Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №13**

по дисциплине Информационная безопасность

Тема: Исследование стеганографического метода на основе преобразования наименее значащих битов

           Студент: Корнелюк. В. В.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Лабораторная работа №13**

**Цель:** изучение стеганографического метода встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих битов (НЗБ), приобретение практических навыков программной реализации данного метода.

**Задачи:**

1. Закрепить теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии.

2. Изучить алгоритм встраивания/извлечения тайной информации на основе метода НЗБ (LSB – Least Significant Bit), получить опыт практической реализации метода.

3. Разработать приложение для реализации алгоритма встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.

4. Познакомиться с методиками оценки стеганографической стойкости метода НЗБ.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

# Теоретические сведения

Стеганографическая система (stegosystem, стегосистема или стеганосистема – в русскоязычной тематической литературе используются оба сокращения) – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.

Абстрактно стеганографическая система обычно определяется как некоторое множество отображений одного пространства (множества возможных сообщений М) в другое пространство (множество возможных стеганосообщений S), и наоборот.

Основные компоненты стеганосистемы:

• контейнер С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение М; именно контейнер является упомянутым скрытым каналом;

• тайное сообщение М, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер; здесь речь может идти о невидимых цифровых водяных знаках (ЦВЗ));

• ключи, или ключевая информация, K системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом встраивания/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий – для предварительного (перед встраиванием) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;

• контейнер со встроенным сообщением, или стеганоконтейнер, S, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

• для полноты упомянем также субъектов системы: отправителя и получателя.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

• аудиостеганография;

• видеостеганография;

• графическая стеганография;

• текстовая стеганография;

• и др.

Стеганографической системой ∑ будем называть совокупность сообщений M, контейнеров C, ключей K, стеганосообщений (заполненных контейнеров) S и преобразований (прямого F и обратного F–1), которые их связывают:

∑ = (M, C, K, S, F, F–1).

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука.

# Ход работы

Было необходимо разработать приложение, реализующее метод НЗБ.

Функция embedMessage принимает на вход оригинальный текст, ссылку на оригинальный контейнер, ссылку на выходой контейнер со встроенным сообщением, а также метод встраивания. Код функции представлен на рисунке 2.1.



Рисунок 2.1 – Функция встраивания сообщения

Функция extractMessage принимает на вход ссылку на контейнер со встроенным сообщением, метод встраивания и извлекает его из контейнера. Код функции представлен на рисунке 2.2.



Рисунок 2.2 – Функция извлечения сообщения

Результат работы приложения с исходным текстом «Korenliuk Valentine Vladimirovich» и внедрением по строкам представлен на рисунке 2.3.

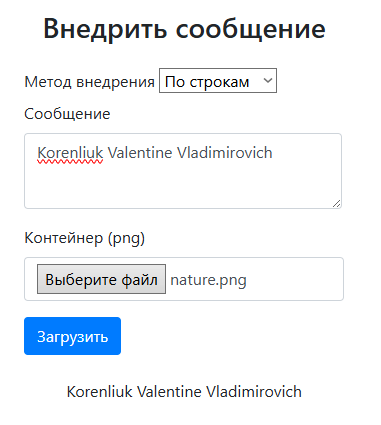


Рисунок 2.3 – Результат работы приложения

Исходный контейнер nature.png представлен на рисунке 2.4.



Рисунок 2.4 – Исходный контейнер

Контейнер со встроенным сообщением представлен на рисунке 2.5.



Рисунок 2.5 – Контейнер со встроенным сообщением

Визуально эти два контейнера ничем не отличаются. Для обнаружения следов осаждения сообщения необходимо сформировать цветовые матрицы.

Цветовая матрица исходного контейнера представлена на рисунке 2.6.



Рисунок 2.6 – Цветовая матрица исходного контейнера

Цветовая матрица контейнера с внедренным сообщением представлена на рисунке 2.7.



Рисунок 2.7 – Цветовая матрица контейнера с внедренным сообщением

В левом верхнем углу можно заметить различия. Различия представлены на рисунке 2.8. Сверху указан исходный контейнер, снизу – контейнер с внедренным сообщением.





Рисунок 2.8 – Следы осаждения сообщения на цветовой матрице при записи по строкам

Результат работы приложения исходным текстом которого является текстовая часть отчета по лабораторной работе №12 и внедрением по столбцам представлен на рисунке 2.9.

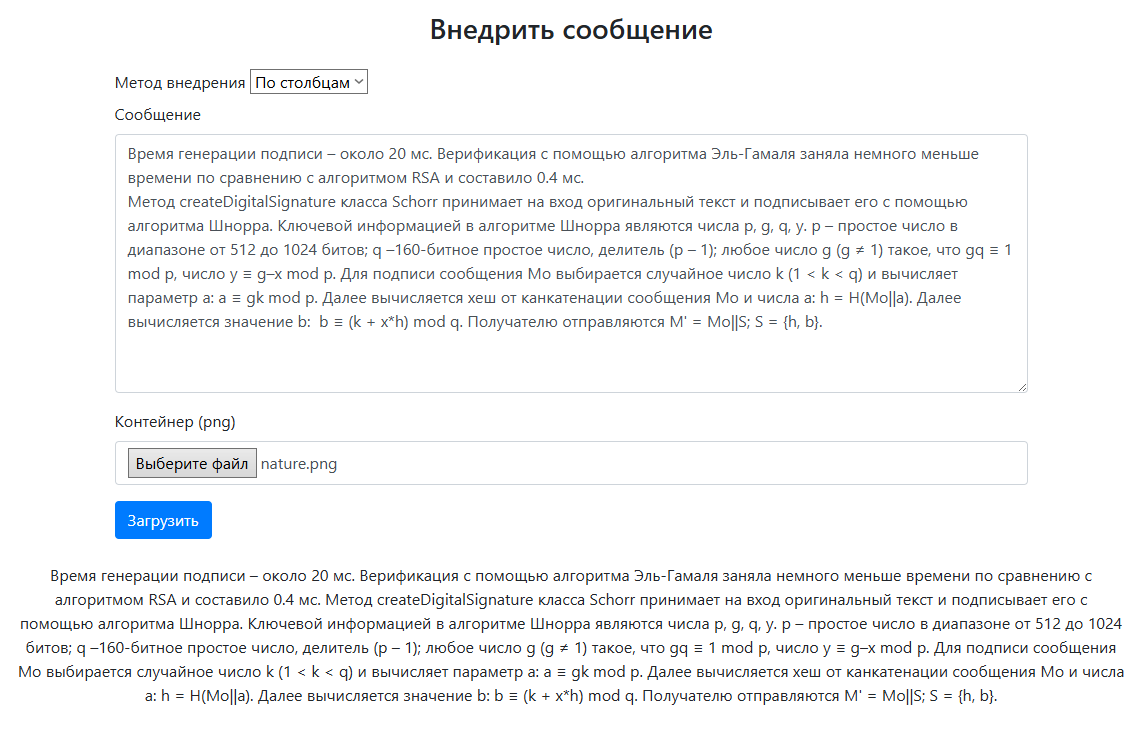


Рисунок 2.9 – Результат работы приложения

Различия в цветовых матрицах контейнеров при встраивании по столбцам представлены на рисунке 2.10. Слева указан исходный контейнер, справа – контейнер с внедренным сообщением.



Рисунок 2.10 – Следы осаждения сообщения на цветовой матрице при записи по столбцам

Проведенный визуальный анализ показывает, что в большинстве случаев визуальных искажений в обработанных изображениях не наблюдается, что подтверждает эффективность стеганографического метода на основе преобразования наименее значащих битов. Также было выявлено, что метод внедрения сообщения по строкам или по столбцам не оказывает существенного влияния на визуальные характеристики конечного изображения.

**Вывод**: в ходе выполнения лабораторной работы были изучены стеганографические методы встраивания/извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих битов (НЗБ). Также было создано приложение, реализующее метод НЗБ с возможностью выбора порядка обхода изображения, а также генерации цветовых матриц для анализа внедрённой информации.