будет пропорциональна составляющей скорости движения объекта в пикселях на кадр по оси x. Таким образом, для вычисления составляющей скорости по оси x следует найти значение τ_x. Определение сдвига сводится к сравнению последовательности $g(t)_x$ с каждой последовательностью множества $\{a_i\}$ и выбору ближайшей из них по расстоянию Хэмминга. Максимальное значение коэффициента $r_{t\,x}$ определяет величину τ_t. Следовательно, коэффициенты корреляции $\max r_{t\,x}$ формируются в точках с теми номерами t функций $g_{t,\,x}$, координаты которых пропорциональны скорости движения объекта. Аналогичные рассуждения справедливы для получения коэффициентов диадной корреляционной функции для направления y.

В работе представлены результаты анализа движения трудноразличимого (скрытного) объекта на изображениях, искаженных аддитивным шумом. Объем вычислений параметров движения можно существенно сократить, если воспользоваться структурными свойствами мажоритарных последовательностей множества $\{a_i(t)\}$ и их упорядочением определенным способом.

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ АППАРАТНЫЕ РЕАЛИЗАЦИИ ПРОЦЕССОРОВ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ ПЛИС С АРХИТЕКТУРОЙ FPGA

М.М. РОДИОНОВ, М.И. ВАШКЕВИЧ, А.А. ПЕТРОВСКИЙ,
А.В. СТАНКЕВИЧ, АЛ.А. ПЕТРОВСКИЙ, М.В. КАЧИНСКИЙ

Предлагаются два варианта аппаратной реализации процессора шифрования алгоритма DES на основе последовательной и конвейерной архитектуры. В последовательном процессоре все циклы алгоритма DES последовательно выполняются на одном вычислительном ядре (далее подход 1). За счет этого возможна экономия аппаратных ресурсов, что позволяет реализовать специализированный процессор со средней производительностью и сравнительно невысокими аппаратными затратами.

В конвейерной архитектуре каждый цикл шифрования реализуется на отдельной вычислительной ступени. Данный вариант позволяет получать выходные результаты в каждом такте работы специализированного процессора. В результате исследований реализаций конвейерного процессора на базе ПЛИС с архитектурой FPGA было установлено, что лучшие показатели производительности достигаются при использовании распределенной памяти кристалла ПЛИС (далее подход 2.1) вместо блочной памяти (далее подход 2.2) для хранения таблиц замен алгоритма DES. Также был реализован конвейерный процессор на основе известного модифицированного представления алгоритма DES (далее подход 2.3), в котором за счет математических преобразований две операции сложения по модулю два с двумя операндами заменяются на одну операцию с четырьмя операндами, что позволяет более эффективно использовать ресурсы ПЛИС.

Для кристалла xc5vlx110 были получены следующие характеристики (логические секции/максимальная тактовая частота, МГц): подход 1 — 151/200; подход 2.1 — 1063/374; подход 2.2 — 997/300, 32 блока памяти; подход 2.3 — 991/377.

Предложенные подходы могут использоваться в приложениях, требующих высокой производительности при шифровании данных.