

Биометрическая технология васкулярной идентификации личности

77-48211/574720

05, май 2013

Глинская Е. В.

УДК 004.056

Россия, МГТУ им. Н.Э. Баумана

glinskaya@bmstu.ru

В настоящее время во всем мире, в различных областях, от масштабов среднего дома и противоугонных систем транспортных средств, до уровня антитеррористических служб, высоко востребованы системы безопасности с низким уровнем риска.

Независимо от того, какая система защиты используется, чаще всего первым шагом работы является идентификация и подтверждение личности (аутентификация).

В прежнее время единственным способом установления личности людей, перемещающихся из одной страны в другую, посетителей частных владений или снимающих наличные деньги в банках являлась осуществляемая человеком тщательная проверка документов. Рост масштабов трансграничных поездок, необходимость обеспечения безопасности на рабочих местах и распространение электронного банковского обслуживания наряду со многими другими изменениями в повседневной жизни сделали этот метод практически неприменимым.

Начало использования паролей для подтверждения личности стало большим шагом в деле защиты информации от несанкционированного доступа. Традиционным подходом для проверки подлинности является необходимость введения имени пользователя и пароля при регистрации в компьютерной системе. Идея введения паролей состоит в создании пользователем случайной последовательности символов. К сожалению, пользователи для упрощения запоминания в качестве пароля берут собственные имена, номера телефонов, даты рождения и т.п., поэтому путем подбора пароля возможна несанкционированная аутентификация.

Подмена личности и мошенничество представляют большие проблемы в деловом мире. Раньше не наблюдалось такой зависимости от паролей, PIN-кодов и идентификационных карт, слишком много сейчас требуется, чтобы уверенно

идентифицировать людей, удостоверить, кем они являются. Все эти средства идентификации имеют большой недостаток - возможность потери или кражи.

В настоящее время существует новый способ проверки личности, основанный на использовании автоматизированных методов и информационно-коммуникационных технологий (ИКТ) для опознания людей по их физическим или поведенческим признакам, широко известный как биометрия. Биометрия применяется для изготовления электронных паспортов, а также для идентификации по кровеносным сосудам пальца в банкоматах и даже для предотвращения продажи сигарет детям торговыми автоматами. В каждом случае измеряется определенный набор индивидуальных характеристик и выполняется автоматическое сравнение результатов с шаблонами, хранящимися на жетонах или в базе данных, для поиска совпадения. Измеряемые характеристики, как правило, являются физическими, но это также могут быть поведенческие характеристики, такие как клавиатурный почерк при наборе слова или фразы.

С повсеместным применением биометрии для установления личности, особенно в открытой сетевой среде, усложняются и приобретают неотложный характер задачи обеспечения конфиденциальности, надежности и безопасности биометрических данных. Любой человек, которому пришлось стоять в очереди на регистрацию в аэропорту, оценит важность скорости и точности считывания электронного паспорта. Аналогично, снимая деньги в банкомате, человек рассчитывает, что никто другой не сможет получить доступ к его счету.

Современные биометрические системы биологического распознавания являются надежными и качественными средствами идентификации и аутентификации личности.

В настоящее время широко используется большое количество методов биометрической аутентификации, которые делятся на два класса.

- Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, присутствующих от рождения и до смерти, находящиеся при нём в течение всей его жизни, и которые не могут быть потеряны, украдены и скопированы.
- Динамические методы биометрической аутентификации основываются на поведенческих характеристиках людей, то есть основаны на характерных для подсознательных движений в процессе воспроизведения или повторения какого-либо обыденного действия

Самой распространенной биометрической технологией аутентификации пользователей является идентификация по отпечаткам пальцев. Технология распознавания личности по радужной оболочке глаза и по сетчатке глаза более сложная и

дорогая, а стоимость всегда была самым большим сдерживающим моментом перед внедрением технологии, но сейчас системы идентификации по радужной оболочке становятся более доступными для различных компаний. Существуют биометрические методы для аутентификации личности использующие форму кисти руки или геометрию лица.

Биометрические системы доступа основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает. Потерять их нельзя. Также невозможна передача идентификатора третьим лицам. Впрочем, можно насильственно изъять параметры. В кинофильмах и анимации было неоднократно показано, что глаза и руки можно ампутировать. Этого недостатка нет у васкулярной аутентификации, которая позволяет идентифицировать только живого человека.

Васкулярный (медицинский термин, лат. Vascularis; лат. Vasculum уменьшительное от vas – сосуд) – сосудистый; относящийся к сосудам.

Васкулярная аутентификация, которая использует распознавание изображений и оптическую технологию для сканирования обычно невидимых структур вен ладони (рис. 1), тыльной стороны ладони, пальцев и т.д., обладает свойствами высокой степени точности и высокой устойчивостью к подделке, подмене и другим нечестным действиям.



Рис. 1. Генерирование изображения ладони человека в около-инфракрасном диапазоне и преобразование данных для хранения в зашифрованном виде.

Из доступных актуальных биометрических решений, аутентификацию по венам ладони предполагает лучшую точность и безопасность. Узоры кровеносных сосудов являются уникальными для каждого человека и, в отличие от отпечатков пальцев или

радужной оболочки, они не изменяются с течением времени, так что, не обязательно проводить перерегистрацию через определенные промежутки времени.

Самое главное, эти сосудистые узоры существуют внутри тела, а не снаружи. Они не могут быть украдены с помощью фотографии, подделки или других подобных методов, что делает этот метод биометрической аутентификации намного более безопасным, чем другие.

Когда ладонь освещается светом, близким к инфракрасному, обезкислороженный гемоглобин внутри вен поглощает этот свет, проявляя вены как темный рисунок поверх остального изображения. Таким образом, область ладони, используемая для аутентификации, фотографируется в близком к инфракрасному свете, и образец узора вен извлекается путем обработки изображения и распознавания. Чтобы авторизовать пользователя, их уникальные образцы узоров вен сверяются с ранее зарегистрированными образцами, хранимыми в базе данных, на смарт-карте, либо в зашифрованном виде на других носителях информации.

Компания Fujitsu разработала первый в мире способ бесконтактной васкулярой аутентификации ладони (рис. 2), который является методом чтения узора вен ладони. Технология Fujitsu PalmSecure обнаруживает образы рисунка вен только живых людей. Процесс сканирования быстр и не требует какого-либо контакта между датчиком и проверяемым человеком. Технология PalmSecure отвечает высоким требованиям гигиены многопользовательской среды общественных мест. Устройство PalmSecure представляет собой биометрический сенсор, который может быть использован совместно с широким спектром действующих приложений. Сенсор излучает близкий к ИК-луч в направлении ладони, подносимой к устройству. В этом свете, уникальные параметры ладони – кровь, текущая в венах ладони, проявляются в виде рисунка, как сложный индивидуальный узор. Специальная оптическая система, интегрированная в сенсор генерирует изображение узора вен ладони. Таким образом, созданное изображение обрабатывается, оцифровывается, шифруется AES и хранится в виде зарегистрированного шаблона. Впоследствии, система контроля доступа сравнивает фактически отсканированный образец с ранее зарегистрированным шаблоном безопасности из архива или с внешнего носителя информации. Совершенные алгоритмы обеспечивают высокий уровень точности.



Рис.2. Бесконтактное распознавание узора вен ладони с помощью сенсора PalmSecure.

Также компания представила первую разработку, созданную по новой технологии – это компьютерная мышь, оснащенная специальными датчиками. Будучи присоединена к компьютеру, мышь определяет, является ли человек его “владельцем” или же это кто-то посторонний, и в зависимости от этого разрешает или запрещает доступ к данным.

В ходе проведенного эксперимента, в котором приняли участие более 700 человек, была подтверждена ничтожно малая вероятность ошибки – она составила не более 0.5%.

Основные преимущества васкулярной идентификации личности:

- Уникальность – узоры вен являются уникальными для отдельных лиц и не изменяются с течением времени
- Точность – передовые алгоритмы выявления соответствия обеспечивают высокий уровень точности
- Гигиеничность – бесконтактный пользовательский интерфейс снимает проблему загрязнения
- Универсальность – технология может быть использована практически всеми
- Простота – интерфейс пользователя способствует максимальной простоте восприятия.

В настоящее время существуют три основные категории применения биометрии: криминологическая, государственная и коммерческая.

В криминологии и судебной медицине широко применяют методы биометрической аутентификации, в частности идентификацию по отпечаткам пальцев и образцам ДНК, что играет значительную роль в уголовных делах. Несмотря на то, что ДНК считается оптимальной биометрической характеристикой для идентификации личности (за

исключением однояйцевых близнецов), сравнение ДНК является слишком инвазивным методом для широкого применения при аутентификации личности.

На важных государственных объектах меры безопасности постоянно модернизируются и укрепляются. Проверка личности на входе и выходе стала играть более важную роль, чем просто мониторинг посещаемости. В целях предотвращения входа неавторизованных либо опасных людей в служебные помещения в настоящее время ведется переход к внедрению систем пропусков на основе биометрической идентификации с помощью смарт-карт, на которых записан шаблон собственных вен сотрудника. Или же шаблон вен всех сотрудников может записываться, храниться и обрабатываться с помощью внутренней системы компании, на сервере.

Исследования показали, что требуется объединение двух и более систем аутентификации, таких как сканирование отпечатков пальцев и радужной оболочки глаза, сканирование вен и распознавание голоса. Правительственные объекты, в целях улучшения процедур работы с различной секретной информацией возлагают большие надежды на системы доступа на основе биометрии. Васкулярная аутентификация является эффективным средством в управлении доступом к секретной информации, допуская к данным только персонал, имеющий зарегистрированный в системе венозный рисунок.

В Европе, Японии (после атаки газом зарин в метро) и Северной Америке (со времен авиа терактов) такие системы уже внедряются в офисах компаний, занимающихся ценными бумагами, технопарках и т.д.

В некоторых развивающихся странах уже начато использование биометрики для регистрации избирателей в ходе подготовки к выборам в целях исключения устаревших списков избирателей и фальсификации результатов голосования.

В Индии, где миллионы сельских жителей не умеют читать и писать, успешно ведется национальный проект по организации социальных выплат малоимущим слоям населения с использованием отпечатков пальцев.

Аутентификация может потребоваться для будущих услуг электронной коммерции, электронного здравоохранения и электронного правительства в работе с биометрическими личными документами, выдаваемыми государственными органами.

В офисные системы внедряется управление входом в системы для персональных компьютеров и приложений, использующих васкулярную проверку подлинности ладони. Эта система позволяет сотрудникам входить в систему, просто поместив ладони над сенсором, избегая применения логина и пароля. Она делает ненужным для сотрудников запоминание множества идентификаторов и паролей для повышения безопасности в офисах, исключая несанкционированный вход в учетную запись.

Финансовые институты также уже начали использовать систему васкулярной аутентификации. Приложение для систем автоматизированной банковской деятельности было реализовано двумя способами: за счет внедрения банкоматов, оснащенных функцией проверки личности, которые используют бесконтактную васкулярную аутентификацию, и в качестве новой услуги отдельной учетной записи для клиентов, которые того пожелают.

В последнем случае, когда клиент открывающий новый счет, работник банка, используя специализированное устройство, регистрирует образец рисунка вен человека. Затем метод васкулярной идентификации с использованием этого образца может быть применен для замены процедур аутентификации по подписи, личной печати, предъявлению документов и денежных карт, в том числе и при снятии наличных.

Это устраняет хлопоты с обработкой подписей, документов и других объектов, и является эффективным методом для предотвращения преступлений происходящих из-за потерь и краж.

В 2011 году Глава правительства РФ Владимир Путин и глава Сбербанка Герман Греф на открытии современного Центра обработки данных Сбербанка «Южный порт» для входа в систему использовали биометрическую технологию PalmSecure васкулярной идентификации личности.

Японский банк Ogaki Kyoritsu запустил в эксплуатацию банкоматы, которые позволяют снимать наличные и управлять средствами с помощью руки владельца счета. Идентификация владельца счета производится по руке с введением пин-кода и даты рождения. Никаких пластиковых карточек банкомату нового типа не требуются.

Помимо удобства для клиентов, Ogaki Kyoritsu решил учесть опыт стихийного бедствия 11 марта 2011 года, когда цунами унесло тысячи жилых домов вместе с наличными деньгами, банковскими документами и карточками. Многие из тех, кому удалось спастись, остались не только без денег, но и без документов, подтверждающих их личность.

В Ogaki Kyoritsu решили, что способ идентификации по рисунку кровеносных сосудов кисти руки без непосредственного касания сканера является гораздо более защищенным, чем, например, объемные сенсоры для пальцев, поскольку "карту вен" подделать невозможно, так как они находятся не на поверхности ладони, а по всему объему кисти.

Пока что сканер капилляров всего лишь дополняет (или даже заменяет) PIN-код карты, но в будущем возможна замена всей карты целиком, то есть оплачивать товар можно будет, предъявив машине руку. Это будет полноценная биометрическая платежная система, существенно повышающая уровень абстракции в понимании денег.

Такая система, разумеется, будет гораздо сложнее, чем нынешняя реализация, ведь вместо простой верификации личности нужно будет осуществить полноценное распознавание личности. В Fujitsu говорят, что недавно провели эксперимент, показавший: система корректно распознает человека по ладони в среднем за 1,34 секунды. А до того, как собственной ладонью можно будет расплатиться в любом магазине, новый способ, по мнению японских экспертов, найдет свое применение в торговых автоматах, очень популярных в Стране Восходящего Солнца.

Альтернативная система сканирования рисунка кровеносных сосудов руки разрабатывается и другими японскими компаниями – Hitachi и Sony.

В системе сканирования компании Sony реализована технология Mofiria, использующая CMOS-сенсор, считывающий рассеянный свет через палец (рис. 3).

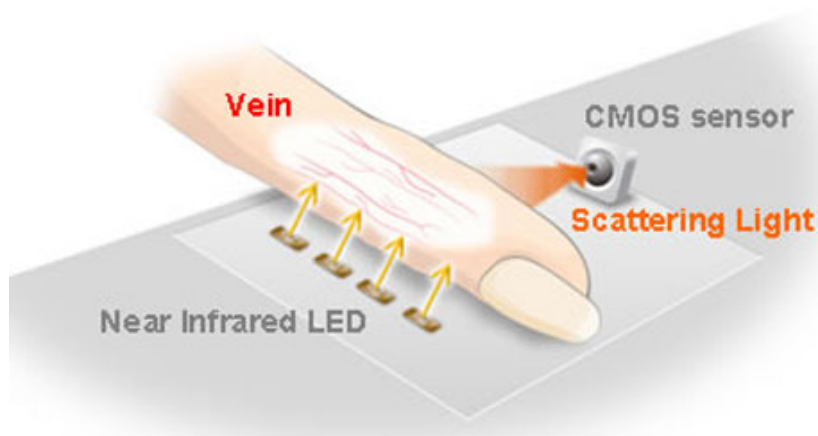


Рис. 3. Комплексный CMOS-сенсор, считывающий рассеянный свет через палец (Vein – вена; Near infrared LED - инфракрасный светодиод; Scattering Light - рассеянный свет; CMOS sensor - CMOS сенсор)

Источником света в длинноволновой инфракрасной области спектра являются специальные светодиоды. Такой комплексный сенсор может быть довольно мал и приспособлен для размещения в ноутбуках и мобильных устройствах. Уровень ошибочных распознаваний пользователя очень мал – 0,0001%, а скорость процесса идентификации – 0,015сек на ПК и 0,25сек на мобильном телефоне.

В настоящее время для будущего применения рассматриваются такие биометрические характеристики, как пульсовое давление крови, запах тела, композиционный состав кожи, схема ногтевого ложа, походка, форма ушей. Для того

чтобы понять, подходят ли какие-либо из них для применения в биометрике, необходимы дальнейшие исследования.

Какая бы система ни использовалась, она должна быть защищенной, гарантировать конфиденциальность и обеспечивать точные результаты. Незащищенная, ненадежная и инвазивная система лишится доверия общества и может стать причиной общего неприятия методов биометрического опознавания.

Биометрические системы уязвимы для атак. Целью может стать любой элемент биометрической системы: датчик, устройство выделения признаков, устройство сопоставления, хранимые биометрические шаблоны или конечная точка принятия решения. Кроме того, атака может осуществляться в обход биометрического датчика или путем взлома устройства выделения признаков или шаблона.

Биометрия опирается на конфиденциальную информацию, однако безопасность системы аутентификации не может зависеть от секретности биометрических данных. Для достижения операционной эффективности система должна обеспечивать целостность и подлинность биометрических данных, и необходимы дополнительные меры безопасности для защиты личных данных.

Обработка биометрических персональных данных регулируется Федеральным Законом от 27.07.2006 N 152-ФЗ (ред. от 23.12.2010) "О персональных данных".

В целях обеспечения безопасной аутентификации в Рекомендациях МСЭ—Т X.1084 и X.1085 определены девять протоколов аутентификации для телебиометрики и описаны профили защиты, а в Рекомендации МСЭ—Т X.1086 представлены руководящие принципы в отношении мер противодействия для создания безопасной среды и сохранения секретности. В Рекомендации МСЭ—Т X.1087 установлены процедуры защиты мультимодальных биометрических данных от атак, предпринимаемых в целях перехвата, изменения или замены данных. Эти процедуры включают шифрование, добавление водяных знаков и преобразование данных. Два следующих стандарта — Рекомендации МСЭ—Т X.1088 и X.1089 — обеспечивают соответственно основу для генерации и защиты биометрических цифровых ключей и способ осуществления биометрической аутентификации.

Разработка международных стандартов — это ключевая стратегия обеспечения правильного выбора и надлежащего использования биометрических методов. Менее чем за десять лет был достигнут значительный прогресс в развитии биометрических датчиков, алгоритмов и процедур, однако все еще сохраняются уязвимости, которые необходимо устранить. По-прежнему принципиальными факторами являются обеспечение неприкосновенности частной жизни и защита конфиденциальных биометрических данных.

Ожидается, что рост финансирования биометрики в основном будет обусловлен коммерческими и государственными приложениями, где отрасли, связанные с биометрическими системами и производством чипов для смарт-карт, будут получать выгоду в связи с правительственными решениями о введении электронных личных документов и биометрических систем. Исходя из того, что в 2008 году на развитие биометрических технологий было израсходовано 3 млрд. долл. США, аналитики рынка в настоящее время прогнозируют увеличение объема инвестиций до 7,3 млрд. долл. США к 2013 году.

В России на основе имеющихся разработок компании Fujitsu по технологии PalmSecure разрабатывается специальная компьютерная плата, для ограничения физического доступа к рабочим станциям. При этом сенсор, подключаемый к USB шине самой станции, может использоваться для последующей авторизации входа в операционную систему.

В сотрудничестве с ведущим поставщиком решений криптозащиты, создаются средства, позволяющие авторизовать использование электронной подписи биометрическими данными.

На основе решений от партнеров компании Fujitsu создаются демонстрационные системы по физическому доступу в помещения.

Внедряются пожаростойкие и пуле-взрывостойкие решения для васкулярной идентификации личности с применением технологии PalmSecure.

Список литературы

1. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Уч. пособие. М.: Гелиос АРВ, 2006, 528 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в современных компьютерных системах. – 2-е издание: М.: Радио и связь, 2001, 376 с.
3. Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. № 2, 2002.
4. Биометрия и стандарты. Наблюдение за развитием технологий. № 1. 2010.
5. Евангели А. Технологии биоидентификации и биометрический рынок. // PC Week /RE. – 2003 - № 7 – с. 24-25.
6. <http://sites.google.com/site/palmsecurerussia/> Технология PalmSecure.
7. <http://www.MCЭ.int/MCЭ-T/techwatch> Отчеты Сектора стандартизации электросвязи МСЭ.