УДК 519.7

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ БОЛЬШИХ МАССИВОВ ИНФОРМАЦИИ ПУТЕМ СТЕГОКОДИРОВАНИЯ ЗВУКОВЫХ И ГРАФИЧЕСКИХ ФАЙЛОВ

Андрианова О.С., Губенко Н.Е.
Донецкий национальный технический университет

У роботі розглянуто проблему захисту авторських прав на WAV-файли за допомогою засобів стеганографії. Розглянуто модифікацію методу кодування з розширенням спектру, що використовує функції вейвлет-перетворювань.

Развитие и повсеместное распространение сетевых методов общения стимулирует желание скрыть от чужих глаз передаваемую информацию, что, в свою очередь, заставлять искать новые методы сокрытия данных в информационных каналах. Вторая проблема – это защита авторских прав на мультимедийную продукцию. Одним из способов решения данной проблемой является использование водяных знаков, подтверждающих авторство произведения [1].

Особенно эффективным решением для подтверждения авторских прав на мультимедийную продукцию, разрабатываемые файлы графических и звуковых форматов является объединение методов компьютерной стеганографии и криптографии.

В данной работе в роли контейнера для передачи секретных текстов или простановки водяных знаков выступает файл в формате WAV, который изначально обладает информационной избыточностью, и это его свойство можно использовать для внедрения большого количества информации без изменения характера его звучания. В данной работе планируется повысить эффективность метода внедрения скрытой информации в звуковые WAV-файлы путем модификации существующих алгоритмов, построенных на базе вейвлет-преобразования вместо традиционного разложения в ряд Фурье [2].

Вейвлеты (wavelets) - это обобщенное название временных функций, имеющих вид волновых пакетов той или иной формы, локализованных по оси независимой переменной (t или x) и способных к сдвигу по ней или масштабированию (сжатию-растяжению). Вейвлеты создаются с помощью специальных *базисных функций* - прототипов, задающих их вид и свойства.

Практика работа с вейвлетами обычно базируется на особой трактовке вейвлет-преобразований в частотной области и позволяет использовать хорошо разработанный аппарат частотной фильтрации и методы быстрого вейвлет-преобразования. Они основаны на

пирамидальном алгоритме Маллата и прореживании спектра вейвлетов по частоте [3].

Рассмотрим подробнее метод кодирования с расширением спектра. ЦВЗ (цифровой водяной знак) внедряется в аудиосигналы (последовательности 8- или 16-битных отсчетов) путем незначительного изменения амплитуды каждого отсчета. Для обнаружения ЦВЗ не требуется исходного аудиосигнала. Пусть аудиосигнал состоит из N отсчетов $x(i)$, $i = 1, \ldots, N$, где значение N не меньше 88200 (соответственно 1 секунда для стереоаудиосигнала, дискретизированного на частоте 44,1 кГц). Для того, чтобы встроить ЦВЗ, используется функция $f(x(i), w(i))$, где $w(i)$ - отсчет ЦВЗ, изменяющийся в пределах $[-\alpha; \alpha]$, α - некоторая константа. Функция f должна учитывать особенности системы слуха человека во избежание ощутимых искажений исходного сигнала. Отсчет результирующего сигнала получается следующим образом:

$$y(i) = x(i) + f(x(i), w(i)) \tag{1}$$

Отношение сигнал-шум в этом случае вычисляется как

$$SNR = 10 \log_{10} \frac{\sum_n x^2(n)}{\sum_n \left[x(n) - y(n)\right]^2} \tag{2}$$

Обнаружение ЦВЗ происходит следующим образом. Обозначим через S следующую сумму:

$$S = \sum_{i=1}^{N} y(i) w(i). \tag{3}$$

Комбинируя (1) и (3), получаем

$$S = \sum_{i=1}^{N} \left[x(i) w(i) + f(x(i), w(i)) w(i)\right]. \tag{4}$$

Первая сумма в (4) равна нулю, если числа на выходе ГСЧ распределены равномерно и математическое ожидание значения сигнала равно нулю. В большинстве же случаев наблюдается некоторое отличие, обозначаемое $w\Delta$, которое необходимо также учитывать. Следовательно, (4) принимает вид

$$S = \sum_{i=1}^{N-\Delta w} x(i) w(i) + \sum_{i=1}^{\Delta w} x(i) w(i) + \sum_{i=1}^{N} f(x(i), w(i)) w(i). \tag{5}$$

Для упрощения алгоритма, а следовательно для сокращения объема вычислений, проанализируем структуру формулы (5). Сумма $\sum_{i=1}^{N-\Delta w} x(i) w(i)$, как показано выше, приблизительно равна нулю. Если в аудиосигнал не был внедрен ЦВЗ, то S будет приблизительно равна

$\left|\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i)\right|$. С другой стороны, если в аудиосигнал был внедрен ЦВЗ, то S будет приблизительно равна $\left|\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i) + \sum_{i=1}^{N} f(x(i), w(i))w(i)\right|$.

Однако, это исходный сигнал, который по условию не может быть использован в процессе обнаружения ЦВЗ. Сигнал x(i) можно заменить на y(i), это приведет к замене $\sum_{i=1}^{\Delta w} x(i)w(i)$ на $\frac{\Delta w}{N} S$. Следовательно, вычитая величину $\frac{\Delta w}{N} S$ из S, и деля результат на $\sum_{i=1}^{N} f(y(i), w(i))w(i)$, получим результат r, нормированный к 1. Детектор ЦВЗ, используемый в этом методе, вычисляет величину r, задаваемую формулой

$$r \hat{=} \left|\frac{S - \frac{\Delta w}{N}|S|}{\sum_{i=1}^{N} f(y(i), w(i))w(i)}\right|. \quad (6)$$

Пороговая величина обнаружения теоретически лежит между 0 и 1, с учетом аппроксимации этот интервал сводится к [0 - ε; 1 + ε]. Опытным путем установлено, что для того чтобы определить действительно ли определенный ЦВЗ находится в сигнале, пороговое значение ЦВЗ должно быть выше 0,7. Работа кодера и декодера представлены на рис.1.

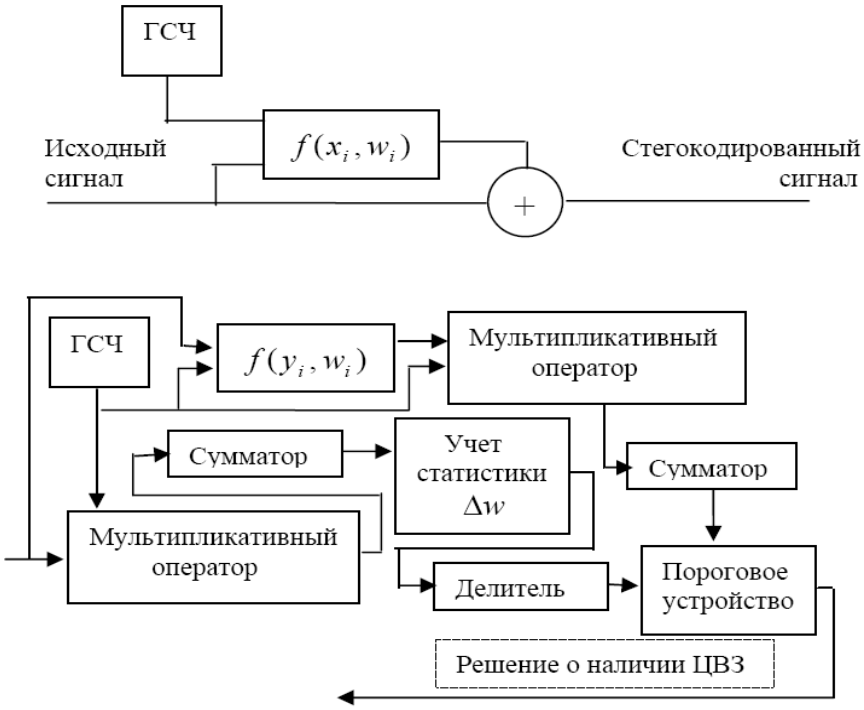

Рис.1. Схема стегокодирования и декодирования

При оценке стойкости разработанного метода к атакам пассивного злоумышленника одной из важных характеристик является оценка вероятности восстановления скрытого сообщения. Было установлено[3], что извлечение информации в отсутствие сведений об использованном вейвлете невозможно.

Таким образом, предложенный метод сокрытия информации в звуковых файлах позволяет сократить объем вычислений, повысить стегостойкость контейнера и не дает возможности выделения ЦВЗ без знания формулы вейвлет-преобразования. Этот метод может быть распространен и на встраивание информации в графические контейнеры распространенных форматов.

Литература

1. Варламов О.О. Системный подход к созданию модели компьютерных угроз информационной безопасности. Таганрог: Издательство ТРТУ, 2004. 61-65 с.
2. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB. К.: ООО ТИД ДС, 2004. 92с.
3. В. Г. Грибунин, И.Н. Оков, И. В. Туринцев. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 261 с.

Получено 25.05.09