встраивать в видеопоследовательность произвольный файл. При создании программы были проанализированы популярные кодеки и подобрано преобразование кадра, обеспечивающее наименьшие искажения и потери данных при сжатии видеофайла. Для исправления возникающих ошибок используется помехоустойчивое кодирование (сверточный код с декодером Витерби).

В работе рассматриваются основные методы встраивания информации в видеофайлы формата MPEG-2, проводится анализ, сравнение и обобщение этих методов для других видеоформатов. Рассматриваются особенности хранения аудиосигнала в видеофайлах и приводятся методы, использующие этот сигнал для сокрытия информации. Исследуются возможности компрометации реализованных алгоритмов с помощью методов статистического анализа.

ЛИТЕРАТУРА

1. *Аграновский А. В., Девянин П. Н., Хади Р. А., Черемушкин А. В.* Основы компьютерной стеганографии. М.: Радио и связь, 2003.
2. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002.
3. *Зырянов А. В.* Методы защиты авторских прав с использованием цифровых водяных знаков в видеоконтейнерах формата MPEG // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 142–156.

УДК 621.391.037.372

О ПРАВИЛЕ ВЫБОРА ЭЛЕМЕНТОВ СТЕГАНОГРАФИЧЕСКОГО КОНТЕЙНЕРА В СКРЫВАЮЩЕМ ПРЕОБРАЗОВАНИИ

Е. В. Разинков, Р. Х. Латыпов

Стеганография — это наука о скрытой передаче информации, достигаемой встраиванием секретного сообщения в цифровой объект, называемый стеганографическим контейнером [1]. В качестве контейнеров обычно используются цифровые изображения, аудио- и видеофайлы. Результат встраивания — стего — передается по каналу связи, контролируемому нарушителем. Основная задача нарушителя состоит в определении наличия встроенной в перехваченный цифровой объект информации [2, 3].

В работе предлагается общий метод повышения стойкости и пропускной способности стеганографических систем.

На стойкость стеганографической системы критическое влияние оказывает правило выбора элементов стеганографического контейнера, модифицируемых в процессе встраивания информации. Под элементом контейнера будем понимать атомарную часть цифрового объекта, модифицируемую в процессе встраивания информации (яркости цветовых компонент пикселов, коэффициенты JPEG-преобразования, коэффициенты вейвлет-преобразования и т. д.).

Задача состоит в построении метода оптимального выбора элементов контейнера для встраивания информации — метода, позволяющего максимизировать либо стойкость стеганографической системы при заданном размере скрываемого сообщения, либо пропускную способность стегосистемы при заданной стойкости.

Различные элементы контейнера могут быть объединены в непересекающиеся группы таким образом, что элементы одной группы будут иметь схожие свойства и одинаковое распределение.

Рассматриваем контейнер как набор из m групп элементов. Каждая группа характеризуется количеством k_i содержащихся в ней элементов и их распределением. Обозначим через C_i область допустимых значений элементов контейнера, входящих в i-ю группу. Предполагается, что модификация одного элемента i-й группы позволяет встроить q_i бит, $q_i = \lfloor \log_2 |C_i| \rfloor$. Таким образом, рассматриваем цифровой объект (контейнер, стего) в виде набора векторов элементов контейнера $c_1^i c_2^i \dots c_{k_i}^i$, $c_j^i \in C_i$, $i = \overline{1,m}$.

Обозначим через x_i количество модифицируемых элементов i-й группы, $0 \leqslant x_i \leqslant k_i$, $\sum x_i q_i = n$.

Пусть $f_i(c)$ — функция плотности распределения элементов i-й группы неизмененного стеганографического контейнера. Скрываемая информация имеет высокую энтропию, так как часто бывает зашифрованной и/или сжатой. Это свойство скрытого сообщения позволяет найти функцию плотности распределения элементов i-й группы контейнера со встроенной информацией — $\bar{f}_i(c, x_i)$, где x_i — количество измененных элементов:

$$\bar{f}_i(c, x_i) = \frac{k_i - x_i}{k_i} f_i(c) + \frac{x_i}{k_i} \cdot \frac{1}{|C_i|}.$$

Обозначим через $P(S)$ вероятность того, что в качестве контейнера будет выбран цифровой объект S:

$$P(S) = \prod_{i=1}^{m} \prod_{j=1}^{k_i} f_i\left(c_j^i\right).$$

Вероятность $\bar{P}(S)$ того, что в результате встраивания информации будет получено стего S, вычисляется аналогично:

$$\bar{P}(S) = \prod_{i=1}^{m} \prod_{j=1}^{k_i} \bar{f}_i\left(c_j^i, x_i\right).$$

Изложенное выше позволяет оценить стойкость стеганографической системы с помощью информационно-теоретического подхода и относительной энтропии (расстояния Кулльбака — Ляйблера) [4]:

$$D(P||\bar{P}) = \sum_S P(S) \log_2 \frac{P(S)}{\bar{P}(S)}.$$

Чем меньше величина $D\left(P||\bar{P}\right)$, тем выше стойкость стегосистемы. Задача оптимального распределения скрываемого сообщения в стеганографическом контейнере сводится к нахождению такого вектора $\{x_i\}_i$, $0 \leqslant x_i \leqslant k_i$, $\sum x_i q_i = n$, при котором величина $D\left(P||\bar{P}\right)$ была бы минимальной. Эта задача может быть решена, если функции $f_i(c)$ известны.

Полученные в работе результаты позволяют значительно повысить пропускную способность стеганографической системы при фиксированной стойкости или повысить стойкость стегосистемы при заданной пропускной способности. Цель последующих исследований состоит в адаптации предложенной модели к распространенным форматам изображений, аудио- и видеофайлов, что позволит создавать более совершенные стеганографические системы.

ЛИТЕРАТУРА

1. *Simmons G. J.* The Prisoners' Problem and the Subliminal Channel // CRYPTO83 — Advances in Cryptology, August 22–24, 1984. P. 51–67.

2. *Wayner P.* Disappearing Cryptography, Second Edition — Information Hiding: Steganography and Watermarking. Elsevier, 2002. 413 p.
3. *Cox I., Miller M., Bloom J., et al.* Digital Watermarking and Steganography. Elsevier, 2008. 593 p.
4. *Cachin C.* An Information-Theoretic Model for Steganography // LNCS. 1998. V. 1525. P. 306–318.

УДК 681.511:3

СТЕГОСИСТЕМЫ ИДЕНТИФИКАЦИОННЫХ НОМЕРОВ, УСТОЙЧИВЫЕ К АТАКЕ СГОВОРОМ[1]

Т. М. Соловьёв, Р. И. Черняк

В связи с бурным развитием медиаиндустрии в настоящее время все более актуальной становится задача защиты интеллектуальной собственности от противоправных действий. Ежегодно медиапиратство наносит колоссальные убытки видео- и аудиоиндустриям. Основной статьей дохода кинокомпаний по-прежнему является прокат фильмов в кинотеатрах, в то время как современные сервисы IPTV, Internet TV и другие остаются в стороне. Такая ситуация во многом обуславливается высокими рисками утечки премьерного фильма и, как следствие, снижения интереса к нему у пользователей.

В настоящее время для защиты от копирования и несанкционированного использования медиаконтента широко применяется такой класс цифровых водяных знаков (ЦВЗ), как идентификационные номера (ИН).

ЦВЗ могут содержать некоторую информацию о собственнике материала или о месте и времени его производства.

В случае применение ИН в контейнер, предназначеный каждому пользователю, внедряется персональный номер, позволяющий контролировать дальнейший путь этого контейнера. Если пользователь окажется медиапиратом и начнет распространение своей копии, то идентификационный номер позволит быстро определить его.

Согласно терминологии, используемой в работе [1], множества ИН называются *стегосистемами идентификационных номеров*. При этом, помимо типичных атак для ЦВЗ, таких, как перекодирование, аффинные и другие преобразования, для стегосистем ИН существует очень опасная *атака сговором*.

Под атакой сговором понимается следующее. Злоумышленник побитно сравнивает имеющиеся у него копии некоторого медиаданного, содержащие различные ИН, и заключает, что биты, в которых сравниваемые данные различаются, суть биты ИН. Затем он устанавливает эти биты в некоторые значения так, чтобы полученный ИН, называемый *ложным*, не совпадал ни с одним из использованных при сравнении. При этом злоумышленник преследует одну из следующих целей: уничтожить ИН либо изменить его таким образом, чтобы он идентифицировал кого-то другого.

Данная работа является продолжением работы [2]. Предлагается решение для противостояния атаке сговором. Продолжается исследование структуры стегосистем идентификационных номеров, устойчивых к данной атаке. Определяется наиболее опасный случай атаки сговором — *мажорирующая атака*. Обсуждается проблема идентификации группы пиратов с помощью полученного ими ложного ИН.

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).