УДК 004.056+003.26

Студ. М. Е. Алексеев
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СРАВНЕНИЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ НА ОСНОВЕ КОНТЕЙНЕРОВ PDF-ФОРМАТА

Стеганографические методы являются одним из перспективных инструментов для аутентификации и маркировки авторской продукции с целью защиты авторских прав на текстовую информацию в электронном виде. Разработаны достаточно эффективные методы для текстов на основе модификации параметров шрифта [1].

В [2, 3] рассмотрены стеганометоды для текстовых контейнеров PDF-формата.

Цель работы: определить основные преимущества и недостатки описанных в [2, 3] методов PDF-стеганографии, а именно: метода инкрементных обновлений, метода выравнивания текста, метода с использования пробельных символов и метода с использованием межсимвольных интервалов; выяснить какой из методов является наиболее стеганостойким. Безопасный стеганографический метод способен скрыть сообщение таким образом, что даже когда предполагается, что объект содержит скрытое сообщение, наличие этих скрытых данных не может быть определено с высокой вероятностью [4].

Ниже (см. табл.) классифицированы основные свойства методов.

Таблица – Основные преимущества и недостатки методов pdf-стеганографии

Метод	Преимущества	Недостатки
1	2	3
Метод инкрементных обновлений	1.Множество способов сокрытия данных; 2.Метод позволяет полностью скрывать данные, если документ открывается обычными средствами просмотра PDF файлов; 3.Возможность сокрыть большой объём данных.	1. Размер файла может сильно измениться, если скрывается много информации; 2.При просмотре документа специальными средствами, отображающими служебную информацию внутри PDF файла, все сокрытые данные очень просто обнаружить. 3.Метод является самым небезопасным среди всех.
Метод выравнивания текста с использованием TJ оператора	1.Максимально тяжело обнаружить скрытую информацию; 2. Размер результирующего документа никак не увеличивается. 3.Метод является самым безопасным.	Очень сложен в реализации.

Продолжение таблицы

1	2	3
Метод с использованием пробельных символов	1.Размер результирующего документа никак не увеличивается; 2.Легко обнаружить сокрытые данные, написав простую программу-парсер.	Объем встраиваемых данных ограничен количеством пробелов в тексте.
Метод с использованием межсимвольных интервалов	1.Возможность сокрыть огромный объём данных; 2.Легко обнаружить сокрытые данные, написав простую программу-парсер.	Размер файла может сильно измениться, если скрывается много информации.

Выяснив плюсы и минусы каждого из методов, можно сделать вывод, что наиболее стойким к взлому является метод выравнивания текста с использованием *TJ* оператора, так как очень тяжело написать программное средство для правильного разбора *TJ* операторов. Это делает метод достаточно стеганостойким.

ЛИТЕРАТУРА

1.Шутько, Н. П. Защита авторских прав на текстовые документы на основе стеганографической модификации цвета символов текста / Н. П. Шутько, П. П. Урбанович // Информационные технологии: материалы 83-й научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 г. – Минск: БГТУ, 2019. – С. 41-43.

2. Карачанская, Е. В. Использование стеганографии для сокрытия сообщения внутри PDF-файлов/ Е. В. Карачанская, К. Н. Коношко [Электронный ресурс]: https://esa-conference.ru/wp-content/uploads /files/pdf/Karachanskaya-Elena-Viktorovna.pdf, Дата доступа: 15.04.2020.

3. Алексеев, М. Е. Текстовая стеганография с использованием контейнера формата PDF/ М. Е. Алексеев // 71-я научно-техническая конференция учащихся, студентов и магистрантов: сб. науч. работ: в4-х ч. – Минск, 20–25 апреля 2020 г. [Электронный ресурс. – Минск: БГТУ, 2020. – Ч. 4.

4.Шутько, Н. П. Стойкость текстового стеганоконтейнера к искажениям / Н. П. Шутько, П. П. Урбанович// Информационные технологии: материалы 84-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 3-15 февраля 2020года [Электронный ресурс] /отв. за издание И.В.Войтов; УО БГТУ. –Минск: БГТУ, 2020. – С. 20-22.