**Федеральное государственное автономное образовательное учреждение**

**высшего образования   
«Национальный исследовательский университет   
«Высшая школа экономики»**

**Московский институт электроники и математики им. А.Н.Тихонова**

Направление подготовки

**«10.03.01 Информационная безопасность»**

Образовательная программа **«Информационная безопасность»**

**О Т Ч Е Т**

**о прохождении**

**учебной практики**

**Студент** Зиганшин А. М**.** БИБ212

(Фамилия И.О.) номер группы

**Руководитель практики студента:**

Младший научный сотрудник информационной

безопасности киберфизических систем

департамента электронной инженерии

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| МИЭМ НИУ ВШЭ |  | Мельман А.С. |  |  |
| должность и место работы |  | Фамилия И.О. |  | подпись |

**Руководитель практики от НИУ ВШЭ:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Зав. каф. информационной безопасности киберфизических систем департамента электронной инженерии МИЭМ НИУ ВШЭ |  | Евсютин О.О. |  |  |
| должность и место работы |  | Фамилия И.О. |  | подпись |

**Практика пройдена с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва, 2023**

**СОДЕРЖАНИЕ**

[1 Введение 3](#_Toc66214855)

[2 Краткая характеристика организации 4](#_Toc66214856)

[3 Описание профессиональных задач 5](#_Toc66214857)

[4 Исполненное индивидуальное задание 6](#_Toc66214858)

[5 Заключение 25](#_Toc66214859)

[6 Список использованных источников 26](#_Toc66214860)

# 1 Введение

Целью прохождения практики является закрепление, расширение и углубление полученных теоретических знаний и приобретение первоначальных практических навыков в решении конкретных проблем.

Задачи практики:

- закрепление и углубление теоретических знаний по прослушанным за время обучения в университете дисциплинам;

- формирование и совершенствование базовых профессиональных навыков и умений в области информационной безопасности;

- знакомство и отработка навыков работы с реальными исследовательскими, промышленными и образовательными проектами;

- формирование информационной компетентности с целью успешной работы в профессиональной деятельности;

- получение навыков самостоятельной работы, а также работы в составе коллектива;

- обработка полученных материалов и оформление отчета о прохождении практики.

# 2 Краткая характеристика организации

МИЭМ НИУ ВШЭ подготавливает экспертов в областях электроники, информационных технологий, связи, вычислительной техники, математики, кибернетики и дизайна.

Коллектив преподавателей МИЭМ включает 1 академика РАН, 4 членов-корреспондентов РАН и 34 лауреата государственных премий РФ. Университет поддерживает тесные связи с ведущими институтами отрасли, академиями наук и международными компаниями, такими как National Instruments, InfoWatch, Zyxel, QNAP, Altium Limited, а также обладает современным оборудованием в лабораториях по 3D-визуализации, лазерным технологиям, связи и кибербезопасности, что обеспечивает подготовку высококвалифицированных профессионалов.

МЭИМ НИУ ВШЭ располагает тремя лабораториями - учебной и двумя учебно-исследовательскими. Учебные лаборатории предназначены для занятий по физике, электронике и другим дисциплинам, а в учебно-исследовательских лабораториях студенты занимаются научными и проектными работами.

В МИЭМ НИУ ВШЭ представлены 5 программ бакалавриата и специалитета, стоимость которых варьируется от 420 до 540 тысяч рублей, а также 7 программ магистратуры со стоимостью обучения в 400 тысяч рублей.[1]

# 3 Описание профессиональных задач

В процессе учебной практики необходимо:

1. Изучить предложенную статью, содержащую описания необходимых алгоритмов.
2. Реализовать алгоритмы встраивания и извлечения водяного знака в частотную область изображения.
3. Провести эксперименты по анализу невидимости, надежности, емкости, производительности и безопасности встраивания водяного знака в изображение.
4. Оценить результаты экспериментов по предложенным метрикам.
5. Составить вывод по проделанной практике.

# 4 Исполненное индивидуальное задание

В качестве эффективного алгоритма встраивания водяного знака в изображение был предложен алгоритм, использующий преобразование Уолша-Адамара (WHT) и корреляцию между матричными коэффициентами в частотной области после преобразования. Сначала цветное изображение разделяется на каналы R, G и B, а каждый канал на блоки 4x4. Затем, исследуя коэффициенты частотной области блоков WHT, можно обнаружить сильную корреляцию между коэффициентами первой строки матрицы частотной области, особенно первого и второго элементов и третьего и четвертого элементов в первой строке. Водяной знак может быть встроен в матричный блок путем точной настройки упомянутых коэффициентов. Информация о водяном знаке может быть извлечена по разнице между двумя коэффициентами.[2]

**4.1 Функции, используемые в процессе встраивания с соответствующим кодом на языке Python**

**4.1.1 Генерация матрицы Адамара**

Обобщенное преобразование Фурье имеет различные вариации, одной из которых является WHT. Оно использует в качестве ядра матрицу Адамара, которая порождается функцией Адамара.

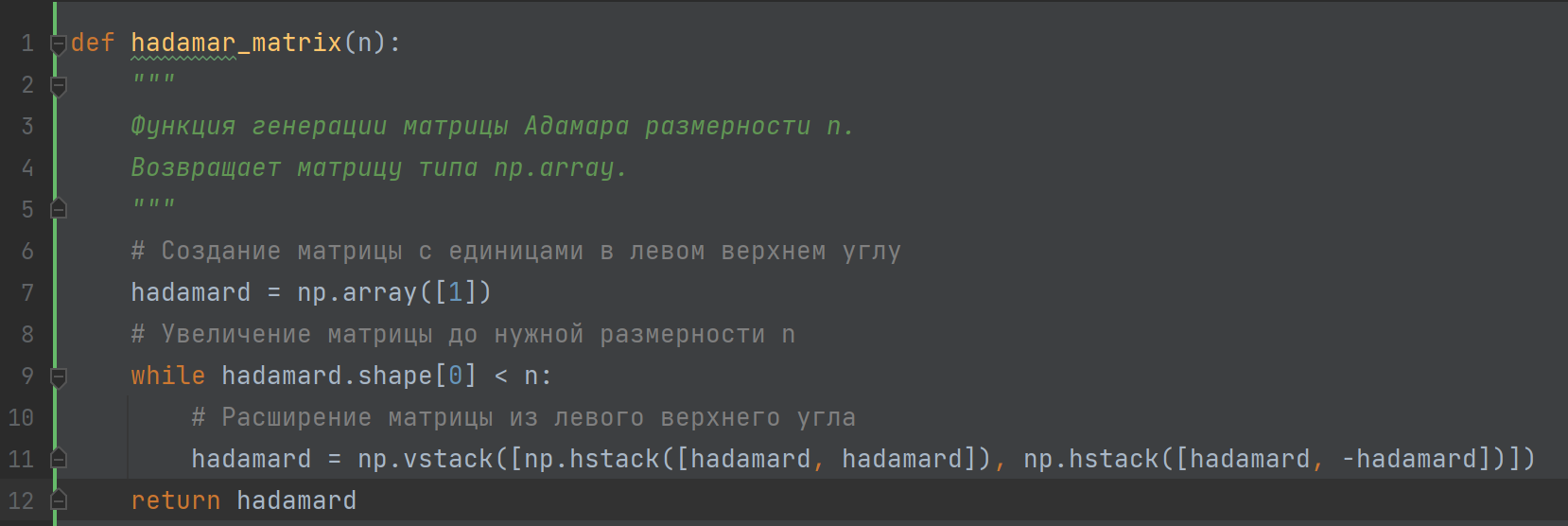


Рисунок 4.1 – функция генерации матрицы Адамара [3]

**4.1.2 Функция прямого и обратного преобразования Уолша-Адамара для двумерных матриц**

Двумерное преобразование Уолша-Адамара (2D-WHT) – это процесс, при котором происходит сосредоточение энергии двумерной матрицы в первой строке матрицы путем умножения на матрицу Адамара. Затем в эту строку встраивается информация.

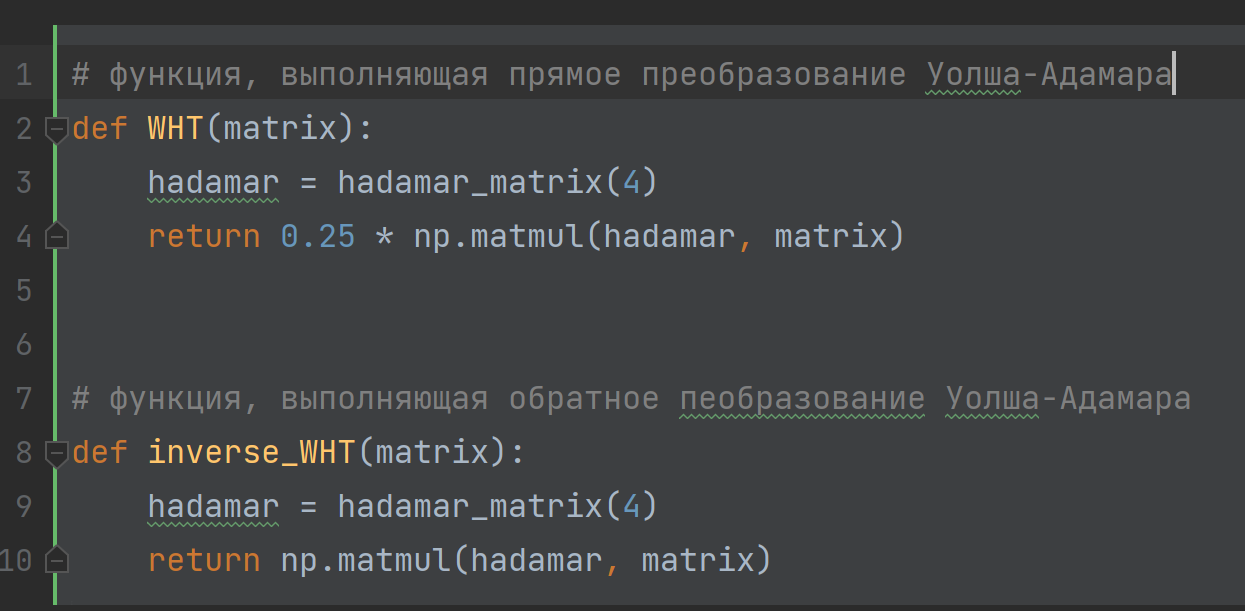


Рисунок 4.2 - Функция прямого и обратного преобразования Уолша-Адамара для двумерных матриц

**4.1.3 Функция, выполняющая преобразование Арнольда**

Преобразование Арнольда заключается в изменении координат пикселей изображения, для повышения безопасности встраивания водяного знака

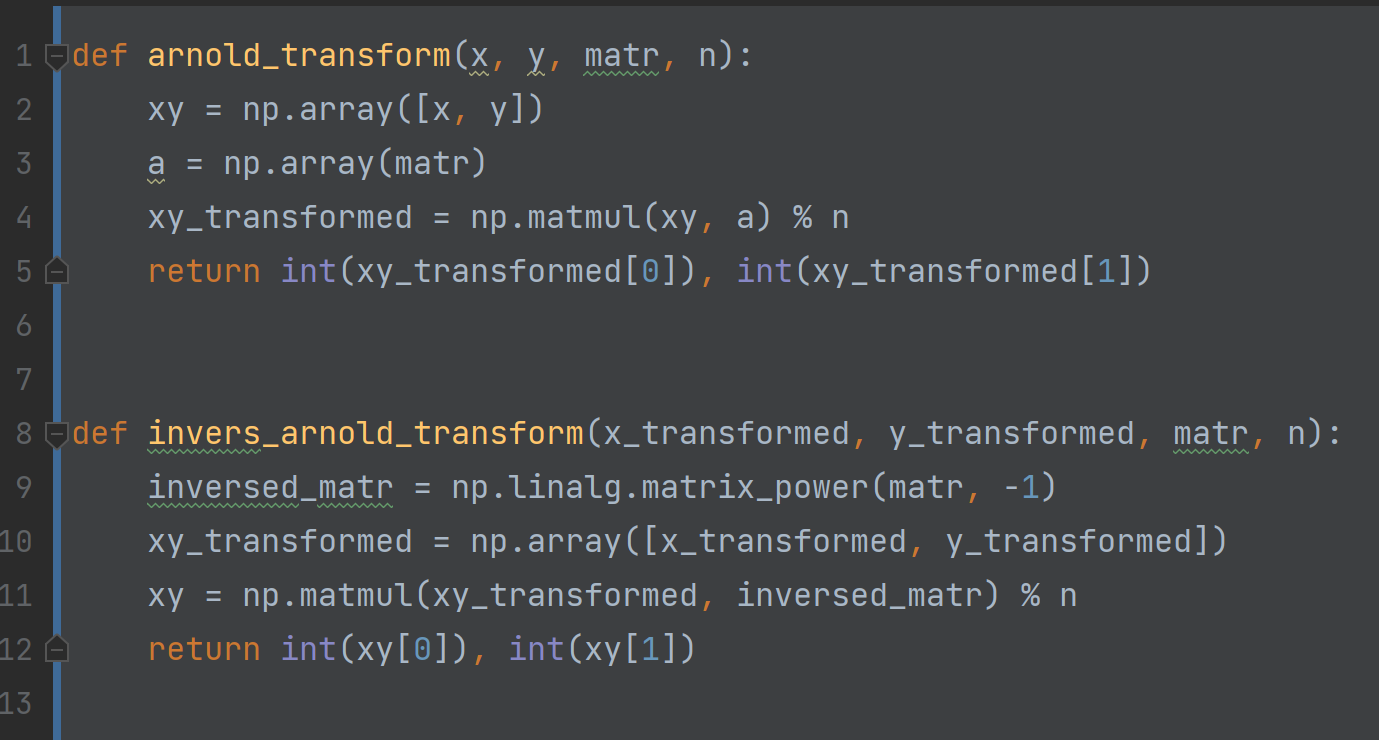
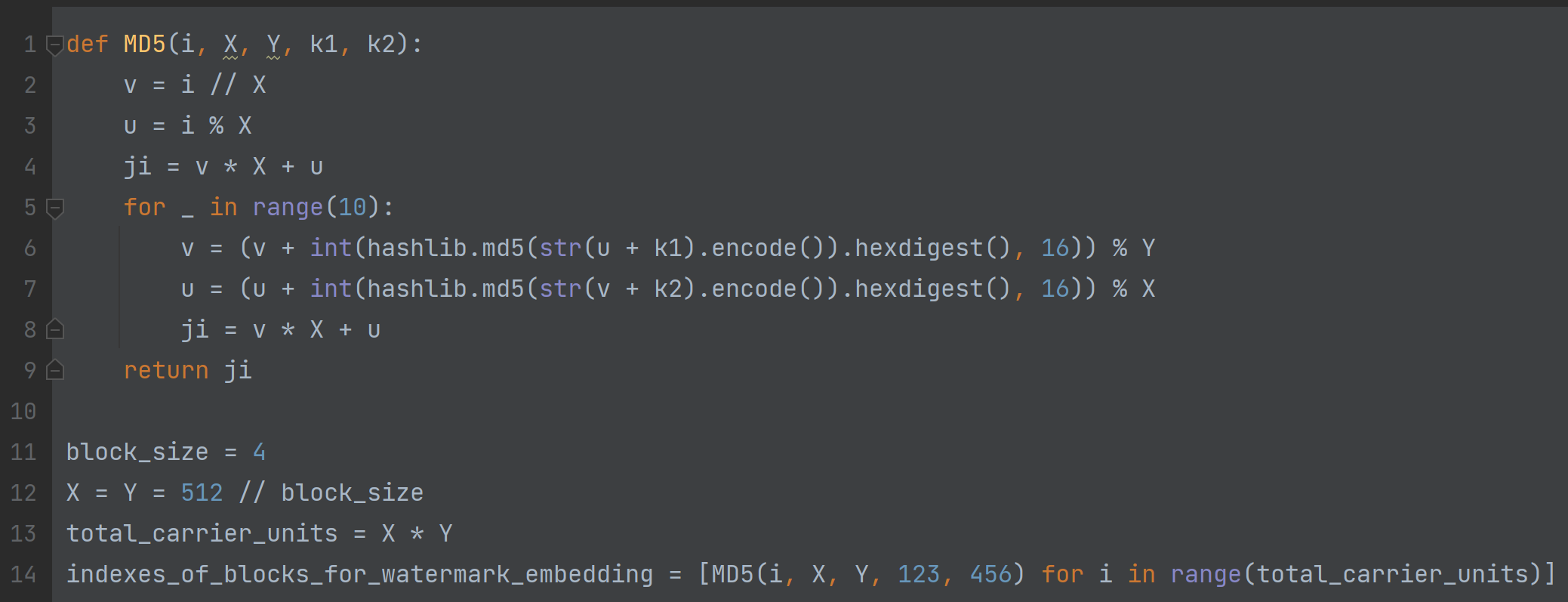


Рисунок 4.3 - Функция прямой и обратной трансформации Арнольда, для матрицы пикселей водяного знака, принимающие на вход координаты пикселя, матрицу Арнольда, и длину ребра изображения водяного знака. Возвращают новое значение координат для пикселя.

**4.1.4 Функция псевдослучайного хеширования MD5**

Этот алгоритм использует безопасную хеш-функцию для создания генератора случайных чисел. Этот генератор создает последовательность случайных чисел, которые не повторяются. Эта последовательность используется в качестве координат для встраивания цифрового водяного знака, которая определяет встроенный блок водяного знака в основном изображении. Такой подход повышает безопасность алгоритма цифрового водяного знака и делает его невидимым для человеческого глаза.[4]  Рисунок 4.4 - Функция генерации последовательности порядка блоков изображения, в которые будет встроен водяной знак

**4.2 Встраивание водяного знака в изображение**

На рисунке 4.5 показан алгоритм внедрения водяных знаков.

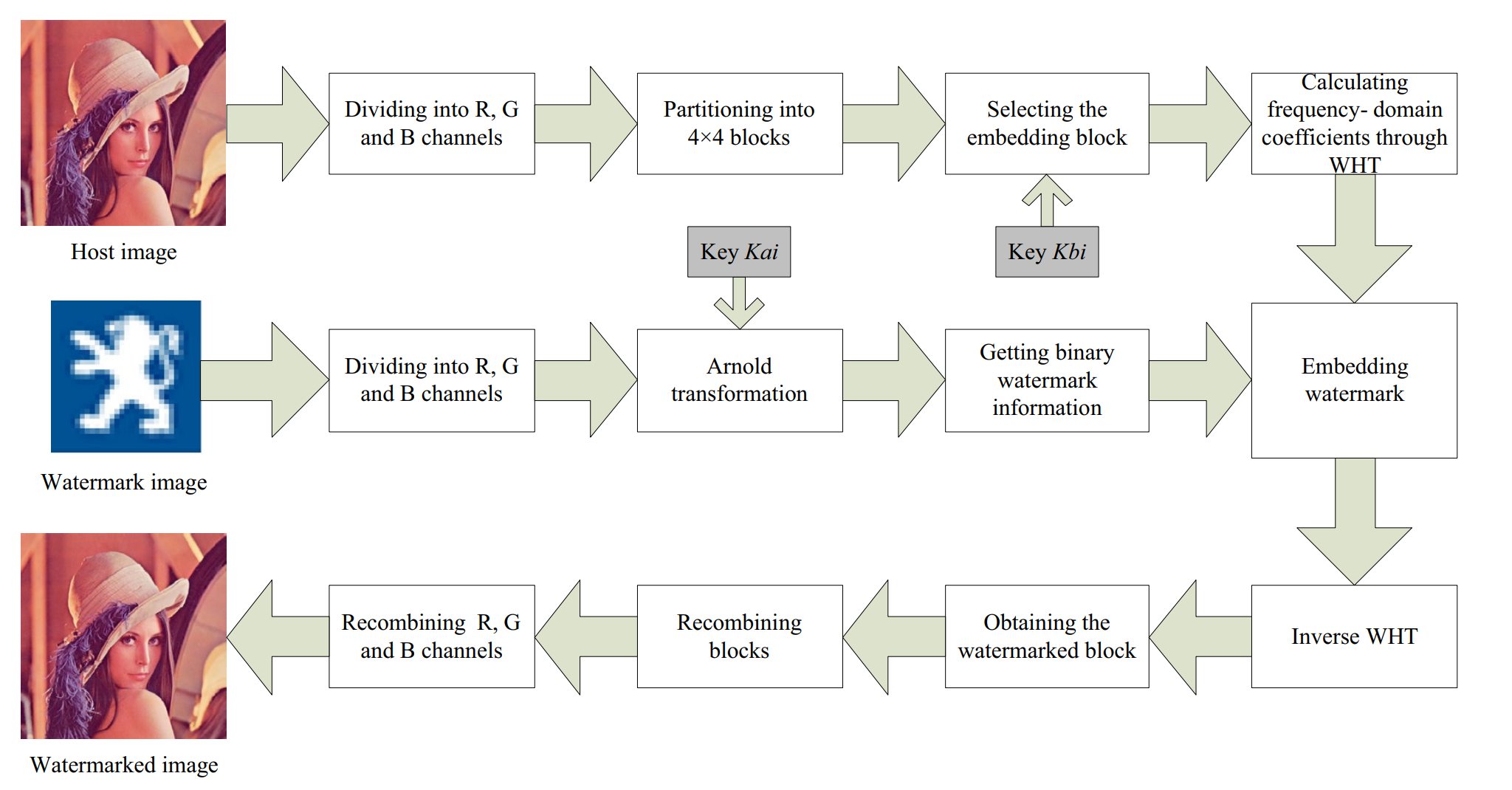
****

Рисунок 4.5 - Блок-схема процесса встраивания водяных знаков

Для начала производится подготовка водяного знака. Она включает в себя разделение изображения на цветовые каналы, преобразование Арнольда и преобразование полученной матрицы пикселей в бинарную последовательность.

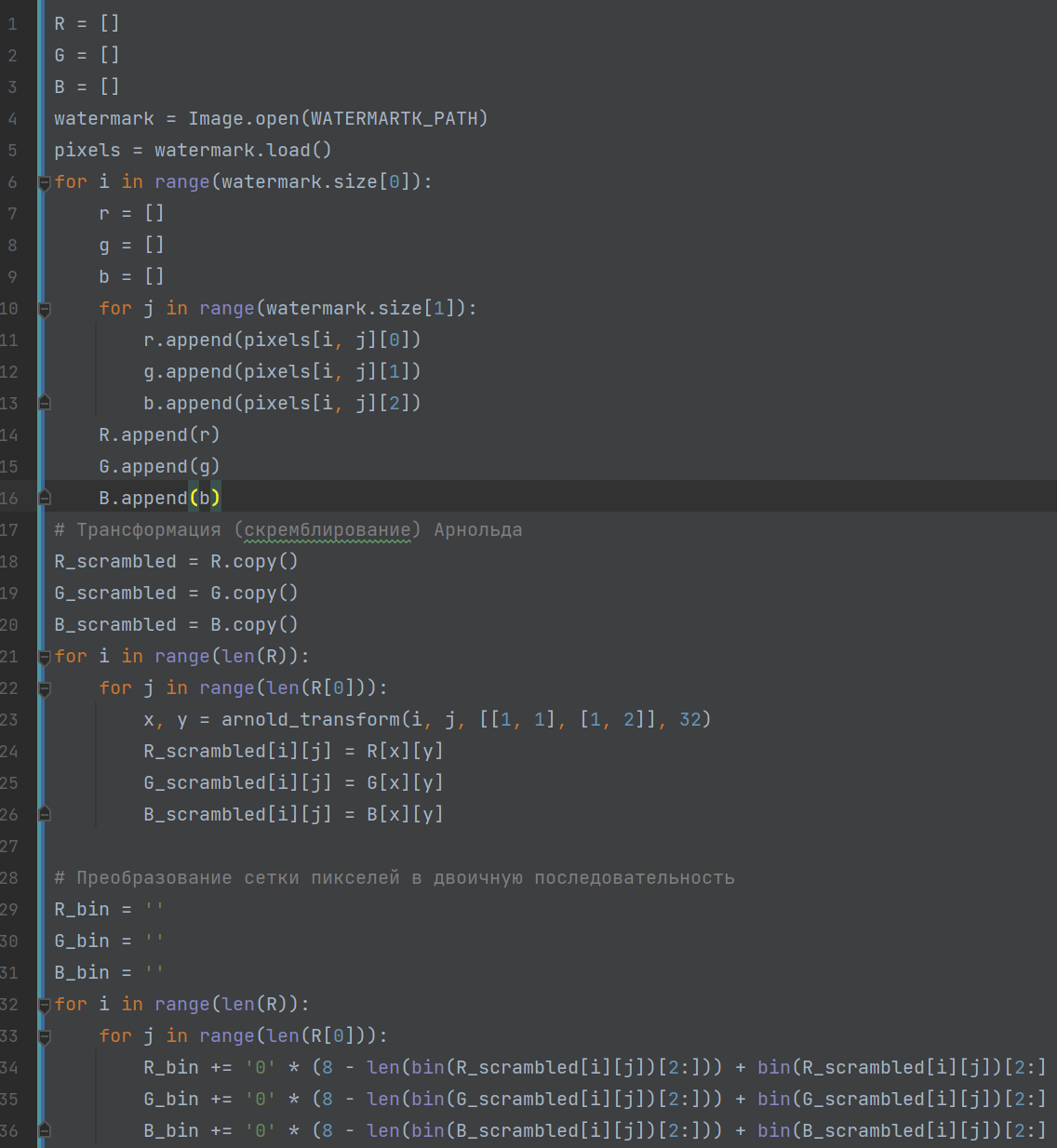


Рисунок 4.6 – подготовка водяного знака к встраиванию

Затем необходимо провести подготовку изображения, в которое будет встроен водяной знак. Для этого необходимо так же разделить изображение на цветовые каналы, затем разбить сетку пикселей на блоки 4 на 4 пикселя и произвести преобразование Уолша-Адамара

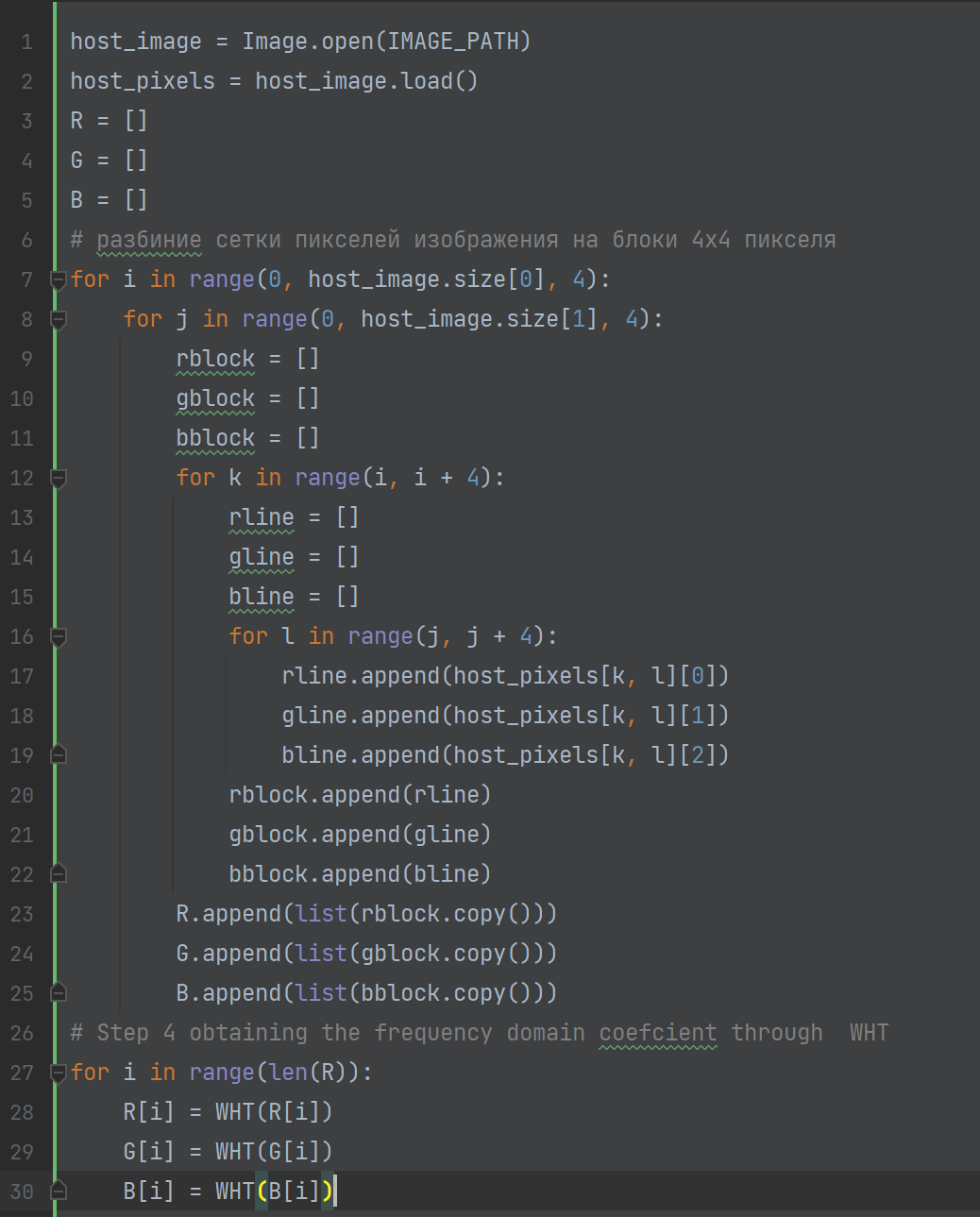


Рисунок 4.7 – подготовка изображения к встраиванию в него водяного знака

После завершения подготовки, производится встраивание битовой последовательности водяного знака в изображение, согласно уравнениям на рисунке 4.8

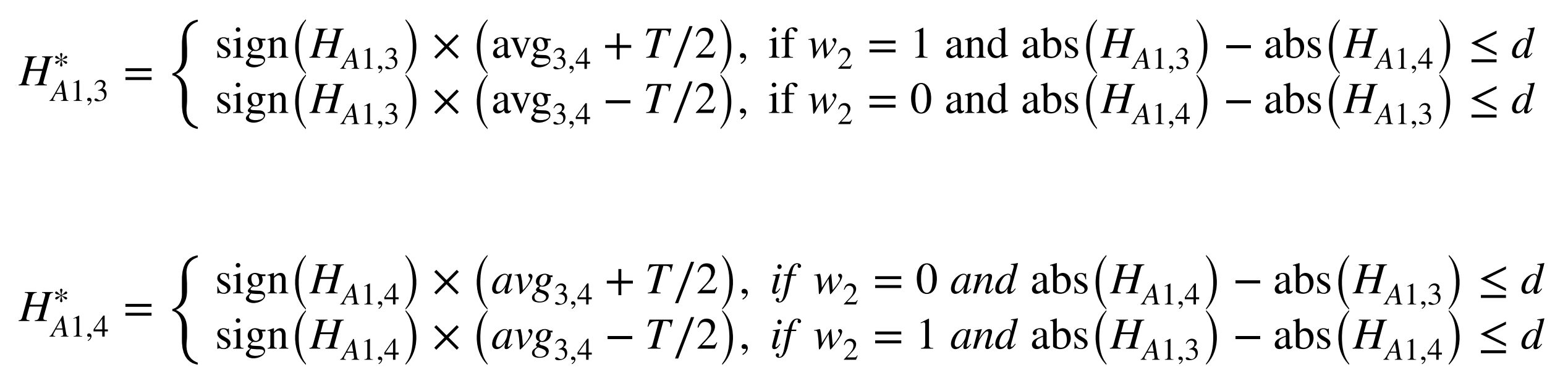
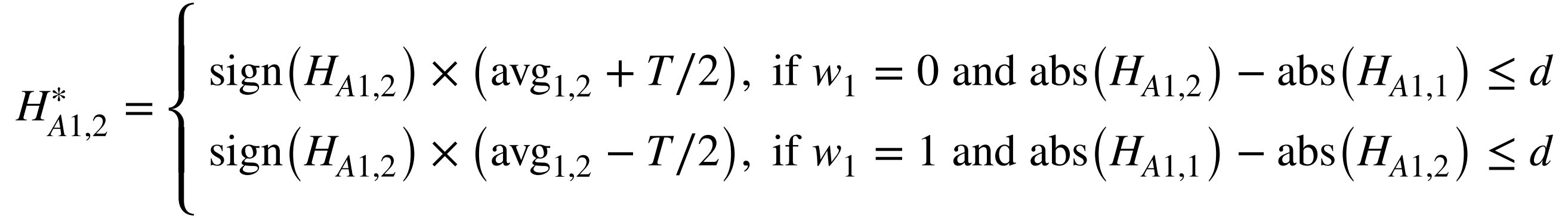
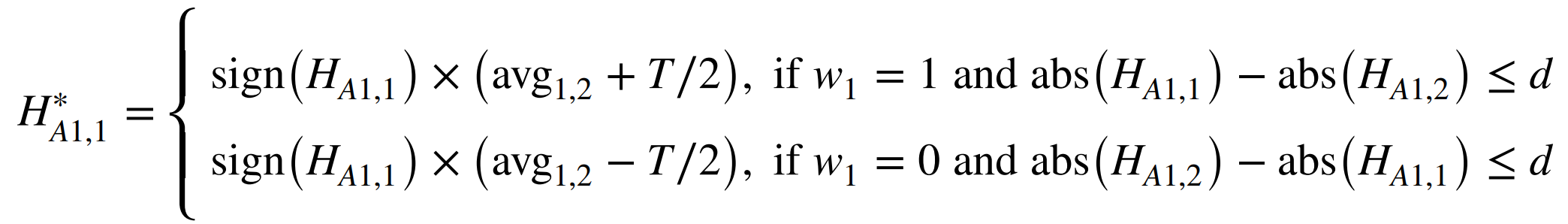
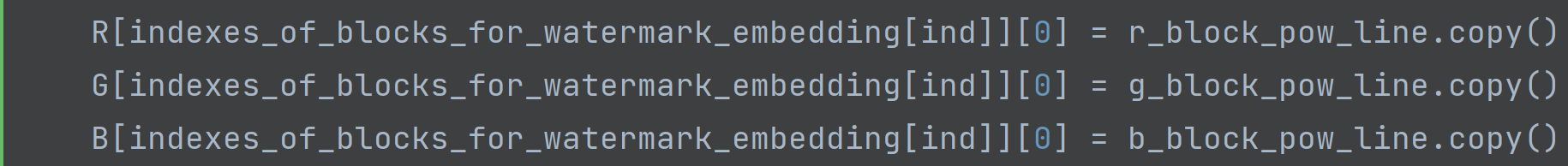


Рисунок 4.8 – алгоритмы изменения основного изображения, в зависимости от битовой последовательности водяного знака и разниц первого и второго и третьего и четвертого элементов, где w – бит водяного знака H – элемент матрицы основного изображения после преобразования Уолша-Адамара, T -шаг квантования, d – параметр ошибки

На рисунке 4.9 изображен код встраивания битов водяного знака в каналы основного изображения. Этот фрагмент кода выполняется для всей последовательности битов водяного знака.

Рисунок 4.9

Встраивание битовой последовательности в блоки основного изображения происходит в порядке, определенном функцией MD5 (рисунок 4.10)

Рисунок 4.10

После встраивания необходимо произвести обратное преобразование Уолша-Адамара и разбить блоки пикселей в пиксельную матрицу. Разбиение необходимо произвести для всех цветовых каналов изображения.

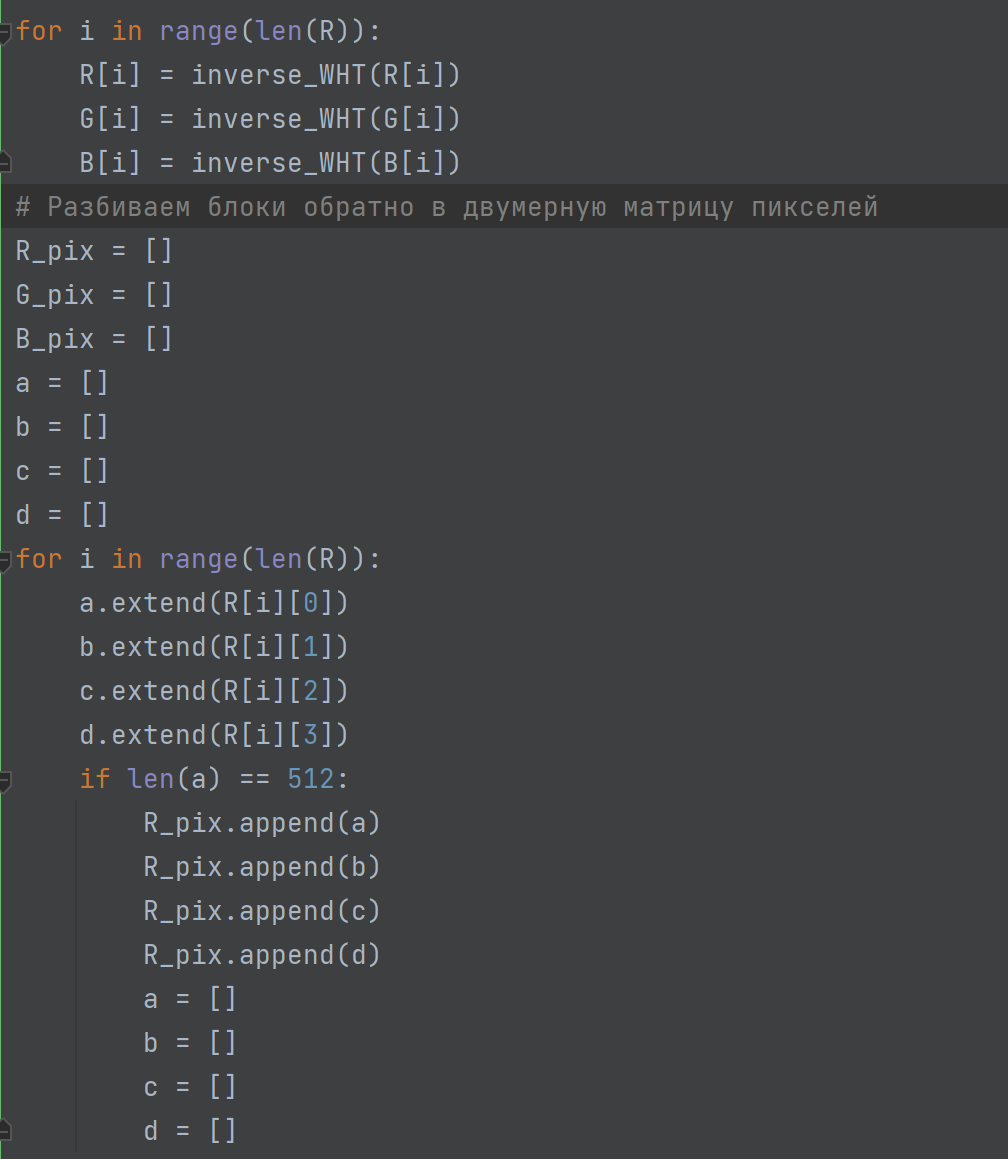
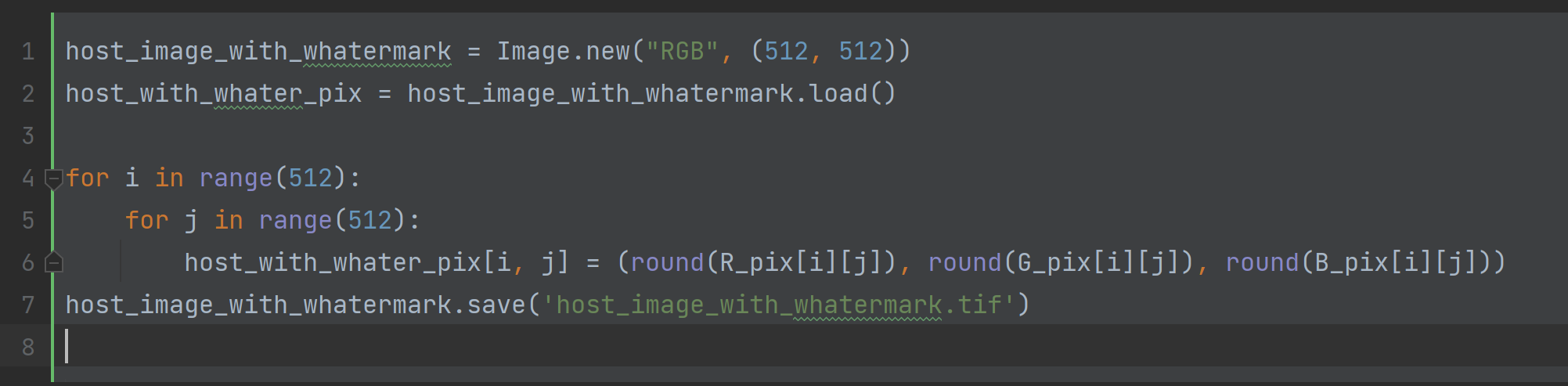


Рисунок 4.11 - обратное преобразование Уолша-Адамара и разбиение блоков пикселей красного канала в пиксельную матрицу

Затем необходимо сохранить полученное изображение со встроенным водяным знаком

Рисунок 4.12 – сохранение изображения со встроенным водяным знаком

**4.3 Извлечение водяного знака из изображения**

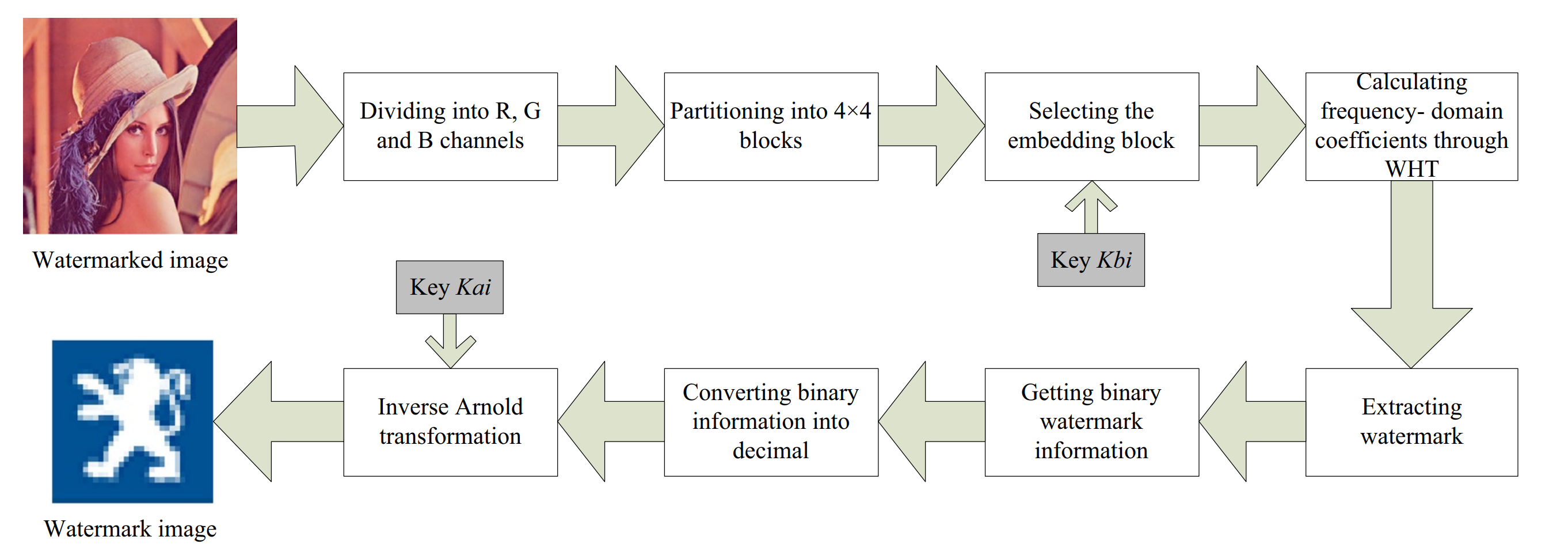


Рисунок 4.13 - Блок-схема процесса извлечения водяного знака

Для начала необходимо разделить изображение на цветовые каналы и сгруппировать матрицу пикселей в блоки 4 на 4 пикселя и провести преобразование Уолша-Адамара.



Рисунок 4.12 - разделение изображения на цветовые каналы, группировка матрицы пикселей в блоки 4 на 4 пикселя и преобразование Уолша-Адамара.

После этого необходимо извлечь встроенные биты водяного знака согласно функциям на рисунке 4.13

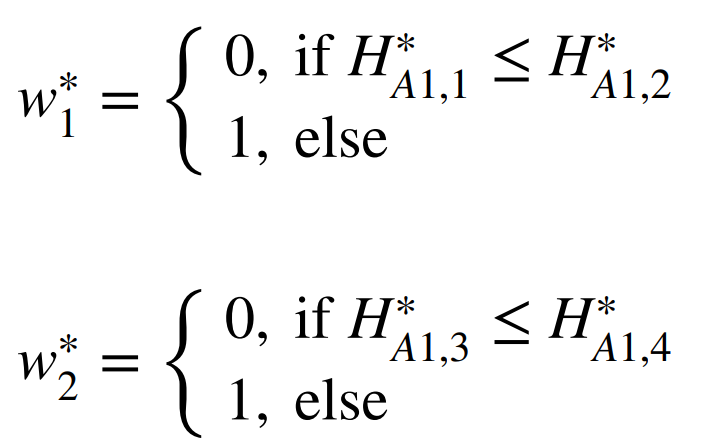


Рисунок 4.13

Блоки для извлечения необходимо выбирать в таком же порядке как и блоки для встраивания (эта последовательность генерируется функцией MD5)



Рисунок 4.14 – извлечение битовой последовательности из каналов изображения с встроенным водяным знаком

Затем необходимо выполнить обратное преобразование Арнольда и получить, и сохранить изображение водяного знака

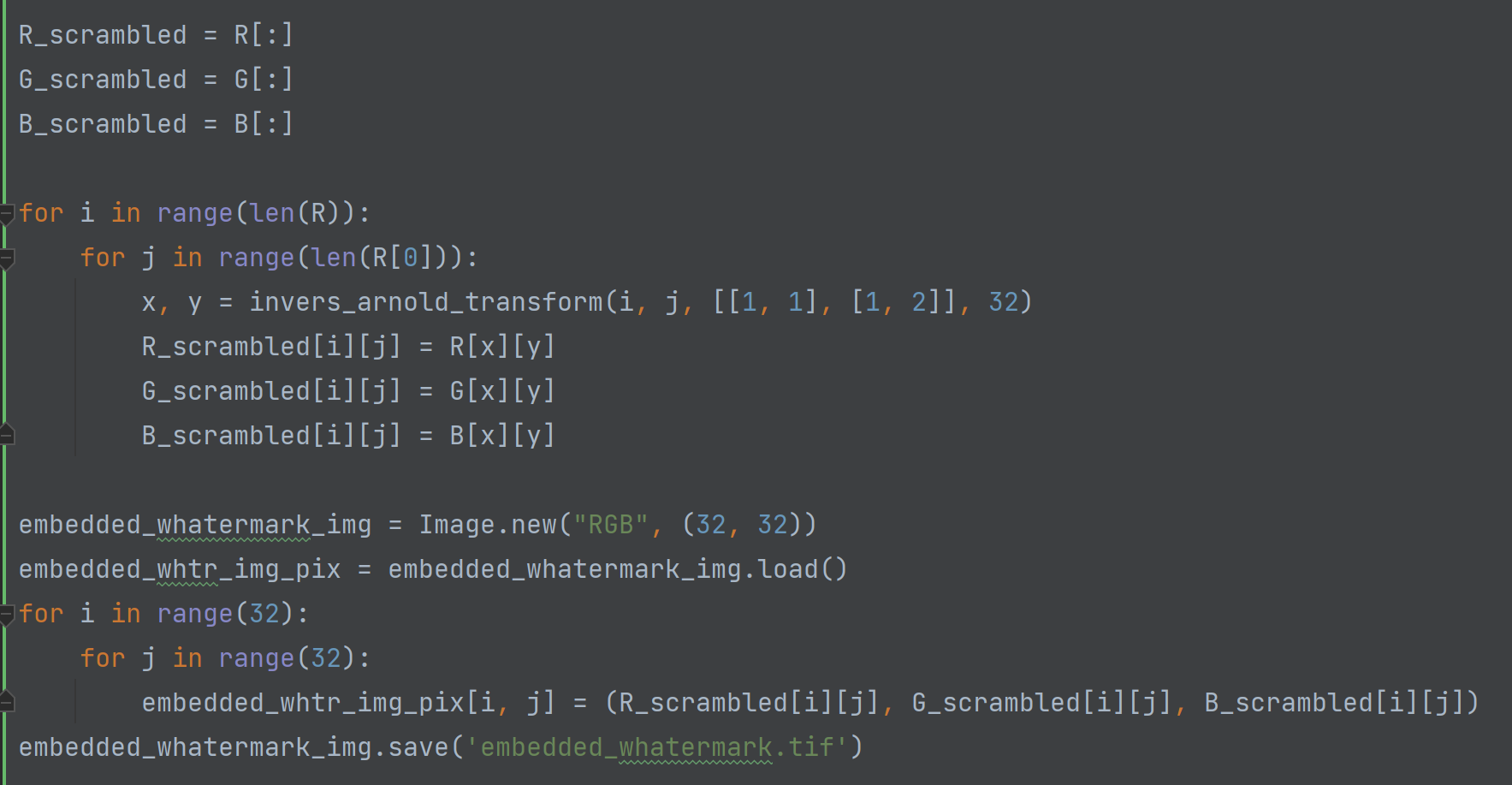


Рисунок 4.15 - обратное преобразование Арнольда и сохранение исходного изображения водяного знака

**4.4 Эксперименты и вычисление метрик**

**4.4.1 Проверка и анализ невидимости**

Для проверки невидимости встраивания будем применять метрики PSNR [5], SSIM [6] и Normalized Cross-coefcient (NC). Произведем вычисление этих метрик для встраивания водяного знака при разных шагах квантования.

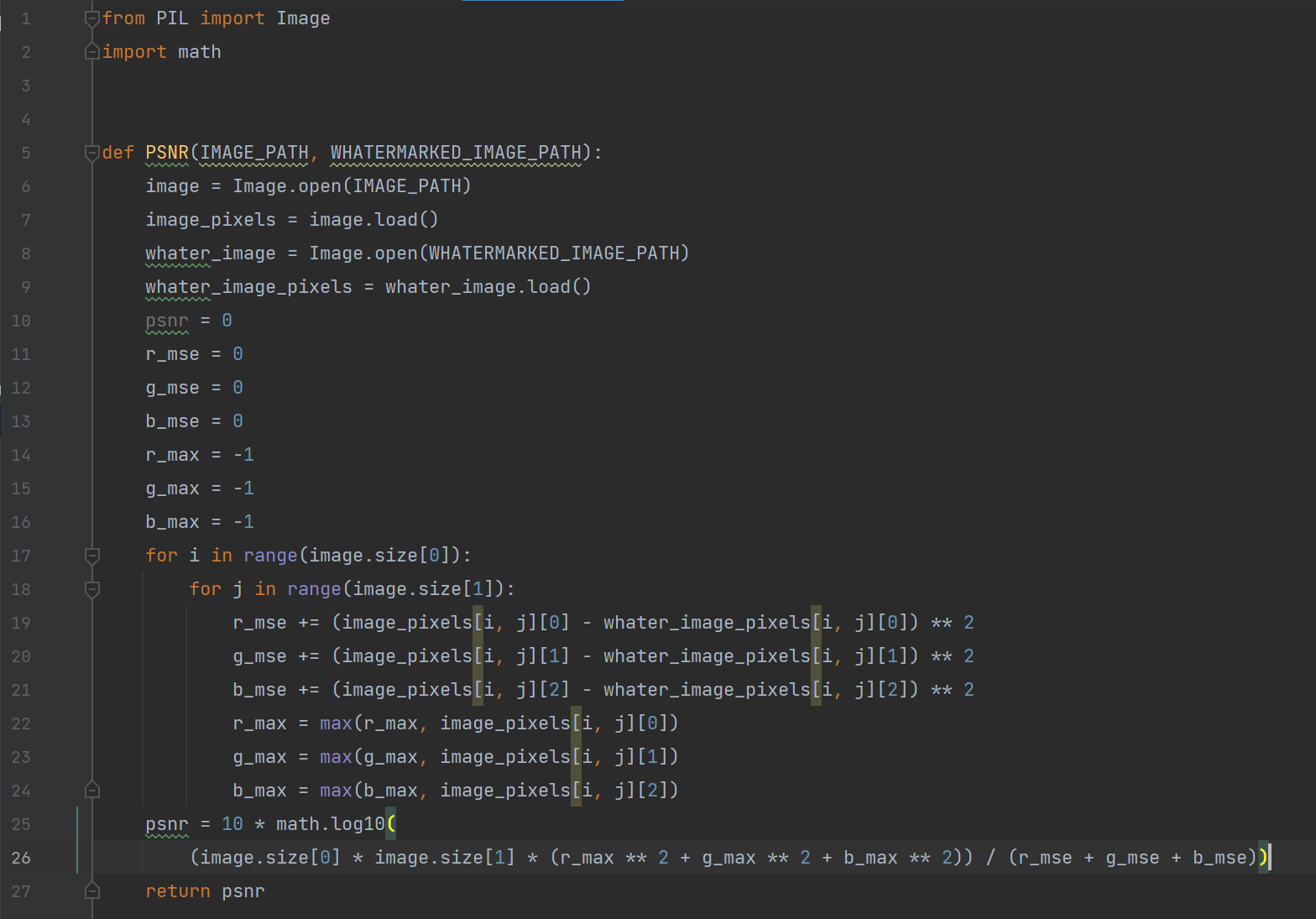


Рисунок 4.16 – код для вычисления метрики PSNR



Рисунок 4.17 – код для вычисления метрики SSIM



Рисунок 4.18 – код для вычисления метрики Normalized Cross-coefcient (NC)

****

Рисунок 4.19 – значения метрики PSNR для шагов квантования от 0.5 до 10

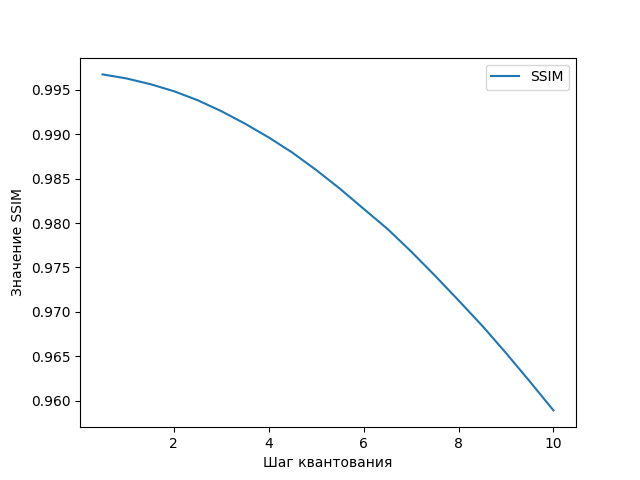


Рисунок 4.20 - значения метрики SSIM для шагов квантования от 0.5 до 10

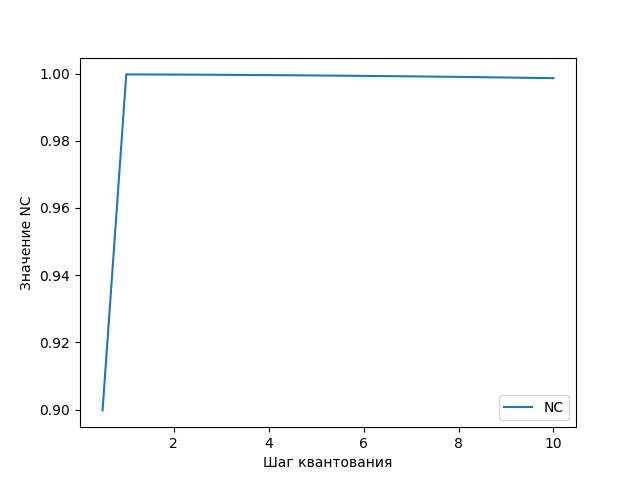
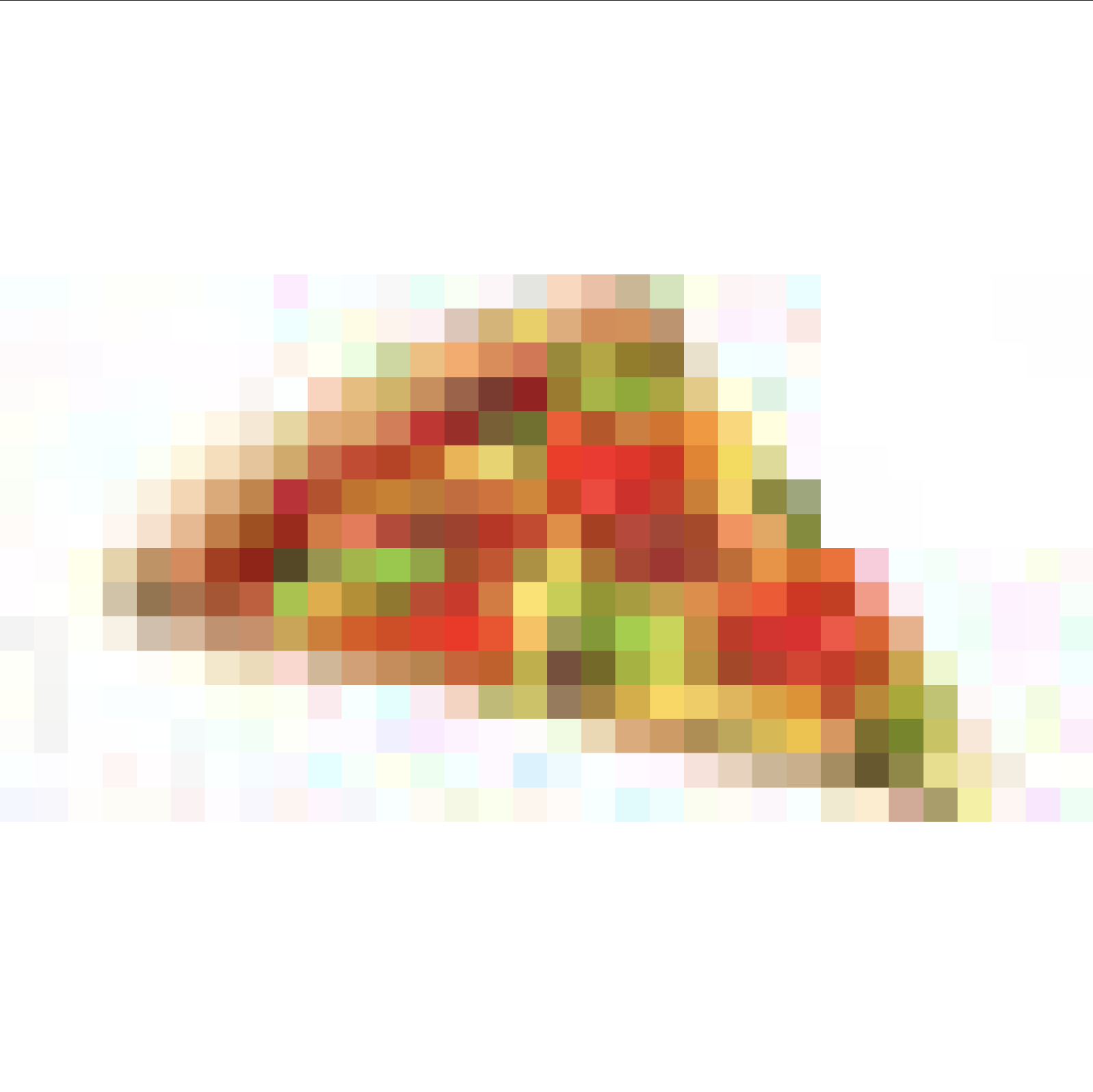


Рисунок 4.21 – значения метрики NC для шагов квантования от 0.5 до 10

Вычислим значение метрики PSNR для различных изображений и водяных знаков. В качестве изображений будем использовать следующие картинки.

Рисунки 4.22-4.24 – изображения, используемые в качестве контейнеров для водяных знаков, взятые из базы данных изображений USC-SIPI[7]

Рисунки 4.25-4.26 - изображения, используемые в качестве водяных знаков

Таблица 1 – значения метрики PSNR для разных изображений

|  |  |  |
| --- | --- | --- |
| Название изображения | Значение PSNR для первого водяного знака (рыцарь) | Значение PSNR для второго водяного знака (пицца) |
| Девушка | 42.552 | 42.682 |
| Самолет | 38.786 | 39.367 |
| Дом | 38.054 | 38.364 |

Таблица 2 – значения метрики SSIM для разных изображений

|  |  |  |
| --- | --- | --- |
| Название изображения | Значение SSIM для первого водяного знака (рыцарь) | Значение SSIM для второго водяного знака (пицца) |
| Девушка | 0.985 | 0.984 |
| Самолет | 0.982 | 0.981 |
| Дом | 0.983 | 0.983 |

Данные, указанные выше, демонстрируют, что различие между изображением с водяным знаком и оригинальным практически незаметно для человеческого глаза. Поэтому этот алгоритм имеет высокую степень незаметности.

**4.4.2 Проверка и анализ способности алгоритма противостоять сжатию**

Для проверки, мы встроим водяной знак в изображение, применим алгоритм сжатия JPEG2000 4:1 и извлечем водяной знак из сжатого изображения, после этого вычислим значение NC между исходным изображением водяного знака и извлеченным изображением.



Рисунок 4.27 – исходное изображение водяного знака

****

Рисунок 4.28 – извлеченное изображение водяного знака после сжатия

Значение метрики **NC = 0.998**

Повторим то же самое для второго водяного знака

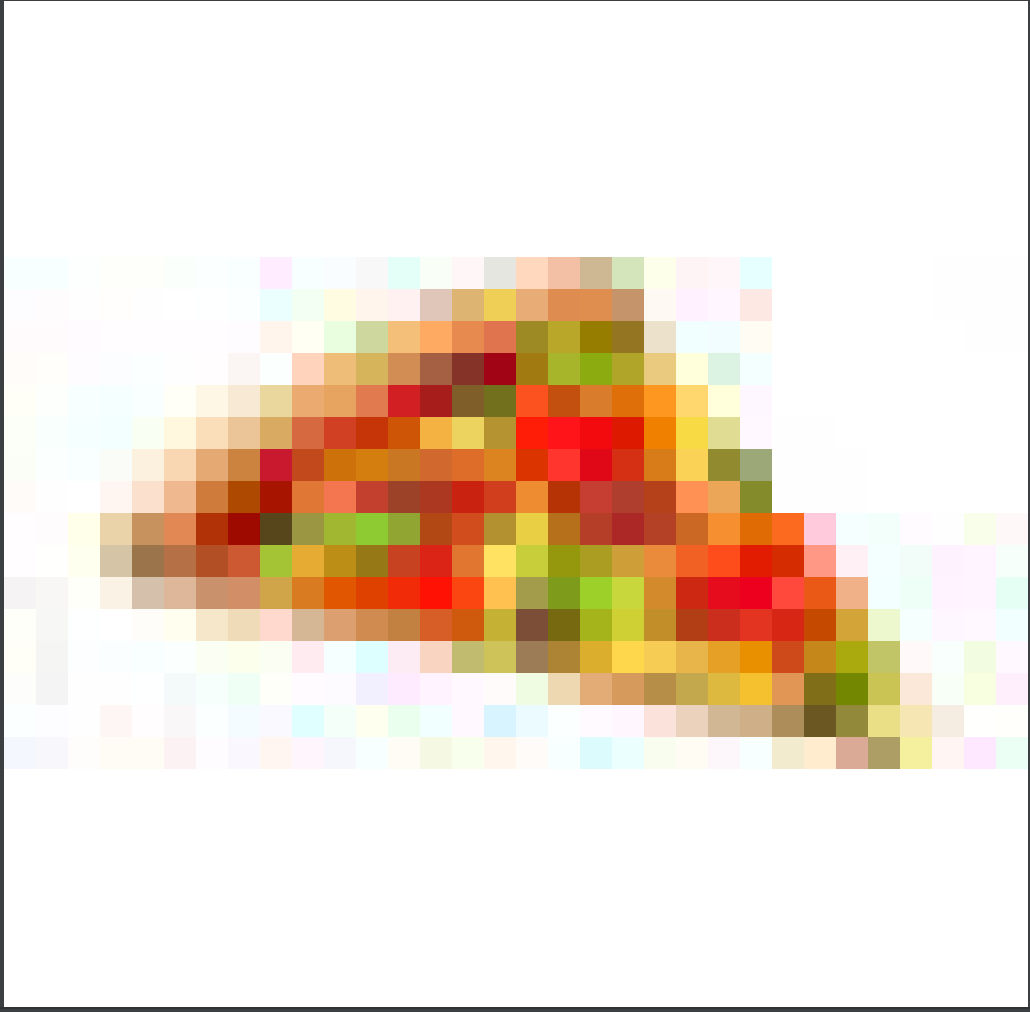
****

Рисунок 4.29 - исходное изображение водяного знака

****

Рисунок 4.29 - извлеченное изображение водяного знака после сжатия

Значение метрики **NC = 0.993**

Достаточно высокие значения метрики NC говорят о хорошей сопротивляемости этого алгоритма встраивания сжатию изображений с водяными знаками.

**4.4.3 Анализ возможностей встраивания**

В технологии водяных знаков максимальная емкость встраивания определяется отношением количества битов внедрения к размеру основного изображения. Большой объем информации, содержащийся в цветных изображениях водяных знаков, требует большей емкости для встраивания. В данной статье авторы разделили цветное изображение 512 × 512 на блоки размером 4 × 4, в каждый из которых могут быть встроены 2 бита двоичных данных водяного знака. Таким образом, максимальная емкость встраивания для этого алгоритма составляет (128 × 128 × 2 × 3) / (512 × 512 × 3) = 0,12500 (бит/пиксель).

**4.4.4 Анализ производительности встраивания**

Измерения скорости работы данного алгоритма производились с помощью встроенной библиотеки time. Время необходимое для встраивания водяного знака составило 0.71009 сек, а для извлечения 0.23628 сек.

Запуск алгоритма производился на платформе с ЦП, работающим на частоте 2.2 ГГц, 8 Гб ОЗУ, Win11, PyCharm Professional.

Этот алгоритм имеет низкую сложность выполнения, так как преобразование Уолша-Адамара довольно просто в осуществлении и требует только операций сложения и вычитания с единицей.

**4.4.5 Анализ безопасности встраивания**

Безопасность — это очень важный аспект алгоритма водяных знаков. Главной целью внедрения и извлечения цифровых водяных знаков является защита авторских прав и определение, было ли изображение подделано. Поэтому безопасность этого процесса очень важна.

Чтобы улучшить безопасность предлагаемого алгоритма, изображение цветного водяного знака сначала разбивается на красный, зеленый и синий каналы, а затем применяется преобразование Арнольда с закрытым ключом. Каждый канал использует ключ, пространство значений которого составляет 2^15. Следовательно, общее пространство значений равно 2^45.

Кроме того, в этом алгоритме последовательность блоков для встраивания определяется псевдослучайным алгоритмом на основе MD5, который имеет пространство ключей 2^63. В данной статье каждый канал использует ключевое пространство в 2^21, а общее пространство ключа равно 2^63. Следовательно, общее ключевое пространство предлагаемого алгоритма составляет 2^108.

# 5 Заключение

В ходе прохождения практики, мной был исследован и реализован алгоритм слепого встраивания водяных знаков в частотную область цветных изображений. Были проведены эксперименты по анализу невидимости, надежности, емкости, производительности и безопасности встраивания водяного знака в изображение. Исходя из результатов экспериментов были сделаны выводы о хороших показателях незаметности встраивания, о хорошей способности предложенного алгоритма противостоять сжатию изображения с водяным знаком, о достаточной емкости контейнера для водяного знака, о хорошей производительности данного алгоритма и его высокой безопасности.

# 6 Список использованных источников

1. Московский институт электроники и математики им. А.Н. Тихонова – URL: https://miem.hse.ru/ (дата обращения 21.03.2023)
2. Chen, S. A high-efficiency blind watermarking algorithm for double color image using Walsh Hadamard transform [Text] / S. Chen, Q. Su, H. Wang, G. Wang // The Visual Computer. – 2022. – V.38. – P.2189-2205.
3. Numpy documentation – numpy.org – URL: <https://numpy.org/doc/stable/index.html> (дата обращения 21.03.2023)
4. Python documentation – python-scripts – URL: <https://python-scripts.com/md5-sha1#md5>
5. PSNR – Википедия – URL: https://ru.wikipedia.org/wiki/PSNR (дата обращения 23.03.2023)
6. SSIM – Википедия – URL: https://ru.wikipedia.org/wiki/SSIM (дата обращения 23.03.2023)
7. SIPI Image Database – URL: https://sipi.usc.edu/database/database.php (дата обращения 21.03.2023)