Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование стеганографического метода на основе преобразования наименее значащих бит»

Выполнил:

студент 3 курса 8 группы ФИТ

Ярмолик Николай Сергеевич

Проверил:

Берников В. О.

Минск 2020

**1. Теоретическая часть**

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 отли- чает стеганографии от криптографии: в первом случае тайной являет- ся 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 [2, 53-56]; 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 харак- теризуют 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 предвари- тельного (перед осаждением) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или за- шифрования) и т. д. [2, 57, 58];

*контейнер с осажденным сообщением* или *стеганоконтейнер*, *S*, который передается по *открытому каналу*, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также *стеганосообщением*;

*Определение* 3. Стеганографической системой ∑ будем называть совокупность сообщений M, контейнеров C, ключей K, стеганосообщений (заполненных контейнеров) S и преобразований.

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, как это показано на рис. 1.1.

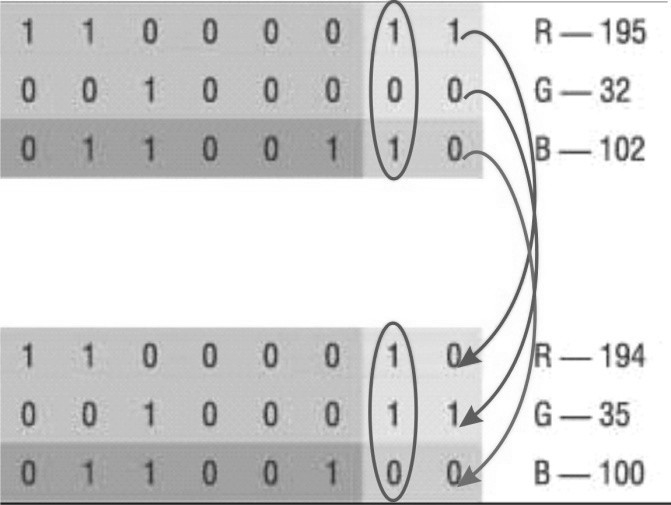
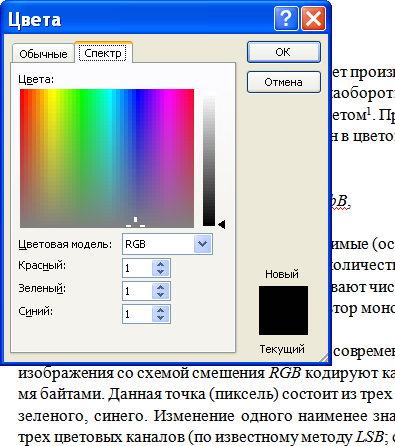
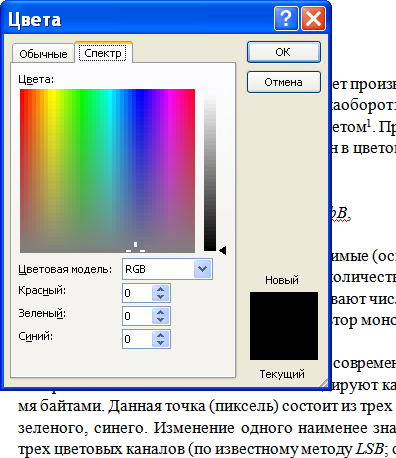


Рисунок 1.1 – Пример, показывающий принцип реализации метода LSB

Младшие биты (выделены бледным, справа) 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.

Рассмотрим простейший пример.

*Пример* 1. Контейнером *С* выступает обычная буква «А». Цвет текста-контейнера «А» – черный: данный цвет представлен в MS Office Word как (00000000, 00000000, 00000000), т.е. (0, 0, 0)

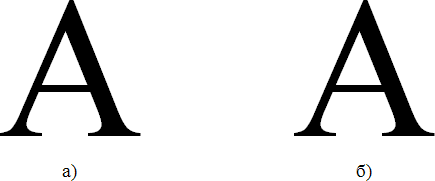
а) б)

Рисунок 1.2 – Диалоговое окно MS Wordс указанием цветовых координат символов текста: (0, 0, 0) – а), (1, 1, 1) – б)

Необходимо внедрить секретное сообщение: *М* = 111 в текст-кон- тейнер *С*, используя текстовый процессор MS Word. Мы решаем зада- чу чисто механически: изменяем младший из символов цветового кода в каждом канале (рис. 1.2), т. е. в десятичном виде это можно представить как (1, 1, 1), а в двоичном – (0000000**1**, 0000000**1**, 0000000**1**). Результат осаждения секретного сообщения (111) в текст- контейнер «А» показан на рисунке 12.3: «пустой» контейнер (*С*) никак визуально не отличается от стеганоконтейнера (*S*).

На рис. 12.4 приведены четыре строки символов, цветовые коор- динаты которых соответствуют различным числам, с изменением вплоть до пятого (справа-налево) бита цветового кода (см. табл. 1.1). В таблице номера столбцов с кодами соответствуют позиции символа в строке на рис едва различимы, притом только в четвертой строке.

Подчеркнем, что именно визуальный анализ графического объек- та является основой наиболее часто используемой (прежде всего, в силу трудозатрат) методики стеганографического анализа.



а) не модифицированный символ-контейнер; б) модифицированный символ-контейнер (со встроенным секретным сообщением «111»)

Рисунок 1.3 Пример практической реализации метода НЗБ

А А А А А А А А А А А А А А А А А А А А А А А А

Рисунок 1.4 Одинаковый символ (А) с различной кодировкой цвета

Таблица 1.1 Цветовая кодировка символов на рис. 1.4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Столбец Строка | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 0,0,0 | 1,1,1 | 2,2,2 | 4,4,4 | 8,8,8 | 16,16,16 |
| 2 | 0,1,2 | 0,2,1 | 0,2,0 | 4,2,1 | 4,8,16 | 16,8,4 |
| 3 | 255,0,0 | 255,1,1 | 254,1,1 | 253,2,2 | 252,4,4 | 251,8,8 |
| 4 | 100,100,10  0 | 99,100,101 | 95,95,95 | 105,110,90 | 90,100,110 | 90,90,90 |

При этом проявляется еще одно важное обстоятельство: примерно в 50% случаев бит, который мы хотим записать, и бит в изображении- контейнере будут совпадать и изменять ничего не нужно.

Понятно, что графические контейнеры в реальной стеганографии много сложнее рассмотренных примеров.

Одним из простейших и понятных для решения наших задач явля- ется 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 некото- рые 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 за- висимость 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 ка- честву 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, *V*M с объемом *V*C используемого контейнера. Например, если размер изображения 500х500 = 250 000 пикселов, а с учетом используемой 3-хцветовой модели имеем 750 000 единиц цветовых ко- ординат. Если мы планируем модифицировать только самые младшие биты всех цветовых каналов матрицы, то максимальный объем осаждаемого сообщения (*V*M max) не должен превышать 750 тыс. бит.

**2. Практическая часть**

Требовалось разработать собственное приложение, в котором должен быть реализован метод НЗБ

Общий интерфейс приложения представлен на рисунке 2.1

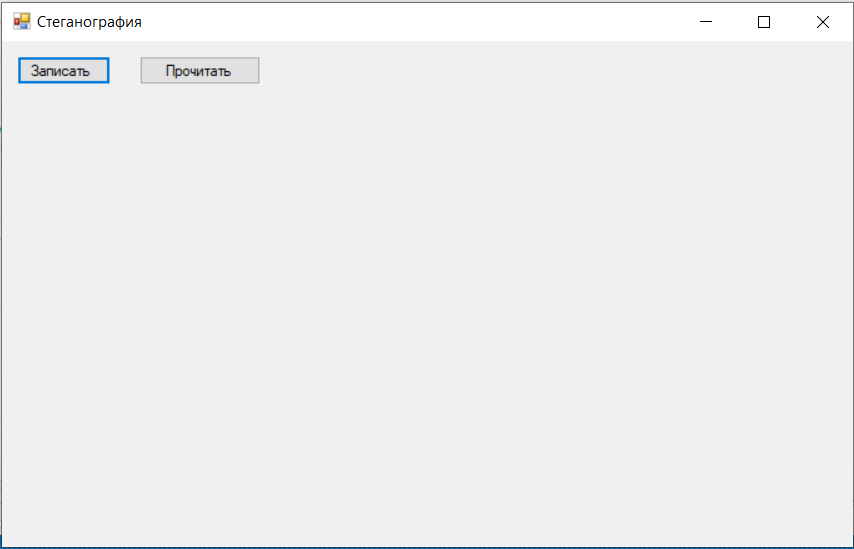


Рисунок 2.1 – Общий интерфейс программы

При нажатии кнопки записать требуется выбрать исходное bmp изображение, текст и директорию для сохранения преобразованного изображения. На рисунке 2.2 приведен скриншот операции.

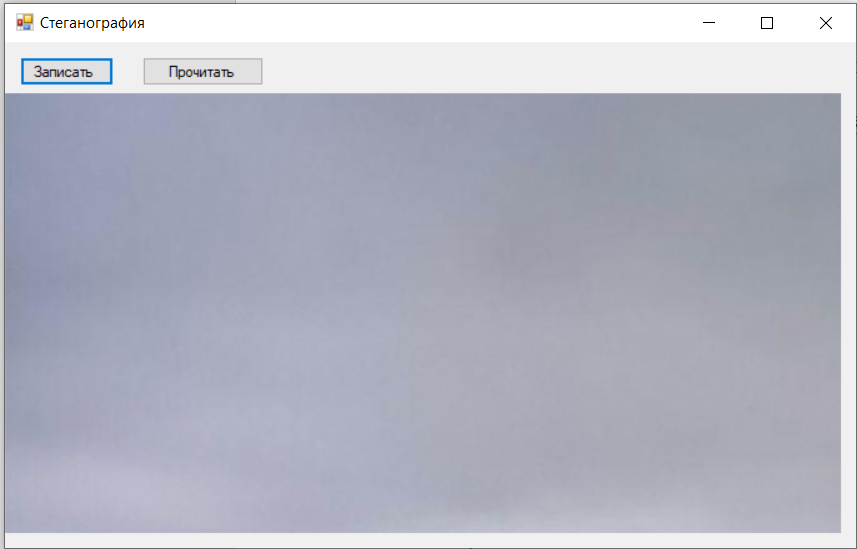


Рисунок 2.2 – Выполнение операции

Для дешифрования выбираем зашифрованное изображение, и указываем файл для выгрузки полученного результата. Если попытаться выбрать файл в котором нет зашифрованного текста будет выдаваться предупреждение на рисунке 2.3

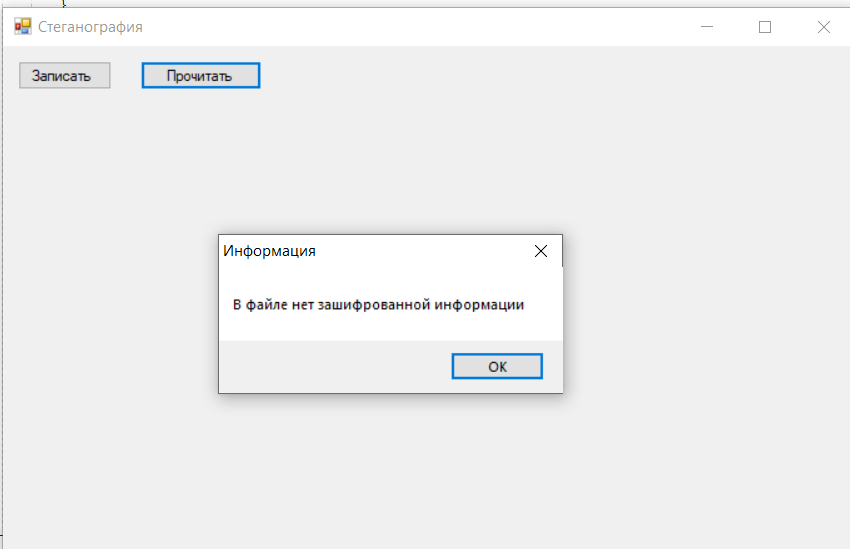


Рисунок 2.3 – Окно предупреждения

Ниже представлены 2 скриншоты исходного изображения и изображения с зашифрованным текстом. Слева исходное изображение, справа изображение с шифртекстом

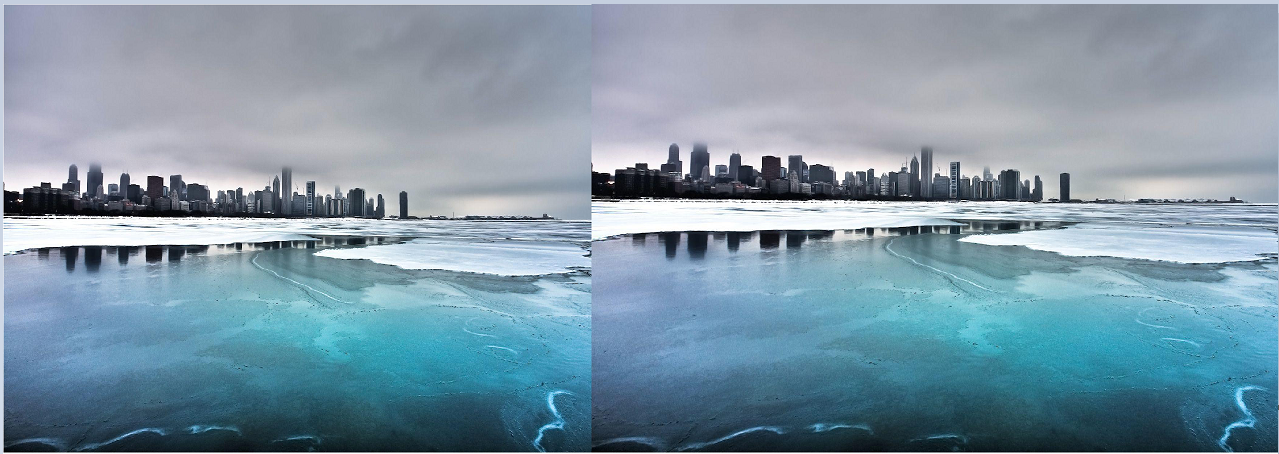


Рисунок 2.4 – Сравнение изображений

Вывод:

В результате лабораторной работы мы ознакомились с стеганографического метода осаждения/ извлечения тайной информации с использованием электронного файла-контейнера на основе преобразования наименее значащих бит (НЗБ), приобретение практических навыков программной реализации данного метода. Также была разработано программное средство реализуемое поставленные в практической части задачи