Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

ОТЧЁТ

по лабораторной работе №8

По дисциплине «Методы защиты информации»

Выполнил:

Студент гр. 853505

Лазарева Е.В.

Проверил:

Олисейчик В.В.

Минск 2021

**1. Постановка задачи**

Необходимо реализовать программное средство сокрытия текстового сообщения в JPEG изображение на основе метода сокрытия в частотной области изображения*.*

**ЗАДАНИЕ:**

1. Изучить теоретические сведения.
2. Реализовать программное средство, сокрытия (извлечения) текстового сообщения в (из) JPEG изображение(я) на основе метода сокрытия в частотной области изображения.

**2. Теоретическая** **сведения**

**Стеганография**

**Назначение стеганографической защиты**

В отличие от криптографической защиты информации, предназначенной для сокрытия содержания информации, стеганографическая защита предназначена для сокрытия факта наличия (передачи) информации.

Методы и средства, с помощью которых можно скрыть факт наличия информации, изучает **стеганография** (от греч. – тайнопись).

Методы и способы внедрения скрытой информации в электронные объекты относятся к **компьютерной стеганографии** .

**Основные стеганографические понятия**

Основными стеганографическими понятиями являются **сообщение** и **контейнер.**

***Сообщением****m ∈ M* , называют секретную информацию, наличие которой необходимо скрыть, где *M* - множество всех сообщений, обычно *M = Z2n* для *n ∈ Z.*

***Контейнером****b ∈ B* называют несекретную информацию, которую используют для сокрытия сообщений, где *B* - множество всех контейнеров, обычно *B=Z 2q* , при этом *q>>n* .

***Пустой контейнер*** (**контейнер-оригинал** )**-** это контейнер *b* , не содержащий сообщения, **заполненный контейнер** (**контейнер-результат** )*bm* - это контейнер *b* , содержащий сообщение *m* .

***Стеганографическим преобразованием*** принято называть зависимости

*F: M×B×K → B,   F -1 : B×K → M,*

которые сопоставляют тройке (сообщение, пустой контейнер, ключ) контейнер-результат, и паре (заполненный контейнер, ключ) исходное сообщение, т.е.

*F(m,b,k) = bm,k , F-1 (b m,k ) = m, где m ∈ M, b, bm ∈ B, k∈K*

***Стеганографической системой*** называют (*F, F-1 , M, B, K* ) совокупность сообщений, контейнеров и связывающих их преобразований [Мотуз].

**Методы компьютерной стеганографии**

Отметим, что, несмотря на то, что методы тайнописи известны с древних времен, компьютерная стеганография является относительно новой областью науки. В настоящее время компьютерная стеганография находится на стадии развития.

Теоретическая база и методы стеганографии только формируются, нет общепризнанной классификации методов, не существуют критерии оценки надежности методов и механизмов стеганографических систем, производятся первые попытки проводить сравнительные характеристики методов, например, в [Барсуков, 54].

Но уже сегодня специалисты признают, что «... на базе компьютерной стеганографии, являющейся одной из технологий информационной безопасности XXI века, возможна разработка новых, более эффективных нетрадиционных методов обеспечения информационной безопасности» [Барсуков, 54, с. 71].

Анализ применяемых на практике методов компьютерной стеганографии позволяет выделить следующие ***основные классы*** .

1. Методы, основанные на наличии свободных участков в представлении/хранении данных.

2. Методы, основанные на избыточности представления/хранения данных.

3.Методы, основанные на применении специально разработанных форматов представления/хранения данных.

Подчеркнем, что методы внедрения скрытой информации в объекты зависят, прежде всего, от назначения и типа объекта, а также от формата, в котором представлены данные. То есть, для любого формата представления компьютерных данных могут быть предложены собственные стеганографические методы.

Остановимся на стеганографических методах, которые часто применяются на практике.

Широко известен ***метод внедрения скрытой информации в младшие биты данных, представленных в цифровом виде*** . Метод основывается на том факте, что модификация младших, наименее значимых битов данных, представленных в цифровом виде, с точки зрения органов чувств человека не приводит к изменению функциональности и даже качества изображения или звука. Отметим, что информация, скрытая в последних битах цифрового контента не является помехоустойчивой, то есть при искажениях или сжатии с потерей данных она теряется.

На практике используются также ***широкополосные сигналы и элементы теории шума*** . Информация скрывается путем фазовой модуляции информационного сигнала (несущей) с псевдослучайной последовательностью чисел. Используется и другой алгоритм: имеющийся диапазон частот делится на несколько каналов, и передача производится между этими каналами.

Достаточно развиты ***методы, применяемые для тайнописи в текстовых файлах.***

· Скрытые гарнитуры шрифтов. Данный метод основан на внесении малозаметных искажений, несущих смысловую нагрузку, в очертания букв.

· Цветовые эффекты. Например, для символов скрываемого сообщения применяют белый цвет на белом фоне.

· «Нулевой шифр». Этот метод основан на выборе определенных позиций символов (иногда используются известные смещения слов\\предложений\\ абзацев).

· Обобщение акростиха. Метод заключается в том, что по определенному закону генерируется осмысленный текст, скрывающий некоторое сообщение.

· Невидимые коды. Символы скрываемого сообщения кодируются определенным количеством дополнительных пробелов между словами или числом пустых строк.

Разработаны ***методы внедрения скрытой информации и для файлов в форматеHTML:***

· в конец каждой строки добавляют определенное число пробелов, кодирующее скрываемую информацию;

· скрываемое сообщение размещают в специальном файле, у которого удаляют заголовок, причем такой заголовок хранится у получателя (скрываемое сообщение обычно дополнительно шифруется);

· присоединяют дополнительные страницы, на которых и размещают скрываемую информацию;

· записывают скрываемую информацию в мета-тэги (эти команды предназначены для сообщения информации о html-документе поисковым серверам и не видны при отображении страницы на экране);

· записывают скрываемую информацию в тэги с неизвестными программам-браузерам идентификаторами;

· применяют цветовые эффекты.

Особое внимание обратим на ***методы, применяемые для внедрения скрытой информации в исполняемые файлы*** .

Большинство из применяемых методов основано на наличии свободных участков в исполняемых файлах: полностью или частично свободные секторы (блоки) файла; структуры заголовков файлов в форматах EXE, NE-executable и PE-executable содержат зарезервированные поля; существуют пустоты между сегментами исполняемого кода и другие. Заметим, что именно такие методы компьютерной стеганографии традиционно используют авторы компьютерных вирусов для внедрения тел вирусов в исполняемые файлы. Обратим внимание, что для удаления скрытой таким образом информации нарушителю достаточно просто «обнулить» все имеющиеся свободные участки.

**Технологии защиты авторских прав на мультимедийную продукцию**

Среди методов и технологий, использующих стеганографическую защиту информации, наиболее развитыми представляются технологии защиты авторских прав на мультимедийную продукцию.

Предлагаемые на рынке программного обеспечения технологии и системы защиты авторских прав используют методы цифровой стеганографии *.* Системы защиты авторских прав сопровождают идентифицирующей информацией объекты, представляющие собой цифровое содержание: графические файлы, аудио- и видео файлы.

Самой известной технологией в области защиты прав автора на графическую информацию является технология Digital Water Marc (цифровой водяной знак) компании Digimarc Corporation (www.digimarc.com). Специальный программный продукт PictureMarc (ключевая часть технологии) позволяет внедрять в изображение цифровой идентификатор (метку) создателя. Для получения собственного идентификатора пользователь обязан зарегистрироваться в сервисном центре компании Digimarc (MarcCentre). Цифровая метка при внедрении в изображение кодируется величиной яркости пикселей, что определяет стойкость метки при различных трансформациях графического файла (редактирование, уменьшение/увеличение изображения, преобразование в другой формат, сжатие). Более того, цифровая метка, внедренная таким способом, не теряется даже после печати и последующего сканирования. Однако, цифровая метка не может быть ни изменена, ни удалена из маркированного изображения. Считывается цифровая метка с помощью программы ReadMarc. Специальный программный продукт MarcSpider просматривает изображения, доступные через Internet, и сообщает о незаконном использовании.

На рынке программного обеспечения в настоящее время предлагается множество систем и технологий, работающих по принципу, аналогичному цифровому водяному знаку. Все они преобразовывают идентификационный код производителя мультимедиа в невидимую цифровую метку и встраивают ее в объект защиты. Обычно такие системы называют системами цифровых водяных знаков. На рынке представлены технологии PixelTag (производства MIT Media Lab); EIKONAMARK (производства Alpha Tec Ltd.); TigerMark (компании NEC) и многие другие.

Некоторые технологии вместо термина «водяной знак» используют термин «отпечаток пальца». На рынке представлена технология FBI (Fingerprinting Binary Images) производства Signum Technologies (www.generation.net/~pitas/sign.html). Сервисные программы, использующие данную технологию, также позволяют встраивать, определять и читать «отпечаток пальца» из цифровых данных.

Внимания также заслуживают возможности комплексной системы управления электронным копирайтом Cryptolope (компании IBM), основанные на технологии Java.

Применяется на практике и специальный протокол защиты мультимедиа MMP (Multimedia Protection Protocol), разработанный для защиты от пиратства при продаже оцифрованных данных через Internet или другие каналы.

Однако необходимо заметить, что существуют и программы, удаляющие цифровые метки из файлов, содержащих изображения. Наиболее известны две из них: UnZign и StirMark, которые анонсированы в качестве средств тестирования стойкости меток, встраиваемых системами цифровых водяных знаков. Использование этих программ показывает, что на сегодняшний день «водяные знаки всех производителей уничтожаются без заметного ухудшения качества изображения» [Николенко, 56].

В настоящее время приобретают широкое распространение стеганографические продукты, позволяющие маскировать целые файлы в других файлах - файлах-контейнерах. Файлами-контейнерами обычно служат графические или звуковые файлы, иногда используются и текстовые файлы (в формате TXT и HTML). К такому классу программ относятся широко известные программы S-Tools, Steganos, Contraband, Hide4PGP и другие.

Широко известны стеганографические (недокументированные) вставки Easter Eggs (www.eeggs.com) в компьютерных программах. Разработчики программного обеспечения внедряют в свои программы самостоятельные модули, вызываемые определенной (часто довольно сложной) комбинацией клавиш или последовательностью действий. Такие программы, называемые секретами, после активизации демонстрируют различного рода шутки, развлекательную анимацию. Часто программа–секрет демонстрирует список разработчиков программного продукта, а иногда даже их фотографии. Поэтому в некоторых публикациях технологию Easter Eggs относят к технологиям защиты авторских прав на компьютерные программы.

Стеганографические методы защиты авторских прав на компьютерные программы сегодня недостаточно развиты. Так, например, среди 146 инструментальных стеганографических средств, представленных в специальном обзоре

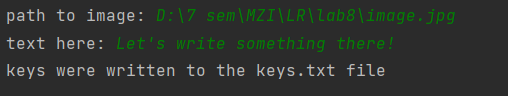
[Steganography and Digital Watermarking Tool Table // www.jjtc.com/Steganography/toolmatrix.htm] средств, основанных на стеганографических методах и технологиях цифровых водяных знаков, анонсировано только одно средство – S–Mail производства Security Software Development (SSD) Ltd., которое встраивает скрытую информацию в EXE- и DLL-файлы.

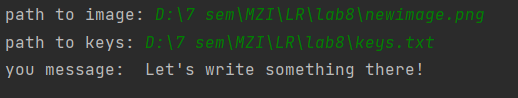
**Резюме**

Анализ тенденций развития технологий, использующихся для обеспечения безопасности информации вообще и, в частности, для защиты авторских прав в области программного обеспечения, показывает, что *применение компьютерной стеганографии наряду с методами, традиционно применяемыми для защиты программных продуктов, увеличивает мощность механизмов защиты* .

Анализ стеганографических методов защиты информации, технологий и стеганографических средств защиты интеллектуальной собственности, представленных на рынке программного обеспечения, а также проблем, связанных с применением данных методов, позволяет сделать следующие выводы.

1. В настоящее время рынок программных средств защиты интеллектуальной собственности только складывается.
2. Несмотря на низкую стойкость цифровых меток, цифровые стеганографические технологии и системы успешно применяются на практике для защиты авторских прав создателей мультимедийной продукции при распространении их продуктов в компьютерных сетях и на цифровых носителях: компакт-дисках, цифровых музыкальных дорожках и видео.
3. В настоящее время среди производителей программного обеспечения только разработчики и издатели мультимедиа обладают средствами, обеспечивающими на том или ином уровне защиту прав авторов.
4. Не все существующие методы компьютерной стеганографии могут быть использованы для защиты авторских прав на компьютерные программы.
5. Наиболее развитые методы и алгоритмы компьютерной стеганографии, относящиеся к цифровой стеганографии, не могут применяться для внедрения скрытой информации, идентифицирующей автора, в исполняемые файлы программ.
6. Стеганографические методы защиты авторских прав на компьютерные программы сегодня недостаточно развиты.
7. **Пример работы программы**





**4. Код программы**

**encrypt.py**

from PIL import Image, ImageDraw  
from random import randint  
  
  
def stega\_encrypt():  
 keys = []  
 img = Image.open(input("path to image: "))  
 draw = ImageDraw.Draw(img)  
 width = img.size[0]  
 height = img.size[1]  
 pix = img.load()  
 f = open('keys.txt','w')  
  
 for elem in ([ord(elem) for elem in input("text here: ")]):  
 key = (randint(1,width-10),randint(1,height-10))  
 g, b = pix[key][1:3]  
 draw.point(key, (elem,g , b))  
 f.write(str(key)+'\n')  
  
 print('keys were written to the keys.txt file')  
 img.save("newimage.png", "PNG")  
 f.close()  
  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 stega\_encrypt()

**decrypt.py**

from PIL import Image  
from re import findall  
  
def stega\_decrypt():  
 a = []  
 keys = []  
 img = Image.open(input("path to image: "))  
 pix = img.load()  
 f = open(input('path to keys: '),'r')  
 y = str([line.strip() for line in f])  
  
 for i in range(len(findall(r'\((\d+)\,',y))):  
 keys.append((int(findall(r'\((\d+)\,',y)[i]),int(findall(r'\,\s(\d+)\)',y)[i])))  
 for key in keys:  
 a.append(pix[tuple(key)][0])  
 return ''.join([chr(elem) for elem in a])  
  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 print("you message: ", stega\_decrypt())

**5. Вывод**

Задача стеганографии в изображениях — встроить информацию в цифровое изображение так, чтобы и сообщение, и сам факт его наличия были скрыты. Полученное изображение с дополнительной скрытой информацией не должно выглядеть аномальным. Это достигается путём внесения изменений, незаметных для человеческого зрения. Многие методы стеганографии используют методики, схожие с методами сжатия изображений.

Цифровые изображения представляют особый интерес в качестве контейнеров для скрытых сообщений, поскольку они имеют большой объём и не вызывают подозрений при публикации в социальных сетях и пересылке по электронной почте. В JPEG изображение размером в 733 килобайта поместились все 272 страницы пьесы Шекспира «Макбет».