4. Интернет-портал [Электронный ресурс]/ ДонНТУ Портал магистров. – Режим доступа: http://masters.donntu.org/2015/fknt/sipakov/library/article6.htm. – Дата доступа: 5.04.2017.

УДК 004.056

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

СТЕГАНОГРАФИЧЕСКАЯ СТОЙКОСТЬ ИЗОБРАЖЕНИЯ-КОНТЕЙНЕРА К ОБЪЕМУ ОСАЖДАЕМОГО ТЕКСТОВОГО СООБЩЕНИЯ

Одной из основных причин популярности исследований в области стеганографии в настоящее время является проблема защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде [1-2]. При помощи методов стеганографии эта проблема решается следующим образом: есть тайное сообщение и контейнер – любая информация, используемая для сокрытия тайного сообщения. При помощи секретного ключа (стегоключа) отправитель встраивает сообщение в контейнер и получает стего. Получатель при помощи ключа может извлечь из стего тайное сообщение или, например, определить автора (рисунок 1).

Рисунок 1 - Стеганографическая система

Не менее важным является изучение вопросов заметности внедренных стеганограмм, потому что это непосредственно влияет на степень сохранности (стойкости) внедренной информации.

Целью исследования было изучить влияние объема осажденной в изображение-контейнер информации на заметность стеганограммы.

Для исследования разработано программное средство (рабочее название «STG 1.0»), реализующее один из стеганографических методов – метод LSB (Least Significant Bit, наименьший значащий

бит). Суть состоит в замене последних значащих бит в файле-контейнере (изображении) на биты скрываемого сообщения. На рисунке 2 приведен вид основного диалогового окна средства.

Данное программное средство позволяет осаждать информацию в определенное количество последних бит каждого байта изображения, (на основе модели RGB), а также извлекать эту информацию обратно в текстовый файл.

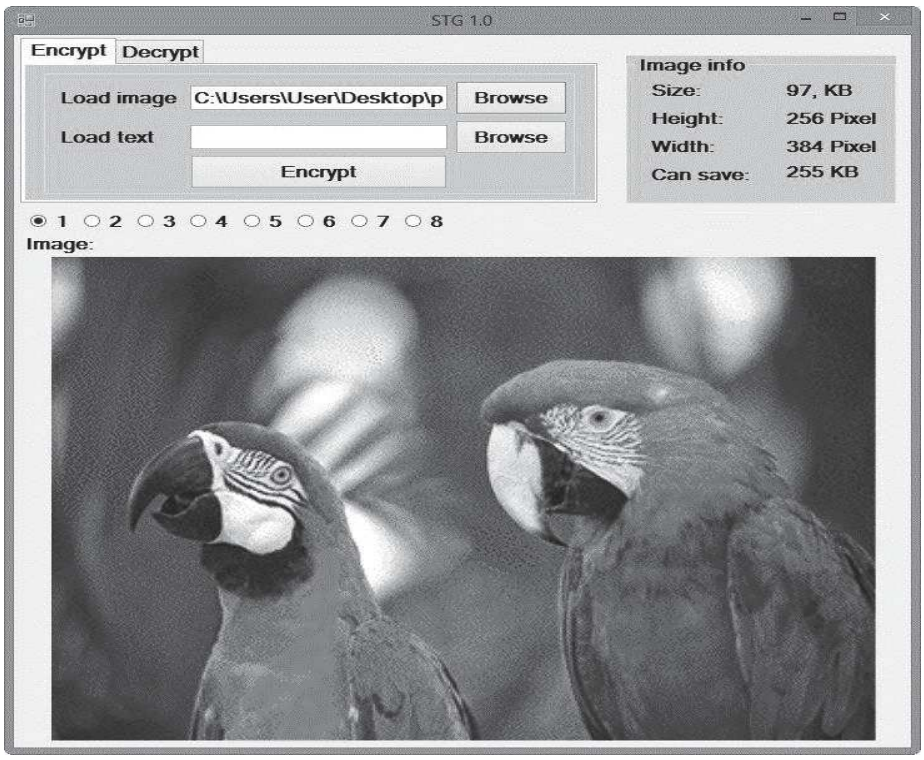

Рисунок 2 –Основное диалоговое окно программного средства «STG 1.0»

В качестве контейнера выбрано изображение в формате BMP, содержащее и мелкие детали, так и крупные части одного цвета. В качестве осаждаемой информации использовался отрывок произведения Historia Langobardorum, письменность – латиница.

Были проведены различные эксперименты с размером осаждаемой информации, количеством осаждаемых бит в изображении, использование различных комбинаций текстовой информации.

Результаты показывают, что при осаждении малого количества информации (по отношению к размеру осаждаемого изображения) или при осаждении небольшого количества бит (1-2) практически невозможно обнаружить видимых различий в изображении, если не использовать специализированных средств. Так как

стеганографическая стойкость определяется, в основном, эффективностью визуального анализа, то в данном случае можно говорить о высокой стеганографической стойкости.

При увеличении объема осаждаемой в изображение информации факт отличия от оригинала был очевиден. Так при осаждении 4-5 бит изображения можно видеть вполне различимое ухудшение качества (четкости) изображения. Изменяется насыщенность и резкость цвета. Наблюдалось уменьшение яркости изображения. Данное количество бит использовать для передачи какие-либо данные крайне опасно, так как такие изменения в изображении легко могут скомпрометировать информацию.

При еще большем увеличении объема осаждаемой в изображение информации, появлялись значительные изменения, детали заднего фона становились почти неразличимыми, изображение полностью теряло свои исходные черты.

В таблице 1 приведена статистика количества внедренной информации в зависимости от используемого количества бит каждого байта изображения.

Таблица 1 - Объем внедрённой информации при использовании различного количества бит

Количество используемых бит контейнера	Внедрено знаков (без пробелов)	Внедрено знаков (с пробелами)	Внедрено слов
1	18726	21674	2992
2	37413	43740	6026
3	56133	65743	9027
4	74635	87051	12055

На основе этого можно сделать вывод, что стеганографическая стойкость изображения-контейнера уменьшается при увеличении объема осаждаемой информации. Но даже если использовать для внедрения лишь небольшое количество последних бит изображения (1 или 2), то можно внедрить довольно большой объем информации и при этом подобное изображение будет обладать высокой стеганографической стойкостью.

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.

УДК 003.26+347.78

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

КЛОД ШЕННОН – ОСНОВОПОЛОЖНИК ЦИФРОВЫХ ТЕХНОЛОГИЙ И ТЕОРИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Клод Элвуд Шеннон (1916-2001 гг.) – американский инженер и математик. Человек, которого называют отцом современных теорий информации и связи.

Теория информации неразрывно связана с опубликованной в 1948 году статьей К. Шеннона «Математическая теория связи». Фактически данная работа предопределила путь, по которому с тех пор развивается теория информации. В своей книге Шеннон изложил способ, как количественно характеризовать сигнал. Для этого он использовал величину, которая называется количеством информации, или энтропией.

Энтропия означает мера неопределённости или непредсказуемости информации. Это количество информации, которое приходится на одно элементарное сообщение источника. Энтропия применяется во многих системах. Рассмотрим применение энтропии для анализа сложности пароля. Энтропия пароля (сложность пароля, измеряемая в битах), сгенерированного случайным образом, находится по следующей формуле:

$$H = L\frac{lnN}{ln2}, \quad (1)$$

где L – набор символов в пароле, N – количество символов в используемом алфавите.

Вывод состоит в том, что чем меньше сложность пароля, измеренная в битах, тем легче его взломать методом полного перебора.