

АЛГОРИТМ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ В ПОТОКОВЫЙ КОНТЕЙНЕР

В. А. Вьюгин, В. С. Садов

Белорусский государственный университет, Минск, Беларусь

Широкое развитие цифровой телекоммуникации и сетевых средств передачи мультимедийной информации (видеопотоков и голосового трафика) повышает актуальность применения систем скрытной передачи информации в потоке данных (поточковых стеганосистем). Используемые алгоритмы стеганокодирования должны не только обеспечивать высокую пропускную способность, но и быть достаточно робастными к сжатию различными методами при передаче по сетям.

Ограничивая круг исследования потокового контейнера только голосовым трафиком, можно определить ряд условий для алгоритма скрытного встраивания информации: 1) высокое быстродействие; 2) внесение минимальных искажений в сигнал; 3) устойчивость к помехам, вносимым пассивным злоумышленником; 4) устойчивость к сжатию.

Преобразования сигналов можно упорядочить по достигаемым выигрышам от кодирования (рис. 1). Под выигрышем от кодирования понимается степень перераспределения дисперсий коэффициентов преобразования [1]. Наименьший выигрыш дает разложение по базису единичного импульса, наибольший – преобразование Карунена-Лоэва (ПКЛ). Преобразования с высокими значениями выигрыша от кодирования (дискретное косинусное преобразование ДКП и вейвлет-преобразование) характеризуются резко неравномерным распределением дисперсий коэффициентов субполос. Низкочастотные субполосы не подходят для алгоритма стеганокодирования из-за основной информационной нагрузки на них, а высокочастотные субполосы – из-за большого шума обработки. Следовательно, необходимо использовать среднечастотные полосы, в которых влияние этих двух факторов проявляется примерно одинаково. Так как таких полос немного, то пропускная способность стеганоканала невелика.

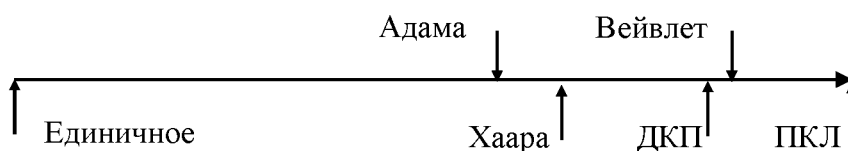


Рис. 1. Различные преобразования, упорядоченные по достигаемым выигрышам от кодирования

В случае применения преобразований с невысоким выигрышем от кодирования (Адамара или Фурье) имеется большее количество среднечастотных субполос. Следовательно, и пропускная способность выше поэтому, лучше применять преобразования с меньшими выигрышами от кодирования, плохо подходящие для сжатия сигналов.

Одним из преобразований, позволяющих осуществить устойчивое к компрессии встраивание мультимедийных данных, является быстрое вейвлет-преобразование (БВП). Применение вейвлет-преобразований в методах стегокодирования может решить основные задачи, которые были поставлены: минимизация вносимых искажений и устойчивость к атакам пассивного злоумышленника. В общем случае итерационная формула БВП [2, 3] имеет вид:

$$a_{m+1,k} = \sum_l h_{l-2k} a_{m,l}, \quad (1)$$

$$d_{m+1,k} = \sum_l g_{l-2k} a_{m,l}. \quad (2)$$

При восстановлении сигнала по его вейвлет-коэффициентам процесс идет от крупных масштабов к мелким и на каждом шаге описывается выражением:

$$a_{m-1,k} = \sum_l (h_{k-2l} a_{m,l} + g_{k-2l} d_{m,l}). \quad (3)$$

Таким образом, для анализа-синтеза сигнала в базисе вейвлетов необходимо выполнить $4LN$ операций, что не превышает числа преобразований для быстрого преобразования Фурье ($M \log_2 N$).

АЛГОРИТМЫ ВСТРАИВАНИЯ И ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ

В соответствии с изложенными требованиями предложен алгоритм стеганографического встраивания данных (рис. 2). В данном алгоритме предлагается встраивать информацию в низкочастотные коэффициенты БВП. В качестве информации выступает последовательность нулей и единиц. Встраивание производится по методу Коха [4, 5], т. е. для передачи бита нуля добиваются того, чтобы разность значений коэффициентов была больше некоторой положительной величины, а для передачи бита единицы, эта разность делается меньше некоторой отрицательной величины. Алгоритм встраивания информации (рис. 1) включает следующие шаги.

1. Загрузка кадра (160 отсчетов) из исходного аудио-контейнера.
2. Разложение сигнала на глубину 3 (пакет вейвлетов Добеши).
3. Выделение коэффициентов быстрого БВП на узле 3.
4. Если коэффициент j больше или равен коэффициенту $(j+1)$, то заносится в память 1, иначе – 0.

5. Если не достигнут конец стеганосообщения, то переход к пункту 1.

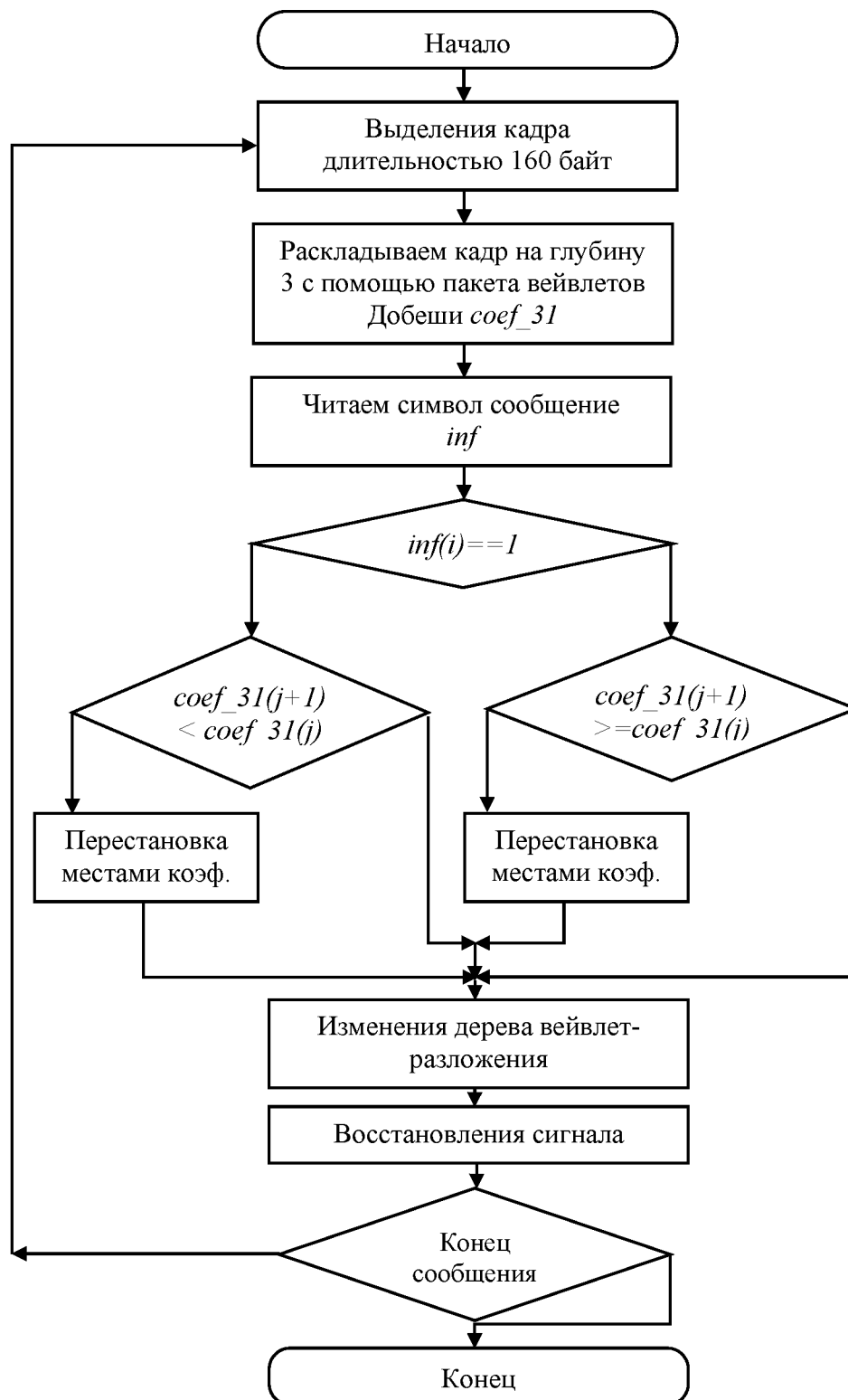


Рис. 2. Алгоритм встраивания информации

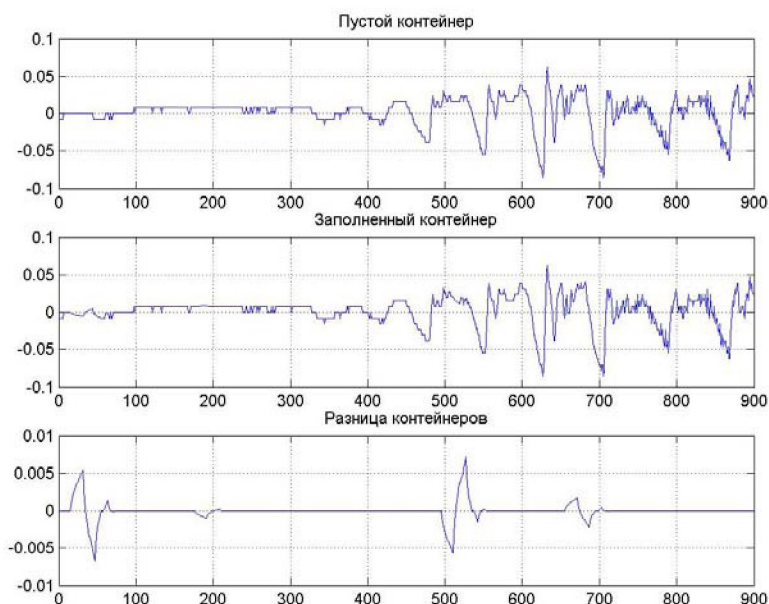


Рис. 3. Результаты встраивания информации

Результаты встраивания информации в потоковый аудио контейнер показаны на рис. 3.

Таким образом, при сравнении пустого и заполненного контейнера заметны лишь небольшие изменения, которые неразличимы при прослушивании. Алгоритм позволяет выбирать коэффициент, в который будет встроена метка и узел дерева быстрого вейвлет-преобразования, из которого выбирается коэффициент. Выбор узла дерева должен основываться на том, что низкочастотные субполосы содержат подавляющую часть энергии сигнала и, следовательно, несут шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ фильтрация. Таким образом, для вложения сообщения наиболее подходящими являются среднечастотные субполосы спектра изображения. Пропускная способность данного алгоритма стеганокодирования составляет 25 бит/с.

Литература

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И.Н. Оков, И. В. Туринцев. М. : СОЛОН-Пресс, 2002 С. 173–178.
2. Яковлев, А. Н. Введение в вейвлет-преобразования. Новосибирск : Изд. НГТУ, 2003.
3. Смоленцев, Н. К. Основы теории вейвлетов. Вейвлеты в Matlab. М. : ДМК Пресс, 2005.
4. Аграновский, А. В. Основы компьютерной стеганографии. М. : Радио и связь, 2003.
5. Федоров, В. М. Метод стеганографии в аудио сигналах и изображениях, устойчивый к компрессии с потерями / В. М. Федоров, О. Б. Макаревич, Д. П. Рублев // Информационное противодействие угрозам терроризма, 2006. № 7.