Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет к лабораторной работе №13**:

Исследование стеганографического метода на основе преобразования наименее значащих битов

Студент: 3 курса 6 группы

Коктыш Е.С.

Преподаватель: Нистюк О.А.

Минск 2024

1. **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 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.

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.

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.

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.

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.

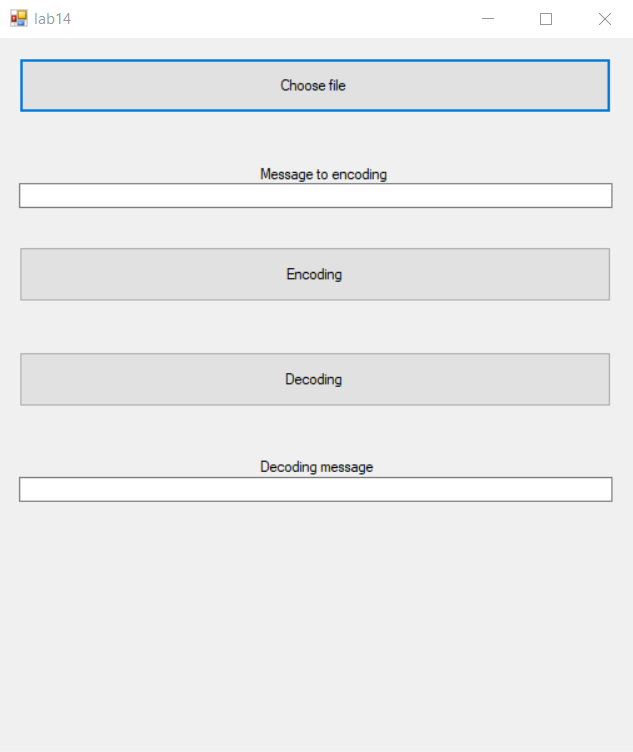


Рисунок 2.1 – Окно приложения

В основе стеганографических преобразований лежит изображение, представленное на рисунке 2.2.



Рисунок 2.2 – Изначальное изображение для преобразований

Для зашифрования сообщения необходимо выбрать изображение, нажав на кнопку «Choose file», написать текст сообщения в поле «Message to encoding» и нажать на кнопку «Encoding.

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.

Изображение с осажденными данными при помощи алгоритма наименее значимых битов сохранится в файл с названием «steganography1.png». Данное изображение представлено на рисунке 2.3.



Рисунок 2.3 — Изображение с сообщением «KoktyshES» методом осаждения в наименее значимых битах

Так же был разработан алгоритм осаждения сообщения в младших разрядах яркости. Метод осаждения в младших разрядах яркости позволяет скрыть данные в изображении, используя младшие биты компоненты яркости каждого пикселя. Результат работы алгоритма сохраняется в файл с названием «stenography2.png», изображенный на рисунке 2.4.



Рисунок 2.4 — Изображение с сообщением «KoktyshES» методом осаждения в младших разрядах яркости

Так же автоматически при выборе контейнера формируется цветовая матрица и результат сохраняется в файл с названием «mat.png», который представлен на рисунке 2.5.



Рисунок 2.5 – Цветовая матрицаконтейнера

Пустой контейнер и контейнер с осажденным сообщением представлены на рисунке 2.6.

При взгляде на эти изображения глазами человека различить их между собой окажется невозможным.

Рисунок 2.6 – Визуальный анализ пустого контейнера и контейнера с осажденным сообщением

Для извлечения сообщения из стеганоконтейнера необходимо нажать на кнопку «Decoding». 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. Результат расшифрования сообщения представлен на рисунке 2.7.

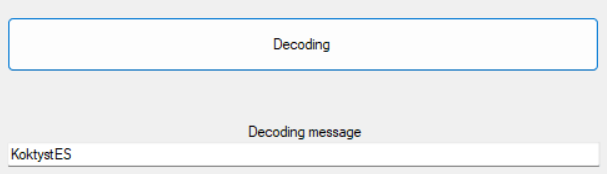


Рисунок 2.7 — Результат расшифрования сообщения

Мы видим сообщение, которое полностью совпадает с секретным текстом, что означает, что все этапы шифрования и расшифрование прошли успешно.

**Вывод**

В данной лабораторной работе были закреплены теоретические знания из области стеганографического преобразования информации, моделирования стеганосистем, классификации и сущности методов цифровой стеганографии. Изучен алгоритм осаждения/извлечения тайной информации на основе метода НЗБ, получен опыт практической реализации метода. Созданы приложения для реализации алгоритма осаждения/извлечения тайной информации с использованием электронного файла-контейнера на основе метода НЗБ.