Северо-Кавказский юридический вестник. 2022. № 3. С. 167–174
North Caucasus Legal Vestnik. 2022;(3):167–174

Проблемы уголовного права и криминалистики

Научная статья
УДК 343.98.065
doi: 10.22394/2074-7306-2022-1-3-167-174

ИДЕНТИФИКАЦИЯ ЧЕЛОВЕКА ПО БИОМЕТРИЧЕСКИМ ДАННЫМ: ОБЗОР СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

Елена Юрьевна Фролова[1], Юлия Александровна Кошлыкова[2]

[1, 2]Южный федеральный университет, Ростов-на-Дону, Россия

[1]frolova@sfedu.ru, https://orcid.org/0000-0001-7347-3747
[2]koshlykova@sfedu.ru, https://orcid.org/0000-0002-4229-6562

***Аннотация*.** Биометрические системы идентификации получили в настоящее время достаточно широкое распространение, поскольку в них для распознавания используются не специализированные физические носители информации, а признаки или особенности самого человека, что позволяет достоверно идентифицировать лицо для заданных целей. Биометрическая идентификация представляет собой процесс сравнения и определения сходства между данными человека и его биометрическим «шаблоном». Биометрия позволяет идентифицировать и провести верификацию человека на основе набора специфических и уникальных черт, присущих ему от рождения. В настоящей статье рассматриваются отдельные виды биометрических данных, проблемы и перспективы их использования для решения идентификационных задач.

Ключевые слова: биометрические данные, идентификация, системы безопасности, отпечатки пальцев, признаки внешности, сетчатка глаза, голос, динамический портрет, ДНК

Для цитирования: Фролова Е. Ю., Кошлыкова Ю. А. Идентификация человека по биометрическим данным: обзор современных технологий // Северо-Кавказский юридический вестник. 2022. № 3. С. 167–174. https://doi.org/10.22394/2074-7306-2022-1-3-167-174

Problems of Criminal Law and Criminalistics

Original article

HUMAN IDENTIFICATION BASED ON BIOMETRIC DATA: A REVIEW OF MODERN TECHNOLOGIES

Elena Yu. Frolova[1], Yulia A. Koshlykova[2]

Southern Federal University, Rostov-on-Don, Russia

[1]frolova@sfedu.ru, https://orcid.org/0000-0001-7347-3747
[2]koshlykova@sfedu.ru, https://orcid.org/0000-0002-4229-6562

***Abstract*:** biometric identification systems have now become quite widespread, since they use not specialized physical media for recognition, but signs or features of the person himself, which makes it possible to reliably identify a person for a given purpose. Biometric identification is the process of comparing and determining the similarity between a person's data and his biometric "template". Biometrics allows you to identify and verify a person based on a set of specific and unique traits inherent in him from birth. This article discusses certain types of biometric data to be identified, problems and prospects of their application.

Key words: biometric data, identification, security systems, fingerprints, signs of appearance, retina, voice, dynamic portrait

For citation: Frolova E. Yu., Koshlykova Yu. A. Human identification based on biometric data: a review of modern technologies. *North Caucasus Legal Vestnik.* 2023;(3):167–174. (In Russ.). https://doi.org/10.22394/2074-7306-2022-1-3-167-174

В современных реалиях значительное число систем безопасности, персональных гаджетов и иных аппаратно-программных комплексов подразумевает в своем функционале технологии считывания биометрических данных и аутентификации по ним конкретных лиц. Биометрию вводят в свой функционал как крупные всероссийские системы безопасности, сеть которых охватывает целую инфраструктуру городов, так и единичные пропускные системы на предприятиях и в организациях. Целесообразность и результативность использования биометрических данных, лежащих в основе конкретных систем безопасности, определяется их целевым назначением и принципом действия конкретных идентификаторов.

Стандартная классификация биометрических данных представляет собой деление на статические (отпечаток пальца, форма кисти, рисунок вен, форма лица, радужная оболочка/сетчатка глаза, ДНК и др.) и динамические (почерк, походка, голос, движение губ и др.) [1, с. 163].

Одним из самых часто используемых видов биометрических данных является отпечаток пальца человека. Папиллярные узоры действительно представляют собой достаточно качественный и уникальный биометрический материал, пригодный для решения идентификационных задач в силу индивидуальности, постоянства (в течение человеческой жизни рисунок не изменяется), восстанавливаемости и отражаемости. Данный вид биометрии имеет довольно широкий спектр применения не только в повседневной жизни (оцифрованные сканы подушечек пальцев используются для идентификации человека при входе в различные закрытые системы – от различных гаджетов до локальных пропускных комплексов), но и лежит в основе современных систем регистрации преступников.

Принцип действия устройств, распознающих папиллярные узоры, заключается в определении структуры линий на подушечках пальцев рук: сканер считывает уникальный рисунок и транслирует в программное обеспечение цифровой биометрический шаблон, по которому непосредственно происходит идентификация личности. Из всех технических этапов данного процесса (получение изображения отпечатка пальца, обработка этого изображения, определение отличительных характеристик, создание шаблона и соответствие шаблону проверяемых отпечатков [2, с. 66]) в рамках раскрытия и расследования преступлений особенно важным является именно процесс отождествления обнаруженных в ходе расследования отпечатков пальцев с имеющимися в базе данных дактокартами зарегистрированных лиц. Поэтому значительное внимание следует уделить совершенствованию технических характеристик, позволяющих достоверно зафиксировать отпечаток и в последующем надлежащим образом определить его принадлежность конкретному лицу.

В настоящее время имеется значительный опыт использования различных оптических и кремниевых сканеров. Оптические сканеры являются наиболее точными с точки зрения определения и считывания папиллярного узора, однако их можно обмануть с помощью силиконовых или латексных накладок и других нехитрых приёмов. Наиболее универсальным и перспективным является считывание отпечатка пальца с помощью специального светоизлучающего датчика (пленка LES), устойчивого к температурам, типу освещения, уровню влажности и иным потенциально искажающим результат факторам. Преимущества данного метода – скорость, простой в использовании технический функционал датчиков, устойчивость к искажающим факторам (освещение, сухость/влажность кожи) и долговечность самой технологии, обеспечивающей биометрическую верификацию.

Наиболее современные сканеры имеют возможность мгновенно проверить качество отпечатка благодаря подсветке для контроля состояния сканирования, а также подразумевают вариант кодирования и декодирования изображение с использованием вейвлет-скалярного квантования (алгоритм WSQ).

В основе функционирования крупномасштабных систем, включающих возможность аутентификации и идентификации, таких, как аппаратно-программные комплексы, составляющие системы безопасности в помещениях и на улицах городов (к примеру, АПК «Безопасный город»), преимущественно лежит распознавание лица по признакам внешности. Кроме этого, методы сбора, изучения и использования данных о внешнем облике человека активно применяются и в повседневной жизни (аутентификация человека по набору заданных точек при разблокировке смартфонов и подтверждении оплаты с помощью электронных кошельков; процесс подтверждения личности при пользовании банкоматом; использование биометрического паспорта при пересечении границ и пребывании за границей), в коммерческих целях сейчас внедряются нейронные сети, позволяющие распознать личность человека по его образу на фотографии (в том числе по цифровому скану паспорта), подтвердить или опровергнуть, что образ принадлежит одному и тому же лицу и найти соответствие образца в заданной базе данных (технология IDX)[1]. Традиционно в качестве массива биометрических данных по данному критерию рассматривается набор антропометрических точек лица, которые считываются в рамках измерения геометрии лица (основными параметрами является расстояние между глазами, от подбородка до лба, диагонали от носа к внутренней стороне глаза и линии от всех выступающих частей лица до ушей). Функционально в большинстве систем, содержащих технологию распознавания лиц, зафиксированный антропометрический портрет преобразуется в зашифрованный код, именуемый сигнатурой лица.

Как работает данная технология? Распознавание лица с помощью функционала камер видеонаблюдения происходит в несколько этапов. Первый этап представляет собой выделение лица человека из многопотокового объема биометрических данных: лица идентифицируются как отдельные, принадлежащие разным индивидам. На данном этапе важно, чтобы лица были в зоне видимости камер под достаточным углом, хотя многие современные устройства способны различать необходимый набор внешних параметров, даже если к камере обращена 1/3 лица. За этим следует довольно сложный технологически процесс вычисления антропометрических точек [3, с. 255-265]. Система определяет набор опорных точек на лице, в результате чего можно составить индивидуальную характеристику внешних признаков. Следующим этапом является преобразование полученного изображения: проводится фотомонтаж, позволяющий повысить четкость изображения, внести цветовые корректировки и даже изменить наклон головы. Завершающий этап – вычисление набора характеристик, описывающих лицо вне зависимости от посторонних факторов (прическа/аксессуары/головной убор). На этом этапе задействуются дескрипторы, позволяющие с максимальной точностью оценить соотношение полученного изображения с хранящимися в определенной заданной базе и понять, относятся они к одному человеку или нет. Тем не менее, антропометрический портрет не является стопроцентной гарантией достоверной идентификации лица, в связи с чем возникают идеи замены традиционного распознавания 3D технологиями. Но в данном контексте уместно рассматривать внедрение специальных модулей распознавания, которые будут хранить в себе весь массив 3D сканов лиц для их последующей идентификации.

Наравне с антропометрическим портретом, немаловажную роль в идентификации человека по его изображениям играет динамический портрет. По исследованиям физиологов наиболее эффективно человека можно распознать по следующим признакам: поза, жестикуляция, мимика, походка (японские исследователи обнаружили, что с помощью

[1] https://iidx.ru/uslugi/raspoznavanie-lits/

3D-съемки человека можно корректно идентифицировать его по походке в 90% случаев). В условиях, когда анатомо-морфологические признаки трудно различимы системой видеонаблюдения, распознание динамико-функциональных признаков позволило бы создать достаточно полный портрет. В данном случае для полноценной идентификации необходимо усовершенствовать пространственное соотношение расположения камер видеонаблюдения в системах безопасности: в конкретных интересующих правоохранителей пространствах камеры должны быть установлены в таком соотношении друг с другом, чтоб расстояние до каждой точки помещения не превышало расстояние 75 м (т.к. по среднестатистическим данным в обычной жизни человек может распознать жестикуляцию, походку, осанку и прочие динамические параметры с расстояния 150 м, учитывая несовершенство видео-фиксации, возьмём половинную величину). На данный момент на практике узконаправленно применяются программы, характеризующие состояние человека в моменты, когда он идет или стоит (встроенные в смартфоны акселерометры и гироскопы, которые считают количество шагов и пройденный за определенный промежуток времени километраж). Длина шага, усилия, прикладываемые для удержания равновесия, и скорость передвижения и иные индивидуальные динамический параметры также позволяют нам воссоздать базовые характеристики динамического портрета, что может иметь колоссальную практическую пользу как для бытовых целей (оценки уровня физической нагрузки), так и для идентифицирующего функционала систем безопасности.

На практике распознавание лиц по признакам внешности может быть реализована следующим образом. В систему безопасности технически включается возможность использования различных программных комплексов распознавания лиц («Face-интеллект» «Визирь», «Нетрис»), которые находят лица на видеоизображении, сравнивают их с заданной базой данных, осуществляют дальнейшие запрограммированные действия и отправляют органам внутренних дел сигнал об идентификации разыскиваемого преступника. Указанные системы могут сравнивать лица с базами данных госучреждений и правоохранительных органов, могут осуществлять быстрый поиск видеозаписей с лицами, интересующими службу безопасности или правоохранительные органы по фотографии, фотороботу или видеокадру.

Сегодня практика такого рода в функционале систем безопасности отсутствует, хотя технические проекты этих систем подразумевают такую возможность. Пока поиск осуществляется при проверке конкретных данных — стыковки с базами нет, задача полномасштабной идентификации не решена. Встает вопрос, что с технической точки зрения будет проще реализовать и что принесет наиболее быстрый и достоверный результат: соотнесение с готовыми базами данных органов и учреждений или включение в программное обеспечение собственной базы? Что и в каких пропорциях целесообразнее задействовать, государственные базы криминалистического учета, биометрические базы банков или операционных систем персональных гаджетов, в которые люди добровольно согласились предоставить свои биометрические данные?

По нашему мнению, наиболее оптимальным вариантом представляется возможность выделить правоохранительным органам закрытый сектор системы безопасности (к примеру, в Ростовской области правоохранители используют для данных целей АПК «Безопасный город»), оснащенный дополнительным модулем распознавания. На практике уже реализуется функция подключения в автономном порядке определенных баз данных: организация может загрузить в программу локальную базу (на 200-300 лиц). В более долгосрочной перспективе, на наш взгляд, представляется результативным интегрировать современные системы безопасности с ПК «Face-интеллект» при проверке по базам данных: тогда все процессы будут происходить в реальном времени, а задержать распознанное лицо при наличии такой необходимости можно будет в кратчайшие сроки.

Одним из достаточно сложных видов биометрических данных с точки зрения физиологии и динамики является голос, технология распознавания которого попадает в сферы и биологических, и поведенческих биометрических данных. Технологии верификации и идентификации по голосу имеют ценность как в рамках функционирования коммерческих информационных ресурсов (Банком России был разработан механизм удаленной идентификации, при котором человек может добровольно предоставить в установленном порядке образец голоса и в дальнейшем получать банковские услуги удаленно, подтвердив свои биометрические данные в мобильном приложении), так и на уровне деятельности правоохранительных органов и обеспечения гос. безопасности (помимо криминалистики и судебной экспертизы распознавание по голосу в радио-разведке, контрразведке и антитеррористическом мониторинге [4, с. 1]).

Современные системы распознавания способны различить из физиологических параметров форму голосового тракта человека, движения носа, рта и гортани и непосредственно определить воспроизводимый звук. Из поведенческих характеристик можно распознать тон голоса, темп говорения, акцент и иные индивидуализирующие признаки. Рассмотрение указанных характеристик в совокупности составляет так называемую голосовую подпись, которая является достоверным объектом идентификации в нормальных условиях (методика не применима при болезни человека и иных факторах, препятствующих функционированию гортанной системы).

В настоящее время существуют программные комплексы, успешно идентифицирующие людей по голосу. К примеру, это IDVoice, – голосовое биометрическое ядро из свёрточной нейронной сети, способное извлечь характеристики голоса и сравнить с записанными в базе данных голосами (обширно используется для мобильного банкинга и программного обеспечения колл-центров). Основная проблема заключается в том, что идентификация личности по голосу и речи, осуществленная по одному единственному произнесению, никогда не будет корректной и достоверной.

В соответствии со статистикой фонетических исследований, когда измеряют длительность, высоту основного тона, интенсивность и т.д., результаты, даже если объектом исследования являются несколько произнесений одного и того же диктора, будут колебаться [5, с. 35]. Иначе говоря, необходимо статистически обработать определенный набор произнесений фигуранта экспертизы (т.е. подвергнуть статистическому анализу полученную в процессе проведения экспертного исследования выборку), чтобы получить достоверные значения идентификационных признаков, характеризующих голос и речь данного индивидуума [6, с. 248].

Еще одним биологическим параметром, позволяющим решить идентификационные задачи, является сетчатка глаза. Область применения пока не столь обширна: технологии распознавания по сетчатке глаза пытаются внедрить банки, тестирующие различные биометрические параметры для повседневного использования, а также некоторые компании, разрабатывающие аутентификационные программы для персональных гаджетов. Относительно успешно данный метод распознавания используется предприятиями, располагающими передовыми пропускными системами: при регулярном взаимодействии с лицом технология поэтапно считывает сначала статические и динамические признаки внешности, а затем, обладая достаточным количеством ракурсов и качественных характеристик, сохраняет образец сетчатки, идентифицируя человека в дальнейшем в том числе и данным способом.

Современные идентифицирующие устройства позволяют в режиме реального времени считать и проанализировать сетчатку глаза на расстоянии и в движении. Предполагается, что подобные считывающие конструкции могут составить конкуренцию традиционным для систем безопасности технологиям распознания человека по антропометрическим данным. Процесс считывания сетчатки подразумевает сканирование капилляров,

расположенных внутри глаза, благодаря камерам ближнего инфракрасного диапазона, качественную обработку изображения и преобразования данных в биометрический шаблон для верификации или идентификации.

Данный метод обладает рядом преимуществ: сетчатка является одним из самых стабильных и надежных биометрических параметров, практически не изменяющимся на протяжении жизни; учитывая небольшой объем считываемых и анализируемых данных при сканировании сетчатки, система способна быстро подтверждать личность человека; из-за значительного количества уникальных признаков, которыми обладает сетчатка, вероятность ложного срабатывания минимизирована. Применение данного вида биометрических данных является очень результативным, но, тем не менее, скорее в перспективе будущего, т.к., во-первых, из-за высоких требований к идентифицируемому объекту может понадобиться неоднократное количество попыток аутентификации, во-вторых, имеется риск получения результатов в течение достаточно длительного времени. Помимо этого, с практической точки зрения обеспечение считывания указанных характеристик на дальнем расстоянии и высокая стоимость оборудования затрудняет внедрение распознавания по сетчатке глаза в функционал современных систем безопасности.

В настоящее время самой известной программой по идентификации и верификации личности по сетчатке глаза является HBOX (EyeLock) – устройство наподобие видеокамеры, позволяющее считывать в реальном времени до 50 сетчаток глаз в минуту. Производители заявляют, что сканер имеет возможности интеграции со всеми доступными стандартными системами и платформами управления доступом, что должно обеспечить его эффективное внедрение в городские и локальные системы безопасности.

Довольно давнюю и обширную практику имеет процесс идентификации лица по его ДНК. Проводится она для идентификации личности человека при работе с пропавшими без вести, в расследовании таких тяжких преступлений, как убийства, изнасилования/насильственные действия сексуального характера, нанесение телесных повреждений, при выявлении жертв катастроф и в иных случаях, когда человека можно опознать по геномному материалу.

Идентификационными объектами обычно выступают выделения биологического материала: кровь, сперма, эякуляционный секрет, следы эпителия, частицы внутренних органов на орудиях убийства и т.п. ДНК содержит последовательности коротких тандемных повторов (short tandem repeat sequences), с помощью которых можно достоверно идентифицировать личность, сравнивая их с другими STR в базе данных. Генетическая экспертиза обладает широким спектром возможностей: ПДРФ-анализ (один из первых методов генетического анализа, широкая разрешающая способность, в настоящее время вытеснен ПЦР-анализом), ПЦР-анализ (восстановление информации по очень малым (деградирующим) образцам, многократная амплификация участков ДНК), КТП-анализ (установление различия между индивидуумами), митохондриальный анализ (ядерная ДНК, является полезным дополнением при идентификации в таких случаях, как поиск пропавших без вести лиц, когда имеются только родственники по материнской линии.

Основная проблема в данном случае заключается в том, что зачастую геномный материал сложно изъять из-за недостаточного объема или возможного наслоения биологических следов. Изъять и выделить интересующий след из множества оставленных на объекте иногда затруднительно по причине того, что в биологии нет понятия «последние руки»: изымая с предмета какой-либо клеточный материал, эксперт собирает всю массу клеточного материала, который был оставлен на предмете на протяжении его существования. ДНК считается наиболее точной биометрической характеристикой, однако, на данный момент эта технология применяется в основном для решения экспертных задач.

Что касается технической части, конкретных систем, осуществляющих идентификацию по ДНК, в коммерческом обороте не имеется, а эксперты с правом проведения генети-

ческих экспертиз используют технологию Power Plex 16, выпускаемую компанией Promega, включающую 15 STR-маркеров, обязательных при проведении генетической экспертизы в России согласно приказу[1] МВД РФ № 70 от 10.02.2006 г.

На основании всего вышесказанного можно сделать вывод, что каждый отдельный рассмотренный нами вид биометрии считывается и преобразуется с помощью специализированного технического комплекса, который хоть и подразумевает в своем функционале достаточно достоверные методы идентификации, но в силу своей узкой направленности на конкретный вид данных не может быть использован в случаях, если используемый в качестве идентификатора параметр не обнаружен.

По нашему мнению, интеграция отдельных технологий считывания конкретных биометрических параметров представляется наиболее эффективной в рамках функционирования современных систем безопасности. Именно задействование комплексных систем идентификации по совокупности биометрических параметров поможет минимизировать существующие риски и обеспечить достоверное распознавание субъектов и результативную деятельность систем безопасности, что позволит обеспечить наиболее достоверную идентификацию.

Список источников

1. Тульских В. Д. Использование биометрических технологий в экспертно-криминалистической деятельности // Армия и общество. 2013. №1. С. 161-164.

2. Нечаева В. С. Идентификация отпечатков пальцев в биометрической системе безопасности // Вестник магистратуры. 2021. №5-3 (116). С. 65-66.

3. Кухарев Г.А., Казиева Н. Применение цифровой лицевой антропометрии // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 2. С. 255-270.

4. Сорокин В. Н., Вьюгин В. В., Тананыкин А. А. Распознавание личности по голосу: аналитический обзор // Информационные процессы. 2012. Т. 12. № 1. С. 1-30.

5. Зиндлер Л. Р. Общая фонетика. М.: Высшая школа, 1979. 312 с.

6. Каганов А. Ш. Криминалистическая идентификация личности по голосу и звучащей речи как интегральное научно-экспертное исследование // Филологические науки. Вопросы теории и практики. 2019. Т. 12. № 6. С. 246-250.

References

1. Tulskikh V. D. The use of biometric technologies in forensic activity. *Army and society.* 2013;(1):161-164. (In Russ.)

2. Nechaeva V.S. Fingerprint identification in the biometric security system. *Bulletin of the Magistracy.* 2021;5-3 (116):65-66. (In Russ.)

3. Kukharev G.A., Kazieva N. Application of digital facial anthropometry. *Scientific and Technical Bulletin of information Technologies, Mechanics and Optics.* 2019;19(2):255-270. (In Russ.)

[1] Приказ МВД РФ от 10.02.2006 N 70 "Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации" (вместе с "Инструкцией по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации", "Правилами ведения экспертно-криминалистических учетов в органах внутренних дел Российской Федерации")

4. Sorokin V. N., Vyugin V. V., Tananykin A. A. Personality recognition by voice: an analytical review. *Information processes.* 2012;12(1):1-30. (In Russ.)

5. Zinder L. R. General phonetics. Moscow: Higher School; 1979. 312 p. (In Russ.)

6. Kaganov A.Sh. Criminalistic identification of a person by voice and sounding speech as an integral scientific expert study. *Philological sciences. Questions of theory and practice.* 2019; 12(6):246-250. (In Russ.)

Информация об авторах

Е. Ю. Фролова – канд. юрид. наук, доцент кафедры уголовного процесса и криминалистики юридического факультета ЮФУ;

Ю. А. Кошлыкова – студент юридического факультета ЮФУ.

Information about the authors

E. Yu. Frolova – Associate Professor of the Department of Criminal Process and criminalistics of the Faculty of Law of Southern Federal University;
Yu. A. Koshlykova – Bachelor of the Department of Criminal Process and criminalistics of the Faculty of Law of Southern Federal University.

Автор заявляет об отсутствии конфликта интересов.
The author declares that there is no conflict of interest.

Статья поступила в редакцию 07.07.2022; одобрена после рецензирования 22.07.2022; принята к публикации 23.07.2022.
The article was submitted 07.07.2022; approved after reviewing 22.07.2022; accepted for publication 23.07.2022.