Лабораторная работа № 6
Простейшие способы скрытой передачи данных

1. Цель работы

Изучить основные принципы скрытой передачи (хранения) информации.

2. Общие сведения

Стеганография — это наука, изучающая такие методы организации передачи (и хранения) секретных сообщений, которые скрывают сам факт передачи информации.

Криптография превращает открытый текст в нечитаемый набор символов (шифрограмму). Шифрограмма передаётся по открытому каналу связи, и защита информации держится на сложности подбора секретного ключа. Факт передачи криптограммы не скрывается от противника.

Стеганография нацелена на сокрытие факта передачи информации. Сообщение (его называют вложением) помещают (внедряют) в контейнер, вид и потребительские свойства которого практически не меняется из-за сделанного внедрения.

Стеганография чаще всего используется совместно с криптографией.

Скрываемое сообщение помещается внутрь безобидного на вид контейнера таким образом, чтобы постороннему наблюдателю было бы сложно заметить наличие встроенного тайного послания. Контейнерами могут быть чемодан с двойным дном, монета с отворачивающейся крышкой, почтовая марка с микроплёнкой, письмо, написанное симпатическими чернилами (например, хлоридом кобальта).

В настоящее время чаще используются электронные контейнеры, в которых может быть скрыт текст, рисунок (фотография), звук и даже видео.

Все контейнеры можно разделить на контейнеры-оригиналы и контейнеры-результаты. Контейнер-оригинал (или «пустой» контейнер) — это контейнер, который не содержит скрытой информации. Контейнер-результат (или «заполненный» контейнер, стего) — это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения (внедрения) сообщения в контейнер.

Все контейнеры могут быть разделены на два типа: статические и динамические. Статические контейнеры могут быть использованы как для скрытого хранения информации, так и для её скрытой передачи. Примером может служить цифровая фотография. Динамические контейнеры могут

быть использованы только для скрытой передачи информации. В качестве примера можно назвать пакеты, передаваемые по протоколу TCP/IP.

Число разнообразных контейнеров и методов внедрения вложений велико. Многие приёмы сокрытия информации основываются на «обмане» органов чувств человека. При сокрытии информации в графических и видео файлах изменение изображения столь незначительно, что глаз человека не регистрирует это изменение.

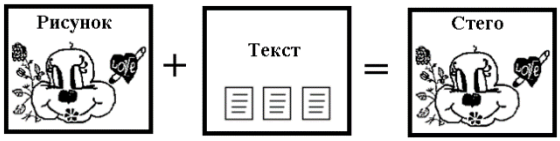
При сокрытии информации в текстовых документах умышленно выбирают цвета символов и бумаги одинаковыми (скажем, зелёные). В электронных документах используют невидимые (непечатаемые) символы (пробел, табуляцию).

В звуковых Midi-файлах незначительно изменяют длительности звучания нот и за счёт этого скрывают передаваемое сообщение. При вложении информации в аудио файлы изменения контейнера не должны регистрироваться слухом человека.

Однако такие требования к степени сокрытия информации могут использоваться лишь в простейших случаях. При передаче ценной конфиденциальной информации сделанные вложения не должны обнаруживаться даже с помощью специальных программно-аппаратных средств и профессиональных алгоритмов стегоанализа (например, с помощью статистического анализа контейнеров, спектрального анализа и т.п.).

Упрощённо идею стеганографии иллюстрирует следующий рисунок. Рисунок нужно трактовать так. Добавление скрываемого текста практически не изменяет контейнер. В данном случае контейнером служит графическое изображение. Заметим, что внедрение дополнительной информации в контейнер не изменяет потребительских свойств контейнера (рисунок по-прежнему можно использовать).

Обычно размеры контейнера в несколько раз превышают объем встраиваемых в них сообщений. Колоссальные объёмы HTML-страниц, графических, текстовых, звуковых и видео файлов, хранящихся на серверах Интернета, позволяют практически неконтролируемо и незаметно обмениваться секретной информацией между пользователями, находящимися в разных точках земного шара.



Рассмотрим пример сокрытия информации в текстовых документах. Следующая фраза на первый взгляд посвящена описанию природы:

Среди **т**емных **е**лей **г**роздьями **а**лели **н**ебольшие **о**стровки **г**устой рябины – **а**бсолютно **ф**антастические, **и**зумительно **я**ркие.

Тем не менее, предыдущий текст — это всего лишь контейнер, в котором студентка Виктория Подольская запрятала секретное слово **стеганография** (нужно читать только первые буквы каждого слова). Подобным образом можно передавать различные скрытые сообщения. Сходная идея используется в акростихах**.**

Акростих — стихотворение, в котором начальные буквы строк составляют слово или фразу.

В следующем стихотворении поэт Николай Гумилёв поместил имя любимой женщины - Анны Ахматовой.

Ангел лёг у края небосклона.
Наклонившись, удивлялся безднам.
Новый мир был синим и беззвёздным.
Ад молчал, не слышалось ни стона.
Алой крови робкое биение,
Хрупких рук испуг и содроганье.
Миру снов досталось в обладанье
Ангела святое отраженье.
Тесно в мире! Пусть живёт, мечтая
О любви, о грусти и о тени,
В сумраке предвечном открывая
Азбуку своих же откровений.

Акростихи могут составляться так, что информация будет скрыта не в первых буквах строк, а в последних.

Это вовсе не пустя**к,**
И склероз мой не забав**а:**
Завинтить забыл я кра**н,**
Прибежал сосед мой Слава**,**
И, конечно, был он пра**в:**
Старость хуже, чем отрава**.**

Текст найден в Интернете студенткой Калинкиной Алиной ПС-91.

Известны исторические примеры, когда для сокрытия факта передачи информации сообщение писали молоком между строк готового письма (симпатические чернила). После нагревания листка с невидимым текстом над открытым пламенем свечи появлялся текст. В приведённом примере контейнером для передачи скрытого сообщения служило безобидное бытовое письмо с описанием каких-то повседневных подробностей. Но ценная информация была записана между строк и на беглый взгляд цензоров была

незаметна.

Хрестоматийным стал пример передачи скрытой информации, использованный в древности. Рабу брили голову, делали татуировку на голове, ждали, когда вырастут волосы, и отправляли раба в назначенное место. В месте приёма информации его опять брили и читали секретное сообщение. Контейнером служила курчавая голова человека. Почта в те времена работала неспешно.

При сокрытии сообщений методами компьютерной стеганографии часто используют информацию, скрытую в последнем (наименьшем) значащем бите LSB (**L**ast **S**ignificant **B**its). В отечественных публикациях для его обозначения используют аббревиатуру НЗБ (наименьший значащий бит). При цифровом представлении графики и звука последний бит контейнера является малозначимым, часто изменяющимся по случайному закону. Шумы, возникающие при аналого-цифровом преобразовании звука и изображения (шумы квантования), случайным образом изменяют последний бит каждого отсчёта.

Рассмотрим простейший учебный пример.

Предположим, что имеется последовательность двоичных чисел (8 байт), отображающих в цифровом виде какой-то графический образ в формате BMP:

10100001-10101110-11010110-11001110-11000111-11001010-11010110-11101101

В данном примере каждое число контейнера представлено восьмью битами информации. Во многих случаях последний бит может быть безболезненно изменён, и пользователь не заметит произошедшей подмены. Например, при вариации младшего бита невозможно визуально заметить отличия в цветной графической картине, где каждый пиксель представлен двадцатью четырьмя битами. Также нельзя на слух уловить изменения, происходящие в звуковом файле с 16-ти битным квантованием по уровню.

Предположим, что в приведённый выше фрагмент контейнера необходимо «запрятать» русскую букву «А», представленную с помощью кодовой таблицы CP-1251. Десятичное представление буквы «А» имеет вид 192D, а двоичное — 11000000B.

Модифицируя имеющийся блок двоичных чисел (контейнер), поместим в контейнер двоичное число 11000000B. При этом 8 бит файла-сообщения записываются в 8 чисел файла-контейнера:

10100000-10101110-11010110-11001110-11000110-11001010-11010111-11101101

Эта же процедура внедрения скрытой информации иллюстрируется

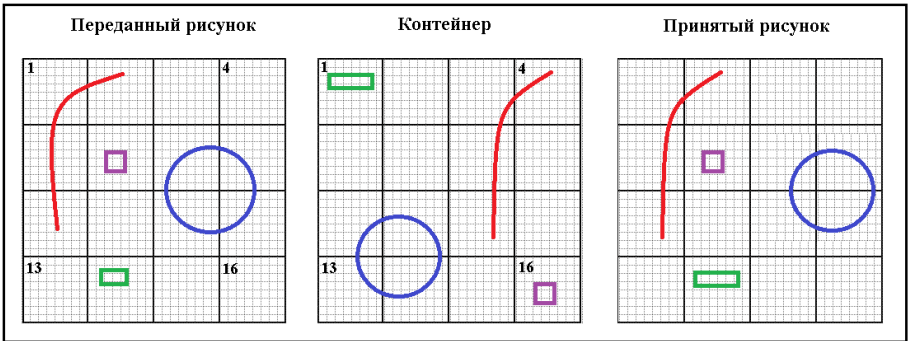
следующей таблицей. Заметим, что здесь буква «А» записана, начиная с младших битов.

Следующая таблица наглядно показывает порядок внедрения битов.

Пиксель 1			Пиксель 2			Пиксель 3		
R	G	B	R	G	B	R	G	B
Байт 1	Байт 2	Байт 3	Байт 4	Байт 5	Байт 6	Байт 7	Байт 8	Байт 9
0	0	0	0	0	0	1	1	…
↑	↑	↑	↑	↑	↑	↑	↑	
0	0	0	0	0	0	1	1	Биты

Возможно внедрение не только скрываемого текста в мультимедийные контейнеры, но и скрытая передача одного мультимедийного продукта в другом мультимедийном контейнере.

Примером может служить стегосистема для сокрытия цифровых данных в графических или звуковых файлах (патент США 6_023_511). Стегосистема делит исходный (скрываемый) файл и файл контейнер на множество одинаковых по размеру блоков данных, нумерует блоки данных файла контейнера (формирует индексы), сравнивает каждый блок данных скрываемого файла с блоками данных контейнера, отыскивает наиболее похожие блоки данных в контейнере, определяет номера индексов наиболее сходных блоков данных в контейнере для каждого блока данных из скрываемого файла и скрывает все полученные индексы в младших разрядах младших слов контейнера.



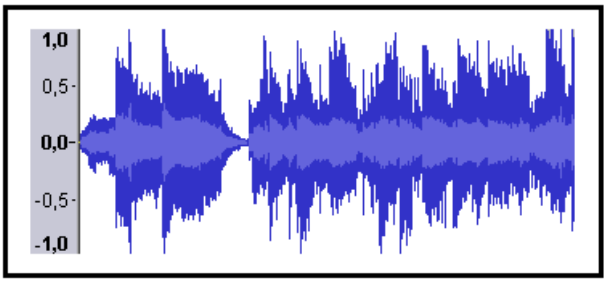
Идея скрытой передачи одного рисунка в другом рисунке состоит в том, что исходный рисунок и графический контейнер разбивают на блоки одинакового размера (в показанном выше примере размер каждого блока 8x8 пикселей, а число блоков равно 16). Каждый блок передаваемого рисунка заменяют блоком контейнера, который имеет наибольшее сходство с заменяемым блоком. Для нахождения наиболее сходных блоков используется логическая операция Исключающее ИЛИ.

На принимающую сторону передают номера блоков контейнера в нужной последовательности. Для показанных рисунков последовательность такая: 3-4-2-2-7-16-9-10-11-2-13-14-2-1-2-2. Нумерация блоков выполнена слева направо и сверху вниз.

Таким образом, передаваемый рисунок заменяется числами (индексами). Принятый рисунок будет отличаться от переданного, так как он состоит из фрагментов другого рисунка. Понятно, что воспроизведение на приёме будет тем точнее, чем больше полностью совпадающих блоков в передаваемом рисунке и контейнере. В приведённых рисунках полностью совпадают незаполненные (пустые) блоки, а также блок 6 исходного рисунка полностью идентичен блоку 16 контейнера.

Этот способ позволяет не только скрытно передать изображение, но и сжать информацию. Каждый блок исходного изображения (для цветного изображения 8x8x24 = 1536 бит) заменяется одним числом. В 24-х битном рисунке 1600x800 (объём 3,66 Мбайт) содержится 20 тысяч блоков 8x8. Для записи номеров этих блоков достаточно пяти десятичных цифр, то есть 40 бит на каждый блок. Для скрытой передачи рисунка с помощью индексов достаточно 0,1 Мбайт информации. Таким образом можно осуществить сжатие в 36 раз. Однако это будет сжатие с потерями, так как принятый рисунок отличается от исходного.

Эта идея может быть использована и для скрытой передачи одного звукового файла в другом звуковом файле (в контейнере). В этом случае отыскивают сходные отсчёты (семплы) и также передают лишь номера отсчётов контейнера.



Легче всего проиллюстрировать идею скрытой передачи информации с помощью фотографий и рисунков. В настоящее время практически у каждого взрослого человека имеется фотоаппарат (например, встроенный в сотовый телефон). Число фотографий, ежедневно появляющихся на нашей планете, оценивается миллиардами штук. Фотографии легко использовать для скрытой передачи информации, например, с помощью MMS или электронной почты.

Рассмотрим несколько примеров.

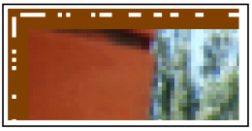
На следующих фотографиях скрыто слово «ФБТО». Эта аббревиатура означает: «Факультет Базового Телекоммуникационного Образования». На первой фотографии изображены 32 студента (средний ряд), которые сидят в определённом порядке (в виде матрицы 8x4). Каждая буква закодирована одним байтом (причём юноши соответствуют логическим единицам, а девушки - нулям).

Первый байт 11010100 (отсчёт сверху вниз, слева направо). Эта комбинация соответствует букве «Ф». Второй байт – 11000001 - буква «Б» и т.д.

Это же слово на второй фотографии скрыто несколько иным способом: единицы – это сидящие студенты, а нули – это пустые места.

Потенциальные возможности сокрытия информации в фотографиях огромные: можно в качестве отличительных признаков использовать наличие или отсутствие головных уборов, цвет одежды, положение рук и т.п.

Информацию можно скрыть, нанеся малозаметные метки на рамке рисунка. При этом логические единицы и нули заменяются точками разных цветов. Следующая фотография содержит портрет велосипедистки, помещённый в рамку. Справа изображён левый верхний угол фотографии в увеличенном масштабе. Здесь хорошо видны внедрённые знаки.

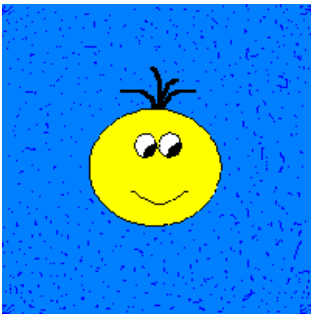


Очевидно, что если противнику известно, где размещена скрытая информация, то извлечение и декодирование сообщения не представляет труда. Усложнить стеганоанализ можно путём предварительного шифрования скрываемого текста.

Ещё один способ повышения криптостойкости скрытого сообщения заключается в том, что окрашиваемые пиксели размещают не линейно (последовательно), а с помощью псевдослучайных чисел. При этом эта последовательность чисел становится секретным ключом, который известен только доверенным лицам на передающей и приёмной сторонах.

Скрыть секретный текст на фотографии можно, разукрасив определённым способом лампочки на ёлочной гирлянде.

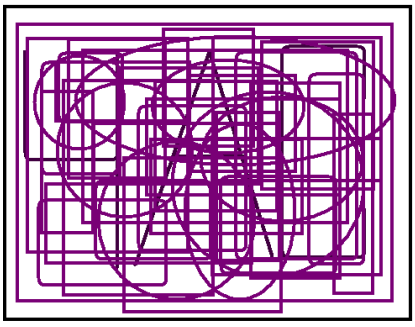
Скрыть буквы можно с помощью рисунка, у которого фон выглядит в виде пёстрой мозаики. При этом скрываемые символы располагаются в определённых (заранее оговорённых) местах изображения. На следующем рисунке скрытно передаваемые буквы расположены в углах картинки в виде искажённой матрицы пикселей. Алгоритм искажения символов определяется секретным ключом.



В войсках для маскировки военной техники используют маскирующие сети. Благодаря сетям объекты сложно различить с большой высоты и с большого расстояния. Эту идею можно использовать для сокрытия информации в электронных графических контейнерах.

Одна из возможных реализаций может быть выполнена следующим образом. В графическом редакторе на белом листе пишется секретный текст буквами определённого цвета. Поверх текста наносится сетка хаотической формы, причём цвет сетки должен незначительно отличаться от цвета скрываемых букв (одна из цветовых составляющих R, G, B изменяется на одну единицу).

На приёмной стороне рисунок «проявляют» (извлекают скрытую информацию). Для извлечения скрытого текста в графическом редакторе выполняют заливку сетки белой краской. В результате этого сетка исчезает и проступает секретный текст.



3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие информации в текстовом документе

В соответствии с номером своего варианта необходимо скрыть текстовую информацию в документе MS Word (табл. 3.1.1).

Таблица 3.1.1

Вар.	Файл	Текст
1.	Вариант 1.doc	Мы учимся, увы, для школы, а не для жизни. *Сенека*
2.	Вариант 2.doc	Сегодня первый день твоей оставшейся жизни. *NN*
3.	Вариант 3.doc	Пока не наступит завтра, ты не поймёшь, как хорошо тебе было сегодня. *Л. Левинсон*
4.	Вариант 4.doc	Сорняки растут не везде, а только там, где они не нужны. *М. Генин*
5.	Вариант 5.doc	Усложнять просто, упрощать сложно. *Закон Майера*
6.	Вариант 6.doc	Всем правит случай. Знать бы ещё, кто правит случаем. *С. Лец*
7.	Вариант 7.doc	Смех – кратчайшее расстояние между двумя людьми. *В. Борж*
8.	Вариант 8.doc	Женщины в основном помнят только тех мужчин, которые заставляли их смеяться, а мужчины - только тех женщин, которые заставляли их плакать. *А.Ренье*
9.	Вариант 9.doc	Хорошему человеку бывает стыдно даже перед собакой. *А. Чехов*
10.	Вариант 10.doc	Если у вас ничего нет, то имейте хотя бы совесть. *Г. Яблонский*
11.	Вариант 11.doc	Нет, нет и ещё раз да! *NN*
12.	Вариант 12.doc	Тот, кто храпит, засыпает первым. *А. Блох*
13.	Вариант 13.doc	Дискуссия – это обмен знаниями, спор – обмен невежеством. *Р. Куиллен*
14.	Вариант 14.doc	Твоя судьба целиком находится под твоей шляпой. *Пшекруй*
15.	Вариант 15.doc	Брось везунчика в воду, и он выплывет с рыбой в зубах. *Ю. Тувим*
16.	Вариант 16.doc	Мудрость – это не морщины, а извилины. *В. Жемчужников*

3.2. Задание 2. Извлечение информации из текста

В соответствии с номером варианта необходимо извлечь текстовую информацию, которая скрыта в документе MS Word. Имя файла совпадает с номером варианта. Местоположение файлов указывается преподавателем.

3.3. Задание 3. Сокрытие текстовой информации в рамке рисунка

В соответствии с номером варианта необходимо скрыть текстовую информацию (табл. 3.3.1) в рамке рисунка. При сокрытии нужно взять первые 10 символов указанного текста.

Таблица 3.3.1

Вариант	Файл	Текст
1.	1.bmp	Без любви человек есть призрак. *В.Г. Белинский*
2.	2.bmp	Надо верить тому, кого любишь. *В. Брюсов*
3.	3.bmp	Рассуждать о любви – терять рассудок. *С. Буффлер*
4.	4.bmp	Любовь – сладкая тирания. *Э. Бок*
5.	5.bmp	Разлука для любви – ветер для огня. *Р. Бюсси-Рабютен*
6.	6.bmp	Любовь травами не лечится. *Овидий*
7.	7.bmp	Чтобы любить, надо уметь прощать. *А Вампилов*
8.	8.bmp	Постоянство – всегдашняя мечта любви. *Л. Вовенарг*
9.	9.bmp	Любви все возрасты покорны. *А. Пушкин*
10.	10.bmp	Любовь – это желание жить. М. *Горький*
11.	11.bmp	Умирать от любви, - значит жить ею. *В. Гюго*
12.	12.bmp	Где есть любовь – там нет страдания. *Ф. Дзержинский*
13.	13.bmp	В любви победитель тот, кого любовь победила. *Санайи*
14.	14.bmp	Любовь вдохновляет на великие дела. *А. Дюма*
15.	15.bmp	Когда любишь, сомневаешься во всем. *Г. Колетт*

16.	16.bmp	Любовь – огонь, тоска по счастью. *Лопе де Вега*

3.4. Задание 4. Извлечение текстовой информации

В соответствии с номером варианта необходимо извлечь текстовую информацию, скрытую в рамке рисунка. Имя файла-контейнера (стего) совпадает с номером варианта.

3.5. Задание 5. Сокрытие шифрованной текстовой информации

В соответствии с номером варианта необходимо скрыть слово, состоящее из четырёх букв (таблица 3.5.1), в графическом файле-контейнере с помощью алфавита, показанного на следующем рисунке. Буквы должны быть предварительно зашифрованы (искажены) методом перестановок пикселей.

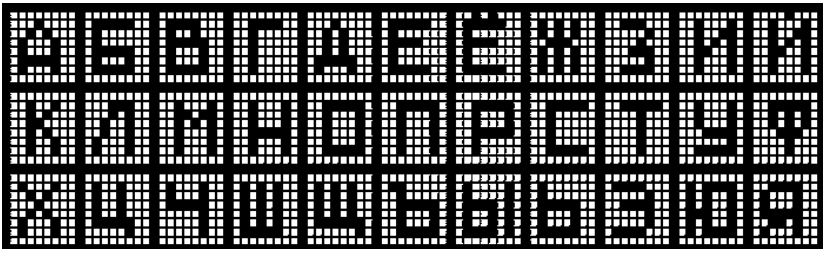


Таблица 3.5.1

Вариант	Слово	Контейнер
1	ПИЛА	1.bmp
2	БУРЯ	2.bmp
3	ШИРЬ	3.bmp
4	ПЕЧЬ	4.bmp
5	ПЕНА	5.bmp
6	СИЛА	6.bmp
7	ЗАРЯ	7.bmp
8	ГОРА	8.bmp
9	СВЕТ	9.bmp
10	СТАЯ	10.bmp
11	ТИШЬ	11.bmp
12	РЫБА	12.bmp
13	ПУЛЯ	13.bmp
14	ЛУНА	14.bmp
15	ДЕЛО	15.bmp
16	УРОК	16.bmp

В табл. 3.5.2 указаны величины циклических сдвигов влево в каждой строке матрицы, которые необходимо сделать при шифровании.

Таблица 3.5.2

Варианты / Строки	1	2	3	4	5	6	7	8
1	2	1	5	3	2	4	2	1
2	1	2	5	4	6	3	1	4
3	2	4	3	1	2	1	3	5
4	3	5	1	2	1	4	4	2
5	4	2	2	5	4	6	1	1
6	1	1	3	4	3	2	3	5
7	2	3	4	2	2	4	1	5
8	1	5	3	1	4	3	4	2

Продолжение таблицы 3.5.2

Варианты / Строки	9	10	11	12	13	14	15	16
1	3	2	4	1	1	3	2	3
2	6	3	2	2	3	5	1	4
3	1	1	1	3	5	1	5	1
4	2	4	6	4	2	2	3	2
5	5	5	2	1	1	3	4	5
6	1	2	4	3	5	1	4	6
7	1	1	3	5	3	1	2	3
8	3	5	1	4	1	5	1	4

3.6. Задание 6. Извлечение зашифрованного текста из рисунка

В соответствии с номером варианта необходимо извлечь текст из графического файла-контейнера. Величина циклического сдвига вправо при расшифровании букв в каждом варианте определяется с помощью таблицы 3.6.1.

Таблица 3.6.1

Варианты / строки	1	2	3	4	5	6	7	8
1	2	1	3	2	2	4	3	2
2	1	4	6	3	6	3	5	1
3	3	6	1	1	2	1	1	5
4	2	3	3	4	5	4	2	3
5	4	6	3	5	1	6	3	4
6	1	3	3	4	5	2	3	5
7	2	5	4	2	2	4	1	5
8	1	5	3	1	4	3	4	2

Продолжение таблицы 3.6.1

Варианты / строки	9	10	11	12	13	14	15	16
1	3	5	2	1	1	3	2	1
2	4	2	4	3	3	2	6	4
3	1	8	3	5	5	3	2	3
4	2	4	6	4	2	3	4	3
5	5	1	2	3	1	1	2	1
6	1	2	3	4	5	4	6	4
7	5	8	4	5	3	5	2	3
8	3	5	1	5	1	3	4	2

3.7. Задание 7. Извлечение текстовой информации, скрытой в рамке графического объекта с помощью азбуки Морзе

Извлечь текст, скрытый в рамке графического объекта с помощью азбуки «Морзе». Имя графического контейнера совпадает с номером варианта. Местоположение папки с файлами-контейнерами указывается преподавателем.

3.8. Задание 8. Извлечение текстовой информации из графического объекта «Гирлянда»

Извлечь текстовую информацию из графического объекта. Имя графического контейнера (стего) совпадает с номером варианта.

4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1.

Для того чтобы скрыть информацию в текстовом документе, необходимо текст из таблицы 3.1.1 поместить в заданный текстовый документ. Затем выделить скрываемый текст и нажать на кнопку **Цвет шрифта**. Выбрать из палитры белый цвет. Белый шрифт на белом фоне не будет виден.

4.2. Методические указания к заданию 3.2.

Для того чтобы отобразить информацию, скрытую в текстовом документе, необходимо выделить весь текст и, нажав на кнопку **Цвет шрифта**, выбрать из палитры чёрный цвет.

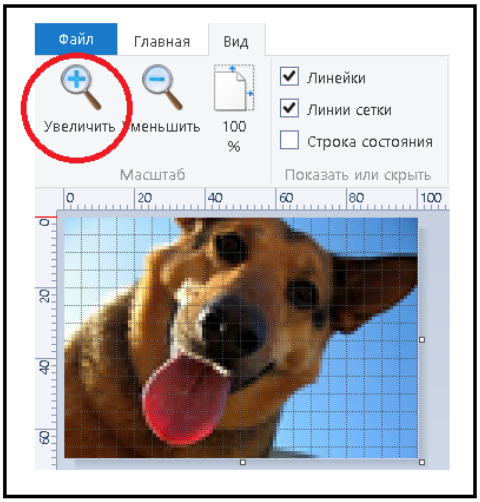
4.3. Методические указания к заданию 3.3.

Рассмотрим порядок сокрытия информации в рамке графического объекта. Пусть дана последовательность символов **«Жить – значит мыслить».** Предварительно необходимо преобразовать каждую букву фразы с помощью таблицы CP-1251 в десятичное число, а затем в двоичный код.

Таблица 4.3.1

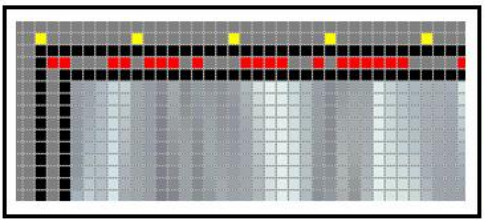
	Буква	**Число десятичное**	**Число двоичное**
1.	Ж	198	11000110
2.	и	232	11101000
3.	т	242	11110010
4.	ь	252	11111100
5.	Пробел	32	00100000
6.	-	45	00101101
7.	Пробел	32	00100000
8.	з	231	11100111
9.	н	237	11101101
10.	а	224	11100000
11.	ч	247	11110111
12.	и	232	11101000
13.	т	242	11110010
14.	Пробел	32	00100000
15.	м	236	11101100
16.	ы	251	11111011
17.	с	241	11110001
18.	л	235	11101011
19.	и	232	11101000
20.	т	242	11110010
21.	ь	252	11111100

Скрытое изображение формируется с помощью графического редактора MS Paint. При формировании стего нужно получить изображение в большом масштабе. Для этого следует использовать кнопку **Увеличить**, которая находится на вкладке **Вид**.



Для формирования скрытой информации потребуется координатная сетка, которая выводится с помощью опций: **Вид – Линии сетки.**

Вначале необходимо вокруг рисунка начертить две тёмные рамки. Промежуток между рамками целесообразно выбрать равным одному пикселю. Внедряемая информация в виде разноцветных пикселей размещается между рамками, начиная с левого верхнего угла. Для облегчения процедуры записи букв (представленных байтами) можно временно выделить каждый восьмой пиксель ярким цветом, например, жёлтым.



Обозначив логическую единицу и логический ноль разными цветами, следует выполнить запись двоичных чисел, которыми закодирован скрываемый текст.

Аналогично кодируются остальные комбинации двоичных символов. В результате получается двойная чёрная рамка с разноцветными «вкраплениями» - закодированной информацией.

4.4. Методические указания к заданию 3.4.

Для того чтобы извлечь информацию, скрытую в рамке графического объекта, необходимо выполнить следующие операции.

1. Выделить первую комбинацию двоичных символов.
2. Перевести полученное двоичное число в десятичное число.
3. С помощью таблицы **СР-1251** перевести десятичное число в букву.
4. Аналогично извлечь следующие буквы.

4.5. Методические указания к заданию 3.5.

Рассмотрим пример шифрования символа путём циклического сдвига влево пикселей по строкам. Скроем слово «ТЕНЬ» в графическом файле с именем пример.bmp. Первая буква «Т» с помощью алфавита представлена в виде:

	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	0
2	0	0	**1**	**1**	**1**	**1**	**1**	0
3	0	0	0	0	**1**	0	0	0
4	0	0	0	0	**1**	0	0	0
5	0	0	0	0	**1**	0	0	0
6	0	0	0	0	**1**	0	0	0
7	0	0	0	0	**1**	0	0	0
8	0	0	0	0	0	0	0	0

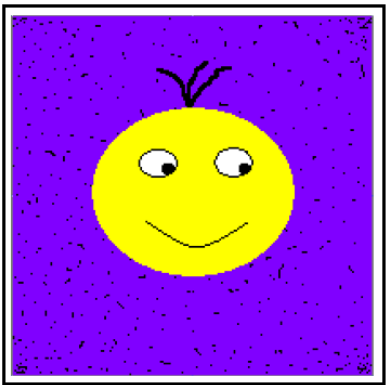
Затем каждая строка матрицы сдвигается циклически влево на число позиций, в соответствии с ключом 3 5 7 6 2 4 1 2.

ключ		1	2	3	4	5	6	7	8
3	1	0	0	0	0	0	0	0	0
5	2	**1**	**1**	0	0	0	**1**	**1**	**1**
7	3	0	0	0	0	**0**	**1**	0	0
6	4	0	0	0	0	0	0	**1**	0
2	5	0	0	**1**	0	0	0	0	0
4	6	**1**	0	0	0	0	0	0	0
1	7	0	0	0	**1**	0	0	0	0
2	8	0	0	0	0	0	0	0	0

Аналогично шифруются остальные буквы слова.

Полученные матрицы 8×8 с четырьмя зашифрованными буквами помещают в углы рисунка, начиная с верхнего левого угла по часовой стрелке.

Таким образом, получается графическое изображение вида:



4.6. Методические указания к заданию 3.6.

Для того чтобы извлечь информацию, необходимо проделать такие операции.

1. Графическое изображение поместить в редактор MS Paint.
2. Извлечь матрицы из углов рисунка.
3. По ключу восстановить исходное положение каждого пикселя. Для этого нужно выполнить циклический сдвиг вправо элементов каждой строки на заданное значение.

4.7. Методические указания к заданию 3.7.

В данном задании для сокрытия слова в рамке графического изображения используется азбука Морзе, представляющая собой чередование символов «точка» и «тире».

Таблица 4.7.1

Код Морзе	Русский алфавит	Латинский алфавит	Код Морзе	Русский алфавит	Латинский алфавит
▪–	А	A	▪– ▪	Р	R
– ▪▪▪	Б	B	▪▪▪	С	S
▪– –	В	W	–	Т	T
– – ▪	Г	G	▪▪–	У	U
– ▪▪	Д	D	▪▪– ▪	Ф	F
▪	Е	E	▪▪▪▪	Х	H
▪▪▪–	Ж	V	– ▪– ▪	Ц	C
– – ▪▪	З	Z	– – – ▪	Ч	
▪▪	И	I	– – – –	Ш	
▪– – –	Й	J	– – ▪–	Ш	Q
– ▪–	К	K	– ▪– –	Ы	Y
▪– ▪▪	Л	L	– ▪▪–	Ь	X
– –	М	M	▪▪– ▪▪	Э	
– ▪	Н	N	▪▪– –	Ю	
– – –	О	O	▪– ▪–	Я	
▪– – ▪	П	P			

Для того чтобы извлечь информацию из графического объекта, необходимо проделать следующие действия.

1. Графическое изображение поместить в редактор MS Paint.
2. Выявить первую комбинацию символов.
3. С помощью азбуки Морзе перевести символы в букву.
4. Аналогично извлечь остальные буквы.

4.8. Методические указания к заданию 3.8.

В этом задании использован графический контейнер с изображением новогодней ёлки.

В крайней правой гирлянде скрыта текстовая информация с помощью двоичного кода (таблица CP-1251). Информация скрыта с помощью цветных лампочек, слегка отличающихся между собой цветовым оттенком. Розовый цвет лампочки соответствует «0», а зелёный цвет лампочки – «1».

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать исходные данные и результаты преобразований.

6. Контрольные вопросы

6.1. В чём состоит основная идея стеганографии?

6.2. Предложите свой способ скрытой передачи информации в графическом контейнере.

6.3. Как скрытно передать сообщение в текстовом документе?

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. Что означает термин «стего»?

6.8. Что такое акростих?

7. Список литературы

1. Алексеев А.П. Информатика 2015: учебное пособие/ Алексеев А.П. – М: СОЛОН-Пресс, 2015. – 400 с. ISBN 978-5-91359-158-6.

2. Алексеев А.П., Орлов В.В., Сухова Е.Н. Изучение стеганографии на уроках информатики //Информатика и образование, № 8, 2007, стр. 65-72.

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

4. Алексеев А.П., Садовая В.В. Передача скрытых сообщений методами стеганографии. Мет. указания на проведение лабораторных работ. Самара: ПГУТИ, 2008. - 30 с.