0.1. *Коноваленко О.В.* Методы стеганографии для сокрытия данных

В условиях роста объемов цифровой информации и повышения требований к её конфиденциальности особую актуальность приобретают методы стеганографии для сокрытия данных [1]. В работе проведён сравнительный анализ существующих методов стеганографии [2], включая классический метод наименее значимого бита (LSB), сокрытие данных в метаданных EXIF и метод наложения. Оценка эффективности выполнена по ключевым метрикам: ёмкости контейнера, пиковому отношению сигнала к шуму (PSNR) и индексу структурного сходства (SSIM) [3].

В работе предложен новый модифицированный LSB-метод, обеспечивающий повышенную стойкость к обнаружению. Основные особенности модификации: использование внутреннего ключа, внедряемого в начальные пиксели контейнера, адаптивное распределение скрываемых данных с переменными пропусками и сдвигами, а также динамическая инверсия битов на основе псевдослучайной последовательности, инициализируемой параметрами изображения. Такой подход значительно усложняет анализ контейнера стандартными стегоаналитическими инструментами.

Для практической реализации и тестирования разработано программное приложение на языке Python с графическим интерфейсом, поддерживающее работу с изображениями, видео и аудиофайлами. Программа позволяет применять как классические, так и предложенный модифицированный методы, а также дополнительно шифровать данные с использованием стандартизированного алгоритма AES.

Экспериментальные исследования показали, что модифицированный метод сохраняет высокие визуальные характеристики стегоизображений (средние значения PSNR > 52 дБ, SSIM > 0.998), при этом обеспечивая значительно более равномерное распределение скрываемых данных. Статистический анализ по критерию χ^2 подтвердил, что для большинства тестовых изображений значение критерия у модифицированного метода оказывается ниже порогового (3.841), что свидетельствует о высокой степени незаметности, в то время как классический LSB легко детектируется. Таким образом, разработанный метод представляет собой эффективное решение для задач, требующих надёжного и незаметного сокрытия информации в мультимедийных контейнерах.

Список литературы

[1] Грибунин В. Г., И.Н. Оков, И.В. Туринцев Цифровая стеганография/ Москва: Солон-Прессо, 2009. 264 с.

[2] Юданов Р. С. Основные методы применения стеганографии в различных областях // Тенденции развития науки и стеганографии. 2024. № 18. С. 158–160.

[3] Hegarty M. T. Steganography, The World of Secret Communications / North Charleston: CreateSpace Independent Publishing Platform, 2018. 88 p.