Федеральное агентство связи

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

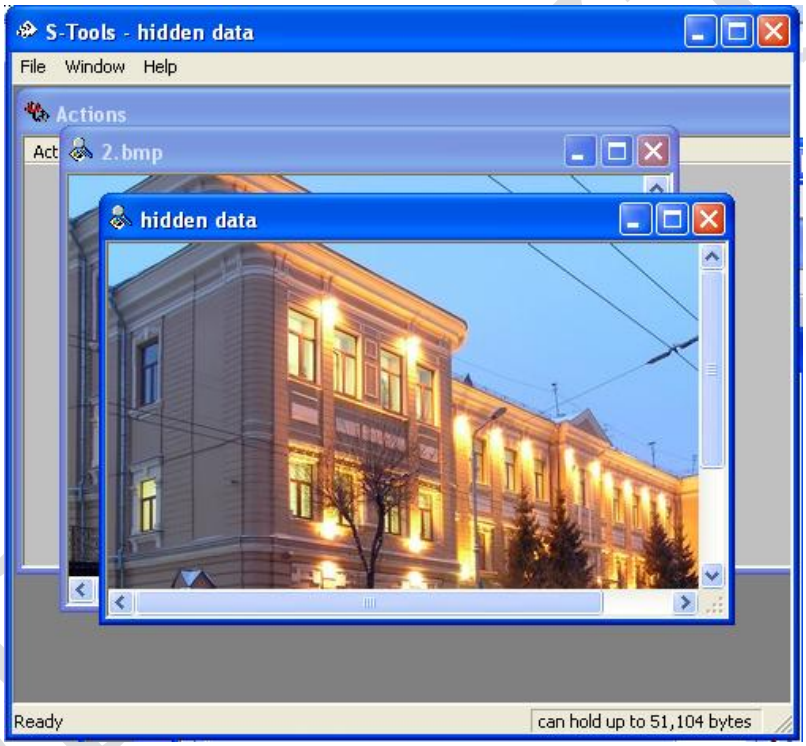
Самара

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ
Кафедра Информатики и вычислительной техники

Методические указания на проведение лабораторных работ

«Сокрытие информации методом временного распределения»

по дисциплине «Информатика»,
специальности 210400…210406, 210302, 090106.



Авторы-составители:
доц., к.т.н. **Алексеев А.П.,**

Под общей редакцией Алексеева А.П.

Самара, 2010

Введение

Защищенные методы обмена информацией можно разделить на два больших направления: криптографию и стеганографию.

При криптографическом способе защиты информации факт передачи информации не скрывается от противника. Однако сообщение шифруется, и вскрыть такое сообщение (криптограмму) без знания секретного ключа бывает очень сложно. Для взлома такого сообщения используют распределенную вычислительную сеть, состоящую из множества быстродействующих ЭВМ.

Стеганография предполагает такой способ передачи информации, при котором факт передачи информации остается незаметным для противника (конкурента). Передаваемое сообщение встраивают в электронные контейнеры (рисунки, звуки, видеоклипы).

Смысл метода заключается в том, что для информационной страницы создают страницу-близнец, которая внешне ничем не отличается от информационной страницы. На сайте постоянно демонстрируются страница-близнец, которая не содержит секретной информации. В определенный момент времени (известный только на передающей и на приемной сторонах) происходит замена страницы-близнеца на информационную страницу.

В данной работе студенты освоят метод сокрытия информации методом временного распределения. А именно, разработают программу на языке JavaScript для сокрытия рисунков формата bmp или gif, освоят программу S-Tools – это профессиональная программа, и ее используют для незаметной передачи информации внутри звуковых или графических файлов.

Сокрытие информации методом временного распыления

1. Подготовка к работе

Изучить базовые средства языка программирования JavaScript, порядок работы с программой S-Tools. Ответить на контрольные вопросы.

2. Контрольные вопросы

2.1. В чем состоит основная идея стеганографии?
2.2. Для чего предназначена программа S-Tools?
2.4. В чем принципиальное различие криптографии и стеганографии?
2.5. Что означает термин «контейнер»?
2.6. Приведите примеры контейнеров, которые могут быть использованы для скрытой передачи информации.
2.7. Какие контейнеры используются в программе S-Tools?
2.9. Каковы сферы использования стеганографии?
2.10. Какова структура web-страницы?
2.11. Что располагается между тегами <body>< /body >?
2.12. Как с помощью программы S-Tools скрыть файл в графическом контейнере?
2.13. С помощью каких тегов создается таблица?
2.14. Как восстановить данные, скрытые программой S-Tools в графическом файле?
2.15. Какие страницы называются динамическими www-страницами?
2.16. Как сделать выравнивание текста в абзаце?
2.17. Какой тег отвечает за отображение иллюстрации на странице?
2.18. Какой объект отвечает за отображение времени?
2.19. Как объединить несколько ячеек в таблице?
2.20. Поясните строки программы, отвечающие за смену изображения.
2.21. Как сделать разметку страницы невидимой?

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие текста в графическом контейнере (программа S-Tools)

3.2.1. В соответствии со своим вариантом с помощью S-Tools скрыть заданный текст в указанном графическом файле. Графические файлы (пустые контейнеры) следует выбрать из папки NEW, причем имена подпапок совпадают с номерами вариантов. Скрываемый текст и файл, в который его нужно поместить выбирается в соответствии с таблицей 1. Пароль и метод шифрования нужно выбрать самостоятельно. Зашифрованный файл (начиненный контейнер) следует сохранить в своей папке.

Выполненное задание пошагово заносится в отчет лабораторной работы.

В отчете необходимо указать максимально допустимый объем скрываемой информации в данном графическом файле, описать порядок сокрытия текстового файла в графическом контейнере с помощью программы S-Tools, а также привести выбранный алгоритм шифрования и пароль.

Таблица 1

№ варианта	Имя файла	Текст
1	1.bmp	Диссонанс есть величайшая сила музыки
2	2.bmp	Не количество жизни дорого, а качество.
3	3.bmp	Слово «завтра» придумано для людей нерешительных и для детей.
4	4.bmp	Там хорошо, где нас нет: в прошлом нас уже нет, и оно кажется прекрасным.
5	5.bmp	Время – движущийся образ неподвижной вечности.
6	1.bmp	Ничего не откладывай на после, ибо после тебе легче не будет.
7	2.bmp	Самая большая трата, которую только можно сделать, - это трата времени.
8	3.bmp	Время – самое драгоценное из всех средств.
9	4.bmp	Мы восхищаемся древностью, но живем сейчас.
10	5.bmp	Самый мудрый человек тот, кого больше всего раздражает потеря времени.
11	1.bmp	Ничто не вечно под солнцем.
12	2.bmp	Минуты длительны, а годы скоротечны.
13	3.bmp	Не те уж годы, да и настроение не то.
14	4.bmp	Время – это капитал работника умственного труда.
15	5.bmp	Нельзя убивать время, не вредя этим вечности.
16	1.bmp	Кто долго раздумывает, не всегда находит лучшее решение.
17	2.bmp	День дорог для того, кто умеет жить.

3.2. Задание 2. Разработка программы на языке JavaScript для временного распределения информации

3.1.1. Реализовать стеганографический метод сокрытия информации с помощью JavaScript.

В соответствии со своим вариантом создать web-страницу на основе шаблона index.html, на которой информация будет скрываться в рисунках. Скрипты, осуществляющие подмену рисунков, реализовать с помощью языков программирования JavaScript.

На странице поместить изображения из папки NEW, имена подпапок совпадают с номерами вариантов (подобно заданию 1). Также на ней должно

находиться: время выполнения задания, размещенное в верхнем левом углу, фамилия и имя студента, группа и вариант. Ниже располагается заголовок и 4 рисунка, один из которых в определенное время заменяется файлом, начиненным секретной информацией (из задания 1). Имя заменяемого рисунка, а также интервал времени, на который появляется зашифрованный файл, выбирается в соответствии с таблицей 2.

В отчете необходимо разместить листинг программы на языке JavaScript; начальную информационную страницу, используя Print Screen (чтобы создать копию активного окна, нажмите клавиши ALT+ Print Screen), причем размер рисунков выбирается таким образом, чтобы была видима вся область страницы; страницу – близнец с измененным содержимым, рисункам дать названия самостоятельно.

Таблица 2

№ варианта	Имя заменяемого файла	Интервал времени появления секретной информации (мин)
1	5.jpg	4
2	4.jpg	3
3	1.jpg	2
4	2.jpg	5
5	3.jpg	8
6	5.jpg	1
7	4.jpg	2
8	1.jpg	5
9	2.jpg	6
10	3.jpg	3
11	5.jpg	7
12	4.jpg	6
13	1.jpg	6
14	2.jpg	5
15	3.jpg	2
16	4.jpg	1
17	5.jpg	1

4. Методические указания

Методические указания к п. 3.1 (пример выполнения задания по варианту 17).

Для сокрытия данных в звуковом или графическом файле с помощью программы S-Tools нужно выполнить следующие действия.

1. В папке NEW найти папку, имя которой совпадает с номером варианта (в данном случае 17), затем «перетащить» мышью файл 2.bmp в открытое окно программы S-Tools.

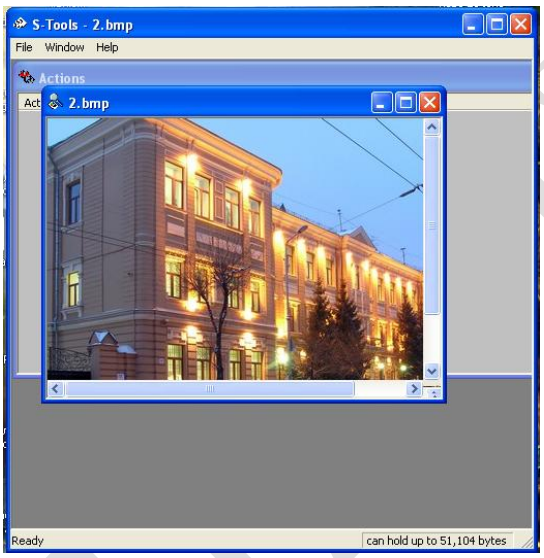


Рис. 1 – Файл-контейнер.

2. Далее «перетащить» созданный txt-файл с текстом «День дорог для того, кто умеет жить» в окно файла-контейнера (максимально возможный размер скрываемой информации указан в нижнем правом углу окна S-Tools).

3. Если размер файла достаточен для сокрытия данных в нем, то появится новое окно. В нем следует ввести пароль (Passphrase), подтвердить его (Verify Passphrase), а также выбрать алгоритм шифрования (Encryption Algorithm).

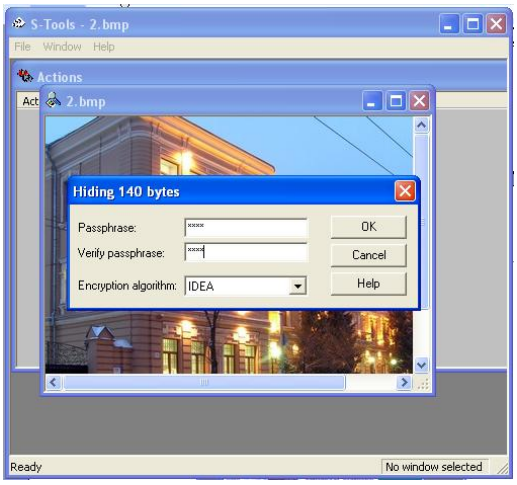


Рис. 2 – Окно задания атрибутов для зашифрованного файла.

4. Далее может появиться меню задания свойств (для изображений) - Convert to a 24-bit image (Конвертировать в 24-битное изображение) и Attempt colour reduction (Уменьшение цветовой гаммы).

5. Результат преобразования появится в окне Hidden data (Скрытые данные).

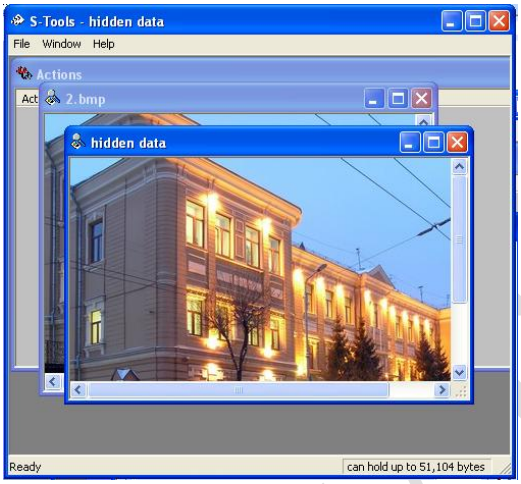


Рис. 3 – Результат преобразования

Для сохранения результатов шифрования, нужно щелчком правой кнопки мыши выбрать опцию **Save as…** (Сохранить как…), указать имя файла, расширение, и выбрать месторасположение. Сохранить нужно с именем crypto17.txt, где 17 - это № варианта.

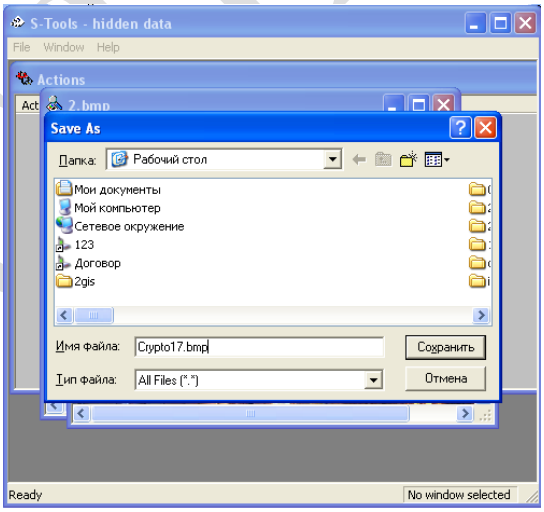


Рис. 4 – Окно сохранения

Далее этот файл с зашифрованной информацией будет использоваться в пункте 3.2

Методические указания к п. 3.2 (пример выполнения задания по варианту 17).

Открыть страницу-шаблон index.html с помощью Notepad (Блокнот). Далее требуется сделать правку документа таким образом, чтобы на www-странице стояли фамилия и имя студента, его группа, номер варианта путем изменения строк кода в выше названном документе. Для этого нужно:

1. В строке <H5 align=right><B> Студент группы
 Вариант № </B></H5> после слова «Студент» добавить свою фамилию и имя, после слова «группы» добавить номер своей группы, после фразы «Вариант №» добавить номер варианта.

Следом за этим нужно в папке NEW найти папку, имя которой совпадает с номером варианта (в данном случае 17), выяснить какие рисунки должны появиться на странице (в нашем случае это файлы 1, 3, 4, 5). Подписи должны соответствовать изображениям, что также выполняется путем изменения скрипта.

1. В строке <td align="center"><H4><B>ГазБанк</B></H4> между тегами <B></B> вписать название первой фотографии.
2. В строке <IMG src="1.jpg" width=300> указать название файла с первой фотографией, соответствующей названию в п. 2, width=300 – указание размера фотографии;
3. Аналогично делаются изменения в строках – <td align="center"><H4><B>НомосБанк</B></H4> <IMG src="3.jpg" width=300, <td align="center"><H4><B>СберБанк на ул. Гагарина</B></H4> <IMG src="4.jpg" width=300>;
4. Найти фрагмент кода if ((time >= st) && (time < et)) document.write("<H4 align=center><B>ГУ СберБанк</B></H4><P align=center><img src=\"2.bmp\" width=150</P>") и в нем также сделать подобные изменения, учитывая, что он отвечает за появление фотографии с зашифрованными данными;
5. Данная строка else document.write("<H4 align=center><B>АвтоВазБанк</B> </H4 ><P align=center><img src=\"5.jpg\" width=300</P>") отвечает за исчезновение изображения 5.jpg, здесь также требуется внести изменения в название фотографии и имени файла.

Следующим пунктом станет замена изображений одного другим на определенный промежуток времени. В нашем случае требуется замена рисунка 5.jpg зашифрованным файлом crypto17.bmp (из п. 3.1) на 1 минуту (таблица 2). Для этого нужно(для варианта 17):

1. В строке start.setHours(23) поставить час исчезновения изображения 5.jpg и появления 2.bmp, в start.setMinutes(52) – минуту исчезновения;
2. В строке end.setHours(23) – час исчезновения 2.bmp и появления 5.jpg, в end.setMinutes(53) – минуту.

В данном случае получилось, что в 23.52 исчезает изображение 5.jpg и появляется 2.bmp, а в 23.53 5.jpg обратно заменяет 2.bmp.

В итоге листинг программы будет иметь вид:

```
<html>
<head>
<table align="center" width="100%" cellpacing="0" cellpadding="0" border="3">
<tr>
<td>
  <body leftmargin=0 topmargin=0>
<script language="JavaScript">
  cDate = new Date();
  document.write("Время выполнения задания: "+ cDate.toLocaleString());
</script>
</body>
</td>
</tr>
<tr>
<td COLSPAN=4>
<H5 align=right><B> Студент группы <BR> Вариант № </B></H5>
</td>
</tr>
<tr>
<td COLSPAN=4><H2 align=center><B> Сокрытие информации методом временного
 распыления</B></H2>
</td>
</tr>
<tr>
<td align="center"><H4><B>ГазБанк</B></H4>
<IMG src="1.jpg" width=300>
</td>
<td align="center"><H4><B>НомосБанк</B></H4>
<IMG src="3.jpg" width=300
</td>
</tr>
<tr>
<td align="center"><H4><B>СберБанк на ул. Гагарина</B></H4>
<IMG src="4.jpg" width=300>
</td>
</head>
<body>
<td>
<script language="JavaScript">
  var start = new Date();
  var end = new Date();
```

```
start.setHours(23);
start.setMinutes(52);
end.setHours(23);
end.setMinutes(53);
var now = new Date();
st = start.getTime();
et = end.getTime();
time = now.getTime();
if ((time >= st) && (time < et)) document.write("<H4 align=center><B>ГУ СберБанк</B></H4><P align=center><img src=\"2.bmp\" width=150</P>");
else document.write("<H4 align=center><B>АвтоВазБанк</B> </H4 ><P align=center><img src=\"5.jpg\"  width=300</P>");
</script>
</td>
</body>
</tr>
</table>
</html>
```

Список литературы

1. Алексеев А.П. Информатика 2007. – М.: СОЛОН-ПРЕСС, 2007. – 608 с.
2. Алексеев А.П. Введение в Web-дизайн. – М.: Солон-Пресс, 2008. – 192 с.
3. Усенков Д. Уроки Web-мастера. – М.: Лаборатория Базовых Знаний, 2001. – 432 с.
4. Алексеев А.П., Жеренов Ю.В. Пространственно-временное распыление информации – Тезисы конференции – Самара, 2010.
5. Алексеев А. П., Орлов В.В. Стеганографические и криптографические методы защиты информации; учебное пособие. Самара: ИУНЛ ПГУТИ, 2010. - 330 с.

Приложение 1

Файлы Web-страниц, написанные на языке HTML (Hypertext Markup Language – язык разметки гипертекста), определяют внешний вид в окне браузера таких элементов как текст, таблицы и изображения. При этом HTML работает только со статическими элементами.

JavaScript – это наиболее популярный язык сценариев, который может применяться в файлах Web-страниц наряду с HTML. Эти возможности позволяют динамически управлять элементами Web-страниц. Например, можно предусмотреть, чтобы текст, отображаемый в текстовом поле формы, изменялся.

Сценарий JavaScript может выполняться в браузере без каких-либо дополнительных программных средств.

Начинается и завершается любая страница парой тегов <html></html>. Они сигнализируют браузерам о том, что программа написана на языке HTML. Между тегами <head> </head> помещаются сведения о названии страницы и служебная информация. Содержимое страницы, воссоздаваемое на экране монитора, располагается между тегами <body></body>.

Итак, HTML – набор команд(тегов), вставляемых в текст www-страницы и определяющих форматирование абзацев, вид шрифта, ссылки на внешние источники и т.д. Интернет-страница – обособленный документ, хранящийся в отдельном файле на диске и включающий в себя текст, отображаемый на экране во время просмотра в браузере, а также специальные команды языка HTML, дополненный хранящимися в отдельных файлах и подгружаемых дополнительно по размещенным в тексте страницы ссылкам. Сайт – набор www-страниц, составляющих единую подборку и связанных между собой перекрестными ссылками. Одна из них является стартовой и играет роль содержания книги. Динамические www-страницы – Интернет - страницы, текст которых содержит фрагменты программного кода (скрипты). В отличие от обычных, содержимое которых практически не меняется от посещения к посещению, если его только не изменит владелец сайта, содержимое динамической страницы может меняться по заранее заданному сценарию.

Приложение 2

Описание программ S-Tools

Порядок работы с программой **S-Tools** достаточно прост. Он базируется на принципе Drag and Drop (Перенеси и положи). Вначале нужно развернуть окно программы S-Tools так, чтобы оно занимало небольшую часть экрана (примерно 25%). 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 объема файла-сообщения. Затем по технологии Drag and Drop внутрь программы нужно перенести иконку файла. После этого следует ввести пароль и сохранить зашифрованное сообщение.

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

При изучении методов стеганографии часто используется понятие «контейнер». Дадим определение этому термину.

Контейнер – это файл (звуковой, графический, текстовый или видео), в который помещается скрываемая информация. Внедрение скрываемой информации вызывает столь незначительные изменения контейнера, что практически они не обнаруживаются органами чувств человека (зрением и слухом).

При шифровании сообщений методами компьютерной стеганографии чаще всего используют информацию, запрятанную в изменении последних (наименьших) значащих битов LSB (**L**east **S**ignificant **B**its). При цифровом представлении графики и звука последний бит в байтах контейнера является малозначимым, часто изменяющимся по случайному закону. Шумы, существующие при аналого-цифровом преобразовании звука и изображения, случайным образом изменяют последний бит каждого отсчета.

При аналого-цифровом преобразовании звуков причиной практически случайного изменения LSB являются электромагнитные наводки на проводах звукозаписывающей аппаратуры, посторонние акустические шумы в студии, слышимое дыхание певца перед микрофоном и т.п.