УДК 004.056+347.78

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

СТЕГАНОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ТЕКСТОВ-КОНТЕЙНЕРОВ НА ОСНОВЕ ЯЗЫКОВ РАЗМЕТКИ

Во все времена существовала необходимость передавать информацию, но в XXI веке этот вопрос стоит на первом месте. Зачастую передаваемая информация имеет строго конфиденциальный характер и нуждается в тайной пересылке. С задачей тайной передачи «справляется» криптография, делая невозможным чтение передаваемой информации без знания ключа. Но есть другой подход к защите пересылаемых данных. Можно не шифровать информацию, а делать ее «невидимой». Для этих целей используют стеганографию. Стеганография – это наука и искусство передавать сокрытые данные, внутри других, не сокрытых данных. Скрываемую информацию называют стегосообщением, а данные, внутри которых располагается стегосообщение, называют контейнером. Основным преимуществом стеганографии над криптографией является то, что само наличие скрытой информации определить затруднительно.

Цифровая стеганография — направление стеганографии, основанное на внедрении дополнительной информации в цифровые объекты. В качестве контейнеров цифровой стеганографии можно использовать изображения, видео, музыку, текст.

Метод основанный на стеганографии подразумевает, что сам контейнер, несущий в себе данные, подвергнется незначительным изменениям. Наиболее важным в данном процессе является то, что эти изменения не должны отразится на визуальном отображении контейнера.

Роль стеганографического контейнера может выполнить html-документ. Основной акцент при встраивании информации в html-документ делается на то, что не все символы разработанного документа видны при отображении в браузере.

Известно, что при интерпретации html-документа браузер не придает значения тому, какой тип кавычек используется при его создании. Следовательно, если заменить какую-нибудь пару кавычек в валидном html-документе, например, с двойной на одинарную, то при визуальном анализе документа со стороны пользователя в браузере

никакой разницы видно не будет. Используя эту технику, в html-документ можно осадить бинарную последовательность.

Перед тем как начинать осаждение информации нужно убедиться в том, что контейнер имеет достаточную информационную емкость. Емкость контейнера определяется как количество пар кавычек во всем документе.

При встраивании последовательности бит условимся, что единице будет соответствовать двойная кавычка, а нулю одинарная. Начиная с первой пары кавычек в документе будем ставить ей в соответствие бит встраиваемого сообщения и, при необходимости, изменять тип кавычки на противоположный (например, первая пара кавычек в документе двойная, а первый бит осаждаемой последовательности – нулевой, следовательно, необходимо тип кавычек заменить на одинарный).

При использовании данного метода также необходимо заранее определить количество бит, отводимое под один символ сообщения. Установка количества бит позволяет не использовать впустую место в контейнере. Ведь если необходимо передать текст, состоящий только из букв английского алфавита, то для представления одного символа в двоичном виде будет вполне достаточно семи бит, в отличие от русского алфавита где для представления одного символа необходимо уже как минимум одиннадцать бит.

В конец осажденного сообщения встраивается уникальная последовательность, указывающая на то, что сообщение закончилось.

Для демонстрации вышеописанного метода создано программное средство (HTMLStego), которое позволяет осаждать в html-документ текстовую информацию.

При создании программного средства использовался язык программирования C#.

В процессе создания были разработаны следующие классы (рисунок 1): HTMLFile, FileManager, Embedder, Extracter.

HTMLFile – в своем составе имеет свойство File, представляющее собой загруженный файл html, а также метод GetContainerCapacity, позволяющий в зависимости от количества бит отводимых под один символ вычислять емкость контейнера.

FileManager – предназначенный для ввода и вывода html-документа.

Embedder – предназначенный непосредственно для осаждения информации. Метод MakeBinaryString конвертирует сообщение в двоичный вид. Метод EmbedMessage, последовательно проходя по

сообщению и ставя в соответствие очередную пару кавычек, изменяет ее при необходимости.

Extracter – при помощи ExtractMessage извлекает бинарную последовательность из прочитанного документа пока сообщение не закончится (проверяет IsEndOfMessage). После извлечения использовав метод RestoreMessage из бинарной последовательности получаем исходное сообщение.

Для осаждения сообщения следует указать количество бит, отводимое под один символ сообщения, затем загрузить контейнер, нажав на кнопку «Открыть HTML файл» и выбрать из файловой системы html-документ (рисунок 2).

После загрузки контейнера существует возможность узнать максимально возможное количество символов, которое можно осадить в контейнер. Осаждаемое сообщение вводится в поле «Встраиваемое сообщение». Для осаждения сообщения необходимо нажать кнопку «Встроить».

Для извлечения осажденного сообщения достаточно открыть стегоконтейнер, нажав на кнопку «Извлечь сообщение» и выбрать html-документ из файловой системы.

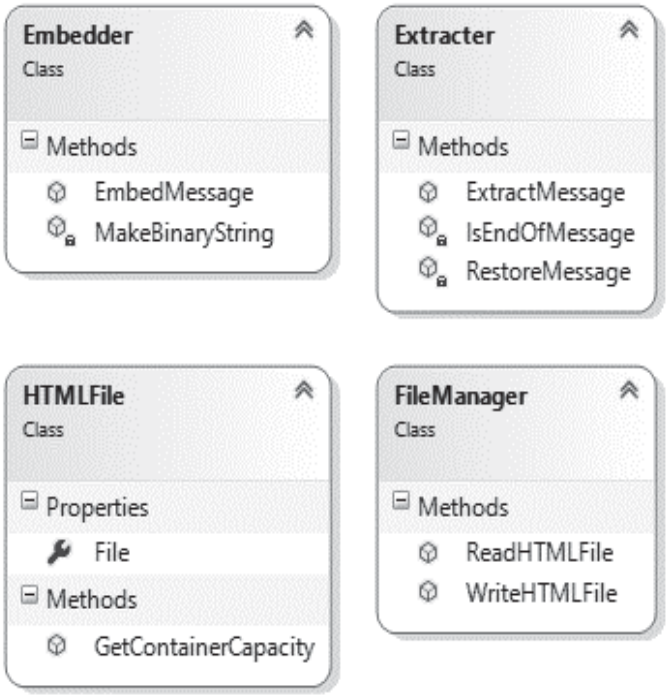

Рисунок 1 – Классы, представляющие функционал для осаждения информации

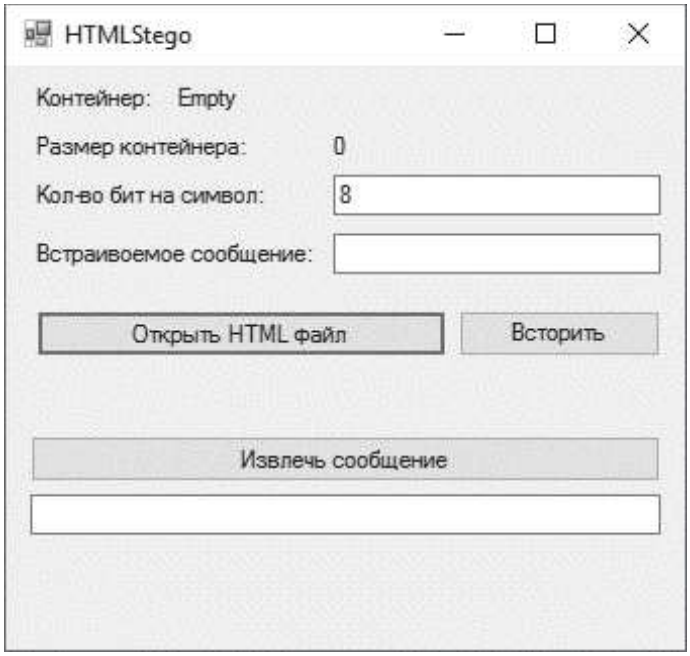

Рисунок 2 – Главное окно программного средства HTMLStego

Изложенный выше метод позволяет в документы типа html/xml встраивать текстовую информацию. Основная идея заключается в том, что при встраивании битовой последовательности каждому биту ставится в соответствие определенный тип кавычек, и при необходимости этот тип изменяется. При модификации контейнера его структура практически не изменяется.

В документе с n парами кавычек можно закодировать n бит сообщения. Выявить данный метод возможно только при просмотре кода html-документа. Подозрение может вызвать то, что зачастую при разработке сайтов используется какой-либо один тип кавычек.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стега-нографии и обфускации/ П.П. Урбанович. – Минск : БГТУ, 2016, – 220 с.

2. Интернет-портал [Электронный ресурс]/ Стеганография & путешествия. – Режим доступа:http://www.nestego.ru/2012/05/xml-html.html. – Дата доступа: 20.03.1017.

3. Интернет-портал [Электронный ресурс]/ Стеганография & путешествия. – Режим доступа: http://www.nestego.ru/2012/05/blog-post_03.html. – Дата доступа: 20.03.1017.

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