

Ордена Трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

На правах рукописи



Магомедова Дженнет Исламутдиновна

**МАРКИРОВКА НЕПОДВИЖНЫХ ИЗОБРАЖЕНИЙ И АУДИОСИГНАЛОВ
С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ ПРОЦЕССОВ ДЛЯ ЗАЩИТЫ
АВТОРСКИХ ПРАВ**

Специальность 2.3.6 –

Методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ

на соискание ученой степени

кандидата технических наук

Научный руководитель:
доктор технических наук,
профессор Шелухин О.И.

Москва – 2023

Оглавление

Введение.....	5
Глава 1 Анализ существующих методов встраивания цифровых водяных знаков (ЦВЗ).....	13
1.1 Основные характеристики методов добавления ЦВЗ.....	13
1.2 Алгоритмы встраивания водяных знаков.....	14
1.3 Встраивание водяных знаков на основе фрактального анализа.....	15
1.4 Особенности использования 2D ДВП для встраивания ЦВЗ.....	23
1.5 Атаки на системы ЦВЗ.....	28
1.6 Критерии оценки эффективности стеганографических систем.....	29
1.7 Выводы.....	30
Глава 2 Маркирование аудиосигналов с использованием фрактального гауссовского шума.....	32
2.1 Алгоритм встраивания A1.....	32
2.2 Генерация фрактального гауссовского шума.....	37
2.3 Алгоритм извлечения.....	39
2.4 Выбор уровня разложения.....	42
2.5 Выбор длины последовательности ФГШ.....	45
2.6 Выбор параметра alpha.....	46
2.7 Выбор значения показателя Хёрста единичной последовательности H1.....	49
2.8 Выбор порога $N_{\text{пор}}$	52
2.9 Сравнительный анализ качества извлечения ПСП алгоритмом A1 с алгоритмом расширения спектра.....	53
2.10 Выводы.....	55
Глава 3 Фрактальные алгоритмы встраивания ЦВЗ в изображения.....	56
3.1 Алгоритм A2 защиты неподвижных изображений с использованием двухкомпонентного контейнера и 2D ДВП.....	56
3.1.1 Алгоритм встраивания ЦВЗ.....	57
3.1.1.1 Алгоритм A21 генерации фрактального контейнера.....	58

3.1.1.2 Оценка емкости фрактального контейнера.....	63
3.1.1.3 Результаты встраивания ЦВЗ во фрактальный ключ.....	66
3.1.1.4 Результаты встраивания фрактального ключа в контейнер.....	68
3.1.2 Алгоритм извлечения ЦВЗ.....	70
3.1.3 Выбор уровня разложения	72
3.1.4 Выбор типа коэффициентов вейвлет разложения для замены.....	74
3.1.5 Выбор параметра α	76
3.1.6 Выбор параметра Thr	78
3.2 Алгоритм защиты неподвижных изображений АЗ с использованием фрактального гауссовского шума и 2D ДВП.	79
3.2.1 Алгоритм встраивания	79
3.2.2 Алгоритм извлечения	81
3.2.3 Выбор уровня разложения	84
3.2.4 Выбор типа коэффициентов вейвлет-разложения.....	85
3.2.5 Выбор параметра α	86
3.2.6 Выбор длины последовательности ФГШ	87
3.2.7 Выбор значения показателя Херста единичной последовательности H_1	88
3.2.8 Выбор порога $N_{\text{пор}}$	89
3.3 Сравнительный анализ эффективности алгоритмов встраивания ЦВЗ фрактальными методами в отсутствие атак	90
3.4 Выводы.....	92
Глава 4 Исследование устойчивости разработанных алгоритмов к различным атакам.....	95
4.1 Исследование устойчивости алгоритма А2.....	95
4.2 Исследование устойчивости алгоритма АЗ.....	101
4.3 Сравнительный анализ устойчивости предложенных алгоритмов с известными методами встраивания ЦВЗ.....	104
4.4 Выводы.....	105
Заключение	106

Список сокращений и условных обозначений	108
Список использованных источников	109
Приложение А. Акты о внедрении и использовании результатов диссертационной работы.....	121
Приложение Б. Свидетельства о государственной регистрации программы для ЭВМ	123
Приложение В. Численные результаты экспериментов.....	125
Приложение Г. Листинги программ реализации разработанных алгоритмов.....	157

Введение

Актуальность темы исследования. Использование чужой интеллектуальной собственности в коммерческих целях является актуальной проблемой защиты информации на сегодняшний день. При этом технологии защиты авторских прав особенно актуальны из-за непрерывного роста использования цифровых объектов во всех областях жизни общества. Согласно статье 146 УК РФ под нарушением авторских и смежных прав понимается присвоение авторства (плагиат) или незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта.

Доказательство нарушения авторских прав применительно к фото или аудиоконтенту является трудоемкой задачей в том числе и потому, что растет число и квалификация злоумышленников. Одной из областей, направленной на решение подобных задач защиты информации, является стеганография. Методы стеганографии в основном используются для обеспечения передачи секретных данных по открытым каналам связи, но могут применяться и для защиты авторских прав и доказательства целостности контента. При этом в оригинальные покрывающие объекты или контейнеры добавляются специальные метки – цифровые водяные знаки (ЦВЗ), которые несут в себе информацию, доказывающую исключительное права автора (собственника).

Методы встраивания информации в аудио сигналы и неподвижные изображения с помощью стеганографии разрабатывались рядом отечественных исследователей (Грибунин В.Г., Дворянкин С.В., Коржик В.И., Коханович Г.Ф., Туринцев И.В., Молдовян Н.А., Молдовян А.А., Шелухин О.И., Шакурский М.В. и др.), а также зарубежными авторами (Han-Yang Lo, Topiwala S, Kim J.R, Wang J.I., Dumitrescu C., Banik B.G., Bandyopadhyay S.K., Dhanraj. R., Jayasudh S., Baby D.,

Thomas J., Augustine G., George E., Michael N.R., Saxena N., Agrawal G., Linta J. L., Joy H., и др.)

Цифровые платформы, занимающиеся продажей цифровых объектов, рассматривают стеганографию как альтернативу технологии NFT для защиты объектов авторского права от неправомерного использования. Услуги добавления ЦВЗ в целях защиты авторского права предоставляют, например компании IMATAG (Франция) и DigiMarc (США), в России подобные услуги недоступны.

Анализ научной периодики подтверждает актуальность разработки новых методов и алгоритмов защиты информации от неправомерного использования. К их числу относится такая технология как фрактальный анализ. Методам фрактального анализа в различных областях техники посвящено достаточно много работ таких исследователей, как Божокин С.В., Паршин Д.А., Басараб М.А., Лаврова Д.С., Шелухин О.И., Mandelbrot B.B., Willinger W., Taqqu M.S., Abry P., Veitch D. и др.

Специфическую хаотичную природу фракталов можно использовать для защиты цифровой мультимедийной информации от воздействия атак и попыток злоумышленников-хакеров удалить встроенные метки. Однако в известных работах, например Грибунина В.Г., Коржика В.И., Коробейникова А.Г. и Шакурского М.В. разработке фрактальных алгоритмов встраивания ЦВЗ в мультимедийную продукцию (подверженную воздействию возмущающих факторов внешней среды и неправомерному использованию квалифицированными злоумышленниками), уделено недостаточно внимания.

В связи с вышесказанным возникает актуальная научная задача разработки и исследования новых алгоритмов защиты авторских прав в фото и аудиоконтенте от угроз неправомерного использования, основанных на технологии фрактального анализа.

Целью диссертационного исследования является повышение функциональной эффективности алгоритмов защиты и фото и аудио контента от угроз не-

правомерного использования.

Достижение поставленной цели предусматривает решение **частных задач**:

1. Сравнительный анализ существующих стеганографических методов и алгоритмов встраивания ЦВЗ в файлы аудио и фото контента для защиты информации и обеспечения авторских прав пользователей, в том числе с использованием фрактального анализа.

2. Разработка нового алгоритма и соответствующего программного обеспечения (ПО) для встраивания псевдослучайных последовательностей в аудио файлы с использованием дискретного вейвлет преобразования (ДВП) и одномерного фрактального гауссовского шума (ФГШ), обеспечивая рациональный выбор параметров алгоритма для минимизации искажений оригинала и извлечения информации с высокой достоверностью при воздействии атак и угроз правомерного использования.

3. Разработка новых алгоритмов и ПО для встраивания водяных знаков в неподвижные изображения:

- встраивания ЦВЗ с использованием двухкомпонентного контейнера и двумерного дискретного вейвлет преобразования 2DDВП;
- скрытия ЦВЗ с помощью ФГШ на основе использования 2DDВП.

4. Анализ устойчивости разработанных алгоритмов к атакам злоумышленников, направленным на удаление или искажение ЦВЗ.

Выработка практических рекомендаций по выбору параметров разработанных алгоритмов, а также реализация специального программного обеспечения фрактальной маркировки для защиты информации фото и аудио контента.

Объект исследования – стеганографические методы защиты цифровой аудио и фото информации.

Предмет исследования – модели и методики фрактального встраивания ЦВЗ в фото и аудио контент.

Методы исследования: теория фракталов, методы математического чис-

ленного моделирования, математическая статистика, спектральный и корреляционный анализ, технология цифровой обработки звуковых сигналов и растровых изображений, алгоритмы фильтрации и стеганографии.

Основные научные положения, выносимые на защиту:

1. Разработанный алгоритм (А1) встраивания ЦВЗ в виде псевдослучайной последовательности (ПСП) в аудио сигналы с использованием ФГШ и ДВП обеспечивает высокую (не менее 0,95) достоверность извлечения знака при мешающих воздействиях с сохранением высокого качества аудио контейнера на уровне $PSNR > 40$ дБ, не требующий наличия оригинального аудиоконтейнера при извлечении ЦВЗ.

2. Разработанный алгоритм (А2) встраивания ЦВЗ в неподвижные изображения с использованием двухкомпонентного контейнера в виде оригинального изображения и дополнительного алгебраического фрактала с последующим 2ДДВП преобразованием, что позволяет при воздействии атак обеспечить высокое качество встраивания и извлечения водяного знака на уровне $PSNR > 40$ дБ, не уступая известным аналогам, основанным на расширении спектра, по качественным показателям, и в отличие от них не требуя наличия оригинального контейнера при извлечении ЦВЗ.

3. Разработанный алгоритм (А3) встраивания ЦВЗ в виде ПСП на основе двумерного ФГШ и 2ДДВП, позволяющий получить статистические показатели не хуже, чем у эталонных алгоритмов при воздействии широкого спектра атак, обеспечив при этом меньшую вероятность ошибки извлечения (менее 10^{-3}).

Теоретическая значимость результатов исследования состоит в развитии перспективного научного направления применения фракталов в стеганографии, а именно в разработке новых алгоритмов для защиты информации с помощью фрактальных процессов и ДВП, позволяющих повысить защищенность аудиосигналов и неподвижных изображений от неправомерного использования контента.

Научная новизна состоит в следующем:

1. Разработан и программно реализован новый алгоритм встраивания и извлечения ПСП в аудиофайлы с использованием ФГШ и ДВП, отличающийся от известных заменой части коэффициентов детализации вейвлет разложения на элементы фрактального шума, что позволяет повысить защищенность аудиосигналов от атак и угроз неправомерного использования (пункт 15 паспорта специальности).

2. Разработан и программно реализован новый алгоритм встраивания ЦВЗ с использованием двухкомпонентного контейнера в виде оригинального изображения и алгебраического фрактала (ключа) и 2DДВП для неподвижных изображений, обеспечивающий высокое качество извлечения водяного знака при воздействии атак и угроз неправомерного использования (пункт 15 паспорта специальности).

3. Разработан и программно реализован новый алгоритм встраивания ЦВЗ с использованием ФГШ путем замены части диагональных коэффициентов детализации 2DДВП вейвлет разложения неподвижных изображений на элементы фрактального шума с разной фрактальной размерностью, обеспечивающий высокое качество извлечения водяного знака при воздействии атак и угроз неправомерного использования (пункт 15 паспорта специальности).

Практическая ценность работы:

Заключается в разработке и программной реализации алгоритмов защиты авторских прав путем встраивания в аудио и фотоконтейнеры оригинальных водяных знаков на базе фрактального анализа, обеспечивая повышение устойчивости алгоритмов встраивания ЦВЗ к действиям квалифицированных злоумышленников.

Разработаны практические рекомендации по рациональному выбору материнских вейвлетов (используемых при ДВП и 2D ДВП), уровня вейвлет разложения, длительности и фрактальной размерности ФГШ, порогов решающего устройства, обеспечивающих требуемую эффективность защиты информации от непра-

вомерного использования в условиях воздействия помех и внешних атак.

Разработано специальное программное обеспечение для реализации фрактального метода маркировки аудио сигналов с использованием коэффициентов вейвлет разложения, защищённое свидетельством о государственной регистрации программы для ЭВМ.

Достоверность результатов диссертационной работы подтверждается сходимостью результатов имитационного моделирования с результатами экспериментальных данных, корректным использованием современного математического аппарата, а также достаточно широким рядом публикаций, обсуждением основных положений со специалистами на научных конференциях.

Внедрение результатов работы

Результаты диссертационных исследований, подтвержденные соответствующими актами, используются в:

- научно-производственной деятельности ООО «Альфаnova» (г. Москва), а именно:

- 1) метод и алгоритмы встраивания псевдослучайных последовательностей в звуковые сигналы с использованием фрактального гауссовского шума;
- 2) методические рекомендации по подбору параметров алгоритма встраивания, обеспечивая незаметность и заданную достоверность извлечения информации, что подтверждено актом о внедрении.

- в учебном процессе МТУСИ в части новых алгоритмов встраивания ЦВЗ в изображения с использованием фрактальных процессов.

Апробация результатов

Основные результаты работы докладывались и обсуждались на 9 научных конференциях:

- Международная научно-техническая конференция «Телекоммуникационные и вычислительные системы», Москва, 2017;
- XII международная отраслевая научно-техническая конференция "Техноло-

гии информационного общества", Москва, 2018;

– Международная научно-техническая конференция «Фундаментальные проблемы радиоэлектронного приборостроения «INTERMATIC-2018», Москва, 2018;

– 9-я всероссийская научно-техническая конференция «Безопасные информационные технологии», г. Москва, 2018;

– XII Международная отраслевая научно-техническая конференция «Технологии информационного общества», 2018;

– 24-я международная конференция Ассоциации открытых инноваций FRUCT, Москва, 2018;

– Международная конференция «Системы синхронизации, формирования и обработки сигналов в инфокоммуникациях» СИНХРОИНФО, 2020, 2021;

– Международная конференция “ Системы генерации и обработки сигналов в области бортовых коммуникаций”, Москва, 2021.

Публикации

Основные положения диссертации опубликованы в 14 научных печатных работах, в том числе: 3 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ [8-10], 4 – в научных рецензируемых изданиях, индексируемых в базе Scopus [11-14], 7 – в материалах конференций и других изданиях [15-21]. Получено 2 свидетельства о государственной регистрации программ для ЭВМ [22,23].

Соответствие паспорту специальности. Диссертация соответствует пункту 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» паспорта научной специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Личный вклад автора. Основные научные результаты, в том числе разра-

ботка алгоритмов встраивания и извлечения ЦВЗ в аудио сигналы и неподвижные изображения, получение количественных оценок вероятностей ошибок разработанных алгоритмов в условиях воздействия атак, а также разработка методических рекомендаций по подбору параметров алгоритмов получены автором лично. Вклад соавторов ограничивался постановкой задач на исследования и обсуждением полученных результатов.

Связь работы с научными программами, темами, грантами. Исследования выполнялись в инициативном порядке, в рамках работы по гранту аспирантам, соискателям и молодым ученым на исследования, направленные на обеспечение информационной безопасности для задач цифровой экономики и по государственной поддержке ведущих научных школ Российской Федерации в области информационной безопасности.

Объем и структура диссертационной работы. Диссертация написана на русском языке, состоит из введения, четырех глав, заключения, списка используемой литературы из 93 наименований и 4 приложений. Полный объем диссертации составляет 166 стр. (в том числе приложения 46 стр.), включая 70 рисунков и 47 таблиц.

Глава 1 Анализ существующих методов встраивания цифровых водяных знаков (ЦВЗ)

1.1 Основные характеристики методов добавления ЦВЗ

Актуальность проблемы незаконного использования цифрового контента растет с каждым годом. Количество судебных споров по авторскому праву ежегодно растет более чем на 40% [24, 25]. Однако чаще всего злоумышленникам удается избежать наказания в связи со сложной процедурой доказательства исключительного права на интеллектуальную собственность. Очевидно, существует необходимость разработки простого и надежного средства защиты авторских прав.

Стеганографические алгоритмы добавления ЦВЗ частично решают эту проблему. Цифровой водяной знак – это процесс внедрения цифровой информации в мультимедийный объект путем невоспринимаемого искажения объекта. Необходимость использования цифрового водяного знака возникает при попытке преодолеть ограничения шифрования в обеспечении и защите прав интеллектуальной собственности. По сравнению с идеей шифрования информация водяного знака вставляется в исходную форму и не мешает пользователям слушать, просматривать, смотреть или манипулировать контентом [26].

Однако стеганографические алгоритмы добавления ЦВЗ обладают рядом недостатков, которые не позволяют широко использовать их в целях доказательства авторского права.

Основной проблемой является частичное или полное повреждение ЦВЗ при сжатии стегоконтейнера [27, 28]. Форматы со сжатием, такие как JPEG, MPEG4, MP3, являются основными для своих типов данных. Невозможность работы с этими форматами значительно ограничивает область применения стеганографических алгоритмов.

Помимо этого, существует проблема устойчивости ЦВЗ к удалению путем воздействия различных преобразований, таких как, добавление шума, фильтрация, геометрические атаки и так далее. Разрабатываемые алгоритмы встраивания ЦВЗ, направленные на решение проблем устойчивости к воздействию атак, обладают низким объемом скрытия или высокой вычислительной сложностью, что уменьшает возможности их практического применения.

1.2 Алгоритмы встраивания водяных знаков

Стеганографические алгоритмы можно классифицировать по различным критериям. По типу контейнера методы делятся на методы встраивания в текст, аудио, изображения, видео, сетевые пакеты и т.д [29]. Наиболее распространенными контейнерами являются аудиосигналы и изображения, поскольку являются наиболее часто передаваемым типом информации и обладают информационной избыточностью, обеспечивающей высокий объем встраивания.

Наиболее известные стеганографические методы встраивания ЦВЗ, в рамках которых разработано значительное количество алгоритмов были предложены в [30].

Алгоритмы встраивания ЦВЗ можно также разделить по принципу сокрытия на алгоритмы непосредственной замены и спектральные. Алгоритмы непосредственной замены используют избыточность контейнеров. Встраивание в таком случае реализуется путем замены малозначительной части контейнера данными ЦВЗ. Спектральные алгоритмы для сокрытия данных используют спектральные представления коэффициенты (например, коэффициенты дискретного косинусного преобразования (ДКП), преобразования Фурье, дискретного вейвлет-преобразования (ДВП) и т.д.).

Алгоритмы непосредственной замены отличаются низкой вычислительной сложностью и возможностью сокрытия большого объема данных. Главным недостатком таких алгоритмов является их неустойчивость в условиях воздействия на

стегоконтейнер. Поэтому на сегодняшний день основные исследования направлены на разработку алгоритмов в спектральной области встраивания, позволяющих достичь высокой устойчивости встраивания водяных знаков.

Одним из наиболее перспективных направлений защиты авторских прав являются фрактальные методы и алгоритмы.

1.3 Встраивание водяных знаков на основе фрактального анализа

Фрактальный анализ может быть использован для встраивания больших объемов информации в одномерные (звуковые сигналы) или двумерные (изображения) контейнеры, не влияя на их качество и сделать скрытую информацию устойчивой и достаточно эффективной к мешающим воздействиям и неправомерному использованию [31-34].

Фрактальная техника позволяет скрыть секретную информацию без фактического ухудшения качества и структуры контейнера (аудио или видео) [35].

Теория фракталов охватывает широкий класс стохастических процессов от долговременной зависимости (ДВЗ), самоподобия, до мультифракталов [36]. Для оценки степени самоподобия используются понятия фрактальной размерности множества (по Хаусдорфу) D и показатель Херста H , характеризующий степень самоподобия процесса, которые связаны между собой соотношением: $D = 2 - H$.

Фрактальная размерность множества (по Хаусдорфу) определяется соотношением

$$D = - \lim_{\varepsilon \rightarrow 0} \frac{\lg[N(\varepsilon)]}{\lg[\varepsilon]}, \quad (1)$$

где $N(\varepsilon)$ - минимальное число непустых кубов размером ε , покрывающих заданное множество.

Среди множества процессов с ДВЗ в теории вероятности и фрактальном встраивании информации важны самоподобные процессы, из-за их связи с пре-

дельными теоремами и их довольно простой структуре.

Рассмотрим стационарный процесс $\{Y_i, i \in Z\}$, $Y = \{Y_i, i \in Z\}$ с автоковариационной функцией

$$\gamma(k) = \text{Cov}[Y_i, Y_{i+k}], k \in Z. \quad (2)$$

Автокорреляционная функция задается при помощи $\rho(k) = \gamma(k)/\gamma(0)$ и функции спектральной плотности мощности

$$f(\lambda) = \frac{1}{2\pi} \sum_{k=-\infty}^{\infty} \gamma(k) e^{ik\lambda}, \lambda \in [\pi, -\pi]. \quad (3)$$

Определение 1. Процесс $\{Y_i, i \in Z\}$, называется стационарным процессом с долговременной зависимостью (или длинной памятью), если существует действительное число $H \in (0,5; 1)$ и постоянная $c_\rho > 0$, такие что

$$\lim_{k \rightarrow \infty} \frac{\rho(k)}{c_\rho k^{2H-2}} = 1, \quad (4)$$

где H называется показателем Херста, который измеряет степень долговременной зависимости.

Для кратковременно зависимых (КВЗ или процессов с «короткой» памятью) процессов автокорреляционная функция ограничена геометрически, т.е. $\lim_{k \rightarrow \infty} \rho(k)/c^k = 1$, $0 < c < 1$ и поэтому $\sum_k \rho(k) < \infty$.

Процесс, для которого справедлива формула (4) при $0 < H < 0,5$ и $\sum_k \rho(k) < \infty$ называется процессом с промежуточной памятью.

Стохастический процесс является самоподобным, если он инвариантен в распределительном смысле при масштабировании во времени и в пространстве. Для точных самоподобных процессов существует строгое правило масштабирования, определяемое при помощи показателя Херста (H) на всех доступных масштабах времени. Так самоподобный гауссовский процесс называется фрактальным броуновским движением (ФБД).

Определение 2. Действительнозначный процесс $\{Y(t), t \in R\}$ является са-

моподобным с показателем $H > 0$ (H-ss), если для всех $a > 0$ конечномерные распределения для $\{Y(at), t \in \mathbb{R}\}$ идентичны конечномерным распределениям для $\{a^H Y(t), t \in \mathbb{R}\}$, т.е. для любых $k \geq 0, t_1, t_2, \dots, t_k \in \mathbb{R}$ и любых $a > 0$,

$$(Y(at_1), Y(at_2), \dots, Y(at_k)) \stackrel{d}{=} (a^H Y(t_1), a^H Y(t_2), \dots, a^H Y(t_k)) . \quad (5)$$

Соотношение можно записать более сжато:

$$Y(at) \stackrel{d}{=} a^H Y(t) . \quad (6)$$

Для практических целей важен лишь диапазон $0,5 < H < 1$. В этом диапазоне автокорреляционная функция процесса приращений $Y(t)$, которая может быть определена в дискретном времени как

$$Z_k = Y(k) - Y(k-1), k \in \mathbb{Z} . \quad (7)$$

имеет следующий вид:

$$\rho(k) = \frac{1}{2} [(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}] . \quad (8)$$

Показатель Херста H характеризует степень самоподобия процесса:

1. $0 < H < 0,5$ – случайный процесс, который не обладает самоподобием, характеризуется стремлением к среднему значению;
2. $H = 0,5$ – полностью случайный процесс без выраженной тенденции;
3. $H > 0,5$ – трендо устойчивый процесс, который обладает длительной памятью и является самоподобным.

В зависимости от назначения и способов генерации двумерные фракталы подразделяются на три большие группы: природные, алгебраические и геометрические.

Наибольшей группой являются алгебраические или динамические фракталы, которые строятся на основе итераций нелинейных отображений, задаваемых простыми алгебраическими формулами. В общем случае отображение $f(z)$ сопо-

ставляет комплексное число $z_n = x_n + iy_n$ другому комплексному числу $z_{n+1} = x_{n+1} + iy_{n+1}$ согласно итерационному правилу $z_{n+1} = f(z_n)$, где n -номер итерации.

Наиболее используемым является обобщенное квадратичное отображение на комплексной плоскости.

$$Z_{n+1} = Z_n^2 + C, \quad (9)$$

где $C = \text{Re } C + i \text{Im } C$ – комплексная константа – точка на комплексной плоскости.

Можно отметить закономерности в поведении системы при различных значениях параметров:

- если $C=0$ и $|Z_n| < 1$, то Z_n при $n \rightarrow \infty$ будет всегда оставаться в пределах единичного круга;
- если $|Z_n| > 1$, значения итераций будут уходить в бесконечность.

Таким образом, существует только два аттрактора: нуль и бесконечность. Если C не равно нулю, значения функции будут ограничены в пределах определенной границы или уходить в бесконечность.

В зависимости от поведения системы можно выделить некоторые виды алгебраических фракталов. Например, множество Мандельброта, которое можно определить как множество всех точек C , для которых итерации $Z_{n+1} = Z_n^2 + C$ ($Z_0 = 0$) остаются ограниченными при $n \rightarrow \infty$ [37]. В общем случае множество Мандельброта не является самоподобным, но содержит в составе различные самоподобные структуры – кардиоды, хвосты морских коньков, круги. Самоподобными являются некоторые частные случаи, например «кактус Мандельброта», состоящий из большой сердцевидной кардиоды и большого числа маленьких «лепестков» круглой формы.

При $Z_0 \neq 0$ квадратичное отображение может отображаться в виде различных фрактальных множеств. Множество значений Z_0 при заданном значении C и

ограниченном количестве итераций может отображаться в виде заполненных множеств или терять связность и рассыпаться на осколки. Заполненные множества носят название множество Жюлиа, несвязные осколки – пыль Фату.

На рисунке 1 изображен «кактус Мандельброта».

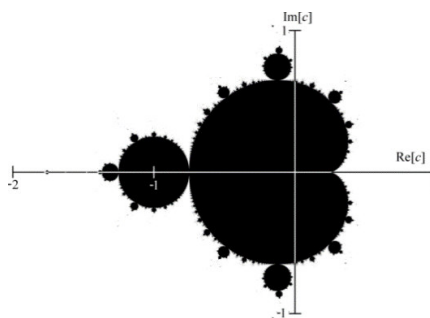


Рисунок 1 – «Кактус Мандельброта» [38]

Принадлежность точки c к «кактусу Мандельброта» влияет на вид множества Жюлиа:

- если константа C лежит внутри основной кардиоиды множества Мандельброта ($\text{Re} c \in [-0.75, 0.25]$), то некоторая фрактально деформированная окружность охватывает единственную притягивающую неподвижную точку;
- если C лежит в пределах окружности с центром на вещественной оси в точке $(-1, 0)$, которая примыкает к главной кардиоиде, ($\text{Re} c \in [-1.25, 0.75]$), множества Жюлиа имеют аттрактор периода 2, который возникает в результате бифуркации неподвижной точки, когда C перемещается внутрь этой окружности;
- если C лежит внутри одной из почек, то множество Жюлиа состоит из бесконечного числа фрактально деформированных окружностей, охватывающих точки периодического аттрактора и их прообразы;
- если C является точкой прорастания почки, то имеет место параболический случай; граница имеет усики, дотягивающиеся до маргинально устойчивого аттрактора;
- если C является любой другой точкой границы кардиоиды или почки, то мы имеем диск Зигеля.

Однако эти типовые случаи не исчерпывают разнообразия множеств Жюлиа. При внимательном рассмотрении оказывается, что множество Мандельброта окружено иглоподобными более или менее разветвленными и изогнутыми антеннами. На каждую антенну множества Мандельброта нанизано множество его маленьких копий, и между двумя большими копиями имеется еще одна, меньшая, и так без конца. Эти иглоподобные формы называются дендритами. Если поместить C на самый конец одной из таких антенн, то при тех же значениях C мы получим и множества Жюлиа подобной формы.

При выходе за границы множества Мандельброта множества Жюлиа распадается в облако точек, превращаются в пыль Фату. Эта пыль становится все мельче и мельче по мере удаления C от множества Мандельброта. Если C находится вблизи границы множества Мандельброта, то пыль образует область заворачивающих фигур — долину морских коньков в окрестности $z_0 \approx 0$ [39].

На рисунке 2 графически представлена описанная выше зависимость формы фрактального множества от точки C .

Фрактальная геометрия широко используется при разработке новых стеганографических методов встраивания информации [40-43].

В [44] предлагается алгоритм встраивания информации в аудиосигнал, основанный на хаотичной замене наименее значащих бит коэффициентов фрактального сжатия. Предлагаемый алгоритм обеспечивает высокое качество маркированного аудио при увеличении возможного объема встраивания на 30% по сравнению с известными методами. Однако он обладает высокой вычислительной сложностью из-за использования фрактального сжатия.

В [45] представлен алгоритм встраивания изображений на основе алгебраических фракталов для цветных изображений. Множество Жюлиа и множество Мандельброта генерируются для получения ключевого потока. Далее выполняется активное перемешивание пикселей до тех пор, пока они не будут полностью разупорядочены и применяется рассеивание значений с операцией XOR.

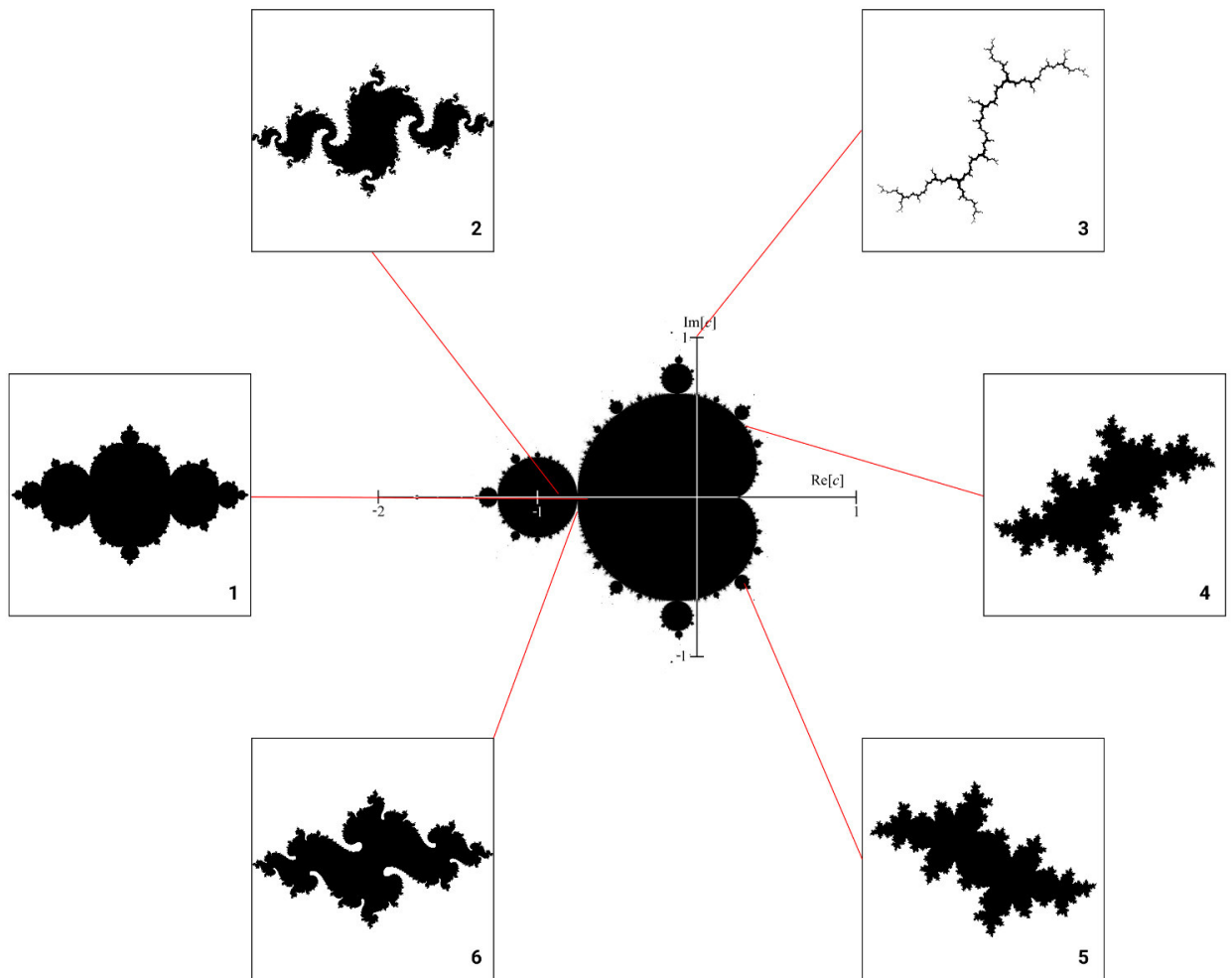


Рисунок 2 – Различные виды множества Жюлиа в зависимости от начальной точки

Такой алгоритм эффективен в целях скрытия самого изображения, но не предоставляет возможности для встраивания секретной информации или добавления ЦВЗ.

Большая часть алгоритмов встраивания с использованием фрактальной геометрии использует фракталы в качестве контейнеров.

В [46] предлагается алгоритм скрытия водяного знака в виде изображения без контейнера, основанный на теории фракталов. Секретная информация скрывается путем управления цветом пикселей в процессе генерации алгебраического

фрактала. В зависимости от длины встраиваемого сообщения и размера контейнера, каждый бит сообщения может быть представлен в виде пикселя или последовательности пикселей на фрактальном изображении. Надежность, незаметность и способность сопротивления стегоанализу уравниваются длиной последовательности пикселей, используемой для встраивания одного бита водяного знака. Поскольку алгоритм напрямую генерирует изображения-контейнеры, он может обеспечивать устойчивость к обнаружению большинством существующих методов стегоанализа.

В [47] представлен альтернативный стеганографический алгоритм, в котором секретные данные скрываются в процессе генерации множества Жюлиа. Отправитель и получатель формируют свои открытые ключи, которые определяют часть параметров множества Жюлиа. В качестве секретного ключа используется значение начальной точки Z_0 , на основе которой производятся итерации. Встраивание информации осуществляется в пиксели сгенерированного фрактала. На приемной стороне с помощью того же закрытого ключа генерируется аналогичный фрактал и секретные данные извлекаются путем сравнения пустого и заполненного контейнера.

В [48] предложен слепой алгоритм стеганографии цветных изображений, использующий сингулярное разложение, целочисленное вейвлет-преобразование и дискретное вейвлет-преобразование. Предлагаемый алгоритм скрывает цветное секретное изображение внутри фрактального изображения контейнера, создавая таким образом уникальное стегоизображение, которое практически является точной копией исходного изображения контейнера.

В [49] предлагается алгоритм, где наряду с фракталами для встраивания информации используются хаотические процессы. Предлагаемый алгоритм основан на процессе перетасовки фрактального ключа с хаотической последовательностью. Добавление фрактального ключа и хаотической последовательности повышает надежность алгоритма к атакам по сравнению с традиционными алгоритма-

ми. Но в результате использования данного алгоритма происходит полное искажение оригинального контейнера.

Ведутся активные исследования в области разработки фрактальных алгоритмов встраивания. Однако, учитывая сложность, ряд вопросов, связанных с защитой авторских прав, остается нерешенным.

Анализ существующих алгоритмов показал, что в большинстве случаев встраивание ЦВЗ осуществляется путем изменения фрактальных свойств изображения или основано на процессе генерации фракталов. Недостаток этих алгоритмов заключается в том, что как правило они требуют при извлечении ЦВЗ оригинала контейнера (в первом случае), либо область их практического применения (во втором случае) ограничена.

В отличие от известных алгоритмов предлагается разработать двухконтейнерные схемы. Либо в качестве промежуточного контейнера – ключа использовать алгебраические фракталы. Либо встраивать фрактал в контейнер путем изменения фрактальных свойств отдельных параметров контейнера, как аудио, так и фото (изображения).

Одним из популярных методов нахождения фрактальной размерности является вейвлет анализ.

1.4 Особенности использования 2D ДВП для встраивания ЦВЗ

Известно большое разнообразие алгоритмов стеганографического встраивания ЦВЗ с использованием вейвлет преобразований. По методу модификации их можно разделить на аддитивные алгоритмы, квантизацию и объединение.

К наиболее известным алгоритмы стеганографического встраивания, оперирующие в области вейвлет преобразований, можно отнести алгоритмы, представленные в [50-56]. Ведутся активные исследования в области разработки алгоритмов с использованием ДВП.

В [57] представлен метод стеганографии изображений, который скрывает

секретное изображение и ключ внутри цветного изображения контейнера с помощью дискретного вейвлет преобразования (ДВП) и целочисленного вейвлет-преобразования (ЦВП). Значения коэффициентов изображения контейнера и секретного изображения объединяются с использованием техники слияния. Изображение контейнер представляет собой цветное изображение, а секретное изображение представляет собой изображение в градациях серого. Этот алгоритм сначала разделяет цветовые плоскости RGB покрываемого изображения. Затем алгоритм извлекает либо коэффициенты ДВП, либо коэффициенты ЦВП красной составляющей как изображения контейнера, так и секретного изображения. Эти две полученные матрицы коэффициентов объединяются в одно изображение с помощью метода слияния на основе вейвлетов. Стегоизображение формируется путем применения обратного вейвлет-преобразования.

В [58] предложена схема стеганографии изображений с разложением по двойной матрице и несколькими областями покрытия. На первом этапе контейнер преобразуется мультивейвлет-преобразованием, а затем выбирается скрытая область, охватывающая несколько поддиапазонов вейвлета, в вейвлет области изображения контейнера. Скрытая область используется для скрытия секретных данных. К скрытой области применяется преобразование Арнольда, разложение Хессенберга и сингулярное разложение. На заключительном этапе секретная информация встраивается в изображение контейнер путем добавления коэффициента интенсивности.

В [59] предложен алгоритм, основанный на модели зрительной системы человека. В этом алгоритме ДВП коэффициенты используются как носитель скрытого сообщения. Визуальные искажения в этом методе устраняются введением другого алгоритма, который создается на основе модели зрительной системы человека. На первом этапе определяется максимально допустимое изменение каждого коэффициента ДВП с использованием визуальной модели человека. Затем модель подгоняется к гистограмме коэффициентов низкой точности и биты сооб-

щения кодируются в соответствии с этой моделью. На последнем этапе биты зашифрованного сообщения встраиваются в коэффициенты с учетом максимально возможных изменений, которые визуальны незаметны.

Вейвлет преобразования являются современным видом преобразования, используемым в спектральных методах встраивания ЦВЗ [60-64]. Применение ДВП эффективно по двум важным причинам. Во-первых, оно имеет неравномерное распределение значений при обратном преобразовании. Во-вторых, оно имеет низкую линейную сложность, которая требует меньших вычислительных затрат $O(n)$ по сравнению с вычислительными затратами, потребляемыми преобразованиями Фурье и косинусными, равными $O(n \log(n))$.

При внедрении ЦВЗ в изображения используется двумерное дискретное вейвлет преобразование (2D ДВП), которое вычисляется путем выполнения низкочастотной и высокочастотной фильтрации пикселей изображения. На каждом уровне, высокочастотный фильтр формирует подробную (детальную) информацию пикселей изображения, в то время как низкочастотный фильтр осуществляет грубые приближения входного изображения. После очередного уровня разложения количество низкочастотных и высокочастотных коэффициентов уменьшается примерно в 2 раза. Для того чтобы обеспечить 2D ДВП, дважды применяется одномерное 1D ДВП путем горизонтальной и вертикальной фильтрации. Другими словами, 2D ДВП может быть осуществлено, сначала, выполняя 1D ДВП каждой строке изображения, которое в этом случае называется горизонтальной фильтрацией, с последующим 1D ДВП каждого столбца, которое называется в этом случае вертикальной фильтрацией.

При двумерном вейвлет-преобразовании реализуют двумерную масштабную функцию $\phi(x,y)$ и три двумерные вейвлет-функции $\psi^H(x,y)$, $\psi^V(x,y)$ и $\psi^D(x,y)$ [65].

Данные функции могут быть представлены в виде:

$$\begin{aligned}
\varphi(x, y) &= \varphi(x)\varphi(y) \\
\psi^H(x, y) &= \psi(x)\phi(y) \\
\psi^V(x, y) &= \varphi(x)\psi(y) \\
\psi^D(x, y) &= \psi(x)\psi(y)
\end{aligned} \tag{10}$$

Семейство базисных функций можно задать с помощью операций масштабирования и сдвига.

$$\begin{aligned}
\varphi_{k,m,n}(x, y) &= 2^{k/2} \varphi(2^k x - m, 2^k y - n), \\
\psi_{k,m,n}^\delta(x, y) &= 2^{k/2} \psi^k(2^k x - m, 2^k y - n),
\end{aligned} \tag{11}$$

где m, n – сдвиг по горизонтали и вертикали соответственно, k – уровень разложения, $\delta = \{H, V, D\}$ определяет конкретную вейвлет-функцию.

Дискретное вейвлет-преобразование (ДВП) изображения $S(x, y)$ размерностью $M \times N$ вычисляется по формулам

$$\begin{aligned}
W_\varphi(j_0, m, n) &= \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} S(x, y) \varphi_{j_0, m, n}(x, y); \\
W_\psi^i(j, m, n) &= \frac{1}{\sqrt{M_j N_j}} \sum_{x=0}^{M_j} \sum_{y=0}^{N_j} S(x, y) \psi_{j, m, n}^i(x, y); \quad i = H, V, D,
\end{aligned} \tag{12}$$

где x и y – координаты пикселя по горизонтали и вертикали соответственно.

Исходное изображение $S(x, y)$ может быть восстановлено при помощи обратного дискретного вейвлет-преобразования вида

$$\begin{aligned}
S(x, y) &= \frac{1}{\sqrt{MN}} \sum_m^M \sum_n^N W_\varphi(j_0, m, n) \varphi_{j_0, m, n} + \\
&+ \sum_{i=H, V, D} \sum_{j_0}^{M_1} \sum_{m_1}^{N_1} [\sum_{m_2}^{M_2} \sum_{n_2}^{N_2} W_\psi^i(j=1, m_1, n_1) \psi_{j=1, m_1, n_1}^i(x, y) + \\
&+ \sum_{m_2}^{M_2} \sum_{n_2}^{N_2} W_\psi^i(j=2, m_2, n_2) \psi_{j=2, m_2, n_2}^i(x, y) + \\
&+ \sum_{m_3}^{M_3} \sum_{n_3}^{N_3} W_\psi^i(j=3, m_3, n_3) \psi_{j=3, m_3, n_3}^i(x, y)].
\end{aligned} \tag{13}$$

На рисунке 3 показано три уровня разложения. На первом уровне изображение раскладывается на четыре поддиапазона, которые несут информацию о частоте, как в горизонтальном, так и вертикальном направлениях. Для того чтобы сформировать несколько уровней разложения, алгоритм применяется рекурсивно к поддиапазону $W_\phi(j,m,n)$.

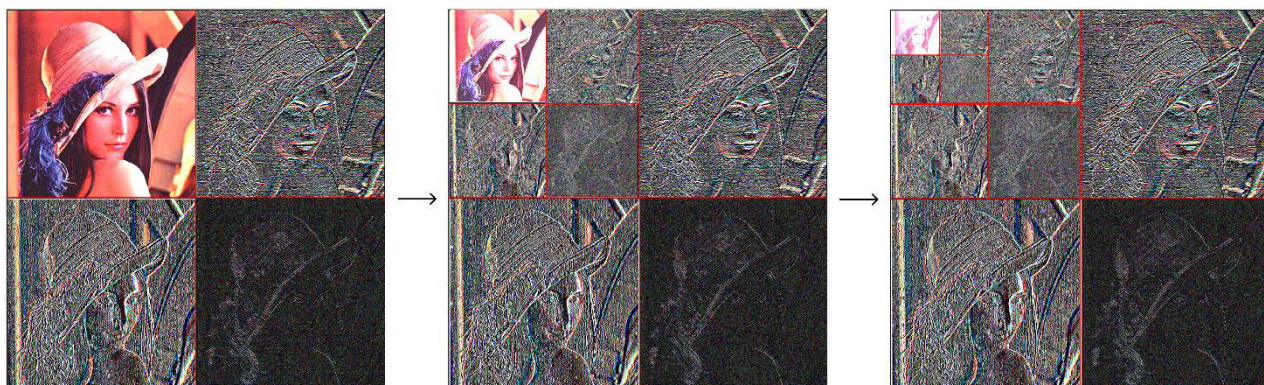
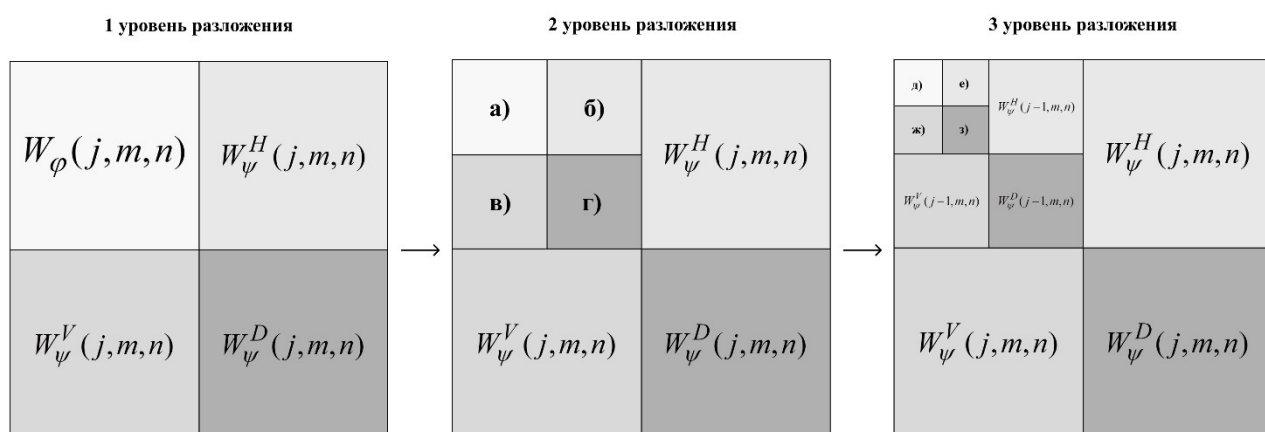


Рисунок 3 – Три уровня 2D ДВП

Использование 2D ДВП при встраивании ЦВЗ является актуальным направлением исследования. Несмотря на ряд преимуществ, связанных с низкой вычислительной сложностью и повышении устойчивости к сжатию, существующие алгоритмы имеют ряд недостатков. Как правило, извлечение ЦВЗ производится путем сравнения оригинальных и измененных значений коэффициентов ДВП, что приводит к необходимости наличия оригинала контейнера на приемной стороне. Либо при встраивании одного бита используется набор пикселей, что приводит к уменьшению возможного объема встраиваемого ЦВЗ.

В отличие от известных алгоритмов предлагается использовать двухкомпонентные системы, в которых производится замена всех коэффициентов ДВП на определенном уровне разложения значениями фрактального ключа-контейнера.

1.5 Атаки на системы ЦВЗ

Оценка устойчивости к воздействию атак (как намеренных, так и непреднамеренных) является важной частью оценки эффективности стеганографической системы. В зависимости от назначения системы, она должны быть стойкой к определенным типам атак.

Атаки на системы ЦВЗ можно разделить на основные виды [66]:

1. Обнаружение присутствия ЦВЗ.
2. Извлечение встроенного ЦВЗ.
3. Удаление ЦВЗ без значительного искажения стегообъекта.
4. Ложное погружение других ЦВЗ.

Наиболее типичными для систем ЦВЗ являются последние две атаки, причем то, какая из них является наиболее опасной, зависит от цели, выполняемой при помощи вложения ЦВЗ.

Техники выполнения атак по удалению ЦВЗ весьма разнообразны и зависят от конкретного построения систем ЦВЗ. Основными преобразованиями, которые используются в качестве атак на системы ЦВЗ, являются

следующие [67]:

- добавление небольшого аддитивного шума;
- фильтрация (в том числе двумерная для изображений);
- масштабирование;
- вырезание фрагментов изображений;
- переквантование цифровых сигналов;
- вставка и удаление отсчетов;
- сжатие цифровых сигналов;
- оценка вложенного ЦВЗ и его вычитание (при аддитивном вложении ЦВЗ);
- геометрическое преобразование изображений с вложениями ЦВЗ;
- использование последовательных преобразований Д/А и А/Д.

1.6 Критерии оценки эффективности стеганографических систем

Оценка эффективности стеганографических систем представляет собой сложную задачу. Оценить стегосистемы можно по двум компонентам: эффективностью встраивания и устойчивостью к атакам.

Оценку стеганографической системы с точки зрения встраивания проводят на основе трёх критериев [68]:

1. Степень сокрытия информации.
2. Пропускная способность.
3. Визуальная незаметность.

Степень сокрытия информации может быть оценена с использованием статистических показателей, среди которых можно выделить расстояние Бхаттачарьи [69] и дивергенцию Кульбака-Лейблера [70].

Расстояние Бхаттачарьи оценивается как мера различия гистограмм распределения значений интенсивностей пикселей изображения и может быть вычислено с помощью соотношения [71, 72]:

$$d[P(S), Q(S^*)] = \sum_{u=1}^{256} \sqrt{P_u(S) Q_u(S^*)}, \quad (14)$$

где $P_u(S)$ – значения ячеек гистограммы контейнера, $Q_u(S^*)$ – значения ячеек гистограммы стегоконтейнера, u – номер ячейки гистограммы, g – общее число ячеек гистограммы.

Расстояние или дивергенция Кульбака-Лейблера— это мера, позволяющая определить, насколько информационная энтропия одного распределения отлична от энтропии другого распределения. Для определения значения параметра необходимо вычислить информационную энтропию обоих распределений и найти их разность.

Энтропия изображения определяется следующим образом:

$$P = - \sum_{i=0}^{n-1} p_i \log p_i, \quad (15)$$

где n – количество уровней серого.

Расстояние Кульбака-Лейблера можно получить с помощью соотношения:

$$D_{KL}(P(S) \parallel Q(S^*)) = \int_X P(S) \log \frac{P(S)}{Q(S^*)} d\mu. \quad (16)$$

В идеальном случае при полном соответствии двух изображений рассматриваемые метрики равны нулю.

Пропускная способность определяет максимально возможный объем встраивания. Под визуальной незаметностью следует понимать невозможность определения факта встраивания путем визуальной или слуховой оценки стегоконтейнера.

1.7 Выводы

1. Количество инцидентов, связанных с неправомерным использованием объектов авторского права, стремительно растет. При этом сложная процедура доказательства исключительного права на цифровой объект приводит к отсут-

ствию наказания для злоумышленников.

2. Классические алгоритмы стеганографии, направленные на защиту авторских прав, обладают рядом недостатков, связанных с низкой устойчивостью к атакам и мешающим воздействиям.

3. Использование специфической хаотичной природы фракталов позволяет достичь устойчивости к воздействию атак и попыток удаления встроенных водяных знаков. Однако существующие фрактальные алгоритмы требуют наличия оригинального контейнера на приемной стороне или ограничивают возможности выбора контейнера, что делает невозможным их использование в целях защиты авторских прав.

4. В связи с вышесказанным возникает актуальная научная задача разработки и исследования новых алгоритмов защиты авторских прав в фото и аудио контенте от угроз неправомерного использования, основанных на технологии фрактального анализа.

Глава 2 Маркирование аудиосигналов с использованием фрактального гауссовского шума

Как было показано в главе 1, существующие алгоритмы маркирования аудиосигналов обладают рядом недостатков, связанных с низким качеством аудиосигнала после встраивания и низкой устойчивостью к воздействию мешающих воздействий. Большой проблемой является необходимость наличия оригинального немаркированного аудио для извлечения ЦВЗ.

В главе предлагается алгоритм А1 защиты аудиосигналов путем встраивания ПСП с использованием фрактального гауссовского шума (ФГШ), разработка которого направлена на решение обозначенных проблем.

2.1 Алгоритм встраивания А1

В качестве водяного знака будет использоваться ключевая последовательность в виде двоичной псевдослучайной последовательности $ПСП(p) \in \{0, 1\}$, $p = \overline{1, P}$, однозначно определяющая пользователя.

Каждому биту ПСП в соответствие ставится непрерывнозначная последовательность $\{X_{\text{ФГШ}}(t_l); l = \overline{1, L}\} = \{X_{\text{ФГШ}, l}; l = \overline{1, L}\}$, где $L = N / P$ в виде фрактального гауссовского шума (ФГШ) с заданной фрактальной размерностью, характеризуемой показателем Херста H [73, 74]. Именно сформированные фрактальные последовательности будут использоваться при маркировании аудиосигнала.

Алгоритм встраивания p -го бита ПСП в аудиосигнал будем описывать соотношением:

$$y_p^*(t) = f\{S_{a,n}, \alpha, ПСП(p), X_{\text{ФГШ}, l}\}, \quad (17)$$

где α – масштабирующий коэффициент. Для встраивания ПСП будем использовать декомпозицию аудиосигнала в виде дискретного вейвлет разложения (ДВП).

Как известно [75] процесс $y_p(t)$, при конечном числе уровней разложения J , можно представить в виде упорядоченной совокупности коэффициентов разложения по системе масштабирующих и вейвлет-функций:

$$y_p(t) = \sum_{k=1}^{2^{L-M}} a_{m,k} \varphi_{m,k}(t) + \sum_{m=1}^M \sum_{k=1}^{2^{L-M}} d_{m,k} \psi_{m,k}(t), \quad m = \overline{1, M}, k = \overline{1, K}, p = \overline{1, P}, \quad (18)$$

где $\varphi_{m,k}(t)$ – базисная масштабирующая функция; $\psi_{m,k}(t)$ – базисная вейвлет-функция; $a_{m,k}, d_{m,k}$ – аппроксимирующие и детализирующие коэффициенты; m, k – параметры масштаба и сдвига в пространстве целых чисел I .

В компактном виде выражение (18) можно записать как:

$$y_p(t) = y_{p,J}(t) + \sum_{j=1}^J D_j(t), \quad (19)$$

где $y_{p,J}(t) = \sum_{k=0}^{L/2^J-1} a_{J,k} \varphi_{J,k}(t)$ – функция начальной аппроксимации, соответствующая масштабу $J < J_{\max}$; $a_{J,k} = \langle y_p(t), \varphi_{J,k} \rangle$ – масштабный коэффициент аппроксимации, равный скалярному произведению исходного ряда $y_p(t)$ и масштабной функции «самого грубого» масштаба J , смещенной на k единиц масштаба вправо от начала координат

$$D_j(t) = \sum_{k=0}^{L/2^j-1} d_{j,k} \psi_{j,k}(t). \quad (20)$$

Функция детализации j -го масштаба; $d_{j,k} = \langle y_p(t), \psi_{j,k} \rangle$ – вейвлет-коэффициент детализации масштаба j , равный скалярному произведению исходного ряда $y_p(t)$ и вейвлета масштаба j , смещенного на k единиц масштаба вправо от начала координат [76].

Выполняя ДВП для выборок внутри выбранного окна, размер которого равен длительности бита в L отсчетов, в каждый момент времени t_i , будем получать

на j - м масштабном уровне набор коэффициентов аппроксимации $\{a_{1x}, a_{2x}, a_{3x}, \dots, a_{nx}\}_{t,j}$ и детализации $\{d_{1x}, d_{2x}, d_{3x}, \dots, d_{nx}\}_{t,j}$.

Причем количество коэффициентов n на уровне j в окне L будет определяться выражением $n = \frac{M}{2^j}$. В частном случае $J=3$, процесс формирования аппроксимирующих и детализирующих коэффициентов разложения показан на рисунке 4.

$$\begin{aligned}
 y_p(t) &= y_{p,J}(t) + \sum_{j=1}^{J=3} D_j(t) = y_{p,J}(t) + D_1(t) + D_2(t) + D_3(t) = \\
 &= y_{p,J}(t) + \sum_{k=1}^{L/2} d_{1,k} \psi_{1,k}(t) + \sum_{k=1}^{L/4} d_{2,k} \psi_{2,k}(t) + \sum_{k=1}^{L/8} d_{3,k} \psi_{3,k}(t); p = \overline{1, P}.
 \end{aligned} \quad (21)$$

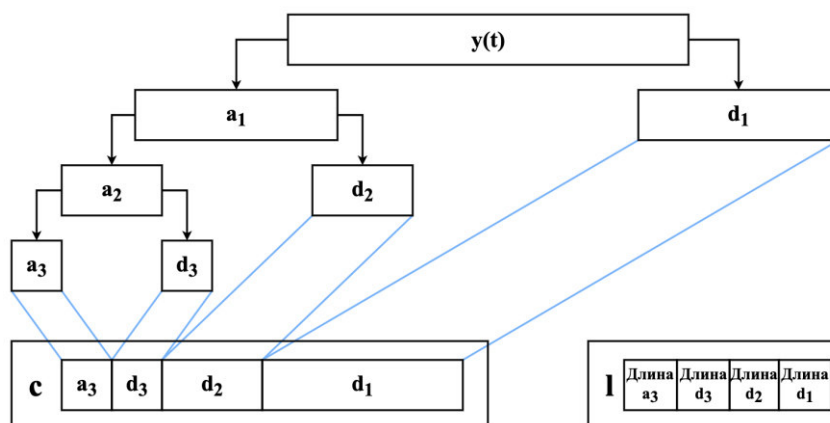


Рисунок 4 – Процедура трехуровневой вейвлет-декомпозиции

В результате формируются два вектора: C – содержащий информацию о значениях всех вейвлет коэффициентов (аппроксимирующих и детализирующих), и информирующий вектор l , характеризующий длину каждого уровня разложения.

В качестве примера на рисунке 5 представлено трехуровневое разложение сегмента аудиосигнала при $N = 2000$ и использовании материнского вейвлета Хаара.

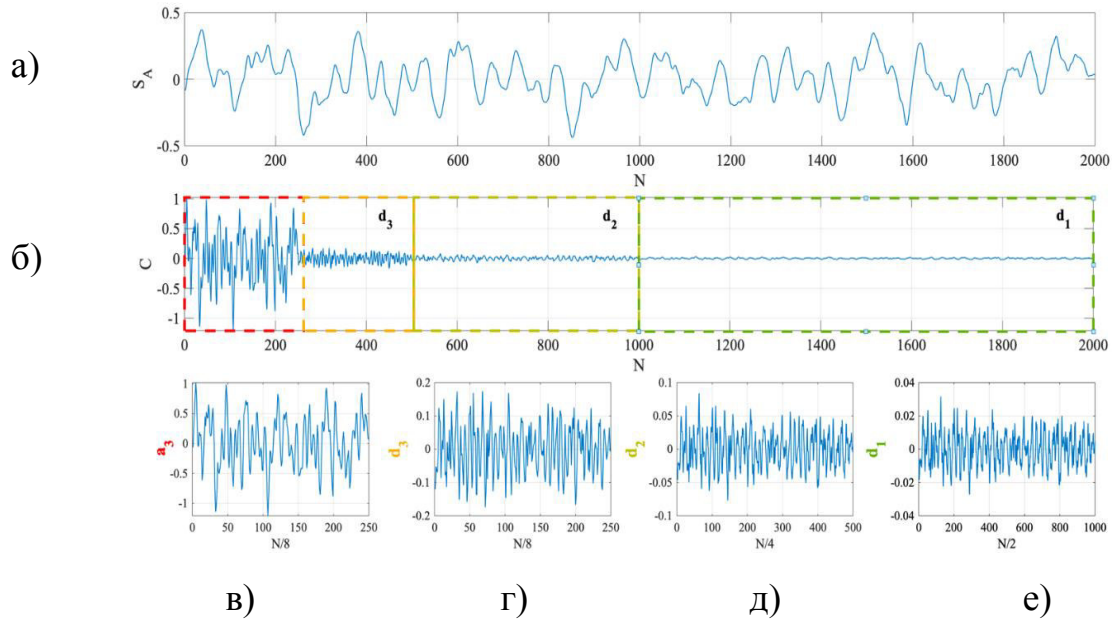


Рисунок 5 – Вейвлет декомпозиция аудио сегмента

а) Исходный сегмент аудиосигнала; б) вейвлет коэффициенты после декомпозиции; в) коэффициенты аппроксимации; г) коэффициенты детализации третьего уровня; д) коэффициенты детализации второго уровня; е) коэффициенты детализации первого уровня разложения

Воспользовавшись (17), (18) и (19) запишем алгоритм А1 встраивания элемента ПСП в h -й сегмент аудиосигнала путем изменения коэффициентов детализации на J -м уровне декомпозиции:

$$y_p^*(t) = y_{p,J}(t) + D_h^*(t) + \sum_{\substack{j \neq h \\ j=1}}^J D_j(t), \quad p = \overline{1, P}, \quad (22)$$

где

$$D_h^*(t) = \begin{cases} \alpha \sum_{k=1}^{\frac{L}{2^{J-1}}} X_k^{H=H_1} \psi_{h,k}(t); \text{при ПСП}(j) = 1 \\ \alpha \sum_{k=1}^{\frac{L}{2^{J-1}}} X_k^{H=H_0} \psi_{h,k}(t); \text{при ПСП}(j) = 0 \end{cases}. \quad (23)$$

В частном случае $J=3$ и $h=1$ можно записать

$$y^*(t) = y_J(t) + \alpha \sum_{k=1}^{\frac{N}{2}} X_k^H \psi_{1,k}(t) + \sum_{k=1}^{\frac{N}{4}} d_{2,k} \psi_{2,k}(t) + \sum_{k=1}^{\frac{N}{8}} d_{3,k} \psi_{3,k}(t) = y_J + D_1^*(t) + D_2(t) + D_3(t). \quad (24)$$

$$D_1^*(t) = \begin{cases} \alpha \sum_{k=1}^{\frac{N}{2}} X_k^{H=0.9} \psi_{1,k}(t); & \text{при } \lambda(t) = 1 \\ \alpha \sum_{k=1}^{\frac{N}{2}} X_k^{H=0.5} \psi_{1,k}(t); & \text{при } \lambda(t) = 0 \end{cases}. \quad (25)$$

Для встраивания «0» используется ФГШ с фрактальной размерностью, характеризуемой показателем Херста H_0 , а для встраивания «1» - ФГШ с показателем Херста H_1 . Длина фрактальной последовательности L определяется длиной сегмента аудиосигнала и уровнем вейвлет разложения, в коэффициенты которого встраивается ПСП.

На заключительном этапе встраивания происходит вейвлет реконструкция аудиосигнала с измененными коэффициентами детализации, как это показано на рисунке 6.

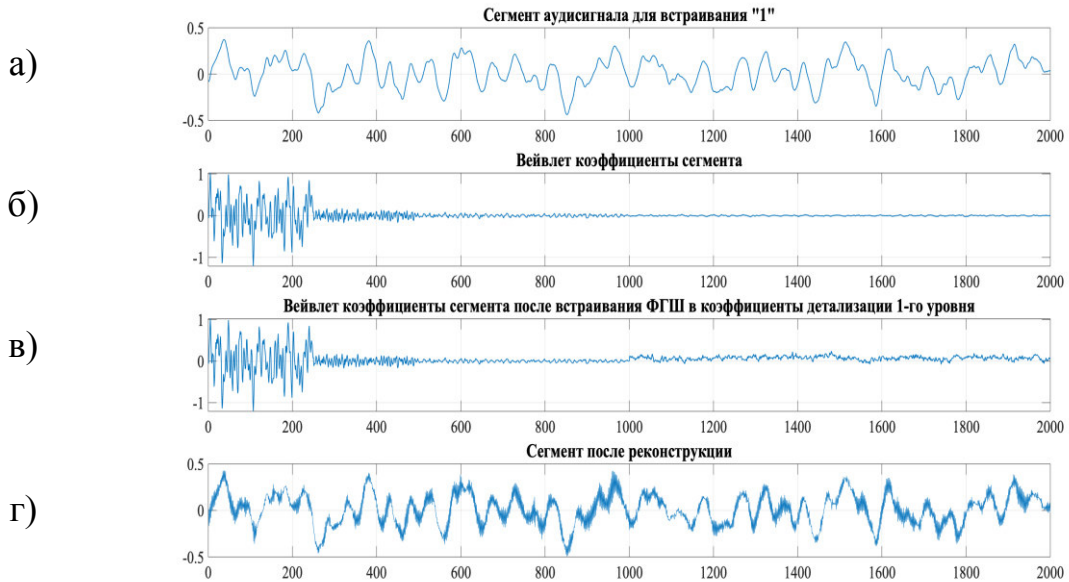


Рисунок 6 – Процесс вейвлет реконструкция аудиосигнала с использованием ФГШ на первом уровне разложения при $H_1 = 0.95$ при $\text{ПСП}(p) = 1$ ($\alpha = 0.1$)

а) Сегмент аудиосигнала до встраивания, б) вейвлет-коэффициенты сегмен-

та, в) вейвлет-коэффициенты сегмента после встраивания ФГШ в коэффициенты детализации первого уровня разложения, г) сегмент аудиосигнала после реконструкции

2.2 Генерация фрактального гауссовского шума

Необходимость преобразования исходного спектра узкополосного сигнала в спектр, сравнимый с естественным шумом, возникает при появлении потребности обеспечения «невидимости» встраиваемого сигнала. При этом фрактальный гауссовский шум позволяет сформировать шум с необходимым показателем Херста (H). ФГШ обладает следующим преимуществом: при встраивании ЦВЗ, модифицированного быстрым преобразованием Фурье (БПФ) [77], в сегмент аудиосигнала, структура фрактального шума остается неизменной. Благодаря этому ФГШ способен противостоять внешним модификациям, а значит, извлеченный ЦВЗ совпадает со встроенным. Следовательно, исчезает необходимость использования аудио-сигнала до встраивания и генератора ПСП. Для «слепого» считывания ЦВЗ необходимо минимизировать ошибку первого рода при считывании ЦВЗ путем корректной настройки порогового уровня. Таким образом, ФГШ способен обеспечить «слепое» определение встроенного водяного знака.

Для генерации фрактального гауссовского шума (ФГШ) будем использовать алгоритм быстрого преобразования Фурье, который позволяет генерировать самоподобные последовательности. Алгоритм генерации ФГШ основан на вычислении нормированной ковариационной функции вида [78, 79]:

$$r(\tau) = \frac{|\tau+1|^{2H} - 2|\tau|^{2H} + |\tau-1|^{2H}}{2}, \quad (26)$$

На первом этапе строятся комплексные числа, значения которых регулируются нормальным распределением, после чего применяется обратное БПФ. На рисунке 7 показан алгоритм формирования ФГШ при помощи БПФ.

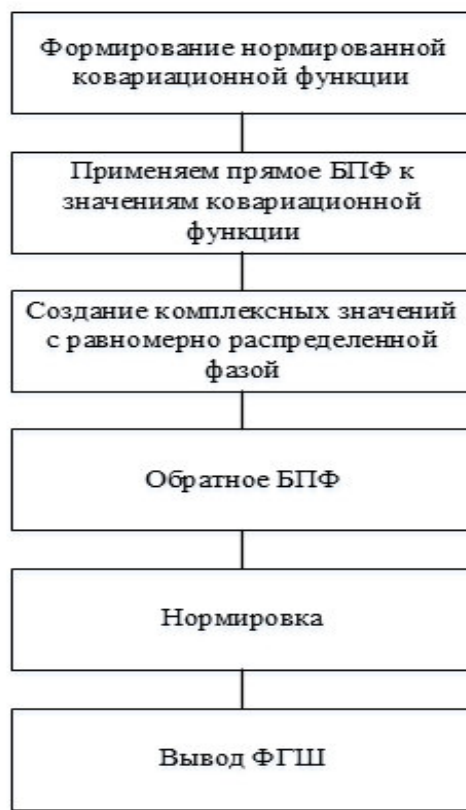


Рисунок 7 – Алгоритм генерации ФГШ

По шаговый алгоритм генерации ФГШ имеет следующий вид:

1. Формируется последовательность значений $\{k_1, \dots, k_i\}$ для построения нормированной ковариационной функции.
2. Строится нормированная ковариационная функция $r(k)$ от полученных на предыдущем шаге значений.
3. Применяя БПФ к значениям ковариационной функции и оценивается реальную часть полученных комплексных значений.
4. Генерируется последовательность комплексных чисел $\{Z_1, \dots, Z_i\}$, для которой $|Z_i| = \sqrt{r}$ и фаза Z_i является нормально распределенной.
5. Применяется обратное БПФ к полученным комплексным значениям и берем реальную часть и выполняем нормировку полученных значений.

На рисунке 8 показан сгенерированный шум для показателя Херста 0.15 и 0.95

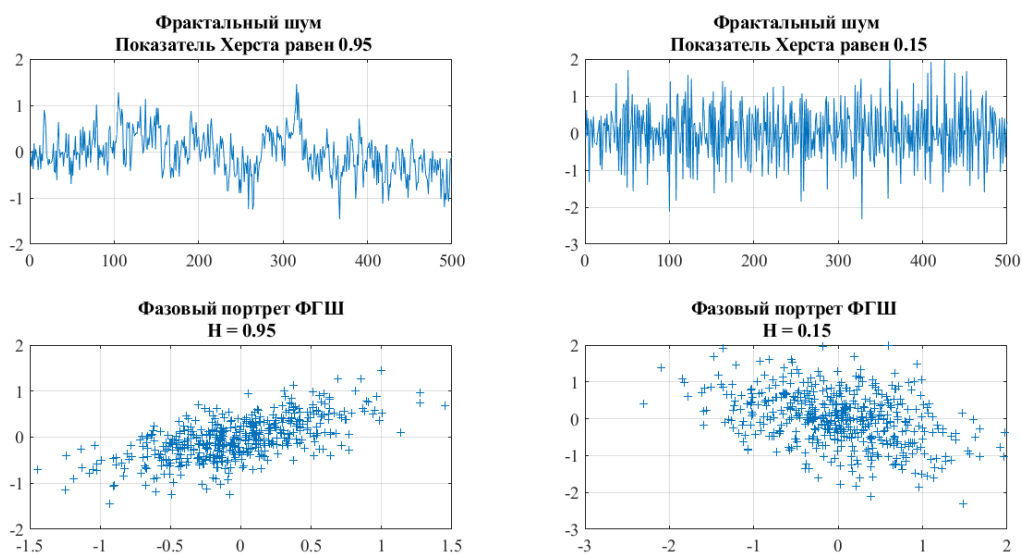


Рисунок 8 – ФГШ с показателем Херста 0.95(а) и с показателем Херста 0.15 (б)

2.3 Алгоритм извлечения

Принятый аудиосигнал делится на сегменты, к каждому сегменту применяется процедура разложения на вейвлет коэффициенты. Выделяется та часть детализирующих коэффициентов первого уровня и производится оценка индекса Херста H [80], по которой пороговое устройство определяет, передавался «0» или «1» в рассматриваемом сегменте аудио.

Для корректного извлечения ЦВЗ нужно знать длину встраиваемой последовательности P , длину сегментов на которые нужно делить сигнал L , параметры вейвлет декомпозиции: $\varphi_{m,k}(t)$ –масштабирующую и $\psi_{m,k}(t)$ – базисную вейвлет-функции, количество уровней разложения K . Для нахождения текущей оценки параметра Херста $\hat{H}_m$ при m -ом положении окна анализа необходимо выполнить линейную регрессию на шкале j в диапазоне $[j_1, j_2]$ в соответствии с уравнением

$$\log_2(\mu_{j,m}) = \log_2\left(\frac{1}{n_j} \sum_k |d_x^{(m)}(j,k)|^2\right) = (2\hat{H}_m - 1)j + \hat{c} = \alpha_m j + \hat{c}, \quad (27)$$

где $\hat{c} = const$.

Формула (16) описывает возможный способ оценки показателя Херста ДВЗ-процессов в виде линейной зависимости. Это означает, что, если процесс $\{y_p^*(t), p = \overline{1, P}\}$ является долговременно зависимым процессом с показателем Херста H_m , то график зависимости $\log_2(\mu_{j,m})$ от j , имеет линейный наклон $2\hat{H}_m - 1$ и масштабный показатель $\hat{a}_m = (2\hat{H}_m - 1)$ может быть получен путем оценки наклона графика функции $\log_2(\mu_{j,m})$ от j при каждом m -м положении окна анализа. Извлечение элемента ПСП осуществляется с использованием найденной оценки в соответствии с формулой

$$ПСП^*(p) = \begin{cases} 1 & \text{при } H_i \geq H_{пор} \\ 0 & \text{при } H_i < H_{пор} \end{cases}. \quad (28)$$

Если найденная оценка показателя Херста в анализируемом сегменте ПСП выше заданного порога $H_{пор}$, то принимается решение о встраивании «1», в противном случае – «0». Как правило величина порогового уровня $H_{пор}$ определяется по величине допустимой вероятности ошибки первого рода. На рисунке 9 показан пример реализации операции извлечения элементов ПСП^{*}(p) путем сравнения текущей оценки показателя Херста с пороговым уровнем.

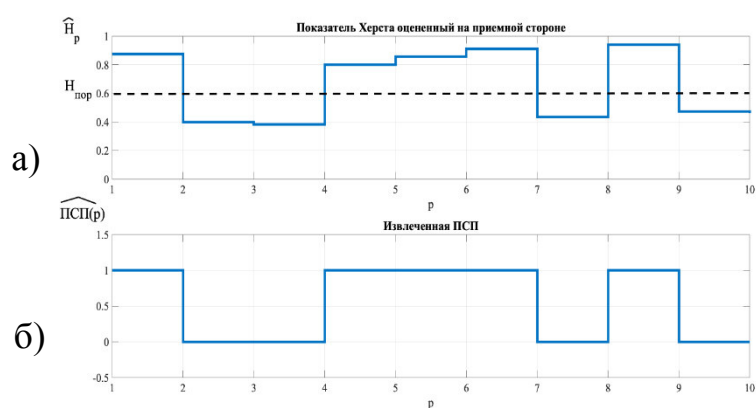


Рисунок 9 – Формирование элементов ПСП а) текущие оценки $\hat{H}_p$; б) $ПСП^*(p)$

На заключительном этапе вычисляется корреляционная функция между извлеченной из аудиосигнала ПСП^{*}(p) и опорной ПСП_p, сгенерированной на приемной стороне.

$$B_{ПСП}(i) = \frac{1}{M} \sum_{m=1}^M ПСП_p ПСП_{p+i}^* . \quad (29)$$

Сравнивая результат вычисления $B_{ПСП}(i=0)$ с пороговым уровнем, делается вывод о наличии и отсутствии ЦВЗ в аудиофайле.

Для определения рациональных параметров алгоритма, позволяющих достигнуть баланса между качеством встраивания и извлечения, проведены эксперименты с использованием набора аудио сигналов трех классов:

- класс 1: число каналов 1, частота дискретизации 8000 Гц, число бит для кодирования одного отсчёта 8;
- класс 2: число каналов 2, частота дискретизации 22050 Гц, число бит для кодирования одного отсчёта 16;
- класс 3: число каналов 2, частота дискретизации 44100 Гц, число бит для кодирования одного отсчёта 16.

Качество аудио файла, содержащего скрытую метку, зачастую оценивается на слух. Но такой подход имеет ряд недостатков: необходимость присутствия человека-оператора на передающем конце, различия в строении слухового аппарата у людей, высокие временные затраты и невозможность количественной оценки отличий между оригинальным аудио и аудио, содержащим встроенные данные. Поэтому наиболее предпочтительным является использование статистических метрик, позволяющих автоматизировать процесс оценки качества стеганографического аудио файла [81].

Для оценки аудио файла, содержащего скрытую метку, предложено использовать две метрики: среднеквадратичную ошибку MSE (*Mean Square Error*) и пиковое соотношение сигнал/шум PSNR (*Peak Signal to Noise Ratio*):

$$MSE = \frac{1}{N} \sum_{n=1}^N \delta_p^2(\alpha, L, \psi), n = \overline{1, N}, \quad (30)$$

$$\text{где } \delta(\alpha, N, \psi) = y(t) - y^*(t) = D_1(t) - D_1^*(t) = \sum_{k=1}^{\frac{N}{2}} \psi_{1,k} (d_{1,k} - \alpha X_k^*);$$

$$PSNR = 10 \lg \frac{N \max(y_p(t)^2)}{\sum_{p=1}^P \delta_p^2(\alpha, L, \psi)}. \quad (31)$$

Среднеквадратичная ошибка характеризует количественную меру отклонения аудиосигнала, содержащего скрытые данные, от оригинального пустого аудиосигнала. В качественных стегосистемах уровень MSE близок к нулю. Для пикового соотношения сигнал/шум справедлива обратная закономерность: чем выше PSNR, тем выше качество аудио. Оптимальный порог может быть определен путем проведения слуховых тестов [82].

Для определения достоверности извлечения вычислялось значение дисперсии функции дисперсии $V_{\text{ПСП}}(i=0)$ извлеченного и опорного ПСП (18). Уровень достоверности был определен, как доля извлеченных ПСП, для которых $V_{\text{ПСП}}(i=0) \geq 0.95$. Допустимый уровень достоверности извлечения был установлен на уровне 0,95.

Рассмотрим зависимости статистических метрик от значений параметров стегосистемы, таких как уровень разложения, длина шума, показатель Херста единичной последовательности H_1 и порог $N_{\text{пор}}$. Численные результаты экспериментов приведены в приложении В.1.

2.4 Выбор уровня разложения

На рисунке 10 представлена зависимость MSE от уровня разложения аудиосигнала, на котором производилась замена коэффициентов при $L=1000$, $N=1000$.

При исследовании рассматривались 4 типа вейвлет разложения: Хаар [83], Добеши 4 [84], Симлет 4 [85], Койфлет 4 [86].

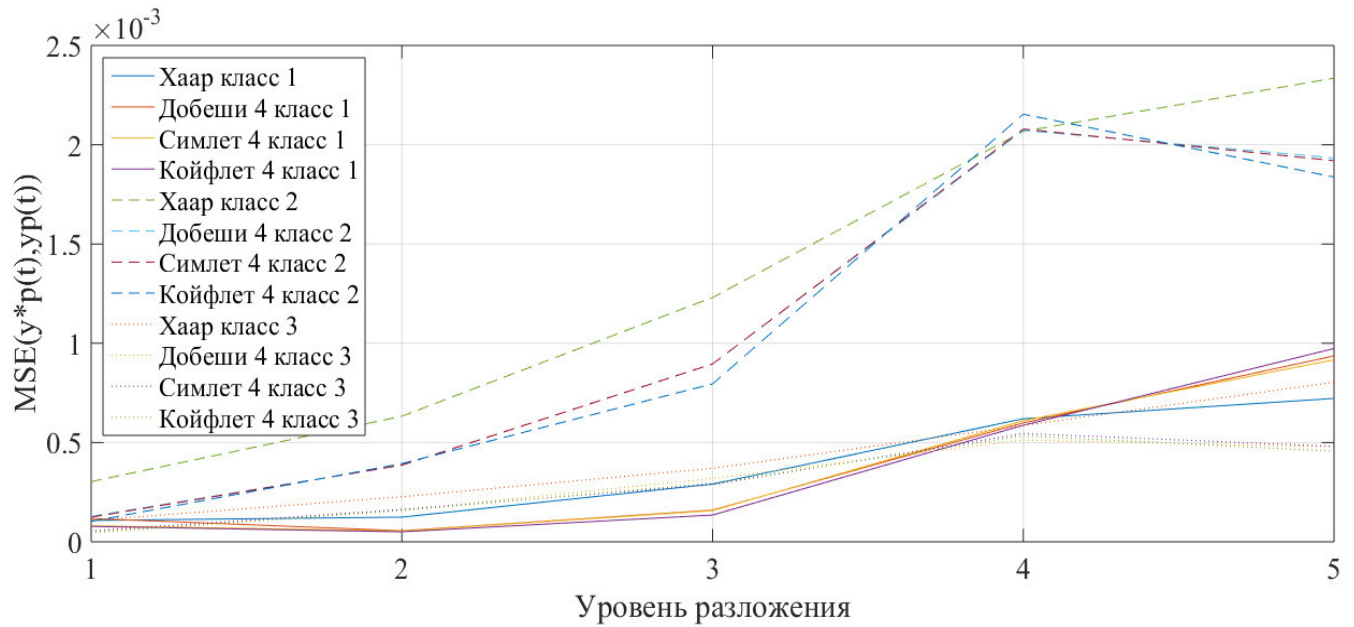


Рисунок 10 – Зависимость MSE маркированного аудиосигнала от уровня разложения аудиосигнала

На рисунке 11 представлена зависимость PSNR от уровня разложения при аналогичных параметрах алгоритма.

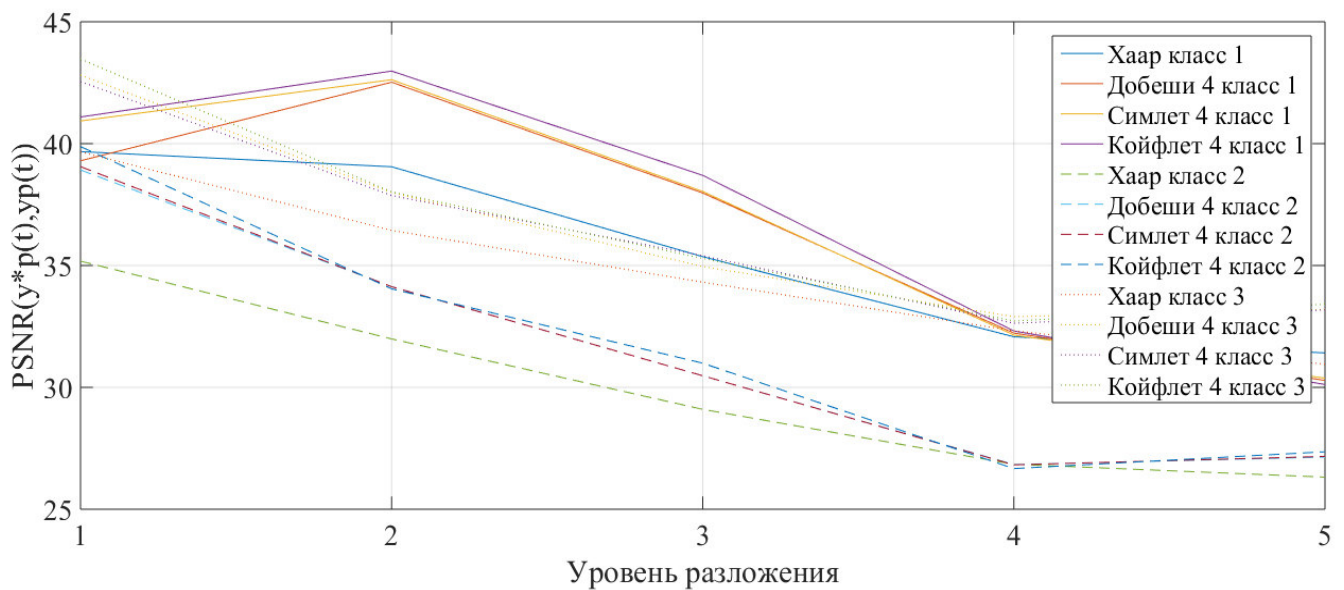


Рисунок 11 – Зависимость PSNR маркированного аудиосигнала от уровня разложения аудиосигнала

Анализ полученных результатов показал, что качество заполненного аудиосигнала ухудшается при увеличении уровня разложения, используемого для встраивания. Для аудио класса 1 при использовании вейвлетов Добеши 4, Симлет 4 и Койфлет 4, наилучшие показатели качества достигаются при использовании коэффициентов 2 уровня разложения. Однако разница незначительна (~ 1 дБ), что позволяет рекомендовать использовать для встраивания ПСП коэффициенты 1-го уровня разложения. Наилучшие результаты скрытия наблюдаются при использовании вейвлета Койфлет и Симлет.

На рисунке 12 представлены зависимости максимального значения корреляционной функции извлеченной и опорной ПСП от уровня вейвлет разложения, на котором производилась замена коэффициентов.

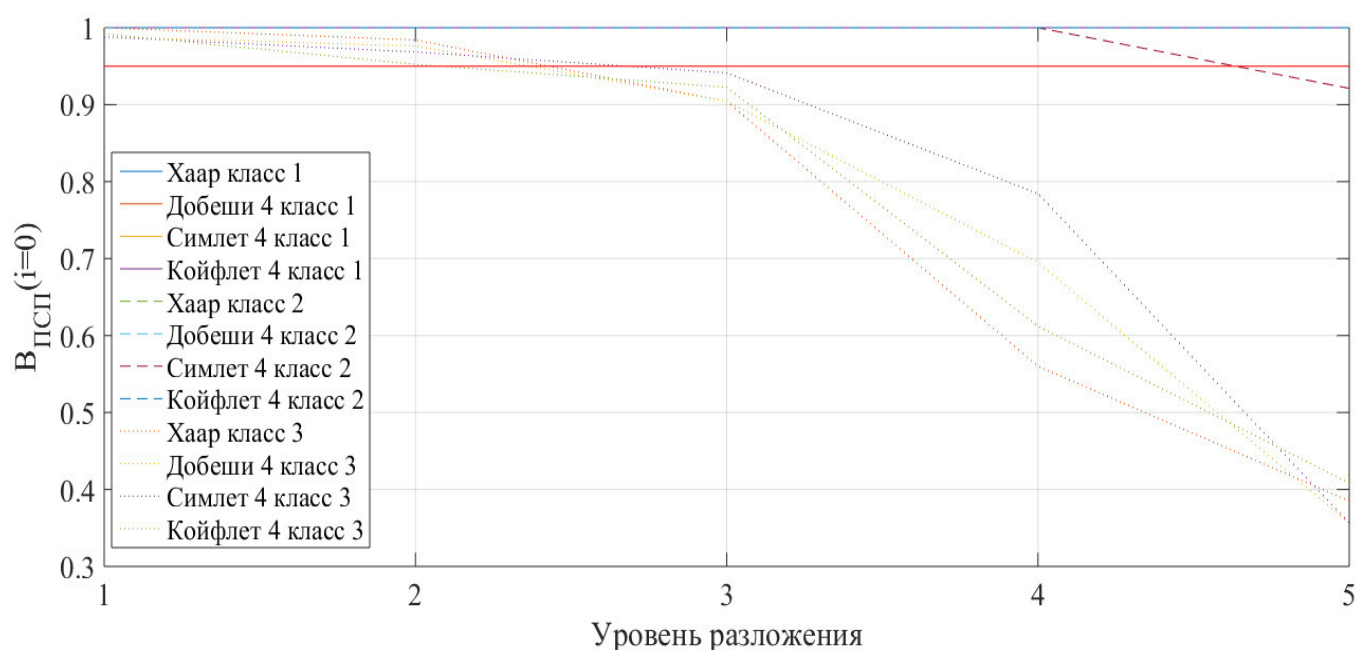


Рисунок 12 – Зависимость $V_{\text{псп}}(i=0)$ от уровня разложения

На полученных графиках можно наблюдать, что заданное пороговое значение корреляции $V_{\text{псп}}(i=0) \geq 0.95$ достигается на всех 5 уровнях разложения для аудио класса 1, на уровнях 1-4 для аудио класса 2 и на уровнях 1-2 для аудио класса 3.

Исходя из вышеизложенного, можно сделать вывод о том, что наиболее

предпочтительными для встраивания являются коэффициенты 1 уровня вейвлет-преобразования, обеспечивающие лучшее качество встраивания и извлечения вне зависимости от типа вейвлета или класса аудио.

2.5 Выбор длины последовательности ФГШ

Длина последовательности ФГШ влияет на максимально допустимый размер ПСП. Чем выше длина фрактальной последовательности, тем меньше значений ПСП можно встроить. Однако недостаточно длинная шумовая последовательность может привести к ошибкам при извлечении. На рисунке 13 представлена зависимость MSE заполненного аудиосигнала от длины последовательности ФГШ при $L=1000$, $J=1$. На рисунке 14 представлена зависимость PSNR от длины последовательности ФГШ. На рисунке 15 представлена зависимость $V_{\text{сп}}(i=0)$ от длины последовательности ФГШ.

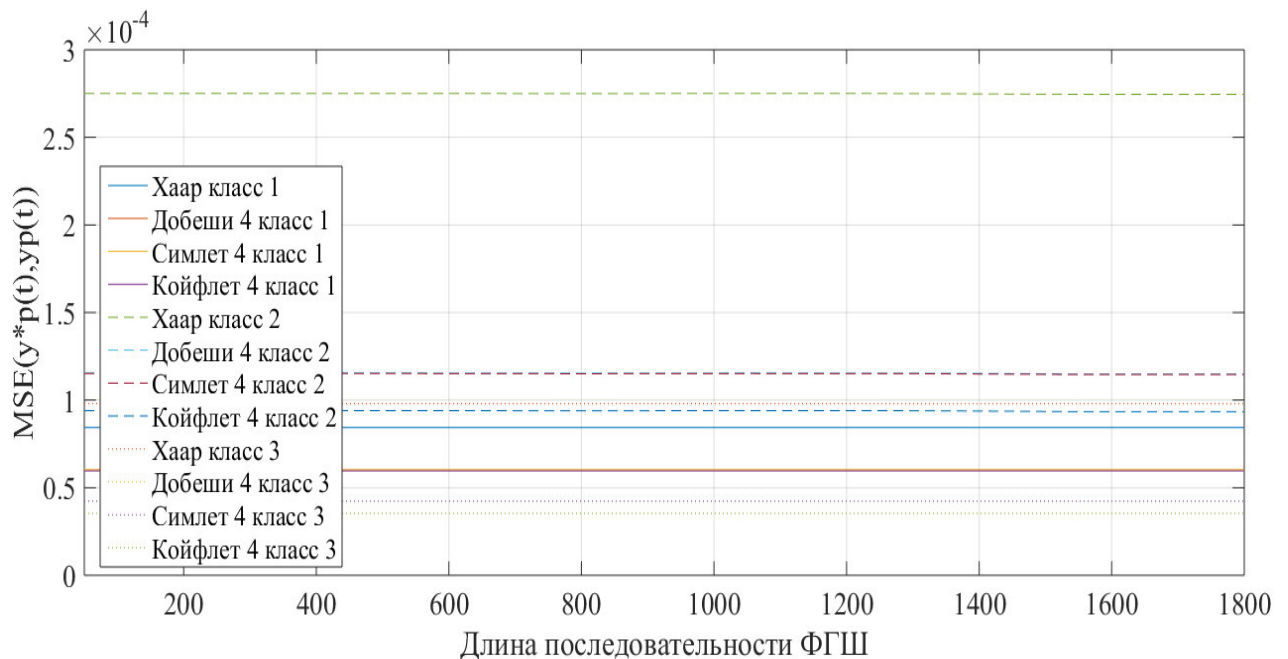


Рисунок 13 – Зависимость MSE маркированного аудиосигнала от длины последовательности ФГШ

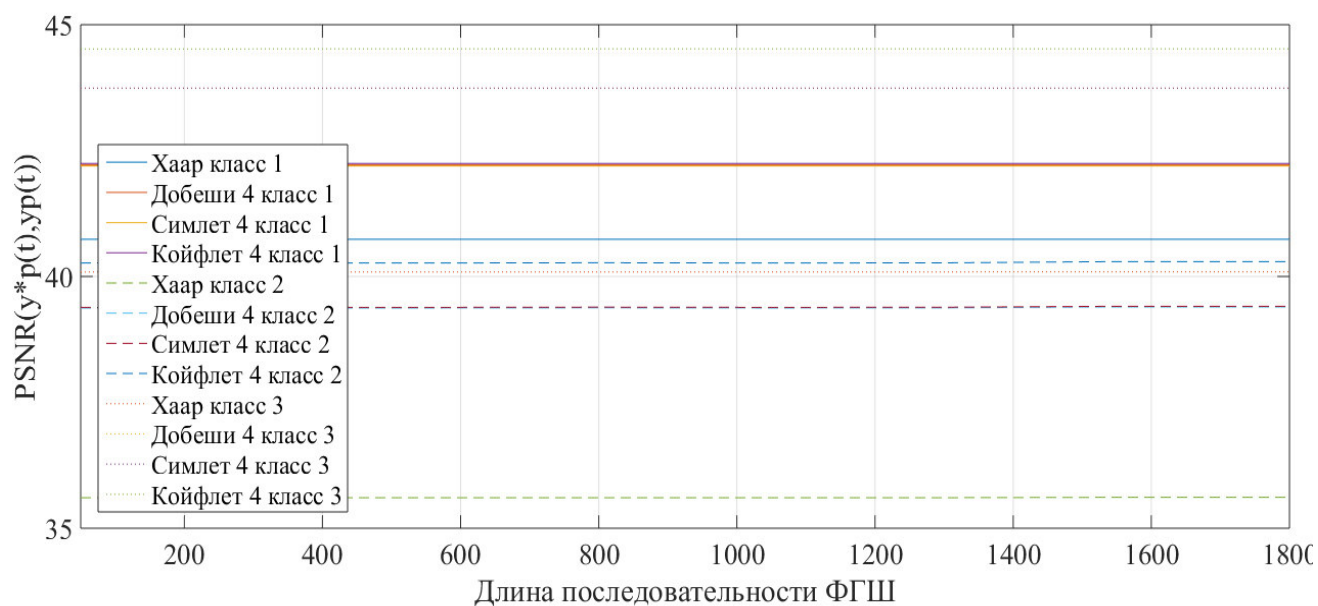


Рисунок 14 – Зависимость PSNR маркированного аудиосигнала от длины последовательности ФГШ

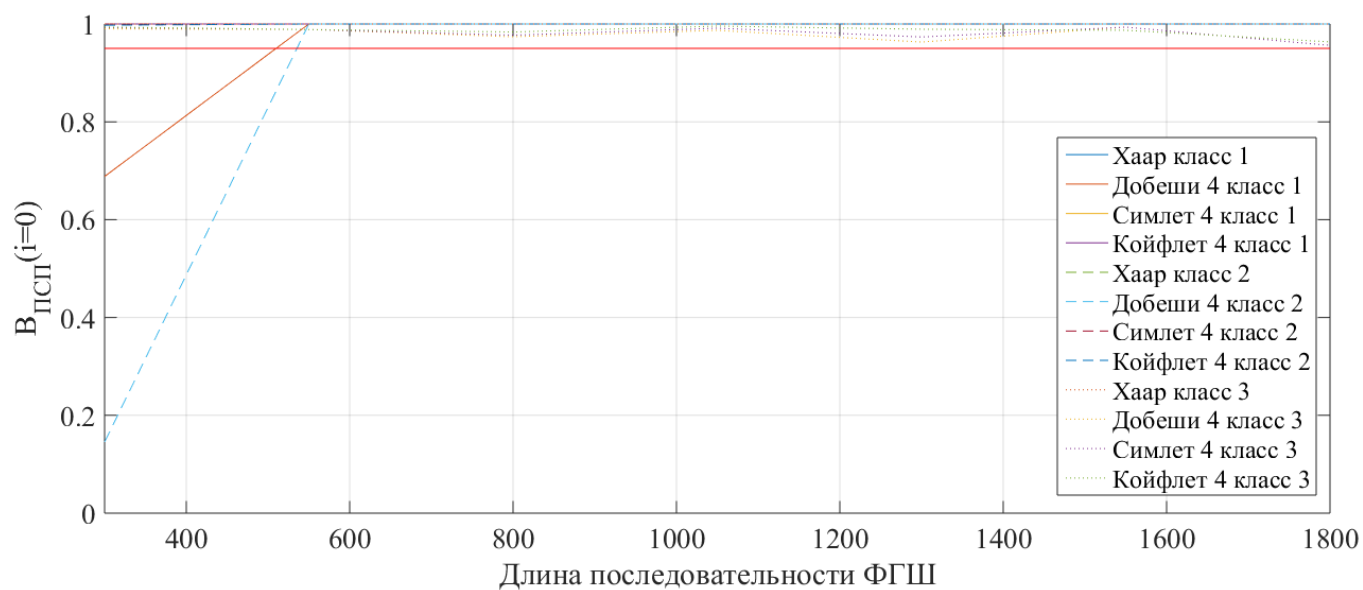


Рисунок 15 – Зависимость $V_{\text{ПСП}}(i=0)$ от длины последовательности ФГШ

Как видно из приведенных зависимостей, заданное качество извлечения достигается при длине последовательности ФГШ ≥ 500 .

2.6 Выбор параметра alpha

Значение масштабирующего коэффициента α выбирается исходя из требо-

ваний незаметности встраивания ЦВЗ в аудиоконтейнер. Правильно подобранная величина α позволяет уменьшить влияние добавляемого ФГШ на качество аудиосигнала и избежать изменений, заметных для слуха человека. При этом следует учитывать, что слишком маленькое значение масштабирующего коэффициента может привести к искажению встроенной шумовой последовательности при вейвлет реконструкции маркированного аудиосигнала, что приводит к недостоверному извлечению ПСП на приемной стороне.

На рисунке 16 представлена зависимость MSE от значения масштабирующего коэффициента α при $L=1000$, $N=1000$, $J=1$.

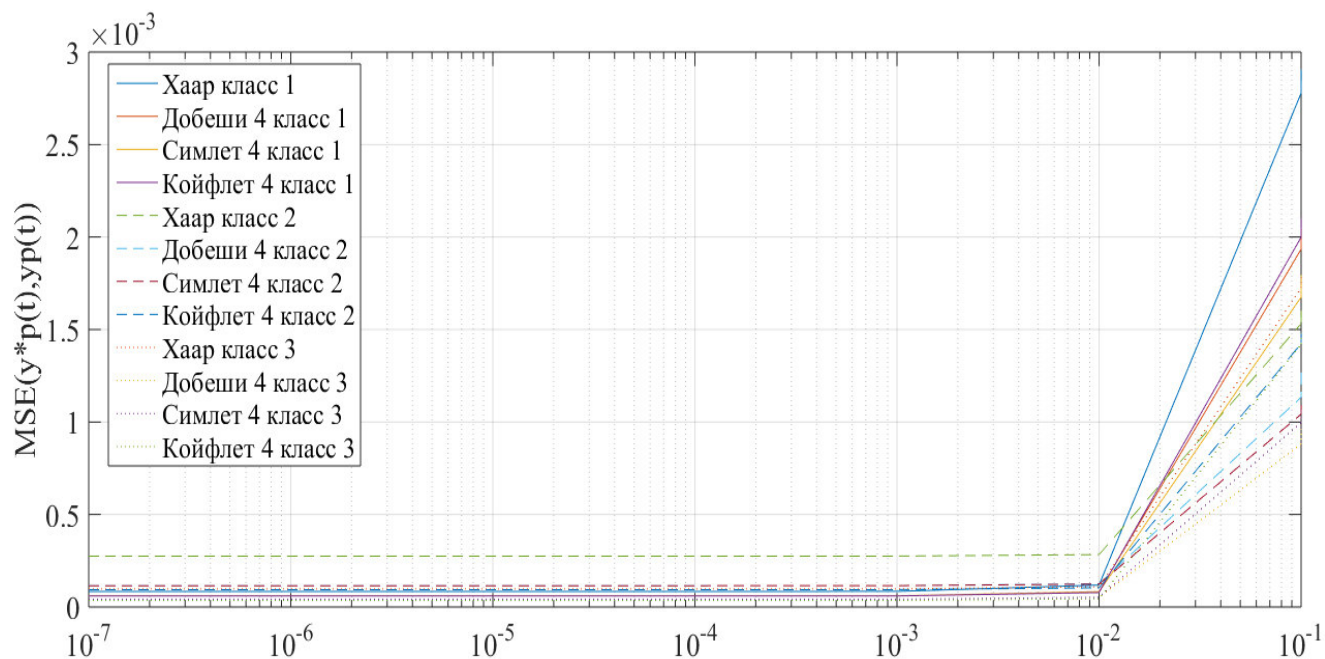


Рисунок 16 – Зависимость MSE маркированного аудиосигнала от значения масштабирующего коэффициента α

На рисунке 17 представлена зависимость PSNR маркированного аудиосигнала от значения масштабирующего коэффициента при аналогичных параметрах алгоритма.

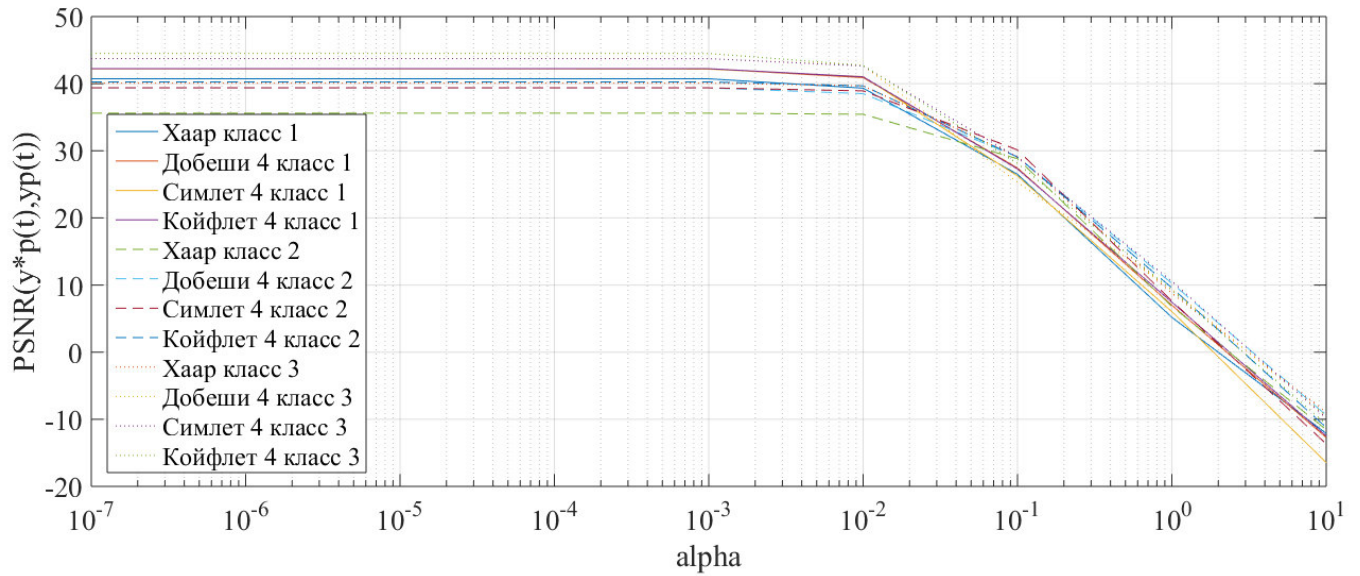


Рисунок 17 – Зависимость PSNR маркированного аудиосигнала от значения масштабирующего коэффициента α

На рисунке 18 представлена зависимость $B_{\text{псп}}(i=0)$ от α .

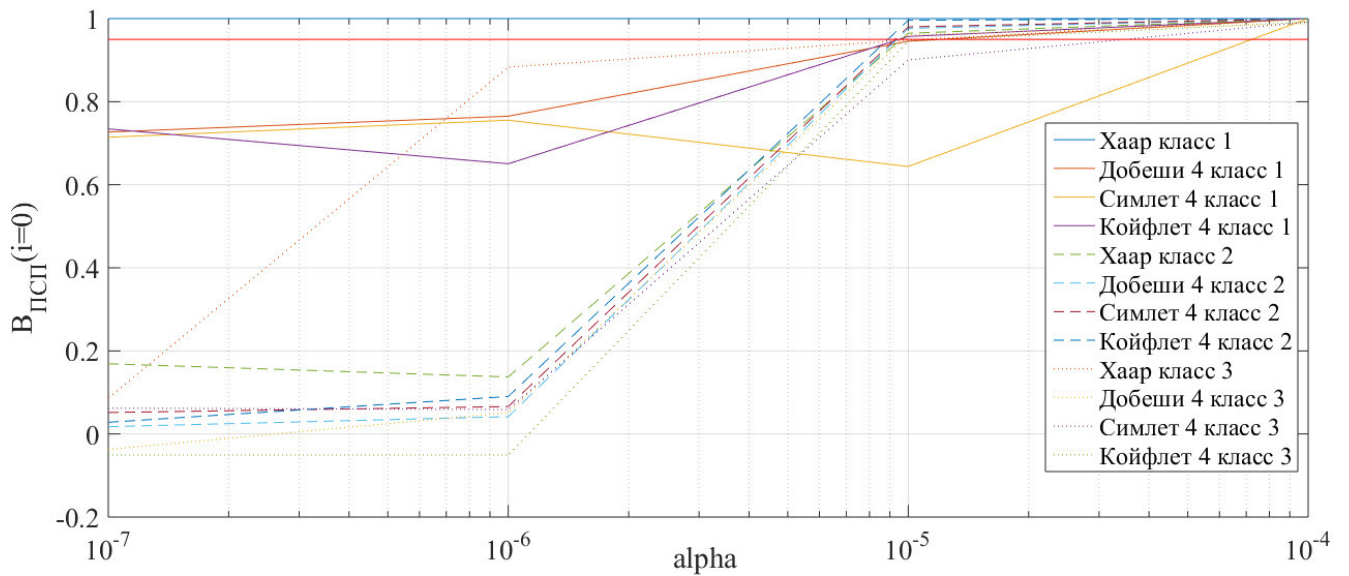


Рисунок 18 – Зависимость $B_{\text{псп}}(i=0)$ от значения масштабирующего коэффициента α

На представленных зависимостях можно наблюдать, что точка $\alpha=10^{-2}$ является пороговой, после которой следует ухудшение значений статистических параметров: MSE увеличивается, PSNR уменьшается. Проведенные слуховые тесты

подтверждают полученные результаты. При значении $\alpha \geq 10^{-2}$ в маркированных аудиосигналах отчетливо слышны артефакты в виде шумов и «потрескиваний». Таким образом, рекомендуется использовать масштабирующий коэффициент $\alpha < 10^{-2}$.

При анализе зависимостей дисперсии можно наблюдать, что достоверное извлечение достигается при $\alpha \geq 10^{-4}$. Таким образом, рекомендуется использовать $\alpha \in [10^{-4}; 10^{-2})$

2.7 Выбор значения показателя Хёрста единичной последовательности H_1

В процессе вейвлет реконструкции маркированного аудиосигнала на передающей стороне и вейвлет разложения на приемной стороне неизбежно возникают искажения в добавленных шумовых последовательностях, что ведёт к погрешностям при оценке показателя Хёрста. Для того чтобы данные погрешности не влияли на достоверность извлечения ПСП, рекомендуется чтобы показатели Хёрста для нулевой и единичной последовательности значительно отличались.

Исходя из изложенного в параграфе 1.3, рекомендовано использовать в качестве нулевой ПСП белый фрактальный гауссовский шум и установить $H_0 = 0.5$. Для выбора значения H_1 проводилось исследование в пределах от 0.55 до 0.95 с шагом 0.05.

На рисунке 19 представлены зависимости MSE маркированного аудиосигнала от значения показателя Хёрста единичной последовательности H_1 при $L=1000$, $N=1000$, $J=1$ и $\alpha=10^{-3}$, а на рисунке 20 показаны зависимости PSNR при аналогичных параметрах алгоритма.

На рисунке 20 представлена зависимость $V_{псп}(i=0)$ от значения показателя Хёрста единичной последовательности H_1 для двух различных видов нулевых последовательностей.

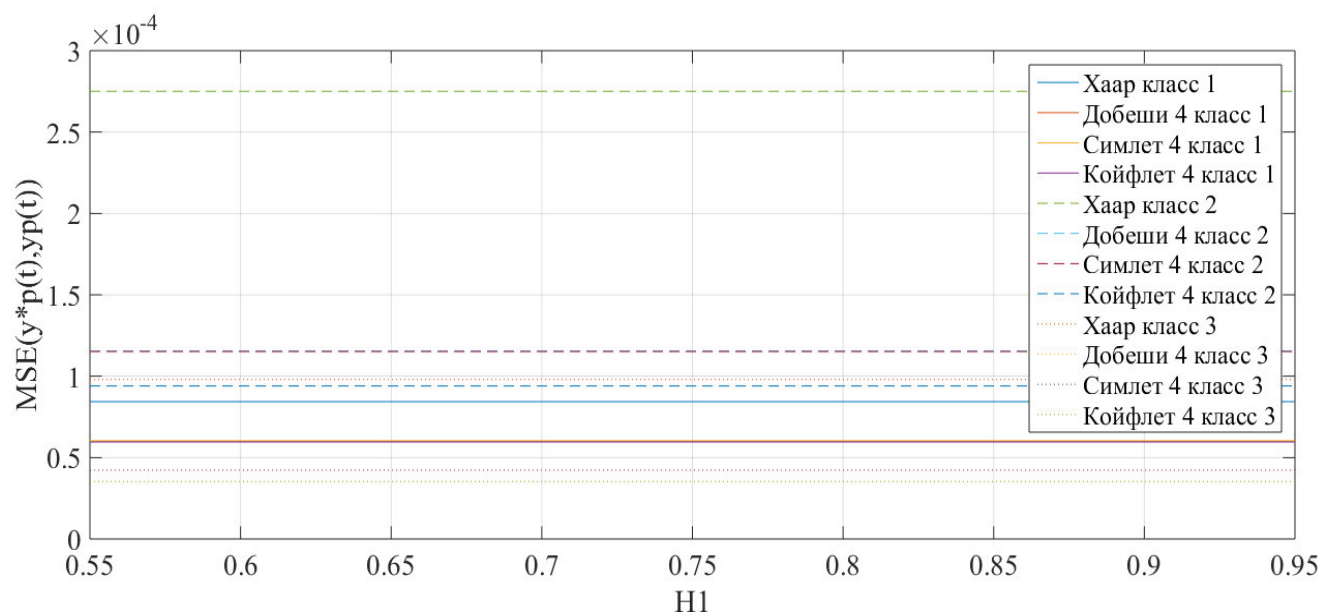


Рисунок 19 – Зависимость MSE маркированного аудиосигнала от значения показателя Хёрста единичной последовательности H_1

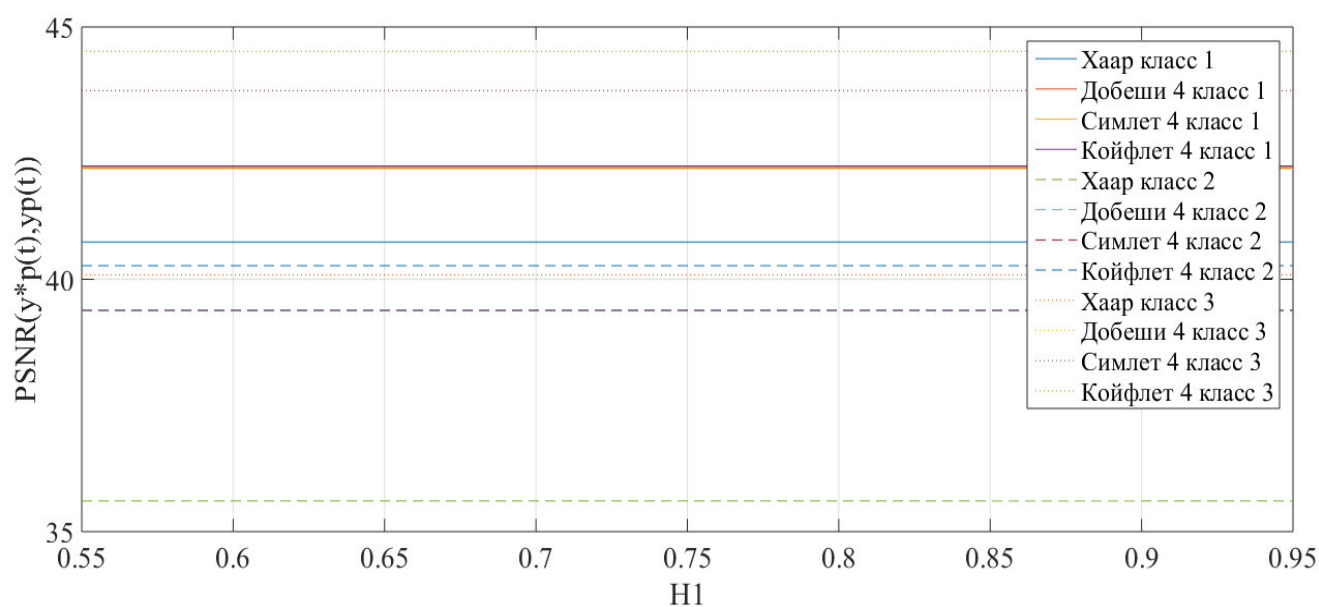
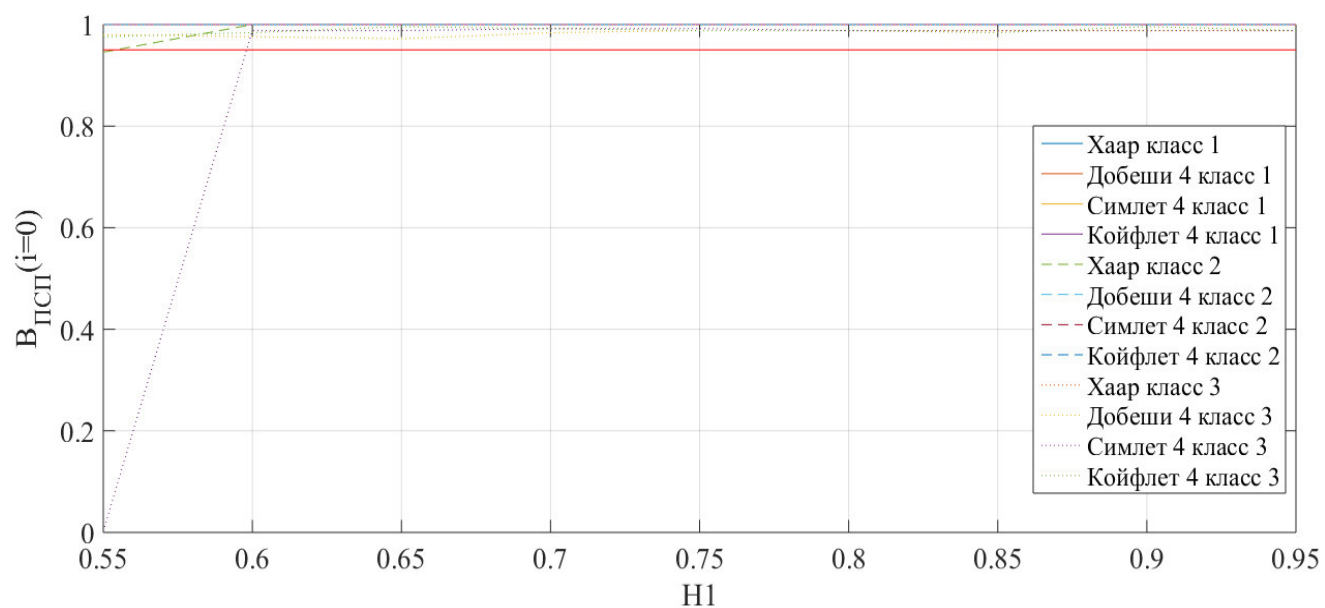
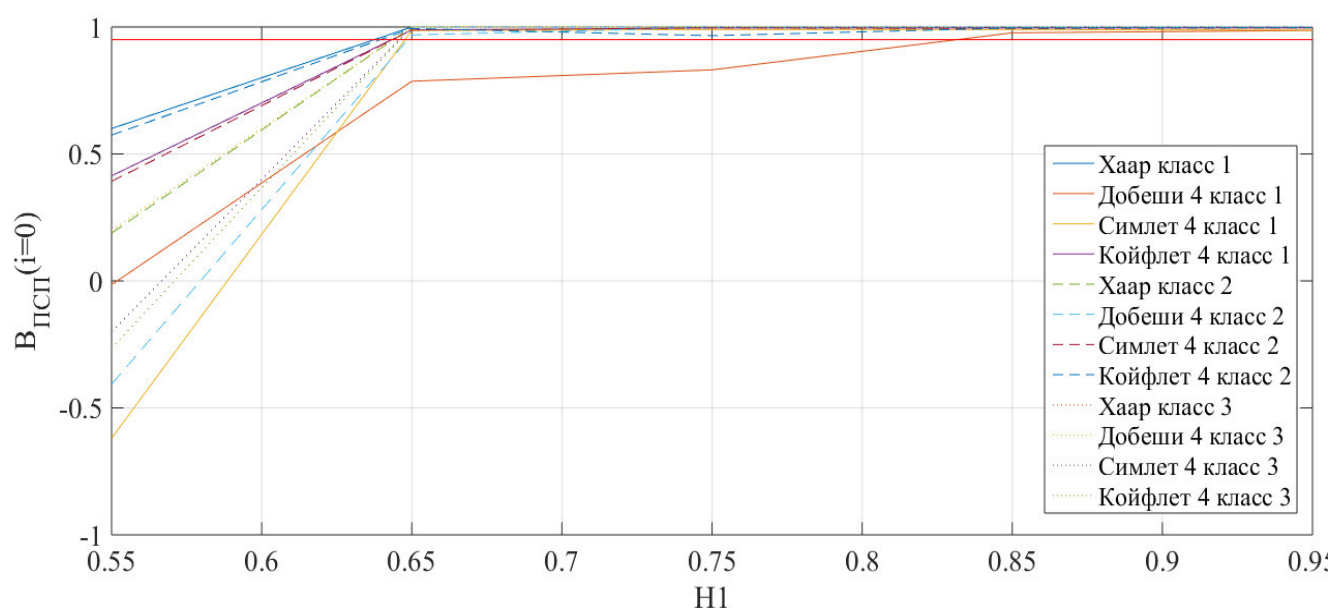


Рисунок 20 – Зависимость PSNR маркированного аудиосигнала от значения показателя Хёрста единичной последовательности H_1 .



а)



б)

Рисунок 21 – Зависимость $V_{\text{ПСП}}(i=0)$ от значения показателя Хёрста единичной последовательности N_1 .

а) при использовании ФГШ в качестве нулевой последовательности;

б) при $N_0 = 0.5$.

Как видно из полученных зависимостей значение N_1 не влияет на качество маркированного аудиосигнала. При извлечении заданное пороговое значение

максимума корреляционной функции достигается при $H_1 \geq 0.6$, если в качестве нулевой последовательности используется белый шум и при $H_1 \geq 0.85$ при $H_0 = 0.5$.

2.8 Выбор порога $H_{\text{пор}}$

При оценке показателя Хёрста на приемной стороне могут возникать погрешности, которые необходимо учитывать при выборе порога $H_{\text{пор}}$.

На рисунке 22 представлены зависимости $V_{\text{псп}}(i=0)$ от значения порога $H_{\text{пор}}$ при $L=1000$, $N=1000$, $J=1$, $\alpha=10^{-3}$, $H_0=0.5$ и $H_1=0.95$.

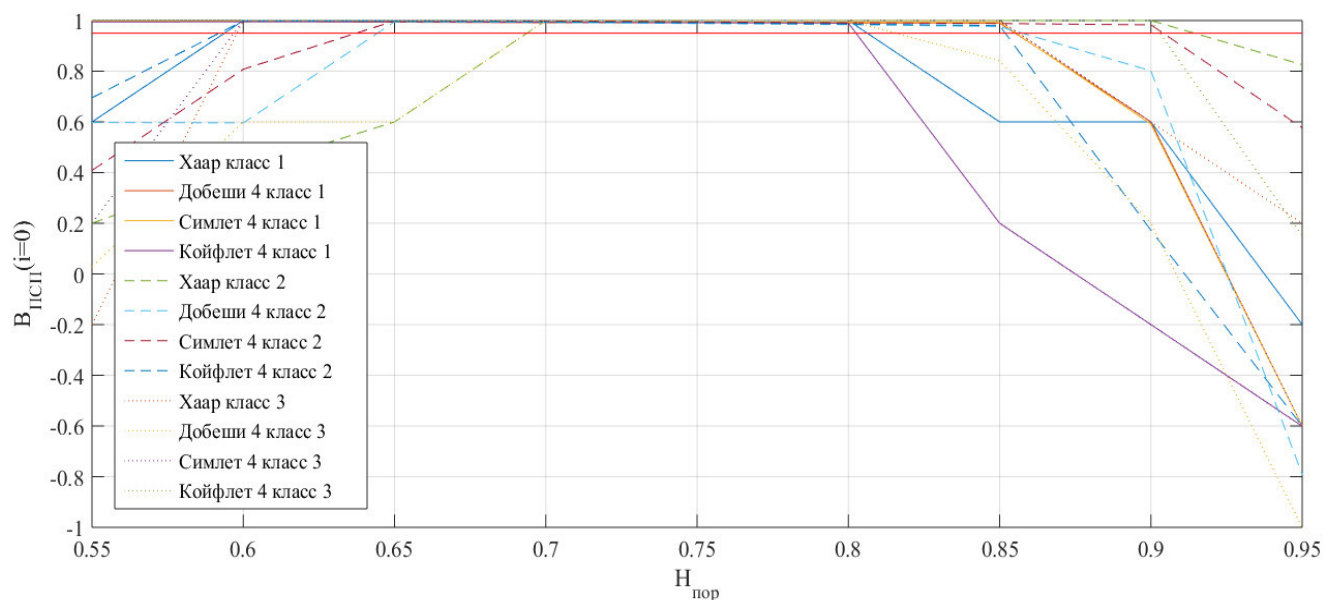


Рисунок 22 – Зависимость $V_{\text{псп}}(i=0)$ от значения порога $H_{\text{пор}}$

Заданное качество извлечения было достигнуто при $H_{\text{пор}} \in [0.7; 0.8]$.

На рисунке 23 показана зависимость $V_{\text{псп}}(i=0)$ от величины SNR зашумленного аудиосигнала при $L=1000$, $N=1000$, $J=1$, $\alpha=10^{-3}$, $H_0=0.5$ и $H_1=0.95$.

Из представленных зависимостей видно, что заданное качество извлечения достигается для аудио класса 1 при $\text{SNR} \geq 35$ при $\text{SNR} \geq 50$ для аудио класса 2 и 3.

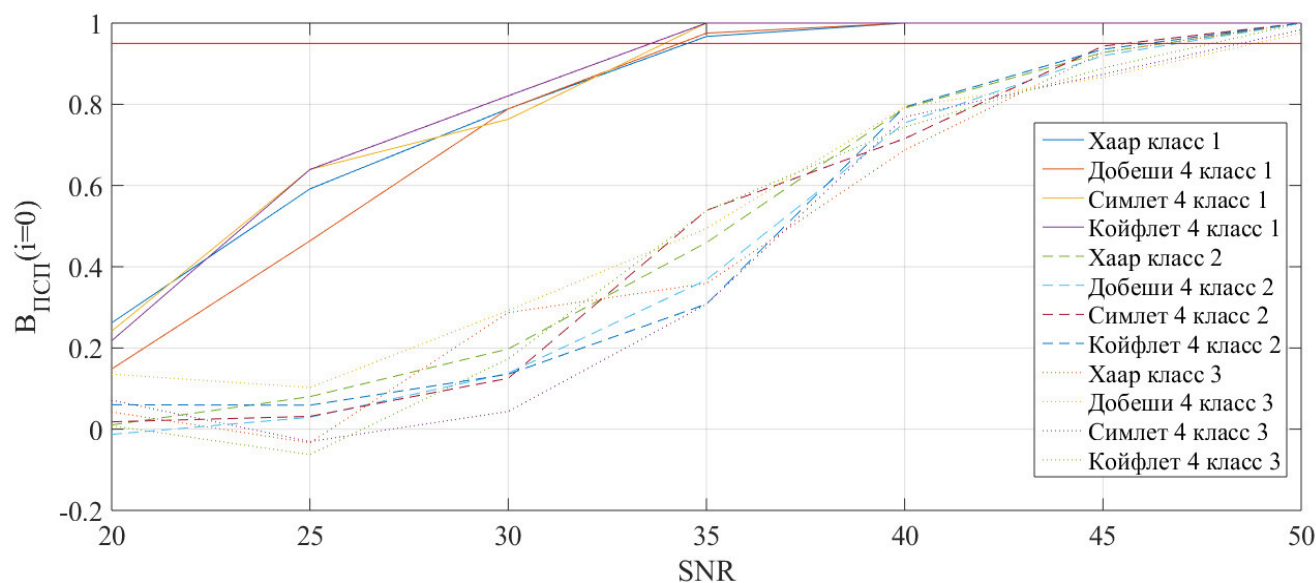


Рисунок 23 – Зависимость $V_{\text{ПСП}}(i=0)$ от SNR зашумленного аудиосигнала

2.9 Сравнительный анализ качества извлечения ПСП алгоритмом A1 с алгоритмом расширения спектра

Разработанный алгоритм A1 является модификацией алгоритма расширения спектра. Встраивание водяного знака в алгоритме расширения спектра осуществляется путем сложения исходных данных с ослабленной последовательностью расширенных данных. Каждый встраиваемый бит представляется в виде ПСП, которая инвертируется или сохраняет свой знак в зависимости от значения встраиваемого бита.

$$y^*(i) = y(i) + \alpha p(i)\omega, \quad (32)$$

где y – оригинальный аудио сигнал, α – масштабирующий коэффициент, p – чип-последовательность ПСП, ω – знак, значение, которого зависит от значения бита ЦВЗ. Распределение водяного знака по всему спектру аудиосигнала обеспечивает большую степень защиты от непреднамеренного или преднамеренного нападения.

На рисунке 24 представлены зависимости MSE от масштабирующего коэффициента α для алгоритма A1 и алгоритма расширения спектра, на рисунке 25 представлены зависимости PSNR.

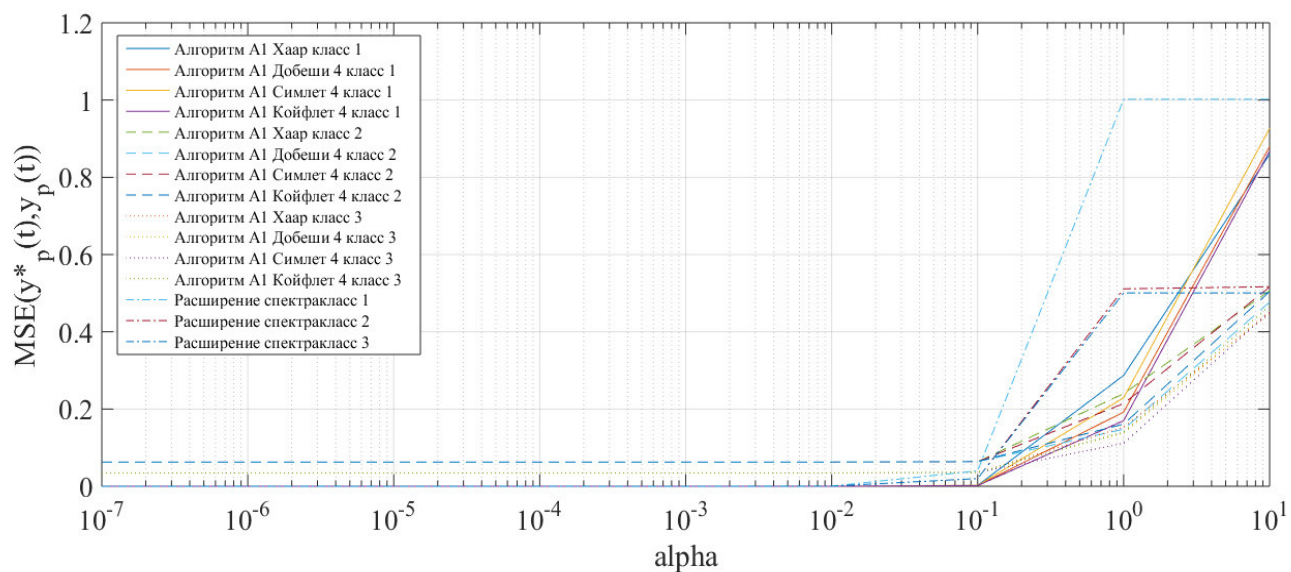


Рисунок 24 – Зависимость MSE от alpha

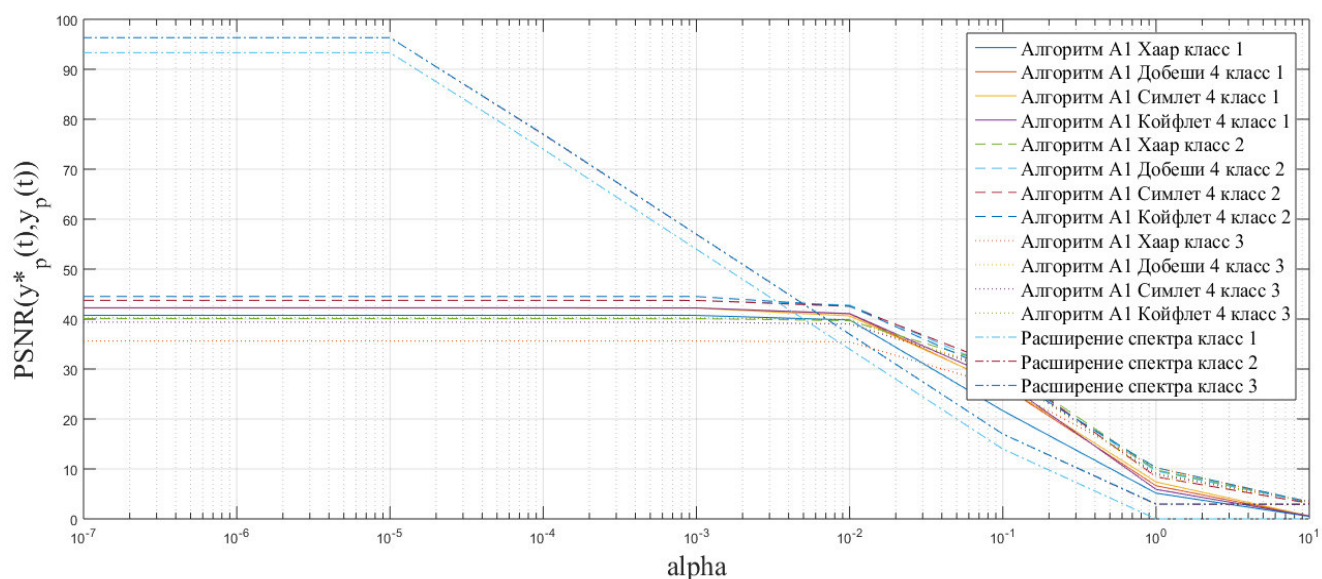


Рисунок 25 – Зависимость PSNR от alpha

Сравнительный анализ показал, что алгоритм расширения спектра позволяет встроить водяной знак большого объема при сохранении высокого качества аудиосигнала. Однако недостатком алгоритма расширения спектра является необходимость наличия оригинального аудио на приемной стороне.

Разработанный алгоритм A1 позволяет устранить указанный недостаток при сохранении основных преимуществ оригинального метода.

2.10 Выводы

1. Разработан новый алгоритм встраивания и извлечения ПСП в аудио файлы с использованием ФГШ и ДВП, отличающийся от известных заменой части коэффициентов детализации вейвлет разложения на элементы фрактального шума.

2. Разработанный алгоритм предоставляет возможность реализации извлечения встроенного ПСП в «слепом» режиме, без использования копии оригинала аудиоконтейнера на приемной стороне в отличие от известного метода расширения спектра.

3. Найдено, что наилучшие результаты скрытия информации в аудиофайлах наблюдаются при встраивании в вейвлет коэффициенты детализации 1-го уровня декомпозиции и использовании вейвлетов типа Койфлет и Симлет.

4. Выявлено, что для достижения высокого качества и достоверности извлечения встраиваемой информации, необходимо использовать значение масштабирующего коэффициента из диапазона $\alpha \in [10^{-4}; 10^{-2}]$.

5. Вероятность ошибки извлечения ПСП на уровне 10^{-3} при $L=1000$ для аудио класса 1 достигается при длине ФГШ ≥ 500 , выборе показателей Хёрста для нулевого бита $H_0=0.5$ и $H_1 \in [0.85; 0.95]$ для единичного бита ПСП. Аналогичная достоверность достигается при использовании коэффициентов 1-го уровня разложения и вейвлетов Хаара.

6. Показано, что в сравнении с известным алгоритмом расширения спектра, при слепом извлечении ПСП достигается заданная достоверность извлечения для аудио 1-го класса при $PSNR \geq 35$ дБ и для аудио 2-го и 3-го классов при $PSNR \geq 50$ дБ.

Глава 3 Фрактальные алгоритмы встраивания ЦВЗ в изображения

Наряду с аудио, неподвижные изображения зачастую являются целью злоумышленников. Недостатки существующих алгоритмов, обозначенные в главе 1, актуальны и для стеганографических алгоритмов с использованием фотоконтейнеров.

Рассмотрим особенности построения и реализации алгоритмов защиты неподвижных фотоизображений от угроз неправомерного использования путем встраивания в изображения водяных знаков с использованием фрактальных процессов и 2D ДВП. В зависимости от специфики задачи и структуры угроз разработано два новых алгоритма.

3.1 Алгоритм А2 защиты неподвижных изображений с использованием двухкомпонентного контейнера и 2D ДВП

В данном разделе предлагается алгоритм А2, который использует двухкомпонентный контейнер в виде фотоконтейнера S и алгебраического фрактала F в качестве секретного ключа. Алгоритм использует алгебраические фракталы для скрытия ЦВЗ в виде двоичной матрицы Q . Секретная информация встраивается во фрактальный ключ (перед встраиванием в контейнер) и используется в качестве параметров генерации алгебраического фрактала. Хотя фрактальные изображения, как вид нелинейных графиков, имеют очень сложный вид, они могут быть легко получены на основе комбинации нелинейной модели динамической системы и компьютерной графики. Злоумышленникам, осуществляющим попытки неправомерного доступа к изображению-контейнеру, требуется теоретически бесконечное число итераций для получения желаемого аттрактора в силу случайного характера параметров алгебраического фрактала.

Внедрение секретной информации производится одновременно с генерацией фрактальных изображений, в которых сами секретные данные используются в качестве параметров, необходимых для генерации фрактальных изображений.

Фрактальные изображения формируются по заданным параметрам, и требуется огромное количество итераций для получения желаемого аттрактора. Несанкционированные пользователи не заметят «секретное» исходное изображение за фрактальным изображением. Однако даже если злоумышленникам станет известно, что в изображении есть скрытая информация, им будет практически невозможно получить доступ к ней из-за случайных параметров алгебраического фрактала [87, 88].

3.1.1 Алгоритм встраивания ЦВЗ

Алгоритм А2 встраивания ЦВЗ состоит из 7-и последовательных шагов:

1. Перевод двоичной матрицы ЦВЗ $Q(Q_w, Q_h)$ размером $Q_w * Q_h$ в вектор $Q(Q_l)$ размером $Q_l = Q_w * Q_h$.
2. Генерация фрактального контейнера $F_{j,m,n}(x,y)$ с помощью алгоритма А21.
3. Вычисление матрицы яркости $Y(x,y)$ из оригинального контейнера $S(x,y)$ путем перехода из пространства RGB в YCbCr:

$$\begin{aligned} Y(x,y) &= 0.299 * R(x,y) + 0.587 * G(x,y) + 0.114 * B(x,y); \\ C_B(x,y) &= -0.1687 * R(x,y) - 0.3313 * G(x,y) + 0.5 * B(x,y); \\ C_R(x,y) &= 0.5 * R(x,y) - 0.4187 * G(x,y) - 0.0813 * B(x,y). \end{aligned} \quad (33)$$

4. 2DDВП матрицы яркости, вычисление коэффициентов вейвлет-разложения $W_\varphi(j_0, m, n)$ и $W_\psi^i(j, m, n) (i = H, V, D)$.

Для 2DDВП матрицы яркости вычисление коэффициентов вейвлет-разложения $W_\varphi(j_0, m, n)$ и $W_\psi^i(j, m, n) (i = H, V, D)$.

$$\begin{aligned}
W_\varphi(j_0, m, n) &= \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} Y(x, y) \varphi_{j_0, m, n}(x, y), \\
W_\psi^i(j, m, n) &= \frac{1}{\sqrt{M_j N_j}} \sum_{x=0}^{M_j} \sum_{y=0}^{N_j} Y(x, y) \psi_{j, m, n}^i(x, y), \quad i = H, V, D.
\end{aligned} \tag{34}$$

5. Замена диагональных коэффициентов $W_\psi^D(j, m, n)$ контейнера $S(x, y)$ значениями $F_{j, m, n}(x, y)$ с масштабирующим коэффициентом α :

$$W_\psi^{i=D}(j=2, m_2, n_2) = \frac{1}{M_2 N_2} \alpha \sum_{x=0}^{M_2} \sum_{y=0}^{N_2} F_{j, m_2, n_2}(x, y) \psi_{j, m_2, n_2}^D(x, y). \tag{35}$$

6. Вычисление матрицы яркости $Y^*(x, y)$ путем обратного 2D ДВП с использованием $F_{j, m, n}(x, y)$:

$$\begin{aligned}
Y^*(x, y) &= \frac{1}{\sqrt{MN}} \sum_m \sum_n W_\varphi(j_0, m, n) \varphi_{j_0, m, n} + \sum_{i=H, V, D} \sum_{j_0} \left[\sum_{m_1} \sum_{n_1} W_\psi^i(j=1, m_1, n_1) \psi_{j=1, m_1, n_1}^i(x, y) + \right. \\
&\quad \left. + \sum_{m_2} \sum_{n_2} W_\psi^i(j=2, m_2, n_2) \psi_{j=2, m_2, n_2}^i(x, y) + \sum_{m_3} \sum_{n_3} W_\psi^i(j=3, m_3, n_3) \psi_{j=3, m_3, n_3}^i(x, y) \right].
\end{aligned} \tag{36}$$

7. Получение стегоконтейнера $S^*(x, y)$ путем вычисления цветовых компонент на основе измененной матрицы яркости $Y^*(x, y)$.

3.1.1.1 Алгоритм A21 генерации фрактального контейнера

Генерация фрактального контейнера осуществляется на основе алгоритма времени убегания [89, 90], который использует комплексные отображения, где комплексное число $Z_{n+1} = x_{n+1} + iy_{n+1}$ ставится в соответствие другому числу $Z_n = x_n + iy_n$ по итерационному правилу $Z_{n+1} = f(Z_n)$, где $f(Z)$ – некоторая нелинейная функция аргумента Z , а n – номер итерации.

Алгоритм использует квадратичный комплексный полином $f(Z) = Z^2 + C$, где $C = p + iq$ начальная точка на комплексной плоскости, на основе которой строится множество Жюлиа.

Алгоритм построения множества Жюлиа состоит из следующих 5 шагов:

1. Выбираем точку c для задания полинома $f(Z) = Z^2 + C$;

2. Вычисляем радиус R для заданного полинома $f(Z) = Z^2 + C$;
3. Выбираем порог времени убегания T , определяющий значение максимальной итерации. Чем он выше, тем выше точность и тем медленнее алгоритм;
4. Генерируем массив цветов от менее яркого к более яркому. Будем обозначать цветом зависимость удаления точки от множества Жюлиа;
5. Для каждой точки вычисляем, является ли она частью заполненного множества Жюлиа или нет, а также номер итерации, на которой порог был превышен. Если $|Z| > R$, то используем первый цвет, далее используем тот цвет палитры, на каком номере итерации был превышен порог.

Реализация алгоритма начинается с построения прямоугольника $|x|$, в пределах которого будет построено множество Жюлиа. С помощью изменения его параметров можно “приблизить” интересующие сосредоточения множества с высокой точностью. Полученный прямоугольник делится на части с координатами $z_{i,j}$ в зависимости от числа пикселей изображения.

Каждая точка $z_{i,j}$ входит в итерационный цикл $f(Z) = Z^2 + C$. Количество итераций зависит от параметра T . Если после заданного количества итераций точка не уйдёт в бесконечность, то такая точка принадлежит множеству Жюлиа.

В зависимости от того, какая область множества Жюлиа будет сгенерирована ($|x|$), определённое количество точек уйдёт в бесконечность, не дойдя до максимальной итерации.

Для оптимизации алгоритма и весомого сокращения времени генерации множества Жюлиа был принят следующий подход: для комплексного числа C считается радиус $R = \frac{1}{2} + \frac{\sqrt{1+4|C|}}{2}$ и на каждой итерации происходит проверка $z_{i,j} > R$, для точек, удовлетворяющих данному условию, итерации больше не производятся.

Точки $z_{i,j}$ выходящие за этот радиус уйдут в бесконечность через определённое количество итераций, так как их аттрактором является бесконечно удалён-

ная точка (точки $z_{i,j} > R$ входят в бассейн аттрактора $A(\infty)$). Бассейном аттрактора точки Z функции f называется такое подмножество точек $A(Z)$ из окрестности Z , при котором любая траектория, начинающаяся в одной из этих точек, сходится к точке Z .

Процесс построения промежуточного фрактального контейнера основан на технологии «времени убегания», имеет особенности, связанные с вычислением матрицы ЦВЗ $Q(Q_w, Q_h)$. В общем виде алгоритм A21 формирования промежуточного фрактального контейнера $F(F_w, F_h)$ состоит из следующих трех шагов.

1. Пусть F_w, F_h – размеры фрактального изображения, $s=r+qi$ – начальная точка на комплексной плоскости. Тогда установим:

$$\Delta Fx = 2 * l / (F_w - 1); \quad (37)$$

$$\Delta Fy = 2 * l / (F_h - 1). \quad (38)$$

2. Для всех точек (n_x, n_y) , где $n_x = 1, 2, \dots, F_w$, $n_y = 1, 2, \dots, F_h$ выполняются следующие шаги:

2.1. Задаются стартовые значения:

$$\begin{aligned} Fx_0 &= -1 * l + n_x * \Delta Fx; \\ Fy_0 &= l + n_y * \Delta Fy; \\ t &= 0. \end{aligned} \quad (39)$$

2.2. Вычисляются переменные Fx_{t+1}, Fy_{t+1} на каждой итерации:

$$\begin{aligned} Fx_{t+1} &= Fx_t^2 - Fy_t^2 + p; \\ Fy_{t+1} &= 2Fx_t Fy_t + q; \\ t &= t + 1. \end{aligned} \quad (40)$$

2.3. Вычисляется значение r :

$$r = Fx_t^2 + Fy_t^2. \quad (41)$$

3. Осуществляется проверка соотношений $r \leq R$ или $r > R$.

3.1. Если $r \leq R$ и $t = T$, то считывается текущий бит ЦВЗ. Если он равен «0», то пиксель фрактального ключа F с координатами (n_x, n_y) окрашивается в цвет фрактала $F(n_x, n_y) = 1$. Если бит равен «1», то пиксель окрашивается в цвет не фрактальной области $F(n_x, n_y) = 0$. Возврат к шагу 2.1.

3.2. Если $r > R$, то пиксель с координатами (n_x, n_y) окрашивается в цвет не фрактальной

На основе разработанного алгоритма были сгенерированы фракталы 6 типов, которые представлены на рисунке 27.

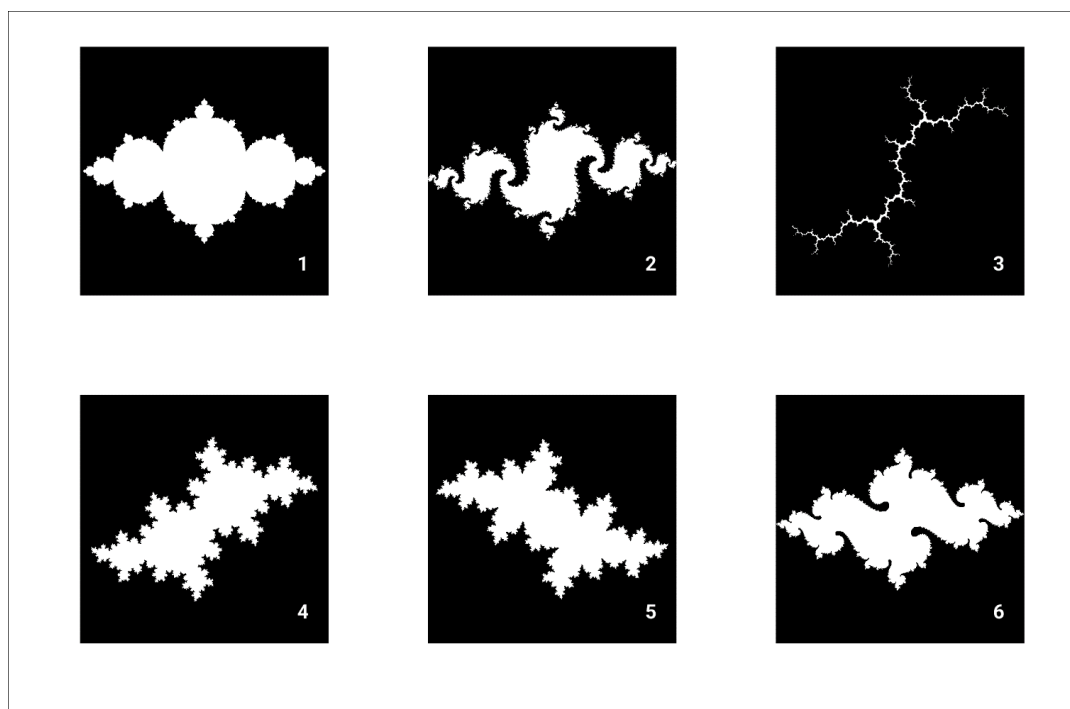


Рисунок 27 – Различные типы алгебраических фракталов в зависимости от значений начальных параметров

В таблице 1 приведены параметры p и q сгенерированных фракталов и определены их типы. Для всех типов фракталов заданы параметры $l=1.5$ и $T=30$. Исключением является фрактал 3 дендрит, который генерируется при $T=15$, поскольку при больших значениях T он распадается на несвязные точки.

Таблица 1 – Параметры p и q сгенерированных фракталов

№	Тип фрактала	p	q
1	Множество Жюлиа с одним аттрактором	-0.7	0
2	Множество Жюлиа с аттрактором периода 2	- 0.83	0.16
3	Дендрит	0	1
4	Диск Зигеля	-0.39054	0.58678
5	Множество Жюлиа с аттрактором периода 5 (параболический бассейн)	-0.481762	-0.531657
6	Множество Жюлиа из долины морских коньков	-0.7454	0.113

3.1.1.2 Оценка емкости фрактального контейнера

Общее количество пикселей фрактального контейнера, которое может быть использовано для встраивания ЦВЗ, вычисляется по следующему алгоритму.

1. Для всех точек (n_x, n_y) , где $n_x = 1, 2, \dots, F_w$, $n_y = 1, 2, \dots, F_h$ выполняются шаги 2.1-2.3 Т раз.

2. Если $r \leq R$, то считаем, что точка $F(n_x, n_y)$ относится к фрактальному множеству и эта точка доступна для встраивания ЦВЗ.

На рисунке 28 представлена зависимость максимального объема встраивания Quan фрактального контейнера в пикселях от значения Т при разных начальных точках С для фрактального изображения с параметрами $F_w=1000$, $F_h=1000$ и $l=1.5$.

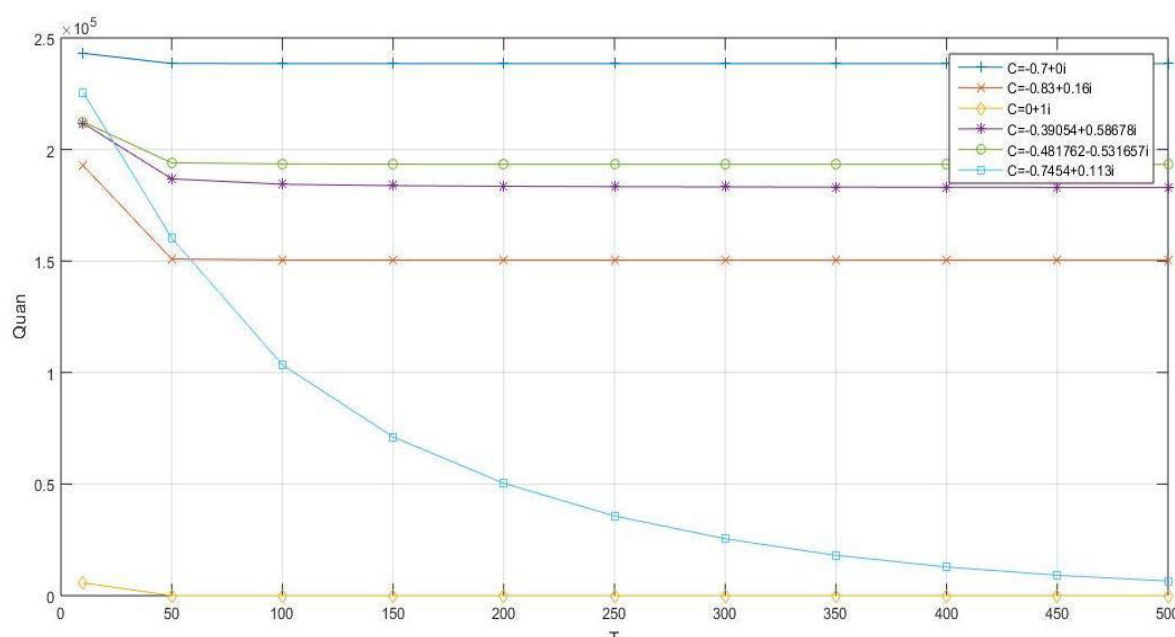


Рисунок 28 – Изменение максимального количества пикселей, доступных для встраивания ЦВЗ при изменении значения порога времени убегания Т и различных значениях начальной точки С при $l=1,5$

Как видно из графиков, при увеличении порога Т происходит уменьшение количества возможных точек для встраивания. При этом заметно, что для четырех видов фракталов, а именно множества Жюлиа с одним аттрактором, множества

Жюлиа с аттрактором периода 2, множества Жюлиа с аттрактором периода 5 и диска Зигеля при $T > 50$ значение $Quan$ изменяется незначительно или не изменяется совсем.

Множество Жюлиа с одним аттрактором имеет максимальную емкость при всех значениях порога времени убегания.

Дендрит позволяет встроить наименьшее количество данных, поскольку рассыпается при $T > 20$.

Для Жюлиа из долины морских коньков емкость встраивания заметно уменьшается при увеличении значения T . При $T < 30$ полученные множества не обладают фрактальными свойствами, поэтому рекомендуется использовать значение $T = 30$ для получения максимальной емкости встраивания.

На рисунке 29 показана зависимость максимального объема встраивания $Quan$ при изменении значения параметра l для различных начальных точек C для фрактала с параметрами $F_w = 1000$, $F_h = 1000$, $T = 30$.

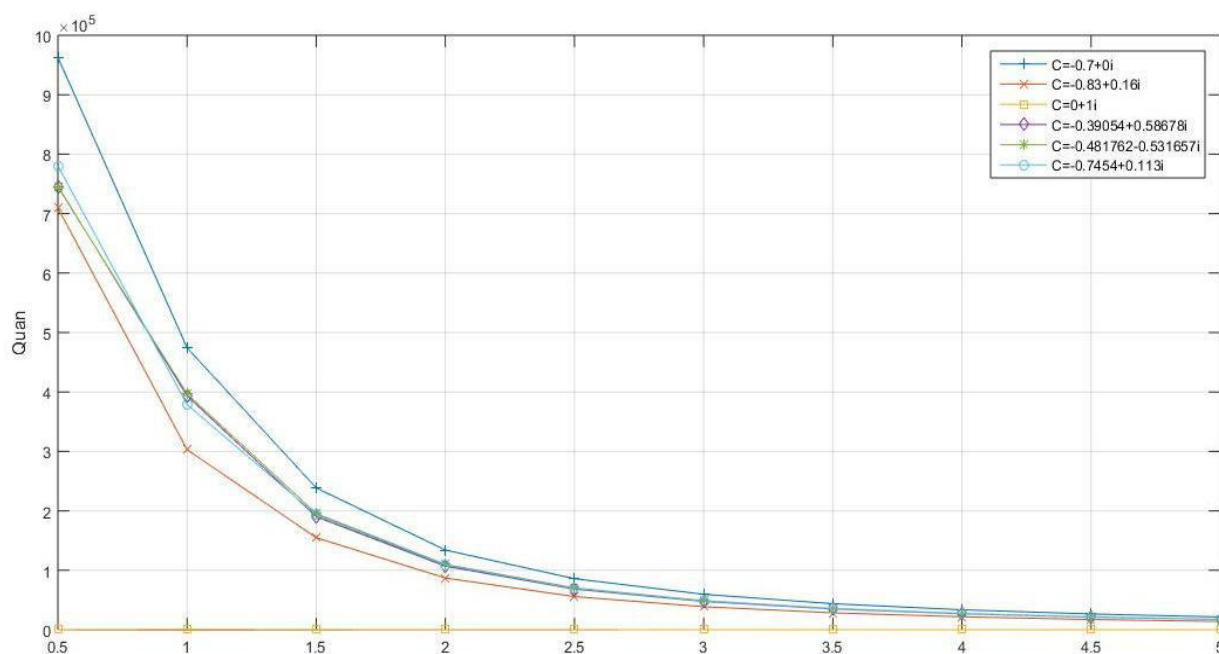


Рисунок 29 – Изменение максимального количества пикселей, доступного для встраивания ЦВЗ при различных значениях начальной точки C при $T = 30$ и изменении параметра l

При анализе полученных зависимостей можно наблюдать, что увеличение параметра l приводит к уменьшению максимального объема встраивания. Однако при значениях $l=0.5$ и $l=1$ сгенерированные множества не обладают фрактальными свойствами. Поэтому рекомендуется использовать значение $l=1.5$, которое позволит встроить ЦВЗ наибольшего размера.

В таблице 2 представлены значения максимального объема встраивания в пикселях и максимально возможные размеры ЦВЗ Q_w , Q_h для 6 типов фракталов с параметрами из таблицы 1 при размерах фрактального контейнера $F_w = 1000$, $F_h = 1000$ и рекомендуемых параметрах $l=1.5$ и $T=30$ для 5 типов фракталов и $T=15$ для дендрита, поскольку он рассыпается на несвязные точки при больших значениях T .

Таблица 2 – Максимальный объем встраивания для разных типов фракталов

Тип фрактала	Максимальный объем встраивания Q_{an}	Максимально возможные размеры ЦВЗ $Q_w \times Q_h$
1	238560	488x488
2	154786	393x393
3	444	21x21
4	190234	436x436
5	195406	442x442
6	193282	439x439

Наибольший объем встраивания можно достичь при использовании множества Жюлиа с одним аттрактором, наименьший – при использовании дендрита. Диск Зигеля, множество Жюлиа с аттрактором периода 5 и множество Жюлиа из долины морских коньков позволяют встроить ЦВЗ примерно одинакового размера, в то время как множество Жюлиа с аттрактором периода 2 имеет меньший размер среди рассмотренных множеств.

3.1.1.3 Результаты встраивания ЦВЗ во фрактальный ключ

Дальнейшие исследования проводились для 5 типов фракталов за исключением дендритов, показавших неудовлетворительные результаты при оценке емкости. Для всех рассматриваемых фракталов были выбраны рекомендуемые параметры $T=30$ и $l=1.5$. Для демонстрации результатов работы алгоритма был выбран фрактал с наибольшей емкостью – множество Жюлиа с одним аттрактором.

На рисунке 30 представлены оригинальный незаполненный фрактал размером $F_w = 1000$, $F_h = 1000$, а также ЦВЗ в виде QR кода размером $Q_w=488$, $Q_h=488$, а на рисунке 31 показаны примеры заполненных фрактальных контейнеров при разной степени заполнения.

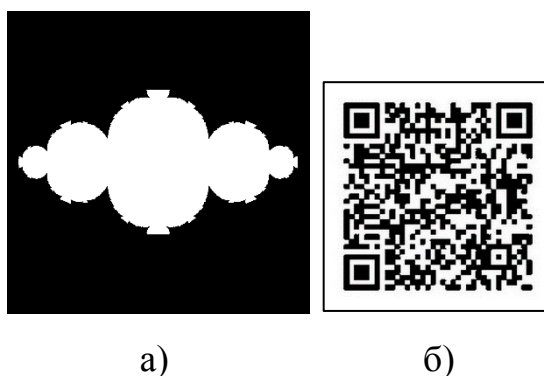


Рисунок 30 – а) оригинальный фрактал без заполнения размером 1000x1000 пикселей; б) ЦВЗ в виде QR-кода размером 439x439 пикселей

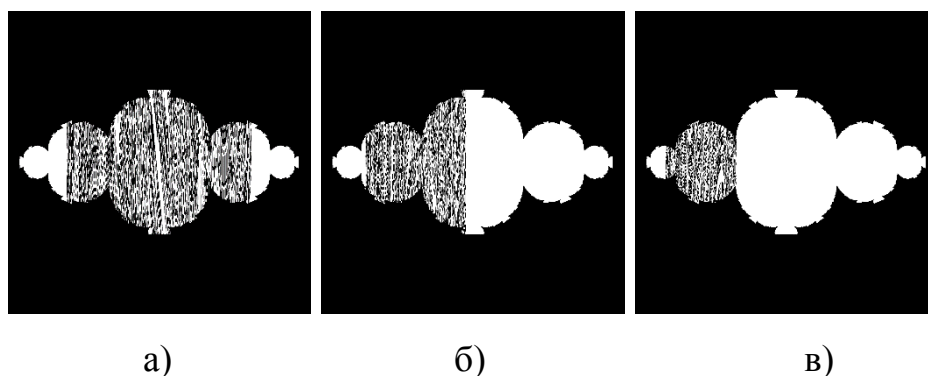


Рисунок 31 – Фрактальный контейнер при разном уровне заполнения

а) 100% б) 50% в) 25%

На рисунке 32 показана степень искажения при добавлении ЦВЗ путем ге-

нерировании фрактала. На графике приведена зависимость нормированной среднеквадратичной ошибки NMSE при сравнении фрактала без ЦВЗ и фрактального контейнера при разном объеме заполнения $Pr = \frac{Q_w * Q_h}{F_w * F_h}$.

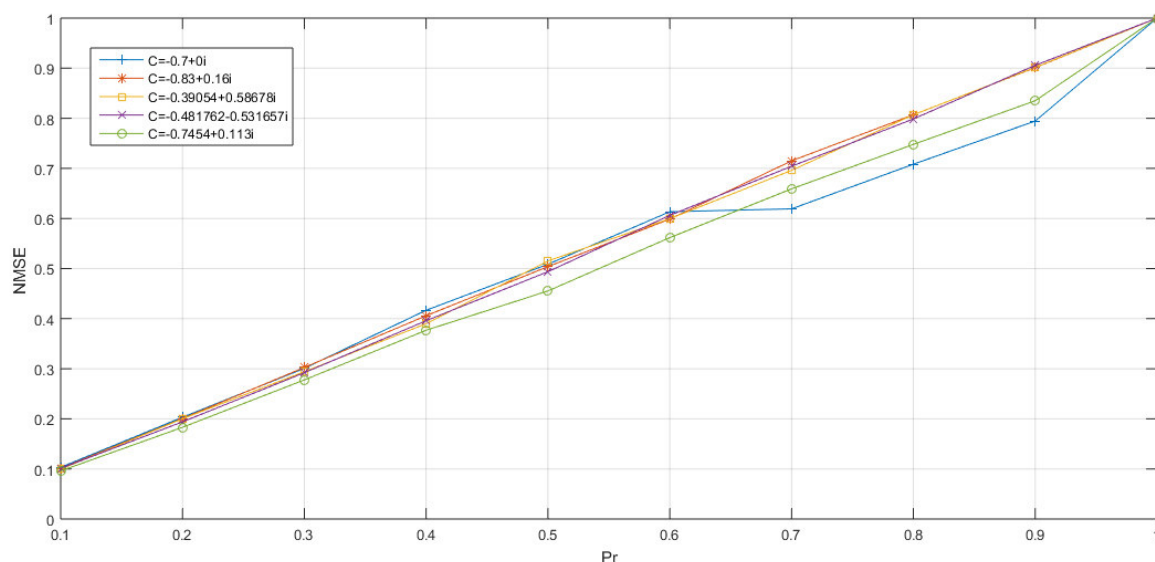


Рисунок 32 – Зависимость нормированной MSE при сравнении фрактала без ЦВЗ и фрактального контейнера с разной степенью заполнения

Очевидно, что увеличение процента заполняемости контейнера влечет за собой увеличение ошибки. Для 3-х типов фрактала: множество Жюлиа с аттрактором периода 2, множество Жюлиа с аттрактором 5 и диск Зигеля, значение NMSE может быть оценено соотношением:

$$NMSE = Pr. \quad (42)$$

Для множества Жюлиа с одним аттрактором соотношение (42) справедливо при объеме заполнения $\leq 60\%$. При больших объемах заполнения значение ошибки уменьшается. Зависимость нормированной среднеквадратичной ошибки от объема заполнения для данного типа фрактала может быть описано соотношением:

$$NMSE = \begin{cases} Pr, & \text{если } Pr \leq 0.6 \text{ и } Pr = 1 \\ 0.88 * Pr, & \text{если } 0.6 < Pr < 1 \end{cases}. \quad (43)$$

Множество Жюлиа из долины морских коньков искажается меньше остальных типов фракталов при любых значениях параметра Pr . Значение нормированной среднеквадратичной ошибки может быть вычислено по формуле:

$$NMSE \approx 0.93 * Pr. \quad (44)$$

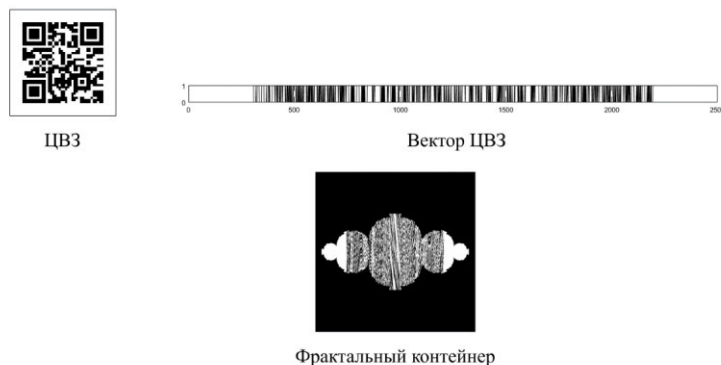
Исходя из полученных зависимостей, можно сделать вывод, что для сохранения низкого уровня ошибок при любом объеме заполнения фрактального контейнера рекомендуется использовать множество Жюлиа из долины морских коньков. В случае необходимости заполнения большого объема фрактального контейнера ($Pr > 0.6$), рекомендуется использовать множество Жюлиа с одним аттрактором.

3.1.1.4 Результаты встраивания фрактального ключа в контейнер

После генерации фрактального ключа (первичного контейнера) на шаге 3 алгоритма A2 выполняется процедура встраивания фрактального контейнера $F(F_w, F_h)$ в оригинальное изображение $S(S_w, S_h)$ путем замены матрицы коэффициентов ДВП фрактальным контейнером.

На рисунке 33 представлен поэтапный алгоритм встраивания ЦВЗ в двухкомпонентный контейнер.

Перевод ЦВЗ в вектор и генерация фрактального контейнера



Переход из RGB в YCbCr



Дискретное вейвлет преобразование



Обратное дискретное вейвлет преобразование



Получение стегоконтейнера





Рисунок 33 – Алгоритм встраивания A2

3.1.2 Алгоритм извлечения ЦВЗ

Алгоритм извлечения состоит из следующих 6-и шагов:

1. Вычисление матрицы яркости $Y^*(x,y)$ из стегоконтейнера $S^*(x,y)$ путем перехода из пространства RGB в YCbCr.

2. Дискретное вейвлет преобразование матрицы яркости, вычисление коэффициентов вейвлет разложения $W_\varphi(j_0, m, n)$ и $W_\psi^i(j, m, n) (i = H, V, D)$.

3. Извлечение фрактального контейнера $F_{j,m,n}^*(x,y)$ путем сравнения значений диагональных коэффициентов с порогом Thr .

$$\begin{aligned} F_{j,m_2,n_2}^*(x,y) &= 1, \text{ если } W_\psi^D(j, m_2, n_2) > Thr; \\ F_{j,m_2,n_2}^*(x,y) &= 0, \text{ если } W_\psi^D(j, m_2, n_2) \leq Thr. \end{aligned} \quad (45)$$

4. Генерация алгебраического фрактала $\hat{F}_{j,m,n}(x,y)$ с использованием алгоритма времени убегания и параметров генерации l , $maxstep$, F_w , F_h , R . Также необходимо знать размер ЦВЗ в битах.

5. Извлечение вектора ЦВЗ $Q^*(Q_l)$ путем вычитания сгенерированного $\hat{F}_{j,m,n}(x,y)$ и извлеченного фрактала $F_{j,m,n}^*(x,y)$.

6. Перевод вектора ЦВЗ $Q^*(Q_l)$ в матрицу $Q^*(Q_w, Q_h)$.

На рисунке 34 показан пошаговый алгоритм извлечения ЦВЗ из двухкомпонентного контейнера.

Вычисление матрицы яркости



Контейнер



Красная компонента R



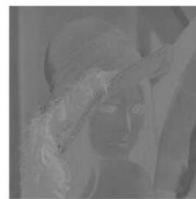
Зеленая компонента G



Синяя компонента B



Яркость Y



Синяя компонента Cb



Красная компонента Cr

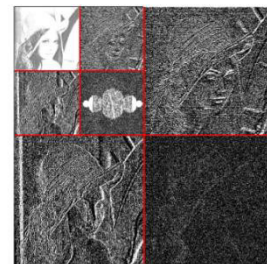
Дискретное вейвлет преобразование



Яркость Y

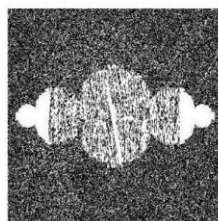


1 уровень разложения

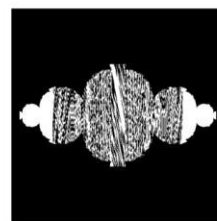


2 уровень разложения

Фильтрация коэффициентов путем сравнения с порогом

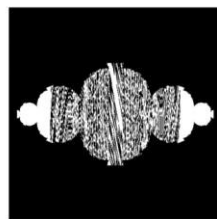


Извлеченные коэффициенты ДВП

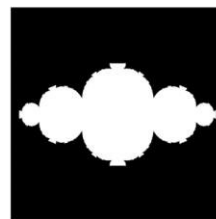


Фрактальный контейнер после фильтрации

Извлечение ЦВЗ



Фрактальный контейнер после фильтрации



Оригинальный фрактал



Извлеченный ЦВЗ

Рисунок 34 – Алгоритм извлечения АЗ

Для выбора вейвлет-преобразования при исследовании рассматривались 4 типа разложений: Хаара, Добеши 4, Симлет 4, Койфлет 4.

Для определения рациональных параметров алгоритма производилось встраивание в 20000 контейнеров из двух баз изображений, используемых для оценки стегосистем. Первые 10000 изображений – изображения в оттенках серого из базы BOWS2OrigEp3 [91], вторые 10000 изображений – полноцветные изображения размером 512x512 из базы PPG-LIRMM-COLOR [92].

Для оценки качества встраивания производилось вычисление пикового соотношения сигнал/шум PSNR.

Качество извлечения оценивалось с помощью коэффициента взаимной корреляции. На приемной стороне генерировался такой же ЦВЗ, что использовался при встраивании. Затем вычислялось значение коэффициента взаимной корреляции извлеченного и опорного ЦВЗ [93].

$$D(Q, Q^*) = \frac{\sum_{Q_w} \sum_{Q_h} (Q(Q_w, Q_h) - \bar{Q})(Q^*(Q_w, Q_h) - \bar{Q}^*)}{\sqrt{(\sum_{Q_w} \sum_{Q_h} (Q(Q_w, Q_h) - \bar{Q})^2)(\sum_{Q_w} \sum_{Q_h} (Q^*(Q_w, Q_h) - \bar{Q}^*)^2)}} , \quad (46)$$

где $\bar{Q}, \bar{Q}^*$ - среднее арифметическое величин яркости пикселей исходного и извлеченного ЦВЗ.

Если величина коэффициента корреляции превышала заданное пороговое значение, принималось утверждение, что в изображение встроен искомый ЦВЗ.

В качестве порогового значения было выбрано значение 0,8, позволяющее сохранить визуальную узнаваемость ЦВЗ и избежать значительных ошибок второго рода. Численные результаты экспериментов представлены в приложении В.2.

3.1.3 Выбор уровня разложения

Встраивание может быть реализовано на разных уровнях разложения. Выбор уровня разложения, на котором будет производиться замена коэффициентов, влияет как на искажения контейнера, так и на искажения ЦВЗ.

На рисунке 35 показана зависимость PSNR для заполненного контейнера от уровня разложения, на котором производилось встраивание. На рисунке 36 показана зависимость среднего значения коэффициента корреляции извлеченного и опорного ЦВЗ от уровня разложения, на котором производилось встраивание.

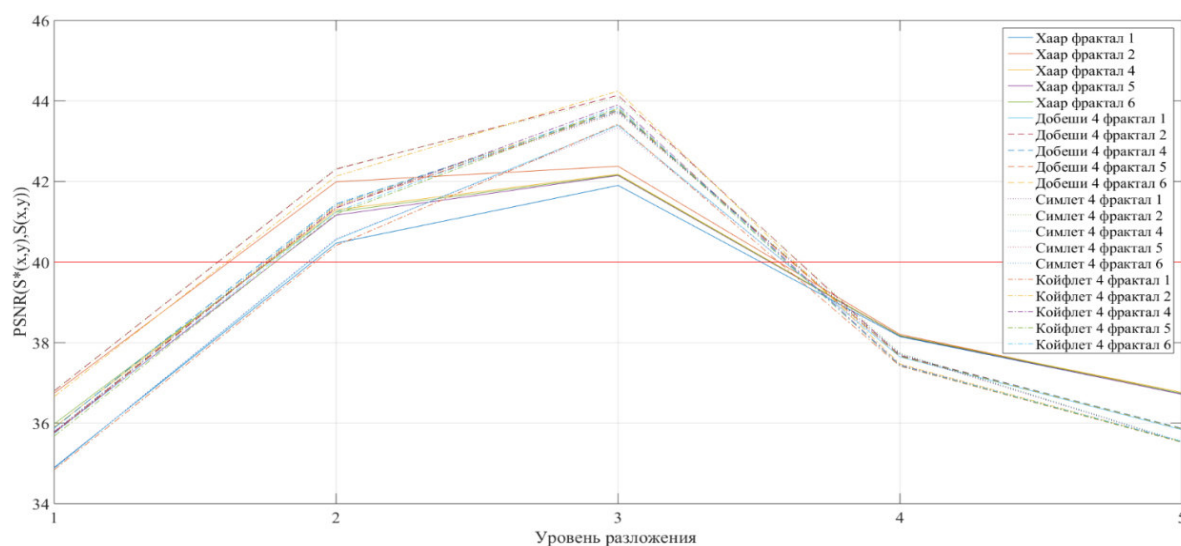


Рисунок 35 – Зависимость PSNR заполненного контейнера от уровня разложения

На основе анализа полученных зависимостей можно сделать вывод о том, что допустимый уровень $PSNR > 40$ достигается только при замене коэффициентов 2-го и 3-го уровня разложения.

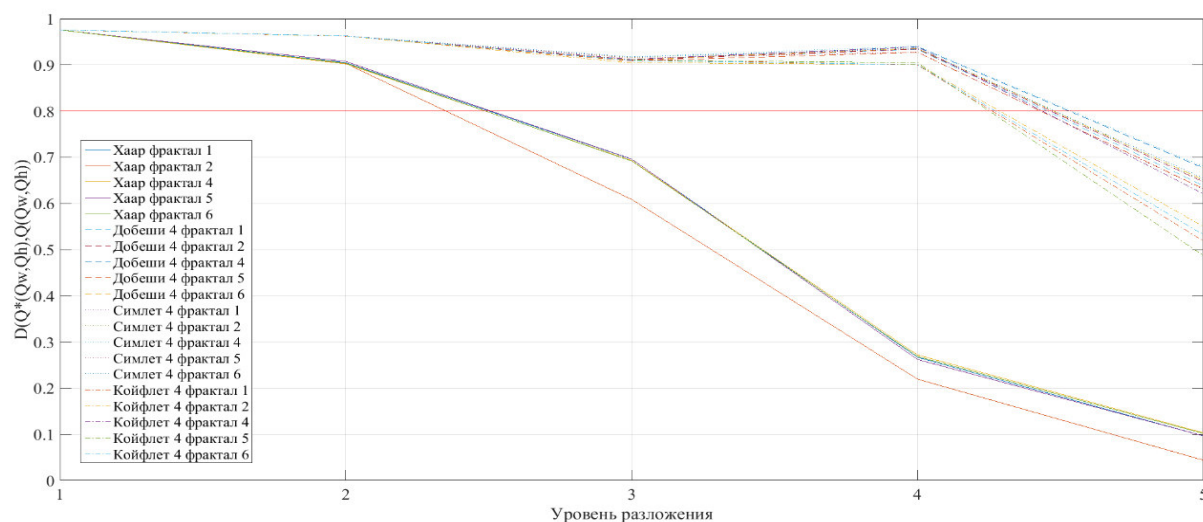


Рисунок 36 – Зависимость коэффициента корреляции извлеченного и опорного ЦВЗ от уровня разложения

Как видно из рисунка среднее значение корреляции выше установленного порога достигается на 1 и 2 уровне для вейвлета Хаара и на уровнях 1-4 для вейвлетов Добеши 4, Симлет 4 и Койфлет 4.

Анализ полученных результатов показал, что наиболее подходящим для встраивания информации является 2-й уровень вейвлет разложения, поскольку при замене коэффициентов 2-го уровня можно достичь как высокого уровня встраивания, так и высокого уровня извлечения.

3.1.4 Выбор типа коэффициентов вейвлет разложения для замены

На рисунке 37 представлена зависимость PSNR для заполненного контейнера при замене различных детализирующих коэффициентов вейвлет разложения: горизонтальных $W_{\psi}^H(j, m, n)$ вертикальных $W_{\psi}^V(j, m, n)$ и диагональных $W_{\psi}^D(j, m, n)$. Коэффициенты аппроксимации $W_{\varphi}(j_0, m, n)$ не рассматривались, поскольку они содержат основную энергию изображения и их изменение влечет за собой значительное искажение контейнера. На рисунке 38 показана зависимость коэффициента корреляции извлеченного и опорного ЦВЗ от типа коэффициентов, используемых при встраивании. Основные характеристики распределений коэффициентов вейвлет-разложения представлены в таблице 3.

Таблица 3 – Основные характеристики распределений коэффициентов вейвлет-разложения

		$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар	min	-139.5	-183.5	-39.25
	max	143.25	201	49.25
	M	0.0265	0.0349	-2.2e-04
	D	61.0961	88.0688	3.8593
Добеши 4	min	-57.5588	-84.013	-20.117
	max	63.5728	93.7817	22.9595
	M	0.0039	0.0056	8.3649e-04

	D	11.2092	15.9749	0.6252
Симлет 4	min	-62.8731	-99.8326	-29.2969
	max	70.2461	94.1859	24.4029
	M	0.0038	0.0040	-6.3157e-04
	D	11.6023	16.4285	0.0691
Койфлет 4	min	-53.9218	-84.9916	-17.2404
	max	54.4611	83.9383	15.3355
	M	0.0011	-0.0011	-5.5889e-04
	D	8.277	11.5275	0.5876

Исходя из значений в таблице можно сделать вывод, что вертикальные коэффициенты распределены в наиболее широком, а диагональные коэффициенты в наименьшем диапазоне значений. При использовании вейвлетов Хаара распределение коэффициентов разложения имеет более широкие границы по сравнению с другими типами разложения.

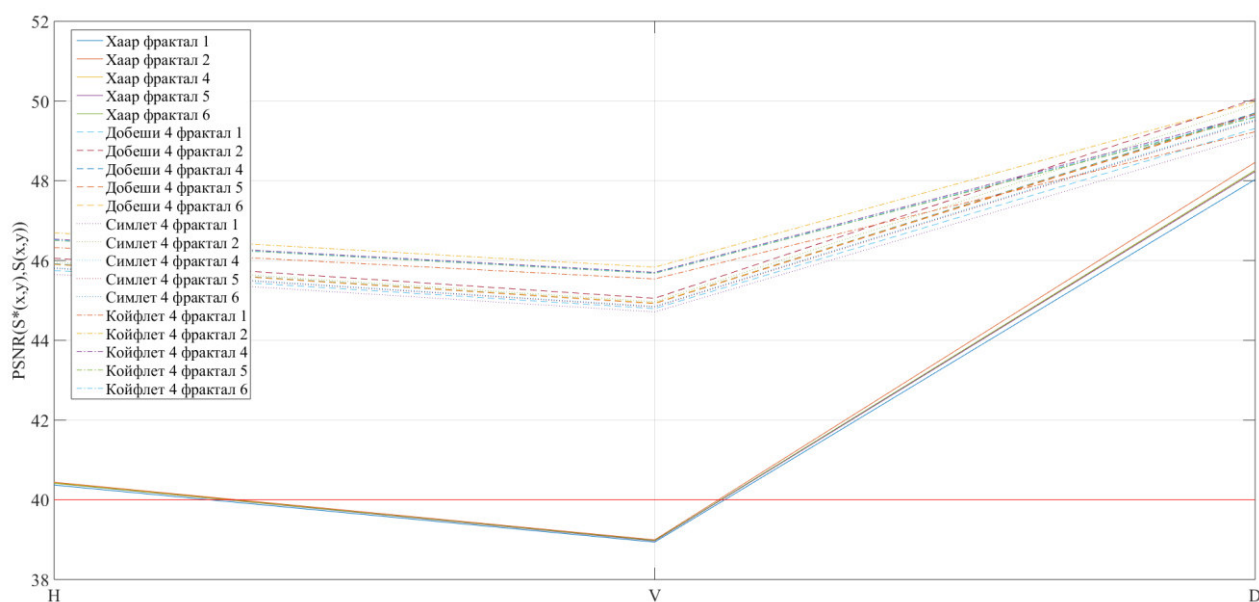


Рисунок 37 – Зависимость PSNR стегоконтейнера от типа изменяемых коэффициентов разложения

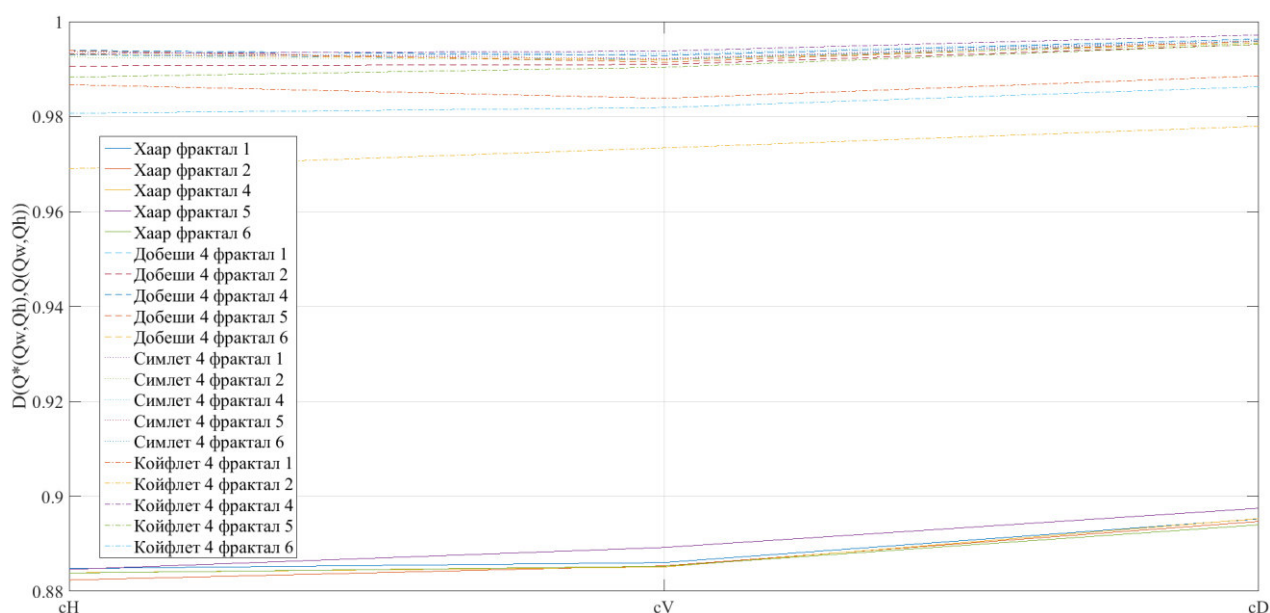


Рисунок 38 – Зависимость взаимной корреляции извлеченного и опорного ЦВЗ от типа коэффициентов вейвлет разложения

Из представленных зависимостей видно, что PSNR <40дБ при замене вертикальных коэффициентов вейвлет разложения Хаара. Самый высокий уровень отношения сигнал/шум достигается при замене диагональных коэффициентов, самый низкий – при замене вертикальных коэффициентов.

Полученные результаты позволяют сделать, что выбор типа коэффициентов вейвлет разложения не влияет на достоверность извлечения. В данном случае рекомендуется использовать диагональные коэффициенты разложения, поскольку их изменение вносит меньше всего искажений в контейнер при встраивании.

3.1.5 Выбор параметра α

Перед непосредственной заменой коэффициентов вейвлет разложения фрактальный контейнер умножается на параметр α . Путем изменения его значения можно влиять на искажения контейнера и ошибки при извлечении. На рисунке 39 представлена зависимость пикового отношения сигнал/шум от значения параметра α . На рисунке 40 представлена зависимость коэффициента корреляции извлеченного и опорного ЦВЗ от значения параметра α .

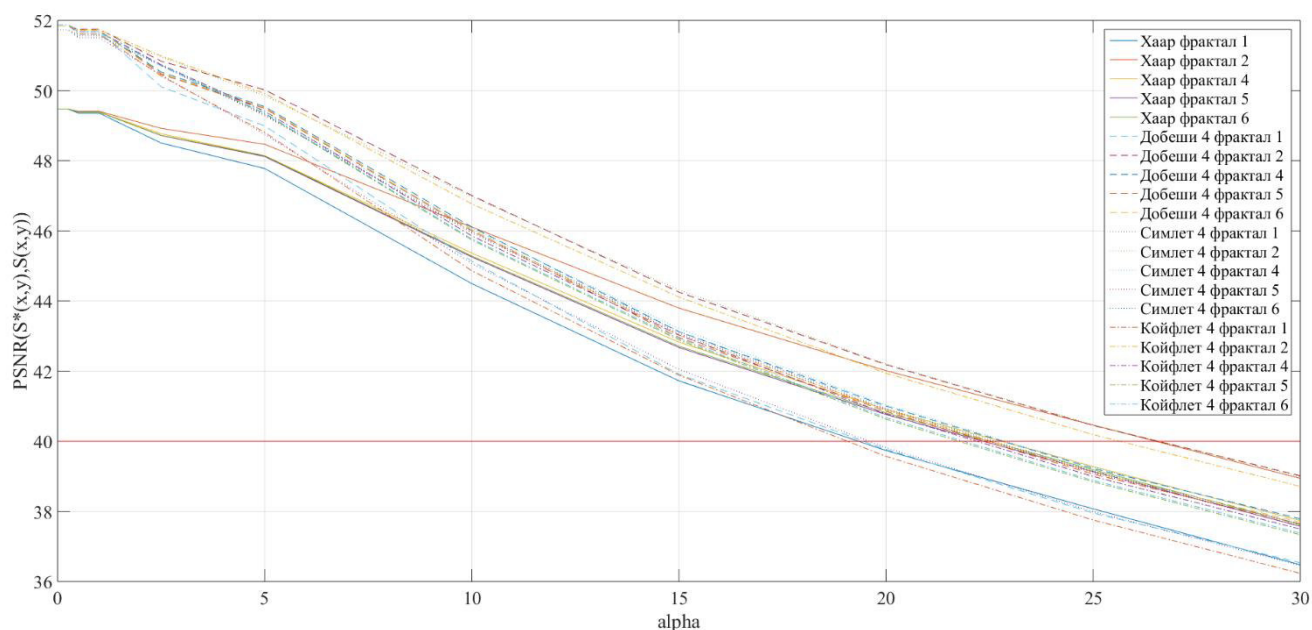


Рисунок 39 – Зависимость PSNR заполненного контейнера от значения параметра alpha

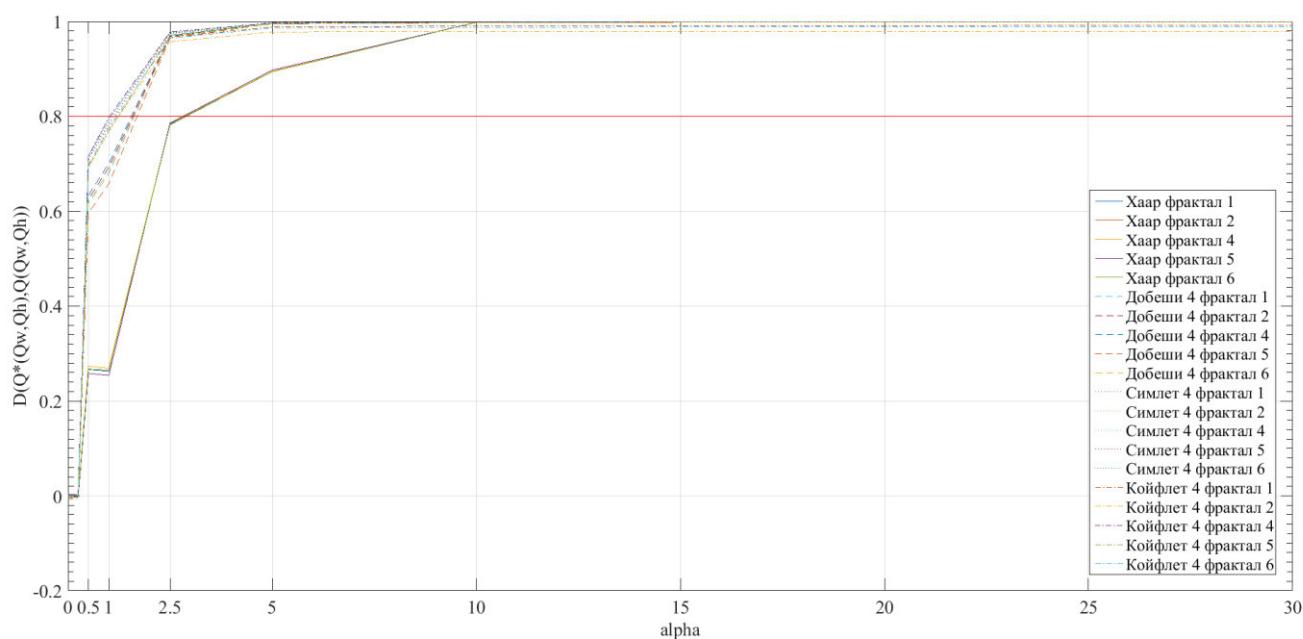


Рисунок 40 – Зависимость взаимной корреляции извлеченного и опорного ЦВЗ от значения параметра alpha

По результатам проведенных исследований можно сделать вывод о том, что для сохранения высокого качества стегоконтейнера и получения достоверных результатов извлечения необходимо использовать $\alpha \in [5; 18]$ для вейвлет разло-

жения Хаара и $\alpha \in [2.5; 18]$ в остальных случаях.

3.1.6 Выбор параметра Thr

В процессе извлечения, для фильтрации извлекаемого из контейнера фрактального контейнера от шумов, возникающих в процессе обратного вейвлет преобразования, используется пороговый уровень Thr. Величина порога подбирается на основании анализа значения параметра α . На рисунке 41 показана зависимость взаимной корреляции извлеченного и опорного ЦВЗ от соотношения Thr/alpha.

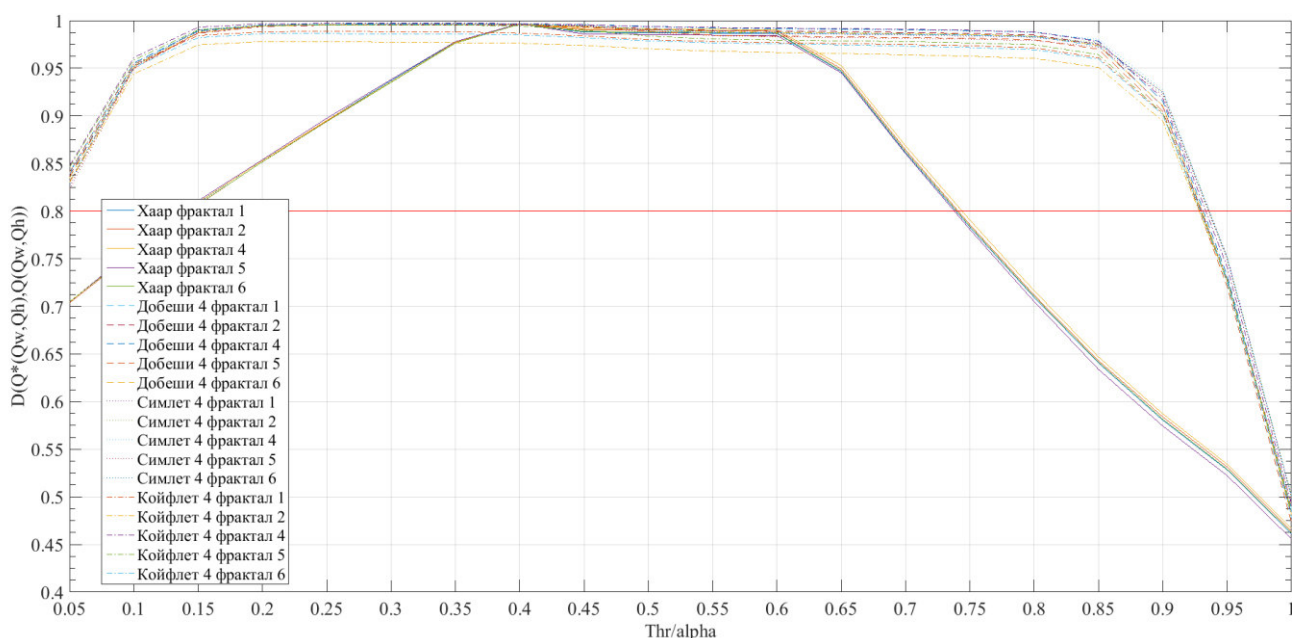


Рисунок 41 – Зависимость коэффициента корреляции взаимного и опорного ЦВЗ от соотношения Thr/alpha

На основе полученных результатов рекомендуется использовать следующие значения: $\text{Thr}/\alpha \in [0.25; 0.4]$ для вейвлет разложения Хаара и $\text{Thr}/\alpha \in [0.2; 0.45]$ для Добеши 4, Симлет 4 и Койфлет 4.

Использование в алгоритме A2 комбинации алгебраических фракталов и 2D ДВП существенно затрудняет возможность неправомерного доступа для квалифицированного злоумышленника по сравнению с известными алгоритмами, поскольку для извлечения ЦВЗ теперь необходима дополнительная информация о

значениях параметров алгоритма, получение которой крайне затруднительно.

Несмотря на указанные достоинства, применение алгоритма А2 ограничено размерами оригинального изображения и встраиваемого ЦВЗ. В качестве фрактального контейнера $F_{j,m,n}(x,y)$ необходимо использовать двумерные изображения, размеры которых зависят от набора параметров и возможный объем встраивания нельзя рассчитать или предсказать заранее без предварительной генерации алгебраического фрактала.

3.2 Алгоритм защиты неподвижных изображений А3 с использованием фрактального гауссовского шума и 2D ДВП.

Для преодоления указанных выше недостатков алгоритма А2, предлагается алгоритм А3 с использованием ФГШ, являющийся модификацией алгоритма А1 для изображений. Водяной знак в виде ПСП заменяется последовательностями ФГШ, из которых формируется двумерная матрица. Полученная матрица ФГШ встраивается в оригинальный контейнер путем замены матрицы коэффициентов ДВП.

3.2.1 Алгоритм встраивания

В общем случае алгоритм А3 состоит из 7-и последовательных шагов:

1. Генерация ЦВЗ в виде ПСП.
2. Вычисление матрицы яркости $Y(x,y)$ из оригинального контейнера $S(x,y)$ путем перехода из пространства RGB в YCbCr.
3. ДВП матрицы яркости. Вычисление коэффициентов вейвлет-разложения $W_\varphi(j_0, m, n)$ и $W_\psi^i(j, m, n) (i = H, V, D)$.
4. Генерация ФГШ $X^H(j)$. Генерация двух последовательностей ФГШ с заданным H_0 и H_1 .
5. Формирование новой матрицы диагональных коэффициентов 2ДДВП путем объединения последовательностей ФГШ в матрицу с коэффициентом α .

$$W_\psi^{i=D}(j=2, m_2, n_2) = \frac{1}{M_2 N_2} \alpha \sum_{x=0}^{M_2} \sum_{y=0}^{N_2} X_{j, m_2, n_2}^H(x, y) \psi_{j, m_2, n_2}^D(x, y). \quad (47)$$

6. Вычисление новой матрицы яркости $Y^*(x,y)$ путем обратного 2ДДВП с использованием фрактального контейнера $F_{j,m,n}(x,y)$.

7. Формирование стегоконтейнера $S^*(x,y)$ путем вычисления цветowych компонент на основе измененной матрицы яркости $Y^*(x,y)$.

На рисунке 42 проиллюстрирован поэтапный алгоритм встраивания.

Переход из RGB в YCbCr



Контейнер



Красная компонента R



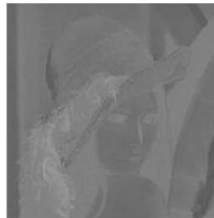
Зеленая компонента G



Синяя компонента B



Яркость Y



Синяя компонента Cb



Красная компонента Cr

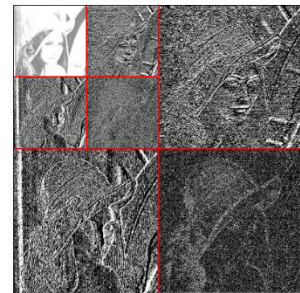
Дискретное вейвлет преобразование



Яркость Y



1 уровень разложения



2 уровень разложения

Получение стегоконтейнера



Новая компонента яркости Y^*



Синяя компонента Cb

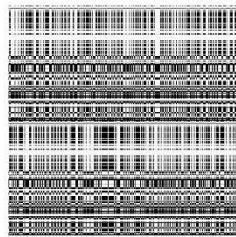


Красная компонента Cr



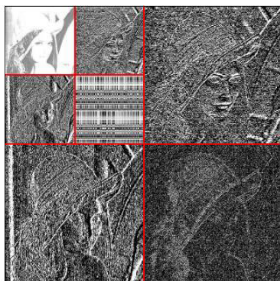
Красная компонента R^* Зеленая компонента G^* Синяя компонента B^* Стегоконтейнер

Формирование новой матрицы диагональных коэффициентов



Матрица ФГШ

Обратное дискретное вейвлет преобразование



2 уровень разложения



1 уровень разложения



Новая компонента яркости Y^*

Рисунок 42 – Последовательность преобразований при реализации алгоритма встраивания АЗ

3.2.2 Алгоритм извлечения

Алгоритм извлечения состоит из следующих 7-и шагов:

1. Вычисление матрицы яркости $Y^*(x,y)$ из стегоконтейнера $S^*(x,y)$ путем перехода из пространства RGB в $YCbCr$.
2. Дискретное вейвлет преобразование матрицы яркости, вычисление коэффициентов вейвлет разложения $W_\varphi(j_0, m, n)$ и $W_\psi^i(j, m, n) (i = H, V, D)$.

3. Выделение последовательностей ФГШ из матрицы коэффициентов вейвлет разложения.

4. Оценка показателя Херста полученных сегментов $\hat{H}(p)$.

5. Сравнение оценок показателя Херста $\hat{H}(p)$ с пороговым значением $H_{пор}$ и извлечение элементов ПСП $ПСП^*(p)$ согласно правилу:

$$ПСП^*(p) = \begin{cases} 1, & \text{если } H(p) \geq H_{пор} \\ 0, & \text{если } H(p) < H_{пор} \end{cases}. \quad (48)$$

6. Генерация «опорной» ПСП $ПСП(p)$.

7. Вычисление корреляции «опорной» и извлеченной ПСП для последующей оценки достоверности извлечения и сравнение с порогом.

$$B_{ПСП}(i) = \frac{1}{P} \sum_{p=1}^P ПСП_p^* ПСП_{p+i}. \quad (49)$$

На рисунке 43 проиллюстрирован поэтапный алгоритм извлечения ПСП.

Для определения рациональных параметров алгоритма производилось тестирование с использованием баз BOWS2OrigEp3 и PPG-LIRMM-COLOR. Оценка качества встраивания производилась с использованием пикового соотношения качество/шум PSNR. Для оценки качества извлечения использовалось значение $B_{ПСП}(i=0)$. Пороговое значение было установлено как $B_{ПСП}(i=0) = 0.95$. Численные результаты экспериментов представлены в приложении В.3.

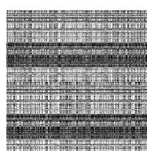
Вычисление матрицы яркости



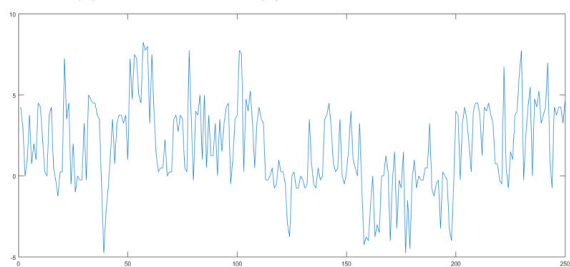
Дискретное вейвлет преобразование



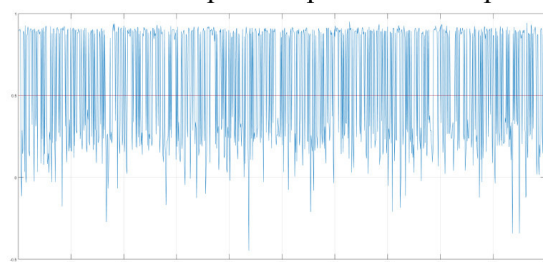
Извлечение матрицы ФГШ



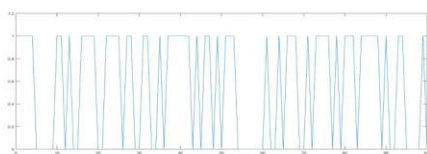
Выделение последовательностей ФГШ



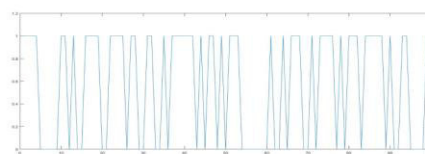
Оценка показателя Херста и сравнение с порогом



Извлечение ПСП



Генерация опорного ПСП



Вычисление взаимной корреляции и сравнение с порогом

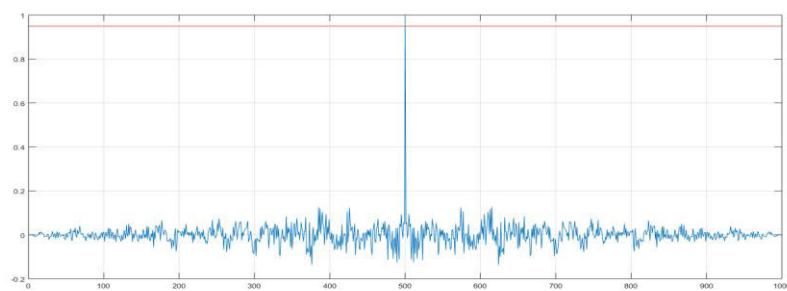


Рисунок 43 – Последовательность преобразований при реализации алгоритма извлечения АЗ

3.2.3 Выбор уровня разложения

На рисунке 44 представлена зависимость PSNR стегоконтейнера от уровня разложения вейвлет преобразования, на котором производилась замена диагональных коэффициентов.

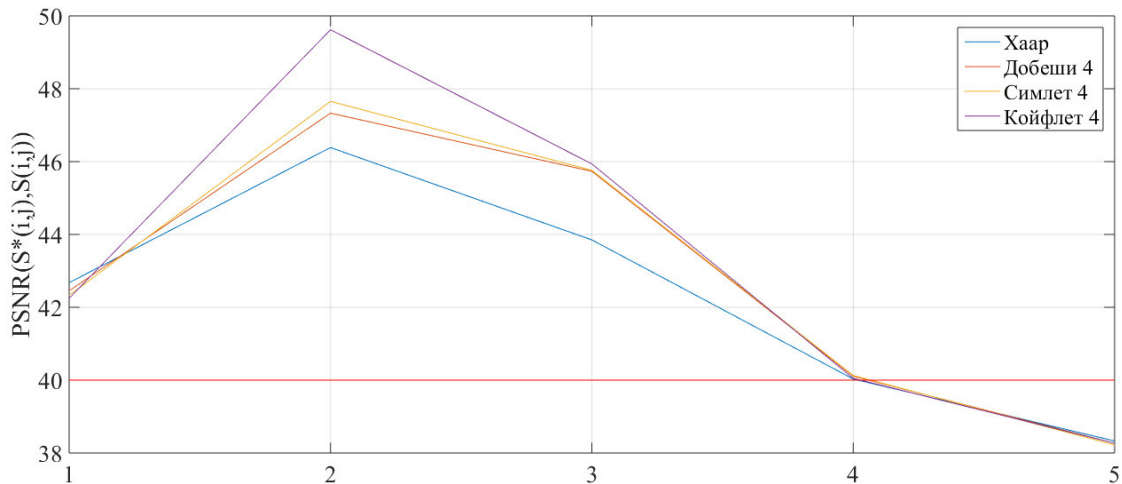


Рисунок 44 – Зависимость PSNR стегоконтейнера от уровня разложения вейвлет преобразования

Как видно допустимый уровень $PSNR > 40$ достигается при замене коэффициентов на первых трех уровнях разложения. Лучшее соотношение сигнал/шум получено при замене коэффициентов 2-го уровня разложения.

На рисунке 45 показана зависимость $V_{\text{ПСП}}(i=0)$ от уровня разложения.

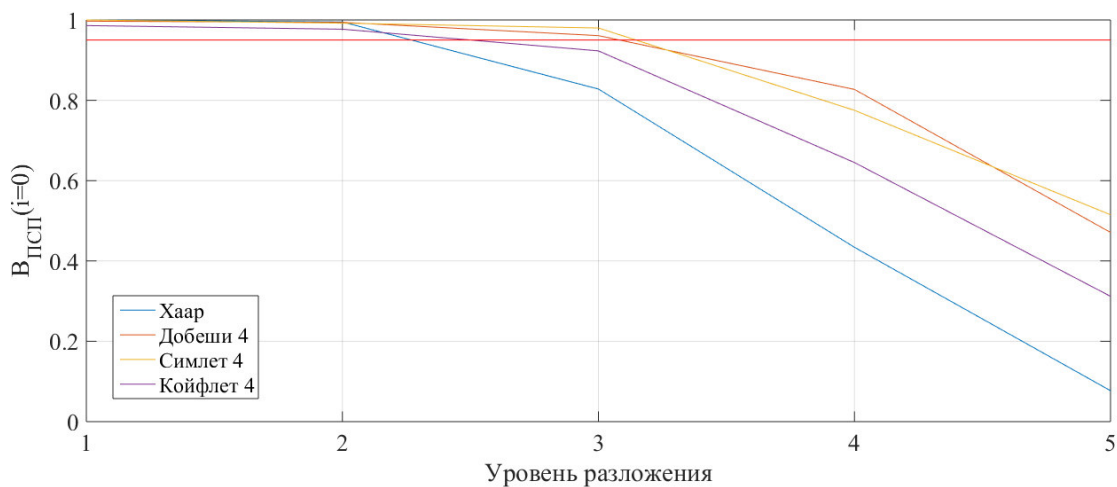


Рисунок 45 – Зависимость $V_{\text{ПСП}}(i=0)$ от уровня разложения

Полученные результаты иллюстрируют, что наилучшие результаты при встраивании и извлечении достигаются при встраивании в 1-й и 2-й уровни вейвлет разложения.

3.2.4 Выбор типа коэффициентов вейвлет-разложения

На рисунке 46 представлена зависимость PSNR стегоконтейнера от типа коэффициентов вейвлет-разложения, которые использовались для встраивания: H – горизонтальные коэффициенты, V – вертикальные коэффициенты, D – диагональные коэффициенты.

Видно, что наименьшие искажения в контейнере возникают при изменении диагональных коэффициентов, а наибольшие – при изменении вертикальных коэффициентов. Уровень $PSNR < 40$ достигается только при замене вертикальных коэффициентов с использованием вейвлета Хаара.

На рисунке 47 показана зависимость $V_{ПСП} (i=0)$ от типа коэффициентов вейвлет-разложения.

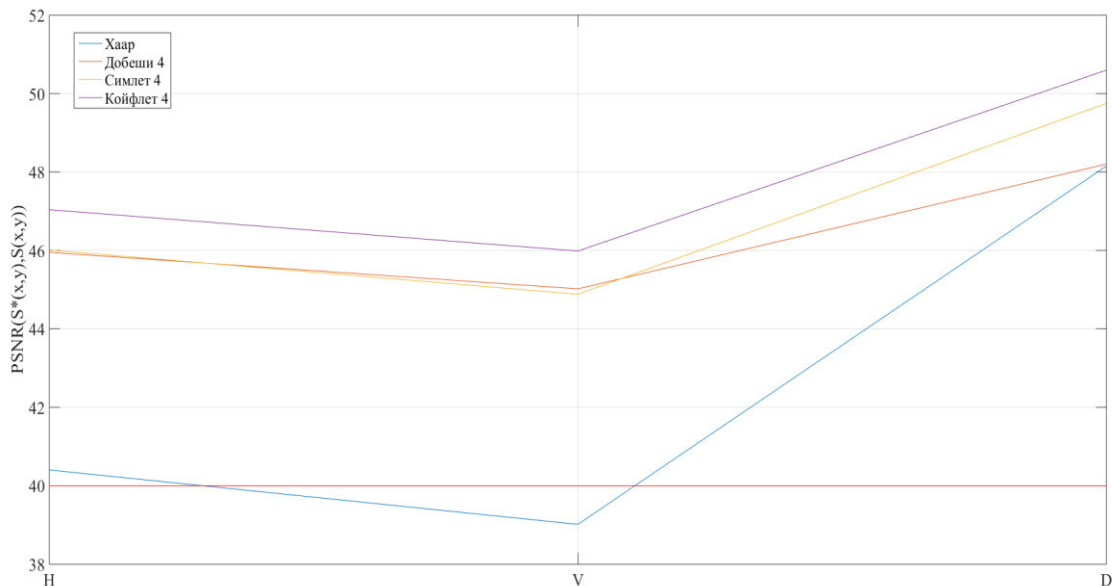


Рисунок 46 – Зависимость PSNR контейнера от типа коэффициентов вейвлет-разложения

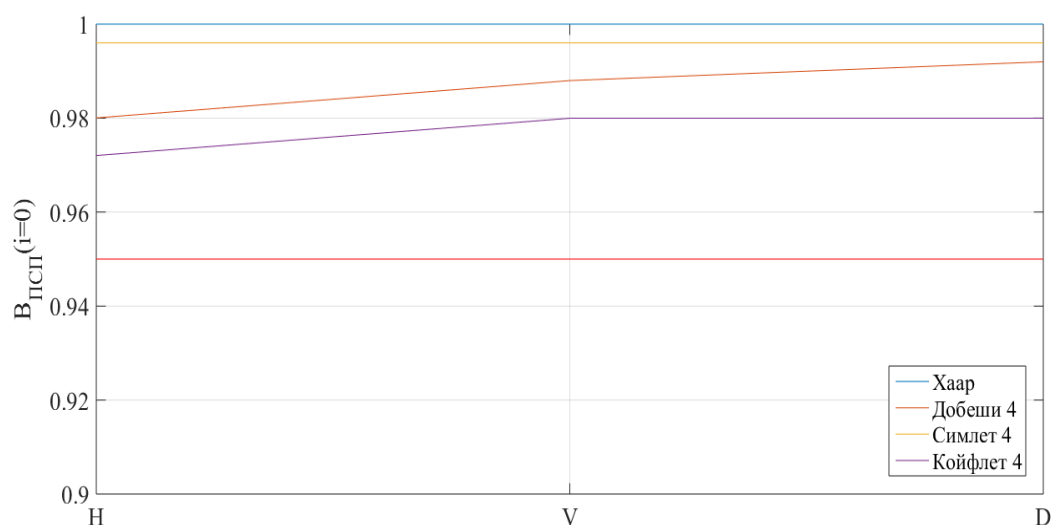


Рисунок 47 – Зависимость $V_{\text{ПСП}}(i=0)$ от типа коэффициентов вейвлет разложения

С учётом полученных результатов встраивания и извлечения рекомендуется использовать диагональные или горизонтальные коэффициенты для встраивания ЦВЗ.

3.2.5 Выбор параметра alpha

На рисунке 48 представлена зависимость пикового соотношения сигнал/шум PSNR стегоконтейнера от значения параметра alpha.

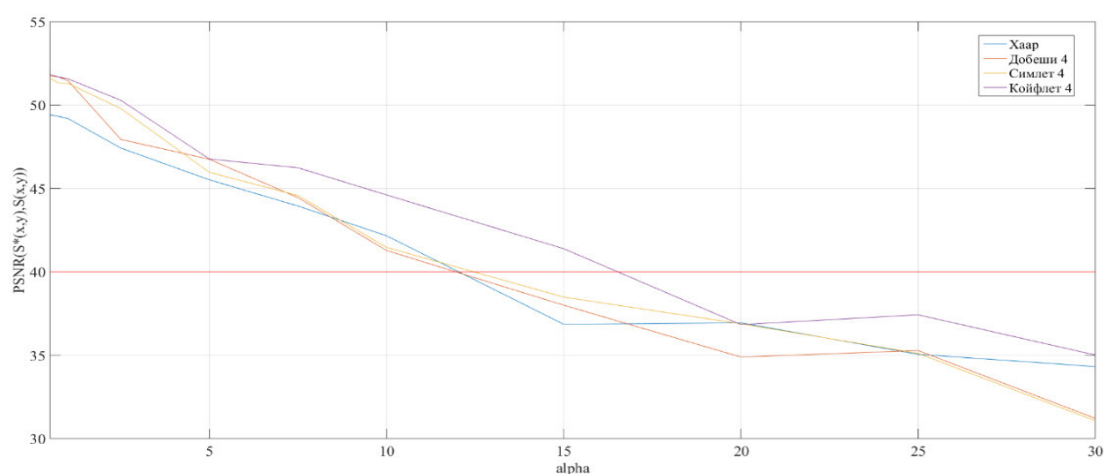


Рисунок 48 – Зависимость PSNR стегоконтейнера от параметра alpha

При анализе полученных зависимостей можно отметить, что допустимый уровень $\text{PSNR} \geq 40$ достигается при $\alpha \leq 12.5$ для всех вейвлетов Хаара, Добеши

4 и Симлет 4. Для вейвлета Койфлет 4 значение PSNR=40 достигается при $\alpha > 15$. Наибольшие искажения в контейнере появляются при использовании вейвлета Хаара, наименьшие – при использовании вейвлета Койфлет 4.

На рисунке 49 представлена зависимость $V_{\text{ПСП}}(i=0)$ от значения α .

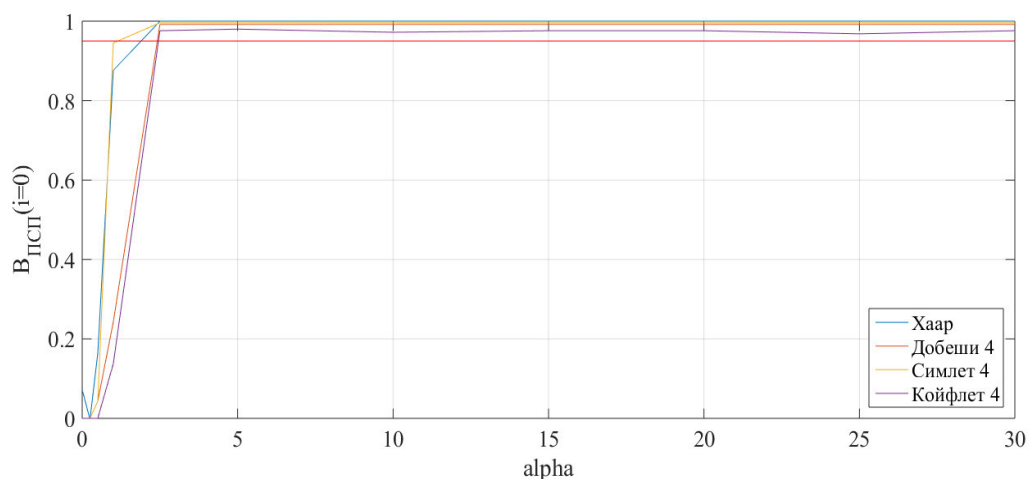


Рисунок 49 – Зависимость $V_{\text{ПСП}}(i=0)$ от параметра α

Для достижения баланса между качеством встраивания и извлечения рекомендуется использовать $\alpha \in [2.5; 12.5]$.

3.2.6 Выбор длины последовательности ФГШ

На рисунке 50 представлена зависимость PSNR стегоконтейнера от длины последовательности ФГШ.

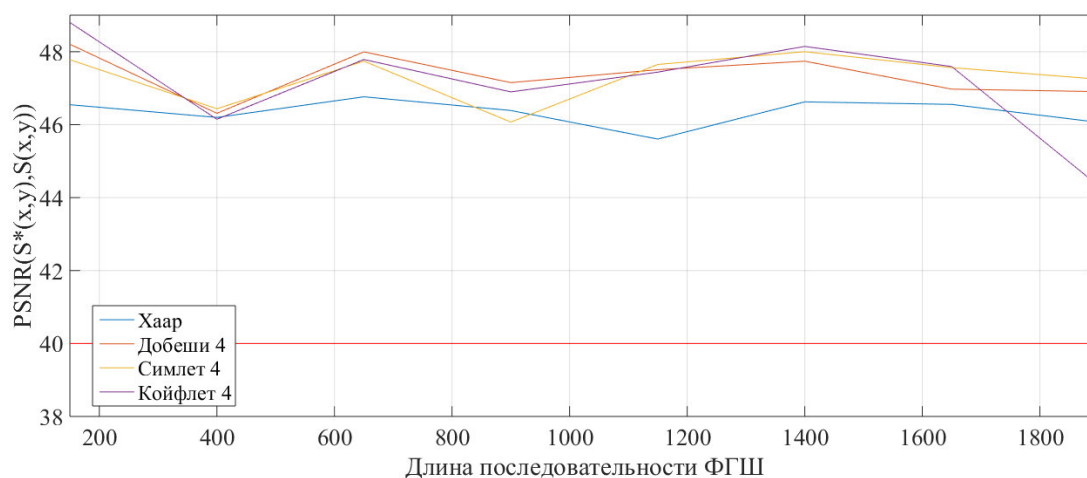


Рисунок 50 – Зависимость PSNR стегоконтейнера от длины последовательности ФГШ

На рисунке 51 представлена зависимость $V_{\text{ПСП}}(i=0)$ от длины ФГШ.

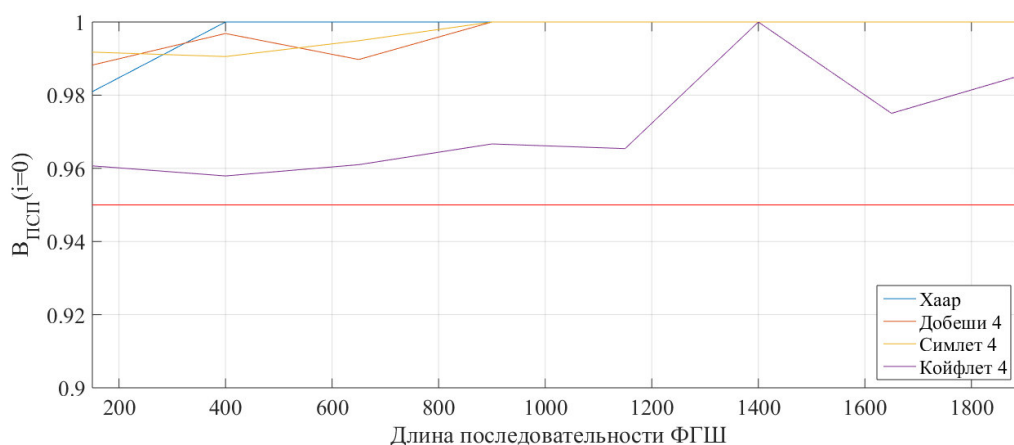


Рисунок 51 – Зависимость $V_{\text{ПСП}}(i=0)$ от длины последовательности ФГШ

Из полученных значений можно сделать вывод о том, что длина последовательности ФГШ незначительно влияет на качество извлечения.

3.2.7 Выбор значения показателя Херста единичной последовательности H_1

На рисунке 52 представлена зависимость пикового соотношения сигнал/шум PSNR стегоконтейнера от значения показателя Херста единичной последовательности H_1 . На рисунке 53 представлена зависимость $V_{\text{ПСП}}(i=0)$ от значения показателя Херста единичной последовательности H_1 .

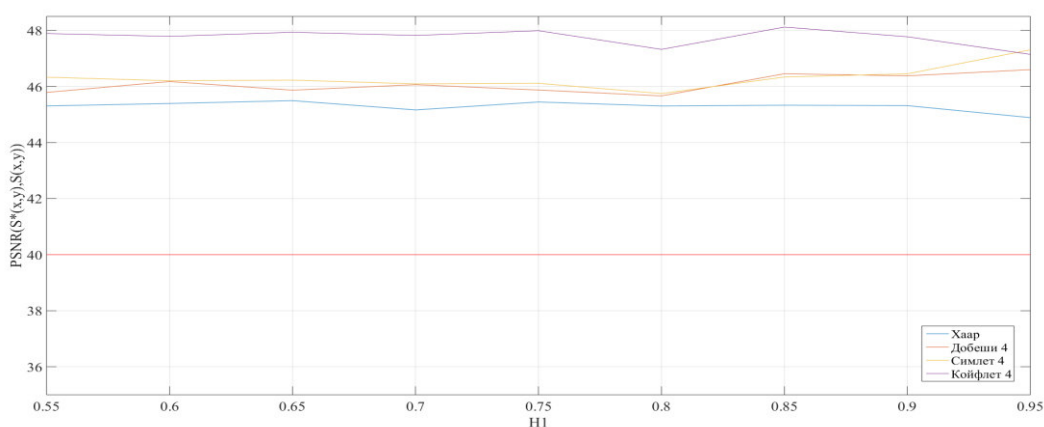


Рисунок 52 – Зависимость PSNR стегоконтейнера от значения показателя Херста единичной последовательности H_1

Можно видеть, что прямой зависимости между значением показателя Херста H_1 и степенью искажения контейнера нет. Все полученные значения превы-

шают предельный уровень $PSNR=40$. При использовании вейвлета Хаара достигаются наименьшие значения $PSNR \in (47.5; 48.5)$, при использовании вейвлета Койфлет – наибольшие значения $PSNR \in (50; 50.5)$.

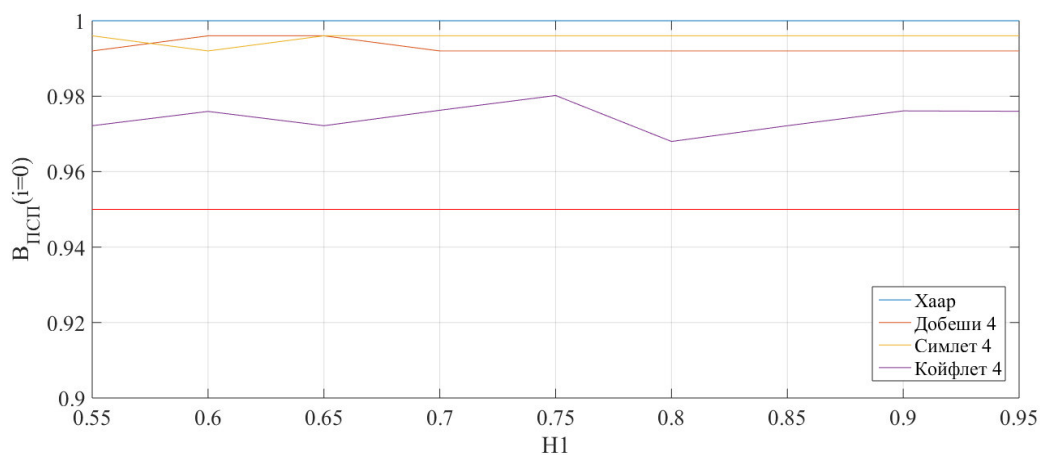


Рисунок 53 – Зависимость $V_{ПСП}(i=0)$ от значения показателя Херста единичной последовательности H_1

Исходя из полученных результатов, рекомендуется использовать $H_1 \geq 0.7$ для вейвлетов Добеши 4, Симлет 4 и Койфлет 4.

3.2.8 Выбор порога $H_{пор}$

На рисунке 54 представлена зависимость $V_{ПСП}(i=0)$ от порогового значения $H_{пор}$

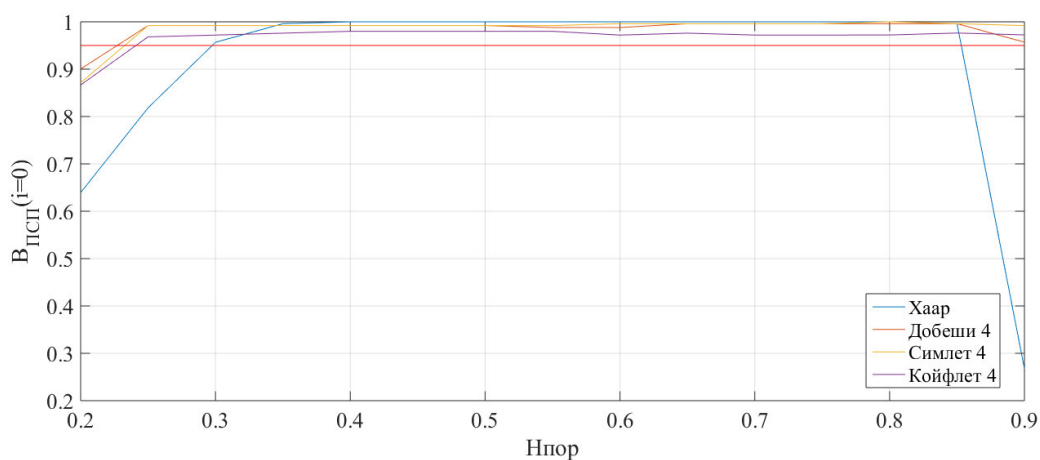


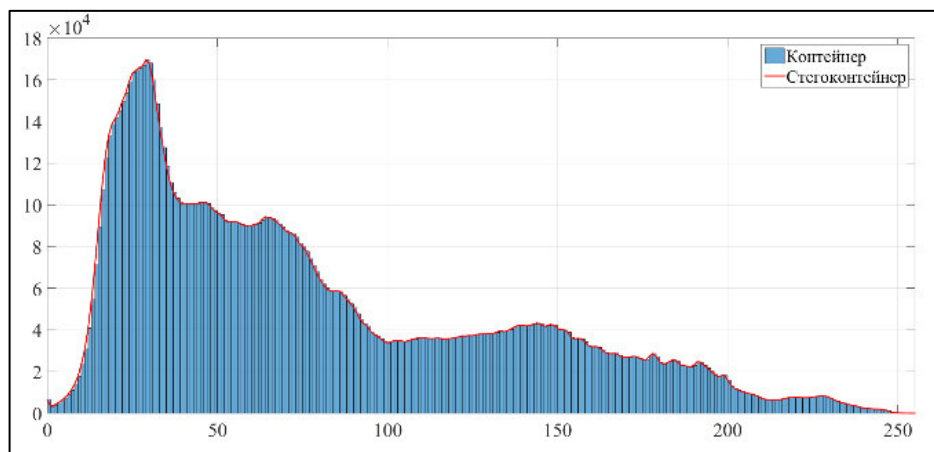
Рисунок 54 – Зависимость коэффициента корреляции от порога $H_{пор}$

На основе анализа полученных результатов можно сделать вывод, что при

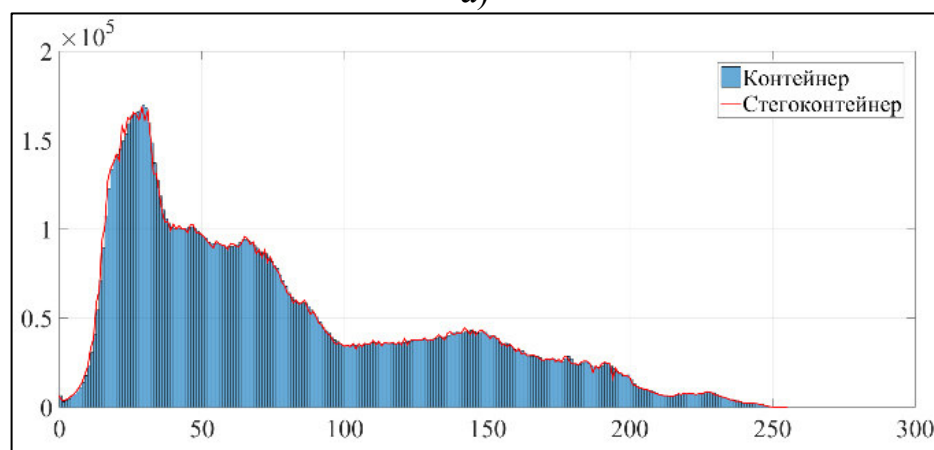
использовании вейвлета Хаара рекомендуется использовать значение порога $N_{thr} \in [0.35; 0.75]$, для вейвлетов Добеши 4 и Симлет 4 рекомендуется $N_{thr} \in [0.4; 0.75]$, для Койфлет 4 - $N_{thr} \in [0.3; 0.55]$.

3.3 Сравнительный анализ эффективности алгоритмов встраивания ЦВЗ фрактальными методами в отсутствие атак

Для оценки степени скрытности встраивания ЦВЗ в неподвижные изображения-контейнеры применялся метод статистического анализа гистограмм-распределений, которые представлены на рисунке 55.



а)



б)

Рисунок 55 – Гистограммы распределения значений интенсивности яркости «пустых» и «заполненных» стегоконтейнеров при использовании алгоритмов

а) А2, б) А3

Из рис. 55а видно, что алгоритм А2 показывает высокие результаты поскольку его гистограмма полностью сохраняет сигнатуру в сравнении с гистограммой «пустого» контейнера. Это означает, что визуальное и численное сравнение гистограмм не дает возможности злоумышленнику обнаружить в изображении скрытой метки. При анализе стегоконтейнера А3 (рис.55б) видно, что форма гистограммы сохраняется, а малые погрешности (расхождение не более 1-2%) не являются индикатором наличия встроенной метки.

Сравнительный анализ эффективности встраивания ЦВЗ с помощью фрактальных алгоритмов А2 и А3 производился путем сравнения их статистических показателей с эталонным алгоритмом прямого расширения спектра Э1. Статистический анализ близости распределений S и S^* проводился с использованием следующих метрик: взаимная корреляция, расстояние Кульбака-Лейблера и расстояние Бхаттачария.

В таблице 4 представлены результаты вычисления статистических показателей разработанных алгоритмов А2 и А3 и эталонного алгоритма Э1.

Таблица 4 – Результаты вычисления статистических показателей

Алгоритм	Вейвлет	Фрактал	$D/\max(D)$	$D_{KL}/\max(D_{KL})$	$d[P(S),Q(S^*)]/\max(d)$
A2	Хаар	1	0.99	0,8355	0,9074
A2	Хаар	3	0.99	0,8647	0,9074
A2	Хаар	4	0.99	0,8824	0,9074
A2	Хаар	5	0.99	0,8385	0,9074
A2	Хаар	6	0.99	0,8592	0,9074
A2	Добеши 4	1	0.99	0,8993	0,9074
A2	Добеши 4	3	0.99	0,8995	0,9074
A2	Добеши 4	4	0.99	0,9518	0,9074
A2	Добеши 4	5	0.99	0,9100	0,9167
A2	Добеши 4	6	0.99	0,9303	0,9074
A2	Симлет 4	1	0.99	0,9215	0,9074
A2	Симлет 4	3	0.99	0,9339	0,9074

A2	Симлет 4	4	0.99	1,0000	0,9074
A2	Симлет 4	5	0.99	0,9068	0,9074
A2	Симлет 4	6	0.99	0,9259	0,9074
A2	Койфлет 4	1	0.99	0,8796	0,9074
A2	Койфлет 4	3	0.99	0,8854	0,9074
A2	Койфлет 4	4	0.99	0,9164	0,9074
A2	Койфлет 4	5	0.99	0,8495	0,9074
A2	Койфлет 4	6	0.99	0,8773	0,9074
A3	Хаар		0.99	0,8916	0,8796
A3	Добеши 4		0.98	0,7896	1,0000
A3	Симлет 4		0.98	0,8102	0,9907
A3	Койфлет 4		0.99	0,9624	0,8611
Э1			0.1	0,0392	0,1667

Полученные результаты показывают, что хотя новые алгоритмы A2 и A3 уступают эталонному алгоритму Э1 по статистическим показателям близости, однако являются «слепыми» и не требуют наличия копии контейнера на приемной стороне при извлечении ЦВЗ. Наличие дополнительных ключей делает разработанные алгоритмы A2 и A3 более устойчивыми к угрозам неправомерного использования по сравнению с Э1. Для обоснования выводов об эффективности разработанных алгоритмов был проведен анализ их устойчивости при воздействии атак.

3.4 Выводы

1. Разработан новый алгоритм A2 с использованием двухкомпонентного контейнера в виде алгебраического фрактала и дискретного вейвлет-преобразования. Произведен анализ параметров алгоритма (уровень вейвлет разложения, тип коэффициентов, масштабирующий коэффициент α и порог Thr) для достижения баланса между качеством встраивания и достоверностью извлечения.

2. Показано, что наилучший баланс между качествами встраива-

ния/извлечения достигается при замене диагональных коэффициентов второго уровня 2D ДВП; параметр α должен находиться в пределах: 5...18 - при использовании вейвлета Хаара; 2.5...18 - при использовании вейвлетов Добеши 4, Симлет 4 и Койфлет. Минимальная вероятность ошибки извлечения ЦВЗ достигается при соотношении порога к α из диапазона $\{0.25...0.4\}$ - для вейвлета Хаара и $\{0.2...0.45\}$ - для Добеши 4, Симлет 4 и Койфлет 4. При этом наибольшие искажения при встраивании /извлечении наблюдаются для вейвлета Хаара.

3. Разработан новый алгоритм А3 с использованием дискретного вейвлет-преобразования и фрактального гауссовского шума, который является интерпретацией алгоритма А1 для изображения. Произведен анализ параметров алгоритма (уровень вейвлет разложения, тип коэффициентов, масштабирующий коэффициент α , длина последовательности ФГШ, показатель Хёрста единичной последовательности и порог Thr) для достижения баланса между качеством встраивания и достоверностью извлечения. Преимуществом алгоритма А3 по сравнению с алгоритмом А2 является более высокий и независимый от параметров фракталов возможный объем встраивания. Алгоритм А3 рекомендуется использовать в случаях, когда необходимо встроить ЦВЗ заданного объема или при высокой вероятности возникновения мешающих воздействий. В других случаях рекомендуется использовать алгоритм А2.

4. Показано, что наилучший баланс между качеством контейнера $S^*(x,y)$ и качеством извлечения ЦВЗ достигается при замене диагональных и горизонтальных коэффициентов 1-го или 2-го уровня 2ДДВП разложения. Наименьшие ошибки извлечения наблюдаются при использовании вейвлета Койфлет 4, наибольшие – при использовании вейвлета Хаара.

5. Произведенный анализ эффективности встраивания разработанных алгоритмов с использованием статистических показателей показал, что хотя новые алгоритмы А2 и А3 уступают эталонному алгоритму Э1 по статистическим показателям близости, однако являются «слепыми» и не требуют наличия копии

контейнера на приемной стороне при извлечении ЦВЗ. Наличие дополнительных ключей делает разработанные алгоритмы А2 и А3 более устойчивыми к угрозам неправомерного использования по сравнению с Э1.

Глава 4 Исследование устойчивости разработанных алгоритмов к различным атакам

В главе представлены результаты исследования устойчивости разработанных алгоритмов к случайному добавлению шума различного типа и атакам, направленным на удаление ЦВЗ (усредняющий фильтр и сжатие JPEG).

4.1 Исследование устойчивости алгоритма A2

Для оценки качества предлагаемого алгоритма контейнер, содержащий ЦВЗ, подвергался воздействию следующих атак: добавление шума, фильтрация и сжатие jpeg.

Использовалось три типа шума с различными параметрами:

- гауссовский шум с математическим ожиданием 0 и дисперсией 0.01, 0.015, 0.02, 0.025, 0.03, 0.035, 0.04, 0.045, 0.05, 0.055;
- импульсный шум (соль и перец) с интенсивностью d (доля искаженных пикселей) 0.01, 0.015, 0.02, 0.025, 0.03, 0.035, 0.04, 0.045, 0.05, 0.055;
- мультипликативный шум с дисперсией 0.01, 0.015, 0.02, 0.025, 0.03, 0.035, 0.04, 0.045, 0.05, 0.055.

Для оценки устойчивости разработанного алгоритма к фильтрации на заполненный контейнер воздействовал усредняющий низкочастотный фильтр с различными размерами маски: 2x2, 3x3, 4x4, 5x5, 6x6, 7x7, 8x8, 9x9 и 10x10.

Для оценки устойчивости алгоритма к сжатию JPEG заполненный контейнер подвергался сжатию различного уровня: 0%, 10%, 20%, 30%, 40%, 50%.

На рисунке 56 проиллюстрированы результаты извлечения ЦВЗ при воздействии гауссовского шума для фрактального контейнера 1 и вейвлет разложения Хаара. На рисунке 57 представлены зависимости корреляции извлеченного и опорного ЦВЗ от дисперсии гауссовского шума для разных типов вейвлет разложений.

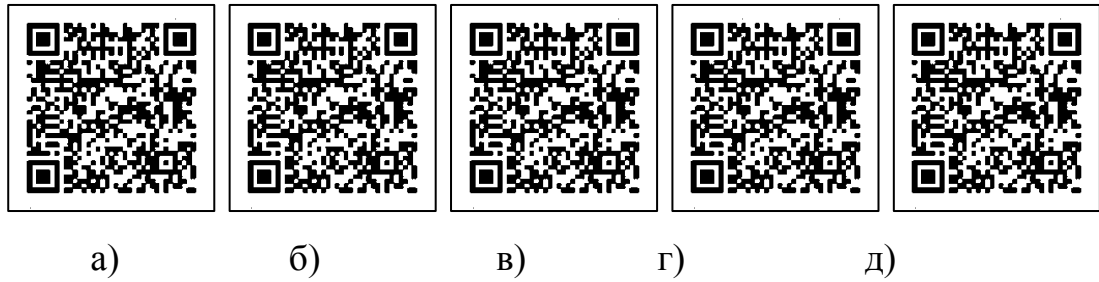


Рисунок 56 – Результаты извлечения ЦВЗ при воздействии гауссовского шума с математическим ожиданием $m=0$ и различной дисперсией v на заполненный контейнер при использовании фрактального контейнера 1-го типа и вейвлет разложения Хаара

а) $v=0.01$ б) $v=0.02$ в) $v=0.03$ г) $v=0.04$ д) $v=0.05$

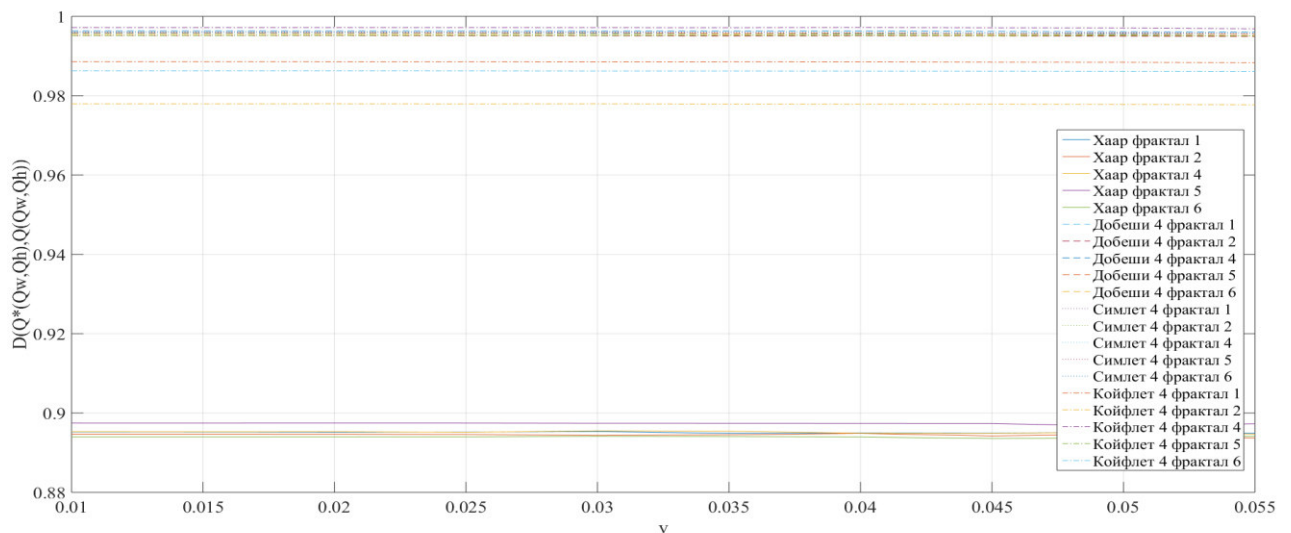


Рисунок 57 – Зависимость корреляции извлеченного и опорного ЦВЗ от дисперсии гауссовского шума

Из полученных результатов видно, что гауссовский шум не вносит серьезных искажений во встроенный ЦВЗ. Лучшие результаты были получены Добеши 4 и Койфлет 4. Тип фрактала практически не влияет на устойчивость алгоритма к воздействию шума.

На рисунке 58 показаны результаты извлечения ЦВЗ при воздействии на стегоконтейнер импульсного шума с различной интенсивностью. На рисунке 59 представлена зависимость корреляции извлеченного и опорного ЦВЗ от интен-

сивности шума.

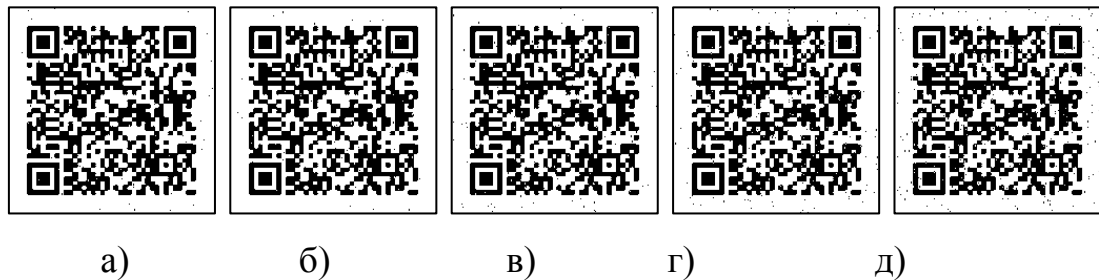


Рисунок 58 – Результаты извлечения ЦВЗ при воздействии импульсного шума на заполненный контейнер с различными значениями интенсивности импульсной составляющей шума d при использовании фрактального контейнера 1-го типа и вейвлет разложения Хаара

а) $d=0.01$ б) $d=0.02$ в) $d=0.03$ г) $d=0.04$ д) $d=0.05$.

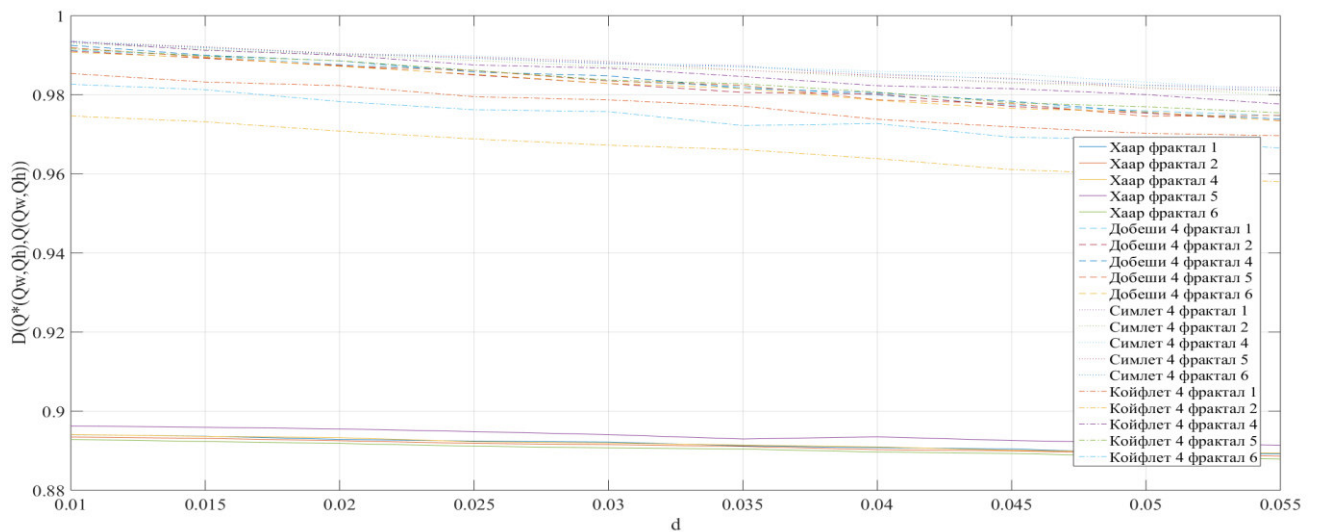


Рисунок 59 – Зависимость корреляции извлеченного и опорного ЦВЗ от интенсивности импульсного шума

Из представленных зависимостей можно наблюдать незначительное уменьшение значения корреляции при увеличении интенсивности шума. Однако все полученные значения превышают заданный порог 0.8, что говорит об устойчивости алгоритма к данному виду воздействия.

На рисунке 60 представлены результаты извлечения ЦВЗ при воздействии на стегоконтейнер мультипликативного шума с различной дисперсией. На рисун-

ке 61 представлена зависимость корреляции извлеченного и опорного ЦВЗ от дисперсии мультипликативного шума.

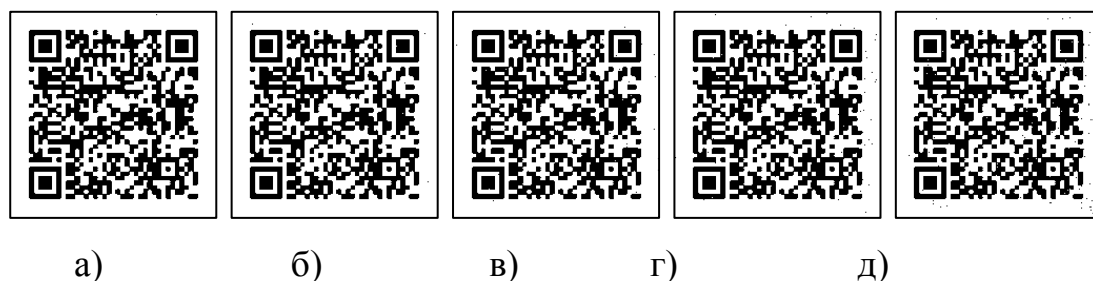


Рисунок 60 – Результаты извлечения ЦВЗ при воздействии мультипликативного шума с различной дисперсией v на заполненный контейнер при использовании фрактального контейнера 1-го типа

а) $v=0.01$; б) $v=0.03$; в) $v=0.05$; г) $v=0.07$; д) $v=0.09$

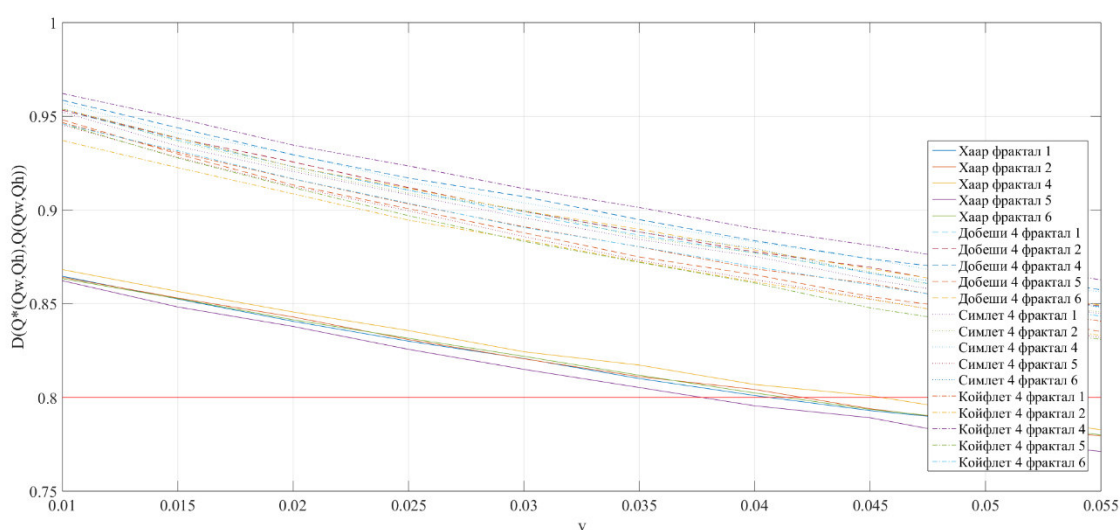


Рисунок 61 – Зависимость корреляции извлеченного и опорного ЦВЗ от дисперсии мультипликативного шума

Анализ полученных зависимостей показывает, что мультипликативный шум оказывает большее деструктивное воздействие по сравнению с другими видами шума. При использовании вейвлета Хаара для всех типов фракталов среднее значение корреляции опускается ниже заданного порога при дисперсии мультипликативного шума, превышающей значение 0.035.

На рисунке 62 представлены результаты извлечения ЦВЗ при фильтрации

стегоконтейнера. На рисунке 63 представлена зависимость корреляции извлеченного и опорного ЦВЗ от размера маски.

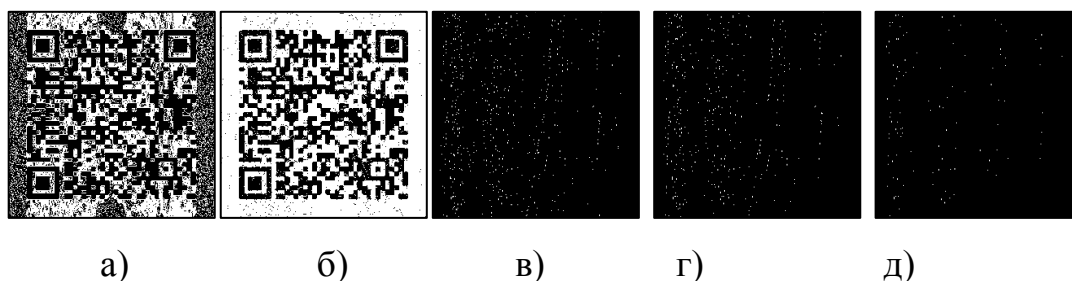


Рисунок 62 – Результаты извлечения ЦВЗ при воздействии усредняющего фильтра на заполненный контейнер с различным размером маски h при использовании фрактального контейнера 1-го типа

а) $h=2$; б) $h=3$; в) $h=5$; г) $h=7$; д) $h=9$

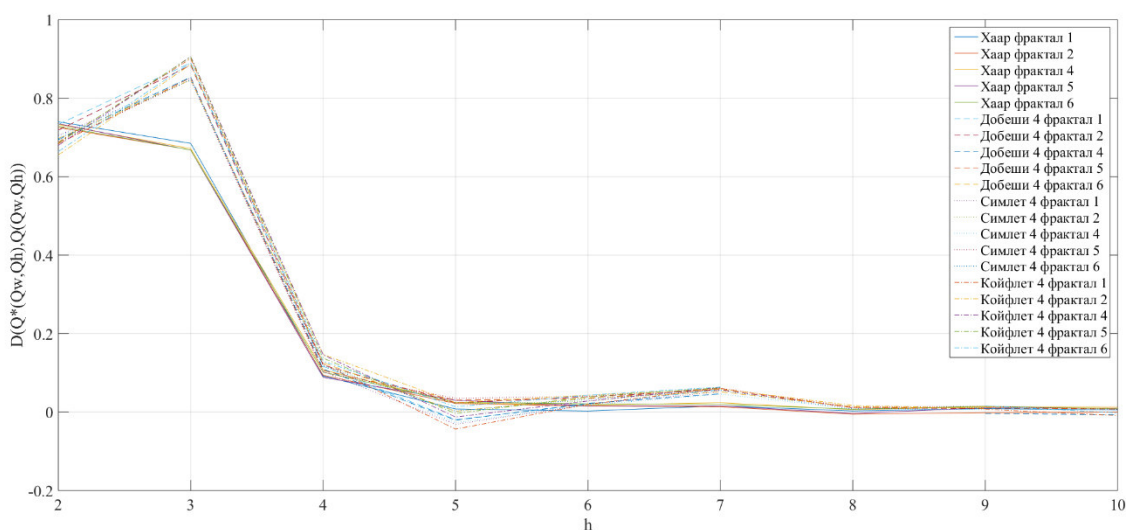


Рисунок 63 – Зависимость вероятности ошибки извлечения ЦВЗ от размера маски усредняющего фильтра

Как видно из полученных зависимостей алгоритм А2 позволяет достичь заданного качества извлечения только при воздействии усредняющего фильтра с маской 3×3 и вейвлет-преобразований Добеши 4, Симлет 4 и Койфлет 4.

На рисунке 64 показаны результаты извлечения ЦВЗ при различном уровне сжатия. На рисунке 65 представлена зависимость корреляции извлеченного и опорного ЦВЗ от уровня сжатия JPEG.

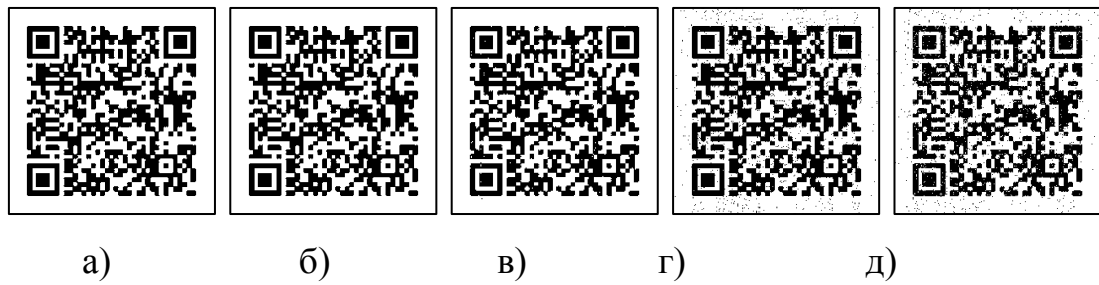


Рисунок 64 – Результаты извлечения ЦВЗ при воздействии JPEG сжатия различного уровня на заполненный контейнер при использовании фрактального контейнера 1-го типа и вейвлет разложения Хаара
а) 0% ; б) 10% ; в) 20% ; г) 30% ; д) 50%

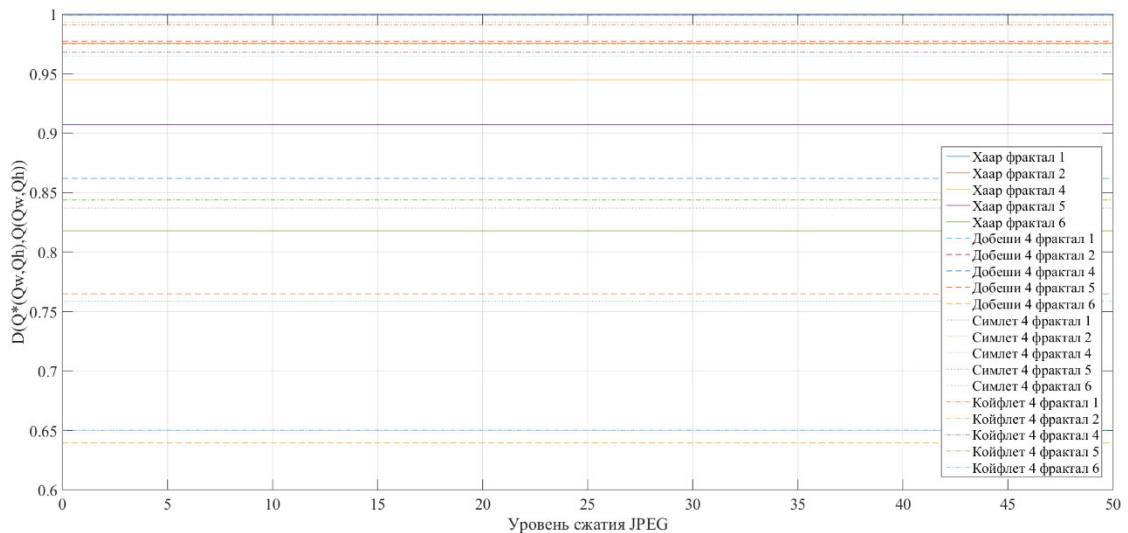


Рисунок 65 – Зависимость корреляции извлеченного и опорного ЦВЗ от уровня сжатия JPEG

Как видно на качество извлечения при воздействии сжатия JPEG влияют тип вейвлета и тип фрактала. 4 комбинации этих параметров из 20 (Добеши 4 фрактал 6-го типа, Койфлет 4 фрактал 6-го типа, Симлет 4 фрактал 4-го типа и Добеши 4 фрактал 4-го типа) не могут обеспечить заданную корреляцию извлеченного и опорного ЦВЗ при воздействии сжатия.

Получилось, что использование алгоритма A2 позволяет повсеместно обеспечить высокое качество извлечения при воздействии гауссовского и импульсного шума. Наибольшая устойчивость к мультипликативному шуму достигается при

использовании вейвлетов Добеши 4, Симлет 4 и Койфлет 4. При использовании вейвлета Хаара заданное качество достигается при воздействии мультипликативного шума с дисперсией $\sigma^2 < 0,035$. При воздействии усредняющего фильтра с маской 3x3 и сжатия JPEG $\leq 50\%$ заданное качество извлечения достигается для более чем 80% рассматриваемых комбинаций «тип фрактала - тип вейвлета».

4.2 Исследование устойчивости алгоритма АЗ

В качестве водяного знака в данном алгоритме используется ПСП, однозначно определяющая владельца цифрового контента. По сравнению с ЦВЗ в виде изображения в рассматриваемом случае пороговое значение корреляции извлеченного и опорного ПСП, было установлено в значении 0.95.

На рисунке 66 показана зависимость $V_{\text{ПСП}}(i=0)$ от дисперсии гауссовского шума.

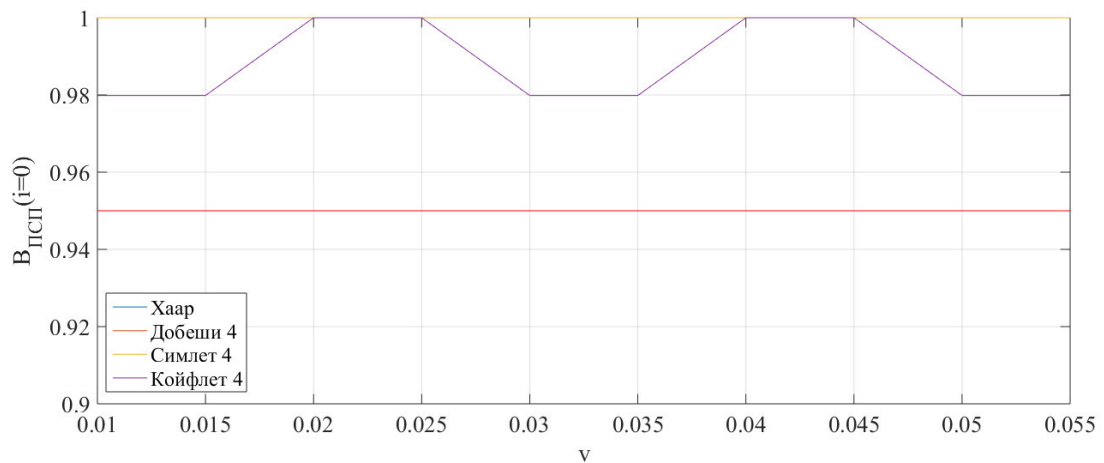


Рисунок 66 – Зависимость $V_{\text{ПСП}}(i=0)$ от дисперсии гауссовского шума

Из представленных зависимостей можно видеть, что всех рассматриваемых случаях была достигнуто пороговое значение корреляции. Для вейвлет-разложений Хаара, Добеши 4 и Симлет 4 значение корреляции сохранялось одинаковым на протяжении всего эксперимента. При использовании вейвлет-разложения Койфлет 4 можно наблюдать уменьшение значения корреляции на некоторых участках графика, но все полученные результаты сохраняются в пре-

делах нормы.

На рисунке 67 представлены зависимости $V_{\text{ПСП}}(i=0)$ в зависимости от интенсивности импульсного шума.

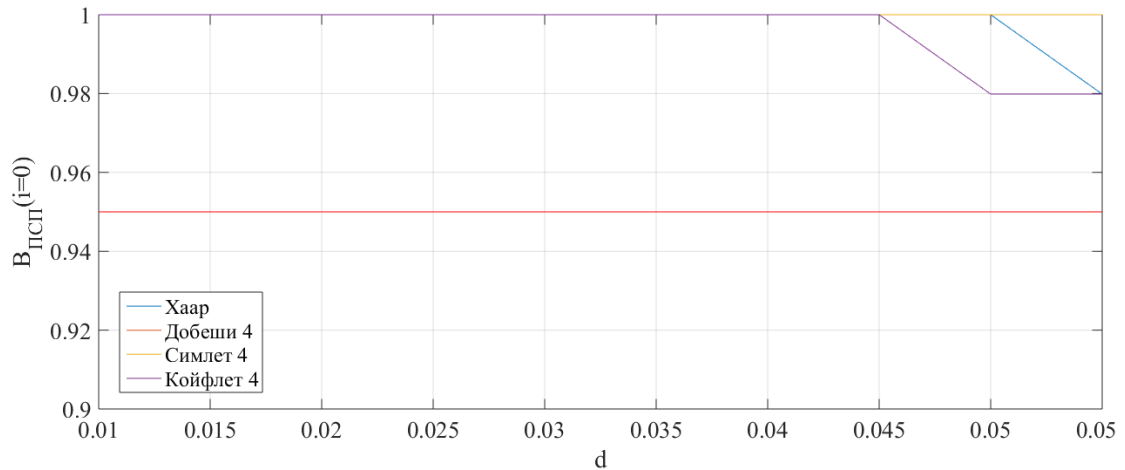


Рисунок 67 – Зависимость $V_{\text{ПСП}}(i=0)$ от интенсивности импульсного шума

Из представленных зависимостей можно видеть, что импульсный шум способствует возникновению ошибок при интенсивности $d \geq 0.45$. Однако все полученные значения корреляции превышают заданный порог.

На рисунке 68 представлена зависимость $V_{\text{ПСП}}(i=0)$ от дисперсии мультипликативного шума.

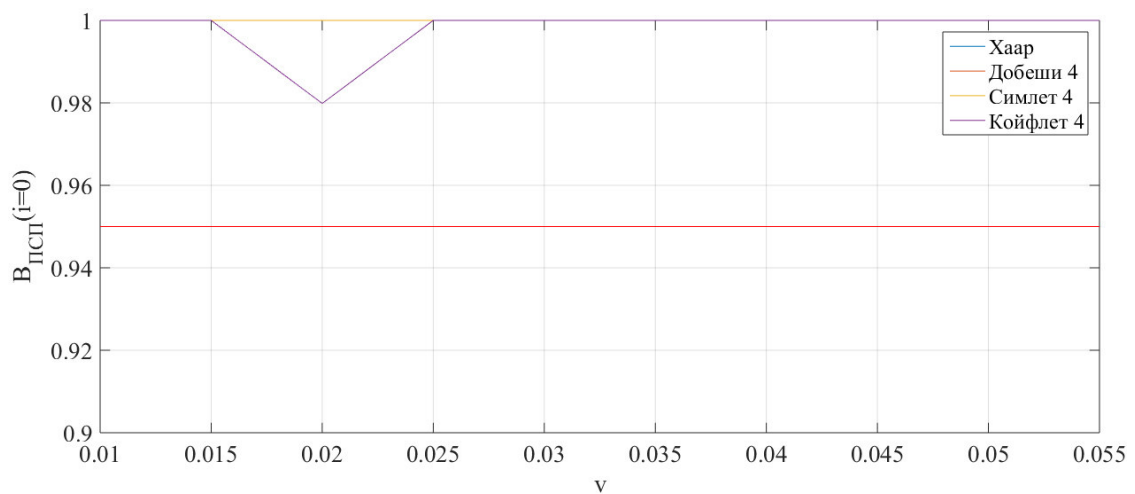


Рисунок 68 – Зависимость $V_{\text{ПСП}}(i=0)$ от дисперсии мультипликативного шума

На полученных зависимостях можно наблюдать только один спад на графиче-

ках: при $v=0.02$ и вейвлет разложения Койфлет 4. В остальных случаях полученное значение корреляции достигало максимального значения, равному 1.

На рисунке 70 представлена зависимость $V_{\text{ПСП}}(i=0)$ от размера маски усредняющего фильтра.

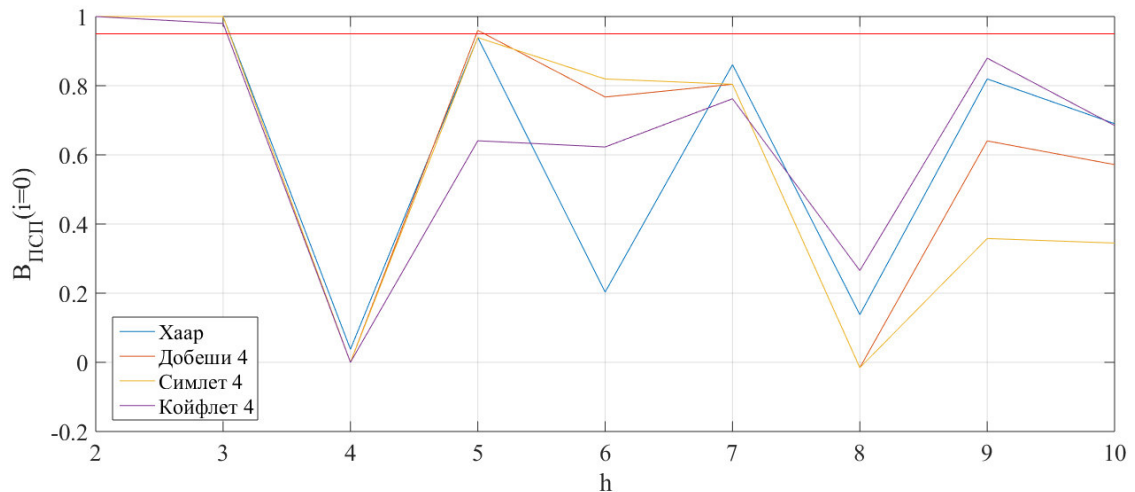


Рисунок 69 – Зависимость $V_{\text{ПСП}}(i=0)$ от размера усредняющего фильтра

Заданное пороговое значение корреляции было получено при воздействии усредняющего фильтра с маской 2x2 и 3x3, а также при маске 5x5 и вейвлет преобразования Добеши 4.

На рисунке 71 представлена зависимость $V_{\text{ПСП}}(i=0)$ от уровня сжатия JPEG.

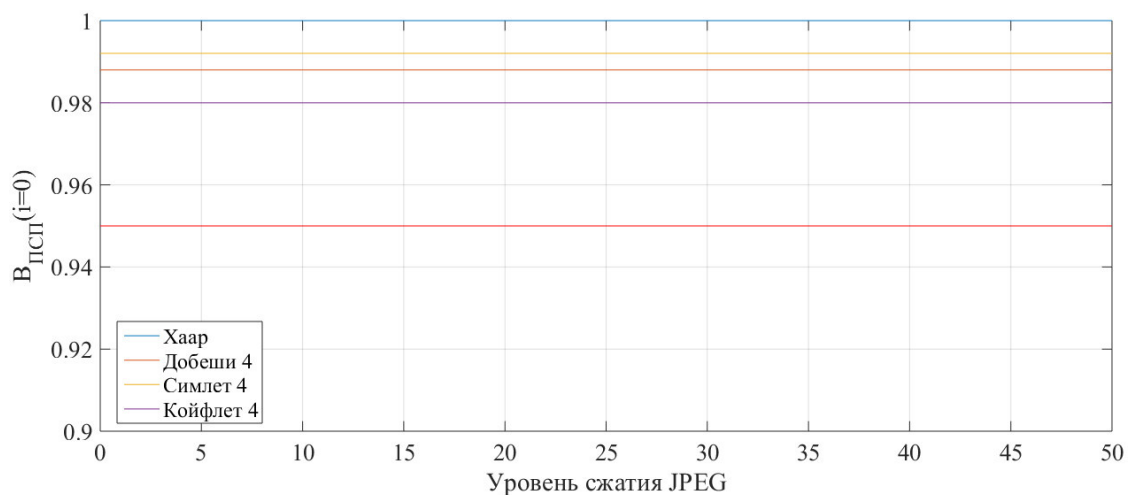


Рисунок 70 – Зависимость $V_{\text{ПСП}}(i=0)$ от уровня сжатия JPEG

По полученным зависимостям можно наблюдать то, что заданная корреляция была получена во всех рассматриваемых случаях. Наилучшие результаты по-

лучены при использовании вейвлет-разложения Хаара, худшие – при использовании Койфлет 4.

Проведенные эксперименты показывают, что использование ФГШ повышает устойчивость алгоритма А3 к атакам по сравнению с алгоритмом А2. Рассматриваемый алгоритм устойчив ко всем видам шума и сжатию JPEG без ограничений на выбор параметров алгоритма. По сравнению с алгоритмом А2 алгоритм А3 устойчив к фильтру также при размере маски 2x2.

4.3 Сравнительный анализ устойчивости предложенных алгоритмов с известными методами встраивания ЦВЗ

Для сравнения достоверности извлечения ЦВЗ в условиях воздействия атак производилось тестирование разработанных алгоритмов с использованием 20000 изображений из двух баз изображений, используемых для оценки стегосистем.

В таблице 5 представлены значения вероятности ошибки извлечения для 3 предложенных алгоритмов, а также результаты вычислений для известных методов НЗБ и алгоритма расширения спектра.

Таблица 5 – Вероятность ошибки извлечения ЦВЗ при воздействии атак

Алгоритм	Вейвлет	Фрактал	Вероятность ошибочного извлечения				
			Гауссовский шум $v=0.5$	Соль и перец $v=0.5$	Мультипликативный шум $v=0.5$	Фильтрация $h=2$	JPEG 30%
A2	Хаар	1	7,8895e-05	0,00331	0,01988	0,0342	0,006
A2	Хаар	3	0,000105	0,00344	0,02153	0,0301	0,004
A2	Хаар	4	2,6298e-05	0,00389	0,024720	0,0357	0,005
A2	Хаар	5	2,6298e-05	0,00407	0,024930	0,0294	0,005
A2	Хаар	6	7,8895e-05	0,00420	0,023879	0,0309	0,005
A2	Добеш 4	1	$<10^{-3}$	0,01036	0,003681	0,0123	0,114
A2	Добеш 4	3	$<10^{-3}$	0,01070	0,004549	0,0088	0,103
A2	Добеш 4	4	$<10^{-3}$	0,00925	0,007153	0,0114	0,117
A2	Добеш 4	5	$<10^{-3}$	0,01136	0,006916	0,0132	0,104
A2	Добеш 4	6	$<10^{-3}$	0,00796	0,006548	0,0110	0,119
A2	Симлет 4	1	$<10^{-3}$	0,00578	0,003208	0,0112	0,084
A2	Симлет 4	3	$<10^{-3}$	0,00662	0,003839	0,0087	0,087
A2	Симлет 4	4	$<10^{-3}$	0,00581	0,005207	0,0110	0,08
A2	Симлет 4	5	$<10^{-3}$	0,00691	0,005207	0,0111	0,087
A2	Симлет 4	6	$<10^{-3}$	0,00552	0,005443	0,0097	0,081
A2	Койфлет 4	1	$<10^{-3}$	0,00749	0,003024	0,0410	0,019
A2	Койфлет 4	3	$<10^{-3}$	0,00796	0,004996	0,0397	0,021
A2	Койфлет 4	4	2,6298e-05	0,00767	0,005706	0,0418	0,021

A2	Койфлет 4	5	$<10^{-3}$	0,00807	0,004996	0,0449	0,019
A2	Койфлет 4	6	$<10^{-3}$	0,00857	0,005259	0,0421	0,019
A3	Хаар		$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$	0,006
A3	Добеш 4		0,004	0,004	0,004	0,006	0,1
A3	Симлет 4		0,004	0,004	0,004	0,004	0,002
A3	Койфлет 4		0,012	0,012	0,012	0,008	0,049
Э1			$<10^{-3}$	0,001	$<10^{-3}$	0,069	0,065

Из таблицы видно, что наименьшие значения вероятности ошибки наблюдаются при использовании алгоритма A3 в комбинации с вейвлет разложением Хаара. Полученные значения на 3 порядка ниже, чем у эталона Э2, при воздействии усредняющего фильтра и на 1 порядок выше при воздействии сжатия JPEG.

4.4 Выводы

1. Произведен сравнительный анализ устойчивости разработанных алгоритмов к воздействию атак на основе анализа 20000 изображений.

2. Показано, что использование алгоритма A2 позволяет повсеместно обеспечить высокое качество извлечения при воздействии гауссовского и импульсного шума. Наивысшая устойчивость к мультипликативному шуму достигается при использовании вейвлетов Добеш 4, Симлет 4 и Койфлет 4. При использовании вейвлета Хаара заданное качество достигается при воздействии мультипликативного шума с дисперсией $\sigma^2 < 0,035$. При воздействии усредняющего фильтра с маской 3x3 и сжатия JPEG $\leq 50\%$ заданное качество извлечения достигается для более чем 80% рассматриваемых комбинаций «тип фрактала - тип вейвлета».

3. Показано, что Использование ФГШ дополнительно повышает устойчивость алгоритма A3 ко всем видам шума и JPEG сжатию по сравнению с алгоритмами A2 и Э1.

4. Численный эксперимент по оценке качества извлечения алгоритмов A2 и A3 в условиях шумов и атак показал, что наименьшее значение вероятности ошибки $\sim 10^{-3}$ соответствует алгоритму A3 в комбинации с вейвлет разложением Хаара.

Заключение

В результате диссертационного исследования решена актуальная научная задача и достигнута поставленная цель, заключающаяся в повышении эффективности алгоритмов защиты информации аудиосигналов и неподвижных изображений от угроз неправомерного использования квалифицированного злоумышленника путем применения технологии фрактальных процессов совместно с ДВП. Это подтверждается следующими полученными научными и практическими результатами:

1. Разработан и программно реализован новый алгоритм А1 встраивания ЦВЗ (в виде псевдослучайной последовательности) в аудиофайлы с использованием ДВП и одномерного ФГШ, обеспечивающий защиту аудиоконтента от угроз неправомерного использования аудиоконтента. Для достижения высокого качества и достоверности «слепого» извлечения встраиваемой информации ПСП на уровне 10^{-3} используются коэффициенты ДВП Хаара со значениями масштабирующего коэффициента в диапазоне $\alpha \in [10^{-4}; 10^{-2}]$. Достоверность извлечения при $L = 1000$ для аудио класса 1 достигается при длительности ФГШ ≥ 500 , выборе показателей Хёрста $H_0 = 0.5$ и $H_1 \in [0.6; 0.95]$.

2. Разработан и программно реализован новый фрактальный алгоритм А2 и соответствующее программное обеспечение для встраивания ЦВЗ в неподвижные изображения с использованием двухкомпонентного контейнера с добавлением 2ДДВП, обеспечивающий повышенную достоверность извлечения при воздействии атак и угроз неправомерного использования квалифицированным злоумышленником.

Наибольший объем встраиваемой информации достигается при использовании в качестве алгебраического фрактала множества Жюлиа с одним аттрактором. Наилучший баланс между качеством встраивания и качеством извлечения дости-

гается при замене диагональных коэффициентов второго уровня 2D ДВП и использования вейвлетов Симлет 4.

4. Разработан и программно реализован новый алгоритм А3 встраивания ЦВЗ в неподвижные изображения в виде ПСП на основе двумерного ФГШ и 2ДДВП. Наилучший баланс между качествами оригинального изображения и извлечения ЦВЗ достигается при замене диагональных и горизонтальных коэффициентов первого или второго уровня вейвлет-разложения на реализации фрактального шума с разной размерностью. Наименьшие ошибки извлечения наблюдаются при использовании вейвлета Койфлет 4, наибольшие – при использовании вейвлета Хаара.

4. Численный расчёт и экспериментальные результаты качества извлечения ЦВЗ при воздействии ряда атак показали, что наименьшие значения вероятности ошибки $\sim 10^{-3}$ имеют место при использовании алгоритма А3 в комбинации с вейвлет разложением Хаара. Преимуществом алгоритма А3 по сравнению с алгоритмом А2 является более высокий и независимый от параметров фракталов возможный объем встраивания. Алгоритм А3 рекомендуется использовать в случаях, когда необходимо встроить ЦВЗ заданного объема или при высокой вероятности возникновения мешающих воздействий.

5. Разработано специальное программное обеспечение, реализующее технологию фрактального метода маркировки аудио сигналов с использованием коэффициентов вейвлет разложения, защищённое в ФИПС РФ.

6. Результаты проведённых диссертационных исследований могут найти применение:

- при оценке угроз неправомерного использования аналогичных систем защиты авторских прав на цифровые объекты интеллектуальной собственности;
- для обеспечения эффективности существующих и разрабатываемых алгоритмов защиты информации от неправомерного использования в условиях воздействия помех и внешних атак квалифицированных злоумышленников.

Список сокращений и условных обозначений

БПФ – быстрое преобразование Фурье

ВЧ – высокочастотный

ДВП – дискретное вейвлет-преобразование

ДКП – дискретное косинусное преобразование

ЗСЧ – зрительная система человека

НЗБ – наименее значащие биты

НЧ – низкочастотный

ПСП – псевдослучайная последовательность

ССЧ – слуховая система человека

ФГШ – фрактальный гауссовский шум

ФР – фрактальная размерность

ЦВЗ – цифровой водяной знак

Список использованных источников

1. Аргументы и факты: издательский дом [сайт] – Москва, 1997. – Обновляется в течение суток. – URL: https://aif.ru/culture/art/nft_ili_steganografiya_na_rynke_cifrovogo_iskusstva_stanovitsya_zharko (дата обращения: 03.09.2021). – Текст: электронный.
2. Sanivarapu P.V. Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques / Sanivarapu P.V., Rajesh K.N.V.P.S., Hosny K.M., Fouda M.M. // Applied Science. - 2022. – no. 12. – P. 1-13.
3. Sowmya S. Protection of data using image watermarking technique / Sowmya S., Karanth S., Kumar S. // Global Transitions Proceedings. – 2021. – no. 2 – P. 386-391.
4. Wadhera S. A Comprehensive Review on Digital Image Watermarking / Wadhera S., Kamrac D., Rajpal A., Jain A., Jain V. // Workshop on Computer Networks & Communications. – 2021. – P. 126-143.
5. Pei L. Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition / Pei L. // Journal of Mathematics. – 2022. – P. 1-10.
6. Agarwal, S. Secure image transmission using fractal and 2D-chaotic map. / Agarwal, S. // Journal of Imaging. - 2018 – no. 4. – P. 1-17.
7. Gupta S. Image encryption techniques using fractal geometry: A comparative study / Gupta S., Bansal N. // IOSR Journal of Computer Engineering. - 2014 – no. 16. – P. 31–35.
8. Шелухин, О. И. Анализ методов измерения фрактальной размерности цветных и черно-белых изображений / О. И. Шелухин, Д. И. Магомедова //

Наукоемкие технологии в космических исследованиях Земли. – 2017. – Т. 9, № 6. – С. 6-16.

9. Шелухин, О. И. Скрытие информации в аудиосигналах с использованием детерминированного хаоса / О. И. Шелухин, С. Ю. Рыбаков, Д. И. Магомедова // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13, № 1. – С. 80-91. – DOI 10.36724/2409-5419-2021-13-1-80-91.

10. Магомедова, Д. И. Маркировка неподвижных изображений с использованием фрактального гауссовского шума и двумерного дискретного вейвлет преобразования для защиты авторских прав / Д. И. Магомедова // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14, № 6. – С. 20-26. – DOI 10.36724/2409-5419-2022-14-6-20-26.

11. Magomedova, D.I. Fractal Models and Algorithms for Creating a Protective Marking for Integrity and Authenticity Bitmap Images / D.I. Magomedova, O.I. Sheluhin // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2020. – 2020. – Article no 9166069. – DOI 10.1109/SYNCHROINFO49631.2020.9166069.

12. Sheluhin, O.I. Data Hiding and Transmission over Occupied Audio Channels Using Deterministic Chaos / O.I. Sheluhin, D.I. Magomedova, S.Y. Rybakov // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings. – 2021. – Article no 9415979. – DOI 10.1109/IEEECONF51389.2021.9415979.

13. Marking audio signals using fractal gaussian noise / O. I. Sheluhin, D. I. Magomedova, S. Y. Rybakov, A. G. Simonyan // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 - Conference Proceedings. – 2021. – Article no 9488381. – DOI 10.1109/SYNCHROINFO51390.2021.9488381.

14. Sheluhin, O.I. Forecasting the State of Infocommunication Systems Using Time Series with Defined Fractal Properties / O.I. Sheluhin, M.V. Polkovnikov, D.I.

Magomedova // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2020. – 2020. – Article no 9166054. – DOI 10.1109/SYNCHROINFO49631.2020.9166054.

15. Шелухин, О. И. Оценка влияния встраивания водяных знаков на фрактальную размерность стеганограмм / О. И. Шелухин, Д. И. Магомедова // Телекоммуникационные и вычислительные системы - 2017: Труды международной научно-технической конференции, Москва, 22 ноября 2017 года. – Москва: Научно-техническое издательство "Горячая линия-Телеком", 2017. – С. 206-207.

16. Шелухин, О. И. Использование алгебраических фракталов в качестве секретных ключей при внедрении водяных знаков в изображения стеганографическими методами / О. И. Шелухин, Д. И. Магомедова // Фундаментальные проблемы радиоэлектронного приборостроения. – 2018. – Т. 18, № 4. – С. 1066-1070.

17. Магомедова, Д. И. Использование алгебраических фракталов для защиты информации стеганографическими методами от несанкционированных воздействий / Д. И. Магомедова, А. Г. Симонян, М. А. Смычек // Вестник НГИЭИ. – 2018. – № 8(87). – С. 5-15.

18. Шелухин, О. И. Исследование методов встраивания и обнаружения стеговложений в неподвижные изображения с использованием алгебраических фракталов / О. И. Шелухин, Д. И. Магомедова // XII Международная научно-техническая конференция "Технологии информационного общества", 14-15 марта 2018 г. : сборник трудов : [в 2 т.]. Т. 2. – Москва : Медиа пабlishер, 2018. – С. 22-23.

19. Магомедова, Д. И. Повышение стойкости стеганографических алгоритмов при использовании фрактальных ключей / Д. И. Магомедова // Безопасные информационные технологии : девятая всероссийская научно-техническая конференция, (Москва, 4-5 декабря 2018 года) : сборник трудов конференции. – Москва : МГТУ им. Н. Э. Баумана : НУК "Информатика и системы управления", 2018. – С. 119-123.

20. Sheluhin, O. Image Steganography Technique Using Algebraic Fractals / O. Sheluhin, D. Magomedova // Conference of Open Innovations Association, FRUCT. – 2019. – No. 24. – P. 716-721.

21. Магомедова, Д. И. Фрактальные модели и алгоритмы создания защитной маркировки для обеспечения целостности и аутентичности растровых изображений / Д. И. Магомедова, О. И. Шелухин // Системы синхронизации, формирования и обработки сигналов. – 2020. – Т. 11, № 1. – С. 57-67.

22. Свидетельство о государственной регистрации программы для ЭВМ № 2021618262 Российская Федерация. Фрактальный метод маркировки аудиосигналов с использованием коэффициентов вейвлет разложения : № 2021616964 : заявл. 11.05.2021 : опубл. 25.05.2021 / О. И. Шелухин, Д. И. Магомедова, С. Ю. Рыбаков ; заявитель Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики».

23. Свидетельство о государственной регистрации программы для ЭВМ № 2019666989 Российская Федерация. Программа для вычисления фрактальной размерности изображений : № 2019665963 : заявл. 29.11.2019 : опубл. 17.12.2019 / О. И. Шелухин, Д. И. Магомедова ; заявитель Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ).

24. В России выросло число исков по авторским правам на фотографии. — Текст: электронный // Правову: [сайт]. — URL: <https://pravo.ru/news/237129/> (дата обращения: 22.12.2021).

25. Анализ судебной практики за 2020 год по спорам, связанным с защитой авторских прав на фотографические произведения, размещенные в сети «Интернет». — Текст: электронный // RTM Group: [сайт]. — URL:

<https://rtmtech.ru/research/analiz-sudebnoj-praktiki-za-2020-g-zashhita-avtorskih-prav-na-foto/> (дата обращения: 22.12.2021).

26. Tao H. Robust Image Watermarking Theories and Techniques: A Review / Tao H., Chongmin L., Zain J.M., Abdalla A.N. // Elsevier. – 2014. – no. 12. – P. 122 – 138.
27. Zhang Y. A framework of adaptive steganography resisting JPEG compression and detection / Zhang Y., Luo X., Yang C., Ye D., Liu F. // Secur. Commun. Netw. — 2016. —vol. 9, no. 15. — P. 2957–71.
28. Asikuzzaman M. An overview of digital video watermarking / Asikuzzaman M., Pickering M.R. // IEEE Trans. Circuits Syst. Video Technol. – 2018. - vol. 28, no. 9 – P. 2131 – 2153.
29. Шелухин О.И. Стеганография. Алгоритмы и программная реализация / Шелухин О.И., Канаев С.Д. – Горячая линия Телеком – М, 2018 – 592 с.
30. Bender W. Techniques for Data Hiding / Bender W., Gruhl D., Morimoto N., Lu A. // IBM Systems Journal. – 1996. – no. 35. - P. 313-336.
31. Rawat C. S. A Hybrid Image Compression Scheme using DCT and Fractal Image Compression / Rawat C. S., Meher S. // The International Arab Journal of Information Technology. – 2013. – vol. 10, no. 6. – P. 553-562.
32. Thamizhchelvy K. A Novel Approach to Generate Fractal Images Using Chaos Theory / Thamizhchelvy K. // Indian Journal of Computer Science and Engineering. – 2014. - vol. 5, no. 4. - P. 152–157.
33. Wu Y. Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform / Wu Y., Noonan J.P. // International Journal of Innovation, Management and Technology. – 2012. – vol.3, no.3. – P.285 – 289.
34. Garg A. An Improved Algorithm of Fractal Image Compression / Garg A. // International Journal of Computer Applications. – 2011. – vol.34, no.2 – P. 17-21.
35. Шелухин О.И. Мультифракталы. Инфокоммуникационные приложения - Горячая линия — Телеком — М, 2011 – 562 с.

36. Мандельброт Б. Фрактальная геометрия природы. — Москва: Институт компьютерных исследований, 2002 - 656 с.
37. Шредер М. Фракталы, хаос, степенные законы – Ижевск: Издательство «Регулярная и хаотическая динамика» (РХД), 2005 – 528 с.
38. Множество Мандельброта [Электронный ресурс]: Википедия. Свободная библиотека – Режим доступа: https://ru.wikipedia.org/wiki/Множество_Мандельброта (дата обращения: 24.07.2022).
39. Деменок С.Л. Фрактал: между мифом и ремеслом - Санкт-Петербург: Ринвол Академия исследования культуры, 2011 – 296 с.
40. Channapragada R.S.R. Digital Watermarking Using Fractal Coding / Channapragada R.S.R., Prasad M.V.N.K. // Intelligent Systems and Computing. - 2015 – P. 1 -10.
41. Awarayi N. S. A Digital Image Watermarking Using Dwt and Lshaped Tromino Fractal Encryption / Awarayi N.S., Appiah O., Weyori B.A., Ninfaakang C.B. // I.J. Image, Graphics and Signal Processing. - 2021 – P. 33-43.
42. Kiani K. A new fractal watermarking method for images of text / Kiani K., Mousavi A., Shamshirband S. // International Journal of Advanced Intelligence Paradigms. – 2019. – P. 207-219.
43. Sun T. Medical image security authentication method based on wavelet reconstruction and fractal dimension / Sun T, Wang X, Lin D // International Journal of Distributed Sensor Networks. – 2021. – no. 17(4). – P. 1-10.
44. Caballero-Hernandez, H. Steganographic Method to Data Hiding in RGB Images Using Pixels Redistribution Combining Fractal-Based Coding and DWT. / Caballero-Hernandez, H., Muñoz-Jimenez, V., Ramos, M.A. // Intelligent Computing. Lecture Notes in Networks and Systems. – 2021. – P. 1-18.
45. Ali A.H. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain / Ali A.H., George L.E.,

Zaidan A.A., Mokhtar M.R. // *Multimedia Tools and Applications*. – 2018. – P. 31487–31516.

46. Zhang X. A Coverless Image Information Hiding Algorithm Based on Fractal Theory / Zhang X., Peng F., Lin Z. // *International Journal of Bifurcation and Chaos*. - 2020. – P. 1-20.

47. Alia M. Improved Steganography Scheme based on Fractal Set / Alia M., Suwais K. // *The International Arab Journal of Information Technology*. – 2020. – P. 128-136.

48. Durafe A. Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover / Durafe A., Patidar V. // *Journal of King Saud University Computer and Information Sciences*. – 2020. – P. 1-16.

49. Masood F. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map / Masood F., Ahmad J., Shah S.A., Jamal S.S., Hussain I. // *Entropy*. – 2020. – P. 1-28.

50. Barni M. ADWT-based technique for spatio-frequency masking of digital signatures. / Barni M., Bartolini F., Cappellini V., Lippi A., Piva A. // In Ping Wah Wong, editor, *Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents*. – 1999. – P. 357-372.

51. Kim J.R. A robust wavelet-based digital watermark using level adaptive thresholding / Kim J.R., Moon Y.S. // *Proceedings of the 6th IEEE International Conference on Image Processing, ICIP '99*. – 1999. – P. 226-230.

52. Kim Y.-S. Wavelet based watermarking method for digital images using the human visual system / Kim Y.-S., Kwon O.-H., Park R.-H. // *Electronic Letters*. - 1999. – P. 466–467.

53. Kundur D. A robust digital image watermarking method using wavelet-based fusion / Kundur D., Hatzinakos D. // *Proceedings of the IEEE International Conference on Image Processing, ICIP '97*. – 1997. – P. 544–547.

54. Kundur D. Digital watermarking using multiresolution wavelet decomposition / Kundur D., Hatzinakos D. // Proceedings of IEEE ICASSP '98. - 1998. - P. 2969–2972.
55. Kundur D. Towards a telltale watermarking technique for tamperproofing / Kundur D., Hatzinakos D. // Proceedings of the IEEE International Conference on Image Processing, ICIP'98. - 1998. – P. 409–413.
56. Corvi M. Wavelet-based image watermarking for copyright protection. / Corvi M., Nicchiotti. G. // In Scandinavian Conference on Image Analysis, SCIA '97, Lappeenranta, Finland. - 1997. – P. 157.
57. Abbasi M. Color Image Steganography using Dual Wavelet Transforms // International Journal of Computer Applications. – 2019. – P. 32-38.
58. Pan P. Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage / Pan P., Wu Z., Yang C., Zhao B. // Entropy. – 2022. - P. 1-21.
59. Fakhredanesh M. Steganography in discrete wavelet transform based on human visual system and cover model / Fakhredanesh M., Rahmati M., Safabakhsh R. // Multimedia Tools and Applications. – 2019. - P. 18475–18502.
60. Tushara M. Image Steganography Using Discrete Wavelet Transform – A Review / M. Tushara, K.A. Navas // International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. – 2016. – P. 207-212.
61. Harbi S.J. Steganography Based Human Skin Using Wavelet Transformation in RGB Image / J.S. Harbi, Z.N. Nabeel // International Letters of Chemistry, Physics and Astronomy. – 2015. – vol.52 – P.84-89.
62. Rajini G-K. A Fractional Random Wavelet Transform Based Image Steganography / Rajini G-K, Ramachandra Reddy G // Research Journal of Applied Sciences, Engineering and Technology. - 2015. – P. 943-951.

63. Pilania U. An ROI-based robust video steganography technique using SVD in wavelet domain / Pilania U., Tanwar R., Gupta P. // Open Computer Science. – 2022. – P. 1-16.
64. Taha N.A. Steganography using dual tree complex wavelet transform with LSB indicator technique / N.A. Taha, Z. Qasim, A. Al-Saffar, A. Abdullatif // Periodicals of Engineering and Natural Sciences. – 2021. – P. 1106-1114.
65. Седов А.В. Двумерное вейвлет-преобразование в задачах краткосрочного анализа и моделирования нагрузок энергосистем / Седов А.В., Тришечкин Е.В. // Вестник южного научного центра РАН, 2011 - Том 7, № 2 – сс. 15-21.
66. Кочкарев А.И. Исследование и разработка многобитовых систем цифровых «водяных» знаков в условиях возможных атак: диссертация на соискание ученой степени кандидата технических наук: 05.12.13 / Кочкарев Александр Игоревич; [Место защиты: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича] – Санкт-Петербург, 2019 – 140 с.
67. Коржик, В. И. Цифровая стеганография и цифровые водяные знаки. Часть 2 Цифровые водяные знаки / В.И. Коржик, С.О. Анфиногенов, А.И. Кочкарев, И.А. Федянин, А.Г. Жувикин, Д.А. Флакман, В.Г. Алексеев. – СПбГУТ. – СПб, 2017.
68. Шакурский М.В. Инвариантные системы стеганографической защиты информации в реальном времени с использованием двухкомпонентных контейнеров: диссертация на соискание ученой степени доктора технических наук: 05.13.19 / Шакурский Максим Викторович; [Место защиты: Уфимский государственный авиационный технический университет] – Самара, 2021 – 343 с.
69. Bhattacharyya A. On a measure of divergence between two statistical populations defined by their probability distributions// Bulletin of the Calcutta Mathematical Society. -1943. – P. 99–109.
70. Kullback S. On Information and Sufficiency / Kullback, S., Leibler, R.A. // The Annals of Mathematical Statistics. – 1951. - P. 79-86.

71. Вражнов Д.А. О качестве работы алгоритмов слежения объектов на видео / Вражнов Д.А., Шаповалов А.В., Николаев В.В. // Компьютерные Исследования и Моделирование – 2012 – т. 4 № 2 – сс. 303-313.
72. Comaniciu D. Kernel-Based Object Tracking / Comaniciu D., Ramesh V., Meer P. // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2003. - vol. 25, no. 5 – P. 564 – 577.
73. Millan G. On the Hurst Exponent, Markov Processes, and Fractional Brownian Motion // arXiv:2103.05019. - 2021. – P. 1-3.
74. McCauley J. Hurst exponents, Markov processes, and fractional Brownian motion / McCauley J., Gunarathe G.H., Bassler K.E. // Munich Personal RePEc Archive. - 2016 – 23 p.
75. Шелухин О.И. Мультифракталы. Инфокоммуникационные приложения - Горячая линия — Телеком — М, 2011 – 562 с.
76. Skodras A. Discrete Wavelet Transform: An Introduction // Hellenic Open University: Technical Report HOU-CS-TR-2003-02-EN. – 2015. – P. 1-26.
77. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления свертки. — Радио и связь – М, 1985 – 248 с.
78. Wang Y. Generating fractal rough surfaces with the spectral representation method / Wang Y., Azam A., Wilson M. CT. , Neville A., Morina A. // Proceedings of the Institution of Mechanical Engineers, Part J: Journal of Engineering Tribology. - 2021 – P. 2640-2653.
79. Molz F.J. Fractional Brownian motion and fractional Gaussian noise in subsurface hydrology: A review, presentation of fundamental properties, and extensions / Molz F.J., Liu H.H. // Water Resources Research. – 1997. - vol. 33, no. 10 – P. 2273-2286.
80. Ceballos R.F. On The Estimation of the Hurst Exponent Using Adjusted Rescaled Range Analysis, Detrended Fluctuation Analysis and Variance Time Plot: A

Case of Exponential Distribution // Ceballos R.F., Largo F.F. // Imperial Journal of Interdisciplinary Research. - 2017. – vol. 3. – P. 424-434.

81. Аккафу Аду, Г. Д. Оценка качества аудиофайла после вложения информации в блоки наименьших значащих бит / Г. Д. Аккафу Аду, К. А. Ахрамеева, Е. Ю. Герлинг // Региональная информатика и информационная безопасность : Сборник трудов конференций: Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 28–30 ноября 2020 года. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2020. – С. 240-244.

82. Mazdak Z. Mazdak Technique for PSNR Estimation in Audio Steganography / Mazdak Z., Azizah Bt A.M., Shahidan M.A., Saman S.C. // Applied Mechanics and Materials Vols 229-231. – 2012. – P. 2798 – 2803

83. Haar A. On Theory of Orthogonal Functional Systems // Mathematische Annalen. – 1910. – P. 331-371.

84. Daubechies I. Ten Lectures on Wavelets // SIAM. – 1992. - p. 194.

85. Daubechles I. Orthonormal Bases of Compactly Supported Wavelets // Fundamental Papers in Wavelet Theory. Princeton University Press. - 2019. - P. 564–652.

86. Beylkin G. Fast wavelet transforms and numerical algorithms / G. Beylkin, R. Coifman, V. Rokhlin // Comm. Pure Appl. Math., 44. – 1991. - P. 141–183.

87. Zhang H. A steganography based on fractal images / Zhang H.A., Hu J., Wang G., Zhang Y. // 2011 Second International Conference on Networking and Distributed Computing. – 2011. – P. 28-31.

88. Arfat B. Steganography Based on Fractal Set / Arfat B., Mhatre R. // International Journal of Scientific & Engineering Research. – 2021. – vol. 12. , iss. 3. – P. 243-246.

89. Sisson P.D. Fractal art using variations on escape time algorithms in the complex plane // Journal of Mathematics and the Arts. – 2007. – vol. 1. - P. 41-45.
90. Aslan N. A different construction of the classical fractals via the escape time algorithm / Aslan N., Saltan M., Demir B. // Journal of Abstract and Computational Mathematics. – 2018. - P.1-15.
91. Bas P. Break our steganographic system. The ins and outs of organizing BOSS / Bas P., Filler T., Pevn'ý T. // LNCS. – 2011. – P. 59 - 70.
92. Abdulrahman H. Color Image Steganalysis Based on Steerable Gaussian Filters Bank / Abdulrahman H., Chaumont M., Montesinos P., Magnier B. // IH&MMSec'2016, in Proceedings of the 4th ACM workshop on Information Hiding and Multimedia Security. – 2016. – P. 1-6.
93. Chernoff H. The use of maximum likelihood estimates in χ^2 test for goodness of fit (англ.) / Chernoff H., Lehmann E. L. // The Annals of Mathematical Statistics. — 1954. — Vol. 25. — P. 579—586.

Приложение А. Акты о внедрении и использовании результатов диссертационной работы



Общество с ограниченной ответственностью «Альфа́нова»

117393, г. Москва ул. Профсоюзная, д.56 этаж 3, помещение XIX, комн.80

тел.+7(903)275-48-98, alphanova@inbox.ru

ОГРН 1207700200828, ИНН 9728005508/КПП 772801001

Р/с 40702810212010843499 в Филиал «Корпоративный» ПАО «СОВКОМБАНК» (г. Москва)

БИК 044525360, к/с 30101810445250000360

Исх. №28/5 от «12» октября 2022 г.

«УТВЕРЖДАЮ»



Генеральный директор
ООО «Альфа́нова»
/В.А. Иванов/

А К Т

о внедрении результатов диссертационной работы

Магомедовой Д.И.

«Маркировка неподвижных изображений и аудио сигналов с использованием фрактальных процессов для защиты авторских прав»

Комиссия в составе:

- Председатель – исполнительный директор, к.т.н. Иванов Ю.А.
- Член комиссии:
- Начальник технического отдела – Поверин А.Г.;
- Ведущий инженер – Никитин В.А.

составила настоящий акт о том, что результаты диссертационной работы Магомедовой Д.И. «Маркировка неподвижных изображений и аудио сигналов с использованием фрактальных процессов для защиты авторских прав» используются в научно-производственной деятельности в ООО «Альфа́нова» (г. Москва), а именно:

- метод и алгоритм встраивания псевдослучайных последовательностей в звуковые сигналы с использованием фрактального гауссовского шума систем автоматизированного контроля и учета электроэнергии (АСКУЭ);
- методические рекомендации по подбору параметров алгоритма встраивания, позволяющий обеспечить незаметность встраивания и заданную достоверность извлечения информации в системах АСКУЭ.

Применение разработанных алгоритмов позволяет повысить функциональность и защищенность разрабатываемых средств автоматизированного контроля и учета электроэнергии у оптовых и индивидуальных пользователей

Председатель комиссии
Исполнительный директор, к.т.н.

_____/Ю.А. Иванов/

Члены комиссии
Начальник технического отдела

_____/А.Г. Поверин /

Ведущий инженер

_____/В.А. Никитин /

«УТВЕРЖДАЮ»

Ректор ордена Трудового Красного Знамени
федерального государственного бюджетного
образовательного учреждения высшего
образования «Московский технический
университет связи и информатики»

 С.Д. Ерохин
« 14 » октября 2022 г.

Акт об использовании в учебном процессе научных
результатов диссертационной работы Магомедовой Д.И.
«Маркировка неподвижных изображений и аудиосигналов
с использованием фрактальных процессов для защиты авторских прав»

Комиссия в составе:

— начальника отдела планирования и сопровождения учебного про-
цесса МТУСИ Кузнецовой В.А.;

— декана факультета «Кибернетика и информационная безопас-
ность» Иевлева О.П.;

— заведующего кафедрой ИБ Шелухина О.И. удостоверяет, что в
учебном процессе кафедры ИБ при чтении курса лекций и проведении
практических занятий по дисциплине «Стеганографические методы скры-
тия информации» для бакалавров направления 10.03.01 «Информационная
безопасность» используются результаты диссертационного исследования
Магомедовой Д.И., а именно: проведенный диссертантом анализ алгорит-
мов и методов встраивания ЦВЗ в изображения с использованием фрак-
тальных процессов, а также разработанные диссертантом алгоритмы, по-
лученные в диссертационном исследовании.

Начальник отдела планирования и сопро-
вождения учебного процесса МТУСИ

 В.А. Кузнецова

Декан факультета
«Кибернетика и информационная
безопасность»

 О.П. Иевлев

Заведующий кафедрой
«Информационная безопасность»,
д.т.н., профессор

 О.И. Шелухин

**Приложение Б. Свидетельства о государственной регистрации программы
для ЭВМ**

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ
№ 2021618262

**Фрактальный метод маркировки аудиосигналов с
использованием коэффициентов вейвлет разложения**

Правообладатель: *Ордена Трудового Красного Знамени
федеральное государственное бюджетное образовательное
учреждение высшего образования «Московский технический
университет связи и информатики» (МТУСИ) (RU)*

Авторы: *Шелухин Олег Иванович (RU), Магомедова Джаннет
Исламудиновна (RU), Рыбаков Сергей Юрьевич (RU)*

Заявка № **2021616964**
Дата поступления **11 мая 2021 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **25 мая 2021 г.**

Руководитель Федеральной службы
по интеллектуальной собственности


Г.П. Ивлиев



РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ

№ 2019666989

Программа для вычисления фрактальной размерности изображений

Правообладатель: *Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ) (RU)*

Авторы: *Шелухин Олег Иванович (RU),
Магомедова Джениет Исламудиновна (RU)*

Заявка № **2019665963**
Дата поступления **29 ноября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **17 декабря 2019 г.**



Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев Г.П. Ивлиев

Приложение В. Численные результаты экспериментов

В.1 Численные результаты экспериментов для алгоритма A1

Таблица 6 – Усредненные значения PSNR маркированного аудиосигнала в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар класс 1	40,74	39,37	35,40	32,08	40,74
Добеши 4 класс 1	42,22	43,68	38,12	32,24	42,22
Симлет 4 класс 1	42,19	43,71	38,14	32,15	42,19
Койфлет 4 класс 1	42,25	43,96	38,92	32,32	42,25
Хаар класс 2	35,61	32,03	29,11	26,85	26,32
Добеши 4 класс 2	39,37	34,18	30,49	26,84	27,14
Симлет 4 класс 2	39,39	34,18	30,48	26,82	27,17
Койфлет 4 класс 2	40,27	34,09	31,00	26,67	27,36
Хаар класс 3	40,09	36,53	34,33	32,33	30,95
Добеши 4 класс 3	43,74	38,13	34,99	32,91	33,20
Симлет 4 класс 3	43,74	38,00	35,42	32,64	33,18
Койфлет 4 класс 3	44,52	38,19	35,31	32,73	33,41

Таблица 7 – Усредненные значения MSE маркированного аудиосигнала в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар класс 1	1,08E-04	1,24E-04	2,91E-04	6,20E-04	7,22E-04
Добеши 4 класс 1	1,18E-04	5,60E-05	1,59E-04	5,99E-04	9,36E-04
Симлет 4 класс 1	8,07E-05	5,47E-05	1,57E-04	6,10E-04	9,17E-04
Койфлет 4 класс 1	7,78E-05	5,04E-05	1,35E-04	5,87E-04	9,74E-04
Хаар класс 2	3,03E-04	6,33E-04	1,23E-03	0,0021	0,0023
Добеши 4 класс 2	1,28E-04	3,86E-04	8,96E-04	0,0021	0,0019

Симлет 4 класс 2	1,24E-04	3,86E-04	8,96E-04	0,0021	0,0019
Койфлет 4 класс 2	1,03E-04	3,94E-04	7,96E-04	0,0022	0,0018
Хаар класс 3	1,08E-04	2,27E-04	3,70E-04	5,86E-04	8,04E-04
Добеши 4 класс 3	5,24E-05	1,59E-04	3,19E-04	5,13E-04	4,79E-04
Симлет 4 класс 3	5,56E-05	1,63E-04	2,88E-04	5,46E-04	4,81E-04
Койфлет 4 класс 3	4,50E-05	1,58E-04	2,96E-04	5,34E-04	4,56E-04

Таблица 8 – Усредненные значения $V_{\text{псп}}(i=0)$ маркированного аудиосигнала в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар класс 1	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 1	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 1	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 1	1,00	1,00	1,00	1,00	1,00
Хаар класс 2	1,00	1,00	1,00	1,00	0,92
Добеши 4 класс 2	1,00	1,00	1,00	1,00	0,92
Симлет 4 класс 2	1,00	1,00	1,00	1,00	0,92
Койфлет 4 класс 2	1,00	1,00	1,00	1,00	1,00
Хаар класс 3	1,00	0,98	0,90	0,56	0,39
Добеши 4 класс 3	0,99	0,98	0,90	0,69	0,36
Симлет 4 класс 3	0,99	0,97	0,94	0,78	0,36
Койфлет 4 класс 3	0,99	0,95	0,92	0,61	0,41

Таблица 9 – Усредненные значения PSNR маркированного аудиосигнала в зависимости от длины последовательности ФГШ

[illegible]

Таблица 10 – Усредненные значения MSE маркированного аудиосигнала в зависимости от длины последовательности ФГШ

[illegible]

Добеши 4 класс 3	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05
Симлет 4 класс 3	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05
Койфлет 4 класс 3	3,5E-05	3,5E-05	3,5E-05	3,5E-05	3,5E-05	3,5E-05	3,5E-05	3,5E-05

Таблица 11 – Усредненные значения $V_{\text{псп}}(i=0)$ маркированного аудиосигнала в зависимости от длины последовательности ФГШ

	Длина последовательности ФГШ							
	50	300	550	800	1050	1300	1550	1800
Хаар класс 1	NaN	0,99	0,99	0,98	1,00	0,99	0,99	0,96
Добеши 4 класс 1	NaN	0,99	0,99	0,98	0,99	0,97	0,99	0,96
Симлет 4 класс 1	NaN	0,99	0,99	0,97	0,99	0,96	0,99	0,96
Койфлет 4 класс 1	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Хаар класс 2	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 2	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 2	NaN	0,15	1,00	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 2	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Хаар класс 3	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 3	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 3	NaN	0,69	1,00	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 3	NaN	1,00	1,00	1,00	1,00	1,00	1,00	1,00

Таблица 12 – Усредненные значения PSNR маркированного аудиосигнала в зависимости от alpha

	alpha							
	1,0e-07	1,0e-06	1,0e-05	0,0001	0,001	0,01	0,1	1
Хаар класс 1	40,74	40,74	40,74	40,74	40,73	39,34	26,50	5,18
Добеши 4 класс 1	42,22	42,22	42,22	42,22	42,20	40,91	27,43	6,99
Симлет 4 класс 1	42,19	42,19	42,19	42,19	42,17	41,05	26,24	6,04
Койфлет 4 класс 1	42,25	42,25	42,25	42,25	42,23	41,02	27,29	7,44
Хаар класс 2	35,61	35,61	35,61	35,61	35,60	35,45	28,82	6,82

Добеши 4 класс 2	39,37	39,37	39,37	39,37	39,37	38,52	29,10	10,26
Симлет 4 класс 2	39,39	39,39	39,39	39,39	39,38	38,93	30,13	7,63
Койфлет 4 класс 2	40,27	40,27	40,27	40,27	40,26	39,69	29,08	9,58
Хаар класс 3	40,09	40,09	40,09	40,09	40,09	39,67	29,14	8,76
Добеши 4 класс 3	43,74	43,74	43,74	43,74	43,73	42,71	25,30	9,34
Симлет 4 класс 3	43,74	43,74	43,74	43,74	43,73	42,64	29,01	10,57
Койфлет 4 класс 3	44,52	44,52	44,52	44,52	44,50	42,74	28,11	9,21

Таблица 13 – Усредненные значения MSE маркированного аудиосигнала в зависимости от α

	α							
	1,0e-07	1,0e-06	1,0e-05	0,0001	0,001	0,01	0,1	1
Хаар класс 1	8,4E-05	8,4E-05	8,4E-05	8,4E-05	8,5E-05	0,000116	0,002237	0,30
Добеши 4 класс 1	6,0E-05	6,0E-05	6,0E-05	6,0E-05	6,0E-05	8,12E-05	0,001809	0,20
Симлет 4 класс 1	6,0E-05	6,0E-05	6,0E-05	6,0E-05	6,1E-05	7,85E-05	0,002374	0,25
Койфлет 4 класс 1	6,0E-05	6,0E-05	6,0E-05	6,0E-05	6,0E-05	7,9E-05	0,001865	0,18
Хаар класс 2	2,8E-04	2,8E-04	2,8E-04	2,8E-04	2,8E-04	0,000285	0,001314	0,21
Добеши 4 класс 2	1,2E-04	1,2E-04	1,2E-04	1,2E-04	1,2E-04	0,000141	0,001229	0,09
Симлет 4 класс 2	1,2E-04	1,2E-04	1,2E-04	1,2E-04	1,2E-04	0,000128	0,00097	0,17
Койфлет 4 класс 2	9,4E-05	9,4E-05	9,4E-05	9,4E-05	9,4E-05	0,000107	0,001236	0,11
Хаар класс 3	9,8E-05	9,8E-05	9,8E-05	9,8E-05	9,8E-05	0,000108	0,00122	0,13
Добеши 4 класс 3	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	5,36E-05	0,002948	0,12
Симлет 4 класс 3	4,2E-05	4,2E-05	4,2E-05	4,2E-05	4,2E-05	5,45E-05	0,001257	0,09
Койфлет 4 класс 3	3,5E-05	3,5E-05	3,5E-05	3,5E-05	3,6E-05	5,32E-05	0,001544	0,12

Таблица 14 – Усредненные значения $B_{\text{псп}}(i=0)$ маркированного аудиосигнала в зависимости от α

	α							
	1,0e-07	1,0e-06	1,0e-05	0,0001	0,001	0,01	0,1	1
Хаар класс 1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 1	0,73	0,76	0,95	1,00	1,00	1,00	1,00	1,00

Симлет 4 класс 1	0,71	0,76	0,64	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 1	0,73	0,65	0,96	1,00	1,00	1,00	1,00	1,00
Хаар класс 2	0,17	0,14	0,96	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 2	0,02	0,04	0,98	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 2	0,05	0,07	0,98	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 2	0,03	0,09	1,00	1,00	1,00	1,00	1,00	1,00
Хаар класс 3	0,09	0,88	0,95	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 3	-0,04	0,05	0,96	0,99	1,00	1,00	1,00	1,00
Симлет 4 класс 3	0,06	0,06	0,90	0,99	1,00	1,00	1,00	1,00
Койфлет 4 класс 3	-0,05	-0,05	0,95	0,99	1,00	1,00	1,00	1,00

Таблица 15 – Усредненные значения PSNR маркированного аудиосигнала в зависимости от H_1

[illegible]

Добеши 4 класс 3	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 3	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 3	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00

Таблица 18 – Усредненные значения $V_{\text{псп}}(i=0)$ маркированного аудиосигнала в зависимости от H_1 при $H_0 = 0.5$

	H_1								
	0,55	0,60	0,65	0,70	0,75	0,80	0,85	0,90	0,95
Хаар класс 1	-0,27	0,23	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 1	-0,200	0,30	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Симлет 4 класс 1	0,20	0,70	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 1	0,20	0,70	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Хаар класс 2	0,57	0,77	0,99	0,99	0,97	0,97	1,00	1,00	1,00
Добеши 4 класс 2	0,39	0,62	0,99	0,99	1,00	1,00	0,99	0,99	1,00
Симлет 4 класс 2	-0,41	0,09	0,97	0,97	1,00	1,00	1,00	1,00	1,00
Койфлет 4 класс 2	0,19	0,69	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Хаар класс 3	0,41	0,74	0,99	0,99	1,00	1,00	1,00	1,00	1,00
Добеши 4 класс 3	-0,62	-0,12	0,99	0,99	0,99	0,99	0,99	0,99	0,99
Симлет 4 класс 3	-0,01	0,49	0,79	0,79	0,83	0,83	0,98	0,98	0,99
Койфлет 4 класс 3	0,60	0,80	1,00	1,00	1,00	1,00	1,00	1,00	1,00

Таблица 19 – Усредненные значения $V_{\text{псп}}(i=0)$ в зависимости от порога H_{thr}

H_{thr}									
	0,55	0,60	0,65	0,70	0,75	0,80	0,85	0,90	0,95
Хаар класс 1	0,600	1,000	1,000	1,000	1,000	1,000	0,600	0,600	-0,200
Добеши 4 класс 1	0,997	0,996	0,994	0,991	0,991	0,991	0,990	0,600	-0,600
Симлет 4 класс 1	0,998	0,998	0,996	0,994	0,994	0,994	0,993	0,591	-0,600
Койфлет 4 класс 1	0,994	0,995	0,995	0,993	0,991	0,990	0,200	-0,200	-0,601
Хаар класс 2	0,200	0,413	0,600	1,000	1,000	1,000	1,000	1,000	0,826

[illegible]

В.2. Численные результаты экспериментов для алгоритма A2

Таблица 20 – Усредненные значения PSNR стегоконтейнера в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар фрактал 1	35,74	41,25	43,85	37,43	35,55
Хаар фрактал 3	35,68	41,19	43,81	37,43	35,53
Хаар фрактал 4	35,78	41,34	43,91	37,45	35,53
Хаар фрактал 5	36,66	42,13	44,25	37,47	35,54
Хаар фрактал 6	34,84	40,41	43,42	37,42	35,52
Добеши 4 фрактал 1	35,79	41,41	43,74	37,73	35,54
Добеши 4 фрактал 3	35,77	41,37	43,70	37,71	35,54
Добеши 4 фрактал 4	35,89	41,46	43,72	37,70	35,54
Добеши 4 фрактал 5	36,81	42,33	44,08	37,74	35,54
Добеши 4 фрактал 6	34,89	40,58	43,34	37,70	35,53
Симлет 4 фрактал 1	35,78	41,40	43,80	37,66	35,86
Симлет 4 фрактал 3	35,75	41,35	43,75	37,66	35,85
Симлет 4 фрактал 4	35,88	41,44	43,77	37,67	35,87
Симлет 4 фрактал 5	36,80	42,31	44,14	37,68	35,86
Симлет 4 фрактал 6	34,88	40,56	43,39	37,64	35,84
Койфлет 4 фрактал 1	35,98	41,25	42,16	38,17	36,74
Койфлет 4 фрактал 3	35,77	41,16	42,15	38,17	36,72
Койфлет 4 фрактал 4	35,90	41,30	42,18	38,18	36,76
Койфлет 4 фрактал 5	36,74	41,99	42,38	38,20	36,74
Койфлет 4 фрактал 6	34,90	40,47	41,90	38,15	36,72

Таблица 21 – Усредненные значения коэффициента корреляции взаимного и опорного ЦВЗ в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар фрактал 1	0,976	0,905	0,696	0,267	0,096
Хаар фрактал 3	0,976	0,903	0,609	0,219	0,044
Хаар фрактал 4	0,976	0,902	0,693	0,272	0,103
Хаар фрактал 5	0,976	0,907	0,696	0,262	0,096
Хаар фрактал 6	0,976	0,904	0,692	0,268	0,102
Добеши 4 фрактал 1	0,976	0,963	0,911	0,934	0,638
Добеши 4 фрактал 3	0,976	0,962	0,910	0,935	0,647
Добеши 4 фрактал 4	0,976	0,962	0,912	0,939	0,677
Добеши 4 фрактал 5	0,976	0,962	0,909	0,927	0,632
Добеши 4 фрактал 6	0,976	0,962	0,911	0,936	0,651
Симлет 4 фрактал 1	0,976	0,963	0,917	0,934	0,647
Симлет 4 фрактал 3	0,976	0,963	0,916	0,936	0,650
Симлет 4 фрактал 4	0,976	0,963	0,917	0,941	0,680
Симлет 4 фрактал 5	0,976	0,963	0,915	0,928	0,631
Симлет 4 фрактал 6	0,976	0,963	0,917	0,936	0,654
Койфлет 4 фрактал 1	0,976	0,963	0,912	0,900	0,519
Койфлет 4 фрактал 3	0,976	0,963	0,904	0,901	0,550
Койфлет 4 фрактал 4	0,976	0,963	0,912	0,939	0,620
Койфлет 4 фрактал 5	0,976	0,963	0,910	0,905	0,487
Койфлет 4 фрактал 6	0,976	0,963	0,910	0,900	0,532

Таблица 22 – Вероятность ошибки извлечения ЦВЗ в зависимости от уровня разложения.

	Уровень разложения				
	1	2	3	4	5
Хаар фрактал 1	0	0	0,004	0,06	0,11
Хаар фрактал 3	0	0	0,003	0,05	0,11
Хаар фрактал 4	0	0	0,003	0,05	0,11
Хаар фрактал 5	0	4,12E-05	0,004	0,06	0,11
Хаар фрактал 6	0	0	0,003	0,05	0,11
Добеши 4 фрактал 1	0	0	2,44E-04	0,01	0,03
Добеши 4 фрактал 3	0	0	2,44E-04	0,01	0,03
Добеши 4 фрактал 4	0	0	2,59E-04	0,01	0,03
Добеши 4 фрактал 5	0	0	2,44E-04	0,01	0,03
Добеши 4 фрактал 6	0	0	2,44E-04	0,01	0,03
Симлет 4 фрактал 1	0	0	6,56E-04	0,01	0,05
Симлет 4 фрактал 3	0	0	6,56E-04	0,01	0,05
Симлет 4 фрактал 4	0	0	6,41E-04	0,01	0,05
Симлет 4 фрактал 5	0	0	6,56E-04	0,01	0,05
Симлет 4 фрактал 6	0	0	6,56E-04	0,01	0,05
Койфлет 4 фрактал 1	0	0	1,12E-04	0,16	0,29
Койфлет 4 фрактал 3	0	0	1,28E-04	0,16	0,30
Койфлет 4 фрактал 4	0	0	4,80E-05	0,16	0,29
Койфлет 4 фрактал 5	0	0	9,60E-05	0,17	0,30
Койфлет 4 фрактал 6	0	0	1,28E-04	0,16	0,29

Таблица 23 – Усредненные значения PSNR стегоконтейнера в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар фрактал 1	40,00	40,00	40,00
Хаар фрактал 3	40,00	40,00	40,00
Хаар фрактал 4	40,00	40,00	40,00
Хаар фрактал 5	46,52	45,69	49,61
Хаар фрактал 6	46,50	45,68	49,59
Добеши 4 фрактал 1	46,54	45,70	49,66
Добеши 4 фрактал 3	46,69	45,83	49,98
Добеши 4 фрактал 4	46,33	45,54	49,23
Добеши 4 фрактал 5	45,81	44,85	49,52
Добеши 4 фрактал 6	45,80	44,83	49,50
Симлет 4 фрактал 1	45,82	44,85	49,54
Симлет 4 фрактал 3	45,96	44,97	49,90
Симлет 4 фрактал 4	45,65	44,71	49,13
Симлет 4 фрактал 5	45,91	44,93	49,68
Симлет 4 фрактал 6	45,90	44,92	49,66
Койфлет 4 фрактал 1	45,92	44,93	49,70
Койфлет 4 фрактал 3	46,06	45,05	50,05
Койфлет 4 фрактал 4	45,75	44,80	49,31
Койфлет 4 фрактал 5	40,42	38,98	48,27
Койфлет 4 фрактал 6	40,41	38,97	48,23

Таблица 24 – Усредненные значения коэффициента корреляции взаимного и опорного ЦВЗ в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар фрактал 1	0,885	0,886	0,895
Хаар фрактал 3	0,882	0,885	0,895
Хаар фрактал 4	0,884	0,885	0,895
Хаар фрактал 5	0,885	0,889	0,897
Хаар фрактал 6	0,884	0,885	0,894
Добеши 4 фрактал 1	0,993	0,992	0,996
Добеши 4 фрактал 3	0,991	0,991	0,995
Добеши 4 фрактал 4	0,994	0,993	0,996
Добеши 4 фрактал 5	0,994	0,991	0,996
Добеши 4 фрактал 6	0,993	0,992	0,995
Симлет 4 фрактал 1	0,993	0,992	0,996
Симлет 4 фрактал 3	0,992	0,992	0,995
Симлет 4 фрактал 4	0,994	0,993	0,996
Симлет 4 фрактал 5	0,994	0,992	0,996
Симлет 4 фрактал 6	0,993	0,993	0,996
Койфлет 4 фрактал 1	0,987	0,984	0,989
Койфлет 4 фрактал 3	0,969	0,973	0,978
Койфлет 4 фрактал 4	0,993	0,994	0,997
Койфлет 4 фрактал 5	0,988	0,990	0,995
Койфлет 4 фрактал 6	0,981	0,982	0,986

Таблица 25 – Вероятность ошибки извлечения ЦВЗ в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар фрактал 1	2,13E-04	2,33E-04	0
Хаар фрактал 3	7,69E-05	1,35E-04	0
Хаар фрактал 4	1,38E-04	9,88E-05	0
Хаар фрактал 5	3,40E-04	2,67E-04	0
Хаар фрактал 6	1,73E-04	2,05E-04	0
Добеши 4 фрактал 1	2,25E-04	2,05E-04	0
Добеши 4 фрактал 3	1,01E-04	1,22E-04	0
Добеши 4 фрактал 4	2,69E-04	2,69E-04	0
Добеши 4 фрактал 5	2,55E-04	2,81E-04	0
Добеши 4 фрактал 6	1,49E-04	1,49E-04	0
Симлет 4 фрактал 1	1,64E-04	1,43E-04	0
Симлет 4 фрактал 3	4,06E-05	2,03E-04	0
Симлет 4 фрактал 4	1,24E-04	3,31E-04	0
Симлет 4 фрактал 5	2,30E-04	2,55E-04	0
Симлет 4 фрактал 6	1,16E-04	2,15E-04	0
Койфлет 4 фрактал 1	1,46E-04	1,46E-04	2,09E-05
Койфлет 4 фрактал 3	4,13E-05	4,13E-05	6,20E-05
Койфлет 4 фрактал 4	1,91E-04	1,70E-04	4,25E-05
Койфлет 4 фрактал 5	1,82E-04	2,60E-04	2,60E-05
Койфлет 4 фрактал 6	1,19E-04	1,19E-04	5,08E-05

Таблица 26 – Усредненные значения PSNR стегоконтейнера в зависимости от α .

	α				
	0,25	0,50	1,00	2,50	5,00
Хаар фрактал 1	51,88	51,70	51,70	50,82	49,61
Хаар фрактал 3	51,88	51,70	51,70	50,81	49,59
Хаар фрактал 4	51,88	51,71	51,71	50,85	49,66
Хаар фрактал 5	51,88	51,74	51,74	51,02	49,98
Хаар фрактал 6	51,88	51,67	51,67	50,61	49,23
Добеши 4 фрактал 1	51,73	51,58	51,58	50,80	49,52
Добеши 4 фрактал 3	51,73	51,58	51,58	50,79	49,50
Добеши 4 фрактал 4	51,73	51,59	51,59	50,81	49,54
Добеши 4 фрактал 5	51,73	51,62	51,62	50,98	49,90
Добеши 4 фрактал 6	51,73	51,55	51,55	50,62	49,13
Симлет 4 фрактал 1	51,84	51,73	51,73	50,65	49,68
Симлет 4 фрактал 3	51,84	51,73	51,73	50,63	49,66
Симлет 4 фрактал 4	51,84	51,73	51,73	50,66	49,70
Симлет 4 фрактал 5	51,84	51,75	51,75	50,87	50,05
Симлет 4 фрактал 6	51,84	51,71	51,71	50,41	49,31
Койфлет 4 фрактал 1	49,47	49,40	49,40	48,80	48,27
Койфлет 4 фрактал 3	49,47	49,39	49,39	48,79	48,23
Койфлет 4 фрактал 4	49,47	49,40	49,40	48,83	48,26
Койфлет 4 фрактал 5	49,47	49,41	49,41	48,93	48,46
Койфлет 4 фрактал 6	49,47	49,38	49,38	48,67	48,03
	α				
	10,00	15,00	20,00	25,00	30,00
Хаар фрактал 1	46,22	43,46	41,25	39,47	37,98
Хаар фрактал 3	46,18	43,42	41,19	39,41	37,92
Хаар фрактал 4	46,29	43,56	41,34	39,57	38,09
Хаар фрактал 5	46,91	44,29	42,13	40,38	38,91
Хаар фрактал 6	45,54	42,68	40,41	38,61	37,10

Добеши 4 фрактал 1	46,37	43,59	41,41	39,65	38,16
Добеши 4 фрактал 3	46,33	43,54	41,37	39,61	38,11
Добеши 4 фрактал 4	46,40	43,63	41,46	39,70	38,22
Добеши 4 фрактал 5	47,06	44,43	42,33	40,60	39,13
Добеши 4 фрактал 6	45,71	42,80	40,58	38,79	37,28
Симлет 4 фрактал 1	46,39	43,53	41,40	39,64	38,18
Симлет 4 фрактал 3	46,35	43,49	41,35	39,59	38,13
Симлет 4 фрактал 4	46,42	43,57	41,44	39,68	38,22
Симлет 4 фрактал 5	47,09	44,38	42,31	40,58	39,14
Симлет 4 фрактал 6	45,73	42,73	40,56	38,77	37,30
Койфлет 4 фрактал 1	45,59	43,11	41,25	39,65	38,10
Койфлет 4 фрактал 3	45,54	43,05	41,16	39,55	38,01
Койфлет 4 фрактал 4	45,64	43,18	41,30	39,69	38,16
Койфлет 4 фрактал 5	46,10	43,79	41,99	40,44	38,93
Койфлет 4 фрактал 6	45,05	42,41	40,47	38,84	37,26

Таблица 27 – Усредненные значения коэффициента корреляции взаимного и опорного ЦВЗ в зависимости от alpha

	alpha				
	0,25	0,50	1,00	2,50	5,00
Хаар фрактал 1	-0,0007	0,2663	0,2628	0,7840	0,8952
Хаар фрактал 3	-0,0010	0,2674	0,2645	0,7819	0,8947
Хаар фрактал 4	0,0020	0,2733	0,2690	0,7851	0,8953
Хаар фрактал 5	-0,0032	0,2584	0,2537	0,7862	0,8975
Хаар фрактал 6	0,0008	0,2673	0,2638	0,7827	0,8940
Добеши 4 фрактал 1	-0,0018	0,6164	0,6790	0,9692	0,9958
Добеши 4 фрактал 3	0,0026	0,6248	0,6927	0,9680	0,9952
Добеши 4 фрактал 4	0,0021	0,6337	0,7008	0,9703	0,9963
Добеши 4 фрактал 5	-0,0033	0,5960	0,6584	0,9642	0,9959
Добеши 4 фрактал 6	-0,0014	0,6180	0,6852	0,9671	0,9955
Симлет 4 фрактал 1	-0,0013	0,7116	0,7867	0,9768	0,9960

Симлет 4 фрактал 3	0,0019	0,7154	0,7942	0,9753	0,9954
Симлет 4 фрактал 4	-0,0013	0,7167	0,7956	0,9774	0,9963
Симлет 4 фрактал 5	-0,0021	0,7085	0,7816	0,9746	0,9960
Симлет 4 фрактал 6	-0,0018	0,7137	0,7915	0,9761	0,9959
Койфлет 4 фрактал 1	-0,0022	0,6980	0,7746	0,9669	0,9886
Койфлет 4 фрактал 3	0,0009	0,6906	0,7695	0,9573	0,9780
Койфлет 4 фрактал 4	0,0036	0,7167	0,7977	0,9779	0,9972
Койфлет 4 фрактал 5	-0,0067	0,6951	0,7681	0,9716	0,9952
Койфлет 4 фрактал 6	-0,0024	0,6973	0,7761	0,9649	0,9863
	alpha				
	10,00	15,00	20,00	25,00	30,00
Хаар фрактал 1	0,9980	0,9988	0,9991	0,9994	0,9996
Хаар фрактал 3	0,9979	0,9986	0,9990	0,9993	0,9996
Хаар фрактал 4	0,9984	0,9991	0,9994	0,9996	0,9997
Хаар фрактал 5	0,9983	0,9990	0,9994	0,9996	0,9997
Хаар фрактал 6	0,9981	0,9988	0,9992	0,9995	0,9997
Добеши 4 фрактал 1	0,9979	0,9988	0,9992	0,9994	0,9996
Добеши 4 фрактал 3	0,9979	0,9987	0,9992	0,9994	0,9996
Добеши 4 фрактал 4	0,9985	0,9990	0,9993	0,9996	0,9997
Добеши 4 фрактал 5	0,9979	0,9988	0,9992	0,9995	0,9996
Добеши 4 фрактал 6	0,9980	0,9987	0,9991	0,9993	0,9995
Симлет 4 фрактал 1	0,9980	0,9987	0,9991	0,9994	0,9996
Симлет 4 фрактал 3	0,9977	0,9986	0,9989	0,9993	0,9995
Симлет 4 фрактал 4	0,9981	0,9989	0,9992	0,9995	0,9997
Симлет 4 фрактал 5	0,9979	0,9987	0,9992	0,9994	0,9996
Симлет 4 фрактал 6	0,9979	0,9987	0,9990	0,9993	0,9995
Койфлет 4 фрактал 1	0,9905	0,9909	0,9912	0,9913	0,9913
Койфлет 4 фрактал 3	0,9793	0,9794	0,9795	0,9794	0,9796
Койфлет 4 фрактал 4	0,9987	0,9993	0,9995	0,9997	0,9998
Койфлет 4 фрактал 5	0,9977	0,9988	0,9992	0,9995	0,9996
Койфлет 4 фрактал 6	0,9879	0,9886	0,9889	0,9889	0,9890

Таблица 28 – Вероятность ошибки извлечения ЦВЗ в зависимости от alpha

	alpha				
	0,25	0,50	1,00	2,50	5,00
Хаар фрактал 1	0,52	0,17	0,19	1,16E-04	0
Хаар фрактал 3	0,52	0,17	0,20	3,85E-05	0
Хаар фрактал 4	0,52	0,17	0,20	5,93E-05	0
Хаар фрактал 5	0,52	0,17	0,20	7,28E-05	0
Хаар фрактал 6	0,52	0,17	0,19	1,10E-04	0
Добеши 4 фрактал 1	0,52	0,15	0,18	2,05E-05	0
Добеши 4 фрактал 3	0,52	0,15	0,18	4,06E-05	0
Добеши 4 фрактал 4	0,52	0,15	0,17	2,07E-05	0
Добеши 4 фрактал 5	0,52	0,15	0,18	2,55E-05	0
Добеши 4 фрактал 6	0,52	0,15	0,18	1,65E-05	0
Симлет 4 фрактал 1	0,52	0,40	0,45	1,35E-03	0
Симлет 4 фрактал 3	0,52	0,39	0,45	1,08E-03	0
Симлет 4 фрактал 4	0,52	0,39	0,45	1,51E-03	0
Симлет 4 фрактал 5	0,52	0,40	0,45	1,15E-03	0
Симлет 4 фрактал 6	0,52	0,40	0,45	1,24E-03	0
Койфлет 4 фрактал 1	0,52	0,39	0,42	0,06	2,09E-05
Койфлет 4 фрактал 3	0,52	0,39	0,42	0,06	6,20E-05
Койфлет 4 фрактал 4	0,52	0,38	0,40	0,06	4,25E-05
Койфлет 4 фрактал 5	0,52	0,39	0,42	0,05	2,60E-05
Койфлет 4 фрактал 6	0,52	0,39	0,42	0,06	5,08E-05
	alpha				
	10,00	15,00	20,00	25,00	30,00
Хаар фрактал 1	0	0	0	0	0
Хаар фрактал 3	0	0	0	0	0
Хаар фрактал 4	0	0	0	0	0
Хаар фрактал 5	0	0	0	0	0
Хаар фрактал 6	0	0	0	0	0
Добеши 4 фрактал 1	0	0	0	0	0

Добеши 4 фрактал 3	0	0	0	0	0
Добеши 4 фрактал 4	0	0	0	0	0
Добеши 4 фрактал 5	0	0	0	0	0
Добеши 4 фрактал 6	0	0	0	0	0
Симлет 4 фрактал 1	0	0	0	0	0
Симлет 4 фрактал 3	0	0	0	0	0
Симлет 4 фрактал 4	0	0	0	0	0
Симлет 4 фрактал 5	0	0	0	0	0
Симлет 4 фрактал 6	0	0	0	0	0
Койфлет 4 фрактал 1	0	0	0	0	0
Койфлет 4 фрактал 3	0	0	0	0	0
Койфлет 4 фрактал 4	0	0	0	0	0
Койфлет 4 фрактал 5	0	0	0	0	0
Койфлет 4 фрактал 6	1,69E-05	0	0	0	0

Таблица 29 – Усредненные значения коэффициента корреляции взаимного и опорного ЦВЗ в зависимости от Thr

	Thr									
	0,050	0,100	0,150	0,200	0,250	0,300	0,350	0,400	0,450	0,500
Хаар фрактал 1	0,705	0,759	0,809	0,853	0,895	0,937	0,978	0,996	0,988	0,987
Хаар фрактал 3	0,704	0,757	0,807	0,852	0,895	0,936	0,977	0,996	0,991	0,990
Хаар фрактал 4	0,705	0,759	0,809	0,853	0,895	0,936	0,977	0,997	0,992	0,991
Хаар фрактал 5	0,704	0,760	0,811	0,854	0,897	0,938	0,978	0,997	0,986	0,985
Хаар фрактал 6	0,705	0,758	0,807	0,852	0,894	0,935	0,976	0,996	0,989	0,988
Добеши 4 фрактал 1	0,841	0,955	0,989	0,995	0,996	0,996	0,996	0,996	0,994	0,991
Добеши 4 фрактал 3	0,837	0,952	0,987	0,994	0,995	0,995	0,996	0,995	0,994	0,992
Добеши 4 фрактал 4	0,840	0,955	0,989	0,995	0,996	0,997	0,997	0,996	0,996	0,994
Добеши 4 фрактал 5	0,830	0,950	0,987	0,995	0,996	0,996	0,996	0,996	0,993	0,989
Добеши 4 фрактал 6	0,835	0,952	0,987	0,994	0,995	0,996	0,996	0,996	0,994	0,991
Симлет 4 фрактал 1	0,827	0,952	0,990	0,995	0,996	0,996	0,996	0,996	0,995	0,989
Симлет 4 фрактал 3	0,830	0,952	0,990	0,995	0,995	0,995	0,996	0,995	0,994	0,991
Симлет 4 фрактал 4	0,832	0,955	0,991	0,996	0,996	0,996	0,997	0,996	0,996	0,993
Симлет 4 фрактал 5	0,823	0,949	0,988	0,995	0,996	0,996	0,996	0,996	0,994	0,987
Симлет 4 фрактал 6	0,829	0,953	0,990	0,995	0,996	0,996	0,996	0,996	0,995	0,990
Койфлет 4 фрактал 1	0,841	0,954	0,984	0,988	0,989	0,988	0,988	0,987	0,984	0,980
Койфлет 4 фрактал 3	0,830	0,944	0,974	0,978	0,978	0,977	0,977	0,976	0,974	0,970
Койфлет 4 фрактал 4	0,847	0,961	0,993	0,997	0,997	0,997	0,997	0,997	0,996	0,994
Койфлет 4 фрактал 5	0,846	0,959	0,990	0,995	0,995	0,995	0,995	0,994	0,990	0,984
Койфлет 4 фрактал 6	0,839	0,951	0,982	0,986	0,986	0,986	0,986	0,985	0,982	0,979

	Thr									
	0,550	0,600	0,650	0,700	0,750	0,800	0,850	0,900	0,950	1,000
Хаар фрактал 1	0,987	0,986	0,946	0,861	0,783	0,709	0,640	0,580	0,528	0,461
Хаар фрактал 3	0,990	0,989	0,949	0,864	0,786	0,712	0,643	0,584	0,531	0,464
Хаар фрактал 4	0,991	0,990	0,953	0,868	0,791	0,716	0,647	0,587	0,534	0,466
Хаар фрактал 5	0,985	0,984	0,945	0,860	0,781	0,705	0,634	0,574	0,522	0,456
Хаар фрактал 6	0,987	0,987	0,948	0,863	0,784	0,710	0,642	0,581	0,529	0,462
Добеши 4 фрактал 1	0,988	0,987	0,986	0,986	0,985	0,983	0,973	0,910	0,725	0,478
Добеши 4 фрактал 3	0,990	0,989	0,988	0,987	0,987	0,985	0,975	0,910	0,727	0,482
Добеши 4 фрактал 4	0,992	0,992	0,991	0,991	0,990	0,988	0,979	0,915	0,732	0,483
Добеши 4 фрактал 5	0,985	0,984	0,983	0,982	0,981	0,980	0,970	0,905	0,721	0,473
Добеши 4 фрактал 6	0,988	0,987	0,987	0,986	0,985	0,984	0,974	0,910	0,729	0,481
Симлет 4 фрактал 1	0,987	0,986	0,986	0,985	0,984	0,982	0,975	0,925	0,752	0,501
Симлет 4 фрактал 3	0,989	0,988	0,987	0,987	0,986	0,984	0,977	0,924	0,751	0,501
Симлет 4 фрактал 4	0,992	0,991	0,991	0,990	0,989	0,987	0,980	0,927	0,752	0,501
Симлет 4 фрактал 5	0,984	0,983	0,982	0,981	0,980	0,979	0,972	0,922	0,750	0,500
Симлет 4 фрактал 6	0,988	0,987	0,986	0,985	0,984	0,983	0,976	0,924	0,750	0,500
Койфлет 4 фрактал 1	0,978	0,977	0,976	0,975	0,974	0,971	0,961	0,902	0,729	0,488
Койфлет 4 фрактал 3	0,968	0,967	0,965	0,964	0,963	0,960	0,951	0,894	0,727	0,488
Койфлет 4 фрактал 4	0,993	0,992	0,992	0,991	0,990	0,988	0,978	0,918	0,741	0,492
Койфлет 4 фрактал 5	0,981	0,980	0,979	0,978	0,977	0,975	0,964	0,903	0,727	0,485

Койфлет 4 фрактал 6	0,977	0,976	0,974	0,973	0,972	0,969	0,960	0,901	0,729	0,487
---------------------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------

Таблица 30 – Вероятность ошибки извлечения ЦВЗ в зависимости от Thr

	Thr									
	0,050	0,100	0,150	0,200	0,250	0,300	0,350	0,400	0,450	0,500
Хаар фрактал 1	0,03	0,01	1,05E-03	1,1E-03	0	0	0	0	0	0
Хаар фрактал 3	0,03	0,01	1,00E-03	1,0E-03	0	0	0	0	0	0
Хаар фрактал 4	0,04	0,01	1,05E-03	1,1E-03	0	0	0	0	0	0
Хаар фрактал 5	0,03	0,01	1,04E-03	1,0E-03	0	0	0	0	0	0
Хаар фрактал 6	0,04	0,01	1,43E-03	1,4E-03	0	0	0	0	0	0
Добеши 4 фрактал 1	0,05	0,01	9,83E-04	9,8E-04	0	0	0	0	0	2,05E-05
Добеши 4 фрактал 3	0,05	0,01	9,54E-04	9,5E-04	0	0	0	0	0	0
Добеши 4 фрактал 4	0,05	0,01	1,28E-03	1,3E-03	2E-05	2E-05	0	0	0	0
Добеши 4 фрактал 5	0,05	0,01	8,42E-04	8,4E-04	0	0	0	0	0	0
Добеши 4 фрактал 6	0,05	0,01	8,76E-04	8,8E-04	0	0	0	0	0	0
Симлет 4 фрактал 1	0,04	0,01	2,54E-03	2,5E-03	6,1E-05	2E-05	0	0	0	0
Симлет 4 фрактал 3	0,04	0,01	2,23E-03	2,2E-03	4E-05	0	0	0	0	2,03E-05
Симлет 4 фрактал 4	0,04	0,01	2,79E-03	2,8E-03	6,2E-05	0	0	0	0	0
Симлет 4 фрактал 5	0,05	0,01	2,98E-03	3,0E-03	2,5E-05	0	0	0	0	0
Симлет 4 фрактал 6	0,04	0,01	2,81E-03	2,8E-03	4,9E-05	0	0	0	0	1,65E-05

Койфлет 4 фрактал 1	0,03	0,01	1,05E-03	1,1E-03	0	0	0	0	0	0
Койфлет 4 фрактал 3	0,03	0,01	1,00E-03	1,0E-03	0	0	0	0	0	0
Койфлет 4 фрактал 4	0,04	0,01	1,05E-03	1,1E-03	0	0	0	0	0	0
Койфлет 4 фрактал 5	0,03	0,01	1,04E-03	1,0E-03	0	0	0	0	0	0
Койфлет 4 фрактал 6	0,04	0,01	1,43E-03	1,4E-03	0	0	0	0	0	0
	Thr									
	0,550	0,600	0,650	0,700	0,750	0,800	0,850	0,900	0,950	1,000
Хаар фрактал 1	0	1,94E-05	9,70E-05	0,00	0,00	0,01	0,05	0,17	0,35	0
Хаар фрактал 3	0	1,92E-05	1,92E-05	0,00	0,00	0,01	0,05	0,17	0,35	0
Хаар фрактал 4	0	1,98E-05	5,93E-05	0,00	0,00	0,01	0,05	0,17	0,35	0
Хаар фрактал 5	0	2,43E-05	9,71E-05	0,00	0,00	0,01	0,05	0,17	0,35	0
Хаар фрактал 6	0	1,57E-05	7,87E-05	0,00	0,00	0,01	0,05	0,17	0,35	0
Добеши 4 фрактал 1	2E-05	4,09E-05	6,14E-05	0,00	0,00	0,00	0,03	0,13	0,32	2,05E-05
Добеши 4 фрактал 3	0	0,00E+00	6,09E-05	0,00	0,00	0,00	0,03	0,13	0,32	0
Добеши 4 фрактал 4	0	2,07E-05	8,26E-05	0,00	0,00	0,00	0,02	0,13	0,32	0
Добеши 4 фрактал 5	0	2,55E-05	0,000179	0,00	0,00	0,00	0,02	0,13	0,31	0
Добеши 4 фрактал 6	0	0	4,96E-05	1,3E-04	3,6E-04	2,1E-03	0,03	0,13	0,32	0
Симлет 4 фрактал 1	2E-05	6,14E-05	0,000102	2,5E-04	9,6E-04	8,2E-03	0,07	0,24	0,44	2,05E-05
Симлет 4 фрактал 3	2E-05	2,03E-05	4,06E-05	8,1E-05	4,3E-04	8,0E-03	0,07	0,24	0,44	2,03E-05
Симлет 4 фрактал 4	0	4,13E-05	0,000145	2,5E-04	7,0E-04	8,1E-03	0,07	0,24	0,44	0
Симлет 4 фрактал 5	0	0,00E+00	5,10E-05	1,3E-04	7,1E-04	9,0E-03	0,07	0,24	0,43	0

Симлет 4 фрактал 6	1,6E-05	3,30E-05	4,96E-05	1,8E-04	8,1E-04	8,6E-03	0,07	0,24	0,44	1,65E-05
Койфлет 4 фрактал 1	1,4E-04	1,99E-02	6,98E-02	0,13	0,19	0,25	0,31	0,36	0,41	1,46E-04
Койфлет 4 фрактал 3	1,2E-04	2,04E-02	6,70E-02	0,12	0,19	0,25	0,30	0,35	0,41	1,24E-04
Койфлет 4 фрактал 4	2,9E-04	1,98E-02	6,74E-02	0,12	0,18	0,24	0,29	0,34	0,39	2,97E-04
Койфлет 4 фрактал 5	5,2E-05	2,02E-02	6,84E-02	0,13	0,19	0,25	0,31	0,36	0,42	5,21E-05
Койфлет 4 фрактал 6	1,3E-04	1,97E-02	6,71E-02	0,12	0,19	0,25	0,30	0,35	0,41	1,35E-04

В.3 Численные результаты экспериментов для алгоритма АЗ

Таблица 31 – Усредненные значения PSNR стегоконтейнера в зависимости от уровня разложения.

	Уровень разложения				
	1	2	3	4	5
Хаар	47,21	50,08	46,29	37,56	35,57
Добеши 4	45,56	49,97	45,80	37,82	35,56
Симлет 4	46,65	48,81	45,88	37,76	35,87
Койфлет 4	45,20	48,23	43,43	38,29	36,74

Таблица 32 – Усредненные значения $W_{\text{сп}}(i=0)$ в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар	1.000	0.995	0.828	0.434	0.077
Добеши 4	0.997	0.994	0.961	0.827	0.471
Симлет 4	1.000	0.992	0.980	0.775	0.515
Койфлет 4	0.986	0.977	0.923	0.645	0.312

Таблица 33 – Вероятность ошибки извлечения ПСП в зависимости от уровня разложения

	Уровень разложения				
	1	2	3	4	5
Хаар	4,00E-05	2,00E-04	6,00E-04	2,90E-03	5,50E-03
Добеши 4	6,00E-05	0	1,00E-04	6,00E-04	3,50E-03
Симлет 4	2,00E-04	1,00E-04	3,00E-04	7,00E-04	3,50E-03
Койфлет 4	4,00E-06	4,00E-04	2,00E-03	3,30E-03	5,00E-03

Таблица 34 – Усредненные значения PSNR стегоконтейнера в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар	47,04	45,99	50,60
Добеши 4	46,01	44,88	49,75
Симлет 4	45,95	45,02	48,20
Койфлет 4	40,40	39,02	48,15

Таблица 35 – Усредненные значения $W_{\text{псп}}(i=0)$ в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар	0,964	0,955	0,971
Добеши 4	0,932	0,815	0,929
Симлет 4	0,903	0,757	0,925
Койфлет 4	0,868	0,779	0,904

Таблица 36 – Вероятность ошибки извлечения ПСП в зависимости от типа коэффициентов вейвлет-разложения

	Тип коэффициентов		
	$W_{\psi}^H(j, m, n)$	$W_{\psi}^V(j, m, n)$	$W_{\psi}^D(j, m, n)$
Хаар	1,80E-04	1,50E-04	1,50E-04
Добеши 4	4,00E-05	2,00E-05	6,00E-05
Симлет 4	6,00E-05	2,00E-05	2,00E-05
Койфлет 4	3,00E-05	2,00E-05	2,00E-05

Таблица 37 – Усредненные значения $В_{\text{сп}}(i=0)$ в зависимости от α

	α					
	0,01	0,25	0,5	1	2,5	5
Хаар	51,84	51,68	51,59	50,29	46,77	46,24
Добеши 4	51,62	51,31	51,32	49,79	45,97	44,57
Симлет 4	51,76	51,68	51,48	47,94	46,75	44,45
Койфлет 4	49,42	49,32	49,20	47,42	45,52	43,95
	α					
	10	15	20	25	30	
Хаар	44,61	41,38	36,83	37,42	35,01	
Добеши 4	41,47	38,48	36,89	35,11	31,07	
Симлет 4	41,28	38,00	34,89	35,28	31,21	
Койфлет 4	42,16	36,85	36,94	35,05	34,32	

Таблица 38 – Усредненные значения $В_{\text{сп}}(i=0)$ в зависимости от α

	α					
	0,01	0,25	0,5	1	2,5	5
Хаар	0,041	0,077	0,220	0,489	0,787	0,953
Добеши 4	-0,023	0,163	0,396	0,621	0,836	0,921
Симлет 4	-0,028	0,211	0,421	0,698	0,889	0,927
Койфлет 4	0,041	0,206	0,426	0,669	0,865	0,900
	α					
	10	15	20	25	30	
Хаар	1,000	1,000	1,000	1,000	1,000	
Добеши 4	0,946	0,951	0,957	0,948	0,946	
Симлет 4	0,937	0,947	0,949	0,949	0,942	
Койфлет 4	0,907	0,910	0,910	0,912	0,911	

Таблица 39 – Вероятность ошибки извлечения ПСП в зависимости от alpha

	alpha					
	0,01	0,25	0,5	1	2,5	5
Хаар	5,23E-03	1,3E-03	4,1E-04	1,5E-04	1,6E-04	1,5E-04
Добеши 4	3,60E-03	4,8E-04	1,1E-04	6,0E-05	5,0E-05	5,0E-05
Симлет 4	4,95E-03	4,8E-03	1,2E-03	1,0E-05	4,0E-05	2,0E-05
Койфлет 4	4,42E-03	3,4E-03	2,6E-03	0	0	0
	alpha					
	10	15	20	25	30	
Хаар	1,7E-04	1,8E-04	1,7E-04	1,5E-04	1,8E-04	
Добеши 4	7,0E-05	4,0E-05	6,0E-05	6,0E-05	3,0E-05	
Симлет 4	2,0E-05	2,0E-05	3,0E-05	2,0E-05	3,0E-05	
Койфлет 4	0	0	0	0	0	

Таблица 40 – Усредненные значения PSNR стежоконтейнера в зависимости от длины последовательности ФГШ

	Длина последовательности ФГШ							
	150	400	650	900	1150	1400	1650	1900
Хаар	50,48	50,20	50,43	49,85	50,42	50,13	49,94	49,44
Добеши 4	50,33	50,13	50,45	49,65	50,31	49,92	50,10	49,42
Симлет 4	50,14	50,21	50,25	49,67	49,24	50,09	49,10	49,62
Койфлет 4	48,63	48,34	48,51	48,39	48,63	48,17	47,66	48,25

Таблица 41 – Усредненные значения $В_{псп}(i=0)$ в зависимости от длины последовательности ФГШ

	Длина последовательности ФГШ							
	150	400	650	900	1150	1400	1650	1900
Хаар	0,98	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеша 4	0,99	1,00	0,99	1,00	1,00	1,00	1,00	1,00
Симлет 4	0,99	0,99	0,99	1,00	1,00	1,00	1,00	1,00
Койфлет 4	0,96	0,96	0,96	0,97	0,97	1,00	0,98	0,99

Таблица 42 – Вероятность ошибки извлечения ПСП в зависимости от длины последовательности ФГШ

	Длина последовательности ФГШ							
	150	400	650	900	1150	1400	1650	1900
Хаар	1,9E-04	1,9E-04	1,9E-04	1,4E-04	8,6E-05	5,3E-05	6,2E-05	7,1E-05
Добеша 4	3,5E-05	6,3E-05	2,6E-05	0	0	0	0	0
Симлет 4	5,9E-05	1,6E-05	0	0	0	0	0	7,5E-05
Койфлет 4	7,1E-04	1,6E-05	2,3E-04	7,2E-05	0	0	0	0

Таблица 43 – Усредненные значения PSNR стежоконтнера в зависимости от H_1

	H_1								
	0,55	0,6	0,65	0,7	0,75	0,8	0,85	0,9	0,95
Хаар	50,32	50,42	50,36	50,00	50,28	50,23	50,37	50,38	50,32
Добеша 4	49,47	49,12	49,06	49,31	49,25	49,21	49,61	49,74	49,88
Симлет 4	49,23	49,33	49,40	49,08	49,06	49,16	49,03	49,09	49,72
Койфлет 4	47,71	47,65	47,83	47,88	47,97	47,75	47,94	47,57	48,31

Таблица 44 – Усредненные значения $В_{сп}(i=0)$ в зависимости от H_1

	H_1								
	0,55	0,6	0,65	0,7	0,75	0,8	0,85	0,9	0,95
Хаар	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Добеши 4	0,99	1,00	1,00	0,99	0,99	0,99	0,99	0,99	0,99
Симлет 4	1,00	0,99	1,00	1,00	1,00	1,00	1,00	1,00	1,00
Койфлет 4	0,97	0,98	0,97	0,98	0,98	0,97	0,97	0,98	0,98

Таблица 45 – Вероятность ошибки извлечения ПСП в зависимости от H_1

	H_1								
	0,55	0,6	0,65	0,7	0,75	0,8	0,85	0,9	0,95
Хаар	1,7E-04	2,2E-04	1,8E-04	3,2E-04	1,8E-04	1,9E-04	1,7E-04	1,5E-04	1,7E-04
Добеши 4	7,0E-05	6,0E-05	8,0E-05	5,0E-05	7,0E-05	5,0E-05	5,0E-05	4,0E-05	7,0E-05
Симлет 4	4,1E-04	4,0E-05	6,0E-05	3,0E-05	4,0E-05	2,0E-05	3,0E-05	3,0E-05	2,0E-05
Койфлет 4	1,5E-03	1,8E-03	8,1E-04	7,6E-04	2,2E-04	1,4E-04	7,0E-05	4,0E-05	1,0E-05

Таблица 46 – Усредненные значения $В_{сп}(i=0)$ в зависимости от $H_{пор}$

	$H_{пор}$							
	0,2	0,25	0,3	0,35	0,4	0,45	0,5	0,55
Хаар	0,64	0,82	0,96	1,00	1,00	1,00	1,00	1,00
Добеши 4	0,90	0,99	0,99	0,99	0,99	0,99	0,99	0,99
Симлет 4	0,87	0,99	0,99	0,99	0,99	0,99	0,99	0,99
Койфлет 4	0,87	0,97	0,97	0,98	0,98	0,98	0,98	0,98
	$H_{пор}$							
	0,6	0,65	0,7	0,75	0,8	0,85	0,9	
Хаар	1,00	1,00	1,00	1,00	1,00	1,00	0,27	
Добеши 4	0,99	1,00	1,00	1,00	1,00	1,00	0,96	
Симлет 4	1,00	1,00	1,00	1,00	1,00	1,00	0,99	
Койфлет 4	0,97	0,98	0,97	0,97	0,97	0,98	0,97	

Таблица 47 – Вероятность ошибки извлечения ПСП в зависимости от $H_{пор}$

	$H_{пор}$							
	0,2	0,25	0,3	0,35	0,4	0,45	0,5	0,55
Хаар	1,6E-03	8,2E-04	3,7E-04	1,9E-04	1,6E-04	1,6E-04	1,5E-04	1,3E-04
Добеши 4	1,5E-03	6,2E-04	1,5E-04	5,0E-05	4,0E-05	5,0E-05	5,0E-05	5,0E-05
Симлет 4	1,5E-03	5,9E-04	2,2E-04	5,0E-05	3,0E-05	2,0E-05	3,0E-05	3,0E-05
Койфлет 4	3,4E-03	2,9E-03	2,2E-03	1,4E-03	7,3E-04	2,7E-04	3,0E-05	0
	$H_{пор}$							
	0,6	0,65	0,7	0,75	0,8	0,85	0,9	
Хаар	1,5E-04	1,7E-04	2,1E-04	4,2E-04	5,3E-04	6,3E-04	1,0E-03	
Добеши 4	5,0E-05	6,0E-05	7,0E-05	7,0E-05	8,0E-05	2,7E-04	6,7E-04	
Симлет 4	3,0E-05	3,0E-05	4,0E-05	8,0E-05	3,8E-04	3,2E-03	5,2E-03	
Койфлет 4	0	1,0E-05	2,4E-04	1,3E-03	3,9E-03	5,1E-03	5,2E-03	

Приложение Г. Листинги программ реализации разработанных алгоритмов

Г.1 Алгоритм А1

Embed.m – встраивание ПСП

```
clear; clear all;
wavelet={'haar', 'db4', 'sym4', 'coif4'};
for aud=1:1500
    for wav=1:4
        clear audioSegment2;
        audioName=['cover/',int2str(aud),'.wav'];
        [y,Fs]=audioread(audioName);
        audio=y(:,1);
        Message=PSP(1000);
        [L,C]=dwt(audio,wavelet{wav});
        CC=C;
        segmentSize=fix(length(CC)/length(Message));
        [seqZeros,seqOnes]=sequence(0.5,0.95,segmentSize);
        a=0.001;
        j=1;
        for i=1:length(Message)
            if Message(i)==-1
                CC(j:j+segmentSize-1)=a*seqZeros;
            else
                CC(j:j+segmentSize-1)=a*seqOnes;
            end
            j=j+segmentSize;
        end
        newAudio=idwt(L,CC,wavelet{wav});
        if aud>500
            newAudio(:,2)=y(:,2);
        end
        newAudio-
        Name=['test/new',int2str(aud),'_',wavName{wav},'.wav'];
        audiowrite(newAudioName,newAudio,Fs);
    end
end
```

Extract.m – Извлечение ПСП

```
clear; clear all;
wavelet={'haar', 'db4', 'sym4', 'coif4'};
for aud=1:1500
    for wav=1:4
```

```

clear Message2;
audio-
Name=['test/new',int2str(aud),'_',wavName{wav},'.wav'];
[y1,Fs1]=audioread(audioName);
Message=PSP(1000);
audio1=y1(:,1);
[L,CC]=dwt(audio1,wavelet{wav});
segmentSize=fix(length(CC)/length(Message));
j=1;
for i=1:length(Message)
    CD1=CC(j:j+segmentSize-1);
    H(i)=wavH(CD1,'haar',2);
    j=j+segmentSize;
end
for i=1:length(Message)
    if H(i)>0.7
        Message2(i,1)=1;
    else
        Message2(i,1)=-1;
    end
end
end
end
end

```

Г.2 Алгоритм А2

Embed.m – Встраивание ЦВЗ

```

for im=1:20000
    if im<=10000
        contName=['D:\Кандидатская диссертация\Код\PPG-LIRMM-
COLOR\' ,int2str(im),'.ppm'];
        imgRGB=imread(contName);
        imgycbr = rgb2ycbcr(imgRGB);
        imgY = imgycbr(:,:,1);
    else
        contName=['D:\Кандидатская
диссертация\Код\BOWS2OrigEp3\' ,int2str(im-50),'.pgm'];
        imgRGB=imread(contName);
        imgY=imgRGB;
    end
    for wav=1:4
        for ind=1:5

            markName=['dvt3/',wavName{wav},'fr',int2str(ind),'.png'];
            mark=imread(markName);
            alpha=5;
            mark1=alpha*(mark(:,:,1)/255);
            wavelet = w{wav};
            [cA,cH,cV,cD]=dwt2(imgY,wavelet);
            [cA2,cH2,cV2,cD2]=dwt2(cA,wavelet);
            cA1_new = idwt2(cA2,cH2,cV2,mark1,wavelet);
            new_img_Y=idwt2(cA1_new(1:size(cA,1),1:size(cA,2)),cH,
            cV,cD,wavelet);
            if im<=10000
                imgY_new = imgycbr;
                imgY_new(:,:,1)=uint8(new_img_Y);
                imgRGB_new = ycbcr2rgb(imgY_new);
            else
                imgRGB_new=uint8(new_img_Y);
            end
            newImgName=['dvt3/test/lena',int2str(im),'_',wavName{w
            av},int2str(ind),'.png'];
            imwrite(uint8(imgRGB_new),newImgName);
        end
    end
end
end

```

Extract.m – извлечение ЦВЗ

```

clc; clear all;
w={'haar','db4','sym4','coif4'};

```

```

wc={'h','ds','ds','c'};
wavName={'haar','db','sym','coif'};
sizze=[500,505,505,517];
for im=1:20000
    for wav=1:4 % по вейвлетам
        for ind=1:5 % по фракталам

imgName=['dvt3/test/lena',int2str(im),'_',wavName{wav},int2str(ind),
'.png'];

            imgRGB=imread(imgName);
            if im<=10000
                imgycbr = rgb2ycbcr(imgRGB);
                imgY = imgycbr(:,:,1);
            else
                imgY=imgRGB;
            end
            wavelet = w{wav};
            [cA1,cH1,cV1,cD1]=dwt2(imgY,wavelet);
            [cA2,cH2,cV2,cD2]=dwt2(cA1,wavelet);
            [cA3,cH3,cV3,cD3]=dwt2(cA2,wavelet);
            [cA4,cH4,cV4,cD4]=dwt2(cA3,wavelet);
            [cA5,cH5,cV5,cD5]=dwt2(cA4,wavelet);
            newFr=cD2;
            Thr=1.25;
            for i=1:size(newFr,1)
                for j=1:size(newFr,2)
                    if newFr(i,j)>Thr
                        newFr(i,j)=255;
                    else
                        newFr(i,j)=0;
                    end
                end
            end
            end
            fr1Name=['dvt3/',wavName{wav},int2str(ind),'.png'];
            fr1=imread(fr1Name);
            newFr=uint8(newFr);
            W1=newFr/255;
            qr_size=50^2;
            p=pp(ind);
            q=qg(ind);
            a=sizze(wav); %ширина
            b=sizze(wav); %высота
            T=30; %maxstep
            C=p+q*1i;
            R=0.5+0.5*sqrt(1+4*abs(C));
            xmin=-1.5;
            xmax=1.5;
            ymin=-1.5;
            ymax=1.5;

```

```

deltax=(xmax-xmin)/(a-1);
deltay=(ymax-ymin)/(b-1);
k=1;
for nx=1:a
    for ny=1:b
        x(1)=xmin+nx*deltax;
        y(1)=ymin+ny*deltay;
        t=1;
        while(t<T)
            x(t+1)=x(t)^2-y(t)^2+p;
            y(t+1)=2*x(t)*y(t)+q;
            t=t+1;
            r=x(t)^2+y(t)^2;
            if (t==T)
                if (r<=R)
                    if k<=qr_size
                        if W1(ny,nx)==0
                            cvz(k)=0;
                        else
                            cvz(k)=W1(ny,nx);
                        end
                        k=k+1;
                    end
                end
                elseif (r>R)
                    t=T;
                end
            end
        end
    end
end
cvz=reshape(cvz,sqrt(qr_size),sqrt(qr_size));
cvz=cvz*255;

cvzName=['dvt3/filt/cvz',int2str(im),'_',wavName{wav},int2str(ind),'
_level',int2str(alpha),'.png'];
imwrite(cvz,cvzName);
cvzOrig=imread('qr/50.png');
cvz2=cvzOrig(:,:,1);
cvz1=uint8(cvz(:,:,1))/255;
r=corr2(cvz1,cvz2);
errQr(ind,alpha,wav)=errQr(ind,alpha,wav)+r;
if r<0.8
    errP(ind,alpha,wav)=errP(ind,alpha,wav)+1;
end
end
end
end
end
end
wavName={'Хаар','Добеши 4','Симлет 4','Койфлет 4'};

```

```

lineType={'-','--',':','-.'};
figure(1)
for i=1:4
    for j=1:5
        labelName=[wavName{i},' фрактал ',int2str(j)];

plot(1:3,errQr(j,:,i)./100,lineType{i},'DisplayName',labelName);
        hold on;grid on;
    end
end
end

```

Алгоритм A21

```

clc; clear all;
pp=[-0.7,-0.83,-0.39054,-0.481762,-0.7454];
qq=[0,0.16,0.58678,-0.531657,0.113];
img=imread('lena2000.png');
cD2=img(:,:,3);
for ind=1:1
    p=pp(ind);
    q=qq(ind);
    a=size(cD2,1);%ширина
    b=size(cD2,2);%высота
    T=30;%maxstep
    C=p+q*1i;
    R=0.5+0.5*sqrt(1+4*abs(C));
    xmin=-1.5;
    xmax=1.5;
    ymin=-1.5;
    ymax=1.5;
    deltax=(xmax-xmin)/(a-1);
    deltay=(ymax-ymin)/(b-1);
    qr=double(imread('Qr/50.png'));
    cvz=reshape(uint8(qr(:,:,1)),1,[]);
    k=1;
    for nx=1:a
        for ny=1:b
            x(1)=xmin+nx*deltax;
            y(1)=ymin+ny*deltay;
            t=1;
            while(t<T)
                x(t+1)=x(t)^2-y(t)^2+p;
                y(t+1)=2*x(t)*y(t)+q;
                t=t+1;
                r=x(t)^2+y(t)^2;
                if (t==T)
                    if (r<=R) && (k<=size(cvz,2))
                        if cvz(k)==0

```

```

        W(ny,nx)=0;
    elseif cvz(k)==1
        W(ny,nx)=1;
    end
    k=k+1;
    t=T+1;
    elseif (r<=R) && (k>size(cvz,2))
        W(ny,nx)=1;
    end
    elseif (r>R)
        W(ny,nx)=cD2(ny,nx);
        t=T;
    end
end
end
end
fractName=['dvt3/testhaarNew',int2str(ind),'.png'];
imwrite(W,fractName);

end

```

Г.3 Алгоритм А3

Embed.m – встраивание ПСП

```

clear all;clc;
wavelet={'haar','db4','sym4','coif4'};
wavName={'haar','db','sym','coif'};
for im=1:20000
    if im<=10000
        contName=['D:\Кандидатская диссертация\Код\PPG-LIRMM-
COLOR\'',int2str(im),'.ppm'];
        imgRGB=imread(contName);
        imgycbr = rgb2ycbcr(imgRGB);
        imgY = imgycbr(:,:,1);
    else
        contName=['D:\Кандидатская
диссертация\Код\BOWS2OrigEp3\'',int2str(im-50),'.pgm'];
        imgRGB=imread(contName);
        imgY=imgRGB;
    end
    for wav=1:4
        for a=1:1
            wave=wavelet{wav};
            [cA,cH,cV,cD]=dwt2(imgY,wave);
            [cA2,cH2,cV2,cD2]=dwt2(cA,wave);
            PSPSize=500;
            noiseSize=fix(size(cD2_Vector,2)/PSPSize);
            qr_Vector=PSP(PSPSize);
            [seqZeros,seqOnes]=sequence(0.15,0.95,noiseSize);
            j=1;
            alpha=2.5;
            for i=1:size(qr_Vector,1)
                if qr_Vector(i)==-1
                    cD2_Vector(j:j+noiseSize-1)=alpha*seqZeros;
                else
                    cD2_Vector(j:j+noiseSize-1)=alpha*seqOnes;
                end
                j=j+noiseSize;
            end
            cD2New=reshape(cD2_Vector,size(cD2,1),size(cD2,2));
            cA1_new = idwt2(cA2,cH2,cV2,cD2New,wave);
        end
        new_img_Y=idwt2(cA1_new(1:size(cA,1),1:size(cA,2)),cH,cV,cD,wave);
        if im<=10000
            imgY_new = imgycbr;
            imgY_new(:,:,1)=uint8(new_img_Y);
            imgRGB_new = ycbcr2rgb(imgY_new);
        else
            imgRGB_new=uint8(new_img_Y);
        end
    end
end

```



```

        end

imgName=['test3/lena',wavName{wav},int2str(im),'_',int2str(a),'.png'
];
        imwrite(uint8(imgRGB_new),imgName);
    end
end
end

```

Extract.m

```

clear all;clc;
H1=0.55:0.05:0.95;
Hthr=0.2:0.05:0.9;
alpha=[0.01 0.25 0.5, 1, 2.5, 5, 10, 15, 20, 25, 30];
wavelet={'haar','db4','sym4','coif4'};
% coeff={'cH','cV','cD'};
noiseDisp=[0.01 0.015 0.02 0.025 0.03 0.035 0.04 0.045 0.05 0.055];
mask=2:10;
% imgOrig=imread('lena2000.png');
qual=0:10:50;
NSize=150:250:2000;
errPSP=zeros(6,4);
errP=zeros(6,4);
wavName={'haar','db','sym','coif'};
for im=1:20000
    for wav=1:4
        for ind=1:size(qual,2)
            Message2=0;
            wave=wavelet{wav};

imgName=['jpeg/jpeg',wavName{wav},int2str(im),'_1','.jpg'];
            img=imread(imgName);
            if im<=50
                imgycbr = rgb2ycbcr(img);
                imgY = imgycbr(:,:,1);
            else
                imgY=img;
            end
            [cA1,cH1,cV1,cD1]=dwt2(imgY,wave);
            [cA2,cH2,cV2,cD2]=dwt2(cA1,wave);
            cD2_Vector=reshape(cD2,1,[]);
            PSPSize=500;
            j=1;
            noiseSize=fix(size(cD2_Vector,2)/PSPSize);
            Message=PSP(PSPSize);
            for i=1:PSPSize
                cDPart=cD2_Vector(j:j+noiseSize-1);
            end
        end
    end
end

```

```

        j=j+noiseSize;
        H(i)=wavH(cDPart,'haar',2);
    end
    for i=1:PSPSize
        if H(i)>0.5
            Message2(i,1)=1;
        else
            Message2(i,1)=-1;
        end
    end
    corr_Message=corr(Message,Message2);
    if isnan(corr_Message)==1
        corr_Message=0;
    end
    errPSP(ind,wav)=errPSP(ind,wav)+corr_Message;
    if corr_Message<0.95
        errP(ind,wav)=errP(ind,wav)+1;
    end
end
end
end

```