В. А. Ворона, В. О. Костенко, Биометрические технологии идентификации в системах контроля и управления доступом, *Comp. nanotechnol.*, 2016, выпуск 3, 224–241

2.2. БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Ворона Владимир Андреевич, доктор технических наук профессор, военнослужащий по контракту. vorona-1950@yandex.ru

Костенко Виталий Олегович, доцент, военнослужащий по контракту. dir@inform-stcurity

Аннотация: В статье рассмотрены биометрические технологии идентификации в системах контроля и управления доступом. Приведена классификация современных биометрических средств идентификации на основе статических и динамических физиологических характеристиках человека, а также физические принципы их реализации и статистические оценки эффективности применения.

Ключевые слова: система контроля и управления доступом, биометрические идентификаторы, физиологические характеристики человека, рисунки папиллярных линий пальцев, радужная оболочка глаза, капилляры сетчатки глаз, тепловое изображение лица, геометрия руки, ДНК, почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре.

2.2. BIOMETRIC IDENTIFICATION TECHNOLOGY IN MONITORING SYSTEMS AND ACCESS CONTROL

Vorona Vladimir Andreevich, doctor of technical sciences, professor, contract serviceman. vorona-1950@yandex.ru

Kostenko Vitaly Olegovich, assistant professor, contract serviceman. dir@inform-stcurity.ru

Abstract: The article deals with biometric technologies of identification in systems of control and access control. Presented classification of modern biometric identification tools based on static and dynamic physiological characteristics of person as well as the physical principles of their realization and statistical evaluation of the application efficiency.

Index terms: monitoring systems and access control, biometric identifier, physiological characteristics of person, pictures of the papillary lines of fingers, iris of the eye, capillaries of the retina, thermal image of the face, hand geometry, DNA, handwriting and signature dynamics, voice and speech features, rhythm of work on the keyboard.

Защита любого объекта включает в себя несколько рубежей. Во всех случаях важным рубежом будет система управления и контроля доступа (СКУД) на объект. Современные технические средства СКУД позволяют решать ряд важных задач:

- противодействие промышленному шпионажу;
- противодействие воровству;
- противодействие саботажу;
- противодействие умышленному повреждению материальных ценностей;
- защита конфиденциальности информации;
- регулирование потока посетителей;
- контроль въезда и выезда транспорта;
- учет рабочего времени;
- контроль своевременности прибытия и убытия сотрудников.

Под СКУД понимают объединенные в комплексы электронные, механические, электротехнические, аппаратно-программные и иные средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (ПЭВМ, автомобиль, сейф и т.д.) и ограничивающие доступ лиц, не имеющих такого права. Такие системы могут осуществлять контроль перемещения людей и транспорта по территории охраняемого объекта, обеспечивать безопасность персонала и посетителей, а также сохранность материальных и информационных ресурсов предприятия [1-3].

Существующий в стране ГОСТ устанавливает классификацию, общие технические требования, методы испытаний и подразделяет СКУД по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
- уровню защищенности системы от несанкционированного доступа.

СКУД состоит из управляемых преграждающих устройств в составе преграждающих конструкций и исполнительных устройств; устройств ввода идентификационных признаков в составе считывателей и идентификаторов, устройств управления, в составе аппаратных и программных средств.

Общая схема СКУД показана на рис. 1. Несмотря на уникальность каждой конкретной системы контроля доступа, она содержит три основных элемента: идентификатор пользователя (карта-пропуск, ключ), устройство идентификации, управляющий контроллер и исполнительные устройства.

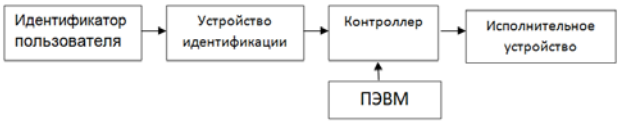


Рис. 1. Общая схема СКУД

Функционирование СКУД в упрощенном виде можно описать следующим образом. Каждый сотрудник или постоянный посетитель организации получает идентификатор (электронный ключ) – пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. Персональная «электронная карточка» владельца и код его «электронного ключа» связываются друг с другом и заносятся в специально организованные компьютерные базы данных.

У входа в здание устанавливаются считыватели, считывающие с карточек их код и информацию о правах доступа владельца карты и передающие эту информацию в контроллер системы. Контроллер открывает или блокирует двери (замки, турникеты), переводит помещение в режим охраны, включает сигнал тревоги и т.д. Все факты предъявления карточек и связанные с ними действия (проходы, тревоги и т.д.) фиксируются в контроллере и сохраняются в компьютере.

Для идентификации в составе СКУД применяются *атрибутные и биометрические* идентификаторы. В качестве атрибутных идентификаторов используют автономные носители признаков допуска: магнитные карточки, бесконтактные проксимити карты, брелки Touch Memory, различные радиобрелки, биометрические: изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони, черты лица и многие другие физические признаки. Каждый идентификатор характеризуется определенным уникальным двоичным кодом. В СКУД каждому коду ставится в соответствие информация о правах и привилегиях владельца идентификатора.

В настоящее время используются считыватели карт (проксимити, Виганда, с магнитной полосой и т. п). Они имеют свои неоспоримые преимущества и удобства в использовании, однако при этом в автоматизированном пункте доступа контролируется «проход карточки, а не человека». В то же время карточка может быть потеряна или украдена злоумышленниками. Все это снижает возможность использования СКУД, основанных исключительно на считывателях карт, в приложениях с высокими требованиями к уровню безопасности. Несравненно более высокий уровень безопасности обеспечивают всевозможные биометрические устройства контроля доступа, использующие в качестве идентифицирующего признака биометрические параметры человека (отпечаток пальца, геометрия руки, рисунок сетчатки глаза и т. п.), которые однозначно предоставляют доступ только определенному человеку – носителю кода (биометрических параметров).

Биометрический контроль доступа – это автоматизированный метод, с помощью которого идентифицируется не внешний предмет, принадлежащий человеку, а собственно сам человек. У всех биометрических технологий существуют общие подходы к решению задачи идентификации, хотя все методы отличаются удобством применения, точностью результатов. Любая биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;

сравнение текущего шаблона с базой данных.

В биометрических идентификаторах используются *статические,* основанные на физиологических характеристиках человека (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, тепловое изображение лица, геометрия руки, ДНК), и *динамические* (почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре) методы. Предполагается использование таких уникальных статических методов как идентификация по подногтевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела и динамических – идентификация по движению губ при воспроизведении кодового слова, по динамике поворота ключа в дверном замке и т.д. Известны разработки СКУД, основанные

на считывании и сравнении конфигураций сетки вен на запястье, образцов запаха, преобразованных в цифровой вид, анализе носящего уникальный характер акустического отклика среднего уха человека при облучении его специфическими акустическими импульсами и т.д.

Классификация современных биометрических средств идентификации показана на рис. 2. Любая биометрическая технология применяется поэтапно: сканирование объекта, извлечение индивидуальной информации, формирование шаблона, сравнение текущего шаблона с базой данных.

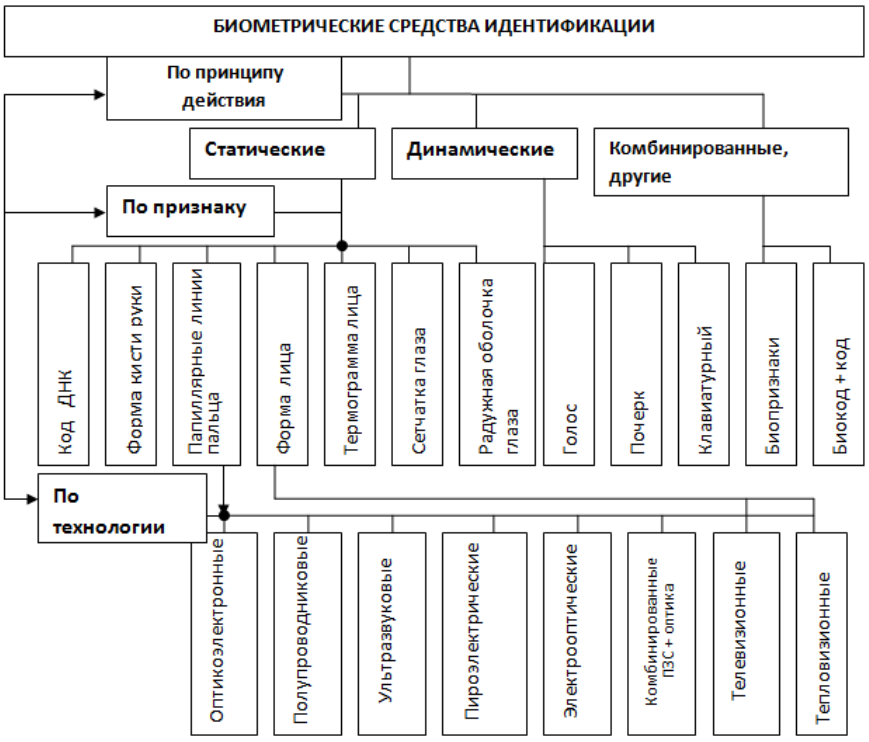


Рис. 2. Классификация современных биометрических средств идентификации.

Идентификация по рисунку папиллярных линий. Дактилоскопия (распознавание отпечатков пальцев) – наиболее разработанный на сегодняшний день биометрический метод идентификации личности. Весь процесс идентификации по рисунку папиллярных линий занимает не более нескольких секунд и не требует усилий от тех, кто использует данную систему доступа. Существует два основных алгоритма сравнения полученного кода с имеющимся в базе шаблоном: по характерным точкам и по рельефу всей поверхности пальца. В первом случае выявляются характерные участки, и запоминается их взаиморасположение. Во втором случае запоминается вся «картина» в целом.

В самом простом случае при обработке изображения на нем выделяются характерные точки (например, координаты конца или раздвоения папиллярных линий, места соединения витков). Можно выделить до 70 таких точек и каждую из них охарактеризовать двумя, тремя или даже большим числом параметров. В результате можно получить от отпечатка пальца до пятисот значений различных характеристик. Более сложные алгоритмы обработки соединяют характерные точки изображения векторами и описывают их свойства и взаимоположение (рис. 3). В результате можно получить от отпечатка пальца до пятисот значений различных характеристик. Набор данных, получаемых с отпечатка, занимает до 1 Кбайт.

Рис. 3. Изображение отпечатка пальца *(а)* и его «образ» (б)

В современных системах используется также комбинация обоих алгоритмов, что позволяет повысить уровень надежности системы. Дополнительно привлекается информация о морфологической структуре отпечатка пальца: относительное положение замкнутых линий папиллярного узора, «арочных» и спиральных линий.

Дактилоскопия построена на двух основных качествах, присущих папиллярным узорам кожи пальцев и ладоней:

- стабильности рисунка узора на протяжении всей жизни человека;

- уникальности, что означает отсутствие двух индивидуумов с одинаковыми дактилоскопическими отпечатками.

Процедура аутентификации приведена на рис. 4.

Рис. 4. Процесс аутентификации по отпечаткам пальцев

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), которые характеризуются их местоположением в декартовых координатах.

Известны *три основных подхода* к реализации систем идентификации по отпечаткам пальцев. Самый распространенный на сегодня способ строится на использовании оптики – призмы и нескольких линз со встроенным источником света (рис. 5).

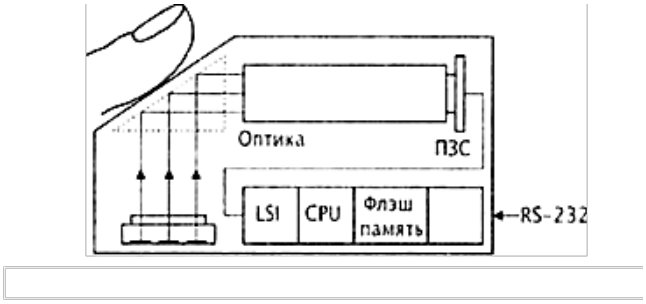


Рис. 5. Функциональная схема системы FIU фирмы SONY

Свет, падающий на призму, отражается от поверхности, соприкасаемой с пальцем пользователя, и выходит через другую сторону призмы, попадая на оптический сенсор (обычно, монохромная видеокамера на основе ПЗС-матрицы), где формируется изображение. Недостатки такой системы: отражение сильно зависит от параметров кожи – сухости, присутствия масла, бензина, других химических элементов. Например, у людей с сухой кожей наблюдается эффект размытия изображения. Как результат – высокая доля ложных срабатываний.

Другой способ использует методику измерения электрического поля пальца с использование полупроводниковой пластины. Когда пользователь устанавливает палец в сенсор, он выступает в качестве одной из пластин конденсатора (рис. 6). Другая пластина конденсатора – это поверхность сенсора, которая состоит из кремниевого чипа, содержащего 90 000 конденсаторных пластин с шагом считывания 500-dpi. В результате получается 8-битовое растровое изображение гребней и впадин пальца.

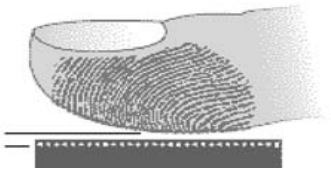


Рис. 6. Система идентификации на основе полупроводниковой пластины

В основе третьего метода реализации систем лежит использование TactileSense – электрооптического полимера. Этот материал чувствителен к разности электрического поля между гребнями и впадинами кожи. Градиент электрического поля конвертируется в оптическое изображение высокого разрешения, которое затем переводится в цифровой формат, который в свою очередь уже можно передавать в ПК по параллельному порту или USB интерфейсу. Характеристики некоторых методов приведены в табл. 1.

Таблица 1

Характеристики типовых систем идентификации по отпечаткам пальцев

Свойства	Оптическая система	Полупроводниковая технология	Электрооптический полимер
Небольшие размеры	нет	да	да
Восприимчивость к сухой коже	нет	да	да
Прочность поверхности	средняя	низкая	высокая
Энергопотребление	среднее	низкое	низкое
Цена	средняя	высокая	низкая

Полученный одним из описанных методов аналоговый видеосигнал преобразуется в цифровую форму, после чего из него извлекается комплект характеристик, уникальных для этого отпечатка пальца. Эти данные однозначно идентифицируют личность. Данные сохраняются и становятся уникальным шаблоном отпечатка пальца конкретного человека. При последующем считывании новые

отпечатки пальцев сравниваются с хранимыми в базе.

Хранение данных и сравнение при идентификации происходит в компьютере. С целью идентификации личности по рисунку папиллярных линий пальца проверяемый набирает на клавиатуре свой идентификационный номер и помещает указательный палец на окошко сканирующего устройства. При совпадении получаемых признаков с эталонными, предварительно заложенными в память ЭВМ и активизированными при наборе идентификационного номера, подается команда исполнительному устройству. Если один из пальцев поврежден, для идентификации можно воспользоваться «резервным» отпечатком (отпечатками), сведения о которых, как правило, также вносятся в биометрическую систему при регистрации пользователя.

Практически каждый производитель аппаратной части вместе с системой поставляет и уникальное программное обеспечение, адаптированное чаще всего под Windows NT.

Применение систем автоматической идентификации по отпечатку пальца (AFIS) получило широкое распространение в более чем 30 странах мира. Преимущества доступа по отпечатку пальца – простота использования, удобство и надежность. В настоящее время уже производятся подобные системы размером меньше половины коробка спичек (рис. 7).

Рис. 7. Сканер Precise 250 MC

Процент ложных отказов при идентификации по отпечатку пальцев составляет около 3 %, ошибка ложного (ошибочного) доступа – меньше 0,00001% (1 на 1000000). При оценке надежности аутентификационной процедуры необходимо учитывать возможность копирования отпечатка и использования другими лицами для получения несанкционированного доступа. В качестве одной из возможностей по обману терминала специалисты называют изготовление искусственной кисти с требуемыми отпечатками пальцев (или изъятия «подлинника» у законного владельца). Но существует и способ борьбы с такой фальсификацией. Для этого в состав терминального оборудования должны быть включены инфракрасный детектор, который позволит зафиксировать тепловое излучение от руки (или пальца), и (или) фотоплетизмограф, который определяет наличие изменений отражения света от поверхности потока крови. Другим способом подделки является непосредственное нанесение папиллярного узора пальцев законного пользователя на руки злоумышленника с помощью специальных пленок или пленкообразующих составов.

Преимущества метода. Высокая достоверность – статистические показатели метода лучше показателей способов идентификации по лицу, голосу, росписи. Низкая стоимость устройств, сканирующих изображение отпечатка пальца. Достаточно простая процедура сканирования отпечатка.

Недостатки: папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами. Люди, использовавшие сканеры на предприятиях с численностью персонала порядка нескольких сотен человек заявляют о высокой степени отказа сканирования. Многие из сканеров неадекватно относятся к сухой коже и не пропускают стариков. Так же присутствует недостаточная защищённость от подделки изображения отпечатка, отчасти вызванная широким распространением метода.

Идентификация по радужной оболочке глаз. Радужная оболочка глаза является уникальной характеристикой человека. Рисунок радужки формируется на восьмом месяце внутриутробного развития, окончательно стабилизируется в возрасте около двух лет и практически не изменяется в течение жизни, кроме как в результате сильных травм или резких патологий. Рисунок радужки в большой степени случаен и уникален. Вероятность того, что два разных человека имеют один и тот же рисунок радужной оболочки глаза, равняется приблизительно 10^{-78}, в то время как все население Земли составляет примерно 10^{10}. Текстура радужки имеет степень свободы равной 250, что гораздо больше степени свободы отпечатков пальцев (35) и изображений лиц (20). Метод является одним из наиболее точных среди биометрических методов.

Система идентификации личности по радужной оболочке подразделяется на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю и вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду о допуске исполнительному устройству. Время первичной обработки изображения в современных системах примерно 300-500мс, скорость сравнения полу-

ченного изображения с базой имеет уровень 50000-150000 сравнений в секунду на обычном ПК. Такая скорость сравнения не накладывает ограничений на применения метода в больших организациях при использовании в системах доступа. При использовании же специализированных вычислителей и алгоритмов оптимизации поиска становится даже возможным идентифицировать человека среди жителей целой страны.

Алгоритмы идентификации личности по радужной оболочке глаза преобразовывают необработанные видеоизображения глаза в уникальный идентификационный двоичный поток, называемый Iris-код, полученный в результате определения позиции радужки, ее границы и выполнения других математических операций для описания текстуры радужки в виде последовательности чередования фаз, похожей на штрих код. Полученный таким образом Iris-код используется для поиска совпадений в базах данных (скорость поиска – около 1 млн. сравнения Iris-кодов в секунду) и для подтверждения или не подтверждения заявленной личности.

Различают *активные и пассивные* системы распознавания. В системах первого типа пользователь должен сам настроить камеру, передвигая ее для более точной наводки. Пассивные системы проще в использовании, поскольку камера в них настраивается автоматически.

Методы идентификации личности по радужной оболочке построены по одному и тому же принципу – выделение частотной или какой-либо другой информации о текстуре радужки из изображения и сохранение этой информации в виде специального кода (для системы Daugman этот код получил специальное название – IrisCode (радужковый код)). Можно сравнивать коды радужек, и хранить коды радужек разных людей в базе данных.

Построение кода производится в три этапа:

1. Выделение радужки из общего изображения

2. Предобработка полученного изображения – например убирание шума(denoising), улучшение изображения (enhansing), в том числе выравнивание гистограммы, убирание блика. Большинство методов работает с изображениями в градациях серого либо картами яркости изображений, то есть цветовая составляющая является избыточной.

3. Составление кода – предобработанное изображение фильтруется способом, зависящим от конкретного метода. По результатам фильтрации составляется представление в виде кода.

Для локализации радужной оболочки глаза некоторые методы, например Wildes, используют специальное оборудование для захвата изображения, чтобы полученное изображение глаза было высокого разрешения, с хорошей контрастностью, освещением и центрировано (радужка должна находиться в центре изображения). Кроме того, система камер должна быть не инвазивна, то есть не принуждать человека сесть в определенную позу на фиксированном расстоянии от камеры при специальном освещении. Иногда делается дополнительный снимок инфракрасной камерой. Для того, чтобы отделить собственно радужку от остальных деталей на изображении, в простейшем случае можно использовать выделение краев (путем анализа первой производной) и последующую аппроксимацию границ радужки простыми геометрическими объектами. Так, окружность зрачка и внешнюю границу радужки можно найти при помощи преобразования Хафа (Hough transform). Другие методы дополнительно определяют границу радужки и век двумя параболами, как Wildes, либо просто отрезают те части изображения, которые могут не относиться к радужке, как Daugman, Ma. Часто для дальнейшей работы производится перевод изображения радужки из полярных координат в декартовы. К полученному изображению можно применить фильтрацию гауссовым фильтром для устранения высокочастотного шума или медианную фильтрацию.

К классическим способам составления кода можно отнести пространственно-частотную свертку изображения фильтрами Габора (Gabor's filters), предложенную Daugman. Каждый бит кода определяется знаком результата воздействия двухмерного фильтра Габора на некоторую небольшую окрестность текстуры радужки. Для кода Daugman и подобных ему в качестве сравнения используется расстояние Хэмминга (количество отличающихся бит кода). Развитием этого направления является применение специальных симметричных функций Circular symmetric filter.

Другой модификацией кода на основе фильтров Габора является составление кода на основе среднего абсолютного отклонения (average absolute deviation, AAD) отфильтрованного изображения от оригинального. В этом случае функцией сравнения будет выступать евклидово расстояние между векторами.

Результирующее изображение представляется как лапласова пирамида изображений, подвергну-

тых действию гауссовых фильтров, и призвано представлять пространственные характеристики радужки. В этом случае для дальнейшего сравнение используются нормированная корреляция обрабатываемого изображения и изображений из базы данных. Нормализованная корреляция показывает меру соответствия точек двух изображений или областей изображений друг другу. Инвариант относительно масштаба входного изображения во многих системах регулируется приведением текстуры радужки к карте фиксированного размера. Обеспечение стабильности относительно поворота достигается за счет хранения нескольких изображений одной радужки в базе данных – под несколькими углами поворота.

Классические системы составления кода:

- *Daugman* – основа для составления кода – фильтры Габора, критерий сравнения кодов – расстояние Хэмминга;

- *Wildes* – использует преобразование Хафа для локализации радужки, Лапласову пирамиду фильтров Гаусса для составления кода;

- *Boles* – где изображение радужной оболочки представляется одномерной функцией, которая фильтруется вейвлетами специального вида;

- *Noh* – основе лежит использование анализа независимых компонент с переменной разрешающей способностью (Multiresolution Independent Component Analysis).

Дифференциатор ключей для идентификации личности по рисунку радужной оболочки глаза осуществляет поиск в базе данных для нахождения соответствующего идентификационного кода. При этом база данных может состоять из неограниченного числа записей кодов IrisCode.

Разработкой технологии идентификации личности на основе принципа сканирования радужной оболочки глаза в настоящее время занимаются более 20 компаний, в том числе British Telecom, Sensar, японская компания Oki. В качестве примера современной системы идентификации на основе анализа радужной оболочки глаза рассмотрим решение от компании LG. Система IrisAccess позволяет менее чем за секунду отсканировать рисунок радужной оболочки глаза, обработать и сравнить с 4 тыс. других записей, которые она хранит в своей памяти, а затем послать соответствующий сигнал в охранную систему. Технология – полностью бесконтактная. На основе изображения радужной оболочки глаза строится компактный цифровой код размером 512 байт. IrisAccess 3000 состоит из оптического устройства внесения в реестр EOU3000, удаленного оптического устройства ROU3000, контрольного устройства опознавания ICLI3000, платы захвата изображения, дверной интерфейсной платы и PC-сервера.

Преимущество сканеров для радужной оболочки глаза состоит, прежде всего, в том, что они не требуют от пользователя сосредоточения на цели, так как образец пятен на радужной оболочке находится на поверхности глаза. Фактически, видеоизображение глаза может быть отсканировано на расстоянии менее метра.

Недостатком такого метода является высокая цена систем идентификации и низкая доступность готовых системных решений. На данный момент удельный вес технологий идентификации по радужной оболочке глаза на мировом биометрическом рынке составляет по разным подсчетам от 6 до 9%.

Идентификация по сетчатке глаза. При идентификации по сетчатке глаза измеряется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и другие признаки. Капиллярый рисунок сетчатки глаз различается даже у близнецов и может быть с большим успехом использован для идентификации личности. Всего насчитывают около 250 признаков. Такие биометрические терминалы

обеспечивают высокую достоверность идентификации, сопоставимую с дактолоскопией, но требуют от проверяемого лица фиксации взгляда на объективе сканера.

Сканирование сетчатки происходит с использованием инфракрасного излучения низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Характерным устройством для системы такого типа является бинокулярный объектив. При осуществлении процедуры аутентификации пользователь должен прильнуть глазами к окулярам и, глядя вовнутрь, сфокусировать взгляд на изображении красного цвета. Затем ему следует дождаться смены цвета на зеленый (что укажет на правильную фокусировку) и нажать на стартовую кнопку. Сканирование глазного дна выполняется источником инфракрасного излучения, безопасного для глаз. Достаточно смотреть в глазок камеры менее минуты. За это время система успевает подсветить сетчатку и получить отраженный сигнал. Отраженное от ретины излучение фиксируется специальной чувствительной камерой.

Замеры ведутся по 320 точкам фотодатчиками и результирующий аналоговый сигнал с помощью микропроцессора преобразуется в цифровой вид. При этом используется алгоритм быстрого преоб-

разования Фурье. Полученный цифровой вектор, состоящий из коэффициентов Фурье, сравнивается с зарегистрированным эталоном, хранящимся в памяти системы. Благодаря такому методу преобразования и представления изображения глазного дна, для хранения каждого эталона расходуется по 40 байт. Память терминала, реализующего этот алгоритм, рассчитана на запоминание до 1200 эталонов. Время регистрации составляет примерно 30 с, время аутентификации – 1,5 с. Коэффициент ошибок I-го рода – 0,01%, II-го рода – 0,0001% (т.е. вероятность ошибок I-го рода – 0,0001, II-го рода – 0,000001).

Преимуществом систем ***и****дентификации* по сетчатке глаза является высокий уровень статистической надёжности. С точки зрения безопасности данная система выгодно отличается от других, использующих биометрические терминалы, не только малым значением коэффициентов ошибок как I-го, так и II-го рода, но и использованием специфического аутентификационного атрибута, который практически невозможно негласно подменить для обмана системы при проверке.

К недостаткам подобных систем следует в первую очередь отнести психологический фактор: не всякий человек согласен смотреть в темное отверстие, где что-то светит в глаз. К тому же надо следить за положением глаза относительно отверстия, поскольку подобные системы, как правило, чувствительны к неправильной ориентации сетчатки и учитывать возможное заболевание глаз, например, катаракту. Высокая стоимость, технические сложности и неудобство в использовании значительно замедлили скорость развития метода.

Сканеры сетчатки глаза получили широкое распространение в системах контроля доступа на особо секретные объекты, так как у них один из самых низких процентов отказа в доступе зарегистрированных пользователей и практически не бывает ошибочного разрешения доступа.

Идентификация по форме лица. *Идентификация человека по чертам (геометрии) лица* – одно из самых динамично развивающихся направлений в биометрической индустрии. Распознавание по геометрии лица причисляют к «трем большим биометрикам» вместе с распознаванием по отпечаткам пальцев и радужной оболочке. В данном методе идентификации строится трехмерный образ лица человека. На лице выделяются контуры бровей, глаз, носа, губ и т.д., вычисляется расстояние между ними и строится не просто образ, а еще множество его вариантов на случаи поворота лица, наклона, изменения выражения. Количество образов варьируется в зависимости от целей использования данного способа (для аутентификации, верификации, удаленного поиска на больших территориях и т.д.).

Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Рост мультимедийных технологий, благодаря которым можно увидеть все больше видеокамер, установленных на городских улицах и площадях, аэропортах, вокзалах и других местах скопления людей, определили развитие этого направления.

Техническая реализация метода более сложная (с математической точки зрения) задача, чем распознавание отпечатков пальцев, и, кроме того, требует более дорогостоящей аппаратуры (нужна цифровая видео- или фотокамера и плата захвата видеоизображения). У этого метода есть один существенный плюс: для хранения данных об одном образце идентификационного шаблона требуется совсем немного памяти, так как человеческое лицо можно «разобрать» на относительно небольшое количество участков, неизменных у всех людей. Например, для вычисления уникального шаблона, соответствующего конкретному человеку, требуется всего от 12 до 40 характерных участков.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что, во-первых, не требует специального дорогостоящего оборудования. Для большинства приложений достаточно только персонального компьютера и обычной видеокамеры. Во-вторых, отсутствует физический контакт человека с устройствами. Не надо ни к чему прикасаться или специально останавливаться и ждать срабатывания системы. В большинстве случаев достаточно просто пройти мимо или задержаться перед камерой на несколько секунд.

Распознавание изображений аналогично распознаванию образов и предусматривает выполнение любой из следующих функций: аутентификация – установление подлинности «один в один», идентификация – поиск соответствия «один из многих». Данная область делится на два направления: 2D-распознавание и 3D-распознавание. У каждого из них есть достоинства и недостатки, однако многое зависит еще и от области применения и требований, предъявленных к конкретному алгоритму.

2D-распознавание лица – один из самых статистически неэффективных методов биометрии, применялся, в основном, в криминалистике, что и способствовало его развитию. Впоследствии появились компьютерные интерпретации метода, в результате чего он стал более надежным. В настоящее время он применяется, в основном, в мультимодальной – перекрестной биометрии. Статистические показатели метода достаточно скромные, но позволяет проводить скрытую съемку лиц в людных местах.

3D-распознавание лица сейчас является более привлекательной областью для разработчиков. Метод проецирования шаблона состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается – чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через «жалюзи». Затем видимый свет был заменен инфракрасным, который обладает рядом преимуществ. Обычно на первом этапе обработки отбрасываются изображения, на которых лица не видно вообще или присутствуют посторонние предметы, мешающие идентификации. По полученным снимкам восстанавливается 3D-модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели – выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных. Время захвата и обработки изображения составляет 1-2 с для лучших моделей. Считается, что статистическая надежность метода сравнима с надежностью метода идентификации по отпечаткам пальцев.

В настоящее время существует четыре основных метода распознавания лица, различающихся сложностью реализации и целью применения:

- «eigenfaces» («собственное лицо»);
- анализ «отличительных черт»;
- анализ на основе «нейронных сетей»;

метод «автоматической обработки изображения лица».

Технология ***«Eigenface»*** использует двумерные изображения в градациях серого, которые представляют отличительные характеристики изображения лица. Метод «eigenface» часто используются в качестве основы для других методов распознавания лица. Комбинируя характеристики 100-120 «eigenface» можно восстановить большое количество лиц. В момент регистрации, «eigenface» каждого конкретного человека представляется в виде ряда коэффициентов. Для режима установления подлинности, в котором изображение используется для проверки идентичности, «живой» шаблон сравнивается с уже зарегистрированным шаблоном, с целью определения коэффициента различия. Степень различия между шаблонами и определяет факт идентификации.

Методика ***анализа «отличительных черт»*** – наиболее широко используемая технология идентификации. Эта технология подобна методике «Eigenface», но в большей степени адаптирована к изменению внешности или мимики человека (улыбающееся или хмурящееся лицо). В технологии «отличительных черт» используются десятки характерных особенностей различных областей лица, причем с учетом их относительного местоположения. Индивидуальная комбинация этих параметров определяет особенности каждого конкретного лица. Так как этот анализ рассматривает локальные участки лица, допустимые отклонения могут находиться в пределах до 25° в горизонтальной плоскости, и приблизительно до 15° в вертикальной плоскости и требует достаточно мощной и дорогой аппаратуры, что соответственно сокращает степень распространения данного метода.

В методе, основанном на ***нейронной сети***, характерные особенности обоих лиц – зарегистрированного и проверяемого сравниваются на совпадение. «Нейронные сети» используют алгоритм, устанавливающий соответствие уникальных параметров лица проверяемого человека и параметров шаблона, находящегося в базе данных, при этом применяется максимально возможное число параметров. Этот метод увеличивает качество идентификации лица в сложных условиях.

Метод ***«автоматической обработки изображения лица»*** – наиболее простая технология, использующая расстояния и отношение расстояний между легко определяемыми точками лица, такими как глаза, конец носа, уголки рта. Хотя данный метод не столь мощный как «eigenfaces» или «нейронная сеть», он может быть достаточно эффективно использован в условиях слабой освещенности.

Задачу идентификации личности человека по видеоизображению можно разбить на несколько этапов.

1. Локализация лица в кадре. Для локализации лица в кадре разработан алгоритм на основе

нейронной сети, который сканирует исходное изображение в различных масштабах, оценивая по ключевым признакам каждый участок изображения с определенной вероятностью и классифицирует, является ли данный участок лицом или нет. Выделение ключевых признаков осуществляется путем автоматического анализа достаточно большой обучающей выборки, охватывающей большинство возможных ситуаций (например, изменение внешности, условий освещенности, ракурса и т.п.).

2. *Определение положения головы.* Определение положения головы человека является важным этапом и позволяет внести поправки при дальнейшем распознавании. На этом этапе созданная компанией трехмерная модель головы сопоставляется с изображением головы в кадре. При этом оцениваются такие параметры как угол поворота головы по осям X,Y,Z, точный замер и смещение изображения в кадре.

3. *Отслеживание перемещения лица от кадра к кадру*. При идентификации движущегося в поле зрения камеры человека необходимо отслеживать перемещение лица от кадра к кадру. Имея несколько изображений одного и того же человека в разных ракурсах, программа выбирает наиболее удачный с ее точки зрения кадр и сохраняет его в базе данных. Обрабатывая несколько изображений одного и того же человека в разных ракурсах, можно добиться очень высокой точности распознавания.

4. *Сравнение изображения с данными базы.* В настоящее время компания ISS ведет разработки алгоритма сравнения лица с имеющимся в базе данных. Этот этап является логическим завершением в цепочке алгоритма идентификации личности по видеоизображению.

Оценочные характеристики при проверке эффективности различных вариантов таких устройств приведены в таблице 2.

Таблица 2.

Проверка эффективности распознавания черт лица

Условия оценки эффективности	Уровень ошибочных подтверждений (в %)	Уровень ошибочных отказов (в %)
Один и тот же день, одно и то же освещение	**2**	**0.4**
Один и тот же день, разное освещение	**2**	**9**
Различные дни	**2**	**11**
Различные дни в течение 1,5 лет	**2**	**43**

Основой любой системы распознавания лица является метод его кодирования. В ряде случаев используется анализ локальных характеристик для представления изображения лица в виде статистически обоснованных, стандартных блоков данных. Данный математический метод основывается на том, что все лица могут быть получены из репрезентативной выборки лиц с использованием современных статистических приемов. Они охватывают пиксели изображения лица и универсально представляют лицевые формы. Фактически в наличии имеется намного больше элементов построения лица, чем количество самих частей лица. Идентичность лица определяется не только характерными элементами, но и способом их геометрического объединения (т.е. учитываются их относительные позиции). Полученный сложный математический код индивидуальной идентичности – шаблон Faceprint – содержит информацию, которая отличает лицо от миллионов других, и может быть составлен и сравнен с другими с феноменальной точностью. Шаблон не зависит от изменений в освещении, тона кожи, наличия/отсутствия очков, выражения лица, волос на лице и голове, устойчив к изменению в ракурсах до 35^{o} в любых направлениях.

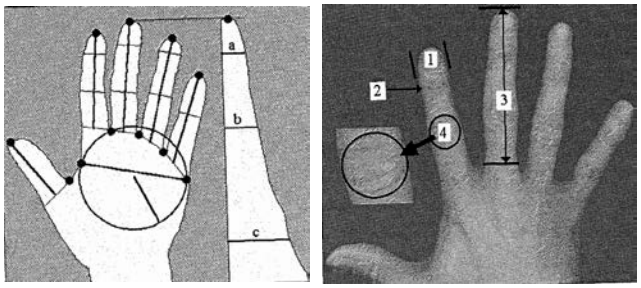
Преимущества метода – нет необходимости контактировать со сканирующим устройством. Низкая чувствительность к внешним факторам, как на самом человеке (появление очков, бороды, изменение прически), так и в его окружении (освещенность, поворот головы). Высокий уровень надежности, сравнимый с метом идентификации по отпечаткам пальцев.

Недостатки метода – дороговизна оборудования. Имеющиеся в продаже комплексы превосходили по цене даже сканеры радужной оболочки. Изменения мимики лица и помехи на лице ухудшают статистическую надежность метода. Метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

Удельный вес технологий распознавания по геометрии лица в общем объеме мирового биометрического рынка можно оценивать в пределах 13-18%. В России к данной технологии также проявляется больший интерес, чем, например, к идентификации по радужной оболочке.

Идентификация по геометрии кисти руки. Метод идентификации пользователей по геометрии руки по своей технологической структуре и уровню надежности вполне сопоставим с методом идентификации личности по отпечатку пальца. Статистическая вероятность существования двух кистей рук с одинаковой геометрией чрезвычайно мала [4].

В биометрике выделяются два основных метода распознавания по геометрии кисти руки. Первый основан исключительно на геометрических характеристиках кисти руки. С точки зрения компактности образа этот класс систем является самым экономичным. В простейшем варианте хранится только информация о длине и ширине пальцев, и требуется всего 9 байт. Естественно, что для систем, учитывающих только длину и ширину пальцев, может быть легко изготовлен картонный муляж руки оригинала. Более сложными являются системы, измеряющие профиль руки, что включает объем кисти, пальцев, неровности ладони, расположение складок кожи на сгибах.



а б

Рис. 8. Контрольные точки (а) и признаки (б) силуэта руки

На рис. 8,а показаны контрольные (характеристические) точки силуэта руки и 17 исходных геометрических признаков руки, в данном случае отмеченные отрезками прямых линий, которые не входят в силуэты кисти. Как видно, исходными биометрическими признаками руки являются ширина ладони, радиус вписанной в ладонь окружности, длины пальцев (определяемые как расстояния от выделенных верхних контрольных точек до середин линий, соединяющих нижние контрольные точки), ширина пальцев и высота кисти руки в трех пунктах, отмеченных линиями a, b и c.

Второй (более современный) – основан на смешанных характеристиках геометрических и образовых. К последним, относятся образы на сгибах между фалангами пальцев, узоры (расположение) подкожных кровеносных сосудов. С руки снимаются четыре характеристики, из которых три являются скалярами и относятся к размерам пальцев (рис. 8,б). Три первые характеристики – это ширина указательного пальца 1, высота указательного пальца 2 и длина среднего пальца 3, оцениваемая так, как показано на рисунке. Характеристика 4 в рассматриваемом случае представляет собой изображение складок кожи на сгибе между средней и нижней фалангами указательного пальца. Вся информация о руке в рассматриваемом классе систем может быть записана не более чем 9 байтами.

Для считывания геометрических характеристик кисти ее кладут ладонью вниз на специальную панель (рис. 9).

Рис. 9. Устройство идентификация по геометрии кисти руки и способ ее применения.

Через прорези в ее поверхности оптические сенсорные ячейки сканируют четыре кольца. Эти ячейки определяют стартовые точки по двум парам пальцев – указательному и среднему, безымянному и мизинцу. Каждый палец сканируется по всей длине, при этом замеряется длина, изгиб и расстояние до «соседа». Если каждое измерение укладывается в определенные допустимые рамки зарегистрированного эталонного набора данных, то результат аутентификации будет для пользователя положительным. Цифровой эталон хранится либо в базе данных, либо в памяти идентификационной карточки. При этом с целью обеспечения защиты данные шифруются.

Более популярные устройства сканируют как внутреннюю, так и боковую сторону ладони, используя для этого встроенную видеокамеру и алгоритмы сжатия. При этом оценивается более 90 различных характеристик, включая размеры самой ладони (три измерения), длину и ширину пальцев, очертания суставов и т.п. Через прорези в ее поверхности оптические сенсорные ячейки сканируют четыре кольца. Эти ячейки определяют старто-

вые точки по двум парам пальцев – указательному и среднему, безымянному и мизинцу. Каждый палец сканируется по всей длине, при этом замеряется длина, изгиб и расстояние до «соседа».

Математическая модель идентификации по данному параметру требует 9 байт, что позволяет хранить большой объем записей и быстро осуществлять поиск. Вероятность ошибок I-го рода составляет 0,01, но ошибок II-го рода – 0,000001. Время обработки занимает 2 с, время регистрации при оформлении допуска – 20 с. Память систем идентификации позволяет хранить до 220 эталонов.

*Преимущества – м*атематическая модель идентификации по данному параметру требует немного информации – всего 9 байт, что позволяет хранить большой объем записей и быстро осуществлять поиск.

Недостатки – признаки руки меняются с возрастом, а само устройство имеет сравнительно большие размеры.

В настоящее время идентификация пользователей по геометрии руки используется в законодательных органах, международных аэропортах, больницах, иммиграционных службах и т.д. Преимущества идентификации по геометрии ладони сравнимы с плюсами идентификации по отпечатку пальца в вопросе надежности, хотя устройство для считывания отпечатков ладоней занимает больше места.

Идентификация по венозному рисунку руки. Это новая технология в сфере биометрии, широкое применение её началось всего лет 5-10 назад. Рисунок вен на ладони не меняется с двухлетнего возраста.

Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК-излучение. В результате степень отражения уменьшается и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством.

Преимущества метода. Отсутствие необходимости контактировать со сканирующим устройством. Высокая достоверность – статистические показатели метода сравнимы с показаниями радужной оболочки. Скрытость характеристики: в отличие от всех вышеприведённых – эту характеристику очень затруднительно получить от человека «на улице», например сфотографировав его фотоаппаратом. Являясь довольно точным, этот метод не требует столь дорогого оборудования, как, например, методы распознавания по геометрии лица или радужной оболочке.

Недостатки метода. Недопустима засветка сканера солнечными лучами и лучами галогеновых ламп. Некоторые возрастные заболевания, например артрит – сильно ухудшают характеристики метода. Метод менее изучен в сравнении с другими статическими методами биометрии.

Распознавание по рисунку вен руки является довольно новой технологией, и в связи с этим ее удельный вес на мировом рынке невелик и составляет около 3%.

Динамические методы биометрической аутентификации основываются на поведенческой (динамической) характеристике человека, то есть построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

Идентификация по почерку и динамике подписи. Основой аутентификации личности по почерку и динамике написания контрольных фраз (подписи) является уникальность и стабильность динамики этого процесса для каждого человека, характеристики которой могут быть измерены, переведены в цифровой вид и подвергнуты компьютерной обработке. Таким образом, при аутентификации выбирается для сравнения не продукт письма, а сам процесс и исследует его.

Для идентификации человека *по рукописному почерку* используется его роспись (иногда написание кодового слова). Подпись – такой же уникальный атрибут человека, как и его физиологические характеристики. Кроме того, это и более привычный для любого человека метод идентификации, поскольку он, в отличие от снятия отпечатков пальцев, не ассоциируется с криминальной сферой. Одна из перспективных технологий аутентификации основана на уникальности биометрических характеристик движения человеческой руки во время письма. Для контроля рукописной подписи используются дигитайзеры

Цифровой код индентификации формируется, в зависимости от необходимой степени защиты и наличия оборудования (графический планшет, экран корманного компьютера Palm и т.д.), двух типов:

- по самой росписи, то есть для идентификации используется просто степень совпадения двух картинок;

- по росписи и динамическим характеристикам написания, то есть для идентификации строится свертка, в которую входит информация по непосредственно подписи, временным характеристикам нанесения росписи и статистическим характеристикам динамики нажима на поверхность.

При формировании «эталона» необходимо учитывать, что для одного и того же человека характерен некоторый разброс характеристик почерка от одного акта к другому. Чтобы определить эти флуктуации и назначить рамки, пользователь при регистрации выписывает свою подпись несколько раз. В результате формируется некая «стандартная модель» (сигнатурный эталон) для каждого пользователя, которая записывается в память системы.

Обычно выделяют два способа обработки данных о подписи: простое сравнение с образцом и динамическую верификацию. Первый весьма ненадежен, так как основан на обычном сравнении введенной подписи с хранящимися в базе данных графическими образцами. Из-за того, что подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок.

Способ динамической верификации требует намного более сложных вычислений и позволяет в реальном времени фиксировать параметры процесса подписи, такие как скорость движения руки на разных участках, сила давления и длительность различных этапов подписи. Это дает гарантии того, что подпись не сможет подделать даже опытный графолог, поскольку никто не в состоянии в точности скопировать поведение руки владельца подписи.

Пользователь, используя стандартный дигитайзер и ручку, имитирует свою обычную подпись, а система считывает параметры движения и сверяет их с теми, что были заранее введены в базу данных. При совпадении образа подписи с эталоном система прикрепляет к подписываемому документу информацию, включающую имя пользователя, адрес его электронной почты, должность, текущее время и дату, параметры подписи, содержащие несколько десятков характеристик динамики движения (направление, скорость, ускорение) и другие. Эти данные шифруются, затем для них вычисляется контрольная сумма, и далее все это шифруется еще раз, образуя так называемую биометрическую метку. Для настройки системы вновь зарегистрированный пользователь от пяти до десяти раз выполняет процедуру подписания документа, что позволяет получить усредненные показатели и доверительный интервал.

Устройства идентификации по динамике подписи используют геометрические или динамические признаки рукописного воспроизведения подписи в реальном масштабе времени. Подпись выполняется пользователем на специальной сенсорной панели, с помощью которой осуществляется преобразование изменений приложенного усилия нажатия на перо (скорости, ускорения) в электрический аналоговый сигнал. Электронная схема преобразует этот сигнал в цифровой вид, приспособленный для машинной обработки. При формировании «эталона» необходимо учитывать, что для одного и того же человека характерен некоторый разброс характеристик почерка от одного акта к другому. Чтобы определить эти флуктуации и назначить рамки, пользователь при регистрации выписывает свою подпись несколько раз. В результате формируется некая «стандартная модель» (сигнатурный эталон) для каждого пользователя, которая записывается в память системы.

Разработка аутентификационных автоматов на базе анализа почерка (подписи – как варианта объекта исследования), предназначенных для реализации контрольно-пропускной функции, была начата еще в начале 1970-х г. В настоящее время на рынке представлено несколько эффективных терминалов такого типа. В качестве примера реализации такого метода идентификации можно рассматривать систему Automatic Personal Verification System (США). Эта система на испытаниях продемонстрировала следующие результаты: коэффициент ошибок I-го рода – 0,015%, II-го рода – 0,012% (в случае, если злоумышленник не наблюдал процесс исполнения подписи законным пользователем) и 0,25% (если он наблюдал).

Основное достоинство подписи по сравнению с использованием, например, дактилоскопии, в том, что это распространенный и общепризнанный способ подтверждения своей личности. В то же время подделка динамики подписи – дело очень трудновыполнимое (в отличие, скажем, от воспроизведения рисунка подписи). Росписи не на бумаге, а на сенсорной панели, значительно затрудняется копирование злоумышленником ее начертания.

Недостатки – подписи все еще легко подделать. Это препятствует внедрению идентификации личности по подписи в высокотехнологичные системы безопасности.

Идентификация по голосу и особенностям речи. Причинами внедрения систем с идентификацией голоса являются повсеместное распространение телефонных сетей и практика встраивания

микрофонов в компьютеры и периферийные устройства (построении «интеллектуальных зданий».). Распознающие автоматы производят аутентификацию (распознавание) голосов объективно, на основе строго детерминированных и априори заданных признаков. Процесс сравнивания образцов состоит из следующих стадий: фильтрация шумов, спектральное преобразование сигнала, постфильтрация спектра, лифтеринг, наложение окна Кайзера, сравнение.

Выбор параметров речевого сигнала способных наилучшим образом описать индивидуальность голоса, является самым важным этапом при построении систем автоматической аутентификации по голосу. Такие параметры сигнала, называемые признаками индивидуальности, помимо эффективности представления информации об особенностях голоса диктора, должны обладать рядом других свойств. Во-первых, они должны быть легко измеряемы и малозависимы от мешающих факторов окружающей среды (шумов и помех). Во-вторых, они должны быть стабильными во времени. В-третьих, не должны поддаваться имитации.

Разрабатываются комбинированные системы, состоящие из блоков идентификации и верификации голоса. Существует достаточно много способов построения кода идентификации по голосу, как правило это различные сочетания частотных и статистических характеристик голоса. Выбор параметров речевого сигнала способных наилучшим образом описать индивидуальность голоса является, пожалуй, самым важным этапом при построении систем автоматической аутентификации по голосу. Во-первых, они должны быть легко измеряемы и мало зависеть от мешающих факторов окружающей среды (шумов и помех). Во-вторых, они должны быть стабильными во времени. В-третьих, не должны поддаваться имитации.

При решении задачи идентификации находится ближайший голос (или несколько голосов) из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Вопросы оценки близости речевых характеристик того или иного индивидуума к заранее известному эталону-образцу тесно связаны с понятием стабильности голосовых и речевых характеристик человека. Известно, что голос лица, подлежащего идентификации, не может быть охарактеризован одним единственным произнесением, поскольку и голос и речь индивидуума по своей природе вариативны. Необходимо обработать ряд произнесений статистически (обработать полученную в процессе исследования выборку), чтобы определить характерные особенности голоса конкретного индивидуума.

Парольные фразы могут состоять из четырехсловного предложения, причем каждое слово было односложным. Каждая фраза представляется 84 байтами информации. Время аутентификации составляло 5,3 сек. Для предотвращения возможности использования заранее записанного на магнитофон пароля система генерировала слова в произвольной последовательности. Общее время проверки составляло 15 сек. на одного человека. Для четырех парольных фраз ошибка I-го рода составила 0,3%, II-го рода – 1%.

В последнее время ведутся активные разработки по усовершенствованию и модификации голосовых систем идентификации личности, поиск новых подходов для характеристики человеческой речи, комбинации физиологических и поведенческих факторов. Известны системы аутентификации по голосу, где применяется метод совместного анализа голоса и мимики, ибо, как оказалось, мимика говорящего характерна только ему и будет отличаться от говорящего те же слова мимики другого человека.

Для построения системы распознавания речи возможно использование *нейросетей.* Любой речевой сигнал можно представить как вектор в каком-либо параметрическом пространстве, затем этот вектор может быть запомнен в нейросети. Одна из моделей нейросети, обучающаяся без учителя – это самоорганизующаяся карта признаков Кохонена. В ней для множества входных сигналов формируется нейронные ансамбли, представляющие эти сигналы. Этот алгоритм обладает способностью к статистическому усреднению, т.е. решается проблема с вариативностью речи. Как и многие другие нейросетевые алгоритмы, он осуществляет параллельную обработку информации, т.е. одновременно работают все нейроны. Тем самым решается проблема со скоростью распознавания – обычно время работы нейросети составляет несколько итераций.

Задача повышения надежности распознавания может быть решена за счет привлечения грамматической и семантической информации в системах распознавания речи. Для решения этой задачи разработана (при участии экспертов: лингвистов, рядовых носителей языка) модель

входного языка, учитывающая особенности их грамматического и семантического поведения (28 основных грамматических классов, около 300 грамматических разрядов слов), ее компьютерное воплощение – лингвистическая база знаний (ЛБЗ) и лингвистический процессор (ЛП). Лингвистический модуль (ЛБЗ и ЛП) позволяет повысить надежность акустического и фонетического распознавания с 94-95% до 95-97%.

Для борьбы против использования магнитофонных записей парольных фраз, перехваченных во время установления контакта законного пользователя с аутентификационным терминалом применяют генерацию системой псевдослучайных паролей, которые повторяются вслед за ней пользователем, а также применение комбинированных методов проверки (дополняя вводом идентификационной карточки или цифрового персонального кода). Злоумышленникам, обладающим способностью к имитации голоса противостоит автомат, который в отличие от человека, не обладая способностью улавливать обобщенную характеристику голоса, свой вывод делает, привязываясь к конкретным параметрам речевого сигнала и производя их точный количественный анализ. Разрабатываются комбинированные системы, состоящие из блоков идентификации и верификации голоса. При решении задачи идентификации находится ближайший голос (или несколько голосов) из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Система практически используется при обеспечении безопасности некоторых особо важных объектов.

Основным и определяющим недостатком этого подхода является низкая точность идентификации. На результаты распознавания оказывают влияние помехи в микрофонах, шумы, ошибки при произнесении парольных фраз, различное эмоциональное состояние проверяемого в момент регистрации эталона и при каждой идентификации, использование разных устройств регистрации при записи эталонов и идентификации, помехи в низкокачественных каналах передачи данных и т.п.

Сегодня идентификация по голосу используется для управления доступом в помещения средней степени секретности, например, лаборатории производственных компаний.

Идентификация по клавиатурному почерку (по ритму работы на клавиатуре). Современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью, что позволяет достаточно однозначно идентифицировать пользователя. Применяются статистические методы обработки исходных данных и формирования выходного вектора, являющегося идентификатором данного пользователя. В качестве исходных данных используют временные интервалы между нажатием клавиш на клавиатуре и время их удержания. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой – резкий удар или плавное нажатие.

Основной характеристикой, по которой строится свертка для идентификации по ритму работы на клавиатуре – динамика набора кодового слова. Идентификация проводится и по ритму работы на клавиатуре основана на измерении временных интервалов между двумя последовательными ударами по клавишам при печатании знаков. Применяются статистические методы обработки исходных данных и формирования выходного вектора, являющегося идентификатором данного пользователя. В качестве исходных данных используют временные интервалы между нажатием клавиш на клавиатуре и время их удержания. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой – резкий удар или плавное нажатие [6].

Идентификация пользователя по клавиатурному почерку возможна следующими способами:

- по набору ключевой фразы;
- по набору произвольного текста.

Принципиальное отличие этих двух способов заключается в том, что в первом случае используется ключевая фраза, задаваемая пользователем в момент регистрации его в системе (пароль), а во втором случае используются ключевые фразы, генерируемые системой каждый раз в момент идентификации пользователя.

Подразумевается два режима работы: обучение и идентификация. На этапе обучения пользователь вводит некоторое число раз предлагаемые ему тестовые фразы. При этом рассчитываются и запоминаются эталонные характеристики данного пользователя. Начальный этап обработки данных – фильтрация. На этом этапе из потока данных удаляется информация о «служебных» клавишах – клавишах управления курсором, функциональных клавишах и т. д. Затем выделяется информация, относящаяся к следующим характеристикам пользователя: количество ошибок при наборе, интер-

валы между нажатиями и время удержания клавиш, число перекрытий между клавишами, степень аритмичности при наборе, скорость набора. Увеличить число эталонных характеристик, а следовательно, увеличить надежность системы можно, выполнив разделение входного потока на данные, относящиеся к левой и правой руке соответственно.

Эталонные характеристики пользователя, полученные на этапе обучения системы, позволяют сделать выводы о степени стабильности клавиатурного почерка пользователя и определить доверительный интервал разброса параметров для последующей идентификации пользователя (см. табл. 3). Время становления почерка работы с клавиатурой, при котором достигается необходимая вероятность идентификации пользователя – 6 месяцев.

Таблица 3

Оценка стабильности клавиатурного почерка пользователя

Ошибки,%	Аритмичность, %	Скорость, зн./мин	Характеристика перекрытий		Оценка
			Число перекрытий, %	Используемое число пальцев	
менее 2	менее 10	более 200	более 50	все	отлично
менее 4	менее 15	более 150	более 30	большинство	хорошо
менее 8	менее 20	более 100	более 10	несколько	удовл.
более 8	более 20	менее 100	менее 10	по одному	неуд.

На этапе идентификации рассчитанные оценки сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка. В задаче идентификации пользователя важным этапом является обработка первичных данных. В результате этой обработки входной поток данных разделяется на ряд признаков, характеризующих те или иные качества идентифицируемой личности. В дальнейшем эти признаки, подвергаясь статистической обработке, позволяют получить ряд эталонных характеристик пользователя.

Наиболее перспективным методом решения задачи идентификации пользователя по клавиатурному почерку представляется использование трехслойного перцептрона Розенблатта следующей конфигурации:

- первичный слой – входной, состоит из *к* формальных нейронов с линейной активаторной функцией, где *k*-размерность входного вектора, содержащего параметры клавиатурного почерка пользователя;

- второй слой – скрытый, состоит из *k* формальных нейронов с сигмоидной активаторной функцией,

- третий слой – выходной, состоит из *n* формальных нейронов с сигмоидной активаторной функцией, где *n* – число зарегистрированных пользователей.

Предлагаемый подход к задаче идентификации пользователя по клавиатурному почерку позволяет увеличить размерность вектора, содержащего эталонные характеристики пользователя. Применение нейронных сетей позволяет упростить математический аппарат обработки данных и уменьшить вероятность возникновения ошибок второго рода – положительного результата идентификации для незарегистрированных пользователей. В результате возможно существенное повышение надежности и устойчивости работы систем идентификации пользователя по клавиатурному почерку.

В последние годы применяют нейросетевой подход к задаче идентификации**.** Нейронные сети – это обобщенное название нескольких групп алгоритмов, обладающих одним ценным свойством: они умеют обучаться на примерах, извлекая скрытые закономерности из потока данных. Если между входными и выходными данными существует какая-то связь, пусть даже не обнаруживаемая традиционными корреляционными методами, нейронная сеть способна автоматически настроиться на нее с заданной степенью точности.

Применение нейросетевого подхода к задаче идентификации пользователя по клавиатурному почерку позволяет решить ряд проблем, возникающих при использовании стандартных методов статистической обработки входного потока данных. В частности, применение статистических методов обработки данных базируется на утверждении, что входные величины подчинены нормальному закону распределения, хотя в ряде случаев это утверждение неверно. Например, проведенные исследования показывают, что время удержания клавиш – при малом шаге дискретизации – описывается пересечением двух нормальных распределений, что приводит к большим погрешностям при расчете эталонных характеристик пользователя.

Кроме того, нейронная сеть обладает свойством фильтрации случайных помех, присутствующих во входных данных, что позволяет отказаться от алгоритмов сглаживания экспериментальных зависимостей, необходимых при статистической обработке данных.

Применение нейронных сетей позволяет упростить математический аппарат обработки данных и уменьшить вероятность возникновения ошибок второго рода – положительного результата идентификации для незарегистрированных пользователей. В результате возможно существенное по-

вышение надежности и устойчивости работы систем идентификации пользователя по клавиатурному почерку.

Преимуществом Метод я является то, что при проведении идентификации не нужно никакого специального оборудования, кроме стандартной клавиатуры. Основной характеристикой, по которой строится свертка для идентификации, является динамика набора кодового слова.

Недостатки – применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, т. е. к программистам, секретарям и т. д. В противном случае вероятность неправильного опознания «легального» пользователя существенно возрастает и делает непригодным данный способ идентификации на практике.

Биометрические идентификаторы обеспечивают очень высокие показатели: вероятность несанкционированного доступа – 0,1 – 0,0001 %, вероятность ложного задержания – доли процентов, время идентификации – единицы секунд, но имеют более высокую стоимость по сравнению со средствами атрибутной идентификации. Качественные результаты сравнения различных биометрических технологий по точности идентификации и затратам на их реализацию показаны на рис. 10.

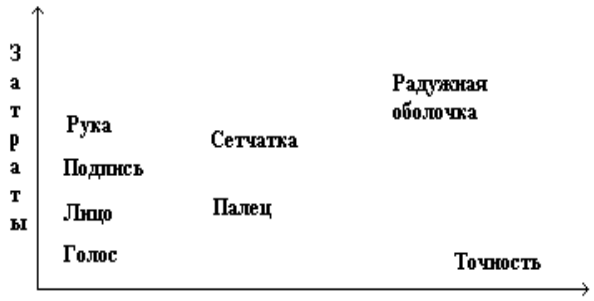


Рис. 10. Зависимость точности СКУД от ее стоимости

Биометрические технологии будущего. Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. К ним относятся технологии на основе [7]:

- термограммы лица в инфракрасном диапазоне излучения;
- характеристик ДНК;
- клавиатурного почерка;
- анализ структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи);
- анализ отпечатков ладоней;
- анализ формы ушной раковины;
- анализ характеристик походки человека;
- анализ индивидуальных запахов человека;
- распознавание по уровню солености кожи;
- распознавание по расположению вен.

Технология построения и анализа ***термограммы*** является одним из последних достижений в области биометрии. Термограмма лица является уникальной, вследствие чего можно уверенно различать даже абсолютно похожих близнецов. Из дополнительных свойств этого подхода можно отметить его инвариантность по отношению к любым косметическим или косметологическим изменениям, включая пластическую хирургию, изменения макияжа и т.п., а также скрытность процедуры регистрации.

Технология, построенная на анализе ***характеристик ДНК*** (метод геномной идентификации) является хотя и самой продолжительной, но и наиболее перспективной из систем идентификации. Метод основан на том, что в ДНК человека имеются полиморфные локусы (локус – положение хромосомы (в гене или аллели), часто имеющие 8-10 аллелей. Определение набора этих аллелей для нескольких полиморфных локусов у конкретного индивида позволяет получить своего рода геномную карту, характерную только для этого человека. Точность данного метода определяется характером и количеством анализируемых полиморфных локусов и на сегодняшний день позволяет достичь уровня ошибки 1 на 1 млн. человек.

Динамика ударов по клавиатуре – ***клавиатурный почерк*** – компьютера при печатании текста, или клавиатурный почерк, анализирует способ (ритм) печатания пользователем той или иной фразы. Существуют два типа систем распознавания клавиатурного почерка. Первые предназначены для аутентификации пользователя при попытке получения доступа к вычислительным ресурсам. Вторые осуществляют мониторинговый контроль уже после предоставления доступа и блокируют систему, если за компьютером начал работать не тот человек, которому доступ был предоставлен первоначально. В литературе описаны 4 математических подхода к решению задачи распознавания клавиатурного почерка пользователя ЭВМ: статистический, вероятностно-статистический (на базе теории распознавания образов) и нечеткой логики (на основе нейросетевых алгоритмов).

Для идентификации человека по руке используют несколько биометрических параметров – это

геометрическая форма кисти руки или пальцев, расположение подкожных кровеносных сосудов ладони, узор линий на ладони.

Технология анализа ***отпечатков ладоней*** стала развиваться сравнительно недавно, но уже имеет определенные достижения, разрабатывают технологии, анализирующие не рисунок линий на коже, а очертание ладони, которое также имеет индивидуальный характер. Компьютеризация этого процесса позволит использовать отпечатки ладоней более широко и приведет к существенному увеличению раскрываемости преступлений. Следует отметить, что устройства сканирования ладони, как правило, имеют высокую стоимость.

Идентификация ***по венозному рисунку руки*** – новая технология в сфере биометрии, широкое применение её началось всего лет 5-10 назад. Рисунок вен на ладони не меняется с двухлетнего возраста. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК-излучение. В результате степень отражения уменьшается и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством. Распознавание по рисунку вен руки является довольно новой технологией, и в связи с этим ее удельный вес на мировом рынке невелик и составляет около 3%.

Технология анализа ***формы ушной раковины*** является одной из самых последних подходов в биометрической идентификации человека. С помощью даже недорогой Web-камеры можно получать довольно надежные образцы для сравнения и идентификации. Этот способ недостаточно изучен, в научно-технической литературе достоверная информация о текущем состоянии дел отсутствует.

В настоящее время ведутся разработки систем «электронного носа» реализующих процесс распознавания ***по запаху***. Наличие генетического влияния на запах тела позволяют считать эту характеристику перспективной для использования в целях биометрической аутентификации личности. Как правило, «электронный нос» представляет собой комплексную систему, состоящую из трех функциональных узлов, работающих в режиме периодического восприятия пахучих веществ: системы пробоотбора и пробоподготовки, линейки или матрицы сенсоров с заданными свойствами и блока процессорной обработки сигналов матрицы сенсоров.

Среди признаков лица, используемых для идентификации человека, наиболее устойчивыми и трудно изменяемыми является также признаки ***изображения его кровеносных сосудов***. Распределение на лице артерий, снабжающих кровью кожу, которые выделяют тепло, уникальною. Путем сканирования изображения лица в инфракрасном диапазоне света создается уникальная температурная карта лица – *термограмма.* Идентификация по термограмме обеспечивает показатели, сравнимые с показателями идентификации по отпечаткам пальцев.

Ожидается, что в самом ближайшем будущем пароли и PIN-коды уступят место новым, более надежным средствам авторизации и аутентификации. Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах контроля и управления доступом. В настоящее время структура этого рынка представлятся следующим образом: верификация голоса – 11 %, распознавание лица – 15 %, сканирование радужной оболочки глаза – 34 %, сканирование отпечатков пальцев – 34 %, геометрия руки – 25 %, верификация подписи – 3 %.

Список литературы:

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом». Учебное пособие. – М.: Горячая линия – Телеком. – Серия «Обеспечение безопасности объектов». Книга 2. 2010 -272 с.:ил.

2. Татарченко Н.В., Тимошенко С.В. Биометрическая идентификация в интегрированных системах безопасности. Специальная техника, №2, 2002.

3. Минаев В.А. Современные технологии обеспечения информационной безопасности. «Биометрический квартал». 16.05.02 г.

4. Дахва М.С. Идентификация по геометрии кисти руки. 2012.

5. Джонатан П., Филипс и др. Введение в оценку биометрических систем. «Открытые системы», №3. 2000.

6. Завгородний В.В., Мельников Ю.Н. Идентификация по клавиатурному почерку. «Банковские технологии», №9,1998.

7. А. Гинце. Новые технологии в СКУД. Системы безопасности, №6. 2005.