Федеральное агентство связи

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

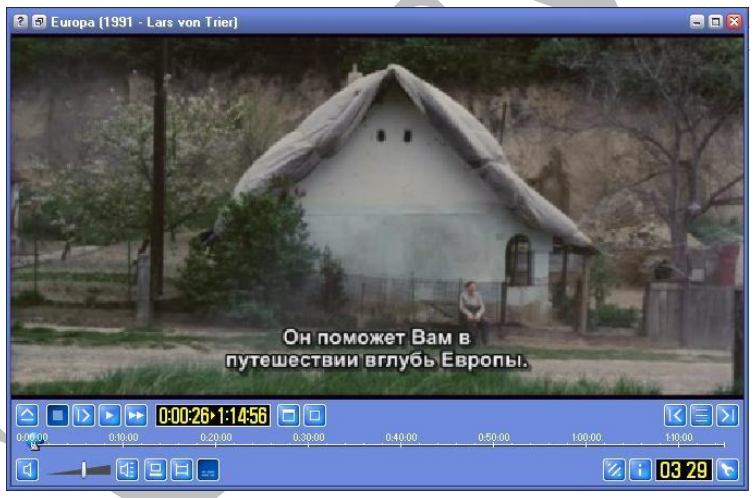
Самара

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ
Кафедра Информатики и вычислительной техники

Методические указания на проведение лабораторных работ

"Сокрытие информации в субтитрах"

по дисциплине «Информатика»,
специальности: 210400, 210401, 210402, 210403, 210404, 210405, 210406, 210302, 090106



Авторы-составители: доц., к.т.н. **Алексеев А.П.,**
ассист. **Макаров М.И.**
Под общей редакцией Алексеева А.П.

Самара, 2010

В в е д е н и е

Большой объём обрабатываемой цифровой информации выводит в наиболее актуальные проблемы сохранение интеллектуальной собственности - авторство и конфиденциальность. Их решением занимается наука стеганография. Подтверждение авторства реализуется с помощью цифровой подписи, а обеспечение конфиденциальности – путём сокрытием информации.

С начала нашего века, вследствие популяризации изучения разговорных иностранных языков по фильмам с оригинальными звуковыми дорожками, среди рядовых пользователей появляется тенденция к использованию субтитров. Эту сферу интеллектуальной собственности также не обошла стороной проблема авторства.

Данное методическое указание позволит студентам освоить методы сокрытия информации разрядов субтитрах.

Контейнерами является файлы субтитров, формат которых студенты изучат во время выполнения лабораторной работы.

Рекомендуемая литература

1. Алексеев А.П. Информатика 2007. – М.: СОЛОН-ПРЕСС.- 2007.- 608 с.
2. Алексеев А.П. Введение в Web-дизайн. Учебное пособие.- М.: СОЛОН-ПРЕСС, 2008.- 184 с.
3. Алексеев А.П., Орлов В.В., Сухова Е.Н. Изучение стеганографии на уроках информатики //Информатика и образование, № 8, 2007, стр. 65…72.
4. Алексеев А.П., Алексеев П.А., Мартяшина О.М., Сухова Е.Н. Изучение криптографии на уроках информатики //Информатика и образование, № 4, 2003, стр. 33…42.
5. Алексеев А. П., Орлов В.В. Стеганографические и криптографические методы защиты информации; учебное пособие. Самара: ИУНЛ ПГУТИ – 2010. - 330 с.

Лабораторная работа
«Сокрытие информации в субтитрах»

1. Подготовка к работе

По указанной литературе и методическим указаниям изучить основные понятия стеганографии и криптографии, уяснить принцип сокрытия информации в субтитрах. Ответить на контрольные вопросы.

2. Контрольные вопросы

2.1. В чем состоит принципиальное различие между криптографией и стеганографией?
2.2. Криптография и стеганография конкурируют между собой или дополняют друг друга?
2.3. Что такое цифровая подпись и сферы её применения?
2.4. В каком месте субтитров удобно размещать скрываемый текст?
2.5. Приведите примеры контейнеров, которые могут быть использованы в стеганографии.
2.6. Как преобразовать символ открытого текста в двоичное число?
2.7. Как преобразовать десятичное число в двоичное?
2.8. Как преобразовать двоичное число в десятичное?
2.9. Перечислите форматы видео файлов.
2.10. Перечислите методы сокрытия информации в текстовых документах.
2.11. На чём основан метод сокрытия информации с помощью младших разрядов?

Задание 3.1. Создание файла субтитров

3.1.1. Создать файл субтитров, используя текстовый редактор Notepad (Блокнот). Файл заполнить текстом и временем отображения в соответствии с вариантом. Данные для заполнения указаны в табл. 3.1

Таблица 3.1

Вар.	Стихи	Начало показа (мин:сек.)	Окончание показа (мин:сек)
1	Однажды летом в январе слона увидел я в ведре, слон закурил, пустив дымок, и мне сказал: не пей сынок. (Игорь Губерман)	1 : 00 1 : 30 2 : 10 3 : 5 4 : 10	1:25 1:40 2:30 3:50 4:30
2	Поэзия – нет дела бесполезней в житейской деловитой круговерти, но всё, что не исполнено поэзии, бесследно исчезает после смерти. (Игорь Губерман)	1 : 7 1 : 23 2 : 17 2 : 40 3 : 30	1:20 1:55 2:35 3:20 3:50
3	Слова – лишь символы и знаки того ручья с бездонным дном, который в нас течет во мраке и о совсем журчит ином. (Игорь Губерман)	1 : 5 1 : 39 1 : 55 3 : 00 3 : 23	1:30 1:53 2:50 3:20 3:50
4	Возможность лестью в душу влезть никак нельзя назвать растлением, мы бескорыстно ценим лесть за совпаденье с нашим мнением. (Игорь Губерман)	1 : 26 1 : 50 2 : 29 3 : 15 4 : 19	1:45 2:20 3:10 4:00 4;40
5	Много раз, будто кашу намасливал, книги мыслями я начинял, а цитаты из умерших классиков по невежеству сам сочинял. (Игорь Губерман)	1 : 1 1 : 21 2 : 28 2 : 40 2 : 50	1:15 1:50 2:30 2:45 3:00
6	Не тужи, дружок, что прожил ты свой век не в лучшем виде: все про всех одно и то же говорят на панихиде. (Игорь Губерман)	1 : 3 1 : 12 3 : 18 3 : 27 3 : 40	1:10 1:50 3:20 3:35 3:55
7	Между слухов, сказок, мифов, просто лжи, легенд и мнений мы враждуем жарче скифов	1 : 6 1 : 36 2 : 22	1:30 2:20 2:30

	за несходство заблуждений. (Игорь Губерман)	2 : 39 4 : 17	2:50 4:10
8	По будущему мысленно скитаясь и дали различая понемногу, я вижу, как старательный китаец для негра ставит в Туле синагогу. (Игорь Губерман)	1 : 28 1 : 36 2 : 00 3 : 13 3 : 27	1:30 1:50 2:50 3:20 3:35
9	Сызмальства сгибаясь над страницами, всё на свете помнил он и знал, только засорился эрудицией мыслеиспускательный канал. (Игорь Губерман)	1 : 40 1 : 50 2 : 25 3 : 00 3 : 20	1:45 2:15 2:50 3:10 3:50
10	Плодит начальников держава, не оставляя чистых мест; где раньше лошадь вольно ржала, теперь начальник водку ест. (Игорь Губерман)	1 : 23 1 : 40 2 : 11 3 : 27 4 :00	1:30 2:00 2:55 3:50 4:30
11	Мужчина – хам, зануда, деспот, мучитель, скряга и тупица; чтоб это стало нам известно, нам просто следует жениться. (Игорь Губерман)	1: 00. 1 : 21 2 : 22 3 : 35 4 : 20	1:15 1:40 2:50 3:55 4:35
12	Подпольно, исподволь, подспудно, родясь, как в городе – цветы, растут в нас мысли, корчась трудно сквозь битый камень суеты. (Игорь Губерман)	1 : 11 1 : 21 2 : 00 3 : 25 3 : 50	1:18 1:50 2:55 3:45 4:15
13	Из лет, надеждами богатых, навстречу ветру и волне мы выплываем на фрегатах, а доплываем – на бревне. (Игорь Губерман)	1 : 2 1 : 38 2 : 52 3 : 5 4 : 12	1:20 1:50 3:00 3:40 4:30
14	Всю молодость любил я поезда, поэтому тот час мне неизвестен, когда моя счастливая звезда взошла и не нашла меня на месте. (Игорь Губерман)	1 : 5. 1 : 16 2 : 23 3 : 28 3 : 40	1:15 2:00 2:50 3:35 3:50
15	За что люблю я разгильдяев, блаженных духом, как тюлень, что нет меж ними негодяев и делать пакости им лень.	1 : 4 1 : 23 2 : 00 3 : 15	1:20 1:30 2:50 3:50

	(Игорь Губерман)	4 : 00	4:50
16	Когда сидишь в собраньях шумных, язык пылает и горит; но люди делятся на умных и тех, кто много говорит. (Игорь Губерман)	1 : 6 1 : 38 2 : 9 2 : 25 2 : 50	1:30 1:50 2:20 2:40 3:10

Задание 3.2. Сокрытие информации в контейнере и ее извлечение

3.2.1. В соответствии со своим вариантом зашифровать заданный текст и поместить его в контейнер, в качестве которого используется файл субтитров. Открытый текст указан в таблице 3.2.

Таблица 3.2

№ варианта	Афоризм
1	Коль много накопишь, то много исчезнет.
2	Закон достойных — творить добро и не ссориться.
3	Кто думает, что постиг все, тот ничего не знает.
4	Какое слово скажешь, такое в ответ и услышишь.
5	Нет ничего худшего, чем блуждать в чужих краях.
6	Не выноси приговора, не выслушав обеих сторон.
7	Мудрее всего — время, ибо оно раскрывает все.
8	Сделанное наспех редко бывает хорошо сделано.
9	Никто не становится хорошим человеком случайно.
10	Серьезное разрушается смехом, смех — серьезным.
11	Желание избежать ошибки вовлекает в другую.
12	Жизнь ничего не дарует без тяжких трудов и волнений.
13	Люди охотно верят тому, чему желают верить.
14	Знать истину следует всегда, изрекать — иногда.
15	Поиск истины важнее, чем обладание истиной.
16	Опасность всегда существует для тех, кто ее боится.

3.2.2. Выполнить обратное преобразование, то есть извлечь зашифрованный текст из контейнера и произвести его дешифрацию. Номер контейнера, из которого следует извлекать текст, соответствует номеру варианта.

Задание 3.3. Сокрытие с применением ключа

3.3.1. В соответствии со своим вариантом зашифровать заданный текст при помощи непечатаемых знаков и ключа. В качестве контейнера используется файл субтитров. Открытый текст и ключ указан в таблице 3.3.

Таблица 3.3

№	Афоризм	Ключ
1	Благородство чувств непременно дает благородство манер.	6
2	Борьба есть условие жизни: жизнь умирает, когда оканчивается борьба.	5
3	Воспитание - великое дело: им решается участь человека.	7
4	Наш ум — это металл, извлеченный из формы, а форма — это наши действия.	4
5	Поджечь дом, чтобы поджарить себе яичницу, - в характере эгоиста.	9
6	Только когда мы приходим к цели, мы решаем, что путь был верен.	6
7	То, что мы знаем, - ограниченно, а то, чего мы не знаем, - бесконечно	9
8	Делать то, что доставляет удовольствие, - значит быть свободным.	7
9	Знать много языков - значит иметь много ключей к одному замку.	4
10	История - самый лучший учитель, у которого самые худшие ученики.	8
11	Ценность идеала в том, что он удаляется по мере приближения к нему.	5
12	Мудрость - мыслить с пессимизмом, действовать с оптимизмом.	7
13	Нет ничего опасней для новой истины, как старое заблуждение.	9
14	Когда суть дело обдумана заранее, слова приходят сами собой.	5
15	Мыслитель имеет определенную цель, мечтатель не имеет никакой.	7
16	Тот человек, который не смотрит вверх, неминуемо будет смотреть вниз.	4

3.3.2. Выполнить обратное преобразование, то есть извлечь зашифрованный текст из контейнера и произвести его дешифрацию. Номер контейнера, из которого следует извлекать текст, соответствует номеру варианта, ключ из таблицы 3.3.

Методические указания

Методические указания к пункту 3.1.1.

Файл субтитров представляет из себя текстовый файл записанный по специальным правилам, в зависимости от формата субтитра, определяемых расширением. В этой лабораторной работе рассматриваются SRT-субтитры.

Чтобы создать файл субтитров необходимо выполнить следующие действия.

1. Создать с помощью текстового редактора Блокнот новый документ (в меню Файл->Создать) и сохранить с расширением srt (Файл->Сохранить как, в появившемся меню указать имя файла, при этом расширение сменить с .txt указанное по умолчанию на .srt).

2. Заполнить файл по следующему примеру:

```
1
00:00:22,500 --> 00:00:25,985
Первое сообщение

2
00:00:52,000 --> 00:00:53,100
Второе сообщение
```

Где “1” номер отображаемой строки, 00:00:22,500 – часы : минуты : секунды, миллисекунды начало времени отображения субтитра, 00:00:25,985 – время окончание субтитра, “Первое сообщение” – текст выводимого сообщения на экран. Первый и второй блок форматирования текста обязательно должна разделять пустая строка.

Методические указания к пункту 3.2.1.

Чтобы поместить информацию в контейнер, необходимо выполнить следующие действия.

1. Преобразовать каждый символ открытого текста, включая пробелы и знаки препинания, в десятичное число, используя таблицу CP-1251 (Приложение 1).

Таблица 1

Открытый текст	Десятичное число
Ж	198
И	232
З	231
Н	237
Ь	252
Пробел	032

П	239
Р	240
Е	229
К	234
Р	240
А	224
С	241
Н	237
А	224
!	033

2. Поместить полученные десятичные числа в файл субтитров. Скрываемые данные помещают в младшие разряды меток времени. Например, нужно зашифровать слог “Жи” в текст субтитра:

1
00:00:22,500 --> 00:00:25,335
Первое сообщение

2
00:00:52,000 --> 00:00:53,100
Второе сообщение

3
00:01:06,023 --> 00:02:01,035
Третье сообщение

После замены младших разрядов сообщение принимает вид:

1
00:00:22,50**1** --> 00:00:25,33**9**
Первое сообщение

2
00:00:52,00**8** --> 00:00:53,102
Второе сообщение

3
00:01:06,023 --> 00:02:01,032
Третье сообщение

Методические указания к пункту 3.2.2.

Чтобы извлечь скрытую информацию из контейнера, необходимо выполнить следующие действия.

1. Открыть файл субтитров, содержащий скрытый текст..
2. Выписать значение младших разрядов временных меток, группируя в трёхзначные числа, до тех пор, пока не встретится метка – “777” (метка конца вложения).
3. Определить по таблице CP-1251 (Приложение 1) символы, соответствующие этим десятичным числам.

Таблица 2

Десятичное число	Открытый текст
198	Ж
232	и
231	з
237	н
252	ь
032	пробел
239	п
240	р
229	е
234	к
240	р
224	а
241	с
237	н
224	а
033	!

Из полученных символов составить фразу.

Методические указания к пункту 3.3.1.

Чтобы поместить информацию в контейнер, необходимо выполнить следующие действия.

1. Преобразовать каждый символ открытого текста, включая пробелы и знаки препинания, в десятичное число, используя таблицу CP-1251 (Приложение 1).
2. Преобразовать полученные десятичные числа в двоичные (таблица 1 методических указаний).

Таблица 1

Открытый текст	Десятичное число	Двоичное число
Ж	198	11000110
и	232	11101000
з	231	11100111

н	237	11101101
ь	252	11111100
пробел	32	00100000
п	239	11101111
р	240	11110000
е	229	11100101
к	234	11101010
р	240	11110000
а	224	11100000
с	241	11110001
н	237	11101101
а	224	11100000
!	33	00100001

4. Поместить полученный шифртекст в файл субтитров. Скрываемый текст размещают в конце текста субтитра и отделяется от следующей временной метки пустой строкой, причем вместо единиц записываются пробелы, а вместо нулей – символы табуляции. Каждый символ располагается на отдельной строке. Ключ определяет число титров, в которых не скрывается информация. Отсчёт идет с первого титра. Например ключ 8 говорит о том что текст скрывается после 1, 10, 19 и т.д.

Удобнее сначала ввести данные в документ MS Word, где можно увидеть вводимые символы, используя режим “Непечатаемые знаки” (кнопка “Непечатаемые знаки” находится на Стандартной панели), а уже потом скопировать полученную последовательность символов в Блокнот.

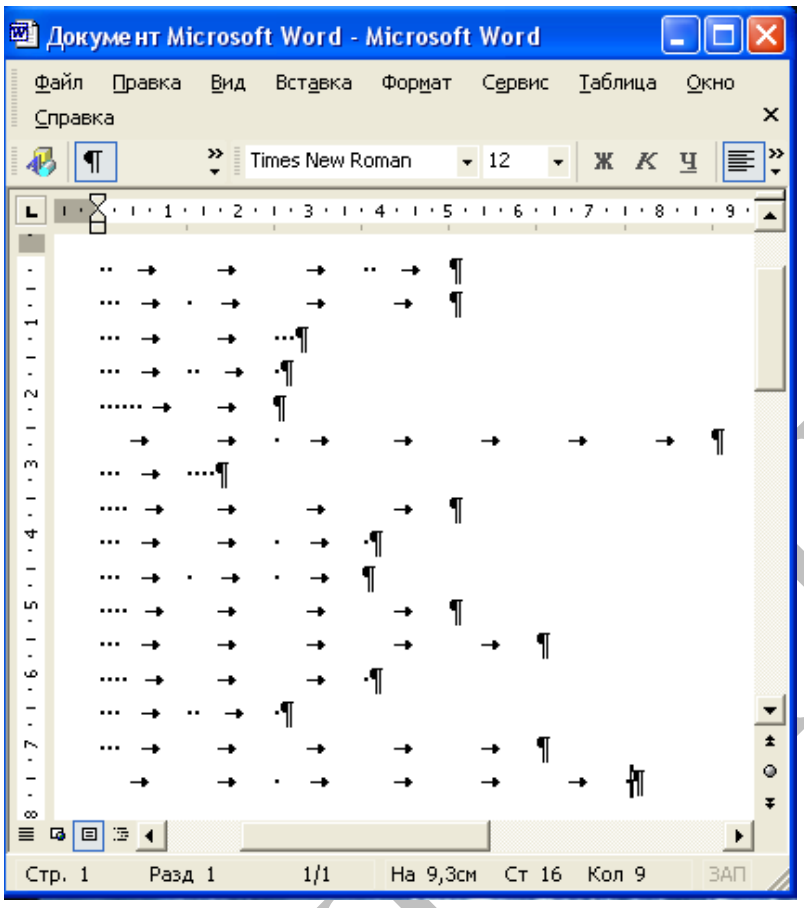


Рисунок 1. Непечатаемые символы.

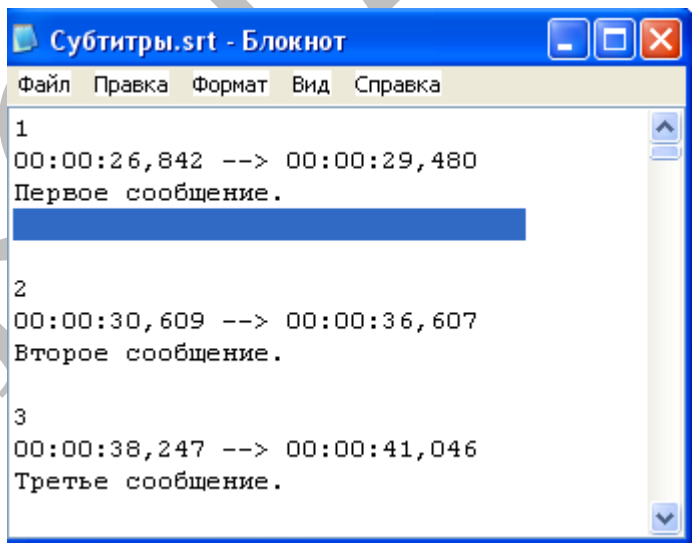


Рисунок 2. Файл субтитров сокрытым текстом

Методические указания к пункту 3.3.2.

Чтобы извлечь скрытую информацию из контейнера, необходимо выполнить следующие действия.

1. Открыть файл субтитров, содержащий текст.
2. Создать документ MS Word, и скопировать в него содержимое строк в соответствии с ключом.
3. Войти в режим “Непечатаемые знаки” (кнопка “Непечатаемые знаки” находится на Стандартной панели). Полученные комбинации пробелов и символов табуляции представляют собой двоичные числа, где пробел эквивалентен единице, а символ табуляции – нулю.
4. Преобразовать двоичные числа в десятичные
5. Определить по таблице CP-1251 (Приложение 1) символы, соответствующие этим десятичным числам.

Таблица 2

Двоичное число	Десятичное число	Открытый текст
11000110	198	Ж
11101000	232	и
11100111	231	з
11101101	237	н
11111100	252	ь

Приложение 1

Таблица CP-1251

пробел	32	**!**	33	**"**	34	**#**	35	**$**	36
%	37	**&**	38	**'**	39	**(**	40	**)**	41
*****	42	**+**	43	**,**	44	**-**	45	**.**	46
/	47	**0**	48	**1**	49	**2**	50	**3**	51
4	52	**5**	53	**6**	54	**7**	55	**8**	56
9	57	**:**	58	**;**	59	**<**	60	**=**	61
>	62	**?**	63	**@**	64	**A**	65	**B**	66
C	67	**D**	68	**E**	69	**F**	70	**G**	71
H	72	**I**	73	**J**	74	**K**	75	**L**	76
M	77	**N**	78	**O**	79	**P**	80	**Q**	81
R	82	**S**	83	**T**	84	**U**	85	**V**	86
W	87	**X**	88	**Y**	89	**Z**	90	**[**	91
****	92	**]**	93	**^**	94	**_**	95	**`**	96
a	97	**b**	98	**C**	99	**d**	100	**e**	101
f	102	**g**	103	**H**	104	**i**	105	**j**	106
k	107	**l**	108	**M**	109	**n**	110	**o**	111
p	112	**q**	113	**R**	114	**s**	115	**t**	116
u	117	**v**	118	**W**	119	**x**	120	**y**	121
z	122	**А**	192	**Б**	193	**В**	194	**Г**	195
Д	196	**Е**	197	**Ж**	198	**З**	199	**И**	200
Й	201	**К**	202	**Л**	203	**М**	204	**Н**	205
О	206	**П**	207	**Р**	208	**С**	209	**Т**	210
У	211	**Ф**	212	**Х**	213	**Ц**	214	**Ч**	215
Ш	216	**Щ**	217	**Ъ**	218	**Ы**	219	**Ь**	220
Э	221	**Ю**	222	**Я**	223	**а**	224	**б**	225
в	226	**г**	227	**д**	228	**е**	229	**ж**	230
з	231	**и**	232	**й**	233	**к**	234	**л**	235
м	236	**н**	237	**о**	238	**п**	239	**р**	240
с	241	**т**	242	**у**	243	**ф**	244	**х**	245
ц	246	**ч**	247	**ш**	248	**щ**	249	**ъ**	250
ы	251	**ь**	252	**э**	253	**ю**	254	**я**	255