электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

Молодежный научно-технический вестник # 01, январь 2013
УДК: 003.26.004.056.57
авторы: Гончаров Н. О., Заикин М. А.

Целью работы является изучение и исследование эффективности метода сокрытия сообщений с использованием эхо-сигнала. Как известно [1], метод подразумевает под собой встраивание данных в аудио сигнал - контейнер путем введения в него эхо-сигнала. Данные скрываются изменением трех параметров эхо-сигнала: начальной амплитуды, скорости затухания сдвига. Отдельные теоретические аспекты рассмотрены в работе [2].
Этапы проведения исследования:

- анализ известных данных о методах применения «Эхо-кодирования»;
- синтез полученных данных для получения представления об эффективности метода;
- выявление основных достоинств и недостатков.

Из эмпирических методов использовались:

- изучение метода «Эхо-кодирования» на примере работы В. Бендера и Н. Моримото « Методы сокрытия данных»[1];
- опытно – экспериментальная работа по реализации метода ««Эхо-кодирования» в автоматизированной математической среде MathCad.
- запись произвольно выбранного стего методом эхо – кодирования;
- восстановление стего по известному ключу;
- последовательное увеличение объёма стего для определения границы пропускной способности.

1. Описание работы алгоритма

Метод подразумевает под собой встраивание данных в аудио сигнал - контейнер путем введения в него эхо-сигнала. Данные скрываются изменением трех параметров эхо-сигнала: начальной амплитуды, скорости затухания. Когда сдвиг (задержка) между первичным и эхо-сигналом уменьшается, начиная с некоторого значения задержки, ССЧ становится не способной обнаружить разницу между двумя сигналами, а эхо-сигнал воспринимается только как дополнительный резонанс. Упомянутое значение трудно

определить точно, поскольку оно зависит от качества первичной звукозаписи, типа звука, для которого формируется эхо-сигнал, и в конечном итоге, — от слушателя.

Стеганокодер использует два времени задержки: одно для представления двоичного нуля, а другое — для представления двоичной единицы. Оба времени задержки меньше того предельного времени, за которое ССЧ способна распознать эхо-сигнал. Помимо уменьшения времени задержки, устанавливаются уровни начальной амплитуды и времени затухания, которые не превышают порог чувствительности ССЧ.

Извлечение вложенной информации подразумевает под собой выявление интервала между эхо-сигналами отдельных сегментов. Для этого необходимо исследовать в двух позициях амплитуду автокорреляционной функции (АКФ) косинус-преобразования Фурье натурального логарифма спектра мощности (кепстр) кодированного сигнала. Результат вычисления кепстра делает интервал между эхо-сигналом и исходным сигналом более выраженным. АКФ кепстра позволяет выделить из множества импульсов, полученных на предыдущем шаге, первый.

2. Определение предельной пропускной способности

В рамках одного контейнера было рассмотренно кодирование сообщений длиной 5, 10, 20 и 50 символов (соответственно каждый символ – 8 бит).

Для начала закодируем сообщение длиной 5 символов (40 бит). Значения исходного и декодированного сообщения приведены в таблице 1.

Таблица 1 - Значения исходного и декодированного сообщения длины 5 символов

исходное сообщение(apple) :				
1	2	3	4	5
97	112	112	108	101
декодированное сообщение:				
1	2	3	4	5
97	112	112	108	101

На сравнительном графике сигналов исходного аудиофайла - рисунок 1 видно, что чем больше колебания амплитуды исходного сигнала, тем сильнее влияние стего кодирования на результирующий сигнал. Мы выбирали немонотонный отрывок аудиозаписи с меняющейся интенсивностью.

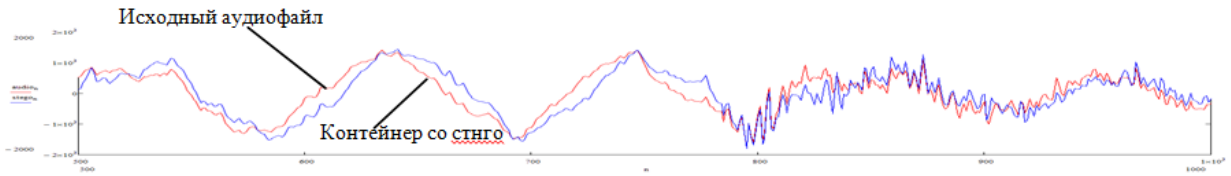

Рисунок 1. сравнительном графике сигналов со стего для 5 символов

Слуховое впечатление дает возможность сравнивать частоты двух тонов при быстром переключении с одного на другой и обнаруживать даже небольшую разницу между частотами двух тонов и замечать небольшие изменения частоты тона. Не трудно заметить усиление низких частот на графике спектров – рисунок 2.

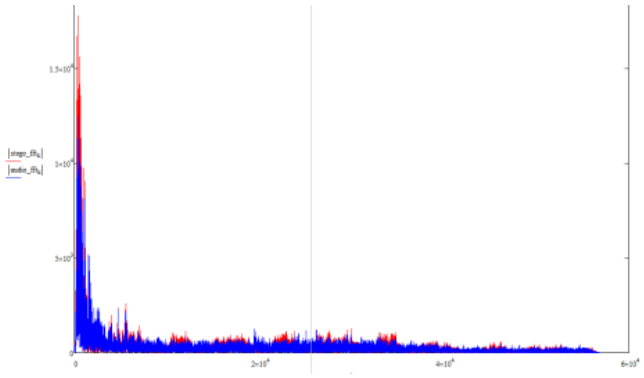

Рисунок 2. Сравнение спектров исходного аудиосигнала и с контейнера со стего

Все зависит от качества аудиозаписи, звуковоспроизводящей аппаратуры и слуховых качеств человека. Люди с музыкальным слухом безусловно услышат разницу между файлами, но в данном исследовании мы ориентируемся на среднестатистического человека.

Далее мы производим кодирование сообщения длиной 10 символов (80 бит). Значения исходного и декодированного сообщения приведены в таблице 2.

Таблица 2 - Значения исходного и декодированного сообщения длины 10 символов

исходное сообщение (appleapple):									
1	2	3	4	5	1	2	3	4	5
97	112	112	108	101	97	112	112	108	101
декодированное сообщение:									
1	2	3	4	5	1	2	3	4	5
97	112	112	108	101	97	112	112	108	101

Реакция на скачки амплитуды стала более выраженной, что можно заметить на рисунке 3. При этом стоит учесть, что при количестве бит на уровень квантования, равном 16, непременно возникнут перегрузки, которые уже проще различить на записи.

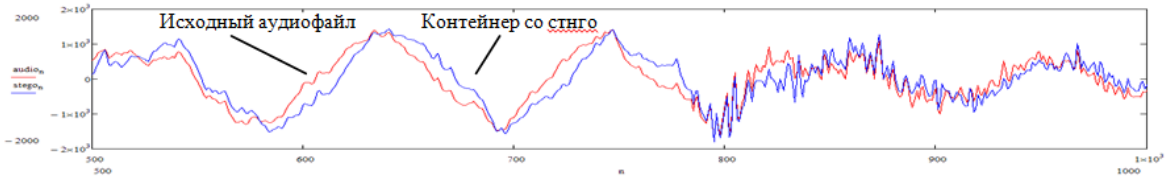

Рисунок 3. Сравнительный график сигналов со стего 10 символов

С помощью данного метода вполне возможно скрывать/извлекать информацию с минимальным изменением первичного сигнала при пропускной способности, приблизительно, в 16 бит/с. Длительность выбранного нами контейнера составляет примерно 5 секунд, а значит сообщение длиной 10 символов (80 бит) – теоретически максимальное, которое можно передать без существенной разницы между модифицированным и первичным сигналами.

Стего корректно распознается декодером, а изменения сигнала все еще не различимы для неискушенного слушателя [3]. Следовательно, заявленная граница 16 бит/с подтверждается на практике.

На третьем этапе мы производим кодирование сообщения длиной 20 символов (160 бит). Значения исходного и декодированного сообщения приведены в таблице 3.

Таблица 3 - Значения исходного и декодированного сообщения длины 10 символов

исходное сообщение (appleapple…..appleapple…… apple):															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
97	50	112	108	97	97	16	80	108	101	97	112	16	108	109	…
декодированное сообщение:															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
97	112	112	108	101	97	112	112	108	101	97	112	112	108	101	…

На модифицированной записи отчетливо слышно эхо наиболее выделяющихся фрагментов. Декодированное сообщение не совпадает с оригинальным. Возникают множественные одиночные ошибки. Все указывает на то, что контейнер не способен вместить в себе сообщение данной длины. Сравнительный график сигналов представлен на рисунке 4.

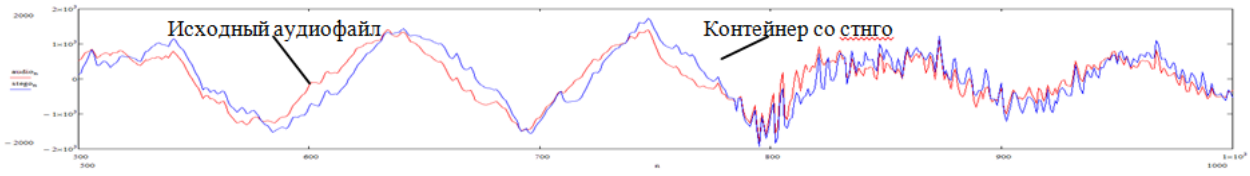

Рисунок 4. Сравнительном графике сигналов со стего для 20 символов

На последнем третьем этапе мы производим кодирование сообщения длиной 50 символов (400 бит). Значения исходного и декодированного сообщения приведены в таблице 4.

Таблица 4 - Значения исходного и декодированного сообщения длины 10 символов

исходное сообщение (appleapple…..appleapple…… apple):															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
97	50	112	108	97	97	16	80	108	101	97	112	16	108	109	…
декодированное сообщение:															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
97	112	112	108	101	97	112	112	108	101	97	112	112	108	101	…

Исходный сигнал сильно искажен, ошибки декодирования уже не одиночные, а групповые. Разница между файлами слышна «невооруженным» ухом. . Сравнительный график сигналов представлен на рисунке 5.

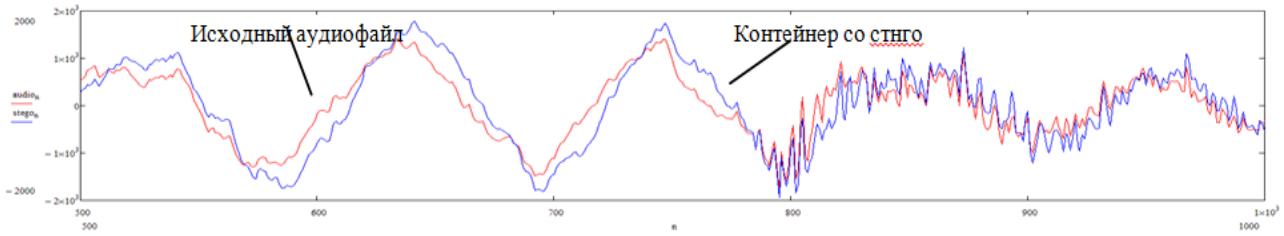

Рисунок 5. Сравнительном графике сигналов со стего для 50 символов

Заключение

В ходе исследования было выявлено, что при увеличении размера стего, график спектра сигнала значительно не менялся, что подтверждает факт об устойчивости эхо-метода к частотным атакам, сжатию.

Метод эхо-кодирования не является универсальным. На качество кодирования влияет множество факторов: сам аудиосигнал, его амплитудные характеристики, слуховые качества распознающего, и другие. Также, при приближении к границе пропускной способности, увеличивается вероятность появления одиночных ошибок. Данную проблему можно решить путем использования кодов, исправляющих ошибки, однако тогда граница будет смещаться в меньшую сторону.

По сравнению с другими методами, эхо-кодирование характеризуется весьма небольшим соотношением сигнал/шум (примерно 4) и высоким параметром среднеквадратической ошибки (порядка 10^5). Но данный метод выигрывает за счет большой пропускной способности и устойчивости к амплитудным и частотным атакам.

Литература:

1. W.Bender, D.Gruhl, N.Morimoto, A.Lu, Tchniques for Data Hiding. IBM Systems Journal, 35(3&4); pp. 313-336, 1996.
2. Чичварин Н.В. Сопоставительный анализ областей применения и граничных возможностей характерных стеганографических алгоритмов //3-я Международная научно – технической конференции «Безопасные информационные технологии – 2012»: труды. М.: НИИ радиоэлектроники и лазерной техники, 2012. С. 174-179.
3. Иофе В. К., Корольков В. Г., Сапожков М. А., «Справочник по акустике» - Связь 1979 г. 312 с