кладовая многочисленных полезных элементов, в которых так нуждаются клетки и ткани нашего организма. Так же это самый богатый источник витамина А, который прекрасно усваивается. Помимо этого в нём также содержится большое количество витаминов В, С и D. Сок из моркови – это продукт, богатый живыми органическими щелочными элементами, такими как натрий и калий, а также кальцием, магнием и железом.

Мы в своей работе решили попытаться связать такие аспекты производства натурального морковного сока, как производство моркови и производство сока таким образом, чтобы обосновать все параметры этих производств с точки зрения технологии и экономики производства с учётом использования принципов ресурсосберегающих и безотходных технологий. Считаем, что результатом нашей работы будет проект экономически целесообразного комплексного предприятия по выращиванию моркови и производству сока и других продуктов из неё.

Работа выполняется на кафедре технологии переработки сельскохозяйственной продукции под руководством Коряковой Е.А http://www.famous-scientists.ru/10775.

32-РАЗРЯДНЫЕ МИКРОКОНТРОЛЛЕРЫ СЕМЕЙСТВА AVR32

Ефремов Д.А., Борисов В.А.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: los@pgta.ru

В настоящее время активно развивается мультимедийное направление, которое требует выполнения всё более сложных алгоритмов обработки информации, что увеличивает вероятность достижения предела возможностей любого встраиваемого микроконтроллера (МК). Алгоритмы быстрого преобразования Фурье (БПФ), инверсного дискретного косинусного преобразования (*iDCT*) и другие математически-насыщенные алгоритмы, которые редко реализовывались на встраиваемых МК еще несколько лет назад, становятся более востребованными сегодня. В мультимедийных системах такие алгоритмы, как правило, используются для кодирования/декодирования данных, в т.ч. форматов *MP*3 и *MPEG*-4. Это требует высокой производительности элементной базы, на которой построены указанные приборы.

Задача повышения производительности решается за счет увеличения рабочей тактовой частоты процессора либо реализации многоядерных решений (*ARM* + *DSP*). По причине высокого энергопотребления такие решения могут использоваться не во всех встраиваемых системах.

При этом складываются следующие требования к МК: высокая производительность; низкое энергопотребление; высокая степень интеграции; простота использования; развитые средства разработки.

Задачей построения МК с перечисленными выше требованиями еще в 2001 году занялась группа разработчиков компании *Atmel*, которая предложила решать её не повышением тактовой частоты, а улучшением архитектуры ядра процессора, который должен выполнить максимальное количество действий за один такт.

Первым семейством МК, выполненных на *RISC* ядре *AVR*32, стало семейство *AP*7. Его отличительной особенностью является 7-стадийный конвейер обработки инструкций, обеспечивающий высокую производительность. Также они содержат наборы инструкций *DSP* и *SIMD*, значительно повышающих производительность операций цифровой обработки сигнала. Помимо реализации на основе нового процессорного ядра данные МК примечательны степенью интеграции: в их состав интегрированы практически все функциональные блоки, необходимые для реализации мультимедийных систем, использующихся в сотовых телефонах, цифровых камерах, персональных цифровых помощниках, автомобильной и домашней аудио/видеотехнике, ТВ-приставках, сетевом оборудовании, промышленных принтерах и одноплатных компьютерах. МК полностью интегрируют тракт ввода (интерфейс фотоприемника изображения), обработки (сопроцессор векторного умножения для оптимизации масштабирования изображений и преобразования форматов *YUV/RGB*) и вывода (графический контроллер *TFT/STN* ЖК-дисплея с разрешающей способностью 640×320 и 320×240) графической информации. Для вывода звуковой информации предусмотрен 16-битный аудио ЦАП и цифровой интерфейс *I2S/AC*`97. Кроме того, МК оснащены обширными инструментами для организации последовательного и параллельного обмена данными, в т.ч. трансивер *USB* 2.0 480 Мбит/сек, 2-канальный контроллер *Ethernet* (опционально), интерфейс *IDE*, интерфейс карт памяти *CF/SD/MMC*, а также порты *IrDA*, 3×*SPI*, *I2C*, 3×*SSC*, 4×УСАПП.

В состав семейства входят три МК *AT*32*AP*7000, *AT*32*AP*7001, *AT*32*AP*7002. Вслед за семейством *AP*7 компания *Atmel* еще одно семейство 32-разрядных микроконтроллеров *AVR*32 *UC*3. По сути, ядро *UC*3 представляет собой урезанную версию ядра *AP*7.

Для ядра *AVR*32 фирма *IAR Systems* разработала компилятор языка *C*. В качестве альтернативы этому коммерческому продукту предлагается бесплатный компилятор *GCC*, который по компактности кода проигрывает в 1,5-2 раза.

В качестве аппаратного средства разработки предлагается стартовый набор. В состав набора включен дистрибутив ОС *Linux*. Единственным на сегодняшний день недостатком построения системы на базе этой ОС является необходимость использования компилятора *GCC*, так как продукт *IAR Systems* не может компилировать проекты на основе *Linux*.

Список литературы

1. Jo Uthus, Joyvind Strjom MCU Architectures for Compute-Intensive Embedded Applications // www.atmel.com.
2. www.eemoc.org.
3. www.avrfreaks.net.

ИСПОЛЬЗОВАНИЕ ОТПЕЧАТКОВ ПАЛЬЦЕВ В ЗАДАЧАХ БИОМЕТРИЧЕСКОГО ОГРАНИЧЕНИЯ ДОСТУПА

Ефремов Д.А., Борисова С. Н.,

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: iis@pgta.ru

Задача идентификации и аутентификации пользователей является ключевой задачей защиты информации от несанкционированного доступа (НСД), решаемой системой защиты информации (СЗИ НСД) в любой информационной системе, т.к. разграничительная политика доступа к ресурсам формируется посредством задания прав доступа для пользователей вычислительной системы. Эволюция систем аутентификации привела от аутентификации по паролю к появлению других, более надежных защитных мер, а именно, появление программно-аппаратных средств аутентификации, многофакторной аутентификации, когда пароли или другая удостоверяющая информация хранится на внешних носителях. Параллельно с внедрением программно-аппаратных средств аутентификации исследовалась и развивалась биометрия.

Биометрия – это использование для аутентификации индивидуальных признаков человека (его голоса, формы лица, руки, рисунка радужной оболочки глаза, подпись). Как биометрическая характеристика отпечатки пальцев имеют длинную и интересную историю [1]. На внутренней поверхности ладони и ступни человека есть мелкие бороздки (рис. 1).

Рис. 1. Изображение отпечатка пальца

С позиции анализа в каждом отпечатке пальца можно определить два типа признаков – глобальные и локальные.

1. **Глобальные признаки** – это те, которые можно увидеть невооружённым глазом: папиллярный узор; область образа, выделенный фрагмент отпечатка, в котором локализованы все признаки; ядро, пункт, локализованный в середине отпечатка или некоторой выделенной области; пункт «дельта», начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки); тип линии – две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа; счётчик линий, число линий на области образа, либо между ядром и пунктом «дельта».

2. **Локальные признаки** (их называют минуциями) – уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т.д.), ориентацию папиллярных линий и координаты в этих пунктах. Каждый отпечаток содержит до 70 минуций. Согласно стандартам РФ [2] существует два основных типа минуций (контрольных точек): точка окончания основы гребня и точка бифуркации основы гребня (или точка разветвления). Помимо указанных типов в отпечатках пальцев реже встречаются и другие типы информативных точек, имеющих более сложные определения. На рис. 2 представлены некоторые варианты расположения и измерения контрольных точек.

Рис. 2. Расположение и ориентация контрольных точек

Данные об отпечатке пальца пользователя формируются в соответствующую структуру согласно [2], которая имеет различные поля: идентификатор формата; номер версии; длина записи; идентификационный номер биометрического сканера; уровень настроек получения изображений; число изображений пальцев/ладоней; единица измерения разрешения; разрешение сканирования (горизонтальное); разрешение сканирования (вертикальное); разрядность шкалы градаций серого; Алгоритм сжатия изображения.

Применение отпечатков пальце в идентификации личности позволяет упростить и ускорить (автоматизировать) многие выполняемые человеком операции, поскольку обычное удостоверение личности, которое можно утратить, забыть, заменяется собственным отпечатком. При этом гарантируется высокая точность и надежность идентификации личности. С использованием технологии идентификации по отпечаткам пальцев надежно решаются следующие задачи: банковские транзакции, аутентификации водительских прав, задачи пограничного контроля, допуск на рабочие места и др. В перспективе имеется множество задач, где еще может применятся данная технология.

Список литературы

1. Болл Р., Коннел Дж. Руководство по биометрии. – М.: Техносфера, 2007.
2. ГОСТ Р ИСО/МЭК 19794-2-2005 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки.

ФАКТОРЫ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Жаринов А.А., Шмокин М.Н.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: los@pgta.ru

Одной из проблем, возникающих при планировании системы информационной безопасности предприятия, является необходимость оценить актуальность угроз, создаваемых различными источниками. Оценка актуальности этих угроз и целесообразности применяемых мер противодействия должна основываться на вероятностях реализации этих угроз. Оценить вероятность реализации тех или иных угроз можно лишь, основываясь на публикациях экспертных организаций, которые проводят расследование инцидентов в области информационной безопасности, а также выполняют тесты на проникновение.

В общем случае можно выделить три основных возможности проникновения в информационные системы компаний:

– использование ошибок в настройках телекоммуникационного оборудования и серверов;

– уязвимости *Web*-приложений, когда злоумышленник использует ошибки, допускаемые разработчиками этих приложений;

– использование нарушителем уязвимостей рабочих мест пользователей в сочетании с методами социальной инженерии.

Анализ недостатков сетевой инфраструктуры показывает, что залогом успешной атаки является не отсутствие тех или иных средств защиты, а неправиль-