УДК 681.3

И.С. Ломов

АНАЛИЗ ВОЗМОЖНОСТЕЙ СКРЫТИЯ ИНФОРМАЦИИ В АУДИОФАЙЛАХ

Компания «Проектинжиниринг», г.Воронеж

В статье рассматриваются основные характеристики подходов, позволяющих проводить скрытие информации в аудиофайлах. Указаны требования, при выполнении которых не будет обнаружена скрываемая информация.

Ключевые слова: защита информации, аудиофайлы.

В настоящее время идет активное развитие различных способов защиты информации. Одним из перспективных подходов, требующих исследований, является скрытие информации в звуковых файлах [1-3].

Целью данной работы является анализ возможных способов защиты информации в аудиофайлах.

При практическом использовании скрытие информации может использоваться различными компонентами документооборота [4-5].

Отметим основные требования, которые могут рассматриваться при оценке возможностей практического использования стегосистем, которые применяются для того, чтобы обеспечить встраивание информации в звуковые сигналы:

- та информация, которую необходимо скрыть должна обладать свойствами стойкости по отношению к тому, что существуют различные окрашенные шумы, происходит сжатие с потерями, осуществляется фильтрование, делается аналогово-цифровое и цифро-аналоговое преобразования;

- информация, которая подвергается скрытию, не должна в сигнале делать искажения, которые далее могут быть восприняты слуховой системой людей;

- при осуществлении попытки удаления скрываемой информации должно происходить сильное повреждению контейнера (относится к ЦВЗ);

- та информация, которая подвергается скрытию, не должна приводить к заметным изменениям в статистике контейнера.

Интересно, что для внедрения скрываемой информации в звуковые сигналы можно применять методы, которые используются в других типах стеганографии. Можно, например, осуществлять внедрение информации,

путем замещения наименее значимых битов (то есть, всех или некоторых). Также можно проводить построение стегосистем, базируясь на определенных особенностях звуковых сигналов или слуховой системы людей.

Эта слуховая система может быть представлена в виде анализатора частотного спектра. При этом он имеет возможности к обнаружению и распознаванию сигналов, лежащих в диапазоне 10 – 20000 Гц. Такую слуховую систему человека можно промоделировать в виде 26 пропускающих фильтров, у которых происходит увеличение полосы пропускания по мере роста частоты. В системе слуха людей различия изменений фаз сигнала происходят слабее, чем для изменений амплитуд или частот.

В настоящее время аудио-сигналы подразделяются на такие три класса:

- сигналы, соответствующие разговору телефонного качества в диапазоне 300 – 3400 Гц;
- сигналы, соответствующие широкополосной речи, для частоты в диапазоне 50 – 7000 Гц;
- аудио-сигналы, являющиеся широкополосными, с частотами 20 – 20000 Гц.

К способам, которые при своем использовании опираются не только на какие-то характеристики аудио-сигналов, но и особенности слуховой системы людей может быть отнесен метод маскирования сигнала. Эффект маскирования связан с тем, что если есть слабое, но при этом способное быть услышанным звуковое колебание, то оно потом становится неслышимым когда возникает другое более громкое (называемым сигналом маскирования). Этот эффект маскирования определяется спектральными и временными характеристиками, которые существуют в как в маскируемом сигнале, так и в сигнале маскирования.

Интересно отметить, что говорят как о маскировании по частоте, так и маскировании по времени. Первый подход связан с тем, что в том случае, когда одновременно два сигнала размещены в определенной ограниченной частотной области, то тот сигнал, который более слабый, не будет услышан в присутствии более сильного. В этом случае есть зависимость порога маскирования от нескольких составляющих: от того, какая частота, уровень подавления сигнала и тональная или шумовая характеристика маскируемого сигнала и сигнала маскирования. Практика показывает, что на основе широкополосного шумового сигнала легче осуществлять маскирование тонального колебания, чем наоборот. Также, маскировка

более высокочастотных колебаний проходит легче. Проведение маскирования по времени дает такой эффект: для более слабого сигнала его слышимость становится нулевой за 5 – 20 мс до того, как будет включены колебания маскирования и слышимость возобновляется через 50 – 200 мс после их выключения.

С использованием известных подходов скрытия информации могут быть оценены риски ее раскрытия [6-9].

На основе информации о том, как проходит маскирование по частоте для слуховой системы людей, имеется возможность определения спектральных характеристик внедряемой информации. Например, при обработке импульсных сигналов, к которым относится звук кастаньет, может возникнуть весьма отчетливо слышимое пре-эхо. Для того, чтобы убрать такой эффект при осуществлении процессов внедрения информации его необходимо обязательно учитывать.

Проведем рассмотрение конкретного способа внедрения ЦВЗ (которая представляет собой псевдослучайную последовательность) на основе применения эффекта маскирования. В этом случае каждый аудиосигнал помечают кодовым словом, которое уникально. С целью использования маскирующих характеристик слуховой системы людей по частоте требуется провести соотношение этой псевдослучайной последовательности с определенным порогом для маскирования сигнала. Но необходимо понимать, что требуется принять во внимание эффект временного маскирования. Трудно обеспечить внедрение большого количества информации в сигнал, у которого достаточно малая мощность. Иначе информацию просто можно будет услышана. Это связано с тем, что при проведении преобразования Фурье, имеющего фиксированную длину невозможно достичь хорошую локализацию во временной и частотной областях. В том случае, когда длительность сигнала, имеющего высокую мощность, больше длительности окна, тогда происходит распространение его энергии по всем частотам. Из этого можно сделать вывод, что требуется производить взвешивание ЦВЗ с энергией сигнала. Для того, чтобы внедрить ЦВЗ требуется провести вычисление порога маскирования сигнала. С целью того, чтобы облегчить обнаружение ЦВЗ требуется провести увеличение его мощности, но при этом требуется стремиться к тому, чтобы спектральная плотность мощности ЦВЗ была меньше, чем порог маскирования. В том случае, когда полученный в результате вычислений ЦВЗ будет меньше чем шаг квантования, то необходимо провести его увеличение таким образом, чтобы не было потери ЦВЗ при осуществлении процесса квантования. В том случае, когда для всех отрезков времени ЦВЗ лежит ниже, чем порог маскирования, то тогда можно говорить о том, что нельзя услышать ЦВЗ.

Выводы. При создании системы защиты на основе аудиофайлов необходимо, в первую очередь, определить частотный диапазон, в котором проходит работа. Следующим важным шагом является выбор временного или частотного маскирования. Требуется проводить взвешивание ЦВЗ с энергией сигнала, что позволит определить порог маскирования.

ЛИТЕРАТУРА

1. Кленяева Г.В., Преображенский А.П. Современные проблемы речевой акустики и построения систем автоматического распознавания речи / Вестник Воронежского института высоких технологий. 2007. № 2-1. С. 71-74.
2. Головинов С.О., Мироненко С.Г., Щепилов Е.В., Преображенский А.П. Цифровая обработка сигналов / Вестник Воронежского института высоких технологий. 2009. № 4. С. 64-65.
3. Кайдакова К.В. Проблемы защиты информации в современных электронных документах / Успехи современного естествознания. 2012. №6. с.107-108.
4. Олейник Д.Ю. Некоторые вопросы использования информационных технологий в туристической индустрии / Успехи современного естествознания. 2012. №6. с.110.
5. Землянухина Н.С. О применении информационных технологий в менеджменте / Успехи современного естествознания. 2012. №6. с.106-107.
6. Бекетнова Ю.М., Львович И.Я. Решение задачи раннего выявления рисков нарушения финансовой и информационной безопасности юридического лица в терминах теории распознавания образов // Информация и безопасность. 2013. Т. 16. № 2. С. 191-194.
7. Ермилов Е.В., Попов Е.А., Жуков М.М., Чопоров О.Н. Риск-анализ распределенных систем на основе параметров рисков их компонентов // Информация и безопасность. 2013. Т. 16. № 1. С. 123-126.
8. Жуков М.М., Ермилов Е.В., Чопоров О.Н., Бабурин А.В. Построение динамической риск-модели для компонент распределенной системы на основе заданного закона распределения ущерба // Информация и безопасность. 2012. Т. 15. № 4. С. 449-460.

I.S. Lomov

THE ANALYSIS OF POSSIBILITIES OF HIDING INFORMATION IN AUDIOFILES

Company «Proektinzhiniring» Voronezh

The paper examines the main characteristics of the approaches that allow to hide information in audio files. The requirements under which the information will not be detected are shown.

Keywords: information security, audio files.