

СОДЕРЖАНИЕ

Обозначения и сокращения	7
Введение	8
1 Общие положения и описание стеганографических методов защиты информации	9
1.1 Основные понятия	9
1.2 Цифровые водяные знаки и цифровые отпечатки	10
1.3 Обобщенные стеганографические методы	12
1.4 Стегоанализ	12
2 Скрытия методом наименее значимого бита	14
2.1 Общие сведения	14
2.2 Алгоритм	15
2.3 Формат файла PNG	17
2.4 Реализация LSB для контейнера PNG	20
3 Скрытие в спектральной области	24
3.1 Дискретное косинусное преобразование	24
3.2 JPEG	25
3.3 JSteg	31
3.4 Метод относительной замены величин коэффициентов ДКП ..	35
4 Стегоанализ	38
4.1 Методы стегоанализа	38
4.2 Субъективная атака LSB	38
4.3 Атака оценки числа переходов значений младших бит в соседних элементах контейнера	39
4.4 Атака хи-квадрат	41
4.5 Методы противодействия	43
5 Экономическая оценка проекта	45
5.1 Постановка задачи	45
5.2 Оценка стоимости объектов интеллектуальной собственности ..	45
5.3 Оценка стоимости разработки	49
5.4 Оценка стоимости использования оборудования и сопровождения системы	49
5.5 Экономическое обоснование проекта	50

Заключение	51
Список использованных источников	52
Приложение А Реализация метода Бенгама-Мемона-Эо-Юнга на Python	53

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

CRC — cyclic redundancy code (циклический избыточный код)

LSB — least significant bit (наименее значащий бит)

DRM — digital rights management (цифровое управление правами)

ЦВЗ — цифровой водяной знак

RGB — red, green, blue (красный, синий, зеленый)

ДКП — дискретное косинусное преобразование

DCT — discrete cosine transform (дискретное косинусное преобразование)

НИР — научно-исследовательская работа

ОИС — объект интеллектуальной собственности

ГПСЧ — генератор псевдослучайных чисел

ВВЕДЕНИЕ

Стеганография — это практика сокрытия сообщения внутри другого сообщения или физического объекта. Тогда как криптография скрывает содержимое сообщения, стеганография скрывает сам факт существования какого-либо сообщения.

Стеганография часто используется совместно с криптографией, дополняя ее. Стеганографические методы сокрытия сообщения снижают вероятность обнаружения самой передачи сообщения. Если сообщение к тому же зашифровано, то это обеспечивает еще большую защищенность.

В настоящее время наибольшее распространение получила цифровая стеганография. Особенностью цифровой стеганографии является сокрытие информации внутри других цифровых объектов, таких как текст, изображения, видео, аудио и другие. Со все большим возрастанием роли интернет-технологий в жизни человека значимость стеганографии также возрастает.

Области применения стеганографии включают в себя:

- а) Защита авторского права и DRM (digital rights management).
- б) Незаметная передача информации.
- в) Защита конфиденциальной информации от несанкционированного доступа.

Цифровая стеганография является молодым и бурно развивающимся направлением. В последние годы стеганография все больше находит применение в области защиты прав собственности на информацию.

В своей работе я хочу рассмотреть основные стеганографические алгоритмы, определить области их применения, достоинства и недостатки, а также провести анализ возможных уязвимостей этих алгоритмов.

1 Общие положения и описание стеганографических методов защиты информации

1.1 Основные понятия

а) Стеганографическая система (стегосистема) — совокупность методов и средств, используемых для создания скрытого канала для передачи информации. Основные требования, предъявляемые к стегосистеме:

1) Безопасность системы определяется секретностью ключа. Это означает, что даже если потенциальный враг представляет работу стеганографической системы и статистические характеристики сообщений и контейнеров, это не дает ему дополнительных преимуществ при выявлении наличия или отсутствия сообщения в конкретном контейнере.

2) При обнаружении противником наличия скрытого сообщения он не должен смошь извлечь сообщение до тех пор, пока он не будет владеть ключом.

3) Алгоритм сокрытия информации не нарушает ее целостность и аутентичность. В некоторых случаях дополнительно требуется, чтобы алгоритм обеспечивал целостность сообщения при деформации контейнера.

4) Система с цифровым водяным знаком должна иметь низкую вероятность ложного обнаружения скрытого сообщения.

б) Сообщение — информация, передачу которой нужно скрыть.

в) Контейнер — любая информация, используемая для сокрытия тайного сообщения. Контейнер может находиться в одном из двух состояний:

1) Пустой контейнер — контейнер, не содержащий сообщение.

2) Заполненный контейнер (стегоконтейнер) — контейнер, содержащий сообщение.

г) Стеганографический канал (стегоканал) — канал передачи стегоконтейнера.

д) Ключ (стегоключ) — секретный ключ, нужный для сокрытия стегоконтейнера. По аналогии с криптографией стегоключи подразделяются на 2 типа:

- 1) Закрытый стегоключ. В системах с закрытым стегоключем ключ должен быть создан до начала обмена сообщениями, либо передан по защищенному каналу связи.
- 2) Открытый стегоключ. Такой ключ может быть передан по открытому незащищенному каналу связи. Открытый стегоключ должен обладать таким свойством, чтобы по нему вычислительно нецелесообразно было восстанавливать закрытый ключ.

1.2 Цифровые водяные знаки и цифровые отпечатки

Цифровой водяной знак (ЦВЗ) — технология, созданная для защиты авторских прав на цифровые объекты. В связи с быстрым развитием информационных технологий все более актуальным становится вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами цифровых объектов могут выступать аудиозаписи, видеозаписи, изображения, электронные книги и другие. ЦВЗ могут быть как видимыми, так и невидимыми. Решение о наличии в цифровом объекте невидимого ЦВЗ принимаются на основе процедуры декодирования.

В общем виде стегосистема ЦВЗ может быть разбита на части следующим образом:

- а) Прекодер — часть, которая приводит ЦВЗ к удобному для встраивания в стегоконтейнер виду.
- б) Стегокодер — часть, которая вкладывает сообщение в стегоконтейнер.
- в) Выделение встроенного сообщения — процедура, выделяющая сообщение из стегоконтейнера.
- г) Стегодетектор — часть, определяющая наличие ЦВЗ.
- д) Декодер — часть, восстанавливающая исходное сообщение.

Контейнер, содержащий ЦВЗ, может подвергаться преднамеренным атакам или случайным помехам. Стегосистема ЦВЗ должна обеспечивать как различимость самого стегоконтейнера человеком, потому как в качестве стегоконтейнера выступает интеллектуальная собственность, направленная на конечного потребителя, так и различимость ЦВЗ стегодетекто-

ром, который может подтвердить или опровергнуть авторские права на интеллектуальную собственность. В связи с этим в стегосистемах ЦВЗ применяется помехоустойчивое кодирование и метод широкополосного сигнала.

Одной из основных характеристик ЦВЗ является надежность. Под надежность понимается устойчивость к различным деформациям контейнера. По отношению к этой характеристики ЦВЗ распадается на три класса:

а) Хрупкие. Такие ЦВЗ разрушается при небольших модификациях заполненного стегоконтейнера. Такие ЦВЗ применяются для аутентификации сигнала. Например, такие ЦВЗ используются для подтверждения подлинности цифрового объекта.

б) Полухрупкие. Такие ЦВЗ чувствительны к некоторым преобразованиям контейнера и нечувствительны к другим. Например, ЦВЗ, встроенное в изображение, может быть нечувствительно к его компрессии, но в то же время быть чувствительно к вырезке из этого изображения фрагмента.

в) Робастные или надежные. Такие ЦВЗ устойчивы к разным видам воздействия на контейнер. Такие ЦВЗ часто применяются при защите от копирования.

Чтобы осуществить вложение ЦВЗ в стегоконтейнер, ЦВЗ преобразуют к более удобному виду. Например, если ЦВЗ является изображением, то удобно будет представить его как двумерную битовую матрицу. Так же если ЦВЗ является изображением, разумно будет использовать не само изображение, а его Вайвлет преобразование или дискретное косинусное преобразование. Изображения обладают большой визуальной избыточностью. Данные преобразования концентрируют большую часть энергии (визуальной информации) в нижних частотах. Поэтому их можно использовать как низкочастотные фильтры. То же самое относится и к контейнерам.

Похожим на ЦВЗ, но отличающимся понятием является цифровой отпечаток. ЦВЗ предполагает встраивание одного и того же сообщения в различные контейнеры. В случае же цифрового отпечатка в каждый контейнер встраивается уникальное сообщение. Часто областью применения цифровых отпечатков становится защита исключительного права. В каче-

стве сообщения в таком случае встраивается информация, указывающая на идентифицирующие данные покупателя. Эти данные позволяют отследить источник распространения, если произойдет утечка стегоконтейнера.

1.3 Обобщенные стеганографические методы

К настоящему моменту разработано множество стеганографических методов скрытия информации. Для их систематичного изучения удобно группировать их по схожим признакам.

а) Пространственные методы. Особенностью этих методов является сокрытие информации напрямую в пространственной области контейнера. Например, в случае звукового контейнера таким пространством могут быть семплы, а в случае изображения — пиксели.

б) Частотные методы. Такие методы сначала используют одно из интегральных преобразований сигнала, чтобы перейти в его частотную область. Далее кодирование сообщение производится за счет изменения частотных характеристик сигнала. После этого используется обратное преобразование, чтобы получить модифицированный сигнал, содержащий закодированное сообщение.

в) Алгоритмы, использующие особенности формата файла. Такие алгоритмы как правило записывают сообщение в метаданные файла или в иные неиспользуемые поля файла.

1.4 Стегоанализ

Стегоанализ — это наука о выявлении сообщений, скрытых методами стеганографии. Задача стегоанализа — выявить подозрительные контейнеры, определить, есть ли в них скрытое сообщение, и, если возможно, восстановить это сообщение.

Если в случае криptoанализа аналитик начинает работу сразу с зашифрованным сообщением, то в случае стегоанализа аналитик начинает работу с множества подозрительных файлов, о которых как правило мало что известно. Деятельность аналитика в таком случае начинается с сокра-

щения этого множества файлов до подмножества, в котором файлы скорее всего были заполнены сообщением.

Самой простым методом стегоанализа является субъективная атака. Атака заключается в попытке “на глаз” определить, содержит тот или иной контейнер стего. Несмотря на свою простоту, атака часто применяется на начальном этапе стегоанализа системы.

Основной техникой, используемой в стегоанализе, является статистический анализ. Сначала множество незаполненных контейнеров одного типа анализируется для получения различной статистики. Затем эта статистика используется при классификации контейнера как заполненного или пустого. При такой классификации могут быть использованы самые различные наблюдения:

а) Сокрытие информации может приводить к изменению статистической структуры контейнера, в результате чего соседние элементы контейнера становятся попарно ближе друг к другу. На этом основана атака хи-квадрат.

б) Сокрытие информации увеличивает энтропию контейнера. В результате чего он хуже поддается сжатию. На этом основана атака с помощью алгоритмов сжатия.

в) Различные статистические данные контейнера и его областей можно использовать как вектор признаков. Собрав большой датасет таких признаковых описаний объектов стего, на нем можно обучить нейросеть, которая будет классифицировать изображения.

2 Сокрытия методом наименее значимого бита

2.1 Общие сведения

LSB (least significant bit) — стеганографический метод сокрытия информации, основанный на замене последних значащих бит элементов контейнера битами сообщения. Этот метод использует тот факт, что уровень детализации во многих контейнерах гораздо выше того, что может воспринять и различить человек. Следовательно, заполненный контейнер будет неотличим от оригинального для человеческого восприятия. В качестве примера можно взять полутоновое изображение с градациями серого. Цвет кодируется одним байтом. Человеческий глаз воспринимает только первые 7 бит, а самый младший бит вносит там мало информации, что человек не сможет заметить разницу.

LSB обладает следующими достоинствами:

- а) Простота реализации и эффективность.
- б) Низкая вычислительная сложность.
- в) Пустой и заполненный контейнер неразличимы для органов восприятия человека

И недостатками:

- а) Метод применим лишь к контейнерам, которые хранят данные без сжатия или используют сжатие без потерь, так как информация, закодированная в наименее значимых битах, может быть потеряна в процессе сжатия.
- б) Небольшие трансформации контейнера приводят к невозможности восстановить сообщение. Например, если сообщение скрыто в изображении методом LSB, то небольшие линейные трансформации (вращение, движение, отражение, гомотетия, сжатие, растяжение) уничтожают сообщение. Так же сообщение разрушается в результате сжатия с потерями. Все это говорит о том, что метод обладает низкой робастостью.
- в) Факт сокрытия изображения легко обнаруживает методами стеганализа.

Ввиду перечисленных выше недостатков очевидной кажется недопустимость использования данного методы для сокрытия ЦВЗ.

2.2 Алгоритм

Перейдем к конкретным реализациям этого метода. Алгоритм 1 демонстрирует псевдокод сокрытия методом LSB.

Алгоритм 1: LSB Кодирование

Data: Контейнер, Сообщение

Result: Заполненный стегоконтейнер

$N \leftarrow$ Длина сообщения в битах;

$Message \leftarrow$ Бинарное представление сообщения;

$Container \leftarrow$ Массив с элементами контейнера;

for $i = 1, 2, \dots, N$ **do**

if $Container[i] \equiv Message[i] \pmod{2}$ **then**

continue;

else

$Container[i] \leftarrow (Container[i] \wedge \neg 1) \vee Message[i];$

Алгоритм 2: LSB Декодирование

Data: Заполненный контейнер

Result: Сообщение в бинарном представлении

$Message \leftarrow$ Пустой список;

$Container \leftarrow$ Массив с элементами контейнера;

$N \leftarrow$ Длина $Container$;

for $i = 1, 2, \dots, N$ **do**

if $Container[i] \equiv 0 \pmod{2}$ **then**

$Message.append(0);$

else

$Message.append(1);$

Как видно, сначала сообщение преобразуется в бинарный вид, а затем кодируется в элементах контейнера за счет изменения четности младшего бита. Логические операции в данном случае соответствуют бинарным операциям на компьютере. В итоге последние биты элементов контейнера в точности повторяют сообщение. Так же можно заметить, что

единственная часть алгоритма, зависящая от контейнера — это выделение массива элементов из контейнера. Алгоритм 2 показывает, как декодировать сообщение из заполненного стегоконтейнера.

Реализуем этот алгоритм в виде класса на Python. Как уже было сказано, существенная часть алгоритма не зависит от контейнера, поэтому целесообразно реализовать алгоритм как абстрактный класс, от которого будут наследоваться реализации для конкретных контейнеров. Реализация приведена в листинге 2.1.

Листинг 2.1 — Абстрактный класс LSB

```
1 import numpy as np
2 from abc import ABC, abstractmethod
3 from bitarray import bitarray
4
5
6 class LSB(ABC):
7     def __init__(self, container, message: bytes = None) -> None:
8         """
9             Возвращает простой lsb кодер,
10            принимает на вход контейнер и сообщение массив( байт).
11            """
12
13     if message is None:
14         # По умолчанию сообщение пустое
15         self.message = []
16     else:
17         self.message = message
18
19     self._container = container
20
21     def encode(self) -> None:
22         """
23             Кодирует сообщение в контейнер.
24             """
25
26     # Получаем последовательность элементов контейнера
27     elements = self._to_elements()
28
29     # Преобразуем сообщение к бинарному виду
30     np_message = np.unpackbits(np.frombuffer(
31         self.message, dtype=np.uint8)).ravel()
32
33     # Меняем наименее значимый бит так,
34     # чтобы он кодировал биты сообщения
35     elements[:n] = (elements[:n] & ~1) | np_message
36
37     # Из элементов собираем контейнер обратно
38     self._from_elements(elements)
```

```

35
36     def decode(self) -> bytes:
37         """
38             Декодирует сообщение из контейнера.
39         """
40
41         # Получаем последовательность элементов контейнера
42         elements = self._to_elements()
43
44         # Выбираем размер сообщения так, чтобы он был кратен размеру байта
45         size = len(elements) // 8 * 8
46
47         # Сообщение считываем из наименее значащих бит элементов контейнера
48         np_message = (elements[:size] & 1)
49
50         # Преобразуем битовую последовательность в байты
51         message = np.packbits(np_message.reshape(-1, 8), axis=-1).tobytes()
52         return message
53
54
55     @abstractmethod
56     def _to_elements(self) -> np.array:
57         """
58             Преобразует контейнер в последовательность элементов.
59         """
60
61         pass
62
63     @abstractmethod
64     def _from_elements(self, elements: np.array) -> None:
65         """
66             Собирает контейнер из элементов.
67         """
68
69         pass

```

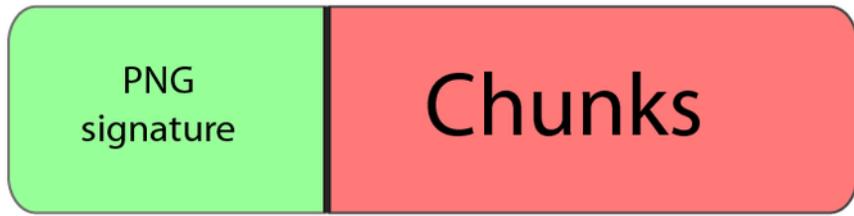
Как видно, в методах нет циклов **for**. Они скрыты за интерфейсом библиотеки `numtr`. Интерфейс библиотеки `numtr` позволяет нам применять операции к матрицам, из-за чего код выглядит лаконичнее. К тому же библиотека написана на языке C, поэтому ее код работает очень быстро.

Напишем реализацию LSB для PNG. Прежде чем реализовать метод LSB для PNG-контейнера, имеет смысл кратко изложить формат данных PNG.

2.3 Формат файла PNG

В самом общем виде PNG файл представляет из себя сигнатуру, за которой следует последовательность блоков, как показано на рисунке 2.1

Рисунок 2.1 — Общий вид формата PNG



Сигнатурой PNG файла состоит из 8 байт, в hex нотации они выглядят так: **89 50 4E 47 0D 0A 1A 0A**.

Каждый блок состоит из четырех секций: длина, тип, содержание, CRC, — как показано на рисунке 2.2: В длине указывается длина блока в

Рисунок 2.2 — Общий вид чанка

Length (длина)	Тип (имя) чанка	Содержание чанка	CRC
4 байта	4 байта	<i>Length</i> байт	4 байта

байтах. Тип указывается с помощью четырех ascii символов, чувствительных к регистру. С помощью регистра декодеру передает дополнительная информация, а именно:

- Регистр первого символа сообщает, является данный блок критическим или нет. Критические блоки распознаются каждым декодером. Если декодер не может распознать тип такого блока, он аварийно завершает работу.
- Регистр второго символа задает публичность или приватность блока. Публичные блоки обычно официальные и хорошо задокументированы. Чтобы закодировать в библиотека какую-то специфичную информацию, его тип можно изменить на приватный.
- Регистр третьего символа зарезервирован на будущее. По умолчанию там стоит символ в большом регистре.

г) Регистр четвертого символа сообщает возможность копирования данного блока редакторами.

Список критических блоков:

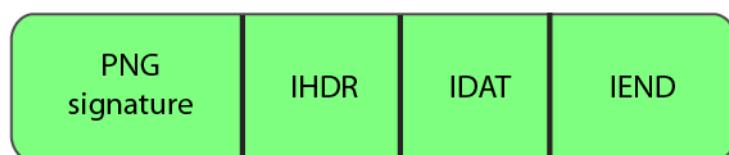
- а) IHDR — заголовочный блок, содержащий основную информацию об изображении.
- б) PLTE — палитра изображения.
- в) IDAT — содержит непосредственно изображение. В любом PNG файле должно быть не менее одного такого блока.
- г) IEND — завершающих чанк. Должен находиться в самом конце файла.

Список некритических блоков:

- а) bKGD — блок, задающий фоновый цвет изображения.
- б) cHRM — блок, используемый для задания цветового пространства CIE 1931.
- в) gAMA — определяет гамму.
- г) hIST — хранит гистограмму изображения либо общее содержания каждого цвета в рисунке.
- д) iTXT — содержит текст в UTF-8
- е) pHYs — содержит размер пикселя или отношение сторон изображения.
- ж) sRGB — свидетельствует об использовании sRGB схемы.
- и) tIME — дата последнего изменения изображения.
- к) tRNS — информация о прозрачности.

Согласно вышесказанному, минимальный PNG файл выглядит так, как показано на рисунке 2.3

Рисунок 2.3 — Минимальный PNG



В следующей секции представлены данные блока. В секции CRC записан CRC блока.

Наиболее интересными для нас являются блоки с типами IHDR и IDAT. IHDR — заголовочный блок, который является обязательным для PNG файла. Он содержит следующие интересующие нас поля:

- а) Ширина изображения в пикселях.
- б) Высота изображения в пикселях.
- в) Битовая глубина, задающее количество бит на каждый сэмпл.
- г) Тип цвета. Возможны следующие значения:
 - 1) Градация серого
 - 2) RGB
 - 3) Индексы из палитры
 - 4) Градация серого и альфа-канал
 - 5) RGB и альфа-канал

Блок IDAT содержит сжатые данные изображения. На данный момент поддерживается только сжатие по алгоритму deflate.

2.4 Реализация LSB для контейнера PNG

PNG изображение представимо в виде матрицы, элементами которой являются пиксели. В случае RGB каждый пикセル представляет элементы из трех каналов, каждый из каналов в отдельности может рассматриваться как градация серого. В случае градации серого каждый пикセル просто представлен значением от 0 до 255. Чтобы закодировать сообщение в эту матрицу, склеим ее строки друг с другом в одну большую строку, равно как и склеим каналы, чтобы они образовали последовательность элементов. Именно это делает метод `_to_elements`. Такой метод одинаково хорошо подходит и для разных типов цвета: RGB, RGB и альфа-канала, градации серого, градации серого и альфа-канала. Чтобы из элементов получить двумерную RGB матрицу, проделаем обратную операцию, что и делает метод `_from_elements`.

В функции `main` используем как сообщение книгу “Алиса в стране чудес” в оригинале. Считаем файл с книгой как последовательность байт и закодируем в изображение с помощью LSB. Далее выполним декодиро-

вание и сверим полученные данные. Исходный код представлен в листинге 2.2.

Листинг 2.2 — реализация LSB для PNG

```
1 import numpy as np
2 from lsb import LSB
3 from PIL import Image
4
5
6 class PNG(LSB):
7     """
8     Реализация алгоритма LSB для файлов формата PNG.
9     """
10
11     def __init__(self, file_name: str, message: bytes = None) -> None:
12         """
13         Возвращает простой PNG кодер,
14         принимает на вход имя файла и сообщение.
15         """
16         self._file_name = file_name
17         container = np.array(Image.open(file_name))
18         super().__init__(container, message)
19
20     def _to_elements(self) -> np.array:
21         """
22         Возвращает представление контейнера
23         как последовательности элементов.
24         """
25         return self._container.ravel()
26
27     def _from_elements(self, elements: np.array) -> None:
28         """
29         Строит контейнер по последовательности
30         элементов.
31         """
32         self._container.ravel()[:] = elements
33
34     def save(self) -> None:
35         """
36         Перезаписывает исходный файл
37         новым контейнером.
38         """
39         image = Image.fromarray(self._container)
40         image.save(self._file_name)
41
42     def save_as(self, file_name: str) -> None:
```

```

43     """
44     Сохраняет контейнер в файл,
45     заданный параметром file_name.
46     """
47     image = Image.fromarray(self._container)
48     image.save(file_name)
49
50
51 def main() -> None:
52     # Считываем сообщение.
53     with open("Messages/Alice in wonderland.txt", "rb") as f:
54         message = f.read()
55
56     # Запоминаем длину сообщения.
57     size = len(message)
58     # Кодируем сообщение.
59     png = PNG("Images/Lenna.png", message)
60     png.encode()
61     png.save_as("Images/LSB_Lenna.png")
62     # Переоткрываем изображение.
63     png = PNG("Images/LSB_Lenna.png")
64     # Декодируем сообщение.
65     decoded = png.decode()
66
67     # Проверяем, что сообщения до и после совпадают.
68     new_message = decoded[:size]
69     print(f"{new_message == message}")
70
71
72 if __name__ == "__main__":
73     main()

```

Сравнение изображение до и после заполнения контейнера методом LSB приведено на рисунке 2.4. Как видно, два рисунка визуально неотличимы, хотя в одном из них закодировано 150 килобайт информации.



(a) Оригинал



(b) После применения LSB

Рисунок 2.4 — Изображение до и после применения LSB

3 Сокрытие в спектральной области

3.1 Дискретное косинусное преобразование

Дискретное косинусное преобразование (ДКП) — одно из дискретных преобразований Фурье. ДКП представляет конечную последовательность в виде суммы функций косинуса, колеблющихся на разных частотах. ДКП широко используется при обработке сигналов и сжатии данных. Например, ДКП используется при сжатии в изображениях (JPEG, HEIF), аудиофайлах (Dolby Digital, MP3), видеофайлах (MPEG, H.26x), в цифровом телевидении (SDTV, HDTV, VOD) и в других.

ДКП является линейным ортогональным преобразованием. Как любое дискретное линейное преобразование, ДКП можно представить в виде матрицы. Будучи ортоганальным преобразованием, обратное к ДКП преобразование задает транспонированной матрицей ДКП, домноженной на какой-то коэффициент.

Использование косинусных, а не синусоидальных функций имеет решающее значение для сжатия, поскольку для аппроксимации типичного сигнала требуется меньше косинусных функций. ДКП подобно дискретному преобразованию Фурье, но использующее только действительные числа.

Существует 8 стандартных типов ДКП, однако наиболее употребимым является второй тип, который часто называют просто ДКП (DCT-II). Формула дискретного косинусного преобразования выглядит так, как показано в формуле 3.1:

$$X_k = \sum_{n=0}^{N-1} x_n \cos \left[\frac{\pi}{N} \left(n + \frac{1}{2} \right) k \right] \quad k = 0, \dots, N - 1 \quad (3.1)$$

Формула для матрицы преобразования выглядит как формуле 3.2:

$$DCT-2_n = \left[\cos \left(k \left(l + \frac{1}{2} \right) \frac{\pi}{n} \right) \right]_{0 \leqslant k, l < n} \quad (3.2)$$

Как и в случае быстрого преобразования Фурье, существуют алгоритмы быстрого ДКП преобразования.

DCT-II часто используется для сжатия с потерями благодаря своему свойству уплотнения энергии: в типичных случаях большая часть инфор-

мации, которую содержит сигнал, концентрируется в нескольких первых коэффициентах разложения.

Существуют так же многомерные ДКП, которые получаются из одномерных путем композиции ДКП по каждому измерению. Вывод такого преобразования для двумерного случая показан в формуле 3.3.

$$\begin{aligned} X_{k_1, k_2} &= \sum_{n_1=0}^{N_1-1} \left(\sum_{n_2=0}^{N_2-1} x_{n_1, n_2} \cos \left[\frac{\pi}{N_2} \left(n_2 + \frac{1}{2} \right) k_2 \right] \right) \cos \left[\frac{\pi}{N_1} \left(n_1 + \frac{1}{2} \right) k_1 \right] \\ &= \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1, n_2} \cos \left[\frac{\pi}{N_1} \left(n_1 + \frac{1}{2} \right) k_1 \right] \cos \left[\frac{\pi}{N_2} \left(n_2 + \frac{1}{2} \right) k_2 \right] \end{aligned} \quad (3.3)$$

Здесь $[x_{n_1, n_2}]$ — матрица до преобразования, и $[X_{k_1, k_2}]$ — матрица после преобразования. В матричном виде это преобразование может быть представлено так, как показано в формуле 3.4, где x — матрица, которую нужно преобразовать.

$$X = (DCT\text{-}2_n)x(DCT\text{-}2_n^T) \quad (3.4)$$

Именно такое преобразование используется при компрессии в JPEG.

3.2 JPEG

JPEG является широко используемым методом сжатия с потерями для цифровых изображений. Степень сжатия регулируется, что позволяет выбирать между качеством и размером изображения. JPEG наиболее широко используемый стандарт сжатия изображений в мире и наиболее используемый формат цифровых изображений.

ДКП лежит в основе сжатия методом JPEG. Как уже говорилось выше, ДКП был выбран именно благодаря свойству уплотнения энергии. Чтобы прояснить, о чём идет речь, мной была сделана визуализация преобразования ДКП.

Выберем на изображении область 32x32 пикселя, как показано на рисунке 3.1.

Сначала рассмотрим матрицу пикселей как двумерную дискретную функцию. Расположим координаты так, чтобы в левом верхнем углу рас-



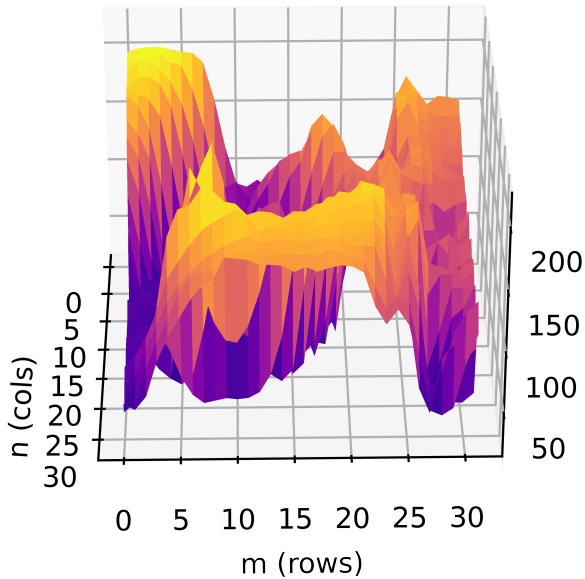
Рисунок 3.1 — Выбираем область

полагался пиксель с координатами p_{kj} , $k = 0, j = 0$. Визуализацию можно посмотреть на рисунке 3.2.

Умножим эту функцию справа на транспонированную матрицу ДКП по формуле 3.4. Мы получим новую функцию, которая показана на рисунке 3.3. Таким образом фактически ДКП применилось к каждой строке матрицы. Из изображения видно, что наибольшие коэффициенты расположены в нижней части спектра, то есть ближе к нулевому столбцу.

К полученной матрице применим ДКП еще раз, в этот раз по столбцам. В полученной матрице наибольшее значение имеет коэффициент с координатами $k = 0, j = 0$. Этот коэффициент называется DC-коэффициент. Остальные коэффициенты называются AC-коэффициентами. Матрица показана на рисунке 3.4.

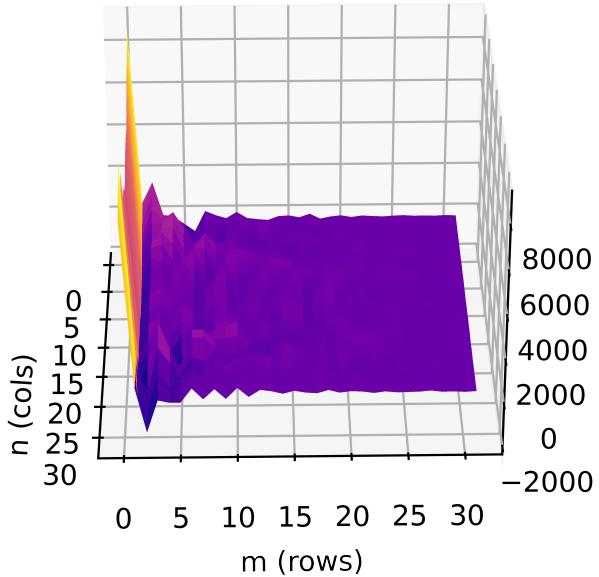
Рисунок 3.2 — Визуализация пикселей



DC-коэффициент блока равен среднему всех пикселей в блоке, взято-му с определенным коэффициентом. Удаляя все коэффициенты, кроме DC, мы можем аппроксимировать блок пикселей их средним арифметическим. Чем дальше коэффициент располагается от DC, тем меньше психовизуаль-ной информации он несет для человека, и тем более незаметные детали изображения он хранит в себе. Соответственно, основная идея алгоритма состоит в отбрасывании наименее значимых коэффициентов. Это позволяет производить сжатие изображения с потерями.

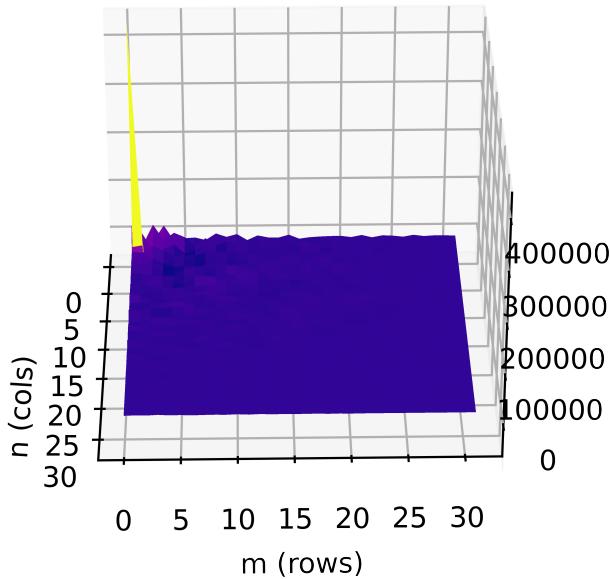
Алгоритм сжатия JPEG работает с каждым каналом отдельно, поэто-му для простоты рассмотрим работу JPEG на изображении в режиме града-ции серого. В самом начале своей работы алгоритм разбивает изображение на блоки 8x8 пикселей. К каждому блоку применяется ДКП преобразова-ние, что равносильно разложению исходной матрицы по базису, состояще-му из 64 функций. Эти 64 функции показаны на рисунке 3.5. Из этого рисунка видно, что помере отдаления от левого верхнего которая функции становятся все более рельефными, что объясняет, почему они несут наи-

Рисунок 3.3 — После применения ДКП к строкам матрицы



более мелкие детали изображения. Так же видно, что функция, соответствующая DC-коэффициенту, представлена плоскостью. Очевидно, что лучшим константным приближением функции является ее математическое ожидание. После применения ДКП преобразования к блоку матрице 8×8 получается другая матрица той же размерности. В соответствии с вышесказанным эта матрица делится на области низких, средних и высоких частот. В таком порядке убывает информативность коэффициентов. Это можно увидеть на рисунке 3.6. Далее коэффициенты полученной ДКП матрицы квантуются. Квантование происходит с применением специальных мат-

Рисунок 3.4 — После применения ДКП к столбцам матрицы

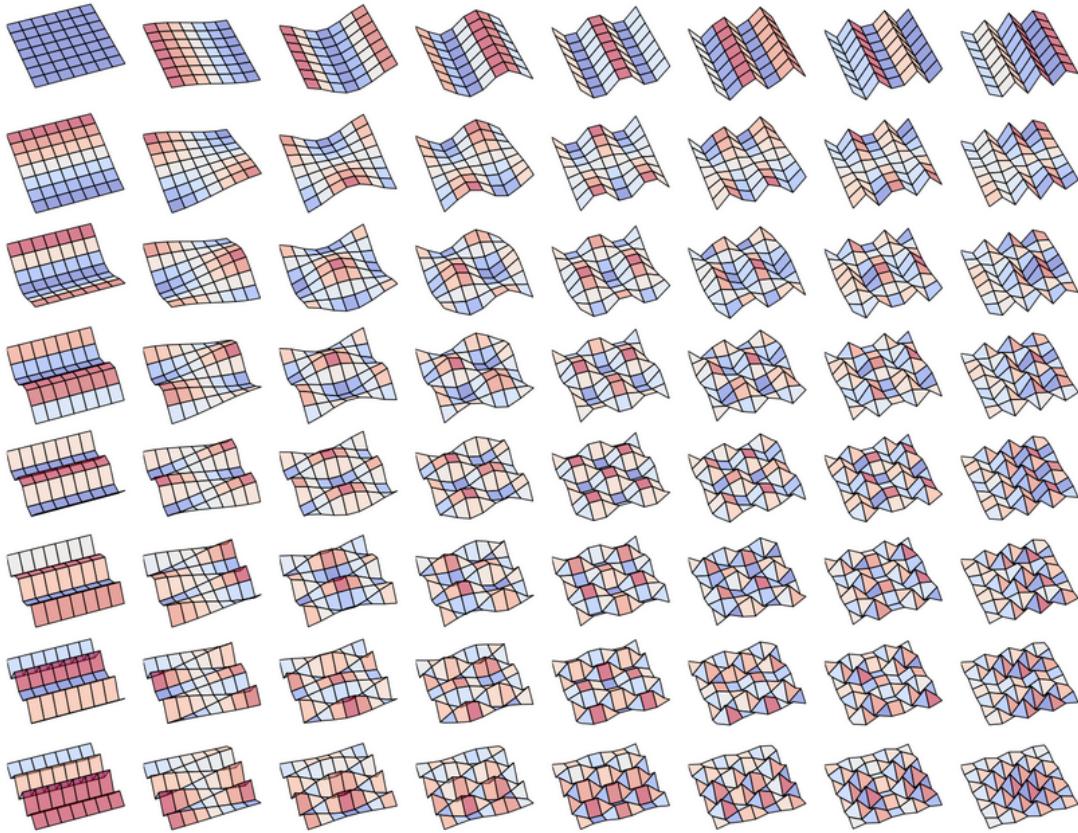


риц, одна из таких матриц представлена в формуле 3.5.

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}. \quad (3.5)$$

Это матрица для 50% качества, указанная в исходном стандарте JPEG. Каждый элемент ДКП матрицы делится на коэффициент матрицы квантования, стоящий в той же позиции. После этого результат округляется. В результате этой операции обычно бывает так, что многие высокочастотные компоненты округляются до нуля, а многие из остальных становятся небольшими положительными или отрицательными числами, для представления которых требуется гораздо меньше бит.

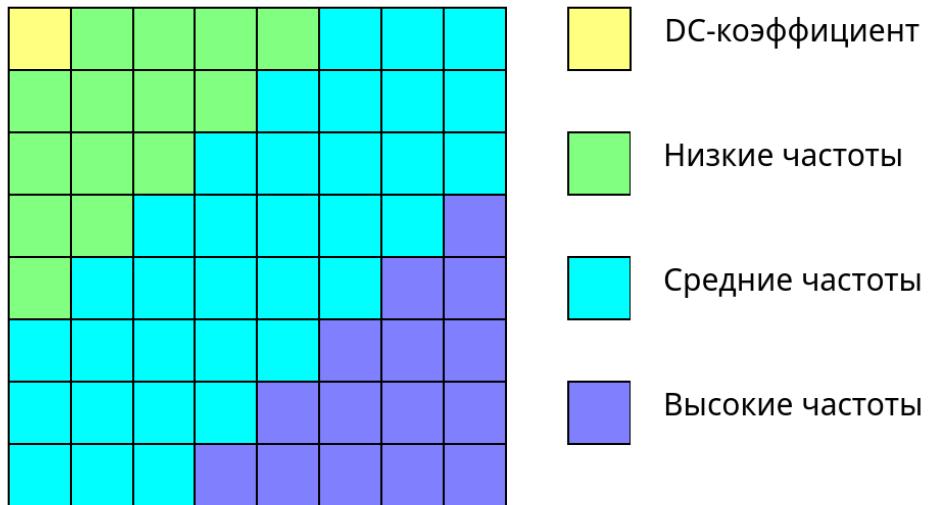
Рисунок 3.5 — Базис ДКП



При декодировании происходит обратный процесс — матрица квантованных коэффициентов почленное умножается на матрицу квантования, но из-за того, что до этого значения были округлены, они восстанавливаются с некоторой погрешностью. Чем больше коэффициент квантования, тем выше будет эта погрешность.

После квантования коэффициенты записываются в специальном зигзагообразном порядке, показанном на рисунке 3.7. Таким образом коэффициенты упорядочиваются от низких частот к высоким. После этого DC и AC коэффициенты кодируются отдельно. Поскольку в изображениях часто встречаются градиентные области, то DC коэффициенты соседних блоков скорелированы, поэтому первым этапом их кодирования становится дифференциальная импульсно-кодовая модуляция (ДИКМ). То есть кодируются не сами коэффициенты, а разница между двумя соседними коэффициентами. AC коэффициенты кодируются с помощью кодирования длин серий (КДС). То есть повторяющиеся символы заменяются на сим-

Рисунок 3.6 — Частотные области ДКП



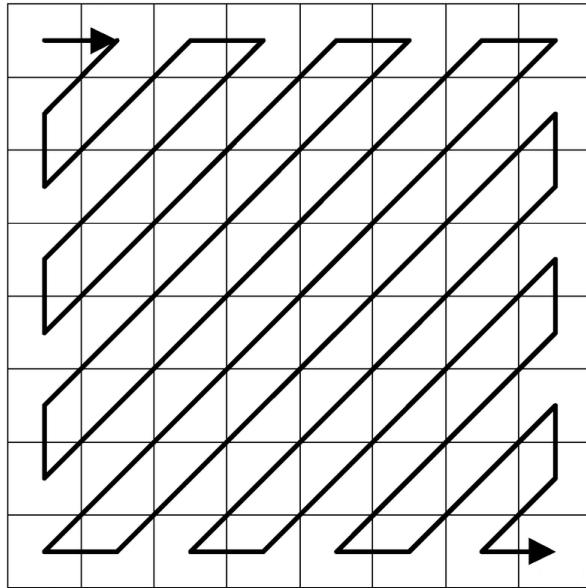
вов и количество его повторов. После этого к DC и AC коэффициентам применяется энтропийное кодирование с помощью алгоритма Хаффмана.

Мы разобрали работу алгоритма для одноканального изображения. В RGB изображениях такой алгоритм применяется к каждому каналу отдельно. Так же часто кодированию предшествует дополнительный этап, на котором RGB преобразуется в цветовое пространство $Y\text{C}_\text{B}\text{C}_\text{R}$. Дело в том, что человеческий глаз более чувствителен к перепадам яркости, чем к перепаду цвета. В $Y\text{C}_\text{B}\text{C}_\text{R}$ первый канал Y отвечает за яркость, C_B и C_R отвечают за синюю и красную компоненты. После преобразования в $Y\text{C}_\text{B}\text{C}_\text{R}$ над C_B и C_R производится субдискретизация: каналы разбиваются на небольшие блоки и значения пикселей в этих блоках усредняются. Таким образом разрешение в этих каналах понижается еще сильнее и изображение сжимается еще сильнее. Вся схема алгоритма представлена на рисунке 3.8

3.3 JSteg

JSteg — стеганографический алгоритм, работающий с JPEG файлами. JSteg во многом опирается на работу кодировщика JPEG. Алгоритмы кодирования и декодирования JPEG абсолютно симметричны. JSteg вмешивается в работу декодировщика, а именно прерывает его на этапе умножения ДКП коэффициентов на матрицу квантования. После этого JSteg записывает в упорядоченные зигзагообразным образом ДКП коэффициенты

Рисунок 3.7 — Зигзагообразный порядок



кодируемую информацию методом LSB. После этого вызывается кодировщик, который записывает измененные ДКП коэффициенты обратно в JPEG изображение.

Рассмотрим достоинства и недостатки этого метода. К достоинствам можно отнести следующее:

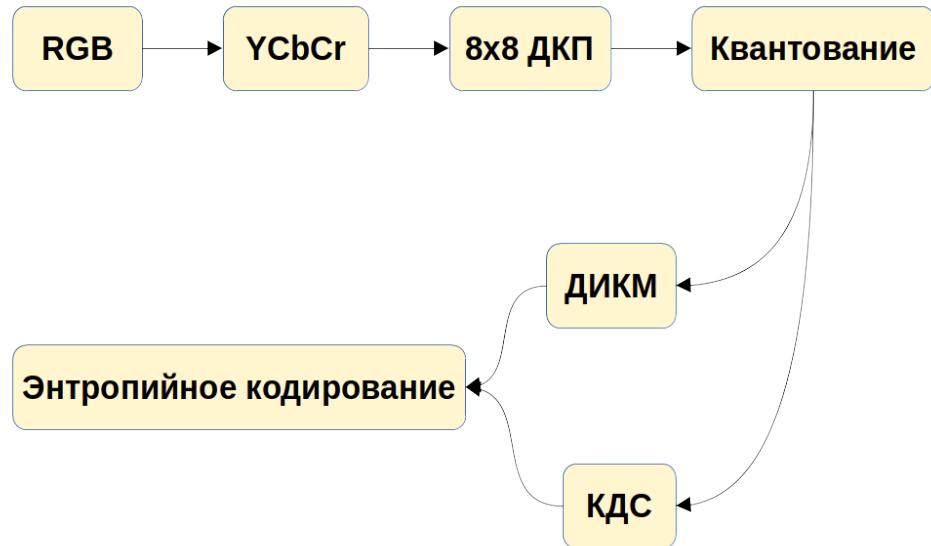
- а) Низкая вычислительная сложность.
- б) Алгоритм обеспечивает большую вместимость стегосообщений: стегосообщение может занимать до 13% объема контейнера.
- в) Изменения, вносимые в контейнер, незаметны для человеческого глаза.

Но у метода так же есть и существенные недостатки:

а) Метод неустойчив к квантованию ДКП коэффициентов. Как уже говорилось ранее, операция квантования восстанавливает и сохраняет коэффициент с некоторой погрешностью, поэтому если открыть в редакторе стегоконтейнер, в котором содержится сообщение, закодированное методом JSteg, то после пересохранения этого файла сообщение полностью уничтожится.

б) Из предыдущих соображения становится ясно, что метод не устойчив к сжатию. Это так же обусловлено еще и тем, что при сжатии коэффициенты квантования увеличиваются, а значит часть ДКП коэффициентов

Рисунок 3.8 – Схематичное изображение JPEG



обнулится, а у другой части погрешность восстановления станет еще больше.

Рассмотрим реализацию метода на Python. Код приведен в листинге 3.1. По сути метод представляет собой LSB, только вместо пространственной области используется спектральная. В данном случае наименее значимый бит меняется у коэффициентов ДКП изображения, упорядоченных зигзагообразным способом.

Листинг 3.1 — Реализация JSteg

```
1 import jpegio as jio
2 import numpy as np
3 import cv2
4 from lsb import LSB
5
6
7 class JSteg(LSB):
8     """
9         Реализация стеганографического алгоритма JSteg.
10    """
11
12    def __init__(self, file_name: str, message: str = None) -> None:
13        """
14            Возвращает простой JSteg кодер,
15            принимает на вход имя файла и сообщение.
```

```

16     """
17     self.file_name = file_name
18     # Считываем все коэффициенты ДКП
19     self.dct = jio.read(self.file_name)
20     # Оставляем только  $C_b$  канал.
21     # Коэффициенты упорядочены в зигзагообразном порядке
22     container = self.dct.coef_arrays[1]
23     super().__init__(container, message)
24
25     def _to_elements(self) -> np.array:
26         """
27             Возвращает представление контейнера
28             как последовательности элементов.
29         """
30
31         return self.container.ravel()[:]
32
33     def _from_elements(self, elements: np.array) -> None:
34         """
35             Строит контейнер по последовательности
36             элементов.
37         """
38
39         self.dct.coef_arrays[1].ravel()[:] = elements
40
41     def save(self) -> None:
42         """
43             Перезаписывает исходный файл
44             новый контейнером.
45         """
46
47         jio.write(self.dct, self.file_name)
48
49     def save_as(self, file_name: str) -> None:
50         """
51             Сохраняет контейнер в файл,
52             заданный параметром file_name.
53         """
54
55         jio.write(self.dct, file_name)
56
57     def main() -> None:
58         """
59             Проверяет работоспособность программы.
60         """
61
62         # Считываем сообщение.
63         with open("Messages/Alice in wonderland.txt", "rb") as f:
64             message = f.read()[:80000]

```

```

62     # Запоминаем длину сообщения.
63     size = len(message)
64     # Кодируем сообщение.
65     jsteg = JSteg("Images/Lenna.jpg", message)
66     jsteg.encode()
67     jsteg.save_as("Images/JSteg_Lenna.jpg")
68     # Переоткрываем изображение.
69     jsteg = JSteg("Images/JSteg_Lenna.jpg")
70     # Декодируем сообщение.
71     decoded = jsteg.decode()
72
73     # Проверяем, что сообщения до и после совпадают.
74     new_message = decoded[:size].decode()
75     print(f"new_message == message.decode() {new_message == message.decode()}")
76
77
78 if __name__ == "__main__":
79     main()

```

3.4 Метод относительной замены величин коэффициентов ДКП

Этот метод использует идеи, схожие с методами расширения спектра, а именно: вместо того, чтобы кодировать 1 бит информации в одном коэффициенте ДКП, метод предлагает кодировать 1 бит информации за счет нескольких коэффициентов ДКП. Этого можно добиться, кодируя информацию за счет изменения разности между набором различных коэффициентов ДКП.

Алгоритм Коха-Жао использует 2 коэффициента ДКП. Формальное описание приводится в алгоритме 3. Алгоритм декодирования строится симметрично. Это простейший метод из данного семейства. К достоинствам метода можно отнести то, что он устойчив к квантованию ДКП-коэффициентов и сжатию. Особенno если применять его в паре с помехоустойчивым кодированием. Но у метода так же есть и серьезные недостатки:

- Метод вносит заметные искажения в контейнер.
- Метод легко детектируется.

Модифицированной версией этого метода является метод Бенгама-Мемона-Эо-Юнга. Модификации подверглись два направления:

Алгоритм 3: Алгоритм Коха-Жао

Data: Контейнер, Сообщение

Result: Заполненный стегоконтейнер

$N \leftarrow$ Длина сообщения в битах;

$Message \leftarrow$ Бинарное представление сообщения;

$DCT-blocks \leftarrow$ Массив из блоков ДКП контейнера;

$k, l \leftarrow$ Позиция коэффициента ДКП из низкой полосы частот;

for $i = 1, 2, \dots, N$ **do**

if $Message[i] = 0$ **then**

 Сделать $|DCT-blocks[i][k][l] - DCT-blocks[i][k][l]| < 25$;

else

 Сделать $|DCT-blocks[i][k][l] - DCT-blocks[i][k][l]| > 25$;

$Container \leftarrow$ Новый контейнер, полученный из обратного

преобразования ДКП-блоков;

- a) Встраивание происходит только в наиболее подходящие ДКП-блоки.
- б) Используются не 2, а 3 коэффициента ДКП. Это существенно снижает вносимые в контейнер искажения.
 - . Рассмотрим каждую модификацию в отдельности.

Наиболее подходящие коэффициенты выбираются по следующим признакам:

- а) Блок не должен иметь слишком резких переходов яркости.
- б) Блок не должен быть слишком монотонным.

Для оценки этих параметров вводится два коэффициента: P_L и P_H . Превышение первого коэффициента или недостижение второго будет указывать на то, что блок не пригоден для встраивания. Для получения первой оценки нужно просуммировать модуляция низкочастотных коэффициентов, а для получения второй оценки нужно просуммировать модули высокочастотных коэффициентов.

Само встраивание происходит в два этапа. На первом этапе выбираются три коэффициента из низкой полосы частот. Для обеспечения большой стойкости они могут выбираться псевдослучайно. На втором этапе ко-

эффициенты модифицируются. Если кодируется 0, то третий коэффициент должен стать больше первых двух, а если 1, то третий коэффициент должен стать меньше, соответственно. Декодирование происходит симметричным образом. Реализацию метода на Python можно найти в приложении А.

4 Стегоанализ

4.1 Методы стегоанализа

Основными методами, применяемыми в стегоанализе, являются визуальные методы и статистические методы.

Субъективная атака проста по своей сути: аналитик пытается “на глаз” определить, содержит ли контейнер стего. Однако эта атака может применяться в различных вариациях. Например, анализу может подвергаться не само изображение, а какой-то его канал, или же изображение, полученное из данного отбрасыванием нескольких старших бит.

Статистические методы основаны на использовании различных статистик изображения и том факте, что эти статистики могут различаться для пустого и заполненного стегоконтейнера.

4.2 Субъективная атака LSB

Метод LSB является легко обнаружимым. Для начала рассмотрим самую простую ситуацию: допустим, что сообщение, скрытое в стего, не зашифровано. В таком случае стегоконтейнер поддается визуальной атаке, а именно: попробуем посмотреть на визуальное представление последнего бита сообщения. Для этого используем код, представленный в листинге 4.1.

Листинг 4.1 — Визуализация LSB

```
1 import numpy as np
2 import cv2
3
4 # Читаем синий канал оригинала
5 blue_original = cv2.imread("Images/Lenna.png", 0)
6 # Читаем синий канал модифицированного сообщения
7 blue_stego = cv2.imread("Images/LSB_Lenna.png", 0)
8
9 # Получим только последний бит.
10 # Для контрастности умножим полученное значение на 255,
11 # таким образом в матрицу будут лишь значения 0 и 255.
12 bw_original = (blue_original & 1) * 255
13 bw_stego = (blue_stego & 1) * 255
14
15 # Сохраним полученные изображения в градации серого.
```

```
16 | cv2.imwrite("Images/BW_Lenna.png", bw_original)
17 | cv2.imwrite("Images/BW_LSB_Lenna.png", bw_stego)
```

Полученные изображения можно увидеть на рисунке 4.1. Как видно, наименее значащий бит оригинального изображения распределен шумоподобно, в то время как у стегоконтейнера этот бит вносит в изображение какую-то структуру. Так происходит из-за неравномерного распределения символов в исходном сообщении. Так же из изображения можно увидеть примерную длину сообщения.

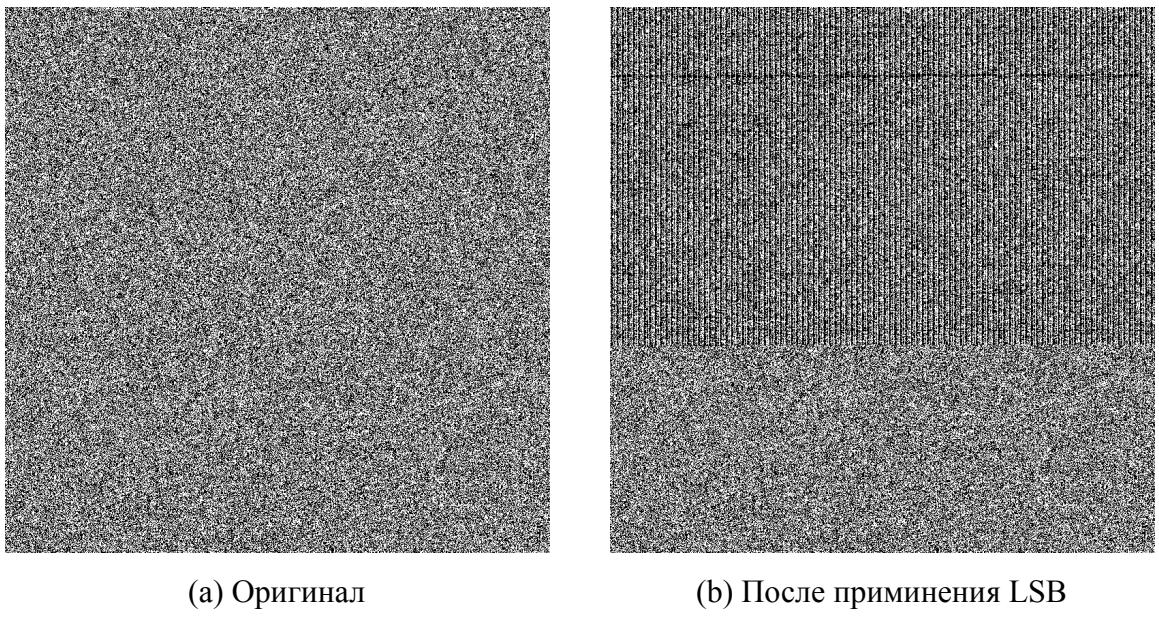


Рисунок 4.1 — Наименее значащий бит до и после LSB

4.3 Атака оценки числа переходов значений младших бит в соседних элементах контейнера

Допустим, что стегосообщение предварительно было зашифровано и скрыто методом LSB. В таком случае сообщение внутри контейнера будет обладать предельной энтропией, а это значит, что наименее значимый бит контейнера будет распределен равномерно: 50% объема будет занимать 0 и другие 50% будет занимать 1. При этом два соседних наименее значимых бита не будут скорелированы. Однако в реальных изображениях это не так. В реальном изображении соседние пиксели скореллированы, и ненулевая вероятность того, что они окажутся одинаковыми. Несмотря на то, что изображение 4.1а выглядит как шум, в нем есть некоторая

статистическая структура. Чтобы выявить ее, нужно попарно сравнить 2 соседних пикселя и посчитать, какой процент этих пикселей совпал. Такое сравнение проводит в листинге 4.2.

Листинг 4.2 — Корреляция LSB

```
1 import numpy as np
2 import cv2
3
4
5 def pretty_stat(X: np.array, name: str) -> None:
6     """
7         Печатает функцию распределения данной дискретной выборки.
8     """
9     size = len(X)
10    # Посчитаем частоты элементов последовательности
11    comparison = dict(zip(*np.unique(X, return_counts=True)))
12    # Выведем статистику на экран
13    stat = f'{name}: '
14
15    for key, value in comparison.items():
16        stat += f"P({key}) = {value / size:.2}, "
17
18    if len(comparison) == 0:
19        print(stat + "empty")
20
21    else:
22        print(stat[:-2])
23
24
25 def main() -> None:
26     """
27         Считает корреляцию НЗБ у изображения,
28         заполненного шумоподобным сообщением,
29         и оригинального изображения.
30     """
31
32     # Считаем синий канал оригинала.
33     blue_original = cv2.imread("Images/Lenna.png", 0)
34
35     # Получим только последний бит.
36     bin_original = (blue_original & 1)
37
38     # Преобразуем матрицу бит в массив бит.
39     bin_original = bin_original.ravel()[:]
40
41     # Для сравнения сгенерируем псевдослучайную
42     # равномерно распределенную последовательность
```

```

42     # бит, чтобы смоделировать стегосообщение.
43     bin_stego = np.random.randint(2, size=len(bin_original))
44
45     # Сравним 2 соседних бита у оригинального изображения
46     # и промоделированного.
47     original_comparison = (bin_original[1:] == bin_original[:-1])
48     stego_comparison = (bin_stego[1:] == bin_stego[:-1])
49
50     # Посмотрим на получившееся распределение
51     pretty_stat(original_comparison, "Original")
52     pretty_stat(stego_comparison, "Stego")
53
54
55 if __name__ == "__main__":
56     main()

```

Вывод программы следующий: “Original: $P(\text{False}) = 0.46$, $P(\text{True}) = 0.54$; Stego: $P(\text{False})=0.5$, $P(\text{True})=0.5$ ”. Как видно, у оригинального сообщения совпадение и несовпадение двух соседних наименее значимых битов не равновероятны.

4.4 Атака хи-квадрат

Допустим, что мы оказались в похожей ситуации: зашифрованное сообщение было скрыто методом LSB, — но в этот раз в контейнере соседние элементы не скорелированы. Построим гистограмму элементов контейнера и рассмотрим элементы, отличающиеся друг от друга в младшем бите. Если это незаполненный стегоконтейнер, то частота двух соседних элементов a и b может сильно отличаться. Однако если к такому контейнеру применить LSB, то в паре двух соседних значений a в 50% случаев не изменится, и в 50% случаев изменится на единицу. То же самое произойдет и с b . Допустим, что a был четным. Тогда в новом распределении частота a будет равна $\frac{f(a) + f(b)}{2}$, где f — функция распределения частот в незаполненном контейнере. То же самое касается и b . То есть соседние элементы будут распределены одинаково. На этом и основана атака хи-квадрат.

Критерий согласия Пирсона (критерий согласия χ^2) — это критерий принадлежности наблюдаемой выборки x_1, x_2, \dots, x_3 теоретическому закону распределения $F(x, \theta)$, где θ — это известный параметр распреде-

ления. Процедура проверки гипотез с использованием критерия χ^2 предусматривает группирование наблюдений. Область определения случайной величины разбивают на k непересекающихся интервалов граничными точками $x_{(0)}, x_{(1)}, \dots, x_{(k)}$. В соответствии с заданным разбиением подсчитывают число n_i выборочных значений, попавших в i -й интервал, и вероятности попадания в интервал $P_i(\theta) = F(x_{(i)}, \theta) - F(x_{(i-1)}, \theta)$ соответствующие теоретическому закону с функцией распределения $F(x, \theta)$. При этом $n = \sum_{i=1}^k n_i$ и $\sum_{i=1}^k P_i(\theta) = 1$. В основе критерия согласия Пирсона лежит измерение отклонений $\frac{n_i}{n}$ от $P_i(\theta)$. Статистика критерия согласия χ^2 Пирсона определяется соотношением 4.1.

$$\chi^2 = n \sum_{i=1}^k \frac{(n_i/n - P_i(\theta))^2}{P_i(\theta)} \quad (4.1)$$

Выделим из изображения все пары элементов, которые отличаются только в младшем бите. Обозначим такие пары через $(2m, 2m + 1)$. Пусть h_i обозначает гистограмму наблюдаемого распределения элементов. Введем новое наблюдаемое распределение $\{o_m\}$ равное $o_m = h_{2m}$ и теоретическое распределение $\{e_m\}$ равное $e_m = \frac{h_{2m} + h_{2m+1}}{2}$. Разница между этими двумя распределениями измеряется критерием 4.2 с $(\nu - 1)$ степенями свободы, где ν — количество пар, отличающихся в младшем бите.

$$\chi^2 = \sum_{e_m \neq 0} \frac{(o_m - e_m)^2}{e_m} \quad (4.2)$$

Степень сходства двух распределений $\{o_m\}$ и $\{e_m\}$ после этого считается с помощью функции распределения по формуле 4.3.

$$p = 1 - \int_0^{\chi^2} \frac{t^{(\nu-2)/2} e^{-t/2}}{2^\nu \Gamma(\nu/2)} dt \quad (4.3)$$

Реализация атаки на python представлена в листинге 4.3.

Листинг 4.3 — Атака хи-квадрат

```

1 from enum import unique
2 import jpegio as jio
3 import scipy.stats
4 import numpy as np
5
```

```

6
7 def chi_attack(file_name: str) -> None:
8     """
9     Реализует атаку хиквадрат- на JPEG файл.
10    """
11    # Считываем ДКП коэффициенты
12    dct = jio.read(file_name)
13    # Выбираем синий канал, в который спрятано сообщение.
14    # Здесь важно, что сообщение представляет собой шум.
15    container = dct.coef_arrays[1].ravel()[:]
16    # Строим гистограмму
17    unique, counts = np.unique(container, return_counts=True)
18    hist = dict(zip(unique, counts))
19    # Ищем соседние пары
20    unique.sort()
21    pairs = [(x, y) for (x, y) in zip(unique[:-1], unique[1:]) if x ^ y ==
22    1]
23    # Строим наблюдаемое и ожидаемое распределения
24    observed = [hist[x] for (x, _) in pairs]
25    expected = [(hist[x] + hist[y]) / 2 for (x, y) in pairs]
26    # Считаем степень сходства
27    _, p = scipy.stats.chisquare(observed, f_exp=expected)
28    print(f"{p:.2}")
29
30
31 def main() -> None:
32     """
33     Проверяет работоспособность программы.
34     """
35     chi_attack("Images/Lenna.jpg")
36     # Заполненный шумом стегоконтейнер
37     chi_attack("Images/JSteg_Lenna.jpg")
38
39
40 if __name__ == "__main__":
41     main()

```

Программа выводит 0.0 для пустого контейнера и 0.99 для заполненного.

4.5 Методы противодействия

Для эффективного противодействия описанным статистическим и субъективным атакам рекомендуется пользоваться следующими рекомендациями при построении стеганографического алгоритма:

- a) Сообщение должно встраиваться в зашифрованном виде для предотвращения субъективных и иных атак.
- б) Сообщение должно встраиваться не в подряд идущие элементы контейнера, а в случайно выбранные элементы, например, с использованием генератора псевдослучайных чисел.
- в) Сообщение должно заполнять лишь малую часть емкости контейнера. Иначе оно может нарушить статистическую структуру контейнера. Так, например, атака хи-квадрат работает намного хуже, когда сообщение рассеяно по всей длине контейнера.

5 Экономическая оценка проекта

5.1 Постановка задачи

Целью дипломного проекта является анализ стеганографических методов защиты информации. Данный раздел содержит расчет трудоемкость и затрат на проведение анализа предметной области, разработки и сопровождения стеганографической системы.

5.2 Оценка стоимости объектов интеллектуальной собственности

Оценка стоимости объектов интеллектуальной собственности (ОИС), созданных на предприятии или по его заказу (при финансировании разработок предприятием) с закреплением за ним по договору прав собственности на них, производится по затратному методу и определяется по формуле 5.1:

$$C_i = C_p + C_n + C_m \quad (5.1)$$

где,

- а) C_p — приведенные затраты на создание объектов интеллектуальной собственности, руб.;
- б) C_n — привиденные затраты на правовую охрану объектов интеллектуальной собственности, руб.;
- в) C_m — привиденные затраты на маркетинговые исследования ОИС, руб.

Приведенные затраты на создание ОИС — сумма фактически произведенных затрат на выполнение научно-исследовательской работы (НИР) в полном объеме (от поиска материалов исследования до формирования отчета) и разработку всей технической документации. Приведенные затраты для НИР состоят из затрат на поисковые работы, включая предварительную проработку проблемы, на теоретические исследования, на проведение экспериментов, испытаний, на услуги сторонних организаций, на составление, рассмотрение и утверждение отчета и прочих затрат.

Приведенные затраты на разработку технической документации (ТД) состоят из затрат на выполнение эскизного проекта, технического задания, рабочего проекта, расчетов, испытаний, услуг сторонних организа-

ций, авторского надзора, дизайна. Кроме того, сюда включаются затраты на доведение ОИС до готовности промышленного использования и коммерческой реализации.

В тех случаях, когда НИР или технологическая и проектная документация выполняется частично или созданию ОИС предшествует проведение только НИР или разработка технической документации, то расчет стоимости ОИС производится по затратам на фактически выполненные работы, для товарных знаков и промышленных образцов — затратам на дизайн.

Приведенные затраты на правовую охрану ОИС — затраты на оформление заявочных материалов на получение патента (свидетельства), переписка по заявке, оплата пошлин за проведение экспертизы, получение патента (свидетельства) и поддержание его в силе и т.д. Данная составляющая отсутствует для таких ОИС, как ноу-хай, НИР, ТД.

Приведенные затраты на маркетинговые исследования — для целей приведения разновременных стоимостных оценок к конечному году применяется коэффициент α_i , но данном случае он будет равен 1, потому что число лет, предшествующих расчетному году равно 0. Затраты, произведенные на выполнение НИР и разработку всех стадий ТД, то есть Ср могут включать в себя:

- а) израсходованные материальные ресурсы;
- б) оплата труда с отчислениями разработчиков;
- в) амортизационные отчисления оборудования, которое использовалось при разработке ОИС;
- г) аренда помещения для разработчиков;

Кроме того, создание любого ОИС или разработка программного обеспечения происходит не всегда согласно производственного задания, где четко оговорены сроки работы. Разработчик может вне плановых заданий выполнить(изготовить) ОИС или написать программу для ЭВМ. В случае если отсутствует документация по затратам на создание ОИС, то их можно определить расчетным путем.

Затраты на создание ОИС в t -том году определяются по следующей формуле:

$$C_{\text{пр}} = \frac{3}{m} Kt \quad (5.2)$$

Где,

- а) 3 — среднемесячная заработка разработчика (разработчиков) с учетом районного коэффициента, руб.;
- б) m — среднее количество рабочих часов в месяце;
- в) K — коэффициент, учитывающий отчисления с заработной платы (страховые взносы). Ставка страховых взносов в 2021 г. составляет 30% от величины фонда оплаты труда. $K = 0,3$;
- г) t — время в часах, затрачиваемое разработчиком (разработчиками) на создание (разработку) ОИС, на отладку и адаптацию ОИС к условиям производства.

Для расчета себестоимости необходимы затраты времени. Весь перечень произведённых работ не был оговорен рамками технического задания с указанием конкретных сроков выполнения. Для обеспечения наибольшей достоверности временных затрат используем метод экспертных оценок. Время работы, согласно плану проведения аудита ИБ учтём в соответствующих этапах.

Для определения средних значений $a_{i \text{ср}}$, $m_{i \text{ср}}$, $b_{i \text{ср}}$ используются экспертные оценки, данные руководителем и автором проекта. Средние значения найдем по формуле 5.4. Значения m_i и b_i рассчитываются аналогично.

$$a_{i \text{ср}} = \frac{3a_{i \text{рук}} + 2a_{i \text{авт}}}{5} \quad (5.3)$$

где,

- а) $a_{i \text{рук}}$ — оценка, данная руководителем;
- б) $a_{i \text{авт}}$ — оценка, данная автором.

Таблица 5.1 — Затраты времени на разработку ОИС

Этапы	Величина затрат		
	Минимальная	Вероятная	Максимальная

	Руководитель	Автор	Средняя	Руководитель	Автор	Средняя	Руководитель	Автор	Средняя
Ознакомление с исходными данными	3	4	3.5	4	6	5	5	7	6
Анализ предметной области	9	17	13	13	25	18	25	41	33
Разработка системы	179	210	190	250	310	280	330	410	370
Вывод в эксплуатацию	9	17	13	17	31	24	25	41	33

Ожидаемая величина затрат для i -го этапа (MO_i) и стандартное отклонение этой величины каждого i -го этапа (G_i):

$$MO_i = \frac{\alpha_i + 4m_i + b_i}{6} \quad (5.4)$$

$$G_i = \frac{b_i - a_i}{6} \quad (5.5)$$

Результаты показаны в таблице 5.2

Таблица 5.2 — Затраты времени на разработку ОИС

Этапы разработки ОИС	Средняя величина затрат времени этапа разработки ОИС			MO_i	G_i
	a_i	m_i	b_i		
Ознакомление с исходными данными	3.5	5	6	4.9	0.4
Анализ предметной области	13	18	33	19.6	3.3
Разработка системы	190	280	370	280	30
Вывод системы в опытную эксплуатацию	13	24	33	23.6	3.3

Зная ожидаемые затраты и стандартное отклонение по каждому этапу, рассчитываются эти показатели в целом по ОИС:

$$MO = \sum_{i=1}^n MO_i \quad (5.6)$$

$$G = \sqrt{\sum_{i=1}^n G_i^2} \quad (5.7)$$

$$MO = 4.9 + 19.6 + 280 + 23.6 = 328.1$$

$$G = \sqrt{0.4^2 + 3.3^2 + 30^2 + 3.3^2} = 30.4$$

5.3 Оценка стоимости разработки

Необходимо определить себестоимость разработки системы. Стоимость разработки ОИС найдём по формуле 5.2 при следующих данных:

- а) среднемесячная заработка разработчика с учетом коэффициента составляет 90 000 руб.;
- б) среднее количество рабочих часов в месяце — 168;
- в) затраты времени на разработку ОИС: $328.1 + 30 = 358.1$ часа.

$$C = \frac{90000}{168} * 358.1 = 191839.3$$

Прочие расходы:

- а) Ставка страховых взносов в 2021 г. составляет 30% от величины фонда оплаты труда. В нашем примере они составят: Страховые взносы = $9000 * 0.3 = 27000$

Общие затраты на разработку составят:

$$Z = Z_{\text{прям}} + Z_{\text{пр}} = 191839.3 + 27000 = 218839.3$$

5.4 Оценка стоимости использования оборудования и сопровождения системы

Для развертывания системы будет использоваться выделенный сервер. Траты для сервера с конфигурацией: четырехядерный процессор с

восьмью потоками, 16 гигабайт оперативной памяти, 1 терабайт SSD — 6 000 рублей/месяц. Сопровождением системы займется системный администратор. По формуле выше найдем затраты на сотрудника при учете месячного оклада 40 000 рублей:

$$C = 40000 + 40000 * 0.3 = 52000 \text{ руб.}$$

Суммарные среднемесячные затраты на систему составляют 58000 рублей.

5.5 Экономическое обоснование проекта

Стоимость разработки проекта составляет 218 839.3 рублей. Анализ показал, что данная система позволит сократить убытки компании от несанкционированного копирования и распространения цифровых объектов в 2 раза. В среднем компания теряет 240 000 рублей в месяц из-за несанкционированного копирования и распространения цифровых объектов компании. Рассчитаем, сколько проект приносит прибыли в месяц:

$$P = \frac{240000}{2} - 52000 = 68000$$

где P — это прибыль. Итого срок окупаемости проекта составляет три месяца.

ЗАКЛЮЧЕНИЕ

После проделанной работы можно подвести следующие итоги:

- а) были описаны общие сведения о стеганографических методах сокрытия информации;
- б) был описан алгоритм сокрытия информации методом наименее значимого бита;
- в) была написана реализация алгоритм сокрытия информации методом наименее значимого бита с использования языка программирования Python;
- г) был проведен анализ разобранного алгоритма, найдены и продемонстрированы его уязвимости;
- д) были описаны и проанализированы алгоритмы сокрытия в спектральной области;
- е) был проведен анализ алгоритмов сокрытия в спектральной области, найдены и продемонстрированы их уязвимости;
- ж) была написана реализация алгоритмов сокрытия в спектральной области на языке Python;
- и) были реализованы атаки на описанные алгоритмы;
- к) были приведены рекомендации по защите от реализованных атак.

Из высказанного можно сделать вывод о том, что мной успешно были рассмотрены основные стеганографические алгоритмы, определены области их применения, разобраны их недостатки и достоинства. Я научился проводить анализ стеганографических алгоритмов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Конахович, Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — МК-Пресс, 2006.
2. *Грибунин, В. Г.* Цифровая стеганография / В. Г. Грибунин, И. В. Тцирнцев, И. Н. Оков. — Солон-пресс, 2020.
3. *Национальная электронная библиотека им. Н.Э. Баумана. Стеганография.* — <https://ru.bmstu.wiki/Стеганография>. — 2021.

ПРИЛОЖЕНИЕ А

РЕАЛИЗАЦИЯ МЕТОДА БЕНГАМА-МЕМОНА-ЭО-ЮНГА НА

PYTHON

```
1 import numpy as np
2 import jpegio as jio
3 import random
4
5
6 class DCT():
7     """
8     Реализация метода БенгамаМемонаЭоЮнга---.
9     """
10
11     def __init__(self, file_name: str, message: bytes = None, seed: int =
0) -> None:
12         """
13         Принимает на вход путь до файла с изображением file_path,
14         байтовое сообщение message и попрождающий элемент seed,
15         используемый для инициализации ГПСЧ. Возвращает простой
16         в использовании JPEG кодер.
17         """
18
19         self._file_name = file_name
20         # Считываем ДКП коэффициенты
21         self._dct = jio.read(self._file_name)
22         # Считываем канал яркости.
23         self._container = self._dct.coef_arrays[0]
24
25         if message is None:
26             self.message = []
27         else:
28             self.message = message
29
30         # Сохраняем seed
31         self.seed = seed
32         # Коэффициенты для встраивания
33         self._stego_coef = [(i, j) for i in range(8) for j in range(8)
34                             if i + j < 5 and (i, j) != (0, 0)]
35
36         # Высокочастотные коэффициенты
37         self._high_coef = np.array(
38             [i + j > 9 for i in range(8) for j in range(8)])
39             ).reshape(8, 8)
40
41         # Низкочастотные коэффициенты
42         self._low_coef = np.array(
```

```

42         [ i + j < 5 for i in range(8) for j in range(8) ]
43     ) . reshape(8, 8)
44
45     # Сохраняем порог различения
46     self._P = 3
47     # Сохраняем порог яркости
48     self._Pl = 210
49     # Сохраняем порог монотонности
50     self._Ph = 40
51
52 def _is_suitable_block(self, block: np.array) -> bool:
53     # Проверяем блок на порог яркости и монотонности
54     l = np.absolute(block[ self._low_coef ].sum())
55     h = np.absolute(block[ self._high_coef ].sum())
56     # return True
57     return l >= self._Pl and h <= self._Ph
58
59 def _encode_block(self, block: np.array, bit: bool) -> np.array:
60     """
61     В данном блоке block кодирует bit за счет
62     изменения соотношения между тремя псевдослучайными
63     элементами.
64     """
65     # С помощью ГПСЧ выбираем случайные элементы блока
66     k1, k2, k3 = random.sample(self._stego_coef, 3)
67
68     # Кодируем ноль, устанавливая block[k3] минимальным
69     # из трех элементов так, чтобы это соотношение
70     # сохранилось после квантования коэффициентов
71     if bit == False:
72         m = min(block[k1], block[k2])
73         block[k3] = m - self._P / 2
74
75         if block[k1] == m:
76             block[k1] += self._P / 2
77         else:
78             block[k2] += self._P / 2
79
80     # Кодируем единицу, устанавливая block[k3] максимальным
81     # из трех элементов так, чтобы это соотношение
82     # сохранилось после квантования коэффициентов
83     else:
84         m = max(block[k1], block[k2])
85         block[k3] = m + self._P / 2
86
87         if block[k1] == m:

```

```

88         block[k1] -= self._P / 2
89     else:
90         block[k2] -= self._P / 2
91
92     return block
93
94 def _decode_block(self, block: np.array) -> bool:
95     """
96     Для данного блока block декодирует
97     bit, закодированный с помощью соотношения
98     между тремя псевдослучайными элементами
99     """
100    # С помощью ГПСЧ выбираем случайные элементы блока
101    k1, k2, k3 = random.sample(self._stego_coef, 3)
102
103    # Находим максимум разницы между третьим
104    # и двумя остальными элементами
105    M = max(block[k1], block[k2], block[k3])
106
107    if block[k3] == M:
108        return True
109
110    else:
111        return False
112
113 def _blockshaped(self, arr: np.array, nrows: int, ncols: int) ->
114     np.array:
115     """
116     Возвращает массив формы  $(n, \text{nrows}, \text{ncols})$ , где
117      $n * \text{nrows} * \text{ncols} = \text{arr.size}$ 
118
119     Если массив – это матрица, тогда возвращает массив,
120     выглядящий как разбиение этой матрицы на подматрицы.
121     """
122     h, w = arr.shape
123     return (arr.reshape(h // nrows, nrows, -1, ncols)
124             .swapaxes(1, 2)
125             .reshape(-1, nrows, ncols))
126
127 def _unblockshaped(self, arr: np.array, h: int, w: int) -> np.array:
128     """
129     Возвращает матрицу формы  $(h, w)$ , где
130      $h * w = \text{arr.size}$ 
131
132     Если матрица формы  $(n, \text{nrows}, \text{ncols})$ , где  $n$  – это подматрицы
133     формы  $(\text{nrows}, \text{ncols})$ , тогда возвращает матрицу, составленную

```

```

133     из этих подматриц.
134
135     """
136     n, nrows, ncols = arr.shape
137     return (arr.reshape(h//nrows, -1, nrows, ncols)
138             .swapaxes(1, 2)
139             .reshape(h, w))
140
141     def encode(self) -> bytes:
142
143         """
144         Кодирует сообщение в контейнер и возвращает позиции подходящих блоков.
145         """
146
147         # Инициализируем ГПСЧ
148         random.seed(self.seed)
149
150         # Разбиваем массив ДКП коэффициентов на блоки
151         blocks = self._blockshaped(self._container, 8, 8)
152
153         # Находим положение подходящих блоков
154         mask = np.array([self._is_suitable_block(block) for block in
155                         blocks])
156
157         # В подходящих блоках меняем соотношения коэффициентов
158         suitable_blocks = blocks[mask]
159
160         # Преобразуем сообщение в бинарный вид
161         np_message = np.unpackbits(np.frombuffer(
162             self.message, dtype=np.uint8)).ravel()
163
164         # Находим длину сообщения
165         n = len(np_message)
166
167         # Кодируем сообщение
168         encoded_blocks = []
169
170         for i in range(n):
171             encoded_blocks.append(self._encode_block(
172                 suitable_blocks[i], np_message[i]))
173
174         # Перезаписываем подходящие блоки
175         suitable_blocks[:n] = np.array(encoded_blocks)
176         blocks[mask] = suitable_blocks
177
178         # Соединяем блоки обратно в контейнер
179         self._container = self._unblockshaped(blocks,
180                                              *self._container.shape)
181
182         # Сохраняем информацию в изображение
183         self._dct.coef_arrays[0].ravel()[:] = self._container.ravel()
184
185         # Возвращаем позиции встраивания
186         return np.packbits(mask).tobytes()
187
188     def decode(self, positions: bytes) -> bytes:
189
190         """
191         Декодирует сообщение из контейнера

```

```

177     """
178     # Инициализируем ГПСЧ
179     random.seed(self.seed)
180     # Разбиваем массив ДКП коэффициентов на блоки
181     blocks = self._blockshaped(self._container, 8, 8)
182     message = []
183     # Находим позиции подходящих блоков
184     mask = np.unpackbits(np.frombuffer(positions,
185                          np.uint8)).astype(bool)
186     # Находим подходящие блоки
187     suitable_blocks = blocks[mask[:len(blocks)]]]
188
189     # Декодируем сообщение
190     for block in suitable_blocks:
191         # Декодируем бит
192         bit = self._decode_block(block)
193         message.append(bit)
194
195     # Из бит собираем исходное сообщение
196     message = np.packbits(message)
197     # Преобразуем его в байты
198     return message.tobytes()
199
200     def save(self) -> None:
201         """
202             Перезаписывает исходный файл
203             новый контейнером.
204         """
205         jio.write(self._dct, self._file_name)
206
207     def save_as(self, file_name: str) -> None:
208         """
209             Сохраняет контейнер в файл,
210             заданный параметром file_name.
211         """
212         jio.write(self._dct, file_name)
213
214     def main() -> None:
215         """
216             Проверяет работоспособность алгоритма.
217         """
218         message = ("Hello, stegoworld!").encode()
219         size = len(message)
220         jpg = DCT("Images/Lenna.jpg", message)
221         positions = jpg.encode()

```

```
222     jpg . save _as ( "Images /DCT_Lenna . jpg" )
223     jpg = DCT( "Images /DCT_Lenna . jpg" )
224     decoded = jpg . decode ( positions ) [ : size ]
225
226     print ( decoded )
227
228
229 if __name__ == "__main__":
230     main ()
```