Академия логистики и транспорта

УДК На правах рукописи

**ДАЙЫРБАЕВА ЭЛЬМИРА НУРБЕККЫЗЫ**

**Разработка и исследование стеганографических алгоритмов, ориентированных на внедрение скрытой информации в изображения**

8D06254-Радиотехника, электроника и телекоммуникации

Диссертация на соискание степени

доктора философии (PhD)

Научный консультант:

PhD, ассоц. проф.

Тойгожинова А.Ж.

PhD, ассоц. проф.

Еримбетова А.С.

Зарубежный консультант:

д.т.н., доцент

Нечта И.В.

(г. Новосибирск, РФ)

Алматы -2023

**СОДЕРЖАНИЕ**

[1 ИНТЕРПОЛЯЦИЯ ИЗОБРАЖЕНИЯ В СТЕГАНОГРАФИИ 3](#_Toc135942459)

[2.1 Анализ задачи 3](#_Toc135942460)

[2.2 Понятие интерполяции 4](#_Toc135942461)

[2.3. Общие сведения об интерполяции Лагранжа 5](#_Toc135942462)

[2.4 Метод NMI 7](#_Toc135942463)

[2.5 Метод INMI 10](#_Toc135942464)

[2.6 Стегоанализ INMI метода 14](#_Toc135942465)

[2.7 Выводы по разделу 18](#_Toc135942466)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ЛИТЕРАТУРЫ** 19](#_Toc135942467)

# 2 ИНТЕРПОЛЯЦИЯ ИЗОБРАЖЕНИЯ В СТЕГАНОГРАФИИ

# 2.1 Анализ задачи

В сети Интернет передается огромное количество медиа контента. Большая часть этих данных является источником дохода его создателя и рассматривается как объект защиты авторского права. Учитывая легкость и нулевую стоимость воспроизводства (создания копии) любого файла возникает потребность отслеживать траекторию его пути (от создателя до конечного потребителя, в том числе нелицензионного). Одним из самых эффективных решений данной проблемы является применение методов стеганографии, которые используют секретные сообщения, встраиваемые в файл. Такие сообщения могут либо идентифицировать автора (цифровые водяные знаки), либо конечного потребителя (цифровой отпечаток пальца).

В научных публикациях встречаются работы, направленные на создание новых методов внедрения и на создание новых методов обнаружения (стегоанализа). Последние используются для выявления фактов утечки информации, например, через служебную переписку.

Таким образом, возникает острая необходимость анализа существующих методов внедрения и создания новых и эффективных методов внедрения скрытых сообщений. Так один из современных подходов стеганографии базируется на методах интерполяции. В данном исследовании изучается применение методов интерполяции для внедрения сообщения, которые, в некотором смысле, является дискретным аналогом голограммы, и обычно применяется для восстановления сигналов и изображений, подвергшихся воздействиям и приведшим к большой потере информации.

В данной главе проведен анализ эффективности методов внедрения скрытых сообщений в изображение: INMI и NMI [115].

В ходе работы было выполнено:

* Подготовка тестовых наборов изображений различного типа и разрешения для использования в качестве контейнеров для скрытой информации.
* Разработано программное обеспечение для внедрения скрытой информации в изображения с использованием известных ранее алгоритмов стеганографии.
* Произведена оценка качества внедрения информации в изображения и экспериментально проанализирована скорость работы алгоритмов на тестовом наборе изображений.
* Оценена устойчивость рассматриваемых алгоритмов к атакам, использующим изменение цветовой палитры.
* Выполнено сравнение полученных результатов с другими существующими методами стеганографии.

# 2.2 Понятие интерполяции

Интерполяция изображений [116] – это процесс восстановления пикселей изображения, которые были потеряны или не были предоставлены, в целях улучшения качества изображения или изменения его размера.

Одним из самых распространенных методов интерполяции изображений является метод бикубической интерполяции, который использует окрестности 16 ближайших пикселей, чтобы определить значение пропущенного пикселя.

Интерполяция также может быть использована для увеличения размера изображения без потери качества. Этот процесс называется масштабированием. Наиболее распространенные методы масштабирования включают билинейную и бикубическую интерполяцию.

Однако, важно понимать, что использование интерполяции может привести к некоторой потере качества и ухудшению четкости изображения, особенно если она применяется несколько раз или в условиях низкой разрешающей способности изображения.

Бикубическая интерполяция [117] – это метод интерполяции, который используется для увеличения размера изображений, чтобы получить более гладкий и качественный результат, чем при использовании других методов интерполяции, таких как билинейная интерполяция. Бикубическая интерполяция использует более сложную математическую модель, чем билинейная интерполяция, для определения значений новых пикселей. Она основывается на кривых сплайнах, которые проходят через четыре ближайших пикселя в исходном изображении. Эти кривые позволяют определить значения новых пикселей, которые более точно соответствуют исходным данным.

Бикубическая интерполяция [118-120] использует 16 ближайших пикселей для вычисления значения нового пикселя, что позволяет получить более гладкое и качественное изображение, чем билинейная интерполяция. Однако, из-за более сложной математической модели, бикубическая интерполяция может быть более ресурсоемкой, чем другие методы интерполяции, и может потребовать больше времени для выполнения. В целом, бикубическая интерполяция является более точным и качественным методом интерполяции, чем билинейная интерполяция, и может быть полезной для увеличения размера изображений в задачах обработки изображений, таких как фотографии, видео и медицинские изображения.

Один из распространенных методов интерполяции для масштабирования изображений - это билинейная интерполяция [121]. Этот метод использует линейные интерполяционные функции для вычисления значений пикселей, которые не были предоставлены при изменении размера изображения. Билинейная интерполяция определяет значения пропущенных пикселей на основе четырех ближайших пикселей [122-124].

Для достижения наилучшего качества при масштабировании изображений, может потребоваться использование более сложных методов обработки, таких как алгоритмы супер-разрешения.

Ниже приведен краткий обзор нескольких новых работ, связанных с интерполяцией изображений:

1. Работа [125] представляет новый метод интерполяции, который использует глубокое обучение для генерации дополнительных кадров между существующими кадрами в видео. Метод основан на модели глубокого обучения, которая была обучена на большом наборе данных видео и позволяет генерировать более плавные и качественные видеокадры.
2. Статья [126] представляет новый метод интерполяции, который использует адаптивную свертку для комбинирования процессов интерполяции и восстановления изображения. Метод позволяет увеличить размер изображения и снизить шум, используя общую модель свертки, которая может адаптироваться к различным типам изображений.
3. Исследование [127] представляет новый метод интерполяции, который использует глубокое обучение для генерации интерполированных изображений. Метод основан на модели сверточных нейронных сетей, которая была обучена на большом наборе данных изображений и позволяет генерировать более качественные и плавные изображения при увеличении их размера.

Эти работы и многие другие [128-131] связанные с интерполяцией изображений продолжают исследовать новые методы и подходы для улучшения качества интерполированных изображений в различных областях, таких как обработка видео, компьютерное зрение, медицинская обработка изображений и т.д.

Одним из основных преимуществ стеганографии с применением методов интерполяции является относительно высокая устойчивость к атакам. Это связано с тем, что замена некоторых пикселей на значения, содержащие скрытую информацию, не изменяет значительно статистические свойства изображения и не приводит к заметным артефактам на изображении. Однако, методы интерполяции могут приводить к потере части информации в изображении, особенно при использовании более сложных методов интерполяции.

# 2.3. Общие сведения об интерполяции Лагранжа

Интерполяция Лагранжа [132] - это метод аппроксимации функции с помощью полинома, проходящего через заданные точки. Этот метод был разработан именно Жозефом Лагранжем в XVIII веке.

Интерполяция Лагранжа является распространенным методом обработки сигналов и изображения [133-136]. Пусть в отрезке  в заданных точках  известны значения функции . Вид многочлена порядка , , значение которого в точках узла равно значению функции  (Eq.2.1):

 (2.1)

Многочлен  (Eq.2.2):

 (2.2)

называется интерполяционным многочленом, построенным по точкам . С помощью интерполяционной формулы Лагранжа можно записывать в виде линейной комбинации значений интерполяции функции  в точках узлов (Eq 2.3):

 (2.3)

Учитывая все соответствующие условия [136], можно увидеть, что определяется как в формуле (Eq.2.4):

 (2.4)

Таким образом, интерполяционный многочлен Лагранжа имеет следующий вид (Eq.2.5):

 (2.5)

Интерполяция Лагранжа имеет некоторые ограничения, включая проблему погрешности интерполяции на концах интервала и проблему слишком высокой степени полинома, что может привести к неустойчивости при аппроксимации. Однако, метод Лагранжа все еще широко используется в научных и инженерных приложениях, благодаря своей простоте и интуитивной понятности.

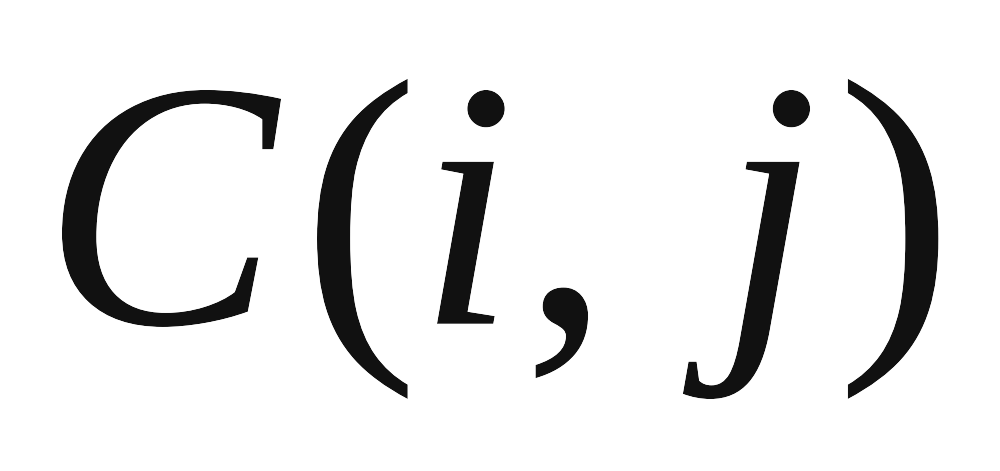
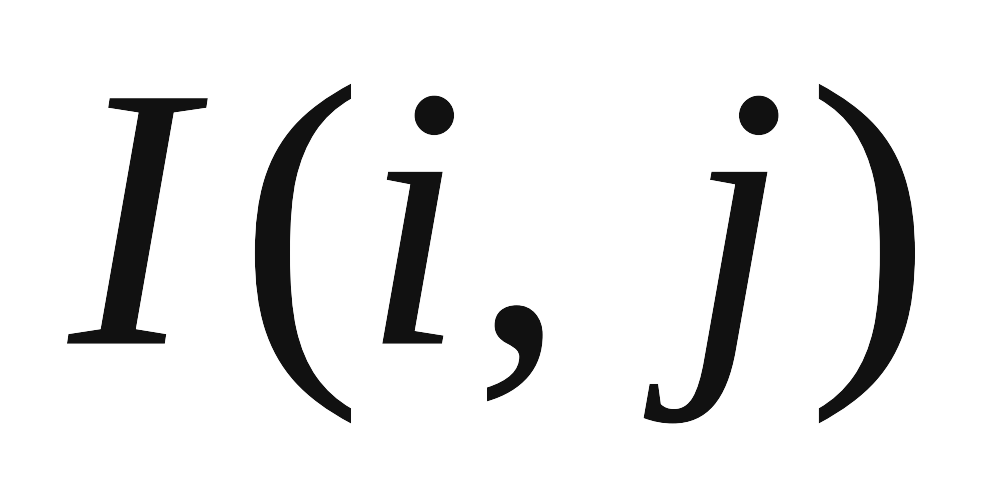
Интерполяция Лагранжа может использоваться в стеганографии для встраивания секретных сообщений в цифровые изображения. Один из подходов заключается в том, чтобы изменять значения пикселей изображения таким образом, чтобы они соответствовали значениям интерполяционного полинома Лагранжа, проходящего через секретное сообщение. Чтобы восстановить секретное сообщение, можно применить обратную операцию интерполяции Лагранжа, используя координаты выбранных пикселей и их измененные значения, чтобы вычислить значения секретного сообщения.

Однако, использование интерполяции Лагранжа для стеганографии может иметь некоторые ограничения, такие как возможность обнаружения внедрения секретного сообщения с помощью стегоанализа. Кроме того, этот метод может быть уязвим к атакам типа сжатия изображений, которые могут изменять значения пикселей и повредить секретное сообщение.

# 2.4 Метод NMI

Neighbor mean interpolation (NMI) [137]- это метод интерполяции, который используется для восстановления изображений с низким разрешением. Этот метод основан на идее усреднения значений яркости пикселей соседних пикселей. При использовании метода NMI пропущенный пиксель восстанавливается путем усреднения значений яркости соседних пикселей. Для каждого пропущенного пикселя вычисляется среднее значение яркости соседних пикселей, которое затем используется для восстановления пропущенного пикселя.

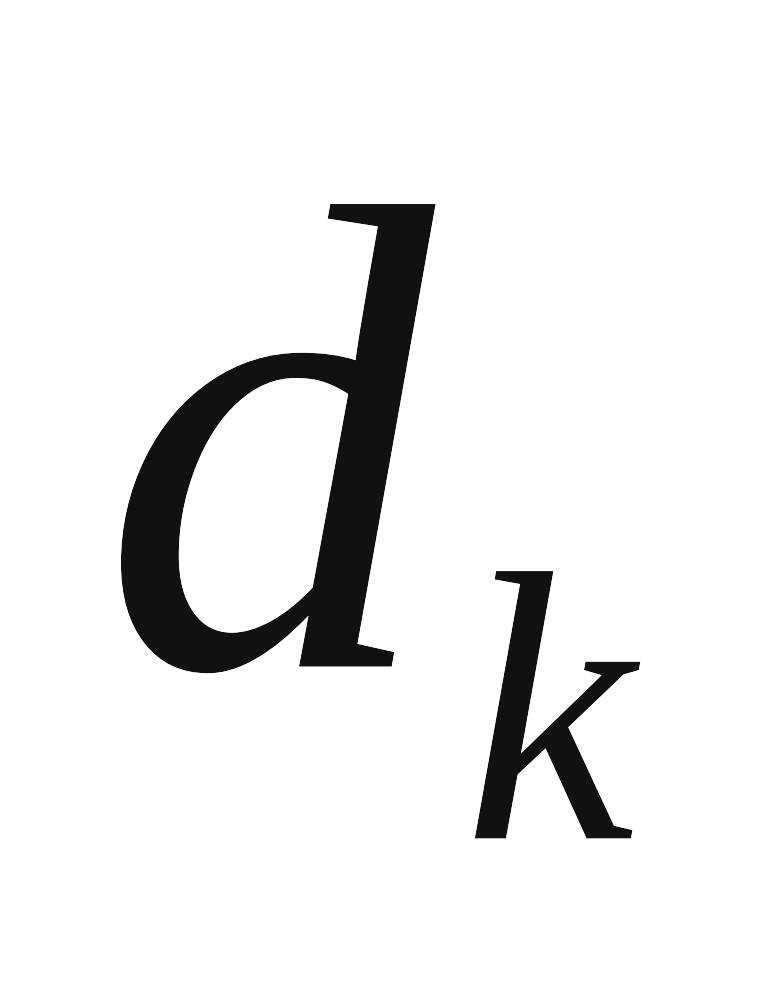
*Рассмотрим подробнее метод NMI*. В данном алгоритме интерполяция изображения осуществляется в следующем виде: пусть – значение пикселя оригинального изображения, тогда значение пикселя изображения-контейнера будет вычисляться по следующей форме (2.6):



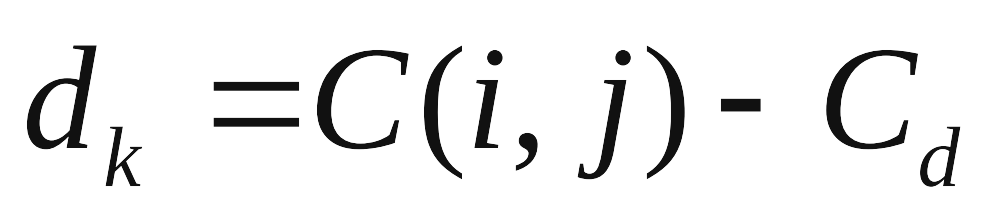
 (2.6)

где .

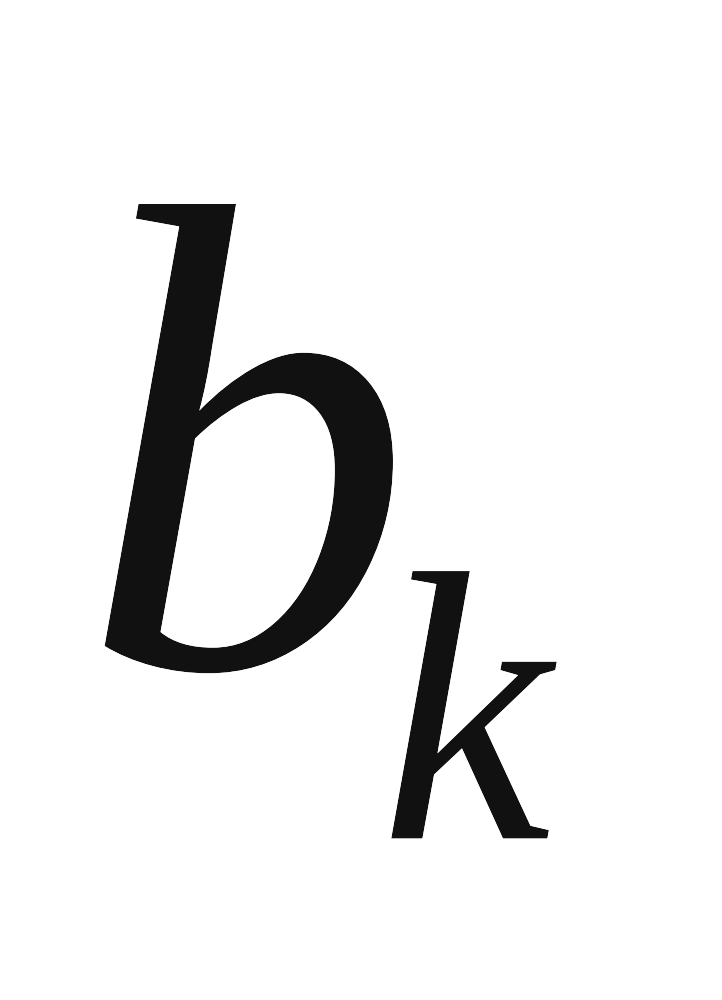
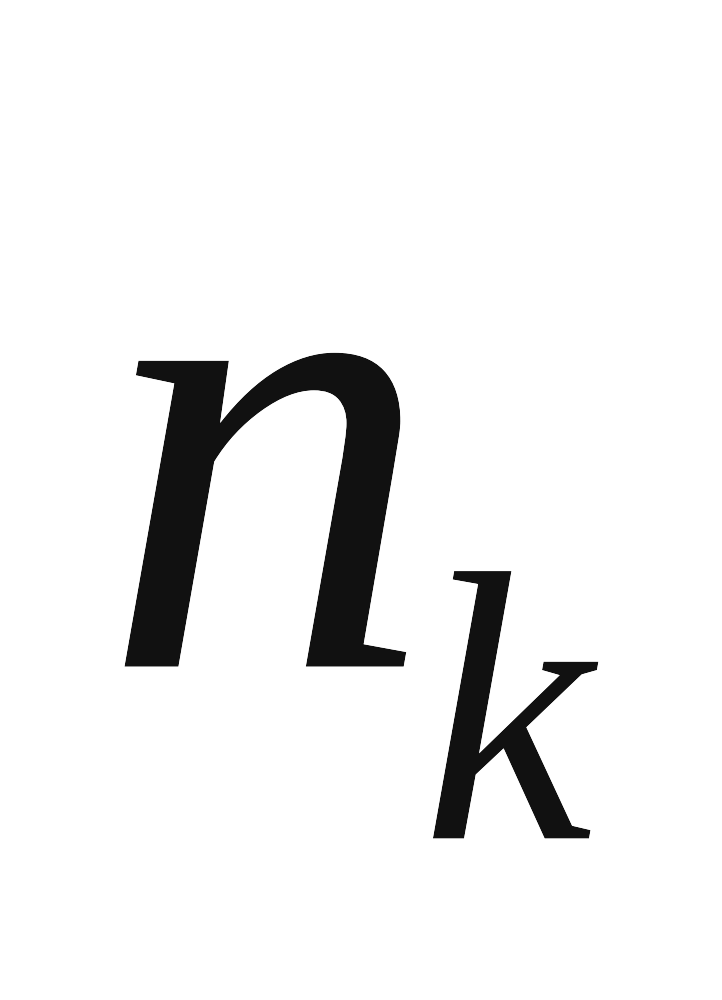
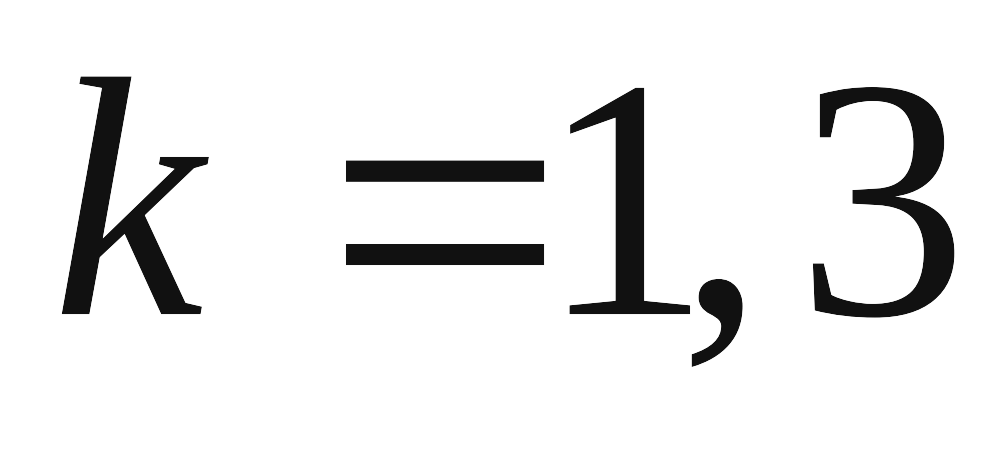
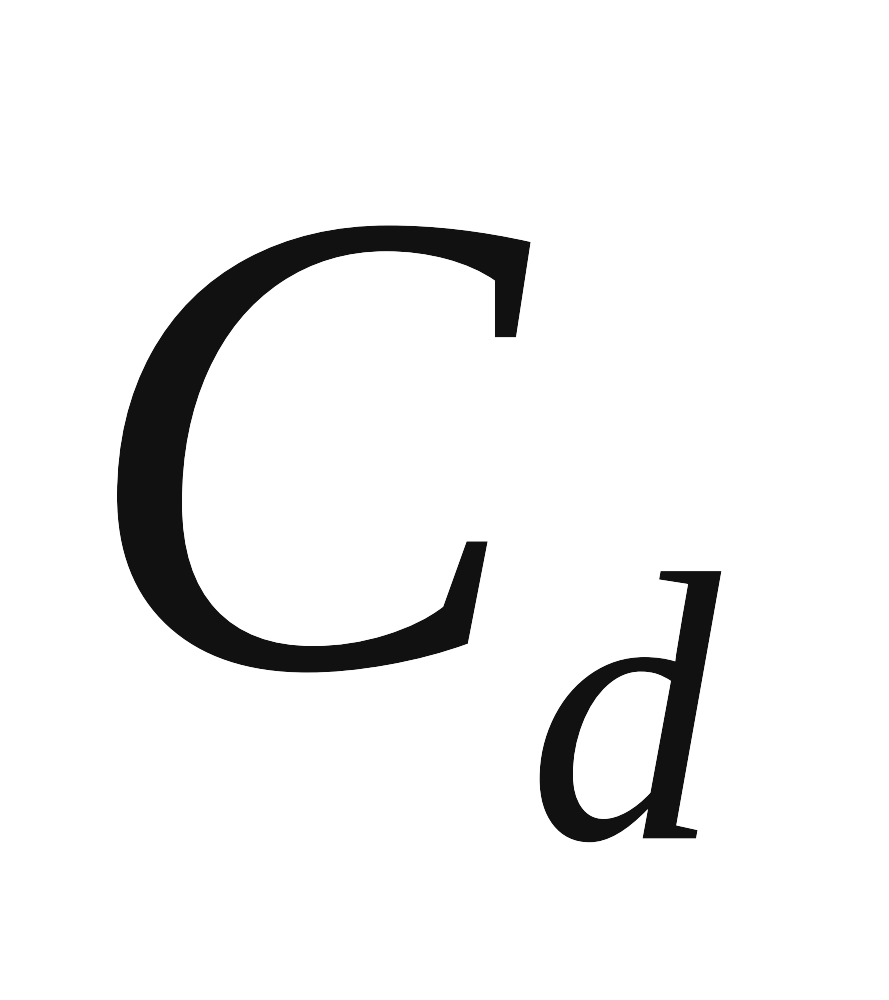
Значение пикселей стегоизображения рассчитываются следующим образом. Для каждого из непересекающихся блоков размером 2х2 пикселя требуется найти величину по формуле [2.7]



, (2.7)



где – левый верхний пиксель блока, , после чего рассчитывается количество битов , которое может быть встроено в блок и его целочисленные представление , и вычисляются значения соответствующих пикселей стегоизображения.



Емкость встраивания по данному методу оказались меньше, при этом возросло качество полученного стегоизображения.

Метод NMI является простым и эффективным методом интерполяции, который может быть использован для восстановления изображений с низким разрешением. Однако, как и любой другой метод интерполяции, он имеет свои ограничения, включая возможность искажения текстур и деталей изображения, особенно при восстановлении изображений с высокой степенью разрешения. Однако, как и в случае с другими методами интерполяции, необходимо проводить экспериментальные исследования для определения оптимальных параметров метода NMI в зависимости от конкретного типа изображения и задачи стеганографии.

Существует множество работ, посвященных методу интерполяции NMI. Некоторые из них представлены ниже:

В статье [138] авторы рассмотрели известный метод NMI, на основе которого они впервые построили новую схему скрытия данных на основе интерполяции изображений (IIDH). В своих исследованиях они использовали интерполяцию среднего значения соседей (NMI) для создания контейнера, с применением LSB внедрения и процесс оптимальной настройки пикселей вместо простого добавления для улучшения визуального качества стегоизображения. По результатам эксперимента: авторы разработали новых схем IIDH, основанные на подходах NMI и DH (LSB и APAP); PSNR всех схем IIDH были экспериментально и теоретически оценены. По мнению авторов статьи, их предложенная схема имеет более высокий PSNR, чем исходная схема NMI.

В статье [139] авторы предложили такой метод скрытие данных, который позволяет восстановить исходное изображение и реализуется с использованием метода интерполяции. Такой метод называется обратимым и реализуется путем корректировки интерполированных пикселей после применения интерполяции NMI. По два бита секретных данных выстраиваются в каждый интерполированный пиксель изображения контейнер, что приводит к среднему значению PSNR 26,94 дБ и полезной нагрузке 1,5 бит/с. Экспериментальные результаты доказывают, что предложенная схема авторами превосходит самые современные схемы с точки зрения качества изображения и скрытности.

В статье [140] разработан обратимый метод сокрытия данных, который использует интерполяцию и метод LSB. Под обратимостью понимается возможность восстановить исходное изображение без внедрения. Здесь, во-первых, используются методы интерполяции для увеличения и уменьшения масштаба изображения контейнера с целью повышения емкости и качества. Во-вторых, метод подстановки LSB используется для встраивания секретные данные. В рисунках 2.1 – 2.2 Приведены процесс встраивания замены LSB и пример метода интерполяции по соседним пикселям:

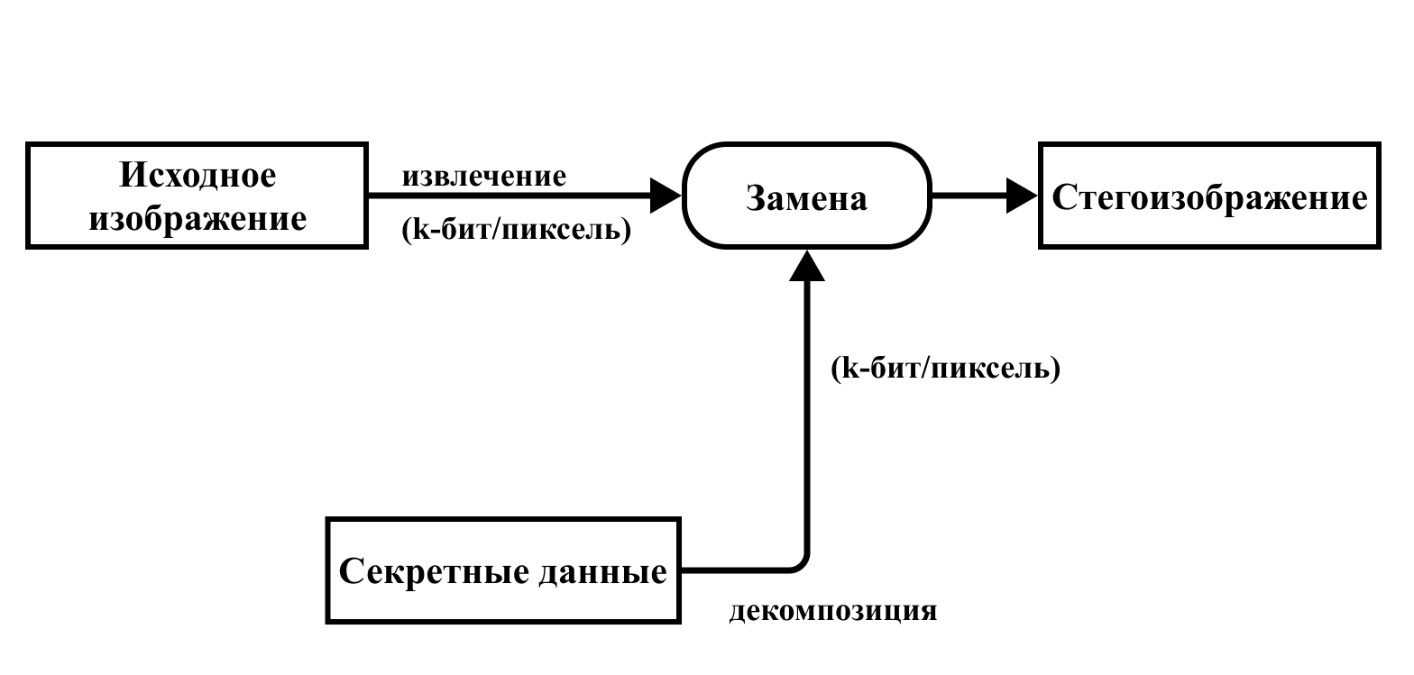


Рисунок 2.1 - Процесс встраивания замены LSB [140]

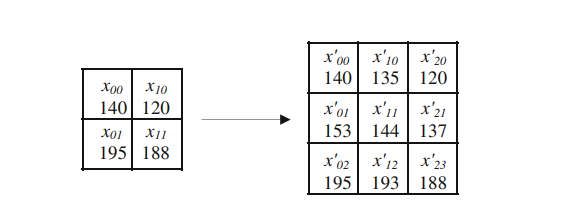


Рисунок 2.2 –Пример метода интерполяции по соседним пикселям [140]

Также согласно графику (рис 2.3) можно увидеть сравнение различных методов по емкости встраивания (бит):

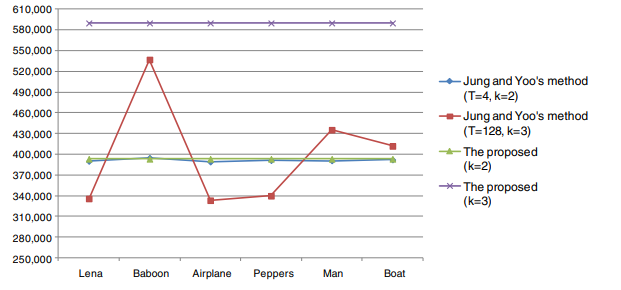


Рисунок 2.3 - Сравнение емкости встраивания (бит) [140]

В данной статье пиковое отношение сигнал/шум (PSNR) используется для измерения скрытности и емкости для объема встроенных данных. Экспериментальные результаты показывают, что предлагаемый метод позволяет внедрять большое количество секретных данных при сохранении высокого визуального качества. Результаты показали, что предложенный метод дает хорошие результаты (PSNR 37,54 дБ (k=3) и 43,94 дБ (k=2)) и работает быстрее, чем другие методы интерполяции.

Таким образом, метод NMI является популярным методом интерполяции в области восстановления изображений с низким разрешением. Различные улучшения и модификации метода NMI позволяют достигать лучших результатов в зависимости от конкретной задачи восстановления изображения.

# 2.5 Метод INMI

Improved neighbor mean interpolation (INMI) [137] - это метод интерполяции, который основан на улучшенной версии метода neighbor mean interpolation (NMI). Этот метод используется для восстановления изображений с низким разрешением путем усреднения значений яркости пикселей соседних пикселей.

В методе INMI соседние пиксели, расположенные вокруг пропущенного пикселя, разделяются на две группы: ближние и дальние пиксели. Ближние пиксели находятся в непосредственной близости от пропущенного пикселя, а дальние пиксели находятся на большем расстоянии. Для каждой группы пикселей вычисляется среднее значение яркости, которое затем усредняется для получения итогового значения яркости пропущенного пикселя.

Одним из преимуществ метода INMI является то, что он позволяет учитывать пиксели, лежащие в некоторой окрестности контекст изображения, при интерполяции, что может улучшить качество восстановленного изображения. Однако, как и любой другой метод интерполяции, INMI также имеет свои ограничения, включая возможность искажения текстур и деталей изображения, особенно при восстановлении изображений с высокой степенью разрешения.

Метод INMI может использоваться в стеганографии для восстановления изображений с низким разрешением, которые могут быть использованы для внедрения скрытой информации. Однако, как и в случае с другими методами интерполяции, необходимо проводить экспериментальные исследования для определения оптимальных параметров метода INMI в зависимости от конкретного типа изображения и задачи стеганографии.

Метод INMI демонстрирует более высокую точность интерполяции, чем классический метод ближайшего соседа, а также является более быстрым и эффективным, чем другие методы интерполяции, такие как билинейная и бикубическая интерполяция. Он может быть использован в различных задачах обработки изображений, таких как масштабирование, поворот, искажение и др. Метод интерполяции INMI был предложен относительно недавно, в 2018 году, поэтому исследований, посвященных этому методу, пока не так много. Однако уже было опубликовано несколько работ, в которых исследовалась эффективность метода INMI в различных задачах обработки изображений.

Например, в работе [141] было проведено сравнение различных методов интерполяции изображений, включая INMI, на основе качественной модели оценки изображений. Результаты исследования показали, что метод INMI демонстрирует высокую точность интерполяции и превосходит другие методы, такие как бикубическая интерполяция.

Например, в статье [142], авторы сравнивают различные методы интерполяции изображений, включая INMI, и описывают его высокую точность и быстродействие.

Также, в статье [143], авторы рассматривают применение метода INMI для увеличения размера изображений и показывают его преимущества в сравнении с другими методами интерполяции.

В статье [144], авторы предложили метод INMI для интерполяции изображений с низким разрешением. Ниже представлена схема извлечения данных (рис. 2.4):

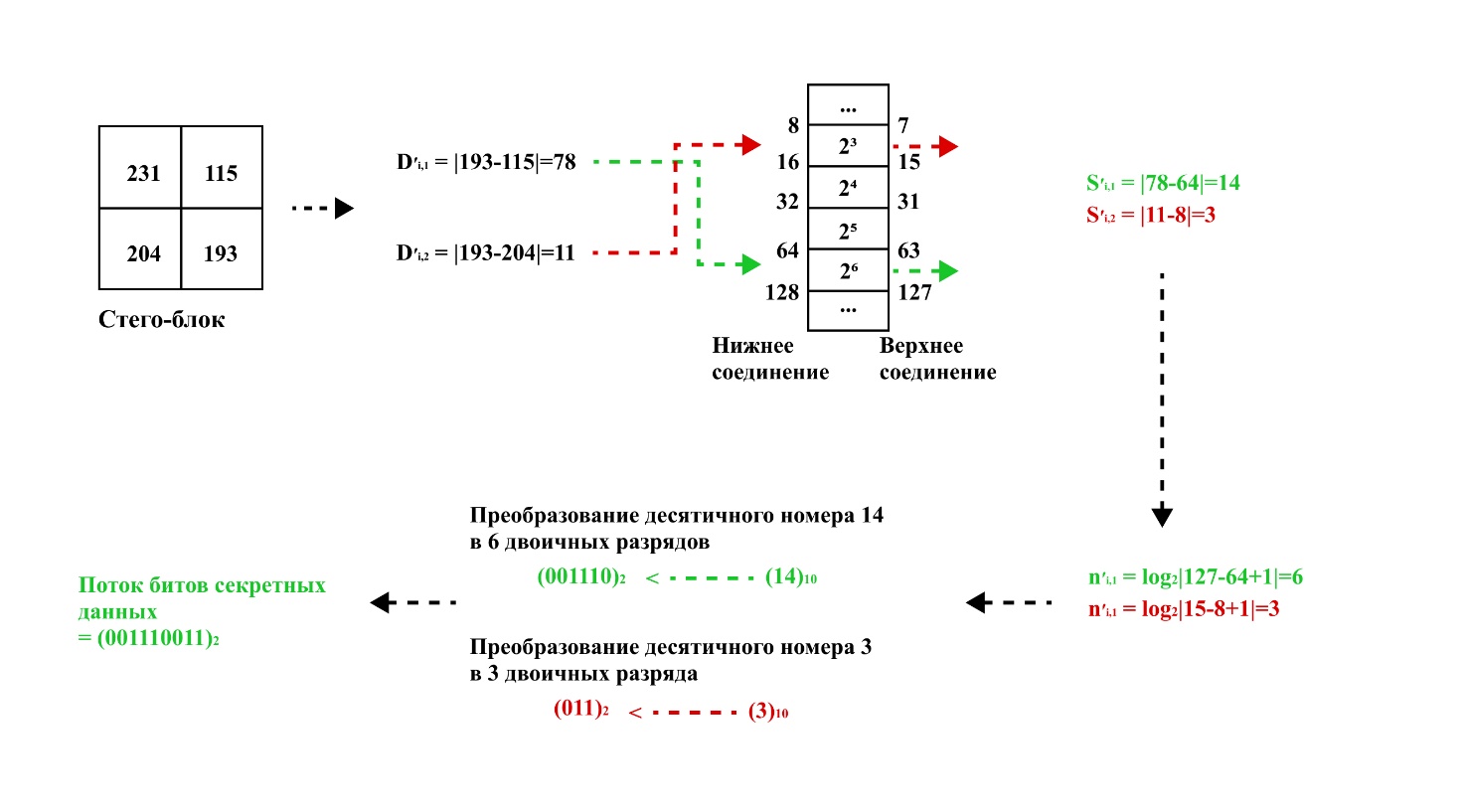


Рисунок 2.4- Пример схемы извлечения [144]

Результаты экспериментов показали, что INMI, являющийся расширением NMI, имеет гораздо меньшие вычислительные затраты. Согласно результатам эксперимента, можно увидеть, что производительность нового предложенного метода интерполяции изображений с точки зрения качества изображения увеличена с 4,87% до 28,77% по сравнению с ENMI. Кроме того, экспериментальные результаты предложенной схемы сокрытия данных показывают, что полезная нагрузка увеличивается с 0,87% до 73,82% без увеличения искажения изображения по сравнению с другими методами.

В статье [145], представлены обратимые методы сокрытия данных с использованием методов интерполяции и проанализированы возможности встраивания и качество визуального изображения. Авторы представили базовую схему обратимого сокрытия данных на основе интерполяции (Рис.2.5)

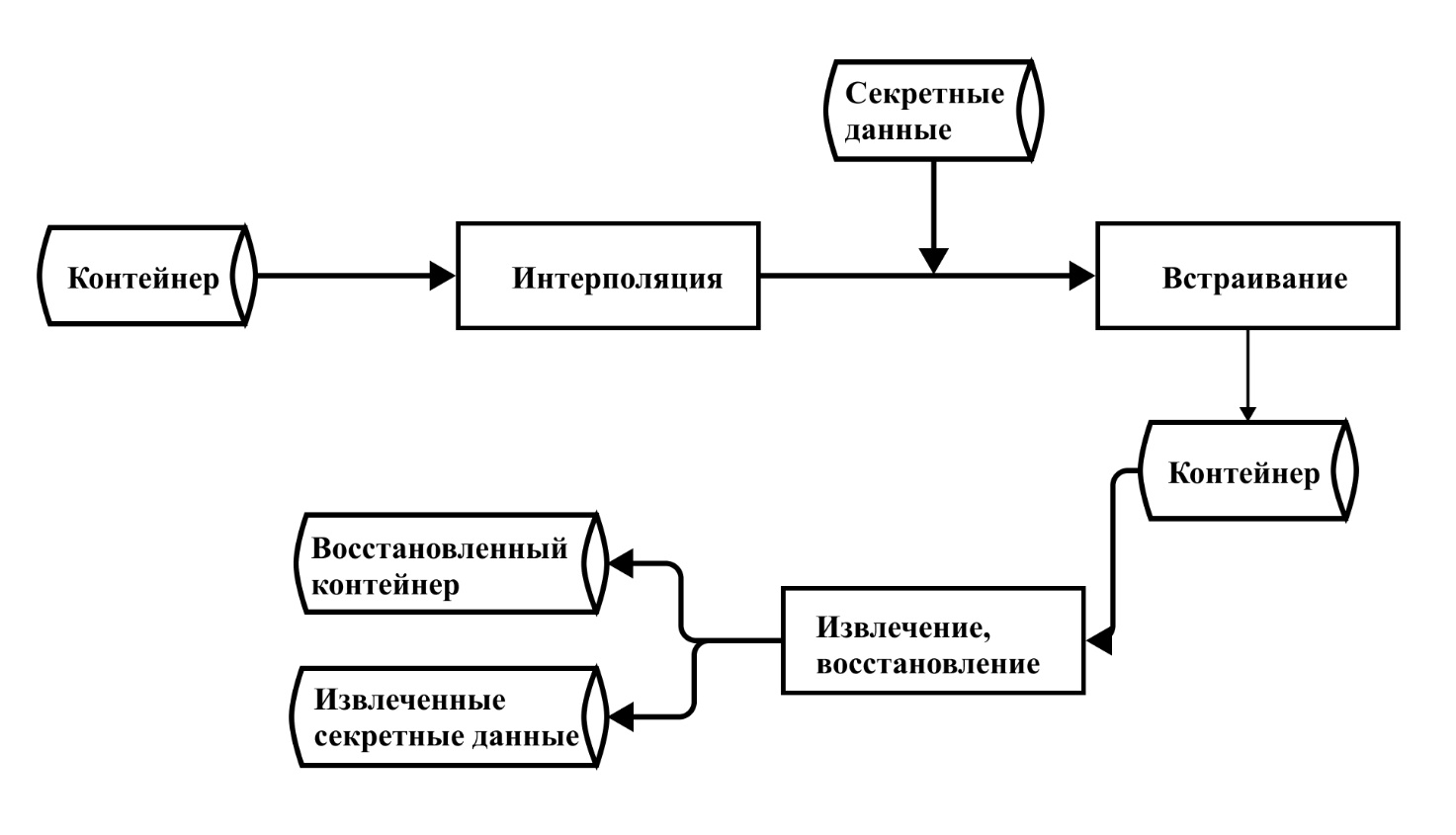
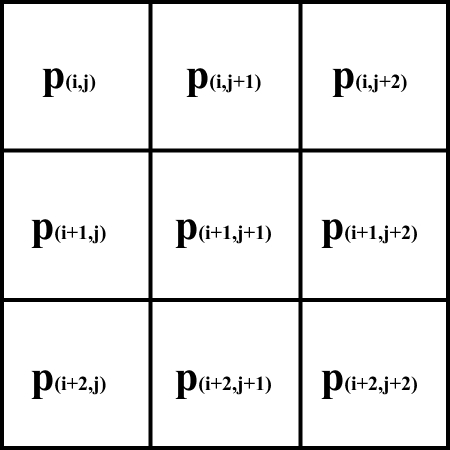
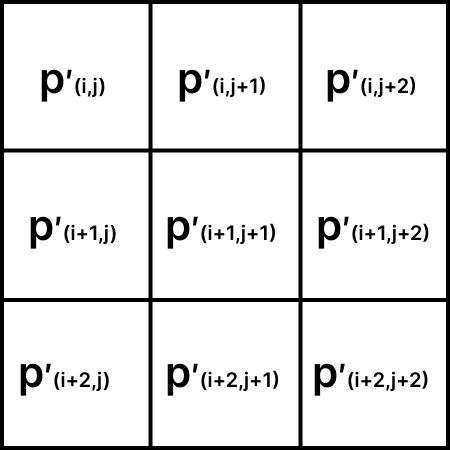


Рисунок 2.5 - Базовая схема обратимого сокрытия данных на основе интерполяции [145]

Также авторы наглядно показали значения пикселей изображения контейнера и стего-изображения (рис. 2.6):



а) пикселы контейнера



б) пикселы стегоконтейнера

Рисунок 2.6- Значения пикселей изображения контейнера и стего-изображения [145]

Авторами были рассмотрены ниже представленные методы (рис.2.7-рис.2.9):

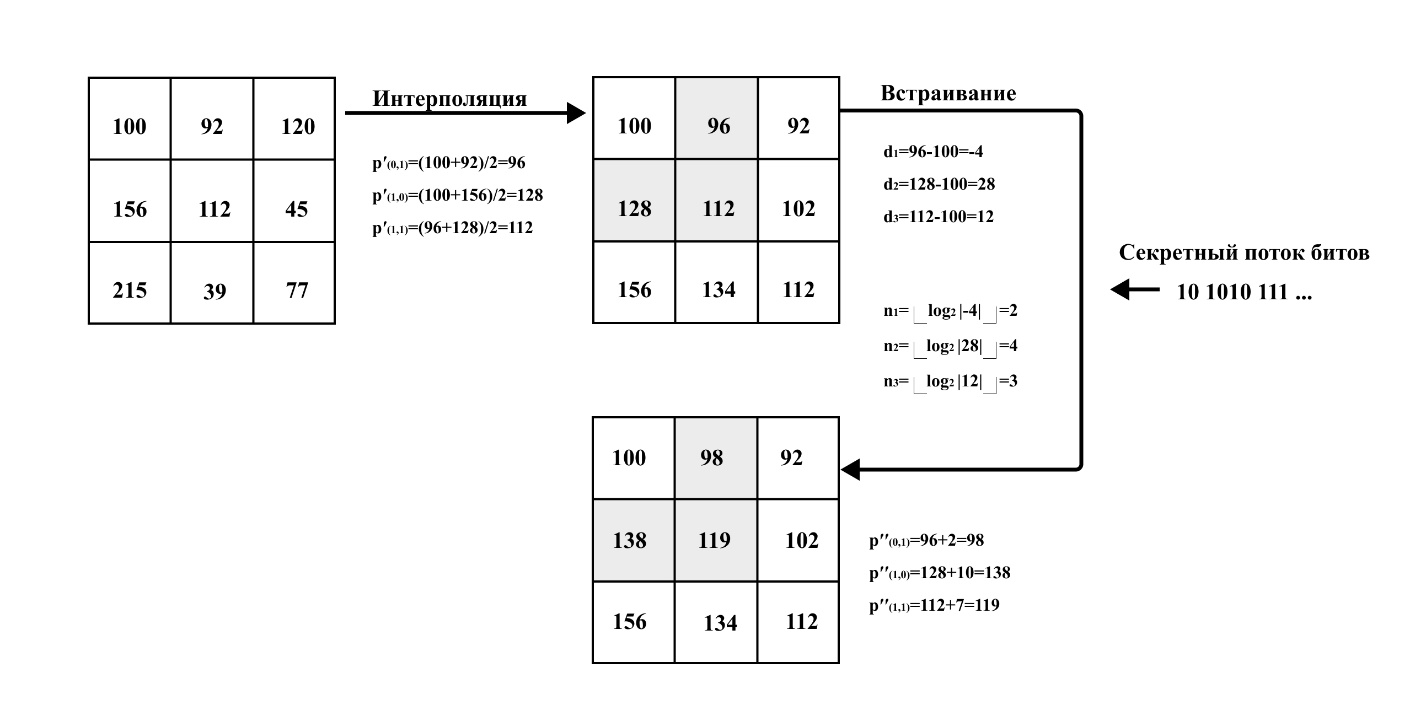


Рисунок 2.7 – Пример метода Jung и Yoo [145]

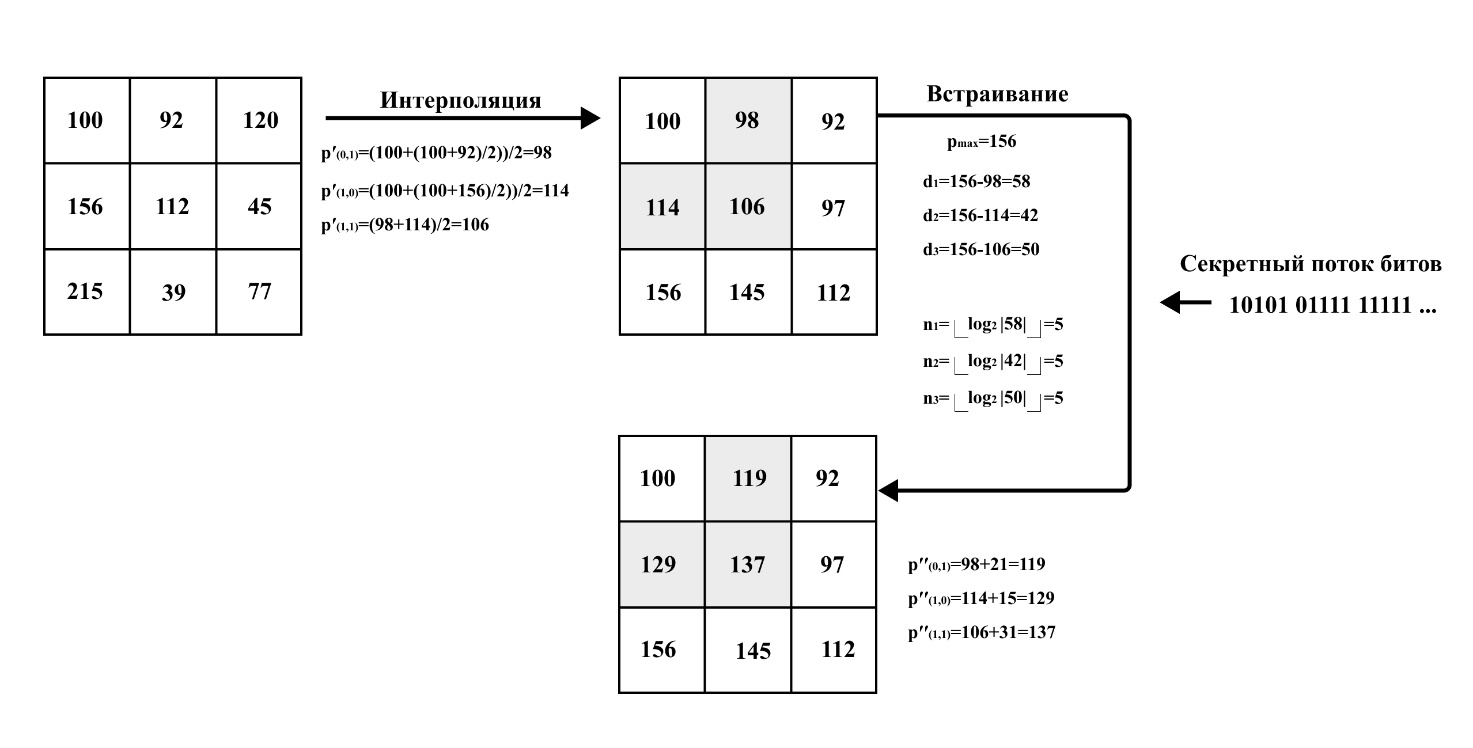


Рисунок 2.8 – Пример метода Lee и Huang [145]

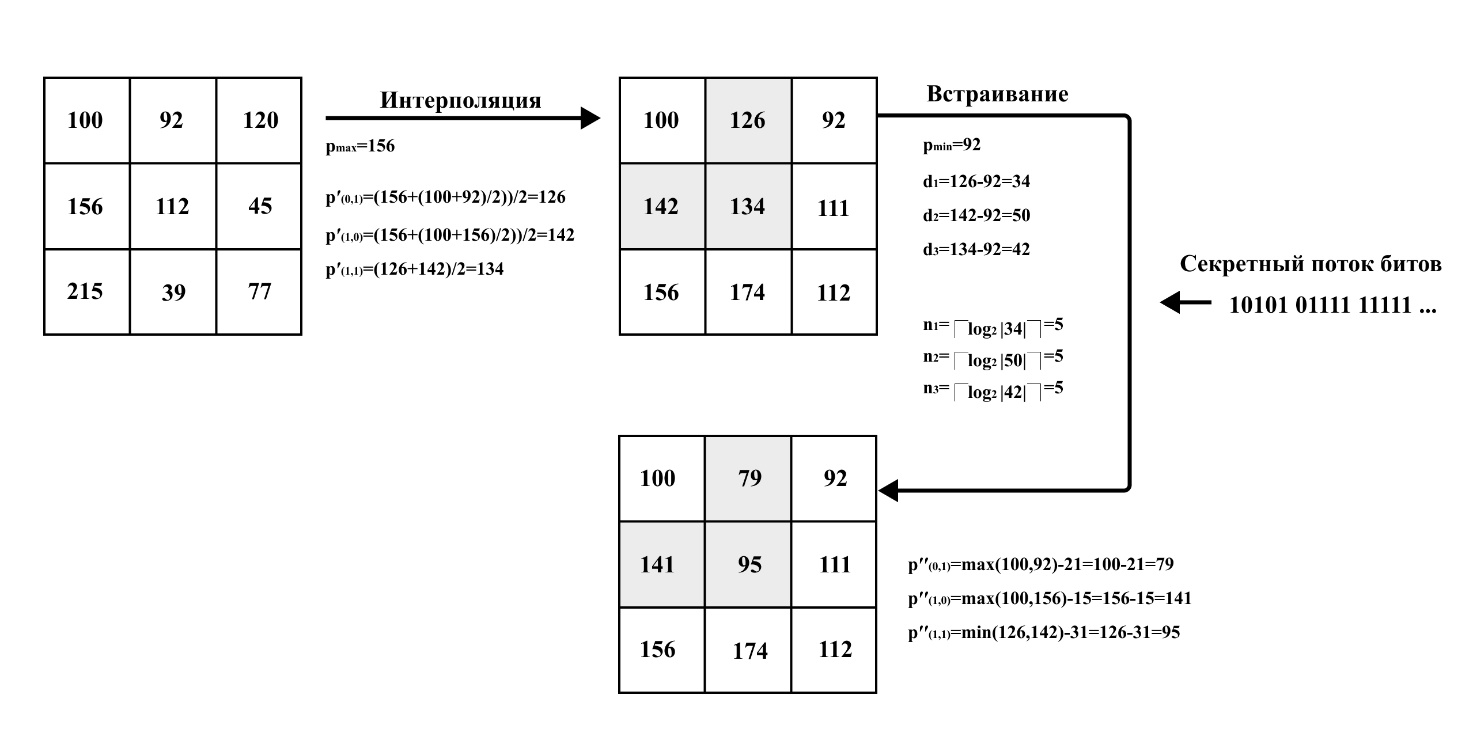


Рисунок 2.9 – Пример метода Hu и Li [145]

В качестве метрик авторами применены PSNR, универсальный индекс Q (для измерения качества визуального изображения) и общее количество встроенных битов или количество встроенных битов на пиксель (bpp) секретных данных на изображении.

Сравнительны результаты по методам показаны в таблице 2.1:

Таблица 2.1 Сравнение средней емкости встраивания и качества визуального изображения [145]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Метод | Усредненные значения | | | | |
| Емкость  (в битах) | Контейнер и интерполированное изображение | | Контейнер и стегоизображение | |
| PSNR (dB) | Q | PSNR (dB) | Q |
| Метод Jung и Yoo | 183,353 | 28.50 | 0.7488 | 28.16 | 0.7413 |
| Метод Lee и Huang | 253,572 | 27.13 | 0.7163 | 27.13 | 0.7278 |
| Метод Hu и LI | 155,488 | 28.35 | 0.7913 | 28/86 | 0.8356 |

В статье [146] представлен обзор основных алгоритмов встраивания информации в цифровые изображения с применением интерполяции, а также предложена собственная модификация INMI, основанного на использовании интерполяционного полинома Лагранжа второй степени для получения изображения – контейнера.

Изображение, полученное путем добавления дополнительных строк и столбцов пикселей к исходному изображению, рассматривали фрагментами по 5 пикселей, пронумерованных от 0 до 4.

Значения пикселей изображения-контейнера получают по следующей формуле (2.8):

 (2.8)

где  – номер пикселя во фрагменте из пяти пикселей.

Выполнено сравнение рассмотренных алгоритмов по таким характеристикам, как пиковое отношение сигнал/шум и максимальная ёмкость (таблица 2.2):

Таблица 2.2 Результаты вычислительных экспериментов с рассмотренными алгоритмами [146]

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Изображение | NMI | | INMI | | INP | | CRS | | Модификация | |
| Ёмкость | PSNR | Ёмкость | PSNR | Ёмкость | PSNR | Ёмкость | PSNR | Ёмкость | PSNR |
| Aerial | 1,17 | 25,24 | 1,46 | 24,15 | 1,88 | 25,32 | 2,35 | 23,59 | 1,44 | 24,65 |
| Airplane | 0,63 | 28,94 | 0,85 | 27,94 | 1,25 | 28,76 | 1,55 | 26,99 | 0,83 | 28,37 |
| Baboon | 1,26 | 22,57 | 1,56 | 22,13 | 2,04 | 22,67 | 2,49 | 21,58 | 1,52 | 22,24 |
| Barbara | 0,88 | 24,42 | 1,13 | 23,90 | 1,51 | 24,50 | 1,90 | 22,98 | 1,10 | 24,07 |
| Boat | 0,78 | 27,98 | 1,06 | 26,93 | 1,43 | 27,89 | 1,83 | 25,53 | 1,04 | 27,34 |
| Goldhill | 0,77 | 29,72 | 1,05 | 28,78 | 1,45 | 29,69 | 1,86 | 26,19 | 1,03 | 29,19 |
| House | 0,84 | 27,52 | 1,11 | 26,64 | 1,45 | 27,46 | 1,83 | 25,15 | 1,07 | 27,05 |
| Lena | 0,57 | 31,64 | 0,80 | 30,27 | 1,20 | 31,61 | 1,50 | 27,68 | 0,78 | 30,92 |
| Peppers | 0,55 | 30,40 | 0,77 | 29,42 | 1,21 | 30,18 | 1,51 | 27,64 | 0,76 | 29,69 |
| Stream | 1,21 | 25,16 | 1,53 | 24,35 | 1,99 | 24,99 | 2,47 | 22,96 | 1,51 | 23,89 |
| СРЗНАЧ | 0,87 | 27,36 | 1,13 | 26,45 | 1,54 | 27,31 | 1,93 | 25,03 | 1,11 | 26,74 |

В целом, метод INMI применяется в различных областях компьютерного зрения и обработки изображений, например, для увеличения разрешения изображений в медицинских и научных приложениях, в системах видеонаблюдения, а также в алгоритмах распознавания образов и идентификации лиц.

Таким образом, метод интерполяции INMI продемонстрировал высокую эффективность и точность в различных задачах обработки изображений и является перспективным направлением исследований в области интерполяции изображений.

# 2.6 Стегоанализ INMI метода

*Проведение RS анализа.* В статье [146] была рассмотрена модификация INMI метода, которая показала улучшение характеристики в виде увеличения значения PSNR при незначительном уменьшении ёмкости встраивания. Максимальное количество информации, которое можно записать в контейнер при использовании метода внедрения называется эмпирической емкостью контейнера. Анализирующая программа RS – анализа выдает количество встроенной информации () в процентах от эмпирической емкости контейнера, которая высчитывается как при LSB-встраивании (2.9):

 бит (2.9)

По значению  можно судить о том, заполнен был контейнер или пуст: при RS классифицирует контейнер как заполненный. Также упомянем о двух гипотезах:означающая, что контейнер содержит стегосообщение, и альтернативная ей гипотеза  означающая, что контейнер не содержит встроенной информации. Правило решения заключается в том, что каждому контейнеру сопоставляется одна из двух гипотез. Здесь возможны два типа ошибок: ошибка первого рода (type I error), которая заключается в установлении гипотезы , когда контейнер пуст, и ошибка второго рода (type II error), когда принято решение  при наличии встроенной информации в контейнере.

В настоящем исследовании [115] проведен RS анализ данной модификации INMI. Схема эксперимента представлена на рисунке 2.10. Исходный контейнер масштабировали при помощи метода интерполяции. Затем, в новые (интерполированные) пикселы встраивалось секретное сообщение. Далее стегоконтейнер подавался на вход RS классификатору.

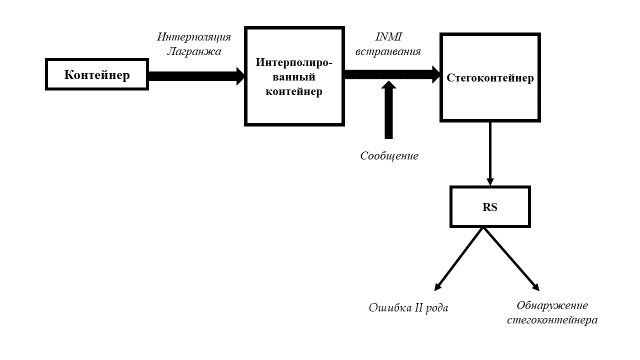


Рисунок 2.10 - Схема экспериментальных исследований

Требовалось определить емкость контейнеров с точки зрения процента вовлечения младших бит матрицы изображения при низкой вероятности обнаружения. Также это необходимо для сравнения полученных результатов стегоанализа с результатами других методов встраивания, рассмотренных в [147].

Исходя из рассмотренного алгоритма INMI, мы определили, что максимальная емкость контейнера составляет 21% и зависит от изображения.

Проведя исследование на наборе из 800 изображений размера 225х225, мы определили, что 60 из них имеют максимальную емкость. Результаты подсчета ошибки первого рода приведены в таблице 2.3, где показано, что ошибка составляет 0%. Результаты RS анализа показаны в таблице 2.4, по которой можно видеть, что метод является устойчивым к RS анализу.

Соответственно результаты исследования для полного набора из 800 изображений, при среднем проценте заполнения 12%, приведены в таблицах 2.3-2.4.

Таблица 2.3. RS анализ на наборе пустых контейнеров (60 картинок)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | | 0% | 1-4% | 5% и более |
| Доля файлов | 225x225 | 54 | 46 | - |

Таблица 2.4 RS анализ на наборе контейнеров, заполненных с помощью метода интерполяции на 21%.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | | 0% | 1-4% | 5% и более |
| Доля файлов | 225x225 | 53 | 47 | - |

Результаты стегоанализа, приведенные в табл. 2.5 и 2.6 свидетельствуют о том, что процент обнаружения встроенной информации по предложенному методу приблизительно равен проценту файлов, в которых была ошибка первого рода.

Таблица 2.5. RS анализ на наборе пустых контейнеров (800 картинок)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | | 0% | 1-4% | 5% и более |
| Доля файлов | 225x225 | 61 | 39 | - |

Таблица 2.6. RS анализ на наборе контейнеров, заполненных с помощью метода интерполяции на 12%.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L | | 0% | 1-4% | 5% и более |
| Доля файлов | 225x225 | 51,5 | 48 | 0,5 |

Очевидно, что чем меньше информации мы встраиваем в изображение, тем меньше вероятность появления обнаружимых признаков в результате процесса внедрения [148]. Как мы можем видеть из полученных результатов, метод INMI по стойкости к RS атаке сопоставим со стегосистемой способа перестановок для растровых изображений, рассмотренной в [147]. Процент изменения младших бит в сравниваемых методах примерно одинаковый и отличается в различных реализациях стегосистемы, рассмотренной там же. Однако, фактически в методе интерполяции задействованы не только младшие биты, поэтому имеет смысл провести также специфический метод анализа степени сжатия пустых и заполненных контейнеров.

*Энтропийный анализ.* В работах [149] был показан подход, позволяющий выявлять факт внедрения сообщения при помощи архиватора. Допустим имеется контейнер, который мы получили самостоятельно и знаем, что это стегоконтейнер. Добавим к нему подозрительный контейнер, который нужно проанализировать и сожмем его. Архиватор сработает так: будет собрана статистика и часто встречающиеся последовательности получают короткие кодовые слова, а редко встречающиеся – длинные. Чем лучше собрана статистика, тем лучше будет сжатие. Если исходный и добавленный контейнеры имеют одно происхождение (например, стего), то статистика у них будет совпадать и добавленный контейнер сожмется также хорошо, как и исходный. Если же они имеют разное происхождение, то статистические свойства у них отличаются, из-за чего сжатие добавленной части будет значительно хуже. Таким образом архиватор применяется для установления статистической взаимосвязи.

В работе [150] была доказана эффективность такого метода для абстрактных контейнеров, которые являются порождением стационарного и эргодического временного источника. Однако, когда мы рассматриваем реальный контейнер заранее не знаем, является ли он эргодическим или стационарным, т.к. не существует адекватных моделей ни одного из типов данных. Данный подход был успешно развит в ряде работ для текстовых контейнеров [151] и для изображений [147, 151]. Тем не менее оставался открытым вопрос о границах применимости. В настоящем исследовании данная граница была найдена.

Известно, что исходный контейнер и добавляемая в него информация статистически независимы, поэтому при добавлении скрытых данных в контейнер, размер его при сжатии вырастает по сравнению с размером сжатого исходного пустого контейнера [147]. Изменения степени сжатия в обратную сторону также свидетельствует о признаках изменения. Было проведено исследование, в котором определим коэффициенты сжатия пустых и заполненных контейнеров. Коэффициент сжатия — основная характеристика алгоритма сжатия. Она определяется как отношение объёма исходных несжатых данных к объёму сжатых данных.

В таблицах 2.7-2.8 показаны результаты сравнения коэффициентов сжатия для пустых и заполненных контейнеров. Здесь- последовательность байтов данных пустого контейнера,- коэффициент сжатия последовательности архиватором ZIP. — последовательность байтов данных заполненного контейнера, - коэффициент сжатия последовательностиархиватором RAR,  - разность между коэффициентами сжатия отрезков последовательностейи*.* Для удобства в таблицах представлены только часть результатов, так как они однообразны для всей выборки файлов.

Таблица 2.7. Сравнение разностей коэффициентов сжатия для пустых и заполненных контейнеров

|  |  |  |  |
| --- | --- | --- | --- |
| Название файла | ,  МБ | ,  МБ |  |
| 001.BMP | 0,133 | 0,134 | 0,02 |
| 002.BMP | 0,137 | 0,138 | 0,01 |
| 003.BMP | 0,086 | 0,086 | 0,00 |
| 004.BMP | 0,105 | 0,106 | 0,01 |
| 005.BMP | 0,151 | 0,153 | 0,00 |
| 006.BMP | 0,033 | 0,033 | 0,00 |
| 007.BMP | 0,146 | 0,148 | 0,02 |
| 008.BMP | 0,125 | 0,126 | 0,01 |
| 009.BMP | 0,117 | 0,118 | 0,01 |
| 010.BMP | 0,072 | 0,072 | 0,00 |
| 117.BMP | 0,065 | 0,065 | 0,00 |
| 140.BMP | 0,059 | 0,059 | 0,00 |
| 180.BMP | 0,129 | 0,131 | 0,02 |
| 222.BMP | 0,134 | 0,135 | 0,01 |
| 244.BMP | 0,102 | 0,103 | 0,01 |
| 25.BMP | 0,135 | 0,136 | 0,01 |
| 250.BMP | 0,072 | 0,072 | 0,00 |
| 258.BMP | 0,129 | 0,131 | 0,02 |
| 317.BMP | 0,071 | 0,072 | 0,01 |
| 37.BMP | 0,133 | 0,134 | 0,01 |
| 388.BMP | 0,108 | 0,109 | 0,01 |
| 405.BMP | 0,086 | 0,086 | 0,00 |
| 465.BMP | 0,132 | 0,134 | 0,02 |
| 521.BMP | 0,098 | 0,099 | 0,01 |
| 528.BMP | 0,117 | 0,118 | 0,01 |
| 610.BMP | 0,100 | 0,100 | 0,00 |
| 68.BMP | 0,150 | 0,152 | 0,02 |
| 72.BMP | 0,105 | 0,107 | 0,02 |
| 752.BMP | 0,147 | 0,149 | 0,02 |
| 785.BMP | 0,114 | 0,115 | 0,01 |
| 796.BMP | 0,069 | 0,069 | 0,00 |
|  |  |  |  |
| *Среднее значение* | *0,108* | *0,109* | *0,01* |

Таблица 2.8. Сравнение разностей коэффициентов сжатия для пустых и заполненных контейнеров (по архиватору RAR)

|  |  |  |  |
| --- | --- | --- | --- |
| Название файла | ,  МБ | ,  МБ | , |
| 001.BMP | 0,099 | 0,101 | 0,02 |
| 002.BMP | 0,104 | 0,107 | 0,03 |
| 003.BMP | 0,068 | 0,069 | 0,01 |
| 004.BMP | 0,088 | 0,090 | 0,02 |
| 005.BMP | 0,114 | 0,117 | 0,03 |
| 006.BMP | 0,029 | 0,029 | 0,00 |
| 007.BMP | 0,110 | 0,114 | 0,04 |
| 008.BMP | 0,091 | 0,094 | 0,03 |
| 009.BMP | 0,089 | 0,091 | 0,02 |
| 010.BMP | 0,058 | 0,058 | 0,00 |
| 117.BMP | 0,049 | 0,049 | 0,00 |
| 140.BMP | 0,041 | 0,041 | 0,00 |
| 180.BMP | 0,093 | 0,096 | 0,03 |
| 222.BMP | 0,091 | 0,093 | 0,02 |
| 244.BMP | 0,078 | 0,080 | 0,02 |
| 25.BMP | 0,089 | 0,091 | 0,02 |
| 250.BMP | 0,060 | 0,060 | 0,00 |
| 258.BMP | 0,099 | 0,102 | 0,03 |
| 317.BMP | 0,056 | 0,057 | 0,01 |
| 37.BMP | 0,101 | 0,104 | 0,03 |
| 388.BMP | 0,074 | 0,076 | 0,02 |
| 405.BMP | 0,066 | 0,067 | 0,01 |
| 465.BMP | 0,100 | 0,103 | 0,03 |
| 521.BMP | 0,071 | 0,073 | 0,02 |
| 528.BMP | 0,087 | 0,089 | 0,02 |
| 610.BMP | 0,085 | 0,087 | 0,02 |
| 68.BMP | 0,112 | 0,115 | 0,03 |
| 72.BMP | 0,076 | 0,079 | 0,03 |
| 752.BMP | 0,108 | 0,112 | 0,04 |
| 785.BMP | 0,079 | 0,080 | 0,01 |
| 796.BMP | 0,057 | 0,058 | 0,01 |
|  |  |  |  |
| *Среднее значение* | *0,082* | *0,083* | *0,01* |

Значение , полученное в результате данного исследования, близко к нулю, что означает сходство статистических структур пустых и заполненных контейнеров. Следовательно, их трудно отличить, применяя такой подход стегоанализа.

# 2.7 Выводы по разделу

В рамках диссертации реализован и исследована наилучшая модификация известного алгоритма INMI. Был проведен стегоанализ данного метода встраивания, получены результаты, которые можно сравнить со стегоанализом методов, рассмотренных в [147].

На основании рассмотренного алгоритма INMI, мы определили, что максимальная емкость контейнера составляет 21% и зависит от изображения. По результату исследования на наборе из 800 изображений размера 225х225, мы определили, что 60 из них имеют максимальную емкость. Полученные результаты подсчета ошибки первого рода показали, что ошибка составляет 0%.

Итоговые результаты RS анализа показаны в таблице 2, по которой можно видеть, что метод INMI является устойчивым к стегоанализу RS и сопоставим по стойкости и ёмкости со стегосистемой, предложенной Мерзляковой Е.Ю. в [147].

Был проведен также специфический метод анализа степени сжатия пустых и заполненных контейнеров. Также в исследовании были определены коэффициенты сжатия пустых и заполненных контейнеров. Значение разностей коэффициентов  полученное в результате данного исследования, близко к нулю, что означает сходство статистических структур пустых и заполненных контейнеров.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Daiyrbayeva E., Yerimbetova A., Nechta I., Merzlyakova E., Toigozhinova A., Turganbayev A. (2022) A Study of the Information Embedding Method into Raster Image Based on Interpolation. J. Imaging, 8, 288. <https://doi.org/10.3390/jimaging8100288>.
2. Kameneva A. (2016) A. Some methods of image interpolation. Scientific community of students: Collection of materials X International Student Scientific and Practical Conference, Cheboksary. – Cheboksary: Limited Liability Company «Center for Scientific Cooperation «Interactive Plus». Рp. 121–123.
3. Yingmin Li, F. Qi and Y. Wan, (2019). Improvements On Bicubic Image Interpolation, 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 2019. Рp. 1316–1320. DOI: 10.1109/ IAEAC47372.2019.8997600.
4. Дайырбаева Э.Н., Еримбетова А.С. Роль метрики в обработке изображений // МНСК-2021 Информационные технологии. Материалы 59-й Международной научной студенческой конференции, 12–23 апреля 2021 г., Новосибирск, РФ, - С.53
5. Parsania P. S., Virparia P. V. A comparative analysis of image interpolation algorithms //International Journal of Advanced Research in Computer and Communication Engineering. – 2016. – Т. 5. – №. 1. – С. 29-34.
6. Yerimbetova A., Daiyrbayeva E., Cherikbayeva L. Embedding hidden information in images based on bicubic interpolation. -Известия НАН РК. Серия информатики, (1), 2023-P. 50-63
7. Han D. Comparison of commonly used image interpolation methods //Conference of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013). – Atlantis Press, 2013. – С. 1556-1559.
8. Sa Y. Improved bilinear interpolation method for image fast processing //2014 7th International Conference on Intelligent Computation Technology and Automation. – IEEE, 2014. – С. 308-311.
9. Arif F., Akbar M. Resampling air borne sensed data using bilinear interpolation algorithm //IEEE International Conference on Mechatronics, 2005. ICM'05. – IEEE, 2005. – С. 62-65.
10. Li J., Su J., Zeng X. A solution method for image distortion correction model based on bilinear interpolation //Компьютерная оптика. – 2019. – Т. 43. – №. 1. – С. 99-104.
11. Choi J., Kweon I. S. Deep iterative frame interpolation for full-frame video stabilization //ACM Transactions on Graphics (TOG). – 2020. – Т. 39. – №. 1. – С. 1-9.
12. Li D. et al. Deep image compression based on multi-scale deformable convolution //Journal of Visual Communication and Image Representation. – 2022. – Т. 87. – С. 103573.
13. Hung K. W., Wang K., Jiang J. Image interpolation using convolutional neural networks with deep recursive residual learning //Multimedia Tools and Applications. – 2019. – Т. 78. – С. 22813-22831.
14. Roy A.M. An efficient multi-scale CNN model with intrinsic feature integration for motor imagery EEG subject classification in brain-machine interfaces //Biomedical Signal Processing and Control. – 2022. – Т. 74. – С. 103496.
15. Tai Y., Yang J., Liu X. Image super-resolution via deep recursive residual network //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2017. – С. 3147-3155.
16. Siu W.C., Hung K. W. Review of image interpolation and super-resolution //Proceedings of The 2012 Asia Pacific Signal and Information Processing Association Annual Summit and Conference. – IEEE, 2012. – С. 1-10.
17. Дайырбаева Э.Н., Еримбетова А.С. Исследование и внедрение встраивания скрытой информации в изображения на основе интерполяции // Российская конференция с международным участием РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ РЕСУРСЫ (DICR-2022) Сборник трудов Россия, г. Новосибирск, 5 – 8 декабря 2022 г. – С. 45-48.
18. Phung V.M., Nguyen V.T., Dinh H.L. Combining Interpolation Schemes and Lagrange Interpolation on the Unit Sphere in ℝN+1. Ukrainian Mathematical Journal. Том 74, Выпуск 4, 2022. –С. 618 – 638. DOI10.1007/s11253-022-02088-0
19. Zadorin A.I., Zadorin N.A. Lagrange Interpolation and the Newton–Cotes Formulas on a Bakhvalov Mesh in the Presence of a Boundary Layer. Computational Mathematics and Mathematical Physics.Т.62, Выпуск 3,2022. С.347 – 358. DOI10.1134/S0965542522030149
20. Georgiev S.G., Erhanİ.M. Lagrange interpolation on time scales. Journal of Applied Analysis and Computation.Том 12, Выпуск 4, 2022. – С. 1294 – 1307. DOI 10.11948/20200461
21. Jean-Paul C., Phung V.M. Lagrange interpolation at real projections of Leja sequences for the unit disk. Proceedings of the American mathematical society Volume 140, Number 12, 201. – P. 4271–4284
22. Исмоилова М.Н., Имомова Ш.М. Интерполяция функции. Вестник Науки и Образования № 3(81). Часть 3. 2020. –С. 5-8.
23. Ki-Hyun Jung, Kee-Young Yoo. (2009). Data hiding method using image interpolation. Computer Standards & Interfaces. -Volume 31, Issue 2.2009. Pр. 465–470. <http://dx.doi.org/10.1016/j.csi.2008.06.001>
24. Yang C. N., Hsu S. C., Kim C. Improving stego image quality in image interpolation based data hiding //Computer Standards & Interfaces. – 2017. – Т. 50. – С. 209-215.
25. Jana M., Joardar S., Jana B. A New Reversible Data Hiding Scheme by Altering Interpolated Pixels Exploiting Neighbor Mean Interpolation (NMI) //Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2022. – Singapore: Springer Nature Singapore, 2022. – С. 393-402.
26. Jung K. H., Yoo K. Y. Steganographic method based on interpolation and LSB substitution of digital images //Multimedia Tools and Applications. – 2015. – Т. 74. – С. 2143-2155.
27. Parsania, Pankaj & Virparia, Dr. (2016). A Comparative Analysis of Image Interpolation Algorithms. IJARCCE. 5. 29-34. 10.17148/IJARCCE.2016.5107.
28. Amanatiadis A., Andreadis I. A survey on evaluation methods for image interpolation //Measurement Science and Technology. – 2009. – Т. 20. – №. 10. – С. 104015.
29. Wang Y. et al. An improved interpolation algorithm using nearest neighbor from VTK //2010 International Conference on Audio, Language and Image Processing. – IEEE, 2010. – С. 1062-1065.
30. Malik A., Sikka G., Verma H. K. Image interpolation based high capacity reversible data hiding scheme //Multimedia Tools and Applications. – 2017. – Т. 76. – С. 24107-24123.
31. Jung, Ki-Hyun. (2018). A survey of interpolation-based reversible data hiding methods. Multimedia Tools and Applications. 77. 10.1007/s11042-017-5066-2.
32. Евсютин О.О., Кокурина А.С., Мещеряков Р.В. Алгоритмы встраивания информации в цифровые изображения с применением интерполяции //Доклады Томского государственного университета систем управления и радиоэлектроники. – 2015. – №. 4 (38). – С. 108-112.
33. Мерзлякова Е.Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах : дис. – Сибирский государственный университет телекоммуникаций и информатики, 2011. – С.161.
34. Елтышева (Мерзлякова) Е.Ю., Фионов А.Н. Построение стегосистемы на базе растровых изображений с учетом статистики младших бит // Вестник ФГОБУ ВПО «СибГУТИ». 2009. № 1. С. 67-84.
35. Ryabko B. Compression-based methods for nonparametric density estimation, on-line prediction, regression and classification for time series // IEEE Information Theory Workshop, Porto, Portugal, 5–9 May, 2008
36. Нечта И.В. Разработка методов обеспечения безопасности использования информационных технологий, базирующихся на идеях стеганографии : дис. – Новосибирск: Нечта Иван Васильевич, 2012.
37. Жилкин М.Ю. Теоретико-информационные методы стегоанализа графических данных //Дисс.... канд. техн. наук. Новосибирск, СибГУТИ. – 2009.