Синтезатор построен на базе сигнального микроконтроллера dsPIC33FJ128GP804 со встроенными аппаратными модулями DMA и DAC. Речевой сигнал формируется по алгоритму, который основан на формировании по псевдослучайному закону аудио фрагментов речи (фонем) в слова и предложения китайского языка. Фонемы располагаются во внешней microSD Flash памяти, что позволяет их хранить в большом объеме и в несжатом виде. В качестве генератора псевдослучайных чисел используется Вихрь Мерсенна, что обеспечивает быструю генерацию высококачественных псевдослучайных чисел и обеспечивает равномерное распределение генерируемых значений. Инициализация генератора осуществляется по значению аналогового шума, полученного с АЦП сигнального микроконтроллера, что исключает повторяемость слов и возможность восстановления информации из формируемого шума современными способами обработки сигналов.

Таким образом, применение современной элементной базы в синтезаторе речеподобных сигналов на китайском языке позволило значительно расширить его возможности, снизить стоимость, повысить надежность и удобство в эксплуатации.

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕХАНИЗМОВ ПАРАЛЛЕЛЬНОЙ КИНЕМАТИКИ

С.Е. Карпович, В.Н. Нестеренко, А.С. Манин

Применение механизмов параллельной кинематики на приводах прямого действия в качестве исполнительных устройств систем пространственных перемещений широкого назначения позволяет в настоящее время разрешить большинство из проблем, присущих традиционной и широко используемой компоновке координатных систем технологического оборудования.

Представленные в докладе математические модели, алгоритмы и программы компьютерного моделирования, разработанные для исследования механизмов параллельной кинематики на поворотных, сегментных и планарных шаговых двигателях прямого действия позволили провести имитационное моделирование прямой и обратной задач кинематики, на основе которых проведено углубленное компьютерное моделирование, включая нахождение границ рабочей области для выбранной конфигурации; генерирование требуемых траекторий в рабочей области с расчетом скорости и ускорения и передаточных функций в каждой точке траектории; анализ предельных возможностей по реализации линейных и угловых перемещений исполнительного звена в рабочей области.

Разработанные программы, реализованные в среде MATLAB, имеют удобный пользовательский интерфейс, позволяют проводить компьютерное исследование в интерактивном режиме с возможностью оптимизации исходной конфигурации и конструктивных параметров исполнительного механизма параллельной кинематики, и могут быть использованы при разработке и создании систем перемещений различного технологического оборудования.

Литература

1. Карпович С.Е., Жарский В.В., Дайняк И.В., Литвинов Е.А. Системы многокоординатных перемещений и исполнительные механизмы для прецизионного технологического оборудования. Минск, 2013.

КОНВЕЙЕРНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА HMAC-SHA1 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич

Первостепенное значение для обеспечения целостности данных и аутентификации источника данных имеют код проверки подлинности сообщений HMAC (Hash-based Message Authentication Code) и хэш-функции. HMAC в комбинации с хэш функциями SHA-1 и MD5 используют такие протоколы, как IPSec (Internet Protocol Security), IKE (Internet Key Exchange), TLS (Transport Layer Security). Поэтому представляет интерес высокопроизводительная аппаратная реализация специализированного процессора HMAC с использованием хэш-функции SHA-1 (HMAC-SHA1) на базе FPGA.

Полная конвейерная реализация процессора HMAC-SHA1 имеет двухуровневую организацию. На верхнем уровне строится конвейер, базовыми блоками которого являются блоки, реализующие алгоритм хэширования SHA-1. На нижнем уровне для построения блоков SHA-1, в свою очередь применяется полностью конвейерная (развернутая) архитектура. При этом принцип

разбиения на ступени следующий: каждая ступень должна содержать один вычислительный блок SHA-1, поскольку он имеет наибольшую временную задержку. На первой ступени конвейера два блока SHA-1 работают параллельно. На остальных ступенях, кроме последней, блок SHA-1 работает параллельно с блоком задержки. На последней ступени работает один блок SHA-1.

Кроме того, на первой ступени начальными значениями переменных состояния A, B, C, D, E являются константы (на остальных ступенях это результат обработки предыдущей ступени), что учитывается при разработке упрощенной структуры вычислительного блока SHA-1 специально для этой ступени.

Рассматриваемая архитектура обеспечивает самую высокую скорость вычисления MAC-значения, однако, требует максимального использования ресурсов FPGA по сравнению с другими вариантами.

АНАЛИЗ МЕТОДОВ ПАРАМЕТРИЗАЦИИ ЛИНИЙ НА ИЗОБРАЖЕНИЯХ

Д.И. Кирилюк, А.В. Костусев, Ю.И. Кулаженко

В настоящее время в связи с развитием мобильных систем наблюдения специального назначения стоит актуальная задача – обработка изображений в реальном масштабе времени. Для ее решения широко используются методы, которые учитывают распределение градиента яркости в окрестностях реперных точек. Однако, в условиях проекционных искажений эффективность градиентного подхода снижается. Устранение данного недостатка возможно за счет геометрического подхода. Геометрические методы применялись в задачах для обработки изображений, имеющих искусственную природу (например, печатные платы, детали конструкций, САПР). Поэтому актуальной задачей в настоящее время является модернизация существующих геометрических методов и создание новых методов для обработки изображений, имеющих естественный характер (например, спутниковые, ландшафтные). Целью настоящей работы является теоретический анализ методов геометрической параметризации линий на изображениях.

Основными требованиями к дескрипторам линий являются: устойчивость к проективным преобразованиям; устойчивость к шуму; высокая скорость формирования; произвольность формы кривой. Теоретический анализ показал, что для решения поставленной задачи, с учетом вышеуказанных требований, наиболее эффективны методы на основе Фурье-дескрипторов, сигнатур или цепных кодов.

Методы на основе Фурье-дескрипторов используют дискретное преобразование Фурье конечной последовательности комплексных чисел (координаты точек рассматриваются как комплексные числа), позволяют по коэффициентам преобразований восстановить линию.

Сигнатуры – одномерные функции, взаимно-однозначно определяющие кривую линию, строятся относительно некоторой фиксированной точки (центра). Особенностью цепных кодов является кодирование направлений и длин прямых отрезков линии.

Вычислительная сложность вышеназванных методов примерно одинаковая. Методы на основе Фурье-дескрипторов устойчивы к повороту, параллельному переносу. Устойчивость методов на основе сигнатур и цепных кодов зависит от выбора фиксированной (начальной) точки.

БЕЗОПАСНОСТЬ USB УСТРОЙСТВ

М.И. Кошевник

Цель исследования – оценить безопасность USB устройств от различного вида угроз.

В ходе работы установлено, что клавиатура отправляет данные о всех исходящих событиях, а в качестве входящих принимает только сведения о состоянии светодиодов – NumLock, CapsLock, ScrollLock. Данное ограничение заложено на уровне операционной системы, что не позволяет организовать аппаратный шпион – аналог программного кейлоггера.

В процессе исследования выявлено, что USB устройства, относящиеся к классу Human Input Device, подвержены разного рода уязвимостям. Так, данные с web-камеры, работающей по принципу постоянного приёма запросов о захвате кадров, могут быть получены в промежуточный момент между запросами.

Драйвер микроконтроллера USB-Flash, находящийся во встроенном ROM, может быть модифицирован в корыстных целях. Операционная система по умолчанию устанавливает драйвера