На правах рукописи

Григорьев Евгений Константинович

ПОИСК И ПРИМЕНЕНИЕ ЦИКЛИЧЕСКИХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ В ЗАДАЧАХ ОБРАБОТКИ ИНФОРМАЦИИ

2.3.1. Системный анализ, управление и обработка информации, статистика

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2025

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» на кафедре вычислительных систем и сетей.

Научный руководитель: доктор технических наук, профессор
Сергеев Михаил Борисович

Официальные оппоненты: **Колбанёв Михаил Олегович**,
доктор технических наук, профессор,
Санкт-Петербругский государственный экономический университет, кафедра информационных систем и технологий, профессор кафедры

Ляхов Павел Алексеевич,
кандидат физико-математических наук, доцент,
Северо-Кавказский федеральный университет, факультет математики и компьютерных наук имени профессора Н.И. Червякова, кафедра математического моделирования, заведующий кафедрой

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», г. Москва

Защита состоится 10 сентября 2025 года в 16.00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 3 июля 2025 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Матрицы играют ключевую роль в различных преобразованиях, используемых в технических системах. Они применяются при сжатии данных, помехоустойчивом кодировании сигналов и изображений, их обработке, а также в методах кодового разделения каналов в телекоммуникациях и др. Среди разнообразия матриц особое место занимают квадратные ортогональные матрицы. К ним относятся, например, матрицы дискретного косинусного преобразования (ДКП), а также матрицы Адамара, Белевича, Хаара и др.

Для решения прикладных задач предпочтительными являются ортогональные матрицы простой структуры. Среди базовых матричных структур на практике особый интерес представляют циклическая и симметричная. Следствием использования структурированных матриц является упрощение преобразований с их использованием, снижение затрат памяти на хранение или сокращение времени генерации матрицы, если это необходимо.

Дополнительно, для практического применения необходимо по возможности обеспечить как можно меньшее количество значений элементов (уровней) матрицы. Идеальными в этом смысле являются известные двухуровневые {1, –1} матрицы Адамара глобального максимума детерминанта. Однако, согласно предположению Р. Пэли, такие матрицы существуют только на порядках $4t$, где t –натуральное число, а согласно гипотезе Г. Райзера, циклические конструкции матриц Адамара ограничены порядком 4. Следует отметить, что ни предположение Р. Пэли, ни гипотеза Г. Райзера до сих пор не доказаны, а среди порядков последовательности матриц Адамара существуют исключения, кратные восьми, и некоторые другие порядки.

Анализ показал, что существуют двухуровневые $\{1, -b\}$ квазиортогональные матрицы Мерсенна локального максимума детерминанта, обобщающие матрицы Адамара и существующие на нечетных порядках $4t - 1$. Существуют различные конструкции таких матриц, но преимущественно они являются циклическими. Они показывают интересные свойства в системах радиолокации и связи с корреляционным приемом, при защитном и помехоустойчивом кодировании информации в каналах распределенных систем и других приложениях. При этом актуальность задачи поиска циклических версий квазиортогональных матриц на большом диапазоне значений их порядков для задач обработки и кодирования информации постоянно возрастает.

Степень разработанности темы. Основополагающие работы по теме поиска малоуровневых ортогональных и обобщающих их квазиортогональных матриц, а также анализа свойств подобных матриц, их взаимосвязей и условий существования, связаны с такими учеными как Ж. Адамар, Р. Пэли, Дж. Сильвестр, У. Скарпи, Г. Райзер, J. Seberry, M. Jamada, D. Djokovic, H. Kharaghani, I. Kotsireas, Л. А. Мироновский, Н. А. Балонин, М. Б. Сергеев, А. М. Сергеев и др.

Вопросы практического применения ортогональных матриц для задач, связанных с темой диссертационной работы, рассматривались в работах N. Ahmed, K. J. Horadam, R. Wang, J. Seberry, M. Jamada, Ch. Koukouvinos, Л.А. Мироновского, В. А. Слаева, М. Б. Сергеева, А.

А. Вострикова и др.

Вопросы практического применения квазиортогональных матриц в области обработки информации в распределенных системах радиолокации и телекоммуникациях рассмотрены в работах А. М. Сергеева, В. А. Ненашева, А. Н. Леухина, А. А. Сенцова, а в области защитного кодирования цифровой визуальной информации – в работах А. А. Вострикова, А. М. Сергеева, Ю. Н. Балонина и др.

Научной задачей диссертационного исследования является разработка метода и алгоритмов на его основе для поиска структурированных квазиортогональных малоуровневых матриц.

Объектом исследования являются двухуровневые квазиортогональные матрицы циклической структуры для обработки информации.

Предметом исследования являются свойства циклических квазиортогональных матриц и их строк, порядки их существования и методы поиска.

Цель работы заключается в поиске новых, не основанных на переборе, методов получения циклических квазиортогональных матриц и анализе результатов их применения в задачах обработки, кодирования и передачи информации.

В рамках достижения цели диссертационного исследования были решены следующие **задачи**:

– разработан метод и алгоритмы поиска двухуровневых циклических квазиортогональных матриц, существующих на порядках $4t - 1$ и представляющих собой «ядро» матриц Адамара;

– проведен анализ корреляционных характеристик кодовых последовательностей, на основе строк двухуровневых циклических квазиортогональных матриц и циклических матриц, основанных на разностных множествах Адамара;

– проанализировано использование двухуровневых циклических квазиортогональных матриц в задачах защитного кодирования цифровой аудио/визуальной информации и выполнена оценка результатов.

– разработан единый подход к определению качества маскирования аудио и визуальной информации.

Научная новизна работы определяется тем, что в ней:

– синтезирован численный метод поиска двухуровневых циклических квазиортогональных матриц на основе анализа взаимосвязей между матрицами максимума детерминанта и кодовыми последовательностями с хорошими корреляционными свойствами;

– показано, что если существует матрица Адамара с циклическим «ядром», представляющим собой циклический сдвиг разностного множества Адамара, то можно найти и квазиортогональную матрицу порядка $4t – 1$, связанную с этим «ядром»;

– предложен единый подход к оценке качества результатов маскирования аудио/визуальной информации на основе их сравнительного анализа с белым шумом, позволяющий оценить степень защищенности маскированной информации.

Теоретическая и практическая значимость работы определяются тем, что в ней:

– показано, что использование символов Лежандра и Якоби позволяет находить квазиортогональные матрицы циклической и производных от нее структур;

– показано, что строки циклических квазиортогональных матриц, найденных предложенным в работе методом, могут найти применение в коммуникационных системах, в качестве несимметричных кодовых последовательностей большой длины для модуляции сигналов;

– строки найденных циклических квазиортогональных матриц обладают улучшенными свойствами апериодической автокорреляционной функции по сравнению с прототипом - кодовыми последовательностями, основанными на разностных множествах Адамара;

– показано, что у строк найденных циклических квазиортогональных матриц, так же, как и у кодовых последовательностей, основанных на разностных множествах Адамара, одноуровневая периодическая автокорреляционная функция;

– предложен единый подход к оценке качества результатов маскирования аудио/визуальной информации на основе их сравнительного анализа с белым гауссовским шумом с нулевым математическим ожиданием и среднеквадратическим отклонением равным аналогичному параметру маскированных данных, позволяющий оценить степень защищенности информации;

– показана простота применения найденных циклических квазиортогональных матриц в распределенных коммуникационных системах для обеспечения конфиденциальности передаваемой информации.

Внедрение результатов диссертационной работы. Научные результаты внедрены в учебном процессе Санкт-Петербургского государственного университета аэрокосмического приборостроения на кафедрах «Вычислительных систем и сетей» и «Инфокоммуникационных технологий и систем связи», а также использованы в следующих научно-исследовательских работах:

– НИР «Поиск и исследование экстремальных квазиортогональных матриц для обработки информации» гос. рег. № АААА-А17-117042710042-9, Госзадание Минобрнауки РФ (соглашение № 2.2200.2017/4.6), а именно: метод и алгоритмы вычисления новых циклических квазиортогональных матриц;

– НИР «Интеллектуальная система управления распределенными радиолокационными средствами для обнаружения БПЛА в условиях плотной городской застройки» (проект РФФИ 19-29-06029) гос. рег. № АААА-А19-119101590059-7, а именно: стратегии вычисления квазиортогональных циркулянтов как основы для формирования новых кодовых последовательностей и новые кодовые последовательности для кодирования сигналов в радиоканале;

– НИР «Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств», гос. рег. № АААА-А20-120060290131-9, Госзадание Минобрнауки РФ (соглашение № FSRF-2020-0004), а именно:

результаты анализа корреляционных характеристик кодовых последовательностей, основанных на строках циклических квазиортогональных матриц;

– НИР «Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга», гос. рег. № 123030100022-6, Госзадание Минобрнауки РФ (соглашение № FSRF-2023-0003), а именно: методы матричного маскирования/демаскирования цифровой звуковой информации, единый подход к анализу качества маскирования цифровой аудиовизуальной информации в части разрушения структуры исходного сообщения.

Методы исследования. При решении задач исследования использовались методология и методы теории квазиортогональных матриц, теории кодирования, а также методы имитационного моделирования.

Положения, выносимые на защиту:

– численный метод поиска матриц, использующий циклические разностные множества Адамара, обеспечивает нахождение циклических квазиортогональных матриц на порядках $4t$-1;

– строки циклических квазиортогональных матриц представляют собой альтернативу кодовым последовательностям, основанным на разностных множествах Адамара, и обеспечивают лучшие автокорреляционные характеристики;

– метод матричного маскирования аудиофайлов, использующий циклические квазиортогональные матрицы, обеспечивает конфиденциальность передачи аудиоданных в распределенных системах за счет преобразования спектральных составляющих аудиофайла к шумоподобному виду;

– впервые предложенный общий подход к оценке качества маскирования аудио и визуальных данных, обеспечивает оценку их защищенности от несанкционированного использования, ранее не производившуюся из-за отсутствия критериев.

Степень достоверности результатов диссертационной работы обеспечивается корректностью постановки научно-технической задачи и результатами моделирования. Полученные результаты не противоречат результатами исследований, опубликованных в открытых отечественных и международных изданиях, проведенных раннее по тематике, близкой к диссертационной работе. Внедрением в практику разработанных метода и алгоритмов на его основе, на которые получены свидетельства о государственной регистрации программ для ЭВМ и патент на изобретение.

Апробация работы. Основные научные положения диссертационного исследования в период 2019-2024 гг. были представлены научному сообществу, и получили положительную оценку:

– на XXVI и XXVII Международных конференциях SPIE «Image and Signal Processing for Remote Sensing» (Шотладния, г. Эдинбург, 2020 г. и Испания, г. Мадрид, 2021 г.),

– на XXIX международной научно-технической конференции «Современные технологии в задачах управления, автоматики и обработки информации» (Алушта, 2020 г.),

– на Международной конференции 13th International KES Conference «Intelligent Decision Technologies-2021». (дистанционно, 2021 г.),

– на международной конференции «XII International Society of Automation (ISA) student research long distance conference» (Санкт-Петербург, 2022 г.),

– на международной конференции «International Conference on Information Processes and Systems Development and Quality Assurance» (Санкт-Петербург, 2023 г.);

– на Третьей и Четвертой Международной научной конференции «Обработка, передача и защита информации в компьютерных системах» (Санкт-Петербург, 2023 и 2024 г.)

Публикации. По материалам диссертации было опубликовано семь статей в журналах из перечня ВАК РФ: «Труды учебных заведений связи», «Электросвязь», «Телекоммуникации», «Труды МАИ», «Вестник Российского фонда фундаментальных исследований». Четыре работы опубликованы в изданиях, индексируемых в международных базах цитирования SCOPUS/WoS и пять работ в иных изданиях и материалах конференций. Получены одиннадцать свидетельств о регистрации программ для ЭВМ и один патент на изобретение.

Личный вклад автора диссертационной работы заключается в:

– классификации двухуровневых квазиортогональных циклических матриц, позволившей установить их взаимосвязь с матрицами Адамара;

– разработке алгоритмов поиска и вычисления двухуровневых квазиортогональных матриц циклической структуры;

– создании программ для обработки цифровых аудиосигналов с применением найденных циклических квазиортогональных матриц, реализующих функции маскирования и демаскирования данных;

– разработке кодовых последовательностей с улучшенными автокорреляционными свойствами;

– разработке общего подхода к анализу качества разрушения маскированных звуковых и визуальных данных.

Соответствие диссертации паспорту научной специальности. Диссертационная работа соответствует пунктам 3, 4, 5 и 12 паспорта научной специальности 2.3.1. «Системный анализ, управление и обработка информации, статистика».

Объем и структура работы. Диссертационная работа состоит из введения, четырех разделов, заключения, списка использованных источников и трех приложений. В приложениях представлены акты о внедрении результатов диссертационной работы, свидетельства о регистрации программ для ЭВМ и патент на изобретение. Общий объем диссертации 129 страниц, включая 30 рисунков и 15 таблиц. Список использованных источников содержит 174 наименования.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении показывается актуальность темы диссертационной работы, определены её цель и задачи. Сформулированы положения, выносимые на защиту, научная новизна результатов, их теоретическая и практическая значимость. Приведены сведенья о практическом использовании научных результатов.

В первом разделе приведены необходимые определения из теории матриц, в частности определения матриц симметричных, персимметричных, циклических, ортогональных и квазиортогональных. Для последних в рамках работы использовано следующее определение – квадратная матрица **A** порядка n называется *квазиортогональной* в случае, если для приведенных к единице максимумам модулей элементов каждого из столбцов, выполняется соотношение:

$$\mathbf{A}\mathbf{A}^{\mathrm{T}}=\mathbf{A}^{\mathrm{T}}\mathbf{A}=\omega\mathbf{I}, \qquad (1)$$

где ω – вес матрицы, а **I** – единичная матрица. Отмечено, что, после нормирования столбцов данные матрицы становятся строго ортогональными.

Сделан вывод о том, что постоянный рост объемов данных, требует вычисления ортогональных и квазиортогональных матриц большой размерности с малым количеством уровней элементов и инвариантами структур. Как следствие целесообразен поиск вычислительно простых методов получения структурированных матриц, не основанных на комбинаторных подходах, что важно как в целом, при решении задач обработки информации, так и, при решении частных теоретических задач – например формирования составных блоков массивов при поиске матриц Адамара высоких порядков.

Во втором разделе Введены допущения, позволяющие осуществлять поиск циклических квазиортогональных матриц больших порядков, а именно:

- матрицы должны быть симметричны относительно побочной диагонали;
- требования к значению отрицательного элемента в матрице до $-b$ должны быть ослаблены, сделав его функцией от порядка n;
- поиск следует осуществлять на нечетных порядках, на единицу меньших $4t$. Именно эти матрицы являются «ядром», которое при замене $-b$ на -1 с добавлением «каймы» позволяют получить матрицы Адамара.

Пример подобных матриц – матрицы Мерсенна с уровнями $\{1, -b\}$, обобщающие матрицы Адамара и существующие на нечетных порядках $4t - 1$, связанные с простыми числами и имеющие, в основном, циклическую структуру. Доказано, что они существуют для всей последовательности порядков $n = 4t - 1$, однако поиск самих матриц является задачей трудоёмкой и требует разработки новых методов.

Проведенный обзор известных некомбинаторных методов поиска квазиортогональных матриц с симметриями позволяет сделать вывод о том, что известные методы, в основном, ориентированы на поиск матриц симметричной структуры.

Проведен анализ взаимосвязей теории матриц и одной из задач радиолокации и связи, а именно – поиска бинарных кодовых последовательностей (КП) с хорошими корреляционными свойствами. Его результаты позволили сделать вывод о том, что поиск

двухуровневых циклических квазиортогональных матриц можно осуществлять на основе циклических разностных множеств типа Адамара с одноуровневой периодической автокорреляционной функцией. На основании полученных выводов синтезирован новый метод поиска (рис.1), при котором дизайн будущей матрицы задается первой строкой последовательности, основанной на разностных множествах Адамара, что упрощает процесс получения матрицы ввиду отсутствия необходимости поиска расположения элементов в ней перебором.

Необходимость этапов 3 – 7 следует непосредственно из квадратичного условия связи квазиортогональных матриц (1), согласно которому все элементы вне главной диагонали должны быть равны нулю.

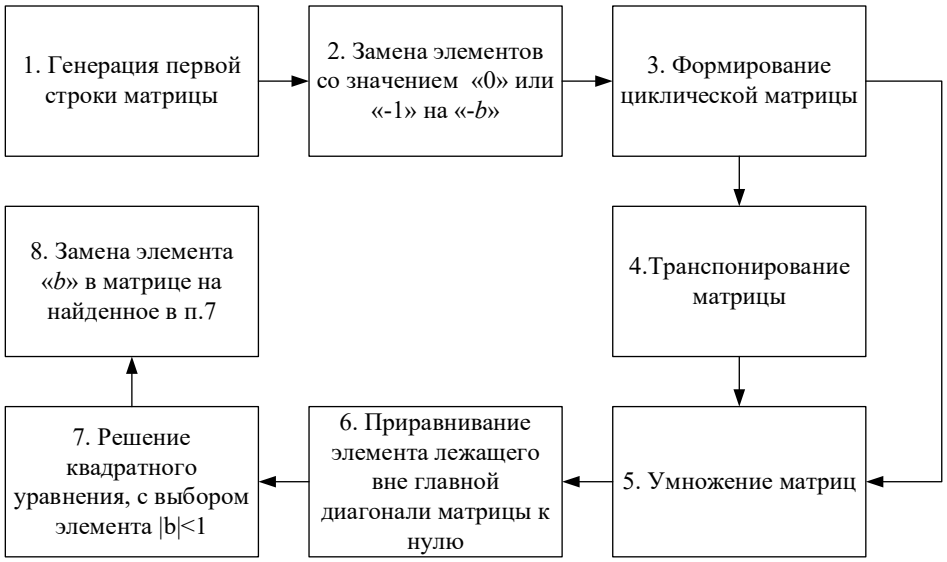


Рис. 1 – Структурная схема предложенного метода

Рассмотрены примеры применения метода. В частности, пусть первая строка матрицы сформирована на основе m-последовательности длиной $n = 15$. Для генерации m-последовательности используется примитивный полином $x^4 + x^3 + 1$ с вектором начального состояния регистра сдвига [0 0 0 1]. Получаем последовательность (1,0,0,0,1,1,1,1,0,1,0,1,1,0,0). В соответствии с методом заменим «0» на «-b», получая первую строку циклической матрицы (1,-b,-b,-b,1,1,1,1,-b,1,-b,1,1,-b,-b). Последовательным циклическим сдвигом вправо первой строки получаем матрицу $\mathbf{M}_{15}$ в виде

$$\mathbf{M}_{15} = \begin{bmatrix} 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b \\ -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b \\ -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 \\ 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 \\ 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b \\ -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 \\ 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 & -b \\ -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 & 1 \\ 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 & 1 \\ 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 & 1 \\ 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b & 1 \\ 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b & -b \\ -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b & -b \\ -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 & -b \\ -b & -b & -b & 1 & 1 & 1 & 1 & -b & 1 & -b & 1 & 1 & -b & -b & 1 \end{bmatrix},$$

Транспонированная матрица соответственно равна:

$$\mathbf{M}_{15}{}^{T} = \begin{bmatrix} 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b \\ -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b \\ -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b \\ -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 \\ 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 \\ 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 \\ 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 \\ 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b \\ -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 \\ 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 & -b \\ -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 & 1 \\ 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b & 1 \\ 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b & -b \\ -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 & -b \\ -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b & 1 \end{bmatrix}.$$

В результате умножения двух матриц получаем, матрицу с элементами $7b^2 + 8$ на главной диагонали, и элементами $3b^2 - 8b + 4$ вне главной диагонали:

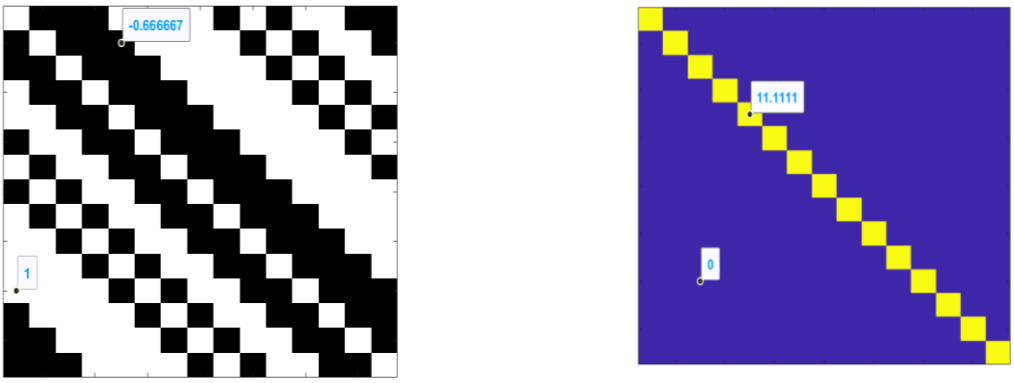
$$\mathbf{M}_{15}\mathbf{M}_{15}^{T}=\begin{pmatrix} 7b^2+8 & 3b^2-8b+4 & \cdots & & 3b^2-8b+4 \\ 3b^2-8b+4 & 7b^2+8 & & & \\ \vdots & & 7b^2+8 & & \\ & & & \ddots & \\ 3b^2-8b+4 & & & & 7b^2+8 \end{pmatrix}.$$

Приравнивая элемент вне главной диагонали к нулю и решая квадратное уравнение, получаем два корня: $b_1 = 0.6667$ и $b_2 = 2$. Выбирая элемент по модулю меньше 1, получаем искомое для квазиортогональной матрицы значение $b = 0.6667$.

Портрет полученной двухуровневой циклической квазиортогональной матрицы и результат ее проверки на квазиортогональность представлены на рис. 2.

В качестве основы для поиска матриц могут быть использованы последовательности Лежандра и Якоби, m-последовательности, GMW-последовательности, WG-последовательности, 3-term и 5-term последовательности.

Предложенный метод поиска квазиортогональных матриц увеличивает их представительство по порядкам и расширяет возможности использования в различных сферах их применения.



а) б)

Рис. 2. – Результат работы предлагаемого метода. Портреты матрицы $\mathbf{M}_{15}$ (а) и результата умножения $\mathbf{M}_{15}\mathbf{M}_{15}^{T}$ (б)

В третьем разделе проведен обзор применения двухуровневых квазиортогональных матриц с симметриями в задачах поиска КП с хорошими корреляционными свойствами, а также сжатия, маскирования и помехоустойчивого кодирования визуальной информации.

Проанализированы математические преобразования для одностороннего и двустороннего маскирования визуальной информации. В первом варианте, исходное

изображение (или фрагмент изображения) $\mathbf{X}_n$ размера $n \times n$ умножается на матрицу $\mathbf{P}_n$ того же размера в виде:

$$\mathbf{Y}_n = \mathbf{X}_n \mathbf{P}_n, \quad (2)$$

где $\mathbf{Y}_n$ – передаваемое по коммуникационному каналу в цифровом виде защищенное изображение.

Во втором варианте исходное изображение (или его фрагмент) умножается на матрицу маскирования $\mathbf{P}_n$ слева и транспонированную матрицу $\mathbf{P}_n^{\mathrm{T}}$ справа в виде:

$$\mathbf{Y}_n = \mathbf{P}_n \mathbf{X}_n \mathbf{P}_n^{\mathrm{T}}, \quad (3)$$

Обратные преобразования для получения исходного изображения при одностороннем и двустороннем маскировании выполняются как:

$$\mathbf{X}_n = \mathbf{Y}_n (\mathbf{P}_n)^{-1}, \quad (4)$$

$$\mathbf{X}_n = (\mathbf{P}_n)^{-1} \mathbf{Y}_n (\mathbf{P}_n^{\mathrm{T}})^{-1}, \quad (5)$$

Математическая простота пар преобразований (2), (4) и (3), (5) позволяет применять их для цифровой информации любого рода, при соответствующей подготовке входных данных. Предложен метод матричного маскирования аудиофайлов, использующий найденные в работе циклические квазиортогональные матрицы.

Подготовка данных в методе матричного маскирования аудиофайлов осуществляется следующим образом: аудиофайлы, представляющие собой набор цифровых отсчетов, преобразуются в квадратную матрицу путем распределения фрагментов аудиоданных последовательно по строкам, как это показано на рис. 3. В случае необходимости данные дополняются нулевыми отсчетами для обеспечения равенства размеров данных и размеров матрицы маскирования.

При этом размеры аудиоданных в матричном виде могут выбираться из двух соображений – либо кратно объему данных, передаваемых, например, в пакетах при передаче по IP-сетям, либо исходя из доступных размеров маскирующей матрицы. В случае, если доступная квазиортогональная матрица значительно меньше размеров входного набора аудиоданных – последний разбивается на блоки, и каждый блок умножается на матрицу маскирования, как показано на рис. 4.

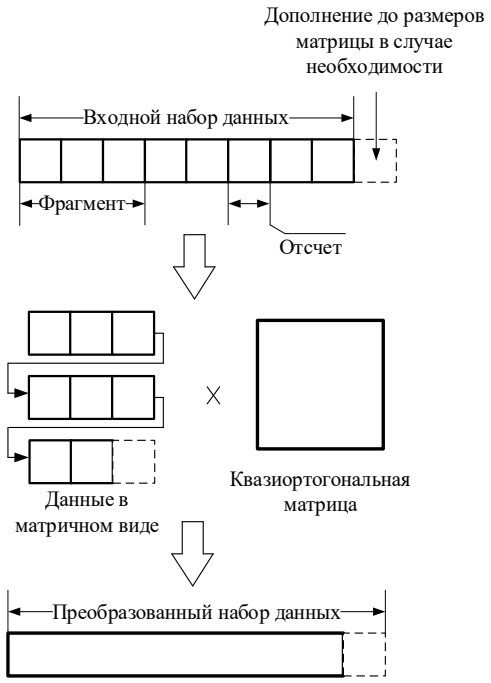


Рис. 3 - Преобразование аудиоданных в матричный вид и их умножение на квазиортогональную матрицу

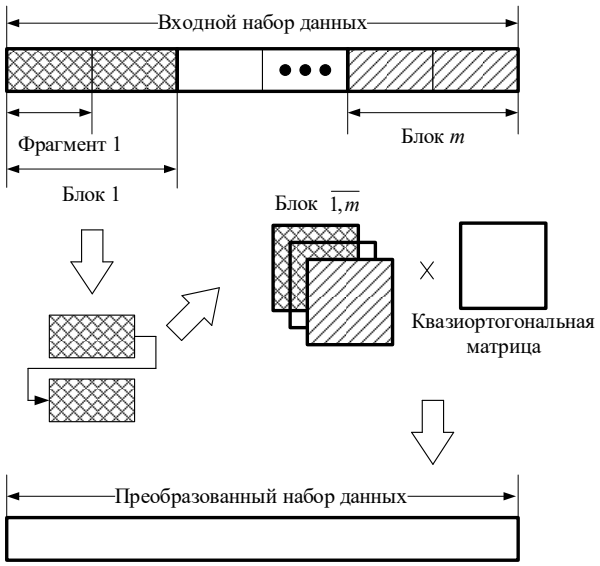


Рис. 4 - Вариант маскирования аудиоданных с использованием матрицы малых размеров

В четвертом разделе выделены три стратегии поиска и вычисления циклических квазиортогональных матриц как основы КП с улучшенными корреляционными свойствами:

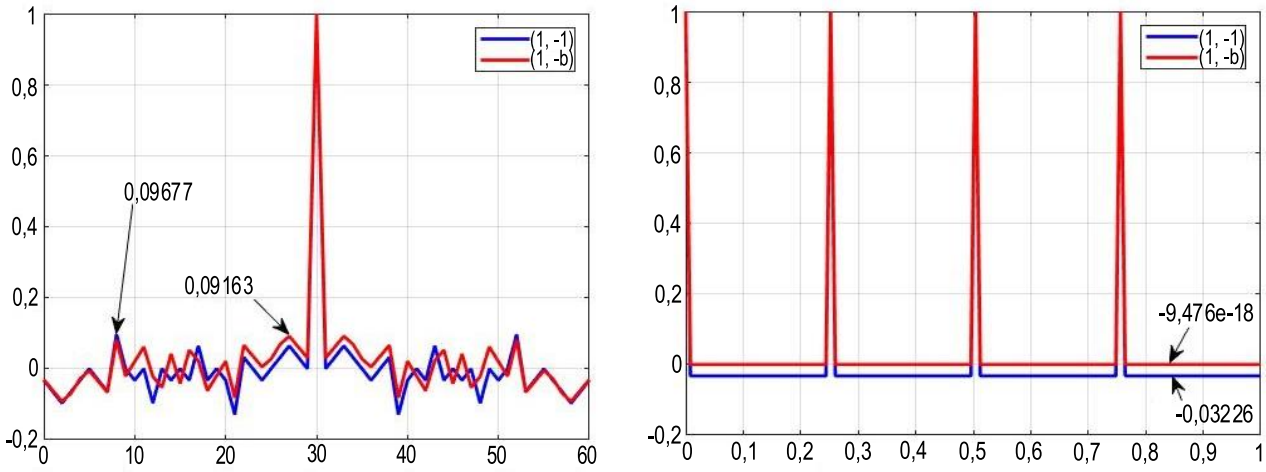
Стратегия 1. Вычисление первой строки циклической матрицы на основе символов Лежандра;

Стратегия 2. Вычисление первой строки циклической матрицы на основе символов Якоби;

Стратегия 3. Вычисление первой строки циклической матрицы на основе m–последовательности.

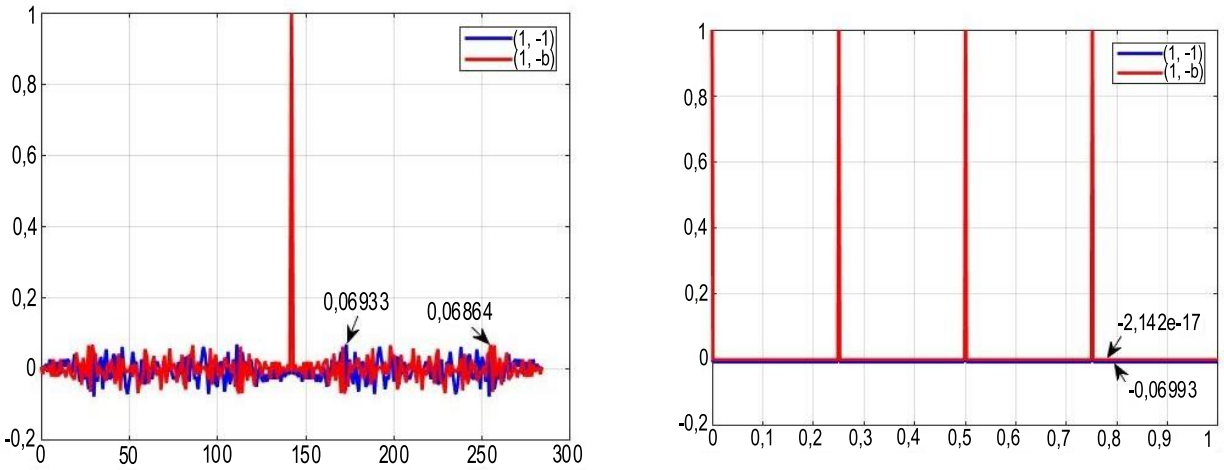
Проведен сравнительный анализ нормированных к единице апериодических автокорреляционных функций (ААКФ) и периодических автокорреляционных функций (ПАКФ) КП, основанных на разностных множествах Адамара и КП, основанных на строках найденных в работе циклических квазиортогональных матриц. Для оценки использовались такие критерии как максимальный уровень бокового лепестка (УБЛ), интегральный уровень бокового лепестка ISLR (аббр. от англ. Integrated Sidelobe Level Ratio) и мерит-фактор (MF, аббр. от англ. Merit Factor) как метрики, наиболее часто используемые для анализа корреляционных функций.

На рис. 5-7 для примера приведены графики, демонстрирующие улучшение корреляционных свойств ААКФ, при сохранении количества уровней ПАКФ для каждой стратегии поиска матриц.



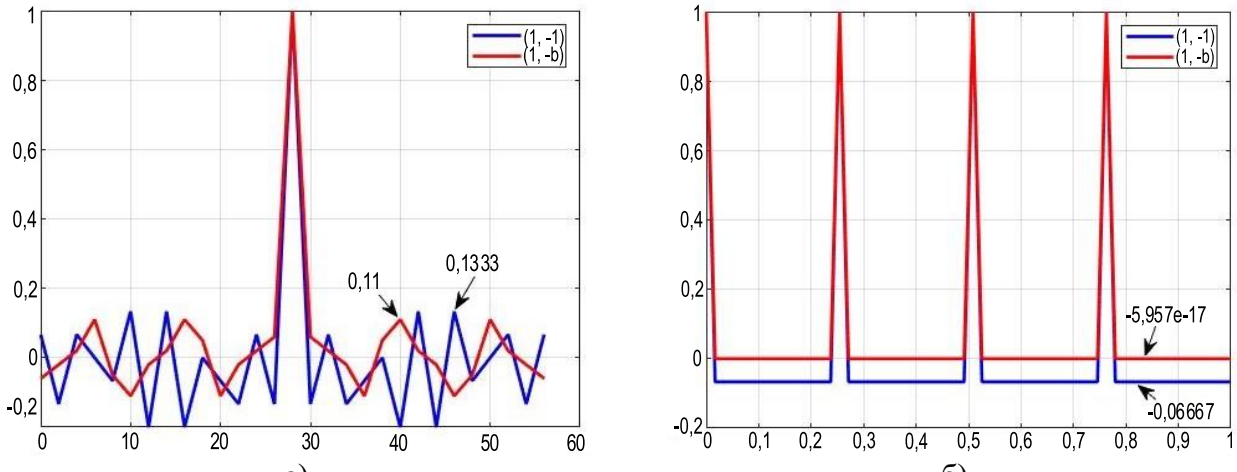
а) ААКФ б) ПАКФ

Рис. 5 - АКФ кодовых последовательностей, полученных по стратегии 1, $N = 31$



а) ААКФ б) ПАКФ

Рис. 6 - АКФ кодовых последовательностей, полученных по стратегии 2, $N = 143$



а) б)

Рис. 7 - АКФ кодовых последовательностей, полученных по стратегии 3, $N = 15$

Результаты, анализа критериев показали, что новые КП с алфавитом $\{1; -b\}$, полученные по стратегиям 2 и 3, обеспечили как снижение максимального УБЛ, так и снижение суммарной энергии боковых лепестков, в отличии от классического подхода, когда алфавит КП представлен элементами (1, –1), на порядках 143 и 899 для стратегии 2 и на

порядках 15 и 511 для стратегии 3. По стратегии 1 наблюдается улучшение по критерию максимального уровня бокового лепестка, однако на длинах кодов 31, 331, 503, 587, 719, 1307, 1423 и 1511 суммарная энергия боковых лепестков выше, чем у кодовых последовательностей с алфавитом (1; –1).

Исследование КП с несимметричным алфавитом {1, $-b$}, основанных на строках циклических квазиортогональных матриц, расширяет математический базис кодирования. Данный результат является практически значимым при разработке современных помехоустойчивых кодов и комбинаций вложенных кодовых последовательностей различной длины. Полученные теоретические результаты могут стать базой для разработки новых радиотехнических устройств и систем нового поколения, предназначенных для обнаружения, оценки координат и формирования радиолокационного изображения, а также новых методов помехоустойчивой и скрытой передачи данных в условиях сложной электромагнитной обстановки.

В разделе проведен спектральный анализ изображений, маскированных квазиортогональными матрицами разных видов и порядков, представленных в табл.1.

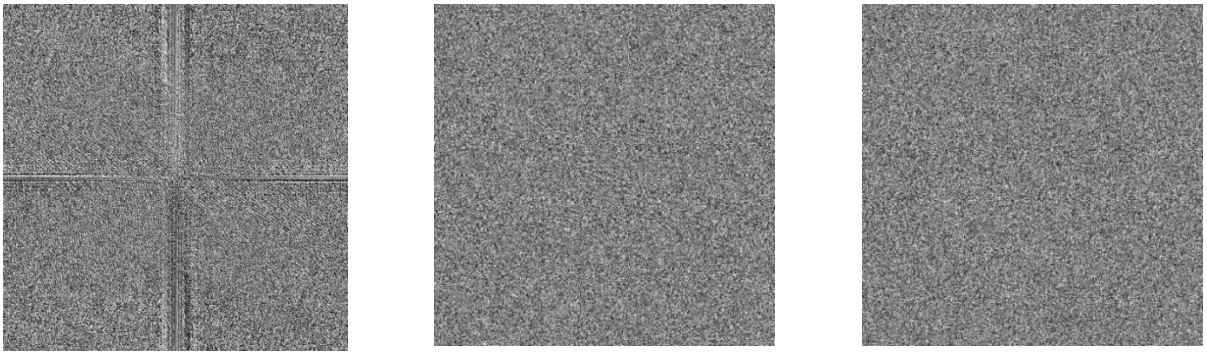
Табл.1. Матрицы, используемые при спектральном анализе результатов маскирования

№	Матрица	Структура	Уровни
1	Адамара, вычисленные методом Сильвестра	Симметричная	+1,-1
2	Адамара, структурированные по Уолшу	Симметричная	+1,-1
3	Мерсенна, структурированные по Уолшу	Симметричная	+1, -b
4	Мерсенна, структурированные по Уолшу, модульно двухуровневая	Симметричная	+1, -1, b, -b
5	На основе m-последовательности (найденные в работе)	Циклическая	+1, -b

Получены новые результаты, представляющие значительный интерес. Например, при одностороннем маскировании матрицами 1, 2 и 4 из табл. 1, из амплитудного и фазового спектров извлекаема информация о размере матрицы маскирования, что позволяет осуществить ее подбор. Однако для матриц 3 и 5 такая информация не извлекается. Дополнительно было выявлено, что при двустороннем маскировании по (3) матрицами циклической структуры, найденными при помощи предлагаемого в диссертационной работе метода, в случае одинакового размера изображения $\mathbf{X}_n$ и матрицы маскирования $\mathbf{P}_n$, фазовый спектр маскированного изображения преобразуется к шумоподобному виду, равномерно распределенному на интервале $[-\pi;+\pi]$, как показано на рис.8.

В области маскирования изображений исследование предлагаемых матриц и их сравнение с матрицами симметричной структуры позволяет сделать вывод, что циклическая структура матрицы приводит фазовый спектр маскированного изображения к виду, близкому по спектру к равномерному шуму, что при равенстве размера изображения и размера матрицы маскирования делает их применение более предпочтительным, исходя из соображений о том,

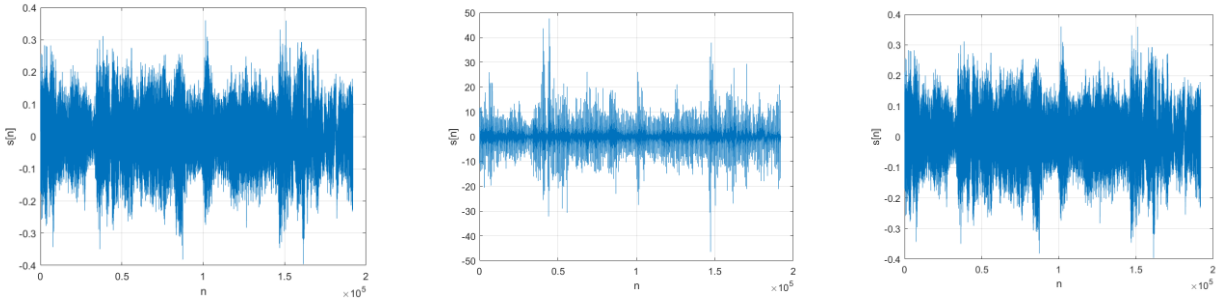
что зрительная система человека крайне чувствительна к фазо-частотным искажениям визуальной информации.



а) б) в)

Рис.8 - Двумерные фазовые спектры: исходного изображения $\mathbf{X}_n$ (а); изображения, маскированного циклической матрицей 5 из табл.1 (б); матрицы с равномерно распределенными элементами на интервале [-π;+π]

Далее в разделе приведены результаты экспериментов по маскированию несжатых аудиоданных формата .wav с использованием циклических матриц, которые были найдены при помощи предлагаемого в диссертационной работе метода. Источником тестовых аудиоданных выбран набор данных «UrbanSound8K». Частота дискретизации аудиофайлов составляет 48 КГц. Для примера на рис. 9 представлен результат маскирования по (3) и демаскирования по (5) звукового файла 108362-2-0-23.wav из указанного набора данных.



а) б) в)

Рис. 9 – Графики отсчетов исходного (а), маскированного (б) и демаскированного (в) аудиофайлов

Графики исходного и демаскированного аудиофайлов совпадают, подтверждая симметричность преобразования. Это подтверждено и объективными метриками MSE (среднеквадратичная ошибка) и SNR (отношение сигнал/шум).

Проведенные многочисленные эксперименты показали, что классические метрики, MSE и SNR не определяют качество маскирования аудиофайлов, поскольку субъективно, на слух, из аудиофайлов с самым низким и самым высоким значениями MSE затруднительно определить их содержание. Сделан вывод о том, что классические объективные метрики

(например MSE, SNR и т.д.) не определяют качество маскирования – разрушения информации до уровня шума.

Предложен подход к определению качества маскирования звукового сигнала, основанный на оценке близости амплитудного спектра маскированных аудиоданных к амплитудному спектру гауссовского шума с математическим ожиданием и среднеквадратическим отклонением, равными аналогичным характеристикам маскированных аудиоданных.

Это предложение обосновывается тем, что из шума невозможно что-либо услышать, а объективно – затруднительно извлечь какую-либо информацию.

В основе подхода лежит следующая последовательность действий:

1) вычисляется математическое ожидание и среднеквадратическое отклонение маскированного аудиофайла;

2) формируется набор отсчетов гауссовского шума с математическим ожиданием и среднеквадратическим отклонением равными аналогичным параметрам маскированного аудиофайла;

3) вычисляется Фурье-спектр шума и маскированного аудиофайла с использованием алгоритма быстрого преобразования Фурье;

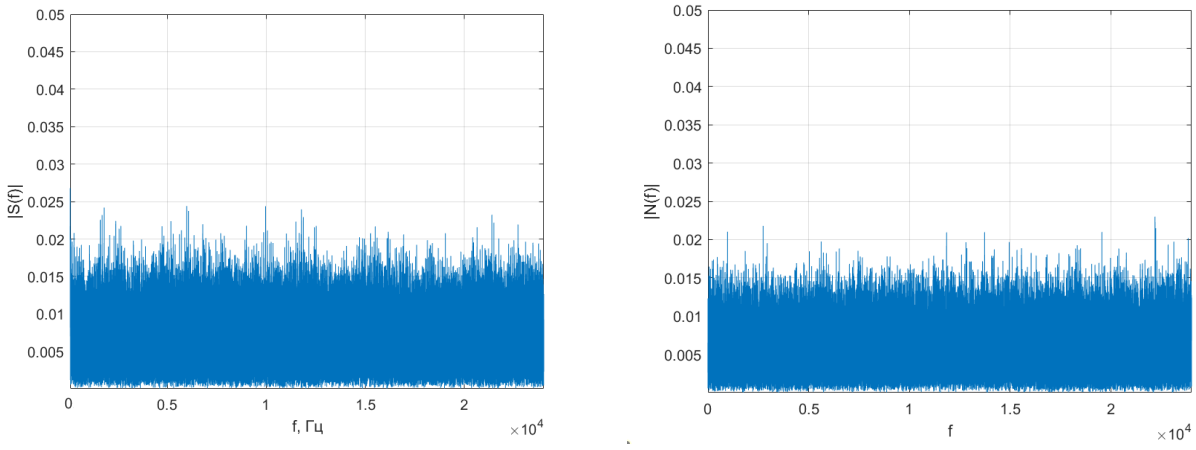
4) вычисляется амплитудный спектр маскированного аудиофайла и шума;

5) осуществляется визуальное сравнение амплитудного спектра маскированного аудиофайла и шума.

6) вычисляется корень из среднеквадратичной ошибки (RMSE) значений амплитудного спектра маскированного аудиофайла и шума.

Матрицы, лучше разрушающие аудиофайлы при маскировании, будут обладать меньшим значением RMSE между значениями амплитудного спектра маскированного аудиофайла и шума.

В качестве примера на рис. 10 приведены амплитудные спектры маскированного аудиофайла (а) и гауссовского шума с математическим ожиданием и среднеквадратическим отклонением, равными аналогичным параметрам маскированного аудиофайла.



а) б)

Рис. 10. Графики амплитудных спектров аудиофайлов

В области маскирования аудиофайлов маскирующее преобразование приводит цифровые аудиоданные к виду, близкому по спектру к белому шуму, что надежно защищает ее в коммуникационном канале от несанкционированного доступа.

Замечено, что маскирующее преобразование усиливает амплитуду входного аудиофайла. И в данном случае использование предлагаемых циклических матриц является преимуществом, поскольку симметричные матрицы Адамара зачастую имеют кайму в виде первой строки и первого столбца, заполненных единицами. Это при умножении матриц дает большее усиление первого элемента первого столбца результата умножения, приводящее к переполнению разрядной сетки вычислителя. В случае двустороннего маскирования эффект будет лишь усиливаться. Предлагаемые в работе циклические матрицы лишены указанного недостатка, поскольку количество положительных и отрицательных элементов в строках и столбцах матрицы отличается всего на единицу.

ЗАКЛЮЧЕНИЕ

Основные результаты проведенных в диссертационной работе исследований направлены на расширение набора доступных матриц для решения задач, связанных с обработкой, кодированием и передачей информации.

Выделенные в диссертации взаимосвязи между бинарными кодовыми последовательностями с одноуровневой периодической автокорреляционной функцией и строками квазиортогональных матриц позволили синтезировать новый метод поиска двухуровневых циклических квазиортогональных матриц. Прикладной стороной метода является его использование при разработке алгоритмов и программ на их основе, реализующих поиск и вычисление структурированных квазиортогональных матриц высоких порядков, строки которых могут быть также использованы в качестве кодовых последовательностей.

Результаты анализа корреляционных характеристик новых кодовых последовательностей, основанных на строках найденных циклических квазиортогональных матриц, показали, что одним из возможных направлений развития систем обработки информации является смена парадигмы о том, что используемые кодовые последовательности должны быть двоичными и симметричными, в пользу недвоичных и несимметричных последовательностей с алфавитом $\{1,-b\}$, что позволит повысить их помехозащищенность. В частности, скрытность может быть повышена за счет трудности вычисления элемента b для сигналов, использующих в своей основе последовательности с несимметричным алфавитом, а помехоустойчивость может быть повышена за счет снижения максимального уровня боковых лепестков и снижения их суммарной энергии.

Результаты моделирования и экспериментов показали, что предлагаемые циклические матрицы могут быть эффективно применены для маскирования аудиофайлов и изображений различного содержания. При этом достигается большее сокрытие спектральных составляющих передаваемых данных, что препятствует несанкционированному доступу к ним

при передаче. Оценка эффективности маскирования при этом впервые производилась за счет разработанного в диссертации единого подхода к оценке качества маскирования цифровой информации, основанного на степени близости спектральных компонент маскированных данных к спектральным компонентам белого шума. Это открывает новые возможности для защиты конфиденциальной цифровой информации с небольшим периодом актуальности в различных областях применения.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, включенных в перечень ВАК

1. Григорьев, Е.К. Анализ спектральных характеристик результатов матричного маскирования изображений / Е.К. Григорьев // Труды учебных заведений связи. – 2024. – Т. 10, № 2. – С. 76-82.

2. Григорьев, Е.К. Оценка качества матричного маскирования цифровых звуковых данных / Е.К. Григорьев, А.М. Сергеев // Труды учебных заведений связи. – 2023. – Т. 9, № 3. – С. 6-13.

3. Григорьев, Е.К. Способ защитного кодирования данных, получаемых оптическими сенсорами беспилотных авиационных систем / Е.К. Григорьев, А.М. Сергеев // Труды МАИ. – 2023. – № 133.

4. Григорьев, Е.К. Анализ корреляционных характеристик новых кодовых последовательностей, основанных на персимметричных квазиортогональных циркулянтах / Е.К. Григорьев // Труды учебных заведений связи. – 2022. – Т. 8, № 2. – С. 83-90.

5. Григорьев, Е.К. Поиск и модификация кодовых последовательностей на основе персимметричных квазиортогональных циркулянтов / Е.К. Григорьев, В.А. Ненашев, А.М. Сергеев, Е.В. Самохина // Телекоммуникации. – 2020. – № 10. – С. 27-33.

Публикации в изданиях, входящих в международные базы цитирования

6. Grigoriev, E.K. Quasi-orthogonal Structured Mersenne Matrices for Masking Digital Video and Audio Data in Distributed Systems / A. M. Sergeev, E. K. Grigoriev // Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance, IPSQDA-2023. – 2023. – P.57-59.

7. Grigoriev, E.K. Triple-Station System of Detecting Small Airborne Objects in Dense Urban Environment / M.B. Sergeev., A.A. Sentsov, V.A. Nenashev, E.K. Grigoriev // Smart Innovation, Systems and Technologies, vol 238. Springer, Singapore. – 2021. – P. 83-93.

8. Grigoriev, E. K. Research of compression characteristics of modulated ultra-wideband signals formed on the basis of circulants of quasi-orthogonal matrices / E. K. Grigoriev, A. M. Sergeev, V. A. Nenashev, I. R. Gordeev // Proceedings of. SPIE V. 11862, Image and Signal Processing for Remote Sensing XXVII. 118620Z.

9. Grigoriev, E. K. Research and analysis of methods for generating and processing new code structures for the problems of detection, synchronization and noise-resistant coding / E.K. Grigoriev,

V. A. Nenashev, A. M. Sergeev, S. A. Nenashev /, Proceedings of. SPIE 11533, Image and Signal Processing for Remote Sensing XXVI. 115331L.

Патент на изобретение

10. Устройство формирования модифицированных М-последовательностей: № 2023105091 от 06.03.2023 / Е.К. Григорьев, А.М. Сергеев, В.А. Ненашев, Д.В. Куртяник / Патент № 2801743 C1 Российская Федерация, МПК H03K 3/00. Заявитель и патентообладатель Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения".

Результаты интеллектуальной деятельности

11. Программа маскирования и демаскирования звуковой цифровой информации. Модуль маскирования. / Е.К. Григорьев, М.Б. Сергеев, А.М. Сергеев / Свидетельство о регистрации программы для ЭВМ № 2023614623 от 03.03.2023.

12. Программа маскирования и демаскирования звуковой цифровой информации. Модуль демаскирования. / Е.К. Григорьев, М.Б. Сергеев, А.М. Сергеев / Свидетельство о регистрации программы для ЭВМ № 2023614622 от 03.03.2023.

13. MATLAB-библиотека для генерации и анализа персимметричных квазиортогональных циркулянтов / Е.К. Григорьев / Свидетельство о государственной регистрации программы для ЭВМ № 2022683231 от 02.12.2022.

14. Программа генерации и анализа корреляционных характеристик новых кодовых конструкций, основанных на персимметричных квазиортогональных циркулянтах / М.Б. Сергеев, Е.К. Григорьев, В.А. Ненашев, С.А. Ненашев / Свидетельство о государственной регистрации программы для ЭВМ № 2021615538 от 09.04.2021.

15. Программа поиска и анализа новых маркированных многоуровневых кодовых конструкций на основе циркулянтов квазиортогональных матриц произвольной длины / Е.К. Григорьев, В.А. Ненашев, И.Р. Гордеев, К.Ю. Рыжов / Свидетельство о государственной регистрации программы для ЭВМ № 2021664610 от 09.09.2021.

16. Программа вычисления структурированных квазиортогональных матриц Мерсенна / А.А. Востриков, А.М. Сергеев, Е.К. Григорьев [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019612775 от 27.02.2019.

17. Программа генерации квазиортогональных циклических матриц, сформированных на основе вычисления квадратичных вычетов / Е.К. Григорьев, А.П. Шепета, М.Б. Сергеев [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019612935 от 04.03.2019

18. Программа генерации специальных квазиортогональных циклических матриц, сформированных на основе вычисления символов Якоби / А.А. Востриков, А.М. Сергеев, Е.К. Григорьев [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019660821 от 13.08.2019.

19. Программа вычисления специальных структурированных квазиортогональных матриц Мерсенна-Уолша / В.А. Ненашев, М.Б. Сергеев, Е.К. Григорьев [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019660998 от 16.08.2019.

20. Программа генерации специальных квазиортогональных матриц, сформированных на основе модифицированных m-последовательностей / Е.К. Григорьев, М.Б. Сергеев, А.М. Сергеев [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019664813 от 13.11.2019.

21. Программа поиска специальных квазиортогональных матриц и генерации новых маркированных кодовых конструкций максимальной длины / Е.К. Григорьев, М.Б. Сергеев, А.П. Шепета [и др.] / Свидетельство о государственной регистрации программы для ЭВМ № 2019664814 от 13.11.2019.

Публикации в других изданиях и сборниках научных трудов и конференций

22. Григорьев, Е.К. О построении интеллектуальной системы управления распределенными радиолокационными средствами для обнаружения объектов малоразмерной авиации в условиях плотной городской застройки / А.А. Сенцов, М.Б. Сергеев, Е.К. Григорьев // Вестник Российского фонда фундаментальных исследований. – 2024. – № 1(121). – С. 45-54.

23. Григорьев, Е.К. Стратегии вычисления персимметричных циклических квазиортогональных матриц как основы кодов / В.А. Ненашев, Е.К. Григорьев, А.М. Сергеев, Е.В. Самохина // Электросвязь. – 2020. – № 10. – С. 58-61.

24. Григорьев, Е.К. Об одном подходе к оценке качества маскирования визуальной информации / Е.К. Григорьев // Обработка, передача и защита информации в компьютерных системах 24: Сборник докладов Четвертой Международной научной конференции, Санкт-Петербург, 8–15 апреля 2024 года. – Санкт-Петербург: ГУАП, 2024. – С. 187-192.

25. Способ сжатия изображений в пространственно-распределенной системе интенсивного обмена информацией / В.А. Ненашев, А.А. Сенцов, Е.К. Григорьев [и др.] // Обработка, передача и защита информации в компьютерных системах’23: Сборник докладов Третьей Международной научной конференции, Санкт-Петербург, 10–17 апреля 2023 года. – Санкт-Петербург: ГУАП, 2023. – С. 196-201.

26. Grigoriev, E.K. Study of code sequences for modulating the phase of a radio signal / E. Grigoriev // Bulletin of the UNESCO department “Distance education in engineering” of the SUAI: Collection of the papers. Issue 7. – Saint-Petersburg: SUAI, 2022. – P. 97-102.

27. Григорьев, Е.К. Помехоустойчивые кодовые конструкции для синхронизации функционирования пространственно-распределенных портативных РЛС / Е.К. Григорьев, С.А. Ненашев // Современные технологии в задачах управления, автоматики и обработки информации: Сборник трудов XXIX Международной научно-технической конференции, Алушта, 14–20 сентября 2020 года. – Москва: Издательский Дом «МЕДПРАКТИКА-М», 2020. – С. 142-143.

28. Grigoriev, E.K. Methods of generation and analysis of strategies for calculating cyclic quasi orthogonal matrices / E.K. Grigoriev // Bulletin of the UNESCO department “Distance

education in engineering” of the SUAI: Collection of the papers. Vol. Issue 5. – Saint-Petersburg: SUAI, 2020. – P. 73-76.

Подписано в печать 30.06.2025. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1