**Цель работы**

Изучить принципы работы шифра с управляемыми перестановками. На основе этого шифра реализовать алгоритм шифрования и дешифрования черно-белого изображения.

**Задание**

С помощью шифра с управляемыми перестановками надо зашифровать/расшифровать исходное сообщение. На основе этого проанализировать основные свойства алгоритма и полученные результаты.

**Результат выполнения работы**

Для шифрования было выбрано изображение, представленное на рисунке 1.



Рисунок 1 – Исходное изображение

**Выбор размера входного блока данных**

Входное сообщение *M* разбивается на блоки Bi. Битовый размер S блоков Bi был взят равным 16 битам. Далее блоки Bi разбиваются на два подблока BL и BR по S/2 = 8 бит в каждом.

**Структура блока управляемой перестановки**

На рисунке 2 показана структура блока управляемой перестановки, используемая в лабораторной работе, а на рисунке 3 его общая схема.

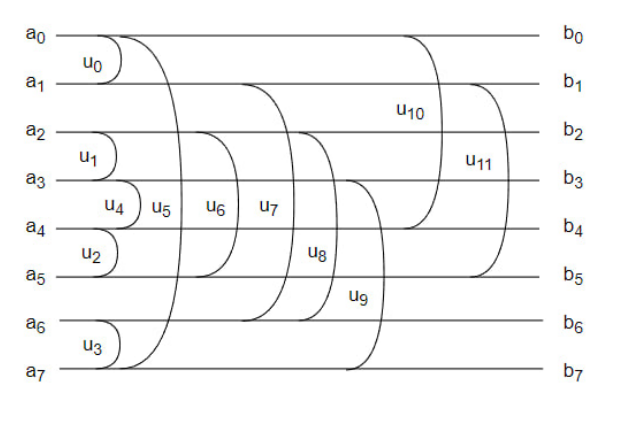


Рисунок 2 – Структура блока управляемой перестановки

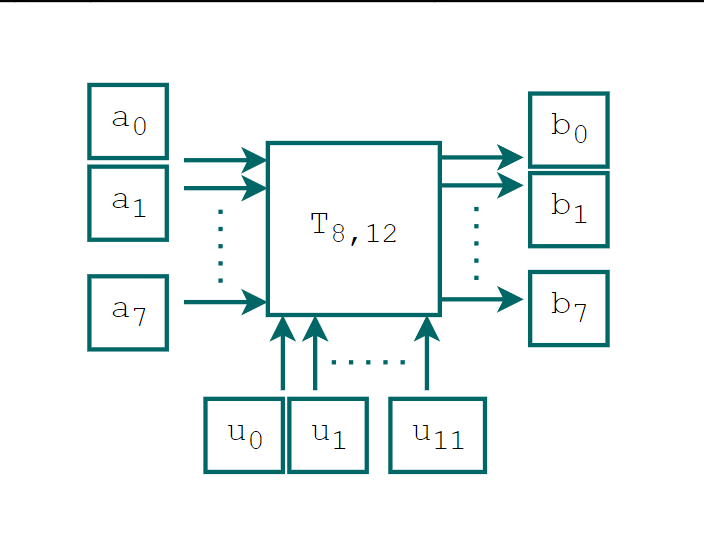


Рисунок 3 – Общая схема блока управляемой перестановки

Основные условия для блоков управляемой перестановки включают в себя следующее:

* Каждый входной бит (ai) способен занять любое место в последовательности выходных битов;
* Каждому выходному значению (bi) должно соответствовать только одно входное значение.

Критерием перестановки в блоках перестановки являются управляющие сигналы (ui). Если u=1 перестановка есть, если u = 0 перестановки нет.

Теоретически для блоков в 8 бит количество управляемых сигналов должно составлять 15, так как число возможных перестановок входных значений равно 8!, а количество управляемых сигналов n определяется выражением 2n=8!. Но в фактической реализации было использовано только 12 управляемых сигналов.

Уменьшение количества управляемых сигналов упростило процесс реализации блока перестановки, но понизило вариативность шифрования изображения, так как оно понизило количество комбинаций для управляемых сигналов.

Для обоснования выбранной схемы управляемых перестановок можно записать следующие уравнения:

b0 = a\_0 \* ¬u\_0 \* ¬u\_5 \* ¬u\_10 +

a\_1 \* u\_0 \* ¬u\_5 \* ¬u\_10 +

a\_2 \* u\_1 \* u\_4 \* u\_10 +

a\_3 \* ¬u\_1 \* u\_4 \* u\_10 +

a\_4 \* ¬u\_2 \* ¬u\_4 \* u\_10 +

a\_5 \* u\_2 \* ¬u\_4 \* u\_10 +

a\_6 \* u\_3 \* u\_5 \* ¬u\_10 +

a\_7 \* ¬u\_3 \* u\_5 \* ¬u\_10;

b1 = a\_0 \* u\_0 \* ¬u\_7 \* ¬u\_11 +

a\_1 \* ¬u\_0 \* ¬u\_7 \* ¬u\_11 +

a\_2 \* ¬u\_1 \* u\_6 \* u\_11 +

a\_3 \* u\_1 \* u\_6 \* u\_11 +

a\_4 \* u\_2 \* ¬u\_6 \* u\_11 +

a\_5 \* ¬u\_2 \* ¬u\_6 \* u\_11 +

a\_6 \* ¬u\_3 \* u\_7 \* ¬u\_11 +

a\_7 \* u\_3 \* u\_7 \* ¬u\_11;

b2 = a\_0 \* u\_0 \* u\_7 \* u\_8 +

a\_1 \* ¬u\_0 \* u\_7 \* u\_8 +

a\_2 \* ¬u\_1 \* ¬u\_6 \* ¬u\_8 +

a\_3 \* u\_1 \* ¬u\_6 \* ¬u\_8 +

a\_4 \* u\_2 \* u\_6 \* ¬u\_8 +

a\_5 \* ¬u\_2 \* u\_6 \* ¬u\_8 +

a\_6 \* ¬u\_3 \* ¬u\_7 \* u\_8 +

a\_7 \* u\_3 \* ¬u\_7 \* u\_8;

…

**Формирование недостающих битов**

Для получения 12 управляющих сигналов из 8 входных битов необходимо расширить входной вектор на 4 бита. Это происходит путем вставки в начало вектора дополнительных битов, которые получаются путем попарного сложения по модулю 2 входных битов (a0 с a1, a1 с a2 и т.д.).

**Структурные схемы прямого и обратного преобразований**

Структурные схемы прямого и обратного преобразований представлены на рисунках 4 и 5.

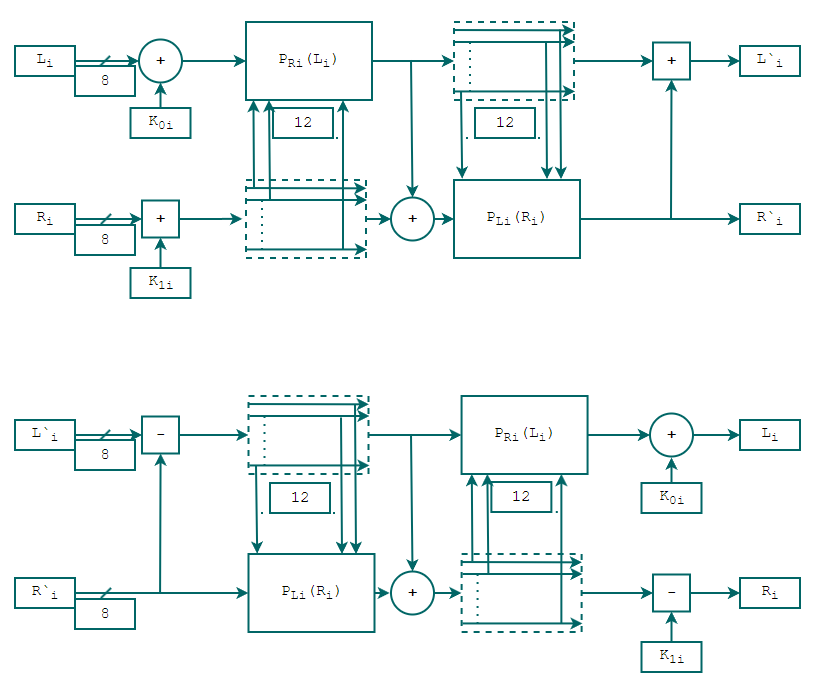


Рисунок 4 – Структурная схема прямого преобразования

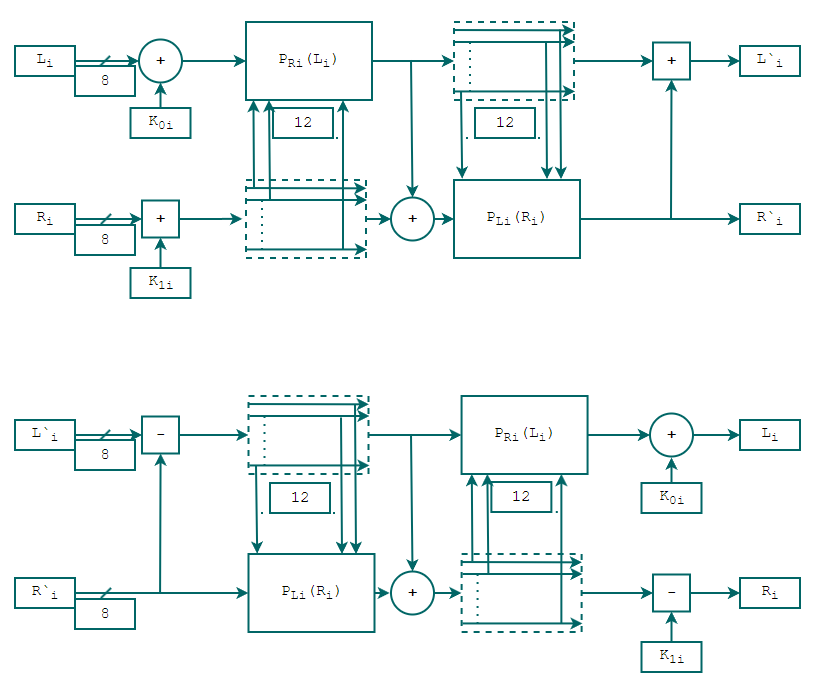


Рисунок 5 – Структурная схема прямого преобразования

**Анализ исходного изображения**

Далее были проведены тесты для исходного изображения. Гистограмма распределения яркости представлена на рисунке 6.

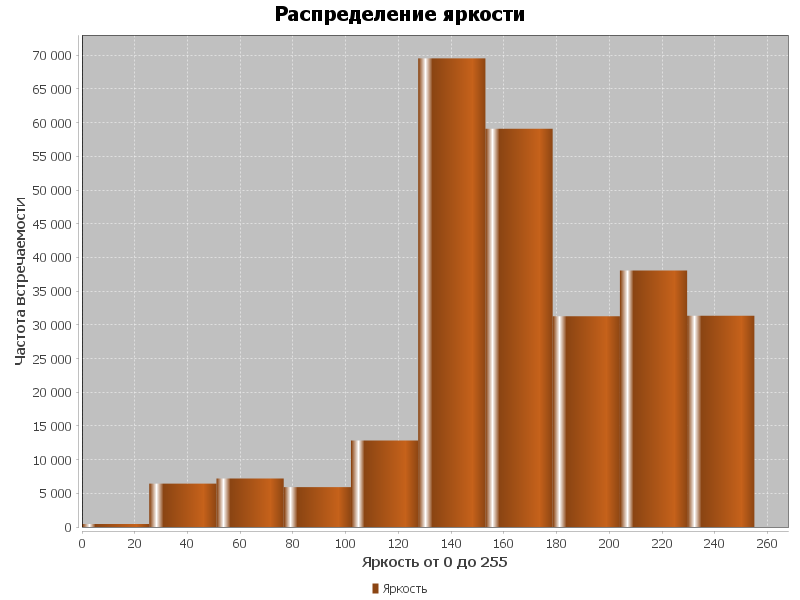


Рисунок 6 – Гистограмма распределения яркости исходного изображения

По этому графику весьма наглядно (и количественно) прослеживается существенная неравномерность распределения значений яркостей по всему диапазону. Часть значений яркости на изображении не представлено. Все это свидетельствует о том, что изображение не шумоподобно.

Диаграмма рассеяния (тест на решётчатость) представлена на рисунке 7.

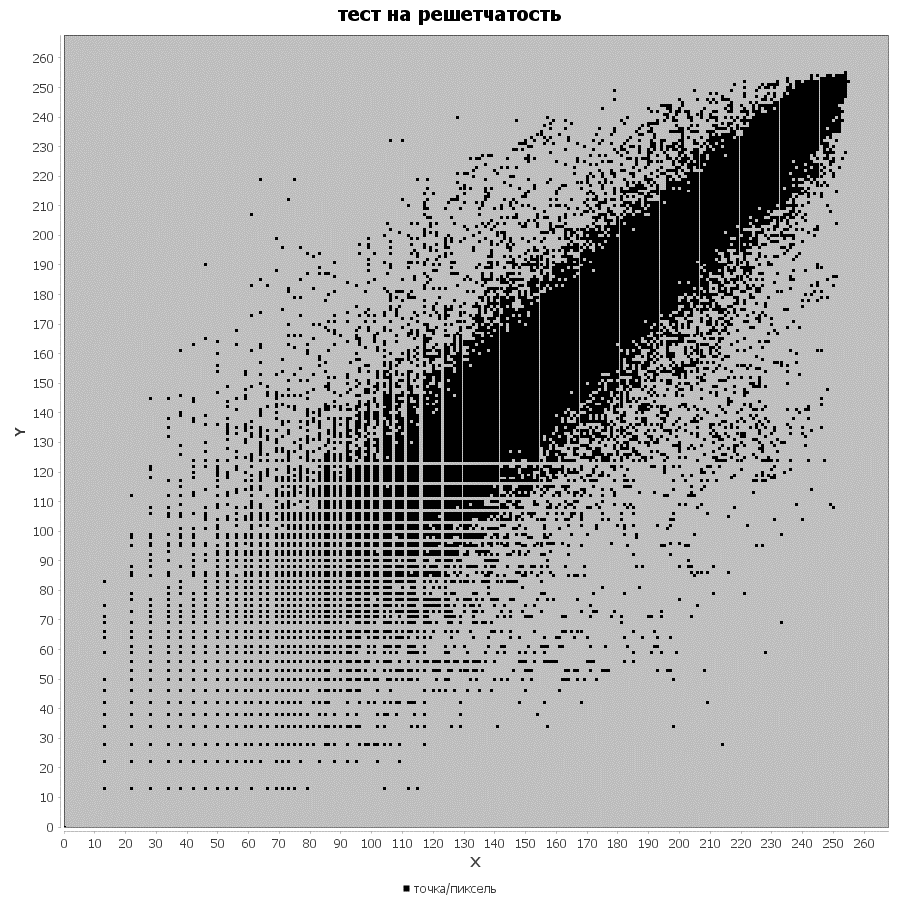
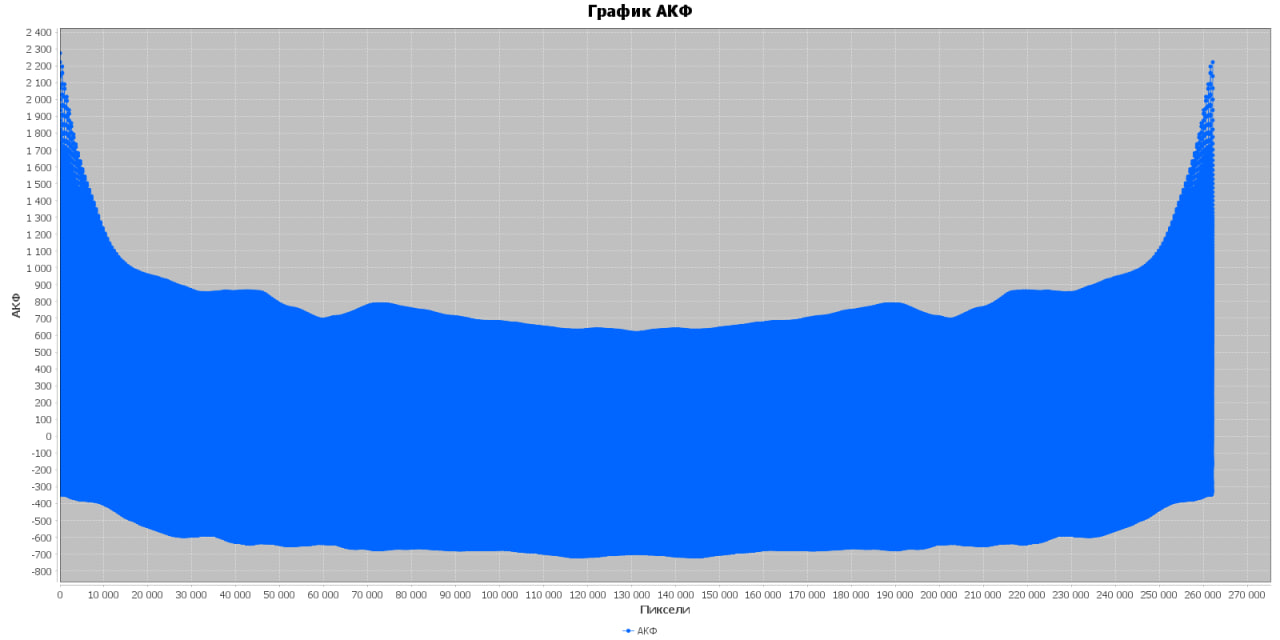


Рисунок 7 - Диаграмма рассеяния исходного изображения

Тест "на решетчатость" предназначен для выявления зависимостей между соседними пикселями в изображении. На графике теста изображения на решетчатость, представленном выше, хорошо заметны как существенная неравномерность распределения, так и полное отсутствие в анализируемой последовательности большого ряда значений яркостей пикселей. Поэтому между соседними пикселями изображения существуют функциональные связи.

График АКФ представлен на рисунке 8.



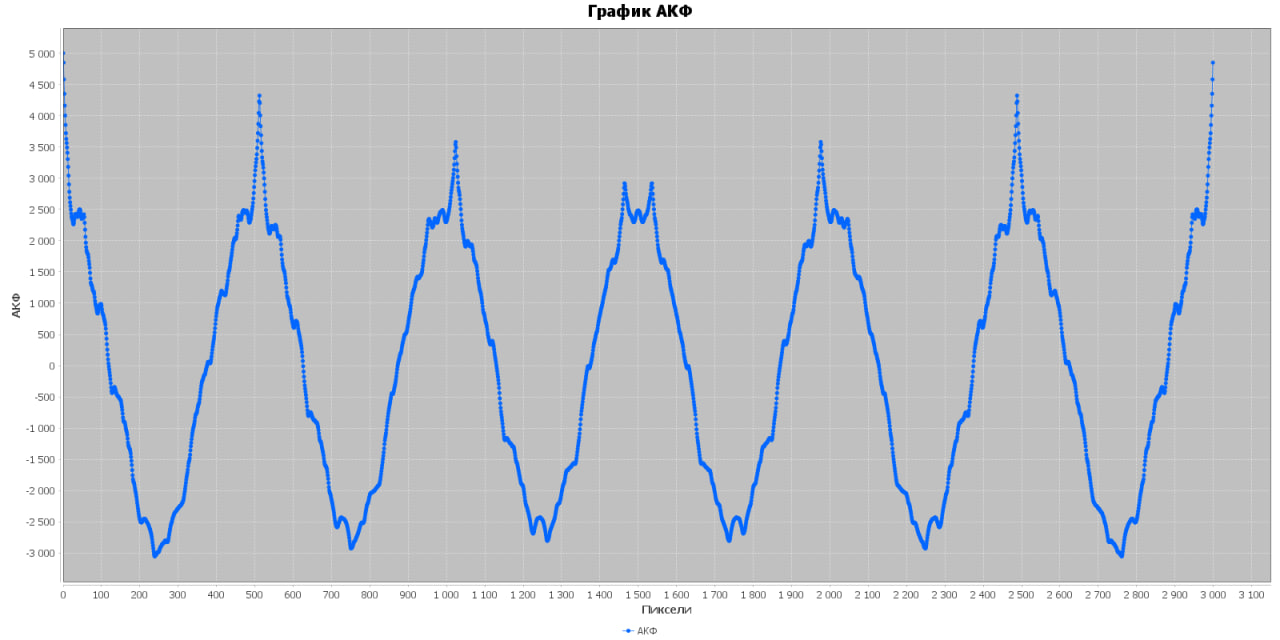


Рисунок 8 – График АФК для исходного изображения

Из графика АКФ хорошо видно, что по своим статистическим свойствам исследуемое изображение не соответствует шуму, поскольку её АКФ не имеет ярко выраженного максимума при нулевом сдвиге копии относительно исходной последовательности (в начале координат), а при ненулевых временных сдвигах значения АКФ исходной последовательности чисел присутствуют периодические участки, что свидетельствует об присутствии корреляции между пикселями в исходном изображении.

**Первый раунд шифрования**

Далее был проведен первый раунд шифрования. Зашифрованное изображение после первого раунда представлено на рисунке 9. Визуально на нем просматриваются основные контуры исходного, значит, изображение было зашифровано неудовлетворительно.



Рисунок 9 - Зашифрованное изображение после первого раунда

Для этого изображения были проведены те же тесты, что и для исходного. Гистограмма распределения яркости представлена на рисунке 10.

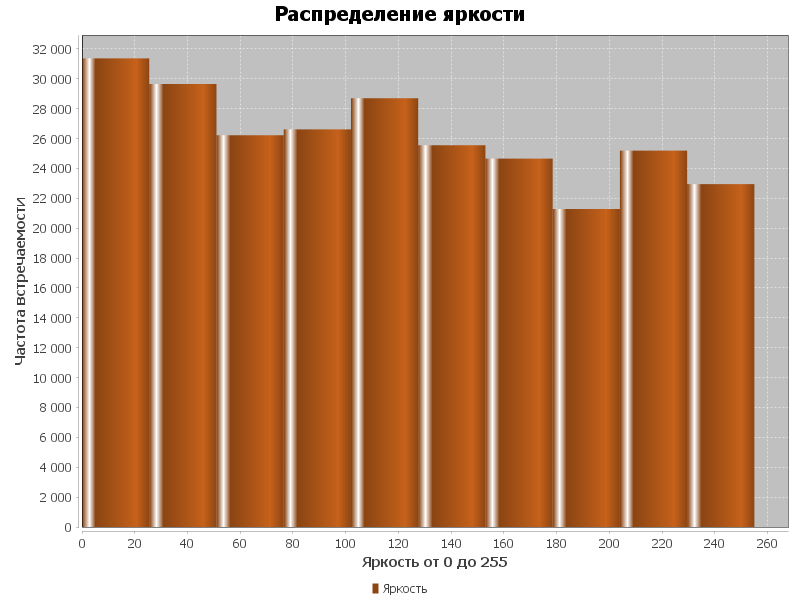


Рисунок 10 – Гистограмма распределения яркости зашифрованного изображения после первого раунда

По этому графику наглядно (и количественно) прослеживается в основном неравномерность распределения значений яркостей по всему диапазону, однако есть участки с равномерным распределением. Это свидетельствует о том, что изображение не полностью шумоподобно.

Диаграмма рассеяния (тест на решётчатость) представлена на рисунке 11.

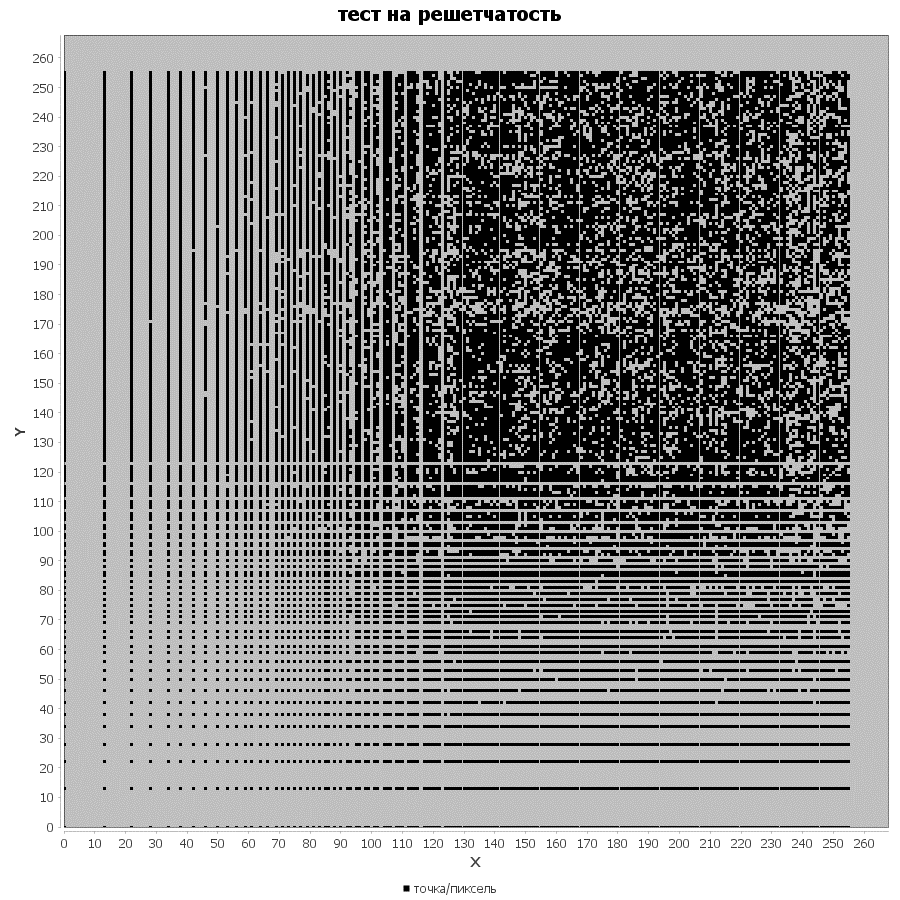
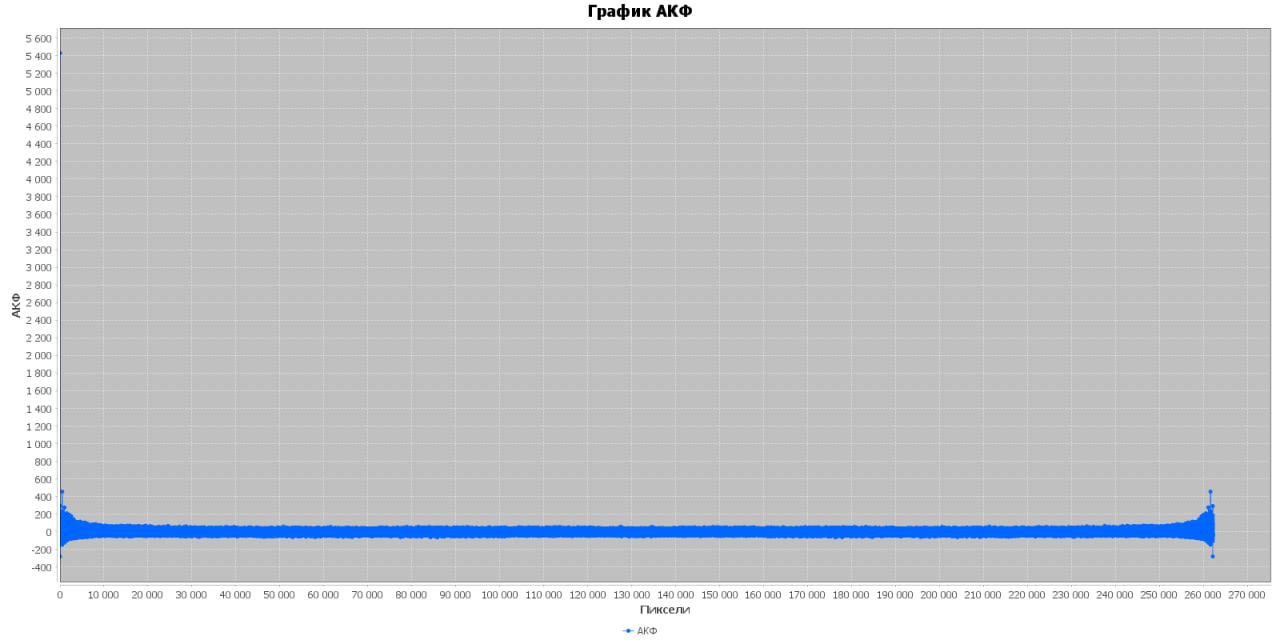


Рисунок 11 – График АКФ для зашифрованного изображения после первого раунда

На графике выше просматривается характерная для последовательностей с заметными внутренними закономерностями «решётка». Поэтому между соседними пикселями изображения все еще существуют функциональные связи.

График АКФ представлен на рисунке 12

­

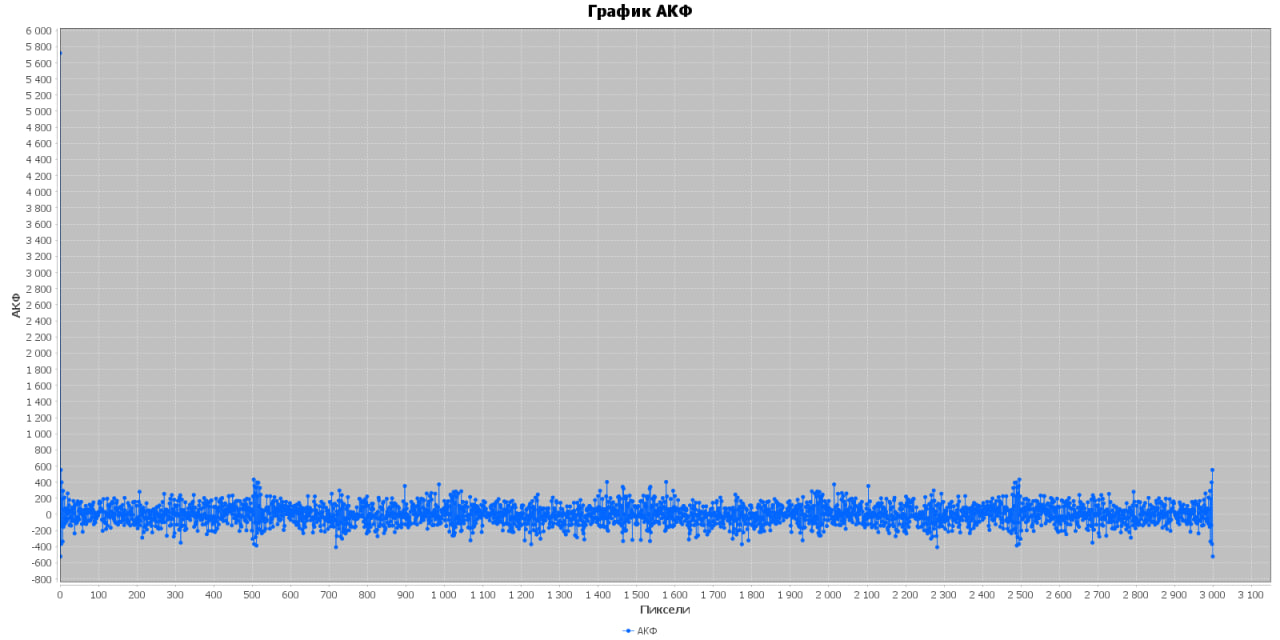


Рисунок 12 - График АКФ для зашифрованного изображения после первого раунда

Из графика АКФ видно, что по своим статистическим свойствам исследуемая последовательность пока не соответствует шумовому процессу, хотя её АКФ имеет ярко выраженный максимум при нулевом сдвиге копии относительно исходной последовательности (в начале координат). Но при ненулевых временных сдвигах значения АКФ исходной последовательности чисел присутствуют периодические участки, что свидетельствует об присутствии корреляции между пикселями в изображении.

**Второй раунд шифрования**

Далее был выполнен второй раунд шифрования изображения, его результат представлен на рисунке 13. Визуально существенных отличий нет Все еще просматриваются основные контуры исходного изображения, значит, изображение было зашифровано неудовлетворительно.



Рисунок 13 - Зашифрованное изображение после второго раунда

Для этого изображения также были проведены тесты. Гистограмма распределения яркости представлена на рисунке 14.

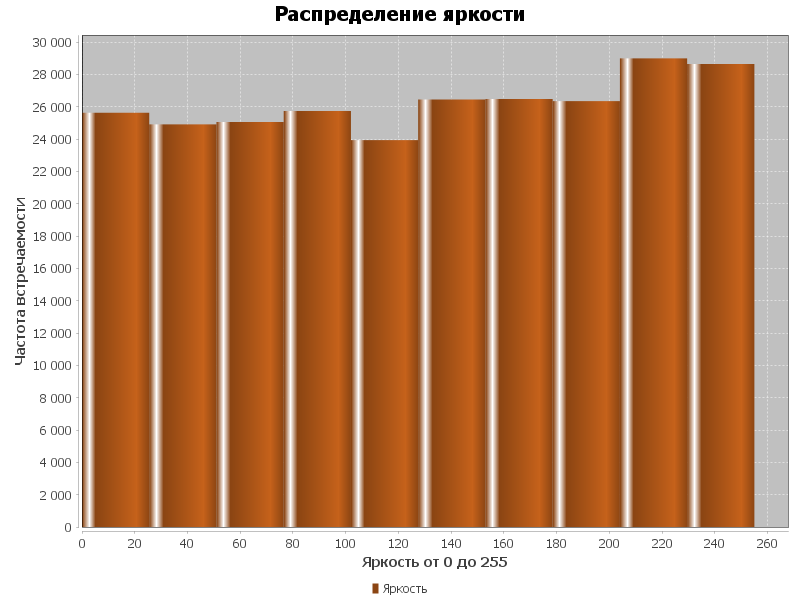


Рисунок 14 – Гистограмма распределения яркости зашифрованного изображения после второго раунда

По этому графику прослеживается неравномерность распределения значений яркостей по всему диапазону, однако есть участки с равномерным распределением. Это свидетельствует о том, что изображение не полностью шумоподобно.

Диаграмма рассеяния (тест на решётчатость) представлена на рисунке 15.

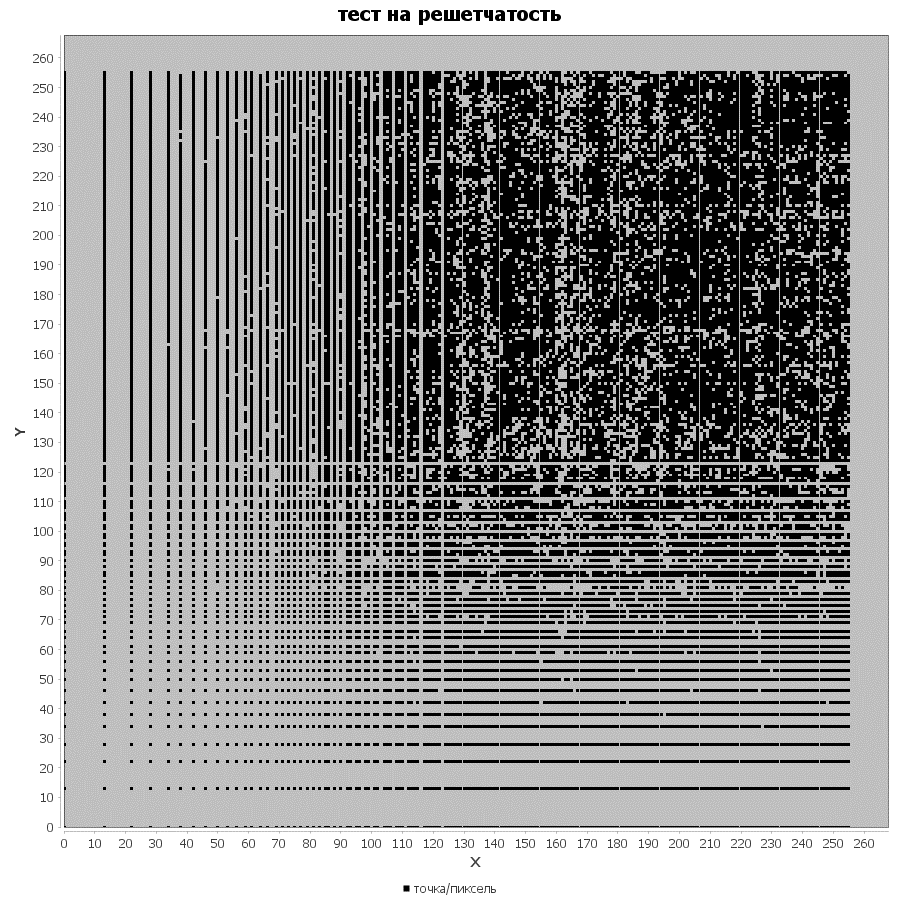
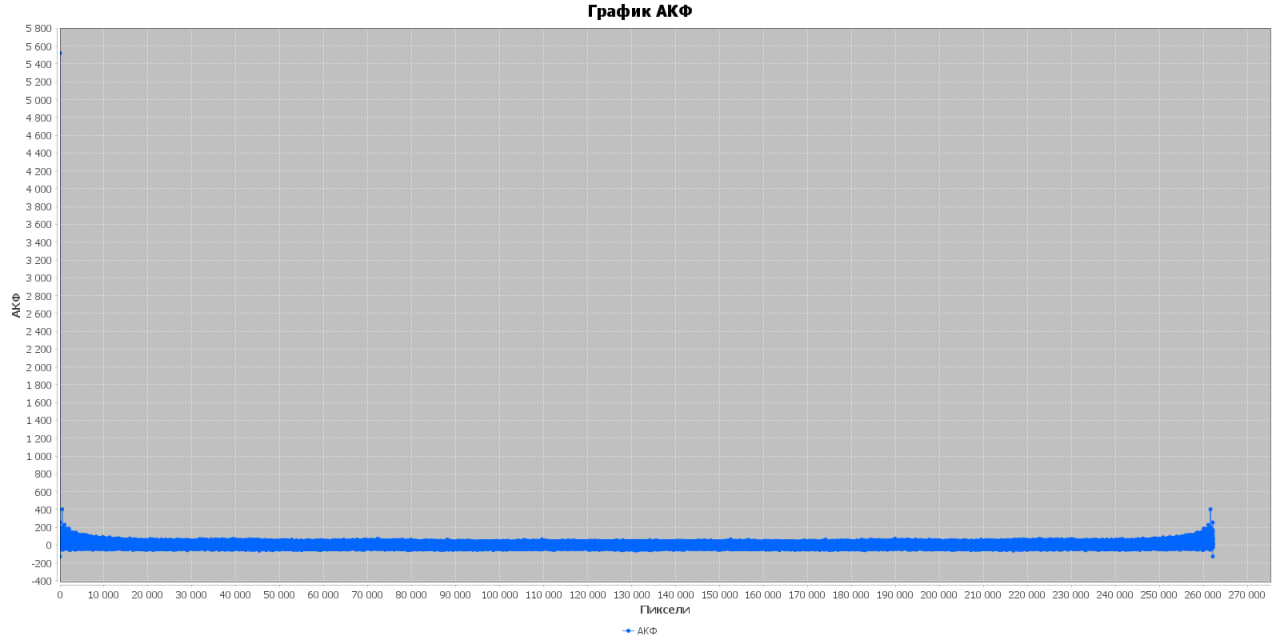


Рисунок 15 – Диаграмма рассеяния для зашифрованного изображения после второго раунда

На графике выше просматривается характерная для последовательностей с заметными внутренними закономерностями «решётка». Поэтому между соседними пикселями изображения все еще существуют функциональные связи.

График АКФ представлен на рисунке 16



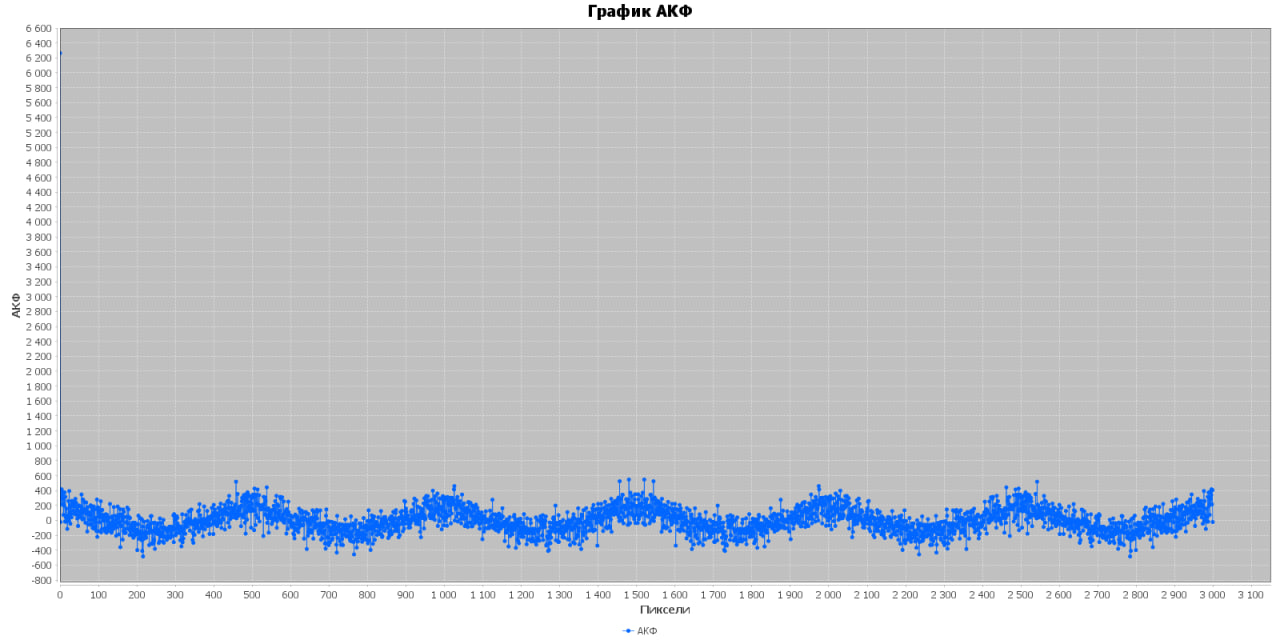


Рисунок 16 - График АКФ для зашифрованного изображения после второго раунда

Из графика АКФ видно, что по своим статистическим свойствам исследуемая последовательность пока не соответствует шумовому процессу, хотя её АКФ имеет ярко выраженный максимум при нулевом сдвиге копии относительно исходной последовательности (в начале координат). Но при ненулевых временных сдвигах значения АКФ исходной последовательности чисел присутствуют периодические участки, что свидетельствует об присутствии корреляции между пикселями в изображении. Однако значение максимумов уменьшилось, следовательно корреляция уменьшилась так же.

**Третий раунд шифрования**

Далее был выполнен третий и итоговый раунд шифрования изображения, его результат представлен на рисунке 17. Визуально основные контуры исходного изображения не просматриваются, значит, изображение было зашифровано удовлетворительно.

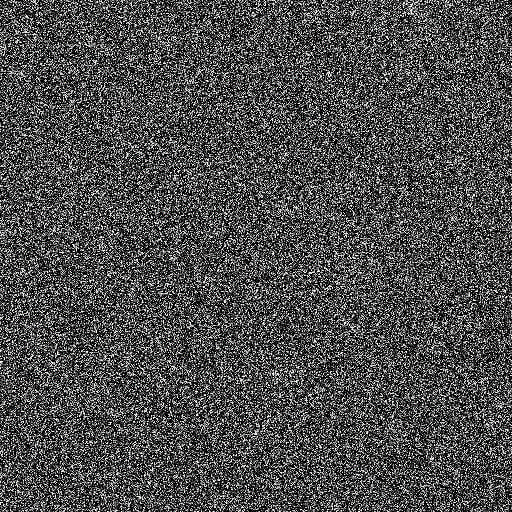


Рисунок 17 – Итоговое зашифрованное изображение

Для этого изображения также были проведены тесты. Гистограмма распределения яркости представлена на рисунке 18.

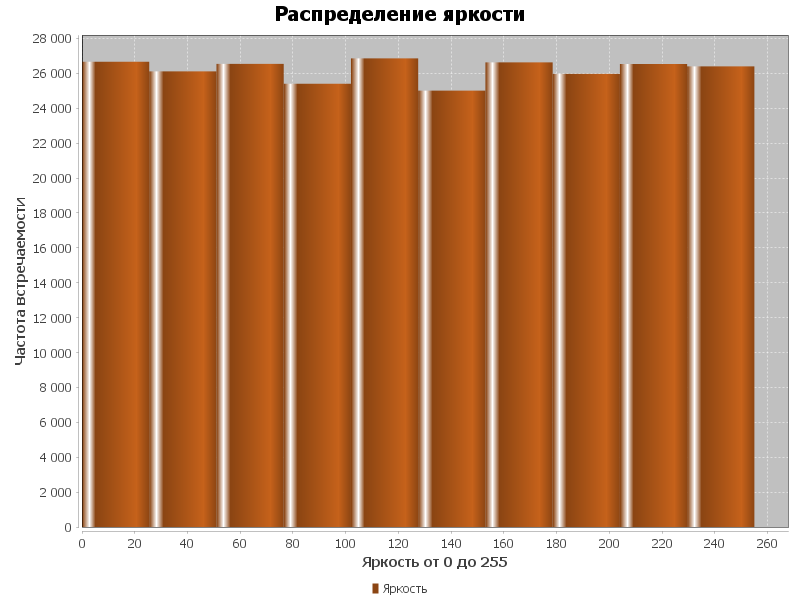


Рисунок 18 – Гистограмма распределения яркости итогового зашифрованного изображения

По этому графику имеем практически равновероятное (равномерное) распределение значений всех значений яркости по диапазону. Это свидетельствует о том, что изображение шумоподобно.

Диаграмма рассеяния (тест на решётчатость) представлена на рисунке 19.

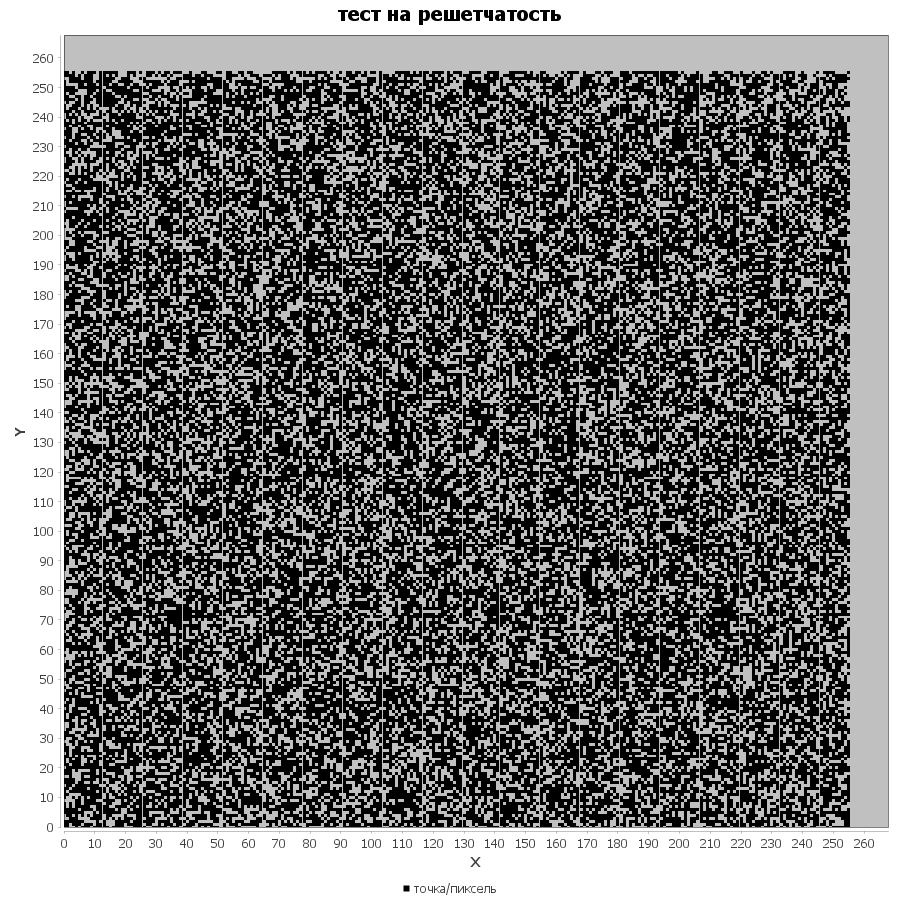
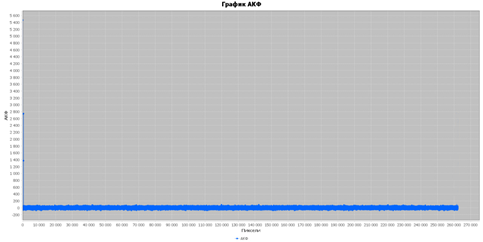


Рисунок 19 – Диаграмма рассеяния для итогового зашифрованного изображения

На этом графике функциональные связи и закономерности между соседними пикселями изображения не просматриваются (скорее всего имеем шумоподобное изображение).

График АКФ представлен на рисунке 20.



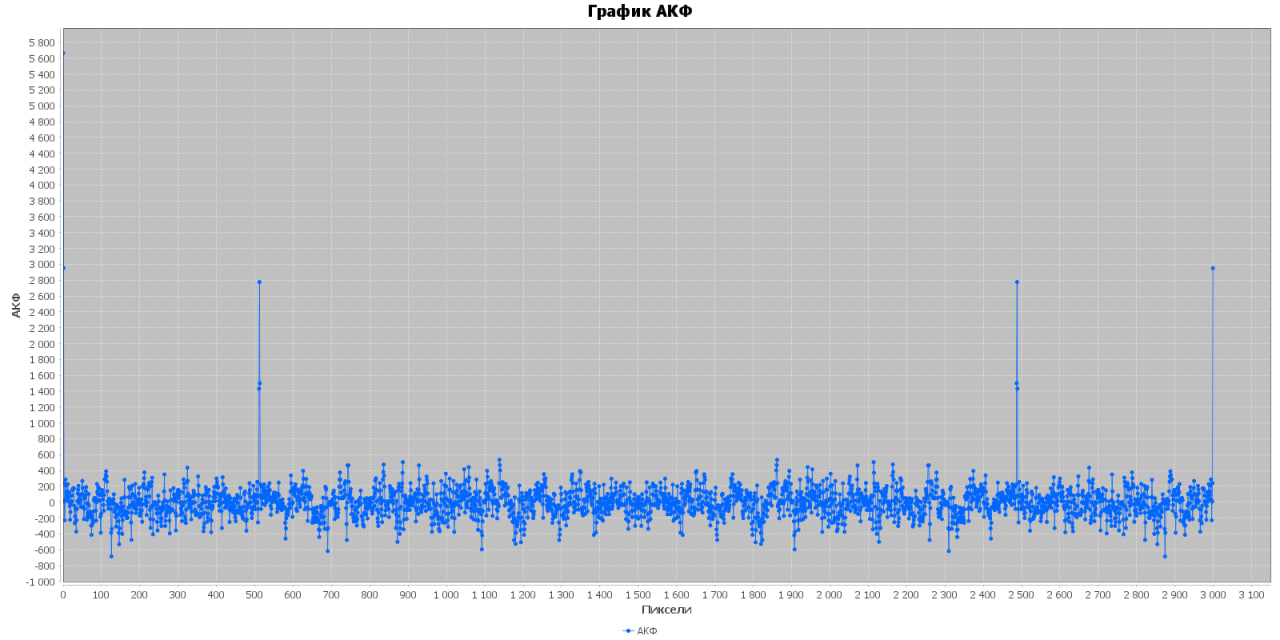


Рисунок 20 - График АКФ для итогового зашифрованного изображения

Из графика АКФ хорошо видно, что по своим статистическим свойствам исследуемая последовательность действительно соответствует шумовому процессу, поскольку её АКФ имеет ярко выраженный максимум при нулевом сдвиге копии относительно исходной последовательности (в начале координат), а при ненулевых временных сдвигах значения АКФ исходной последовательности чисел весьма близки к нулю, что как раз и свидетельствует об отсутствии корреляции между пикселями в изображении.

**Анализ дешифрованного изображения**

Далее было выполнено дешифрование зашифрованного изображения, визуально оно получилось хорошего качества. Результат дешифрования представлен на рисунке 21.



Рисунок 21 – Дешифрованное изображение

Для дешифрованного изображения также были проведены тесты, их результаты в целом похожи на результаты тестов исходного изображения, что говорит о хорошем качестве дешифрования. Гистограмма распределения яркости представлена на рисунке 22.

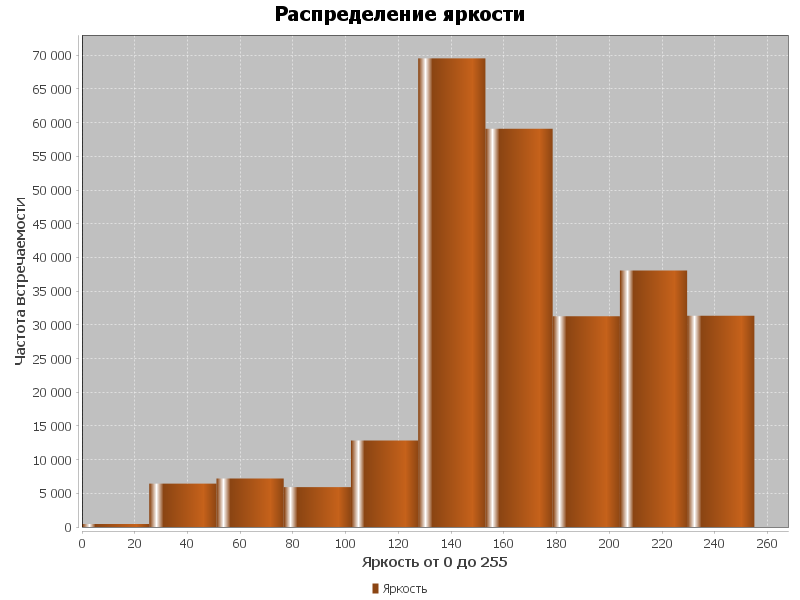


Рисунок 22 – Гистограмма распределения яркости дешифрованного изображения

По этому графику прослеживается существенная неравномерность распределения значений яркостей по всему диапазону. Это свидетельствует о том, что изображение не шумоподобно.

Диаграмма рассеяния (тест на решётчатость) представлена на рисунке 23.

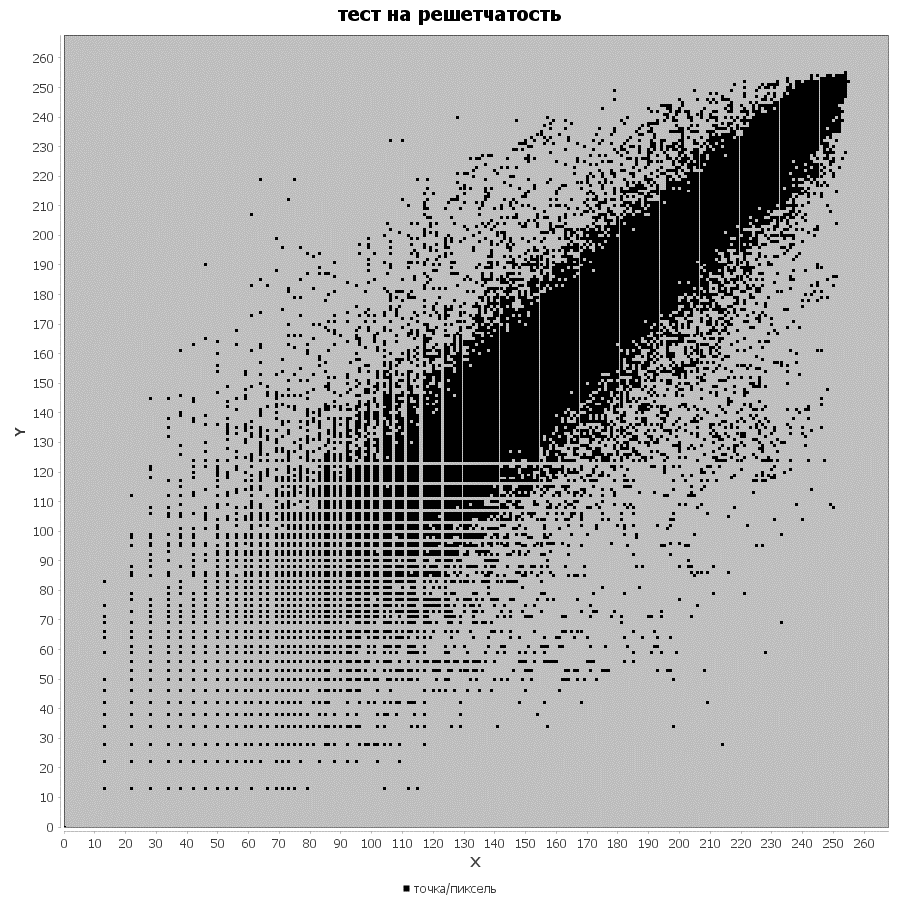
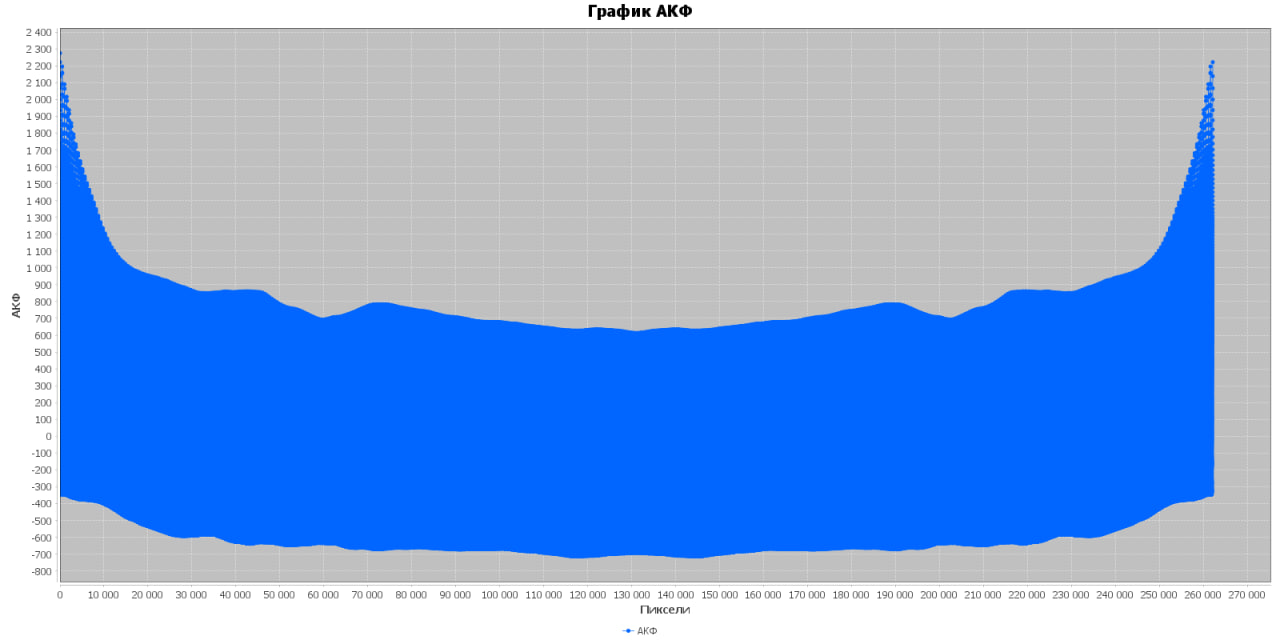


Рисунок 23 - Диаграмма рассеяния дешифрованного изображения

На графике теста изображения на решетчатость, представленном выше, хорошо заметны как существенная неравномерность распределения, так и полное отсутствие в анализируемой последовательности большого ряда значений яркостей пикселей. Поэтому между соседними пикселями изображения существуют функциональные связи.

График АКФ представлен на рисунке 24.



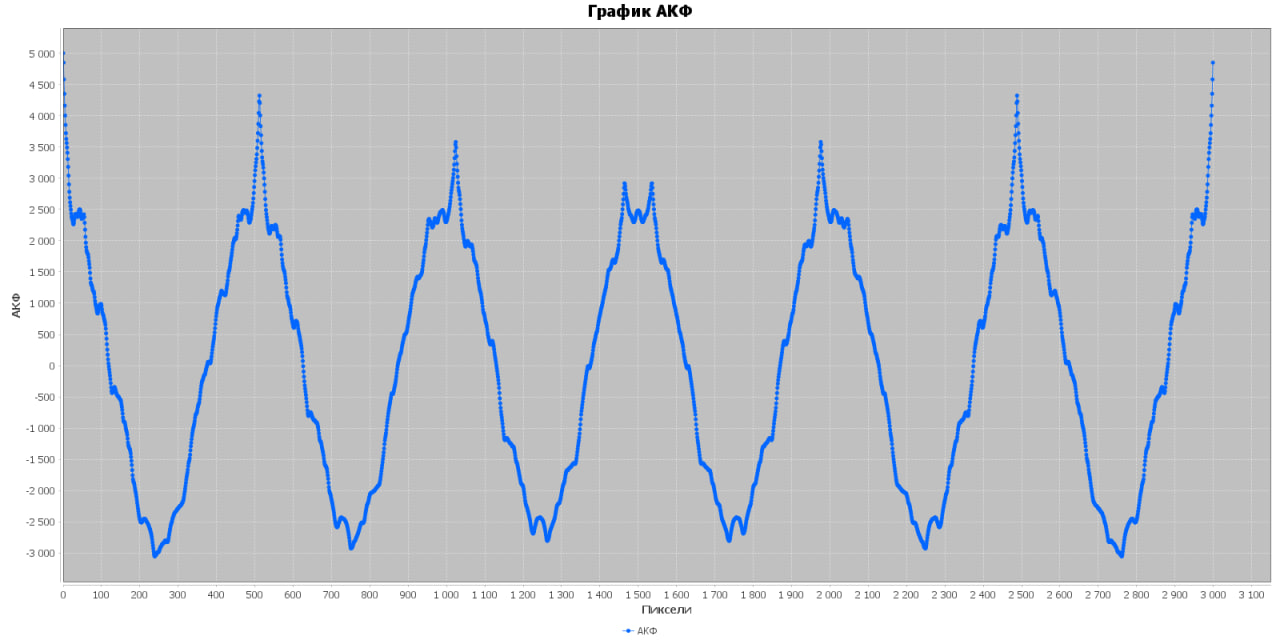


Рисунок 24 – График АФК для дешифрованного изображения

Из графика АКФ хорошо видно, что по своим статистическим свойствам исследуемое изображение не соответствует шуму, поскольку её АКФ не имеет ярко выраженного максимума при нулевом сдвиге копии относительно исходной последовательности (в начале координат), а при ненулевых временных сдвигах значения АКФ исходной последовательности чисел присутствуют периодические участки, что свидетельствует об присутствии корреляции между пикселями в изображении.

**Вывод**

В рамках лабораторной работы было реализовано шифрование с управляемой перестановкой. Реализован алгоритм, производящий шифрование изображения размером 512х512. Изображение делиться на блоки по 16 бит, каждой из которых делится на 2 блока по 8 бит. Блоки участвуют в процессе шифрования друг друга.

Было проведено 3 раунда шифрования. В результате первого раунда изображение обрело зашумленный вид, но на нем видны контуры собаки, что ухудшает сокрытие информации. Второй раунд увеличил визуальную зашумленность (уменьшилась видимость границы дороги) и показал лучшие результатов тестов. На третьем раунде изображение было успешно зашифровано, успешность подтверждают визуальный осмотр и результаты тестов.

Также был реализован алгоритм расшифрования изображения, который путем обратных преобразований качественно расшифровал изображение.