УДК 681.4

ВСТРАИВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АУДИОСИГНАЛ МЕТОДОМ РАСШИРЕНИЯ СПЕКТРА

А.Г. Коробейников, А.Г. Даурских, Н.В. Павлова

В работе рассмотрен стеганографический метод внедрения цифровых водяных знаков в аудиосигнал, а также шаги по его практической реализации. Приведена структура работы алгоритма кодирования и декодирования сообщения.

Ключевые слова: стеганография, аудиосигнал, метод, цифровой водяной знак, расширение спектра.

Введение

Повсеместное применение компьютерных технологий способствует активному использованию мультимедийной информации, т.е. информации, содержащей звуки, неподвижные изображения, текст, видеоизображения. Легкость распространения такой информации заставляет задумываться о защите авторских прав в каждом из названных видов мультимедийного контента. Из наиболее эффективных способов такой защиты стоит отметить использование методов стеганографии, т.е. встраивания в мультимедийные данные так называемых цифровых водяных знаков (ЦВЗ) – цифровых меток, не видимых без специального программного обеспечения и секретного ключа.

Для каждого вида данных существуют свои методы встраивания ЦВЗ, в которых используются определенные свойства этих данных. Так, для аудиосигналов применяются алгоритмы, основанные на особенностях самих сигналов и системы слуха человека (ССЧ). ССЧ работает в сверхшироком динамическом диапазоне – более чем миллиард к одному в диапазоне мощности и более чем тысяча к одному в частотном диапазоне. Кроме этого, высокой является и чувствительность к аддитивному флуктуационному (белому) шуму. Отклонения в звуковом файле могут быть выявлены вплоть до одной десятимиллионной (на 70 дБ ниже уровня внешних шумов) [1].

Несмотря на это, существуют определенные возможности для скрытия информации в аудиосреде. Хотя ССЧ и имеет широкий динамический диапазон, она характеризуется достаточно малым разностным диапазоном. Как следствие, громкие звуки содействуют маскировке тихих звуков. Кроме того, ССЧ не способна различать абсолютную фазу, распознавая только относительную. Наконец, существуют некоторые виды искажений, вызванных окружающей средой, которые настолько обычны для слушателя, что в большинстве случаев им игнорируются [2].

В работе рассмотрена практическая реализация одного из таких методов, работающего во временно́й области – метода кодирования с расширением спектра.

Описание алгоритма

В стандартном канале связи нередко бывает желательным сосредоточить информацию в как можно более узком диапазоне частотного спектра, например, чтобы сохранить имеющуюся полосу пропускания и уменьшить мощность сигнала. С другой стороны, основной метод расширения спектра предназначен для шифрования потока информации путем «рассеивания» кодированных данных по всему возможному частотному спектру. Последнее делает возможным прием сигнала даже при наличии помех на определенных частотах.

В работе рассматривается алгоритм расширения спектра прямой последовательностью (РСПП). Методы РСПП расширяют сигнал данных (сообщения), умножая его на элементарную посылку – псевдослучайную последовательность максимальной длины, модулированную известной частотой.

Поскольку аудиосигналы, используемые в качестве контейнеров, имеют дискретный формат, то для кодирования в качестве элементарной посылки можно использовать частоту дискретизации. Как следствие, дискретный характер сигнала устраняет наиболее сложную проблему, которая возникает при получении сигнала с расширенным прямой последовательностью спектром, – корректное определение начала и конца составляющих элементарной посылки с целью фазовой синхронизации. Следовательно, возникает возможность использования намного более высокой частоты следования элементарных посылок и, таким образом, получения значительной скорости передачи данных. Кроме этого, также могут применяться разнообразные алгоритмы блокирования сигнала, однако в вычислительном плане они являются достаточно сложными.

В РСПП для шифрования и дешифрования информации необходим один и тот же ключ – псевдослучайный шум, который в идеальном случае имеет плоскую частотную характеристику во всем диапазоне частот (так называемый белый шум). Ключ применяется к скрываемой информации и трансформирует ее последовательность в последовательность с расширенным спектром.

Метод РСПП по отношению к аудиосигналам заключается в следующем. Сигнал данных умножается на сигнал несущей и псевдослучайную шумовую последовательность, характеризующуюся широким частотным спектром. В результате этого спектр данных расширяется на всю доступную полосу. В дальнейшем последовательность расширенных данных ослабляется и прибавляется к исходному сигналу как аддитивный случайный шум (рис. 1).

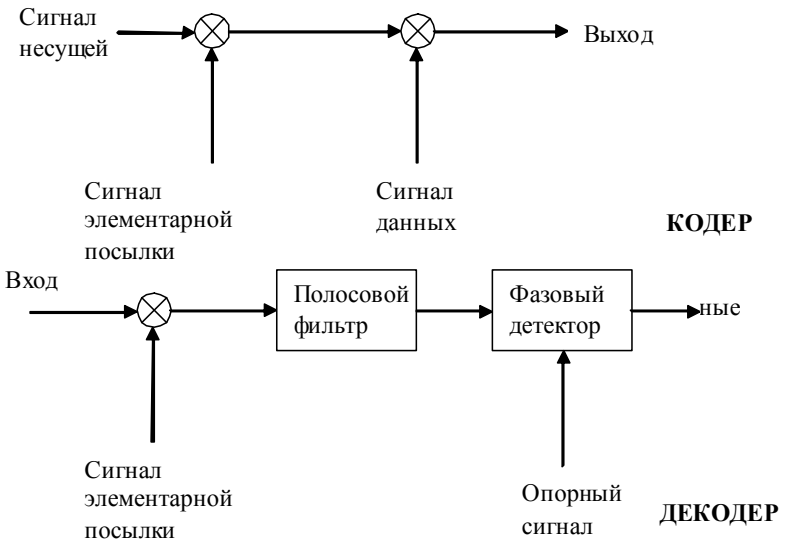

Рис. 1. Структурная схема кодека с расширением спектра

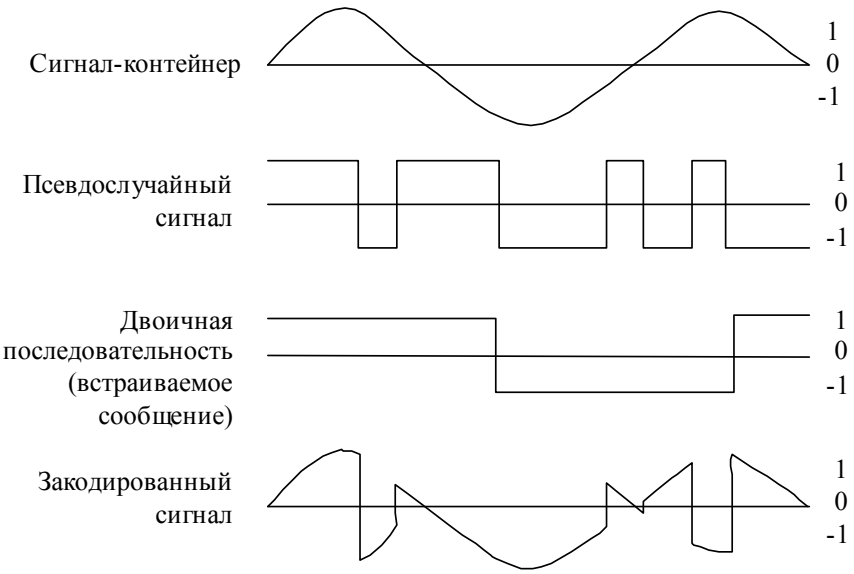

Рис. 2. Информация, синтезированная расширением спектра и шифрованная методом прямой последовательности

РСПП использует двоичную фазовую манипуляцию, поскольку фаза сигнала псевдослучайной последовательности поочередно чередуется с фазой, модулированной двоичной последовательностью сообщения (рис. 2). На стадии извлечения фазовые значения φ_0 и $\varphi_0 + \pi$ интерпретируются, соответственно, как биты «1» и «0», которыми кодировалась двоичная последовательность данных. При этом предусматривается следующее:

– псевдослучайный ключ представляет собой *M*-последовательность (т.е. имеет максимально возможное количество комбинаций, которые равномерно распределены в заданном диапазоне и максимально долго не повторяются). Следовательно, он имеет относительно плоский частотный спектр;
– принимающей стороне известен поток ключей для шифрования, выполнена синхронизация сигнала, а также известны точки начала и конца расширенных данных;
– принимающей стороне также известны частота следования элементарных посылок, скорость передачи данных и частота (вид) несущей.

Объединение несложной техники повторения и кодирования с исправлением ошибок позволяет гарантировать целостность двоичной последовательности. Короткие сегменты двоичной кодовой комбинации объединяются и складываются с сигналом аудиоконтейнера таким образом, чтобы уменьшить шумы переходных процессов. Для этого в процессе декодирования проводится усреднение по всему сегменту.

Реализация алгоритма

Реализация представленного метода кодирования расширением спектра с помощью прямой последовательности имеет следующие этапы.

Шаг 1. Начальные данные:

– считанные и подготовленные аудиоданные из звукового файла, выбираемого пользователем; длина данных I (в качестве контейнера выберем левый канал стереофайла);
– введенное пользователем сообщение M длиной L_M бит.

Для встраивания L_M-битового сообщения в контейнер, имеющий I дискретных отсчетов, последний разобьем на L_M сегментов длиной

$SegLen = Math.Floor(I)$,

где *Math.Floor*() – функция отсечения дробной части (округление до целого числа в меньшую сторону). Каждый сегмент будет предназначен для встраивания одного бита сообщения.

Шаг 2. Для каждого бита сообщения необходимо сгенерировать псевдослучайную последовательность в виде последовательности ± 1 длиной, как минимум, *seglen* элементов. За основу генератора псевдослучайных чисел можно взять регистр сдвига с линейной обратной связью (РСЛОС). Как известно, РСЛОС состоит из двух частей – собственно регистра сдвига и функции обратной связи (рис. 3). Регистр сдвига представляет собой последовательность битов (разрядов) *r*, количество которых *d* определяется длиной регистра сдвига. Обратная связь представляет собой сумму по модулю 2 определенных битов регистра (эти биты называются отводной последовательностью) [3].

Теоретически *d*-битовый РСЛОС может пребывать в одном из $2^d - 1$ внутренних состояний, т.е. может генерировать псевдослучайную последовательность с периодом в $T = 2^d - 1$ бит. Все *T* внутренних состояний регистр пройдет только при определенных отводных последовательностях. Такие РСЛОС имеют максимальный период, а полученный при этом результат называют *M*-последовательностью**.** На рис. 3 значения μ_i (i = 0, 1, …, d) являются весовыми коэффициентами полинома степени *d*, ассоциированного с последовательностью:

$$p(x) = \mu_0 x^0 + \mu_1 x^1 + ... + \mu_{d-1} x^{d-1} + \mu_d x^d .$$

Если $\mu_i = 1$, то соответствующий ключ замкнут, в случае $\mu_i = 0$ – разомкнут.

Неудачное включение сумматоров в цепь обратной связи может привести к получению псевдослучайной последовательности, период повторения которой будет меньше максимально возможного при имеющейся разрядности регистра. Чтобы конкретный РСЛОС имел максимальный период, полином $p(x)$ должен быть примитивным по модулю 2 (т.е. не раскладываться на произведение двоичных полиномов меньшей степени). При этом коэффициенты μ_0 и μ_d всегда равняются 1, поскольку, в случае $\mu_0 = 0$, полином $p(x)$ делится на μ_1 и не является примитивным. Другие коэффициенты выбранного полинома и будут определять схему формирования псевдослучайной последовательности.

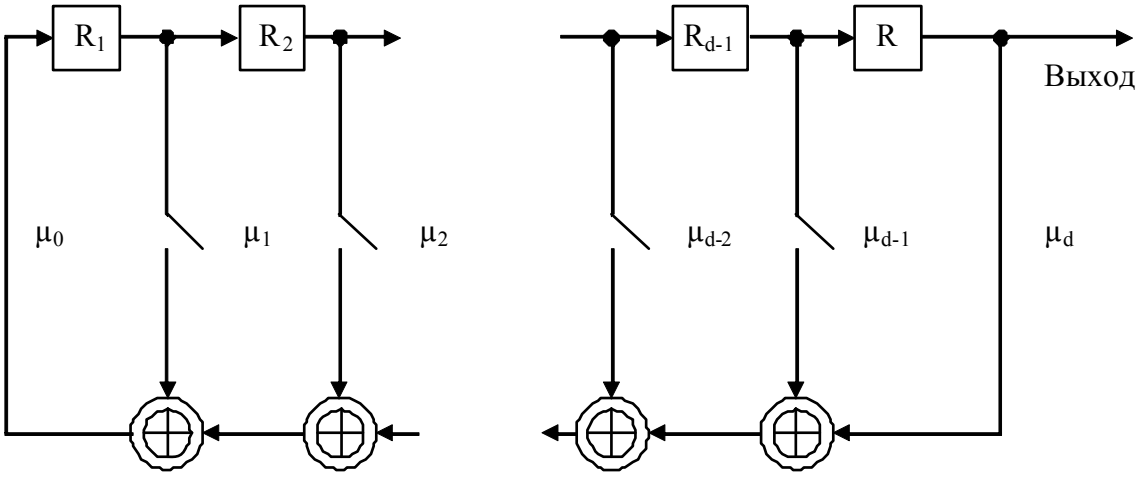

Рис. 3. Обобщенная схема работы регистра сдвига с линейной обратной связью

В нашем случае достаточное количество разрядов регистра составляет

d=*Math.Ceiling*(*Log*2(*SegLen*)),

где *Math.Ceiling*() – функция округления до целого числа в бóльшую сторону. При этом период генерируемой псевдослучайной последовательности составит

$2^d - 1 > SegLen$**.**

Результирующая последовательность определяется наименьшим значащим битом состояния регистра. Руководствуясь достаточностью, процесс генерации длится до получения *SegLen* битов псевдослучайной последовательности. На выходе модуля получается последовательность {0, 1}, преобразованная в последовательность {−1, 1}.

Шаг 3. На этом этапе выполняется непосредственно встраивание битов сообщения в контейнер. Вначале строка символов сообщения преобразовывается в вектор значений {−1, 1}. На этом этапе можно также применить какой-либо криптографический метод для шифрования встраиваемого сообщения.

Далее весь контейнер делится на количество сегментов равной длины, соответствующее количеству битов во встраиваемом сообщении, т.е. для одного бита сообщения отводится один сегмент. Каждый полученный бит накладывается с помощью соответствующей сгенерированной псевдослучайной последовательности на один сегмент исходного контейнера путем модификации каждого 16-битного отсчета внутри сегмента. При этом энергию ЦВЗ задает параметр *alpha*. Он выбирается исходя из требований стойкости встраиваемого ЦВЗ и незаметности модификации носителя. Этот параметр можно рассматривать как уровень шума (в процентах), вносимого при встраивании сообщения, по отношению к исходному сигналу. Рекомендуемое значение – порядка 0,01 (что соответствует примерно 1 % искажения исходного контейнера).

Модифицированные сегменты далее объединяются в общий вектор. После встраивания последнего бита сообщения это вектор удлиняется до длины исходного сигнала конечными, не претерпевшими модификации элементами начального контейнера. При большом значении параметра *alpha* увеличивается вносимый в исходный контейнер аддитивный шум, что приводит к ощутимым на слух искажениям, которые также можно наблюдать на временных диаграммах.

После встраивания ЦВЗ измененный контейнер объединяется со вторым немодифицированным каналом и записывается в WAV-файл.

Шаг 4. Процесс извлечения заключается в следующем. После открытия файла, содержащего ЦВЗ, из массива данных выделяется левый (первый) канал, в который было произведено встраивание. Принимающая сторона должна иметь оригинальный аудиофайл, из которого тоже извлекается соответствующий аудиоканал. Известным также должно быть число *SegLen*, представляющее количество 16-битных отсчетов в одном сегменте.

Считывание ЦВЗ производится с использованием той же псевдослучайной последовательности, что и при встраивании сообщения в сигнал. Определение закодированного значения «0» или «1» происходит на основе анализа разницы между исходным и модифицированным сигналами. Поочередно анализируются все сегменты. В качестве определяющего фактора выступает знак разницы сигналов: если он отрицателен, то встроено значение «0», если положителен – значение «1». Сравнение производится по усредненным значениям всего сегмента, что повышает стойкость к помехам, которые могут возникнуть при передаче сигнала.

В случае применения криптографической защиты при встраивании сообщения извлеченные данные расшифровываются.

Заключение

В работе рассмотрены основные шаги практической реализации алгоритма встраивания ЦВЗ в аудиосигнал методом расширения спектра прямой последовательностью. Выбранный алгоритм имеет отличные показатели скрытности и устойчивости к преобразованию.

Стоит отметить, что применение комбинированных методов защиты – криптографических и стеганографических – является удачным решением, повышающим стой-

кость встроенных данных к обнаружению, модификации, уничтожению, обеспечивая защиту данных одновременно на нескольких уровнях.

Перспективы развития стеганографических методов защиты авторских прав предполагают их дальнейшее изучение с целью увеличения скрытности и стойкости встраиваемой информации, в то время как развитие стегоанализа направлено на поиски новых методик детектирования скрытой информации, ее извлечения и удаления.

Литература

1. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding // IBM Systems Journal. – 1996. – № 35 (3 & 4). – P. 313–336.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. – Киев: МК-Пресс, 2006. – 288 с., ил.
3. Скляр Б. Цифровая связь: Теоретические основы и практическое применение. – 2-е изд., исправл. – М.: Вильямс, 2003. – 1104 с.

Коробейников Анатолий Григорьевич	—	Институт земного магнетизма, ионосферы и распространения радиоволн РАН, заместитель директора, доктор технических наук, профессор, Korobeynikov_A_G@mail.ru
Даурских Александр Геннадьевич	—	Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, sanya219@gmail.com
Павлова Надежда Валерьевна	—	Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, pavlovanv@yahoo.com