

СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ДАННЫХ В ФАЙЛАХ ФОРМАТА OGG VORBIS

А. И. Демидчук, Ю. А. Чернявский

Белорусский государственный университет информатики и радиоэлектроники, кафедра ЭВМ
ул. П.Бровки 6, г. Минск, Беларусь
телефон: 293- 86-17; e-mail: ID23cat@tut.by, Chernyavskiy@academy.edu.by

В данной статье кратко описывается метод сжатия аудио данных алгоритмом Vorbis и приводится алгоритм стеганографического встраивания сообщений в закодированные данные. В основу данного метода положен адаптивный алгоритм встраивания данных в области дискретного косинусного преобразования.

Ключевые слова – OGG, Vorbis, аудио данные, стеганография.

1 ВВЕДЕНИЕ

Целью настоящих исследований является разработка методов и программных средств предназначенных для стеганографического встраивания сообщений в потоковые контейнеры.

Ogg – открытый стандарт формата мультимедиа-контейнера, являющийся основным файловым и потоковым форматом для мультимедиа-кодеков фонда Xiph.Org, а также название проекта, занимающегося разработкой этого формата и кодеков для него. Как и все технологии, разрабатываемые под эгидой Xiph.Org, он является открытым и свободным стандартом, не имеющим патентных или лицензионных ограничений [1].

Vorbis – свободный формат сжатия звука с потерями, официально появившийся летом 2002 года. По функциональности и качеству аналогичен таким кодекам как AAC, AC3 и VQF, превосходящим MP3. Психоакустическая модель, используемая в Vorbis, по принципам действия близка к MP3 и подобным, однако математическая обработка и практическая реализация этой модели существенно отличаются [2].

Для хранения аудиоданных в формате Vorbis чаще всего применяется медиаконтейнер Ogg, такой файл обычно имеет расширение .ogg и называется двойным именем «Ogg/Vorbis» или «Ogg Vorbis». Однако «Ogg Vorbis» называют и сам кодек без контейнера, так как он является частью проекта Ogg.

Перед авторами стояла задача разработать адаптивный алгоритм встраивания данных в области дискретного косинусного преобразования.

2 ФОРМАТ OGG VORBIS

Ogg Vorbis по умолчанию использует переменный битрейт, при этом значения последнего не ограничены какими-то жесткими значениями, и он может варьироваться даже на 1 kbps. При этом стоит заметить, что форматом жестко не ограничен максимальный битрейт, и при максимальных настройках кодирования он может варьировать от 400 kbps до 700 kbps. Такой же гибкостью обладает частота дискретизации – пользователям предоставляется любой выбор в пределах от 2 кГц до 192 кГц.

Процесс сжатия кодером Vorbis приведен на рисунке 1.

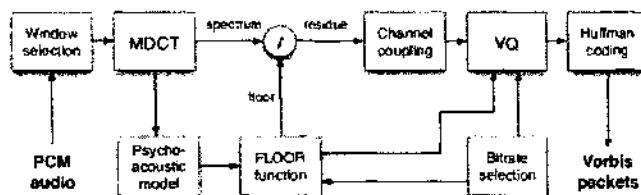


Рис. 1. Схема сжатия данных в формате Vorbis

На этапе Window selection в зависимости от характера сигнала применяются окна переменной длины от 64 до 8192 сэмплов. Процесс сжатия основан на модифицированном дискретно-косинусном преобразовании (MDCT) и квантовании векторов (VQ) применяемых к векторам данных. Более подробно [3], [4].

3 АЛГОРИТМ ВСТРАИВАНИЯ/ИЗВЛЕЧЕНИЯ

Встраивание предполагается производить на этапе между квантованием (VQ) и кодированием Хаффмана (Huffman coding). Это обусловлено тем, что на данном этапе сжатия основная потеря незначительных данных завершена, поэтому модифицированные коэффициенты будут в неизменном виде записаны в результирующий контейнер.

Коэффициенты МДКП на этапе между квантованием и кодированием хаффмана разделены на два вектора. Один содержит данные общие для обоих каналов (в случае стерео сигнала), а второй – разность между каналами. Согласно разработанному алгоритму предполагается встраивать данные в первый вектор содержащий пересечение каналов – couple vector.

Couple vector представляет собой разреженный вектор, содержащий малые целочисленные значения (порядка

0, ±10). Длина вектора в два раза меньше длины ранее выбранного окна.

Пример. Вектор *Couple*, приведен 41 коэффициент из 128 отсчетов: 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 -3.000000 0.000000 0.000000 0.000000 0.000000 -2.000000 -3.000000 2.000000 -1.000000 0.000000 и т.д.

Не нулевые значения в чаще всего находятся в первой половине вектора. Блоксхема алгоритма встраивания представлен на рисунке 2.

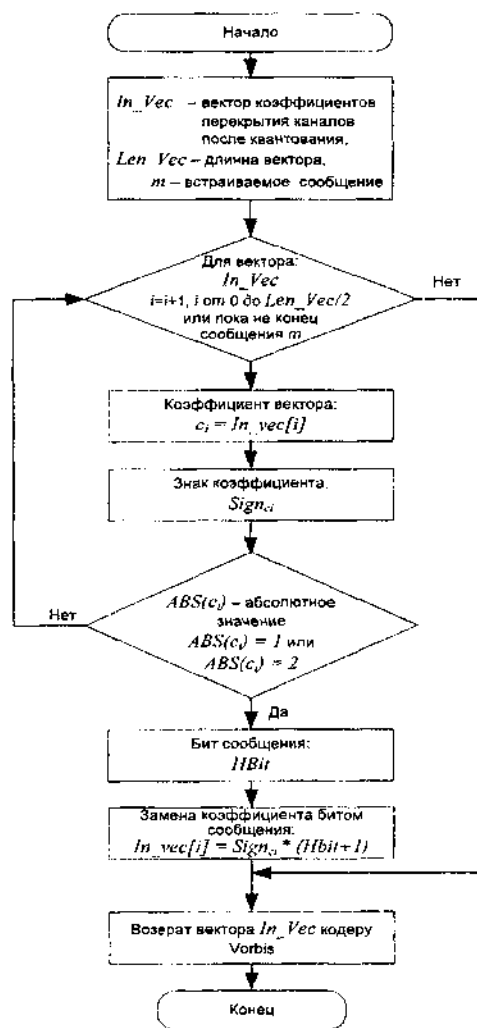


Рис. 2. Алгоритм встраивания бит сообщения

Согласно алгоритму замене подвергается один коэффициент из одного вектора *Couple*. На вход процедуры встраивания подается сам вектор, его длина и встраиваемое

сообщение. В цикле выполняется обход вектора с нулевой позиции до половины, т.к. далее все значения будут нулевыми. На каждой итерации цикла производится проверка на равенство абсолютного значения коэффициента единице или двум. Эти числа выбраны т.к. они чаще встречаются в этих векторах. Для первого коэффициента удовлетворяющему этому условию выполняется замена этого коэффициента на значение бита сообщения увеличенного на 1 и принимающего знак заменяемого коэффициента. Т.о. биты кодируются согласно следующей формуле:

$$\begin{cases} Hbit = 0, & \text{при } c_i = \pm 1 \\ Hbit = 1, & \text{при } c_i = \pm 2 \end{cases} \quad (1.1)$$

Извлечение производится в той же последовательности с учетом того что бит числа равен абсолютному значению коэффициента минус 1.

Выбранный алгоритм позволяет встраивать до 1,5 кВ сообщения в аудио файл длиной 5 мин с битрейтом 141 kbps. При этом пустой и заполненный результирующий контейнер ogg имеют практически одинаковый размер (разница составляет порядка 15 – 20 байт).

4 ЗАКЛЮЧЕНИЕ

Разработанный адаптивный алгоритм позволяет скрывать данные в уже сжатый по алгоритму компрессии OGG Vorbis файл, что снижает вероятность повреждения сообщения. Кроме того встраивание происходит адаптировано к конкретному вектору представляющему часть сигнала, при этом вносятся малые, практически не воспринимаемые человеческим слухом искажения в исходный сигнал.

ЛИТЕРАТУРА

- [1] Проект Xiph.org OGG [Электронный ресурс] – Электронные данные. – Режим доступа: <http://xiph.org/ogg/doc/>. – Дата доступа: 14.10.2009.
- [2] Проект Xiph.org Vorbis [Электронный ресурс]. – Электронные данные. – Режим доступа: <http://xiph.org/vorbis/doc/>. – Дата доступа: 14.10.2009.
- [3] Technical report – Ogg Vorbis: Subjective assessment of sound quality at very low bit rates [Электронный ресурс]. – Электронные данные. – Режим доступа: <http://www.cesnet.cz/doc/techzpravy/2006/vorbis/>. – Дата доступа: 14.10.2009.
- [4] [vorbis] encoder block diagram [Электронный ресурс] – Электронные данные. – Режим доступа: <http://lists.xiph.org/pipermail/vorbis/2003-March/010201.html>. – Дата доступа: 14.10.2009.