УДК 004.932.2

Б. С. Маркин, А. В. Чернышова
Донецкий национальный технический университет, г. Донецк
кафедра прикладной математики и информатики

ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ И КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ВИДЕОФАЙЛОВ

Аннотация

Маркин Б.С., Чернышова А.В. Использование стеганографических и криптографических средств для защиты видеофайлов. *Выполнен анализ стеганографических и криптографических алгоритмов для защиты видеофайлов. Произведен выбор формата видео для внедрения зашифрованной информации.*

Ключевые слова: *стеганография, криптография, ЦВЗ, алгоритм шифрования.*

Постановка проблемы. Задача защиты авторских прав, прав интеллектуальной собственности или конфиденциальных данных от несанкционированного доступа является одной из важнейших на сегодня проблем.

Преимущества представления и передачи данных в цифровом виде, среди которых можно отметить: легкость восстановления данных и высокую потенциальную помехоустойчивость, могут быть легко похищены или модифицированы. Поэтому вопрос использования методов защиты информации, в том числе и видеофайлов является актуальным.

К таким методам можно отнести криптографические и стеганографические методы, которые позволяют подписывать видеофайлы и, таким образом, подтверждать их подлинность при передаче другим пользователям, либо внедрять какую-либо секретную информацию, которая будет доступна только узкому кругу лиц.

Цель статьи – описать возможность использования криптографических и стеганографических средств защиты информации для защиты видеофайлов.

Постановка задачи исследования. Развитие средств вычислительной техники в последнее время дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, такие как речь, аудиозапись, изображения, видео. Известны также предложения по встраиванию информации в текстовые файлы и в исполняемые файлы программ.

Исторически направление стеганографического сокрытия информации было первым, но со временем во многом было вытеснено криптографией. Интерес к стеганографии возродился в последние два десятилетия и был вызван широким распространением мультимедийных технологий.

Таким образом, можно выделить по крайней мере две причины популярности в наше время исследований в сфере стеганографии: ограничение на использование криптографических средств в ряде стран мира и возникновение проблемы защиты прав собственности на информацию, представленную в цифровом виде [1].

Первая причина вызвала большое количество исследований в духе классической стеганографии (т. е., скрытие собственно факта передачи), а вторая – не менее многочисленные работы в сфере так называемых цифровых водяных знаков (ЦВЗ) – специальных меток, скрыто встроенных в изображения или кадры видеофайла с целью дальнейшего контролирования его использования.

ЦВЗ – это технология, созданная для защиты авторских прав мультимедийных файлов. Как правило, цифровые водяные знаки невидимы и представляют собой текст или логотип, который идентифицирует автора [2]. Таким образом, внедренный ЦВЗ может стать элементом защиты видеофайла.

Решение задач и результаты исследований. Для работы с видеоданными, а также для последующей реализации стеганографических и криптографических алгоритмов был выбран формат AVI (Audio Video Interleave — чередование аудио и видео).

Этот формат позволяет одновременно хранить изображение и звук. Изображение и звук записываются попеременно, так что после кадра идет запись звукового сопровождения к нему. Данный формат является наименее сжатым, поэтому является удобным с точки зрения разбиения на кадры и внедрения в них информации.

Результатом работы является программный продукт, с помощью которого можно внедрять информацию в отдельные кадры видеофайла. Общая схема работы программы представлена на рисунке 1.

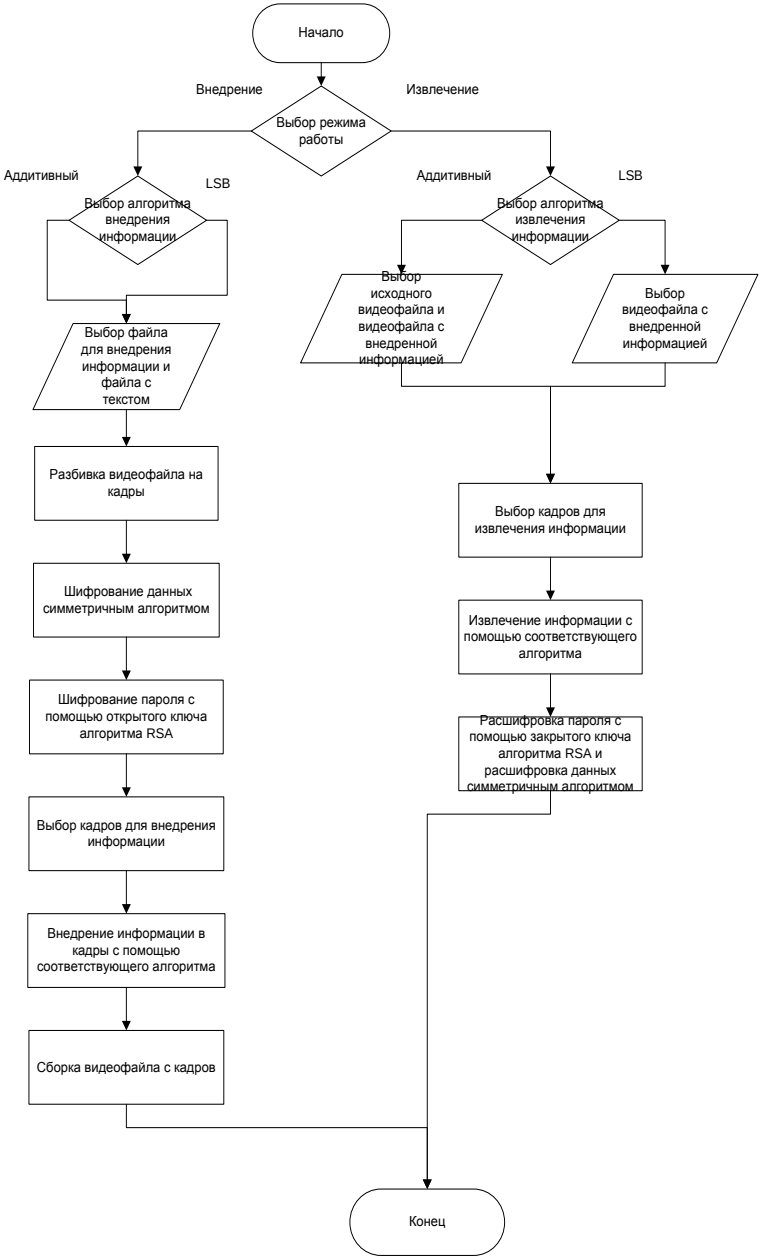

Рисунок 1 – Общая схема работы программы

В начале работы с программой необходимо указать режим работы (внедрение или извлечение информации), а затем выбрать необходимый алгоритм внедрения (аддитивный или lsb).

Далее выбираются необходимые файлы (видеофайл – для разбивки на кадры и текстовый файл, содержащий необходимую информацию для внедрения).

Если используется режим извлечения с применением аддитивного метода – необходимо кроме видеофайла с внедренной информацией открыть и исходный видеофайл без встроенной информации. Выбранные видеофайлы разбиваются на кадры. Для разбиения видеофайла на кадры используется библиотека Mitov VideoLab.

Далее происходит шифрование внедряемой информации с помощью одного из симметричных алгоритмов (DES, 3DES или Rinjdael), который выбирается пользователем. Кроме того, пользователь также может указать для каждого алгоритма желаемую длину ключа из возможных и режим шифрования (CBC, ECB или CFB).

Перед шифрованием данных симметричным алгоритмом, пользователь вводит пароль, который будет принимать участие в формировании ключа. Также данный пароль шифруется ассиметричным алгоритмом RSA для дальнейшей передачи пользователю, который будет извлекать информацию из видеофайла. Пароль шифруется с помощью открытого ключа, а расшифровывается с помощью закрытого. Ключи генерируются программно и записываются в xml файлы.

После шифрования информация внедряется в кадры с использованием выбранного ранее стеганографического метода. Кадры пользователь может выбирать произвольно. После внедрения информации все кадры вновь собираются в видеофайл.

Процесс извлечения происходит в обратной последовательности, т. е. сначала извлекается информация из указанных пользователем кадров, затем пользователь вводит зашифрованный пароль, после чего указывает закрытый ключ для расшифровки пароля с помощью алгоритма RSA.

Далее расшифрованный пароль используется при расшифровке симметричным алгоритмом внедренного сообщения. Исходное сообщение, а также зашифрованный и извлеченный тексты хранятся в текстовых файлах.

Пользовательский интерфейс программного продукта представлен на рисунке 2.

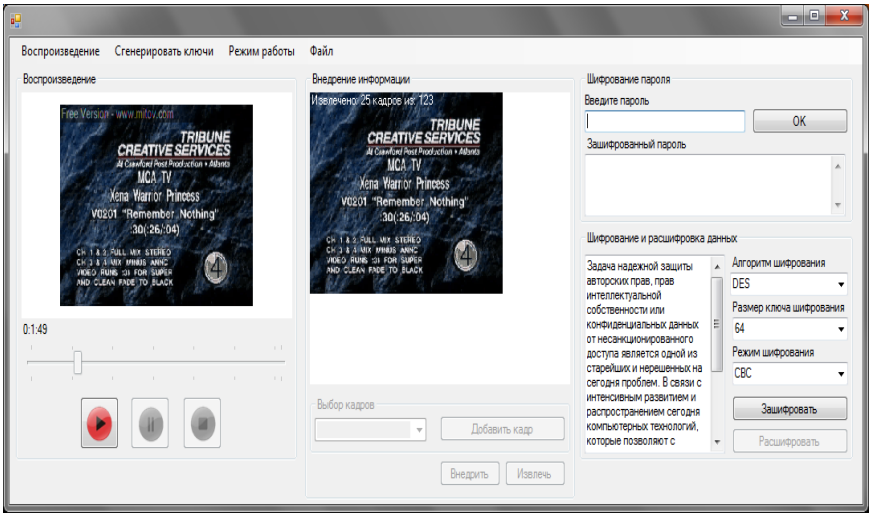

Рисунок 2 – Пользовательский интерфейс программы

Выводы. В результате выполнения данной работы были решены следующие задачи: были рассмотрены основные известные стеганографические алгоритмы и методы сокрытия информации в видеофайлах, а также проанализирован формат AVI, как наиболее подходящий для применения к нему рассмотренных стеганографических и криптографических алгоритмов.

Также следует отметить, что защита информации от несанкционированного доступа является сегодня все более и более актуальной.

Материалы данной работы являются основой для дальнейшей программной реализации алгоритмов сокрытия информации в видеофайлах. Также они могут быть использованы в высших учебных заведениях с целью автоматизации контроля знаний студентов в области стеганографии и криптографии.

Список литературы

1. Г. Ф. Конахевич. Компьютерная стеганография – К.: «МК-Пресс», 2006 – 288с.
2. Википедия. Цифровой водяной знак. Электронный ресурс. [Режим доступа]: http://ru.wikipedia.org/wiki/%D6%E8%F4%F0%EE% E2%EE%E9_ %E2%EE%E4%FF%ED%EE%E9_%E7%ED%E0%EA