УДК 681.3

Д.П. Рублев, О.Б. Макаревич, В.М. Федоров, Е.М. Панченко

МОДЕЛИРОВАНИЕ ВСТРАИВАНИЯ ДАННЫХ НА ОСНОВЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ*

Рассмотрен стеганографический метод для сокрытия сообщений в цифровых аудиосигналах на основе вейвлет-преобразования в соответствии с деревом полной декомпозиции Малла, применяемого к перцептивно важным областям сигнала, что обеспечивает высокую стойкость как к пассивным, так и к активным атакам. Приведено обоснование использования области преобразования сигнала в методах стеганографии, реализующих скрытие сообщений в современных средах передачи медиа-трафика. Исследовано влияние встраиваемых данных на спектральные характеристики и гистограммы цифровых звуковых сигналов при использовании различных типов вейвлетов и модуляции коэффициентов гармоническим сигналом-паттерном.

Стеганография; стегоанализ; алгоритм Маллата; вейвлет-преобразование; спектр мощности; спектрограмма.

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

SIMULATION OF DATA EMBEDDING BASED ON DISCRETE WAVELET TRANSFORM

In this paper the steganographic method for hiding messages in digital audio signals based on wavelet transform in accordance with a tree full decomposition of Mallat is reviewed, applicable to the perceptually important areas of the signal, which provides high robustness to passive as well as to active attacks. The substantiation of the use of signal transformation in steganography methods for hiding message in today's media transfer media traffic is given. The influence of the embedded data to the spectral characteristics and the histograms of digital audio signals is reviewed, for different types of wavelets and harmonic modulation of the signal-pattern.

Steganography; steganalysis; Mallat algorithm; the wavelet transform; power spectrum; spectrogram.

В настоящее время в связи широким применением средств передачи видео- и голосового трафика актуальной является проблема выявления их использования для организации каналов скрытой передачи информации в обход стандартных мер защиты на основе стеганографических средств. Основной проблемой существующих стеганографических систем является низкая стойкость внедренных сообщений к активным атакам, а также при использовании того или иного метода сжатия, основанного на психофизиологической модели восприятия человека, т.е. варианта сжатия с потерями. Последнее особенно актуально при построении потоковых стегосистем для сетевых средств передачи мультимедийной информации, в частности, голосового трафика в IP-телефонии и трафика видеоданных. В частности, если рассматривать оцифрованную речь как один из наиболее распространённых источников мультимедиатрафика, то в зависимости от области применения, используется либо один из вариантов адаптивной модуляции, либо специализированные речевые кодеры на основе вокодерных и гибридных схем. В этом случае 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, 2].

* Работа выполнена при поддержке гранта РФФИ 09-07-00242-а.

При помощи набора вейвлетов в их временном или частотном представлении возможно получить приближение сложного сигнала как идеально точно, так и с некоторой погрешностью. Вейвлеты также обладают преимуществами в представлении локальных особенностей функций и учёте особенностей психофизиологической модели восприятия, благодаря чему они получили широкое распространение при анализе особенностей и сжатии сложных сигналов [1].

Целью работы является разработка математической модели стеганографического встраивания данных в звуковой файл путем декомпозиции его с помощью дискретного вейвлет-преобразования с дальнейшей модуляции коэффициентов разложения синусоидальным сигналом.

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].

В рассматриваемом методе областью встраивания является множество коэффициентов субполос вейвлет-декомпозиции цифрового аудиосигнала. При разложении сигналов с помощью вейвлет-преобразования используется частотный подход с использованием двух фильтров, низкочастотного и высокочастотного, причем используются квадратурные фильтры. Для сигнала x_i используется фильтр, базирующийся на операции свертки:

$$y_n = \sum_k h_k x_{n-k} .$$

Используя понятия частотного анализа, можно записать

$$Y(\omega) = H(\omega)X(\omega).$$

Транспонированный фильтр h^* состоит из тех же коэффициентов, но переставленных в обратном порядке. В частотной области трансформированный фильтр записывается как $\overline{H}(\omega)$. Величина $|X(\omega)|$ характеризует распределение энергии сигнала по частотам.

Разложение сигнала на две компоненты, а именно: высокочастотную и низкочастотную с последующей децимацией на два, лежит в основе БПФ и алгоритмов вейвлет-преобразования представления сигналов. Для этой цели использовали квадратурные зеркальные фильтры H и L, разделяющие сигнал на высокочастотную и низкочастотную составляющие с прореживанием по частоте. Такой подход позволяет точно восстанавливать исходный сигнал по данным, полученным при разложении. Его последовательное применение есть пирамидальный алгоритм Мала, дающий приближение сигнала по мере удаления от вершины дерева детального представления сигнала.

Для встраивания данных предложенным алгоритмом стеганографии [3] использовались коэффициенты субполос. В работах [3, 4] была установлена минимально необходимая глубина разложения, при которой субъективные искажения качества субъективно не воспринимаются, были проведены эксперименты по встраиванию информации в частотные субполосы различных уровней с последующим восстановлением в аудиофайлы. В результате проведённых экспериментов было установлено, что искажения качества звука перестают восприниматься с глубины разложения L=4, при этом встраивание в высокочастотные субполосы практически не оказывает влияние на субъективное качество сигнала при управлении энергией встраиваемого сигнала с глубины декомпозиции L=3. В качестве базисных вейвлетов для встраивания были исследованы вейвлеты Добеши и симлеты.

Для реализации предложенного метода встраивания была разработана программа в системе МАТЛАБ, которая состояла из нескольких блоков: декомпозиция исходного сигнала с выбранной глубиной разложения и выбранным базисом вейвлета, встраивание данных в коэффициенты разложения, восстановление сигнала для передачи по каналам связи.

Для обоснования предложенного метода была разработана математическая модель, позволяющая оценить изменение энергетического вклада субполос при встраивании скрываемых данных.

Для встраивания информации в коэффициенты может быть использовано множество различных способов. При необходимости скрытия информации без обеспечения стойкости к искажениям встраивание может производиться модулированием коэффициентов встраиваемой информпоследовательностью с ёмкостью 1 бит/коэффициент:

$$w_i^{'} = w_i \cdot b_i,$$

где w_i – i-й коэффициент выбранной субполосы,

b_i – символ информационной последовательности.

Восстановление бита сообщения производится по результату сравнения коэффициента с порогом $thrsh$:

$$b_i = \begin{cases} 0 & : w_i \le thrsh \\ 1 & : w_i > thrsh \end{cases}.$$

При последующем сжатии файла, содержащего встроенное сообщение при помощи методов компрессии с потерей качества, в частности MPEG, происходит искажение встроенного сообщения. Повышение стойкости к искажениям контейнера и последующей компрессии может быть достигнуто модуляцией не одного коэффициента, а окна коэффициентов длины l. Для модуляции окна коэффициентов длины l справедливо:

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

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 равна

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

Для сигнала частоты дискретизации 8 кГц при длительности 10 секунд и выборе глубины декомпозиции 4 с длиной окна $l = 1$ пропускная способность стегоканала составит 500 бит/с на одну субполосу вейвлет-декомпозиции.

При извлечении встроенных данных из блоков коэффициентов субполос аудиофайла полученная последовательность содержит битовые ошибки. Вероятность возникновения ошибок зависит, в первую очередь, от параметров звукового файла (частоты дискретизации, разрядности представления одного отсчёта). При встраивании информации прямым изменением коэффициентов единственно информацией, неизвестной злоумышленнику, является выбранный вейвлет. Помимо этого наличие в передаваемой последовательности длиных серий нулей и единиц

способно привести к воспринимаемым на слух артефактам. Также передача одного из состояний бита не изменяет состояния канала – в коэффициент или окно коэффициентов изменения не вносится и сохраняется их статистика в пределах окна, что теоретически допускает проведение стегоанализа на основе последовательностей наименее значимых бит. Для устранения данных недостатков авторами предложены методы встраивания в последовательность коэффициентов не непосредственно битов сообщения, модулированных коэффициентами, а низкочастотного сигнала-паттерна. В качестве сигнала могут выступать синусоидальный низкочастотный сигнал. При этом параметры модулирующего сигнала являются ключом встраивания. Модифицированное встраивание имеет следующие преимущества:

- снижение искажений при встраивании. Существует возможность адаптивного подбора паттерна с учётом модели сигнала;
- повышение скрытности канала. Для извлечения информации злоумышленнику необходимо не только располагать вейвлетом, использованным на этапе скрытия, но также и сигналом-паттерном, по меньшей мере для одного из битовых символов;
- повышение стойкости к стегоанализу, так как из сигнала исключаются немодифицированные участки, на основе которых возможно проведения статистического стегоанализа.

Встраивание осуществлялось в соответствии с выражением

$$w_i^{'} = w_i \cdot (1-\alpha) + seq_i^{b_i} \cdot \alpha ,$$

где $w_i^{'}$ – коэффициент выделенного окна после операции слияния,

w_i – коэффициент выделенного окна до операции слияния,

$seq_i^{b_i}$ – отсчёт сигнала-паттерна, соответствующий встраиваемому в текущее окно биту информации b_i,

α – коэффициент ослабления исходной субполосы.

Экспериментально было найдено, что наименьшая вероятность ошибки наблюдается при встраивании в пятую субполосу. Для проверки данного факта было проведено моделирование вкладов уровней вейвлет-разложения речевого сигнала.

Встраивание данных производилось в поток отсчётов оцифрованной речи диктора с параметрами Fs (частота дискретизации) – 11,025 кГц, разрядность отсчёта – 16 бит.

На рис. 1 приведены гистограммы отсчётов исходного файла без встроенных данных, файла, содержащего данные, встроенные в области вейвлет-коэффициентов 3-го уровня декомпозиции в пятой субполосе и их разность. Как видно из графиков, при встраивании происходит перераспределение частот значений отсчётов и сглаживание пиков с приближением гистограмм к “нормальному” для контейнера распределению. Данный факт является демаскирующим признаком, так как позволяет реализовать атаку при условии доступности незаполненных контейнеров из того же источника [5].

Графики амплитудного и фазового спектров для исходного и разностного сигналов при длине окна 1024 отсчёта и сдвиге по 1 отсчёту приведены на рис. 2. Как видно из спектрограммы, разность сводится к преобладанию аддитивного шума в области высоких частот и наличии множества гармоник, точное определение параметров которых возможно при помощи повторного преобразования Фурье спектрограммы исходного сигнала.

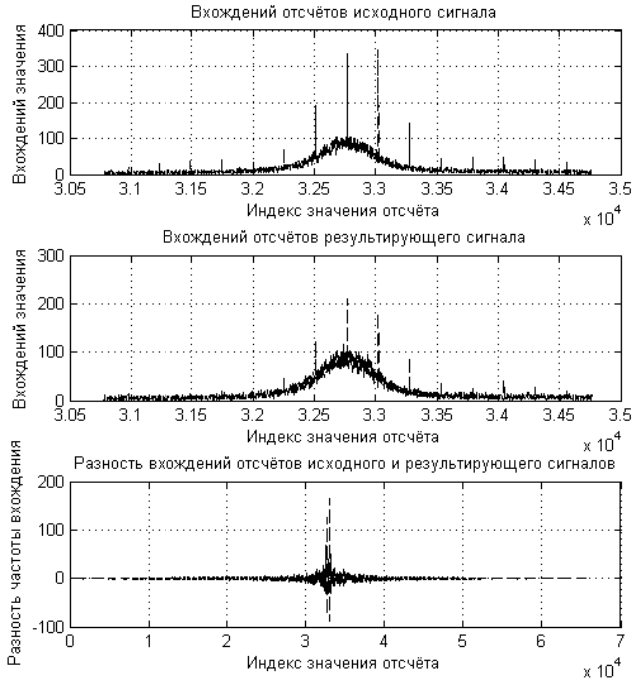

Рис. 1. Гистограммы потока отсчётов исходного файла, файла со встроенными данными и их разность

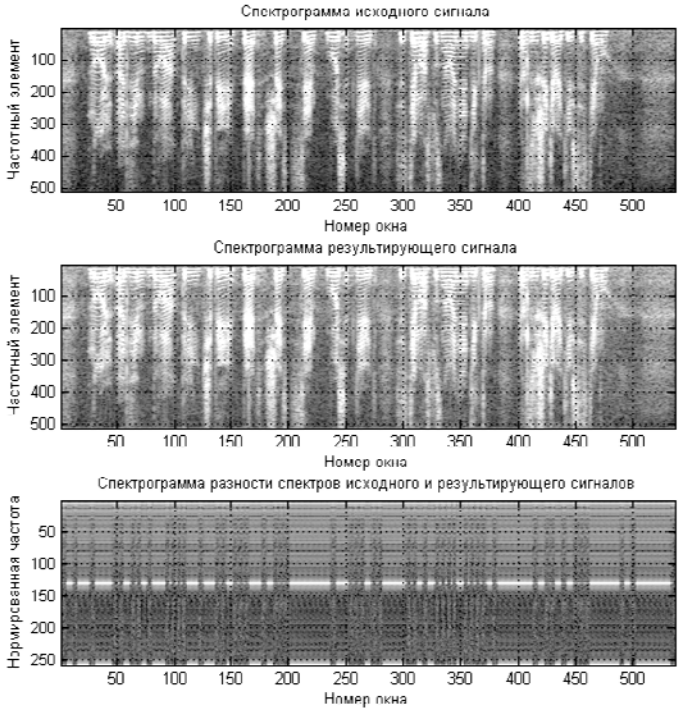

Рис. 2. Спектрограмма исходного и разностного сигналов

Демаскирующие признаки проявляются также и в Фурье-разложении вейвлет-коэффициентов. Так, спектры полос декомпозиции до третьего уровня для исходного и модифицированного сигналов приведены на рис. 3. Спектрограмма формировалась при помощи преобразования Фурье-последовательностей коэффициентов субполос с оконным разбиением по 1024 отсчёта и 50 % перекрытием. Из рисунка видно, что в низкочастотной области наблюдается повышение уровня группы частотных элементов, сохраняющееся на протяжении всей субполосы. Данные максимумы проявляются и при выборе для декомпозиции вейвлета порядка, отличного от использованного при встраивании, а также вейвлета другого семейства.

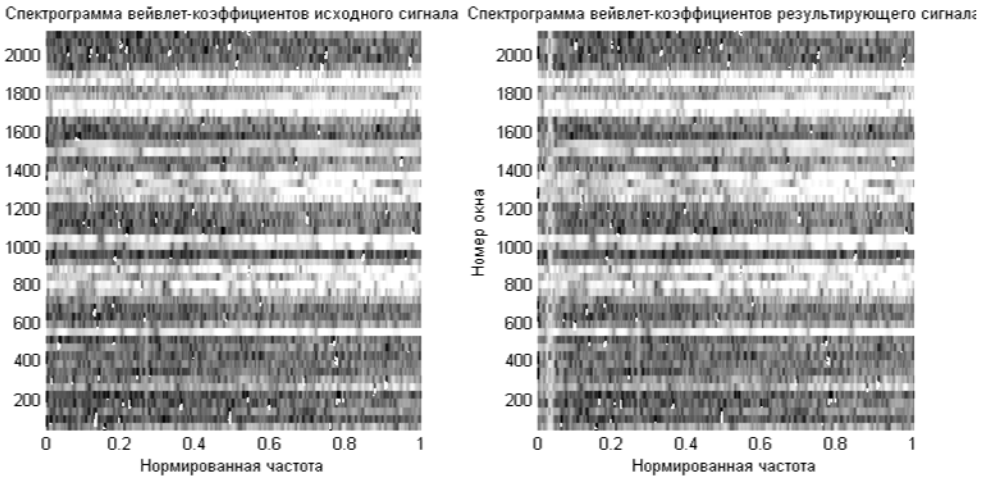

Рис. 3. Спектры вейвлет-коэффициентов пятой субполосы третьего уровня декомпозиции для файлов без встроенного сообщения (а) и со встроенным сообщением (б)

Определяющим является совпадение номера уровня и глубины декомпозиции с использованными при встраивании. На рис. 4 приведены спектрограммы пятой субполосы вейвлет-декомпозиции в базисе Хаара (Добеши-1) и Добеши-20.

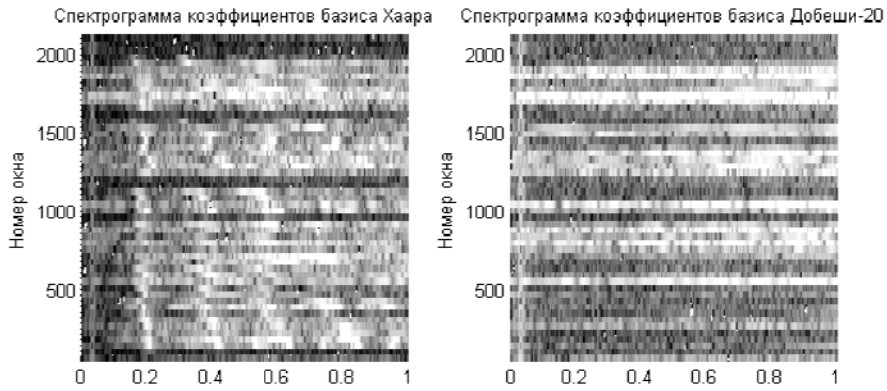

Рис. 4. Спектрограммы коэффициентов базисов Хаара и Добеши-20

Несмотря на несовпадение порядка вейвлетов, использованных на этапе декомпозиции, наблюдается сохранение отличительных особенностей встраивания. Аналогичные особенности наблюдаются при использовании койфлет 3 порядка и симлет 4-го порядка.

Таким образом, установлено, что при использовании метода стеганографического встраивания сообщений на основе вейвлет-преобразования в спектрограммах коэффициентов субполос вейвлет-декомпозиции наблюдается появление гармонических составляющих в масштабах встраивания, а также происходит выравнивание гистограмм отсчётов аудиосигналов со встроенными сообщениями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Lewis A.S., Knowles G.* Image compression using 2-d wavelet transform // IEEE. – Transactions on Image Processing. – 1992. – № 1. – P. 240-250.
2. *Дьяконов В.* Матлаб. Обработка сигналов и изображений. Специальный справочник / Дьяконов В. – СПб.: Питер, 2002. – С. 608.
3. *Рублев Д.П., Макаревич О.Б., Фёдоров В.М.* Встраивание двоичных данных в аудио и статичные изображения на основе дискретного вейвлет-преобразования // 4-я международная научно-техническая и научно-методическая конференция «Проблемы современной системотехники». – Таганрог, 2010. – С. 86-93.
4. *Рублев Д.П. Макаревич О.Б., Фёдоров В.М.* Метод стеганографического встраивания сообщений в аудиоданные на основе вейвлет-преобразования // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 199-206.
5. *Рублев Д.П. Фёдоров В.М., Макаревич О.Б.* Методы разностного стегоанализа изображений // Материалы VII Международной научно-практической конференции. – Таганрог, 2005. – С. 216-220.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Рублёв Дмитрий Павлович
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
347928, г. Таганрог, ул. Чехова, 2.
E-mail: rublev-d@yandex.ru.
Тел.: 88634371905.
Кафедра безопасности информационных технологий; доцент.

Макаревич Олег Борисович
E-mail: mak@tsure.ru.
Тел.: 88634312018.
Кафедра безопасности информационных технологий; зав. кафедрой.

Федоров Владимир Михайлович
E-mail: vladmih@rambler.ru.
Тел.: 88634371905.
Кафедра безопасности информационных технологий; доцент.

Панченко Евгений Михайлович
Научно-исследовательский институт физики Южного федерального университета.
E-mail: kordon@kordon-rnd.ru.
344090, г. Ростов-на-Дону, пр. Стачки, 194.
Тел.: 88632905121.
Зам. директора по НР.

Rublev Dmitry Pavlovich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: rublev-d@yandex.ru.
2, Chekhova Street, Taganrog, 347928, Russia.
Phone: +78634371905.
The Department of Security in Data Processing Technologies; Associate Professor.

Makarevich Oleg Borisovich
E-mail: mak@tsure.ru.
Phone: +78634312018.
The Department of Security in Data Processing Technologies; Head of the Department.

Fedorov Vladimir Mikhailovich
E-mail: vladmih@rambler.ru.
Phone: +78634371905.
The Department of Security in Data Processing Technologies; Associate Professor.

Panchenko Eugene Mikhailovich
Institute of Physics, Southern Federal University.
E-mail: kordon@kordon-rnd.ru.
194, Pr. Strikes, Rostov-on-Don, 344090, Russia.
Phone: +78632905121.
The Deputy Director on Scientific Work

УДК 681.3

И.А. Калмыков, О.И. Дагаева

РАЗРАБОТКА ПСЕВДОСЛУЧАЙНОЙ ФУНКЦИИ ПОВЫШЕННОЙ ЭФФЕКТИВНОСТИ

Рассмотрены вопросы синтеза псевдослучайной функции повышенной эффективности. Доказано, что псевдослучайная функция может быть построена на основе каскадной схемной реализации. Полученные результаты свидетельствуют о том, что разработанная псевдослучайная функция обладает стойкостью к атакующим алгоритмам не хуже, чем у ранее известных реализаций таких функций, при меньшей размерности секретного ключа.

Псевдослучайные функции; параллельная стойкость; каскадная конструкция; l-DDH предположение.

I.A. Kalmikov, O.I. Dagaeva

DESIGN OF ALGEBRAIC PSEUDORANDOM FUNCTIONS WITH IMPROVED EFFICIENCY

There is considered issues related with constructing an algebraic pseudorandom function with improved efficiency. It is proved that the pseudorandom function can be based on a cascade construction. Our pseudorandom function is secure to attacking algorithms not less then counterparts and it uses shorter private keys.

Pseudorandom functions; parallel security; cascade construction; l-DDH assumption.

Введение. В настоящее время псевдослучайные функции (ПСФ) нашли широкое применение в различных сферах. Современная информатика широко использует псевдослучайные числа в самых разных приложениях – от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых ПСФ напрямую зависит качество получаемых результатов. Поэтому вопросам разработки алгоритмов вычисления псевдослучайных функций повышенной эффективности уделяется значительное внимание.