МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ

ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Чувашский государственный университет имени И.Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра вычислительной техники

Лабораторная работа №8

По дисциплине “Защита информации” на тему:

«Метод изменения интервала между предложениями»

Выполнил: ст. гр. ИВТ-11-21

Еремеев С.А.

Проверил: канд. техн. наук. Ковалев С.В.

Чебоксары 2025

**Теоретическая часть**

# Цель работы

Целью работы является знакомство со стеганографическим методом скрытия информации путем изменения интервала между предложениями.

# Задание на работу

В данной лабораторной работе необходимо программно реализовать алгоритмы прямого и обратного стеганографического преобразования.

Пустой и заполненный текстовые контейнеры должны задаваться пользователем в виде файлов либо через графический интерфейс – стандартный диалог выбора файла и/или поле ввода имени файла, либо через параметры командной строки. Выбор вида интерфейса (графический или командной строки) – на усмотрение студента, выполняющего работу. Аналогичным образом задается скрываемое сообщение.

Перед прямым стеганографическим преобразованием должна выполняться предварительная обработка пустого контейнера для замены двух и более пробелов на один пробел после окончания предложения, а также добавление к сообщению маркера окончания. Маркер окончания выбирается студентом самостоятельно таким образом, чтобы выбранный маркер не являлся частью исходного сообщения. До начала стеганографического преобразования предобработчик должен выводить пользователю информацию о максимальной емкости контейнера и возможности размещения заданного сообщения в выбранном контейнере.

Для простоты реализации можно принять, что сообщение начинает размещаться в контейнере с первой возможной позиции (то есть, после первого же предложения) и размещается последовательно; при этом стеганографический ключ отсутствует.

# Основные сведения

Основные понятия стеганографии и обобщенная структурная схема стеганографической системы приведены в тексте лекций.

Метод изменения интервала между предложениями основан на размещении одного или двух пробелов после каждого символа завершения предложения. При этом, обычно, единичным пробелом кодируется бит «1», а двойным пробелом – бит «0». Признаком завершения предложения можно считать точку, вопросительный и/или восклицательный знаки, после которых следует пробел.Скрываемое сообщение в двоичном формате встраивается в контейнер-текст путем размещения соответствующего каждому биту числа пробелов после каждого предложения.

Поскольку контейнер имеет существенно больший объем, чем сообщение, протокол стеганографического обмена должен предусматривать некоторый маркер завершения сообщения. Этот маркер дописывается в конец сообщения на этапе предварительной обработки, до поступления сообщения в стеганокодер. При извлечении сообщения из контейнера, обнаружение маркера позволяет прервать обработку и не анализировать оставшуюся часть контейнера.

В качестве примера представим себе контейнер следующего вида:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| С | л | о | в | а |  | ф | р | а | з | ы |  | 1 | . |  | С | л | о | в | а |  | ф | р | а | з |
| ы |  | 2 | . |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 3 | . |  | С | л | о | в | а |
|  | ф | р | а | з | ы |  | 4 | . |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 5 | . |  |
| С | л | о | в | а |  | ф | р | а | з | ы |  | 6 | ! |  | С | л | о | в | а |  | ф | р | а | з |
| ы |  | 7 | . |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 8 | ? |  | С | л | о | в | а |
|  | ф | р | а | з | ы |  | 9 | . |  | С | л | о | в | а |  | ф | р | а | з | ы |  | А | . |  |

Этот контейнер состоит из десяти предложений и, следовательно, может быть использован для размещения десяти бит скрываемого сообщения. Сообщение представляется в двоичном формате; каждый пробел после очередного предложения контейнера заменяется *двумя* пробелами, если очередной бит сообщения равен нулю, или *одним* пробелом (то есть, остается без изменений), если очередной бит сообщения равен единице. Пусть в нашем примере символ сообщения имеет значение **"М"**, в двоичной форме код символа **"М"** будет представлен битами ASCII("М") = 140d = 10001100b. Тогда заполненный контейнер будет выглядеть следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| С | л | о | в | а |  | ф | р | а | з | ы |  | 1 | . |  | С | л | о | в | а |  | ф | р | а | з |
| ы |  | 2 | . |  |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 3 | . |  |  | С | л | о |
| в | а |  | ф | р | а | з | ы |  | 4 | . |  |  | С | л | о | в | а |  | ф | р | а | з | ы |  |
| 5 | . |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 6 | ! |  | С | л | о | в | а |  | ф |
| р | а | з | ы |  | 7 | . |  |  | С | л | о | в | а |  | ф | р | а | з | ы |  | 8 | ? |  |  |
| С | л | о | в | а |  | ф | р | а | з | ы |  | 9 | . |  | С | л | о | в | а |  | ф | р | а | з |
| ы |  | А | . |  |

Затемнением выделены пробелы после окончания предложений, кодирующие биты скрываемого сообщения. Эта иллюстрация также более наглядно демонстрирует необходимость добавления маркера окончания сообщения до начала стеганографического преобразования: в противном случае на конце сообщения у нас ошибочно «декодировались» бы два единичных бита из той части контейнера, которая не понадобилась для скрытия сообщения.

На практике, стеганографические системы, реализующие рассмотренный и подобные методы, осуществляют предварительную обработку пустого контейнера. В ходе предобработки из текста контейнера удаляются «лишние» пробелы, которые могли оказаться в конце предложений на этапе создания контейнера: это может произойти из-за особенностей конкретного текстового редактора, системы распознавания сканированного текста, или действий человека, набиравшего текст.

**Практическая часть**

# Текст программы

# Пример открытого текста и соответствующей ему шифрограммы

# Вывод