1. Я написал программу “image\_stegano.py” для встраивания и извлечения, она состоит из 4 функций:

- функция str\_2\_bin(secret\_messsage) получает пареметер в виде открытого текста, преобразует его в двоичную строку.

- функция bin\_2\_str(binary\_message) получает пареметер в виде двоичной строки, преобразует его в открытый текст.

- функция encode(filename\_in, secret\_message, filename\_out) для встраивания сообщения в изображение. Она получает первый пареметер - имя файла исходного изображения, второй параметр - текстовое сообщение, третий параметр - выходное изображение. Она встраивает секретное сообщение во исходное изображение, а затем сохраняет выходное изображение со встроенным сообщением.

- функция decode(filename\_in) для извлечения сообщения в изображении. Она получает 1 параметр - имя файла изображения со встроенным сообщением, возвращает встроенное сообщение в виде открытого текста.

2. Рассмотрим алгоритм программы. Для встраивания и извлечения, я использую 8 первых битов для сохранения длины соощения.

Алгоритм встраивания заменяет наименьший значащий бит каждого канала в каждом пикселе битом данных, когда данный заканчивается, программа запивывает новое выходное изображение.

Алгоритм извлечения читает 8 первых битов данных из изображения для определения длины сообщения, потом продолжает читать каждый бит для определения сообщения.

3. Давайте запустим программу:

Встраиваем одно слово, извлекаю сообщение.

Встраиваем длинный текст, извлекаю сообщение.

4. Сейчас покажу вам значения PSNR:

Рассмотрим формулу для вычисления MSE, понятно, что когда количество символов увеличивается, значение MSE увеличивается.

В формуле для вычисления PSNR, когда MSE увеличивается, PSNR уменьшается.

5. Пока проводим атаку:

Если значение НЗБ канала равно 1 программа устанавливаем значение канала 255, если значение НЗБ канала равно 0 устанавливаем значение канала 1

Запуситим программу для обнаружения.

Рассмотрим выходное изображения.

Это все я могу рассказать, до свидания.