УДК 004.4

Использование спектрального метода для внедрения скрытой информации в аудио сигналы

Пасюков Александр Андреевич
Приамурский государственный университет им. Шолом-Алейхема
Магистрант

Баженов Руслан Иванович
Приамурский государственный университет им. Шолом-Алейхема
к.п.н., доцент, зав. кафедрой информационных систем, математики и правовой информатики

Аннотация
Статья посвящена исследованию методов встраивания скрытой информации в аудиофайлы. Предложен способ внедрения секретной информации аудиофайлы. Данный метод позволит не только защитить секретную информацию в аудио файле, но и скрыть сам факт ее существования. Кроме того, предложен способ выявления информации из данного файла.
Ключевые слова: стеганография, спектральный метод, скрытая информация, преобразование Фурье.

The use of the spectral method for the introduction of hidden information into audio signals

Pasyukov Alexandr Andreevich
Sholom-Aleichem Priamursky State University
Master student

Bazhenov Ruslan Ivanovich
Sholom-Aleichem Priamursky State University
Candidate of pedagogical sciences, associate professor, Head of the Department of Information Systems, Mathematics and Law Informatics

Abstract
The article is devoted to the research of methods of embedding hidden information in audio files. The method of introducing secret information audio files is proposed. This method will not only protect the secret information in the audio file, but also hide the very fact of its existence. In addition, a method for identifying information from this file is proposed.
Keywords: steganography, spectral method, hidden information, Fourier transform.

Во все времена высокой актуальностью отличались методы защиты информации. С появлением компьютерных технологий защита информации не только стала активнее развиваться, но и образовалась отдельная ветвь научных исследований. Благодаря современным цифровым устройствам появилась возможность без труда создавать, хранить и передавать информацию в виде видео, аудио и изображений. В наше время имеется несколько методов защиты информации. Самым широко используемым является криптография. В данной статье затронут другой вид защиты информации - стеганография. Стеганография в отличие от криптографии, скрывает сам факт наличия информации, другими словами, позволяет внедрить информацию в какой-либо файл таким образом, что файл - контейнер будет выглядеть как обычный файл без внедренной информации. Термин «стеганография» имеет греческий корни, буквальный перевод которого – «тайность». Защита информации достигалась тем, что о наличии сообщения знали лишь отправитель и предполагаемый получатель. Особый рост в развитии стеганография получила в связи с появлением электрон новычислительных систем. В ней выделились два направления: компьютерная и цифровая стеганографии. Компьютерная стеганография основана на способах скрытия ин формации с использованием особенности компьютерной платформы (например, внедрение информации в свободные кластеры файловой системы). Цифровая стеганография использует методы внедрения информации в цифровые объекты, вызывая некоторые искажения этих объектов. С ростом объема различной информации растет доля сведений, которые необходимо держать в тайне. Применение компьютеров позволило усовершенствовать известные идеи скрытия информации, с тем, чтобы затруднить обнаружение факта её внедрения. В данной работе планируется использовать алгоритм внедрения скрываемой информации в аудио файл путем метода спектрального спектра.

Многие зарубежные и русские ученые занимались данной проблематикой. В работе А. А.Жарких, В. Ю. Пластунов [1] был представлен метод внедрения цифрового водяного знака в аудиосигнал в виде аудиосигнала на основе преобразований конформной алгебры единичного круга. Д. Е.Стародубцев, В. В. Плашенков [2] описали алгоритм реализует процедуру интерпретации двоичного потока сообщения как некоторого мелодического контейнера, хранящегося в формате MIDI-файла. М.А.Заикин, Н.О. Гончаров [3] описали исследование эффективности метода защиты аудио сигнала при передаче по открытому аналоговому каналу связи с использованием скремблирования. P.Jayaram, H.R.Ranganatha, H.S.Anupama [4] описали суть стеганографии аудиосигналов, раскрыли плюсы, минусы и произвели анализ наиболее популярных методов сокрытия информации. В работе M. Zamani [5] описал способы повышения надёжности встраивания цифровых водяных знаков в аудио сигналы. В работе О. Ю. Пескова, Г. Ю. Халабурда [6] представлены базовые принципы сетевой стеганографии для защиты речи.

Перед началом решения данной проблемы требуется использовать спектральный метод. Спектральный метод – один из методов обработки аудио сигналов, основан на разложение звука на составляющие с дискретным применением преобразования Фурье. Преобразование Фурье – некая математическая основа, которая описывает восприятие звука человеческом. Данное преобразование помогает разложить функцию, представляя колебательные процессы в виде набора синусоидальных составляющих - волнообразных кривых, переходящих от максимума к минимуму. Другими словами, преобразование Фурье - функция, описывающая амплитуду и фазу каждой синусоиды, соответствующей определённой частоте (рис. 1).

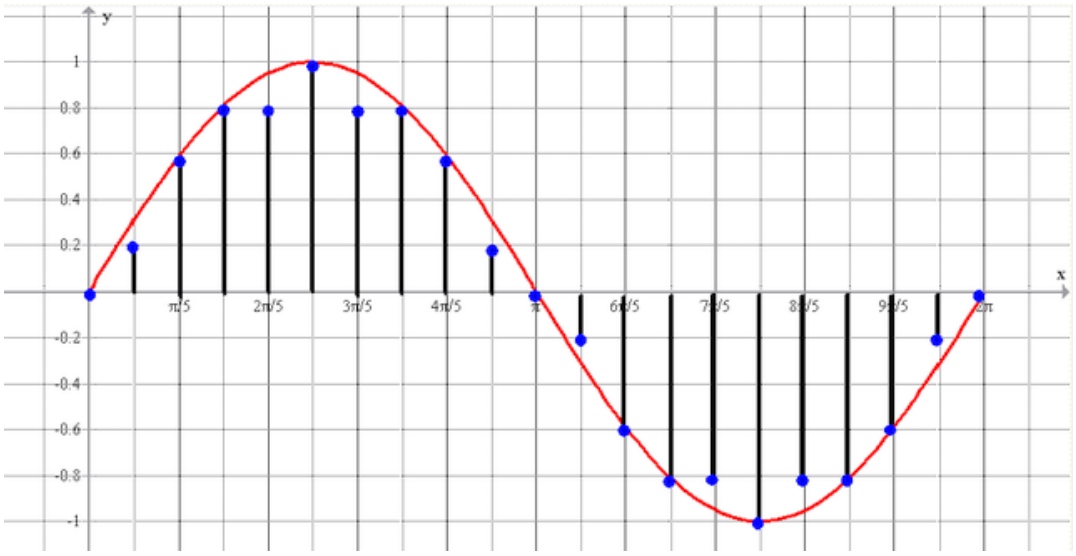

Рисунок 1 - Пример преобразования Фурье

Благодаря тому, что человеческое ухо не может в полной степени различать искажения в аудио звуке, именно это и помогает в полной мере использовать недостатки слуховой системы для сокрытия информации. В предлагаемом методе используется FFT (алгоритм быстрого вычисления дискретного преобразования Фурье), который создает частотный спектр всего исходного аудио файла. Этот спектр разделен на два основных поддиапазона, поддиапазон низких и поддиапазон высоких частот. Внедряемая информация переводится в бинарный вид и после чего внедряется данные частоты. Данные будут внедряться таким способом: если число четное и требуется внедрить «1», то к числу прибавляется «+1», и таким образом оно превращается в нечетное. Если число нечетное и требуется внедрить «1», то с ним ничего не делается. Если число нечетное и требуется внедрить «0», то требуется прибавляется «+1», и если число четное и требуется прибавить «0», то оно не изменяется.

Однако, пре внедрении большого объема информации, информация подвержена сильному искажению. Для повышения устойчивости схемы предлагается изменить четность более значимых цифр коэффициентов. Например, один бит информации может быть встроен во вторую цифру коэффициента. Тогда шум с таким же значением не изменит четность цифры.

Поэтому легко сделать вывод, что чем более значительная цифра коэффициента используется для вставки небольшого количества информации, тем сложнее изменить его четность, и, следовательно, схема будет более устойчивой к шуму. Однако следует отметить, что может быть ситуация, когда добавление к коэффициенту любого числа может изменить четность более значимых цифр.

Для извлечения данных из аудио файла требуется произвести обратное преобразование фурье. Бит информации был встроен в цифру коэффициентов в пределах области. Затем по известным координатам и соответствующим цифрам коэффициенты анализируются и выводится скрытая информация в бинарном виде.

В ходе работы предложен метод внедрения звуковых данных в другой аудио файл для затруднения их обнаружения. Данный метод позволит внедрять файлы любых типов в аудио звук за счет того, что внедряемый файл перед кодированием переводится в бинарный вид. Извлечение данных будет происходить за счет обратного преобразования фурье и за счет четных и нечетных показателей коэффициентов. После внедрения информации, не зная метода внедрения обнаружить её практически невозможно. Требуется подметить, что данный способ очень стойкий к искажениям, что позволит с минимальной вероятностью потерять нужную информацию.

Библиографический список

1. Жарких А. А., Пластунов В. Ю. Новый метод внедрения водяного знака в аудиосигнал // Вестник МГТУ. 2009. №2 С.206-211.
2. Стародубцев Д. Е., Плашенков В. В. Метод стеганографического преобразования информации в гибридный звуковой контейнер // Вестник Череповецкого государственного университета. 2015. №8 (69). С.29-32.
3. Заикин М.А., Гончаров Н.О. Защита аудио сигнала с использованием скремблирования //Молодежный научно-технический вестник. 2013. №. 10. С. 45.
4. Jayaram P., Ranganatha H. R., Anupama H. S. Information hiding using audio steganography–a survey // The International Journal of Multimedia & Its Applications (IJMA). 2011. Т. 3. С. 86-96.
5. Zamani M. A secure audio steganography approach //Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for IEEE, 2009. С. 1-6.
6. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет //Материалы научной конференции» Интернет и современное общество. 2012. С. 348-354.