Программно-аппаратные методы защиты информации

Лекция 13

Стеганография

В отличает от криптографии методы стеганографии позволяют скрыть сам факт передачи секретной информации. При использовании стеганографических методов сокрытия информации сторонний наблюдатель даже не заподозрит, что идет обмен информацией, поскольку секретное сообщение будет надежно спрятано от его взора в неприметном сообщении.

Для сокрытия информации необходим покрывающих объект (некий «невинный» контейнер), в который будет вложена информация.

Стеганография существует с древних времен. Например, в качестве покрывающего объекта может выступать обычное бумажное письмо, в котором между строк с помощью симпатических чернил написано секретное сообщение. Проявляется сообщение нагреванием письма.

Еще один из широко известных в истории методов передачи секретной информации методами стеганографии – послание на голове под волосами. Метод берет свое начало из Древнего Рима. Для передачи сообщения раба брили налысо, затем татуировкой наносили информацию на голову. Когда волосы отрастали, сообщение становилось не видным. Покрывающим объектом в данном случае выступал сам раб.

В современной мире активно развивается цифровая стеганография.

Основными целями использования СГ могут быть:

- невозможность использования КГ по закону или ее нестойкость при слабых шифрах;
- скрытие пользователей, которые нуждаются в хранении или передаче секретной информации;
- тайное отслеживание нелегальных распространителей информации;
- ретрансляция секретной информации через нелегитимных пользователей (в том числе и через Интернет).

В качестве покрывающих сообщений используются:

- Неподвижное изображение
- Видео
- Звук
- Текстовые файлы
- Графический текстовые файлы
- Чертежи
- И другие файлы.

В современной цифровой стеганографии существует много методов. Выбор используемого метода зависит, как правило, от покрывающего сообщения. Но при этом некоторые методы подходят для вложения в разные покрывающие сообщения.

Один из наиболее распространенный метод – вложение в наименее значащие биты (LSB). Существует множество модификаций данного метода.

Также информацию можно вкладывать в пустые поля заголовков файлов или заголовков протоколов.

Вложение можно произвести в графическую часть файла.

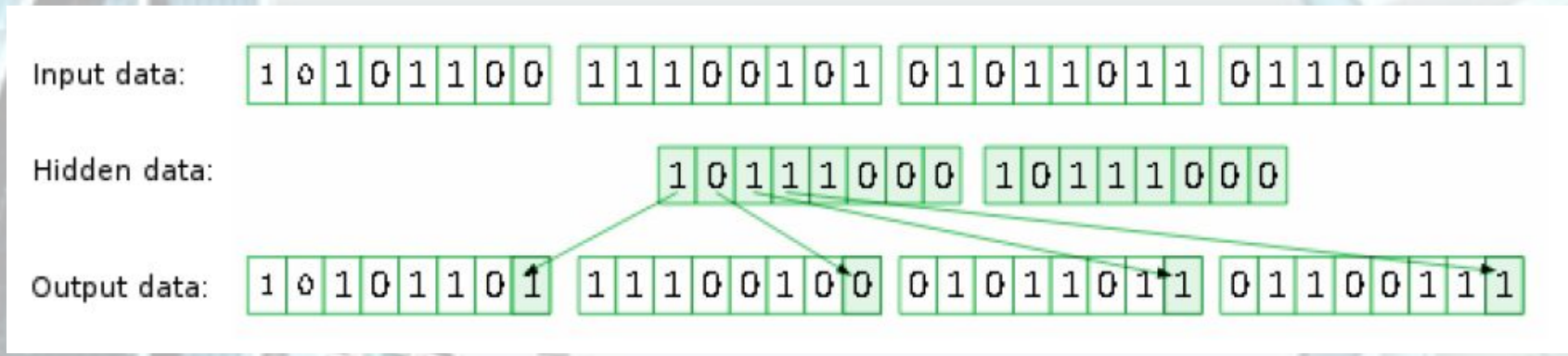
Вложение можно производить в шумовые поля сканированного изображения.

До сих пор активно используется лингвистические методы – изменение смыслового текста для вложения информации.

Вложение в наименее значащие биты – изменение наименее значащего бита в соответствии с битом смыслового сообщения.

В качестве покрывающих сообщений могут быть использованы аудио и видео файлы, изображения.

Наименее значащий бит несет так мало информации, что его замена будет не заметна ни человеческому глазу, ни человеческому уху.



Вложение в пустые поля протоколов зависит от уровня, на котором происходит вложение.

- Прикладной – использование обычных методов стеганографии
- Представительный – погружение данных в поля системных сообщений
- Сессионный – мониторинг чтения пользователями удаленных дисков
- Транспортный – вложение в неиспользованные данные TCP заголовков
- Сетевой – вложение в свободные поля IP пакетов
- Уровень данных – вложение в заголовки фреймов; использование CRC информации
- Физический – конфликтные ситуации с пакетами: “0” – посылка пакета после конфликта с задержкой, “1” – посылка пакета без задержки

Вложение в графический файл осуществляется, например, смещением линий текста.

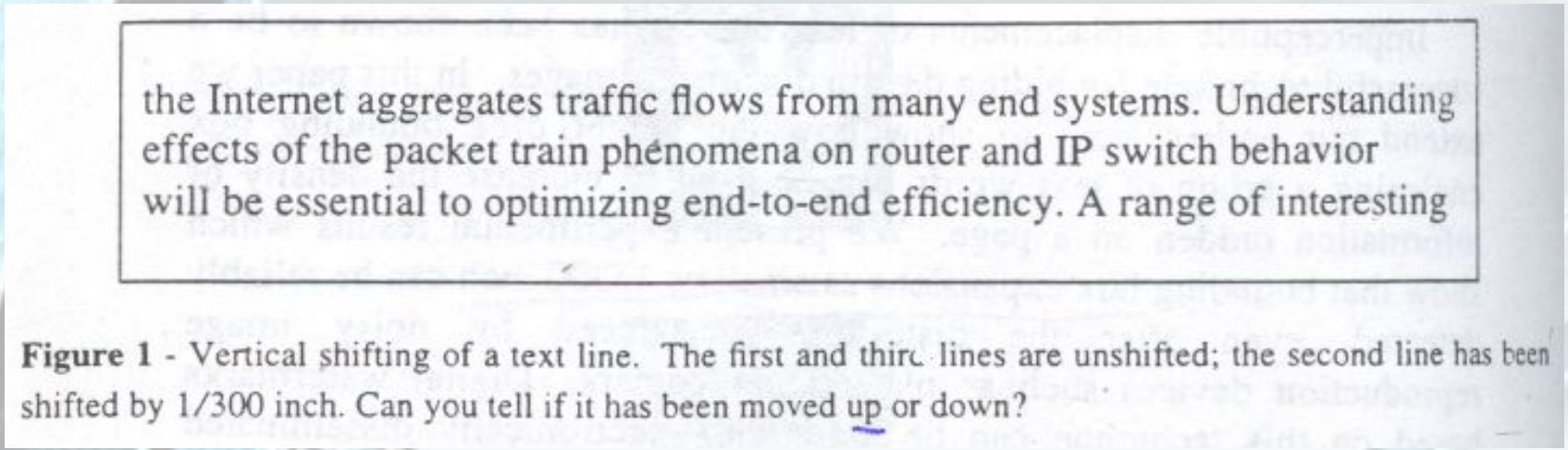
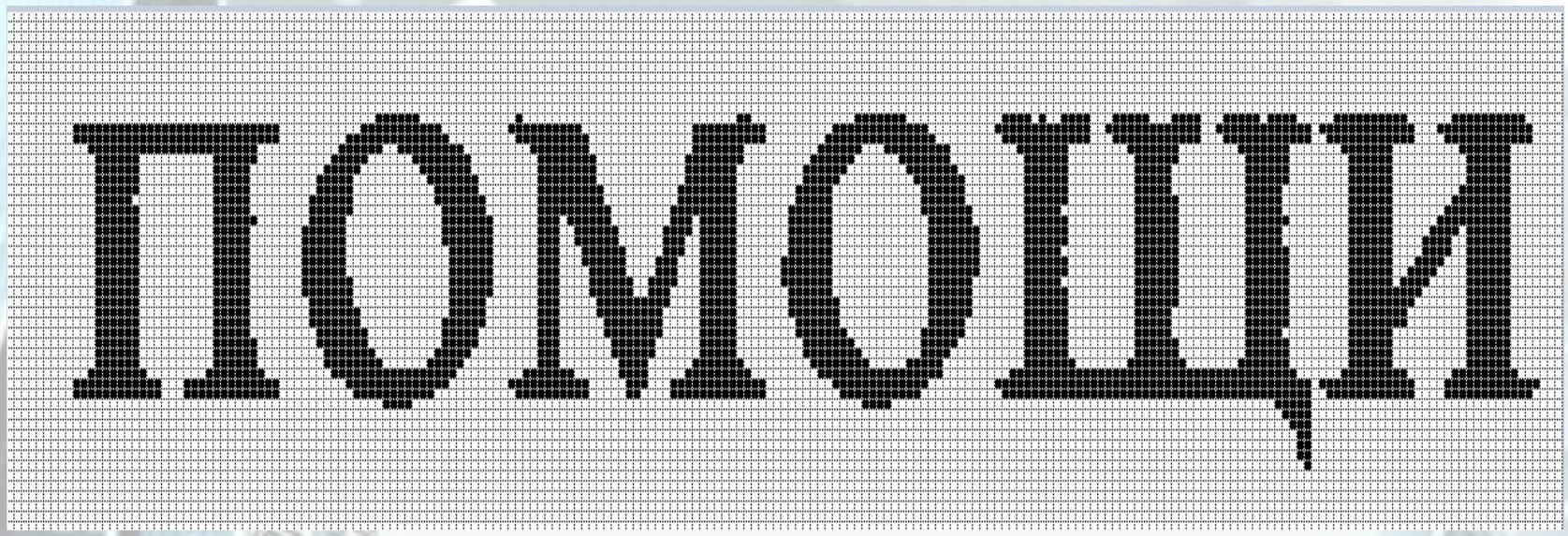

the Internet aggregates traffic flows from many end systems. Understanding effects of the packet train phenomena on router and IP switch behavior will be essential to optimizing end-to-end efficiency. A range of interesting

Figure 1 - Vertical shifting of a text line. The first and third lines are unshifted; the second line has been shifted by 1/300 inch. Can you tell if it has been moved up or down?

Вложение в шумы сканера основано на том факте, что пи некачественном сканировании документа всегда появляются случайные пиксели в виде шумов.



Лингвистическая стеганография основана на подборе пары синонимов и замены синонимов с смысловом тексте, который является покрывающим объектом, в соответствии с той информацией, которую необходимо передать. Примеры абсолютных синонимов:

- Взгляд – взор
- Гостиница – отель
- Доля – часть
- Лгун – лжец