

СТЕГАНОГРАФИЯ И ЕЕ ВЛИЯНИЕ НА ОТОБРАЖЕНИЕ ТЕКСТОВЫХ ДОКУМЕНТОВ

Современный виртуальный мир перенасыщен различными текстами, изображениями, видеороликами и прочими средствами передачи информации. Такое обилие ресурсов каждый человек использует в целях самосовершенствования. Но данные ресурсы можно использовать не только по их прямому назначению. В них можно сокрыть большое количество информации при помощи стеганографии.

Стеганография, что в переводе с греческого буквально означает «тайнопись» – способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи или хранения [1]. Такой способ хранения информации нашел широкое применение в современном информационном обществе. Скрываемые данные обычно называют стегосообщением, а данные, внутри которых находится стегосообщение, называют контейнером.

Существует несколько целей стеганографии. Первая из них – цифровые отпечатки, что подразумевает наличие различных стенографических меток-сообщений для каждой копии контейнера, своеобразная защита контейнера от нелегального распространения. Вторая – стенографические водяные знаки, подразумевает наличие одинаковых меток для каждой копии контейнера. И наконец третья – скрытая передача данных, самая старая из всех целей, подразумевает передачу данных, скрывая сам факт наличия дополнительной, секретной информации [2].

На сегодняшний день можно обобщить около 15 применений стеганографии [2] при формировании ресурсов разного типа.

Учитывая большое количество текстовых документов в современном обществе, стоит обратить внимание на текстовую стеганографию, а именно стеганографию, использующую текстовые контейнеры для сокрытия данных. При сокрытии информации используются допущения при расположении и количестве символов в тексте, не учитываемые при прочтении человеком текстового файла. Это может быть дополнительное количество пробелов и знаков табуляции в разных частях строки, чередование некоторых не учитываемых служебных символов, больших и маленьких букв, букв из разных алфавитов, но похоже выглядящих. К методам текстовой стеганографии относят:

форматирование, изменение порядка следования маркеров конца строки, метод хвостовых пробелов, метод знаков одинакового начертания и изменения кода пробела. К основным элементам форматирования текста относятся следующие характеристики: цвет, кегель, апрош и кернинг. Незначительное изменение этих характеристик отдельно взятого элемента позволит машине распознать выделение, не заметное для человеческого глаза.

Наиболее популярным пакетом программ для работы с документами является MicrosoftOffice. Отличается поддержкой большого количества форматов файлов, в числе которых: TXT, DOC, DOCX, XLS, XLSX, CSV, PPT, PPTX, PPS, DBF и многие другие. Содержит множество полезных функций: поиск по тексту, регулировка его размера и цвета, перевод с иностранных языков, проверка орфографии, добавление изображений, видео-, аудио-контента. Наиболее распространённые форматы для создания и редактирования текстовых документов это *.doc и *.docx, однако для хранения чаще всего используют *.pdf, так как информация при таком хранении не подвергается изменениям под воздействием настроек пользователя, т.е. отображает конечный вариант текстового документа. При печати текстового документа, служащим контейнером для сокрытия информации посредством форматирования текста, и исходного текстового документа не должно быть явно заметных отличий. Поэтому следует учитывать плотность размещения скрытой информации и допустимый диапазон значений параметра, используемого для выделения символов.

При сканировании документа возникают проблемы, некоторая часть информации оказывается потерянной, во-первых, из-за несовершенства сканирующего устройства (к примеру, незначительное отличие высоты символов или их цвета), во-вторых, из-за отличия исходного формата от формата отсканированного документа. При дальнейшем преобразовании форматов текстовых документов возможна частичная потеря отличительных черт сокрытой информации (не удаётся четко определить, что скрыто), к примеру, причиной может быть отличие величины меж буквенных интервалов в разных форматах.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. Стеганография в XXI веке. Цели. Практическое применение. Актуальность. [Электронный ресурс] – <https://habr.com/ru/post/253045/>