УДК 519.7

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ БОЛЬШИХ МАССИВОВ ИНФОРМАЦИИ ПУТЕМ СТЕГОКОДИРОВАНИЯ ЗВУКОВЫХ ФАЙЛОВ

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

Проблема защиты информации неразрывно связана с существованием человечества и общением людей между собой. Ведь предприятия, банки, частные лица хотят не только передавать информацию друг другу, но и защитить ее от посторонних глаз. Так возникла стеганография, направление защиты информации, при котором сообщение кодируется с помощью различных алгоритмов, которые известны лишь передающей и принимающей информацию стороне [1].

Актуальность проблемы скрытой передачи данных постоянно растет и стимулирует поиск новых методов защиты информации. Развитие информационных технологий стимулирует широкое использование цифровых фотографий, графических файлов, dvd фильмов, музыки в формате mp3, WAV. В связи с этим возник практический смысл защиты информации. В настоящее время проходит борьба с незаконным воспроизведением музыкальных произведений. Таким образом при использовании музыкальных файлов нарушается закон об авторских правах на музыкальное произведение. Одним из способов решения данной проблемой является использование водяных знаков, подтверждающих авторство произведения. [2].

Весьма характерной тенденцией в настоящее время в области защиты информации является внедрение криптологических методов. Однако на этом пути много ещё нерешенных проблем, связанных с разрушительным воздействием на криптосредства. Объединение методов компьютерной стеганографии и криптографии, графических и звуковых файлов явилось хорошим

выходом из создавшегося положения.

Обычно стеганографические методы применяют для защиты авторских прав и цифровых подписей. В данной работе музыкальный WAV-файл выступает не в роли объекта защиты, а в роли контейнера для передачи секретных текстов, причем текстов большого размера, ведь в WAV-формате изначально содержится много избыточной информации, которую можно заменить незаметно для человеческого уха. Планируется повышение эффективности методов внедрения скрытой информации в звуковые WAV-файлы путем модификации существующих алгоритмов и разработки программных модулей. А так же применение вейвлет-преобразования вместо разложения Фурье [3].

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 плодотворно использовать хорошо разработанный и давно известный аппарат частотной фильтрации и методы быстрого вейвлет-преобразования. Они основаны на пирамидальном алгоритме Маллата и прореживании спектра вейвлетов по частоте [4].

Рассмотрим подробнее метод кодирования с расширением спектра. ЦВЗ (цифровой водяной знак) внедряется в аудиосигналы (последовательность 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, …, 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 [-α; α], α - некоторая константа. Функция f должна принимать во внимание 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

$$SNR = 10 \cdot \log_{10} \left(\frac{\sum_n x2(n)}{\sum_n \left[x(n) - y(n) \right]^2} \right). \tag{2}$$

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 wΔ, которое необходимо также учитывать. Следовательно, (4) принимает вид

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

Первое слагаемое, как показано выше, приблизительно равно нулю. Если в аудиосигнал не был внедрен ЦВЗ, то значение S будет приблизительно равно

$$\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i). \qquad (6)$$

С другой стороны, если в аудиосигнал был внедрен ЦВЗ, то S будет приблизительно равна

$$\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i) + \sum_{i=1}^{N} f(x(i), w(i))w(i). \qquad (7)$$

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

$$\sum_{i=1}^{\Delta w} x(i)w(i) \to \frac{\Delta w}{N} S, \qquad (8)$$

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

$$r \cong \frac{S - \frac{\Delta w}{N}|S|}{\sum_{i=1}^{N} f(y(i), w(i))w(i)}. \qquad (9)$$

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.

Предложенный метод позволяет сохранять встроенную информацию при конвертировании в формат WAV файла. При оценке стойкости разработанных методов стеганографии к атакам пассивного злоумышленника одной из важных характеристик

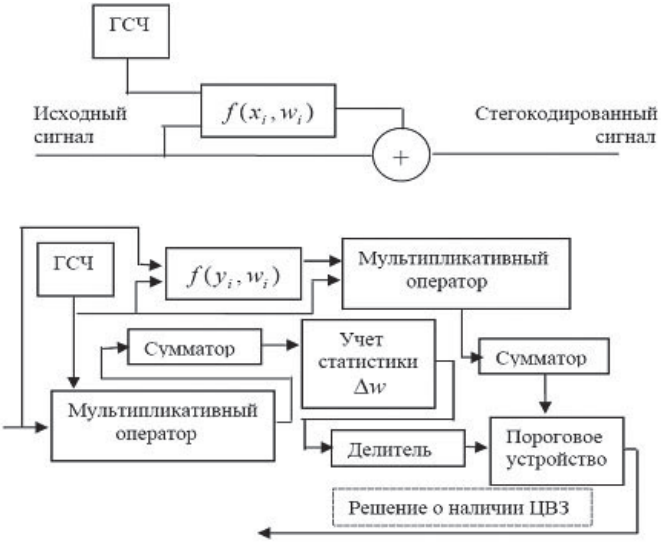

Рисунок 1 – Схема стегокодирования и декодирования

является оценка вероятности восстановления скрытого сообщения. Было установлено, что извлечение информации в отсутствие сведений об использованном вейвлете невозможно.

Литература

[1] Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. - 384 с.

[2] Варламов О.О. Системный подход к созданию модели компьютерных угроз информационной безопасности. Таганрог: Издательство ТРТУ, 2004. С. 61-65.

[3] Домарев В. В. Безопасность информационных технологий. Системный подход. К.: ООО ТИД ДС, 2004. 992с.

[4] Грибунин В.Г., Оков И.Н., Туринцев И.В.. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. - 261 с.