путем удаления нескольких коэффициентов ДКП. 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 [4].

Стегоконтейнер может подвергается атакам, которые будут направлены на удаление или подмену скрываемой информации в видеоданных. Используются следующие виды атак:

– перекодирование видео с использованием алгоритмов сжатия с потерями (компрессия и видео с помощью кодеков изображения);

– изменение порядка кадров исходной видеопоследовательности (удаление одного или нескольких кадров, изменение частоты кадров, вырезание определенного временного отрезка видео);

– геометрические преобразования (изменение размеров кадра, изменение разрешения изображения, сжатие-растяжение).

ЛИТЕРАТУРА

1. Евсютин О.О., Кокурина А.С. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. – 2019. – № 1 (43). – С. 137-154.

2. Разинков Е.В., Латыпов Р.Х. О правиле выбора элементов стеганографического контейнера в скрывающем преобразовании // Прикладная дискретная математика. – 2010. – № 3. – С. 39-41.

3. Радаев С.В., Басов О.О., Мясин К.И., Мотиенко А.И. Встраивание стеганографических сообщений в видеофайлы формата MPEG-4 // Экономика. Информатика. – 2018. – № 4. – С. 773-785.

4. Моденова О.В. Стеганография и стегоанализ в видеофайлах // Прикладная дискретная математика. – 2010. – № 3. – С. 37-39.

УДК 004.56+003.26

Асп. Н.В. Попеня
(БГТУ, г. Минск)

МЕТОДЫ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ВИДЕОИНФОРМАЦИЮ

В настоящее время наблюдается проблема неограниченного неавторизованного копирования видеофайлов. Важной проблемой является определение подлинности полученной информации, то есть ее аутентификация.

Основное требование, которому должна отвечать система защи-

ты видеофинвормации – это, прежде всего, требование высокой надежности. Обычно для аутентификации данных используется средства цифровой подписи. Однако они не совсем подходят для обеспечения аутентификации мультимедийной информации. Дело в том, что сообщение, снабженное электронной цифровой подписью (ЭЦП), должно храниться и передаваться абсолютно точного [1].

ЭЦП применяется для подписывания уже готовых видеофайлов конечной длины. Электронная подпись каждого отдельного кадра не имеет особого смысла, поскольку мультимедийная информация может незначительно искажаться за счет сжатия, так и за счет влияния одиночных или пакетных ошибок в канале связи при передаче. При этом ее качество остается допустимым для пользователя, но цифровая подпись не будет работать. Получатель не сможет отличить истинное, хотя и несколько искаженное, сообщение от ложного. Это обуславливается особенностями зрительной системы человека. К свойствам зрительной системы относят слабую чувствительность к незначительному изменению яркости отдельных фрагментов или всего изображения, а также к незначительному изменению контрастности изображения, эффект маскировки [2].

Кроме того, мультимедийные данные могут быть преобразованы из одного формата в другой. Один из подходов к решению этой проблемы основан на встраивании в цифровые объекты цифровых водяных знаков (ЦВЗ) – специальных и обычно невидимых меток, которые содержат в себе информацию о владельцах объектов.

Можно сказать, что ЦВЗ способны защитить именно содержание видеосообщения, а не его цифровое представление в виде последовательности бит. Применение ЦВЗ не ограничивается приложениями безопасности информации.

Основные области использования технологии ЦВЗ могут быть объединены в следующие группы: защита авторских прав, защита от копирования (использования), скрытая аннотация документов, доказательство аутентичности информации, утентификация контента и скрытая связь [3].

Существует множество подходов, чтобы сделать водяной знак эффективным и стойким к атакам устранения. Алгоритмы ЦВЗ в пространственной области внедряют секретные данные, напрямую манипулируя пикселями в кадрах видеопоследовательности. Простота вычисления являются главным преимуществом таких методов.

Однако, такие методы уязвимы для атак и чувствительны к шуму и традиционным методам обработки сигналов, а также они ухудшают качество кадров видеопоследовательности. По сравнению с ме-

тодами пространственной области более широко применяются методы частотной области, которые встраивают водяные знаки в спектральные коэффициенты кадров последовательности.

Самим ЦВЗ может быть аутентичный код, информация об авторе. ЦВЗ могут быть как видимыми, так и невидимыми.

Обычно ЦВЗ классифицируются по 7 основным параметрам:

– объём характеризует размер сообщения;

– сложность измеряет любые затраченные усилия на внедрение, атаку, детектирование или расшифровку;

– обратимость позволяет говорить о возможность удалить ЦВЗ из помеченного сигнала, если полученный сигнал совпадает с исходным;

– прозрачность при помощи данных эталонного и тестового сигналам измеряет расхождение между ними;

– надёжность определяет тип дополнительной информации необходимой функции обнаружения/извлечения для работы;

– безопасность описывает устойчивость ЦВЗ по отношению к определённым атакам;

– верификация определяет тип дополнительной информации необходимой функции обнаружения/извлечения для работы.

Можно отметить, что основное требование к ЦВЗ, как и к любой системе защиты – это надежность и устойчивость к искажениям информации. Благодаря использованию ЦВЗ пользователи могут делится своим контентом с другими пользователями, сохраняя при этом подлинность видеофайлов. Тем самым стеганография становится одним из лучших на данный момент способов защиты авторских прав на свои произведения.

Одним из вариантов защиты авторского права на видеоинформацию также является контроль доступа к контенту. Это может быть как доступ только внутри определенной сети или доступ только с определенного устройства, так и геоблокировка (географический фильтр информации), которая блокирует контент по регионам и позволяет просматривать видео только в определенных странах. Также доступ к контенту по одноразовым ссылкам исключает часть несанкционированных подключений видеофайлу.

Меры, направленные на ограничение доступа к видеофайлу, должны быть эффективным. Однако, согласно исследованиям, ограничение доступа к ресурсу чаще всего может лишь затруднить доступ пользователя к нему [4].

Следует отметиться технические средства защиты авторских прав (ТСЗАП). В отличие от защиты от копирования, под ТСЗАП

подразумеваются более общий класс технологий, которые могут позволять ограниченное копирование, а также могут налагать другие ограничения, такие, как ограничение срока, в течение которого возможен просмотр или воспроизведение защищаемого произведения. При этом под ТСЗАП понимаются именно технические средства защиты, в то время как защита от копирования может включать также организационные, юридические и другие меры.

Большинство современных систем ТСЗАП использует криптостойкие алгоритмы защиты, однако эти методы не могут использоваться полноценно, поскольку основаны на предположении, что для получения доступа к зашифрованной информации требуется секретный ключ.

ЛИТЕРАТУРА

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: Солон-Пресс. 2009. – 272 с.

2. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Стеганографические системы. Критерии и методическое обеспечение: Учебно-методическое пособие / Под редакцией доктора технических наук В. Г. Грибунина. –Саров: ФГУП "РФЯЦ-ВНИИЭФ". 2016. – С. 25-29.

3. Печенкина А. Н., Карманов И. Н. Применение цифровых водяных знаков для защиты интеллектуальной собственности // Интерэкспо Гео-Сибирь. 2019. №6(2). – С. 59-168.

4. Нуруллаев Р. Т. Ограничение доступа к интернет-ресурсам как новый способ противодействия нарушениям авторских прав // Труды Института государства и права РАН. 2015. №2. – С. 171-181.

УДК 374.31

Доц. М. Ф. Кудлацкая
(БГТУ, г. Минск)

AGILE И SCRUM В ОБРАЗОВАНИИ

Развитие методологии Agile берет свое развитие еще в 30-е годы XX века, именно тогда физик и статистик Уолтер Шухарт из Bell Labs начал применять циклы Планируй-Делай-Изучай-Действуй (Plan-Do-Study-Act, PDSA) для улучшения производимых продуктов и процессов. Метод PDSA применяли в таких известных компаниях как Toyota, Honda, Xerox, Canon и др. [1]. Современный Agile с известными подходами для улучшения производства появился в 2001 году, когда группа программистов опубликовала Agile Manifesto. Тогда