Датчики-сканеры отпечатков пальцев в устройствах биоидентификации. Обзор и перспективы

Андрей Ласорла

В современном «турбулентно меняющемся» мире системы аутентификации и безопасности сталкиваются с новыми вызовами. Повсеместно растут требования по совершенствованию устройств идентификации личности. В связи с этим биометрические технологии стремительно развиваются. Среди них особое место занимают устройства сканирования и преобразования в цифровой вид отпечатков пальцев (далее – сканеры).

За 20 лет от оптической FTIR и ёмкостной, и позже технологии FingerChip (тепловые датчики), эволюция сканеров достигла апогея в наши дни, когда сканеры вмонтированы в СКУД и электронные замки разного назначения, а сканирование может осуществляться бесконтактным, в том числе ультразвуковым методом. На бытовом уровне с помощью программно-реализованных сканеров идентифицируют доступ к функционалу компьютеров и смартфонов, КПК (функционал – контроль доступа, защита персональных данных и модели электронного бизнеса), к электронному оборудованию бытового назначения с программируемым доступом и индивидуальными настройками – телевизоры, банкоматы и POS (в том числе для замены PIN), доступ в дома, помещения, автомобили и др.

Биометрия отпечатков пальцев эффективна ввиду её уникальности и постоянства образцов. Есть небольшой (до 3%) процент пользователей, которые не могут воспользоваться биометрической аутентификацией и быть идентифицированы по дактилоскопическому принципу оттого, что у них не читается отпечаток пальца. Для этих случаев, а также в сочетании со сканированием отпечатков, предусмотрена комплексная аутентификация с помощью видеоконтроля, распознавания лица, сетчатки глаз, рисунка вен ладони, голосовых и других спектро-анализаторов. Аутентификация активно используется не только в быту (частных), коммерческих (СКУД и электронные замки), но и государственных структурах – для контроля доступа к информации, через персонализацию пользователя, контроля перемещения лиц, к примеру, пограничный и таможенный контроль, и во многих других случаях. Комплексная аутентификация с помощью биометрического сканирования и «ручного» введения PIN много лет применяется в банковской сфере, на удалённых терминалах-банкоматах, везде, где ошибки аутентификации слишком дорого обходятся, а потому должны быть минимизированы.

Ошибки идентификации условно можно разделить на две категории. Первая из них – FAR (False Access Rate) – когда человека нет в базе, но электронная система-анализатор определяет и относит отсканированный код к человеку, присутствующему в базе. И вторая – FRR (False Reject Rate) – ошибки другого рода, когда в электронном виде данные человека имеются в базе, но он не определён по техническим причинам, в частности, из-за неудовлетворительного качества (загрязнения) оборудования. Отказы системы доступа и идентификации зависят от некачественной работы сканера. При этом задачи идентификации и задачи верификации, стоящие перед системой, – разные. По-разному устанавливаются пороги чувствительности оборудования, по-разному организована оптимизация и поиск ключевых точек при биометрическом сканировании. Отсюда очевидно, что комплексная аутентификация решает эти задачи лучше, поэтому она и используется в ответственных случаях, а не только биометрическая. И, в частности, не только сканирование по дактилоскопическому принципу.

Сканирование отпечатков – отдельный тип биометрии, характеризующийся тем, что данные конкретного пользователя считываются сканером, папиллярный индивидуальный рисунок с помощью электронного оборудования преобразуется в электрический ток, с помощью встроенного АЦП «картинка» уже в цифровом виде поступает на сервер (совмещённый или удалённый), где анализируется – сопоставляется с цифровым видом «картинки»-эталона (сравниваются два отпечатка пальца), имеющейся в базе данных. При совпадении данных ординара и считанного отпечатка вырабатывается команда на разрешение доступа конкретной персоналии. И (или) в зависимости от задач – данные о персоналии с добавлением в реальном времени момента и места сканирования фиксируются и далее хранятся в памяти удалённого сервера. По определению дактилоскопического принципа идентификации ошибки сравнения двух последовательностей цифровых кодов минимальны. Так работает система электронного сканирования и сравнения отпечатков, важным элементом которой является терминал-считыватель непосредственно с датчиком. Для стабильности и надёжности всей системы к датчику предъявляются определённые требования. Для контактных датчиков устойчивость к «истиранию» определяет долговременность эксплуатации: современные датчики имеют ресурс более 1 000 000 сканирований. Это обеспечивается нанесением специального защитного слоя на рабочую поверхность датчика. Принцип работы сканера отпечатков представлен на рис. 1.

Для иллюстрации к популярным портативным считывателям на рис. 2 представлен внешний вид сканера отпечатков пальцев по технологии FingerChip Digital Persona. Датчик выглядит как чип-на-плате (COB) с 20-pin разъёмом.

Технические характеристики рассматриваемого датчика AT77C101B Atmel

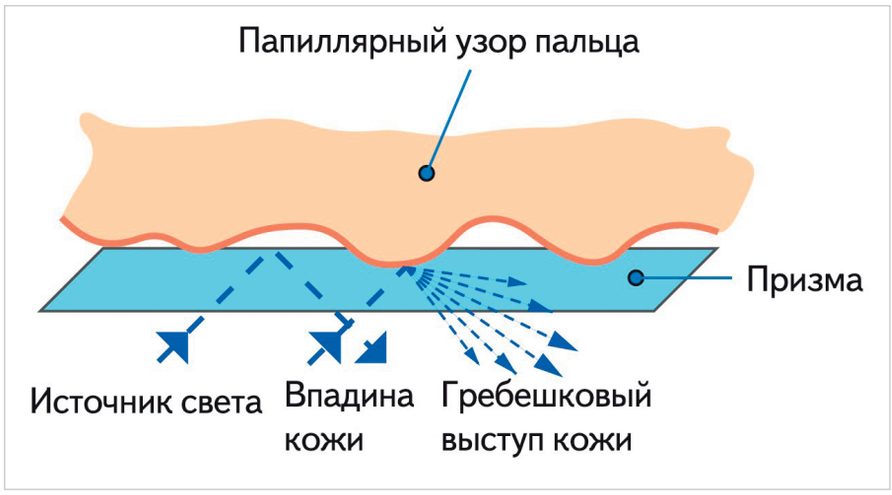


Рис. 1. Общий принцип работы сканера отпечатков

Рис. 2. Сканер отпечатков по технологии FingerChip

Таблица 1. Технические характеристики датчиков отпечатков пальцев ATMEL и FUJITSU

Тип	Разрешение	Кол-во пикселей	Размер области считывания, мм	Рабочая Т, °С	Напряжение питания, В	Потребляемая мощность/ток	Размер корпуса, мм
AT77C101B	500 dpi	280×8	14×0,4	0...+70	3–5,5	20 мВт при U = 3,3 В, раб. частоте 1 МГц и Т = 25°С	COB6, COB с разъёмом, CDIP-20 26,6×9 (COB)
MBF110	500 dpi	300×300	15×15	0...+60	3,3–5	170 мВт при 40 МГц	LQFP-80, VSPA-80 24×24
MBF200	500 dpi	256×300	12,8×15	–20...+85	3,3–5	20 мА	LQFP-80 24×24×1,4
MBF300	500 dpi	256×32	12,8×0,2	0...+60	2,8–5	20 мА	FBGA-54, FLGA-54 14×4,3×1,2
MBF310	500 dpi	218×8	12,8×0,2	–20...+85	2,7–3,6	12 мА	FBGA-42 16,1×6,5×1,2

представлены на сайте производителя, а также в табл. 1. Дополнительные особенности датчика: чувствительный слой поверх КМОП-матрицы 0,8 мкм, массив изображений 8×280 = 2240 пикселей, защита от электростатического разряда > 15 кВ.

Среди подключаемых с помощью кабеля компактных и портативных считывателей (они похожи по форм-фактору и функционалу, отличаясь только моделями и качеством датчика, следовательно, и разрешением сканируемого изображения), модель, приведённая на рис. 1, является востребованной для разработчиков РЭА и часто применяется в современных системах контроля. На рис. 3 представлен внешний вид датчика AT77C101B.

В табл. 1 представлены некоторые технические характеристики датчиков отпечатков пальцев ATMEL и FUJITSU. На рис. 4 представлена распиновка разъёма для датчика AT77C101B-CB02V (Atmel).

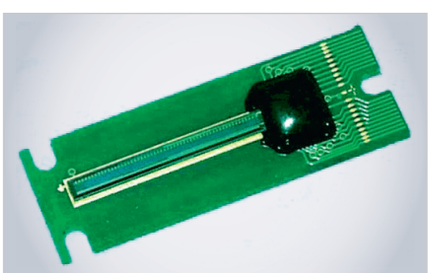


Рис. 3. Внешний вид датчика AT77C101B-CB02V (Atmel)

Считыватели по технологии FingerChip надёжно защищены от электростатических разрядов с напряжением до 16 кВ. На плате датчика AT77C101B-CB02V реализован встроенный тактовый генератор с функцией сброса, предусмотрен экономичный «спящий» режим, когда температурная стабилизация отключается, а выходы управляющих сигналов (выходные линии) переведены в состояние высокого импеданса. В спящем режиме ток потребления ограничивается лишь током утечки. При сканирова-

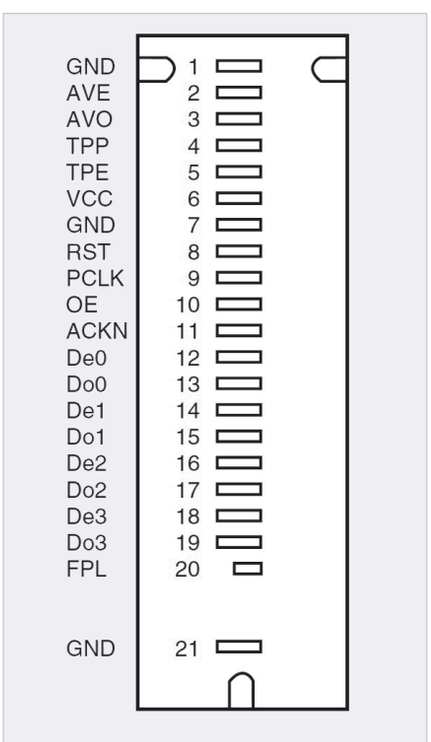


Рис. 4. Распиновка разъёма для датчика AT77C101B-CB02V (Atmel)

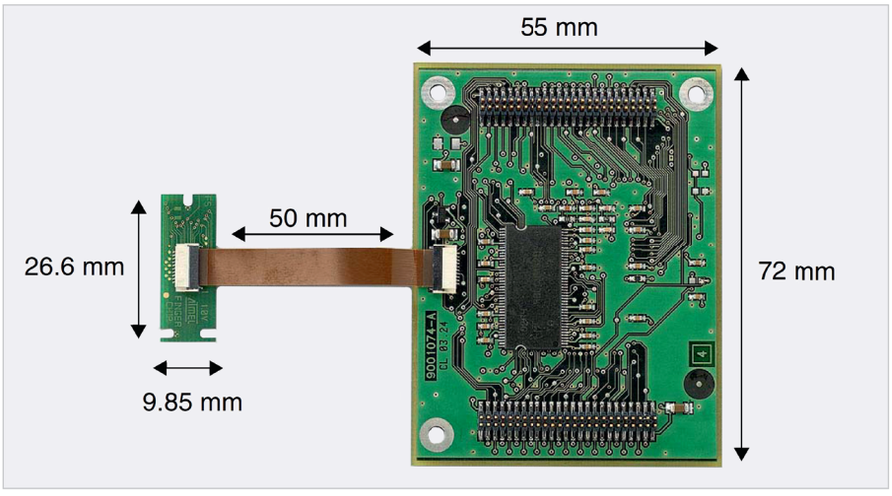


Рис. 5. Внешний вид биометрического модуля AT77SM0101BCB02VKE Atmel

нии, когда разница температур между пальцем и датчиком становится незначительной (менее одного градуса), включается температурная стабилизация. Интеграция температурного метода получения изображения, покадрового восстановления изображения, интеграция схем считывания и преобразования изображения на одной КМОП-подложке снижает стоимость устройства, энергопотребление и увеличивает скорость формирования данных и их передачи на сервер. Ещё лучшие характеристики имеет биометрический сенсор-сканер AT77SM0101BCB02VKE (рис. 5), построенный на базе 32-разрядного микроконтроллера Atmel AT91RM9200.

Биометрический модуль AT77SM0101BCB02VKE также основан на датчике отпечатков пальцев FingerChip от Atmel, который подключается к плате на основе микропроцессора AT91RM9200 на базе ARM9.

С модулем биометрии AT77SM0101BCB02VKE сочетается базовая плата с блоком питания и разъёмами (Ethernet, USB, RS-232, внешней Flash-памяти CompactFlash, SmartMedia, NAND Flash, смарт-карты ISO7816), коммутационный кабель, ПО для Windows и SDK для Linux. Подключение к материнской плате осуществляется через два стандартных разъёма, расположенных по бокам платы модуля. Модуль загружен операционной системой Linux, драйвером Atmel для датчика FingerChip и, по умолчанию, ПО аутентификации (биометрической библиотекой) для извлечения характеристик отпечатков пальцев и сравнения с зарегистрированными шаблонами (bio-engine). AT77SM0101BCB02VKE обеспечивает регистрацию формирования в цифровой вид и регистрацию отпечатка со следующими характеристиками.

- Подключение: через USB-порт 2.0, 3.0 (Full Speed)
- Разрешение: 700 dpi (average x,y over the field)
- Условия сканирования: 8-bit grayscale
- Размер окна сканирования: 14,6 мм (nom. width at center), 18,1 мм (nom. length)
- Уверенная работа в диапазоне температур: 0…+40°C

На основе сенсор-сканера AT77SM0101BCB02VKE реализован водонепроницаемый дверной замок, в 23-м году XXI века устройство распространено в быту и на производстве. Иллюстрация замка LPSECURITY представлена на рис. 6.

Устройство управляет ЭМ-замком с помощью одного слаботочного ЭМ-реле (NO, NC, Common) и обеспечивает контроль доступа по отпечаткам пальцев со следующими особенностями. Металлический водонепроницаемый корпус соответствует классу защиты IP66 и поддерживает до 100 отпечатков и 3000 карт (125 кГц EM-card) на расстоянии считывания 2 см. Имеет режим защёлки, чтобы держать дверь или ворота открытыми, трёхцветный светодиодный индикатор состояния и следующие технические характеристики.

- Рабочее напряжение DC: 9…18 В
- Ток ожидания/действия: ≤ 25 / ≤ 100 мА
- Регулируемое время выхода реле: 0…99 с (по умолчанию 5 с)
- Блокировка выходной нагрузки: макс. ток 2 А
- Рабочая температура: –25…60°C
- Рабочая влажность: 20…98% RH
- Размеры: 115×40×30 мм

Рис. 6. Внешний вид водонепроницаемого дверного замка LPSECURITY с сенсор-сканером AT77SM0101BCB02VKE

Микроэлектромеханический и трёхмерный метод

Микроэлектромеханический метод (MEMS) по состоянию в промежуточной стадии между научно-исследовательскими разработками и внедрением. Для определения выступов и впадин отпечатка пальца разработана матрица микромеханических датчиков, идёт работа над повышением стабильности считывания. Сканировать подушечки пальцев в трёх измерениях можно с помощью ультразвука. На рис. 7 представлена схема, иллюстрирующая такое сканирование.

Принцип работы датчика сродни функционалу медицинских УЗИ-систем. Трёхмерный отпечаток пальца содержит информацию о микровпадинах и выступах, а также о неглубоком подкожном слое. Сия технология признана более надёжной в сравнении с другими сканерами отпечатков – с двухмерным сканированием. Практический пример: после купания в бассейне, а иногда при длительном нахождении руки в любой водной среде встроенный двухмерный сканер iPhone 5s не распознаёт отпечатки — кожа на пальцах сморщивается. Трёхмерному датчику такое изменение папиллярного рисунка не помеха.

Датчик с рабочим напряжением всего 1,8 В (что позволяет использовать в качестве источника питания даже ионистор) основан на технологии мас-

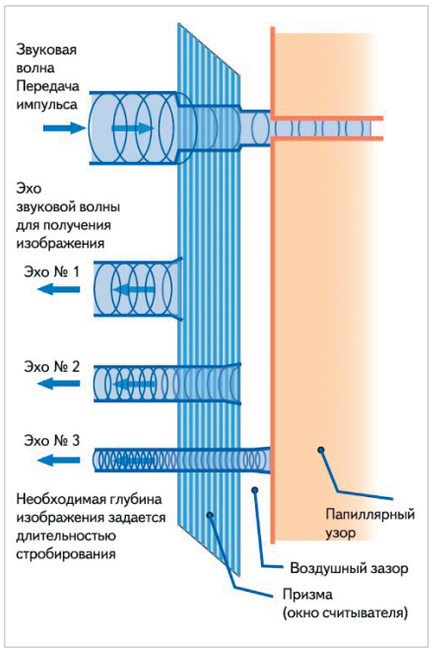


Рис. 7. Схема сканирования ультразвуковым методом

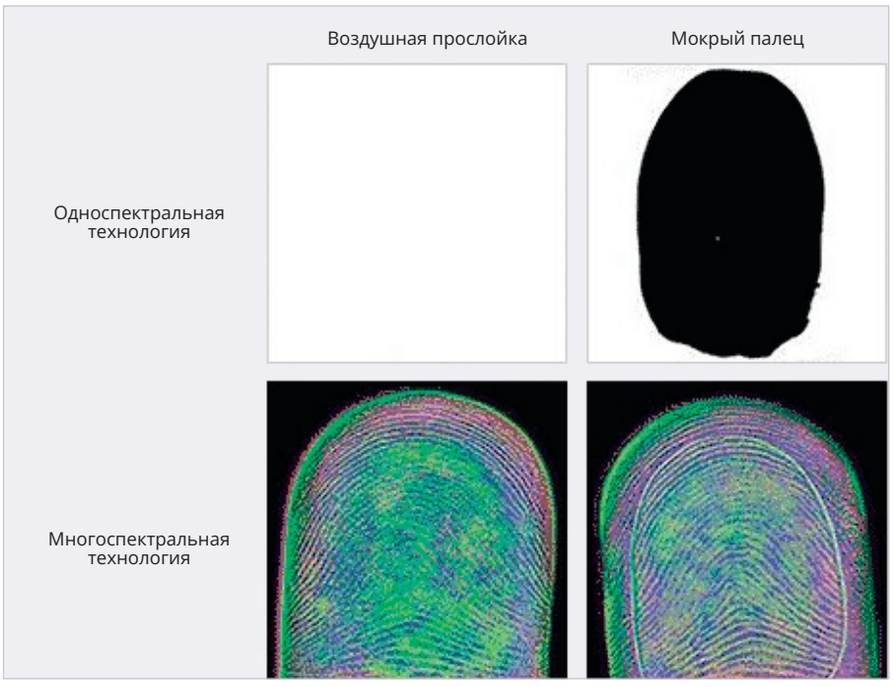


Рис. 8. Отличие одно- и многоспектральной технологии сканирования

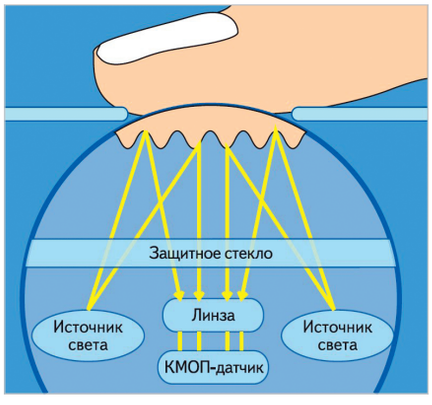


Рис. 9. Иллюстрация ёмкостного принципа считывания отпечатков пальцев

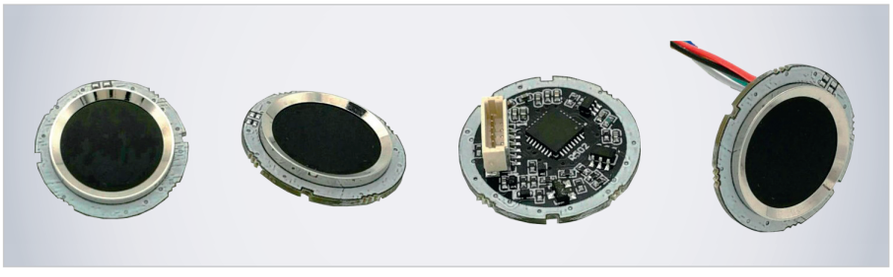


Рис. 10. Внешний вид сканера R502

сивов пьезоэлектрических микро-ультразвуковых преобразователей PMUT (piezoelectric-micromachined ultrasonic transducers). По сути, это интеграционная микро-электромеханическая система (МЭМС) с микроэлектронными и микромеханическими элементами. Датчик-сканер состоит из двух полупроводниковых пластин – МЭМС, обеспечивающий функционал излучения/отражения ультразвуковых волн и контура обработки сигнала. Так, передатчик отправляет ультразвуковые импульсы, приёмник улавливает отражённый от рельефа отпечатка ультразвук (рис. 7). Трёхмерное изображение – более надёжный метод аутентификации, чем обработка двухмерных изображений. Перспектива применения сканера огромна и почти универсальна.

Сканеры фирм Lumidigm (США) модельного ряда M301 (M30x) и NEC (Япония) доказали устойчивость к муляжам. Такие устройства имеют два сканера. Первый работает с многоспектральным излучением, проникающим под кожу. Второй встроенный сканер использует не только изображение отпечатка, но и рисунок вен. Если даже моделировать муляж на узор отпечатка, к примеру, на полимерных плёнках и материалах, из которых изготавливают «бюджетные» оттиски – дубликаты печатей, то узор вен не заменить.

Оптический многоспектральный сенсор отпечатков пальца значительно эффективнее одно- и двухспектрального. Это наглядно проиллюстрировано на рис. 8.

Современное оборудование. Отличительные признаки

Как компактное устройство, заслуживает внимания круглый ёмкостный модуль отпечатков пальцев R502. Сканер отличает относительно большая площадь сканирования, экономичный биометрический датчик, двухцветный кольцевой индикатор со светодиодным управлением. Типовой ряд модулей-считывателей R502 состоит из моделей R502A, R502F, R502AB, R502S, R503. Модель с индексом «F» создана для коммутации с интерфейсом RS-232, остальные – URAT (USB). Вес модулей от 5 до 30 г, рабочая поверхность сканирования 15 мм, у всех «выходная» картинка имеет разрешение 508 DPI. Ёмкостный принцип считывания отпечатков представлен на рис. 9, на рис. 10 представлен внешний вид сканера R502.

На рис. 11 представлен вид готового устройства датчика R502 с исполнительным узлом, управляющим электромагнитным замком в триггерном режиме.

Основные функции ёмкостного модуля отпечатков модели R311 отличаются высокоскоростным алгоритмом идентификации отпечатков и функцией самостоятельного обучения. Внешний вид модуля представлен на рис. 12.

Рис. 11. Вид готового устройства датчика R502 с исполнительным узлом, управляющим электромагнитным замком в триггерном режиме

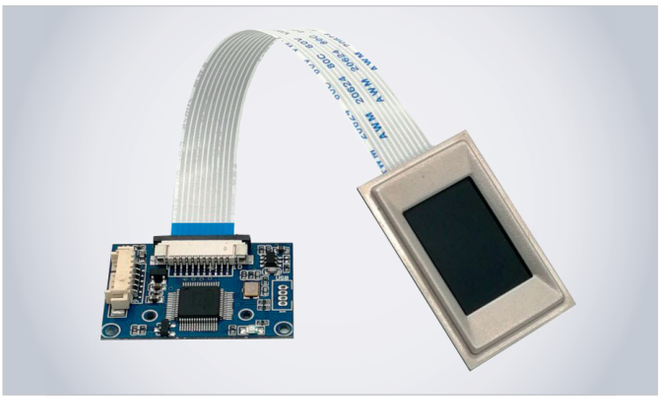


Рис. 12. Внешний вид считывателя R311

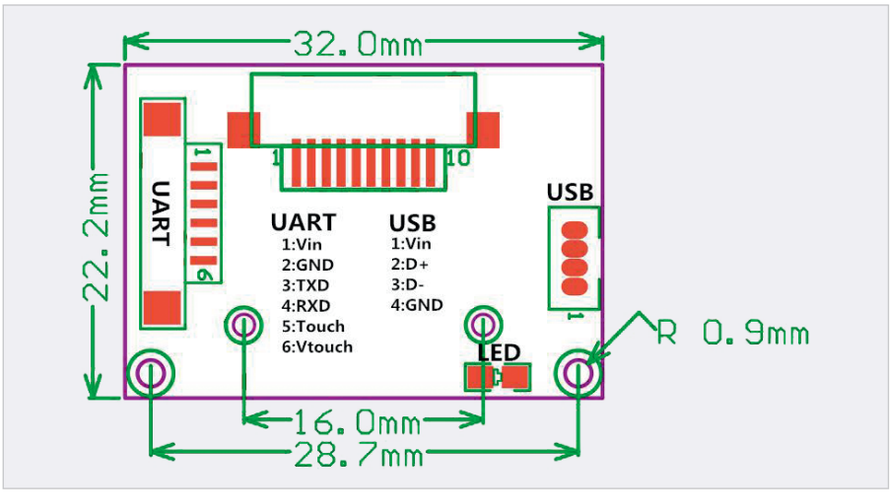


Рис. 13. Схематичный вид платы датчика R311 с распиновкой коммутационного разъёма

Ниже приведены технические характеристики рассматриваемого модуля.

- Интерфейс связи: (2.0, 3.0), UART (RS-232 TTL)
- Функция считывания/записи отпечатков пальцев
- Настройка уровня безопасности
- Возможность установки BaudRate / идентификатор устройства / пароль устройства
- Операционная система: Windows 98, Me, NT4.0, 2000, XP, WIN 7, Android
- Разрешение: 508 DPI
- Питание: DC 4,2…6 В
- Ёмкость эталонов отпечатков: 1000
- Зондирующий массив: 256×360 пикселей
- Размер модуля: 33,4×20,4×1,0 мм
- Эффективная область сканирования: 12,8×18,0 мм
- Кабельный соединитель: MX 1,25 мм 6 Pin
- Скорость сканирования: < 0,2 с
- Скорость проверки: < 0,3 с
- Рабочая температура: –20…+50°C
- Рабочая влажность: 10…85%
- Антистатическая защита: до 15 кВ
- Интенсивность абразивного сопротивления: 1 000 000 раз
- Скорость передачи данных (UART): (9600 × N) бит/с, где N = 1 ~ 12 (по умолчанию N = 6, т.е. 57600 бит/с).

На рис. 13 представлен схематичный вид платы датчика R311 с распиновкой коммутационного разъёма. Сопоставимыми характеристиками обладают датчик R303/R303S и биометрический считыватель отпечатков Smartec ST-FR031EM.

Биометрический считыватель Smartec ST-FR031EM

Биометрический считыватель со встроенным контроллером, высокоскоростным алгоритмом идентификации отпечатков пальцев, настройкой уровня безопасности и функцией самостоятельного обучения.

Работает считыватель под управлением ПО Timex. Разрешение сканера составляет 500 DPI. Память рассчитана на 3000 шаблонов и 10 000 карт, 30 000 событий. Интерфейсы сканера представлены следующими портами: RS-485, USB и Ethernet. Присутствуют Виганд вход/выход, встроенный считыватель EM, релейный выход, тревожный выход, подключение кнопки выхода и датчика положения двери. Питание 12 В, 0,4 А. Размеры 185×62×41 мм. Рабочий температурный режим: –10…+50°C, класс защиты IP65. Интерфейсы связи USB и UART. Присутствует возможность установки BaudRate / идентификатор устройства / пароль устройства. Операционная система: Windows 98, Me, NT4.0, 2000, XP, WIN 7 или Android.

Технические характеристики модуля R303/R303S

Датчик с бесплатным SDK для Android Arduino и дополнительной функцией контактного касания пальцев. Метод соответствия, параметры FRR и FAR аналогичны датчику R311.

- Питание: DC 4,2…6,0 В
- Интерфейс UART (TTL логический уровень) / USB 2,0
- Рабочий/максимальный ток потребления: 40/55 мА
- Зондирующий массив: 208×288 пикселей
- Разрешение: 508 точек/дюйм
- Среднее время поиска: < 0,2 с (1:1000)
- Скорость передачи данных: (9600 × N) bps N = 1 ~ 12 (по умолчанию N = 6)
- Размер файла персонажа: 256 байт
- Регистрация в хранилище изображений (быстродействие): < 0,1 с
- Размер шаблона: 512 байт
- Ёмкость для хранения: 1000 эталонов
- Уровень безопасности: 5 (самый высокий)
- FAR: < 0,0001%
- FRR: < 1%
- Рабочая температура: –20…+45°C
- RH: 10…85%
- Размер окна: 11×15 мм
- Размер датчика: 33,4×20,4 мм

Некоторые недостатки и пути для инженерных решений

«Минусом» рассматриваемой идентификации является зависимость каче-

ства распознавания отпечатка от состояния поверхности пальца и внешних условий (температура, влажность, пыль), нежелание сканировать отпечатки, а также особенности людей (около 3% от всех) с врождёнными плохо выделяющимися или повреждёнными отпечатками пальцев. Кроме того, в состоянии волнения, нездоровья, если человека принуждают сканировать отпечаток для получения доступа, то неровное прикосновение пальцем к считывателю, нарушение папиллярного рисунка, в том числе после воздействия водной или химической среды, или обильное потоотделение увеличивают ошибки FRR, не позволяя корректно считать изображение отпечатка.

Вот и примеры. В любой из известных и действующих биометрических технологий считывания отпечатков есть «минусы». Так, согласно отзывам, техническим характеристикам Lumidigm и статистике FAR и FRR (False Accept Rate, False Reject Rate), устройство неоднократно «требует» повторить сканирование пальца. Это неудобно: уходит время для авторизации, а также допускается около 0,05% ложноположительных срабатываний. Однако нет пределов совершенству, и именно трёхмерный метод (в комплексе с другими, к примеру, с биоакустической подписью) признан наиболее перспективным для дальнейших разработок.

Условный недостаток биометрии по отпечаткам в том, что намеренно или случайно скомпрометированный палец человека не заменишь, в отличие от пин-кода и пароля. Пароль можно сменить, PIN-код, цифровую подпись можно отозвать, но палец с индивидуальным капиллярным рисунком отозвать не получится.

Правовое поле и особенности применения биоидентификации отпечатков

Контроль ситуаций посредством установленных почти повсеместно видеокамер соответствует концепции национальной безопасности, дополнен базами отпечатков пальцев. Их сканирование основано на оптическом считывании папиллярного рисунка кожи подушечки пальца с условно большим качеством и преобразовании «рисунка» в цифровой код. В современных сканерах разного назначения разрешение изображения в диапазоне 500–5000 DPI. В правоохранительных органах оцифрованы отпечатки пальцев огромного числа граждан страны, что может быть полезно при идентификации в разных обстоятельствах. С правовой точки зрения иногда это спорно, кроме случаев, прямо предусмотренных законодательством, причём большинство мировых держав поддерживают сей принцип в национальных концепциях безопасности и охраны правопорядка, к примеру, дактилоскопирование лиц, совершивших преступления или общественно-опасные деяния. Основание: выписка из ст. 11 ФЗ-152: «Обработка биометрических персональных данных может осуществляться только с письменного согласия субъекта ПД, в случае, если данные используются для установления личности субъекта». Это и «плюс», и «минус». За небольшим правовым исключением принцип дактилоскопирования должен быть добровольным. Есть отдельные НПА (нормативно-правовые акты), регламентирующие ограничения сбора и хранения биометрических данных, а правовое регулирование в России организовано так, что пользо-

ватель добровольно даёт согласие на сканирование. К сожалению, есть случаи, когда добровольность условна, к примеру, банк или учреждение при оказании госуслуг навязывает потребителю дактилоскопирование в электронном виде. Это некорректно, но решение при получении услуг остаётся за их получателем.

Перспективы развития и совершенствования электронных сканеров

Распознавание по отпечатку основано на быстром и качественном сканировании пальца, при котором электронная система анализирует расположение характеристических точек. Происходит сравнение моделей – эталона с новым отпечатком. Причём верификация для «пальцевой» биометрии тем лучше, чем больше отпечатков удастся проанализировать системе. Так, сканирование отпечатков двух пальцев – одного за другим или одновременно – значительно уменьшает риск ошибок сканирования. С другой стороны, важным моментом процедуры является скорость электронной аутентификации, ибо никому не понравится терять время на то, чтобы неоднократно – по запросу «нераспознавшей» системы – делать новые попытки дактилоскопической биоидентификации, где бы она ни проходила – на терминале банкомата или в пункте контроля при пересечении государственной границы. На мой взгляд, обоснованный многочисленными тестами, в среднем 5% попыток идентификации через сканирование пальцев выдают отказы оборудования (у одного человека может не один палец плохо распознаваться). А для людей с нарушенными капиллярными линиями («стёртыми») цифра будет ещё выше.

Разнообразие биометрических считывателей отпечатков пальцев обусловлено разными моделями чувствительных сенсоров (сканеров), использующихся в «электронной дактилоскопии». Среди современных популярных решений бесконтактные считыватели, не требующие контакта-прикосновения, и считыватели 10 пальцев одновременно.

В сканерах используют два типа подсветок. Одна традиционная – снизу через призму, и вторая – через палец сбоку и сверху. Это повышает надёжность сканирования путём улучшения равномерности освещения по поверхности цилиндрического углубления. Но есть от этого и другой эффект – снижение зависимости качества изображения отпечатка от состояния кожи (сухая, влажная). Благодаря «обволакивающей» подсветке в устройствах с соответствующим функционалом можно получать дополнительный эффект, как-то: измерение пульса и температуры. В следующей статье (продолжение) мы исследуем возможности и рисковые эффекты при попытках «обмануть систему» – несанкционированного доступа под видом муляжа в виде плёнки, наложенной на палец (с копированным папиллярным рисунком) вместо оригинального пальца. Иначе, гипотетически, можно отрубить палец у человека, чтобы идентифицироваться в системах безопасности вместо него.

Предваряя продолжение этой работы, скажу, что при качественной подсветке в модуле сканирования защита от муляжей реализуется уверенно. Повышение качества съёма «картинки» – разрешение сформированного изображения в цифровом виде также увеличивает надёжность оборудования. Здесь важно понимать нюансы, что на коже пожилых людей и малышей условно большее количество складок, чем у подростка и человека среднего возраста. Это достигается повышением качества оптики, а не только электронного сегмента в считывателе. Сканирование папиллярного рисунка с развёрткой в 120° и в ИК-свете ещё более повышает надёжность оборудования и служит для исключения в рабочей зоне сканера «ненужной» информации в виде загрязнений на поверхности датчика и (или) пальца.

Для повышения уровня защиты системы биометрической идентификации на основе считанных «картинок» отпечатков применяют комплексные методы. Даже при сканировании двух пальцев (не одного) произведение вероятностей ошибок сократится в миллион раз. Считывание отпечатка и комбинации пальцев с введением PIN. В среднесрочной перспективе разработчики работают над тем, чтобы размещать на сканируемой панели сразу несколько пальцев или даже всю руку. С учётом того, что есть незначительное количество шестипалых людей, людей-инвалидов без каких-то пальцев, пальцы могут быть заклеены лейкопластырем, повреждены и иметь стёртый папиллярный рисунок – всё то, о чём мы говорили выше.

Опытные образцы уже работают. Однако технические сложности сопряжены с тем, что требуется большее количество датчиков для устройства, соответствующее ПО и место для внедрения такого устройства на примере банковского терминала (увеличение функционала не всегда, но часто ведет к увеличению размеров устройства).

Вместо заключения

И напоследок немного юмора. Вдумайтесь, как скоро приобретут популярность такие фразы, высказывания или сообщения сервисных систем:

- введите CVV-код с обратной стороны вашего пальца;
- получите обратно 1% от сделанных покупок по вашему пальцу;
- приложите палец с функцией проездного на метро;
- 10% годовых под остаток на пальце;
- палец Electron/Gold/Platinum;
- льготный период до 35 дней по вашему пальцу закончился.

И, разумеется, могут быть и другие версии, и другие мнения.

Литература

1. Common Biometric Exchange File Format (CBEFF), USA National Institute of Standards and Technology (NIST). URL: http://www.nist.gov.
2. *Bishop P.* Atmel FingerChip Technology for Biometric Security. URL: www.atmel.com.
3. *Maltoni D., Maio D., Jain A.K., Prabhakar S.* Handbook of Fingerprint Recognition. Springer, New York, 2003.
4. *Суомалайнен А.* Биоидентификация. URL: https://dmkpress.com/files/PDF/978-5-97060-762-6.pdf .
5. Биометрическая аутентификация: истоки, хаки и будущее. Блог компании ASUS. URL: https://habr.com/ru/company/asus/blog/408407/ .
6. *Задорожный В.* Идентификация по отпечаткам пальцев // PC Magazine/Russian Edition. 2004. № 1. С. 22.
7. Инструкции и datashit по моделям R502, R311 и др. URL: https://www.dropbox.com/sh/pznvlzx8qx5nfr3/AABpzhSyjqH0qWNYgMvxqAA9a?dl=0.
8. Клонирование отпечатка пальца: миф или реальность? URL: https://10guards.com/ru/articles/fingerprint-cloning-is-it-real/.
9. *Суомалайнен А.* Биометрическая защита: обзор технологии. М.: ДМК Пресс, 2019. 104 с.: ил.

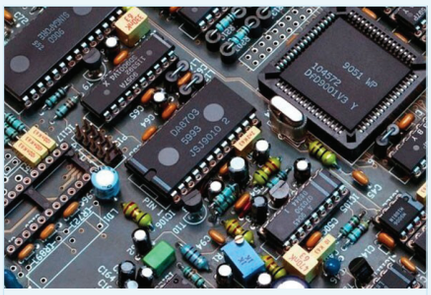
НОВОСТИ МИРА

Япония и Нидерланды согласились присоединиться к санкциям против китайской полупроводниковой индустрии – СМИ

Нидерланды и Япония «в принципе» согласились присоединиться к США в ужесточении контроля за экспортом оборудования для производства передовых чипов в Китай, утверждает агентство Bloomberg со ссылкой на свои источники.

Ожидается, что эти две страны присоединятся по крайней мере к некоторым из ограничений, которые ввели США в отношении полупроводниковой промышленности КНР в октябре. Цель рестрикций – лишить КНР доступа к важнейшим технологиям, необходимым для создания суперкомпьютеров или гиперзвукового оружия, а также производства передовых чипов внутри Китая.

Объявить о присоединении к санкциям Нидерланды и Япония должны «в ближайшие недели». Не исключено, что публикация Bloomberg со столь нечёткими временными рамками может быть попыткой надавить на несговорчивых союзников США. В ноябре это же агентство сообщило, что Нидерланды не пожелали покорно выполнять требование США ограничить поставки полупроводниковых технологий КНР.



В случае поддержки санкций США Японией и Нидерландами тройственный альянс обеспечит почти тотальную блокировку возможностей Китая закупать оборудование для выпуска новейших микросхем, подчёркивает Bloomberg. В настоящий момент в КНР запрещены поставки продукции американских Applied Materials Inc., Lam Research Corp. и KLA Corp. Вашингтон добивается того же от японской Tokyo Electron Ltd и нидерландской ASML.

Пекин со своей стороны в понедельник подал иск к США во Всемирную торговую организацию. Китай считает, что американские санкции угрожают стабильности мировых цепочек поставок. А оправдание рестрикций Вашингтона заботой о национальной безопасности США представляется сомнительным.

Напомним, в июне сообщалось о рекордном росте китайской индустрии полупроводников: тогда 19 из 20 самых быстрорастущих компаний отрасли в мире имели китайские корни, в 2021 таковых было восемь. Эти компании занимаются поставками ПО, процессоров и необходимого для производства чипов оборудования. Последнее важно в контексте нынешнего сообщения Bloomberg.

По неофициальным сведениям, которыми D-Russia.ru располагает со слов представителя отечественной IT-отрасли, у китайских компаний уже есть собственные технологии производства высокопроизводительных микросхем.

industry-hunter.com