

УДК 004.056.53

**ИССЛЕДОВАНИЕ РАЗЛИЧНЫХ МЕТОДОВ КОДИРОВАНИЯ И ШИФРОВАНИЯ  
ПРИ СТЕГАНОГРАФИЧЕСКОМ ВСТРАИВАНИИ LSB**

**Мальков А.А.** (Университет ИТМО)

**Научный руководитель – к.т.н., Волошина Наталия Викторовна**  
(Университет ИТМО)

В данной работе исследуется применение различных методов кодирования и шифрования для стеганографического встраивания LSB

**Введение.** На сегодняшний день стеганография является наряду с криптографией одним из самых популярных и эффективных методов защиты информации. Широкое распространение получили цифровые отпечатки и стеганографические водяные знаки в области авторского права. Стеганография используется и для скрытой передачи информации.

Одним из методов компьютерной стеганографии является метод LSB. При использовании данного метода скрываемая в стеганографический контейнер информация вносится в наименее значимые биты изображения (например формата BMP), при этом для зрителя изображение искажается незначительно.

Существенной задачей применительно к алгоритмам стеганографии является применение кодирования и шифрования встраиваемой информации. Это должно позволить улучшить помехоустойчивость стеганографического канала и повысить уровень защищённости встраиваемой информации с использованием криптографии. Однако применение кодирования и шифрования будет влиять на объем встраивания в контейнер.

Целью данной работы является нахождение наиболее оптимальных методов кодирования и шифрования для стеганографического встраивания LSB в цветное изображение BMP.

**Основная часть.** В данной работе произведено исследование на нескольких наборах данных применения алгоритмов кодирования (кодов Хемминга, Рида-Соломона и других), алгоритмов симметричного и асимметричного шифрования при стеганографическом встраивании LSB в изображение BMP. Были вычислены основные метрики стегако контейнера для определения качества встраивания (MSE, RMSE, PSNR и другие). Наложены импульсные помехи, определена эффективность кодирования различными кодами, произведена оценка объёма встраивания для различных применяемых кодов.

**Выводы.** Результаты работы могут быть использованы при реализации в программном коде защищённого и помехоустойчивого стеганографического канала передачи информации.

Мальков А.А. (автор)

Подпись

Волошина Н.В. (научный руководитель)

Подпись