Белорусский государственный университет информатики и радиоэлектроники

Кафедра информатики

Лабораторная работа № 7

Стеганографические методы

Выполнила студентка гр. 653502: Сулима М.Ф.

Проверил ассистент КИ: Артемьев В. С.

Минск, 2019

Введение

Стеганография (от греч. στεγανός — скрытый и греч. γράφω — пишу, буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Классификация стеганографических методов защиты информации

- Классическая стеганография
- Компьютерная стеганография
- Цифровая стеганография

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты. Как правило, данные объекты являются мультимедиа-объектами (изображения, видео- или аудио-файлы, текстуры 3D-объектов), внесение изменений в которые вызывает лишь незначительные искажения, находящиеся ниже порога чувствительности среднестатистического человека, что не приводит к заметным изменениям этих объектов.

В рамках лабораторной работы необходимо реализовать программные средства сокрытия текстового сообщения в изображение на основе метода сокрытия частной области изображения.

Блок-схема алгоритма

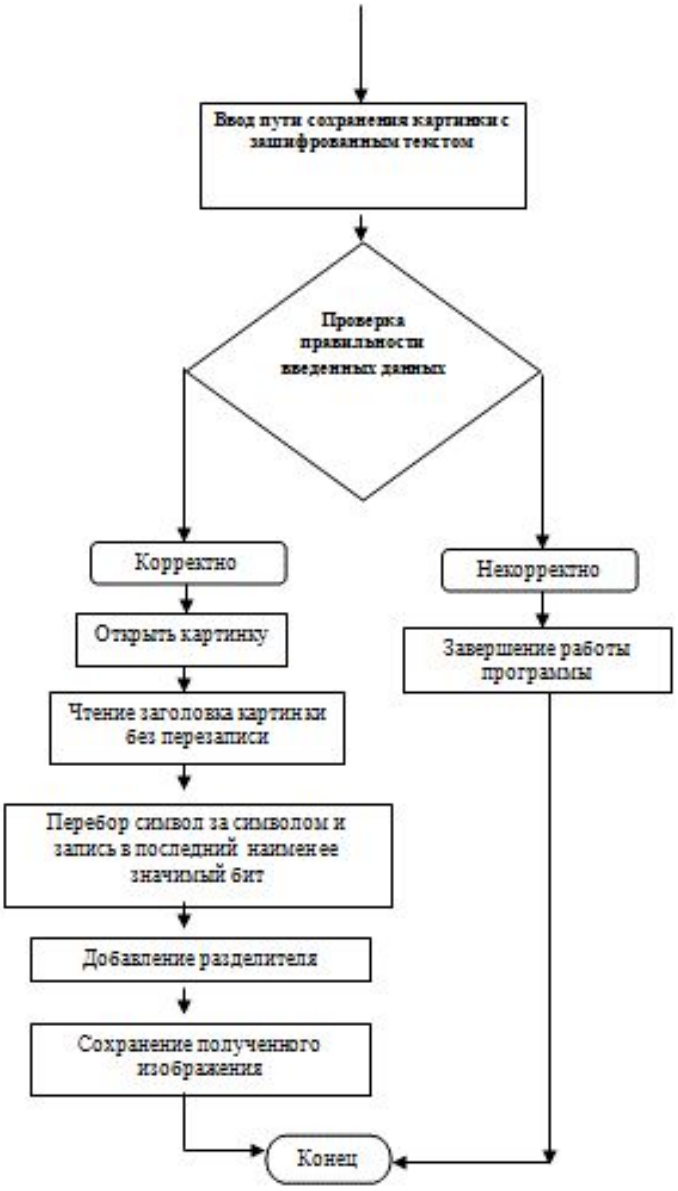

Рис.1. Схема алгоритма

Пример работы программы

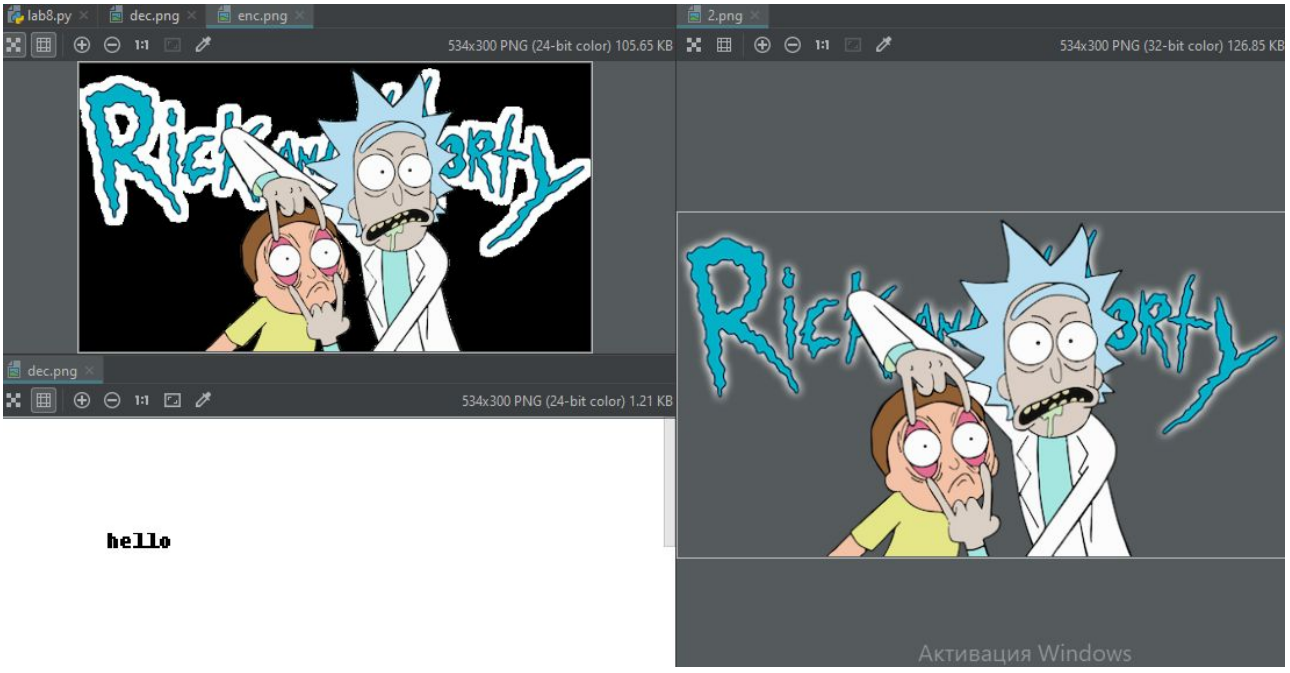

Рис.2. Пример работы

Код программы

```
def encode(text, start_img, enc_img_path):
    red_chanel = start_img.split()[0]
    green_chanel = start_img.split()[1]
    blue_chanel = start_img.split()[2]

    image_text = write_text(text, start_img.size)
    bw_encode = image_text.convert('1')

    enc_img = Image.new("RGB", (start_img.size[0],
start_img.size[1]))
    pixels = enc_img.load()
    for i in range(start_img.size[0]):
        for j in range(start_img.size[1]):
            red_template_pix = bin(red_chanel.getpixel((i,
j)))
            if bin(bw_encode.getpixel((i, j)))[-1] == '1':
                red_template_pix = red_template_pix[:-1] + '1'
            else:
                red_template_pix = red_template_pix[:-1] + '0'
            pixels[i, j] = (int(red_template_pix, 2),
green_chanel.getpixel((i, j)), blue_chanel.getpixel((i, j)))

    enc_img.save(enc_img_path)

def decode(enc_img, img_path):
    red_channel = enc_img.split()[0]

    dec_img = Image.new("RGB", enc_img.size)
    pixels = dec_img.load()
    for i in range(enc_img.size[0]):
        for j in range(enc_img.size[1]):
            if bin(red_channel.getpixel((i, j)))[-1] == '0':
                pixels[i, j] = (255, 255, 255)
            else:
                pixels[i, j] = (0, 0, 0)
    dec_img.save(img_path)
```

Вывод

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление — встраивание цифровых водяных знаков (ЦВЗ) (watermarking), являющееся основой для систем защиты авторских прав и DRM (Digital rights management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам).

В ходе написания лабораторной работы были изучены алгоритмы сокрытия и извлечения текстового сообщения из изображений на основе метода в частотной области изображения, а также написаны их программные реализации.