

Лабораторная работа № 9

Соккрытие информации в звуковых файлах формата MIDI

1. Цель работы

Изучить основные принципы скрытой передачи информации в звуковых контейнерах формата MIDI, получить навыки работы с программой Cakewalk.

2. Общие сведения

Для сокращения информации в музыкальных файлах формата MIDI в данной работе следует использовать музыкальный редактор (секвенсор) Cakewalk [1].

Секвенсор - устройство или компьютерная программа, способные запоминать все сообщения, формируемые при исполнении музыкального произведения. Пробразом секвенсора было механическое пианино с перфолентой, на которой записывалась исполняемая музыкантом композиция. Современные секвенсоры записывают не только партии одного пианино, но и партии остальных инструментов (включая ударные). При этом, как правило, партии отдельных инструментов записываются на отдельную дорожку (на отдельный трек).

Любопытной особенностью формата MIDI является то, что музыкальные композиции записываются с помощью управляющих сигналов (команд). Эти команды определяют высоту, момент начала звучания, длительность и громкость исполняемой ноты. Тембровую окраску звука обеспечивает звуковая карта, на которой хранятся фрагменты звуков (семплы). Музыка в формате MIDI не является оцифровкой аналогового сигнала. Такая форма музыкальных файлов обеспечивает высокую степень сжатия передаваемой информации. Файлы формата MIDI занимают в памяти на два-три порядка меньше места, чем файлы формата WAV и MP3.

Образно технологию MIDI можно представить так.

На передающей стороне находится дирижёр, который формирует управляющие сигналы. Эти сигналы определяют высоту, длительность, громкость, последовательность звучания нот, очерёдность игры различных инструментов и т.п. Сигналы по каналу связи передаются на приёмную сторону. На приёмной стороне находится оркестр, который играет под управлением этих сигналов (этого же дирижёра). Таким образом, сами звуки не передаются по каналу связи. По этой причине размеры MIDI-файлов небольшие.

Скрыть текстовую информацию в музыкальных файлах формата MIDI можно разными способами, например, незначительно изменяя громкость или длительность звучания нот [2]. Фактически соккрытие происходит в управ-

ляющих командах, которые определяют параметры звуков.

Скрытие текста происходит путём малозаметной вариации громкости звучания отдельных нот.

Перед внедрением текстовое сообщение должно быть преобразовано в бинарную форму (в последовательность битов). Затем эти двоичные числа должны быть использованы для изменения музыкального произведения.

Чтобы загрузить в секвенсор Cakewalk нужный файл следует выполнить следующие опции:

File – Open - ... - Задание 1 - v.mid

Вместо многоточия надо указать путь к папке **Задание 1**. Из списка доступных файлов нужно выбрать файл, имя которого v.mid соответствует заданному варианту. Под символом «v» понимается номер варианта.

Затем нужно вывести на экран Лист Событий (Event List). Делается это с помощью опций:

View – Event List

В поле Kind (Вид) указывается вид управляющих сигналов.

В данном случае первые 5 строк описывают системные установки. Начиная со строки 6 (Note), дано описание каждого исполняемого звука (см. рисунок).

The screenshot shows the 'Event List' window in Cakewalk Pro Audio. The window title is 'Cakewalk Pro Audio - [primer.mid - Event List - Track 3]'. The interface includes a menu bar (File, Edit, View, Insert, Realtime, Go, Track, Tools, Window, Help), a toolbar with various icons, and a transport control area with a time display showing 4:01:115. Below the toolbar is a control panel with buttons for Solo, Mute, and other track controls. The main area is a table with columns: Trk, HMSF, MBT, Ch, Kind, and Data. The table contains 13 rows of event data.

Trk	HMSF	MBT	Ch	Kind	Data
3	00:00:00:00	1:01:000	3	Control	121 0
3	00:00:00:00	1:01:000	3	Control	123 0
3	00:00:00:00	1:01:000	3	Control	91-External E 40
3	00:00:00:00	1:01:000	3	Control	93-Chorus dt 0
3	00:00:00:00	1:01:000	3	Control	64-Pedal [su 0
3	00:00:06:12	3:01:000	3	Note	E 5 72 2:033
3	00:00:07:06	3:02:000	3	Note	A 5 66 1:033
3	00:00:07:22	3:02:080	3	Note	C 6 68 73
3	00:00:08:16	3:03:080	3	Note	A 3 63 36
3	00:00:08:24	3:04:000	3	Note	E 5 78 28
3	00:00:08:24	3:04:000	3	Note	C 5 78 28
3	00:00:08:24	3:04:000	3	Note	A 4 78 28
3	00:00:09:18	4:01:000	3	Note	E 5 60 72

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Скрытие информации в MIDI-файлах

В соответствии с номером варианта необходимо скрыть первые десять символов текста в звуковых файлах формата MIDI. Звуковые контейнеры следует взять в папке **Задание 1**. Скрытие информации осуществить путём незначительной вариации громкости звучания музыкального произведения.

Таблица 3.1.1

Вариант	Текст
1	Когда есть ум и толк в словах у нас, Речь хороша и без прикрас. <i>И. Гёте.</i>
2	Но в первые полгода, милый друг, Порядок вам нужнее всех наук. <i>И. Гёте.</i>
3	Кто первым хочет быть и языком владеет, Тот первым быть всегда сумеет. <i>И. Гёте.</i>
4	Между теорией и практикой существует мост, по которому движение идёт в обе стороны. <i>И. Менделеев.</i>
5	Яд, мудрецом тебе предложенный, прими, Из рук же дурака не принимай бальзама. <i>О. Хайям.</i>
6	Ты лучше голодай, чем, что попало есть, И лучше будь один, чем с кем попало. <i>О. Хайям.</i>
7	Ад и рай – не круги во дворце мироздания, Ад и рай – это две половины души. <i>О. Хайям.</i>
8	Только знаю одно: ничего я не знаю - Вот итог всех моих размышлений под старость. <i>О. Хайям.</i>
9	Сгорел мой саквояж, но остались несгораемые идеи. <i>И.Ильф, Е.Петров</i>
10	Одни смотрят и слушают, другие видят и слышат. <i>АПА</i>
11	История должна быть историей не королей и битв, а идей. <i>А.Чехов</i>
12	Вечно человек будет недоволен, вечно будет желать больше, чем ему дано. <i>Р. Роллан</i>
13	Счастье не откладывай ни на час! Счастье надо пить свежим. <i>Р. Роллан.</i>
14	Кто много думает, тот мало говорит, стараясь втиснуть возможно больше мыслей в немногие слова. <i>Ирвинг.</i>
15	На пути к истине мы почти всегда обречены совершать ошибки. <i>Д. Дидро.</i>
16	Мы собрались у Феофанова по случаю диссертации, которую он решил начать писать с понедельника. <i>В. Коклюшкин.</i>

3.2. Задание 2. Извлечение информации, скрытой в MIDI-файлах

В соответствии со своим номером варианта необходимо извлечь текст из музыкальных файлов формата MIDI (номер файла соответствует номеру варианта). Заполненные контейнеры (стега) следует взять из папки **Задание 2**. В этих контейнерах сокрытие информации осуществлено путём вариации длительности звучания отдельных нот.

Логические единицы закодированы нечётными числами, а логические нули – чётными числами или нулями.

В зависимости от варианта внедрение осуществлено в различные треки (см. табл.3.2.1).

В этом задании извлекается только одна буква.

Таблица 3.2.1

Варианты	Треки
1	1
2	1
3	1
4	1
5	6
6	6
7	2
8	1
9	2
10	2
11	3
12	1
13	1
14	1
15	4
16	5

4. Порядок выполнения лабораторной работы

4.1. Методические указания к Заданию 3.1

В предлагаемой лабораторной работе внедрение информации будет осуществляться только в последний и предпоследний столбец команд. Чтобы убрать системные сообщения из списка событий, достаточно щёлкнуть по кнопке **Controller Events** (Контроллер Событий)



Рассмотрим, как в MIDI-файле скрыть русскую букву «Й». В соответствии с таблицей CP-1251 десятичный код этой буквы 201, а двоичный код 11001001. Внедрим полученный двоичный код скрываемой буквы по следующему алгоритму: если внедряется единица, то значение громкости должно быть нечётным числом.

В таблице **Event List** (Лист Событий) величину громкости описывает второй столбец справа. На рис. 2 показан фрагмент управляющих сигналов, в которых скрыта буква «Й».

Cakewalk Pro Audio - [primer.mid - Event List - Track 3]

File Edit View Insert Realtime Go Track Tools Window Help

4:01:080 00:00:10:04

75.00 1 2 3 1:01:000 53:01:000 1:01:000 1:01:000

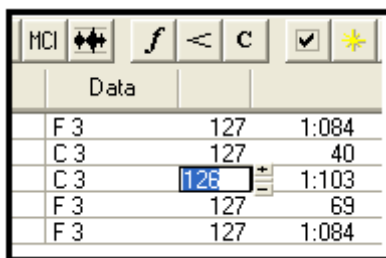
Trk	HMSF	MBT	Ch	Kind	Data		
3	00:00:00:00	1:01:000	3	Control	121	0	
3	00:00:00:00	1:01:000	3	Control	123	0	
3	00:00:00:00	1:01:000	3	Control	91-External E	40	
3	00:00:00:00	1:01:000	3	Control	93-Chorus de	0	
3	00:00:00:00	1:01:000	3	Control	64-Pedal [su	0	
3	00:00:06:12	3:01:000	3	Note	E 5	71	2:033
3	00:00:07:06	3:02:000	3	Note	A 5	67	1:033
3	00:00:07:22	3:02:080	3	Note	C 6	68	73
3	00:00:08:16	3:03:080	3	Note	A 3	64	36
3	00:00:08:24	3:04:000	3	Note	E 5	79	28
3	00:00:08:24	3:04:000	3	Note	C 5	78	28
3	00:00:08:24	3:04:000	3	Note	A 4	78	28
3	00:00:09:18	4:01:000	3	Note	E 5	61	72

Итак, двоичное число 11001001 внедрено в MIDI-файл путем форми-

рования чисел 71-67-68-64-79-78-78-61, которые управляют громкостью звучания каждой ноты трека 3.

Изменение значения громкости осуществляется в два этапа:

- сделать двойной щелчок в поле, где необходима коррекция громкости;
- с помощью счётчика изменить значения громкости (см. рисунок).



Если необходимо сменить номер трека, то нужно воспользоваться кнопкой **Pick Treck** (Выбор трека)



Обнаружить сделанное вложение на слух невозможно, так как, во-первых, изменения громкости незначительны, а, во-вторых, при каждом исполнении одного и того же произведения реальные исполнители играют по-разному.

Кроме того, запись секретной информации может быть осуществлена в партию лишь одного инструмента (например, контрабаса), что при звучании целого оркестра (или ансамбля) ещё больше маскирует скрытое сообщение.

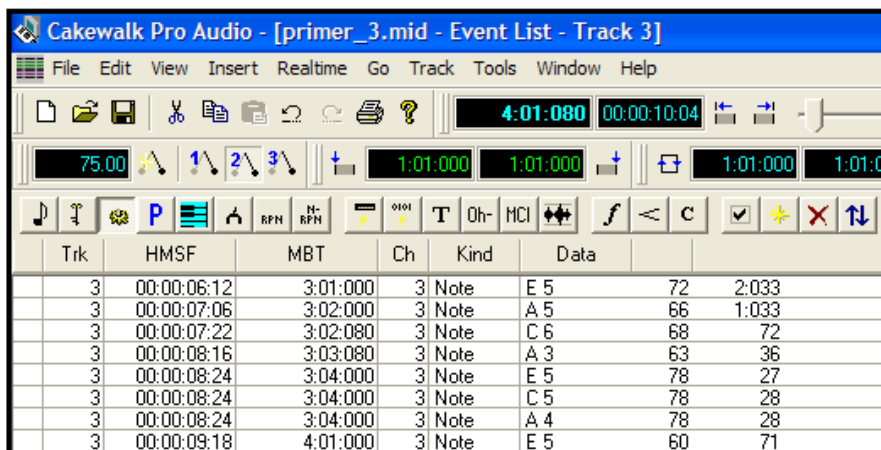
Логические единицы следует закодировать нечётными числами, а логические нули – чётными числами или нулями. Запись информации следует сделать в любой доступный трек.

4.2. Методические указания к заданию 3.2.

Скрытая передача информации может быть осуществлена путём незначительного изменения длительности звучания нот.

Можно договориться, что если некоторая условная длительность звучания ноты является нечётным числом, то это соответствует передаче логической единицы. Если же длительность является чётным числом или нулём, то это соответствует логическому нулю.

Следующий рисунок иллюстрирует порядок сокрытия байта 11001001 в длительности MIDI-файла (см. последний столбец).



Trk	HMSF	MBT	Ch	Kind	Data		
3	00:00:06:12	3:01:000	3	Note	E 5	72	2:033
3	00:00:07:06	3:02:000	3	Note	A 5	66	1:033
3	00:00:07:22	3:02:080	3	Note	C 6	68	72
3	00:00:08:16	3:03:080	3	Note	A 3	63	36
3	00:00:08:24	3:04:000	3	Note	E 5	78	27
3	00:00:08:24	3:04:000	3	Note	C 5	78	28
3	00:00:08:24	3:04:000	3	Note	A 4	78	28
3	00:00:09:18	4:01:000	3	Note	E 5	60	71

Таким образом, с помощью чётных (Ч) и нечётных (Н) чисел сформирована последовательность Н-Н-Ч-Ч-Н-Ч-Ч-Н, которая соответствует байту 11001001.

В этом задании в каждом варианте нужно извлечь из контейнера только одну букву (один байт).

В этом задании номер файла выбирается в соответствии с номером варианта. В таблице 3.2.1 указывается номер трека для каждого варианта.

В данной лабораторной работе рассматриваются лишь основные принципы сокрытия информации в MIDI-файлах. Несложно усовершенствовать рассмотренные методы внедрения секретного текста. Например, это можно сделать, распыляя биты по трекам, поочередно используя внедрение в громкость и длительность звучания нот. В этом случае внедрение должно производиться с помощью секретного ключа, который будет определять порядок распыления информации в пространстве и времени.

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать скриншоты с результатами кодирования (сокрытия информации в громкости звучания) и результат извлечения информации из контейнеров.

6. Контрольные вопросы

- 6.1. В чём состоит основная идея стеганографии?
- 6.2. Что собой представляют звуковые файлы формата MIDI?
- 6.3. Перечислите основные возможности секвенсора Cakewalk.
- 6.4. В чем принципиальное различие криптографии и стеганографии?
- 6.5. Что собой представляет трек?
- 6.6. В каких параметрах музыкального произведения можно скрытно передать информацию?
- 6.7. Чем отличаются музыкальные редакторы и секвенсоры?
- 6.8. Перечислите музыкальные редакторы, которые позволяют обрабатывать файлы формата MIDI.

7. Список литературы

1. Петелин Р. Ю. Cakewalk SONAR 7 Producer Edition: запись и редактирование музыки [Текст] / Р. Ю. Петелин, Ю. В. Петелин. – СПб.: БХВ - Петербург, 2008. - 880 с.
2. Алексеев А.П., Аленин А.А. Методы внедрения информации в звуковые файлы формата MIDI// Инфокоммуникационные технологии, том 9, № 1, 2011. Стр. 84-89.