УДК 004.056.53

Студ. С.А. Юревич
Науч. рук. проф.П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ СТОЙКОСТИ К ВЗЛОМУ СТЕГАНОГРАФИЧЕСКИХ АУДИОКОНТЕЙНЕРОВ

Защита данных, их сокрытие, а также защита авторского права на электронный контент с помощью стеганографии является одним из важных направлений развития ИТ [1].

В докладе рассматривается задача сравнительного анализа стойкости к взлому аудиоконтейнеров, в которые информация осаждалась на основе следующих методов: сокрытия данных в заголовках mp3-файла, сокрытия данных непосредственно в аудиодорожке такого файла.

Аудиостеганография – это вид стеганографии, который использует аудиофайлы разных форматов в виде контейнеров для осаждения скрываемой информации. Мы же будем проводить наш анализ с аудиофайлами mp3-формата, структура которого показана на рисунке.

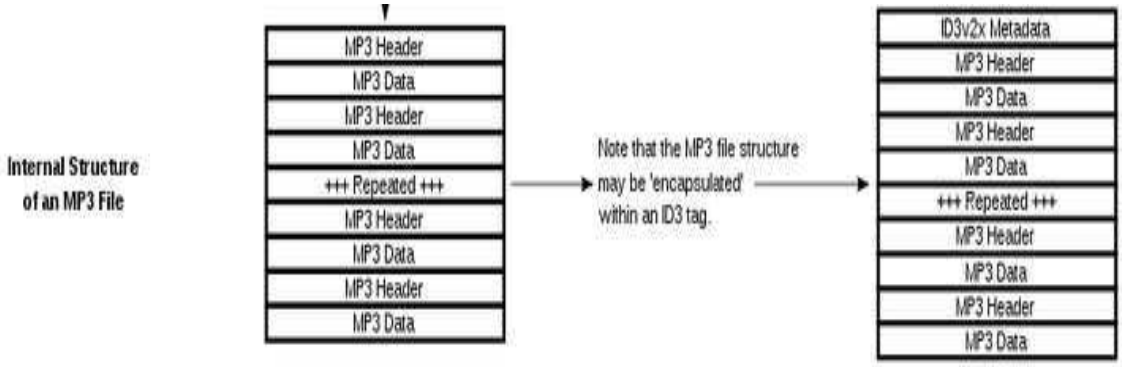

Рисунок – Структура mp3-файла

Структура на рисунке укрепилась как стандарт, поэтому нет ничего необычного в том, что у аудиофайла в описании присутствуют: текст песни, имя исполнителя и название песни, а также обложка в виде картинки – всё это возможно с помощью заголовка ID3v2. В нём мы и реализуем наш первый метод сокрытия информации. Сокрыть информацию внутри него можно, как и в картинке (известным методом LSB), в тексте песни (с помощью пробелов) так и многими другими способами [3]. Такие изменения невозможно услышать, поскольку они не касаются аудиодорожки напрямую.

Следующий метод применяется уже не к заголовкам файла, а непосредственно к аудиодорожке. Заключается он в довольно простом решении: обрезать высокие частоты исходной аудиодорожки и доба-

вить к ней ещё одну высокочастотную дорожку, близкую к 20 кГц (пусть это будет дорожка из сигналов азбуки Морзе). Такое сокрытие могут услышать лишь люди с острым слухом. Достоинства и недостатки методов приведены в таблице.

Таблица – Основные достоинства и недостатки рассмотренных стеганографических методов

Метод	Достоинства	Недостатки
Метод осаждения данных в заголовках mp3-файла	1. Множество вариаций осаждения данных. 2. Использование некоторых методов не влечёт за собой изменения размера файла, а также его контрольной суммы. 3. Аудиодорожка остаётся неизменной, в результате чего осаждаемая информация на слух не воспринимается; можно узнать о факте осаждения данных лишь программно, зная, где искать. 4. Возможность сокрыть большой объём данных.	1. В случае наличия оригинала песни, можно заметить отличия в обложках, в тексте песни и т.д.. 2. При использовании некоторых способов осаждения данных в заголовке (например, добавление архива к обложке), размер файла может существенно измениться.
Метод осаждения данных в аудиодорожке mp3-файла	1. Невозможно выявить осаждение данных по контрольной сумме. 2. Простота метода, достаточно иметь любую программу для создания и редактирования аудио.	1. Размер сокрытой информации ограничен длительностью аудиодорожки. 2. Размер файла неизбежно увеличивается. 3. Качество песни, теряется: появляются шумы. 4. Люди с острым слухом способны услышать тайную информацию.

Проведя анализ, можно сказать, что каждый метод имеет свои плюсы и минусы, но автор отдает свое предпочтение методу осаждения данных в заголовках в связи с наличием большого разнообразия осаждения данных и более трудоемким взломом стеганоконтейнера.

ЛИТЕРАТУРА

1. Urbanovich, P. Text steganography application for protection and transfer of the information / P. Urbanovich, K. Chourikov, A. Rimorev, N. Urbanovich // Przeglądelektrotechniczny. – 2010. – R. 86, № 7.– P.95-97.

2. Nilsson, M. The audio/mpeg Media Type – Internet Engineering Task Force/ M. Nilsson, 2000. – 5 p. (doi:10.17487/RFC3003).

3. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учебно-методическое пособие для студентов/ П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.