Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 4, Is. 2, pp. 61-67, 2015

DOI: 10.13187/vesp.2015.4.61
www.ejournal21.com

UDC 004.5

Methods and the Means of the Biometric Identification of the Personality

Yuri F. Katorin

National research university of information texnologies, mechanics and optics, Russian Federation
197101, Sankt-Peterburg, Kronverkskiy prospekt, 49
Dr. (Military), Professor
E-mail: katorin@mail.ru

Abstract

The article describes the basic methods of biometric identification. Built on its basis the access restriction system can control access to information and repositories in banks, it can be used at the enterprises involved in the processing of valuable information, to protect the means of communication, etc. Also describes the advantages and disadvantages of each method.

Keywords: safety, the control of access, the reliability of identification, biometric characteristics, scanners.

Введение

Надежность (устойчивость к взлому) системы контроля доступа в значительной степени определяется типом используемого идентификатора. Обычно это карточка, брелок, метка, код, вводимый на клавиатуре. Однако для особо важных объектов подобные идентификаторы применять не следует. Например, наиболее распространенные бесконтактные карты «proximity» могут подделываться в мастерских по изготовлению ключей на оборудовании, имеющемся в свободной продаже. Поэтому для объектов, требующих более высокого уровня защиты, подобные идентификаторы не подходят. Принципиально более высокий уровень защищенности обеспечивают биометрические признаки человека. [1]

Основные составляющие биометрического метода – это сканер для измерения биометрической характеристики и алгоритм, позволяющий сравнить ее с предварительно зарегистрированной той же характеристикой (так называемым биометрическим шаблоном). Возможны два режима работы системы – верификация (сравнение одного с одним) и идентификация (сравнение одного со многими). При верификации пользователь вводит имя, пароль или другим способом объявляет системе, «кто он такой». Задача системы в этом случае – проверить достоверность этой информации, т.е. сверить измеряемую биометрическую характеристику с имеющимся шаблоном заявленного индивидуума. При идентификации пользователь просто «предъявляет биометрику», и задача алгоритма – решить, известен ли пользователь системе и кто он. В этом случае измеряемая биометрическая характеристика сравнивается с базой данных ранее записанных шаблонов.

При этом необходимо выполнения следующих условий:

- каждый человек должен обладать той характеристикой, которая требуется для данного биометрического метода;
- характеристика не должна быть одинаковой у двух разных людей. Уникальность можно определить как минимально достижимое для данной биометрии значение FAR (False Acceptance Rate) – вероятности ложного распознавания, т. е. вероятности того, что система спутает двух индивидуумов;
- биометрическая характеристика не должна меняться во времени (так называемое старение биометрического шаблона);
- должно быть небольшое среднее время распознавания (recognition_time). Под временем распознавания подразумевается время верификации либо идентификации, в зависимости от режима, в котором работает система;
- биометрический метод должен быть устойчив к изменению окружающей среды;
- система должна быть устойчивой к подделке (несанкционированному доступу). [2]

Обсуждение

В связи с совершенствованием средств несанкционированного доступа к информации, необходимость новых решений в области обеспечения безопасности несомненна. Различные предприятия, учреждения, банки нуждаются в системах контроля и управления доступом. Биометрическая система может контролировать доступ к информации и хранилищам в банках, ее можно использовать на предприятиях, занятых обработкой ценной информации, для защиты ЭВМ, средств связи и т.д. Кроме того, для правоохранительных органов стала очевидной необходимость точной идентификации в местах массового скопления людей, при контроле пропусков и сверке документов. В первую очередь проблема коснулась безопасности транспортных систем – аэропортов, вокзалов, морских портов, метрополитена, а также государственных и межгосударственных систем – паспортно-визовых, таможенных, миграционных и оперативных служб. И именно биометрические решения вызывают сейчас наибольший интерес в этой сфере во всем мире. Что же касается отдельных сегментов биометрического рынка, здесь эксперты в основном сходятся во мнениях. Так, идентификации по отпечаткам пальцев они отводят в ближайшие годы все еще более половины рынка. [3]

Далее следует распознавание по геометрии лица и радужной оболочке. Это так называемые «три большие биометрики». За ними идут остальные методы распознавания примерно в такой последовательности: геометрия руки, рисунок вен, голос, подпись. С точки зрения экологии методы и средства биометрической идентификации личности совершенно безопасны. Эти вопросы имеют и важный политический аспект, ибо активно развивается международная нормативная техническая и правовая база. Практически сразу после 11 сентября 2001 г. при Международной организации по стандартам (ISO) создан подкомитет SC37 по биометрии, призванный оперативно разработать и утвердить единые международные стандарты использования, обмена и хранения биометрических данных. Аналогичные комитеты созданы во многих национальных органах по стандартам. [3]

Вопрос социальной значимости при использовании указанных методов, стоит достаточно остро. Согласие общества на сбор и использование тех или иных биометрических данных – необходимое условие массового внедрения биометрических методов. Вместе с тем, существуют разные причины, по которым сбор и хранение определенных биометрических характеристик может оказаться неприемлем для общества. Например, отпечатки пальцев традиционно ассоциируются с преступлением. Для многих существенно и то, что распознавание по отпечаткам пальцев – контактный способ, он требует соприкосновения со сканером, используемым другими людьми. Другой серьезный недостаток отпечатков пальцев – это возможность их кражи и использования не только для несанкционированного доступа, но и для фальсификации улик. Возражения против распознавания по радужной оболочке глаза связаны с возможностями иридодиагностики и получения тем самым частной информации о человеке. Зато внешность человека, в отличие от других характеристик, не вызывает возражений, хотя это наиболее естественный идентификатор, который может использоваться, например, оператором-человеком для проверки, данных выданных компьютером. [4]

Основной сферой применения следует считать использование в системах контроля и управления доступом (СКУД). Основными методами, использующими статистические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза человека, рисунку вен руки. Также существует ряд методов, использующих динамические характеристики человека: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке. Продуктами являются технические средства идентификации, производство которых развернуто во многих странах мира. Обобщив результаты для методов, можно сказать, что для средних и больших объектов, а также для объектов с максимальным требованием в безопасности, следует использовать радужную оболочку в качестве биометрического доступа и, возможно, распознавание по венам рук. Для объектов с количеством персонала до нескольких сотен человек оптимальным будет доступ по отпечаткам пальцев. Системы распознавания по геометрии лица весьма специфические. Они могут потребоваться в случаях, когда распознавание требует отсутствия физического контакта, но поставить систему контроля по радужной оболочке невозможно. Например, при необходимости идентификации человека без его участия, скрытой камерой. [3]

На российском рынке, по прогнозам экспертов, доля биометрических систем в ближайшие годы будет составлять значительную часть от общего рынка систем безопасности. Существуют различные прогнозы по развитию биометрического рынка в будущем, однако в целом можно сказать о сохранении тенденции к его дальнейшему росту. В ближайшие годы первое место будет занимать распознавание по отпечаткам пальцев. Идентификация по геометрии лица тоже имеет место на российском рынке, однако предпочтение отдается все-таки дактилоскопическому методу как наиболее изученному. А вот остальные методы биометрии в России производителями пока что практически не представлены. Применение биометрических технологий для контроля доступа в служебные помещения, выхода на летное поле и предотвращения нежелательных действий сотрудников уже реализовано в нескольких аэропортах. В этой сфере рынок предлагает эффективные и надежные биометрические системы. Другая модель использования биометрических технологий в транспортных узлах, которая уже внедряется в некоторых зарубежных аэропортах. [5]

Результаты

Технология биометрической идентификации уже заняла прочные позиции на рынке систем безопасности благодаря ее основному достоинству – производится идентификация физиологических особенностей человека, а не ключа или карточки, которые можно украсть или подделать. За последние два десятилетия биометрические технологии сделали большой шаг вперед. Во многом этому способствовало распространение микропроцессорных технологий. Если в 1980-е годы систему контроля доступа, использующую биометрические характеристики человека, можно было увидеть лишь в фантастических фильмах, то сегодня использование в системах контроля и управления доступом (СКУД) биометрических сканеров стало почти обычным явлением. При этом они практически, не усложняют систему безопасности, и их стоимость для некоторых биометрических методов очень невелика. Более того, около трети ноутбуков выходит сейчас со встроенной системой считывания отпечатка пальцев, а если в ноутбуке есть видеокамера, на него можно установить систему распознавания человека по лицу. Поскольку данные вопросы тесно связаны с методами идентификации, то рассмотрим их применительно к конкретным направлениям. [6]

Распознавания по отпечаткам пальцев занимают более половины биометрического рынка. Множество российских и зарубежных компаний занимаются производством систем управления доступом, основанных на методе дактилоскопической идентификации. По причине того, что это направление является одним из самых давнишних, оно получило наибольшее распространение и является на сегодняшний день самым разработанным. Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. По сути, разработчики достигли уже некоего предела в данной области, и развивать метод дальше некуда. Кроме того, большинство компаний

производят готовые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему самостоятельно, так как это невыгодно и займет больше времени и сил, чем купить готовую и уже недорогую при этом систему, тем более выбор будет действительно широк.

Среди зарубежных компаний, занимающихся системами распознавания по отпечаткам пальцев, можно отметить «Secu Gen» (USB-сканеры для PC, сканеры, которые можно устанавливать на предприятия или встраивать в замки, SDK и ПО для связи системы с компьютером); «Bayometric Inc» (fingerprint scanners, TAA/Access control systems, fingerprint SDKs, embedded fingerprint modules); «Digital Persona, Inc». (USB-scanners, SDK). В России в данной области работают компании «Bio Link» (дактилоскопические сканеры, биометрические устройства управления доступом, ПО); «Сонда» (дактилоскопические сканеры, биометрические устройства управления доступом, SDK); «Смарт Лок» (дактилоскопические сканеры и модули) и др.

Распознавание по геометрии лица причисляют к «трем большим биометрикам» вместе с распознаванием по отпечаткам пальцев и радужной оболочке. Надо сказать, что данный метод довольно распространен, и ему отдают пока предпочтение перед распознаванием по радужке глаза. 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. Как уже упоминалось ранее, существует множество алгоритмов 3D-распознавания. В большинстве своем компании предпочитают развивать готовые системы, включающие сканеры, сервера и ПО. [7]

Однако есть и те, кто предлагает потребителю только SDK. На сегодняшний день можно отметить следующие компании, занимающиеся развитием данной технологии: «Geometrix, Inc» (3D-сканеры лица, ПО), «Genex Technologies» (3D-сканеры лица, ПО) в США, «Cognitec Systems Gmb H» (SDK, специальные вычислители, 2D-камеры) в Германии, «Bioscrypt» (3D-сканеры лица, ПО) — дочернее предприятие американской компании «L-1 Identity Solutions».

В России в данном направлении работает компания «Artec Group» (3D-сканеры лица и ПО) — компания, головной офис которой находится в Калифорнии, а разработки и производство ведутся в Москве. Также несколько российских компаний владеют технологией 2D-распознавания лица — «Vocord», «ITV» и др. [3]

В области распознавания 2D-лица основным предметом разработки является программное обеспечение, так как обычные камеры отлично справляются с захватом изображения лица. Решение задачи распознавания по изображению лица в какой-то степени зашло в тупик — уже на протяжении нескольких лет практически не происходит улучшения статистических показателей алгоритмов. В этой области происходит планомерная «работа над ошибками». [8]

3D-распознавание лица сейчас является куда более привлекательной областью для разработчиков. Хотя этот метод и остается достаточно закрытым, но технические сложности на пути создания 3D-сканера вполне решаемы. Скорее всего, тормозящие факторы развития этой технологии в России — это отсутствие на рынке самостоятельного программного обеспечения распознавания и сложностей, которые могут возникнуть при продвижении продукта на рынок.

На данный момент удельный вес технологий идентификации по радужной оболочке глаза на мировом биометрическом рынке составляет по разным подсчетам от 6 до 9 % (в то время как технологии распознавания по отпечаткам пальцев занимают свыше половины рынка). Следует отметить, что с самого начала развития данного метода его укрепление на рынке замедляла высокая стоимость оборудования и компонентов, необходимых, чтобы собрать систему идентификации. Однако по мере развития цифровых технологий себестоимость отдельной системы стала снижаться. Лидером по разработке ПО в данной области является компания «Iridian Technologies».

Вход на рынок большому количеству производителей был ограничен технической сложностью сканеров и, как следствие, их высокой стоимостью, а также высокой ценой ПО из-за монопольного положения Iridian на рынке. Эти факторы позволяли развиться в области распознавания радужной оболочки только крупным компаниям, скорее всего уже

занимающимся производством некоторых компонентов, пригодных для системы идентификации (оптика высокого разрешения, миниатюрные камеры с инфракрасной подсветкой и т. п.). Примерами таких компаний могут быть LG, «Electronics», «Panasonic», OKI. Они заключили договор с «Iridian Technologies», и в результате совместной работы появились следующие системы идентификации: «Iris Access 2200», BM-ET500, «OKI Iris Pass». В дальнейшем возникли усовершенствованные модели систем, благодаря техническим возможностям данных компаний самостоятельно развиваться в этой области. Следует сказать, что вышеперечисленные компании разработали также собственное ПО, но в итоге в готовой системе отдают предпочтение программному обеспечению «Iridian Technologies». [7]

На российском рынке преобладает продукция зарубежных компаний. Тем не менее, развитие технологий в последние годы позволит производителям провести быструю разработку системы. Так, производитель может использовать в ПО системы стороннюю библиотеку распознавания радужной оболочки. В России это «EyeR SDK». Сканер можно собрать из доступных компонентов: камера, ИК-подсветка, управляемый объектив и различные управляющие элементы. В этом случае общая стоимость системы значительно снизится по отношению к уже готовой. Сложнее, но выгоднее при больших объемах продаж или для получения дополнительных конкурентных преимуществ разработать электронику сканера радужной оболочки. [3]

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 %. Однако к данному методу проявляется все больший интерес. Дело в том, что, являясь довольно точным, этот метод не требует столь дорогого оборудования, как, например, методы распознавания по геометрии лица или радужной оболочке. Сейчас многие компании ведут разработки в данной сфере. Так, например, по заказу английской компании TDSi было разработано ПО для биометрического считывателя вен ладони «PalmVein», представленного компанией «Fujitsu». Сам сканер был разработан компанией «Fujitsu» в первую очередь для борьбы с финансовыми махинациями в Японии. Также в сфере идентификации по рисунку вен работают следующие компании «Veid Pte. Ltd» (scanner, software), «Hitachi Vein ID» (scanners). В России компаний, занимающихся данной технологией, не выявлено. [3]

Что касается сетчатки глаза, на данный момент практически не видно никаких сдвигов в сторону развития данной технологии. Несколько лет назад компания «Eye Dentify» выпустила терминал «Icam-2001». На российском рынке существовало несколько модификаций этого устройства. Также была представлена система Ibex 10 (оптический блок в ней представлял собой передвижную камеру). Стоимость такой системы колебалась в пределах 7–10 тыс. долларов. Безусловно, такая цена не способствовала ее распространению на рынке. Стоимость новой системы — «Icam-2001» — существенно снизилась, однако на российском рынке данные устройства так и не утвердились. Возможно, это связано с некими неудобствами, возникающими при сканировании, а также с чисто психологическими трудностями человека и боязнью перед сканированием сетчатки. Высокая стоимость, технические сложности и неудобство в использовании — все эти факторы значительно замедлили скорость развития метода. [5, 8].

Заключение

В классе средств биометрического распознавания имеется большой выбор систем. Какую из них выбрать? Все зависит от требований к системе безопасности. Самыми статистически надежными и устойчивыми к подделке системами доступа являются системы допуска по радужной оболочке и по сетчатке глаза. Именно на них существует более широкий рынок предложений. Но и это не предел. Системы биометрической идентификации можно комбинировать, достигая астрономических точностей. Самыми дешевыми и простыми в использовании, но обладающими хорошей статистикой, являются системы допуска по отпечаткам пальцев. Допуск по геометрии лица удобен и дешев, но имеет весьма ограниченную область применения из-за плохих статистических показателей [9].

При окончательном выборе конкретного прибора или системы идентификации важно провести анализ следующих характеристик:

- устойчивость к подделке;
- устойчивость к окружающей среде;
- простота использования;
- стоимость;
- скорость срабатывания;
- стабильность биометрического признака во времени.

Как сами методы, так и конкретные образцы аппаратуры распознавания имеют большой потенциал развития. Например, для распознавания по радужной оболочке можно увеличить точность системы практически квадратично, без потерь для времени, если усложнить систему, сделав ее на два глаза. Для дактилоскопического метода — путем комбинирования нескольких пальцев. При распознавании по венам – путем комбинирования двух рук, но такое улучшение возможно только при увеличении времени, затрачиваемого при работе с человеком.

Общепринято, что конкуренцию составляют методы и средства ограничения доступа, в которых используются карточки, ключи, жетоны, пароли и т.д. Однако в данном случае эта конкуренция не является «антагонистической». Наоборот, можно рекомендовать комбинированное использование биометрических систем и традиционных систем безопасности (идентификационные карточки, ключи, видеонаблюдение). Глубокая интеграция таких систем позволит достичь наибольшего эффекта. Что применять — зависит, конечно же, от цены вопроса, от важности хранимой вами информации и от того, чего вы готовы ждать от злоумышленника. Определив это, выбирайте средства защиты, соответствующие задачам.

Примечания:

1. Цыпкин Я.З. Информационная теория идентификации. М.: Наука, 1995.

2. ГОСТ Р 51241-2008 («Средства и системы контроля и управления доступом. Классификация»).

3. Каторин Ю.Ф. Проблемы аутентификации с использованием биометрических характеристик. СПб.: НИУ ИТМО, 2013. Материалы научной конференции по проблемам информатики СПИСОК-2013. С. 688–691.

4. Аманмурадов А.Х., Пиголкин Ю.И., Богомолов Д.В., Золотенкова Г.В., Богомолова И.Н., Федулова М.В. Алгоритмы судебно-медицинской идентификации личности // Альманах судебной медицины, Том 4, N 2 (2001), 2003.

5. Fisher R.A. On an Absolute Criterion for Fitting Frequency Curves. — Statistical Science, vol.12, No. 1 (Feb., 1997). pp. 39-41.

6. Дилигенская А.Н. Идентификация объектов управления. Самара. Самарский государственный технический университет, 2009. 136 с.

7. Егупов Н.Д., Пупков К.А. Методы классической и современной теории автоматического управления. В 5 томах. Том 2. Статистическая динамика и идентификация систем автоматического управления. М.: МГТУ им. Н.Э. Баумана. 2004.

8. Каторин Ю.Ф. Коротков В.В., Нырков А.П. Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы. СПб.: // Журнал университета водных коммуникаций. 2012. №1 (13), С. 98-102.

9. Каторин Ю.Ф., Нырков А.П., Соколов С.С., Ежгуров В.Н. Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. СПб.: // Проблемы информационной безопасности. Компьютерные системы. 2013. № 2. С. 54-58.

References:

1. Tsypkin Ya.Z. Informatsionnaya teoriya identifikatsii. M.: Nauka, 1995.

2. GOST R 51241-2008 («Sredstva i sistemy kontrolya i upravleniya dostupom. Klassifikatsiya»).

3. Katorin Yu.F. Problemy autentifikatsii s ispol'zovaniem biometricheskikh kharakteristik. SPb.: NIU ITMO, 2013. Materialy nauchnoi konferentsii po problemam informatiki SPISOK-2013. S. 688–691.

4. Amanmuradov A.Kh., Pigolkin Yu.I., Bogomolov D.V., Zolotenkova G.V., Bogomolova I.N., Fedulova M.V. Algoritmy sudebno-meditsinskoi identifikatsii lichnosti // Al'manakh sudebnoi meditsiny, Tom 4, N 2 (2001), 2003.

5. Fisher R.A. On an Absolute Criterion for Fitting Frequency Curves. — Statistical Science, vol.12, No. 1 (Feb., 1997). pp. 39-41.

6. Diligenskaya A.N. Identifikatsiya ob"ektov upravleniya. Samara. Samarskii gosudarstvennyi tekhnicheskii universitet, 2009. 136 s.

7. Egupov N.D., Pupkov K.A. Metody klassicheskoi i sovremennoi teorii avtomaticheskogo upravleniya. V 5 tomakh. Tom 2. Statisticheskaya dinamika i identifikatsiya sistem avtomaticheskogo upravleniya. M.: MGTU im. N.E. Baumana. 2004.

8. Katorin Yu.F. Korotkov V.V., Nyrkov A.P. Zashchishchennost' informatsii v kanalakh peredachi dannykh v beregovykh setyakh avtomatizirovannoi identifikatsionnoi sistemy. SPb.: // Zhurnal universiteta vodnykh kommunikatsii. 2012. №1 (13), S. 98-102.

9. Katorin Yu.F., Nyrkov A.P., Sokolov S.S., Ezhgurov V.N. Osnovnye printsipy postroeniya zashchishchennykh informatsionnykh sistem avtomatizirovannogo upravleniya transportno-logicheskim kompleksom. SPb.: // Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy. 2013. № 2. S. 54-58.

УДК 004.5

Методы и средства биометрической идентификации личности

Юрий Федорович Каторин

Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
Доктор военных наук, профессор
E-mail: katorin@mail.ru

Аннотация. В статье описаны основные методы биометрической идентификации. Построенная на их основе система ограничения доступа может контролировать доступ к информации и хранилищам в банках, ее можно использовать на предприятиях, занятых обработкой ценной информации, для защиты средств связи и т.д. Также описаны преимущества и недостатки каждого метода.

Ключевые слова: безопасность, контроль доступа, надежность идентификации, биометрические характеристики, сканеры.