УДК 681.322

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ВЛОЖЕНИЯ ИНФОРМАЦИИ В СУБТИТРЫ МУЛЬТИМЕДИА-КОНТЕЙНЕРОВ ФОРМАТА ASF, AVI И MATROSKA

Макаров М.И., Батаев А.Ф., Алексеев А.П.

Рассматриваются методы скрытой передачи информации в субтитрах видеофильмов.

Ключевые слова: стеганография, субтитры, авторское право.

Постановка задачи

Большое число пользователей персональных компьютеров применяют стеганографические методы сокрытия информации. Объекты, в которые осуществляют внедрение скрытой информации, называют контейнерами. Основными электронными контейнерами являются: текстовые документы, файлы с изображениями (например, фотографии), аудио- и видеозаписи, Web-страницы. Скрытно передавать информацию можно с помощью мессенджеров (например ICQ), чатов и сотовых телефонов (внедряя сообщение в SMS или MMS) и т.д.

Один из ярких примеров применения стеганографии был широко освещен в прессе в июне 2009 г., и впоследствии привлек внимание президента РФ Д. Медведева. На государственном сайте, публикующем информацию о тендерах, был применен метод замены букв кириллицы на сходные по написанию латинские буквы. Замена была сделана для того, чтобы информацию не могли найти «ненужные» заказчики.

Стеганография обеспечивает сокрытие факта передачи (или хранения) информации. Дополнительная защита передаваемой информации обеспечивается шифрованием вложения методами криптографии. Зашифрование и расшифрование информации осуществляется с помощью криптосистемы, о параметрах которой должны заранее договориться адресат и отправитель. Основные принципы криптографии (и стеганографии) предусматривают, что противнику известны алгоритм внедрения сообщения в контейнер и метод шифрования. Это так называемое правило Керкхоффа [1].

Многие мультимедиа файлы, размещенные в Интернете, имеют своих владельцев. Использование стеганографических методов внедрения информации, позволяет решить актуальную проблему: сохранение авторства на созданную мультимедийную продукцию (например, права на фильм).

Мультимедийные файлы обладают большой избыточностью, поэтому позволяют организовать скрытый канал связи с достаточной пропускной способностью. Можно выделить несколько методов сокрытия информации в текстовых документах (например, в субтитрах). В таблице 1 перечислены некоторые из них [2].

Таблица 1

Метод	Описание
Изменение интервала между предложениями	Метод позволяет вставить в текст сообщение, имеющее двоичный формат, путем размещения одного или двух пробелов после каждого символа завершения предложения. При этом одинарным пробелом может кодироваться логический ноль, а двойным пробелом – логическая единица
Изменение количества пробелов в конце тестовых строк	Метод заключается в добавлении пробелов в конце каждой строки. Кодировка может быть осуществлена так же, как в предыдущем методе
Изменение количества пробелов между словами	Метод позволяет скрывать данные в свободных местах текста
Синтаксический метод	Метод позволяет скрывать сообщения с помощью намеренно сделанных в предложении ошибок
Семантический метод	Метод позволяет скрывать сообщение с применением схожих по начертанию шрифтов текста
Метод кернинга	Метод использует для сокрытия информации кернинг (изменение расстояний между соседними буквами)

Первый метод сокрытия информации в субтитрах

В данной статье рассматриваются методы сокрытия информации в субтитрах видеофильма. Первыми широко применяемыми стандартами кодирования видео были MPEG 1 и MPEG 2. Стандарт MPEG 1 применялся для записи на дисках формата VideoCD (устаревший на данный момент времени). Стандарт MPEG 2 использовался для записи на диски DVD. В перечисленных форматах субтитры встраиваются в видеопоток, что усложняет доступ пользователя к редактированию субтитров. Поскольку эти форматы разрабатывались для обеспечения совместимости с аппаратными средствами просмотра (например, DVD-кинотеатр или игровая приставка Sony PlayStation), то работа со встроенными в них субтитрами на программном уровне существенно ограничена. По этой причине в данной статье мы не будем рассматривать их в качестве контейнеров для сокрытия информации.

Кроме перечисленных стандартов можно отметить следующие форматы: ASF, AVI и Matroska. В них применяется ряд видео кодеков, популярнейшими из которых являются представители семейства стандарта MPEG-4. Они позволяют помимо так называемых hard субтитров (те которые встроены в само видео) подключать и soft субтитры (они хранятся в отдельном файле).

Таблица 2

Символ	Десятичное значение	Двоичное значение
С	209	11010001
е	229	11100101
к	234	11101010
р	240	11110000
е	229	11100101
т	242	11110010

Рассмотренный метод сокрытия информации в субтитрах основывается на добавлении невидимых символов после сообщений, выводимых на экран. На рис. 1 изображен файл со скрытой информацией, а на рис. 2 показан кадр из фильма с указанным вложением.

После текста, отображенного на экране, содержится скрытый текст, закодированный невидимыми на экране символами. Для усложнения обнаружения скрытого канала связи вложения можно размещать через определенное число субтитров.

```
1
00:00:26,842 --> 00:00:29,480
Вы будете слушать мой голос.

2
00:00:30,609 --> 00:00:36,607
Он поможет Вам в
путешествии вглубь Европы.

3
00:00:38,247 --> 00:00:41,046
Всякий раз, как Вы услышите мой голос,

4
00:00:41,047 --> 00:00:43,686
с каждым словом, сказанным мною,
```

```
1¶
00:00:26,842·-->·00:00:29,480¶
Вы·будете·слушать·мой·голос.¶
¶
2¶
00:00:30,609·-->·00:00:36,607¶
Он·поможет·Вам·в¶
путешествии·вглубь·Европы.¶
¶
3¶
00:00:38,247·-->·00:00:41,046¶
Всякий·раз,·как·Вы·услышите·мой·голос,¶
¶
4¶
00:00:41,047·-->·00:00:43,686¶
с·каждым·словом,·сказанным·мною,¶
¶
```

Рис. 1. Слева – файл субтитров со скрытой информацией. Справа – тот же файл, но с отображением спецсимволов, которые переносят скрытую информацию

Рис. 2. Отображение видеофайла со скрытой информацией

Секретным ключом является порядковый номер субтитра, после которого находится скрытая информация. Таким способом в одном фильме можно передать текст объемом до 10 Кбайт. Передача большего объема скрытой информации не рекомендуется, так как это может вызвать подозрение третьей стороны.

У рассмотренного метода есть недостаток – некоторые программы воспроизведения субтитров (например, BSPlayer) отображают и непечатаемые (невидимые) символы. В результате этого происходит искажение изображаемого на экране текста субтитров.

Этот недостаток устраняется путем побитного вложения скрываемого сообщения. Для этого после каждого выводимого на экран сообщения помещается всего один невидимый символ, который если и будет воспроизведен, то не воспринимается зрителем как искажение текста. Для повышения криптостойкости скрываемая информация размещается не после каждого субтитра.

Извлечение скрытой таким образом информации происходит с помощью секретного ключа. Каждый субтитр, выводимый на экран, имеет свой порядковый номер. Это позволяет составить ключ, указывающий положение отдельного бита скрываемого сообщения. Например, после каждого пятого субтитра помещается один неотображаемый на экране символ (табуляция или пробел).

Расчет числа передаваемых восьмибитовых символов в одном фильме производится по формуле: $c = \frac{n}{8 \cdot k}$, где c – количество скрытно передаваемых символов, n – число субтитров в фильме, k – ключ. Пусть ключ задан числом 4, это значит, что после каждого четвертого субтитра находится один скрываемый бит. Недостатком этого метода является резкое сокращение объема скрытого текста. В среднем субтитры полуторачасового фильма содержат 1000 сообщений. Указанный в примере ключ, позволяет скрыть 1000 / 4 = 250 бит, что в восьмибитовой кодировке CP-1251 соответствует примерно 31 символу.

Второй метод сокрытия информации в субтитрах

В файле субтитров время показа текста записывается в формате: часы, минуты, секунды, миллисекунды. Изменение момента демонстрации субтитров в пределах от 1 до 9 мС не будет заметным для зрителя. Это объясняется психофизическими особенностями людей. При этом появляется возможность скрыть необходимую информацию.

Пример. Пусть ключ равен 5. Это значит, что после считывания трех десятичных чисел следующие пять чисел не содержат скрытой информации. В соответствии с кодовой таблицей CP-1251 символы открытого текста принимают значения от 0 до 255. При этом каждый символ кодируется всегда тремя десятичными числами. Старшие неиспользуемые разряды заполняются нулями.

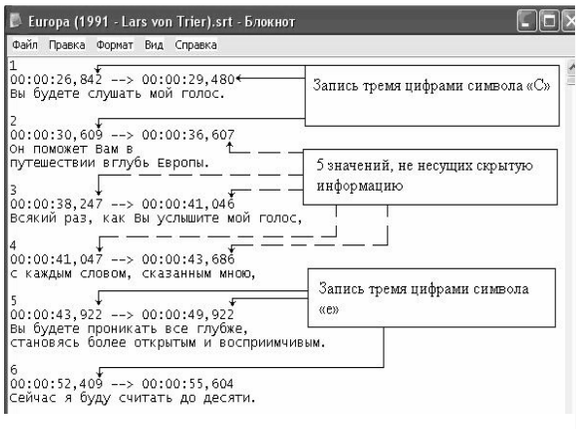

Рис. 3. Вложение информации во временные метки субтитров

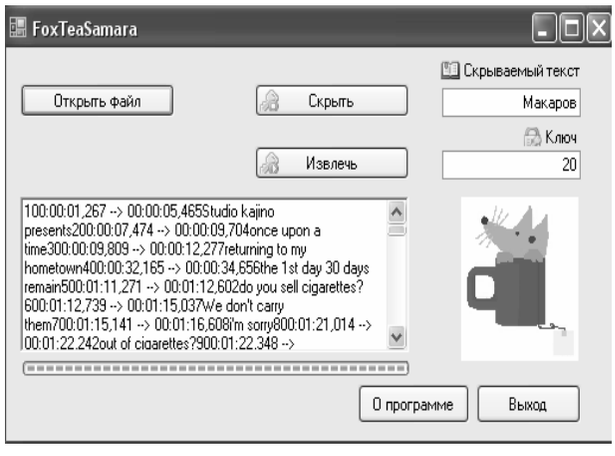

Рис. 4. Программа FoxTeaSamara

Зашифруем слово «Секрет». На рис. 3 в первом и втором субтитрах три цифры, расположенные в тысячных долях секунды (2, 0 и 9), образуют число 209. С помощью этого числа скрыт символ «С». В пятом и шестом субтитрах скрыт символ «е» и т.д. через каждые пять значений.

Расчет числа передаваемых восьмибитовых символов проводится по формуле: $c = \frac{2 \cdot n}{3 + k}$, где c – количество скрытно передаваемых символов, n – число субтитров в фильме, k – ключ. В среднем за полуторачасовой фильм отображается 1000 текстовых сообщений. В них содержится 2000 значений тысячной доли секунды. Для вложения сообщений можно использовать время начала и конца показа сообщения. Так как один символ кодируется тремя десятичными цифрами, то в фильме можно скрыть более 600 символов. Применение ключа уменьшает объем скрываемой информации. Так при шифровании с помощью ключа равного 7, файл субтитров может содержать 200 скрытых символов. Увеличение размера передаваемого сообщения в субтитрах и снижение риска его дешифрации можно осуществить применением криптографического мето-

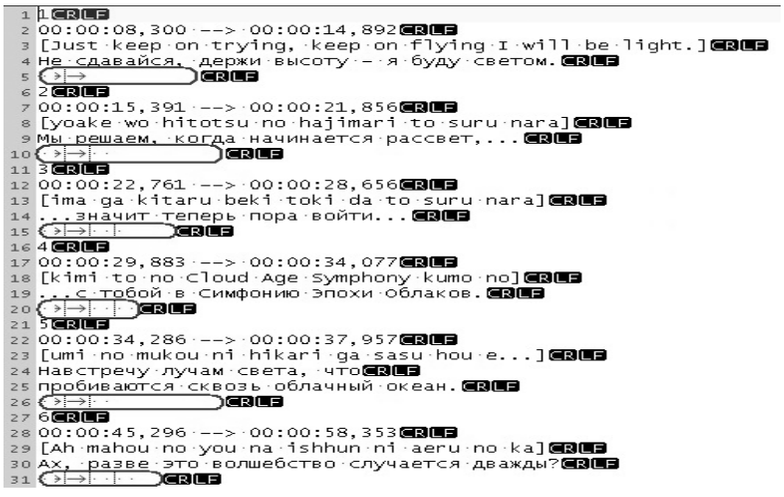

Рис. 5. Субтитры со скрытым сообщением

да шифрования с помощью словаря [3]. Для этого составляется словарь соответствия слов и числовых значений. Такой словарь должен быть у доверенных лиц как на передающей, так и на принимающей стороне. С помощью словаря во временных метках можно скрыть не один символ, а целое слово или даже фразу. Так же можно шифровать сообщения и методом, основанном на невидимых символах. Отличие будет состоять в том, что зашифрованными числами будут не значения из таблицы кодировки, а числа из словаря.

Для сокрытия информации в субтитрах была написана программа FoxTeaSamara, которая реализует метод сокрытия информации в младших разрядах временных меток. Программа составлена на языке C# и может применяться как инструмент цифровой подписи.

Третий метод внедрения сообщения в субтитры

В данном методе сокрытия сообщений используют имеющиеся пустые строки в файле с субтитрами формата *.srt. Пустые строки в таких файлах располагаются перед номерами реплик. В эти пустые строки записывается трехразрядный десятичный код скрываемой буквы (символа). Для скрытого внедрения информации используются символы табуляции, пробела и неразрывного пробела. Символ табуляции применяется для кодирования числа сотен, пробел - для кодирования числа десятков, а неразрывной пробел – числа единиц.

Например, чтобы закодировать число 234 нужно внедрить два символа табуляции, три пробела и четыре неразрывных пробела.

Извлечение вложения осуществляется следующим образом:

- находят строку с вложением;
- подсчитывают число символов каждого вида;
- определяют код вложенного символа;
- устанавливают значение вложенного символа.

На рис. 5 показаны места внедрения информации в субтитрах (они выделены овалами).

Для сокрытия информации в субтитрах с помощью третьего рассмотренного метода была написана программа DragonSamara. Программа составлена на языке Delphi.

Выводы

Стеганографические методы защиты информации увеличивают криптостойкость сообщений. Кроме того, стеганографические методы дают возможность защищать авторские права. В статье рассмотрена возможность скрытного вложения информации в субтитры фильма (например, можно записать фамилию автора фильма или название фирмы, которой принадлежат авторские права).

Литература

1. Алексеев А.П. Информатика 2007. М.: СОЛОН-ПРЕСС, 2007. – 608 с
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. – 288 с.
3. Алексеев А.П., Макаров М.И. Способ сокрытия информации с помощью словаря // Материалы IX МНТК «Проблемы техники и технологий телекоммуникаций». Изд. КГТУ им. А.Н. Туполева. Казань, 2008. – С. 447-448.

STEGANOGRAPHICAL METHODS OF INCLUSION OF THE INFORMATION IN SUBTITLES OF ASF, AVI AND MATROSKA MULTIMEDIA CONTAINER FORMATS

Alekseev A.P., Bataev A.F., Makarov M.I.

The article deals with the problem of information hiding in film subtitles of ASF, AVI and Matroska formats. It describes three ways of hidden data transmission or storage in subtitles. The research also covers the software implementation of stenographic enclosure of secret texts into subtitles.

Keywords: *steganography, subtitles, copyright.*

Макаров Максим Игоревич, ассистент Кафедры «Информатика и вычислительная техника» (ИВТ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 222-09-10. E-mail: ceo@ivt.psati.ru.

Батаев Александр Федорович, аспирант Кафедры ИВТ ПГУТИ. Тел. (8-846) 228-00-58. E-mail: ceo@ivt.psati.ru .

Алексеев Александр Петрович, к.т.н., доцент Кафедры ИВТ ПГУТИ. Тел. (8-846) 262-97-46. E-mail: ceo@ivt.psati.ru .

УДК 681.3

МЕТОД ОБРАБОТКИ ВИДЕОСИГНАЛОВ ДЛЯ ИЗМЕРЕНИЯ СКОРОСТИ ПРОТЯЖЕННЫХ ОБЪЕКТОВ

Васин Н.Н., Куринский В.Ю.

Приводится описание метода обработки видеосигналов для систем измерения скорости движения протяженных объектов. Описан метод определения величины смещения железнодорожного состава в плоскости регистрирующего прибора (ПЗС-матрицы цифровой видеокамеры), функционирование предложенного метода.

Ключевые слова: метод обработки видеосигналов, автоматизированная система измерения скорости движения протяженных объектов, совокупность строк видеоизображения, смещение гистограмм текущего и последующего кадров, повышение точности измерения.

Постановка задачи

Известный метод измерения скорости движения протяженных объектов [1-2] базируется на определении смещения протяженного объекта за период следования кадров. Его недостатком является низкая скорость вычислений, поскольку производится обработка всего кадра, и высокая погрешность измерения параметров протяженного объекта, обусловленная вибрацией видеокамеры, вызванной движущимся объектом измерения. Предлагаемый метод характеризуется высокой производительностью за счет обработки только части видеоизображения и повышенной точностью измерения скорости движения протяженного объекта при наличии вибрации видеокамеры, вызванной движением контролируемого объекта.

Оптическая ось видеокамеры устанавливается перпендикулярно направлению движения объекта. Направление движения объекта, его начало, расстояние до видеокамеры – известны. В качестве примера протяженного объекта выбраны вагоны, роспуск которых производится на сортировочной горке.

Метод определения величины смещения объекта

Для определения величины смещения вагона или другого подвижного объекта за известное время τ следования кадров видеокамеры на текущем *i*-ом кадре выделяется совокупность строк видеоизображения, то есть выделяется горизонтальная полоса по всей длине кадра, с количеством *X* пикселей по длине кадра, и высотой *n* пикселей. Полоса выделяется в области видеоизображения, где происходит отображение движения протяженного объекта. На данной горизонтальной полосе выделяется прямоугольная область, размер которой составляет $m \times n$, где n – высота прямоугольной области в пикселях, m – длина в пикселях (см. рис. 1).