Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе №14**:

Исследование стеганографического метода на основе преобразования наименее значащих битов

Выполнила:

студентка 3 курса 6 группы

Хлыстов Глеб Георгиевич

Преподаватель:

Сазонова Дарья Владимировна

**2023 г.**

1. **Теоретические сведения**

Определение 1. 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.

При этом скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации. «Скрытость» канала передачи тайной информации отличает стеганографии от криптографии: в первом случае тайной является сам факт наличия канала (передачи информации).

Определение 2. 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 осаждения/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий (или третьи) – для предварительного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;
* контейнер с осажденным 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.

Определение 3. 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). (11.1)

Как видим, сущностью рассматриваемой системы является тайное хранение или передача одной информации в другой информации, которая является открытой.

При построении стеганосистемы должны, таким образом, учитываться следующие основные положения:

* свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;
* противник (интруз) имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
* если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;
* потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Большинство исследований в предметной области посвящено использованию в качестве стеганоконтейнеров изображений (текст также можно рассматривать как изображение). Это обусловлено следующими причинами:

* относительно большим объемом цифрового представления изображений, что позволяет внедрять большой объем данных;
* заранее известным размером контейнера, отсутствием ограничений, накладываемых требованиями реального времени;
* наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации;
* слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержанию в нем шума, искажениям вблизи контуров;
* хорошо разработанными в последнее время методами цифровой обработки изображений.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Рассмотрим это на примере 24- битного растрового RGB-изображения. Как известно, каждая точка кодируется 3-мя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из 3-х каналов определяет оттенок пикселя.

Представим пиксель тремя байтами в битовом виде.

Младшие биты дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших бит для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

Одним из простейших и понятных для решения наших задач является формат BMP (BitMaP) – одна из форм представления растровой графики. Изображение представляется в виде матрицы пикселов, где каждая точка характеризуется тремя параметрами: x-координатой, y-координатой и цветом кодом на основе RGB-модели. Все операции графического ввода-вывода на экран монитора (принтера и на некоторые другие устройства) в конечном итоге осуществляются в этом формате. Для работы с этим форматом в ОС Windows предусмотрено много специальных функций и структур API, которые помогают производить все необходимые операции на достаточно высоком логическом уровне.

Контейнеры на основе BMP-формата разделяют на два класса: «чистые» и зашумленные. В первых прослеживается связь между младшими и остальными битами элементов цвета, а также видна зависимость самих младших битов между собой. Осаждение сообщения в такой контейнер нарушает такие зависимости, что легко выявляется аналитиком. Если же картинка зашумлена (например, получена со сканера или фотокамеры), то определить осажденное сообщение сложнее. Таким образом, в качестве файлов-контейнеров для метода LSB рекомендуется использовать файлы, которые не были созданы на компьютере изначально.

Другим из растровых форматов используемых в стеганографии контейнеров является формат PNG (Portable Network Graphics). По качеству цветового отображения данный формат превосходит JPEG (Joint Photographic Experts Group) и GIF (Graphics Interchange Format), но размер файла будет на 30-40% больше.

Вышеприведенные табличные и иллюстративные данные, а также опыт специалистов показывают, что при модификации даже 3-4 младших разрядов состояние графического стеганоконтейнера у экспертов подозрений не вызывает при визуальном его контроле.

Исходя из такой оценки, следует соотносить объем осаждаемого сообщения, VM с объемом VC используемого контейнера. Например, если размер изображения 500х500 = 250 000 пикселов, а с учетом используемой 3-хцветовой модели имеем 750 000 единиц цветовых координат. Если мы планируем модифицировать только самые младшие биты всех цветовых каналов матрицы, то максимальный объем осаждаемого сообщения (VM max) не должен превышать 750 тыс. бит.

Посмотрим далее на некоторые технические детали и особенности реализации метода НЗБ при использовании в качестве контейнера изображения в формате PNG.

Берется незаполненный контейнер. Далее возьмем самый младший бит в каждом цветовом канале и отобразим на этом основании «самый нижний слой» исходного изображения в черно-белых (иначе нельзя) оттенках: нулевое значение младшего бита соответствует белому цвету, единичное – черному.

Теперь наложим изображения на контейнер со следующими кодовыми параметрами пикселов в каждом канале: 1 – 255 (11111111 – в бинарном коде; т.е. классический красный, либо классический зеленый, либо классический синий), 0 – 0 (00000000 – в бинарном коде).

Для того, чтобы этот процесс затруднить, сообщение осаждается в цветовые каналы пикселов в нерегулярной, а в псевдослучайной последовательности. Такая последовательность должна рассматриваться как один из элементов ключа стеганосистемы.

Алгоритм реализации достаточно прост. Прежде всего, нужно определиться с содержанием сообщения М, а далее – выбрать контейнер с учетом наших вышеприведенных оценок. В задачах по защите прав интеллектуальной собственности нужно идти от обратного, т.е., прежде всего, иметь в виду готовый контейнер. В обоих случаях нужно сопоставлять объемы контейнера и осаждаемого сообщения.

Для затруднения стеганоанализа порядок и количество осаждаемых бит в различные цветовые каналы можно подчинить различным правилам. Для операций «размазывания» сообщения по контейнеру могут применяться ключевой файл и пароль в виде, например, текстов, которые символы которых заменяются числами и в совокупности определяют местоположение пикселя для записи в него части секретного сообщения.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать пользовательское приложение, которое должно реализовывать следующие операции:

* выбор файла-контейнера – по согласованию с преподавателем;
* реализовать два варианта осаждаемого/извлекаемого сообщения: ⎫ собственные фамилия, имя и отчество; текстовая часть отчета по одной из выполненных лабораторных работ;
* реализовать два метода (на собственный выбор) размещения битового потока осаждаемого сообщения по содержимому контейнера;
* сформировать цветовые матрицы, отображающие каждый задействованный для осаждения уровень младших значащих бит контейнера;
* выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе выполненного анализа.

Для выполнения задания были разработаны функции для осаждения/извлечения тайной информации на основе метода НЗБ.

После запуска приложения открывается форма, в которой можно ввести тайный текст и выбрать пустой контейнер.

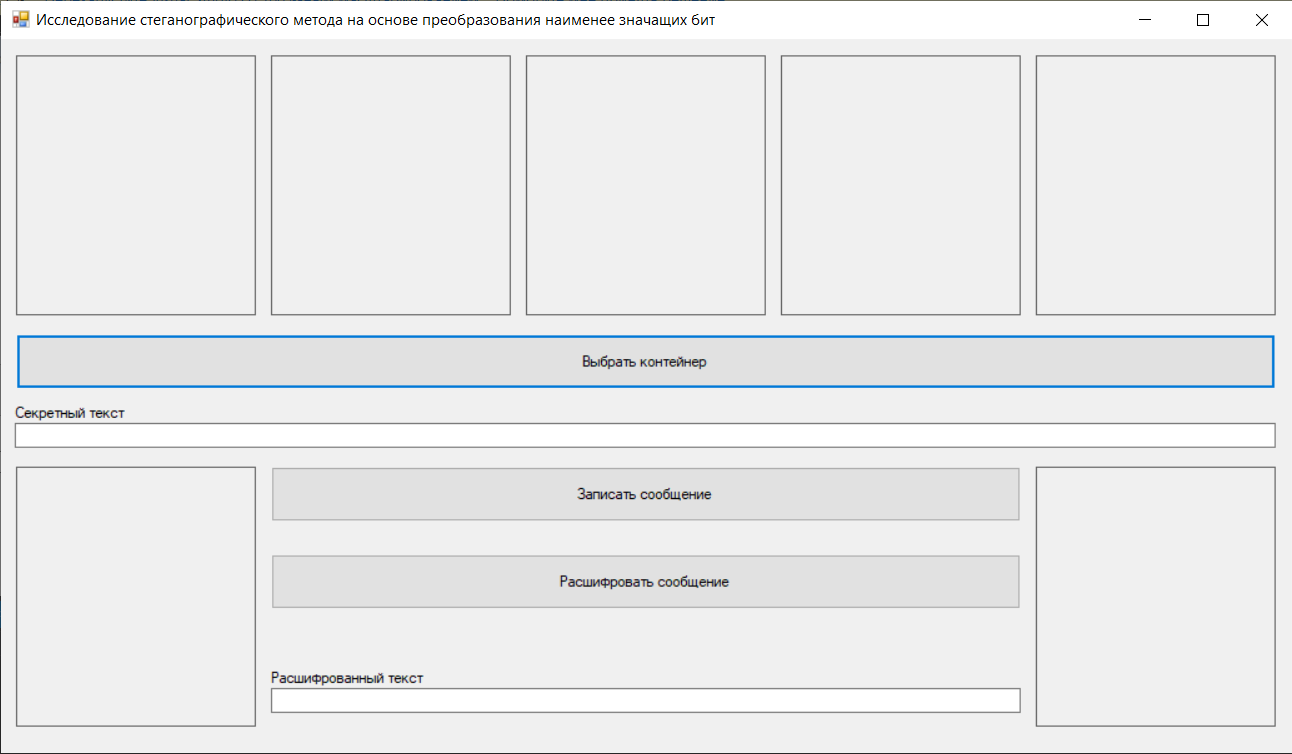


Рисунок 2.1 – Окно приложения

При нажатии на кнопку «Выбрать контейнер» откроется меню, в котором можно выбрать изображение, которое будет служить контейнером для тайного сообщения.

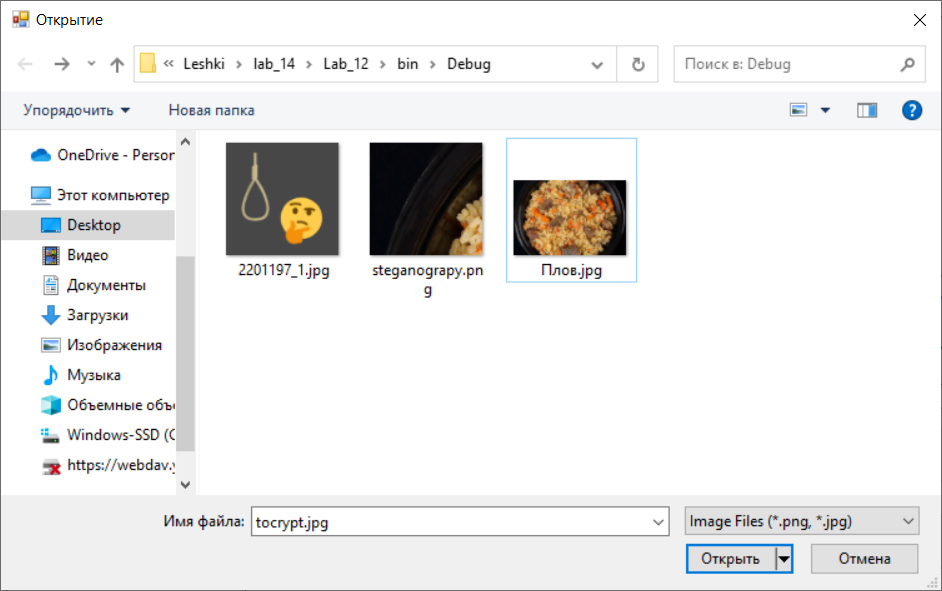


Рисунок 2.2 – Окно выбора пустого контейнера

После нажатия на кнопку «Open» изображение добавится в левую форму для изображения, а также будет создано еще четыре изображения. Первые 3 изображения – это матрицы первых значимых битом для 3 каналов RGB (красного, зеленого, синего). Здесь белый пиксель – если на конце элемента матрицы стоял «0», черный пиксель – если на конце элемента матрицы стоял «1». Четвертое изображение – цветовое отображение наименьших значимых битов. Здесь каждый пиксель прорисован по стандартной модели RGB, только каждый цвет канала передается согласно условию: если в элементе матрицы канала наименьший значимый бит - «0», то в соответствующем канале цветового отображения наименьших значимых битов также будет стоять «0». Но если же там «1» - то соответствующе будет стоять «255».

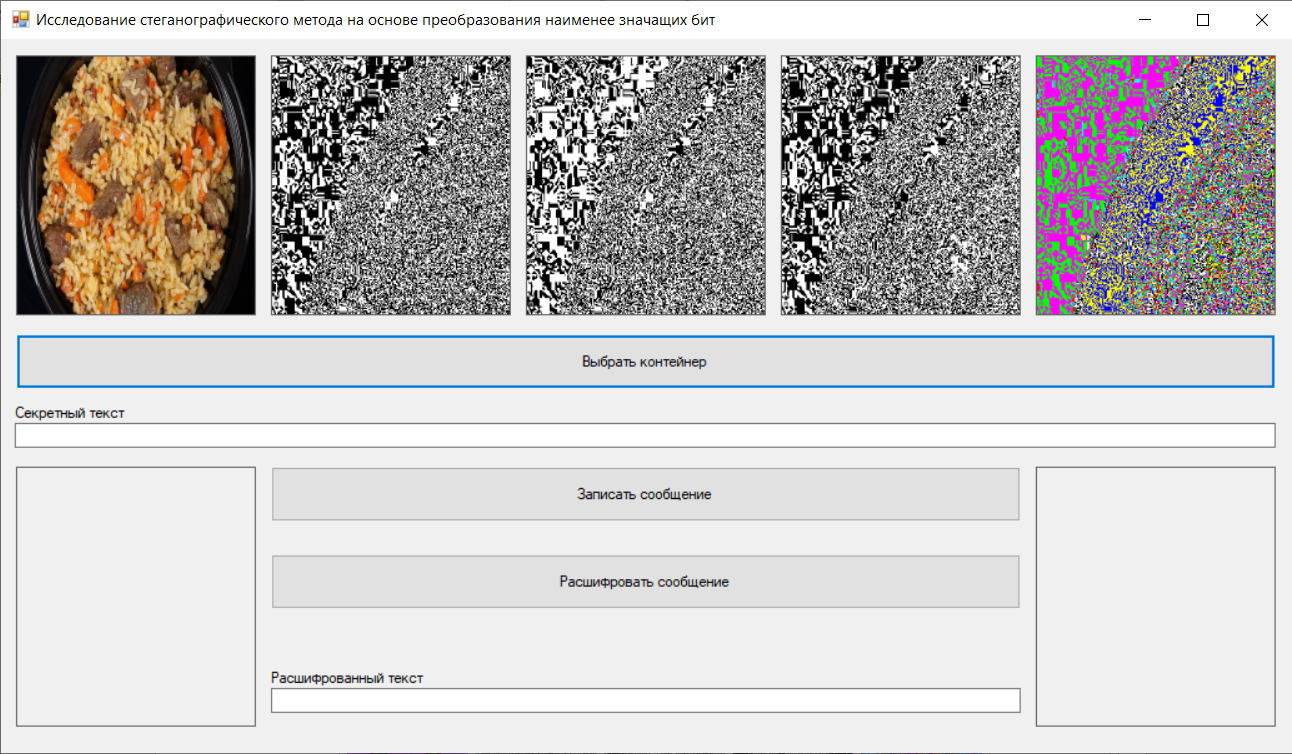


Рисунок 2.3 –Преобразованный контейнер (вид различных каналов)

Если ввести в первое текстовое поле какой-то текст и нажать на кнопку «Записать сообщение», запустится функция «steganographyText». В самом начале мы пробегаемся по каждому пикселю и устанавливаем значение каждого наименьшего значимого бита каждого канала в «0». Тем самым мы освобождаем во всем изображении каждый 8 бит, который будет нужен для записи тайного сообщения.

Текст, который приходит из текстового сообщения, согласно таблице ASCII переводится в двоичную систему. При этом если число символов бинарного тайного сообщения не кратно 3, то оно дополняется справа нулями (т.к. сообщение должно равномерно переноситься на 3 канала).

После чего мы посимвольно пробегаемся по бинарному тайному тексту и записываем «0» или «1» (в зависимости от того, какой бит рассматривается) в наименьший значимый бит каждого из трех каналов каждого пикселя до тех пор, пока бинарное сообщение не закончится.

После всего этого на основе полученной матрицы пикселей формируется изображение, которое сохраняется как файл с расширением .png.

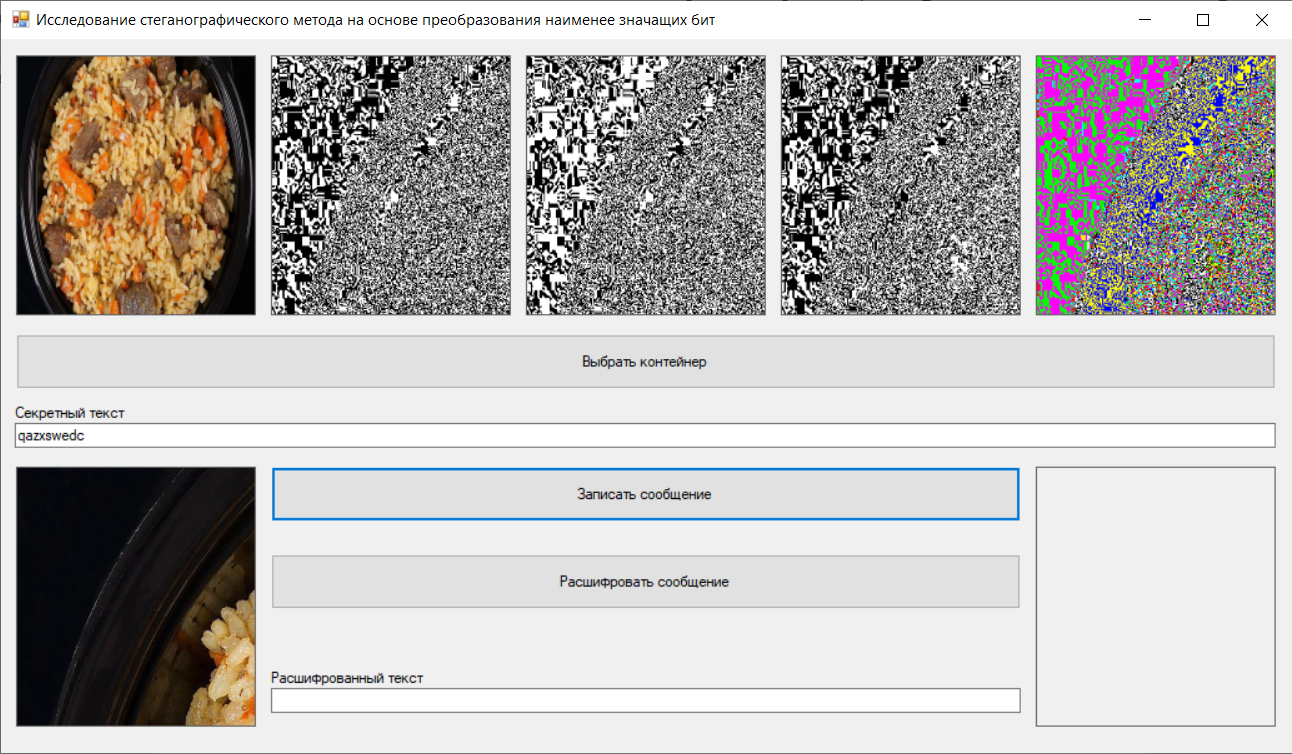
**

Рисунок 2.4 – Контейнер с тайным сообщением

Для того, чтобы достать тайное сообщение из контейнера, необходимо нажать на кнопку «Расшифровать сообщение». После нажатия откроется окно, в котором можно выбрать изображение с предполагаемым тайным сообщением.

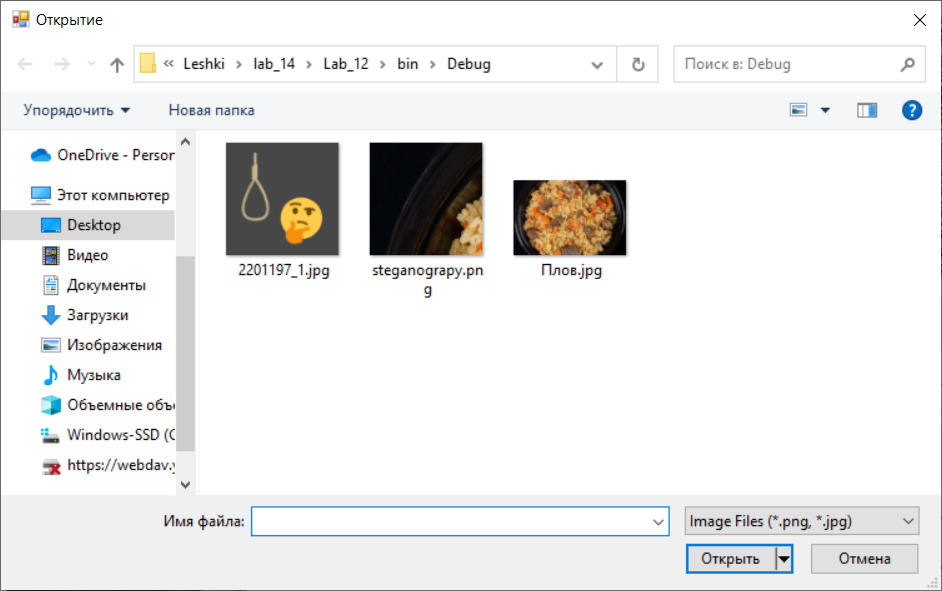


Рисунок 2.5 – Окно выбора контейнера с тайным текстом

После нажатия на кнопку «Открыть» изображение добавится в форму Справа снизу, а также каждый пиксель по каналам запишется в матрицу своего цвета. После чего циклом пробегаемся по всем этим матрицам и записываем попиксельно каждый наименьший значимый бит каждого канала. После чего бинарное сообщение расширяется до числа, кратному восьми справа (заполнение «0»), весь текст делится на блоки по 8 бит и данное 8-битное число переводится в символ ASCII, после чего сформированное сообщение выводится в соответствующее текстовое поле.

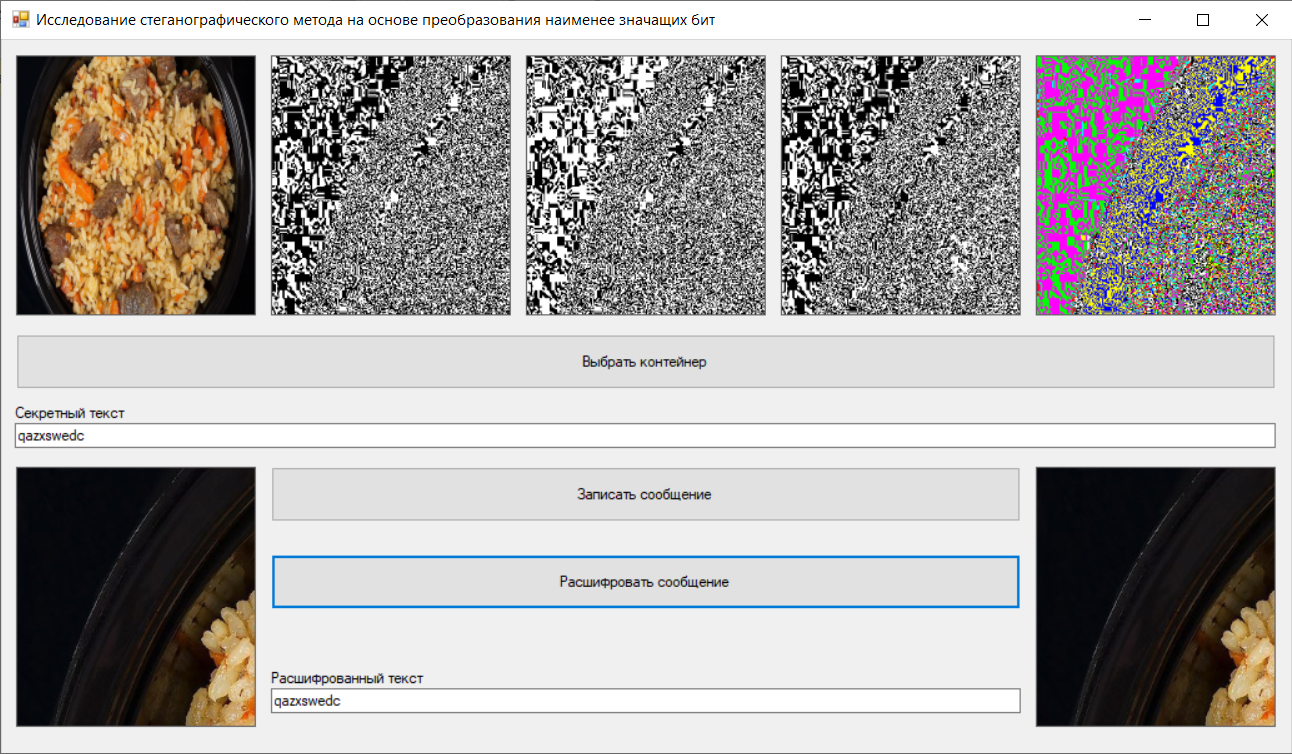


Рисунок 2.6 – Окно выбора контейнера с тайным текстом

В окне «Расшифрованный текст» мы видим сообщение, которое полностью совпадает с секретным текстом, что означает, что все этапы шифрования и расшифрование прошли успешно.

**Вывод**

В данной лабораторной работе я закрепил теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии. Изучил алгоритм осаждения/извлечения тайной информации на основе метода НЗБ, получил опыт практической реализации метода. Разобрал приложения для реализации алгоритма осаждения/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ. А также познакомился с методиками оценки стеганографической стойкости метода НЗБ.