Лабораторная работа № 7
Стеганографические программы Courier и S-Tools

1. Цель работы

Изучить основные принципы скрытой передачи информации, получить навыки работы с программами стеганографического сокрытия информации и редакторами памяти.

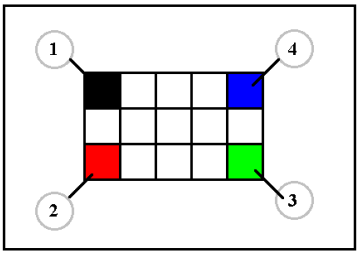
2. Общие сведения

Существует большое число способов скрытой передачи информации в графических файлах. Рассмотрим возможность использования для этого особенности формата BMP. Структура файла показана на рисунке

Два байта 42H и 4DH, представленные в шестнадцатеричной системе счисления, указывают на то, что формат данного файла BMP. В соответствии с кодовой таблицей CP-1251 эти числа после декодирования дают латинские буквы BM (то есть, графический формат Bit Map).

Шестнадцатеричное число 66H, расположенное по адресу 02H, говорит о том, что размер данного файла равен 102 байта. Это значение получено путём перевода шестнадцатеричного числа 66H в десятичную систему счисления. Число 36H, записанное по адресу 0AH, показывает, с какого адреса начинается запись картинки (это – смещение от начала). По адресу 12H указана ширина рисунка, выраженная в пикселях. В данном случае число пикселей равно 5. Высота рисунка указывается в ячейке 16H (для выбранного рисунка 3 пикселя). В ячейке 1AH указано число плоскостей на рисунке – 1. По адресу 1CH указана глубина цвета. В данном случае число 18H говорит о том, что для формирования цветовых оттенков этого рисунка используется

24 бита. В ячейке 22H указывается объем памяти, необходимый для запоминания битовой карты (объем рисунка без служебной информации).



Приведённый файл содержит рисунок, показанный слева.

Рисунок состоит из 15-ти пикселей (прямоугольник 5x3). Одиннадцать пикселей белые, пиксель в левом верхнем углу прямоугольника чёрный (1), в левом нижнем углу красный (2), в правом нижнем – зелёный (3) и в верхнем правом – синий (4).

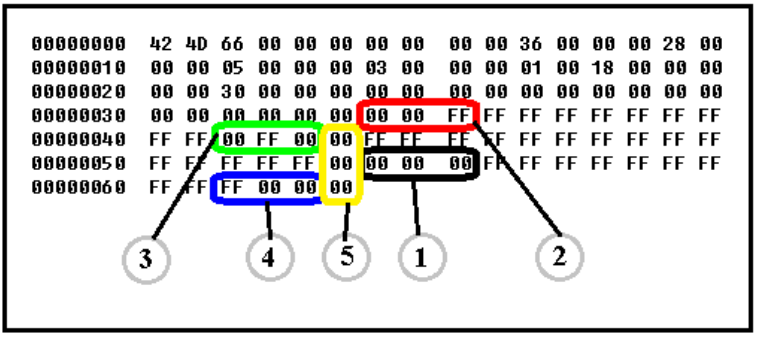
Запись битовой карты в память начинается с левого нижнего угла рисунка. Красный пиксель (2) описывается составляющими R=255, G=0, B=0. Запись в память (при увеличении адреса ячейки) ведётся в обратном порядке B-G-R. Таким образом, в самую первую ячейку битовой карты (адрес 36) заносится синяя составляющая B=00. В ячейку 37 записывается зелёная составляющая красного пикселя G=00, а в ячейку 38 красная составляющая R=FF (см. следующий рисунок). На рисунке красный пиксель обозначен цифрой 2.

Следующие три пикселя в нижней строке белые. Поэтому очередные девять байт имеют максимальное значение FFH (255D). В ячейках 42, 43 и 44 размещаются три байта зелёного пикселя (цифра 3).

В ячейке 45 размещён байт 00 – это дополнение, предназначенное для выравнивания строк дампа памяти. Эта ячейка избыточная, она не несёт никакой полезной информации, но её содержимое передаётся вместе с рисунком.

Следующие пять пикселей рисунка (вторая строка) – белые. Эти пиксели описываются с помощью пятнадцати байт FFH, которые размещены в ячейках памяти 46H…54H. В ячейке 55H помещается выравнивающий байт 00.

В ячейках 56, 57 и 58 размещаются байты 00 – это цветовые компоненты чёрного пикселя. Далее на рисунке размещены 3 белых пикселя верней строки. Им соответствуют девять байт FFH.



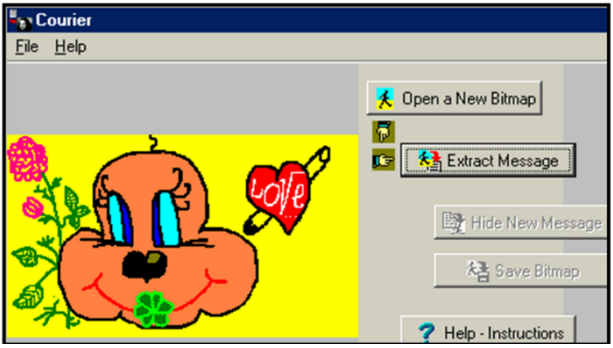
В ячейках 62, 63 и 64 размещаются цветовые составляющие синего пикселя.

Ячейка 65 используется для выравнивания. Три дополнительных байта обозначены цифрой 5.

Дополнительные ячейки появляются в тех случаях, когда произведение числа пикселей на три некратно числу 4. Другими словами, длина данных, описывающих отдельную строку рисунка, должна быть кратна четырём.

Именно дополнительные байты в графическом файле, предназначенные для выравнивания строк, могут быть использованы для скрытой передачи информации в графическом файле.

Для внедрения цифровых данных в мультимедийные контейнеры разработано большое число коммерческих и любительских программ. Например, S-Tools, JPHS, Open Puff, Courier, StegoMagic и др.



На рисунке показан пользовательский интерфейс программы Courier (автор программы — Kelce Wilson). Программа позволяет скрыть передаваемое сообщение внутри рисунка или фотографии. В качестве контейнера используется рисунок, созданный студенткой Е. Яшновой.

Программа управляется с помощью пяти командных кнопок: **Open a New Bitmap** (Открыть новый рисунок), **Extract Message** (Извлечь сообщение), **Hide New Message** (Скрыть новое сообщение), **Save Bitmap** (Сохранить рисунок), **Help — Instructions** (Помощь).

Максимально возможное число символов в сообщении зависит от размера выбранного рисунка-контейнера.

Перед внесением скрываемого текста изображение-контейнер преобразуется в 24-битный рисунок. Это позволяет сделать незаметным для глаза изменения цветов пикселей, в которых запрятана информация. Более 16 миллионов цветовых оттенков делают практически неразличимыми происходящие с рисунком небольшие изменения.

Теоретически один пиксель 24-битной цветной картинки позволяет

скрыть 3 бита секретной информации.

Если размер цветного рисунка или фотографии составляет 400×600 пикселей, то такой контейнер способен вместить $400 \cdot 600 \cdot 3 = 720000$ бит секретной информации. Так как для передачи (или хранения) одного символа текста требуется 1 байт информации, то контейнер может содержать «начинку» объёмом 90 000 байт (т. е. символов, букв, цифр). Такой контейнер-рисунок способен уместить более 30 страниц секретного текста.

Анализ работы программы Courier показал, что её автор не полностью руководствовался теорией стеганографии и для маскировки сообщения использовал два последних (младших) бита файла-контейнера (а не один, как этого требует теория). Это позволило ему вдвое увеличить объем хранимой в контейнере информации.

Заметим, что данная программа может быть использована лишь для учебных целей (для иллюстрации идей стеганографии). Для криптоаналитиков выделить скрытое с помощью программы Courier сообщение не составит особого труда.

Значительно профессиональнее сделана программа Steganography-Tools (сокращённое название S-Tools, автор — Andrew Brown). Данная программа вначале сжимает текст сообщения, затем шифрует его методами криптографии и лишь потом помещает сообщение в файл-контейнер. При этом скрываемая информация равномерно «распыляется» по всей поверхности рисунка.

В качестве контейнера программа допускает использовать как графические, так и звуковые файлы. Графические файлы должны быть представлены в форматах BMP или GIF, а звуковые файлы — в формате WAV.

Криптографическое шифрование осуществляется по одному из алгоритмов (IDEA, DES, Triple DES или MDC) со 128-битным ключом, причём ключ формируется из символов пароля, введённого пользователем.

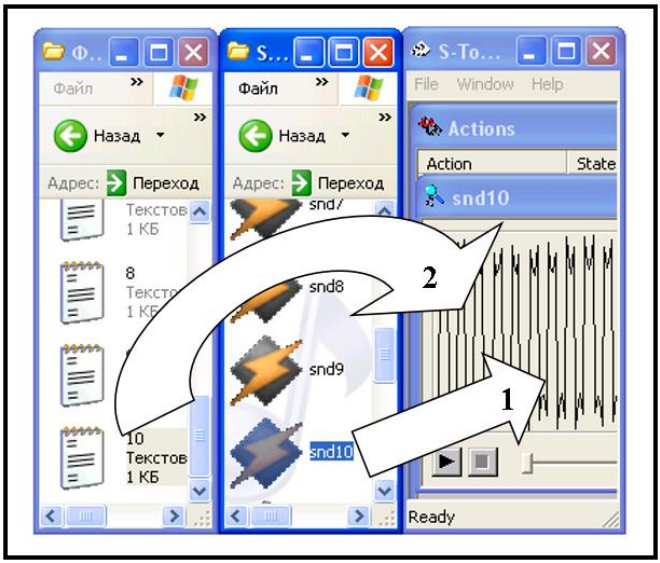
Порядок работы с программой достаточно прост. Он базируется на принципе Drag and Drop (перенеси и положи). Вначале нужно развернуть окно программы так, чтобы оно занимало часть экрана. На свободной части экрана развернуть Проводник или папку Мой компьютер с изображением значка (пиктограммы, иконки) файла-контейнера. Иконку файла-контейнера следует перенести внутрь окна программы S-Tools. В правом нижнем углу программы появится информация с указанием допустимого объёма файла-сообщения. Затем по технологии Drag and Drop внутрь окна нужно перенести иконку файла-сообщения. После этого следует ввести пароль и сохранить зашифрованное сообщение.

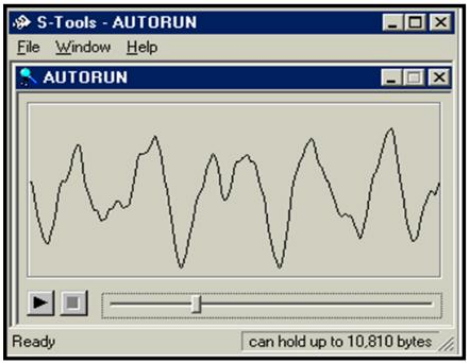
Дешифрация скрытого сообщения ведётся в обратном порядке: вначале скрытый файл перетаскивается (буксируется) внутрь окна программы. Затем правой кнопкой вызывается контекстное меню и вводится использованный пароль (пункт **Reveal**).

На рисунке показан внешний вид программы S-Tools с изображённым

звуковым файлом-контейнером (его имя — AUTORUN). Надпись в правом нижнем углу информирует пользователя о том, что внутрь программы можно запрятать текст объёмом 10 810 байт.

Музыкальные файлы позволяют скрывать большой объем информации. Так, если преобразование аналогового сигнала в цифровой сигнал происходит с частотой дискретизации 44,1 кГц, то это позволяет ежесекундно сохранять 44 100 бит информации в монофоническом сигнале и 88 200 бит — в стереофоническом. Таким образом, в звуке, длящемся 1 секунду, можно поместить текст объёмом более 10 Кбайт.





Завершая данный раздел, приведём краткое сравнение способов создания шифрованных сообщений методами криптографии и стеганографии.

Криптография и стеганография решают сходные задачи, но разными способами. Криптография превращает секретное сообщение в непонятный для непосвящённого человека текст, а стеганография делает секретное сообщение невидимым.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Изучение принципа стеганографии

В соответствии со своим номером варианта необходимо вручную скрыть текст (табл.3.1.1) в указанном контейнере – последовательности двоичных чисел (24 байта, данные записаны построчно).

Контейнер для нечётных вариантов

```
11001010 00110100 10001111 11110011 00011110 10101100
00111011 01010101 01100111 00110011 00011101 11100010
10101011 11110110 00001101 10010001 01011010 00101110
00101010 11010001 00110111 10110010 01010101 01100011
```

Контейнер для чётных вариантов

```
01111001 01110100 00100101 01110111 00010100 10100011
00101001 11010010 01001111 10110101 01001000 00111111
01000010 10110110 11011111 10110001 01011010 10001000
01101110 10010000 01110101 10010110 00010001 11101011
```

Таблица 3.1.1

Вариант	Текст	Вариант	Текст
1	Fox	9	Миг
2	Hug	10	Бит
3	Big	11	Сон
4	Red	12	Час
5	Dog	13	Эра
6	Cat	14	Год
7	Arm	15	Сто
8	Lip	16	Век

3.2. Задание 2. Сокрытие текста в графическом контейнере и его извлечение с помощью программы Courier

3.2.1. Используя программу Courier, скрыть в рисунке свою фамилию, имя и номер группы. Полученный файл сохранить в своей папке. Рисунки-контейнеры находятся в папке Courier_Pic_clean, причём имена (в данном случае порядковые номера) файлов совпадают с номерами вариантов.

3.2.2. Из папки Courier_Pic_secr извлечь информацию, скрытую в файле, имя которого соответствует номеру варианта. Извлечённый текст поместить в отчёт.

3.3. Задание 3. Сокрытие текста в звуковом контейнере и его извлечение с помощью программы S-Tools

3.3.1. В соответствии со своим вариантом скрыть заданный текст в указанном звуковом файле (таблица 3.3.1). Звуковые файлы (контейнеры) следует выбрать из папки Sounds_clean (Звуки чистые). Текст рекомендуется набирать в текстовом редакторе Notepad (Блокнот). Пароль и метод шифрования нужно выбрать самостоятельно. Начинённый контейнер (стего) следует сохранить в собственной папке.

Таблица 3.3.1

Вар	Файл	Текст
1	Snd1.wav	Нашу тайну редко выдаёт тот, кто её знает, а чаще тот, кто её угадывает. *NN*
2	Snd2.wav	Нечитающие не имеют преимуществ над не умеющими читать. *NN*
3	Snd3.wav	Чем больше человек любит самого себя, тем больше он зависит от чужого мнения. *Марк Аврелий*
4	Snd4.wav	Труд делает нечувствительным к огорчениям. *Цицерон*
5	Snd5.wav	Счастье не в том, чтобы делать всегда, что хочешь, а в том, чтобы всегда хотеть того, что делаешь. *Л. Толстой*
6	Snd6.wav	Можно привести лошадь к водопою, но нельзя заставить её пить. *Английская пословица*
7	Snd7.wav	Меня ужасает не мой возраст, а возраст моих ровесников. *NN*
8	Snd8.wav	Ясность украшает глубокие мысли. *Л. Вовенарг*
9	Snd9.wav	Если высыпать содержимое кошелька себе в голову, его уже у вас никто не отнимет. *Б. Франклин*
10	Snd10.wav	Лучше плохой день на рыбалке, чем хороший на работе. *Поговорка*
11	Snd11.wav	Пиши правильно, даже если диктуют ошибочно. *Ю. Булатович*
12	Snd12.wav	Память – единственный рай, из которого нас не могут изгнать. *Ж. Поль*
13	Snd13.wav	Знания забудутся, пробелы в них – никогда. *М. Генин*
14	Snd14.wav	Кто владеет информацией, тот владеет миром. *Н. Ротшильд*
15	Snd15.wav	Сначала собака не любит кошку, а аргументы подыскивает потом. *Я. Ипохор-*

		ская
16	Snd16.wav	Кто умеет - делает, кто не умеет - учит. *Б. Шоу*

3.3.2. Выполнить обратное преобразование, то есть извлечь скрытый текст из звукового файла. Файл с начинённым контейнером находится в папке Sounds_secr (Звуки секретные). Извлечённый файл следует сохранить в своей папке.

Имя файла, пароль и использованный алгоритм шифрования выбираются из таблицы 3.3.2.1 в соответствии с номером варианта.

Таблица 3.3.2.1

Вар	Файл	Пароль	Алгоритм
1	1_hidden.wav	abc	MDC
2	2_hidden.wav	sdfr	DES
3	3_hidden.wav	red	Triple DES
4	4_hidden.wav	mas	IDEA
5	5_hidden.wav	pass	DES
6	6_hidden.wav	word	MDC
7	7_hidden.wav	ais	Triple DES
8	8_hidden.wav	qwerty	IDEA
9	9_hidden.wav	show	Triple DES
10	10_hidden.wav	park	MDC
11	11_hidden.wav	sole	DES
12	12_hidden.wav	star	IDEA
13	13_hidden.wav	moon	MDC
14	14_hidden.wav	ibm	Triple DES
15	15_hidden.wav	intel	DES
16	16_hidden.wav	rain	MDC

3.4. Задание 4. Внедрение текста в графический контейнер и его извлечение с помощью программы S-Tools

3.4.1. В соответствии со своим вариантом скрыть заданный текст в указанном графическом файле (таблица 3.4.1.1). Графические файлы (контейнеры) следует выбрать из папки Pictures_clean (Картинки чистые). Текст рекомендуется набирать в текстовом редакторе Notepad (Блокнот). Пароль и метод шифрования нужно выбрать самостоятельно. Начинённый контейнер следует сохранить в своей папке.

Таблица 3.4.1.1

Вар.	Файл	Текст
1	Pic1.bmp	Настоящую любовь нельзя или найти, или встретить: мимо неё невозможно пройти! *Хомуций*
2	Pic2.bmp	Тот, кто был счастлив в любви, не имеет о ней никакого понятия. *Ж. Ануй*
3	Pic3.bmp	Разлука для любви - что ветер для огня: слабую она гасит, а большую раздувает. *Р. Бюсси*
4	Pic4.bmp	Мужчина, который умно говорит о любви, не очень любит. *Ж. Санд*
5	Pic5.bmp	Любовь – возвышенное чувство и чем оно выше, тем в последствии больнее падать. *А. Погорелкин*
6	Pic6.bmp	Любовь – теорема, которую каждый день надо доказывать! *Архимед*
7	Pic7.bmp	Только в минуты свидания и разлуки люди знают, сколько любви таило их сердце. *Жан Поль*
8	Pic8.bmp	Любовь — это огонь, зажигающий душу. *Джордано Бруно*
9	Pic9.bmp	Всякая любовь истинна и прекрасна по-своему, лишь бы только она была в сердце, а не в голове. *В. Белинский*
10	Pic10.bmp	В любви тоска соперничает с радостью. *Публий*
11	Pic11.bmp	Любовь – самая лучшая косметика. *Д. Лоллобриджида*
12	Pic12.bmp	Даже в чаше высшей любви содержится горечь... *Фридрих Ницше*
13	Pic13.bmp	Любовь одна, но подделок под неё — тысячи. *Ф. Ларошфуко*
14	Pic14.bmp	Любовь - это зубная боль в сердце. *Г. Гейне*
15	Pic15.bmp	Ангелы зовут это небесной отрадой, черти адской мукой, люди – любовью. *Г. Гейне*
16	Pic16.bmp	Мы знаем, что любовь сильна, как смерть; зато хрупка, как стекло. *Г. Мопассан*

3.4.2. Выполнить обратное преобразование, то есть с помощью программы S_Tools извлечь скрытый текст из графического файла. Файл находится в папке Pictures (Картинки). Извлечённый файл следует сохранить в своей папке. Имя файла, пароль и использованный алгоритм шифрования выбираются из таблицы 3.4.2.1.

Таблица 3.4.2.1

	Файл	Пароль	Алгоритм
1	1_hiddpic.bmp	Exit	MDC
2	2_hiddpic.bmp	Freedom	DES
3	3_hiddpic.bmp	Soul	Triple DES
4	4_hiddpic.bmp	Fantasy	IDEA
5	5_hiddpic.bmp	Joke	DES
6	6_hiddpic.bmp	Alone	MDC
7	7_hiddpic.bmp	Thoughts	Triple DES
8	8_hiddpic.bmp	Wars	IDEA
9	9_hiddpic.bmp	Desire	Triple DES
10	10_hiddpic.bmp	Ocean	MDC
11	11_hiddpic.bmp	Every	DES
12	12_hiddpic.bmp	Good	IDEA
13	13_hiddpic.bmp	Things	MDC
14	14_hiddpic.bmp	Mistake	Triple DES
15	15_hiddpic.bmp	Mine	DES
16	16_hiddpic.bmp	Head	MDC

3.5. Задание 5. Изучение алгоритма сокрытия, использованного в программе Courier

В графическом редакторе MS Paint создать рисунок (прямоугольник или квадрат) с заданными атрибутами и указанным цветом заливки бумаги (см. табл. 3.5.1). Для прямоугольника вначале указана его ширина, а затем – высота. Например, размер 10x4 означает, что прямоугольник имеет ширину: 10 точек (пикселей) и высоту 4 точки.

Внедрить в рисунок (поместить в контейнер) с помощью программы Courier заданный текст (табл. 3.5.1).

В отчёте представить битовые карты рисунка без текста и с текстом. Битовые карты следует получить с помощью программы Hex Editor Neo 6.11 (или HEdit32).

С помощью этих битовых карт объяснить принципы стеганографии. В отчёте нужно указать адреса размещения каждого бита каждой буквы.

Таблица 3.5.1

№ варианта	Рисунок	Текст
1	Белый прямоугольник 10x4 пикселей	haL
2	Чёрный прямоугольник 10x4 пикселей	WAu
3	Белый квадрат 10x10 пикселей	AiS
4	Чёрный квадрат 10x10 пикселей	dWq
5	Белый прямоугольник 10x4 пикселей	Asd
6	Чёрный прямоугольник 10x4 пикселей	MiL
7	Белый квадрат 10x10 пикселей	WtS
8	Чёрный квадрат 10x10 пикселей	CiA
9	Белый прямоугольник 10x4 пикселей	Saw
10	Чёрный прямоугольник 10x4 пикселей	LmA
11	Белый квадрат 10x10 пикселей	EnL
12	Чёрный квадрат 10x10 пикселей	CaF
13	Белый прямоугольник 10x4 пикселей	TaK
14	Чёрный прямоугольник 10x4 пикселей	fML
15	Белый квадрат 10x10 пикселей	Net
16	Чёрный квадрат 10x10 пикселей	mLi

4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1.

В соответствии с принципами стеганографии скрываемую информацию представляют в двоичной системе счисления, разбивают на биты, которыми заменяют младшие биты файла-контейнера.

Пример 1.

Дан контейнер, состоящий из восьми байтов:

01011000
01010100
01011011
01110111
01010101
10011000
10100111
01101110

В контейнере необходимо скрыть русскую заглавную букву «К».

Решение.

В соответствии с кодовой таблицей СР-1251 (см. Приложение) буква К кодируется десятичным числом 202D (двоичное число 11001010B).

Следует поочерёдно выделять по одному биту из двоичного кода буквы, начиная с самого младшего бита, и заменять этими битами младшие биты в байтах контейнера (исходной последовательности).

Бит 1 (логический ноль), записанный в первый байт 01011000B, преобразует его в байт 01011000B (исходный байт в данном случае остался неизменным).

Бит 2 (логическая единица), записанный во второй байт 01010100B, преобразует его в байт 01010101B

Бит 3 (логический ноль), записанный в третий байт 01011011B, преобразует его в байт 01011010B и т.д.

Таким образом, каждый исходный и полученный байты одинаковые или отличаются друг от друга не более чем на одну единицу в младшем (правом) разряде.

Результаты выполненных преобразований приведены в таблице 4.1.1.

Табл. 4.1.1

Контейнер	Стего
01011000	0101100**0**
01010100	0101010**1**
01011011	0101101**0**
01110111	0111011**1**
01010101	0101010**0**
10011000	1001100**0**
10100111	1010011**1**
01101110	0110111**1**

В таблице полужирным шрифтом выделена скрываемая информация (русская буква К).

4.2. Методические указания к Заданию 3.2.

Чтобы скрыть сообщение при помощи программы Courier, нужно выполнить следующие действия.

1. Щёлкнуть по кнопке **Open a New Bitmap** (Открыть новый точечный рисунок), выбрать графический файл, который будет использован в качестве контейнера. Исходное изображение появится слева в окне программы Courier.

2. Далее щёлкнуть по кнопке **Hide New Message** (Скрыть новое сообщение). В первой строке появившегося окна указано максимальное количество символов, которые можно скрыть в данном изображении (это зависит от размера графического файла-контейнера). Набрать текстовую информацию. Полученное в результате шифрования изображение будет показано с правой стороны окна программы Courier.

3. Щёлкнуть по кнопке **Save Bitmap** (Сохранить точечный рисунок).

Извлечение скрытого сообщения.

1. Как и для сокрытия сообщения, необходимо щёлкнуть по кнопке **Open a New Bitmap** (Открыть новый точечный рисунок), выбрать необходимый начинённый файл.

2. Щёлкнуть по кнопке **Extract Message** (Извлечь сообщение).

4.3. Методические указания к Заданиям 3.3, 3.4.

Для сокрытия данных в звуковом или графическом контейнере с помощью программы S-Tools необходимо выполнить следующее.

1. «Перетащить» мышью звуковой или графический файл в открытое окно программы S-Tools. Для просмотра файловой системы можно использовать, например, Проводник операционной системы Windows.

2. Далее «перетащить» скрываемый файл в окно файла-контейнера.

3. Если размер контейнера достаточен для сокрытия данных, появится новое окно. В окне следует ввести пароль (**Passphrase**), подтвердить его путём повторного ввода (**Verify Passphrase**), а также выбрать один из предложенных алгоритмов шифрования.

Примечание.

Необходимо обратить особое внимание на то, что в пароле нельзя вместо строчных букв вводить заглавные буквы (и наоборот).

При использовании некоторых графических контейнеров может появиться меню с переключателем пунктов **Convert to a 24-bit image** (Конвертировать в 24-битное изображение) и **Attempt colour reduction** (Попытаться сократить цвета). Эти опции используются в случаях, когда глубина цвета отличается от 24-х бит.

4. Наполненный контейнер появится в новом окне **Hidden data** (Скрытые данные). Для сохранения результатов шифрования щелчком правой кнопки мыши выбрать опцию **Save** (Сохранить), указать имя полученного файла (и расширение), его местоположение.

Для извлечения скрытых данных из файла-контейнера необходимо выполнить следующие действия.

1. «Перетащить» звуковой или графический файл в окно программы S-Tools.

2. Щёлкнув правой кнопкой мыши в области окна открытого файла, выбрать опцию **Reveal** (Показать).

3. Дважды набрать пароль в пунктах **Passphrase** (Пароль) и **Verify Passphrase** (Подтвердить пароль). Указать алгоритм шифрования, использованный при сокрытии данных.

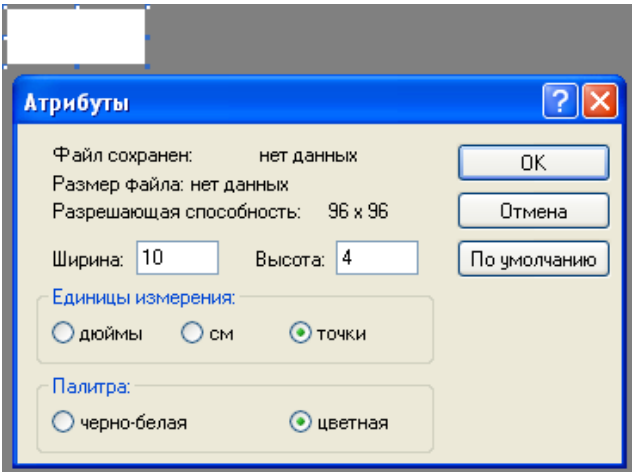
4. Если пароль и алгоритм введены правильно, появится окно **Revealed Archive** (Показанный архив), в котором находится скрытый файл. Щелчком правой кнопкой мыши по скрытому файлу выбрать опцию **Save as…** (Сохранить как…) и указать место на диске, в котором его требуется сохранить.

При использовании для просмотра текстового файла блокнота целесообразно файл сохранять с расширением txt, например, Doc10.txt.

4.5. Методические указания к заданию 3.5.

С помощью графического редактора MS Paint создать изображение прямоугольника с размером и цветом в соответствии с таблицей 3.5.1. При этом в Paint следует использовать опции **Рисунок** – **Атрибуты…** Переключатель **Единицы измерения** установить в положение **точки**. Размеры фигур умышленно выбраны малыми для того, чтобы просматриваемый объем файла был небольшим.

Порядок выбора атрибутов иллюстрирует следующий рисунок. Слева вверху виден белый прямоугольник в увеличенном масштабе.



Созданный рисунок сохранить в своей папке. Новому файлу целесообразно дать имя, которое характеризует его содержимое, например, **Белый_10_4.** С помощью программы Courier в созданный рисунок занести скрываемый текст из табл. 6. Порядок выполнения этой операции был изучен при выполнении Задания 2. Начинённый файл нужно сохранить в своей папке с любым именем, например, **Белый_10_4_SeL.**

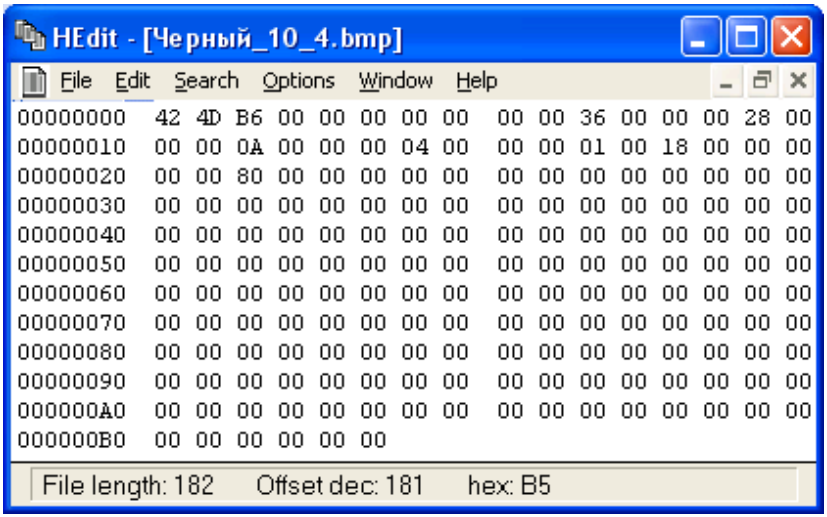
С помощью программы **Hex Editor Neo 6.11** (или **HEdit32)** изучить содержимое пустого и наполненного контейнера, то есть двух ранее созданных графических файлов.

Для примера ниже показано содержимое файла для чёрного прямоугольника размером 10x4 пикселя. Первые строки (54 байт) содержат служебную информацию (заголовок). Так как прямоугольник чёрный, то байты, отображающие цвет прямоугольника, содержат нули (00).

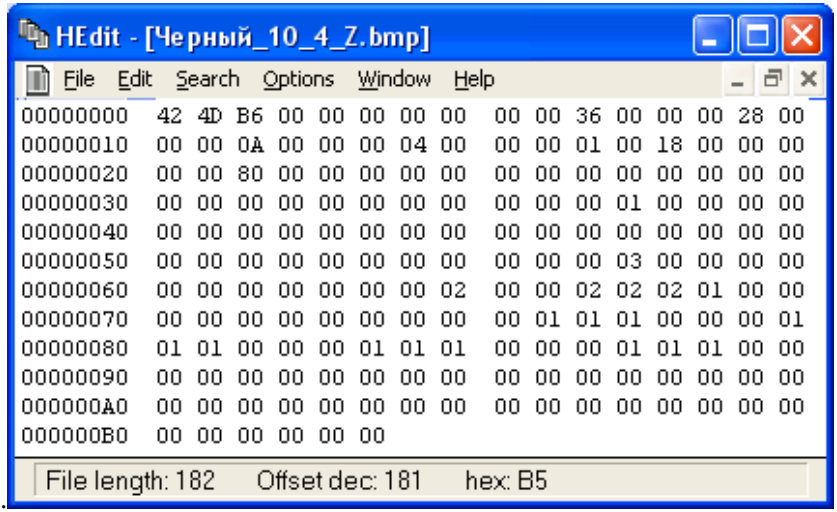
В левом столбце указаны восьмиразрядные шестнадцатеричные числа – адреса ячеек памяти. Правее приведено содержимое ячеек памяти в шестнадцатеричной системе счисления

Нужно обратить внимание на следующую деталь. При статическом распределении оперативной памяти (которое уже не используется в современных ЭВМ) адреса байтов будут совпадать с адресами ячеек памяти ОЗУ. При динамическом распределении памяти физические адреса определяются операционной системой в зависимости от наличия свободного места в ОЗУ.

В дальнейшем при описании принципа стеганографии будем использовать термин «ячейка памяти», понимая под этим адрес байта в исходном файле, не забывая, что при динамическом распределении памяти физический адрес в ОЗУ будет иным.



На следующем рисунке показана память контейнера, в который записана буква Z.



В первых строчках файла содержится служебная информация (ячейки 0…2FH). Ниже приведён фрагмент памяти, где выделены ячейки памяти, в которых размещена скрываемая в контейнере буква Z.

```
0030: 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050: 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00
0060: 00 00 00 00 00 00 00 02 00 00 02 02 02 01 00 00
```

Дадим пояснение к полученному результату.

Десятичный код буквы Z в кодировке CP-1251 равен 90D, что эквивалентно двоичному числу 01011010B.

Буква Z скрыта в дампе памяти последовательностью из четырёх чисел: 10B → 02H, 10B → 02H, 01B → 01H, 01B → 01H. Этот результат получен следующим образом: берут группы по 2 бита из двоичного кода буквы, начиная с младших (правых) разрядов, и заменяют ими 2 младших бита в соответствующих числах исходного файла-контейнера.

Процесс разбиения кода буквы Z на пары битов и порядок их размещения в памяти иллюстрирует следующая таблица:

Двоичная СС	01	01	10	10
Шестнадцатеричная СС	01	01	02	02
Адреса шестнадцатеричные	3B	6D	6A	67

В соответствии с разработанным автором программы Courier алгоритмом младший (правый) байт будет расположен по адресу 67H, второй байт расположен по адресу 6AH, третий – по адресу 6DH. Старший байт будет храниться на некотором отдалении от этих трёх байтов, в ячейке по адресу 3BH.

Рассмотрим ещё один пример. Предположим, что требуется скрыть в файле с изображением чёрного прямоугольника 4x10 латинские буквы RSX.

Вначале приведём содержимое памяти начинённого контейнера, а затем дадим комментарии к полученному результату.

```
0030: 00 00 00 00 00 00 00 00 00 01 01 01 00 00 00 00
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050: 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00
0060: 00 00 00 00 00 00 03 02 02 00 00 01 01 01 00 00
```

На рисунке выделено содержимое двенадцати ячеек, в которых скрыто 24 бита информации (три буквы по восемь бит).

Сделаем анализ памяти для каждой буквы в отдельности.

Определим по кодовой таблице CP-1251 десятичный код заглавной латинской буквы R и переведём это число в двоичную систему счисления:

82D = 01010010B.

После разбиения исходного байта пары битов будут помещены в ячейки памяти, адреса которых указаны в следующей таблице.

Двоичная СС	01	01	00	10
Шестнадцатеричная СС	01	01	00	02
Адреса шестнадцатеричные	3B	6D	6A	67

Аналогичные операции выполним для буквы S: 83D = 01010011B

Двоичная СС	01	01	00	11
Шестнадцатеричная СС	01	01	00	03
Адреса шестнадцатеричные	3A	6C	69	66

Дадим пояснения к порядку размещения в контейнере буквы X:
88D = 01011000B

Двоичная СС	01	01	10	00
Шестнадцатеричная СС	01	01	02	00
Адреса шестнадцатеричные	39	6B	68	65

Для уяснения принципа работы программы Courier следует с помощью четырёх последних таблиц найти места размещения скрываемых букв в файле-контейнере.

Необходимо обратить внимание на то, что файл с изображением белого квадрата (или прямоугольника) содержит шестнадцатеричные числа FF.

Для квадрата 10x10 пикселей адреса размещения скрываемой информации приведены в следующей таблице.

	1 группа битов (СЗР)	2 группа битов	3 группа битов	4 группа битов (МЗР)
1 буква	FB	12D	12A	127
2 буква	FA	12C	129	126
3 буква	F9	12B	128	125

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать исходные данные и результаты преобразований. В отчёте необходимо описать порядок сокрытия текстов в контейнерах с помощью программ Courier и S-Tools.

6. Контрольные вопросы

6.1. В чём состоит основная идея стеганографии?

6.2. Для чего предназначена программа Courier?

6.3. Для чего предназначена программа S-Tools?

6.4. В чем принципиальное различие криптографии и стеганографии?

6.5. Что означает термин «контейнер»?

6.6. Приведите примеры контейнеров, которые могут быть использованы для скрытой передачи информации.

6.7. Какой тип графических файлов (расширение) применим для сокрытия текста в программе Courier?

6.8. Какие контейнеры используются в программе S-Tools?

6.9. Каковы сферы использования стеганографии?

6.10. Что означает аббревиатура LSB?

6.11. Может ли программа Courier скрыть в одном контейнере несколько сообщений?

6.12. Как с помощью программы S-Tools скрыть файл в графическом контейнере?

6.13. Как, используя программу S-Tools, скрыть файл в звуковом контейнере?

6.14. Как восстановить данные, скрытые программой S-Tools в графическом файле?

6.15. Как извлечь скрытые данные из звукового контейнера с помощью программы S-Tools?

6.16. В каких ячейках памяти указывается размер рисунка?

7. Список литературы

1. Патент России 2463670. Орлов В.В., Алексеев А.П. Способ стеганографической передачи информации в сети TCP/IP.

2. Патент США US 6023511 A. Cryptosystem for encrypting digital image or voice file.

3. Алексеев А.П. Скрытая передача информации в графических файлах с использованием особенностей их формата. Материалы XV Международной НТК «Проблемы техники и технологий телекоммуникаций», том 2. – Казань, 2014 г., 299 – 301 с.

4. Алексеев А.П., Сухова Е.Н. Передача скрытых сообщений методами стеганографии. Мет. указания на проведение лабораторных работ. Самара: ПГАТИ, 2003. - 19 с.