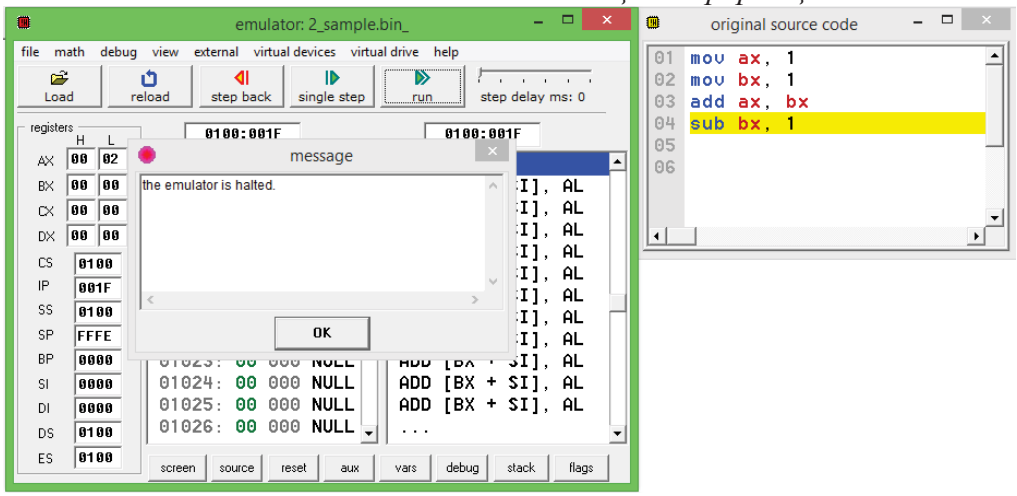

Рисунок 4 – Завершение работы эмулятора

На данной конференции приведён пример простейших операций. Курс разрабатываемых лабораторных работ будет сложнее и его цель – дать общее представление о работе микропроцессора и обучение студентов основам языка Assembler.

УДК 681.391

Студ. А.А. Чопик
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

На сегодняшний день выделяют два основных вида защиты информации: криптографию и стеганографию. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивается в другие данные значительно большего объема и будет выглядеть, например, как изображение, видео, аудиозапись, письмо.

Одной из основных причин популярности исследований в области стеганографии в настоящее время является проблема защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Это проблема повлекла за собой многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контролировать его использование.

В отличие от обычных водяных знаков ЦВЗ, как правило, являются невидимыми. Невидимые ЦВЗ анализируются специальным декодером, который выносит решение об их корректности. ЦВЗ могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию.

ЦВЗ могут быть трех типов: робастные, хрупкие и полухрупкие. Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стего (скрываемую информацию). Робастным ЦВЗ посвящено большинство исследований [1].

Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они применяются для аутентификации сигналов. Хрупкие ЦВЗ все же допускают некоторую модификацию контента. Это важно для защиты мультимедийной информации, так как законный пользователь может, например, пожелать сжать изображение. Другое отличие заключается в том, что хрупкие ЦВЗ должны не только отразить факт модификации контейнера, но также вид и местоположение этого изменения.

Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми к определенным операциям. Например, они могут позволять выполнять сжатие изображения, но запрещать вырезку из него или вставку в него фрагмента.

Для исследования методов использования ЦВЗ нами разработано программное приложение (рабочее название «*Stego* 1.0»), реализующее некоторые из методов внедрения ЦВЗ. На рисунке 1 приведен вид основного диалогового окна.

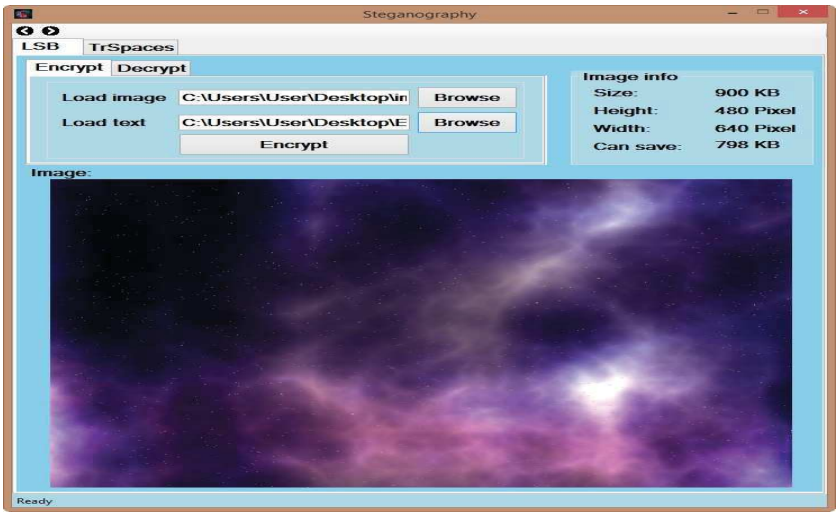

Рисунок 1 - Основное диалоговое окно программного средства «*Stego* 1.0»

Один из реализованных в программе методов – LSB (Least Significant Bit, наименьший значащий бит). Суть его состоит в замене последних значащих бит в контейнере (изображении) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами при этом должна быть не ощутима для человека.

Другой из реализованных методов внедрения ЦВЗ – это метод хвостовых пробелов, который предполагает дописывание в конце каждой строки одного пробела при кодировании единичного бита.

На рисунке 2 приведено окно, отображающее содержание основных компонент исследуемой стеганографической системы [2].

Данная программа позволяет внедрять ЦВЗ как в графические, так и в текстовые файлы.

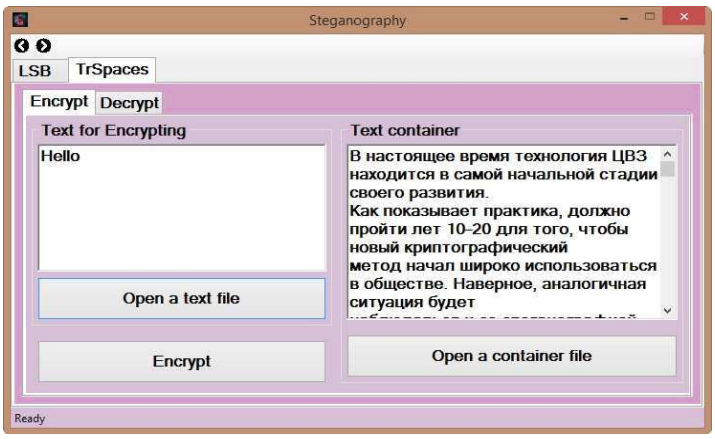

Рисунок 2 - Диалоговое окно программного средства «*Stego* 1.0» с отображением содержания основных компонент системы

Результаты выполненных исследований показали, что метод хвостовых пробелов оказался неэффективным для небольших файлов-контейнеров. В дальнейшем планируется реализовать способ, включающий в себя элементы различных видов внедрения ЦВЗ в текстовые файлы. Для достижения эффективности стремящейся к эффективности LSB-метода.

ЛИТЕРАТУРА

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И.Н. Оков, И. В. Туринцев. - М. : СОЛОН-Пресс, 2002. – 230 с.

2. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. – 2015. – № 6. — С. 152–156.