Тел.: +7 (961) 27-23-100.
Кафедра безопасности информационных технологий; аспирант.

Maro Ekaterina Aleksandrovna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: maro-kat@yandex.ru.
Block "I", 2, Chehov str., Taganrog, 347928, Russia.
Phone: +7 (961) 27-23-100.
The Department of Security of Information Technologies; post-graduate student.

УДК 681.3.067

Д.П. Рублёв, О.Б. Макаревич, В.М. Федоров

МЕТОД СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ СООБЩЕНИЙ В АУДИОДАННЫЕ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ*

Предлагается стеганографический метод встраивания бинарных сообщений в аудиоданные, основанный на модификации вейвлет-коэффициентов, предназначенный для сокрытия двоичных данных в оцифрованных речевых сообщениях. Встраивание осуществляется модуляцией коэффициентов вейвлет-преобразования, что позволяет повысить стойкость скрытых сообщений к преобразованию формата хранения аудиоданных в форматы с потерей качества.

Стеганография; вейвлет-преобразование; корреляция; робастные стегосистемы.

D.P. Rublev, O.B. Makarevich, V.M. Fedorov

STEGANOGRAPHICAL METHOD FOR MESSAGES EMBEDDING TO AUDIODATA BASED ON THE WAVELET-TRANSFORM

We propose a steganographical method of binary messages embedding to audio data based on wavelet coefficient modifying, which is intended to hide binary data in digitized speech messages. Embedding in performed via wavelet coefficients modulation which allows to achieve robustness to lossy compression schemes

Steganography; wavelet transform; correlation; robust stegosystems.

В связи с широким распространением сетевых средств передачи мультимедийной информации, в частности, голосового трафика в IP телефонии и трафика видеоданных, актуальным является построение на их основе потоковых стегосистем. Применение в составе стегосистемы методов стеганографии, использующих модификацию наименее значимых бит (НЗБ) исходных мультимедиа-данных ограничивается тем, что передача практически всех потоков мультимедиа-данных ведётся с применением того или иного метода сжатия, основанного на психофизиологической модели восприятия человека, то есть варианта сжатия с потерями. В частности, если рассматривать оцифрованную речь как один из наиболее распространённых источников мультимедиа-трафика, то в зависимости от области

* Работа выполнена при поддержке гранта РФФИ № 09-07-00242-а

применения используется либо один из вариантов адаптивной модуляции, либо специализированные речевые кодеры на основе вокодерных и гибридных схем. Также при скрытии сообщений в аудиопотоке необходимо учитывать возможность его промежуточной перекодировки в другой формат либо умышленных искажений для стирания предполагаемых встроенных сообщений. В таком случае использование множества НЗБ-методов стеганографии оказывается неэффективным и особую значимость приобретают методы стеганографии, позволяющие производить встраивание сообщений в области, которые не могут подвергаться существенным искажениям при обработке современными кодерами. Одним из преобразований, позволяющих осуществить подобное встраивание, является дискретное вейвлет-преобразование [1].

Набор вейвлетов, в их временном или частотном представлении, может приближать сложный сигнал или изображение, причем как идеально точно, так и с некоторой погрешностью. Вейвлеты имеют явные преимущества в представлении локальных особенностей функций и неявном учёте особенностей психофизиологической модели восприятия. Благодаря этому они широко используются для анализа особенностей, сжатия и реконструкции сложных сигналов [2].

При разработке метода стеганографии, ориентированного на достижение максимальной пропускной способности (скрытая передача и хранение информации), основными задачами являются минимизация вносимых искажений и устойчивость к атакам пассивного злоумышленника [3].

Как известно, набор вейвлетов, в их временном или частотном представлении, может приближать сложный сигнал или изображение, причем как идеально точно, так и с некоторой погрешностью. При разработке метода стеганографии, ориентированного на достижение максимальной пропускной способности (скрытая передача и хранение информации) применением дискретного вейвлет-преобразования можно решить основные задачи стеганографии, а именно: минимизацию вносимых искажений за счёт распределения энергии встраиваемого сообщения по множеству масштабов и стойкость к атакам активного злоумышленника.

Методы встраивания сообщений в области вейвлет-коэффициентов изображений и звуковых данных были предложены в [4, 5]. Основным отличием от методов встраивания в наименее значимые биты, как непосредственной заменой, так и при использовании техник кодирования, является то, что сокрытие при помощи модификации вейвлет-коэффиициентов производится в области вейвлет-преобразования, что обеспечивает дополнительный уровень скрытности, так как для восстановления сообщения необходимо знание использованного при встраивании вейвлета [5].

Выделение области встраивания производится при помощи усовершенствованного алгоритма Маллата [3] декомпозицией сигнала s, содержащегося в аудиофайле. Для этого нормированный сигнал подаётся на фильтры декомпозиции низких и высоких частот, после чего с помощью операции децимации формируются массивы коэффициентов аппроксимации и детализирующих коэффициентов на выходе фильтров на выходе низких и высоких частот (рис. 1). Таким образом, в результате декомпозиции на глубину L на выходе получаются коэффициенты 2^L субполос по $\frac{N}{2^L}$ коэффициентов в полосе. Полученные в результате декомпозиции коэффициенты субполос являются пространством встраивания. Восстановление сигнала производится заменой прямого дискретного вейвлет-преобразования на обратное и прохождением этапов декомпозиции в обратном порядке.

Для установления минимально необходимой глубины разложения, при которой субъективные искажения качества практически не воспринимаются, были проведены эксперименты по встраиванию информации в частотные субполосы различных уровней с последующим восстановлением в аудиофайлы.

Встраивание сообщений в наименее значимые биты при отсутствии модификации контейнера позволяет восстановить неповреждённое исходное сообщение. В отличие от встраивания в область НЗБ, встраивание сообщений в области вейвлет-преобразования даже при отсутствии искажений контейнера вносит несколько типов ошибок.

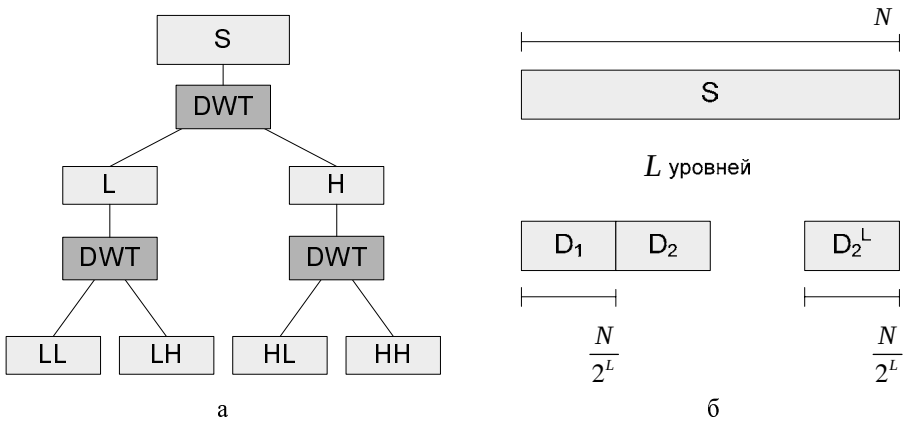

Рис. 1. Декомпозиция при помощи расширенного алгоритма Маллата на глубину 2 (а) и результат декомпозиции N отсчётов сигнала на глубину L (б)

При встраивании сигнала в области вейвлет-коэффициентов возникают ошибки округления, ошибки квантования и ошибка компрессии. Ошибка округления возникает вследствие конечной точности вычислений с плавающей точкой, ошибка квантования обуславливается квантованием при преобразовании отсчёта звукового файла в целочисленное значение, ошибка компрессии возникает ввиду искажений, вносимых этапом компрессии в исходный звуковой сигнал. При совмещении этапов встраивания и компрессии, при котором кодеку передаются отсчёты сигнала непосредственно после встраивания, искажения обусловлены только ошибкой округления. При встраивании во внешние звуковые файлы, являющиеся промежуточным звеном в преобразовании формата, ошибка округления и ошибка квантования суммируются. Графики ошибок округления при встраивании бинарного сообщения в звуковые файлы при изменяющихся пороге и субполосе встраивания приведены на рис. 2 и в табл. 1 для двух различных сигналов. На графике 2 по оси Z отложено значение нормированной ошибки, по осям X и Y соответственно номера субполос и коэффициент встраивания, определяющий энергию сигнала-сообщения. Из графика видно, что ошибка округления существенно зависит от субполосы встраивания.

При встраивании сообщений в цифровые аудиопотоки, которые могут в дальнейшем быть конвертированы в другой формат, необходимо учитывать высокую вероятность применения оконной обработки, и, как следствие, возможность потери синхронизации при дополнении окон в кодере дополнительными отсчётами.

Схема встраивания реализуется в соответствии с рис. 3, а извлечения с рис. 4. При встраивании сообщения формируются два отрезка синусоидального сигнала с заданной длиной окна и периодом колебаний. Встраивание бита производится аддитивно, сложением синусоидальной последовательности с выбранным паттерном.

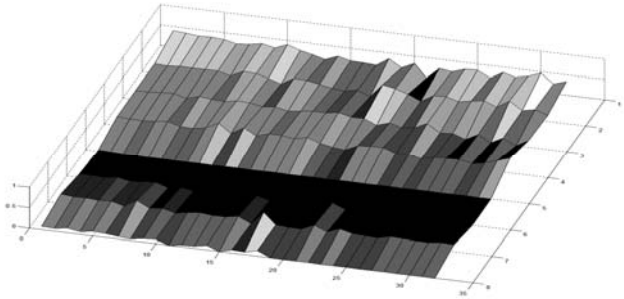

Рис. 2. Ошибка округления при компрессии сигнала (3-й уровень декомпозиции по полному дереву Маллата (8 субполос), длины окон от 128 до 4096)

Таблица 1

Ошибка округления (3-й уровень декомпозиции по расширенному алгоритму Маллата, длины окон от 128 до 4096) при сжатии с потерей качества

Длина окна встраивания	Субполоса декомпозиции							
	1	2	3	4	5	6	7	8
Файл №1								
128	0,4028	0,2346	0,2131	0,2182	0,0350	0,0832	0,2257	0,0813
256	0,3792	0,2179	0,2198	0,2047	0,0321	0,0849	0,1981	0,0670
512	0,3558	0,2385	0,2577	0,2154	0	0,1154	0,1846	0,0673
1024	0,3500	0,3115	0,2077	0,2154	0	0	0,1423	0,0385
2048	0,1833	0,1333	0,2417	0,2833	0	0	0,0750	0,0833
4096	0,3333	0,1500	0,1667	0,3667	0	0	0,1667	0
Файл №2								
128	0,4182	0,2164	0,2079	0,2136	0,0262	0,0893	0,2421	0,0841
256	0,4000	0,2047	0,2292	0,2274	0,0283	0,0877	0,1934	0,0698
512	0,3827	0,2346	0,2558	0,2096	0	0,1308	0,1827	0,0731
1024	0,3654	0,2846	0,2500	0,2231	0	0	0,1385	0,0462
2048	0,2167	0,1417	0,2083	0,2667	0	0	0,0833	0,0833
4096	0,3833	0,1333	0,2500	0,3500	0	0	0,2500	0

В ходе проведённых экспериментов было установлено, что вероятность битовой ошибки составляет порядка единиц процентов, в связи с чем при передаче сообщений, критичных к искажениям, требуются дополнительные меры сохранения целостности информации, такие как корректирующие коды. Повышение стойкости может быть достигнуто модуляцией не одного коэффициента, а окна коэффициентов длины l, а также выбором иного вида модуляции.

Для модуляции окна коэффициентов длины l:

$$w_j^{'} = w_j \cdot b_i, \ \ j = 1..l.$$

Таким образом, для монофонического оцифрованного аудиосигнала частоты дискретизации Fs при встраивании информации в окна коэффициентов длины l

при глубине декомпозиции L пропускная способность стеганографического канала:

$$V = \left\lfloor \frac{\left\lfloor \frac{Fs}{2^L} \right\rfloor}{l} \right\rfloor .$$

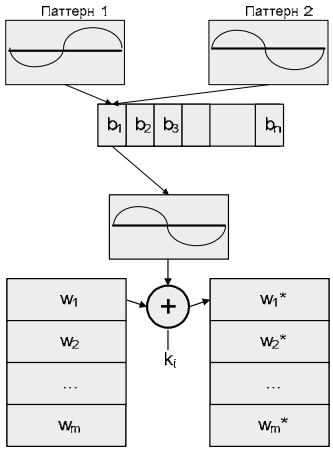

Рис. 3. Схема модификации коэффициентов при встраивании

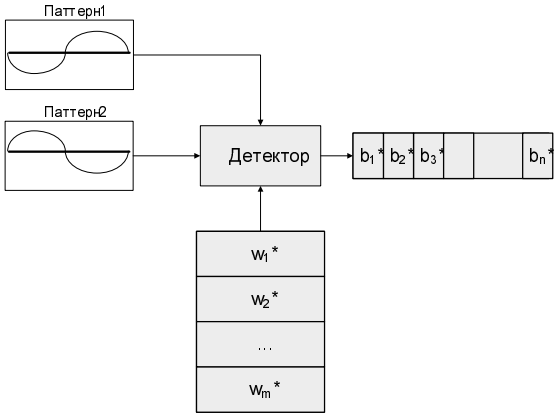

Рис. 4. Извлечение бита сообщения из коэффициентов вейвлет-преобразования

Например, для сигнала частоты дискретизации 8 кГц при длительности 10 секунд и выборе глубины декомпозиции 3 с длиной окна $l = 128$ пропускная способность стегоканала составит 7,8 бит/с на одну субполосу вейвлет-декомпозиции.

Извлечение информации осуществляется нахождением знака коэффициента взаимной корреляции между встроенным и эталонным паттернами:

$$b_i = sign(crosscorr(w_i, Ïàòòåðí1 \quad)) .$$

Значения битовой ошибки при длинах окон от 32 до 4096 и коэффициенте встраивания $\alpha = 0,001$ приведены в табл. 2.

Таблица 2

Вероятность битовой ошибки при квантовании (формат WAV PCM)

Длина окна	Субполоса встраивания							
	1	2	3	4	5	6	7	8
32	0,5065	0,5065	0,4968	0,5009	0,5088	0,5019	0,5032	0,5065
64	0,4963	0,5084	0,4953	0,4935	0,4879	0,5009	0,5084	0,4907
128	0,4645	0,2542	0,2766	0,3056	0,0692	0,1449	0,2953	0,1607
256	0,3019	0,2019	0,2283	0,2604	0,0377	0,1057	0,2000	0,1075
1024	0,1769	0,2308	0,2538	0,1462	0	0,0846	0,2308	0,1538
2048	0,3167	0,1833	0,2167	0,1833	0	0	0,1667	0,2000
4096	0	0	0	0	0	0	0	0

Значения битовой ошибки при длинах окон от 128 до 4096 и коэффициенте встраивания $\alpha = 0,01$ приведены в табл. 3.

Таблица 3

Вероятность битовой ошибки компрессии (формат MPEG-1 Layer 3)

Длина окна	Субполоса встраивания							
	1	2	3	4	5	6	7	8
128	0,2224	0,0486	0,0832	0,0477	0	0,0121	0,0383	0,0150
256	0,0075	0,0509	0,0075	0,0509	0	0	0,0208	0,0132
512	0	0	0,0231	0	0	0	0	0

Зависимость побитовой ошибки от субполосы разложения и выбранного коэффициента усиления при сохранении аудиопотока в формате MPEG-1 Layer 3 кодеком LAME и коэффициенте компрессии 1:10 приведена на рис. 5.

Таким образом, предложенное стеганографическое встраивание сообщений в области коэффициентов вейвлет-преобразования позволяет повысить стойкость скрываемых сообщений к преобразованию формата контейнера в формат с потерей качества MPEG с коэффициентом компрессии 1:10. Исследование предложенного метода показало, что минимальный уровень побитовых ошибок составляет при этом 0,001-0,01 при длине окна встраивания 128 и коэффициенте усиления сигнала сообщения 0,01, что соответствует субъективно невоспринимаемому изменению звучания результирующей записи. Кроме того, установлено, что уровень побитовых ошибок при встраивании существенно зависит от номера субполосы встраивания, оптимальный выбор которого будет осуществлен при дальнейших исследованиях.

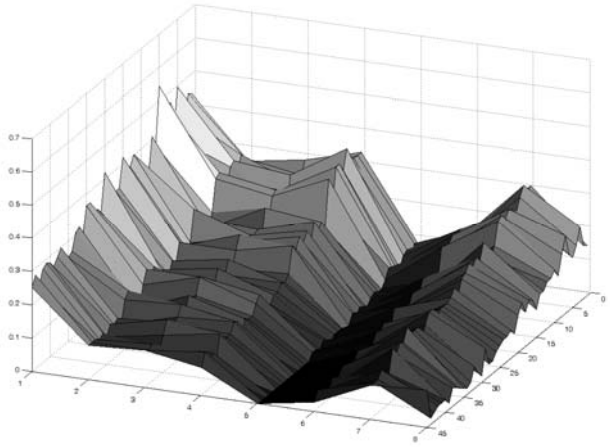

Рис. 5. Зависимость битовых ошибок от субполосы (1-8) и коэффициента усиления сигнала (0,001-0,01)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *J. Fridrich, M. Goljan* "Practical Steganalysis of Digital Images – State of the Art", Security and Watermarking of Multimedia Contents, 2002, vol. SPIE-4675. – P. 1 – 13.

2. *Дьяконов В.П.* Вейвлеты – от теории к практике. – М. СОЛОН-ПРЕСС, 2004. – 440 с.

3. *Maity S.P., Kundu M.K., Mandal M.K.* Capacity improvement in spread spectrum watermarking using biorthogonal wavelet., 48th Midwest Symposium on Circuits and Systems, 2005. Vol. 2. – P. 1426 – 1429.

4. *Рублёв Д.П., Федоров В.М., Макаревич О.Б.* Метод скрытия данных в аудиофайлах, инвариантный к сжатию сигналов // Труды Седьмого международного симпозиума «Интеллектуальные системы», 2006. – С. 417–419.

5. *Федоров В.М., Макаревич О.Б., Рублёв Д.П.* Метод стеганографии в аудиосигналах и изображениях, устойчивый к компрессии с потерями // Материалы VIII Международной научно-практической конференции “Информационная безопасность”, 2006. – С. 201 – 209.

Рублёв Дмитрий Павлович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: rublev-d@yandex.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; ассистент.

Rublev Dmitry Pavlovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: rublev-d@yandex.ru.
2, Chekhova str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
Department of IT-Security; assistant.

Макаревич Олег Борисович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: mak@tsure.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; заведующий кафедрой; профессор.

Makarevich Oleg Borisovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: mak@tsure.ru.
2, Chekhova str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
Department of IT-Security; Head of Department; professor.

Федоров Владимир Михайлович
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: vladmih@rambler.ru.
347928, г. Таганрог, ул. Чехова, 2.
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Fedorov Vladimir Mikhailovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: vladmih@rambler.ru.
2, Chekhova str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
Department of IT-Security; associate professor.

УДК 004.056.053

А.Ф. Чипига

ПОДХОД К РЕШЕНИЮ ПРОБЛЕМЫ СОХРАНЕНИЯ ДАННЫХ ПРИ РАСКРЫТИИ КЛЮЧА ДЕШИФРОВАНИЯ НА ПРИЕМЕ

Раскрыт подход к решению проблемы сохранения данных при компрометации ключа на приеме в одноключевых системах за счет использования физического уровня эталонной модели взаимосвязи открытых систем.

Блочные шифры; размножение ошибок; математическая модель ионосферы; электромагнитная доступность; помехоустойчивость.