УДК 681.3.04

О.А. Нистюк, маг. (БГТУ, г. Минск)

ЗАЩИТА ТЕКСТОВОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ДОБАВЛЕНИЯ КОНТУРА К СИМВОЛАМ ТЕКСТА

Развитие информационных технологий за последние годы привело к тому, что значительная часть информации, относящейся к различным сторонам деятельности предприятий или организаций, теперь находится в электронном виде. Особенную остроту приобретает проблема надежной защиты этих ресурсов, а также иных текстовых документов, программных кодов, баз данных от несанкционированного использования.

Существуют различные способы для реализации такой защиты. К ним можно отнести, в частности, методы текстовой стеганографии, которые в последнее время становятся популярными.

Информация, которая позволяет защитить права собственности на документ, скрывается (осаждается), наподобие цифровых водяных знаков, в документе (контейнере).

Скрывать такую информацию можно, используя различные элементы текста путем их незаметной модификации: например, изменением контура символов. Существует множество методов сокрытия информации другими способами: например, междустрочного интервала, или интерлиньяжа (LineShift Coding), пробельного расстояния между словами (Word-Shift Coding).

Основными объектами сокрытия информации, относящимся к информационным технологиям являются бумажные и электронные версии различных текстовых документов.

Среди множества предлагаемых методов защиты текстовой информации ни один не дает полной гарантии. В последние годы появляется все большее количество методов сокрытия информации на основе стеганографии. При этом защита или передача информации производится путем ее тайного размещения в текстовый документ. Процесс осаждения подразумевает собой изменение некоторых параметров контейнера. В случае с текстовыми документами, в некотором тексте осаждается информация, которую необходимо передать другому пользователю незаметно.

Для понимания сущности метода кратко поясним специфику используемого здесь параметра шрифта. Необходимо выставить определенные параметры символа так, чтобы это было визуально незаметно. Таким образом согласно методу, можно скрыть необходимую информацию в документе-контейнере.

Компьютерная графика добавила символам текста еще одну существенную характеристику – контур, который также может быть ис-

пользован для осаждения тайной информации в текст по аналогии с известными методами графической стеганографии.

На рис. 1 приведен пример применение контура для различных символов алфавита. На рисунке при большом увеличении визуально незаметно. Однако, в первой строке применен контур символов ко всем символам, а в другой строке ни к одному.

Рисунок 1 – Пример применения контура

Далее рассмотрим алгоритмические особенности реализации методов, в которых осаждение информации производится путем изменения контура символа в соответствии с некоторыми правилами сокрытия информации в контейнере текста.

Документ, который мы хотим защитить, называется контейнером, или файлом-контейнером C. Текст, с помощью которого осуществляется защита путем его осаждения в контейнере, или же который размещается для передачи, носит название стегосообщение C. Защищенный документ (контейнер с осажденным сообщением) называется стегоконтейнером S.

Итак, необходимо скрыть некоторую информацию в файле-контейнере для передачи её другому пользователю. У нас есть файл-контейнер C, размер которого N_C, где N – количество слов в тексте. Также имеется сообщение, которое необходимо скрыть в файле-контейнере, X. Следующим шагом сокрытия информации является перевод скрываемой информации в двоичный вид. N_X – количество символов сообщения, переведенного в двоичный вид.

Например, имеется текст «Hello world». Его $N_C = 2$. И скрываемое сообщение «123». Его $N_X = 1111011$.

Таким образом, на первом этапе, необходимо вычислить размер файла-контейнера, узнать скрываемое сообщение, перевести его в двоичный вид и вычислить количество символов X.

Основная среда для работы с текстовыми сообщениями MS Word. Возможности пользователя в этой среде для работы с контуром символа достаточно широки. Можем редактировать следующие параметры: цвет, прозрачность, ширину контура, тип штриха, тип точки и другие. Параметры можно посмотреть на рис. 2.

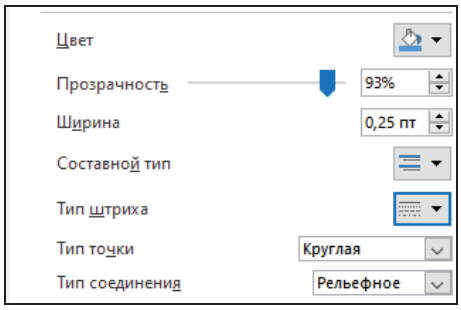

Рисунок 2 – Параметры контура символа

Предполагается осаждение информации в тексте сообщения, переведенного в двоичный вид при соответствующем объеме N_C.

Например, если в сообщении «0», то контур применяем к последней букве встречающегося слова в файле-контейнере, а если «1» – эти же действия производятся над первой буквой слова.

Таким образом, появляется условие, что необходимо пропускать слова, которые содержат 1 букву (предлоги). Это необходимо для того, чтобы наиболее грамотно извлечь в будущем сообщение без потерь данных, так как если в слове одна буква, то неизвестно будет зашифрована «1», либо «0».

Также возникает следующий вопрос. Как шифровать пробелы? Пробелы в двоичном виде также имеют свой код. Именно поэтому, пробелы будут осаждаться аналогично всем словам.

Далее необходимо выяснить как высчитать необходимый размер файла-контейнера для сокрытия необходимого сообщения. То есть,

$$N_c > N_X.$$

Недостаток данного метода в том, что даже для сокрытия одного слова, состоящего из 6 символов, необходим текст размером примерно в 66 слов, не учитывая слов, состоящих из 1 символа.

Далее можно обратиться к анализу влияния контура символов на объем памяти, занимаемой текстом. Логично предположить, что при добавлении каких-либо «качеств» символам, текст станет занимать больше памяти. На графике (рис. 3) отображено данное влияние:

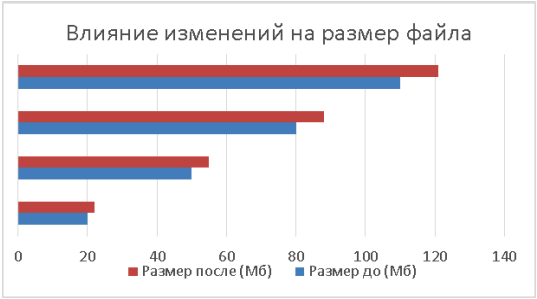

Рисунок 3 – График влияния контура символов на объем памяти

Таким образом, при добавлении контура к символам, объем памяти, занимаемой текстом, увеличивается линейно.

Предложенный и проанализированный метод тайной передачи информации в тексте-контейнере основан на реализации текстовой стеганографии путем изменения такого параметра текста-контейнера, как контур символа.

ЛИТЕРАТУРА

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

УДК 004.032.26

Н.А. Жиляк, доц., канд. техн. наук;
Джеремий Убонг Чарлес, маг.
(БГТУ, г. Минск)

НЕЙРОННЫЕ СЕТИ КАК РЕШЕНИЕ ЗАДАЧИ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ

В данном материале рассматривается, как предобученные нейронные сети могут быть использованы для решения задачи классификации изображений.

За последние годы появилось большое количество моделей, созданных и обученных профессионалами с использованием большого количества данных и огромных вычислительных мощностей. Многие из этих моделей находятся в открытом доступе, и любой может использовать их для решения своих задач совершенно бесплатно.

В качестве примера рассмотрим задачу классификации изображений из конкурса LifeCLEF Plant Identification Task. Задача заключается в том, чтобы предсказать таксономический класс растения, основываясь на нескольких его фотографиях [1].

Для обучения доступно 47815 изображений растений, каждое из которых принадлежит к одному из 500 классов. Необходимо построить модель, которая будет возвращать список наиболее вероятных классов растения. Позиция верного класса растения в списке предсказанных классов (ранг) определяет качество системы.

Эта задача моделирует реальный жизненный сценарий, где человек пытается идентифицировать растение, изучая его отдельные части (стебель, лист, цветок и др.). Таким образом, первичный показатель качества определяется как следующая средняя оценка S: