

Задание 3. Реализация и сравнительный анализ методов обратимой стеганографии (RDH) на основе сдвига гистограмм.

Тема: Реализация и исследование алгоритмов обратимой стеганографии с сохранением целостности контейнера.

Цель: Исследовать различные подходы к обратимой стеганографии на основе методов сдвига гистограмм, описанных в статье "Histogram Shifting as a Data Hiding Technique: An Overview of Recent Developments".

Задание:

- Изучите приложенную статью, опишите основную часть.
- Используйте те же три набора изображений, что и в предыдущих заданиях.
- Разработайте программу, реализующую один из подходов обратимой стеганографии на основе методов из указанной статьи. Пользователь программы выбирает изображение-контейнер и файл с данными для внедрения. Объем встраиваемых данных должен составлять не менее половины от общей ёмкости контейнера.

Вариант (назначает преподаватель):

1 вариант: Data Hiding Algorithm with Multiple Pairs of Peak and Zero Points (раздел 2.1 статьи).

2 вариант: Data Hiding Scheme Using Predictive Coding and Histogram Shifting (раздел 2.2 статьи).

3 вариант: Data Hiding Based on Histogram Modification of Difference Images (раздел 2.3 статьи).

- Реализуйте полное извлечение скрытых данных с восстановлением исходного контейнера.
- Оцените и сравните качество полученных стегоконтейнеров для каждого набора данных соответственно, используя метрику PSNR.

Исследовательская часть

Для **каждого** из трёх наборов изображений (BOSSbase, медицинский, иной) выполните следующее:

1) Анализ сохранения целостности контейнера:

- Проверьте, что после извлечения данных восстанавливается идентичное исходное изображение.
- Рассчитайте процент успешных восстановлений для 20 изображений каждого типа.
- Определите условия (объём данных, тип изображения, параметры алгоритма), при которых нарушается обратимость внедрения.

2) Сравнительный анализ методов:

- Рассчитайте среднее значение PSNR для каждого метода и типа контейнеров.
- Определите доверительные интервалы (уровень значимости $\alpha = 0.05$) для средних значений PSNR по каждому набору изображений.
- Сравните максимальную достижимую ёмкость для каждого метода.

Отчет по работе должен содержать описание метода, ссылку на разработанное приложение, описание работы приложения, скриншоты результатов, примеры полученных файлов. В отчет необходимо также внести подробные результаты выполнения исследовательской части.

Защита работы: демонстрация работы приложения, результаты, выводы, ответы на контрольные вопросы.

Дополнительное задание:

Реализуйте метод Data Hiding Based on Correlation between Sub-sampled Images (раздел 2.5 статьи). Исследуйте влияние параметров субдискретизации и уровня внедрения на трех наборах изображений:

- Протестируйте различные комбинации $(\Delta u, \Delta v) \in \{(2,2), (3,3), (4,4), (2,3), (3,2)\}$ для каждого типа контейнеров;
- Исследуйте уровни внедрения $L \in \{0,1,2,3\}$, определив экспериментально для каждого случая максимальную ёмкость внедрения и качество PSNR на каждом наборе данных;
- Постройте графики зависимости PSNR от уровня внедрения для каждой комбинации $(\Delta u, \Delta v)$ отдельно для BOSSbase, медицинских и иных изображений;

- Определите оптимальные параметры для каждого типа изображений, обеспечивающие баланс между ёмкостью и качеством;
- Сравните максимальную достижимую ёмкость с методами из основной части.

Контрольные вопросы

1. Как обеспечивается обратимость (полное восстановление контейнера) в методах на основе сдвига гистограмм?
2. Почему методы с предсказательным кодированием могут обеспечивать большую ёмкость внедрения при том же уровне искажений?
3. Какие типы изображений наиболее подходят для каждого из трех методов? Обоснуйте ответ.
4. Как изменяется гистограмма изображения после внедрения данных методом сдвига гистограмм?
5. Какие ограничения по объему внедряемых данных существуют для каждого метода?
6. Как можно повысить устойчивость методов обратной стеганографии к случайным искажениям?
7. Почему при одинаковом объеме внедряемых данных PSNR может значительно различаться для разных методов?
8. Какие практические применения имеют методы обратной стеганографии в современных системах защиты информации?