

LSB-СТЕГАНОГРАФИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ DCT-И DWT-АЛГОРИТМОВ

Методы криптографии и стеганографии направлены на решение проблемы защиты информации [1]. Цель криптографии – сокрытие содержимого сообщения за счет шифрования.

Стеганография – это наука, изучающая такие методы организации передачи секретных сообщений, которые скрывают сам факт передачи информации.

Направления применения стеганографии: конфиденциальный обмен сообщениями; контроль доступа; защита авторских прав, маркировка товаров [1, 2].

К популярным алгоритмам, кроме LSB (Least Significant Bit, младший значащий бит) относятся DWT (Discrete Cosine Transform, дискретное косинусное преобразование) и DCT (Discrete Wavelet Transform, дискретное вейвлет-преобразование) [1–3].

Предметом нашего исследования является LSB. Этапы реализации алгоритма LSB приведены ниже.

Размещение данных:

- считать изображение и текстовое сообщение, которое нужно скрыть;
- преобразовать текстовое сообщение в двоичный код.
- определить младший значащий бит каждого пикселя изображения;
- поочередно заменять младший значащий бит изображения на каждый бит секретного сообщения;
- записать полученное стеганографическое изображение (стеганоконтейнер).

Извлечение данных:

- считать изображение-стеганоконтейнер;
- определить младший бит каждого пикселя стеганографического изображения;
- извлечь биты и преобразовать каждые 8 бит в символ (символическое представление).

Для сравнения алгоритмов были использованы следующие метрики: скрытность осажденного сообщения, стеганографическая стойкость алгоритма, PSNR, MSE.

MSE – среднеквадратическое отклонение между оригинальным и восстановленным изображениями. Чем ниже значение MSE, тем меньше разница между оригинальным и восстановленным изображениями.

PSNR – отношение максимального сигнала к шуму между оригинальным и восстановленным изображениями. Чем выше значение PSNR, тем меньше потерь качества между оригинальным и восстановленным изображениями. Результаты сравнения были занесены в табл. 1.

Таблица 1 – Результат сравнения алгоритмов

Метод	LSB	DCT	DWT
Невидимость	Низкая	Высокая	Высокая
Надежность	Низкая	Средняя	Высокая
PSNR	Средняя	Высокая	Низкая
MSE	Средняя	Низкая	Высокая

Основываясь на полученных данных, был сделан вывод, что, несмотря на то, что алгоритм LSB показывает весьма посредственные результаты по выбранным метрикам, простота реализации и факт того, что он лежит в основе многих других алгоритмов, позволяют ему оставаться одним из наиболее популярных способов размещения скрытой информации в изображениях.

ЛИТЕРАТУРА

1. Урбанович, П.П. Использование особенностей формата XML в методах текстовой стеганографии/ П. П. Урбанович [и др.] // Информационные системы и технологии = Information Systems and Technologies: материалы междунар. науч. конгресса по информатике. В 3 ч. Ч. 1, Респ. Беларусь, Минск, 27–28 окт. 2022 г. / Белорус. гос. ун-т ; редкол.: С. В. Абламейко (гл. ред.) [и др.]. – Минск: БГУ, 2022. – С. 120-126.

2. Chandran S. and Bhattacharyya K. Notice of Removal: Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography, 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, India, 2015, pp. 1-5, doi: 10.1109/EESCO.2015.7253657.

3. A Comparative Study of Image Steganography Techniques [Электронный ресурс]. Режим доступа: <https://www.ijsr.net/archive/v3i4/MDCwNDE0MDI=.pdf>. – Дата доступа: 25.04.2023