Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Лабораторная работа № 8

Стеганография

Выполнил: Нетецкая Ю.В.

Проверил: Олисейчик В.В.

Минск 2021

**Постановка задачи**

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

**Описание использованных алгоритмов**

**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);

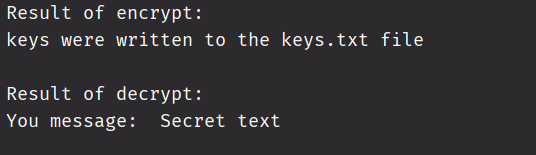
· записывают скрываемую информацию в тэги с неизвестными программам-браузерам идентификаторами;

· применяют цветовые эффекты.

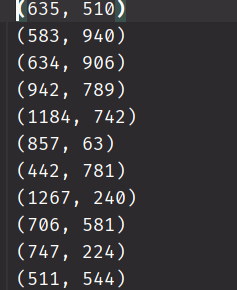
Особое внимание обратим на ***методы, применяемые для внедрения скрытой информации в исполняемые файлы*** .

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.

**Результат работы программы**



Keys



**Код программы**

from PIL import Image, ImageDraw  
from random import randint  
from re import findall  
  
  
def stega\_encrypt(*text\_inp*):  
 keys = [] *# сюда будут помещены ключи* img = Image.open("img.jpg") *# создаём объект изображения* draw = ImageDraw.Draw(img) *# объект рисования* width = img.size[0] *# ширина* height = img.size[1] *# высота* pix = img.load() *# все пиксели тут* f = *open*('keys.txt', 'w') *# текстовый файл для ключей* for elem in ([*ord*(elem) for elem in *text\_inp*]):  
 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()  
  
  
def stega\_decrypt():  
 a = []  
 keys = []  
 img = Image.open('newimage.png')  
 pix = img.load()  
 f = *open*('keys.txt', '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\_\_':  
 text = 'Secret text'  
 *print*('Result of encrypt: ')  
 stega\_encrypt(text)  
 *print*('\nResult of decrypt: ')  
 *print*("You message: ", stega\_decrypt())

**Вывод**

Стеганография, как метод защиты информации, появилась очень давно. Тем не менее данная наука не теряет совей актуальности и сейчас. В развивающемся мире высоких технологий задача сохранения информации обладателя в секрете остается первостепенной, поэтому стеганография тоже не стоит на месте.