УДК 004.3

А. В. Чернышова, ст. преп.,
Б. С. Маркин, студент
Донецкий национальный технический университет

Использование стеганографических и криптографических средств для защиты видеофайлов

В данной работе выполнен анализ стеганографических и криптографических алгоритмов для защиты видеофайлов. Произведен выбор формата видео для внедрения зашифрованной информации.

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

Введение

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.

Описание

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 программная система, с помощью которой можно внедрять информацию в отдельные кадры видеофайла, используя один из выбранных стеганографических алгоритмов. Перед внедрением информация может быть зашифрована с помощью одного из выбранных симметричных алгоритмов шифрования. Общая схема работы программы представлена на рисунке 1.

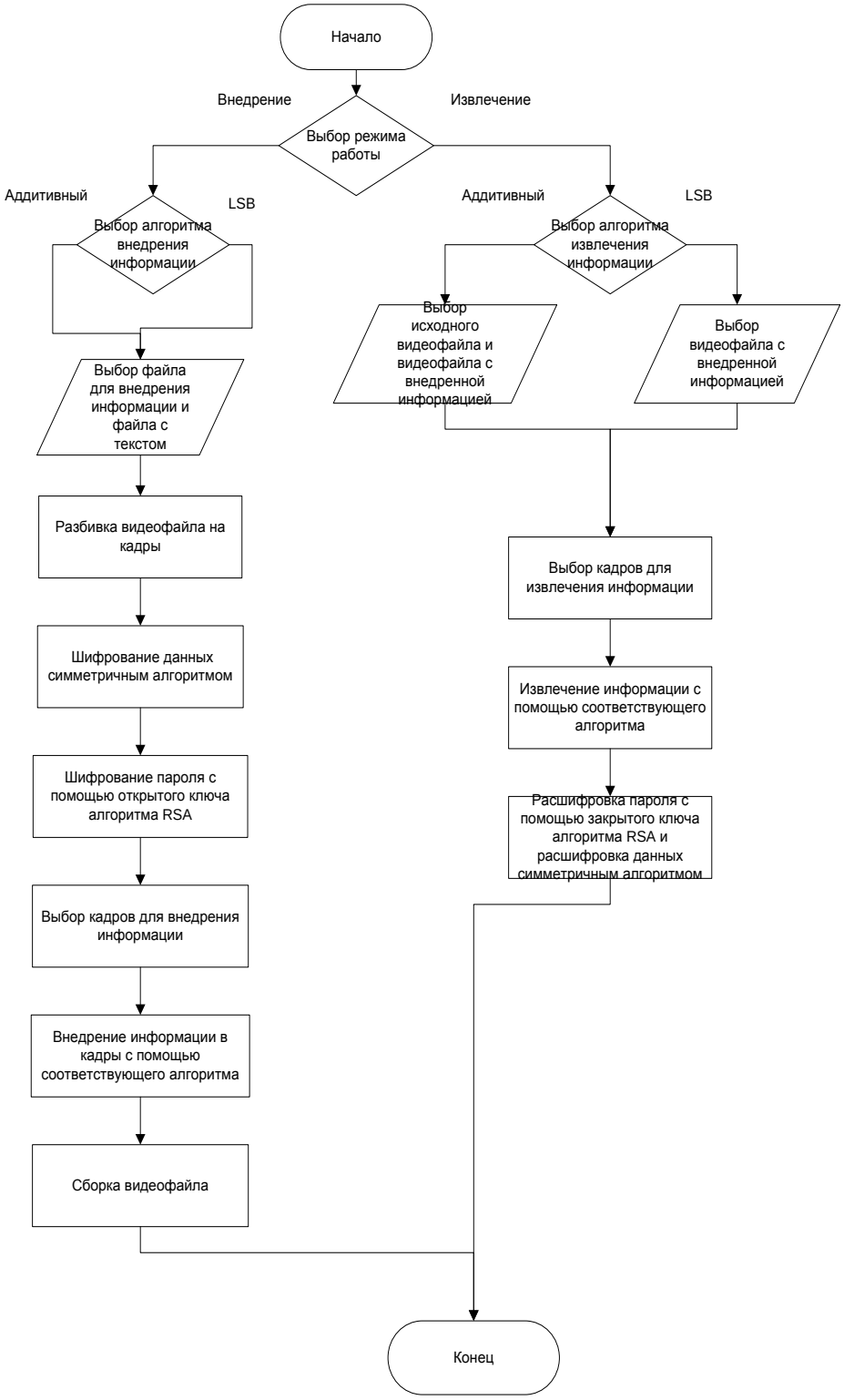

Рисунок 1 – Общая схема работы программы

В начале работы с программной системой необходимо указать режим работы (внедрение или извлечение информации), а затем выбрать необходимый алгоритм внедрения (аддитивный, lsb или алгоритм Куттера-Джордона-Боссена).

В аддитивном методе внедряемые данные представляют собой последовательность чисел w_i, которая внедряется в выбранное подмножество пикселей исходного изображения f. Основное и наиболее часто используемое выражение

для встраивания информации в этом случае имеет следующий вид:

$$f'(x,y) = f(x,y) + Lw_i \quad (1)$$

Где: *f'(x,y)* - цвет пикселя с координатами *x,y* после преобразования; *f(x,y)*- цвет пикселя с координатами *x,y* до преобразования; *L* - весовой коэффициент (целое положительное число); w_i-встраиваемое в пиксель *x,y* число (символ).

При использовании LSB алгоритма для встраивания информации используется младший значащий бит (LSB), который несет в себе меньше всего информации [3].

При использовании метода Куттера-Джордана-Боссена для встраивания информации используется синяя компонента цвета в формате RGB, изменения в которой наименее заметны для человеческого глаза [4]. Встраивание информации происходит по следующей формуле:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}$$

, где $\lambda = 0.1$, $Y_{x,y} = 0.3*R_{x,y}+0.59*G_{x,y}+0.11*B_{x,y}$ (2)

Для извлечения информации необходимо сначала спрогнозировать цвет пикселя:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma} \quad (3)$$

А затем сравнить с исходным цветом:

$$m_i = \begin{cases} 1, \text{при } B^*_{x,y} > \overline{B_{x,y}} \\ 0, \text{при } B^*_{x,y} < \overline{B_{x,y}} \end{cases} \quad (4)$$

Далее пользователю нужно выбрать 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. Библиотека устанавливается в виде дополнительных компонент к Visual Studio, поэтому прописывать пути к dll-файлам не нужно.

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, а также режим шифрования (CBC, ECB или CFB). Для шифрования информации применяются стандартные классы C#, а также пространства имен System.Security и System.Security.Cryptography.

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

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. Если пользователем был выбран аддитивный или lsb методы сокрытия информации, то для внедрения информации используются пиксели, у которых сумма координат является простым числом. Если же используется метод Метод Куттера-Джордана-Боссена, то информация внедряется в пиксели с шагом, равным десяти.

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.

Заключение

В результате выполнения данной работы были рассмотрены и проанализированы основные стеганографические методы внедрения информации, рассмотрена возможность использования криптографических алгоритмов шифрования вместе со стеганографическими для защиты видеофайлов формата AVI, создана программная система, позволяющая работать с видеофайлами формата AVI с применением стеганографических и криптографических алгоритмов. Материалы данной работы могут быть использованы в высших учебных заведениях с целью автоматизации контроля знаний студентов в области стеганографии и криптографии, а также при проектировании и создании программных средств, направленных на комплексную защиту информации в корпоративных системах.

Список литературы

1. Конахевич Г. Ф. Компьютерная стеганография / Г. Ф. Конахевич. – К.: «МК-Пресс», 2006 – 288 с.
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
3. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – Москва.: «СОЛОН-ПРЕСС», 2009 – 265 с.
4. Стеганографический метод Куттера-Джордана-Боссена [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/115287/

Надійшла до редакції 12.03.2014

А.В. ЧЕРНИШОВА, Б.С. МАРКІН
Донецький національний технічний університет

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ ТА КРИПТОГРАФІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ ВІДЕОФАЙЛІВ

Авторами розглянуті основні концепції захисту відеофайлів за допомогою цифрових водяних знаків. Обґрунтовано вибір стеганографічних та криптографічних алгоритмів для захисту відеофайлів формату AVI. Спроектована і реалізована програмна система для захисту відеофайлів формату AVI. Представлені результати роботи програмної системи.

Ключові слова: захист відеофайлів, криптографічні алгоритми, стеганографічні алгоритми, бібліотека Mitov VideoLab.

A.V. CHERNYSHOVA, B.S. MARKIN
Donetsk National Technical University

THE USE OF STEGANOGRAPHIC AND CRYPTOGRAPHIC MEANS FOR PROTECTION OF VIDEO FILES

The authors considered the main concepts of protection of video files by means of digital watermarks. The choice the steganographic and cryptographic algorithms for protection of video files of AVI format is reasonable. The results of program system work are presented.

Keywords: protection of video files, cryptographic algorithms, steganographic algorithms, Mitov VideoLab library.