

УДК 004.934.2

ПРОВЕРКА МУЗЫКАЛЬНЫХ ФАЙЛОВ НА НАЛИЧИЕ СКРЫТЫХ РЕЧЕВЫХ СООБЩЕНИЙ ПРИ ПОМОЩИ СПЕКТРОГРАММ

А.М. Асиненко, В.М. Алефиренко

*Белорусский государственный университет информатики
и радиоэлектроники, Минск, Беларусь*

Аннотация. Представлен метод стеганофонии, использующий спектрограммы для проверки факта скрытия речевой информации в музыкальном файле. Алгоритм предполагает преобразование обоих аудиофайлов (речевого и музыкального) в спектрограммы, визуализирующие их частотный состав. Далее, речевая информация кодируется и встраивается в спектрограмму музыкального файла, например, путем модуляции амплитуды или частоты отдельных частотных составляющих. Полученная модифицированная спектрограмма затем обратно преобразуется в аудиосигнал. Для обнаружения скрытого сообщения сравниваются спектрограммы исходного музыкального файла и модифицированного. Различия, выявленные с помощью специального программного обеспечения, укажут на наличие скрытого сообщения. Программное обеспечение включает в себя модули для преобразования аудио в спектрограммы, алгоритмы встраивания/извлечения данных, и инструменты для анализа и сравнения спектрограмм. Эффективность метода зависит от выбранного алгоритма встраивания и устойчивости к шуму и искажениям.

Ключевые слова: спектрограмма; безопасность связи; защита информации; речевая информация; речевые файлы; музыкальные файлы; скрытая информация; обработка сигналов; преобразования Фурье; спектр сигналов.

CHECKING MUSIC FILES FOR HIDDEN ONES SPEECH MESSAGES USING SPECTROGRAMS

A. M. Asinenko, V. M. Alefirenko

*Educational Institution "Belarusian State University of Informatics and Radioelectronics",
Minsk, Belarus*

Abstract. A steganophony method is presented that uses spectrograms to verify that speech information is hidden in a music file. The algorithm involves converting both audio files (speech and music) into spectrograms that visualize their frequency composition. Further, speech information is encoded and embedded in the spectrogram of a music file, for example, by modulating the amplitude or frequency of individual frequency components. The resulting modified spectrogram is then converted back into an audio signal. To detect a hidden message, the spectrograms of the original music file and the modified one are compared. Differences detected using special software will indicate the presence of a hidden message. The software includes modules for converting audio into spectrograms, algorithms for embedding/extracting data, and tools for analyzing and comparing spectrograms. The effectiveness of the method depends on the chosen embedding algorithm and its resistance to noise and distortion.

Keywords: spectrogram; communication security; information protection; speech information; speech files; music files; hidden information; signal processing; Fourier transform; signal spectrum.

Введение

Значительная часть передаваемой по общедоступным каналам связи информации приходится на долю речевых сообщений. Такое положение дел сохранится и в будущем, поскольку такому универсальному инструменту человеческого общения как речь, обладающему уникальными признаками эффекта присутствия, эмоциональной окраски, аутентификации, информационной избыточности и другими, присущими только данному коммуникативному (переговорному) процессу, трудно найти какую-либо эквивалентную замену во многих системах связи и передачи информации. Вот почему задачи защиты речевой информации занимают одно из ведущих мест в решении общей проблемы информационной безопасности [1].

Для защиты информации могут использоваться специальные программные средства, применяющие в своей основе метод, основанный на использовании спектрограмм.

Основная часть

Спектрограмма – это визуальный способ представления уровня или «громкости» сигнала во времени на различных частотах, присутствующих в форме волны. Для вычисления спектрограммы дискретного сигнала его разбивают на сегменты. Для каждого сегмента находят его спектр в виде коэффициентов дискретного преобразования Фурье. Набор спектров и образует спектрограмму (рис. 1).

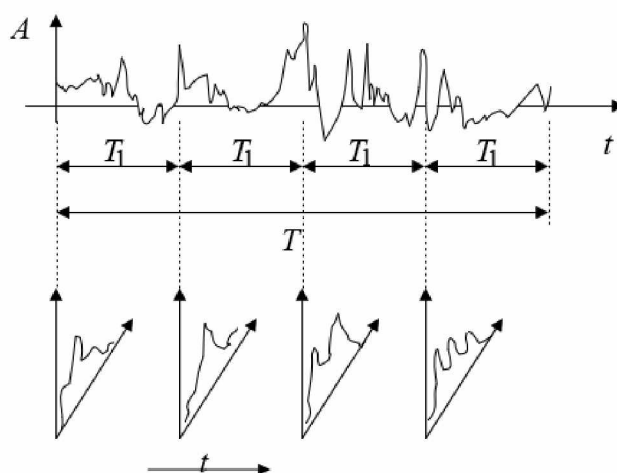


Рис. 1. Спектрограмма
Fig. 1. Spectrogram

В настоящее время существует большое количество хороших программных цифровых анализаторов и редакторов аудио сигналов, предназначенных для визуального анализа звуковых сигналов во временной (осциллограммы, графики уровня мощности сигнала и др.) и, конечно, частотной (сонограммы, кепстры и др.) областях. Среди импортных программных продуктов такого рода следует отметить Cool Edit Pro 1.2, Dart Pro, Sound Forge, Wave Lab, Wave Studio, Ocenaudio и др., среди отечественных – «SIS 5.2», «Win-Аудио», «Лазурь», Signal Quick Viewer 2 (SQV2), Signal Viewer (SV) и др. В ряде звуковых редакторов имеется возможность производить некоторые виды обработки аудио сигнала, которые можно применить и для решения ограниченного числа задач обеспечения безопасности речевых сигналов посредством компьютерных технологий [2]. Для проведения исследований использовалось программное средство Ocenaudio.

Возьмем музыкальный файл и запишем речевое сообщение, которое будет встроено в этот файл. В качестве исходного файла было взято музыкальное произведение длительностью около 3 минут, спектрограмма которого показана на рисунке 2. Речевое сообщение представляло собой короткую фразу произношения подряд нескольких цифр (цифровой пароль), спектрограмма которого показана на рисунке 3. На спектрограммах темным (черным) цветом показано отсутствие сигнала, а оттенками красного цвета – его наличие на соответствующих частотах по вертикальной оси.

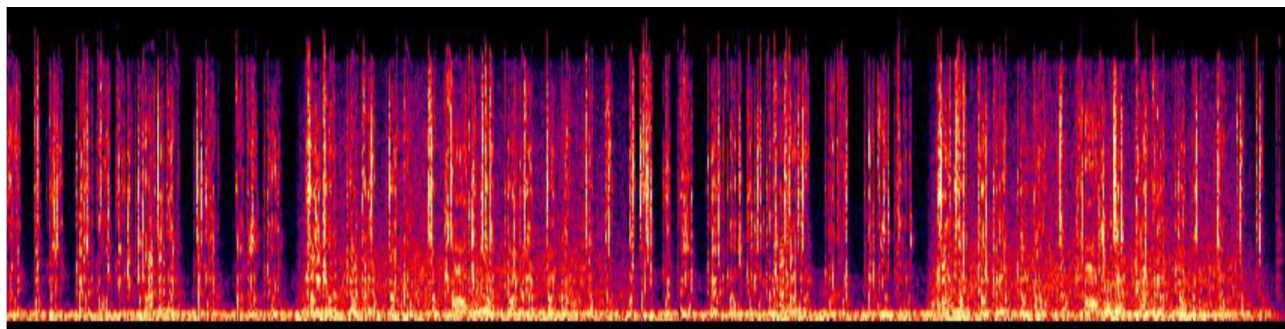


Рис. 2. Спектрограмма музыкального файла
Fig. 2. The spectrogram of the music file

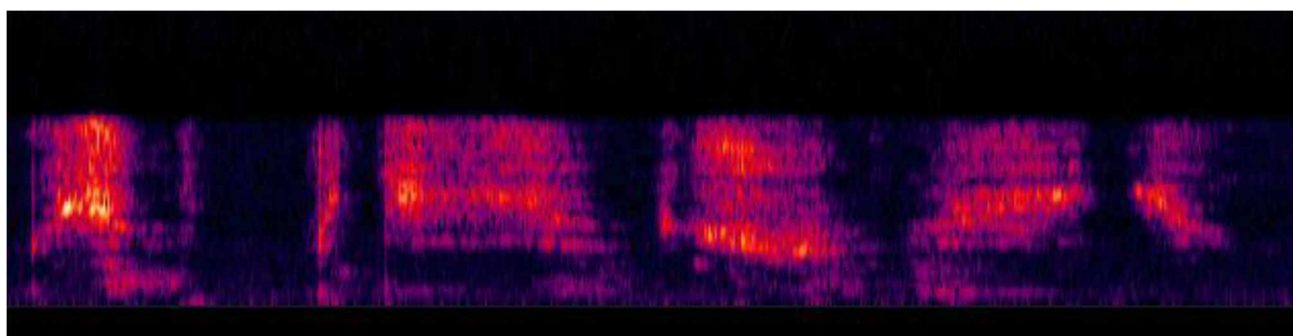


Рис. 3. Спектрограмма встраиваемого речевого файла
Fig. 3. Spectrogram of the embedded speech file

При объединении двух файлов в один получается спектрограмма, представленная на рис. 4. При сравнении исходной спектрограммы на рис. 2 и полученной спектрограммы на рис. 4 можно заметить небольшие различия на нижних частотах (выделены зеленым прямоугольником в левой нижней части), что свидетельствует о наличии скрытого сообщения. При прослушивании совмещенной спектрограммы различия не обнаруживаются.

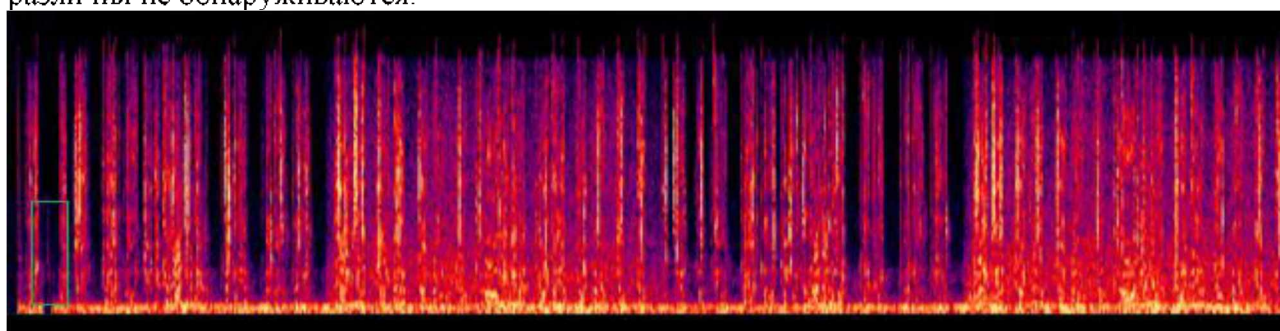


Рис. 4. Спектрограмма совмещенных звуковых файлов
Fig. 4. Spectrogram of combined audio files

Заключение

Прослушав музыкальный файл со скрытым сообщением, можно не заметить различия, отображенные на спектрограммах. Поэтому использование специальных программных средств позволяет определять наличие в различных файлах, в том числе музыкальных, скрытого сообщения.

Список использованных источников

1. Ахмад Х. М., Жирков В. Ф. (2007) *Введение в цифровую обработку речевых сигналов: учеб. пособие*. Издательство Владимирского государственного университета.
2. Асиненко, А. М. (2024) Использование спектрограмм для защиты речевой информации. *Электронные системы и технологии: сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР*, 46–48.

References

1. Akhmad Kh. M., Zhirkov V. F. (2007) *Introduction to digital processing of speech signals: textbook stipend*. Vladimir State University Publishing House (in Russian).
2. Asinenko. A.M. (2024) The use of spectrograms to protect speech information. *Electronic systems and Technologies: proceedings of the 60th Scientific Conference of graduate students, undergraduates and students of BSUIR*, 46-48 (in Russian).

Сведения об авторах

Аснненко А.М., ассистент кафедры электронной техники и технологии. Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». asinenko2016@mail.ru.

Алефиренко В.М., канд. техн. наук, доц., доцент кафедры информационно-компьютерных систем. Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». alefirenko@bsuir.by.

Information about the authors

Asinenko A.M., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics". asinenko2016@mail.ru.

Alefirenko V.M., Cand. Sci. (Tech.), Associate Professor, Associate Professor of Information and Computer-Aided Systems Design Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics". alefirenko@bsuir.by.