Содержание

ВВЕДЕНИЕ

На сегодняшний день средства биометрической идентификации плотно вошли в повседневную жизнь. 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. Начиная с 2010 года в России используются биометрические заграничные паспорта. С 2018 года началось подключение российских банков к Единой биометрической системе, которая сочетает в себе биометрию лица и голоса. Согласно прогнозам BCC Research, мировой рынок биометрических технологий будет расти на 23,2% ежегодно с 2020 по 2024 год.

В рамках масштабного исследования J'son & Partners Consulting была собрана аналитика мирового и российского рынка биометрических технологий (Рисунок 1).

Рисунок 1 - Структура мирового и российского рынка биометрических технологий

Наиболее распространёнными являются методы идентификации по отпечатку пальца и распознавания лица, которые внедряются в большой спектр устройств, в том числе и в смартфоны. Согласно статистике аналитической компании Pew Research Center на 2018 год, 59% опрошенных людей взрослого возраста используют смартфоны. При этом на этот же год

доля рынка смартфонов обладающих сканером отпечатков пальцев составляет 60%.

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

Ключевое различие между биометрическими идентификаторами и классическими идентификационными методами – это понятие степени сходства. Использование аутентификации по паролю дает всегда точный результат на выходе: разрешение доступа при правильном пароле и отказ при неправильном. Такой подход исключает применение вероятности сходства. Но при применении биометрических методов необходимо руководствоваться терминами коэффициентов ошибок.

В основе оценки средств биометрической идентификации лежит понятие ложного сходства и ложного различия [1]. Здесь коэффициентом ложного принятия (англ. False Acceptance Rate) является частота принятия того, что биометрические образцы принадлежат одной личности, хотя это не так. Коэффициентом ложного отказа (англ. False Rejection Rate) является решение, что биометрические образцы принадлежат разным личностям, что так же является ошибкой.

При сравнении методов биометрической идентификации далее будут использованы показатели FRR при фиксированном значении FAR. Можно легко понять, что чем меньше значение FRR системы при одинаковом уровне FAR, 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 [2]. 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)

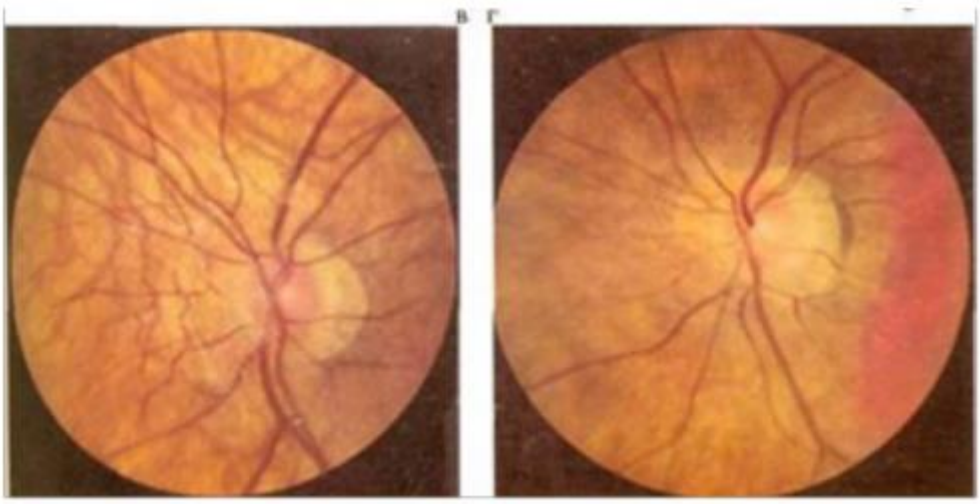

Рисунок 2 - Биометрические образцы сетчатки близнецов

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, для сканера ICAM2001 при FAR=0,001% значение FRR 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 FAR и FRR были предоставлены VeriFinger SDK, полученные при помощи сканера отпечатков пальцев DP U.are.U. При FAR=0,001% значение FRR 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 двухмерных 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 ваше лицо. Он работает в различных условиях и чрезвычайно безопасен.

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

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

1.1.4. Идентификация личности по голосу

Голосовая аутентификация бывает двух основных типов: текстовая и текстовая. В зависимости от текста сравнивается «образец» голоса из 6–10 слогов с эталонным «отпечатком голоса» и вычисляется оценка точности. Независимость от текста позволяет преобразовать более длинный речевой ввод в модель голоса и определить манеры речи в более широком спектре. В зависимости от текста требуется меньше данных, но активная регистрация каждого пользователя (хотя и ~ 30 секунд). Независимость от текста требует значительно большего количества данных, занимает больше времени для обработки, но регистрирует пользователей пассивно, без необходимости запрашивать какое-либо конкретное высказывание. Оба были успешно развернуты для идентификации колл-центра, но текстовая зависимость - единственный жизнеспособный вариант для таких функций, как вход на веб-сайт, который должен быть быстрым и удобным.

Для высококачественного распознавания голоса требуется восходящая обработка на оборудовании серверного класса. Хотя некоторые решения предлагаются для локальной аутентификации на устройстве, количество ложных срабатываний (ложное принятие голосовой записи, чем исходный владелец) резко возрастает. Локальная аутентификация ограничивается тестированием гораздо меньшего числа условий валидации по сравнению с большим набором онлайн-данных, способным анализировать и оценивать сотни условий валидации. Компаниям, рассматривающим возможность развертывания решений голосовой аутентификации, следует ориентироваться

на решения, предлагающие отраслевую норму ложных приемов (FAR) ~ 0,01% и ложных отклонений (FRR) ~ 1% -3%. Имейте в виду, что в большинстве решений голос не является единственным фактором аутентификации. При многофакторной аутентификации распознавание голоса является лишь одним из двух или более факторов, таких как идентификация пользовательского устройства.

1.1.5. 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 FRR и FAR приведено для сканера Palm Vein. Согласно данным разработчика, при FAR 0,0008% FRR составляет 0,01%.

1.2. Перспективные методы биометрической идентификации

В виду того, что перечисленные ниже методы ещё достаточно плохо изучены, то нет достоверной информации по статистическим данным, поэтому приводится только обзорное описание технологий.

1.2.1. Идентификация по запаху тела

Запах для большинства людей – относительно слабо дифференцированное, интегральное ощущение, так как он определяется суммарным эффектом от раздражения обонятельных рецепторов, рецепторов тройничного нерва и рецепторов вомероназального органа; кроме того, возможно, что в ощущение запаха вовлечено восприятие аэрозольной компоненты атмосферы.

Запаховые следы – это газообразные образования, отличающиеся от традиционных материальных следов своей динамичностью. Запаховый след образуется в том случае, если вещество непрерывно из твердого или жидкого состояния переходит в газообразное. Предмет является источником запаха до тех пор, пока с поверхности его отделяются в окружающую среду молекулы вещества.

Основная задача в распознавании запаха - создать модель, максимально похожую на нос человека. С этой точки зрения, электронные/искусственные носы разрабатываются как системы для автоматического обнаружения и классификации запахов, паров, газов.

Сенсорную систему можно представить как массив химических сенсоров, где каждый сенсор измеряет отдельное свойство, поступающего химического вещества, или как одиночное чувствительное устройство или как совокупность обоих. Основная задача этого компонента заключается в том, чтобы поймать запах. Каждый запах, который попадает на сенсорную систему,

создает запись особенного образца запаха. База данных записей строится путем внесения большого количества различных одорантов в сенсорную систему. Система распознавания образов используется для распознавания. Целью этого процесса является обучение и создание системы распознавания, которая будет способна производить уникальную классификацию или группировку каждого запаха так, чтобы могла быть осуществлена автоматическая идентификация.

1.2.2. Идентификация по тону сердца

Форма определяется возрастом, полом, телосложением, здоровьем, другими факторами. В упрощенных моделях описывается сферой, эллипсоидами, фигурами пересечения эллиптического параболоида и трехосного эллипсоида. Мера вытянутости (фактор) формы есть отношение наибольших продольного и поперечного линейных размеров сердца.

Существует возможность идентифицировать человека с использованием тонов (акустических сигналов), издаваемых сердцем (с использованием сердцебиений). Самое главное достоинства такого метода идентификации – практически невозможно подделать тон сердца по сравнению с другими биометрическими методами.

Данный метод состоит из схемы выделения устойчивых признаков, которая базируется на кепстральном анализе. Результаты подтверждают тот факт, что значения параметра тона сердца существенно отличается от таких же параметров, используемых в традиционном кепстральном анализе речи. В частности, тоны сердца должны быть обработаны в течение 0,5 секунды во всем диапазоне частот. Предварительные параметры показали, что при хорошем выборе параметров, точность идентификации достигает 96 %.

1.2.3. ДНК идентификация

Известно, что ДНК любых двух людей почти не отличаются, и преобладающее большинство цепочек в них одинаково. Генетическое распознавание использует тот факт, что существуют сильно отличающиеся повторяющиеся цепочки, называемые минисателлитными ДНК.

ДНК-идентификация является самым надежным, среди статических биометрических методов аутентификации. В теории вероятность FAR-ошибки находится в пределах от 10-10 для RFLP до 10-29 при использовании STR. Конечно, при проведении реального анализа, вероятность ошибки возрастает. Но даже при этом, она остается очень низкой, что позволяет использовать процедуру генетического распознавания в таких ответственных ситуациях, как судебная экспертиза.

Повсеместному распространению ДНК-экспертных систем мешают относительная сложность, дороговизна и большие затраты по времени на проведение анализа.

1.2.4. Идентификация по эмоциональному состоянию и мимике

Эмоциональное состояние и мимика человека постоянно меняются в зависимости от внешних и внутренних факторов. При этом выражение эмоций - это неосознанный процесс (человек не несёт ответственности за свое эмоциональное состояние), что практически исключает возможность сокрытия и подмены этой биометрической характеристики.

Лицо человека, готового к атаке на информационную систему, будет выражать определенные эмоции, которые будут отличаться от повседневных. С учетом этого обоснованным является изучение изменения эмоционального состояния и мимики пользователей для снижения вероятности ошибок первого и второго рода, а также повышения защищенности информации при

попытке нанесения вреда сотрудниками, которые успешно прошли процедуры идентификации и аутентификации.

При проведении исследований в области развития современных методов биометрической аутентификации перспективным является развитие математического аппарата, методов и технологий алгоритмического, информационного и программного обеспечения в данной предметной области.

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	**FAR**	**FRR**
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	0,0008%	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	**Фальсификация**
Отпечаток пальца	Возможна
Распознавание лица 3D	Проблематична
Радужная оболочка глаза	Безуспешна
Сетчатка глаза	Невозможна
Рисунок вен	Невозможна

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:	**Бесконтактная идентификация во время движения**
Отпечаток пальца	Безуспешна
Распознавание лица 2D	На большом расстоянии
Распознавание лица 3D	На среднем расстоянии
Радужная оболочка глаза	На большом расстоянии
Сетчатка глаза	Невозможна
Рисунок вен	На маленьком 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. Так, стоимость считывателя EyeLock NANO NXT на российском рынке составляет 365 000 р., когда как сканеры вен Fujitsu обладают рыночной стоимостью от 34 400 р.

Однако стоимость реализации сканеров вен может быть сокращена, о чем говорится в следующих главах.

2. ОБЗОР РЫНКА ИДЕНТИФИКАТОРОВ ПО РИСУНКУ ВЕН

Автоматическое распознавание вен ладони стало надежной технологией, обеспечивающей больший уровень безопасности персональной системы идентификации.

Для получения изображений вены ладони требуется инфракрасное (ИК) освещение и стандартные камеры с простым датчиком CCD или CMOS. Поэтому изображения вен ладони являются изображениями в градациях серого, на которых на сером фоне появляются прожилки от темно-серого до черного.

2.1. Сканер Fujitsu Palmsecure

Наиболее полное исследование по распознаванию рисунков вен ладони было проведено Fujitsu в Японии. База данных состоит из 150 000 изображений вен ладони из 75 000 субъектов разного возраста. Эта база данных была собрана в коммерческих целях, поэтому подробности недоступны, а воспроизведение исследования невозможно.

Согласно заявлению разработчика, PalmSecure позволяет компаниям обеспечить высокий уровень надежности биометрической защиты, в то же время повышая удобство использования для конечных пользователей и избегая дополнительных затрат, связанных с восстановлением паролей службой технической поддержки. Развитые функции интеграции дают возможность заказчикам создать защищенные решения биометрического контроля для физического доступа к помещениям и устройствам, а также для логического доступа к приложениям и сервисам.

Со слов разработчика, комплексное и масштабируемое решение Fujitsu PalmSecure предлагает все необходимые компоненты для простого и удобного создания решений для биометрической аутентификации, которые могут использоваться практически для любого приложения. Созданная на базе

обновленного центрального сервера верификации, эта система усиливает защиту за счет устранения необходимости для пользователей в регистрации и во входе в многочисленные учетные записи в различных местах, на различных устройствах, приложениях или сервисах. Легкость интеграции с любыми типами приложений и оборудования упрощается с помощью универсального API-интерфейса. Он позволяет внедрять технологию биометрической аутентификации в различные сценарии использования: начиная входом в центры обработки данных, заканчивая созданием учетных данных для промышленного оборудования и единым входом в различные приложения.

Защищенная, простая и гигиеничная технология биометрической аутентификации по рисунку вен. Обеспечение безопасности корпоративных систем стало сложной задачей с учетом того, что атаки возникают не только извне, но и в результате действий внутри организации. Все это делает вопросы контроля безопасности и доступа к корпоративным активам еще более актуальными. Биометрическая аутентификация находит все большее распространение на рынке, поскольку она представляет надежный, точный и эффективный метод подтверждения личности человека, а компании находятся в поиске более защищенных и простых в использовании технологий аутентификации для контроля доступа к данным, физического доступа и общей безопасности. Исследования Fujitsu в области различных биометрических аутентификационных решений, включая распознавание человека по радужной оболочке глаз, чертам лица, отпечаткам пальцев, голосу и подписи, показали, что эти технологии имеют свои уязвимые места, а технология аутентификации по отпечаткам пальцев не соответствует санитарно-гигиеническим требованиям, отметили в Fujitsu.

В бесконтактной системе аутентификации PalmSecure используется биометрическая технология для аутентификации пользователей по уникальному рисунку вен. По утверждению разработчика, алгоритмы аутентификации системы PalmSecure обеспечивают высокий уровень точности и универсальность применения. Коэффициент ложного пропуска

(False Acceptance Rate, FAR) составляет менее 0,00001 процента (1 на 10 миллионов), а коэффициент ложного отказа в доступе (False Rejection Rate, FRR) – 0,01 процента (1 на 10 тысяч). Бесконтактный считыватель соответствует санитарно-гигиеническим требованиям, а также обеспечивает высокий уровень распознавания пользователя системой.