ПОВЫШЕНИЕ ЧУВСТВИТЕЛЬНОСТИ НЕЛИНЕЙНОГО РАДИОЛОКАТОРА

М.М. Иванов

Стремительное развитие микро- и наноэлектроники ставит задачу улучшения чувствительности нелинейного радиолокатора (НРЛ) к закладным устройствам с малыми габаритами.

В традиционной радиолокации применение сложных сигналов разрешает противоречие между энергетическим потенциалом и чувствительностью [1]. В нелинейной радиолокации применение сложных сигналов имеет несколько иной характер [2]: применение сложных сигналов приводит к ухудшению чувствительности и точности измерения дальности, а повышение зондирующей частоты — к ухудшению проникающей способности сигнала.

Решение данной задачи — применение сверхширокоплосных импульсов. При облучении нелинейного объекта одновременно высокочастотным гармоническим сигналом и сверхширокополосными импульсами наблюдается эффект взаимной модуляции [3]. С помощью приемника НРЛ, регистрирующего сигнал, который получен в результате взаимной модуляции, происходит обнаружение нелинейного объекта. Сверхмалая длительность импульсов позволяет достичь разрешения порядка единиц миллиметров. Программная модель подтверждает работоспособность метода.

Литература

1. Лезин Ю.С. Оптимальные фильтры и накопители импульсных сигналов. М., 1969.

2. Горбачев А.А. // Нелинейная радиолокация. Сб. статей № 2. М., 2006.

3. Якубов В.П., Шипилов С.Э., Сатаров Р.Н., Юрченко А.В. // Журнал технической физики. 2015. Т. 85, Вып. 2. С. 122–125.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СКРЫТЫХ КРИПТОКОНТЕЙНЕРОВ ПРИ СОКРЫТИИ ДАННЫХ

А.М. Кадан, И.А. Сазановец

Один из широко распространенных способов защиты цифровых данных – использование зашифрованных виртуальных жёстких дисков, так называемых криптоконтейнеров.

Традиционно, пользователь авторизуется для работы с файлом криптоконтейнера, и криптоконтейнер монтируется как локальный диск. Однако некоторые программы (VeraCrypt, Jetico BestCrypt Container Encryption) позволяют также создавать скрытые криптоконтейнеры в уже готовых контейнерах. Скрытый образ внутреннего контейнера лежит на незанятом пространстве внешнего контейнера.

В работе ставилась задача исследования особенностей использования скрытых криптоконтейнеров при сокрытии данных. Дело в том, что скрыть информацию с помощью таких криптоконтейнеров не сложно, но если допустить некоторые типичные ошибки, то, как минимум, обнаружить факт существования скрытой информации становится возможным, что является весьма значимой угрозой. С этой точки зрения, основное внимание должно быть уделено дополнительным мерам и методам противодействия детектированию наличия факта сокрытия информации.

В работе предложены методы распределения информации по блокам криптоконтейнера в зависимости от уровня ее конфиденциальности, предлагаются методы «отвлечения внимания» злоумышленника от возможного наличия скрытого внутреннего содержимого, которые бы минимизировали возможные потери в случае оказания неприемлемого воздействия на владельца информации.

Методы основаны на стеганографии и учете психологического портрета злоумышленника. Проведенный эксперимент подтвердил, что предложенные методы позволили повысить надёжность сокрытия информации в скрытом криптоконтейнере при попытке детектирования ее наличия специалистами достаточно высокого уровня.

СИНТЕЗАТОР РЕЧЕПОДОБНЫХ СИГНАЛОВ НА КИТАЙСКОМ ЯЗЫКЕ

А.А. Казека, Г.В. Давыдов, В.А. Попов, А.В. Потапович

Синтезатор речеподобных сигналов предназначен для защиты от утечки информации по акустическому каналу. Данное устройство формирует акустические речеподобные сигналы на китайском языке и применяется совместно с генератором акустического белого шума.

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