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