

ИССЛЕДОВАНИЕ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ НА ОСНОВЕ МОДИФИКАЦИИ ПАРАМЕТРОВ

Текстовая стеганография является одним из направлений исследований и разработок, которая позволяет достаточно эффективно решать проблему тайной передачи или хранения информации.

Стеганография – это наука о скрытом передаче сообщений, которая отличается от криптографии, где целью является скрыть содержание сообщения. Вместо того чтобы зашифровывать сообщение, стеганография скрывает сам факт передачи сообщения [1].

Виды стеганографии делятся на следующие:

- скрытые сообщения в изображениях: в этих методах данные встраиваются в изображения, часто изменяя малозаметные детали, такие как младшие биты цветовых компонентов;

- скрытые сообщения в звуке: звуковые файлы могут содержать дополнительную информацию, скрытую в некоторых изменениях амплитуды или частоты;

- скрытые сообщения в тексте: текстовые документы могут содержать скрытые сообщения путем использования специальных символов, стеганографических алгоритмов или даже изменения форматирования текста;

- скрытые сообщения в видео: видеофайлы могут также содержать скрытую информацию, которая может быть встроена в видеопоток или изменена в аспектах кадра;

- скрытые сообщения в сетевом трафике: в сетевом трафике, таком как Интернет или локальные сети, данные могут быть скрыты путем изменения порядка передачи или внедрения скрытых сообщений в пакеты данных;

- физические методы стеганографии: это может включать использование невидимого чернила, нанесение сообщений на материалы специальным образом или даже встраивание микрочастиц в объекты;

- скрытые сообщения в файловых системах: скрытые сообщения могут быть встроены в файловые системы, путем изменения структуры файлов или использования областей файлов.

Методы текстовой стеганографии могут быть разделены на несколько категорий в зависимости от того, как именно текст используется для скрытия сообщений. Вот некоторые из наиболее распространенных методов [2]:

– изменение форматирования текста: скрытые сообщения могут быть встроены в текст путем изменения форматирования, такого как изменение размера шрифта, цвета или стиля текста. Например, изменение цвета фона или текста может быть использовано для кодирования скрытой информации;

– использование скрытых символов: в тексте могут быть использованы специальные символы или комбинации символов, которые не будут замечены при первом взгляде, но которые могут быть интерпретированы как скрытые сообщения, когда применяется соответствующий алгоритм;

– изменение порядка слов или букв: скрытые сообщения могут быть встроены в текст путем изменения порядка слов или букв;

– использование невидимого текста: некоторые методы стеганографии могут использовать невидимый текст, который не будет виден при обычном просмотре документа, но может быть раскрыт с помощью специальных инструментов или процедур;

– изменение структуры текста: скрытые сообщения могут быть встроены в текст, изменяя его структуру, такую как вставка дополнительных пробелов, символов или изменение интервалов между словами.

Для исследования влияния модификации параметров на различные свойства документа-контейнера были выбраны следующие методы текстовой стеганографии:

– метод изменения регистра символов (увеличение/уменьшение размера шрифта);

– метод добавления хвостовых пробелов (увеличение количества пробелов);

– знаки одинакового начертания (изменение символов кириллицы на символы латиницы одинакового начертания и наоборот);

– использование синонимов (использование словаря синонимов);

– опечатки в тексте;

– метод форматирования (изменение значений цвета и гарнитуры шрифта);

– метод добавления контура к символам текста (изменение цвета, прозрачности и ширины контура) [3];

– метод использования скрытых символов (использование символов конца строки и разрыва строки, пробела и неразрывного пробела).

Также для исследования были определены следующие показатели документа-контейнера, на которые неким образом будут влиять изменения в параметрах метода: размер стегоконтейнера, незаметность, емкость встраивания. Влияние модификаций на свойства контейнера представлены в таблице.

Таблица – Влияние модификаций на свойства контейнера

Метод	Размер стегоконтейнера	Незаметность	Емкость встраивания
Метод изменения регистра символов	Увеличивается	Чем больше модуль приращения ($ \Delta $), тем заметнее	Не меняется
Знаки одинакового начертания	Значительно увеличивается	В зависимости от поддержки кириллицы в шрифте	Зависит от количества схожих букв разных алфавитов в тексте-контейнере
Использование синонимов	Изменяется в зависимости от количества символов в новом слове	В зависимости от количества замененных слов	Зависит от объема словаря синонимов
Модификация цвета	Увеличивается при изменении стандартного цвета текста	Чем больше модуль приращения ($ \Delta $) значений отдельных каналов, тем заметнее	Не изменяется
Модификация шрифта	Изменяется в зависимости от размера шрифта	В зависимости от коэффициента сходства начертания символов	Зависит от количества символов, где сходство начертания в разных шрифтах максимально
Метод использования скрытых символов	Уменьшается	Не зависит, за исключением одного случая	Зависит от применения невидимого символа
Метод добавления контура к символам текста	Увеличивается незначительно	Чем больше модуль приращения ($ \Delta $), тем заметнее	Не изменяется

Таким образом, в ходе исследования было выявлено, что такие свойства документа-контейнера, как стегоустойчивость и пропускная способность, не зависят от модификации значений параметров.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович – Минск: БГТУ, 2016. – 220 с.
2. Конахович, Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
3. Нистюк, О.А. Метод и математическая модель стеганографического преобразования информации на основе модификации контура символов текста-контейнера / О.А. Нистюк, П.П. Урбанович // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. – 2022. – № 2 (260). – С. 92–98.