УДК 655.3

Севостьян Д. М., ассистент; Юденков В. С., доцент

ПРИМЕНИМОСТЬ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ В СТЕГАНОГРАФИИ

In connection with rapid development of technologies of multimedia there was a question of protection of copyrights and intellectual property, presented in a digital kind. One of the most effective means of protection of the multimedia information consists in embedding in protected object of invisible labels — digital watermarks (DW). However, ways of embedding can be various. In given clause the opportunity of application of wavelet-transformations in steganografics is analyzed.

Введение. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Один из наиболее эффективных технических средств защиты мультимедийной информации заключается во встраивании в защищаемый объект невидимых меток — цифровых водяных знаков (ЦВЗ). Однако, способы встраивания могут быть различными. Наибольшее применение могут иметь открытые стегосистемы ЦВЗ, которые аналогичны системам скрытой передачи данных. Наибольшую устойчивость по отношению к внешним воздействиям имеют закрытые стегосистемы I типа.

В данной статье анализируется возможность применения вейвлет-преобразований в стеганографии. Вейвлет-преобразование — относительно новое, но, в то же время, мощное средство анализа и обработки сигналов. Успешное применение методов вейвлет-анализа в различных практических и теоретических приложениях лишний раз доказывает его состоятельность. Не умаляя достоинств преобразования Фурье, вейвлет-анализ способен полностью заменить обработку сигналов традиционными методами.

1. Понятие и характеристики контейнера в стеганографии. Рассмотрим подробнее понятие контейнера. До стегокодера — это пустой контейнер, после него — заполненный контейнер, или стего. Стего должен быть визуально неотличим от пустого контейнера. Различают два основных типа контейнеров: потоковый и фиксированный.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что в кодере неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т. д., то скрываемая информация может идти сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи.

У фиксированного контейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение данных оптимальным в некотором смысле образом. Встраивание сообщения в контейнер может производиться при помощи ключа, одного или нескольких.
Ключ — псевдослучайная последовательность (ПСП) бит, порождаемая генератором, удовлетворяющим определенным требованиям (криптографически безопасный генератор). В качестве основы генератора может использоваться, например, линейный рекуррентный регистр. Тогда адресатам для обеспечения связи может сообщаться начальное заполнение этого регистра. Числа, порождаемые генератором ПСП, могут определять позиции модифицируемых отсчетов в случае фиксированного контейнера или интервалы между ними в случае потокового контейнера. Надо отметить, что метод случайного выбора величины интервала между встраиваемыми битами не особенно хорош. Причин этого две. Во-первых, скрытые данные должны быть распределены по всему изображению. Поэтому, равномерное распределение длин интервалов (от наименьшего до наибольшего) может быть достигнуто лишь приближенно, так как мы должны быть уверены в том, что все сообщение встроено, то есть «поместилось» в контейнер. Во-вторых, длины интервалов между отсчетами шума распределены не по равномерному, а по экспоненциальному закону. Генератор же ПСП с экспоненциально распределенными интервалами сложен в реализации [2].

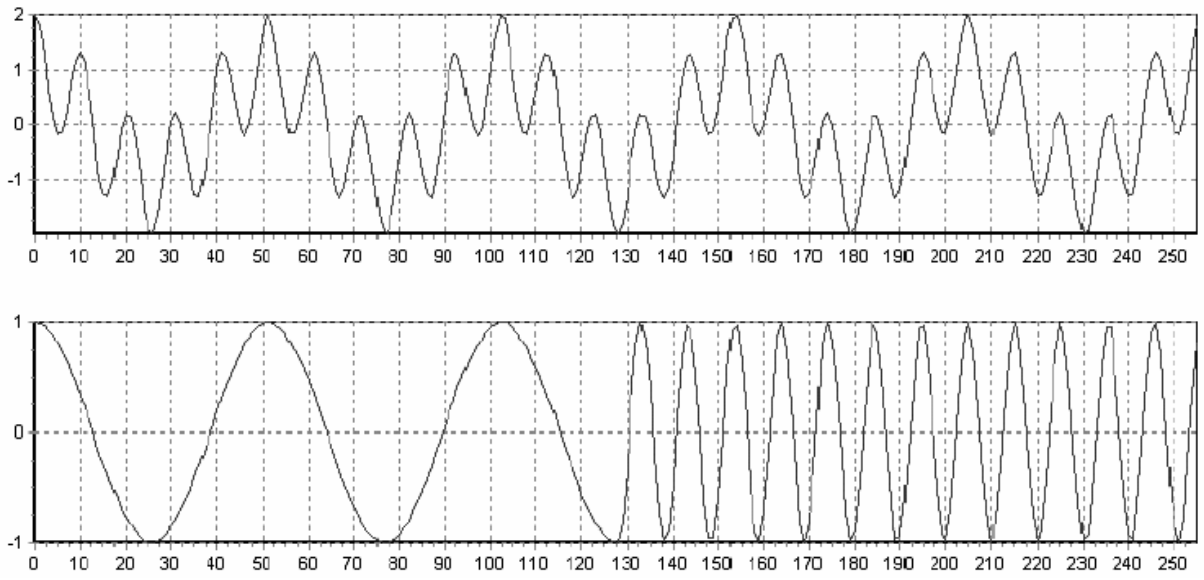


Рис. 1. Два сигнала с подобными Фурье-спектрами

2. Особенности Фурье-преобразований. Одним из основных средств обработки сигналов на сегодняшний день является линейное преобразование. Классическим примером такого преобразования является преобразование Фурье. Линейное преобразование сигнала подразумевает свертку сигнала конечной длины с семейством базисных функций. Многие трудности, возникающие при анализе сигналов с помощью преобразования Фурье, связаны с тем, что реальные сигналы бывает трудно с достаточной точностью описать при помощи взвешенной суммы синусоид различных частот, в особенности если сигнал содержит разрывы 1-го рода.

Как правило, регистрируемые сигналы нестационарны, их частотные и масштабные характеристики со временем меняются, причем очень важно бывает локализовать моменты их изменения [3]. Преобразование Фурье не позволяет решать задачу локализации. Например, оно не отличает сигнал, представляющий собой сумму двух синусоид различных частот от аналогичных синусоид, следующих друг за другом (рис. 1).

Частично эта трудность снимается за счет использования оконного преобразования Фурье. С одной стороны оконное преобразование Фурье локализует анализ, однако, оно не учитывает особенность реальных сигналов, которая заключается в том, что длительность каждой составляющей сигнала обратнопропорциональна ее частоте. Вследствие этого высокочастотная информация должна быть извлечена из относительно малых интервалов времени и наоборот. Иными словами, ширина окна должна уменьшаться с увеличением частоты, что для оконного преобразования Фурье не выполняется.

Конечно, при практическом применении Фурье-анализа проводились эксперименты с окнами переменной длины. И подобные исследования привели, в конце концов, к появлению теории вейвлет-анализа.

Использование вейвлет-преобразований в стеганографии. Особый смысл вейвлет-преобразования приобретают при условии возможных манипуляций с исходным изображением. Так, анализ литературы показывает практически полное отсутствие методов встраивания устойчивых к компрессии мультимедийных данных. Одним из преобразований, позволяющих осуществить подобное встраивание, является дискретное вейвлет-преобразование. 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. Вейвлеты имеют явные преимущества в представлении локальных особенностей функций и неявном учете особенностей психофизиологической модели восприятия [5].

Покажем, что их применение при разработке метода стеганографии, ориентированного на достижение максимальной пропускной способности (скрытая передача и хранение информации) можно решить основные задачи стеганографии, а именно: минимизация вносимых искажений и устойчивость к атакам пассивного злоумышленника.

Рассмотрим частотный подход. В соответствии с этим подходом частотная область вейвлетов может быть разбита на две составляющие — низкочастотную и высокочастотную. Их частота раздела равна половине частоты дискретизации сигнала. Для их разделения достаточно использовать два фильтра — низкочастотный Lo и высокочастотный Hi, к входам которых подключается сигнал s. Фильтр Lo дает частотный образ для аппроксимации (грубого приближения) сигнала, а фильтр Hi для его детализации.

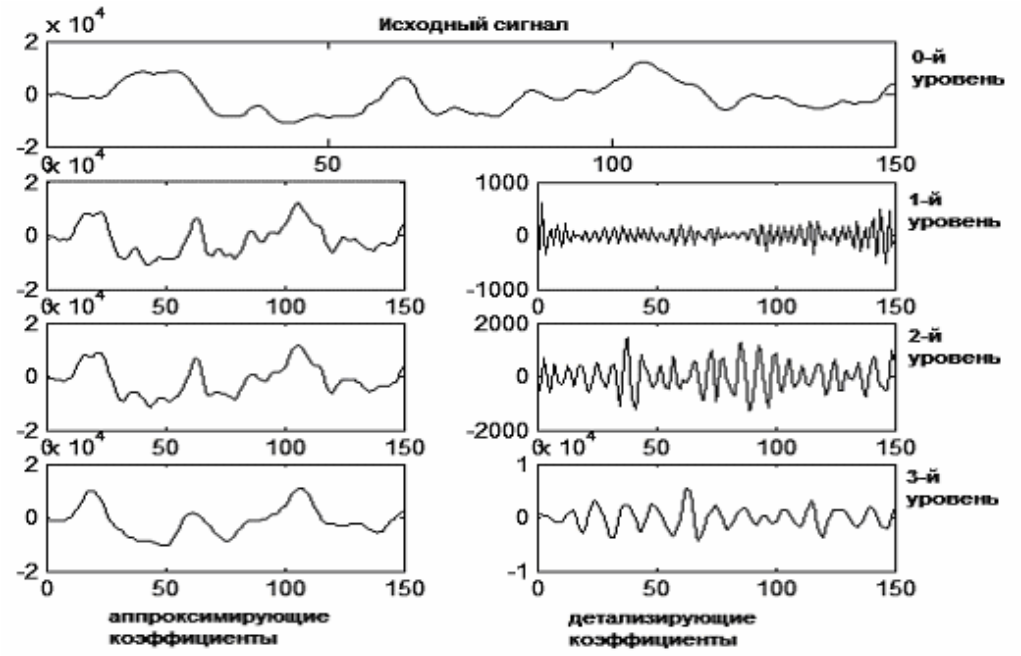
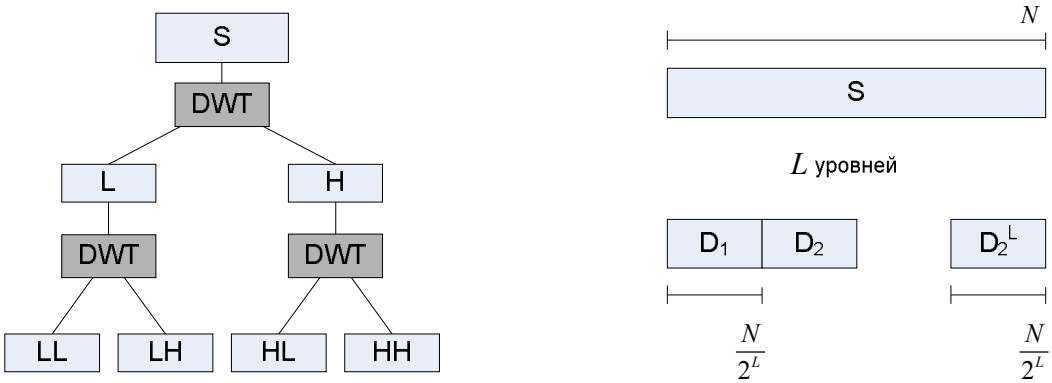


Рис. 2. 3-х уровневая вейвлет-декомпозиция сигнала



(а) (б)

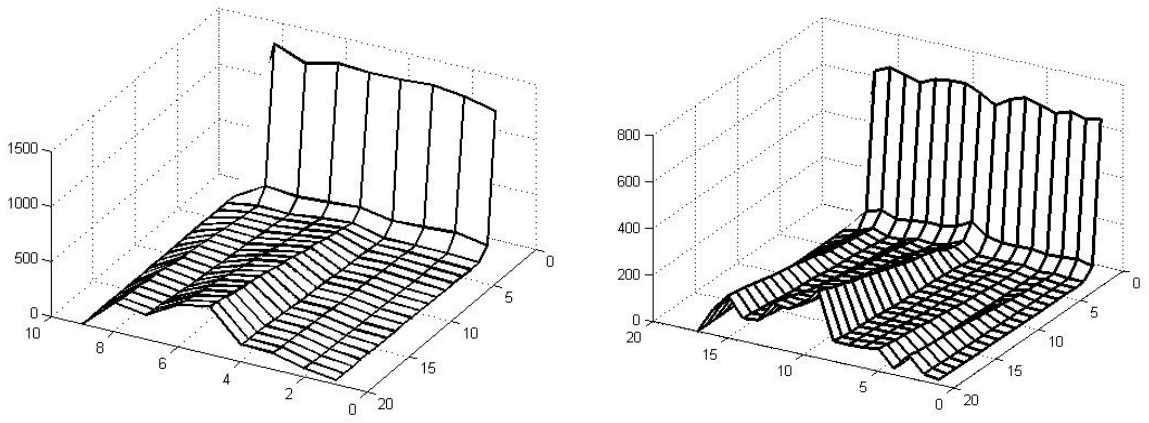
Рис. 3. Декомпозиция при помощи усовершенствованного алгоритма Маллата на глубину 2 (а) и результат декомпозиции N отсчетов сигнала на глубину L (б)

Поскольку фильтры передают только половину всех частотных компонент сигнала, то не попавшие в полосу прозрачности компоненты могут быть удалены [4]. Если просто сложить полученные на выходах фильтров сигналы, то получится исходный сигнал, то есть будет иметь место полная реконструкция сигнала на начальном уровне. Однако Lo-фильтр можно, в свою очередь, разложить на два фильтра и подвергнуть спектры этих новых фильтров операции прореживания по частоте — децимации.

В предлагаемом методе областью встраивания является множество коэффициентов субполос декомпозиции. На первом этапе при помощи усовершенствованного алгоритма Маллата [1] производилась декомпозиция сигнала s. Для этого нормированный сигнал подавался на фильтры декомпозиции низких и высоких частот, после чего с помощью операции децимации ↓2 (уменьшения числа частотных составляющих вдвое) находились коэффициенты аппроксимации и детализирующие коэффициенты на выходе фильтров на выходе низких и высоких частот (рисунок 4а). В результате декомпозиции на глубину L были получены коэффициенты 2^L.

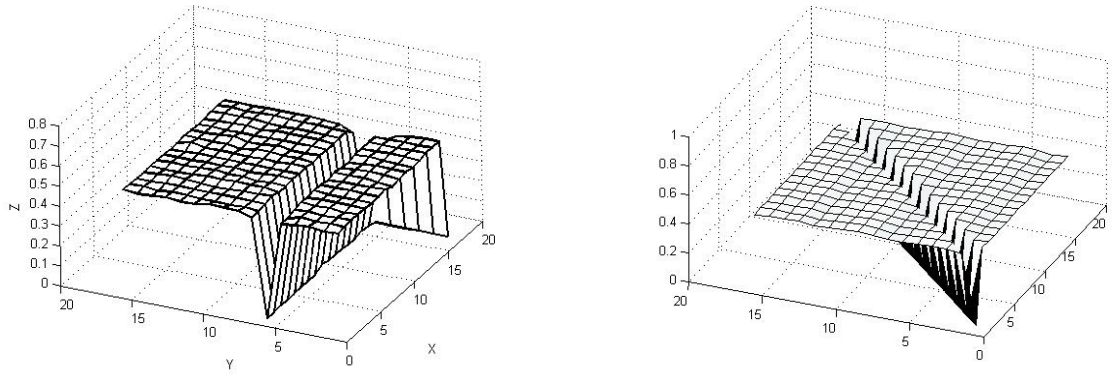
Экспериментальная часть. Экспериментальные данные получены на основе использования программного обеспечения, написанного в среде Microsoft Visual C++. Усредненная оценка битовых ошибок при встраивании бита в два коэффициента приведена на рисунках 5а—5б.

Для усреднения были использованы результаты 30 экспериментов. В каждом из них генерировалась псевдослучайная бинарная последовательность, используемая в качестве сообщения. Зависимость количества битовых ошибок от субполосы разложения и выбранного порога приведена на рисунке 4. На графиках субполос виден четкий минимум количества битовых ошибок, который достигается одновременно для



(а) (б)

Рис. 4. Зависимость количества битовых ошибок от субполосы разложения и выбранного порога для одного (а) и двух (б) коэффициентов на бит информации (по оси Z — логарифмическая шкала)



(а) (б)

Рис. 5. Вероятность битовой ошибки при извлечения бита, скрытого на уровне 5 декомпозиции Добеши шестого порядка вейвлетами порядков 1-16 (а) и средняя вероятность битовой ошибки при рассмотрении вейвлетов Добеши порядков 1-20

каждой из субполос при определенном значении коэффициента. Данное значение находится в зависимости от выбранной глубины декомпозиции и модуляции. Для установления возможности осуществить обнаружение и извлечение информации без знания вейвлета, используемого при встраивании была проведена серия экспериментов.

Сообщение, представляющее собой псевдослучайную битовую последовательность было встроено в коэффициенты субполосы, выделенной при помощи дискретной вейвлет-декомпозиции на глубину $L = 4$. В качестве базисного вейвлета для декомпозиции использовались вейвлеты Добеши.

Встраивание битового потока производилось в выбранную субполосу прямой модуляцией коэффициентов с результирующей емкостью 1 бит/коэффициент.

Выводы. На основе проведенного анализа можно утверждать о целесообразности использования вейвлет-преобразований в стеганографии. Более того, вейвлет-преобразования имеют ряд преимуществ по сравнению с преобразованиями Фурье, применяемыми для тех же типов сигналов. Полученные в ходе экспериментов данные показывают минимум количества битовых ошибок, который для каждой из субполос при определенном значении коэффициента.

Литература

1. Matsui, K. Digital signature on a facsimile document by recursive MH coding / K. Matsui, K. Tanaka, Y. Nakamura // Symposium On Cryptography and Information Security, 1989.

2. Osborne, C. Digital Watermark / C. Osborne, R. van Schyndel, A. A. Tirkel // IEEE Intern. Conf. on Image Processing, 1994. P. 86–90.

3. Anderson, R., editor. // Proc. Int. Workshop on Information Hiding: Lecture Notes in Computer Science. Springer-Verlag, Cambridge. 1996.

4. Chae, J. J. Robust Techniques for Data Hiding in Images and Video / J. J. Chae // PhD thesis, CA, USA, 1999.

5. Corvi, M. Wavelet-based image watermarking for copyright protection / M. Corvi, G. Nicchiotti // Scandinavian Conference on Image Analysis. 1997.