Министерство образования и науки Российской Федерации
Санкт-Петербургский Политехнический Университет Петра Великого
•
Институт кибербезопасности и защиты информации.

Л А Б О Р А Т О Р Н А Я Р А Б О Т А 8

Основы стеганографической защиты информации

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Лобов Е.А

Преподаватель Зубков Е.А.

Санкт-Петербург

2022

Цель работы

Цель работы - приобретение навыков исследования свойств стегоконтейнеров, разработки стегосистем и их применения для сокрытия данных при передаче с помощью графических изображений.

11.ХОД РАБОТЫ

1.1Анализ изображения и написание кода

Откроем изображение с помощью HEX-редактора и рассмотрим его структуру. Первые несколько байт занимают данные о палитре и содержательной части изображения. Размер палитры составляет 24 цвета, что равняется 0x18 в 16-ричной системе (выделено зелёным), размер содержательной части составляет 840000 байт, что равняется 0x000CD140 в 16-ричной системе (выделено оранжевым).

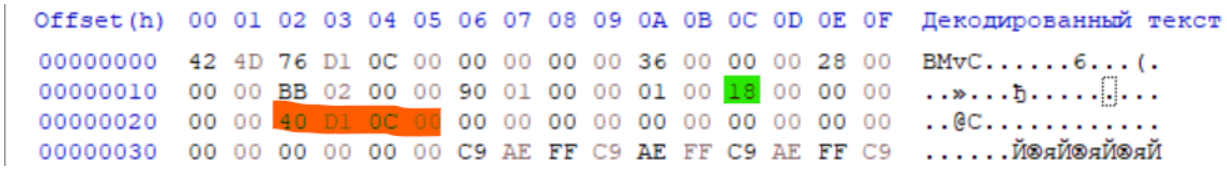


Рисунок 1 - Представление изображения в HEX-редакторе

Прокомментированный код программы представлен в папке source. Из функции main вызываются функции кодирования и декодирования секретного сообщения. Перед шифрованием проводятся проверки, что файл изображения открывается без ошибок, что изображение соответствует формату 24-цветного *.bmp файла, что сообщение не превышает допустимого размера. Далее начинается процесс кодирования. В первые 16 байтов помещается длина сообщения (по 1 младшему разряду в каждом), затем в следующий байт помещается степень сжатия сообщения (сколько бит отводится под сокрытие сообщения), и наконец, кодируются само сообщение.

При декодировании по порядку декодируется длина сообщения, степень сжатия и само сообщение.

В качестве секретного сообщения было выбрано свступление романа Эрнеста Клейна «Первому игроку приготовиться». В качестве стегоконтейнера было выбрано изображение, представленное на Рисунке 2.

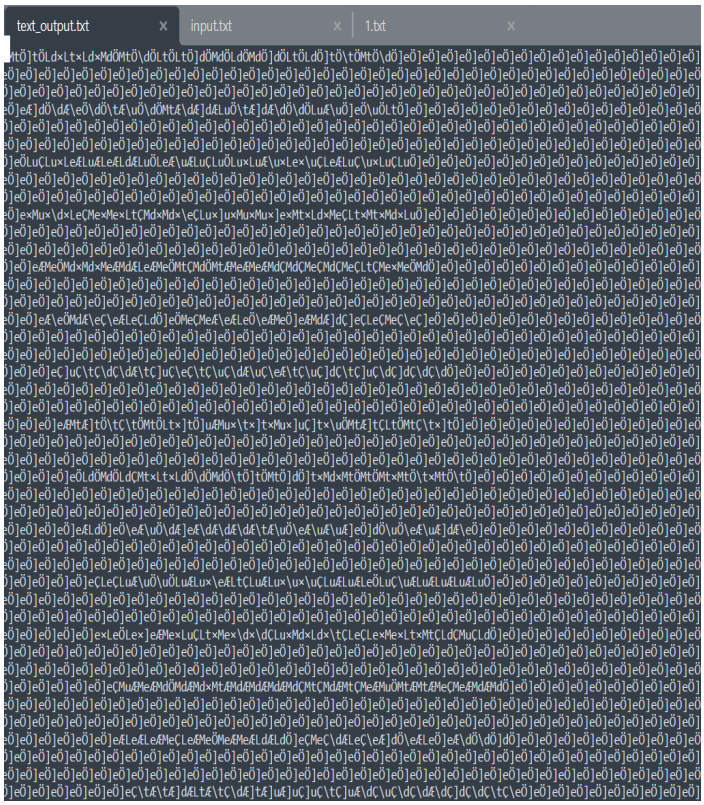
Рисунок 2 - Исходное изображение стегоконтейнера.

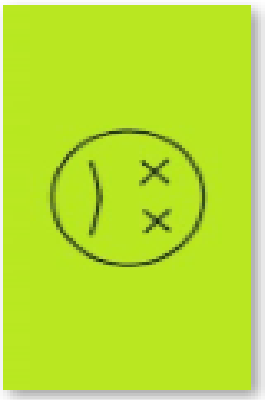
1.1Искажения изображения при различной степени сжатия

Сравним степень искажения изображения при различных степенях сжатия. Стоит отметить, что степень сжатия может принимать значения от 1 до 7 бит, поскольку при 0 ничего не закодируется, а при 8 байт будет полностью заменён. Изображения при сжатии от 1 до 7 представлены в папке «сжатия» дирректории отчета.

1.1Искажения текста при различных искажениях изображения

Если стегоконтейнер повреждён, то и секретное сообщение будет повреждено. Рассмотрим несколько различных повреждений: растяжение, поворот, искажение цветов (напр., изменение яркости или контрастности).Например при повороте изображения результат декодирования будет выглядеть так.





new_image.bmp

1ВЫВОД

В ходе выполнения данной работы были приобретены навыки исследования свойств стегоконтейнеров, разработки стегосистем и их применения для сокрытия данных при передаче с помощью графических изображений. Было выяснено, что чем больше размер стегоконтейнера, тем больше возможный размер сообщения; чем больше степень сжатия, тем больше возможный размер сообщения; однако чем больше степень сжатия, тем больше заметны искажения изображения. Также было выяснено, что любые искажения стегоконтейнера влекут за собой потерю секретного сообщения. На данную работу было потрачено около 8 часов.

LОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ

1.1Какие функции выполняет каждый элемент стегосистемы?

Кодер — устройство, предназначенное для вложения секретного сообщения в другие данные с учетом их модели, например, путем модификации младших значащих бит.

Детектор — устройство, предназначенное для определения наличия стегосообщения.

Декодер — устройство, восстанавливающее скрытое сообщение.

1.1Перечислите основные виды атак на стегосистемы.

Атаки на сообщение, на стегоконтейнер, на детектор, на механизм использования стегосообщения, против дополнительного ЦВЗ.

1.1Что означает термин “стойкость стегосистемы”?

Под стойкостью различных стегосистемы понимается её способность скрывать от квалифицированного нарушителя факт скрытой передачи сообщений, способность противостоять попыткам нарушителя разрушить, исказить, удалить передаваемые сообщения, а также способность подтвердить или опровергнуть подлинность скрытно передаваемой информации. Стегосистема является стойкой, если нарушитель, наблюдая информационный обмен между отправителем и получателем, не способен обнаружить, что под прикрытием контейнеров передаются скрываемые сообщения, и тем более читать эти сообщения.

1.1Какое влияние оказывает сжатие графических изображений на алгоритмы встраивания стегосообщений?

При сжатии графического изображения алгоритм встраивания ЦВЗ разрушается.

1.1Каковы методы противодействия стеганографическим атакам?

Для защиты от атак типа аффинного преобразования (масштабирование, сдвиги, повороты, усечение изображения) можно использовать дополнительные ЦВЗ. Эти ЦВЗ не несут в себе информации, но используются для регистрации выполняемых нарушителем преобразований. Другой альтернативой является вложение ЦВЗ в визуально значимые области изображения, которые не могут быть удалены из него без существенной его деградации. Другим методом защиты от подобных атак является блочный детектор. Модифицированное изображение разбивается на блоки размером 12x12 или 16x16 пикселей, и для каждого блока

анализируются все возможные искажения, т.е. пиксели в блоке подвергаются поворотам, перестановкам и т.п. Для каждого изменения определяется коэффициент ЦВЗ. Преобразование, после которого коэффициент оказался наибольшим, считается реально выполненным нарушителем. Таким образом, появляется возможность обратить внесенные нарушителем искажения.