УДК 003.26+347.78

П. П. Урбанович, проф., д-р техн. наук;
Н. П. Урбанович, студ.; А. В. Риморев, студ.;
Т. В. Коваленок, студ. (БГТУ, г. Минск)

ПРИМЕНЕНИЕ ТЕКСТОВОЙ СТЕГАНОГРАФИИ ДЛЯ ЗАЩИТЫ И ПЕРЕДАЧИ ИНФОРМАЦИИ

В последнее десятилетие возрос интерес к методам скрытия и передачи одной информации в другой. Тот факт, что незаконно может производиться неограниченное количество копий, привел людей к изучению возможности встраивания серийных номеров, а также информации об авторских правах в аудио- и видеоданные, коды программ и текстовые файлы.

Наука, которая занимается исследованием методов сокрытия одной информации в другой, называется стеганографией [1].

Практически все существующие методы в рассматриваемой предметной области и реализующие их алгоритмы (стегоалгоритмы) можно разбить на 4 основные категории: преобразования текста; методы, использующие избыточность аудиоинформации; методы, использующие избыточность видеоинформации; методы, использующие избыточность графической информации.

Текстовая стеганография скрывает сообщения в текстовых файлах (контейнерах) отнюдь не очевидным способом, который называется семаграммой или открытым кодом.

Авторами данной статьи проанализирована эффективности различных методов текстовой стеганографии. Наиболее часто используемый метод заключается во внедрении секретного сообщения путем использования пробелов различной длины между словами текста-контейнера. Наиболее очевидным решением является использование одного пробела для кодирования символа «0» секретного сообщения, а двух для символа «1» (либо наоборот).

Чтобы избежать двойного пробела, который возникает при применении вышеописанного метода, можно использовать тот факт, что пробел кодируется символом с кодом 32, но в тексте его можно заменить также символом, имеющим код 255 (или 0), который является "невидимым" и отображается как пробел. Этот метод получил название метода невидимых символов.

Методы изменения межстрочных интервалов и изменения интервала табуляций аналогичны выше описанному методу изменения количества пробелов, только в этом случае меняется не количество пробелов, а соответственно расстояние между строками и интервал

табуляции. Метод изменения регистра использует регистры букв для внедрения скрытого сообщения.

Метод одинакового начертания символов заключается в том, что большинство стандартных шрифтов (Times New Roman, Arial, Courier New и другие) производят одинаковое отображение на экране разных символов русского и английского алфавита. Таким образом, встраивание стегосообщения в контейнер возможно путем замены символа русского алфавита на такой же одинаково отображаемый символ английского алфавита, принимая в качестве «1» букву русской раскладки клавиатуры, «0» — английской или наоборот. После проведения встраивания стегосообщения в контейнере каких-либо изменений заметно не будет. Очевидно, что при открытии заполненного контейнера в текстовом редакторе будут обнаружены ошибки в правописании, связанные с неверным сочетанием русских и английских символов, неверным написанием слов.

Следующий анализируемый метод Null chipper (в дословном переводе — нулевой лепет) предполагает размещение ключевой информации на установленных позициях слов или в определенных словах текста-контейнера, который, как правило, лишен логического смысла..

Метод Spammimic в качестве контейнера использует обычный спам (или любой нейтральный текст), внутри которого размещаются установленным обеими сторонами способом значащие символы (стегосообщение). С помощью проведенных экспериментов и некоторых расчетов [2, 3] было установлено, что наименее заметным для простого читателя является метод увеличения длины строки, а наиболее — Null chipper.

ЛИТЕРАТУРА

1 Ярмолик, В.Н. Криптография, стеганография и охрана авторского права/ В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. – Минск: Изд. центр БГУ, 2007. – 240 с.

2 Урбанович, Н.П. Стеганографические методы скрытия информации в тексте / Н.П. Урбанович, Т.В. Коваленок // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы XII Республиканской научной конференции студентов и аспирантов: в 2 ч. Ч. 2. – Гомель: ГГУ, 2009. – С. 168.

3 Urbanovich, P. Text steganography application for protection and transfer the information/P. Urbanovich, K.Chourikov, A.Rimorev, N.Urbanovich// 6-th Intern.Conf. NEET-09. Zakopane, Poland, 2009. – P. 60.