Существует множество протоколов программного шифрования, которые защищены от взлома в различной степени. Отличие криптографических алгоритмов защиты информации от всех других методов защиты основано на свойствах самой информации с исключением свойств материальных носителей. Самыми распространенными среди средств криптографической защиты являются следующие типы протоколов: симметричные, в которых для шифрования и расшифровки используется один и тот же ключ: DES, AES, ГОСТ 28147-89, Camellia, Blowfish, RC4 и т.д. [1].

Анализ обучения слушателей переподготовки по специальностям, связанным с информационными технологиями, свидетельствует о недостаточной подготовке в области обеспечения информационной безопасности. Результаты анализа показывают, что в информационные курсы необходимо вводить темы, связанные с криптографической защитой информации. Для этих целей была модернизирована лабораторная работа в рамках курса «Основы алгоритмизации и программирования на языках высокого уровня», которая знакомит слушателей с основными принципами криптографической защиты данных. Знания, полученные в рамках данной работы, повысят уровень теоретической и практической подготовки слушателей, и в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Лебедев А.Н. Криптография с открытым ключом и возможности ее практического применения. Тем. сб. «Защита информации». 1992. Вып. 2.

ДОБАВЛЕНИЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ВИДЕОФАЙЛ ЧЕРЕЗ ИЗМЕНЕНИЕ МЕТАДАННЫХ

Н.В. Попеня

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Добавление цифрового водяного знака в видеофайл через изменение метаданных является одним из способов внедрения информации в видеофайл с помощью стеганографии. Этот метод основан на изменении метаданных видеофайла. Метаданные видеофайла – это информация, связанная с видеофайлом, которая содержит дополнительную информацию о видео, не относящуюся к самому видео, но необходимую для его управления и организации. Метаданные могут содержать информацию о длительности видео, разрешении, формате, частоте кадров, звуковых дорожках, а также информацию о дате создания, настройках камеры и другие данные, которые могут быть изменены без влияния на содержимое видеофайла [1].

Метаданные могут быть внесены в видеофайл во время его создания, например, с помощью программного обеспечения для обработки видео или камеры, которая записывает видео, а также могут быть добавлены после создания видеофайла с помощью специальных программных инструментов.

Алгоритм метода внедрения информации в метаданные видеофайла может включать следующие этапы:

1. Выбор метаданных видеофайла, которые могут быть изменены. Обычно это атрибуты, связанные с авторством, датой создания, идентификатором камеры и т.д.

2. Кодирование информации: информация, которую необходимо внедрить, должна быть закодирована в форму, которую можно вставить в метаданные.

3. Изменение метаданных видеофайла. Информация в метаданных может быть изменена с помощью программного обеспечения, которое позволяет редактировать

метаданные видеофайла. Для этого нужно указать тип метаданных и вставить закодированную информацию.

4. Проверка целостности после внедрения информации в метаданные. Это можно сделать, используя программное обеспечение, которое позволяет проверять контрольную сумму видеофайла или сравнивать файлы до и после внедрения информации.

5. Проверка и подтверждение информации. После проверки целостности необходимо убедиться, что информация была успешно внедрена в метаданные и может быть извлечена из видеофайла. Это можно сделать с помощью программного обеспечения, которое позволяет просматривать метаданные видеофайла или извлекать информацию из них.

Этот метод имеет свои преимущества и недостатки. Среди преимуществ можно выделить то, что изменение метаданных не влияет на содержимое видеофайла и не приводит к потере информации. Кроме того, этот метод может быть легко реализован с помощью специальных программных инструментов. Однако недостатком является то, что этот метод может быть относительно легко обнаружен и удален с помощью различных инструментов для анализа метаданных видеофайла. Кроме того, некоторые форматы видеофайлов могут не поддерживать изменение метаданных.

Список литературы

1. Ганжур М.А., Дзюба Я.В., Панченко В.А. Особенности цифровой стеганографии как метода обеспечения сокрытия данных // Проблемы современного педагогического образования. 2018. № 59-4.

МЕТОДЫ ВНЕДРЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЬ

Н.В. Попеня

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Цифровой водяной знак на видео позволяет скрыть некоторую информацию (например, авторские права) в видеофайле таким образом, чтобы она была невидима для человеческого глаза, но могла быть извлечена специальным программным обеспечением. Цифровой водяной знак может содержать информацию о владельце контента, дате и месте создания, а также служить как индикатор подлинности видео. Частотный и пространственный методы внедрения цифрового водяного знака – это два различных подхода к добавлению цифрового водяного знака кадры видеопоследовательности с помощью компьютерной стеганографии [1].

Частотный метод нанесения цифрового водяного знака заключается во внедрении цифрового водяного знака в частотном диапазоне видеофайла. Для применения этого метода применяется преобразование Фурье, которое позволяет разложить кадры видеопоследовательности на его частотные компоненты. В результате этого преобразования, кадры представляется в виде набора коэффициентов, которые характеризуют амплитуду и фазу различных частотных компонент. Далее, водяной знак внедряется в некоторые из этих коэффициентов. Наиболее эффективным является использование низкоамплитудных компонент, чтобы изменения, внесенные в них, были незаметны для человеческого глаза. После внедрения водяного знака происходит обратное преобразование Фурье, чтобы получить кадры с внедренным водяным знаком.

Частотный метод нанесения цифрового водяного знака может быть эффективен, если кадры видеопоследовательности являются визуально сложными и содержат