коэффициента ДКП и подвергаются следующей модификации: для кодирования 1 и 0 коэффициенты изменяются так, чтобы два из них были больше или меньше третьего на определенное пороговое значение *D*.

Анализу подвергаются все коэффициенты ДКП из области модификации каждого блока (8 коэффициентов). Для этого в каждом блоке вычисляется среднеквадратичное отклонение (СКО) и формируется массив коэффициентов СКО. для полученного массива строится гистограмма распределения коэффициентов, по которой находится значение наиболее часто встречающееся — s_{max}. для пустых контейнеров и контейнеров заполненных с порогом $D>1$ значение s_{max} будет больше ς=0,354. для случая $D=1$ вычисляется отношения количества наиболее часто встречающихся значений к общему количеству коэффициентов СКО. Полученное значение отношения сравнивается со значениями вероятности нахождения скрытой информации по таблице значений, полученных эмпирическим путем.

Предложенный критерий стеганографического анализа JPEG-изображений дает высокий процент (порядка 90%) верных результатов в случае порога $D>1$. Оценка с порогом встраивания $D=1$ дает результат с ошибкой второго рода равной 15,6%. для пустых контейнеров ошибка первого рода примерно равна 20%. Использование предложенного метода оценки изображения в формате JPEG на предмет определения наличия скрытой информации методом Коха–Жао обеспечивает эффективное решение задач стегоанализа.

Литература

1. Zhao J., Koch E. // IEEE Workshop on Nonlinear Signal and Image Processing. Greece, 1995. P. 123–132.

УСТРОЙСТВО СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА РАЗНЫХ ЯЗЫКАХ

О.Б. ЗЕЛЬМАНСКИЙ

Задачей предлагаемого устройства защиты речевой информации является генерирование речеподобных сигналов на разных языках и в режиме реального времени, маскирующих речь участников переговоров. Работа устройства осуществляется следующим образом.

Блок формирования псевдотекста составляет псевдотекст на выбранном языке или нескольких языках с использованием их статистики, получаемой, например, от баз русского, арабского и английского языков. Блок компиляции аллофонов в зависимости от диктора и выбранного языка выбирает необходимые базы аллофонов и озвучивает полученный псевдотекст. в результате получается шумовой речеподобный сигнал, который поступает на управляемый усилитель.

В случае, если требуется синтезировать речеподобный сигнал непосредственно из речи участников переговоров, речевой сигнал, поступающий от встроенного или выносного микрофона, фиксируется блоком детектирования речи. Далее он поступает в блок верификации диктора по голосу, а также в блоки сегментации и классификации с целью формирования аллофонов, которые в свою очередь заносятся в базу аллофонов соответствующего диктора. В базу аллофонов какого диктора следует занести каждый аллофон определяется блоком верификации диктора по голосу, который распознает и подтверждает личность каждого из участников переговоров на основании уникальной информации, выделенной из их речи заранее в процессе регистрации до начала переговоров. Кроме того данный блок позволяет выбрать уже имеющуюся базу аллофонов конкретного диктора для использования в блоке компиляции аллофонов.

Предложенное устройство позволяет защитить речевую информацию от утечки через такие элементы ограждающих конструкций как потолок, пол, стены, оконные стекла, элементы конструкций отопительных и водопроводных сетей, дверные тамбуры и вентиляционные каналы.

ИСПОЛЬЗОВАНИЕ КВАНТОВЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ОПТИЧЕСКОЙ ИНФОРМАЦИИ

А.О. ЗЕНЕВИЧ, А.М. ТИМОФЕЕВ, Ф.А. АХМЕДЖАНОВ

В связи с интенсивным развитием в последние годы волоконно-оптических систем связи возрос интерес к созданию средств обнаружения каналов утечки оптической информации, передаваемой по таким системам. Квантово-криптографические системы передачи информации, в которых для кодирования данных используются состояния фотонов оптического излучения, позволяют обеспечить безусловную защищенность передаваемой информации, однако имеют ряд недостатков, в частности низкие скорости передачи информации (СПИ) — до 50 кбит/с [1], что может ограничивать область применения этих систем. Возможной альтернативой квантово-криптографическим системам передачи информации могут быть квантовые системы передачи и приема информации, в которых для трансляции оптической информации так же, как и в квантово-криптографических системах, используются отдельные фотоны, однако не применяется кодирование передаваемых двоичных символов состояниями передаваемого фотона. Отметим, что защита передаваемой информации в квантово-криптографических системах обеспечивается за счет использования состояний передаваемых фотонов (несанкционированный доступ приводит к нарушению поляризации фотонов, что и выявляет факт доступа к передаваемой информации), а в квантовых — за счет контроля вероятности ошибки регистрации данных (несанкционированный доступ увеличивает вероятность ошибки регистрации данных, что приводит к уменьшению СПИ, контроль которой выявляет наличие канала утечки информации). До настоящего времени квантовые системы передачи и приема информации, позволяющие обнаруживать каналы утечки оптической информации, не разработаны. Поэтому целью данной работы является создание квантовых систем обнаружения каналов утечки оптической информации.

В работе предложены квантовые системы передачи и приема информации, в которых в качестве приемного модуля использовался счетчик фотонов, построенный на базе лавинного фотоприемника.

Выполнена классификация квантовых систем передачи и приема оптической информации, согласно которой такие системы можно разделить по числу фотонов, используемых для передачи каждого бита информации, на однофотонные и многофотонные, а также по способу синхронизации источника и приемника — на синхронные и асинхронные.

Выполненные экспериментальные исследования по определению СПИ созданных квантовых систем показали, что максимально возможная СПИ синхронных однофотонных квантовых систем составила 1,2 Мбит/с, асинхронных — до 50 кбит/с.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т11ОБ-043).

Литература

1. Килин С.Я., Хорошко Д.Б., Низовцев А.П. и др. // Квантовая криптография: идеи и практика. Минск, Белорусская наука, 2007.