https://www.modscires.pro/index.php/msr/article/view/be4-218-030
DOI: 10.30889/2523-4692.2018-04-01-030

УДК 004.056.55

METHOD SEMANTICS HIDE INFORMATION IN THE AUDIO CONTAINER

МЕТОД СЕМАНТИЧЕСКОГО СОКРЫТИЯ ИНФОРМАЦИИ В АУДИО КОНТЕЙНЕРЕ

Plashenkov V.V. / Плашенков В.В.
d.m.s., prof. / д.в.н., проф.
Starodubtsev D.E. / Стародубцев Д.Е.
sen.teacher / ст.препод.
Koroleva E.V. / Королева Е.В.
c.t.s. / к.т.н.
Kaverin O.B. / Каверин О.Б.
c.f.s. / к.ф.н.
SPIN: 2176-192
Zuev A.N. / Зуев А.Н.
c.t.s. / к.т.н.
Cherepovets State University,
Russia, Vologodskaya obl.,Cherepovets, Sovetsky prosp., 8,162600
Череповецкий государственный университет,
Россия, Вологодская обл., Череповец, Советский просп. 8, 162600

Аннотация. *В статье рассматривается метод семантического сокрытия информации в аудио контейнере, позволяющий распознать попытки несанкционированного доступа к находящемуся в контейнере сообщению. Представлен алгоритм стеганографического преобразования. Актуальность представленной статьи заключается в том, что во всех отраслях деятельности человека вопросу информационной безопасности отводится первостепенное значение.*

Ключевые слова: *метод сематического сокрытия, аудио контейнер, преобразование информации, контроль несанкционированного доступа к сообщению.*

В условиях рыночных отношений конкуренция представляет собой один из основных стимулов развития экономики. Конкуренция порождает конфиденциальную информацию внутри субъектов рынка, что влечет необходимость ее защиты от обнаружения ее носителей. Иными словами, появляется необходимость применения на практике стеганографических методов. В настоящее время ведутся исследования и разработки методов маскировки сигналов, содержащих конфиденциальную информацию, на основе применения аудиоданных в интересах сокрытия необходимых сведений. Проведя сравнительный анализ применяемых в настоящее время аудио форматов, можно выделить существенные преимущества формата MIDI [1,с.85]:

- возможность воспроизведения всеми цифровыми устройствами;
- многоканальное хранение звуковой информации, позволяющее осуществить многоуровневое сокрытие полезных данных с возможностью внедрения дезинформации;
- простая программная и аппаратная реализация чтения, записи и редактирования скрытой информации.

Вербальная постановка задачи.

Для данных формата MIDI необходимо разработать метод сокрытия информации, позволяющего обеспечить большую или равную пропускную способность формируемого контейнера по сравнению исходной подбираемого готового контейнера с применением существующих методов в заданном формате. Метод должен обладать лучшей производительностью по сравнению с существующими аналогами.

Методика решения.

Суть предлагаемого метода заключается в преобразовании исходного сообщения в аудио контейнер. Такое преобразование осуществляется интерпретацией в виде мелодической последовательности двоичного потока сообщения. На рис. 1 представлен алгоритм, реализующий указанное преобразование MIDI-файла.

Алгоритм иллюстрирует процедуру интерпретации двоичного потока сообщения в формате MIDI-файла. Ключ пользователя должен содержать [3]:

- матрицу инцидентности сети кодирования (T);
- вероятности отношений между состояниями сети кодирования (P_m);
- число состояний сети, используемое в одном раунде кодирования (n);
- длительность каждого состояния сети в одном раунде кодирования (d_n).

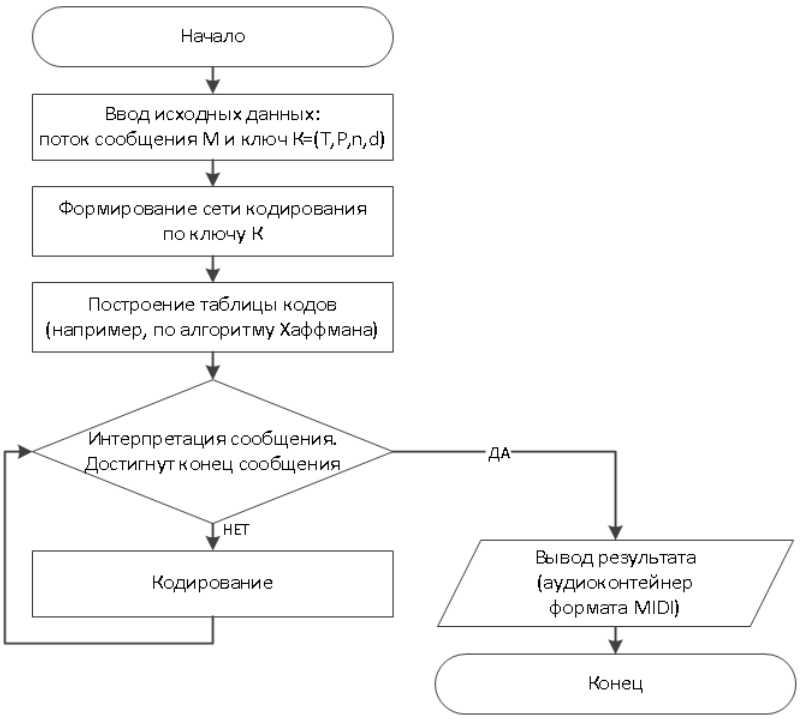

Рис. 1. Блок-схема алгоритма преобразования исходного сообщения в аудио контейнер.

На основании данных ключа формируется сеть кодирования, строится таблица вероятностей мелодических последовательностей, осуществляется преобразование сообщения в мелодический контейнер, который сохраняется в файле формата MIDI. Однако, недостаточно использование только лишь переходных вероятностей, определяемых ключом кодирования. Требуется

вычисление стационарных вероятностей обращения к оценке состояния в некоторый момент времени:

1. Определение полной вероятности по соотношению:

$P_1+P_2+ P_j+\ldots+P_m=1;$

2. Определение стационарных вероятностей состояний сети по соотношению:

$p_i=P_1p_1+ P_2p_2+P_jp_i+\ldots+P_mp_n,$

где n – число состояний сети, определяемое ключом;

m – число отношений, определяемое ключом;

$P_{j=[1,m]}$ – вероятности переходов в состояния\ n, определяемые ключом;

$P_{i=[1,n]}$ – стационарные вероятности состояний сети.

На рис. 2 представлена диаграмма пропускной способности методов сокрытия информации в файлах формата MIDI. Исходными данными являются данные, полученные при сокрытии одного и того же сообщения в одинаковом контейнере тремя различными методами и его преобразованием в мелодический контейнер предлагаемым выше методом. Диаграмма наглядно демонстрирует, что пропускная способность рассматриваемого метода (столбец с волнистой заливкой) выше на 18% по сравнению с тремя существующими методами сокрытия в формате MIDI.

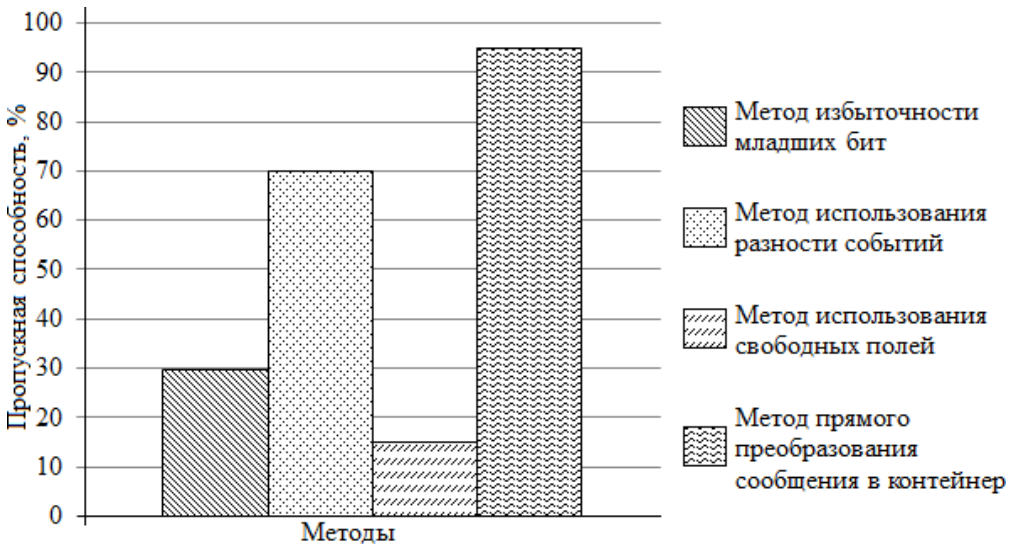

Рис. 2. Диаграмма пропускной способности методов сокрытия информации в MIDI-контейнере.

Предлагаемый алгоритм, согласно классификации методов внедрения информации [2,с.53], реализует гибридный метод, преобразующий исходное сообщение в контейнер путём иной интерпретации двоичного потока сообщения. Под иной интерпретацией следует понимать совпадение неизменных блоков двоичного потока сообщения с блоками мелодического контейнера.

Выводы.

Рассматриваемый в статье метод позволяет:

- рассматривать формируемый контейнер и скрываемое сообщение как

единое целое;

- обеспечить устойчивость контейнера к статистическим стегоатакам;
- предоставить возможность формирования многоканального контейнера;
- увеличить пропускную способность контейнера более чем на 18%;
- создать контейнер необходимой информационной ёмкости.

Литература:

1. Аленин А.А., Алексеев А.П. Исследование методов обнаружения вложений в звуковых файлах формата WAV // Безопасность информационных технологий, 2011.-С. 51-56.

2. Алексеев А.П., Аленин А.А. Методы внедрения информации в звуковые файлы формата MIDI // Инфокоммуникационные технологии. 2011.- Т. 9. С. 84-89.

3. Стародубцев Д.Е., Плашенков В.В. Метод стеганографического преобразования информации в гибридный звуковой контейнер // Вестник Череповецкого государственного университета. – 2015 г. – С. 29-32.

Abstract. *The article deals with the method of semantic concealment of information in an audio container, which makes it possible to recognize attempts to unauthorized access to a message in a container. The algorithm of steganographic transformation is presented. The relevance of the presented article is that in all branches of human activity the issue of information security is given the paramount importance.*

Key words: *method of semantic concealment, audio container, information transformation, control of unauthorized access to the message.*

References:

1. Alenin A.A., Alekseev A.P. (2011). Issledovanie metodov obnaruzheniia vlozheniy v zvukovykh failakh formata WAV [Investigation of methods for detecting attachments in WAV audio files] in *Bezopasnost informatcionnykh tekhnologiy*[Information Security], pp. 51-56

2. Alekseev A.P., Alenin A.A. (2011). Metody vnedreniia informatcii v zvukovye faily formata MIDI [Methods for introducing information into MIDI sound files] in *Infokommunikatcionnye tekhnologii* [Infocommunication technologies], vol.1, pp. 84-89

3. Starodubtcev D.E., Plashenkov V.V. Metod steganograficheskogo preobrazovaniya informatcii v gibridniy zvukovoy konteiner [The method of steganographic transformation of information into a hybrid sound container] in *Vestnik Cherepovetckogo gosudarstvennogo universiteta tekhnologii* [Vestnik Cherepovets State University], pp. 29-32