МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

На правах рукописи

Григорьев Евгений Константинович

ПОИСК И ПРИМЕНЕНИЕ ЦИКЛИЧЕСКИХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ В ЗАДАЧАХ ОБРАБОТКИ ИНФОРМАЦИИ

Специальность 2.3.1. Системный анализ, управление и обработка информации, статистика

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:
д.т.н., профессор М.Б. Сергеев

Санкт-Петербург – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы. 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. Среди разнообразия матриц особое место занимают квадратные ортогональные матрицы. К таким матрицам относятся, например, матрицы дискретного косинусного преобразования (ДКП), а также матрицы Адамара, Белевича, Хаара, и другие.

Для решения прикладных задач, рекомендуется обеспечивать простоту структуры ортогональной матрицы. Среди базовых матричных структур, нашедших практическое применение, 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 существуют следующие проблемы – во-первых, согласно предположению, Раймонда Пэли (гипотезе Адамара) данные матрицы существуют только на четных порядках $4t$, где t-натуральное число, а, во-вторых, согласно гипотезе Г. Райзера циклические конструкции матриц Адамара ограничены четвертым порядком. 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 научной литературы показывает, что существуют двухуровневые {1, $-b$} квазиортогональные матрицы Мерсенна локального максимума детерминанта,

обобщающие матрицы Адамара и существующие на нечетных порядках $4t - 1$, тесно связанных с матрицами Адамара. Существуют различные конструкции таких матриц, но преимущественно они являются циклическими.

Квазиортогональные матрицы Мерсенна 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 Жак Адамар, Раймонд Пэли, Джеймс Сильвестр, Умберто Скарпи, Джон Райзер, Дженифер Себбери, Драгомир Джокович, Л. А. Мироновский, Н. А. Балонин, М. Б. Сергеев, А. М. Сергеев, Натан Блаунштейн, I. Kotsireas и др.

Вопросы практического применения ортогональных матриц для задач, связанных с темой диссертационной работы, рассматривались в работах N. Ahmed, K. J. Horadam, Л.А. Мироновского, В. А. Слаева, М. Ямады, Дж. Себерри, Г. Куковинаса, 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, также 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 Международных научных конференциях «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. Также были 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 подхода к анализу качества разрушения маскированных звуковых и визуальных данных.

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

1 ОРТОГОНАЛЬНЫЕ И КВАЗИОРТОГОНАЛЬНЫЕ МАТРИЦЫ В ОБРАБОТКЕ ИНФОРМАЦИИ

1.1. Основные определения

Термин «матрица» был введен в научный оборот Джеймсом Сильвестром относительно недавно – в 1850 году, хотя так называемые магические таблицы появились еще в древнем Китае и далее использовались как в арабском мире, так и средневековой Европе [1].

В настоящее время, вычисления с использованием матриц применяются во многих областях науки и техники, включая линейную алгебру, физику, компьютерную графику, компьютерные науки, машинное обучение, статистику, экономику, химию, биологию и другие [2-6].

Приведем основные сведения из теории матриц [1-2, 7-8], необходимые для дальнейшего изложения материала.

Определение 1. *Матрицей* будем называть совокупность комплексных или вещественных чисел, собранных в табличной форме в виде:

$$\mathbf{A}=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix},$$

где числа a_{nm} называются элементами матрицы. Индексы n и m означают, что элемент матрицы a_{nm} располагается на пересечении n-й строки и m-го столбца матрицы. В случае $n=m$ матрица будет называться квадратной, а число n (равное m), называется *порядком матрицы* [1].

Определение 2. *Уровни* матрицы – значения, которые имеют ее элементы.

Определение 3. Под *модульными уровнями матрицы* будем понимать модули численных значений элементов, а под *модульной уровневостью*, соответственно, их количество.

Определения 2 и 3 рассмотрим на примере. Пусть дана матрица:

$$\mathbf{A}=\begin{pmatrix} 0 & -1 & -1 & -1 \\ -4 & 0 & 1 & -1 \\ -4 & 4 & 0 & -1 \\ -4 & -4 & -4 & 0 \end{pmatrix}.$$

Данная матрица пятиуровневая {0,-1,1,-4,4} и модульно трехуровневая {0,1,4}.

Определение 4. Матрица **I**, у которой на главной диагонали расположены единицы, а вне главной диагонали нули – *единичная матрица*.

Определение 5. Под *произведением двух матриц*

$$\mathbf{A}=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}, \mathbf{B}=\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

будем понимать матрицу

$$\mathbf{C}=\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1m} \\ c_{21} & c_{22} & \dots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nm} \end{pmatrix},$$

у которой элемент c_{ij} равен:

$$c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj} \qquad \left(i=1,2,\dots n;\ j=1,2,\dots m\right).$$

Отметим тот факт, что умножение двух квадратных матриц одинакового порядка всегда выполнимо.

Определение 6. Под *кронекеровым произведением* двух матриц **A** и **B** будем понимать вставку матрицы **B** по месту каждого элемента матрицы **A** с умножением на этот элемент:

$$\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \dots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \dots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \dots & a_{nn}\mathbf{B} \end{pmatrix}.$$

Определение 7. Под *транспонированием* будем понимать замену строк матрицы **A** ее столбцами:

$$\mathbf{A}=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}, \mathbf{A}^{\mathbf{T}}=\begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \dots & a_{nm} \end{pmatrix}.$$

Определение 8. Если матрица **A** квадратная и неособенная (определитель матрицы не равен нулю), то для нее существует *обратная матрица* $\mathbf{A}^{-1}$, для которой выполняется

$$\mathbf{A}^{-1}\mathbf{A}=\mathbf{I}.$$

Определение 9. *Симметричной матрицей* называется матрица, инвариантная к операции транспонирования $\mathbf{A}^{\mathbf{T}}=\mathbf{A}$.

Определение 10. Матрицу с симметрией относительно побочной диагонали, для которой справедливо $a_{ij} = a_{n-j+1,n-i+1}$, для любых i и j будем называть *персимметричной*.

Определение 11. Матрицу **A** построенную циклическим сдвигом вправо первой строки

$$\mathbf{A}=\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_n & a_1 & \dots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix},$$

будем называть *циклической матрицей*. Циклические матрицы также являются персимметричными матрицами [1].

Определение 12. Матрица **A** называется *ортогональной* в случае выполнения следующего соотношения:

$$\mathbf{A}\mathbf{A}^{\mathbf{T}} = \mathbf{A}^{\mathbf{T}}\mathbf{A} = \mathbf{I},$$

Определение 13. Квадратная матрица **A** порядка n называется *квазиортогональной*, в случае если для приведенных к единице максимумам модулей элементов каждого из столбцов, выполняется следующее соотношение:

$$\mathbf{A}\mathbf{A}^{\mathbf{T}} = \mathbf{A}^{\mathbf{T}}\mathbf{A} = \omega\mathbf{I},$$

где ω – вес матрицы [1]. Таким образом, это матрицы, близкие к ортогональным, и становятся строго ортогональными, если нормировать их столбцы [1].

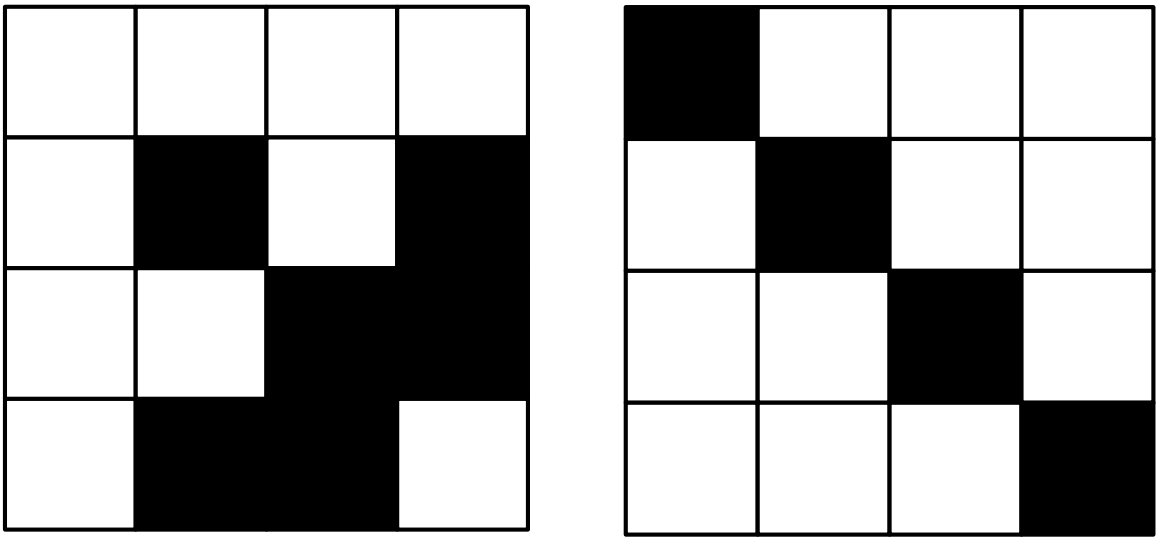
Определение 13. Под *портретом* матрицы будем понимать графическое изображение элементов матрицы в виде множества квадратов, имеющих для каждого из уровней свой цвет.

Портреты являются удобным инструментом для выявления конструктивных особенностей матриц, в том числе всех возможных симметрий.

Наиболее известными квазиортогональными матрицами являются матрицы Адамара **H** – квадратные двухуровневые {-1,1} матрицы размера $n \times n$ для которых вес ω=*n*.

На рисунке 1.1 для примера представлены портреты симметричной (а) и циклической (б) матриц Адамара 4 порядка, на которых элементы со значением «1» имеют белый цвет, а элементы со значением «-1» – черный. Следует отметить, что матрица на рисунке 1.1(б) одновременно симметричная и персимметричная.

Ортогональные и квазиортогональные матрицы обладают удобным свойством – для них обратная матрица равна транспонированной $\mathbf{A}^{-1} = \mathbf{A}^{\mathbf{T}}$, что позволяет повысить точность вычислений из-за отсутствия ошибок при вычислении обратной матрицы.



а) б)

Рисунок 1.1 – Портреты симметричной и персимметричной матриц Адамара порядка 4

Таким образом, в виду особых свойств ортогональных матриц, именно преобразования с ними широко используется в различных сферах научной и технической деятельности.

1.2. Практическое применение ортогональных матриц

На практике, наибольшее распространение получили именно ортогональные матрицы, в виду удобства и симметричности преобразований с их использованием.

Известно применение ортогональных матриц в задачах:

– анализа генетических цепочек [6];

– криптографии [9, 10] и стеганографии [11];

– параметрической оптимизации [9];

– геодезии [12];

– генерации псевдослучайных чисел [13];

– цифровой обработки изображений [14-16], в частности при вращении изображений [14], их сжатии [15] или кодировании [16];

– радиолокации и связи [17-21], например, при синтезе системы сигналов для многопозиционных радиолокационных станций [17, 18], корреляционном приеме [17, 19], помехоустойчивом кодировании [20, 21];

– кристаллографии [22];

– защитном кодировании (маскировании) визуальной [23-24] и звуковой информации [25].

Приведенные выше примеры – всего лишь часть широкого применения ортогональных матриц, требующего поиска матриц с конструктивными особенностями, влияющими на эффективность их практического использования в конкретной задаче.

При использовании матричных методов обработки информации используемые матрицы можно разделить на целочисленные и вещественные, представимые в арифметике с плавающей точкой. Однако современные процессоры позволяют сгладить различия между целочисленной и арифметикой с плавающей точкой [16,26-27], позволяя сосредоточиться не на самих уровнях матрицы, а, например, на их количестве или структурном инварианте.

В области применения ортогональных преобразований можно сформулировать следующие рекомендации:

– матрицы должны существовать на как можно большем числе порядков, в том числе на больших;

– алгоритмы получения (вычисления, генерации) матриц должны быть простыми;

– структура матриц должна быть простой, например, симметричной или циклической, что позволит оптимизировать объем памяти для их генерации и хранения;

– количество уровней матрицы по возможности должно быть минимальным, что позволит оптимизировать объем памяти, используемой для вычислений.

С учетом вышеописанных рекомендаций целесообразен анализ наиболее известных и применяемых на практике ортогональных матриц.

1.3. Используемые на практике ортогональные матрицы

Ортогональная *матрица поворота* — это матрица, которая представляет собой ортогональное преобразование в трехмерном пространстве, описывающее вращение объекта вокруг фиксированной точки.

В декартовой системе координат поворот на некоторый угол α в двумерном пространстве описывается матрицей

$$M\left(\alpha\right)=\begin{pmatrix}\cos\left(a\right) & \sin\left(a\right)\\ -\sin\left(a\right) & \cos\left(a\right)\end{pmatrix}.$$

В декартовом трехмерном пространстве поворот по осям *x*, *y* и *z* на некоторый угол α описывается последовательным произведением матриц:

$$M_x\left(\alpha\right)=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\left(a\right) & -\sin\left(a\right)\\ 0 & \sin\left(a\right) & \cos\left(a\right)\end{pmatrix},$$

$$M_y\left(\alpha\right)=\begin{pmatrix}\cos\left(a\right) & 0 & \sin\left(a\right)\\ 0 & 1 & 0\\ -\sin\left(a\right) & 0 & \cos\left(a\right)\end{pmatrix},$$

$$M_z\left(\alpha\right)=\begin{pmatrix}\cos\left(a\right) & -\sin\left(a\right) & 0\\ \sin\left(a\right) & \cos\left(a\right) & 0\\ 0 & 0 & 1\end{pmatrix}.$$

В задачах обработки сигналов, особенно изображений, значительную роль играют ортогональные базисы, описывающие поворт [1,14]. Следует отметить, что в двумерном и трехмерном вариантах – матрицы симметричны, а также обладают минимальным количеством уровней (с точки зрения решаемой задачи).

Матрица дискретного косинусного преобразования (ДКП) представляет собой основной инструмент в области сжатия данных и обработки сигналов. ДКП используется для преобразования последовательности чисел, таких как значения пикселей изображения или отсчеты амплитуды звукового сигнала. Применение ортогонального преобразования ДКП к изображению или аудиосигналу позволяет перейти к спектральному представлению, которое в большинстве практических приложений обладает более простой структурой по сравнению с исходными данными [1]. В частности, при решении задач сжатия использование матрицы ДКП приводит также и к декорреляции пикселей изображения [26].

Как известно [28], дискретное косинусное преобразование входного набора данных $X(m)$, m=0, 1, … , N-1, определяется как

$$L_x\left(0\right)=\frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}X\left(m\right),$$

$$L_x\left(k\right)=\sqrt{\frac{2}{N}}\sum_{m=0}^{N-1}X\left(m\right)\cos\left(\frac{\left(2m+1\right)\pi k}{2N}\right),$$

k=1, 2, …, N-1, где $L_x(k)$ представляет собой k-й коэффициент дискретного косинусного преобразования.

При записи данного выражения в матричной форме получаем квадратную ($N\times N$) ортогональную матрицу дискретного косинусного преобразования [28].

Возьмем в качестве примера матрицу ДКП размера 6×6:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0.965 & 0.707 & 0.258 & -0.258 & -0.707 & -0.965 \\ 0.866 & 0 & -0.866 & -0.866 & 0 & 0.866 \\ 0.707 & -0.707 & -0.707 & 0.707 & 0.707 & -0.707 \\ 0.5 & -1 & 0.5 & 0.5 & -1 & 0.5 \\ 0.258 & -0.707 & 0.965 & -0.965 & 0.707 & -0.258 \end{pmatrix}$$

Для анализа структуры целесообразно рассмотреть портрет данной матрицы, представленный на рисунке 1.2. Его анализ позволяет сделать вывод об отсутствии простоты структуры такой матрицы ДКП.

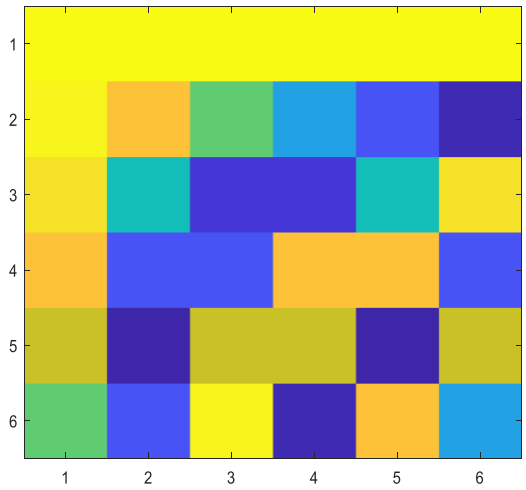


Рисунок 1.2 – Портрет матрицы ДКП 6×6

Матрица ДКП размера 8×8, используемая в стандарте JPEG, имеет еще больше уровней, что делает её неоптимальной с точки зрения вышеописанных рекомендаций. Так, известны работы с применением малоуровневых матриц симметричной структуры, показывающие не худшие по сравнению с матрицей ДКП результаты [29,30]

Матрицы Хаара получаются в результате дискретизации множества функций Хаара {har(n,m,t)} [28].

Рекуррентное соотношение для их получения выглядит следующим образом:

$$har\left(0,0,t\right)=1,t\in\left[0,1\right];$$

$$har\left(r,m,t\right)=\begin{cases} 2^{\frac{r}{2}}, \dfrac{m-1}{2^r}\le t<\dfrac{m-1/2}{2^r}; \\ -2^{\frac{r}{2}}, \dfrac{m-1/2}{2^r}\le t<\dfrac{m}{2^r}; \\ 0, \text{ при остальных } t\in\left[0,1\right], \end{cases}$$

где $0\le r<\log_2 N$ и $1\le m\le 2^r$.

В качестве примера ниже приведена матрица Хаара размером 8x8

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \end{pmatrix}.$$

Портрет данной матрицы представлен на рисунке 1.3.

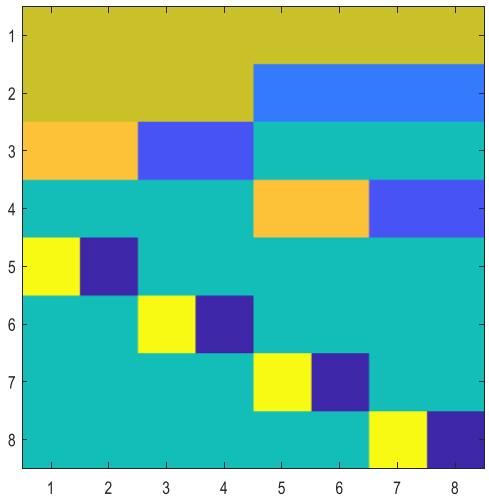


Рисунок 1.3 – Портрет матрицы Хаара 8x8

Анализ рисунка 1.3 позволяет сделать вывод об отсутствии простоты структуры матрицы Хаара, количество уровней данной матрицы не оптимально, при этом матрицы существуют только на порядках, равных степеням двойки.

Матрицы Адамара представляют особый интерес, вызванный их свойствами – они имеют минимальные первую и чебышевскую нормы, глобальный максимум детерминанта, минимальность максимального по модулю элемента и близость элементов между собой [32].

Определение 14. *Матрицей Адамара* называется матрица $\mathbf{H}_n$ порядка n с двумя уровнями элементов {+1,-1} и обладающая свойством

$$\mathbf{H}_n\mathbf{H}_n^{\mathrm{T}} = n\mathbf{I}.$$

Множитель n обратно пропорционален квадрату m-нормы, т.е. $m = 1/\sqrt{n}$ [33].

Матрицы Адамара существуют на порядках $n=4t$, где t – натуральное число. Матрицы Адамара могут иметь различную конструкцию, в том числе симметричную [34-36]. При этом структуры матриц Адамара наследуют свойства используемых методов их вычисления [37].

Исторически первый и наиболее известный – метод Сильвестра, для которого характерно удвоение порядка следующей матрицы относительно предыдущей. Для $n \geq 0$, матрица Адамара H_n порядка 2^n определяется рекурсивно следующим образом:

$$\mathbf{H}_1 = \left(1\right);$$

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

$$\mathbf{H}_{2n} = \begin{pmatrix} \mathbf{H}_n & \mathbf{H}_n \\ \mathbf{H}_n & -\mathbf{H}_n \end{pmatrix}.$$

Портрет матрицы Адамара порядка 8, вычисленной методом Сильвестра, приведен на рисунке 1.4. Здесь заметна ярко выраженная симметрия матрицы, а при увеличении порядка проявляется и симметрия, и фрактальность узора на портрете.

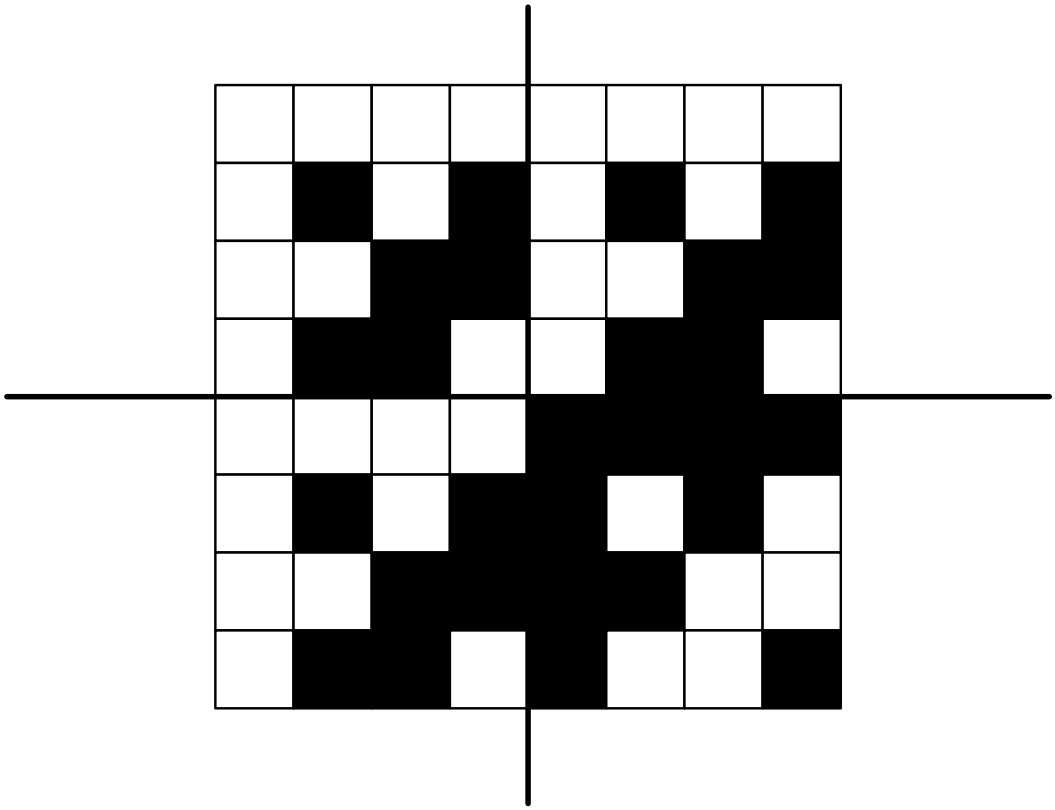


Рисунок 1.4 – Портрет матрицы $\mathbf{H}_8$, вычисленной методом Сильвестра

Умберто Скарпи предложил метод нахождения матриц Адамара с реализацией операции матричной вставки [38, 39], сведя его к операции кронекерова произведения. Метод Скарпи позволяет вычислять матрицы больших порядков, однако не гарантирует симметричность структуры получаемой матрицы. Портрет матрицы Адамара, вычисленной методом Скарпи [39], представлен на рисунке 1.5.

Более поздний, но также считающийся классическим, метод Пэли использует сложные поля Галуа GF(p^m) [40], позволяя осуществлять эффективный поиск матриц, порядки которых связаны со степенями простых чисел. В более простом случае конструкция матрицы представляет собой циклическое ядро (core) порядка $4t - 1$ с окаймлением.

Пример матрицы Адамара порядка 12, полученной методом Пэли, приведен на рисунке 1.6. В зависимости от сложности поля циклические блоки могут быть и составными [37, 40].

Более поздние методы основаны на компьютерных решениях. В качестве примера можно выделить использование массива Вильямсона $\mathbf{W}_n$ [36, 37, 41].

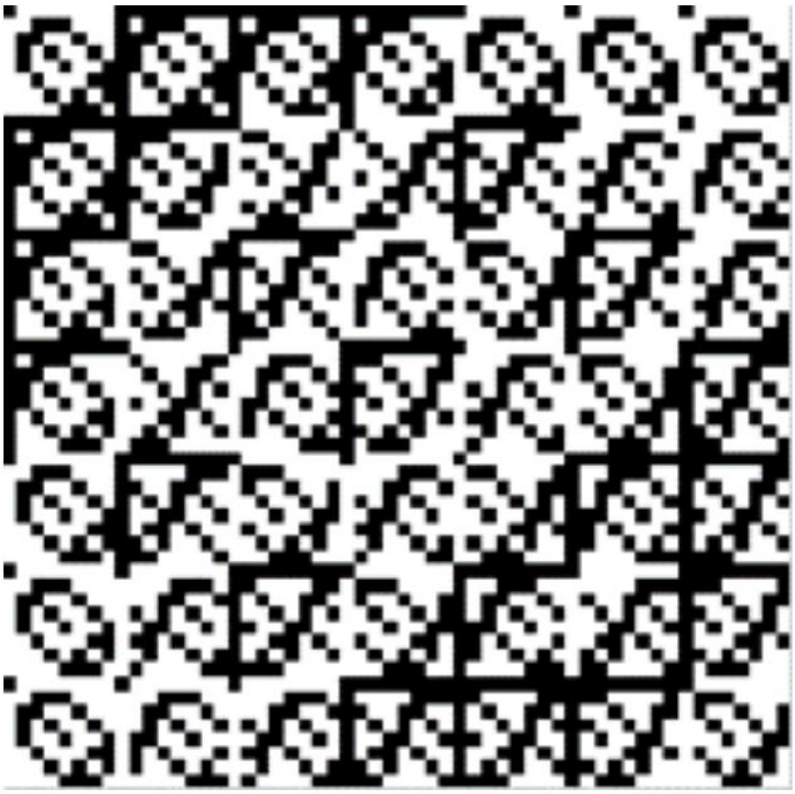


Рисунок 1.5 – Портрет матрицы $\mathbf{H}_{56}$, вычисленной методом Скарпи

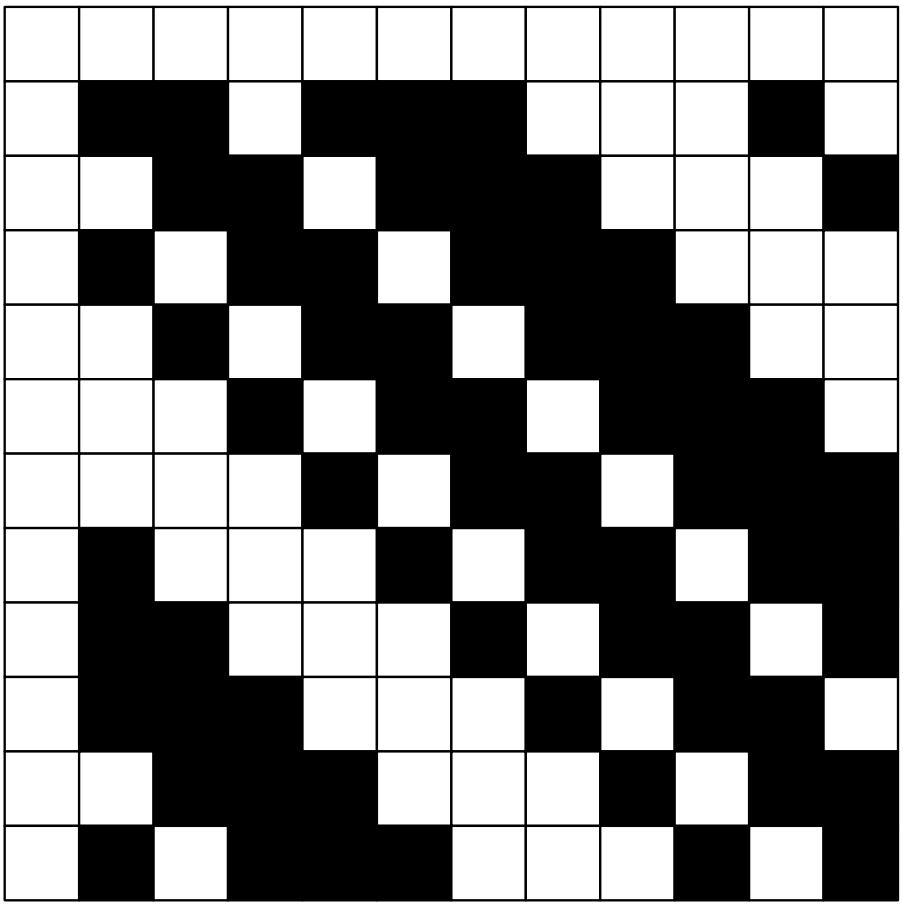


Рисунок 1.6 – Портрет матрицы $\mathbf{H}_{12}$, вычисленной методом Пэли

$$\mathbf{W}_n = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \end{pmatrix}.$$

В нем для поиска используется четыре симметричных блока **A**, **B**, **C** и **D**, удовлетворяющие соотношению

$$\mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B} + \mathbf{C}^{\mathrm{T}}\mathbf{C} + \mathbf{D}^{\mathrm{T}}\mathbf{D} = n\mathbf{I},$$

причем сами по себе блоки не обязательно ортогональны и имеют порядок $n/4$.

В отличие от классических методов использование массива Вильямсона предполагает лишь дизайн [1] и не предполагает распределение самих элементов в блоках матрицы. Сами элементы блоков **A**, **B**, **C** и **D** находятся комбинаторными методами, с вводом некоторых ограничений на структуру [1, 42].

Как отмечается в работе [1], задача поиска упрощается при выборе блоков симметричной циклической структуры. В качестве примера на рисунке 1.8 приведен портрет матрицы Адамара порядка 92, вычисленной в работе [44].

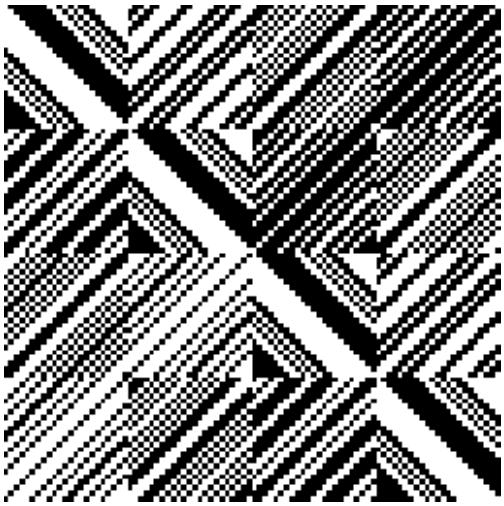


Рисунок 1.8 – Портрет кососимметричной матрицы $\mathbf{H}_{92}$ [44]

Известны модификации массива Вильямсона, например, массивы Гентхальса-Зейделя [45], Вильямсона-Себерри [46-48], Балонина-Себерри [48-50]. Последние матрицы получили название Пропус [48].

Отличие модификаций состоит в том, что первая позволяет найти больше симметричных решений в сравнении с исходным массивом Вильямсона, вторая

гарантирует кососимметрию получаемой матрицы, а третья – позволяет получать матрицы симметричной структуры.

Подводя итоги сказанному выше следует отметить следующее:

– матрицы Адамара являются идеальными (оптимальными) по количеству уровней – их всего два;

– совокупность классических и новых методов позволяет получать различные конструкции матриц, в том числе симметричные и циклические.

Однако, следует отметить, что матрицы Адамара согласно гипотезе Адамара (в современных источниках обосновывается ее переход в теорему [36,37,52]) существуют только на порядках, кратных четырем. Современные методы пока не позволяют найти некоторые матрицы Адамара – например, порядка 668. Циклические матрицы, согласно гипотезе Райзера, ограничиваются порядком 4, бициклические – порядком 32 [51].

Таким образом указанные матрицы хорошо подходят для практического использования, но требуют новых подходов для заполнения отсутствующих порядков, в том числе структурированными матрицами.

Матрицы Белевича, известные как конференц-матрицы или **C**-матрицы, связаны с теоремой теории чисел Эйлера, и являются примером поиска матриц близких по свойствам к матрицам Адамара [20, 32].

Матрицы Белевича – это квадратные матрицы порядков n кратных 2 с нулевыми значениями на главной диагонали и остальными элементами, равными ±1, для которых справедливо:

$$\mathbf{C}_n\mathbf{C}_n^{\mathrm{T}} = (n-1)\mathbf{I}.$$

Условие их существования: число n – 1 должно быть разложимо на сумму двух квадратов. Эти матрицы заполняют четные порядки в последовательности матриц Сильвестра, такие как 6, 10, 14, 18 и так далее. Однако существуют исключения, например, порядки 22, 34, 58, 70 и т.д.

Существуют также обобщения, называемые взвешенными конференц-матрицами [53] с отличающимся от оригинала количеством нулевых элементов

(строки/столбца). Однако заполнение пробелов в последовательностях матриц Адамара посредством С-матриц или взвешенных С-матриц сопряжено с существенными сложностями, что обусловлено вычислительной трудностью их построения. Так, например, С-матрица 66-го порядка остается неизвестной [53,54].

*Матрицы Мерсенна, Эйлера и Ферма***.** При изучении ортогональных матриц, приближенных по свойствам к матрицам Адамара, авторами работы [32] введен новый класс **M**-матриц. Эти матрицы существуют для нечетных порядков $4t–1$, отличаются минимальной абсолютной величиной элементов в классе ортогональных. В отличие от матриц Адамара, они обладают свойством локального максимума детерминанта

Теория **M**-матриц последовательно развивалась в последние 20 лет [55,33,24,57-63]. В работе авторов Сергеева М.Б. и Балонина Н.А приведен обзор квазиортогональных матриц максимального детерминанта, методы их поиска, а также обосновывается обобщение «*класса ортогональных матриц квазиортогональными матрицами*» [60]. В этой же работе, утверждается, что «*квазиортогональные обобщенные матрицы Адамара с элементами, не большими по модулю единицы лежат на пересечении M двух классов D-матриц абсолютного максимума детерминанта (не ортогональных по столбцам) и квазиортогональных W-матриц (безотносительных к оптимуму детерминанта) с некоторым, желательно небольшим, количеством уровней. Классические матрицы Адамара образуют на пересечении D-матриц и W-матриц подмножество H всех матриц с единичными по модулю элементами*» [60]. Это показано на рисунке 1.9.

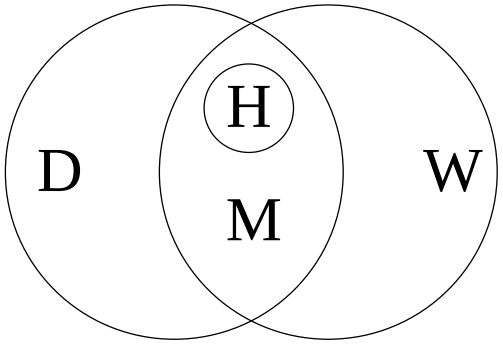


Рисунок 1.9 – Область существования квазиортогональных матриц

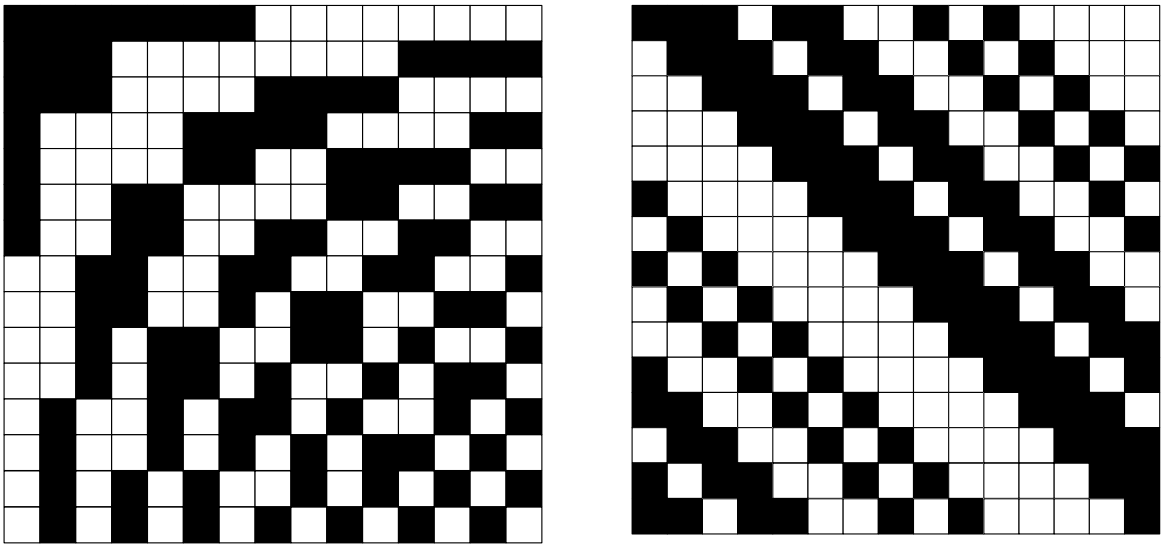
В соответствии с вышесказанным, матрицы Адамара можно также классифицировать как квазиортогональные.

В работе [60] выделены отдельные семейства малоуровневых квазиортогональных матриц, а именно матриц Мерсенна, Эйлера и Ферма.

Определение 15 (взято из работы [60]). Под *матрицами Мерсенна* $\mathbf{M}_n$ будем понимать квазиортогональные матрицы с двумя значениями уровней $\{1,-b\}$, при этом b по модулю меньше единицы, обладающие локальным максимумом детерминанта и существующие на порядках $4t-1$. Данные матрицы удовлетворяют соотношению $\mathbf{M}_n\mathbf{M}_n^{\mathrm{T}} = \omega\mathbf{I}$, при этом вес матрицы есть функция от порядка матрицы [60].

Наименование этих матриц связано с их первоначальным обнаружением на мерсенновских порядках 2^k-1, ($k\in\mathbb{N}$), которые входят в последовательность $4t-1$.

Матрицы Мерсенна в зависимости от метода их получения могут иметь различные структуры. В качестве примера на рисунке 1.10 приведены портреты двух матриц Мерсенна порядка 15 симметричной [58] и циклической [59] структур.



а) б)

Рисунок 1.10 – Портреты симметричной (а) и циклической (б) матриц Мерсенна порядка 15

Определение 16 (взято из работы [60]). *Матрицы Ферма* $\mathbf{F}_n$ – это трехуровневые квазиортогональные матрицы порядков $n=2^k+1$, при этом k – четное,

со значениями элементов {1, -*b*, *s*}, где $s \le b < 1$, удовлетворяющее следующему соотношению $\mathbf{F}_n \mathbf{F}_n^{\mathrm{T}} = \omega \mathbf{I}$ [60].

В качестве примера на рисунке 1.11 приведен портрет матрицы Ферма порядка 65 с явно заметной симметрией структуры. Элементы s матрицы Ферма на портрете выделены серым цветом.

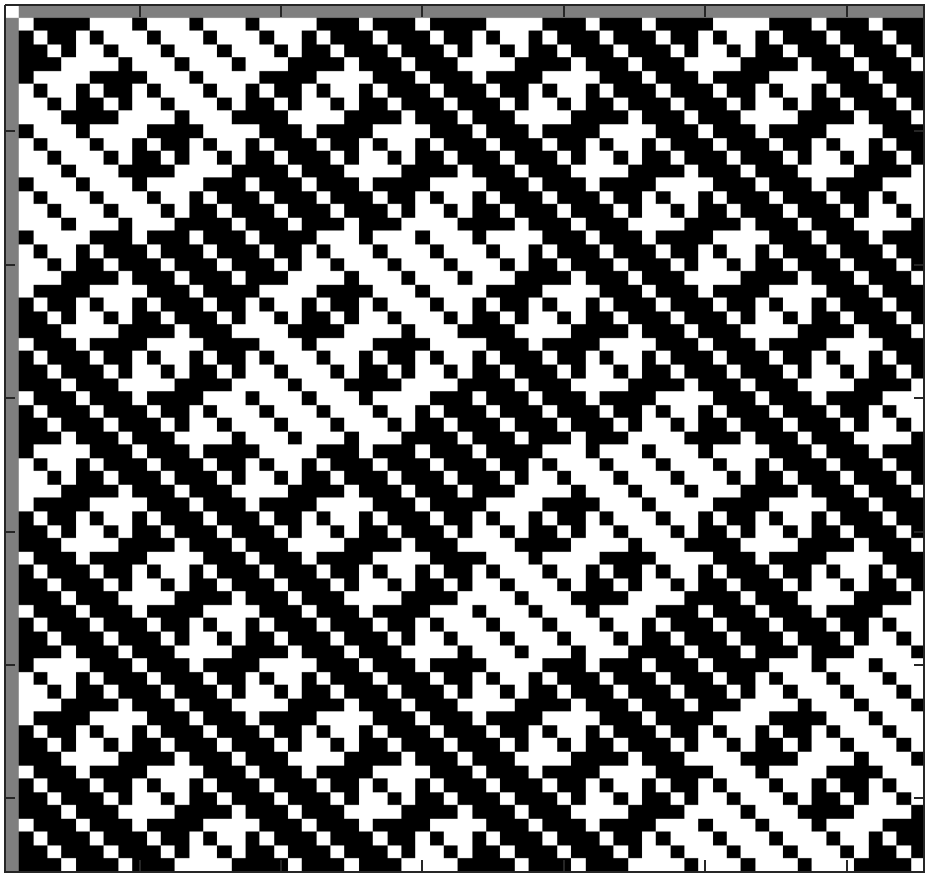


Рисунок 1.11 – Портрет матрицы Ферма порядка 65

Определение 17 (взято из работы [60]). *Матрицы Эйлера* $\mathbf{E}_n$ – это квазиортогональные матрицы порядков $4t - 2$ со значениями элементов {1, -1, *b*, -*b*}, где $|b|<1$, удовлетворяющее соотношению $\mathbf{E}_n \mathbf{E}_n^{\mathrm{T}} = \omega \mathbf{I}$ [60].

Значения функций $\omega = f(n)$ и элементов для матриц **M**, **E** и **F** для удобства сведены в таблицу 1.1, сформированную на основе результатов из работ [60,63].

Как показано в более поздней работе [61], существует глубокая связь между матрицами Мерсенна и Адамара, включая возможность их взаимного преобразования посредством конструкции "ядро с окаймлением". Дальнейшее развитие этих результатов в [62] привело к установлению закономерностей

построения цепочек матриц, объединяющих семейства Мерсенна, Адамара и Ферма.

Таблица 1.1. Значения элементов и весовых функций для матриц **M**, **E** и **F.**

Матрица	n	$\omega=f(n)$	Значения элементов
$\mathbf{M}_n$	$4t$ - 1	$\omega=\frac{\left(n+1\right)+\left(n-1\right)b^2}{2}$	1, -b; $b=\frac{t}{t+\sqrt{t}}$
$\mathbf{F}_n$	$4t$ +1	$\omega=1+\left(n-1\right)s^2$	1, -b, s; $q=n-1=4u^2, p=q+\sqrt{q},$ $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u},$ $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}=\frac{\sqrt{nu-1}}{2u+1}\times\frac{1}{\sqrt{u}}$
$\mathbf{E}_n$	$4t$ - 2	$\omega=\frac{\left(n+2\right)+\left(n-2\right)b^2}{2}$	1, -1, b, -b; $b=\frac{t}{t+\sqrt{2t}}$

Рассмотренные матрицы Мерсенна, Эйлера и Ферма являются малоуровневыми квазиортогональными, существенно расширяющими класс матриц для преобразования информации.

1.4. Выводы по разделу 1

К настоящему времени количество используемых ортогональных и квазиортогональных матриц существенно возросло. Появление в научном обороте малоуровневых квазиортогональных матриц, расширяющих семейство матриц Адамара, показало перспективы их экспансии в алгоритмы обработки и

кодирования информации в радиолокации и телекоммуникациях [64,65], помехоустойчивом кодировании [66], сжатии изображений [15,29-30], защитном кодировании изображений [24, 27] и звука [25] с появлением новых интересных результатов.

Постоянный рост объемов данных, размеров задач с использованием матричных методов обработки и преобразования, требует вычисления ортогональных и квазиортогональных матриц большой размерности с малым количеством уровней элементов и инвариантами структур.

Целесообразен поиск вычислительно простых методов получения структурированных малоуровневых квазиортогональных матриц, не основанных на комбинаторных подходах. Это является важным как для использования при решении задач обработки информации, так и, например, в качестве составных блоков массивов при поиске матриц Адамара высоких порядков.

2 ПОИСК ДВУХУРОВНЕВЫХ ЦИКЛИЧЕСКИХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

2.1. Подходы к поиску квазиортогональных матриц циклической структуры

Циклическая структура матрицы является наиболее удачной для использования в преобразованиях, поскольку, как упоминалось ранее, задается хранимой в памяти первой строкой из n ее элементов.

Однако следует определить – где и как осуществлять поиск циклических матриц. Идеальные с точки зрения количества уровней матрицы Адамара с элементами {1,-1} ограничены гипотезой Райзера для моноциклической структуры порядком 4 [6], для бициклической структуры – порядком 32 [51]. Хотя гипотеза Райзера и ее расширение не доказаны, нет данных, позволяющих их опровергнуть [67]. Следовательно, осуществлять поиск матриц Адамара циклической структуры выше 32 порядка не имеет смысла.

Для поиска циклических ортогональных матриц больших порядков с симметрией следует ввести три допущения. Во-первых, матрицы должны быть симметричны относительно побочной диагонали, т.е. персимметричны. Во-вторых, в ряде случаев следует ослабить требование к значению отрицательного элемента в матрице до $–b$, сделав его функцией от порядка n. В-третьих, такие матрицы следует искать только 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, существующие на нечетных порядках $4t - 1$ и связанные с простыми числами, имеющие, в основном, циклическую структуру [67,68]. Они существуют для всей последовательности порядков $n = 4t – 1$ [56,61]. Таким образом целесообразно осуществлять поиск матриц мерсеннова типа.

В настоящее время для поиска квазиортогональных матриц применяются различные подходы [59,68-71], отличные от традиционных комбинаторных и основанные на связях:

– особенностей структур матриц с решением диофантовых уравнений и расположением точек Гаусса на решетках [68-70];

– строк матриц с теорией групп и полей, в которых определяются положения элементов со значениями 1 и -b или -1 [59, 68-69];

– структур матриц с результатами оптимизационного процесса [68, 71].

Однако, можно выделить и другой подход, который впервые подробно рассматривается мною в рамках данной диссертационной работы, основанный на связи теории матриц и одной из задач радиолокации и связи, а именно – поиска бинарных кодовых последовательностей (КП) с хорошими корреляционными свойствами.

Например, известные КП Баркера или «коды Баркера» [72], используемые в наборе стандартов IEEE 802.11, интересны тем, что у них величина максимального уровня бокового лепестка (УБЛ) апериодической автокорреляционной функции (ААКФ) не превышает 1/N, где N длина КП.

Известные КП Баркера представлены в таблице 2.1.

Таблица 2.1. Известные кодовые последовательности Баркера

N	БП	Версия
2	1,-1	1,1
3	1,1,-1	-
4	1,1,-1,1	1,1,1,-1
5	1,1,1,-1,1	-
7	1,1,1,-1,-1,1,-1	-
11	1,1,1,-1,-1,-1,1,-1,-1,1,-1	-
13	1,1,1,1,1,-1,-1,1,1,-1,1,-1,1	-

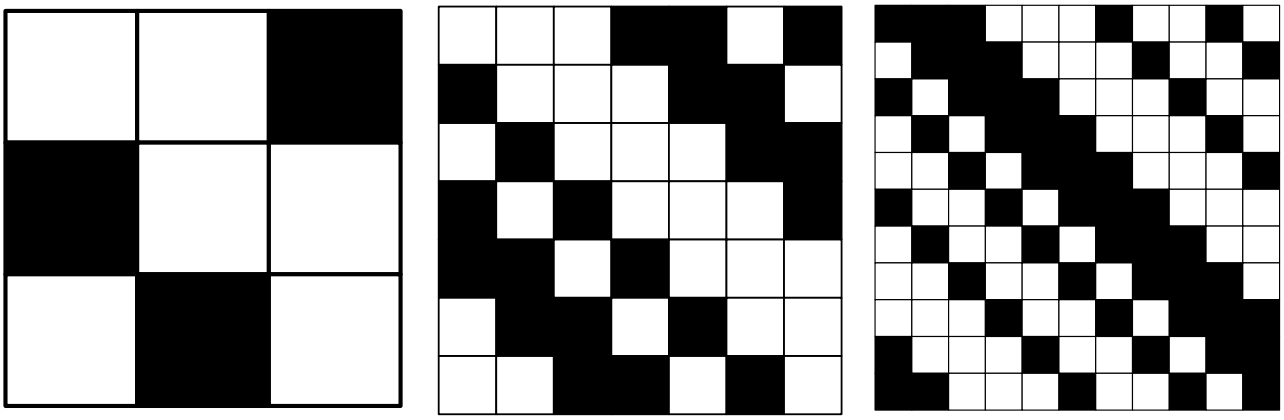
Кодовые последовательности Баркера ограничены порядком 13. Замечено, что у ортогональных матриц максимального детерминанта нечетных порядков

также наблюдается линейный рост уровней и усложнение структуры до критического порядка – 13 [73].

Результаты проведенного анализа свидетельствуют, что КП Баркера, несмотря на их независимое от матричной теории происхождение, фактически представляют собой фрагменты строк матриц с максимальным детерминантом, найденных Г. Барба [74,75].

В работе [64] установлена еще одна взаимосвязь между КП Баркера и теорией матриц: последовательности длиной 3, 7 и 11 при замене элемента "-1" на "-*b*" и последующей инверсии знаков преобразуются в циклические матрицы Мерсенна соответствующих порядков.

В подтверждение сказанного на рисунке 2.1 приведены портреты матриц $\mathbf{M}_3$, $\mathbf{M}_7$ и $\mathbf{M}_{11}$. Элемент «-*b*» для каждой матрицы вычислен по таблице 1.1.



а) б) в)

Рисунок 2.1 – Портреты циклических матриц Мерсенна $\mathbf{M}_3$ с b=0,5 (а), $\mathbf{M}_7$ с b=0.5858 (б), $\mathbf{M}_{11}$ с b = 0.6340 (в)

Еще одну связь можно проследить на основе анализа работ [19, 40, 62, 76]. В работе [40], как уже отмечалось, Р. Пэли предложил ставший уже классическим метод нахождения матриц Адамара на основе линейных рекуррентных последовательностей, или последовательностей квадратичных вычетов, обладающих одноуровневой периодической автокорреляционной функцией (ПАКФ). Это удобно при решении задач радиолокации и связи.

Длины подобных последовательностей соответствуют порядкам $4t - 1 = p$, где p – простое число. Матрицы Мерсенна также существуют на указанных порядках и связаны с матрицами Адамара как

$$\mathbf{H}_{4t} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{M}_{4t-1} \end{pmatrix},$$

при этом λ обозначает собственное число, а e – собственный вектор матрицы Мерсенна после процедуры округления до целочисленных значений.

В качестве примера рассмотрим матрицу $\mathbf{M}_3$, вычисленную методом Пэли. Для нее, после округления собственное число будет равно единице, а $e^{\mathrm{T}} = (1,1,1)$.

Используя указанную взаимосвязь матриц, найдем матрицу $\mathbf{H}_4$:

$$\mathbf{H}_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}, \mathbf{H}_4\mathbf{H}_4^{\mathrm{T}} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

В работе [62] отмечен также и возможный обратный ход данной взаимосвязи. В этом случае из матрицы Адамара удаляется кайма, и происходит инверсия элементов «ядра». Далее изменяются отрицательные значения элементов до расчетного значения «-b».

Как уже отмечалось выше, известна только одна циклическая матрица Адамара порядка 4

$$\mathbf{H}_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Тем не менее, известно большое количество матриц Адамара, состоящих из циклической подматрицы порядка $(n - 1)\times(n - 1)$, с каймой из элементов «+1» [19], например

$$\mathbf{H}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Подобные матрицы в зарубежной литературе начали называть циклическими матрицам Адамара [77]. В рамках диссертации для определенности будем называть такие матрицы матрицами Адамара конструкции «ядро с окаймлением».

Теория их построения связана с теорией разностных множеств

$$D\left(v,k,\lambda\right) = \left\{d_1, d_2, ..., d_k\right\},$$

где d_i – элементы разносного множества, v, k, λ – параметры множества [19].

Порядковые номера столбцов в ядре могут образовывать разностные множества – разностные множества Адамара, с параметрами

$$\left(v,k,\lambda\right) = \left\{4t-1, 2t-1, t-1\right\}.$$

В работе [78] С. Голомб отмечает взаимосвязь между циклическими разностными множествами типа Адамара и бинарными КП с одноуровневой ПАКФ. Им замечено, что у последовательностей Лежандра ПАКФ одноуровневая. Им же, в работе [79] поставлена задача систематического поиска всех математических структур, способных образовывать разностные множества.

Результаты проведенного анализа, и выявленные взаимосвязи между КП с одноуровневой ПАКФ, матрицами Адамара и Мерсенна, позволяют осуществлять поиск последних, на основе первых. Целесообразно провести обзор известных кодовых последовательностей

2.2. Известные кодовые последовательности, основанные на разностных множествах Адамара

Обзоры КП с одноуровневой ПАКФ были проведены в работах [19, 76] и позволяют выделить ряд интересующих, с точки зрения решения задач диссертационной работы, последовательностей.

Последовательности Лежандра, существуют на порядках $4t - 1 = p$, где p простое число и получаются на основе вычисления квадратичных вычетов [75]. Сама последовательность формируется в виде:

$$-1,\left(\frac{1}{p}\right),\left(\frac{2}{p}\right),...,\left(\frac{p-1}{p}\right),$$

где $\left(\frac{a}{p}\right)$ - символ Лежандра или квадратичный вычет по модулю p. При этом, если a – квадратичный вычет по модулю p, то символ равен «+1», в ином случае «-1». Замена первого элемента последовательности «-1» на «+1» также не изменяет количества уровней ПАКФ.

Последовательности Якоби [80] существуют на порядках $4t - 1 = p(p + 2) = pq$, где p и q – нечетные простые числа близнецы. Последовательность задается в следующем виде:

$$\left(\frac{0}{pq}\right),\left(\frac{1}{pq}\right),\left(\frac{2}{pq}\right),...,\left(\frac{pq-1}{pq}\right).$$

При этом символ Якоби $\left(\frac{a}{pq}\right)$ определяется как произведение символов Лежандра $-\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$. Символ Якоби используется при ненулевом значении.

Для получения последовательности следует произвести замену на «+1» при

$$a \in \left\{ 0, q, 2q, ..., \left(p-1 \right) q \right\},$$

и замену на «-1» при

$$a \in \left\{ p, 2p, 3p, ..., \left(q-1 \right) p \right\}.$$

Известны также:

- *последовательности Холла* [81] или последовательности шестеричных вычетов, существующие на порядках $p = 4x^2 + 27$;
- *m-последовательности,* существующие на порядках $4t - 1 = 2^k - 1$, где $k \geq 1$, и k – натуральное число. При этом в выходной последовательности линейного сдвигового регистра значение «0» заменяется на «-1», а «1» на «+1»;
- Четыре типа *последовательностей Гордона-Миллса-Велча (GMW) [76,81-82]:*

1) базовые GMW-последовательности;

2) каскадные GMW-последовательности;

3) обобщенные GMW-последовательности I типа;

4) обобщенные GMW-последовательности II типа.

Позднее были получены последовательности порядков $4t - 1 = 2^k - 1$, а именно:

- *3-term последовательности* [77,84], существующие для нечетных $k = 2t + 1$, где $k \geq 5$);
- *5-term последовательности* (существуют на $2^k - 1$, при $5 \bmod 3 \neq 0$, и $k \geq 7$);
- *WG-последовательности* (последовательности Велча-Гонга) [85],
- *последовательности на основе гиперовалов* [85-86].

2.3. Метод поиска циклической квазиортогональной матрицы на основе последовательности, основанной на разностном множестве Адамара

В монографии Сергеева М.Б. и Балонина Н.А. приводится определение сбалансированного неполного блочного дизайна: «Сбалансированным неполным блочным дизайном (a balanced incomplete block design), обозначаемым BIBD, называется совокупность b блоков, содержащих k различных между собой объектов общей численностью v, такая, что каждый объект содержится в r блоках, а каждая пара объектов содержится в λ блоках. Необходимые условия существования дизайна BIBD(v,k,λ) состоят в выборе пары разрешенных параметров $r = \lambda(v–1)/(k–1)$ и $b = vr/k$. Если количество блоков равно количеству объектов $b = v$, то $r = k$, – такой дизайн называется симметричным SBIBD(v,k,λ)» [1].

В работах [88-89] утверждается, что разностные множества с параметрами (v, k, λ) могут быть основой для построения SBIBD(v, k, λ).

В вышеупомянутой в данном подразделе монографии, также сказано, что «Параметры k, λ связаны с коэффициентами квадратичного условия связи. Произведение двух соседних строк матрицы содержит λ произведений aa, $2(k-\lambda)$ произведений ab ($k-\lambda$ элементов а каждой из строк умножено на b), и остающиеся $n-2k+\lambda$ произведений b^2. Согласно $\mathbf{A}^T\mathbf{A}=\omega(n)\mathbf{I}$ оно равно нулю, что дает уравнение $(n-2k+\lambda)b^2-2(k-\lambda)ab+\lambda a^2=0$, которое будем называть характеристическим. Оно в сжатой форме выражает условие ортогональности бинарной по уровням матрицы» [1]. Отметим, что для матриц Мерсенна уровень a фиксируется на значении «1».

На основании проведенного в данном разделе анализа, который выявил:

– существование связи между циклическими квазиортогональными матрицами Мерсенна и матрицами Адамара, где первые являются «ядром» вторых;

– взаимосвязь разностных множеств с симметричным блочным неполным дизайном (SBIBD);

– наличие обширного класса бинарных последовательностей, порождающих циклические неортогональные матрицы, формирующие ядро матриц Адамара,

в диссертации предлагается новый метод поиска циклических двухуровневых квазиортогональных матриц, последовательность действий которого представлена в виде структурной схемы на рисунке 2.2.

Дизайн будущей матрицы задается первой строкой последовательности, основанной на разностных множествах Адамара, что упрощает процесс получения матрицы ввиду отсутствия необходимости поиска расположения элементов матрицы перебором.

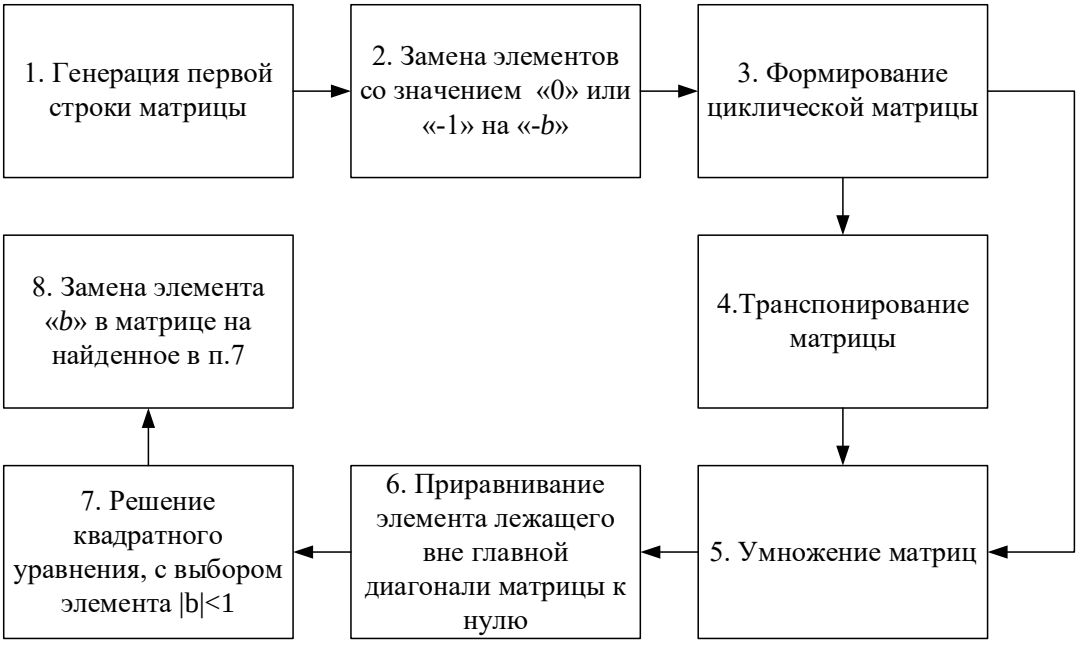


Рисунок 2.2 – Структурная схема предлагаемого метода

Следует пояснить: необходимость этапов 3-7 следует непосредственно из условия связи квазиортогональной матрицы, согласно которому все элементы вне главной диагонали должны быть равными нулю.

Рассмотрим несколько примеров применения предлагаемого метода.

Пример 1. Пусть первая строка матрицы сформирована на основе последовательности Лежандра длиной $n = 7$. Определим символы Лежандра для следующего набора чисел {0,1,2,3,4,5,6}, квадраты по модулю 7 данного набора равны соответственно {0,1,4,2,2,4,1}. Квадратичными вычетами будут являться элементы с индексами {1,2,4}, невычетами соответственно {3,5,6}. Как

обсуждалось ранее (см. п. 2.2), первый элемент последовательности «-1» можно заменить на «1» при этом не увеличивая количество уровней ПАКФ, получая таким образом первую строку матрицы в виде (1,1,1,-1,1,-1,-1). Нетрудно проверить, что циклическая матрица, сформированная из данной последовательности, не будет являться квазиортогональной.

В соответствии с предлагаемым в диссертации методом заменим элементы со значением «-1» на «-*b*», получая первую строку циклической матрицы (1,1,1,-*b*,1,-*b*,-*b*). Последовательным циклическим сдвигом вправо первой строки получаем матрицу $\mathbf{M}_7$,

$$\mathbf{M}_7 = \begin{pmatrix} 1 & 1 & 1 & -b & 1 & -b & -b \\ -b & 1 & 1 & 1 & -b & 1 & -b \\ -b & -b & 1 & 1 & 1 & -b & 1 \\ 1 & -b & -b & 1 & 1 & 1 & -b \\ -b & 1 & -b & -b & 1 & 1 & 1 \\ 1 & -b & 1 & -b & -b & 1 & 1 \\ 1 & 1 & -b & 1 & -b & -b & 1 \end{pmatrix},$$

Транспонированная матрица соответственно будет представлена следующим образом:

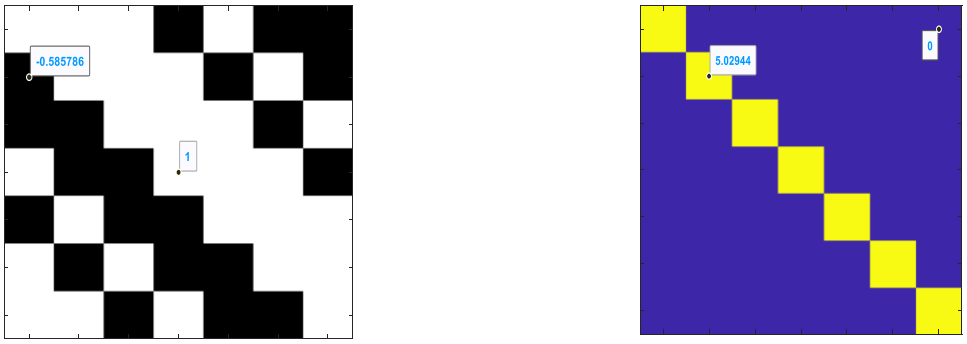
$$\mathbf{M}_7^T = \begin{pmatrix} 1 & -b & -b & 1 & -b & 1 & 1 \\ 1 & 1 & -b & -b & 1 & -b & 1 \\ 1 & 1 & 1 & -b & -b & 1 & -b \\ -b & 1 & 1 & 1 & -b & -b & 1 \\ 1 & -b & 1 & 1 & 1 & -b & -b \\ -b & 1 & -b & 1 & 1 & 1 & -b \\ -b & -b & 1 & -b & 1 & 1 & 1 \end{pmatrix}.$$

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

$$\mathbf{M}_7\mathbf{M}_7^T = \begin{pmatrix} 3b^2+4 & b^2-4b+2 & \cdots & b^2-4b+2 \\ b^2-4b+2 & 3b^2+4 & & \\ \vdots & & 3b^2+4 & \\ & & & \ddots \\ b^2-4b+2 & & & 3b^2+4 \end{pmatrix}.$$

Приравнивая элемент вне главной диагонали к нулю и решая квадратное уравнение, получаем два корня: b_1 = 0.5858 и b_2 = 3.4142. Выбирая элемент по модулю меньше 1, получаем искомое для квазиортогональной матрицы значение b = 0.5858.

Портрет полученной двухуровневой циклической квазиортогональной матрицы и результат ее проверки на квазиортогональность представлены на рисунке 2.3.



а) б)

Рисунок 2.3 – Результат работы предлагаемого метода для примера 1: портрет матрицы $\mathbf{M}_7$ (а) и портрет результата умножения $\mathbf{M}_7\mathbf{M}_7^T$ (б)

Пример 2. 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). Аналогично предыдущему примеру 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 $\mathbf{M}_{15}$,

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

Транспонированная матрица соответственно равна:

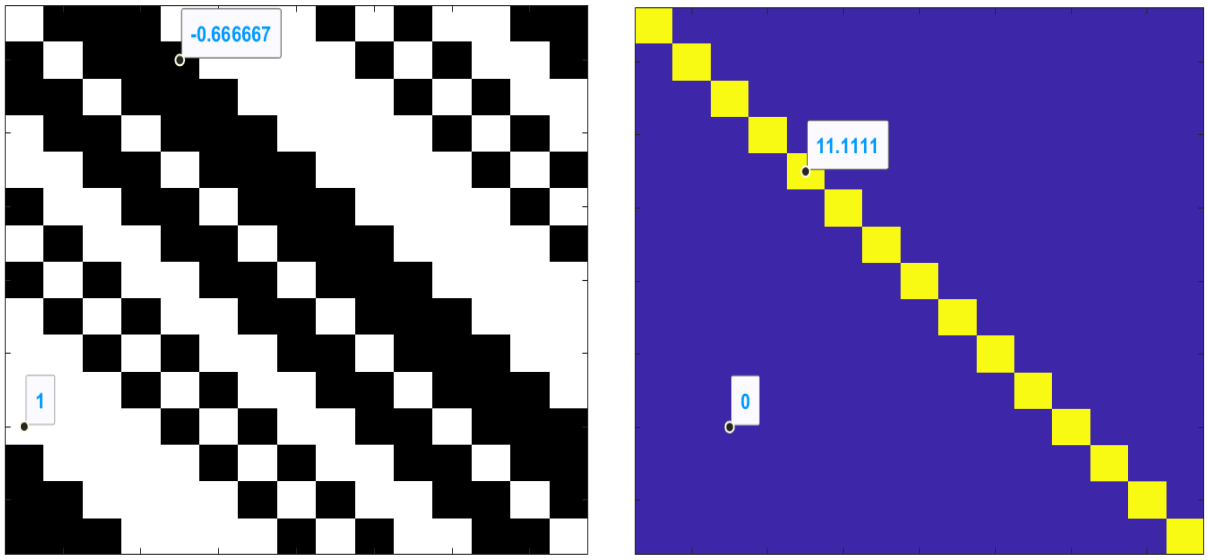
$$\mathbf{M}_{15}^{\,T}=\begin{bmatrix}
1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b & -b \\
-b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b & -b \\
-b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1 & 1 & 1 & -b \\
-b & -b & -b & 1 & -b & -b & 1 & 1 & -b & 1 & -b & 1 & 1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

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 рисунке 2.4.



а) б)

Рисунок 2.4 – Результат работы предлагаемого алгоритма для примера 2: портрет матрицы $\mathbf{M}_{15}$ (а) и портрет результата умножения $\mathbf{M}_{15}\mathbf{M}_{15}^{T}$ (б)

Пример 3. Пусть первая строка матрицы сформирована на основе GMW-последовательности длиной $n = 63$.

Конкретный алгоритм формирования самой GMW-последовательности в виду достаточной освещенности в литературе [77,82-83] оставим за рамками диссертации.

Традиционно GMW-последовательности записываются в виде таблицы. Возьмем, к примеру следующую таблицу из которой получается GMW-последовательность длиной в 63 элемента, представленную в [77] на стр. 239:

$$GMW_{63} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Сама последовательность образуется путем преобразования таблицы в вектор строку построчно, слева на право.

Получаем последовательность:

(0,1,1,1,1,0,1,1,1,0,0,1,1,1,1,0,1,0,0,1,0,1,1,0,1,1,1,0,1,0,0,0,1,1,0,1,0,1,1,0,0,1,1,0,1,0,0
,0,1,1,1,0,1,0,0,0,1,0,0,0,0,0,0).

Аналогично предыдущим примерам в соответствии с предлагаемым методом заменим «0» на «-*b*», получая первую строку циклической матрицы в виде:

(-*b*,1,1,1,1,-*b*,1,1,1,-*b*,-*b*,1,1,1,1,-*b*,1,-*b*,-*b*,1,-*b*,1,1,-*b*,1,1,1,-*b*,1,-*b*,-*b*,-*b*,1,1,-*b*,1,
-*b*,1,1,-*b*,-*b*,1,1,-*b*,1,-*b*,-*b*,-*b*,1,1,1,-*b*,1,-*b*,-*b*,-*b*,1,-*b*,-*b*,-*b*,-*b*,-*b*,-*b*).

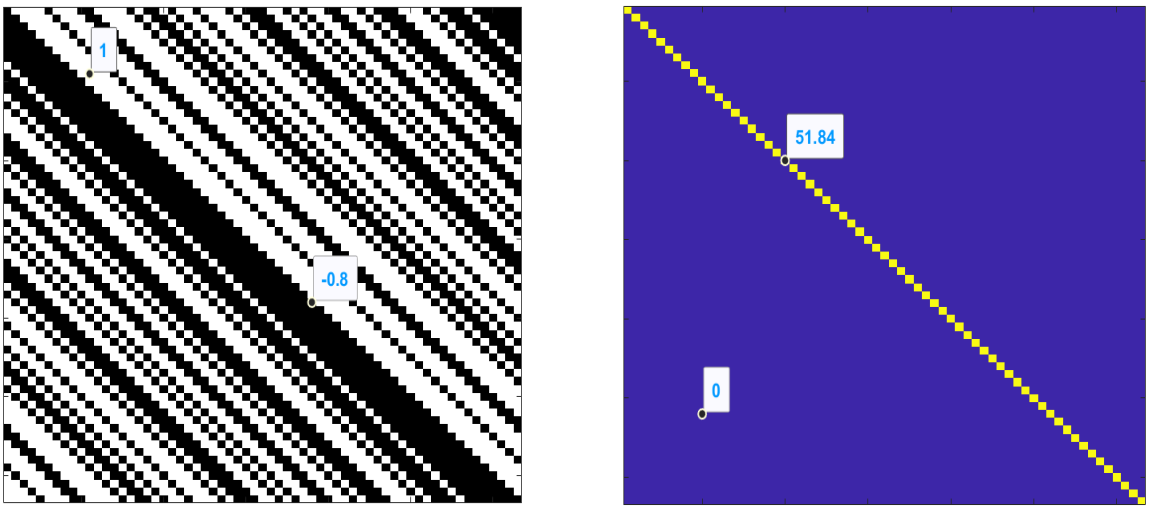
Последовательным циклическим сдвигом вправо первой строки получаем матрицу $\mathbf{M}_{63}$. Для удобства воспользуемся портретным представлением матрицы и представим ее на рисунке 2.5а.

В результате умножения матрицы на саму себя транспонированную получаем матрицу с элементами $31b^2 + 32$ на главной диагонали и элементами $15b^2 - 32b + 16$ вне главной диагонали:

$$\mathbf{M}_{63}\mathbf{M}_{63}^{T} = \begin{pmatrix} 31b^2+32 & 15b^2-32b+16 & \cdots & 15b^2-32b+16 \\ 15b^2-32b+16 & 31b^2+32 & & \\ \vdots & & 31b^2+32 & \\ & & & \ddots \\ 15b^2-32b+16 & & & 31b^2+32 \end{pmatrix}.$$

Приравнивая элемент вне главной диагонали к нулю и решая квадратное уравнение, получаем два корня: $b_1 = 0.8$ и $b_2 \approx 1.3$. Выбирая элемент по модулю меньше 1, получаем искомое для квазиортогональной матрицы значение $b = 0.8$.

Портрет полученной двухуровневой циклической квазиортогональной матрицы и результат ее проверки на квазиортогональность представлены на рисунке 2.5.



а) б)

Рисунок 2.5 – Результат работы предлагаемого алгоритма для примера 3:

Портрет матрицы $\mathbf{M}_{63}$ (а) и портрет результата умножения $\mathbf{M}_{63}\mathbf{M}_{63}^{T}$ (б)

Предлагаемый метод был использован при разработке специального программного обеспечения [90-95] для поиска матриц при выполнении НИР [96].

2.4. Выводы по разделу 2

Предложен новый, не основанный на переборных процедурах, метод поиска двухуровневых циклических квазиортогональных матриц, дополняющий их теорию, и позволяющий получать матрицы циклической структуры на порядках, равных простым числам, в том числе большого значения.

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.

3 ПРИМЕНЕНИЕ ЦИКЛИЧЕСКИХ МАЛОУРОВНЕВЫХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

3.1. Применение строк квазиортогональных циклических матриц в качестве кодовых последовательностей

Обзор областей применения малоуровневых квазиортогональных матриц показал, что с 2011 года они нашли свое применение как в традиционных для матриц областях помехоустойчивого кодирования [24, 66, 97-100], сжатия изображений [15, 24, 29-30, 100], фазовых (амплитудных) модуляций сигналов [64-65, 68-69 75, 101-108], так и в таких сферах, как обеспечение конфиденциальности цифровой информации с малым периодом актуальности [23-25, 27, 109-116], генетический анализ [98] и кристаллография [22]. Отдельно рассматривается возможность применения данных матриц в качестве основы дискретного текстильного орнамента [118, 119]. Рассмотрим подробнее основные области применения.

Особый интерес представляют рассматриваемые матрицы как альтернатива КП Баркера [64-65]. А именно, КП с элементами $\{1,-b\}$, основанные на строках персимметричных циклических квазиортогональных матриц: КП Мерсенна длиной 3, 7 и 11 [64], КП Рагхаварао длиной 5 и 13 [65], а также вложенные КП на их основе [65].

Использование данных КП предполагает незначительное ослабление требований к ААКФ, а именно, существование уровней боковых лепестков (УБЛ) ААКФ, превышающих единицу, что приемлемо в случае, если центральный пик ААКФ значительно превышает единицу.

Данные КП представлены в таблице 3.1, где также приведены отношения главного пика к максимальному боковому лепестку (ОПМБЛ) в децибелах для КП Баркера, Мерсенна и Рагхаварао.

Таблица 3.1. Характеристики ОПМБЛ для КП Баркера, Мерсенна и Рагхаварао

n		КП Баркера	КП Мерсенна и Рагхаварао
2	КП	1 -1 или 1 1	-
	ОПМБЛ	-6 дБ	-
3	КП	1 1 -1	-*b* 1 1
	ОПМБЛ	-9.5 дБ	-13.02 дБ
4	КП	1 -1 1 1 или 1 -1 -1 -1	-
	ОПМБЛ	-12 дБ	-
5	КП	1 1 1 -1 1	1 -*b* 1 1 1
	ОПМБЛ	-14 дБ	-15.92 дБ
7	КП	1 1 1 -1 -1 1 -1	-*b* -*b* 1 -*b* 1 1 1
	ОПМБЛ	-16.9 дБ	-18.68 дБ
11	КП	1 1 1 -1 -1 -1 1 -1 -1 1 -1	-*b* 1 -*b* -*b* -*b* 1 1 1 -*b* 1 1
	ОПМБЛ	-20.8 дБ	-19.08 дБ
13	КП	1 1 1 1 1 -1 -1 1 1 -1 1 -1 1	1 -*b* 1 -*b* -*b* 1 1 1 -*b* 1 1 1 1
	ОПМБЛ	-22.3 дБ	-23.77 дБ

Из таблицы видно, что КП Мерсенна и Рагхаварао обладают преимуществом над КП Баркера по значению ОПМБЛ. Авторами также отмечается, что «*Для кодовой последовательности Мерсенна длины 11 оценка ОПМБЛ АКФ получилась хуже, чем у кода Баркера, на 1,72 дБ, однако этот максимальный боковой лепесток находится на достаточном удалении от главного лепестка АКФ. Для второго максимального по номеру бокового лепестка, расположенного по соседству с главным боковым лепестком, аналогичная оценка превышает уровень боковых лепестков кода Баркера на 2,12 дБ*» [64].

Тем не менее авторами отмечается, что «… *даже приведенные коды Мерсенна и Рагхаварао не всегда достаточны для эффективного решения задач обнаружения и обеспечения помехоустойчивости в открытых радиоканалах*» [65].

Действительно, данные характеристики повышаются (для описанных в работах [64-65] видах модуляции) с увеличением базы сложных сигналов. Когда

возможности расширения спектра ограничены, то увеличение базы возможно лишь за счет увеличения длительности сигнала [119]. В случае использования кодовых последовательностей – за счет увеличения длины последовательности.

Из данных соображений авторами в работе [65] предложены вложенные кодовые последовательности Баркера-Мерсенна-Рагхаварао, позволившие улучшить характеристику ОПМБЛ по сравнению с известными вложенными кодами Баркера [120] для комбинаций: 5×3, 5×5, 5×7, 5×11, 5×13, 7×5, 11×5, 13×3, 13×5, 13×13. Таким образом максимальная длина кода для которых проводилось исследование ограничена значением 169.

Преимуществом циклических квазиортогональных матриц, метод поиска которых предлагается в настоящей диссертационной работе, является возможность получения на их основе КП больших длин, по сравнению с уже исследованными.

3.2. Применение квазиортогональных матриц в сжатии, маскировании и помехоустойчивом кодировании изображений

Данные области применения целесообразно рассмотреть совместно, поскольку в их основе лежит единый математический аппарат – матричное умножение.

Передача визуальной информации по каналу связи на сегодня остается одной из наиболее трудоемких задач, во-первых, в связи с большим объемом данных и ограниченности пропускной способности каналов [121], и, во-вторых, ввиду особенностей восприятия изображений зрительной системой человека [122].

При выборе между процедурами сжатия без потерь и с потерями последняя позволяет достигнуть лучших показателей коэффициента сжатия по сравнению с первой, а также обеспечивает возможность найти оптимальный баланс между степенью сжатия и качеством восприятия изображения.

Одним из популярных форматов сжатия с потерями является формат JPEG с использованием в своей основе ортогональной матрицы дискретного косинусного преобразования, однако, как отмечается в диссертации Сергеева А.М.: «*Выбор ДКП в алгоритмах сжатия изображений при их разработке был обусловлен, в том числе, относительно небольшими размерами кадров. Однако, размер мелких деталей на снимке с высоким разрешением (8К – 32К) соизмерим с размером матрицы ДКП, и часто не приводит к существенному сжатию. Одним из способов решения задачи качественной обработки изображений с высоким разрешением является создание и использование новых фильтров сжатия, основанных на использовании ортогональных и квазиортогональных матриц больших размеров*» [123].

В работах [15, 24, 29-30, 100, 110] отражены результаты анализа особенностей, которыми должны обладать матрицы для замены матрицы ДКП [15, 24, 29]. Они сводятся к рекомендации применения двухуровневых и модульно двухуровневых симметричных квазиортогональных матриц Мерсенна, структурированных по Уолшу [114].

В 2006 году в монографии [66] был предложен стрип-метод преобразования изображений. В основе предложенного метода лежат матричные преобразования, обеспечивающие значительное ослабление амплитуды импульсной помехи [66]. Суть метода заключается в предварительном искажении передаваемого изображения, при котором его фрагменты перемешиваются и накладываются друг на друга. Изображение делится на N прямоугольных фрагментов. Число разбиений по горизонтали обозначается через m, а вертикальных через n. В результате получается блочная матрица, наглядный пример которой показан на рисунке 3.1.

Наибольшая эффективность достигается при умножении каждого блока данных на ортогональную матрицу как слева, так и справа. При этом, авторами показано, что для наилучшего ослабления амплитуды импульсной помехи важно обеспечить, во-первых, минимальность максимального по модулю элемента используемой для преобразования матрицы, а во-вторых, распределение положительных и отрицательных элементов должно быть равномерно.

Соответственно предлагалось использование матриц Адамара и матриц Белевича, поскольку близкие к ним по свойствам квазиортогональные матрицы Мерсенна, Эйлера и Ферма были открыты позднее.

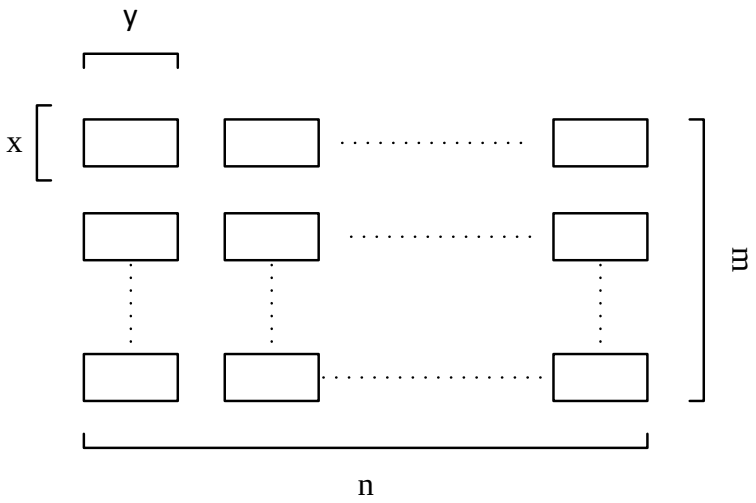


Рисунок 3.1 – Представление изображения в виде блочной матрицы

Следует отметить, что применение матриц Адамара в помехоустойчивом кодировании изображений было известно и раньше, их использование позволило передать первые изображения поверхности Марса во время миссии американского аппарата Маринер 9 [97].

Позднее, с развитием теории малоуровневых квазиортогональных матриц, данный метод был модифицирован, но уже для решения другой задачи – защиты от несанкционированного доступа к цифровым изображениям, имеющим малый период актуальности путем приведения их к шумоподобному виду. Для этого используется термин «маскирование» [109].

Данный метод может быть реализован в двух вариантах.

Первый – одностороннее маскирование, при котором исходное изображение (или фрагмент изображения) $\mathbf{X}_n$ размера $n \times n$ умножается на матрицу $\mathbf{P}_n$ того же размера в виде:

$$\mathbf{Y}_n = \mathbf{X}_n \mathbf{P}_n, \tag{3.1}$$

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

Второй вариант – двустороннее маскирование, при котором исходное изображение (или его фрагмент) умножается на матрицу маскирования $\mathbf{P}_n$ слева и транспонированную матрицу $\mathbf{P}_n^{\mathrm{T}}$ справа в виде:

$$\mathbf{Y}_n = \mathbf{P}_n \mathbf{X}_n \mathbf{P}_n^{\mathrm{T}}, \tag{3.2}$$

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

$$\mathbf{X}_n = \mathbf{Y}_n (\mathbf{P}_n)^{-1}, \tag{3.3}$$

$$\mathbf{X}_n = (\mathbf{P}_n)^{-1} \mathbf{Y}_n (\mathbf{P}_n^{\mathrm{T}})^{-1}, \tag{3.4}$$

Как уже отмечалось выше использование для маскирования ортогональных или квазиортогональных матриц $\mathbf{P}_n$, для которых, $(\mathbf{P}_n)^{-1} = \mathbf{P}_n^{\mathrm{T}}$, упрощает обратные преобразование по (3.3) и (3.4).

Отметим, что в работе [124] для маскирования использовались матрицы Мерсенна, однако на данный момент доступный набор матриц заметно расширился [27, 60].

Отличием от классического стрип-метода является, во-первых, отказ от кронекерова произведения в пользу обычного матричного умножения, что позволяет использовать матрицы высоких порядков [23-25, 27], во-вторых, использование широкого набора маскирующих матриц.

Сергеевым А.М. в диссертации отмечается, что «… Несмотря на тот факт, что стрип-преобразование не является основой метода маскирования, маскированное предлагаемым методом изображение остается устойчивым к возможным искажениям и потерям информации в коммуникационных каналах» [123].

Таким образом подводя промежуточный итог, метод матричного маскирования использует простой математический аппарат, обеспечивающий требуемое качество результата, в том числе, в режиме реального времени [27], для данного метода проработаны вопросы оценки устойчивости к искажениям и сжатию передаваемой информации [124-126], а также, используемые для маскирования матрицы являются обобщением матриц Адамара [60], и существуют

на всех остальных порядках [36-37, 127], что потенциально открывает возможности маскирования изображений любых размеров.

Таким образом, предлагаемый в диссертации метод поиска циклических квазиортогональных матриц может использоваться в области сжатия если провести структурирование по Уолшу найденных матриц, а в области маскирования позволяет расширить набор маскирующих матриц.

3.3. Применение квазиортогональных матриц в маскировании аудиоданных

Обеспечение конфиденциальности аудиоданных традиционно обеспечивается скремблированием [128] и криптографическими методами [129-132], однако в последнее время активно развиваются альтернативные методы, основанные на:

– матричных преобразованиях [133-134],

– комбинированных схемах кодирования [135-139],

с возможностью аппаратной реализации на ПЛИС и процессорах цифровой обработки сигналов [140].

Метод матричного маскирования с использованием пар преобразований (3.1) - (3.3) и (3.2) - (3.4) соответственно, можно применять и в данной области. Однако в отличии от изображений, при работе с аудиоданными требуется их подготовка.

Аудиоданные, представляющие собой набор цифровых отсчетов, преобразуются в квадратную матрицу, путем распределения фрагментов аудиоданных последовательно по строкам, как это показано на рисунке 3.2. 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, с учетом того, что наилучшее качество маскирования достигается при равенстве размеров маскируемой и маскирующей матриц [25,27].

Во втором случае, если доступная квазиортогональная матрица значительно меньше размеров входного набора аудиоданных – последний разбивается на блоки, и каждый блок умножается на матрицу маскирования, как это показано на рисунке 3.3.

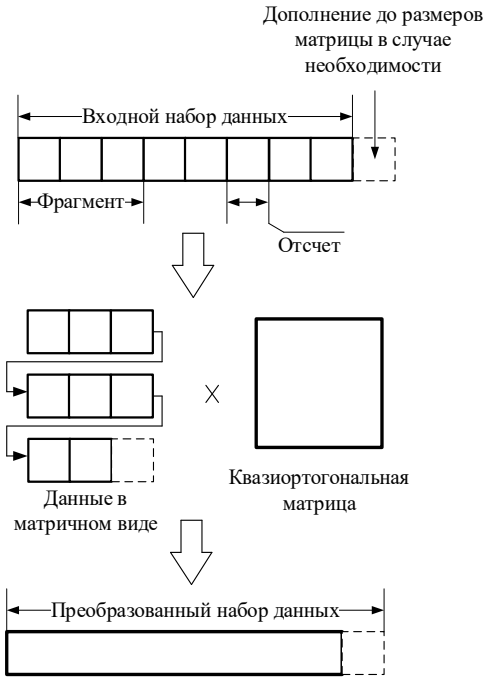


Рисунок 3.2 – Преобразование аудиоданных в матричный вид и их умножение на квазиортогональную матрицу

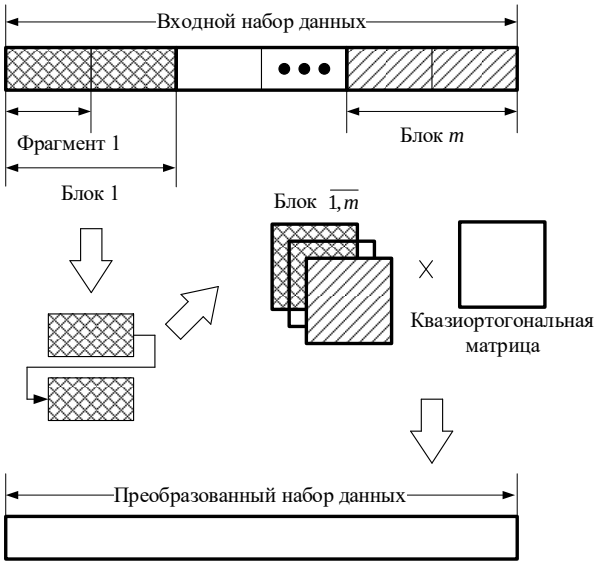


Рисунок 3.3 – Вариант маскирования аудиоданных в случае маскирующей матрицы малых размеров

3.4. Выводы по разделу 3

В области поиска кодовых последовательностей с несимметричным алфавитом для модуляции фазы (амплитуды) сигналов, есть необходимость поиска кодовых последовательностей длиной выше 169. Предлагаемые в диссертационной работе циклические квазиортогональные матрицы связаны с кодовыми последовательностями, основанными на разностных множествах Адамара известными своими корреляционными свойствами, в связи с этим целесообразен анализ корреляционных характеристик последовательностей, основанных на строках предлагаемых матриц.

В области сжатия изображений с использованием квазиортогональных матриц предлагаемый способ формирования циклических квазиортогональных матриц может использоваться если провести их последующее структурирование по Уолшу, однако дальнейшая проработка данного вопроса, исходя из проведенного анализа не требуется.

Вопросы маскирования и помехоустойчивого кодирования визуальной информации в целом достаточно проработаны, однако анализ публикаций по данной теме показал, для маскирования использовались в основном матрицы симметричной структуры, в связи с чем целесообразно провести исследование использования циклических матриц (в том числе большого порядка) на результаты маскирования изображений. Также в данной области до сих пор остается открытым вопрос оценки качества маскирования. В работе [124] для оценки использовались классические метрики MSE, PSNR, SSIM. Однако, ввиду особенностей восприятия визуальной информации зрительной системой человека, при маскировании матрицами малого размера, значения MSE и PSNR могут быть достаточно большими, однако на изображении остаются ярко выраженные контуры, визуальный анализ которых позволяет в некоторых случаях полное восстановление изображения/кадра видеопотока [141]. Структурный индекс сходства изображений (SSIM), в свою очередь, не подходит для точной оценки качества изображения,

поскольку может только оценить сходство двух изображений/кадров видеопотока, а также не всегда правильно оценивает сходство содержимого визуальной информации [142]. Известен также подход [143], основанный на оценке двумерного коэффициента корреляции между исходным и маскированным изображением, который позволил установить эмпирические оценки качества маскирования в зависимости от размера матрицы маскирования, однако данный подход прорабатывался только для визуальной информации, в связи с чем целесообразен дальнейший поиск единого подхода к оценке результатов маскирования цифровой информации.

4 МОДЕЛИРОВАНИЕ И АНАЛИЗ РЕЗУЛЬТАТОВ ПРИМЕНЕНИЯ ЦИКЛИЧЕСКИХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ В ЗАДАЧАХ КОДИРОВАНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

4.1. Анализ корреляционных характеристик новых кодовых последовательностей, основанных на строках циклических квазиортогональных матриц

Во втором разделе диссертации была выделена взаимосвязь между циклическими разностными множествами типа Адамара, циклическими квазиортогональными матрицами и бинарными КП с одноуровневой ПАКФ. На основании анализа, проведенного в третьем разделе, целесообразно оценить корреляционные характеристики строк найденных матриц [144]. Для решения данной задачи было разработано специальное программное обеспечение [145-147].

В ходе анализа были выделены три стратегии [68-69] вычисления циклических квазиортогональных матриц как основы кодовых последовательностей с улучшенными корреляционными свойствами [107-108].

Стратегия 1. Вычисление первой строки циклической матрицы на основе символов Лежандра [68,144],

Стратегия 2. Вычисление первой строки циклической матрицы на основе символов Якоби [68,144],

Стратегия 3. Вычисление первой строки циклической матрицы на основе m–последовательности [68,144].

Наиболее важной характеристикой КП в рассматриваемой постановке вопроса является ее автокорреляционная функция (АКФ). В практических приложениях АКФ КП должна иметь максимальный центральный пик и минимальный уровень боковых лепестков. Для анализа КП следует провести сравнительный анализ апериодической АКФ [107-108, 144, 148]. При этом следует определить, как выявить те, которые имеют максимальный уровень главного пика

апериодической АКФ и минимальный уровень боковых лепестков, так и проследить за тем, чтобы количество уровней ПАКФ осталось неизменным.

Для оценки в работе используются такие критерии как максимальный уровень бокового лепестка, 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 [148].

Рассмотрим подробнее последние две характеристики, а также приведем необходимые формулы для дальнейшего анализа.

ISLR – это отношение суммарной энергии боковых лепестков ААКФ последовательности длины N к энергии главного лепестка, вычисляемое как:

$$ISLR = \sum_{\substack{l=1-N \\ l\neq 0}}^{N-1} \left| C\left(l\right) \right|^2 \Big/ \left| C\left(0\right) \right|^2,$$

где $C(0)$ – значение главного лепестка , а $C(l)$ значение бокового лепестка ААКФ. Чем ниже значение ISLR, тем лучше полученная кодовая последовательность.

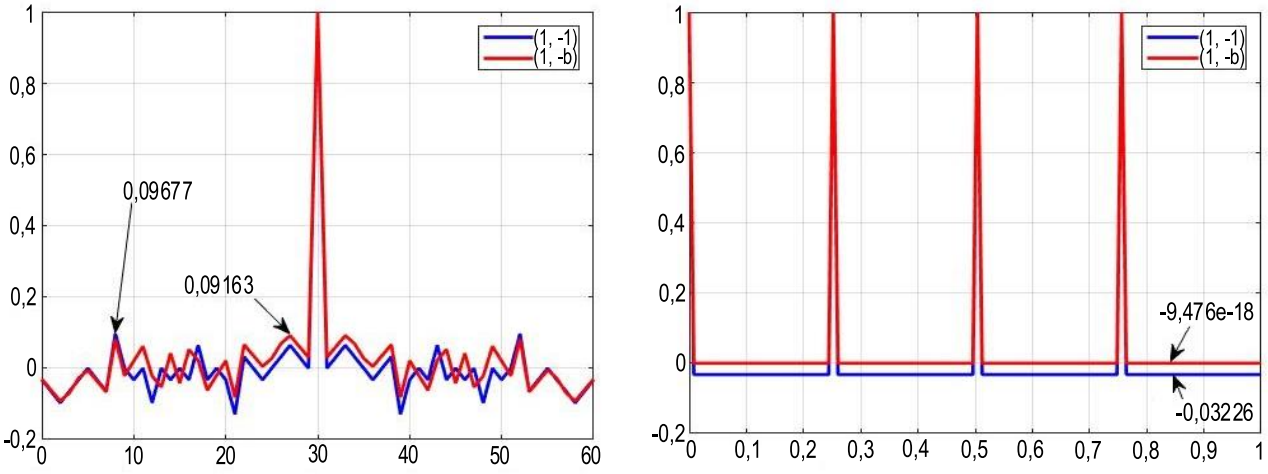
MF – обратная ISLR величина, поэтому чем меньше суммарная энергия боковых лепестков, тем больше величина критерия MF, соответственно, КП с большим значением MF будут лучше.

Полученные результаты, показаны на рисунках 4.1 – 4.3, и в таблице 4.1. На рисунках 4.1а, 4.2а, 4.3а представлены графики нормированных к единице ААКФ КП, полученных по стратегиям 1 – 3, показывающие снижение максимально уровня бокового лепестка ААКФ. Синим цветом на графике обозначены КП с алфавитом (1; –1), а красным цветом – КП с алфавитом (1; $-b$). Следует отметить, что для генерации последовательностей по стратегии 3 было разработано устройство, на которое получен патент на изобретение [149]. В рассматриваемом примере был использован полином $x^4 + x + 1$ с начальными условиями [0,0,0,1] для получения исходной m-последовательности.

На рисунках 4.1б, 4.2б, 4.3б представлены графики нормированных к единице ПАКФ КП, полученных по стратегиям 1 – 3 и проиллюстрирован факт того, что

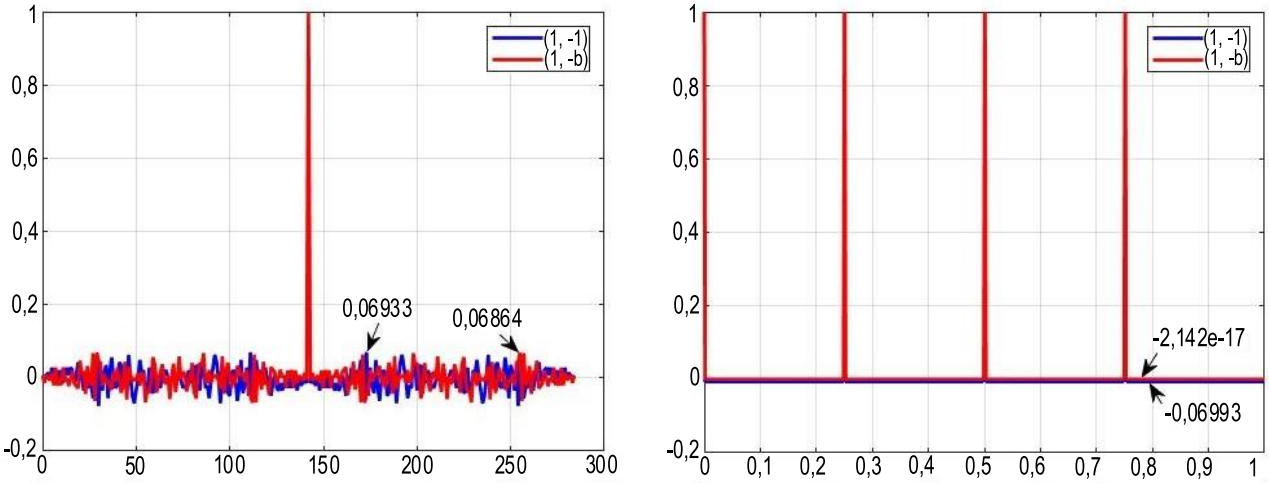
модификация КП и переход к алфавиту (1; –*b*) не добавляет боковых лепестков в периодическую АКФ. Результаты вычисления описанных параметров для каждой стратегии приведены в таблицах 4.1-4.6.

Следует пояснить, каким образом были выбраны кодовые последовательности для анализа. Полным перебором в циклических матрицах с элементами (1,-1) и (1,-*b*), полученных на основе стратегий 1-3, осуществлялся поиск наилучшей, по критерию минимума максимума бокового лепестка нормированной ААКФ. Данная строка из матрицы отбирались в качестве кодовой последовательности для данного порядка, и ее характеристики были занесены в таблицы 4.1-4.6.



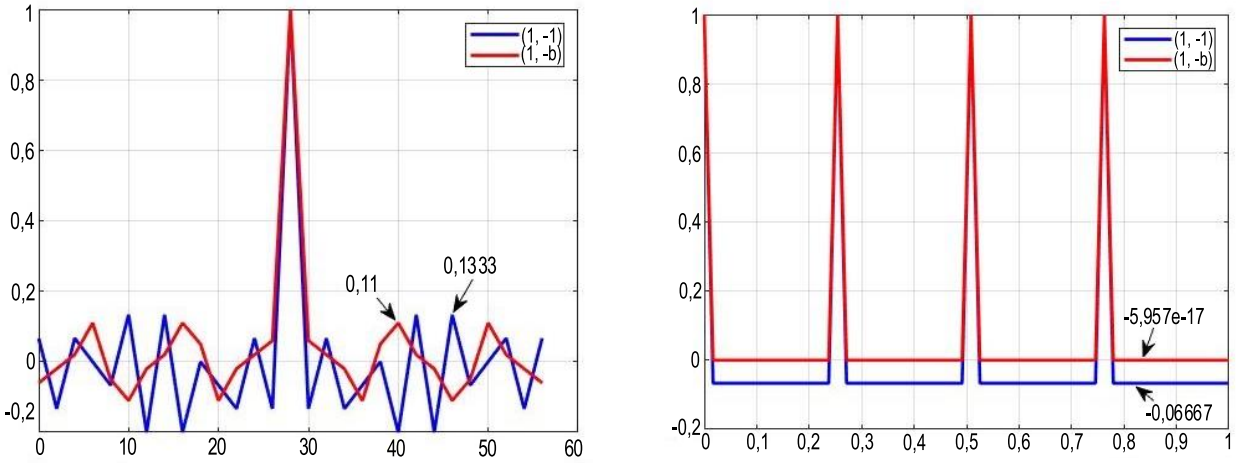
а) б)

Рисунок 4.1 - Апериодическая (а) и периодическая (б) АКФ кодовых последовательностей, полученных по стратегии 1, N = 31



а) б)

Рисунок 4.2 - Апериодическая (а) и периодическая (б)АКФ кодовых последовательностей, полученных по стратегии 2, N = 143



а) б)

Рисунок 4.3 - Апериодическая (а) и периодическая(б) АКФ кодовых последовательностей, полученных по стратегии 3, N = 15

Таблица 4.1. Корреляционные характеристики кодовых последовательностей с алфавитом {1; –1} полученных по стратегии 1

Порядок, N	БЛ$_{max}$	БЛ$_{max}$, дБ	ISLR	MF
31	0,0968	–20,2848	0,1561	6,4067
103	0,0680	–23,3548	0,2849	3,5106
239	0,0460	–26,7401	0,1742	5,7408
331	0,0393	–28,1177	0,1712	5,8420
383	0,0366	–28,7414	0,1751	5,7126
503	0,0338	–29,4224	0,1791	5,5840
587	0,0307	–30,2673	0,1697	5,8919
647	0,0309	–30,1975	0,1738	5,7541
719	0,0278	–31,1140	0,1757	5,6900
727	0,0289	–30,7863	0,1738	5,7545
787	0,0280	–31,0710	0,1698	5,8910
887	0,0259	–31,7239	0,1689	5,9217
907	0,0254	–31,9176	0,1943	5,1461
1019	0,0226	–32,9289	0,1684	5,9372
1123	0,0223	–33,0488	0,1705	5,8657

Продолжение таблицы 4.1

1279	0,0227	–32,8895	0,1712	5,8410
1283	0,0226	–32,9166	0,1669	5,9924
1307	0,0214	–33,3824	0,1668	5,9967
1319	0,0212	–33,4617	0,1696	5,8953
1423	0,0218	–33,2369	0,1676	5,9653
1447	0,0207	–33,6669	0,1695	5,8984
1451	0,0193	–34,2902	0,1693	5,9057
1511	0,0205	–33,7581	0,1679	5,9571
1607	0,0205	–33,7500	0,1681	5,9474
1759	0,0182	–34,8023	0,1679	5,9560

Таблица 4.2. Корреляционные характеристики кодовых последовательностей с алфавитом {1; –b} полученных по стратегии 1

Порядок, N	БЛ$_{max}$	БЛ$_{max}$, дБ	ISLR	MF
31	0,0968	–20,2848	0,1561	6,4067
103	0,0680	–23,3548	0,2849	3,5106
239	0,0460	–26,7401	0,1742	5,7408
331	0,0393	–28,1177	0,1712	5,8420
383	0,0366	–28,7414	0,1751	5,7126
503	0,0338	–29,4224	0,1791	5,5840
587	0,0307	–30,2673	0,1697	5,8919
647	0,0309	–30,1975	0,1738	5,7541
719	0,0278	–31,1140	0,1757	5,6900
727	0,0289	–30,7863	0,1738	5,7545
787	0,0280	–31,0710	0,1698	5,8910
887	0,0259	–31,7239	0,1689	5,9217
907	0,0254	–31,9176	0,1943	5,1461

Продолжение таблицы 4.2

1019	0,0226	–32,9289	0,1684	5,9372
1123	0,0223	–33,0488	0,1705	5,8657
1279	0,0227	–32,8895	0,1712	5,8410
1283	0,0226	–32,9166	0,1669	5,9924
1307	0,0214	–33,3824	0,1668	5,9967
1319	0,0212	–33,4617	0,1696	5,8953
1423	0,0218	–33,2369	0,1676	5,9653
1447	0,0207	–33,6669	0,1695	5,8984
1451	0,0193	–34,2902	0,1693	5,9057
1511	0,0205	–33,7581	0,1679	5,9571
1607	0,0205	–33,7500	0,1681	5,9474
1759	0,0182	–34,8023	0,1679	5,9560

Таблица 4.3. Корреляционные характеристики кодовых последовательностей с алфавитом {1; –1} полученных по стратегии 2.

Порядок, N	$БЛ_{max}$	$БЛ_{max}$, дБ	ISLR	MF
15	0.1333	-17.5012	0.3822	2.6163
35	0.0857	-21.3389	0.2367	4.2241
143	0.0699	-23.1067	0.2777	3.6014
323	0.0464	-26.6622	0.2152	4.6472
899	0.0311	-30.1320	0.2219	4.5072
1763	0.0244	-32.2557	0.1985	5.0382
3599	0.0186	-34.6021	0.1943	5.1464
10365	0.0141	-37.0252	0.1951	5.1267

Таблица 4.4. Корреляционные характеристики кодовых последовательностей с алфавитом {1; $–b$} полученных по стратегии 2.

Порядок, N	$БЛ_{max}$	$БЛ_{max}$, дБ	ISLR	MF
15	0.1389	-17.1466	0.1821	5.4915

Продолжение таблицы 4.4

35	0.1067	-19.4394	0.2394	4.1770
143	0.0686	-23.2683	0.2517	3.9722
323	0.0495	-26.1060	0.2160	4.6305
899	0.0308	-30.2411	0.2124	4.7086
1763	0.0246	-32.1677	0.2189	4.5691
3599	0.0187	-34.5558	0.1986	5.0342
10365	0.0142	-36.9690	0.1951	5.1262

Таблица 4.5. Корреляционные характеристики кодовых последовательностей с алфавитом {1; –1} полученных по стратегии 3.

Порядок, N	$БЛ_{max}$	$БЛ_{max}$, дБ	ISLR	MF
15	0.1333	-17.5012	0.3467	2.8846
31	0.0968	-20.2848	0.1894	5.2802
63	0.0794	22.0074	0.2777	3.6016
127	0.0630	-24.0143	0.2707	3.6942
255	0.0471	-26.5472	0.2829	3.5344
511	0.0391	-28.1478	0.3370	2.9674
1023	0.0313	-30.0945	0.3452	2.8971

Таблица 4.6. Корреляционные характеристики кодовых последовательностей с алфавитом {1; $–b$} полученных по стратегии 3.

Порядок, N	$БЛ_{max}$	$БЛ_{max}$, дБ	ISLR	MF
15	0.1100	-19.1721	0.1260	7.9365
31	0.1086	-19.2867	0.2803	3.5675
63	0.0802	-21.9114	0.2846	3.5137
127	0.0702	-23.0745	0.2789	3.5857
255	0.0503	-25.9719	0.3014	3.3178
511	0.0381	-28.3912	0.3186	3.1387
1023	0.0326	-29.7436	0.3439	2.9077

Результаты, представленные в таблицах 4.3-4.6, 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. Данный вывод сделан на основе анализа значений критериев $БЛ_{max}$, ISLR и MF. КП, с алфавитом {1; –*b*} полученные по стратегии 1, на указанных в таблицах 4.2 длинах лучше по критерию максимального уровня бокового лепестка, однако на длинах 31, 331, 503, 587, 719, 1307, 1423 и 1511 суммарная энергия боковых лепестков выше, чем у кодовых последовательностей с алфавитом (1; –1).

Кодовые последовательности полученные по стратегии 3 были использованы при формировании маркированных сигналов в радиоканале распределенной системы радиолокационных станций в рамках выполнения НИР [150], а результаты анализа корреляционных характеристик рассмотренных в настоящем подразделе КП были использованы в рамках НИР [151].

4.2. Формирование ансамблей квазиортогональных КП с высокой структурной скрытностью на основе строк циклических квазиортогональных матриц

В радиотехнических системах (РТС) использующих метод прямой последовательности для расширения спектра (DSSS – Direct Sequence Spread Spectrum) одним из способов повышения помехозащищенности является увеличение базы сигнала *B*, для улучшения энергетических характеристик и, как следствия, повышения помехоустойчивости [119, 152-155].

Оговорим, что в рамках диссертационной работы под помехозащищенностью будем понимать способность РТС противодействовать помехам высокой мощности. Известно, что помехозащищенность включает в себя

помехоустойчивость и скрытность [156]. В настоящее время в качестве кодовых последовательностей широко используются последовательности Уолша [28], Баркера [72] (в том числе вложенные конфигурации [65, 120]), последовательности максимальной длины [144, 157] и их производные – последовательности Касами [158] и Голда [159]. Данные последовательности апробированы на практике и обеспечивают повышение помехоустойчивости РТС, однако в случае воздействия преднамеренных имитационных помех их известность может привести к снижению помехозащищенности РТС [155].

В данном случае приоритетнее становится другая составляющая помехозащищенности – скрытность, которая, как известно, включает в себя несколько составляющих – информационную, энергетическую и структурную [155-156]. В случае воздействия имитационных помех вскрытие структуры кодовой последовательности является наиболее значимым фактором, влияющим на помехозащищенность.

Подробный разбор вариантов повышения скрытности РТС был проведен в свежих работах [160-161], а их обзор позволяет выделить два актуальных направления – использование криптографических алгоритмов с целью полного сокрытия передаваемой информации, а также повышение структурной скрытности используемых кодовых последовательностей.

Второй вариант, как отмечают авторы [160], является более перспективным в виду того, что «…*сам факт использования методов криптозащиты выступает в качестве явного признака желания сокрытия информации, что может вызвать дополнительный интерес со стороны несанкционированных абонентов к содержанию передаваемого информационного контента*» [160].

Данный факт также подтверждает активность исследований в данной области [153, 155, 158-163]. Анализ указанных работ показывает как актуальность исследований в области разработки новых кодовых последовательностей, так и модификаций известных решений с целью придания им новых свойств.

Среди известных кодовых последовательностей следует выделить GMW (Гордона-Милса-Велча) последовательности [82-83], которые не уступают широко

известным *m*-последовательностям по корреляционным свойствам, но обладают повышенной структурной скрытностью. Данный класс последовательностей и их различные обобщения продолжают активно исследоваться в зарубежной и отечественной литературе [77, 82-83, 128, 155, 164-165]. Последние исследования сосредоточены на поиске предпочтительных пар GMW-последовательностей [155], а также поиске GMW-подобных последовательностей [128].

Проведенное в рамках диссертационной работы исследование демонстрирует, что GMW-последовательности могут служить базисом для построения циклических квазиортогональных матриц. Объединение теории синтеза КП с одноуровневой ПАКФ и теории квазиортогональных матриц открывает возможность наделения GMW-последовательностей новыми свойствами, что в перспективе позволяет создавать ансамбли квазиортогональных кодовых последовательностей с повышенной структурной скрытностью.

Предлагаемый подход к построению квазиортогонального ансамбля на основе GMW-последовательностей основан на взаимосвязях квазиортогональных матриц, которые были рассмотрены во втором разделе диссертации.

Целесообразно проверить, что процедура модификации не меняет основные корреляционные свойства GMW -последовательностей, а именно:

– максимальный уровень БЛ ААКФ соизмерим с максимальным уровнем БЛ для *m*-последовательностей;

– Количество уровней ПАКФ после модификации не изменяется;

– максимальный уровень БЛ периодической взаимокорреляционной функции (ПВКФ) возможных комбинаций пар GMW -последовательностей, не превышают максимальных уровней БЛ ПВКФ *m*-последовательностей.

Для проверки возьмем пару первых строк циклических квазиортогональных матриц с элементами $\{1,-b\}$. Первую из них возьмем из рассмотренного во втором разделе диссертации примера 3, а именно:

(-*b*,1,1,1,1,-*b*,1,1,1,-*b*,-*b*,1,1,1,1,-*b*,1,-*b*,-*b*,1,-*b*,1,1,-*b*,1,1,1,-*b*,1,-*b*,-*b*,-*b*,1,1,-*b*,1,-*b*,1,1,
-*b*,-*b*,1,1,-*b*,1,-*b*,-*b*,-*b*,1,1,1,-*b*,1,-*b*,-*b*,-*b*,1,-*b*,-*b*,-*b*,-*b*,-*b*,-*b*).

Вторую первую строку возьмем на основе GMW-последовательности, приведенной первой в работе [163, с. 5]. Тогда в табличном виде запись, будет иметь следующий вид:

$$GMW_{63} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Процедура нахождения элемента b для значения данного порядка аналогична. В обоих случаях элемент b=0.8.

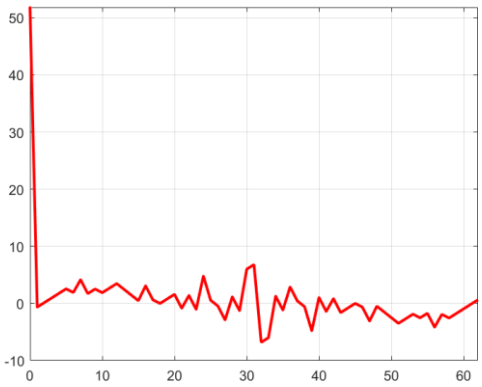
Вторая первая строка циклической квазиортогональной матрицы принимает следующий вид:

(1,1,1,-*b*,1,1,1,1,-*b*,1,1,-*b*,1,1,-*b*,1,-*b*,-*b*,-*b*,1,1,1,1,-*b*,-*b*,1,1,-*b*,-*b*,-*b*,-*b*,-*b*,1,
-*b*,1,1,1,-*b*,1,1,-*b*,-*b*,-*b*,1,1,-*b*,1,-*b*,-*b*,-*b*,-*b*,1,-*b*,1,-*b*,1,-*b*,-*b*,-*b*).

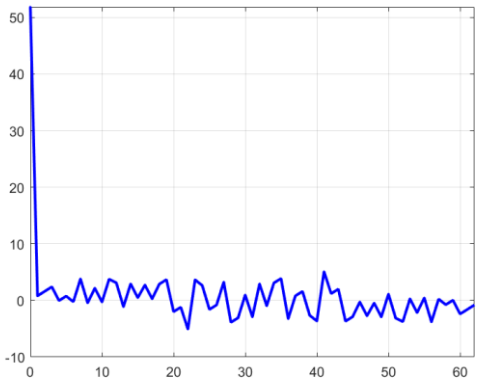
В среде компьютерного моделирования MATLAB были вычислены следующие функции для рассмотренных первых строк циклических квазиортогональных матриц: ААКФ первой строки (рисунок 4.4а), ААКФ второй строки (рисунок 4.4б), ПАКФ строки (рисунок 4.4в), ПАКФ строки (рисунок 4.4г), апериодическая взаимокорреляционная функция (АВКФ) двух строк (рисунок 4.4д) и ПВКФ двух строк (рисунок 4.4е).

Анализ рисунка 4.4 показывает, что процедура замены алфавита с {0,1} на {1,-*b*} не меняет количество уровней ПАКФ, однако максимальный уровень ААКФ для строк циклических квазиортогональных матриц снижается до уровня $\omega(n)$, против n для исходных GMW-последовательностей, что не является критичным для синхронных РТС. ПВКФ двух модифицированных последовательностей также показывает небольшие значения, что согласуется с теорией и в рассмотренном случае также образует предпочтительную пару [155], поскольку модуль

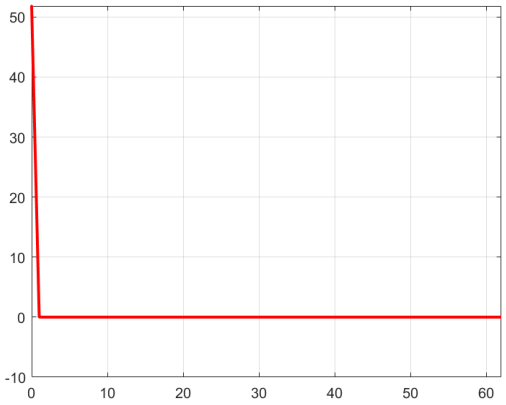
максимального значения не превышает $1+2^{[(k+2)/2]}$, где k определяется из длины GMW-последовательности $n=2^k-1$.



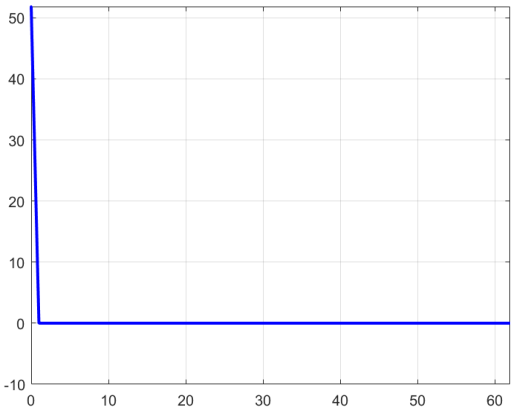
а)



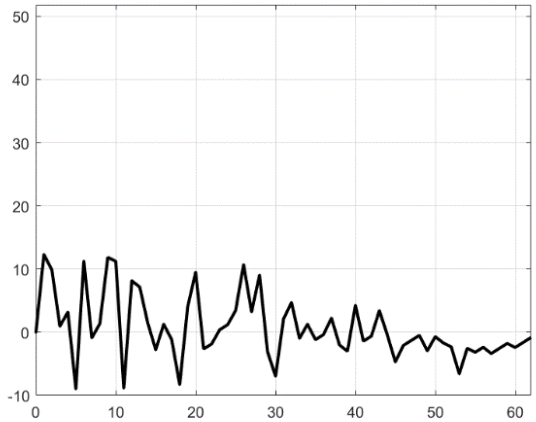
б)



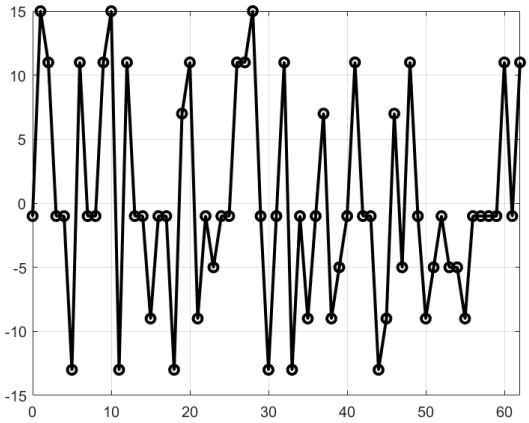
в)



г)



д)



е)

Рисунок 4.4 – Графики корреляционных функций строк циклических квазиортогональных матриц

4.3. Анализ спектральных характеристик результатов матричного маскирования изображений

Для метода матричного маскирования проработаны вопросы оценки устойчивости к искажениям и сжатию передаваемой информации, однако ранее в научной литературе не рассматривался вопрос возможности извлечения полезной информации в случае, если передаваемое маскированное квазиортогональной матрицей изображение стало доступно третьей стороне [166].

Анализ результатов маскирования был проведен для матриц с различным количеством уровней – двухуровневые и модульно двухуровневые, а также различной структурой – циклической и симметричной, которые представлены в таблице 4.7, в том числе с предлагаемыми в диссертационной работе.

Таблица 4.7 Используемые матрицы

№	Матрица	Структура	Уровни
1	Адамара, вычисленная методом Сильвестра	Симметричная	+1,-1
2	Адамара, структурированная по Уолшу	Симметричная	+1,-1
3	Мерсенна, структурированная по Уолшу [99]	Симметричная	+1, $-b$
4	Мерсенна, структурированная по Уолшу, модульно двухуровневая [99]	Симметричная	+1, -1, b, $-b$
5	Мерсенна, на основе модифицированных m - последовательностей [74]	Циклическая	+1, $-b$

Одним из основных методов анализа изображений и сигналов является их спектральный анализ, в основе которого лежит аппарат дискретного преобразования Фурье (ДПФ) [167-168]. Велика вероятность, что доступное третьей стороне маскированное изображение может быть подвергнуто анализу с использованием алгоритмов быстрого преобразования Фурье (БПФ).

Вычислительный эксперимент, при котором изображения подвергались одностороннему и двустороннему маскированию матрицами, указанными в таблице 4.7, проводился в пакете компьютерного моделирования MATLAB следующим образом.

В качестве тестового изображения выбрано широко используемое изображение Lena [169], переведенное в градации серого. Размер изображения 512×512 пикселей. Он определялся с учетом линейки порядков матриц, использованных в эксперименте.

1. Маскирование тестового изображения осуществлялось по формулам (3.1) и (3.2) матрицами Адамара порядков 2^t: 8, 16, 32, 64, 128, 256, 512 и матрицами Мерсенна порядков $2^t - 1$: 7, 15, 31, 63, 127, 255, 511. Следует сразу оговорить, что при размере $\mathbf{P}_n$ меньше размера тестового изображения маскирование осуществлялось блоками, соответствующими размерам $\mathbf{P}_n$. При маскировании матрицами Мерсенна для корректного разделения изображения на блоки оно дополнялось единицами, а для $\mathbf{P}_n$ размером 511×511 в исходном изображении был удален столбец 512 и строка 512.

2. Результат маскирования выводился в виде изображения для его визуального анализа.

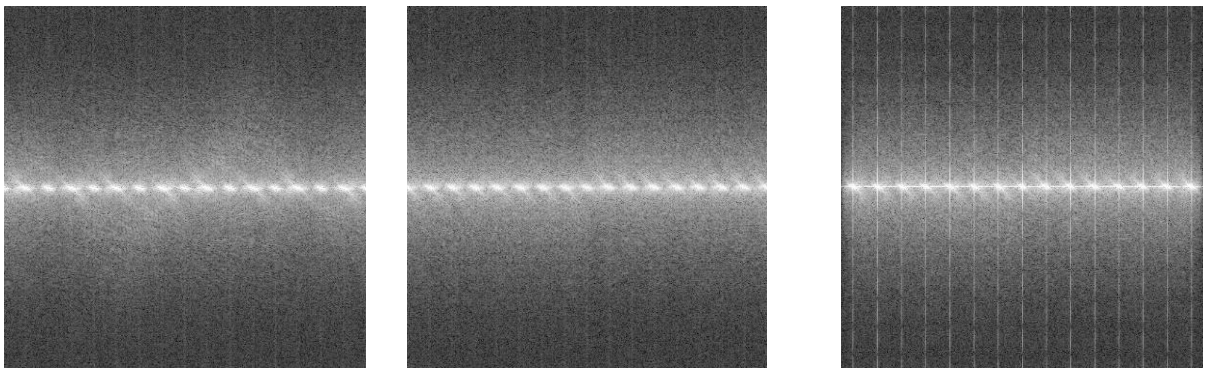
3. При помощи, встроенной в пакет MATLAB функции fft2(), вычислялся двумерный Фурье-спектр маскированного изображения. Вычислялся амплитудный и фазовый спектр маскированного изображения. Осуществлялось построение соответствующих графиков.

4. Осуществлялась попытка восстановить исходное изображение только по информации, содержащейся в фазовом спектре маскированного изображения, исходя из соображений о важности фазы в задании формы исходного изображения [122,168].

Итоги эксперимента подтвердили известные положения о том, что при небольшом размере $\mathbf{P}_n$ в результирующем маскированном изображении данные, хотя и значительно отличаются от исходных численно, однако при визуальном анализе на них определяются контуры объектов, что, благодаря ассоциативности

зрительного аппарата человека, обеспечивает возможность их идентификации [141].

Однако проведение эксперимента позволило получить новые результаты, представляющие значительный интерес. Например, при одностороннем маскировании матрицами 1, 2 и 4, приведенными в таблице 4.7, из графиков амплитудного и фазового спектров извлекаема информация о размере матрицы маскирования (см. рисунок 4.5). Здесь размеры $\mathbf{P}_n$: 16×16 для матриц Адамара и Адамара-Уолша, и 15×15 для матрицы Мерсенна-Уолша [166].



а) б) в)

Рисунок 4.5 – Двумерные амплитудные спектры изображения при одностороннем маскировании: матрицей Адамара (а); матрицей Адамара-Уолша (б); модульно двухуровневой матрицей Мерсенна-Уолша (в) [166]

В случае двустороннего маскирования результат становится еще более наглядным и это демонстрируется амплитудными спектрами изображения на рисунке 4.6. При этом маскирование матрицами 3 и 5 из таблицы 4.7 не позволяет определить размер $\mathbf{P}_n$ ни по амплитудному, ни по фазовому спектру.

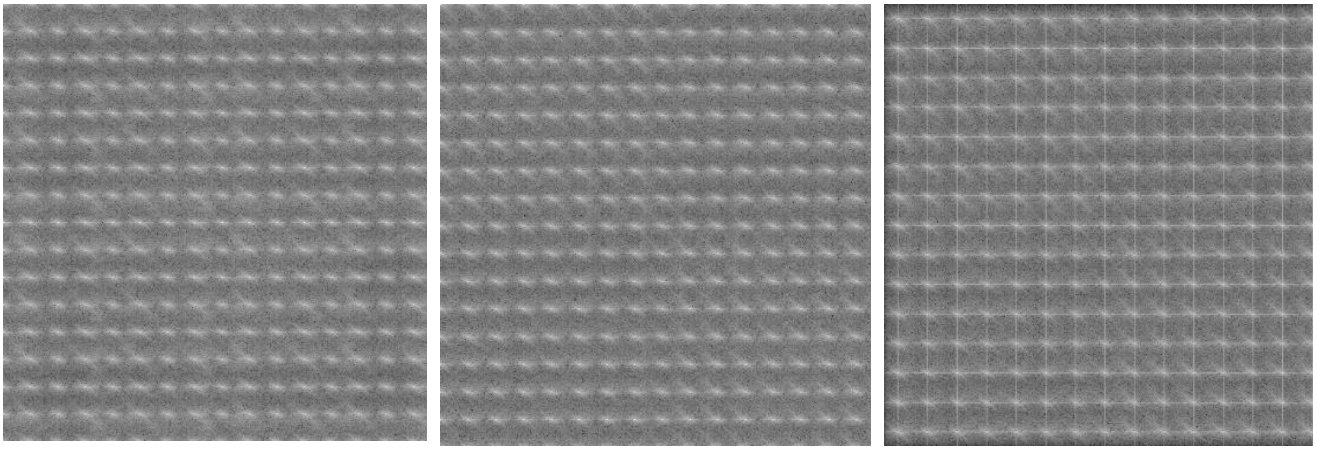
Результаты спектральных характеристик тестового изображения при его одностороннем и двустороннем маскировании всеми матрицами, приведенными в таблице 4.7, представлены в таблицах 4.8 и 4.9 соответственно.

Обзор научной литературы по теме матричного маскирования визуальной информации показывает, что на данный момент не существует универсальной

метрики оценки качества маскирования [143]. В связи с этим для проведения анализа были выбраны 4 критерия:

- критерий 1 – наличие контура в маскированном изображении;
- критерий 2 – наличие закономерностей в амплитудном спектре маскированного изображения;
- критерий 3 – наличие закономерностей в фазовом спектре маскированного изображения;
- критерий 4 – наличие контуров исходного изображения при восстановлении изображения только по фазовому спектру маскированного изображения.

с целью получения субъективной оценки по критериям 1 и 4 для визуального анализа маскированных изображений были привлечены пять независимых испытуемых. При этом испытуемым не было известно ни исходное изображение, ни алгоритм маскирования изображения. Изображения выдавались для визуального анализа от большего размера матрицы маскирования к меньшему. Оценка «+» ставилась если большинство испытуемых верно определили наличие контура исходного изображения, в противном случае ставилась оценка «-».



а) б) в)

Рисунок 4.6 – Двумерные амплитудные спектры изображения при двустороннем маскировании: матрицей Адамара (а); матрицей Адамара-Уолша (б); модульно двухуровневой матрицей Мерсенна-Уолша (в)

Выбор данных критериев обусловлен теми фактами, что, во-первых, наиболее важную информацию об изображениях объектов содержат их контуры,

при этом отметим, что другие компоненты изображения, такие как, например, градиентные или текстурные также важны, но играют меньшую роль [122], а во-вторых, тем, что именно в фазовом спектре изображений заключена информация о наличии и положении световых границ (контуров) изображения [122,168].

По критериям 2 и 3 оценки выставлялись автором самостоятельно на основе визуального анализа, аналогично тому, что было описано для рисунков 4.5 и 4.6.

Таблица 4.8. Результаты, полученные при одностороннем маскировании

Матрица Адамара, вычисленная методом Сильвестра							
Размер матрицы	8×8	16×16	32×32	64x64	128×128	256×256	512×512
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	+	-
Критерий 3	+	+	+	+	+	+	-
Критерий 4	+	+	+	-	-	-	-
Матрица Адамара, структурированная по Уолшу							
Размер матрицы	8×8	16×16	32×32	64×64	128×128	256×256	512×512
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	+	-
Критерий 3	+	+	+	+	+	+	-
Критерий 4	+	+	+	-	-	-	-
Матрица Мерсенна структурированная по Уолшу (2-х уровневая)							
Размер матрицы	7×7	15×15	31×31	63×63	127×127	255×255	511×511
Критерий 1	+	+	+	-	-	-	-
Критерий 2	-	-	-	-	-	-	-
Критерий 3	-	-	-	-	-	-	-
Критерий 4	+	+	-	-	-	-	-
Матрица Мерсенна структурированная по Уолшу (модульно 2-х уровневая)							
Размер матрицы	7x7	15x15	31x31	63x63	127x127	255x255	511x511
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	+	-

продолжение таблицы 4.8

Критерий 3	+	+	+	-	-	-	-
Критерий 4	+	+	-	-	-	-	-
Матрица на основе модифицированной *m* -последовательности							
Размер матрицы	7x7	15x15	31x31	63x63	127x127	255x255	511x511
Критерий 1	+	+	+	+	+	+	+
Критерий 2	-	-	-	-	-	-	-
Критерий 3	-	-	-	-	-	-	-
Критерий 4	+	+	+	-	-	-	-

Таблица 4.9. Результаты, полученные при двустороннем маскировании

Матрица Адамара, вычисленная методом Сильвестра							
Размер матрицы	8x8	16x16	32x32	64x64	128x128	256x256	512x512
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	+	-
Критерий 3	+	+	-	-	-	-	-
Критерий 4	+	-	-	-	-	-	-
Матрица Адамара, структурированная по Уолшу							
Размер матрицы	8x8	16x16	32x32	64x64	128x128	256x256	512x512
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	+	-
Критерий 3	+	+	+	+	-	-	-
Критерий 4	+	-	-	-	-	-	-
Матрица Мерсенна структурированная по Уолшу (2-х уровневая)							
Размер матрицы	7x7	15x15	31x31	63x63	127x127	255x255	511x511
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	-	-	-	-	-	-
Критерий 3	-	-	-	-	-	-	-
Критерий 4	+	+	-	-	-	-	-

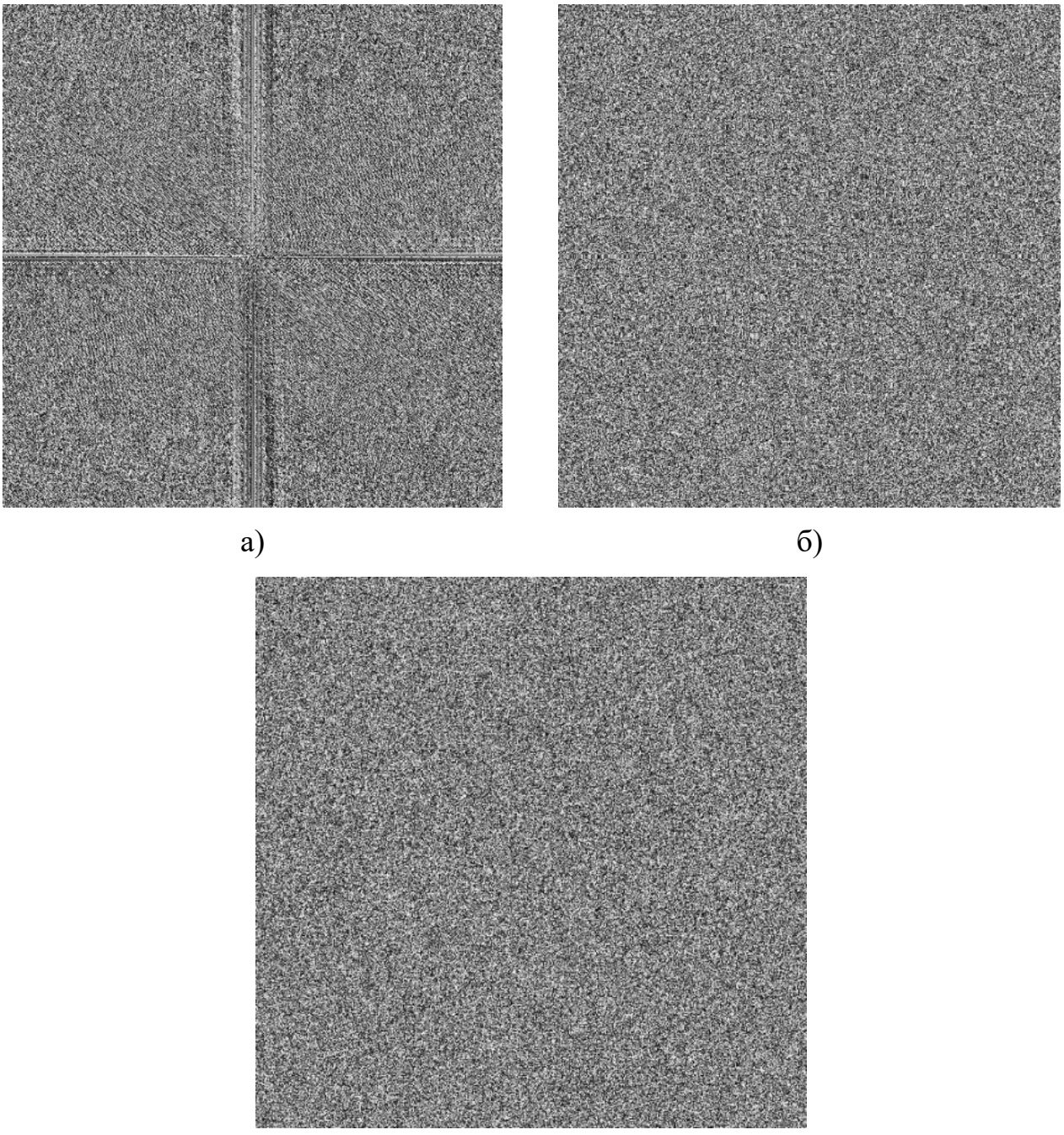
продолжение таблицы 4.9

Матрица Мерсенна структурированная по Уолшу (модульно 2-х уровневая)							
Размер матрицы	7x7	15x15	31x31	63x63	127x127	255x255	511x511
Критерий 1	+	+	+	-	-	-	-
Критерий 2	+	+	+	+	+	-	-
Критерий 3	+	+	+	+	-	-	-
Критерий 4	+	-	-	-	-	-	-
Матрица на основе модифицированной *m* -последовательности							
Размер матрицы	7x7	15x15	31x31	63x63	127x127	255x255	511x511
Критерий 1	+	+	+	+	-	-	-
Критерий 2	-	-	-	-	-	-	-
Критерий 3	-	-	-	-	-	-	-
Критерий 4	+	+	-	-	-	-	-

Дополнительно, в рамках проведения эксперимента, было выявлено, что при маскировании по (3.2), 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 $[-\pi;+\pi]$. В качестве примера на рисунке 4.7 приведены фазовые спектры исходного изображения, маскированного матрицей на основе модифицированной *m*-последовательности и матрицы элементы которой равномерно распределены на интервале $[-\pi;+\pi]$, полученной при помощи функции unifrnd() системы MATLAB.

Размер каждой матрицы 511×511. В дополнение к визуальному анализу двумерного фазового спектра изображения, маскированного циклической матрицей, при помощи критериев согласия Колмогорова-Смирнова и Пирсона была проверена гипотеза H0 – последовательность, сформированная из элементов матрицы фазового спектра принадлежит равномерному закону распределения с

параметрами $a=-\pi$, $b=+\pi$, с уровнем значимости 0.05. Оба критерия не отвергают нулевую гипотезу на заданном уровне значимости.



а) б)

в)

Рисунок 4.7 - Двумерные фазовые спектры: исходного изображения (а); изображения, маскированного циклической матрицей (б); матрицы с элементами, равномерно распределенными на интервале [-π;+π] [166]

4.4. Анализ качества маскирования цифровых аудиоданных

4.4.1. Анализ качества восстановления маскированных аудиоданных

Маскирование аудиоданных (аналогично маскированию изображений) является процедурой, приводящей передаваемые в коммуникациях данные к шумоподобному виду с последующим их восстановлением на приемной стороне.

Эксперименты по маскированию несжатых аудиоданных формата .wav проводились с использованием циклических матриц, которые были найдены при помощи предлагаемого в диссертационной работе метода. Источником тестовых аудиоданных был выбран датасет «UrbanSound8K» [170]. Частота дискретизации аудиофайлов составляет 48 КГц. Файлы, в которых количество отсчетов превышает количество элементов матрицы маскирования, были обрезаны для выравнивания их длин [171].

Некоторые файлы, с которыми проводились эксперименты, приведены в таблице 4.10.

Компьютерный эксперимент с оценкой параметров преобразований проводился по приведенному ниже алгоритму. В качестве матрицы-ключа использовалась квадратная двухуровневая циклическая квазиортогональная матрица на основе m-последовательности размера 511×511 со значениями элементов, равными 1 и $-b$, где $b = 0.9188$. Портрет указанной матрицы приведен на рисунке 4.8.

Таблица 4.10. Пример используемых в эксперименте аудиофайлов

Файл из датасета [170]	**Краткое описание содержимого**
108362-2-0-23.wav	Разговор двух собеседников
7383-3-0-0.wav	Лай собаки
24074-1-0-2.wav	Звуковой сигнал автомобиля

продолжение таблицы 4.10

26270-9-0-35.wav	Концерт на городской площади
40722-8-0-8.wav	Речь на фоне сирены
46669-4-0-37.wav	Высокочастотный писк
57320-0-0-0.wav	Пение птиц
59277-0-0-5.wav	Низкочастотный гул
196087-2-0-0.wav	Детский смех

1. На вход программы преобразования подавались аудиофайлы из файлов (таблицы 4.10).

2. Вычислялся амплитудный спектр аудиофайла.

3. В случае необходимости количество отсчетов аудиофайла выравнивалось с размерами матрицы маскирования.

4. Входной аудиофайл преобразовывался в матрицу с распределением блоков данных последовательно по строкам, как показано на рисунке 3.2, матрица аудиофайла формировалась размером 511×511.

5. Матрица отсчетов аудиофайла умножалась на матрицу маскирования по формуле (3.1) с формированием маскированного аудиофайла.

6. Для маскированного аудиофайла вычислялись метрики MSE и SNR в сравнении с исходным аудиофайлом.

7. С маскированным аудиофайлом производилось обратное преобразование по формуле (3.3) с формированием демаскированного аудиофайла.

8. Для демаскированного аудиофайла вычислялись метрики MSE, SNR для сравнения с входным аудиофайлом.

Эксперименты проводились с использованием специального программного обеспечения, разработанного в процессе выполнения диссертационной работы и реализованного на языке MATLAB [172, 173].

В качестве примера рассмотрим результаты маскирования и демаскирования звукового файла 108362-2-0-23.wav. На рисунке 4.9 приведены графики отсчетов

исходного входного звукового сигнала (а), маскированного (б) по формуле (3.1) и демаскированного (в) по формуле (3.3) [171].

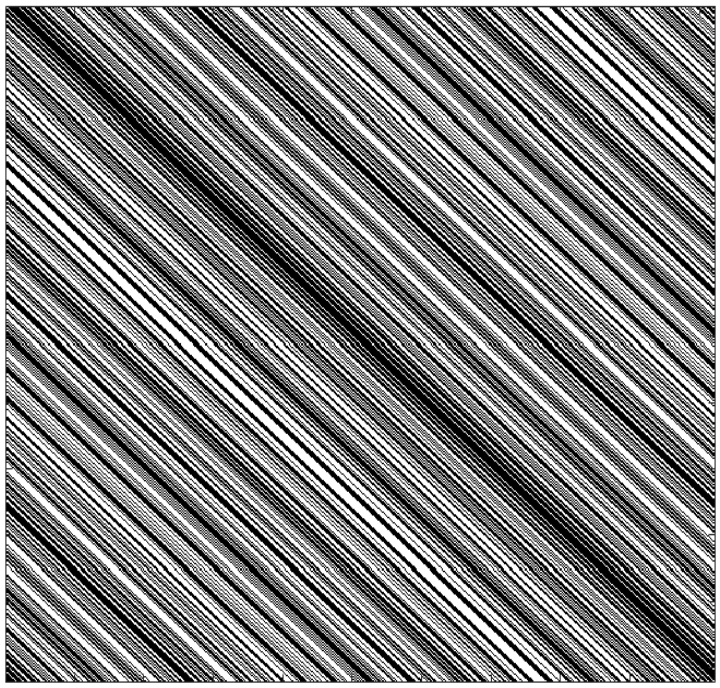
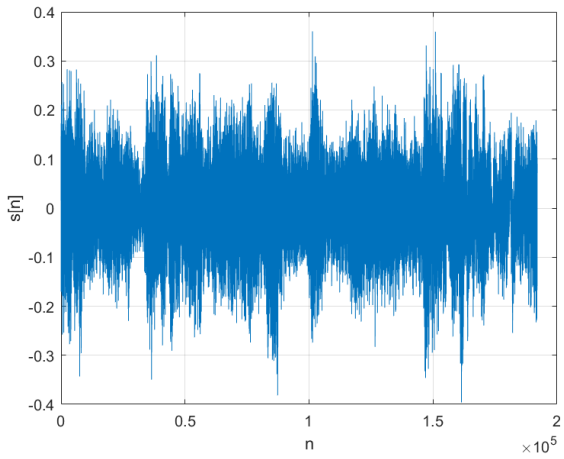


Рисунок 4.8 – Портрет матрицы маскирования

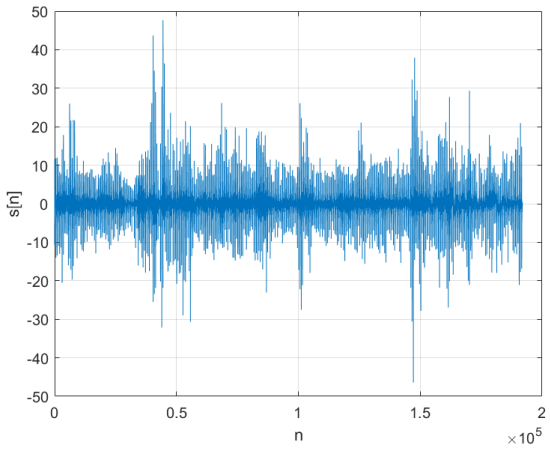
Из рисунка 4.9 следует, что, во-первых, график исходного и демаскированного аудиофайлов совпадают, подтверждая симметричность преобразования. Это подтверждается также метриками MSE и SNR.

Во-вторых, 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. При умножении матриц это даст большее усиление первого элемента первого столбца результата умножения, что может привести к переполнению разрядной сетки вычислителя. В случае двустороннего маскирования эффект будет усиливаться.

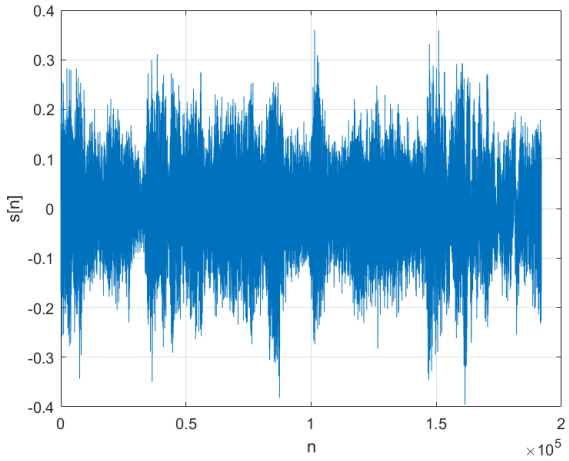
Предлагаемые циклические матрицы лишены указанного недостатка в виду того, что количество положительных и отрицательных элементов в строках и столбцах матрицы практически равно (отличается на единицу).



а)



б)



в)

Рисунок 4.9 – Графики отсчетов исходного (а), маскированного (б) и демаскированного (в) аудиофайлов

В таблице 4.11 приведены объективные метрики для аудиофайлов среднеквадратическая ошибка (MSE) и отношение сигнал-шум в децибелах (SNR). Отрицательные значения SNR для маскированных сигналов говорят о том, что их амплитуда значительно выше амплитуды исходных сигналов. Для демаскированных сигналов метрики MSE и SNR близки к машинному нулю.

Однако, классические метрики MSE и SNR не определяют качество маскирования аудиофайлов, поскольку субъективно, на слух, из аудиофайлов с самым низким и самым высоким значениями MSE (57320-0-0-0.wav и 26270-9-0-35.wav, соответственно) невозможно определить содержание аудиофайла. Если для оценки качества сжатых, обработанных аудиоданных существуют объективные

метрики, к примеру среднеквадратическая ошибка (MSE) или отношение сигнал/шум (SNR), то для оценки качества приведения аудиоданных к шумоподобному виду таких метрик нет, что подтверждает анализ предметной области.

Таблица 4.11. Объективные метрики качества для одностороннего маскирования аудиофайлов

Файл из датасета [170]	Маскированный аудиофайл		Демаскированный аудиофайл	
	MSE	SNR, дБ	MSE	SNR, дБ
108362-2-0-23.wav	2.0100	-26.7326	1.2415e-29	9.6433e-16
7383-3-0-0.wav	2.2712	-26.7326	1.1413e-29	9.6433e-15
24074-1-0-2.wav	6.3564	-26.7326	2.9602e-29	-1.4465e-15
26270-9-0-35.wav	23.6375	-26.7326	2.2560e-28	9.6433e-16
40722-8-0-8.wav	4.7825	-26.7326	3.0260e-29	3.8573e-15
46669-4-0-37.wav	1.1140	-26.7326	2.7322e-30	-3.3751e-15
57320-0-0-0.wav	0.8823	-26.7326	5.4861e-30	-2.8930e-15
59277-0-0-5.wav	13.4536	-26.7326	1.2646e-28	9.6433e-16
196087-2-0-0.wav	1.2740	-26.7326	6.4893e-30	-8.1968e-15

4.4.2. Оценка качества маскирования аудиофайлов

Как показал анализ предметной области, в отличие от существующих оценок качества восстановления данных после манипуляций с ними, для оценки качества маскирования – разрушения цифровых аудиоданных – ни методов, ни метрик не существует.

Мною предлагается подход к определению качества маскирования звукового сигнала [166], 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. Дополнительно проверять близость амплитудного спектра шума и маскированных данных предлагается при помощи среднеквадратического отклонения (RMSE) их значений.

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.

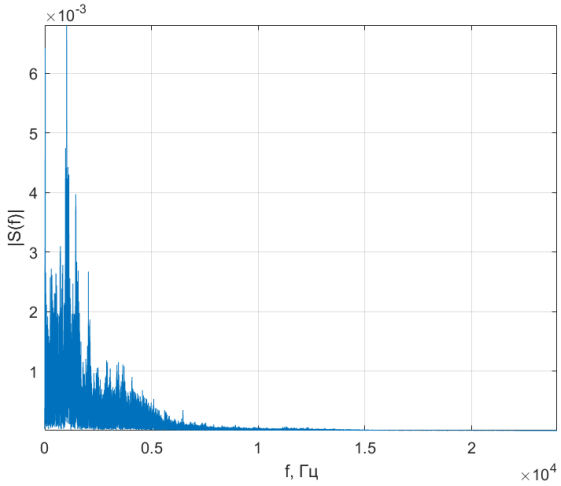
6. Вычисляется корень из среднеквадратичной ошибки (RMSE) значений амплитудного спектра маскированного аудиофайла и шума. Матрицы, которые лучше разрушают аудиофайлы при маскировании будут обладать меньшим значением RMSE между значениями амплитудного спектра маскированного аудиофайла и шума.

В качестве примера на рисунке 4.10 приведены амплитудные спектры входного аудиофайла 108362-2-0-23.wav, а также маскированного и демаскированного соответственно.

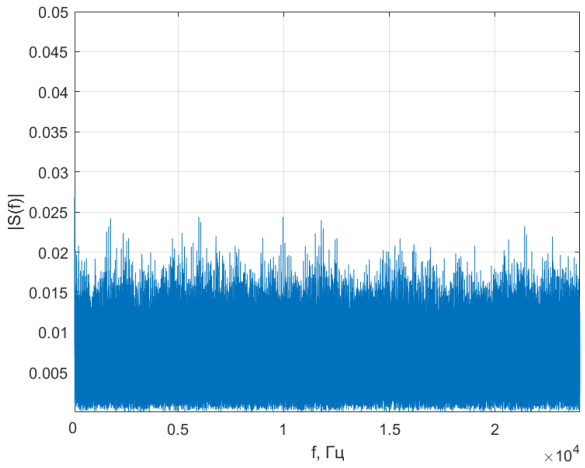
Анализ приведенных на рисунке 4.10 спектров показывает, что:

– амплитудный спектр маскированного аудиофайла равномерно распределен на всем диапазоне частот, в отличии от исходного;

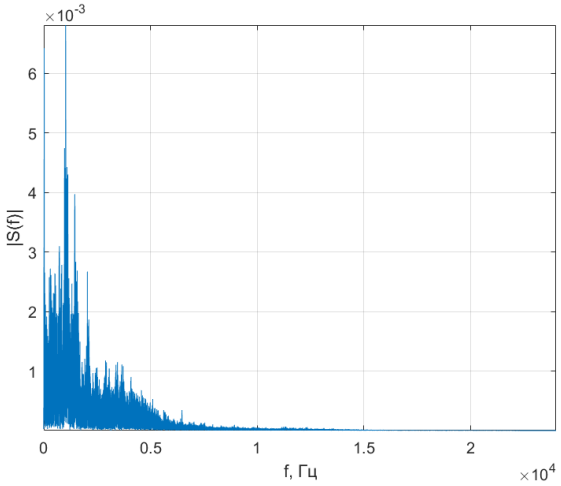
– процедура маскирования подавила все спектральные компоненты входного сигнала, сосредоточенные в диапазоне частот до 5 КГц.



а)



б)

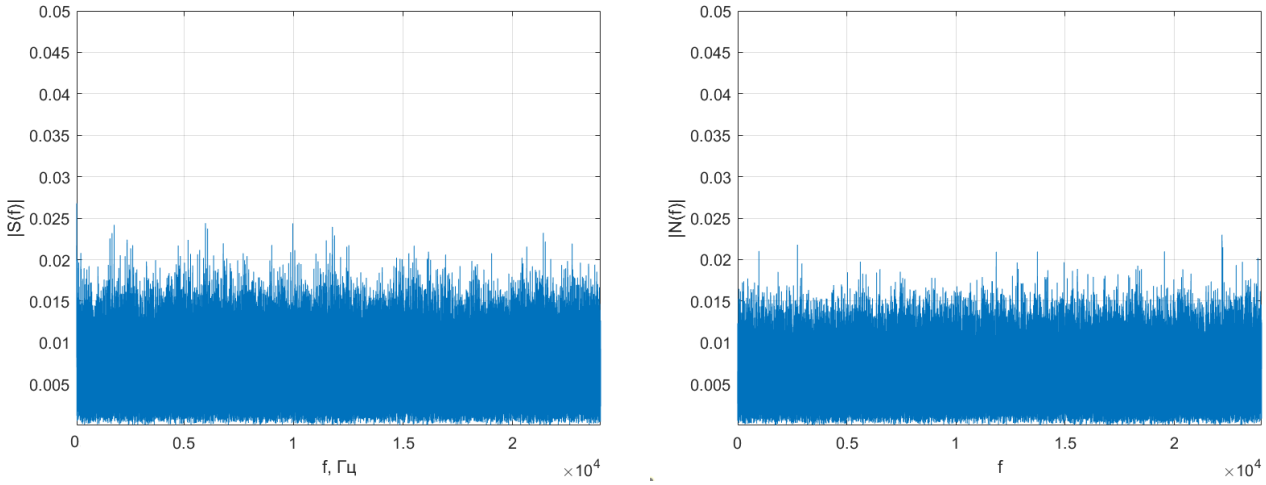


в)

Рисунок 4.10 – Амплитудный спектр исходного (а), маскированного (б) и демаскированного (в) сигналов

На рисунке 4.11 для сравнения приведены амплитудные спектры маскированного аудиофайла и гауссовского шума, с математическим ожиданием и среднеквадратическим отклонением, равными аналогичным параметрам маскированного аудиофайла.

Спектр маскированного аудиофайла близок к спектру белого гауссовского шума, RMSE между ними в рассматриваемом случае составляет $2{,}1379*10^{-05}$.



а) б)

Рисунок 4.11 – Сравнение амплитудных спектров маскированного сигнала (а) и белого гауссовского шума (б)

Эксперименты по матричному маскированию других аудиофайлов из таблицы 4.11 и выбранного датасета показали аналогичные результаты.

Предлагаемый подход был использован при выполнении НИР [174].

При маскировании аудиофайлов, как и видеофайлов, можно воспользоваться вариантом двухстороннего матричного преобразования соответственно по (3.2) и (3.4). В таком варианте осуществляется наиболее полное «перемешивание» фрагментов матрицы исходного сообщения, что соответствующим образом отображается на объективных метриках, которые для двухстороннего маскирования звуковых файлов приведены в таблице 4.12.

Однако, в данном случае, во-первых, пропорционально увеличиваются и вычислительные затраты алгоритма, в связи с этим для ускорения вычислительных процессов целесообразно использовать матрицы порядков, равных матрице, сформированной из исходного сообщения.

Таблица 4.12. Объективные метрики качества для двухстороннего маскирования аудиофайлов

Файл из датасета [170]	Маскированный аудиофайл		Демаскированный аудиофайл	
	MSE	SNR, дБ	MSE	SNR, дБ
108362-2-0-23.wav	949.1217	-53.4653	1.6724e-29	5.7860e-15
7383-3-0-0.wav	1.0678e+03		1.6213e-29	1.0608e-14
24074-1-0-2.wav	2.9936e+03		4.1723e-29	-3.3751e-15
26270-9-0-35.wav	1.1092e+04		2.9338e-28	-3.8573e-15
40722-8-0-8.wav	2.2713e+03		4.0415e-29	1.1572e-14
46669-4-0-37.wav	523.4474		5.2276e-30	-4.8216e-15
57320-0-0-0.wav	418.9160		7.4647e-30	-2.8930e-15
59277-0-0-5.wav	6.3379e+03		1.6126e-28	5.7860e-15
196087-2-0-0.wav	599.0425		9.0774e-30	1.0608e-14

Это становится возможным благодаря расширению класса ортогональных матриц нечетных порядков, в частности – предлагаемыми в данной работе, а, во-вторых, эксперименты показали, что для достижения близости амлитудного спектра маскированного аудиофайла и гауссовского шума достаточно одностороннего маскирования.

4.5. Выводы по разделу 4

Исследование кодовых последовательностей с несимметричным алфавитом $\{1,\text{-}b\}$, 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 являются 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 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.

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 заполненными единицами, что при умножении матриц даст большее усиление первого элемента первого столбца результата умножения, приводящее к переполнению разрядной сетки вычислителя. В случае двустороннего маскирования эффект будет лишь усиливаться. Предлагаемые циклические матрицы лишены указанного недостатка в виду того, что количество положительных и отрицательных элементов в строках и столбцах матрицы отличается всего на единицу.

ЗАКЛЮЧЕНИЕ

Основные результаты проведенных в рамках диссертационной работы 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 с хорошими корреляционными свойствами.

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. 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 конфиденциальности цифровой информации с небольшим периодом актуальности в различных областях применения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Балонин, Н. А. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские / Н. А. Балонин, М. Б. Сергеев. – СПб.: Политехника, 2019. – 196 с.

2. Ильин, В.А. Линейная алгебра: Учеб. Для вузов / В. А. Ильин, Э. Г. Поздняк. – 4-е изд. – М.: Наука: Физматлит, 1999 – 296 с.

3. Шикин Е.В. Начала компьютерной графики / Е. В. Шикин, А. В. Боресков, А. А. Зайцев; под общ. ред. Е.В. Шикина. – М.: Диалог-МИФИ, 1993. – 138 с.

4. Deisenroth M., Faisal A., Cheng Soon C. Mathematics for Machine Learning. Cambridge University Press. 2020. 398 p.

5. Якубова, У. Ш. Некоторые применения теории матриц в экономике / У. Ш. Якубова, Н. Т. Парпиева, Н. Ш. Мирходжаева // Бюллетень науки и практики. – 2021. – Т. 7, № 2. – С. 245-253. – DOI 10.33619/2414-2948/63/24.

6. Ryser H. J. Combinatorial mathematics. The carus mathematical monographs. The mathematical association of America. New York. John Wiley and Sons. 1963. No. 14. 162 p.

7. Гантмахер Ф. Р. Теория матриц. М.: Физматлит, 2010. 560 с.

8. Голуб, Дж. Матричные вычисления / Дж. Голуб, Ч. Ван Лоун. – пер. с англ. – М.: Мир, 1999. – 548 с.

9. Мазурова, Т. А. О применении ортогональных матриц в задачах шифрования, тестирования и оптимизации / Т. А. Мазурова // Известия ТРТУ. – 2004. – № 1(36). – С. 84-87.

10. Horadam K. J. Hadamard Matrices and Their Aplication. Princeton: Princeton University Press. 2007. 280 p.

11. Деундяк, В. М. О применении преобразования Уолша-Адамара в стеганографии / В. М. Деундяк, О. А. Хачумов // Фундаментальные исследования, методы и алгоритмы прикладной математики в технике, медицине и экономике: Материалы 17-ой Международной молодежной научно-практической

конференции, Новочеркасск, 06–07 сентября 2018 года. – Новочеркасск: ООО "Лик", 2018. – С. 135-140.

12. Урмаев, М. С. К теории преобразований координат в геодезии / М. С. Урмаев // Известия высших учебных заведений. Геодезия и аэрофотосъемка. – 2003. – № 2. – С. 8-13.

13. О результатах тестирования генератора псевдослучайных последовательностей на основе ортогональных матриц / О. Б. Макаревич, Т. А. Мазурова, И. Д. Сидоров, А. Г. Чефранов // Известия ТРТУ. – 2003. – № 4(33). – С. 262-265.

14. Гонсалес. Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.

15. Соловьев, Н. В. Особенности применения ортогональных (квазиортогональных) матриц для сжатия растровых изображений / Н. В. Соловьев, А. М. Сергеев // Научная сессия ГУАП : Сборник докладов. В 3-х частях, Санкт-Петербург, 09–13 апреля 2018 года. Том Часть II. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2018. – С. 402-404.

16. Шеремет, И. А. Обработка изображений с помощью целочисленных ортогональных преобразующих матриц / И. А. Шеремет, В. Д. Лебедев, А. П. Рукин // Цифровая обработка сигналов. – 2014. – № 4. – С. 45-52.

17. 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.

18. Гришенцев, А. Ю. Метод синтеза ансамблей широкополосных сигналов на базе ортогональных форм унитарных матриц преобразования Фурье / А. Ю. Гришенцев // Радиотехника. – 2019. – Т. 83, № 6(7). – С. 66-73. – DOI 10.18127/j00338486-201906(7)-12.

19. Леухин, А. Н. Построение циклических разностных множества Адамара / А. Н. Леухин // Математические методы распознавания образов. – 2009. – Т. 14, № 1. – С. 395-398.

20. Belevitch V. Theory of 2n-terminal networks with applications to conference telephony // Electrical Communication. 1950. Vol. 27. P. 231–244.

21. Dziech, A. Application of Enhanced Hadamard Error Correcting Code in Video-Watermarking and his comparison to Reed-Solomon Code / A. Dziech, J. Wassermann // MATEC Web of Conferences. – 2017. – V. 125. – 8 p. – DOI: 10.1051/matecconf/20171250

22. Балонин, Н. А. Матричные модели обобщенной кристаллографии / Н. А. Балонин, М. Б. Сергеев, В. С. Суздаль // Информационно-управляющие системы. – 2016. – № 4(83). – С. 26-33. – DOI 10.15217/issn1684-8853.2016.4.26.

23. Востриков, А. А. Матрицы Адамара - Мерсенна как базис ортогональных преобразований при маскировании видеоизображений / А. А. Востриков, Ю. Н. Балонин // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57, № 1. – С. 15-19.

24. Балонин, Ю. Н. О прикладных аспектах применения М-матриц / Ю. Н. Балонин, А. А. Востриков, М. Б. Сергеев // Информационно-управляющие системы. – 2012. – № 1(56). – С. 92-93

25. Sergeev, A. M. 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.

26. Куликова, М. В. О дифференцировании матричных ортогональных преобразований / М. В. Куликова, Ю. В. Цыганова // Журнал вычислительной математики и математической физики. – 2015. – Т. 55, № 9. – С. 1460. – DOI 10.7868/S0044466915090112.

27. О выборе матриц для процедур маскирования и демаскирования изображений / А. А. Востриков, О. В. Мишура, А. М. Сергеев, С. А. Чернышев // Фундаментальные исследования. – 2015. – № 2-24. – С. 5335-5339.

28. Ахмед, Н. Ортогональные преобразования при обработке цифровых сигналов / Н. Ахмед, К. Р Рао. – пер. с англ.; под ред. И.Б. Фоменко. – М.: Связь, 1980. – 248 с.

29. 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: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2023. – С. 196-201. – DOI 10.31799/978-5-8088-1824-8-2023-3-196-201.

30. Эксперименты по замене ДКП квазиортогональным преобразованием в алгоритмах сжатия изображений / В. А. Ненашев, А. М. Сергеев, Е. А. Капранова, К. Ю. Рыжов // Научная сессия ГУАП: Сборник докладов. В 3-х частях, Санкт-Петербург, 09–13 апреля 2018 года. Том Часть II. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2018. – С. 369-373.

31. Suksmono, A. B. Finding a Hadamard matrix by simulated annealing of spin vectors / A. B. Suksmono // Journal of Physics: Conference Series. – 2017. № 856 012012. P. 10. – DOI 10.1088/1742-6596/856/1/012012.

32. Балонин, Н. А. Матрицы Адамара нечетного порядка / Н. А. Балонин, Л. А. Мироновский // Информационно-управляющие системы. – 2006. – № 3(22). – С. 46-50.

33. Балонин, Н. А. М-матрицы / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2011. – № 1(50). – С. 14-21.

34. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge University Press. 2010. 504 p.

35. Vostricov A., Sergeev M., Balonin N., Sergeev A. Use of symmetric Hadamard and Mersenne matrices in digital image processing // Procedia Computer Science. 2018. Vol.126. P. 1054-1061

36. Балонин, Н. А. Как гипотезе Адамара помочь стать теоремой. Часть 1 / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2018. – № 6(97). – С. 2-13. – DOI 10.31799/1684-8853-2018-6-2-13.

37. Сергеев, А. М. Обоснование перехода гипотезы Адамара в теорему / А. М. Сергеев // Известия высших учебных заведений. Приборостроение. – 2021. – Т. 64, № 2. – С. 90-96. – DOI 10.17586/0021-3454-2021-64-2-90-96.

38. Scarpis U. Sui determinanti di valore Massimo // Rendiconti della R. Istituto Lombardo di scienze e lettere. 1898. No. 31. P. 1441–1446.

39. Сергеев, А. М. Анализ реализаций метода Скарпи при вычислении матриц Адамара высоких порядков симметричных структур / А. М. Сергеев // Наука, технологии, общество - НТО-2021 : сборник научных статей по материалам Всероссийской научной конференции, Красноярск, 29–31 июля 2021 года. – Красноярск: Общественное учреждение "Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений", 2021. – С. 104-110. – DOI 10.47813/dnit-nto.2021.104-110.

40. Paley R. E. A. C. On orthogonal matrices // Journal of mathematics and physics. 1933. Vol. 12. P. 311—320.

41. Handbook of combinatorial designs. Discrete mathematics and its applications. Ed. by Ch. J. Colbourn, J. H. Dinitz. Chapman and Hall. CRC. 2006. 1000 p.

42. Сергеев, А. М. К проблеме поиска матриц Адамара порядка 668 / А. М. Сергеев, Ю. Н. Балонин // Вестник кибернетики. – 2021. – № 3(43). – С. 6-11. – DOI 10.34822/1999-7604-2021-3-6-11.

43. Baumert L. D., Golomb S.W., Marshall H. Discovery of an Hadamard matrix of order 92 JR. Communicated by F. Bohnenblust, California Institute of Technology // Bull. Amer. Math. Soc. 68, 1962, pp. 237-238.

44. THE INITIAL PAPERS [Электронный ресурс]. – Режим доступа: http://mathscinet.ru/catalogue/init/index.php

45. Craigen R., Kharaghani H. Hadamard Matrices and Hadamard Designs // Handbook of Combinatorial Designs. Ed. by Charles J. Colbourn and Jeffrey H. Dinitz. Second ed. — Boca Raton, FL: Chapman &Hall. CRC, 2006. Pp. 273–280.

46. Awyzio G. On Good Matrices and Skew Hadamard Matrices / G. Awyzio, J. Seberry. [Электронный ресурс]. – Режим доступа: http://mathscinet.ru/files/2015_11_Good_matrices.pdf

47. Seberry W. J. A Skew-Hadamard Matrix of Order 92 // Bulletin of the Australian Mathematical Society.1971. Vol. 5. P. 203–204.

48. Балонин, Н. А. Матрицы Пропус 92 и 116 / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2016. – № 2(81). – С. 101-103. – DOI 10.15217/issn1684-8853.2016.2.101.

49. N. A. Balonin and Jennifer Seberry A review and new symmetric conference matrices // Информационно-управляющие системы. – 2014. – № 4. – С. 2 -7

50. Di Matteo O., Djokovic D. Z., Kotsireas I. S. Symmetric Hadamard Matrices of Order 116 and 172 Exist. Special Matrices. 2015. Vol. 3.1. P. 227–234.

51. Балонин, Ю. Н. Двуциклические матрицы Адамара, взвешенные матрицы и гипотеза Райзера / Ю. Н. Балонин, А. М. Сергеев // Информационно-управляющие системы. – 2018. – № 3(94). – С. 2-9. – DOI 10.15217/issn1684-8853.2018.3.2.

52. Балонин, Н. А. Как гипотезе Адамара помочь стать теоремой. Часть 2 / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2019. – № 1(98). – С. 2-10. – DOI 10.31799/1684-8853-2019-1-2-10.

53. Балонин, Н. А. Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2013. – № 5(66). – С. 97-98.

54. Балонин, Н. А. Порядок и беспорядок в мире матриц, принцип неограниченно возрастающей сложности / Н. А. Балонин, А. М. Сергеев // Математические методы и модели в высокотехнологичном производстве: Сборник тезисов докладов II Международного форума, Санкт-Петербург, 09 ноября 2022 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. – С. 14-17.

55. Балонин, Ю. Н. М-матрица 22-го порядка / Ю. Н. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2011. – № 5(54). – С. 87-90.

56. Балонин, Н. А. К вопросу существования матриц Мерсенна и Адамара / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2013. – № 5(66). – С. 2-8.

57. Балонин, Н. А. Вычисление матриц Мерсенна и Адамара методом Скарпи / Н. А. Балонин, Ю. Н. Балонин, М. Б. Сергеев // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 3(91). – С. 103-111.

58. Вычисление матриц Мерсенна-Уолша / Н. А. Балонин, Ю. Н. Балонин, А. А. Востриков, М. Б. Сергеев // Вестник компьютерных и информационных технологий. – 2014. – № 11(125). – С. 51-56. – DOI 10.14489/vkit.2014.011.pp.051-056.

59. Балонин, Н. А. Вычисление матриц Мерсенна методом Пэли / Н. А. Балонин, М. Б. Сергеев // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57, № 10. – С. 38-41.

60. Балонин, Н. А. Матрицы локального максимума детерминанта / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2014. – № 1(68). – С. 2-15.

61. Балонин, Н. А. Матрицы Мерсенна и Адамара / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2016. – № 1(80). – С. 2-15. – DOI 10.15217/issn1684-8853.2016.1.2.

62. О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел / Ю. Н. Балонин, А. А. Востриков, А. М. Сергеев, И. С. Егорова // Труды СПИИРАН. – 2017. – № 1(50). – С. 209-223. – DOI 10.15622/SP.50.9.

63. Сергеев, А. М. От первых М-матриц до семейств квазиортогональных матриц / А. М. Сергеев // EUROPEAN RESEARCH : сборник статей XXVIII Международной научно-практической конференции, Пенза, 07 сентября 2020 года. – Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2020. – С. 49-54.

64. Ненашев, В. А. Исследование и анализ автокорреляционных функций кодовых последовательностей, сформированных на основе моноциклических квазиортогональных матриц / В. А. Ненашев, А. М. Сергеев, Е. А. Капранова //

Информационно-управляющие системы. – 2018. – № 4(95). – С. 9-14. – DOI 10.31799/1684-8853-2018-4-9-14.

65. Сергеев, М. Б. Вложенные кодовые конструкции Баркера - Мерсенна - Рагхаварао / М. Б. Сергеев, В. А. Ненашев, А. М. Сергеев // Информационно-управляющие системы. – 2019. – № 3(100). – С. 71-81. – DOI 10.31799/1684-8853-2019-3-71-81.

66. Мироновский Л.А., Слаев В.А. Стрип-метод преобразования изображении и сигналов: Монография / СПб.: Политехника, СПб., 2006. 163 с.: ил.

67. Сергеев, А. М. Связь симметрии и антисимметрии квазиортогональных циклических матриц с простыми числами / А. М. Сергеев // Труды учебных заведений связи. – 2022. – Т. 8, № 4. – С. 14-19. – DOI 10.31854/1813-324X-2022-8-4-14-19.

68. 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. – DOI 10.34832/ELSV.2020.11.10.008.

69. 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 : Saint-Petersburg State University of Aerospace Instrumentation, 2020. – P. 73-76.

70. Балонин, Н.А. Окружности на решетках и матрицы Адамара / Н.А. Балонин, М.Б. Сергеев, Д. Себерри, О.И. Синицына // Информационно-управляющие системы. – 2019. – № 3 (100). – С. 2-9. DOI:10.31799/1684-8853-2019-3-2-9.

71. Балонин, Н. А. Динамические генераторы квазиортогональных матриц семейства Адамара / Н. А. Балонин, М. Б. Сергеев, В. С. Суздаль // Труды СПИИРАН. – 2017. – № 5(54). – С. 224-243. – DOI 10.15622/sp.54.10.

72. Barker R.H. Group synchronization of binary digital systems, in Jackson. W. (ed.) // Communication Theory. – Academic Press, London, 1953, pp. 273-287.

73. Балонин Н. А., Сергеев М. Б. Нормы обобщенных матриц Адамара // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. – 2014. № 2. – С. 5–11.

74. Barba, G. Intorno al Teorema di Hadamard sui Determinanti a Valore Massimo / G.Barba // Giorn. Mat. Battaglini. 1933

75. 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.

76. Парсаев, Н. В. Синтез и анализ фазокодированных последовательностей с одноуровневой периодической автокорреляционной функцией : специальность 05.12.04 "Радиотехника, в том числе системы и устройства телевидения" : диссертация на соискание ученой степени кандидата технических наук / Парсаев Николай Владимирович. – Йошкар-Ола, 2010. – 225 с.

77. Golomb S.W., Gong G. Signal design for good correlation for wireless communication, cryptography, and radar. Cambridge Univ. Press, 2006.

78. Golomb S.W. Remarks on orthogonal sequences. The Glenn L. Martin Company, Baltimore, MD, July 28, 1954.

79. Golomb S.W. Sequences with randomness properties. Baltimore, Glenn L. Martin Company, 1955.

80. Stanton R. G., Sprott D.A. A family of difference sets. Canadian Journal of Mathematics. 10 (1958).

81. Hall M. Survey of difference sets. Proceedings of the American Mathematical Society. 7 (1956). P.975-986.

82. Gordon B., Mill W.H., Welch L.R. Some new difference sets. Canadian Journal of Mathematics. 14 (1962). P. 614–625.

83. Scholtz R.A., Welch L.R. GMW sequences. IEEE Transactions on Information Theory. 1984. Vol. IT-30, №9.

84. Gong G., Gaal P., Golomb S.W. A suspected infinite class of cyclic Hadamard difference sets. Proceedings of 1997 IEEE Information Theory Workshop. July 6–12, 1997. Longyarbyen, Svalbard, Norway.

85. Gong, G., Youssef, A.M. On Welch-Gong Transformation Sequence Generators. In: Stinson, D.R., Tavares, S. (eds) Selected Areas in Cryptography. SAC 2000. Lecture Notes in Computer Science, 2001. vol 2012. Springer, Berlin, Heidelberg. DOI: 10.1007/3-540-44983-3_16

86. Glynn D. G. Two new sequences of ovals in finite Desarguesian planes of even order. Lecture Notes in Mathematics. V. 1036, Berlin, Springer-Verlag, 1983.P. 217–229.

87. Segre B. Ovals in finite projective plane. Canadian Journal of Mathematics. 1955. V. 7. P. 414–416.

88. Handbook of Combinatorial Designs. Second Edition (Discrete Mathematics and its Applications). 2nd Ed. / C. J. Colbourn (Ed.), J. H. Dinitz (Ed.). London: Chapman and Hall. CRC. 2006. – 1000 p.

89. Balonin N, Seberry J. Two-level Cretan matrices constructed using SBIBD. Special Matrices. 2015. 3(1).

90. 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.

91. 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

92. 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.

93. 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.

94. 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.

95. 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.

96. Исследование связей разложений чисел и окружностей на решетках со структурами квазиортогональных матриц, используемых в помехоустойчивом кодировании и построении орнаментов: отчет о НИР (промежуточный, 3 этап) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Григорьев Е. К. [и др.]. СПб., 2020. 137 с. – № ГР АААА-А17-117042710042-9.

97. Хвощ, С. Т. Матрицы Адамара в космической связи / С. Т. Хвощ // Инженерный вестник Дона. – 2024, – №1. 13 с. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_24__1y24_Chvosh.pdf_a054a7270c.pdf.

98. Balonin, N.A., Sergeev, M.B., Petoukhov, S.V. Development of Matrix Methods for Genetic Analysis and Noise-Immune Coding. In: Hu, Z., Petoukhov, S., He, M. (eds) Advances in Artificial Systems for Medicine and Education III. AIMEE 2019. Advances in Intelligent Systems and Computing. V 1126. Springer. Cham. 2020. DOI: 10.1007/978-3-030-39162-1_4

99. Vostrikov, A., Sergeev, A., Balonin, Y. Using Families of Extremal Quasi-Orthogonal Matrices in Communication Systems. In: Czarnowski, I., Howlett, R.J., Jain, L.C. (eds) Intelligent Decision Technologies. Smart Innovation, Systems and Technologies, V. 238. Springer, Singapore. 2021. DOI: 10.1007/978-981-16-2765-1_8

100. Kapranova E. Distributed matrix methods of compression, masking and noise-resistant image encoding in a high-speed network of information exchange, information

processing and aggregation / V. A. Nenashev, A. M. Sergeev, D. A. Burylev, S. A. Nenashev // Proceedings of SPIE V. 11197, SPIE Future Sensing Technologies. 111970T. DOI: 10.1117/12.2542677

101. Grigoriev, E. 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: Saint-Petersburg State University of Aerospace Instrumentation, 2022. – P. 97-102.

102. 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.

103. Sergeev A., Nenashev V., Vostrikov A., Shepeta A., Kurtyanik D. Discovering and Analyzing Binary Codes Based on Monocyclic Quasi-Orthogonal Matrices // Smart Innovation, Systems and Technologies Volume 143. Springer, 2019. P.113 – 123. DOI: 10.1007/978-981-13-8303-8.

104. Ненашев В.А., Бестугин А.Р., Киршина И.А., Ненашев С.А. Методика поиска модифицированных кодовых последовательностей Баркера // T-Comm: Телекоммуникации и транспорт. 2023. Том 17. №12. С. 15-21.

105. Nenashev, V.A.; Bestugin, A.R.; Rabin, A.V.; Solenyi, S.V.; Nenashev, S.A. Modified Nested Barker Codes for Ultra-Wideband Signal–Code Constructions. Sensors. 2023, 23, 9528. https://doi.org/10.3390/s23239528

106. Sergeev, M., Sentsov, A., Nenashev, V., Grigoriev, E. Triple-Station System of Detecting Small Airborne Objects in Dense Urban Environment. In: Czarnowski, I., Howlett, R.J., Jain, L.C. (eds) Intelligent Decision Technologies. Smart Innovation, Systems and Technologies, vol 238. Springer, Singapore. 2021. P. 83-93. https://doi.org/10.1007/978-981-16-2765-1_7

107. 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. DOI: 10.1117/12.2600133

108. 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. DOI: 10.1117/12.2574238

109. Востриков, А. А. Маскирование цифровой визуальной информации: термин и основные определения / А. А. Востриков, М. Б. Сергеев, М. Ю. Литвинов // Информационно-управляющие системы. – 2015. – № 5(78). – С. 116-123. – DOI: 10.15217/issn1684-8853.2015.5.116.

110. Vostrikov A., Sergeev, M.. Development Prospects of the Visual Data Compression Technologies and Advantages of New Approaches. In: Pietro, G., Gallo, L., Howlett, R., Jain, L. (eds) Intelligent Interactive Multimedia Systems and Services 2016. Smart Innovation, Systems and Technologies, vol 55. Springer, Cham. 2016. P. 179-190. DOI: 10.1007/978-3-319-39345-2_16.

111. Востриков, А. А. О матрицах Адамара-Мерсенна и маскировании изображений / А. А. Востриков // Информационные технологии. – 2013. – № 11. – С. 37-39.

112. Цифровое маскирование матрицами Мерсенна и его особые изображения / Ю. Н. Балонин, А. А. Востриков, Е. А. Капранова [и др.] // Фундаментальные исследования. – 2017. – № 4-1. – С. 13-18.

113. Tokarevskiy, I. V. Features of Matrix Masking of Digital Radar Images / I. V. Tokarevskiy, A. A. Sentsov, M. B. Sergeev // Wave Electronics and Its Application in Information and Telecommunication Systems. – 2022. – Vol. 5, No. 1. – P. 488-491

114. Сергеев, А. М. Структурированные по Уолшу двухуровневые и модульно двухуровневые квазиортогональные матрицы для маскирования изображений / А. М. Сергеев // Известия высших учебных заведений.

Приборостроение. – 2023. – Т. 66, № 5. – С. 399-408. – DOI 10.17586/0021-3454-2023-66-5-399-408.

115. Метод обеспечения конфиденциальности данных с применением ортогональных матриц / М. Б. Сергеев, Т. М. Татарникова, А. М. Сергеев, В. В. Боженко // Инженерный вестник Дона. – 2024. – № 1(109). – С. 201-209.

116. Григорьев, Е. К. Способ защитного кодирования данных, получаемых оптическими сенсорами беспилотных авиационных систем / Е. К. Григорьев, А. М. Сергеев // Труды МАИ. – 2023. – № 133 – 27 с. URL: https://trudymai.ru/published.php?ID=177675.

117. Sergeev A., Sergeev M., Vostrikov A., Kurtyanik D. Portraits of Orthogonal Matrices as a Base for Discrete Textile Ornament Patterns. In: Czarnowski, I., Howlett, R., Jain, L. (eds) Intelligent Decision Technologies 2019. Smart Innovation, Systems and Technologies. V. 143. Springer, Singapore. 2019. P. 135-143. DOI: 10.1007/978-981-13-8303-8_12.

118. Сергеев, А. М. Матричный портрет как основа дискретного текстильного орнамента / А. М. Сергеев, Д. В. Куртяник, К. Ф. Тарашкевичус // Известия высших учебных заведений. Технология легкой промышленности. – 2019. – Т. 44, № 2. – С. 102-107.

119. Быстров, Н. Е. Синтез сигналов с псевдослучайным законом амплитудно-фазовой манипуляции и методы их обработки в РЛС с квазинепрерывным режимом работы : специальность 05.12.14 "Радиолокация и радионавигация" : диссертация на соискание ученой степени доктора технических наук / Быстров Николай Егорович. – Великий Новгород, 2005. – 260 с.

120. Банкет В.Л. Композитные коды Баркера / В. Л. Банкет, М.С. Токарь // Цифрові технології. – 2007, – №2. – С.8-17.

121. Костров, Б. В. Сжатие изображений на основе ортогональных преобразований / Б. В. Костров, А. С. Бастрычкин // Известия Тульского государственного университета. Технические науки. – 2016. – № 9. – С. 113-119.

122. Красильников Н. Н. Теория передачи и восприятия изображений. М.: Радио и связь, 1986. 246 с.

123. Сергеев, А. М. Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц: специальность 05.12.13 "Системы, сети и устройства телекоммуникаций»: диссертация на соискание ученой степени кандидата технических наук / Сергеев Александр Михайлович. – Санкт-Петербург, 2020. – 153 с.

124. Чернышев, С. А. Разработка и исследование метода матричного маскирования видеоинформации в глобально распределенных системах: специальность 05.12.13 "Системы, сети и устройства телекоммуникаций": диссертация на соискание ученой степени кандидата технических наук / Чернышев Станислав Андреевич, 2018. – 120 с.

125. Востриков, А. А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами / А. А. Востриков, С. А. Чернышев // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – № 5(87). – С. 99-103.

126. Востриков, А. А. О восстановлении маскированного изображения при возникновении информационных потерь в процессе передачи / А. А. Востриков, С. А. Чернышев // Научная сессия ГУАП, Санкт-Петербург, 07–11 апреля 2014 года. Том Часть II. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2014. – С. 185-189.

127. Балонин, Н. А. Критские матрицы Одина и Тени, сопровождающие простые числа и их степени / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2022. – № 1(116). – С. 2-7. – DOI: 10.31799/1684-8853-2022-1-2-7.

128. Владимиров, С. С. Обработка широкополосных последовательностей Гордона-Миллса-Велча с использованием двойственного базиса на основе двух регистров / С. С. Владимиров, О. С. Когновицкий // Труды учебных заведений связи. – 2019. – Т. 5, № 2. – С. 49-58. – DOI 10.31854/1813-324X-2019-5-2-49-58.

129. Advanced encryption standard (AES) (FIPS 197). [Электронный ресурс].Режим доступа: ttps://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

130. Rahman Md. M., Saha T.K., Bhuiyan Md. A. Implementation of RSA algorithm for speech data encryption and decryption. International Journal of Computer Science and Network Security. 2012. V. 12. Issuse. 3. P 74-82.

131. Gnanajeyaraman R., Prasadh K. Audio encryption using higher dimensional chaotic map. International Journal of Recent Trends in Engineering. 2009. V. 1. Issue. 2. P. 103-107.

132. Hassan N., Al-Mukhtar F., Ali E. Encrypt Audio File using Speech Audio File As a key. IOP Conference Series: Materials Science and Engineering. 2020. V. 928 032066. P. 79-84. DOI:10.1088/1757-899X/928/3/032066

133. Farsana F.J., Devi V.R., Gopakumar K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. Applied Computing and Informatics. 2020. V. 16. Issue. 2. DOI: 10.1016/j.aci.2019.10.001.

134. Cai C. et al. Simultaneous Audio Encryption and Compression Using Parallel Compressive Sensing and Modified Toeplitz Measurement Matrix. Electronics. 2021. V. 10 Issue 23. P. 2902. DOI: 10.3390/electronics10232902

135. Adhikari S., Karforma S. A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence. International Journal of Information Technology. 2021. V. 13. P. 1463–1471. DOI: 10.1007/s41870-021-00714-x

136. Al-laham Mohamad M. et al. A Method for Encrypting and Decryptingwave Files. International Journal of Network Security & Its Applications (IJNSA). 2018. V. 10. Issue. 4. P. 11-21.

137. Abdallah H.A., Meshoul S. A. Multilayered Audio Signal Encryption Approach for Secure Voice Communication. Electronics. 2023. V. 12. Issue. 1. P. 2. DOI: 10.3390/electronics12010002

138. Hameed Y.M., M. Ali Nada. An efficient audio encryption based on chaotic logistic map with 3D matrix. Journal of Theoretical and Applied Information Technology. 2018. V. 96. Issue. 16. P. 5142-5152.

139. Luis M., Daniel L., Isabel A. et al. A new multimedia cryptosystem using chaos, quaternion theory and modular arithmetic. Multimedia Tools and Applications. 2023. DOI: 10.1007/s11042-023-14475-1

140. Ge X., Sun G., Zheng B., Nan R. FPGA-Based Voice Encryption Equipment under the Analog Voice Communication Channel. Information. 2021. V. 12. Issue 11. P. 456. DOI: 10.3390/info12110456

141. Ерош, И. Л. О защите цифровых изображений при передаче по каналам связи / И. Л. Ерош, А. М. Сергеев, Г. П. Филатов // Информационно-управляющие системы. – 2007. – № 5(30). – С. 20-22..

142. Старовойтов В. В. Индекс ssim не является метрикой и плохо оценивает сходство изображений // Информатика. 2019. №. 2. С. 1–17

143. 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: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2024. – С. 187-192. – DOI 10.31799/978-5-8088-1899-6-2024-4-187-191

144. 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. – DOI 10.31854/1813-324X-2022-8-2-83-90.

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

146. 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.

147. 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.

148. Шаров, С. Н. Поиск бинарных кодовых последовательностей с низким уровнем боковых лепестков эволюционным способом / С. Н. Шаров, С. Г. Толмачев // Информационно-управляющие системы. – 2020. – № 1(104). – С. 44-53. – DOI: 10.31799/1684-8853-2020-1-44-53.

149. Устройство формирования модифицированных М-последовательностей: № 2023105091 от 06.03.2023 / Е. К. Григорьев, А. М. Сергеев, В. А. Ненашев, Д. В. Куртяник / Патент № 2801743 С1 Российская Федерация, МПК H03K 3/00.

150. Интеллектуальная система управления распределенными радиолокационными средствами для обнаружения БПЛА в условиях плотной городской застройки: отчет о НИР (заключительный) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Григорьев Е. К. [и др.]. СПб., 2023. 70 с. – № ГР АААА-А19-119101590059-7.

151. Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств: отчет о НИР (заключительный) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Рабин А. В.; исполн.: Григорьев Е. К. [и др.]. СПб., 2022. 530 с. – № ГР АААА-А20-120060290131-9.

152. Spread spectrum technology research and its application in power line communication systems / E. M. Dmitriyev, E. V. Rogozhnikov, A. K. Movchan [et al.] // T-Comm. – 2020. – Vol. 14, No. 10. – P. 45-52. – DOI 10.36724/2072-8735-2020-14-10-45-52.

153. Kim, D. Novel Algorithm for Blind Estimation of Scramblers in DSSS Systems / D. Kim, D. Yoon // IEEE Transactions on Information Forensics and Security. – 2023. – Vol. 18. – P. 2292-2302. – DOI 10.1109/tifs.2023.3265345.

154. Асинхронная передача данных с использованием многослойных ортогональных структур в системах с кодовым разделением каналов / Д. С. Кукунин, А. А. Березкин, Р. В. Киричек, К. А. Елисеева // Электросвязь. – 2023. – № 1. – С. 26-35. – DOI 10.34832/ELSV2023.38.1.003.

155. Стародубцев, В. Г. Предпочтительные пары ГМВ-последовательностей с периодом N=1023 для систем передачи цифровой информации / В. Г. Стародубцев, Е. Ю. Подолина, А. Х. Келоглян // Известия высших учебных заведений. Приборостроение. – 2022. – Т. 65, № 1. – С. 28-35. – DOI 10.17586/0021-3454-2022-65-1-28-35.

156. Варакин, Л.Е. Системы связи с шумоподобными сигналам / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

157. Кукунин, Д. С. Многослойные ортогональные структуры на основе последовательностей максимальной длины / Д. С. Кукунин, А. А. Березкин, Р. В. Киричек // Инфокоммуникационные технологии. – 2022. – Т. 20, № 2. – С. 42-50. – DOI 10.18469/ikt.2022.20.2.05.

158. Стародубцев, В. Г. Формирование множеств троичных касамиподобных последовательностей для систем передачи цифровой информации / В. Г. Стародубцев, Е. А. Четвериков // Известия высших учебных заведений. Приборостроение. – 2023. – Т. 66, № 10. – С. 807-817. – DOI 10.17586/0021-3454-2023-66-10-807-817.

159. Владимиров, С. С. Коды Голда и коды максимальной длины в сетевом кодировании / С. С. Владимиров // Электросвязь. – 2020. – № 1. – С. 61-66. – DOI 10.34832/ELSV.2020.2.1.009.

160. Манаенко, С. С. Теоретические аспекты формирования сигнальных конструкций сложной структуры / С. С. Манаенко, С. В. Дворников, А. В. Пшеничников // Информатика и автоматизация. – 2022. – Т. 21, № 1. – С. 68-94. – DOI 10.15622/ia.2022.21.3.

161. Chaotic Orthogonal Composite Sequence for 5G NR Time Service Signal Capture Algorithm / Zh. Mao, H. Wu, D. Zhao, X. Jiang // Electronics. – 2024. – Vol. 13, No. 13. – P. 2648. – DOI 10.3390/electronics13132648.

162. Оценка структурной скрытности ансамблей многофазных ортогональных кодовых последовательностей / А. П. Жук, А. В. Студеникин, И. В. Макаров, А. А. Беседин // Телекоммуникации. – 2024. – № 3. – С. 13-21. – DOI 10.31044/1684-2588-2024-0-3-13-21.

163. Юдачев, С. С. Ансамбли последовательностей GMW для систем с кодовым разделением каналов / С. С. Юдачев, В. В. Калмыков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2012. – № 1. – С.1- 18.

164. Кренгель, Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча / Е. И. Кренгель // Техника средств связи. Серия: Техника радиосвязи. – 1979. – № 3. – С. 31—34.

165. Стародубцев, В.Г. Алгоритм формирования последовательностей Гордона – Миллса – Велча / В. Г. Стародубцев // Известия высших учебных заведений. Приборостроение. – 2012. – Т. 55, – № 7. – С. 5-9.

166. Григорьев, Е. К. Анализ спектральных характеристик результатов матричного маскирования изображений / Е. К. Григорьев // Труды учебных заведений связи. – 2024. – Т. 10, № 2. – С. 76-82. – DOI 10.31854/1813-324X-2024-10-2-76-82.

167. Чекотило, Е. Ю. Спектральный анализ вероятностных характеристик изображений / Е. Ю. Чекотило, П. К. Кузнецов // Вестник Самарского государственного технического университета. Серия: Физико-математические науки. – 2006. – № 42. – С. 212-215.

168. Gonzalez R., Woods R. Digital Image Processing (4th Edition). Pearson. 2017. 1192 p.

169. The Lenna Story [Электронный ресурс]. Режим доступа: http://lenna.org

170. UrbanSound8K dataset [Электронный ресурс]. Режим доступа: https://urbansounddataset.weebly.com/urbansound8k.html

171. 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. – DOI 10.31854/1813-324X-2023-9-3-6-13.

172. 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.

173. 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.

174. Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга: отчет о НИР (промежуточный, 1 этап) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Рабин А. В.; исполн.: Григорьев Е. К. [и др.]. СПб., 2023. 445 с. – № ГР 123030100022-6.

Приложение А

Свидетельства о регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019612775

Программа вычисления структурированных квазиортогональных матриц Мерсенна

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***Востриков Антон Александрович (RU), Сергеев Александр Михайлович (RU), Куртяник Даниил Владимирович (RU), Ненашев Сергей Александрович (RU), Григорьев Евгений Константинович (RU)***

Заявка № **2019611351**
Дата поступления **14 февраля 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 февраля 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019612935

Программа генерации квазиортогональных циклических матриц, сформированных на основе вычисления квадратичных вычетов

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***Ненашев Вадим Александрович (RU), Шепета Александр Павлович (RU), Сергеев Михаил Борисович (RU), Чернышев Станислав Андреевич (RU), Григорьев Евгений Константинович (RU)***

Заявка № **2019611539**

Дата поступления **19 февраля 2019 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***04 марта 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019660821

Программа генерации специальных квазиортогональных циклических матриц, сформированных на основе вычисления символов Якоби

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***см. на обороте***

Заявка № **2019619765**
Дата поступления **05 августа 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 августа 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Авторы: ***Востриков Антон Александрович (RU), Сергеев Александр Михайлович (RU), Куртяник Даниил Владимирович (RU), Ненашев Вадим Александрович (RU), Григорьев Евгений Константинович (RU), Шепета Александр Павлович (RU), Скуратов Вадим Вячеславович (RU)***

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019660998

Программа вычисления специальных структурированных квазиортогональных матриц Мерсенна-Уолша

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***Ненашев Вадим Александрович (RU), Сергеев Михаил Борисович (RU), Чернышев Станислав Андреевич (RU), Востриков Антон Александрович (RU), Ненашев Сергей Александрович (RU), Григорьева Наталья Никифоровна (RU), Григорьев Евгений Константинович (RU)***

Заявка № **2019619831**

Дата поступления **05 августа 2019 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***16 августа 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019664813

Программа генерации специальных квазиортогональных матриц, сформированных на основе модифицированных m-последовательностей

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***см. на обороте***

Заявка № **2019663534**
Дата поступления **30 октября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 ноября 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Авторы: ***Ненашев Вадим Александрович (RU), Сергеев Михаил Борисович (RU), Сергеев Александр Михайлович (RU), Григорьев Евгений Константинович (RU), Иванова Мария Станиславовна (RU), Ненашев Сергей Александрович (RU)***

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019664814

Программа поиска специальных квазиортогональных матриц и генерации новых маркированных кодовых конструкций максимальной длины

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***см. на обороте***

Заявка № **2019663538**
Дата поступления **30 октября 2019 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***13 ноября 2019 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Авторы: ***Ненашев Вадим Александрович (RU), Сергеев Михаил Борисович (RU), Шепета Александр Павлович (RU), Григорьев Евгений Константинович (RU), Ненашев Сергей Александрович (RU), Скуратов Вадим Вячеславович (RU)***

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2021615538

Программа генерации и анализа корреляционных характеристик новых кодовых конструкций, основанных на персимметричных квазиортогональных циркулянтах

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***Сергеев Михаил Борисович (RU), Григорьев Евгений Константинович (RU), Ненашев Вадим Александрович (RU), Ненашев Сергей Александрович (RU)***

Заявка № **2021614858**

Дата поступления **09 апреля 2021 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***09 апреля 2021 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0x02A5CFBC00B1ACF59A40A2F08092E9A118
Владелец **Ивлиев Григорий Петрович**
Действителен с 15.01.2021 по 15.01.2035

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2021664610

Программа поиска и анализа новых маркированных многоуровневых кодовых конструкций на основе циркулянтов квазиортогональных матриц произвольной длины

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Авторы: ***Григорьев Евгений Константинович (RU), Ненашев Вадим Александрович (RU), Гордеев Иван Романович (RU), Рыжов Константин Юрьевич (RU)***

Заявка № **2021663951**

Дата поступления **09 сентября 2021 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***09 сентября 2021 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0x02A5CFBC00B1ACF59A40A2F08092E9A118
Владелец **Ивлиев Григорий Петрович**
Действителен с 15.01.2021 по 15.01.2035

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022683231

MATLAB-библиотека для генерации и анализа персимметричных квазиортогональных циркулянтов

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (RU)***

Автор(ы): ***Григорьев Евгений Константинович (RU)***

Заявка № **2022683278**
Дата поступления **02 декабря 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***02 декабря 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 68b80077e14e40f0a94edbd24145d5c7
Владелец **Зубов Юрий Сергеевич**
Действителен с 20.03.2022 по 26.05.2023

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023614623

Программа маскирования и демаскирования звуковой цифровой информации. Модуль маскирования

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения" (RU)***

Авторы: ***Григорьев Евгений Константинович (RU), Сергеев Михаил Борисович (RU), Сергеев Александр Михайлович (RU)***

Заявка № **2023613794**
Дата поступления **03 марта 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***03 марта 2023 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 68b80077e14e40f0a94edbd24145d5c7
Владелец **Зубов Юрий Сергеевич**
Действителен с 20.03.2022 по 26.05.2023

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023614622

Программа маскирования и демаскирования звуковой цифровой информации. Модуль демаскирования

Правообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения" (RU)***

Авторы: ***Григорьев Евгений Константинович (RU), Сергеев Михаил Борисович (RU), Сергеев Александр Михайлович (RU)***

Заявка № **2023613793**
Дата поступления **03 марта 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***03 марта 2023 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 68b80077e14e40f0a94edbd24145d5c7
Владелец **Зубов Юрий Сергеевич**
Действителен с 20.03.2022 по 26.05.2023

Ю.С. Зубов

Приложение Б

Патент на изобретение

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2801743

Устройство формирования модифицированных М-последовательностей

Патентообладатель: ***Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения" (RU)***

Авторы: ***Григорьев Евгений Константинович (RU), Сергеев Александр Михайлович (RU), Ненашев Вадим Александрович (RU), Куртяник Даниил Владимирович (RU)***

Заявка № **2023105091**
Приоритет изобретения **06 марта 2023 г.**
Дата государственной регистрации
в Государственном реестре изобретений
Российской Федерации **15 августа 2023 г.**
Срок действия исключительного права
на изобретение истекает **06 марта 2043 г.**

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 429b6a0fe3853164baf96f83b73b4aa7
Владелец **Зубов Юрий Сергеевич**
Действителен с 10.05.2023 по 02.08.2024

Ю.С. Зубов

Приложение В

«УТВЕРЖДАЮ»
Проректор ГУАП по научно-
технологическому развитию
д-р техн. наук, профессор
_____ Н. Н. Майоров
«04» 11 2024 г.

АКТ

внедрения научных результатов диссертационной работы
Григорьева Евгения Константиновича на тему «Поиск и применение циклических квазиортогональных матриц в задачах обработки информации», представляемой на соискание ученой степени кандидата технических наук по специальности 2.3.1 — Системный анализ, управление и обработка информации, статистика (технические науки)

Комиссия в составе

Татарниковой Татьяны Михайловны, доктора технических наук, профессора, директора института информационных технологий и программирования,
Шепеты Александра Павловича, доктора технических наук, профессора кафедры прикладной информатики,
Сергеева Александра Михайловича, кандидата технических наук, доцента кафедры вычислительных систем и сетей

составила настоящий акт о том, что научные результаты, полученные лично Григорьевым Евгением Константиновичем, а именно:

1) метод и алгоритмы вычисления новых циклических квазиортогональных матриц;
2) стратегии вычисления квазиортогональных циркулянтов как основы для формирования новых кодовых последовательностей и новые кодовые последовательности для кодирования сигналов в радиоканале;
3) методы матричного маскирования/демаскирования цифровой звуковой информации, единый подход к анализу качества маскирования цифровой аудиовизуальной информации в части разрушения структуры исходного сообщения,

использованы в

НИР «Поиск и исследование экстремальных квазиортогональных матриц для задач обработки информации» (гос. рег. № АААА-А17-117042710042-9), выполняемой при поддержке Минобрнауки РФ в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/4.6,

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,

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),

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).

Директор института информационных технологий и программирования, доктор технических наук, профессор — Т. М. Татарникова

Профессор кафедры прикладной информатики, доктор технических наук, профессор — А. П. Шепета

Доцент кафедры вычислительных систем и сетей, кандидат технических наук — А. М. Сергеев

«УТВЕРЖДАЮ»
Проректор ГУАП по научно-технологическому развитию
д-р техн. наук, профессор
_____ Н. Н. Майоров
«15» 10 2024 г.

АКТ

внедрения научных результатов диссертационной работы Григорьева Евгения Константиновича на тему «Поиск и применение циклических квазиортогональных матриц в задачах обработки информации», представляемой на соискание ученой степени кандидата технических наук по специальности 2.3.1 — Системный анализ, управление и обработка информации, статистика (технические науки)

Комиссия в составе:

доктор технических наук, профессор, профессор кафедры вычислительных систем и сетей Гордеев Александр Владимирович,

доктор технических наук, доцент, профессор кафедры вычислительных систем и сетей Балонин Николай Алексеевич,

доктор технических наук, профессор, заведующий кафедрой инфокоммуникационных технологий и систем связи Тюрликов Андрей Михайлович

составила настоящий акт о том, что результаты диссертационной работы Григорьева Е. К., выполненной на кафедре вычислительных систем и сетей федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», внедрены в учебный процесс:

1) на кафедре вычислительных систем и сетей в дисциплинах, включенных в программы подготовки по направлению «Информатика и вычислительная техника» (бакалавриат – 09.03.01 и магистратура – 09.04.01):
   – «Цифровая обработка изображений» (Лабораторная работа «Матричные способы обработки изображений»);

– «Ортогональные преобразования» (Лекционный материал),

2) на кафедре инфокоммуникационных технологий и систем связи в лекционном курсе дисциплины «Методы и средства обработки изображений», включенной в программу подготовки по направлению 11.03.02 – «Инфокоммуникационные технологии и системы связи».

Члены комиссии А. В. Гордеев

Н. А. Балонин

А. М. Тюрликов