

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

УДК 003.26

СТЕГАНОГРАФИЯ И СТЕГОАНАЛИЗ В ВИДЕОФАЙЛАХ

О. В. Моденова

В настоящее время в связи с ростом объемов информации и увеличением пропускной способности каналов связи все большую актуальность приобретает вопрос сокрытия информации в видеопоследовательностях. Передача цифрового видео в последние годы является типичным событием и не вызывает подозрения. Например, сервис YouTube насчитывает сотни миллионов видеофайлов, причем один и тот же видеоматериал встречается в разных форматах и разном качестве. Огромное количество видеофайлов размещается в P2P-сетях.

Были рассмотрены некоторые особенности использования форматов видеофайлов для сокрытия информации. Несмотря на то, что существует большое количество видеоформатов, на практике для сокрытия информации используются форматы MPEG-2 и MPEG-4. На русском языке практически отсутствуют публикации, посвященные встраиванию информации в другие видеоформаты [1–3].

В [2] описаны три способа внедрения информации в файлы формата MPEG-2: встраивание на уровне коэффициентов, на уровне битовой плоскости и за счет энергетической разницы между коэффициентами. Рассмотрим преимущества и недостатки этих способов.

Метод встраивания информации на уровне коэффициентов. Биты скрываемой информации встраиваются в коэффициенты дискретного косинусного преобразования (ДКП). Главной проблемой модификации коэффициентов ДКП в сжатом потоке видео является накопление сдвига или ошибок. Искажения, вызванные изменением коэффициентов ДКП, могут распространяться во временной и в пространственной областях. Поэтому для компенсации искажений добавляют специальный сигнал. В силу ограничения на битовую скорость, при внедрении изменяются только 10–20 % коэффициентов ДКП. При использовании данного метода скрываемая информация сохраняется при фильтровании, зашумлении (аддитивным шумом) и дискретизации.

Метод встраивания информации на уровне битовой плоскости. Этот метод отличается высокой пропускной способностью и небольшой вычислительной сложностью. Но есть и существенный недостаток: информация, встроенная таким образом, может быть легко удалена. При повторном наложении последовательности бит качество видео ухудшится незначительно, а скрываемая информация будет уничтожена.

Метод встраивания информации за счет энергетической разницы между коэффициентами. В основе этого метода лежит дифференциальное встраивание энергии (ДЭВ). Сложность алгоритма ДЭВ незначительно выше сложности метода встраивания на уровне битовой плоскости и значительно ниже сложности метода, основанного на корреляции с компенсацией ошибок предсказания. Метод ДЭВ может быть применен не только к видеоданным MPEG, но и к другим алгоритмам сжатия видео. Информация встраивается путем удаления нескольких коэффициентов ДКП, и

это имеет свои преимущества. Во-первых, в сжатый поток видеоданных не надо ничего добавлять, можно обойтись без повторного сжатия восстановленного потока видео. Во-вторых, удаление высокочастотных коэффициентов будет уменьшать размер стегообраза потока сжатых видеоданных по сравнению с исходным потоком. Алгоритм ДЭВ вносит в видео несколько меньше искажений, чем метод встраивания информации на уровне битовой плоскости. Для удаления скрытой информации требуется проведение более сложных вычислительных операций, чем встраивание новой произвольной битовой последовательности.

Если размер скрываемой информации небольшой по сравнению с объемом контейнера, то можно вносить изменения не в каждый кадр, а с некоторым интервалом. Это уменьшит накопление ошибок и может затруднить обнаружение факта сокрытия информации с помощью методов статистического стегоанализа.

Как правило, для сокрытия информации в видеопоследовательностях используются методы, использующие только видеопоток. Практически нет информации о сокрытии информации в аудиосигнале видеофайлов, хотя это позволило бы скрывать больший объем информации. В видеофайлах может быть упаковано различное количество звуковых дорожек, от 1 до 8 каналов для нескольких языков или нескольких вариантов переводов.

При переносе принципов сокрытия информации в неподвижных изображениях и в аудиофайлах нужно учитывать особенности, связанные со способами кодирования цифрового видео. Во время скрытия данных в видеопоследовательностях возникают трудности, так как одной из составляющих алгоритмов компрессии видеoinформации (в дополнение к компрессии неподвижного кадра) является кодирование векторов компенсации движения.

Для исправления возникающих ошибок при восстановлении информации из сжатого видео можно использовать помехоустойчивое кодирование. Например, использование сверточного кода с декодером Витерби обеспечивает достаточно высокую вероятность восстановления.

Применение вейвлет-преобразований и преобразований ДКП лучше подходит в случае необходимости защиты информации от активного злоумышленника, так как эти алгоритмы хорошо отделяют существенные детали от второстепенных.

Основной задачей стегоанализа является определение факта наличия скрытого сообщения в предполагаемом контейнере. Решается эта задача путем изучения статистических свойств сигнала. Например, распределение младших бит сигналов имеет, как правило, шумовой характер. Стегоаналитик проверяет соответствие реально наблюдаемой статистики ожидаемой. Обычно для этих целей используется критерий хи-квадрат.

Далее контейнер подвергается атакам, которые могут быть направлены на удаление или подмену скрываемой информации. Атаки применяются и в частотной, и в пространственной областях видеопоследовательностей. Основные типы атак на видеоконтейнер можно разделить на:

- 1) перекодирование видео с использованием алгоритмов сжатия с потерями;
- 2) изменение порядка кадров исходной видеопоследовательности (частный случай — удаление одного или нескольких кадров);
- 3) геометрические преобразования (всевозможные аффинные преобразования).

В целях анализа современного развития данного направления стеганографии был проведен поиск и исследование работы программ, реализующих сокрытие информации. В широком доступе была обнаружена лишь MSU StegoVideo, которая позволяет

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 пикселей, 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.