.....	13
1.5.2. Сканер Купол-Биопроф.....	13
1.6. Заключение к первой главе.....	13
2 Аппаратная разработка модуля.....	14
2.1. Обзор свойств венозной крови.....	14
2.2. Устройство сканера.....	16
2.3. Сканирующая матрица.....	18
2.4. Датчик расстояния.....	20
2.5. Фильтр ближнего инфракрасного диапазона.....	21
2.6. Сборка модуля идентификации.....	22
2.7. Заключение ко второй главе.....	
3. Внешнее программное обеспечение модуля	
3.1. Методы сегментации изображения для выделения шаблона	
3.1.1.	
4 Тестирование устройства и анализа результатов.....	
Заключение.....	

ВВЕДЕНИЕ

Конфиденциальность информации является одной из составляющих информационной безопасности, а обеспечение практической реализации мер по обеспечению конфиденциальности современных информационных систем – одной из основных задач информационной безопасности.

Одним из практических средств обеспечения конфиденциальности информации являются процедуры идентификации, аутентификации и авторизации. Существуют разные методы идентификации, среди которых выделяют отдельную группу биометрических методов идентификации, где в качестве идентификатора выступает биометрия.

Под биометрией понимается система идентификации человека по его одной или нескольким биологическим или поведенческим чертам. Технологии биометрической идентификации активно используются как в частной жизни, так и в бизнесе.

Наиболее распространёнными являются методы идентификации по отпечатку пальца и распознаванию лица, которые внедряются в большой спектр устройств, в том числе и в смартфоны. Также существуют биометрические методы идентификации, которые обладают наиболее высокой точностью – идентификация по радужке и сетчатке глаза.

Однако данные методы идентификации обладают рядом существенных недостатков в определённых областях использования, например, при достаточно большом числе зарегистрированных пользователей системы идентификации. Данные недостатки зачастую не могут быть исправлены, так как биометрическая система идентификации должна отвечать ряду

требований, которые часто несовместимы друг с другом. Основными требованиями являются достаточно низкий уровень ошибок ложного доступа, ложного отказа доступа при удовлетворении требований к безопасности, удобству и конфиденциальности.

1. МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

1.1. Сравнительный обзор методов биометрической идентификации

Методы биометрической идентификации различаются прежде всего по используемым биометрическим идентификаторам, где биометрический идентификатор – это биометрический уникальный признак объекта, по которому объект можно однозначно идентифицировать. Также существуют классические идентификационные методы, например, идентификация по паролю. В отличие от небиеметрических методов, биометрические используют понятие степени подобия. Использование аутентификации по паролю дает всегда точный результат на выходе: разрешение доступа при правильном пароле и отказ при неправильном. Такой подход исключает применение вероятности подобия. Но при применении биометрических методов необходимо руководствоваться терминами коэффициентов ошибок.

В основе оценки средств биометрической идентификации лежит понятие ложного допуска и ложного недопуска. Здесь вероятностью ложного допуска (ВЛД) является частота принятия того, что биометрические образцы принадлежат одной личности, хотя это не так. Вероятностью ложного недопуска (ВЛНД) является решение, что биометрические образцы принадлежат разным личностям, что также является ошибкой.

При сравнении методов биометрической идентификации далее будут использованы показатели ВЛНД при фиксированном значении ВЛД. Можно

легко понять, что чем меньше значение ВЛНД системы при одинаковом уровне ВЛД, тем система является надёжней. Также будет рассмотрена характеристика окружающей среды, оценивающая влияние внешних свойств на работу системы. Ещё одним рассматриваемым параметром для биометрического сканера является устойчивость к подделке, то есть возможность ложного доступа при снятии биометрического образца с объекта, имитирующего признаки зарегистрированного лица. Также важным этическим фактором является простота использования сканера. Физическими параметрами самой биометрической системы идентификации является скорость работы и её стоимость.

1.1.1. Идентификация личности по рисунку сосудов глазного дна

Сканирование рисунка кровеносных сосудов глазного дна было одним из первых методов идентификации личности, обладающих достаточно высокой надёжностью. Оно берёт лучшие черты от идентификации по радужной оболочке и по венам руки. Для реализации метода достаточно внешней подсветки глазного дна, чтобы различить капилляры. Уникальность рисунка сосудов сетчатки была доказана ещё в 1935 году [4]. Рисунок этих капилляров неподвижен по своей структуре, не изменяется с возрастом. Изменения возможны только при некоторых болезнях, затрагивающих глазное дно, например, катаракте. При этом, полученные образцы будут различаться даже у близнецов (Рисунок 2)

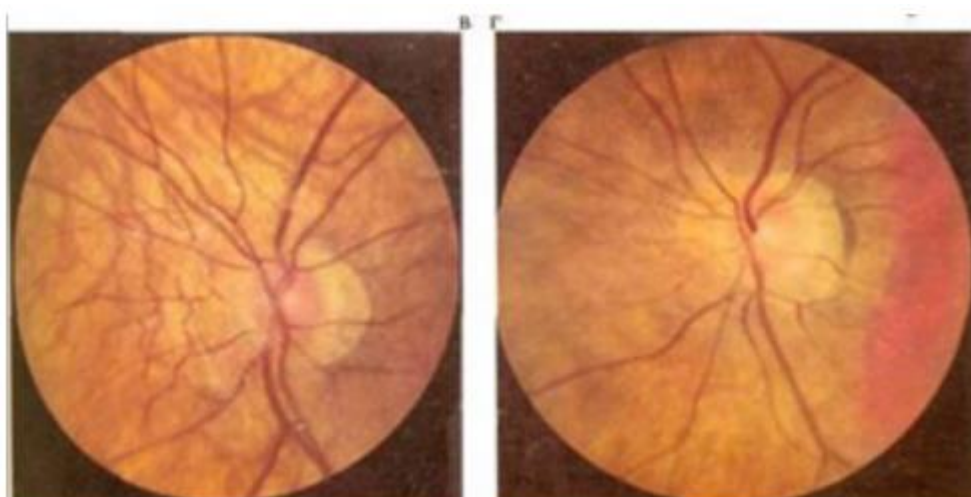


Рисунок 1 - Биометрические образцы сетчатки близнецов

Само сканирование заключается в инфракрасной подсветке окуляра, в который смотрит человек, и снятии изображения глазного дна, в котором выделяется рисунок кровеносных сосудов.

Одной из проблем данного метода биометрической идентификации является психологический фактор, поскольку процедура сканирования может вызвать дискомфорт у субъекта сканирования. Также нельзя упускать и техническую сложность устройства сканера, которым является дорогостоящая оптическая система. К тому же время работы данной системы достаточно велико, что опять же может вызвать дискомфорт у субъекта сканирования.

Ошибки сканировании происходят из-за отклонений головы субъекта сканирования и неверной фокусировкой им взгляда на удаленном источнике света. При этом, технически пока невозможно изготовить муляж, способный обмануть систему.

Сканирование сетчатки глаза пользуется особой популярностью в СКУД на секретных и государственных объектах, поскольку данные системы обладают одним из самых низких процентов отказа в доступе среди зарегистрированных субъектов и почти невозможным ошибочным разрешением доступа. По данным компании EyeDentify [5], для сканера ICAM2001 при ВЛД=0,0001% значение ВЛНД составляет 0,4%.

1.1.2. Идентификация личности по отпечатку пальца

Использование отпечатков пальцев для идентификации личности началось в первой половине XX века в криминалистике. На сегодняшний день дактилоскопия является самым распространённым и доступным методом биометрической идентификации. Папиллярный узор каждого человека уникален, что позволяет принять этот фактор за основу для идентификации.

Идентификация по отпечатку пальца начала переходить на автоматизацию в конце 1960-х годов вместе с появлением компьютерных технологий.

Отпечаток пальца обычно выглядит как серия темных линий, которые представляют собой высокую, выступающий гребень, в то время как впадина между этими гребнями выглядит как белое пространство и представляет собой низкую неглубокую часть.

Для получения цифрового изображения поверхности отпечатка пальца используются различные типы датчиков - оптические, емкостные, ультразвуковые и тепловые. Оптические датчики снимают изображение отпечатка пальца и сегодня являются наиболее доступными и распространенными датчиками.

Также стоит отметить, что время, затрачиваемое на идентификацию, в современных системах не превышает 1 с, в зависимости от числа зарегистрированных пользователей.

Статистические данные ВЛД и ВЛНД были предоставлены VeriFinger SDK [6], полученные при помощи сканера отпечатков пальцев DP U.are.U. При ВЛД=0,001% значение ВЛНД составляет 0,6%.

1.1.3. Идентификация личности по 3D распознаванию лица

Распознавание лиц в 3D стало тенденцией исследований как в промышленности, так и в академических кругах. Он наследует преимущества

традиционного 2D-распознавания лиц, такие как естественный процесс распознавания и широкий спектр приложений. Более того, системы трехмерного распознавания лиц могут точно распознавать человеческие лица даже при тусклом свете и с различными положениями лица и выражениями, в таких условиях системы распознавания двумерных лиц будут иметь огромные трудности в эксплуатации.

Для получения трехмерных образцов лица требуется специальное оборудование, которое можно разделить на активные системы сбора данных и пассивные системы сбора данных в зависимости от используемых технологий. Активные системы сбора данных активно излучают невидимый свет, например, инфракрасные лазерные лучи, чтобы осветить целевое человеческое лицо. Затем системы измеряют отражение, чтобы определить особенности формы лица цели.

В iPhone X используется Face ID - технология, которая позволяет разблокировать телефон с помощью сканирования в инфракрасном и видимом свете, чтобы однозначно идентифицировать лицо субъекта. Он работает в различных условиях и полностью безопасен.

Полные данные о ВЛНД и ВЛД для алгоритмов этого класса на сайтах производителей открыто не приведены. Но для моделей фирмы Bioscript (3D EnrolCam, 3D FastPass) [7] при ВЛД = 0,0005% ВЛНД составляет 0,1%.

Считается, что статистическая надежность метода сравнима с надежностью метода идентификации по отпечаткам пальцев.

1.2. Перспективные методы биометрической идентификации

На сегодняшний день имеется множество разработок в области перспективных методов биометрической идентификации. Среди них выделяют такие методы, как ДНК-идентификация, идентификация по запаху тела, идентификация по тону сердца, идентификация по эмоциональному состоянию и мимике, идентификация по рисунку вен ладони. Однако данные

методы, за исключением последнего, ещё недостаточно изучены, чтобы сравниться по характеристикам с распространёнными методами идентификации. Идентификация по рисунку вен ладони является перспективным методом, который способен сравниться по характеристикам с распространёнными методами биометрической идентификации.

1.2.1. Идентификация по рисунку вен ладони

Идентификация путем сканирования вен ладони прочно зарекомендовала себя как метод обеспечивающий достаточно высокий уровень безопасности. В отличие от упоминавшихся ранее методов, таких как технология идентификации по сканированию отпечатка пальца, геометрии рук и лица, васкулярное сканирование обладает явным преимуществом, поскольку рисунок вен у совершеннолетнего человека не меняется с возрастом, рисунок вен практически невозможно подделать, а также на сканирование не влияют внешние дефекты кожи. Можно заметить, что данный метод имеет некоторое сходство с методом сканирования сетчатки глаза, поскольку за объект сравнения также берётся рисунок кровеносных сосудов. К тому же сканирование сетчатки глаза на сегодняшний день является одним из самых надёжных биометрических методов. Однако васкулярное сканирование лишено основного недостатка систем сканирования сетчатки – негативного психологического фактора. К тому же глаза более подвержены болезням, влияющим на рисунок сосудов, например, катаракте.

Значение ВЛНД и ВЛД приведено для сканера Fujitsu PalmSecure. Согласно данным разработчика, при ВЛД = 0,00008%, ВЛНД составляет 0,01%.

1.3. Сравнение современных методов биометрической идентификации

Для самых популярных на сегодняшний день методов биометрической идентификации средние значения FAR и FRR выглядят следующим образом:

Таблица 1 – Сравнительный анализ характеристик FAR и FRR

Метод идентификации	ВЛД	ВЛНД
Отпечаток пальца	0,001%	0,6%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,00008%	0,01%

Следует также учитывать возможность фальсификации объекта сканирования. Данный фактор по каждому методу указан в Таблице 2.

Таблица 2 – Сравнительный анализ возможности фальсификации

Метод идентификации	Устойчивость к подделке
Отпечаток пальца	Низкая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Высокая

При сканировании большую роль играют внешние факторы. Влияние этих факторов на результат указана в Таблице 3.

Таблица 3 – Чувствительность методов идентификации к внешним факторам

Метод идентификации	Чувствительность к влиянию внешних факторов
Отпечаток пальца	Высокая
Распознавание лица 2D	Высокая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Средняя

Также рассматриваются такие факторы как скорость работы и возможность бесконтактной аутентификации в Таблице 4 и Таблице 5

Таблица 4 – Сравнительный анализ скорости аутентификации

Биометрическая СКУД использует:	Скорость идентификации
Отпечаток пальца	Высокая
Распознавание лица 2D	Средняя
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Высокая
Сетчатка глаза	Низкая
Рисунок вен	Высокая

Таблица 5 – Возможность бесконтактной идентификации

Биометрическая СКУД использует:	Возможность бесконтактной идентификации
Отпечаток пальца	Отсутствует
Распознавание лица 2D	На большом расстоянии
Распознавание лица 3D	На небольшом расстоянии
Радужная оболочка глаза	На большом расстоянии
Сетчатка глаза	Отсутствует
Рисунок вен	На небольшом расстоянии

Делая общий вывод к приведённым таблицам, можно сказать, что наиболее выигрышным в сфере безопасности и удобства использования на сегодняшний день являются методы сканирования сетчатки глаза и васкулярное сканирование. Однако первый метод обладает достаточно большой стоимостью реализации. Стоит сказать, что стоимость сканеров сетчатки глаза может в десятки раз превышать стоимость сканеров вен. Обусловлено это технической сложностью исполнения сканирования сетчатки глаза.

1.4. Формулировка цели работы

Как уже было сказано ранее, метод идентификации по рисунку вен обладает преимуществами по сравнению с остальными и требует дальнейшего изучения. Однако, стоит отметить, что данный метод всё равно является куда затратнее, чем распространённые методы идентификации: 3D-сканирования лица и идентификация по отпечатку пальца. Идентификация методом

сканирования вен ладони может быть реализована в том же ценовом сегменте, что и выше перечисленные методы, при этом приблизившись по показателям ВЛД и ВЛНД к данным методам.

Целью работы является программно-аппаратная разработка модуля идентификации по рисунку вен ладони, соответствующего требованиям стоимости для метода идентификации по отпечатку пальца. В ходе работы будет разработан программно-аппаратный модуль идентификации, для извлечения биометрических идентификаторов, а также программное обеспечение для выделения шаблона из изображения.

1.5. Обзор разработок в области идентификации по рисунку вен

1.5.1. Сканер Fujitsu PalmSecure

На сегодняшний день лидером в области идентификации по рисунку вен является японская компания Fujitsu. Данная организация обладает самой обширной на сегодняшний день базой изображений ладоней, снятых с помощью сканера. База насчитывает более 150000 изображений, что представляет огромные возможности для машинного обучения. Однако она была собрана для коммерческого использования, что делает невозможным её использование в открытом доступе.

Сканеры PalmSecure обладают лидирующими показателями ВЛД и ВЛНД среди всех имеющихся разработок, однако обладают достаточно высокой стоимостью. Для получения изображения сканер использует длину волны 760 нм.

1.5.2. Сканер КУПОЛ-БИОПРОФ

Данный сканер является отечественной разработкой в области идентификации по рисунку вен. Стоит отметить, что большинство имеющихся

на сегодняшний день разработок повторяют технологию Fujitsu, имея при этом лишь небольшие различия. В данном случае сканеры не являются бесконтактными, что является достаточно большим минусом для устройства.

1.6. Заключение к первой главе

В данной главе были рассмотрены распространённые на сегодняшний день методы биометрической идентификации. Также были рассмотрены перспективные методы биометрической идентификации, среди которых метод идентификации по рисунку вен ладони был сравнен с распространёнными методами. Было показано, что данный метод не уступает распространённым методам биометрической идентификации, но нуждается в дальнейшей разработке. Также была поставлена цель работы и проведён анализ разработок в области васкулярной идентификации.

2. АППАРАТНАЯ РАЗРАБОТКА МОДУЛЯ

2.1. Обзор свойств венозной крови

Метод биометрической идентификации по рисунку вен ладони основывается на свойстве крови поглощать излучение в ближнем инфракрасном (ИК) диапазоне. При формировании изображений в данном спектре на снимке можно увидеть немного затемнённые пути вен.

При этом, стоит отметить, что основная составляющая крови – гемоглобин. При васкулярной идентификации в зону сканирования попадают разные фракции гемоглобина, имеющие различные спектры поглощения. Наиболее распространённые фракции – оксигемоглобин и дезоксигемоглобин. Спектры их поглощения можно увидеть на Рисунке 2.

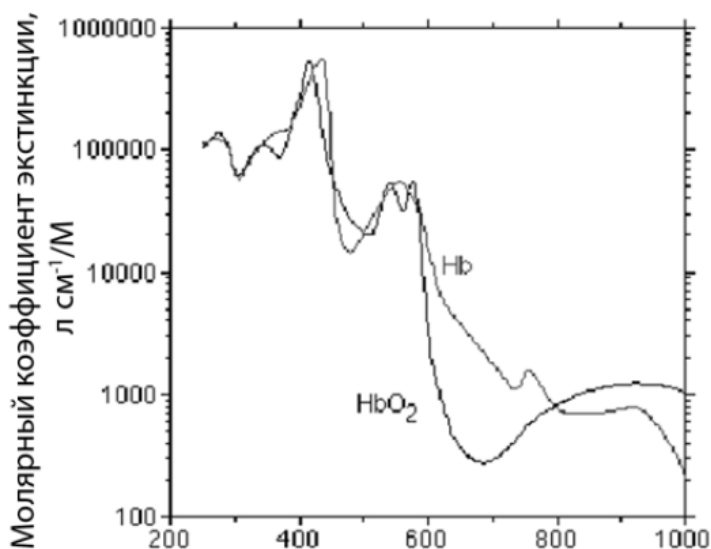


Рисунок 2 - Спектры поглощения оксигемоглобина и дезоксигемоглобина

На Рисунке 2 отчетливо видно, что наибольший коэффициент поглощения для обеих фракций лежит в видимом спектре. Однако этот участок спектра не подходит для метода васкулярной идентификации, поскольку в видимом спектре изображение вен перекрывают кожные покровы.

Интересующий нас диапазон лежит в ближнем инфракрасном спектре. В работе [КР] было продемонстрировано, что диапазон, где коэффициент

поглощения крови принимает максимальные значения ограничен 664-932 нм. При этом, стоит учитывать, что локальным минимумом в выбранном диапазоне является длина волны 730 нм.

Дальнейшую аппаратная разработка была произведена с учетом данных свойств крови, а также имеющихся технических возможностей.

2.2. Устройство сканера

На данном этапе разработки различают два типа конструкции сканера. Первый метод основан на принципе сквозного просвечивания. Конструкция такого сканера изображена на Рисунке 3.

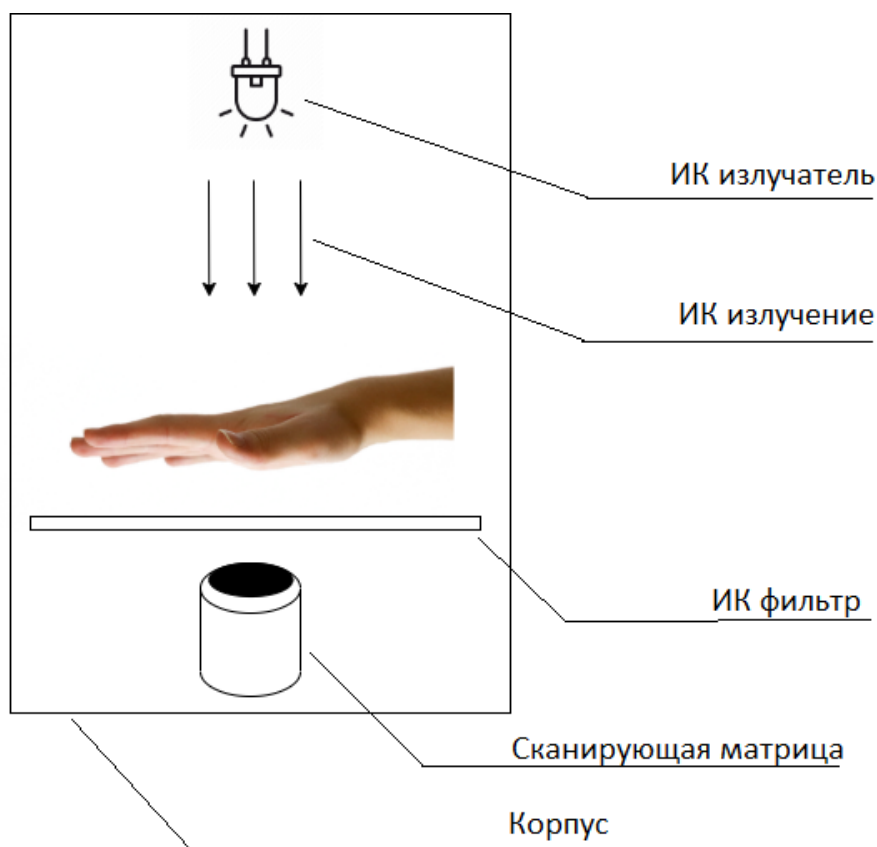


Рисунок 3 - Конструкция сканера, использующего метод просвечивания

За счет того, что сам процесс сканирования происходит внутри корпуса устройства, увеличивается качество изображений вен на снимках, так как рассеивание лучей излучателя в окружающую среду сведено к минимуму.

Однако данный метод имеет недостатки в виде достаточно громоздкого корпуса и неудобства использования пользователями.

Второй метод построен на эффекте отражения. Здесь и сканирующая матрица, и инфракрасный излучатель находятся с одной стороны. Лучи ИК диапазона, исходящие от излучателя, отражаются от ладони, частично поглощаясь венозной кровью, и попадают на матрицу. Конструкционная схема изображена на Рисунке 4.



Рисунок 4 - Конструкция сканера, использующего метод отражения

Данный метод даёт преимущества в виде компактного корпуса, удобства использования, однако изображения, выходящие со сканера, обладают качеством худшим, чем при использовании первым методом, так как часть излучения рассеивается в окружающей среде.

Несмотря на достаточно серьёзный недостаток, второй метод получил большее распространение среди производителей биометрических сканеров. В данной работе также принято решение использовать конструкцию, использующую метод отражения.

2.3. Сканирующая матрица

Сканирующая матрица, входящая в конструкцию модуля, должна соответствовать двум требованиям: обладать достаточно высоким качеством снимков и иметь диапазон, включающий ближнее ИК излучение. Высокое качество снимков необходимо прежде всего с учетом того, что при создании шаблона интересующая область будет обрезана, то есть шаблон будет обладать худшим качеством, чем исходный снимок.

Стоит отметить, что современные матрицы, использующие технологию «комплементарная структура металл-оксид-полупроводник» (КМОП), обладают достаточным качеством изображений при низкой стоимости, в отличие от матриц, использующих технологию «прибор с зарядовой связью» (ПЗС).

Необходимое условие в виде регистрации излучения в ближнем ИК диапазоне на сегодняшний день выполняют почти все КМОП-матрицы. Следовательно, под данное условие подпадают любые камеры видимого диапазона, использующие в своей основе КМОП-матрицу с удалённым, а также с удалённым объектива ИК-фильтром.

В данной работе был выбран модуль камеры FLN_H62. Данная матрица обладает следующими характеристиками:

- Матрица КМОП: 2 млн. пикселей;
- Разрешение снимков: 1280 на 720 пикселей;
- Угол обзора объектива: 48 градусов.

Ключевым фактором в выборе данной камеры была её низкая стоимость при высоких значениях характеристик. Также с объектива камеры был удален фильтр, отсекающий ближнее ИК излучение. Процесс удаления фильтра изображен на Рисунке 5.

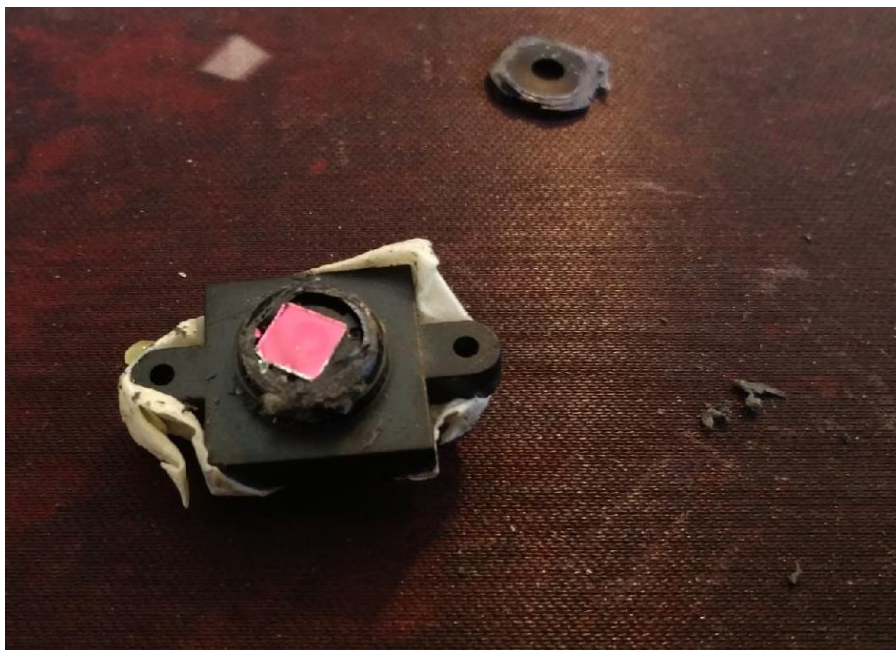


Рисунок 5 - Удаление ИК фильтра с объектива матрицы

После удаления фильтра снимки, поступающие с камеры, получили искажение цвета. При этом, рисунок вен руки стало возможно различить даже без вспомогательной подсветки. Пример снимка изображен на Рисунке 6.

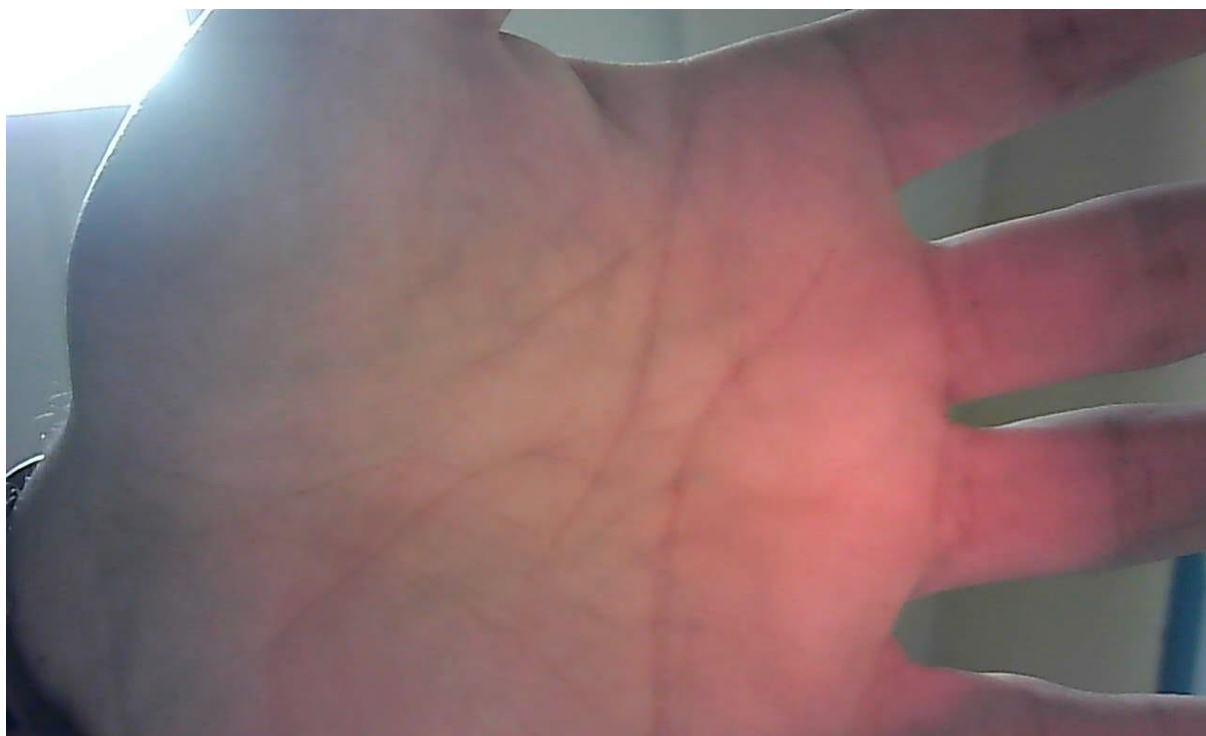


Рисунок 6 - Пример снимка ладони на камеру без ИК фильтра

2.4. Датчик расстояния

Датчик расстояния как физическое устройство не было включено в схему конструкции сканера, однако без него невозможно автоматическое использование модуля. Для начала цикла идентификации необходимо распознать, что пользователь хочет начать процесс идентификации. Для этого в схему включается датчик расстояния, чтобы регистрировать появление ладони на некотором расстоянии от модуля.

На сегодняшний день доступны несколько видов датчиков расстояния. Наиболее распространённые виды датчиков расстояния:

- Лазерные
- Ультразвуковые

Наиболее точными являются лазерные датчики расстояния, однако из-за того, что в своём большинстве данные лазеры работают в ближнем ИК диапазоне и могут помешать работе сканера, а также из-за достаточно высокой стоимости далее рассматриваться не будут.

Ультразвуковые датчики расстояния уступают по точности и скорости работы лазерным, но имеют низкую стоимость и полностью удовлетворяют беспрепятственной работе сканера.

В данной работе был выбран ультразвуковой датчик расстояния US-026, изображённый на Рисунке 7.



Рисунок 7 - Датчик расстояния US-026

Датчик расстояния US-026 обладает следующими техническими характеристиками:

- Дальность измерения: 2 – 600 см;
- Точность измерения: 0.2 см;
- Угол измерения: 15 градусов.

Учитывая тот факт, что угол обзора объектива камеры позволяет сделать снимок ладони целиком на расстоянии от 20 см, то данный датчик подходит для успешной работы модуля.

2.5. Фильтр ближнего инфракрасного диапазона

В разделе 2.1 описывалось свойство венозной крови поглощать излучение ближнего ИК диапазона. Чтобы наиболее точно зарегистрировать данный эффект между сканирующей матрицей и идентификатором помещается светофильтр, пропускающий некоторую полосу частот в ближнем ИК диапазоне. Данный фильтр необходимо выбирать в диапазоне от 664 до 932 нм.

На данный момент наиболее распространены и доступны светофильтры на 720 нм, 760 нм, 850 нм, 950 нм и 980 нм.

Фильтры со значениями 720 нм и 760 нм достаточно затруднительно использовать, так как при выборе длины волны фильтра также выбирается и длина волны ИК излучателей. Светодиоды с излучаемой длиной волны 720 нм и 760 нм обладают достаточно высокой стоимостью и труднодоступны. К тому же в работе [КР] было показано, что на значениях, близких к 730 нм происходит спад коэффициента поглощения ИК излучения крови.

Основываясь на Рисунке 2, для данной работы был выбран фильтр с пропускаемой длиной волны 850 нм.

2.6. Сборка модуля идентификации

(построить в компасе модельку и собрать заново)

3. ВНЕШНЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОДУЛЯ

3.1. Методы сегментации изображения для выделения шаблона

Поскольку для дальнейших процессов аутентификации и авторизации будут использоваться шаблоны, основывающиеся на идентификаторах пользователей, то крайне важен уровень точности сделанного шаблона.

После того как идентификационный модуль сделал изображение, происходит сегментация полученного рисунка до области шаблона или так называемого «региона интереса» (англ. region of interest, ROI).

Далее будут представлены различные методы вычисления ROI, сравнение данных методов, а также тестирование на собранном модуле.

3.1.1. Метод сегментации по центроиду и двум точкам

Данный метод получения ROI является одним из самых простых. Общий алгоритм метода изложен на Рисунке 8.

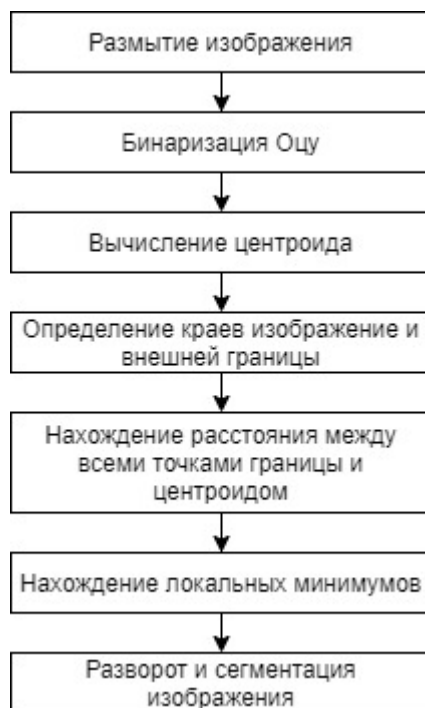


Рисунок 8 - Алгоритм вычисления ROI по центроиду и двум точкам

В данном алгоритме особую роль играет бинаризация Оцу. Бинаризация Оцу – алгоритм, по которому вычисляется порог бинаризации. Данный алгоритм широко распространён в области компьютерного зрения.

Суть алгоритма заключается в том, чтобы разделить изображение на два класса: классы полезных и фоновых пикселей. Разделение на классы осуществляется посредством вычисления порога бинаризации. Порог бинаризации вычисляется путём решения задачи максимизации межклассовой дисперсии (1).

$$\sigma_b^2 = \omega_1 \omega_2 (a_1 - a_2)^2, \quad (1)$$

где ω_1 и ω_2 - вероятности первого и второго классов, a_1 и a_2 средние арифметические значения для каждого из классов.

Результат выполнения бинаризации Оцу с помощью изображения (Рисунок 9), предоставленного разработанным аппаратным модулем, прошедшего операцию размытия (Рисунок 10), представлен на Рисунке 11.



Рисунок 9 - Изображение, полученное с модуля



Рисунок 10 - Изображение после операции размытия



Рисунок 11 - Изображение после бинаризации Оцу

Вычисление центроида осуществляется путем нахождения моментов изображения, где моментом изображения является конкретное

средневзвешенное значение интенсивности пикселей изображения. Вычисление центроида можно увидеть в формуле (2).

$$\begin{aligned} C_x &= \frac{M_{10}}{M_{00}} \\ C_y &= \frac{M_{01}}{M_{00}} \end{aligned}, \quad (2)$$

где C_x и C_y – координаты центроида.

Определение центроида и внешней границы можно увидеть на рисунках 12 и 13 соответственно.

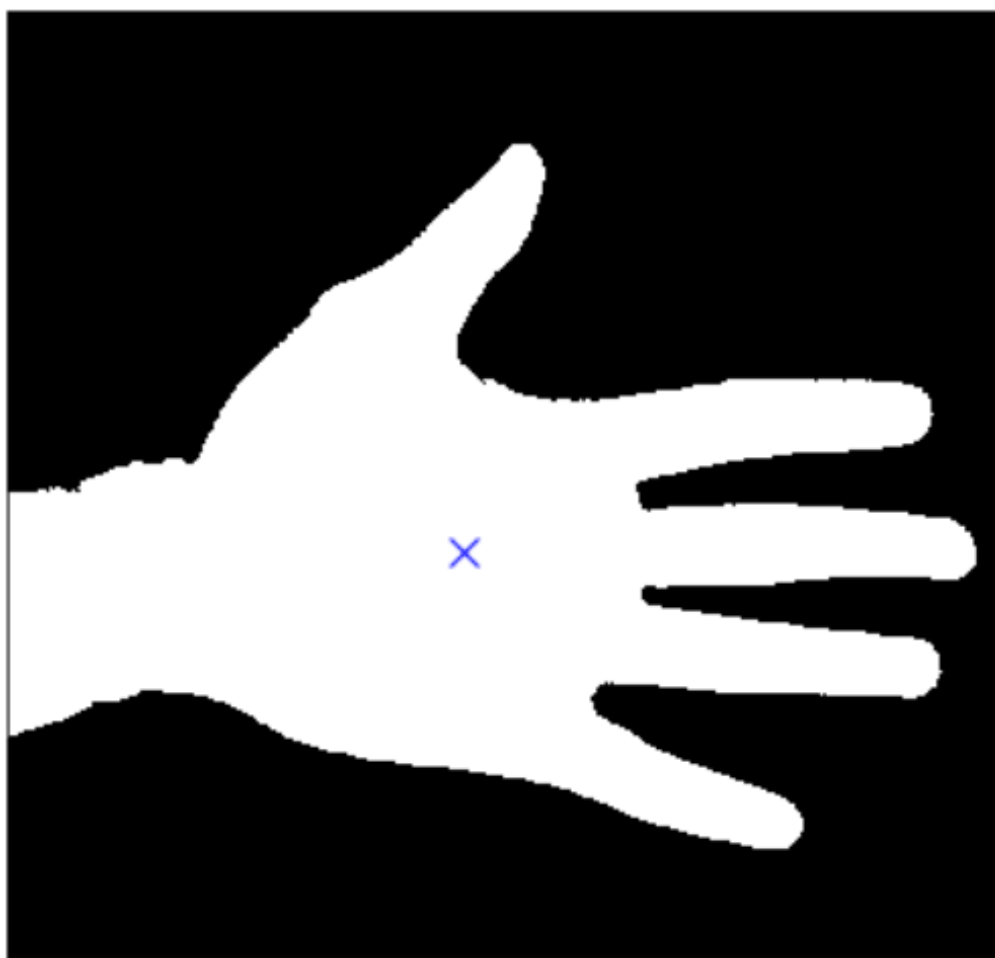


Рисунок 12 - Определение центроида

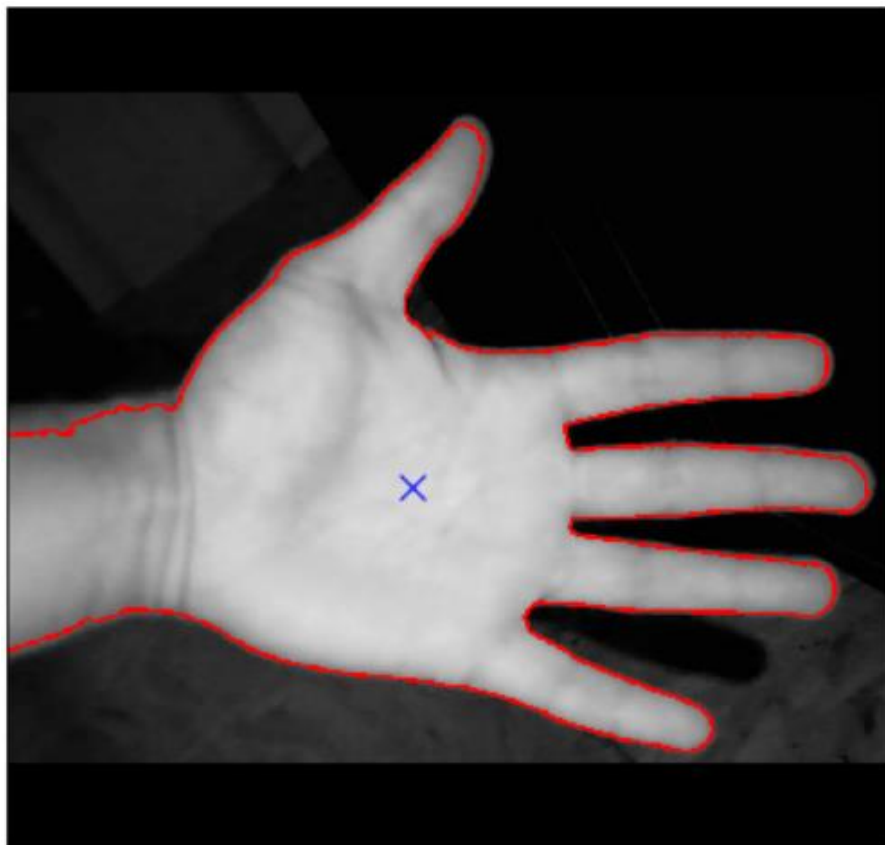


Рисунок 13 - Определение внешней границы ладони

Нахождение опорных точек по локальным минимумам изображено на Рисунке 14.

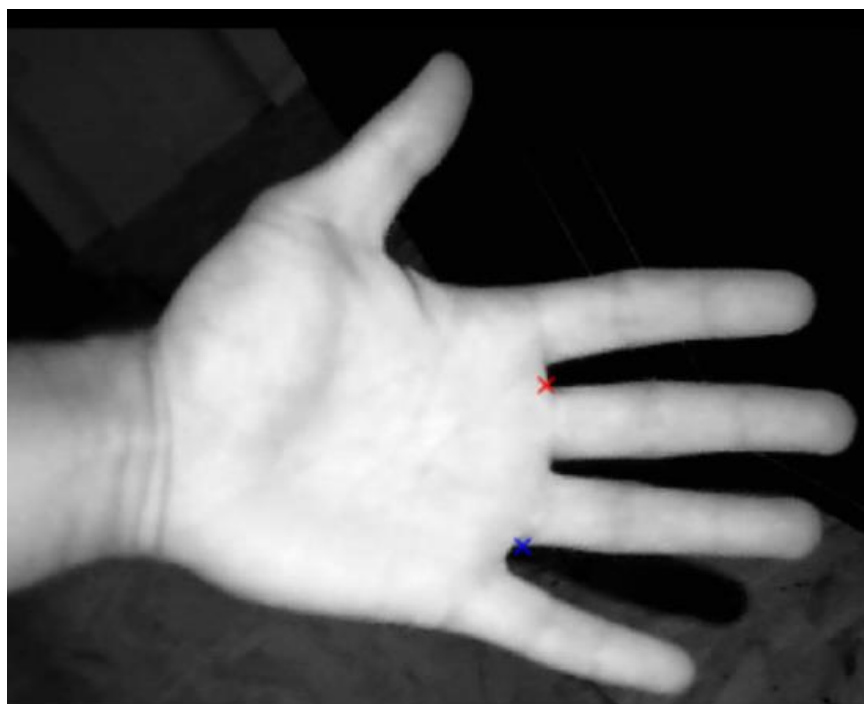


Рисунок 14 - Нахождение опорных точек на изображении

Разворот изображения и выделение ROI изображено на Рисунке 15.

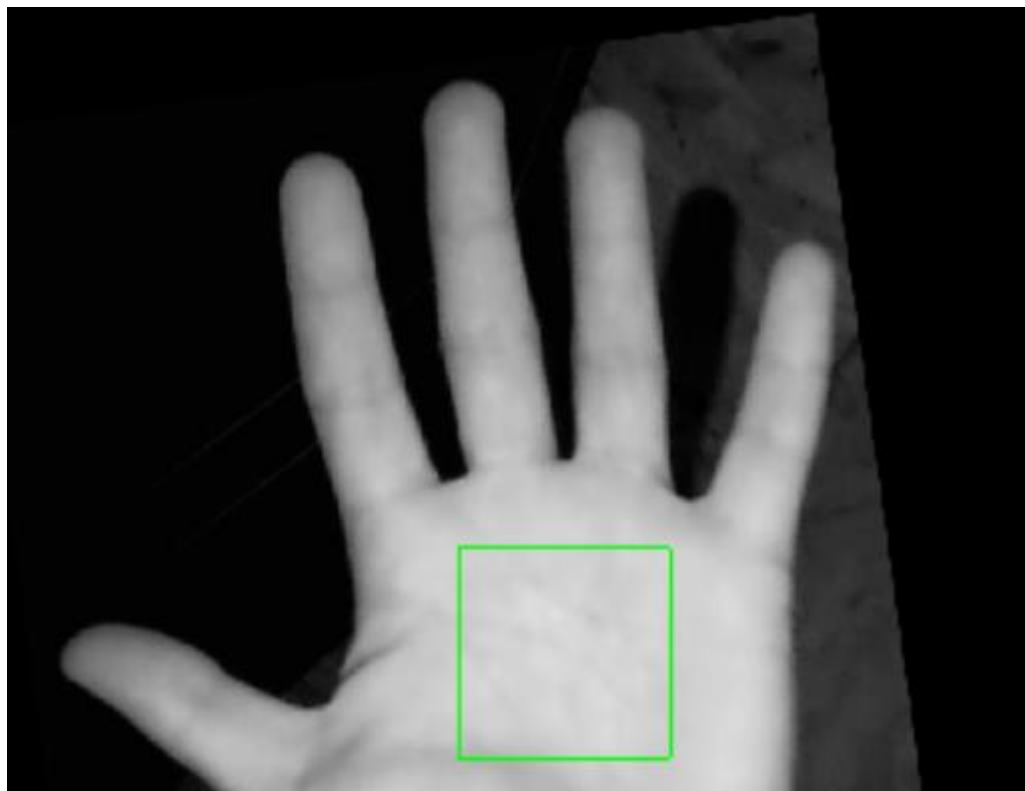


Рисунок 15 - Выделение ROI на изображении