

СЕКЦИЯ 1
СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ,
ОБРАБОТКА ИНФОРМАЦИИ

DOI: 10.58168/PPSPM2025_10-17

УДК 625.7/.8

ПРИМЕНЕНИЕ И СРАВНЕНИЕ РАЗЛИЧНЫХ БИБЛИОТЕК ДЛЯ
СТЕГАНОГРАФИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

В.И. Анциферова, А.А. Сахаров

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Статья посвящена исследованию стеганографии в цифровых изображениях, а также реализации и сравнению алгоритма LSB-кодирования при помощи различных библиотек на языке программирования Python. На основе полученных данных составлены сравнительные таблицы об исследуемых библиотеках.

Ключевые слова: стеганография, стеганоанализ, LSB-кодирование, наименьший значащий бит.

APPLICATION AND COMPARISON OF VARIOUS LIBRARIES FOR
STEGANOGRAPHY IN DIGITAL IMAGES

V.I. Antsiferova, A.A. Sakharov

Voronezh State University of Forestry and Technologies named after G.F. Morozov

The article is devoted to the study of Steganography in digital images, as well as the implementation and comparison of the LSB-code algorithm using various libraries in the Python programming language. Based on the data obtained, comparative tables about the studied libraries are compiled.

Keywords: steganography, steganoanalysis, LSB-encoding, least significant bit.

Введение

В нынешнюю цифровую эпоху защита информации имеет решающее значение из-за быстрой передачи данных через Интернет. Криптография делает данные нечитаемыми для неавторизованных пользователей, но может привлечь внимание, заставляя данные выглядеть явно зашифрованными [1]. Стеганография, напротив, скрывает существование самой информации. Стеганография — это способ сокрытия секретной информации внутри файлов или изображений [2].

С развитием компьютерных технологий методы стеганографии в цифровых изображениях приобрели особую актуальность. Они применяются в различных сферах — от защиты авторских прав и маркировки контента до обеспечения конфиденциальности в коммуникациях [3, 4, 5]. Однако эти же методы могут использоваться и в злонамеренных целях, например, для скрытой передачи вредоносного кода или организации скрытых каналов утечки информации.

В данной статье будут рассмотрены основные принципы стеганографии в цифровых изображениях на примере популярного метода встраивания данных LSB-кодирования, протестированы и проанализированы наиболее популярные модули для языка программирования Python по данной теме.

LSB-кодирование

Методов для сокрытия секретной информации существует множество и различаются они по разным критериям: типу носителя, области внедрения, устойчивости к обнаружению и преобразованиям. LSB-кодирование (Least Significant Bit — "наименьший значащий бит") — это один из самых простых и распространенных методов стеганографического встраивания информации в цифровые изображения [6]. Его суть состоит в том, что биты секретного сообщения встраиваются в младшие (крайние правые) значащие биты пикселей изображения.

Данный метод считается наиболее популярным для стеганографии в цифровых изображениях ввиду своей простоте, эффективности и возможности использования в комбинации с другими методами стеганографии.

Рассматриваемые данные

Для данной работы были подготовлены данные: одна тысяча черно-белых изображений в разрешении 256x256 точек (рисунок 1) и перекодированы в формат JPG для решения одной проблемы, о которой будет сказано позже.



Рисунок 1 – Пример подготовленных данных

Используемые библиотеки

Первой библиотекой будет StegoPy — это инструмент для стеганографии на Python, реализующий метод LSB-кодирования.

Из положительных особенностей модуля можно отметить:

- простоту использования (вызов функции производится из терминала в одну строку);
- возможность шифрования для увеличения надежности сокрытия информации;
- возможность настраивать баланс - количество младших битов, задействованных в стеганографии в диапазоне от 1 до 4.

Но принцип использования накладывает серьезное ограничение: обработка изображения помещает результат с фиксированным именем «out.png» в директорию проекта, что в последствии будет мешать распараллеливанию процесса и серьезно ударит по производительности. Так же стоит отметить невозможность работы с изображениями в формате PNG из-за чего было принято решение сконвертировать все изображения в формат JPG. Еще одним минусом является то, что функционал библиотеки ограничен одним лишь методом LSB.

Следующим объектом исследования стал модуль Stegano. Из отличительных особенностей библиотеки можно выделить:

- множество поддерживаемых методов стеганографии;
- простота интеграции в python-проекты;
- быстрая скорость обработки.

Последней рассматриваемой библиотекой будет Pillow. Pillow — это современная и удобная библиотека для работы с изображениями в Python, являющаяся форком старой библиотеки PIL (Python Imaging Library). Она предоставляет широкие возможности для редактирования, сохранения и анализа изображений в различных форматах. При том, что Pillow не разрабатывалась как библиотека для стеганографии, богатый функционал библиотеки предоставляет возможность для этого.

Pillow поддерживает множество операций с изображениями, включая:

- Открытие и сохранение в форматах: JPEG, PNG, BMP, GIF, TIFF, WebP и др.;
- Изменение размеров (resize, thumbnail, crop);
- Наложение фильтров (размытие, контрастность, цветокоррекция);
- Рисование (линии, фигуры, текст);
- Работа с метаданными (EXIF, IPTC);
- Преобразование цветовых моделей (RGB, HSV, Grayscale).

Сравнение результатов

Для задачи LSB-стеганографии важны три основные метрики качества изображений: PSNR, MSE и SSIM.

PSNR (Peak Signal-to-Noise Ratio – «пиковое отношение сигнал/шум») — метрика, оценивающая уровень искажений между оригинальным и изменённым изображением, выражая отношение максимальной мощности сигнала к мощности шума (искажений). Чем выше PSNR, тем меньше искажений и выше качество изображения. В контексте LSB-стеганографии значения около 45 дБ и выше означают, что изменения в изображении практически незаметны для глаза.

MSE (Mean Squared Error – «среднеквадратичная ошибка») - среднее значение квадратов разностей пикселей между оригиналом и стего-изображением.

SSIM (Structural Similarity Index – «индекс структурного сходства») — метрика, оценивающая сходство между двумя изображениями с учётом яркости, контраста и структуры, моделируя восприятие человека. SSIM варьируется в диапазоне от -1 до 1, где 1 означает совершенное совпадение изображений.

Численные метрики проведенного LSB кодирования представлены в сравнительной таблице 1.

Таблица 1 – Результаты измерения численных метрик LSB-кодирования.

Метрика	Pillow	Stegano	StegoPy
PSNR, дБ	46.96	46.96	46.74
MSE, пикселей	1.55	1.55	1.61
SSIM	0.9962	0.9962	0.9960
Время кодирования 1000 изображений, сек	26.56	21.63	301,52

Таблица сравнения модулей по характеристикам и опыту использования представлена ниже (таблица 2).

Таблица 2 – Сравнение характеристик и опыт использования.

Характеристика	Pillow	Stegano	StegoPy
Поддержка форматов	Все	PNG, BMP, JPEG (EXIF)	JPG, BMP
Поддержка шифрования	Нет	Нет	Да (DES)
Методы стеганографии	Только LSB	LSB + EXIF + генераторы	Только LSB
Уровень контроля	Высокий (низкоуровневый подход)	Средний	Низкий
Простота кода	Средняя	Высокая	Очень высокая

Таким образом, можно сделать вывод об использовании того или иного модуля для LSB-кодирования засекреченных сообщений: если нужен полный контроль над процессом, подойдет низкоуровневая и быстрая библиотека Pillow: если превалирует быстрота и легкость написания кода, то Stegano; если в проекте важно шифрование, то StegoPy.

Выводы

Стеганография изображений представляет собой надежное средство встраивания конфиденциальной информации в цифровые изображения для облегчения безопасной связи. В этом проекте успешно реализована технология кодирования и декодирования на основе наименее значимого бита (LSB) на языке программирования Python. Выбранный метод эффективно демонстрирует, как цифровые изображения могут служить незаметными носителями скрытых сообщений, не вызывая подозрений и не ставя под угрозу качество изображения.

Список литературы

1. Солодуха Р.А. Концепция формирования системы противодействия стеганографическим каналам в компьютерных сетях органов внутренних дел // Вестник Воронежского института МВД России, 2021. – №1. – С. 131-142.
2. Солодуха Р.А., Атласов И.В., Кубасов И.А. Стеганоанализ цифровых изображений: технологии, алгоритмы, программная реализация. Воронеж: Воронежский институт МВД России, 2022. – 177 с.
3. Бегларян М.Е., Возняк Г.Н. Судебная компьютерно-техническая экспертиза. Москва : ЮНИТИ-ДАНА, 2015. – 72 с.
4. Солодуха Р.А., Атласов И.В., Кубасов И.А. Оценка достоверности результатов стеганоанализа серии изображений // Вестник Воронежского института МВД России, 2018. – №1. – С. 51-65.
5. Атласов И.В., Солодуха Р.А. Стеганоанализ цифровых изображений: автоматизация, оптимизация, достоверность: монография. Электр. дан. и прогр. Воронеж: Воронежский институт МВД России, 2020. – 171 с.
6. Солодуха, Р. А. Формирование текстурных параметров изображения на основе гауссовских марковских случайных полей как предварительный этап стеганоанализа // Охрана, безопасность, связь. – 2021. – № 6-2. – С. 278-284.
7. Солодуха, Р. А. Формирование текстурных параметров изображения на основе вычисления фрактальной размерности // Охрана, безопасность, связь. – 2022. – № 7-2. – С. 276-280.
8. Свидетельство о государственной регистрации программы для ЭВМ № 2022682838 Российская Федерация. Автоматизация стеганографических приложений: № 2022682094 : 28.11.2022 / Р. А. Солодуха.
9. Feature Extractors for Steganalysis [Электронный ресурс]. Режим доступа: http://dde.binghamton.edu/download/feature_extractors/ (дата обращения: 10.06.2023)

10. L. Fillatre, Adaptive steganalysis of Least Significant Bit replacement in grayscale natural images // IEEE Transactions on Signal Processing, 2012. – vol. 60. – issue 2. – pp. 556-569.
11. Dumitrescu S., Wu X., Memon D. On steganalysis of random LSB embedding in continuous-tone images // Proceedings of ICIP. 2002. pp.641-644.
12. Солодуха Р.А. Статистический стегоанализ фотореалистичных изображений с использованием градиентных путей // Вопросы кибербезопасности, 2022. – №1. – С. 26-36.
13. Liu Q. Steganalysis of DCT–embedding based adaptive steganography and YASS / Proceedings of the 13th ACM Multimedia & Security Workshop, 2011. – pp. 77-86.
14. Оксюта, О.В. Модель системы планирования и оперативного управления экономическим объектом / О.В. Оксюта, А.Л. Курина // Моделирование систем и процессов. – 2017. – Т. 10, № 1. – С. 60-64.
15. Сазонова, С.А. Решение задачи статического оценивания систем газоснабжения / С.А. Сазонова // Вестник Воронежского государственного технического университета. – 2011. – Т. 7, № 11-1. – С. 139-141.
16. Анализ методов оценки поставщиков товаров, использующих транспортные логистические компании / В.В. Лавлинский, С.И. Лыков, А.И. Лыков, В.Ю. Обоимова // Моделирование систем и процессов. – 2017. – Т. 10, № 4. – С. 43-49.

References

1. Solodukha R.A. Concept of formation of the system of counteraction to steganographic channels in computer networks of internal affairs bodies // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia, 2021. - No. 1. - P. 131-142.
2. Solodukha R.A., Atlasov I.V., Kubasov I.A. Steganalysis of digital images: technologies, algorithms, software implementation. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 2022. - 177 p.
3. Beglaryan M.E., Voznyak G.N. Forensic computer-technical examination. Moscow: UNITY-DANA, 2015. - 72 p.
4. Solodukha R.A., Atlasov I.V., Kubasov I.A. Assessing the reliability of the results of steganalysis of a series of images // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia, 2018. - No. 1. - P. 51-65.

5. Atlasov I.V., Solodukha R.A. Steganalysis of digital images: automation, optimization, reliability: monograph. Elektr. dan. i progr. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 2020. - 171 p.
6. Solodukha, R.A. Formation of texture parameters of an image based on Gaussian Markov random fields as a preliminary stage of steganalysis // Security, safety, communications. - 2021. - No. 6-2. - P. 278-284.
7. Solodukha, R.A. Formation of texture parameters of an image based on the calculation of the fractal dimension // Security, safety, communications. – 2022. – No. 7-2. – P. 276-280.
8. Certificate of state registration of computer program No. 2022682838 Russian Federation. Automation of steganographic applications: No. 2022682094: 28.11.2022 / R. A. Solodukha.
9. Feature Extractors for Steganalysis [Electronic resource]. Access mode: http://dde.binghamton.edu/download/feature_extractors/ (date of access: 10.06.2023)
10. L. Fillatre, Adaptive steganalysis of Least Significant Bit replacement in grayscale natural images // IEEE Transactions on Signal Processing, 2012. – vol. 60. – issue 2. – pp. 556-569.
11. Dumitrescu S., Wu X., Memon D. On steganalysis of random LSB embedding in continuous-tone images // Proceedings of ICIP. 2002. pp.641-644.
12. Solodukha R.A. Statistical steganalysis of photorealistic images using gradient paths // Cybersecurity Issues, 2022. - No. 1. - P. 26-36.
13. Liu Q. Steganalysis of DCT-embedding based adaptive steganography and YASS / Proceedings of the 13th ACM Multimedia & Security Workshop, 2011. - pp. 77-86.
14. Oksyuta, O.V. Model of the planning and operational management system of an economic entity / O.V. Oksyuta, A.L. Kurina // Modeling of systems and processes. – 2017. – Vol. 10, No. 1. – P. 60-64.
15. Sazonova, S.A. Solution of the problem of static assessment of gas supply systems / S.A. Sazonova // Bulletin of the Voronezh State Technical University. – 2011. – Vol. 7, No. 11-1. – P. 139-141.
16. Analysis of methods for assessing suppliers of goods using transport logistics companies / V.V. Lavlinsky, S.I. Lykov, A.I. Lykov, V.Yu. Obimova // Modeling of systems and processes. – 2017. – Vol. 10, No. 4. – P. 43-49.