Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Стеганография

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Дубалеко В.В.

Минск 2020

1. **Теоретические сведения**

Определение 1. Стеганографическая система (stegosystem, стегосистема или стеганосистема – в русскоязычной тематической литературе используются оба сокращения) – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.

При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации. «Скрытость» канала передачи тайной информации отличает стеганографии от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

Определение 2. Абстрактно стеганографическая система обычно определяется, как некоторое множество отображений одного пространства (множества возможных сообщений, М) в другое пространство (множество возможных стеганосообщений, S, и наоборот.

Основные компоненты стеганосистемы:

контейнер, С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается)

тайное сообщение, М; именно контейнер является упомянутым скрытым каналом; тайное сообщение, М, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер [2, 53-56]; здесь речь может идти о невидимых цифровых водяных знаках, ЦВЗ);

ключи или ключевая информация, K системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом осаждения/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий (или третьи) – для предварительного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д. [2, 57, 58];

контейнер с осажденным сообщением или стеганоконтейнер, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

для полноты упомянем также субъектов системы: отправителя и получателя.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы [2, 52, 5964]:

* аудиостеганография,
* видеостеганография,
* графическая стеганография,
* текстовая стеганография и др.

Определение 3. Стеганографической системой ∑ будем называть совокупность сообщений M, контейнеров C, ключей K, стеганосообщений (заполненных контейнеров) S и преобразований (прямого F и обратного F-1), которые их связывают.

При построении стеганосистемы должны, таким образом, учитываться следующие основные положения:

* свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;
* противник (интруз) имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
* если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;
* потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

1. **Практическая часть**

Разработать собственное приложение, в котором должен быть реализован метод НЗБ:

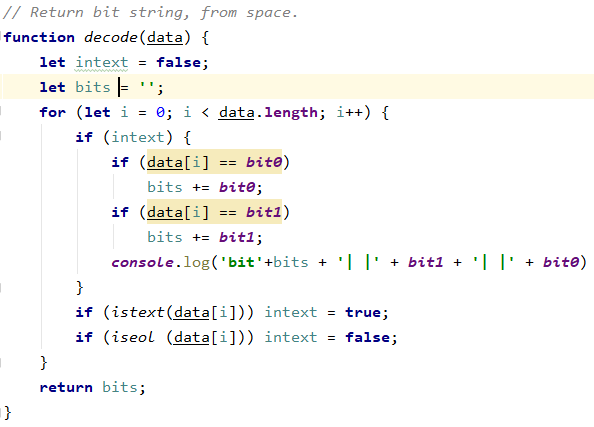
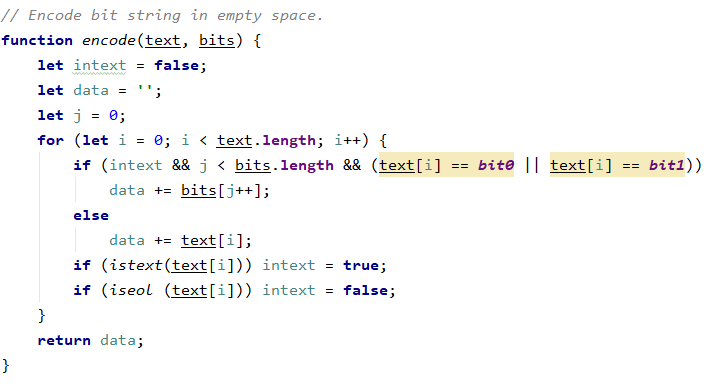


Рисунок 2.1 – Листинг кода для дешифрования

Пример кода для шифрации:



Пример стеганографии нашего кода:

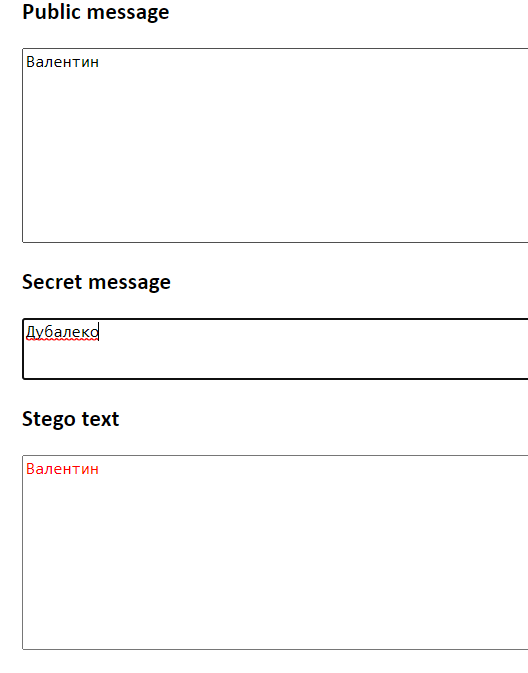


Рисунок 2.2 – Пример стеганосообщения

Рассмотрим на примере изображения с фотографией Стива Джобса:



Рисунок 2.3 – Исследуемое изображение

Применим к этому изображению визуальную атаку, построим новые изображения из отдельных значащих бит соответствующих разрядов:

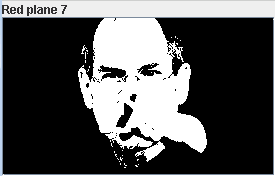
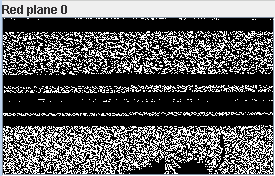
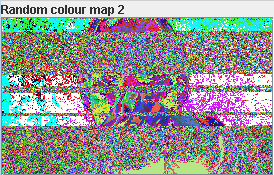
  

Рисунок 2.4 – Исследуемое изображение с визуальными атаками

На втором и третьем изображении заметны области с высокой энтропией (высокой плотностью данных) — это и есть внедренное сообщение.

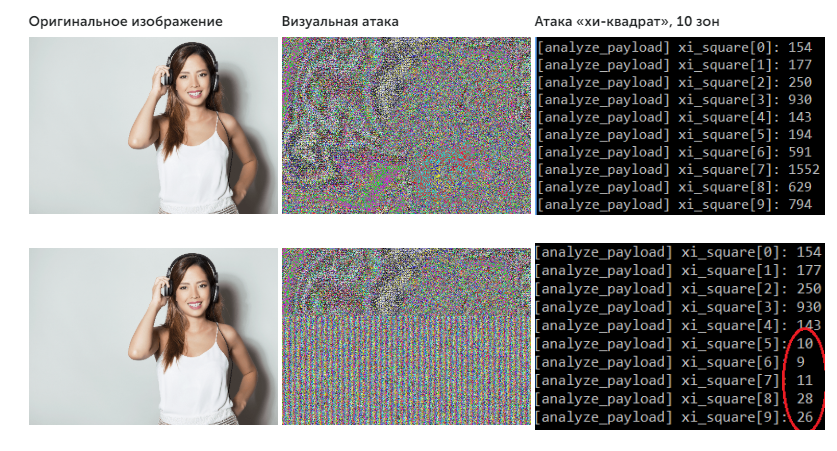


Рисунок 2.5 – Исследуемое изображение с xи-квадратом

Пороговые значения распределения хи-квадрат для p=0,95 и p=0,99 соответственно 101.9705929 и 92.88655838. Таким образом, для зон, у которых рассчитанное значение хи-квадрат меньше порогового, можно принять исходную гипотезу «распределение частот соседних цветов — одинаковое, следовательно, это заполненный стегоконтейнер

**Вывод:** В ходе выполнения лабораторной было получено понимание того, что такое стеганография и было разработано приложение которое реализовывало метод НЗБ.