**СОДЕРЖАНИЕ**

[1 Задание на практическую работу 3](#_Toc119240564)

[2 Краткая теоретическая часть 5](#_Toc119240565)

[2.1 Метод LSB 5](#_Toc119240566)

[2.2 Метод PM1 5](#_Toc119240567)

[2.3 Метод QIM 6](#_Toc119240567)

[2.4 Метод PVD 6](#_Toc119240567)

[2.5 Метод NMI 7](#_Toc119240567)

[2.6 Оценка эффективности встраивания 8](#_Toc119240567)

[3 Программная реализация стеганографического метода QIM 11](#_Toc119240568)

[4 Вычислительные эксперименты 14](#_Toc119240569)

[5 Выводы о проделанной работе 19](#_Toc119240570)

[6 Список использованных источников 20](#_Toc119240571)

# 1 Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации стеганографического встраивания информации в пространственную область цифровых изображений.

В рамках практической работы необходимо выполнить следующее:

1. написать программную реализацию одного из следующих стеганографических методов для цифровых изображений по выбору студента: QIM, PVD, NMI;
2. провести вычислительные эксперименты с полученной программной реализацией и сделать выводы об эффективности рассмотренного метода встраивания;
3. подготовить отчет о выполнении работы.

Программа должна обладать следующей функциональностью:

1. при встраивании:

* принимать на вход цветное (RGB) изображение-контейнер;
* принимать на вход сообщение для встраивания;
* рассчитывать показатели качества встраивания;

1. при извлечении:

* принимать на вход цветное стегоизображение;

1. осуществлять встраивание или извлечение информации по выбору пользователя.

Вычислительные эксперименты с полученной программной реализацией должны включать следующее:

1. встраивание максимально возможного для данного контейнера объема информации с оценкой незаметности встраивания;
2. встраивание разного количества информации и сравнение незаметности встраивания;
3. извлечение встроенной информации из стегоизображений в условиях отсутствия постобработки и при наличии различных операций обработки изображений, оценка робастности;
4. сравнение гистограмм изображений до и после встраивания.

# 2 Краткая теоретическая часть

Стеганография – это наука о скрытой передаче и хранении информации таким образом, чтобы сам факт наличия этой информации был тайной для третьих лиц. Цифровая стеганография работает с цифровой информацией. В качестве контейнеров для секретных сообщений могут выступать самые разные цифровые объекты: мультимедиа-данные, исполняемые файлы, интернет-трафик, данные с датчиков «интернета вещей» и т.д.

Одним из наиболее распространенных типов контейнеров для стеганографического встраивания являются цифровые изображения. В первую очередь это связано с их высокой избыточностью: наиболее распространенная цветовая модель RGB содержит различных цветов, поэтому небольшое изменение оттенка отдельных пикселей остается незаметным для глаза человека. Кроме того, цифровые изображения обладают так называемой пространственной избыточностью, которая состоит в том, что соседние пиксели изображения в большинстве случаев похожи друг на друга. Это свойство также широко используется в методах обработки цифровых изображений.

Существует большое количество различных методов встраивания дополнительной информации в цифровые изображения, отличающихся разными особенностями. Все существующие методы делятся на два больших класса: методы пространственного встраивания и методы частотного встраивания. Методы пространственного встраивания напрямую изменяют значения пикселей изображения, в то время как методы частотного встраивания вносят изменения в значения частотных коэффициентов, полученных после применения некоторого частотного преобразования к матрице пикселей.

**2.1 МЕТОД LSB**

Одним из самых простых методов пространственного встраивания является метод замены наименее значимых битов (Least Significant Bits, LSB) [1]. Для встраивания секретное сообщение необходимо преобразовать в двоичную последовательность. Метод LSB предполагает замену одного или нескольких младших битов пикселей битами секретного сообщения при встраивании информации. Чтобы извлечь встроенную информацию, необходимо последовательно обойти пиксели изображения и сформировать последовательность из нужного количества младших битов каждого пикселя.

**2.2 МЕТОД PM1**

Метод «плюс-минус один» (Plus-Minus One, PM1) является модификацией метода LSB. Данный метод меняет младший бит пикселя на бит сообщения посредством случайного уменьшения или увеличения значения пикселя на единицу в следующих случаях:

* если значение пикселя четное, и бит секретного сообщения равен единице;
* если значение пикселя нечетное, и бит секретного сообщения равен нулю.

Соответствующая формула встраивания имеет вид:

где – значение пикселя изображения до встраивания, – значение пикселя после встраивания, – случайное число из множества .

Чтобы извлечь встроенную информацию, необходимо, как и в методе LSB, последовательно обойти пиксели изображения и сформировать последовательность из нужного количества младших битов каждого пикселя.

**2.3 МЕТОД QIM**

Метод модуляции индекса квантования (Quantization Index Modulation, QIM) [3] состоит в изменении значений пикселей изображения в зависимости от значений встраиваемых битов сообщения. Данная операция называется модуляцией. Встраивание бита осуществляется в пиксель контейнера по формуле

где – шаг квантования (четное число), – взятие целой части от деления.

Для извлечения моделируется ситуация встраивания в пиксель нулевого и единичного битов, после чего результирующий бит определяется на основании того, к какому из двух значений ближе имеющееся значение . Формула извлечения одного бита выглядит следующим образом:

.

**2.4 МЕТОД PVD**

В методе разности значений пикселей (Pixel Value Difference, PVD) [4] изображение разбивается на непересекающиеся пары пикселей и для каждой пары считается разность их значений , . Абсолютное значение разности пары пикселей попадает в один из шести отрезков вида . Эти отрезки заданы заранее и обычно определяются следующим образом: , , , , , .

Количество битов сообщения, которое может быть встроено в пару пикселей , определяется по формуле

|  |  |
| --- | --- |
|  |  |

Далее фрагмент сообщения длиной битов представляется в виде целого числа и вычисляется новое значение разности для данной пары пикселей по формуле

|  |  |
| --- | --- |
|  |  |

Встраивание фрагмента сообщения в пару пикселей осуществляется по формуле:

|  |  |
| --- | --- |
|  |  |

Извлечение сообщения выполняется по формуле

**2.5 МЕТОД NMI**

Метод встраивания на основе интерполяции по среднему значению соседей (Neighbor Mean Interpolation, NMI) устроен следующим образом. Исходное изображение разрешением преобразуется в изображение разрешением по схеме, представленной на рисунке 1. Именно изображение выступает в качестве контейнера для встраивания сообщения.

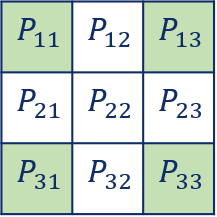
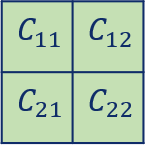


Рисунок 1 – Интерполяция изображения на этапе встраивания

Значения пикселей изображения рассчитываются по следующим формулам:

После этого для каждого из непересекающихся блоков пикселей размером интерполированного изображения вычисляется три разностных значения по следующей формуле:

где – левый верхний пиксель блока.

Фрагмент сообщения длиной битов представляется в виде целого числа и встраивается в пиксель по формуле

Таким образом, в каждый блок пикселей размером может быть встроено три фрагмента сообщения.

Чтобы извлечь сообщение из стегоконтейнера , сначала необходимо восстановить изображение и посредством интерполяции сформировать изображение , как это показано на рисунке 2.

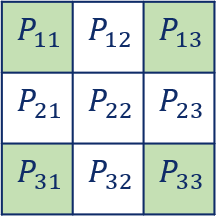
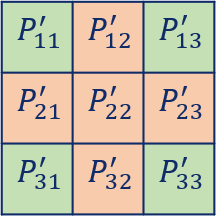
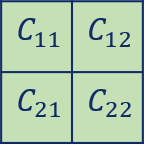


Рисунок 2 – Интерполяция изображения на этапе извлечения

После этого стегоизображение разбивается на блоки размером пикселя и из каждого блока извлекается три фрагмента встроенного сообщения по формуле

**2.6 ОЦЕНКА ЭФФЕКТИВНОСТИ ВСТРАИВАНИЯ**

Для оценки качества стеганографического встраивания информации в изображения используются различные характеристики. Наиболее распространенными из них являются незаметность и емкость встраивания. Незаметность отражает различие между изображениями до и после встраивания и обычно оценивается метриками PSNR, MSE, RMSE, SSIM:

где – значение пикселя изображения-контейнера, – значение пикселя изображения с вложением;

где – среднее значение пикселей изображения-контейнера, – среднее значение пикселей изображения с вложением, – дисперсия пикселей изображения-контейнера, – дисперсия пикселей изображения с вложением, – ковариация между пикселями обоих изображений, и – константы.

Емкость показывает, сколько битов встроенной информации приходится на каждый пиксель изображения, и выражается следующей формулой:

где – размеры изображения, – это общее число битов, встроенных в изображение.

Для оценки устойчивости встраивания к деструктивным воздействиям, таким как изменение яркости, JPEG-сжатие и т.д. обычно применяются метрики BER и NCC:

где – количество ошибок, возникших при извлечении (измененных битов);

где – исходное сообщение, – извлеченное сообщение.

Метрика NCC обычно применяется, когда встроенное сообщение является изображением.

Важным показателем качества стеганографического встраивания является устойчивость перед стегоанализом. Существует множество схем стегоанализа для пространственной области изображений. Простейшие из них анализируют сходство гистограмм изображений до и после встраивания.

# 3 Программная реализация стеганографического метода QIM для цифровых изображений.

Программная реализация метода QIM представлена на рисунках 1, 2 и 3.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 1 - Программная реализация метода QIM. Часть 1

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 2 - Программная реализация метода QIM. Часть 2

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 3 - Программная реализация метода QIM. Часть 3

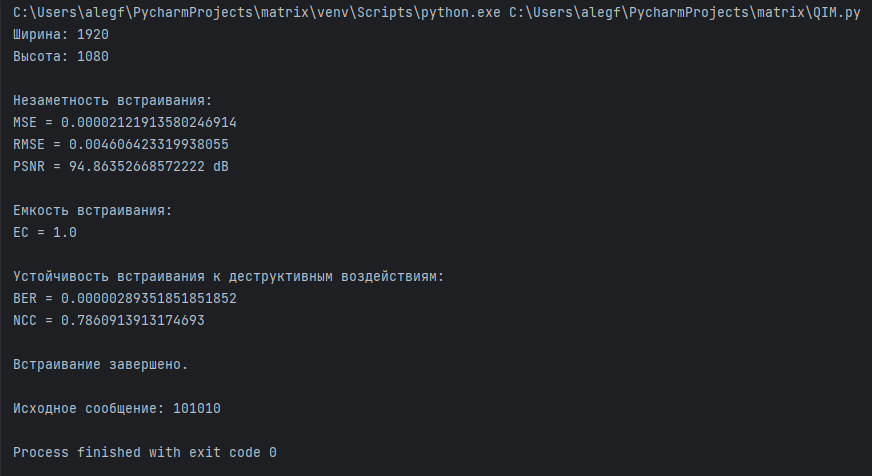


Рисунок 4 – Пример результата выполнения программы

# 4 Вычислительные эксперименты.

4.1 Встраивание максимально возможного для данного контейнера объема информации:

Возьмём для оценки фотографию, представленную на рисунке 5:



Рисунок 5 – Фотография

Ширина этой картинки = 600 пикселей, высота = 800 пикселей. Для начала встраиваем в изображение сообщение состоящее из одной “1”. Для этого используем функцию print(encryption("5.jpg", "1", 4)) из программы, предоставленной в 3 пункте. В данном случае метрики незаметности встраивания имеют значения, продемонстрированные на рисунке 6.

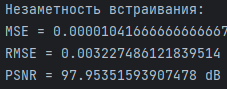


Рисунок 6 – Метрики незаметности встраивания для сообщения из 1 символа

Теперь встраиваем сообщение, состоящие из 480000 символов используя функцию print(encryption("5.jpg", "1" \* 600 \* 800, 4)). Получаем значения незаметности встраивания, предоставленные на рисунке 7.

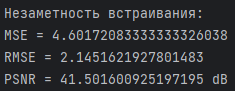


Рисунок 7 – Метрики незаметности встраивания для сообщения из 480000 символов

В первом случае значения MSE и RMSE очень малы, а значение PSNR очень высоко. Это указывает на то, что разница между оригинальным изображением и стегоизображением очень мала, и встраивание информации было выполнено с высокой степенью незаметности.

Во втором случае значения MSE и RMSE выше, а значение PSNR ниже. Это указывает на то, что разница между оригинальным изображением и стегоизображением больше, и встраивание информации было менее незаметным.

Таким образом, сравнивая эти два случая, можно сказать, что в первом случае встраивание информации было более незаметным, чем во втором случае.

4.2 Проверим, как изменяются метрики незаметности встраивания от встраивания разного количества информации в изображении из рисунка 5.

Для этого воспользуемся функцией print из программы, представленной в пункте 3. Получаем значения, продемонстрированные в таблице 1:

Таблица 1 – Изменения метрик незаметности встраивания

|  |  |  |  |
| --- | --- | --- | --- |
| Размер сообщения от макс. возможного значения | Метрика MSE | Метрика RMSE | Метрика PSNR |
| 10 % | 0.45496 | 0.6745 | 51.55098 |
| 25 % | 1.14479 | 1.0699 | 47.54353 |
| 50 % | 2.28488 | 1.5115 | 44.54216 |
| 75 % | 3.43519 | 1.8534 | 42.77128 |
| 100 % | 4.60172 | 2.1451 | 41.50160 |

В итоге получаем зависимость значений метрик незаметности встраивания от размера сообщения. Значит, чем меньше значение MSE и RMSE, тем лучше качество встраивания, и чем ниже значение PSNR, тем ниже качество встраивания.

4.3 Встроим сообщения состоящие из 240 000 единиц в картинку, представленную на рисунке 5. Затем, применяем сжатие с помощью функции, представленной на рисунке 8.



Рисунок 8 – Функция сжатия

Выполнив расшифровку, получаем:

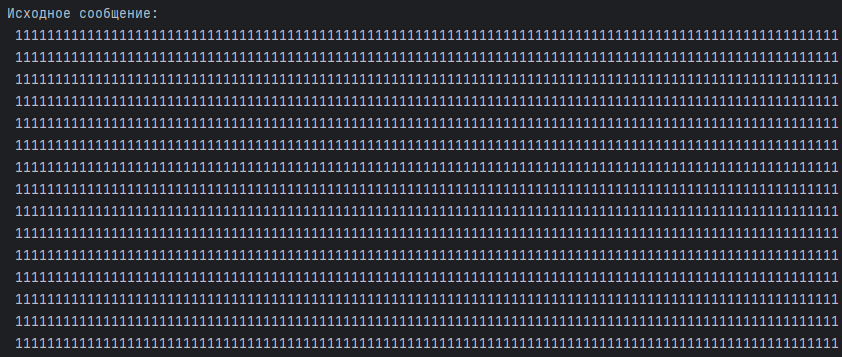


Рисунок 9 – Результат расшифровки

Видим, что в результате сжатия картинки в формате png, исходное изображение осталось тем же, что указывает на высокую робастность метода встраивания.

4.4 Сравнение гистограмм изображений до и после встраивания.

Встроим сообщения состоящие из 240 000 единиц в картинку, представленную на рисунке 5. Для построения гистограмм воспользуемся программой, представленной на рисунке 10.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 10 – Программа для построения гистограмм

Результат работы программы представлен на рисунке 11.

Изображение выглядит как текст, снимок экрана, диаграмма, График

Автоматически созданное описание

Рисунок 11 – Гистограммы

Гистограммы изображений показывают распределение значений пикселей в двух изображениях, где image 1 – это картинка до встраивания, а image 2 – после встраивания. Сравнивая гистограммы двух изображений, можно увидеть, как изменилось распределение значений пикселей. Видим, что гистограмма стала более неровной и появились артефакты. Это указывает на ухудшение качества изображения.

**5 Выводы о проделанной работе**

В ходе выполнения лабораторной работы были рассмотрены различные аспекты сжатия изображений и встраивания информации в них. Были рассмотрены различные метрики, используемые для оценки качества встраивания, такие как MSE, RMSE, PSNR, BER и NCC. Также был получен навык программной реализации стеганографического метода QIM.

# 6 Список использованных источников

Tutorial - Pillow. – URL: https://pillow.readthedocs.io/en/stable/handbook/tutorial.html (дата обращения 29.05.2023).