НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

**ОСНОВЫ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ**

**Практическая работа 4**

**Стеганографическое встраивание информации в пространственную область цифровых изображений**

**Евсютин О.О., Мельман А.С.**

Москва 2023

**1 ЦЕЛЬ РАБОТЫ**

Целью данной работы является приобретение навыков программной реализации стеганографического встраивания информации в цифровые изображения.

**2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

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.

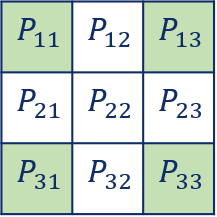
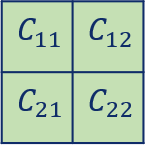


Рисунок 1 – Интерполяция изображения на этапе встраивания

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.

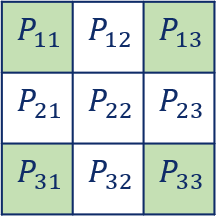
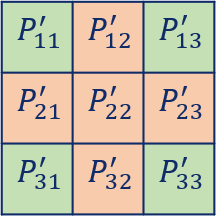
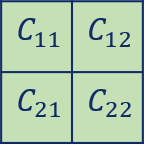


Рисунок 2 – Интерполяция изображения на этапе извлечения

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 ЗАДАНИЕ**

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.

Отчет должен содержать следующие составные части:

1. раздел с заданием;
2. раздел с краткой теоретической частью;
3. раздел с результатами работы программы;
4. раздел с результатами вычислительных экспериментов;
5. раздел с выводами о проделанной работе.

**4 ЛИТЕРАТУРА**

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
2. Fridrich J. Steganography in Digital Media. Principles, Algorithms and Applications / J. Fridrich. – New York: Cambridge University Press, 2010. – 437 p.
3. Mitekin V. A new QIM-based watermarking algorithm robust against multi-image histogram attack / V. Mitekin, V. Fedoseev // Procedia Engineering. – 2017. – Vol. 201. – P. 453-462.
4. Wu D.-C. A steganographic method for images by pixel-value differencing / D.-C. Wu, W.-H. Tsai // Pattern Recognition Letters. – 2003. – Vol. 24, № 9-10. – P. 1613–1626.
5. Jung K.-H. Data hiding method using image interpolation / K.-H. Jung, K.-Y. Yoo // Computer Standards & Interfaces. – 2009. – Vol. 31. – P. 465–470.