МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №12 НА ТЕМУ:

Исследование стенографического метода на основе преобразования наименее значащих битов

Выполнила:

Студентка 3 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

**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 эксперимент.

**Теоретические сведения**

Стеганографическая система(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:

Сущностью рассматриваемой системы является тайное хранение или передача одной информации в другой информации, которая является открытой.

При построении стегосистемы необходимо, чтобы:

– свойства контейнера были модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле;

– противник 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 устанавливать факт присутствия и содержания скрытого сообщения;

– если противник узнает о факте существования, это не должно позволить ему извлечь сообщение, 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 и слуха человека.

Причины частого использования изображений в качестве стеганоконтейнеров:

– относительно большой объем цифрового представления изображений позволяет внедрять большой объем данных;

– заранее известны размеры контейнера;

– некоторые изображения имеют шумовую структуру и хорошо родходят для встраивания информации;

– слабая чувствительность глаза к незначительным изменениям цветов изображения.

Каждая точка кодируется тремя байтами.

Каждый байт определяется интенсивностью красного, зеленого и синего цветов.

Совокупность интенсивностей цвета в каждом из трех каналов определяет оттенок пикселя.

Младшие биты дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или нескольких младших битов для человека будет почти незаметна.

Именно визуальный анализ графического объекта является основой наиболее часто используемой (прежде всего в силу трудозатрат) методики стеганографического анализа.

Примерно в 50% случаев бит, который мы хотим записать, и бит в изображении-контейнере будут совпадать, и изменять ничего не нужно.

BMP (BitMaP) – одна из форм представления растровой графики.

Изображение представляется в виде матрицы пикселей, где каждая точка характеризуется тремя параметрами: *x*-координатой, *y*-координатой и цветовым кодом на основе RGB-модели.

Контейнеры на основе BMP-формата разделяют на два класса:

1) Чистые: прослеживается связь между младшими и остальными битами элементов цвета, а также видна зависимость самих младших битов между собой.

2) Зашумленные

**Ход работы**

Разработать собственное приложение, в котором должен быть реализован метод НЗБ. При этом:

• выбор файла-контейнера – по согласованию с преподавателем;

В качестве типа файла-контейнера были выбраны изображения. Незаполненный контейнер имеет вид, показанный на рисунке 1.



Рисунок 1 – Вид «пустого» контейнера

• реализовать два варианта осаждаемого/извлекаемого сообщения:

− собственные ФИО;

− текстовая часть отчета по одной из выполненных лабораторных работ;

Была использована текстовая часть отчета по данной лаб-й работе.

Приложение предоставляет две кнопки. Кнопка «Записать» просит выбрать в проводнике файл с расширением .bmp, затем выбрать текстовый файл с сообщением, которое пользователь желает осадить, и название нового .bmp-файла со скрытой информацией.

Приложение выглядит следующим образом (рисунок 2).

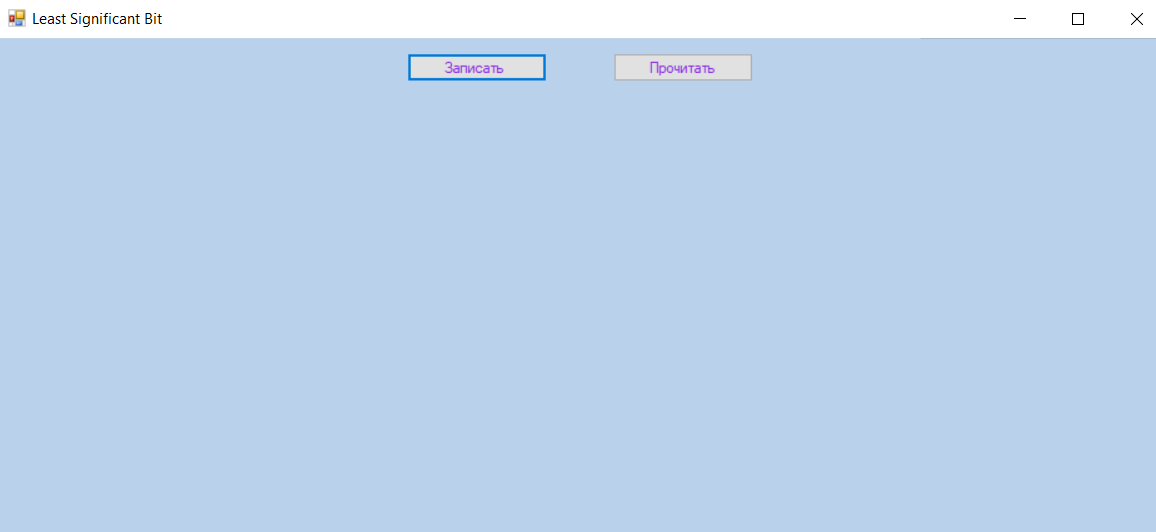


Рисунок 2 – Контейнер с ФИО

Результат осаждения ФИО представлен на рисунке 3.



Рисунок 3 – Контейнер с ФИО

Результат осаждения отчета представлен на рисунке 3.



Рисунок 3 – Контейнер с отчетом

Так же по условию задания необходимо было разработать два метода размещения битового потока осаждаемого сообщения по содержимому контейнера.

Для этого были использованы встроенные библиотеки языка python. В первой ситуации (листинг 1) мы используем файл-контейнер и сам текст сообщения (собственное фио) в результате получая файл-контейнер с зашифрованным сообщением. Для расшифрования используется метод reveal.

from stegano import lsb

secret = lsb.hide("pic.bmp", "SEK")

secret.save("pic\_secret.bmp")

result = lsb.reveal("pic\_secret.bmp")

print(result)

Листинг 1 – Шифрования и расшифрования методом lsb

Второй способ (листинг 2) показывает осаждение сообщения с использованием ключа. Сначала у нас генерируется ключ, представленный на рисунке 11, а затем мы осуществляем непосредственное зашифрование и расшифрование.

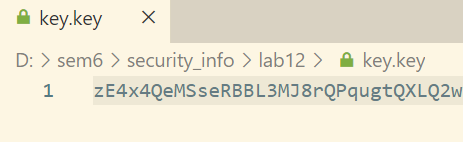


Рисунок 11 – Файл-контейнер с зашифрованным сообщением

Steganography.generate\_key("")

secret = Steganography.encrypt("key.key", "img/pic.bmp", "secret\_message.txt")

secret.save("pic\_secret\_with\_key.bmp")

result = Steganography.decrypt("key.key", "pic\_secret\_with\_key.bmp")

print(result)

Листинг 2 – Шифрования и расшифрования методом lsb с ключом

Чтобы считать осажденный текст, требуется нажать на кнопку «Прочитать», выбрать файл с секретной информацией и ввести название текстового файла, куда запишется результат.

• выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе выполненного анализа.

После выполнения визуального анализа выяснилось, что человеческий глаз не может определить различия между пустым контейнером и контейнером с сообщением.

**Ответы на вопросы**

1. Охарактеризовать цели, задачи и области применения стеганографии.

Цель **–** скрыть сам факт существования секретного сообщения.

Задачи стеганографии – это разработка методов скрытой передачи информации, обеспечивающих сохранность передаваемой информации и ее невидимость для посторонних.

Область применения стеганографии – это информационная безопасность и криптография, когда скрытая информация может быть использована для хранения секретных данных, обеспечения безопасности сети или транспортировки сообщений в условиях, когда прямая передача информации затруднена или нежелательна. Стеаганография также может использоваться для целей контроля и наблюдения, например, для обеспечения конфиденциальности корпоративных данных и надзора за работниками.

2. В чем состоят сходства и различия между стеганографией и криптографией.

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

3. Дать определение стеганографической системы. Охарактеризовать составные части стеганосистемы и их взаимосвязь?

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

4. Основные классификационные критерии методов стеганографии.

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

• аудиостеганография;

• видеостеганография;

• графическая стеганография;

• текстовая стеганография;

• и др.

5. Пояснить сущность основных атак на стеганосистемы?

Атака по известному заполненному контейнеру: злоумышленник знает, какой файл используется в качестве контейнера и пытается извлечь скрытую информацию без знания ключа.

Атака по известному встроенному сообщению: злоумышленник знает, какое сообщение было встроено в контейнер, и пытается извлечь ключ, используя знание сообщения.

Атака на основе выбранного скрытого сообщения: злоумышленник выбирает скрытое сообщение и пытается извлечь его из контейнера.

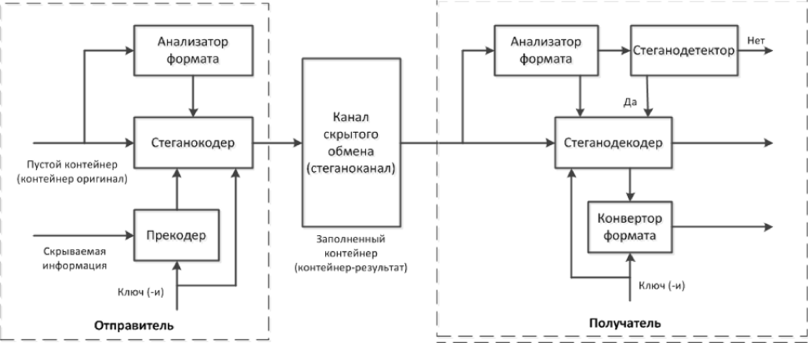
Атака на основе выбранного заполненного контейнера: злоумышленник выбирает заполненный контейнер и пытается извлечь скрытую информацию без знания ключа.

Атака на основе известного пустого контейнера: злоумышленник знает, что контейнер пуст, и пытается найти скрытую информацию, если она есть.

Атака на основе выбранного пустого контейнера: злоумышленник выбирает пустой контейнер и пытается встроить в него скрытое сообщение.

Атака по известной математической модели контейнера: злоумышленник знает, как устроена математическая модель контейнера, и пытается использовать эту информацию для извлечения скрытой информации.

6. Изобразить структурную схему стеганографической системы.



7. Сущность метода НЗБ. Области его применении?

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Младшие биты (выделены бледным, справа) дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

Области применения метода LSB в стеганографии включают:

1. Защита авторских прав - в стеганографическом изображении можно скрыть информацию о правообладателе, дате создания, лицензии и т.д. Это позволяет защитить авторские права на изображение и легализовать его использование.
2. Безопасность данных - метод LSB может использоваться для скрытия конфиденциальной информации в видео- или аудиофайлах, что позволяет обмениваться информацией без вызова подозрений у третьих лиц.
3. Маркирование изображений - метод LSB может использоваться для маркирования изображений, чтобы облегчить их последующее распознавание и идентификацию.
4. Контроль и наблюдение - метод LSB может использоваться для контроля и наблюдения за сотрудниками, например, для отслеживания активности в интернете и нежелательного использования корпоративных ресурсов.
5. Скрытый обмен сообщениями - метод LSB может использоваться для скрытого обмена сообщениями в условиях, когда прямая передача информации затруднена или нежелательна.
6. Восстановление поврежденных данных - метод LSB может использоваться для восстановления поврежденных данных, если в них была скрыта дополнительная информация.
7. Контроль целостности данных - метод LSB может использоваться для контроля целостности данных, т.е. проверки, не были ли изменены данные в процессе передачи или хранения.

8. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при передаче этих сообщений.

*Алгоритм встраивания сообщения на основе метода НЗБ:*

1. Разбить исходное сообщение на блоки размером *N*.
2. Выбрать блоки, в которых можно внести незначительные изменения, например, изменить значения младших битов в каждом пикселе изображения.
3. Вычислить разницу между значениями исходных и измененных блоков.
4. Разбить скрытое сообщение на блоки размером *M*, где *M* < *N*.
5. Внести изменения в выбранные блоки исходного сообщения, используя значения блоков скрытого сообщения.
6. Обновить значения выбранных блоков исходного сообщения.
7. Вернуть измененное сообщение.

*Алгоритм извлечения сообщения на основе метода НЗБ:*

1. Разбить измененное сообщение на блоки размером *N*.
2. Выбрать блоки, в которых были внесены незначительные изменения.
3. Вычислить разницу между значениями исходных и измененных блоков.
4. Разбить полученную разницу на блоки размером *M*, где *M* < *N*.
5. Восстановить скрытое сообщение, используя значения блоков разницы.
6. Вернуть скрытое сообщение.

**Вывод:** были изучены и приобретены практические навыки разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.