Бурдастых Юлия Николаевна
студентка
Пашкова Анна Сергеевна
студентка
Вихарева Анна Валерьевна
студентка
ФГБОУ ВО «Юго-Западный государственный университет»
г. Курск, Курская область

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СТЕГОВЛОЖЕНИЙ В ФАЙЛЫ ВИДЕОФОРМАТА

Аннотация: *в век развивающихся компьютерных технологий, информация часто представлена в виде аудио/видео файлов, поэтому возникает вопрос, как защитить видеофайл от изменений, копии. Такая наука, как стеганография, помогает скрыть и защитить информацию в видеопоследовательностях. В статье рассмотрены способы внедрения стеговложений в файлы формата MPEG-2, а также методы защиты от внесения изменений в видеофайл.*

Ключевые слова: *видеофайл, метод, стегоанализ, ДКП, битовая скорость, вилеоформат, алгоритм, стеганографии.*

В настоящее время все большую актуальность приобретает вопрос сокрытия информации в видеопоследовательностях. Рассмотрим некоторые особенности использования форматов видеофайлов (медиаконтейнеров) для сокрытия информации. Среди большого количества видеоформатов таких как MPEG, MPEG-1, MPEG-2, MPEG-4, HD, на практике основное предпочтение отдают форматам MPEG-2, MPEG-4. Рассмотрим несколько наиболее популярных метода внедрения информации в файлы формата MPEG-2: встраивание на уровне коэффициентов, на уровне битовой плоскости и за счет энергетической разницы между коэффициентами.

1. 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% коэф- фициентов ДКП. При использовании данного метода скрываемая информация сохраняется при фильтровании, зашумлении (аддитивным шумом) и дискретизации.

2. 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.

3. 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 сокрытия информации в видеопоследовательностях используются методы, использующие только видеопоток. 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 видеоинформации (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. Для исправления возникающих ошибок используется помехоустойчивое кодирование (сверточный код с декодером Витерби). В работе рассматриваются основные методы встраивания информации в видео-файлы 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.

Список литературы

1. [Электронный ресурс]. – Режим доступа: http://documents.tips/documents/54563e7bb1af9fa1628b49e4.html

2. [Электронный ресурс]. – Режим доступа: http://litfile.me/pages/406173/413000–414000?page=47

3. [Электронный ресурс]. – Режим доступа: http://www.rulit.me/books/.html

4. [Электронный ресурс]. – Режим доступа: http://mreadz.com

5. [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru

6. Моденова О.В. Стеганография и стегоанализ в видеофайлах Steganography and steganalysis in video files Текст научной статьи по специальности «Автоматика. Вычислительная техника» [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/steganografiya-i-stegoanaliz-v-videofaylah