УДК 004.056.55

МЕТОДЫ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В АУДИОФАЙЛАХ ФОРМАТА MIDI И WAV

В.В. МИРОНЧИК, Е.С. ШЕЛЕСТ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
Violet-88@tut.by

Передача скрытой информации в аудиофайлах является актуальной в контексте защиты авторских прав от несанкционированного использования мультимедийной продукции. Рассмотрены методы скрытой передачи информации в аудиофайлах формата MIDI и WAV.

Ключевые слова: формат MIDI, формат WAV, аудиофайлы, скрытие информации.

В современном мире человек постоянно находится в окружении различных звуков. Развитие и распространение сетевых методов общения привело к появлению новых методов передачи скрытой информации в аудиофайлах. Эффективным решением для передачи скрытой информации в аудиофайлах является объединение методов компьютерной стеганографии и криптографии [1]. При использовании криптографии информация модифицируется по определенному алгоритму, в результате преобразований скрывается смысл сообщения. Стеганография скрывает сам факт передачи или хранения информации путем внедрения ее в различные мультимедийные объекты, которые не теряют от этого своих потребительских свойств. Не смотря на большое разнообразие форматов аудиофайлов, одними из наиболее распространенными являются MIDI и WAV.

Формат MIDI является распространенным форматом хранения и передачи музыки, который используют композиторы, музыканты и обычные пользователи ЭВМ. Известен метод внедрения информации в MIDI-файлы путем использования разности времени между записанными в файл событиями, которые не изменяют характеристики (настройки) устройства воспроизведения [2]. Это происходит, например, когда подряд следуют несколько одинаковых управляющих событий. Суть данного метода заключается в кодировке скрытого сообщения временем между изменением уровня громкости аудиосигнала. Недостатком в данном случае является отсутствие секретного ключа, который предотвращал бы возможность чтения внедренной информации любым пользователем.

Существует также метод внедрения скрытой информации в MIDI-фа йлы с помощью кодирования информации двоичным кодом, а двоичный код, в свою очередь управляет громкостью звучания нот, следующих друг за другом. В данном случае используется следующий алгоритм: если скрывается логическая единица, то значение громкости должно быть нечетным числом, а если скрывается логический нуль – четным. Обнаружить сделанное вложение на слух невозможно, так как, во-первых, изменения громкости незначительны, а во-вторых, изменение громкости на одну единицу невозможно зарегистрировать на слух, однако можно использовать для скрытой передачи информации. Кроме того, запись секретной информации может быть осуществлена в партию лишь одного инструмента (например, контрабаса), что при звучании целого оркестра (или ансамбля) еще больше акустически маскирует скрытое сообщение [3].

Таким образом, формат MIDI может быть успешно использован для передачи или хранения конфиденциальной информации. При этом для сокрытия информации следует использовать большое число различных событий, которые управляют процессом воспроизведения музыкальной композиции.

Файл формата WAV содержит в себе квантованные цифровые значения амплитуды сигнала, измеренные в дискретные моменты времени (так называемые отсчеты). Для файла формата WAV наиболее известным и распространенным методом сокрытия секретной информации является метод замены наименьшего значащего бита (НЗБ) [4].

При внедрении информации в звуковые файлы формата WAV методом НЗБ приходится решать задачу выбора номера разряда отсчета, в который можно поместить скрываемую информацию, с учетом двух конфликтующих требований. С одной стороны, необходимо увеличивать объем скрываемой информации в одном файле (увеличивать пропускную способность канала), а с другой стороны, нужно обеспечить высокую степень скрытности вложенной информации. На данный момент разработано программное обеспечение, позволяющее решать поставленные задачи.

Программа Crypto предназначена для скрытой передачи информации в аудиофайлах, с использованием принципов стеганографии. Для повышения скрытности внедренной информации в программе использован модифицированный метод замены наименьшего значащего бита. Информация разделяется на фрагменты и распределяется по нескольким звуковым файлам. Ключом для извлечения сообщения служит последовательность файлов, в которых были скрыты фрагменты сообщения.

Программа WaveCrypto позволяет внедрять информацию в один звуковой файл с использованием ключа, распределяющего внедряемую информацию по всему контейнеру. Ключ распределения генерируется в зависимости от размера файла и требующегося соотношения между наполняемостью и скрытностью. Если в контейнере содержится «полная тишина» (отсчеты с малой амплитудой), то программа пропускает их, внедряя информацию на других участках фонограммы. Программы Crypto и WaveCrypto создают несколько уровней защиты информации: шифруют открытый текст одним из криптографических методов, внедряют зашифрованный текст в звуковые файлы, распыляя скрываемые биты не только внутри одного файла, но и среди нескольких звуковых файлов [5].

Передача скрытой информации в аудиофайлах позволяет решить проблему защиты авторских прав на мультимедийную продукцию. Но в тоже время, скрытая информация в аудиоформате может оказать негативное влияние на психоэмоциональное состояние человека, так как различные звуки могут воздействовать на мысли и эмоции людей. При прослушивании аудиофайла, содержащего в себе скрытую информацию в виде формулы внушения, человек может на подсознательном уровне подвергаться воздействию. Обнаружение скрытой передачи информации с целью защиты человека от негативного воздействия на его подсознание является на данный момент актуальной задачей.

Список литературы

1. *Андрианова О.С., Губенко Н.Е.* // Моделирование и компьютерная графика. Материалы третьей международной научно-технической конференции Донецк 7 – 9 октября 2009 г. С.389 – 392.

2. *Walter J.M.* Method and apparatus for encoding security information in a MIDI datastream United States Patent US 6798885 B1 Sep. 28, 2004.

3. *Алексеев А.П., Аленин А.А.* Методы внедрения информации в звуковые файлы формата MIDI // Инфокоммуникационные технологии. 2011. Т. 9. № 1. С. 84 – 89.

4. *Алексеев А.П., Орлов В.В.* Стеганографические и криптографические методы защиты информации: учебное пособие. Самара: ИУНЛ ПГУТИ, 2010.

5. *Аленин А.А., Алексеев А.П.* Исследование методов обнаружения вложений в звуковых файлах формата WAV // Безопасность информационных технологий. 2011. Т. 9. №1. С. 51 – 56.