МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №13**

**«ИССЛЕДОВАНИЕ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ»**

Выполнил:

Cтудент 3 курса 3 группы

Шедько Е. А.

Проверил:

Преподаватель-стажер

Копыток Д.В.

Минск 2022

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

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. Результатывыполнения лабораторной работыоформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

6. Закрепить теоретические знания из области текстовой стеганографии, классификации, моделирования стеганосистем подобного вида и сущности основных методов.

7. Изучить основные алгоритмы встраивания/извлечения тайной информации на основе методов текстовой стеганографии, получить опыт практической реализации методов.

8. Разработать приложение для реализации алгоритмов встраивания/извлечения тайной информации на основе методов текстовой стеганографии.

9. Познакомиться с методиками оценки стеганографической стойкости методов.

Выполнение работы:

Программная реализация выполнена на языке C# с использованием консольного приложения и формы.

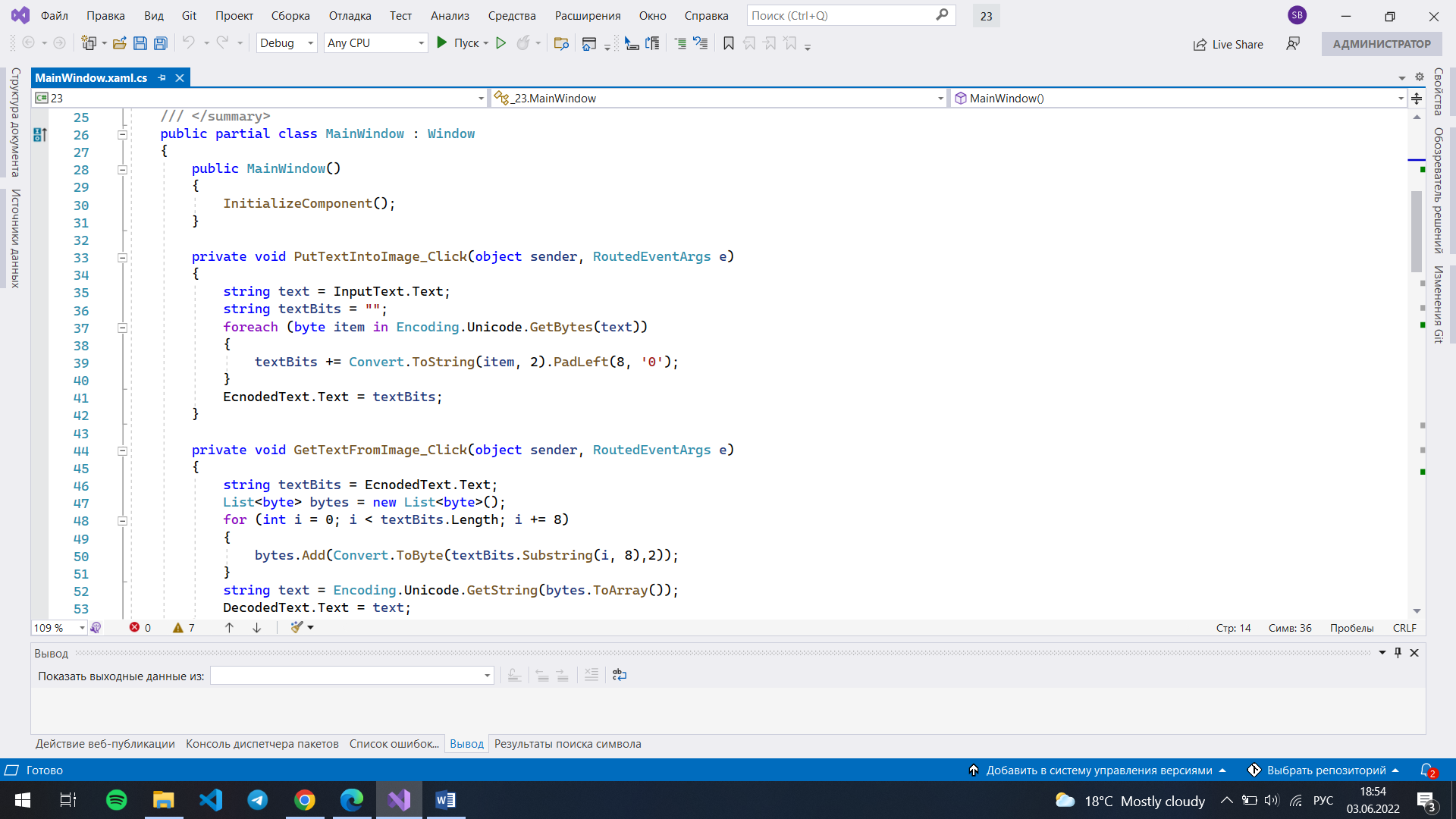


Рисунок 1 – Пример кода

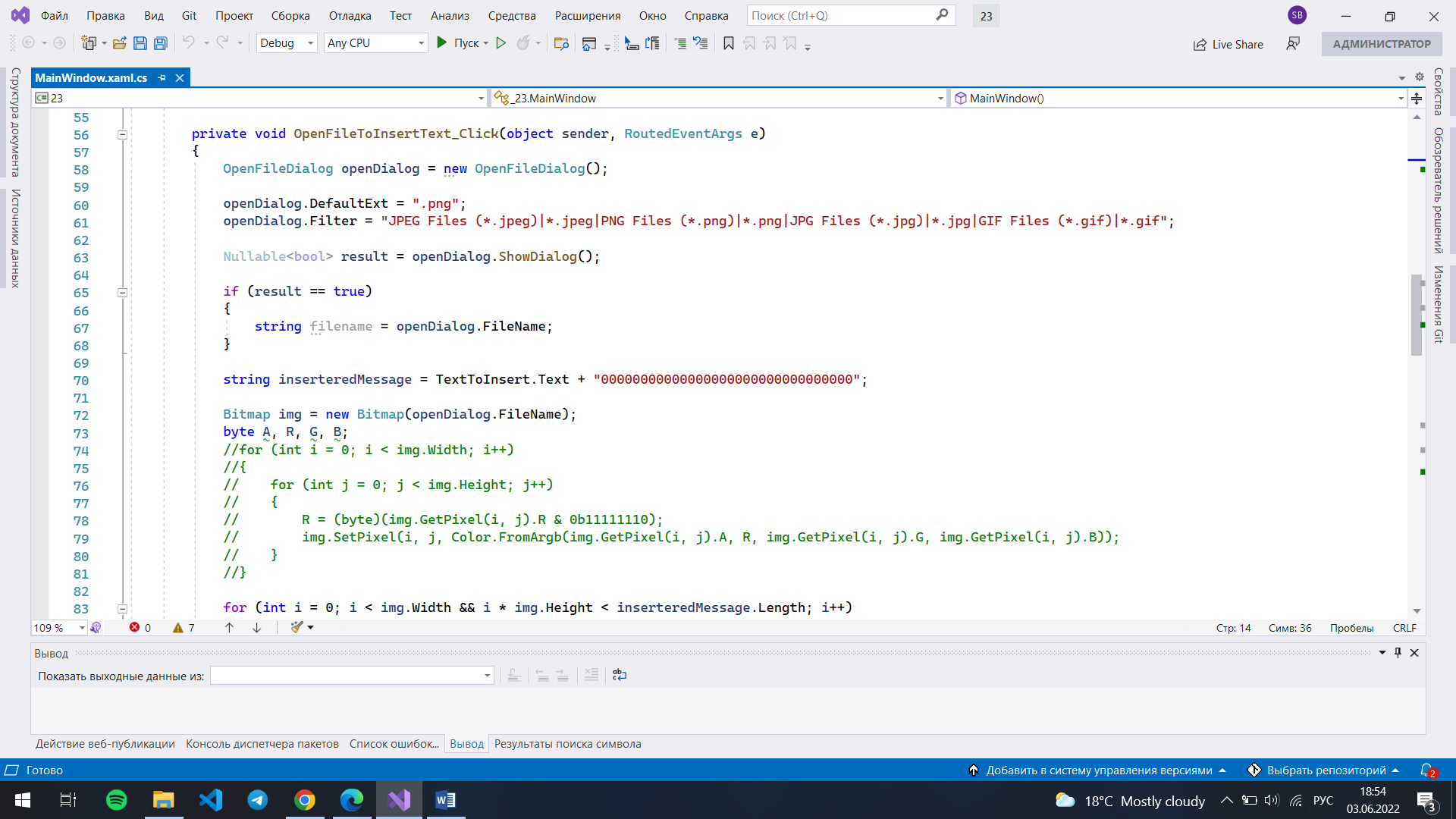


Рисунок 2 – Пример кода

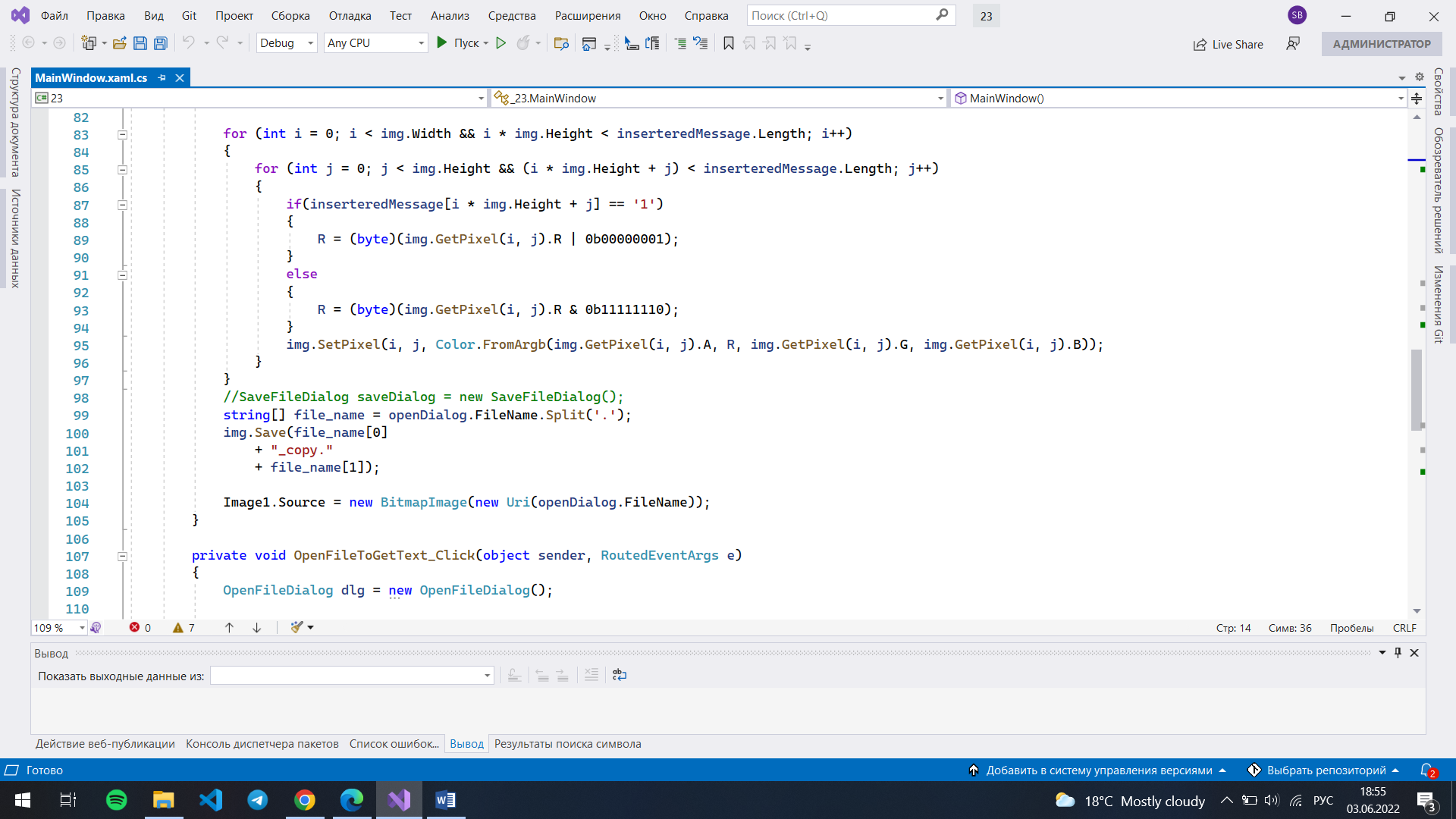
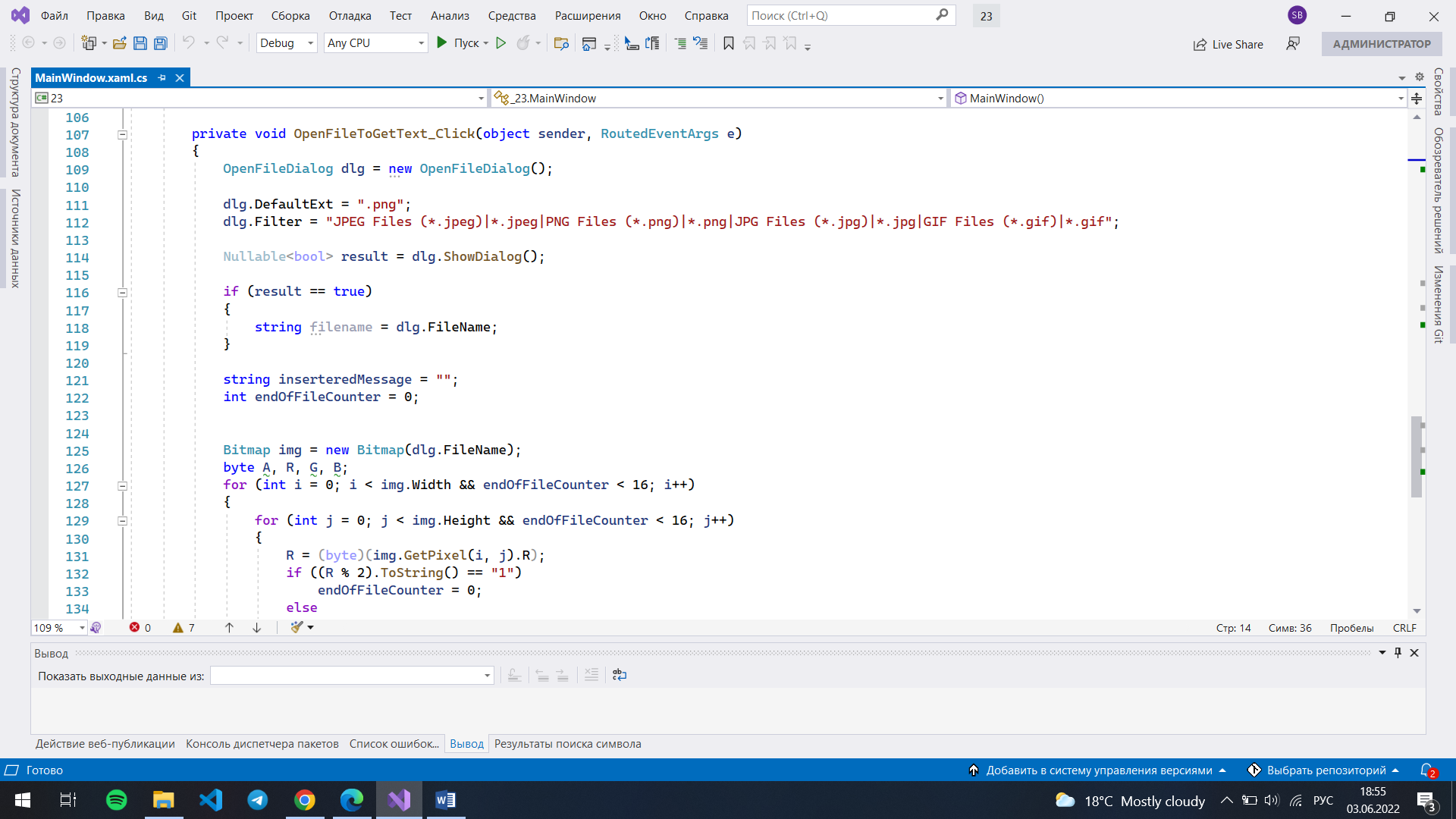


Рисунок 3 – Пример кода

Рисунок 4 – Пример кода

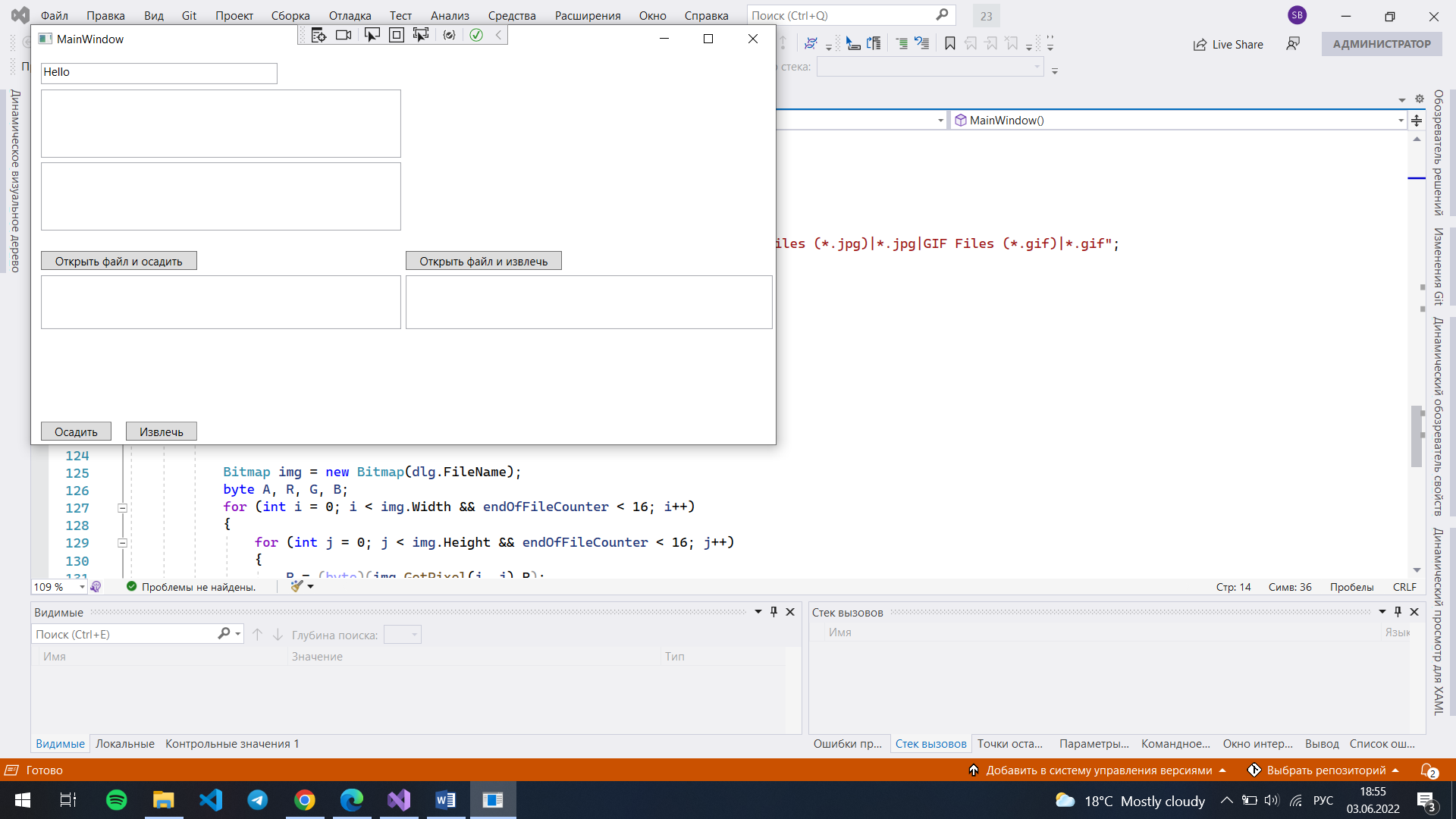


Рисунок 5 – Визуализация программы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации стеганграфии в рамках битовых контейнеров изображений