Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

На правах рукописи

Сергеев Александр Михайлович

МЕТОДЫ ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЙ И КОДИРОВАНИЯ СИГНАЛОВ В КАНАЛАХ РАСПРЕДЕЛЕННЫХ СИСТЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, доцент
Балонин Николай Алексеевич

Санкт-Петербург – 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Диссертация посвящена решению части крупной научной проблемы развития и совершенствования теории преобразования изображений и сигналов, в том числе в прикладных задачах распределенных видеосистем. Акцент делается на улучшении характеристик процессов дискретных преобразований данных и повышения защищенности и надежности обмена информацией в условиях внешних помех за счет разработки, исследования и применения специальных ортогональных матриц, являющихся альтернативными используемым известным.

Актуальность темы. Цифровая визуальная информация сегодня является самым распространенным видом данных, используемых как в производственной деятельности, так и повседневной жизни человека. Постоянное увеличение пропускной способности каналов и скорости обработки информации в распределенных IP-системах аппаратно-программными средствами встраиваемого класса компенсируется, во-первых, постоянным ростом объема как открытой, так и конфиденциальной визуальной цифровой информации, передаваемой в реальном времени, во-вторых, возрастающими требованиями к разрешению такой информации. Это приводит к необходимости совершенствования, а часто, пересмотра основ построения методов и средств преобразования такой информации в объектах распределенных систем на основе гетерогенных сетей, в том числе на основе радиоканала.

Основные преобразования изображений сводятся к сжатию, защите в канале от несанкционированного ознакомления, от помех естественного и искусственного происхождения, в основе которых лежат ортогональные матричные преобразования.

В связи с этим интерес исследователей к дискретным ортогональным преобразованиям информации сегодня связан с тем, что:

– расширение набора базовых ортогональных матриц позволяет выбрать наиболее рациональную для решения конкретной задачи;

– появились задачи цифровой обработки, решаемые наиболее эффективно с использованием новых дискретных базисов таких матриц;

– достигнуты большие успехи в области процессоров цифрой обработки сигналов и программируемой логики с возможностью структурной реализации алгоритмов любой сложности.

При этом главным аспектом актуальности является улучшение базовых характеристик процессов в телекоммуникационных системах на основе ортогональных преобразований.

Степень разработанности темы. Значительное место при разработке алгоритмов сжатия, преобразования изображений и кодирования сигналов занимают ортогональные преобразования с использованием матриц Хаара, функций Уолша, дискретного преобразования Фурье, преобразования Адамара-Уолша и др. Большое число работ таких ученых как Адамар (J. Hadamard), Сильвестр (J. Sylvester), Пэли (R. Paley), Скарпи (U. Scarpis), Вильямсон (J. Wiliamson), Райзер (H. Ryser) связано с развитием теории ортогональных матриц, вопросов их вычисления и анализа свойств.

Вопросам исследования и развития процессов преобразования информации с использованием ортогональных матриц посвящено большое число научных монографий, статей и других публикаций. В частности, в области применения ортогональных матриц для рассматриваемых в диссертации задач широко известны работы N. Ahmed, K. Rao, R.Wang, K. J. Horadam, Ch. Koukouvinos, D. Prabhakar, В. А. Сойфера, Л. А. Мироновского, В. А. Слаева, А. А. Шелупанова, А. Ю. Тропченко и др.

Однако тематика малоуровневых квазиортогональных матриц, обобщающих ортогональные матрицы, получила свое развитие с появлением, начиная с 2011 года, работ отечественных ученых Н. А. Балонина, Л. А. Мироновского и М. Б. Сергеева. Позже к этим исследованиям присоединились такие зарубежные ученые как Дж. Себерри (J. Seberry), Д. Джокович (D. Djoković), Н. Блаунштейн (N. Blaunstein), Офер Хадар (Ofer Hadar) и др.

Примеры использования квазиортогональных матриц и оценки перспектив их использования приведены в работах Н. А. Балонина, М. Б. Сергеева, А. А. Вострикова, Ю. Н. Балонина, С. А. Чернышева. Однако в этих работах внимание акцентируется на применимости отдельных квазиортогональных матриц, в частности, матриц Мерсенна и Мерсенна-Уолша, и не затрагиваются более общие вопросы, способные стимулировать

исследования в области разработки новых алгоритмов и процедур преобразований в рассматриваемых в диссертации задачах.

Именно вопрос оценки применимости широкого класса квазиортогональных матриц, с учетом их особенностей, в алгоритмах сжатия, маскирования, кодирования и др. требует отдельных исследований.

Целью диссертации является повышение защищенности передачи цифровой визуальной информации в телекоммуникационных каналах за счет разработки новых методов с использованием расширенного семейства специальных ортогональных матриц и учета их свойств.

Для достижения указанной цели в работе решаются следующие **задачи.**

1. Анализ алгоритмов преобразований изображений и сигналов в распределенных системах, в основе которых лежит использование ортогональных матриц.
2. Развитие теории малоуровневых ортогональных матриц на порядках, равных числам известных последовательностей, их классификация и разработка новых конструкций малоуровневых квазиортогональных матриц.
3. Разработка метода покадрового маскирующего матричного преобразования визуальных данных для защиты от несанкционированного ознакомления при хранении изображений и их передаче в открытых коммуникациях.
4. Разработка кодовых последовательностей и конструкций для фазовой (амплитудной) модуляции аналоговых сигналов в радиоканале сетевых систем передачи данных, для обеспечения повышения помехоустойчивости.

Объектом исследования являются распределенные телекоммуникационные системы, реализующие обработку данных и обмен ими по открытым коммуникационным каналам.

Предметом исследования являются процессы преобразования изображений и кодирования сигналов в телекоммуникационных системах.

Методология и методы исследования. При решении поставленных в работе задач использованы методы теории чисел, линейной алгебры, теории информации, цифровой обработки изображений, модуляции и кодирования сигналов.

Положения, выносимые на защиту.

1. Расширение класса ортогональных матриц специальными квазиортогональными матрицами, позволяющими расширить область применимости ортогональных преобразований и совершенствовать известные процедуры преобразования данных и кодирования сигналов.
2. Метод симметричного двустороннего матричного маскирования/демаскирования цифровых визуальных данных с использованием специальных квазиортогональных матриц, обеспечивающий математически упрощенную реализацию разрушения кадров – защиту визуальных данных от несанкционированного ознакомления.
3. Новые двухуровневые несимметричные $\{1, -b\}$ кодовые последовательности длин 3 и 7 для фазовой (амплитудной) модуляции сложных сигналов в радиоканале, обладающие лучшими автокорреляционными характеристиками, чем у кодов Баркера.
4. Вложенные кодовые последовательности, построенные на комбинации пар кодовых последовательностей Баркера и Мерсенна длин 3, 7 и 11, обеспечивающие повышение помехозащищенности сигналов в радиоканале.

Научная новизна работы определяется тем, что в ней:

– предлагается новый класс математических объектов – специальные квазиортогональные матрицы, расширяющие возможность применения процедур ортогональных преобразований при решении широкого класса задач связи, защиты и радиолокации;

– впервые классифицированы экстремальные малоуровневые квазиортогональные матрицы и выявлена связь структур таких матриц, построенных на порядках последовательностей $4t$ и $4t-1$, обеспечивающая гарантированное вычисление нового вида матриц Адамара; расширено существующее семейство ортогональных матриц, используемых для обработки цифровых данных, за счет введения новых бициклических симметричных матриц структур Мерсенна-Уолша двухуровневых и модульнодвухуровневых;

– предложена модификация метода раздельного покадрового маскирования и демаскирования цифровых визуальных данных с использованием

двустороннего умножения матрицы изображения на специальные структурированные квазиортогональные матрицы;

– предложен новый подход к формированию несимметричных кодовых последовательностей для фазовой (амплитудной) модуляции сигналов в радиоканале, обладающие лучшими автокорреляционными функциями, чем существующие; предложены сложные конструкции вложенных кодов с улучшенными характеристиками по сжатию сигнала на основе комбинирования кодов Мерсенна и Баркера.

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

– предложены варианты представления квазиортогональных матриц Мерсенна в виде структур Уолша для реализации задач фильтрации изображений;

– предложена классификация малоуровневых квазиортогональных матриц, позволившая найти метод вычисления матриц симметричных конструкций, в том числе двуциклических;

– значительно расширен выбор квазиортогональных матриц для методов преобразования данных, в том числе матричного маскирования, сжатия изображений;

– для матриц Мерсенна, Мерсенна-Уолша, Эйлера, Ферма получены особые изображения, инвариантные к их двустороннему матричному преобразованию в методе покадрового маскирования;

– метод матричного маскирования цифрового видеоизображения реализуются программно и аппартно-программно в реальном масштабе времени в системах встраиваемого класса на основе DSP и FPGA;

– предложенные модификации базового метода позволяют обеспечить маскирование цифровой информации в широком классе распределенных IP-видеосистем на основе Wi-Fi, Ethernet и др.;

– разработанные программные реализации алгоритмов маскирования/демаскирования на основе предложенного метода при различном представлении исходных изображений позволяют расширить сферу его применения, обеспечивая устойчивость маскированных изображений к искажениям в коммуникационном канале.

Степень достоверности результатов работы обеспечивается корректностью постановки научно-технической задачи исследования, строго обоснованной совокупностью ограничений и допущений, обширным библиографическим материалом, строгостью применения математического аппарата, непротиворечивостью полученных теоретических и практических результатов, апробацией полученных результатов, а также внедрением в практику разработанных алгоритмов, на программные реализации которых получены свидетельства о государственной регистрации программ для ЭВМ.

Апробация результатов. Основные научные положения и результаты диссертационной работы докладывались, обсуждались и получили одобрение на научных семинарах кафедры «Вычислительные системы и сети» ГУАП в 2007 – 2017 гг., на XI International Symposium on Problems of Redundancy in Information and Control Systems (Saint-Petersburg, 2007), научно-техническом семинаре НИИ информационно-управляющих систем ИТМО (Санкт-Петербург, октябрь 2015), 69-й научной сессии ГУАП (Санкт-Петербург, апрель 2016), на Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России», Санкт-Петербургской международной конференции «Региональная информатика» (Санкт-Петербург, 26-28 октября 2016), на 70-й научной сессии ГУАП (Санкт-Петербург, апрель 2017), на II международном семинаре «Специальные матрицы: вычисление, структуры, применение» (Санкт-Петербург, 20 – 22 июня 2018), на 71-й научной сессии ГУАП (Санкт-Петербург, апрель 2018), на 22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (Белград, 2 – 6 сентября 2018), на 72-й научной сессии ГУАП (Санкт-Петербург, апрель 2019), на 11th KES International Conference on Intelligent Decision Technologies (KES-IDT 2019) (Мальта, 17 – 19 июня 2019).

Внедрение результатов диссертационной работы. Результаты внедрены в учебный процесс федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» при подготовке по направлению «Информатика и вычислительная техника» в дисциплинах «Проектирование систем обработки и передачи информации» и «Цифровая обработка изображений» и при подготовке по направлению

«Инфокоммуникационные технологии и системы связи» в дисциплине «Технологии стеганографии в системах инфокоммуникаций».

Метод матричного покадрового маскирования видеопоследовательности с использованием специальных матриц внедрен в виде программной реализации для системы-на-кристалле с DSP-сопроцессорами (ADSP-BF523KBCZ и др.), используемой в видеорегистраторах мобильного назначения, разработанных ООО «АСК Лаборатория» (г. Санкт-Петербург). На специальное программное обеспечение для маскирования с использованием квазиортогональных матриц, помехоустойчивого кодирования, сжатия и беспроводной передачи видеоизображений с малым временем актуальности получено свидетельство о государственной регистрации программы для ЭВМ № 2017616930. На специальное программное обеспечение для приема по беспроводному каналу, декодирования, демаскирования с использованием квазиортогональных матриц, декомпрессии и воспроизведения видеоизображений с малым временем актуальности получено свидетельство о государственной регистрации программ для ЭВМ № 2017616795.

Помехоустойчивые коды Мерсенна на основе моноциклических матриц используются в АО «Концерн «Гранит-Электрон» (г. Санкт-Петербург) при разработке перспективных радиолокационных станций.

Результаты диссертационной работы использованы в:

НИР «Оптико-электронный модуль мобильного применения» гос. рег. № 117032810028-3, 2018 г., а именно: метод маскирования изображений с использованием найденных новых специальных матриц блочно-симметричных конструкций;

НИР «Поиск и исследование экстремальных квазиортогональных матриц для обработки информации» гос. рег. № АААА-А17-117042710042-9, а именно: структуры новых специальных малоуровневых квазиортогональных матриц, цепочки квазиортогональных матриц, численные методы и алгоритмы вычисления двуциклических симметричных матриц Адамара, новые кодовые последовательности длин 3, 7 и 11 для кодирования сигналов в радиоканале.

Личный вклад автора диссертационной работы заключается в:

– классификации малоуровневых квазиортогональных матриц, позволившей установить взаимосвязи симметричных ортогональных матриц порядков последовательностей $4k$ и $4k$-1;

– разработке метода поиска квазиортогональных матриц бициклических структур;

– разработке модификации метода двустороннего матричного покадрового маскирования/демаскирования цифровой визуальной информации с функцией помехозащищенного кодирования;

– вычислении впервые особых изображений маскирующих матриц Эйлера, Ферма, Мерсенна-Уолша;

– расширении гипотезы Райзера на предельно достижимые порядки симметричных матриц бициклических структур;

– разработке программного обеспечения для преобразования цифровых изображений с использованием уникальных квазиортогональных матриц, обеспечивающего покадровое маскирование фото и видеокадров в устройствах встраиваемого класса для последующей передачи по сетям общего пользования и демаскирования принятого кадра с использованием ПК;

– разработке новых помехоустойчивых кодов длин 5, 7 и 11 для фазовой (амплитудной) модуляции сигналов;

– предложении формирования вложенных кодов на основе комбинаций кодов Мерсенна и Баркера.

Публикации. Материалы, отражающие основное содержание и результаты диссертационной работы, опубликованы в 26 печатных работах. Из них 1 монография, 11 работ опубликованы в рецензируемых научных журналах, внесенных в перечень ВАК, 4 работы опубликованы в изданиях, индексируемых SCOPUS и Web of Science. Получены 7 свидетельств о государственной регистрации программ для ЭВМ.

Объем и структура работы. Диссертация состоит из введения, четырёх разделов, заключения. Полный объём диссертации составляет 153 страницы, включая 65 рисунков, 7 таблиц и 2 приложения, включающие описание спроектированной с участием автора среды моделирования и акты внедрения. Список литературы содержит 150 наименований.

1 Ортогональные матрицы и преобразование информации

1.1 Основные определения

Определение 1. Матрица – это совокупность элементов, собранных в табличной форме. Номера строк и столбцов такой таблицы называются индексами элементов матрицы [1, 2]. Индексы пишутся, начиная с номера строки

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

Матрица размера $n \times m$ называется прямоугольной, квадратной она называется при равенстве числа ее строк и столбцов $n = m$.

Размер n квадратной матрицы называется порядком.

Квадратная матрица вида $\mathbf{I} = \mathrm{diag}(1, 1, \ldots, 1)$ с единичными элементами вдоль главной диагонали (остальные нули), называется единичной матрицей.

Определение 2. Обратной к матрице **A** называется матрица $\mathbf{A}^{-1}$, для которой выполняется $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$.

Если результатом преобразования, заключающемся в умножении матрицы **P** порядка n на ортогональную матрицу **A** того же порядка является матрица $\mathbf{P}^*$, то умножение $\mathbf{P}^*$ на обратную матрицу $\mathbf{A}^{-1}$ приводит к получению (восстановлению) матрицы **P** с точностью до погрешностей вычисления. Основное условие – матрица **A** не является плохо обусловленной [1,2].

Определение 3. Операция замены всех строк матрицы **A** ее столбцами называется транспонированием, результат ее действия обозначается как $\mathbf{A}^{\mathrm{T}}$.

Операция транспонирования квадратных матриц сводится к попарной перестановке элементов, расположенных симметрично относительно основной диагонали.

Можно ввести обобщенное транспонирование относительно любой из двух диагоналей, и даже относительно вертикальной или горизонтальной осевых линий.

Это замечание является существенным для понимания, что природа рассматриваемой в работе симметрии может быть разной.

Определение 4. Матрица **A** является ортогональной, если для нее выполняется $\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}^{T}\mathbf{A} = \mathbf{I}$ [1].

Если большинство элементов ортогональной матрицы равны между собой, ее вид можно упростить масштабированием – делением на самый распространенный у матрицы элемент.

Масштабированные матрицы не теряют попарной ортогональности своих строк и столбцов, поскольку масштабирование не меняет диагонального вида правой части.

Очевидно, ортогональность позволяет заменить матрицу $\mathbf{A}^{-1}$ на $\mathbf{A}^{T}$ при восстановлении **P** из матрицы $\mathbf{P}^{*}$. Такая замена гарантирует более высокую точность вычислений, при которых отсутствует накапливающаяся погрешность от неточного вычисления $\mathbf{A}^{-1}$.

Эта особенность ортогональных матриц гарантирует простое обратное преобразование, делая в целом преобразования с ортогональными матрицами симметричными.

Среди ортогональных матриц простотой элементов отличаются матрицы Адамара.

Определение 5. Матрица Адамара **H** размера $n \times n$, это квадратная матрица с элементами 1, –1, удовлетворяющая уравнению $\mathbf{H}^{T}\mathbf{H} = n\mathbf{I}$ [3].

Все столбцы (строки) такой матрицы попарно ортогональны между собой – их скалярное произведение равно 0, а квадрат нормы равен n.

Для большей строгости рассуждений и выводов такие матрицы будем называть *квазиортогональными*, имея ввиду, что они не ортогональны в

строгом смысле этого слова, но близки к ортогональным с точностью до коэффициента масштабирования.

Считается, что впервые такие матрицы были определены Сильвестром в 1867 [4], хотя они были известны и другим его современникам.

Матрицы Адамара существуют на порядках 1, 2 и $n = 4k$, где k – натуральное число.

Определение 6. Значения элементов ортогональных (квазиортогональных) матриц будем называть уровнями [5].

Привлекательность матриц Адамара состоит в том, что они имеют всего два целочисленных уровня 1 и -1 и алгоритмы вычисления с ними, поэтому, очень просто реализуемы.

Матрицы Адамара принято изображать не только в математическом представлении как матрицы, но и графически – в виде «портретов» матриц [6, 7] для удобства оценки особенностей их структуры, наличия симметрий, цикличностей и др. Впервые представление матрицы в виде портрета использовали Голомб (Golomb), Баумерт (Baumert) и Холл (Hall).

Определение 7. Портретом двухуровневой матрицы будем называть графическое изображение в виде совокупности квадратов, где квадрат черного цвета соответствует элементу со знаком минус, квадрат белого цвета – положительному элементу [6, 7].

Портреты классических матриц Адамара порядков 12 и 20, найденных самим Адамаром, приведены на рис. 1.1.

Среди возможных структур матриц Адамара, ввиду их особенностей, выделяются: циклические, негациклические, симметричные, блочно-симметричные, двуциклические, трехциклические, ядро с окаймлением и др. В отдельных матрицах возможно совмещение нескольких структурных особенностей.

На рис. 1.2 приведены портреты матриц Адамара порядка 4 и 8. Циклическая матрица порядка 4 является двояко симметричной.

Двуциклическая (бициклическая) матрица порядка 8 является одновременно симметричной и блочно-симметричной.

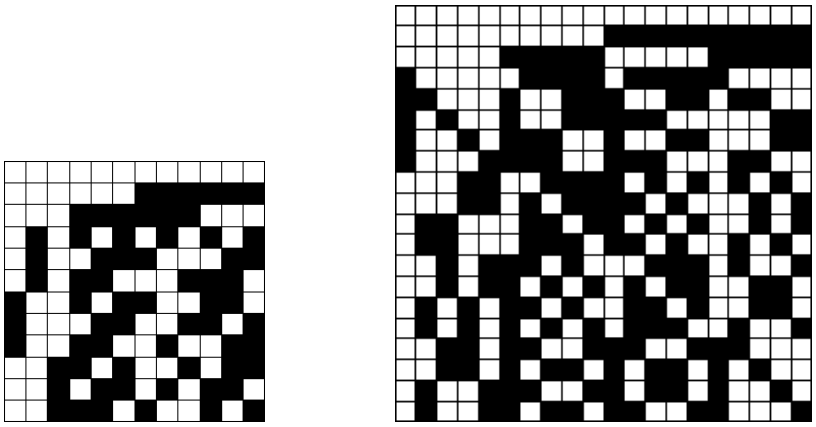


Рисунок 1.1 – Портреты матриц Адамара порядков 12 и 20

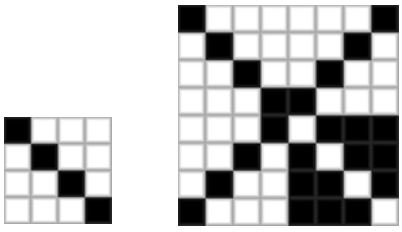


Рисунок 1.2 – Портреты матриц $\mathbf{H}_4$ и $\mathbf{H}_8$

Наиболее ранним источником вариаций матриц Адамара является кронекерово произведение пары матриц.

Определение 8. Кронекеровым произведением [8, 9] двух матриц **A** и **B** называется операция (×) вида

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

Поскольку ортогональность – инвариант кронекерова произведения, то результатом умножения двух матриц Адамара порядков n и m является

матрица Адамара порядка *nm*. Это свойство и квазиортогональных (отмасштабированных ортогональных) матриц.

В последнее время большой интерес представляют вариации матриц Адамара, связанные с их блочными структурами.

Определение 9. Блочными матрицами будем называть матрицы вида

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix},$$

состоящие из блоков (матриц) одинакового порядка *n*.

Транспонирование блочных матриц сводится к транспонированию всех ее блоков с попарной перестановкой блоков, расположенных симметрично относительно основной диагонали.

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} \mathbf{A}^{\mathrm{T}} & \mathbf{C}^{\mathrm{T}} \\ \mathbf{B}^{\mathrm{T}} & \mathbf{D}^{\mathrm{T}} \end{pmatrix}.$$

1.2 Ортогональные преобразования в обработке информации

Многие прикладные задачи распределенных систем сбора, хранения и передачи информации включают в себя процессы ее сжатия, преобразования форматов, сохранения конфиденциальности, защиты от искажений и выделения передаваемой информации на фоне помех в канале [9 – 16]. Цифровая визуальная информация является наиболее трудоемкой в обработке в таких распределенных системах на основе IP-сетей, реализуемых на комбинированной основе – проводных и беспроводных.

В диссертационной работе будут рассмотрены основные задачи, связанные с хранением и передачей по коммуникационным каналам.

Два понятия – «хранение» и «коммуникация» – тесно связаны друг с другом [9]. Если функция хранения – передача информации во времени, то функция коммуникации – передача ее в пространстве.

Обе указанные функции в идеальных условиях, имея пассивный характер, не предполагают активного преобразования информации. Однако задачи, возникающие при разработке и эксплуатации реальных распределенных систем хранения и передачи информации (каналов связи), во многом схожи и ориентированы на обеспечение перечисленных выше задач, а именно:

– сжатия,

– защиты ее от искажений и несанкционированного ознакомления,

– выделения полезной информации на фоне естественных и искусственных шумов в беспроводных коммуникациях.

Сжатие. Для большинства распределенных систем, таких как многофункциональные системы регистрации (МСР™), охранные распределенные системы, системы мониторинга объектов, территорий и другие основным видом информации является изображение (последовательность изображений). В них используют в качестве основных форматы покадрового сжатия видеоинформации и изображений JPEG, MJPEG, JPEG2000 [10].

В отличие от алгоритмов, построенных на межкадровой разнице, такие алгоритмы обеспечивают полное покадровое хранение и передачу изображений, что в большинстве применения таких систем является определяющим.

Покадровое сжатие в алгоритме JPEG реализуется в виде укрупненной схемы, приведенной на рис. 1.3.

В качестве одного из основных в цепочке преобразований исходных изображений (кадров) в них используется дискретное косинусное преобразование (ДКП) с квадратной ортогональной матрицей [10].

Рисунок 1.3 – Структурная схема последовательности выполнения алгоритма сжатия JPEG

Используемое ДКП является преобразованием массива пикселей изображения в массив значений пространственной частоты. Изображение **P**, представленное матрицей пикселов размера $n \times m$, преобразовывается по фрагментам размера 8×8 умножением на уникальную матрицу **D** размера 8×8 вида

$$\mathbf{D} = \begin{bmatrix} 0.353553 & 0.353553 & 0.353553 & 0.353553 & 0.353553 & 0.353553 & 0.353553 & 0.353553 \\ 0.490393 & 0.415818 & 0.277992 & 0.097887 & -0.097106 & -0.277329 & -0.415375 & -0.490246 \\ 0.461978 & 0.191618 & -0.190882 & -0.461673 & -0.462282 & -0.192353 & 0.190145 & 0.461366 \\ 0.414818 & -0.097106 & -0.490246 & -0.278653 & 0.276667 & 0.490710 & 0.099448 & -0.414486 \\ 0.353694 & -0.353131 & -0.354256 & 0.352567 & 0.354819 & -0.352001 & -0.355378 & 0.351435 \\ 0.277992 & -0.490246 & 0.096324 & 0.416700 & -0.414486 & -0.100228 & 0.491013 & -0.274673 \\ 0.191618 & -0.462282 & 0.461366 & -0.189409 & -0.193822 & 0.463187 & -0.460440 & 0.187195 \\ 0.097887 & -0.278653 & 0.416700 & -0.490862 & 0.489771 & -0.413593 & 0.274008 & -0.092414 \end{bmatrix}$$

Элементы матрицы **D** вычислены приближенно – с округлением до 10^{-6}. Это преобразование является симметричным – обратным с точностью до ошибок округления. Оно позволяет переходить от пространственного представления изображения к его спектральному представлению умножением на матрицу **D**, а умножением результата на $\mathbf{D}^{\mathrm{T}}$ – обратно к пространственному.

Иными словами ортогональность матрицы **D** гарантирует простое обратное преобразование – разжатие изображений (кадров).

Время появления перечисленных алгоритмов сжатия совпало с господством стандартов PAL, SECAM и NTSC и способствовало их длительному широкому использованию.

Бурное развитие в последние 15 – 20 лет технологий производства цифровых видеоматриц, видеоконтрольных устройств отображения привело к значительному увеличению размеров кадров – 8К, 16К, 32К и более. Появившаяся технология выделенного окна качества изображений (кадров) произвольного размера (Quality box) для экономии трафика в распределенных видеосистемах, допускает его произвольно малые размеры, в том числе меньшие 0,5К.

Обозначенное противоречие между значительно возросшими размерами матриц изображений и оставшимися неизменными алгоритмами сжатия стимулируют работы, в том числе, в части поиска новых ортогональных матриц различных размеров как альтернативы матрице ДКП и другим в алгоритмах сжатия.

Помехоустойчивое кодирование. На принципе симметричности преобразований с использованием ортогональных матриц основаны и другие преобразования изображений (кадров), в частности, их помехоустойчивое кодирование и защита от несанкционированного ознакомления при их передаче в коммуникационных каналах.

Одним из способов помехоустойчивого кодирования является стрип-преобразование изображений [9], которое изначально разрабатывалось для кодирования сигналов и изображений, передаваемых в каналах с импульсными помехами.

Его основа – «разрезание» изображения **P** на передающей стороне распределенной системы на фрагменты **X** равной длины – полоски (strip), двустороннее умножение на ортогональную матрицу не высокого порядка, формирование их линейных комбинаций и обратного ортогонального преобразования с последующим «склеиванием» на приемной стороне.

Известны две лучшие модификации стрип-преобразования: с двусторонним матричным кронекеровым умножением [9] и простым двусторонним матричным умножением [17, 18] с использованием ортогональных матриц. Рис. 1.4 демонстрирует последовательность преобразований.

В обеих модификациях двустороннее матричное преобразование с кронекеровым (×) умножением **X** на ортогональную матрицу слева и справа «полоски» изображения (полученные оператором S), обеспечивает лучшее перемешивание фрагментов изображения и, в конечном итоге, ослабление амплитуды импульсной помехи, накладываемой в канале на конкретное место на преобразованном изображении.

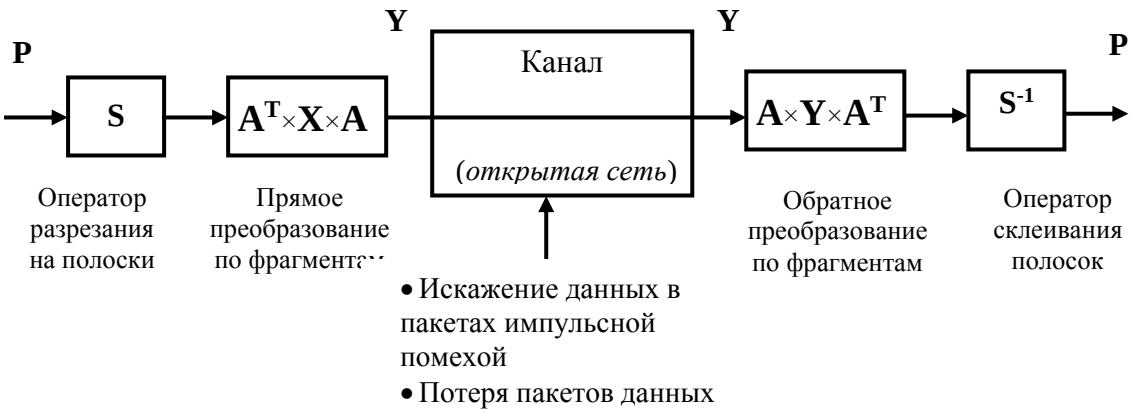


Рисунок 1.4 – Схема двустороннего стрип-преобразования

Преобразование фрагментов изображения осуществляется согласно формуле

$$\mathbf{Y} = \mathbf{A}^{\mathbf{T}} \times \mathbf{X} \times \mathbf{A} \qquad (1.1)$$

Восстановление на приемной стороне сформированного из фрагментов **Y** изображения, переданного по коммуникационной сети, производится через обратное двустороннее преобразование в виде

$$\mathbf{X} = (\mathbf{A}^{\mathbf{T}})^{-1} \times \mathbf{Y} \times \mathbf{A}^{-1} \qquad (1.2)$$

Результирующее изображение **P** является итогом дефрагментации из фрагментов вида **X** принятого изображения.

Двухстороннее (двумерное) стрип-преобразование изображений демонстрируется приведенным на рис. 1.5 примером, взятым из [9]. Здесь а – исходное изображение, б – стрип-преобразованное изображение, в – восстановленное изображение после передачи в канале с импульсной помехой с использованием стрип-преобразования, д – восстановленное изображение после передачи в канале с помехой без использования стрип-преобразования.

Приведенный пример стрип-преобразования реализован с использованием матрицы Адамара размера 4×4, а однократная помеха соответствует прямоугольнику пикселей размером 30×30.

Ослабление влияния импульсной помехи реализуется тем, что при обратных преобразованиях, выполняемых на приемной стороне с транспонированной ортогональной матрицей, помеха равномерно распределяется по всему восстановленному изображению.

Для максимального ослабления амплитуды помехи в стрип-преобразовании используются, как правило, экстремальные ортогональные матрицы Адамара [9, 17] порядков 4 и 8.

Матрицы Адамара существуют на порядках $4t$, где t – натуральное число. На каждом порядке таких матриц более двух. Однако существующие алгоритмы вычисления матриц Адамара обеспечивают наследие только структур матриц, соответствующих данным методам. Нет их структурного и количественного разнообразия на порядках существования.

Маскирование. Широкое распространение социальных сетей, IP-видеосистем различного назначения, сетевого телевидения обеспечивает постоянный прирост доли видеоинформации в объеме сетевого трафика ведущих стран мира [19].

Рисунок 1.5 – Изображение на этапах цикла двухстороннего стрип-преобразования (взято из книги [9])

По прогнозу компании Cisco, начиная с 2008 года ежегодное удвоение трафика передаваемого «видео на заказ» («IP TV»), сохранится и в ближайшие годы [20]. При этом «…предполагается, что поток видеоданных составит более 90% пользовательского телекоммуникационного трафика…», включая видеоконференции, мобильную телефонию и распределенные системы видеонаблюдения и управления с видеоканалом в обратной связи, для которых время актуальности передаваемого видео мало [14, 15, 21]. Поскольку для передачи видеопотоков в основном используются структура

Интернет – открытые телекоммуникационные каналы, то указанная тенденция делает актуальной задачу сохранения видеоданных от несанкционированного использования при передаче по ним.

Сегодня известны различные методы защиты цифровых видеоданных в Интернет от несанкционированного использования: специальные каналы, специальные протоколы, криптографические методы, а также методы, использующие только криптографические примитивы [22, 23]. Однако, одни из них не могут быть использованы в ряде применений, применение других невозможно в системах real-time из-за требуемых для их реализации больших вычислительных затрат, которые не могут быть выполнены на процессорах IP-видеокамер.

Видеоинформация, передаваемая и хранящаяся в распределенных видеосистемах, часто не является секретной, но требует защиты от тиражирования, подмены, преднамеренного искажения и несанкционированного ознакомления и использования. Это, в частности, характерно при использовании открытых коммуникаций для специализированных приложений МСР, передающих документированную видеоинформацию с мест стихийных и техногенных катастроф, систем документирования событий на массовых мероприятиях и др.

Как показали исследования [23], использование криптографических методов для обеспечения конфиденциальности является в ряде случаев избыточным, в других – невыполнимым даже в темпе 24 – 30 кадров/с из-за большой вычислительной сложности.

Перспективный подход заключается в использовании методов матричного маскирования цифровых кадров видеопоследовательности на передающей стороне и их восстановление (демаскирование) – на приемной, с использованием малоуровневых иррациональных матриц [14]. При этом выполняемые матричные операции могут быть значительно ускорены аппаратными решениями на PLM, а иррациональность элементов применяемых матриц создает препятствия для

попыток стороннего демаскирования из-за невозможности применения переборных процедур для поиска таких матриц. Теоретический задел для реализации такого подхода в задаче защиты real-time видеопотоков заложен в работах [24 – 29]. К матричным методам маскирования можно отнести методы, изложенные в работах [9, 14, 30] и др.

Рассмотренное выше стрип-преобразование [9], в котором реализуется «перемешивание» фрагментов изображений, может также рассматриваться и как способ их защиты от несанкционированного ознакомления в канале распределенной системы, схема реализации которой приведена на рис. 1.6.

Первый этап преобразования состоит в «…разбиении исходного изображения **P** на одинаковые по размеру квадратные» [9] фрагменты **X** размера $n \times n$. Разрезания на полоски как в классическом стрип-методе не производится. Неполные фрагменты дополняются нулями до полных. На втором этапе «…исходное изображение **P**, разбитое на фрагменты, рассматривается как блочная матрица» [9], состоящая из квадратных матриц **X** порядка n.

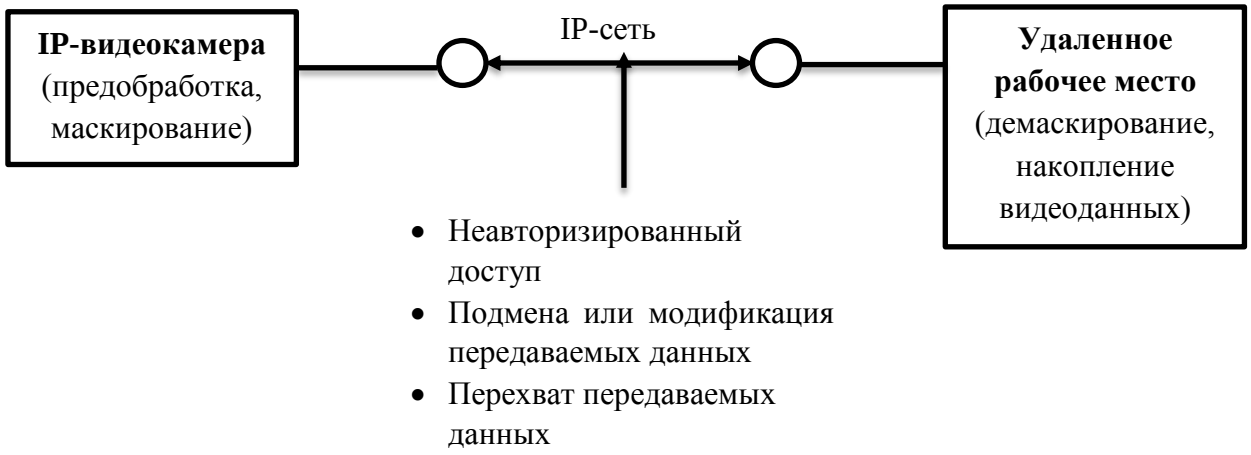


Рисунок 1.6 – Схема применения маскирования/демаскирования

Прямое преобразование фрагментов изображения на передающей стороне осуществляется в виде

$$\mathbf{Y} = \mathbf{M}^{\mathrm{T}}\mathbf{X}\,\mathbf{M}, \qquad (1.1)$$

а обратное преобразование на приемной стороне – в виде

$$\mathbf{X} = (\mathbf{M}^{\mathbf{T}})^{-1}\mathbf{Y}\,\mathbf{M}^{-1} \qquad (1.2)$$

Здесь **M** – специальная матрица, имеющая обратную. Результирующее изображение **P** является итогом дефрагментации из фрагментов вида **X** принятого изображения. Для двухстороннего матричного маскирования использование ортогональных матриц **M,** для которых $\mathbf{M}^{-1} = \mathbf{M}^{\mathbf{T}}$ упрощает вычисления (1.2) до вида $\mathbf{X} = \mathbf{M}\mathbf{Y}\mathbf{M}^{\mathbf{T}}$.

Результаты маскирования с использованием матрицы Адамара размера 12×12, приведенной на рис. 1.7 при однократной помехе в канале, как и в предыдущем примере, приведены на рис. 1.8 [29].

Здесь на рис. 1.8а приведено исходное изображение, на 1.8б – маскированное изображение, 1.8в – демонстрирует наложение помехи на маскированное изображение в канале, на рис. 1.8г – восстановленное изображение с использованием обратного преобразования, на 1.8д – изображение после передачи в канале с помехой без маскирования.

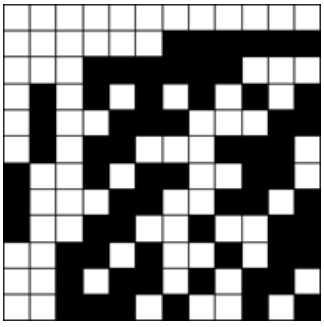


Рисунок 1.7 – Портрет матрицы Адамара порядка 12.

Из рисунка видно, что изображение после маскирования лучше разрушено, чем после стрип-преобразования на рис. 1.5б, и, значит, лучше защищено от несанкционированного ознакомления.

Рисунок 1.8 – Процесс двухстороннего матричного маскирования (взято из работы [29])

В этом случае результат обратного преобразования совпадает с исходным изображением, с точностью до транспонирования маскирующей матрицы: отпадает необходимость отдельно хранить не только саму обратную матрицу, но и ее половину в виду ее симметрии. Это экономит память при непосредственной реализации метода в системе.

Именно приведенный упрощенный вариант стрип-преобразования (без использования кронекерова умножения и разрезания изображения на полоски), но реализуемый с уникальными матрицами, получил название – маскирование [31].

Наилучшие результаты при маскировании достигнуты в диссертационной работе Чернышева С. А. [18], в которой используется семейство уникальных симметричных двухуровневых матриц Мерсенна порядков 7, 15, 31 и 255. Очевидно, что это семейство мало и для реальных применений требует значительного расширения.

Для повышения степени защищенности при покадровой передаче видеоизображений значительное практическое применение может найти гибридный метод сжатия/маскирования.

Кроме перечисленных задач сжатия, помехоустойчивого кодирования и маскирования, можно указать задачу внедрения цифрового водяного знака (ЦВЗ) в статические изображения для их маркирования [32]. При применении ортогональных преобразований их эффективность определяется незаметностью встроенного с их помощью в изображение ЦВЗ, его стойкостью к наиболее распространенным операциям обработки изображения: JPEG-сжатию, зашумлению, изменению яркости и размера, эквализации гистограммы изображения.

В качестве ортогональных преобразований в алгоритмах цифрового маркирования, как и при сжатии, наиболее часто применяют ДКП [33, 34], что связано с его использованием в форматах JPEG и JPEG 2000. Однако в ряде работ [35–42] и др. для цифрового маркирования неподвижных изображений (кадров) используется дискретные преобразования Хаара и Адамара, ядро которого составляет матрица Адамара порядка $n = 2^k$, где k – натуральное число.

Следует отметить, что матричные методы преобразования информации очень практичны, поскольку предполагают эффективную структурную

реализацию как в PLM, так и программную реализацию во всех современных микропроцессорных структурах, ориентированных на цифровую обработку сигналов.

Помехозащищенное кодирование в открытом канале передачи цифровых данных. Передача информации в коммуникационном канале немыслима без применения кодирования. Сегодня известно множество кодов и синтезированных по ним сложных широкополосных сигналов, модулированных по амплитуде, частоте и фазе или одновременно по нескольким параметрам.

Для повышения помехоустойчивости каналов радиолокационных систем (РЛС), выделения полезного сигнала на фоне шумов в коммуникационных каналах распределенных систем, широко применяются методы сжатия сложных сигналов с фазовой модуляцией (ФМ) [11, 13, 43 – 46].

При фазовой модуляции сигналов используют *m*-последовательности, псевдослучайные последовательности, коды Франка, Баркера, Льюиса и Кречмера, полифазные коды, сложные коды, комплементарные коды и др. [11, 13, 45, 47 – 50].

Однако не все сложные сигналы, полученные с использованием приведенных кодов, одинаково эффективны при решении конкретной задачи обнаружения или надежной передачи данных в условиях воздействия помех естественного и искусственного происхождения [44, 46].

Наилучшими являются модулированные кодовой последовательностью сигналы, у которых:

– отношение пика автокорреляционной функции (АКФ) к максимальному по модулю боковому лепестку (ОПМБЛ) – наибольшее;

– ширина главного лепестка АКФ по уровню -3дБ наименьшая;

– потери в отношении сигнал/шум минимальны.

На практике наибольшее распространение при помехоустойчивом кодировании и обнаружении полезного сигнала в условиях сложной помеховой обстановки получили коды Баркера, представляющие собой двоичные последовательности (коды) конечных длин *n*, равных 3, 4, 5, 7, 11 и 13. Так, например, помехоустойчивый код Баркера длины 11 вида 111-1-1-11-1-11-1 используется в наборе стандартов связи IEEE 802.11 для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4, 3,6 и 5 ГГц [51]. В канале такой код представляется иначе: единице соответствует единичное значение сигнала, а -1 – нулевое значение.

Кодовая последовательность Баркера длины 11 и соответствующая ему огибающая ФМ-сигнала представлены на рис. 1.9.

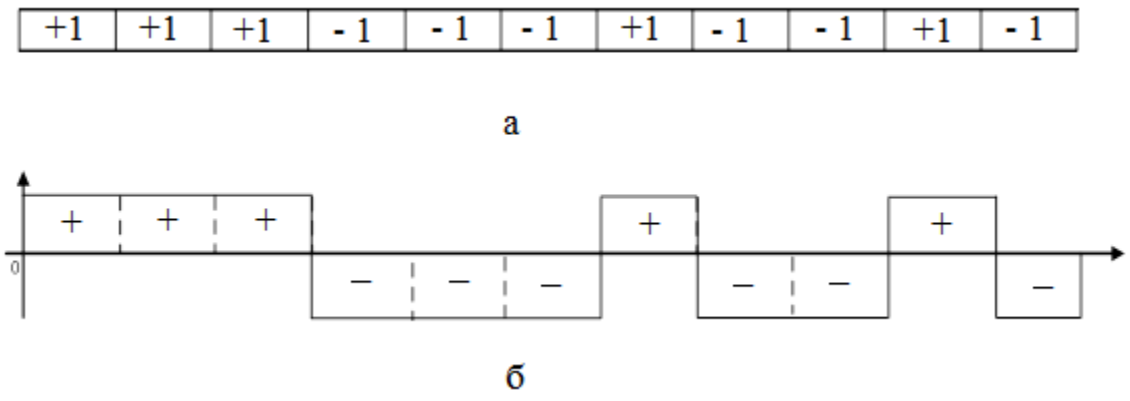


Рисунок 1.9 – Код Баркера *n* = 11 (*а*) и огибающая ФМ-сигнала этим кодом (*б*)

При решении задачи обнаружения и передачи в условиях помех, основной характеристикой, является ОПМБЛ. У кодов Баркера оно равно 1/*n*, где *n* – длина кода, что является лучшим значением среди других кодов. В связи с этим коды Баркера получили распространение при решении многих задач обнаружения и помехоустойчивого кодирования в коммуникационных каналах [11, 48, 51]. Они являются особыми двоичными кодами с максимальными уровнями боковых лепестков по шкале времени, равными – 20log(*n*). Энергия в области бокового лепестка минимальная и одинаково

распределена, за счет чего реализуется равенство амплитуд всех боковых максимумов автокорреляционных функций при их минимально возможном уровне. Код Баркера является единственным однородным фазовым кодом, достигающим этого уровня.

Иными словами, коды Баркера можно рассматривать как специальные кодовые последовательности, позволяющие выделять полезный сигнал из зашумленного принятого сигнала методом корреляционного детектирования – анализа автокорреляционных функций.

Однако не существует доказательства, что полученные Баркером коды являются лучшими и невозможно получить более совершенные коды. Например, в качестве кодовых последовательностей, являющихся набором 1 и -1, для фазовой модуляции, очевидно, могут быть использованы усеченные строки ортогональных матриц Адамара или строки других двухуровневых матриц.

1.3 Требования к семействам матриц для современных задач обработки и передачи информации. Специальные матрицы

Анализ показывает, что в области обработки изображений и видеокадров требования к их качеству и разрешению постоянно возрастают – это является современной тенденцией, реализуемой как производителями видеоматриц, так и производителями матриц дисплеев видеоконтрольных устройств, мониторов, телевизоров.

Сегодня цифровой формат ультравысокой четкости UHD (Ultra High Definition), становясь наиболее распространенным, требует обработки кадров размеров 3840x2160 (4K) и 7680x4320 (8K), а технология «окна качества» (Quality Box) требует обработки кадров вообще произвольного размера.

Указанные обстоятельства порождают необходимость для процедур сжатия, маскирования, маркирования, помехозащищенного кодирования изображений и других иметь широкое семейство ортогональных матриц, включая матрицы не только больших порядков, неизвестные до настоящего времени, но и матрицы нечетных порядков [52 – 55], желательно симметричных структур [56].

Матрицы Адамара существуют на порядках $4t$ и это существенно ограничивает возможности их применения для изображений произвольного разрешения. Кроме того, отсутствует универсальный алгоритм их вычисления, а известные методы не позволяют найти матрицы Адамара всех порядков $4t$.

Таким образом, можно кратко сформулировать общие требования к семейству матриц в следующем виде:

– порядки матриц должны соответствовать возможно большему количеству чисел натурального ряда для возможности выбора лучших матриц (или кратного их использования) для изображений различных размеров;

– для обеспечения альтернативности выбора на каждом порядке должно существовать более одной квазиортогональной матрицы;

– с целью оптимизации объема памяти при хранении матриц и упрощения вычислительных процедур количество возможных значений элементов (уровней) матриц должно быть минимальным, а их структуры должны иметь симметрии.

Дополнительные требования к матрицам двустороннего матричного маскирования заключаются в необходимости обеспечения:

– устойчивости маскированной информации к помехам и потерям в коммуникационном канале;

– инвариантности матриц к двустороннему матричному преобразованию.

Прежде, чем перейти к формулированию условий, при которых можно удовлетворить указанные требования, отметим важный для этого факт – в современных вычислительных средствах вычисления с плавающей точкой и в целых числах практически неразличимы по времени и сложности реализации.

Как показывает анализ публикаций [57 – 62], именно отход от требования целочисленности элементов матриц, характерного для матриц Адамара, позволил ввести в научный оборот новое, отличное от приведенного в определении 4, определение квазиортогональных матриц, существующих на значительно большем числе порядков, принадлежащих, что важно, известным числовым последовательностям.

Определение 10. Квазиортогональной матрицей называется квадратная матрица **A** порядка n с ограниченными по модулю элементами $|a_{ij}| \leq 1$ такая, что $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$, где **I** – единичная матрица, $\omega(n)$ – весовая функция [5].

Приведенное условие несколько слабее, чем для матриц Адамара (определение 5), что значительно расширяет возможность их существования.

Из всего многообразия таких матриц наилучшим образом отвечают сформулированным выше требованиям квазиортогональные матрицы с двумя значениями элементов – двухуровневые.

Одними из показательных представителей двухуровневых квазиортогональных матриц являются матрицы Мерсенна [59], у которых один уровень (элемент) имеет значение 1, а второй вычисляется исходя из условия удовлетворения соотношению $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ и обозначается как $-b$. $|b| < 1$ всегда и это отличает матрицы Мерсенна от матриц Адамара с элементами 1 и –1, обеспечивая возможность их существования на нечетных порядках.

Поиск новых, более эффективных кодовых последовательностей и их комбинаций, синтез сигналов для коммуникационных каналов по найденным кодам может быть основан также на ослаблении требований, но в этом

случае к АКФ. Следует допустить значения вторичных пиков, превышающих единицу, что может быть приемлемым в том случае, когда центральный пик АКФ значительно больше единицы.

Среди квазиортогональных матриц, строки которых, как и у матриц Адамара, могут служить двоичными кодами, следует сосредоточиться на поиске двухуровневых матриц порядков 3, 7 и 11, у которых количество положительных значений на единицу больше отрицательных значений, как в кодах Баркера. Интересен тот факт, что ослабление требований к АКФ можно трактовать как открытие возможности использования несимметричной пары значений элементов кода: 1 и $-b$, где $|b| < 1$, т.е. как у матриц Мерсенна.

Конечно, простая замена в кодовых последовательностях Баркера значения −1 на $-b$ желаемого результата не принесет. Однако коды на парах $\{1, -1\}$ и $\{1, -b\}$ хотя и будут отличаться, но будут кодовыми последовательностями одного типа.

Именно использование несимметричного представления при фазовой модуляции сигналов может стать источником новых, более удачных, кодовых последовательностей, для которых будут обеспечены следующие требования, характерные для кодов фазовой модуляции [47]:

– функция взаимной корреляции любой пары из группы последовательностей одинаковой длины должна быть минимизирована;

– количество вариантов для маскирования кодовой последовательности одной длины должно быть максимальным в целях затруднения возможности их радиоразведки;

– длина кода должна быть произвольной;

– уровень максимальных по модулю боковых лепестков автокорреляционной функции должен быть не хуже, чем у кода m-последовательности.

Наличие асимметрии в представлении модулирующей последовательности сигнала при этом возможно будет являться его маркером, облегчающим идентификацию сигнала в канале.

Таким образом, учитывая изложенное выше, можно сформулировать определение специальных матриц для применения в рассматриваемом спектре решаемых ортогональных преобразований.

Определение 11. Специальные матрицы для задач преобразования и передачи цифровых изображений – это квазиортогональные матрицы простых симметричных структур с двумя значениями уровней, не превышающими по модулю единицы, существующие на четных и нечетных порядках.

1.4 Методы вычисления двухуровневых квазиортогональных матриц. Проблемные порядки

Методы вычисления и поиска квазиортогональных матриц, разработанные до сегодняшнего дня, весьма разнообразны. Сегодня вычисленными являются практически все возможные матрицы Адамара невысоких порядков. Существенного прогресса в вычислении матриц высоких порядков удалось добиться лишь при использовании суперкомпьютеров и квантовых вычислений [63, 64] и оптимизационных процедур [62].

К сожалению, подавляющее большинство методов не позволяют получить результат в виде структурированной матрицы с симметриями.

Одним из классических методов поиска ортогональных по столбцам (квазиортогональных) двухуровневых матриц с элементами {1, –1} четных порядков $n = 2^k$, где k – целое, был метод, предложенный Сильвестром (Sylvester) [4]. Он является методом вычисления матриц Адамара по

предиктору – начальной матрице $\mathbf{S}_n$ с дальнейшим удвоением порядка искомых матриц.

Сильвестр выделил среди матриц с ортогональными столбцами (строками) последовательность, порождаемую рекурсией с начальным условием $H_1=1$, n – порядок матрицы.

Процесс вычислений описывается приведенной на рис. 1.5 схемой.

$$\mathbf{S}_{2n} = \begin{pmatrix} \mathbf{S}_n & \mathbf{S}_n \\ \mathbf{S}_n & -\mathbf{S}_n \end{pmatrix},$$

Рисунок 1.5 – Схема вычислений по методу Сильвестра

Очевидные недостатки метода Сильвестра заключается в том, что:

– искомая матрица наследует структуру предиктора и не обеспечивает ее вариативность;

– применяемое удвоение порядка значительно сужает значимость результатов из-за возрастающих пропусков порядков.

Для метода Сильвестра теоретически находимыми являются матрицы Адамара порядков 2, 4, 8, 16, 32, 64, 128 и т.д. Принципиально не вычисляемыми являются порядки 12, 20, 28, 36, 40, 44, 52 и т.д., поскольку предикторов порядков 6, 10, 14 и др. не существует.

Другим методом, считающимся классическим, является метод Пэли (Paley) [65]. Однако, ввиду его специфики, метод не дает возможности вычисления матриц порядков: 92, 116, 156, 172, 184, 188, 232, 236, 260, 268, 292, 324, 356, 372, 376, 404, 412, 428, 436, 452, 472, 476, 508, 520, 532, 536, 584, 596, 604, 612, 652, 668, 712, 716, 732, 756, 764, 772, 808, 836, 852, 856, 872, 876, 892, 904, 932, 940, 944, 952, 956, 964, 980, 988, 996... см. [66 - 68].

Первый оригинальный метод нахождения матриц Адамара, сводившийся к вычислению матриц высоких порядков на основе матриц

более низких порядков, предложил итальянский математик У. Скарпи (Scarpis) [69].

Следует отметить, что порядки матриц, найденных Скарпи $(n–1)n$, для $n=4k$, где $k = 1, 2, 3…$ Метод заключается в том, что вместо каждого элемента матрицы в нее вставляется она сама. Таким образом, порядок вычисляемой матрицы увеличивается в 4 раза.

В отношении некоторых порядков результат оказался не превзойденным даже при использовании более позднего метода Пэли [65], однако количество пропусков порядков вычисляемых матриц существенно возросло.

Другие схемы вычисления эксплуатируют идею блочного построения квазиортогональных матриц. В частности, известно построение бициклических матриц Адамара [70] из двух циклических блоков (матриц) **A** и **B** в виде

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}, \qquad (1.3)$$

где $\mathbf{B}^{\mathrm{T}}$ – транспонированная матрица **B**, а $-\mathbf{A}^{\mathrm{T}}$ – транспонированная **A** с инверсными знаками элементов. При этом матрица **H** может быть ортогональной даже если **A** и **B** не являются таковыми. И наоборот – если матрицы **A** и **B** ортогональны, то ортогональность матрицы **H** не может быть гарантирована.

Особенность поиска бициклических матриц заключается в том, что заранее невозможно предсказать комбинацию 1 и –1 в начальной строке. Требуется выбор начальных условий на основе тщательного отбора генерируемых комбинаций.

Двухблочную конструкцию построения матриц Адамара обобщает конструкция, называемая массивом Вильямсона [71] и состоящая из четырех циклических блоков **A**, **B** и **C**, **D** в виде:

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \end{pmatrix}$$

Сегодня, кроме методов, использующих предикторы и циклические матрицы-блоки, известны и другие методы вычисления квазиортогональных матриц, основанных на различных принципах и опирающихся на известные особенности матриц. Часть из этих методов базируется на случайных процессах распределения 1 и -1 по матрице с дальнейшей проверкой ее на ортогональность. Недостаток такого подхода очевиден – он заключается в низкой продуктивности, существенно падающей с ростом порядков вычисляемых матриц. Кроме того, при таком подходе не может гарантироваться поиск симметричных структурированных матриц.

Использование суперкомпьтеров при таком случайном поиске не позволило добиться каких-либо существенных результатов.

Некоторые методы основаны на переборных процедурах. В комбинации с другими подходами они оказались продуктивными и позволили найти редкие матрицы [72, 73].

1.5 Выводы по разделу 1

Поиск новых семейств ортогональных матриц является неотъемлемой частью совершенствования и создания новых алгоритмов и процедур обработки цифровых изображений, разработки новых методов защиты информации в сетях и системах телекоммуникаций, разработки новых видов модулирования сигналов для обеспечения высокой надежности обмена информацией в условиях воздействия внешних помех.

Наибольший интерес для указанных применений представляют специальные матрицы, характеризуемые двумя уровнями их элементов, симметричностью структур, в том числе блочной симметрией.

Для поиска и формирования семейств специальных матриц, необходима их классификация, позволяющая выделить их связи и взаимные трансформации для различных способов вычисления матриц, а также новые алгоритмы вычислений.

Для совершенствования помехозащищенного кодирования в каналах телекоммуникаций и выделения полезного сигнала в условиях повышенной помеховой обстановки, существует потребность в получении новых, более совершенных кодовых последовательностей – особых двухуровневых ортогональных функций, которые могут формироваться из строк квазиортогональных матриц.

2 Квазиортогональные матрицы: классификация и связи

2.1 Экстремальные квазиортогональные матрицы и числовые последовательности

Как показывают исследования, с известными числовыми последовательностями соотносимы локально и глобально экстремальные квазиортогональные матрицы, у которых максимален детерминант.

То, что экстремальные квазиортогональные матрицы имеют порядки, соответствующие элементам числовой последовательности $4t$, где t – натуральное число, заметил еще Адамар [3]. Гипотеза Адамара раскрывает разнообразие систем чисел и ортогональных базисов. Предположение, высказанное и подкрепленное примерами матриц в работе [5], состоит в том, что семейства экстремальных матриц существуют не только на четных порядках вида $4t$ и $4t – 2$, но и на нечетных порядках вида $4t – 1$ и $4t – 3$.

Приведенные числовые последовательности распадаются на вложенные в них последовательности простых чисел p, степеней простых чисел p^m, где m – натуральное число, пар близких простых чисел p и p+2, чисел Мерсенна (Mersenne) $2^k – 1$, где k – натуральное число, чисел Ферма (Fermat) $n = 2^{2^k} + 1$ где k – не отрицательное целое число и др.

Согласно нашему предположению, на соответствующие подсемейства распадаются также и матрицы, подробно рассмотренные в работе [74].

Из приведенного в разделе 1 определения 10 видно, что отличие квазиортогональных матриц от ортогональных состоит в наличии весовой функции $\omega(n)$ – масштабном коэффициенте для матриц порядков n.

Определение 12. Локальный максимум $|\det(\mathbf{A})|$ квазиортогональной матрицы достигнут, если любое достаточно малое по параметрам изменение матрицы не нарушает вида уравнения связи $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ при свободно

заданном значении веса $\omega(n)$, но приводит к уменьшению модуля детерминанта [5].

Как показано в работе [5], «… допустимыми являются любые изменения параметров варьируемой матрицы, не нарушающие условие ортогональности ее столбцов. Весовая функция в задачах поиска условного максимума $|\det(\mathbf{A})|$ при ограничении вида $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ заранее не задана, и сама является предметом поиска. В этом состоит важное их отличие от задачи поиска матриц Адамара с жестко заданным заранее весом $\omega(n) = n$».

Там же показано, что «…квазиортогональные матрицы имеют следующие принципы деления их на семейства и подсемейства по аналогии с семействами и подсемействами чисел. Крупное семейство матриц порядков, равных числам некоторой достаточно общей числовой последовательности, отличается от прочих матриц количеством их элементов – уровней».

Например, матрицы Адамара являются двухуровневыми матрицами, причем значения уровней не зависит от их порядков. Функции уровней – константы.

Для экстремальных двухуровневых матриц один из уровней равен 1 (или –1), иначе значение детерминанта матрицы можно повысить элементарным масштабированием. Следовательно, варьируемая функция уровня семейства двухуровневых матриц – всего одна.

Подсемейства квазиортогональных матриц строятся на порядках, вложенных в основные числовые последовательности. Элементы подсемейств различаются между собой структурами.

Простейшими структурами являются циклические, бициклические и негациклические матрицы. Если регулярная структура не реализуема, появляются более сложные структуры, содержащие в своем составе циклические, обратные циклические, негациклические и др. составные блоки матриц, а также кайму.

В ряде работ Балонина Н. А. и Сергеева М. Б. отмечена «… также возможность выделения некоторой универсальной структуры для всех подсемейств семейства матриц, разрешимой для любого вложения. Например, для матриц Адамара такой является структура из четырех блоков. Отделять универсальные структуры от частных полезно, они различимы на всех порядках $4t$, $4t - 1$, $4t - 2$, $4t - 3$ ($4t + 1$) основных семейств».

Ими же показано, что «…семейство квазиортогональных матриц порядков $4t - 3$ дисперсное, значения порядков вложенных матриц нарастают в нем не аддитивно, поскольку по своей конструкции матрицы являются специфичными производными от основных матриц».

В данном семействе есть оригинальные подсемейства с нарастающими по величине пропусками порядков и особыми порядками, на которых матриц не существует или их существование ставится под сомнение. А вот «…свойство числа 9 последовательности $4t - 3$ распадаться на пару множителей 3 последовательности $4t - 1$ находит свое отражение в блочной структуре матрицы Якобсталя (Jacobsthal) – основе матрицы Белевича из семейства порядков $4t - 2$».

Для разделения сугубо различных между собой подсемейств удобно пользоваться разными обозначениями $4t - 3$ (матрицы Зейделя) и $4t + 1$ (матрицы Ферма) этих порядков.

Семейство двухуровневых матрицы Адамара порядков $4t$ характеризуется глобальным максимумом детерминанта. Как уже оказалось, для матриц соседних семейств важно не то, что максимум глобальный – он может быть и локальным, но число уровней минимально – два.

Осознав это, можно уйти от исследования матриц с глобальным максимумом детерминанта по причинам, рассмотренным в работе [5]. Матрицы, отличающиеся глобальным максимумом детерминанта на уравнении связи $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ соответствуют своему семейству чисел. На

нечетных порядках $4t - 1$ или $4t - 3$ количество уровней не постоянно, оно растет почти линейно как $(n + 1)/2$.

На порядках 3 и 5 имеются 2 и 3 уровня, соответственно. На последующих порядках количество уровней отличаются не более, чем на 1, от оценочного. На четных порядках усложнения матриц не наблюдается, для $4t - 2$ они являются трехуровневыми (иногда количество уровней больше). Особые точки на $4t - 2$ – предмет отдельных исследований.

Порядок 13 – критический [5], для него и далее для всех нечетных порядков количество уровней квазиортогональных матриц глобального максимума детерминанта значительно превышает приведенную выше линейную оценку.

Переход от матриц с абсолютным условным экстремумом к матрицам локального максимума детерминанта принципиален.

На рис. 2.1 приведены «портреты» пяти оптимальных матриц $\mathbf{A}_3$, $\mathbf{A}_5$, $\mathbf{A}_7$, $\mathbf{A}_9$, $\mathbf{A}_{11}$, $\mathbf{A}_{13}$ и количества их модульных уровней на гистограммах. Здесь и далее элементы матрицы различных уровней изображаются квадратами разного цвета или оттенка серого.

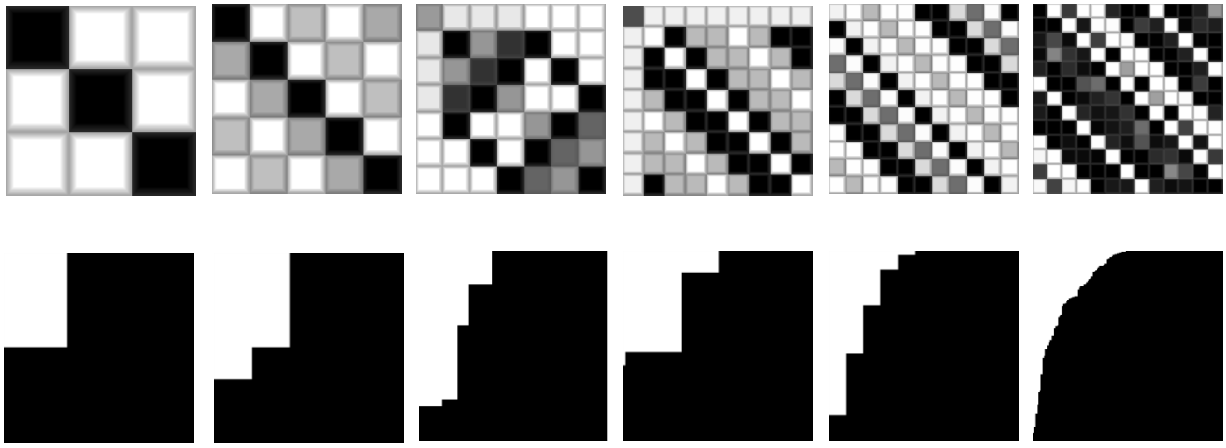


Рисунок 2.1 – Портреты матриц $\mathbf{A}_3$, $\mathbf{A}_5$, $\mathbf{A}_7$, $\mathbf{A}_9$, $\mathbf{A}_{11}$, $\mathbf{A}_{13}$ с гистограммами модулей уровней их элементов (взят из [2])

В работе [5] показано, что «…малое число уровней гарантирует лишь «слабый оптимум» матриц, но именно оно соответствует обширным семействам чисел. Отказ от поисков матриц глобального условного экстремума, характерного только для четных порядков, позволяет установить достаточно прочную связь между числами и квазиортогональными матрицами». Наиболее предпочтительны для использования в обработке информации, как было сказано ранее, ортогональные (не обязательно оптимальные по детерминанту) матрицы с минимальным количеством значений элементов – уровней матрицы.

Первый алгоритм вычисления ортогональных по столбцам (квазиортогональных) двухуровневых матриц с элементами {1, –1} четных порядков $n = 2^k$, где k – целое, был предложен Сильвестром [4].

Адамар сформулировал гипотезу о существовании таких матриц на порядках 1, 2 и $4t$, где t – натуральное число, включающих порядки 2^k, заложив основы масштабных исследований, во-первых, соответствия последовательностей целых чисел и квазиортогональных матриц на порядках, равных этим числам, во-вторых, вложенности числовых последовательностей при сохранении качества соответствия чисел и матриц.

С последовательностью Адамара $4t$ соседствуют известные последовательности нечетных чисел $4t + 1$ и $4t – 1$ ($4t + 3$), на обособленные числовые свойства которых обратили внимание еще Ферма и Эйлер (Euler).

Последовательность нечетных чисел включает последовательность чисел Мерсенна, задаваемую как $n = 2^k - 1$, где k – натуральное число, и начинающуюся с чисел 1, 3, 7, 15, 31,… Она принадлежит последовательности чисел вида $4t – 1$ и, соответственно содержит порядки 1, 3, 5, 7, 11, 15...

Последовательность чисел Ферма, определяемая формулой $n = 2^{2^k} + 1$, начинается с чисел 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, … и принадлежит последовательности чисел вида $4t + 1$.

В работе [60] рассматривается последовательность трехуровневых ортогональных матриц, порядки которых равны числам Ферма, а также числам вида $n = 2^k + 1$, где k – четное целое число (за исключением $k = 1$): 3, 5, 17, 65, 257, 1025, … .

Нечетные числа последовательностей $4t - 3$ (или $4t + 1$) и $4t - 1$ (или $4t + 3$) ввели Ферма и Эйлер. Ферма установил, что всякое простое число вида $4t + 1$ может быть представлено в виде суммы двух квадратов, причем единственным образом. Например, $5 = 1 + 4$.

Простые числа вида $4t + 3$ в виде суммы квадратов не представимы. Это обстоятельство используется в теории квазиортогональных матриц четных порядков $n = 4t - 2$, поскольку критерий Эйлера-Ферма о разложимости числа $n - 1 = 4t - 3$ (не всегда простого) на сумму двух квадратов входит в проверку необходимых условий их существования.

Разнообразие последовательностей чисел дает возможность отойти от универсальных алгоритмов поиска квазиортогональных матриц или матриц максимума детерминанта только на последовательности $4t$ и кардинально расширить базис квазиортогональных матриц, одновременно ускорив их вычисление за счет использования новых подходов и методов.

2.2 Классификация матриц глобального и локального максимума детерминанта

В работе [5] отмечается, что «…отличительной особенностью матриц Адамара, поставленных в соответствие последовательности чисел Сильвестра $n = 2^k$, является их оптимальность по детерминанту». В общем случае квазиортогональные матрицы могут иметь как глобальный, так и локальный максимум детерминанта [5, 58].

Определение 13. Строго оптимальную «…по детерминанту квазиортогональную матрицу порядка, равного некоторому числу числовой

последовательности, будем называть матрицей, ассоциированной с этим числом».

Данное определение приведено впервые в работе [5].

Далее будет показано, что последовательностям чисел соответствуют последовательности матриц, которые по аналогии будем называть ассоциированными с ними последовательностями матриц.

На четных порядках это могут быть оптимальные матрицы Адамара, Белевича (С-матрицы) [75] и т.п., на нечетных – субоптимальные матрицы, ассоциированные с последовательностями Мерсенна и Ферма.

Указанное обстоятельство дает хорошую ориентацию в разнообразии базисов и позволяет разработчикам технических систем значительно облегчить выбор матрицы, оптимальной для конкретной задачи обработки или преобразования информации.

Для того чтобы оперировать с любыми четными и нечетными порядками понятие минимаксности квазтортогональных матриц необходимо расширить. Как известно, минимум может быть двух видов. Абсолютный минимум функции и локальный – частный минимум.

Матрицы Адамара минимаксны в первом смысле абсолютного минимума максимума ее элементов. Остальные двухуровневые матрицы отвечают локальному максимуму, поскольку на нечетных порядках минимизация m-нормы приводит к значительному росту числа уровне с ростом порядка [5].

Только у матриц четных порядков число уровней с ростом порядка не растет. Таковы матрицы Адамара и трехуровневые матрицы Белевича с элементами 0, 1, –1.

Таким образом, двух и трехуровневые минимаксные в указанном широком смысле матрицы образуют специфическое расширенное семейство матриц Адамара с малым числом уровней и произвольных (четного или нечетного) порядков. Это обстоятельство и позволяет говорить о

значительном расширении базиса для ортогональных преобразований в прикладных задачах.

В работе [59] предложены квазиортогональные матрицы Адамара-Мерсенна, существующие на нечетных порядках $n = 2^k - 1$, соответствующих последовательности Мерсенна.

Определение 14. Матрица Адамара-Мерсенна $\mathbf{M}_n$ – квадратная матрица порядка $n = 4t - 1$, состоящая из чисел $\{a = 1, -b\}$, столбцы которой ортогональны $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\mathbf{I}$, $b = \frac{t}{t+\sqrt{t}}$, $\mu = \frac{p+qb^2}{2}$, $p = n-1$, $q = n+1$ (порядок матрицы Адамара).

Определение 15. Матрица Адамара-Эйлера $\mathbf{E}_n$ [61] – квадратная матрица порядка n, состоящая из чисел $\{a = 1, -a, b, -b\}$, столбцы которой ортогональны

$$\mathbf{E}_n^{\mathrm{T}}\mathbf{E}_n = \xi\,\mathbf{I},$$

где $b = \frac{1}{2}$ при $n = 6$, в остальных случаях $b = \frac{q-\sqrt{8q}}{q-8}$, $q = n + 2$ (порядок матрицы Адамара), вес $\xi = \frac{(n+2)+(n-2)b^2}{2}$ учитывает, что $\frac{q}{2}$ модулей элементов каждого столбца такой матрицы имеют значения $|a| = 1$, модули остальных элементов равны $|b| < 1$.

Определение 16. Матрица Адамара-Ферма $\mathbf{F}_n$ [60] – квадратная трехуровневая матрица порядков $n = 2^k + 1$, при четных значениях k с элементами $\{1, -b, s\}$, где $s \le b < 1$, удовлетворяющие квадратичному условию связи

$$\mathbf{F}^{\mathrm{T}}\mathbf{F} = \omega(n)\mathbf{I},$$

где $\mathbf{I}$ – единичная матрица, вес $\omega(n) = 1 + (n-1)s^2$. Модульные уровни $b = s = 2/3$ при $n = 5$, в общем $b = \frac{2n-p}{p}$, элементы канвы $s = \frac{\sqrt{nq-2\sqrt{q}}}{p}$

составляют первые строку и столбец, за исключением первого единичного элемента, $p = q + \sqrt{q}$, q=n–1 (порядок соседних матриц Адамара).

Определение 17. Матрица Белевича [75] – «…квадратная трехуровневая матрица $\mathbf{C}_n$, состоящая из элементов трех уровней {1, 0, –1}, столбцы которой ортогональны

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

а нулевые элементы сосредоточены на диагонали».

Определение 18. Квазиортогональными матрицами Зейделя (Seidel) $\mathbf{S}_n$ [76] называются трехуровневые матрицы порядков $n = 4k + 1$ со значениями элементов $\{1, -b, d\}$, где $d < b < 1$, удовлетворяющие квадратичному условию связи

$$\mathbf{S}_n{}^{\mathrm{T}}\mathbf{S}_n = \omega(n)\mathbf{I}_n.$$

Здесь $\omega(n) = d + (n-1)\dfrac{1+b^2}{2}$ − переменный вес. Диагональные элементы матрицы $d = \dfrac{1}{1+\sqrt{n}}$, $b = 1 - 2d$.

Перечислим возможные минимаксные квазиортогональные матрицы с малым числом различающихся значений уровней элементов.

В зависимости от остатка r деления порядка n на 4 они могут быть классифицированы как матрицы вида [74]:

- r=0 – матрицы Адамара (**H**), включающие матрицы последовательности Сильвестра;
- r=1 – матрицы Ферма (**F**), включающие матрицы порядков последовательности чисел Ферма;
- r=2 – матрицы Эйлера (**E**), дополняющие матрицы Белевича (**C**) на исключениях, определяемых критерием Эйлера-Ферма;
- r=3 – матрицы Мерсенна (**M**), включающие матрицы порядков последовательности чисел Мерсенна.

Малоуровневые матрицы включают, таким образом, матрицы **H**, **F**, **E** и **M** множества квазиортогональных матриц, в которых последовательности Сильвестра и Мерсенна, по предположению [74], являются системообразующими.

Оценки плотности охвата числовой оси значениями порядков матриц основываются, соответственно, на сходных гипотезах:

– гипотезе Адамара (Hadamard conjecture) – перенос свойств матриц порядков последовательности Сильвестра на матрицы **H**,

– гипотезе Балонина (Balonin conjecture) [74] – перенос свойств матриц порядков последовательности Мерсенна на матрицы **M**.

Для обобщения понятий матриц Адамара-Мерсенна позже было предложено определение матриц Мерсенна как квадратной матрицы $\mathbf{M}_n$ порядка n, вложенного в последовательность $4t - 1$, при сохранении значения модулей элементов матрицы, состоящей из $\{a = 1, -b\}$, столбцы которой ортогональны $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\mathbf{I}$. Здесь $b = a/2$ при $n = 3$, в остальных случаях $b = \dfrac{q - \sqrt{4q}}{q - 4}$, $q = n + 1$ (порядок матрицы Адамара).

Аналогично обобщены понятия матриц Адамара-Эйлера и Адамара-Ферма и предложены определения матриц Эйлера и Ферма, существующие на порядках, соответствующих последовательностям $4t - 2$ и $4t + 1$.

Для большей определенности в типах рассматриваемых квазиортогональных матриц приведем таблицу 2.1 матриц порядков $n = 4t \pm l$, здесь $l \leq 3$, классифицируемых по принадлежности их элементов заданным константам (как у матриц Адамара) или функциям уровня, зависящим от порядка n.

Порядки $4t - 3$ (или $4t + 1$) сложнее прочих тем, что ортогональность столбцов матриц достижима при введении дополнительного уровня d для элементов диагонали (матрицы Зейделя) или каймы s (матрицы Ферма).

Таблица 2.1 – Значения элементов семейств матриц

Символ	Порядок n	Матрица	Значения элементов
H	$4t$	Адамара	1, –1
C	$2t$, $4t$	Белевича	1, –1, 0
M	$4t-1$	Мерсенна	1, $-b$, где $b=\frac{t}{t+\sqrt{t}}$
E	$4t-2$	Эйлера	1, $-b$, где $b=\frac{t}{t+\sqrt{2t}}$
S	$4t-3$	Зейделя	1, $-b$, d, где $b=1-2d$, $d=\frac{1}{1+\sqrt{n}}$
F	$4t+1$	Ферма	1, $-b$, s, где $q=n-1=4u^2$, $p=q+\sqrt{q}$, $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u}$, $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}=\frac{\sqrt{nu-1}}{2u+1}\times\frac{1}{\sqrt{u}}$

Предложенная автором классификация включает в себя все возможные случаи четных и нечетных порядков, в том числе порядки, кратные 2 [74].

В пояснение сформулированной автором гипотезы Балонина о существовании матриц Мерсенна порядков $4k$–1, Балониным Н. А. найдены матрицы Мерсенна $\mathbf{M}_{11}$ и $\mathbf{M}_{19}$, портреты которых приведены на рис. 2.2 [77].

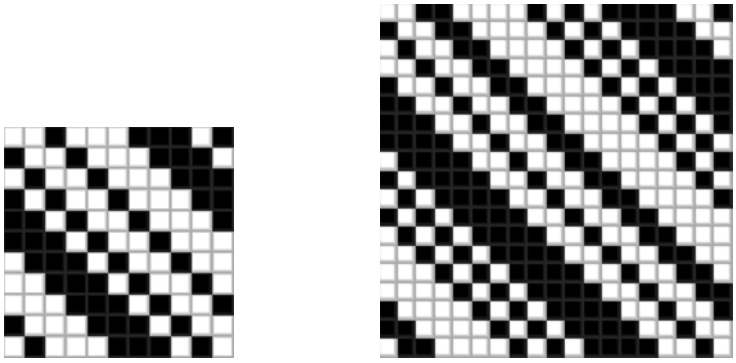


Рисунок 2.2 – Портреты матриц Мерсенна порядков 11 и 19

Следует отметить, что гипотеза Балонина значительно увеличивая количество малоуровневых минимаксных квазиортогональных матриц, рассмотренных в работах [57, 78, 79], является важным и принципиальным для теории квазиортогональных матриц.

Другие взаимосвязи последовательностей квазиортогональных матриц, построенных на известных последовательностях чисел, приведены в работах [80, 81].

2.3 Взаимосвязи квазиортогональных матриц

Как было отмечено, гипотеза Балонина имеет системное значение для матриц Мерсенна и отвечает гипотезе Адамара, расширяя трактовку четных порядков Сильвестра на нечетные порядки.

Покажем взаимосвязи матриц и способы нахождения матриц Мерсенна, дополнительных к основной последовательности. Ассоциированные с числами последовательностей Сильвестра и Мерсенна матрицы встречаются чаще, чем относительно более редкие матрицы, ассоциированные с числами последовательности Ферма.

Исследования показали, что матрицы Адамара порядков $4t$, можно получить на основе матриц Мерсенна порядков $4t - 1$ (и наоборот). Последовательности чисел Сильвестра и Мерсенна связаны между собой однозначно, столь же однозначно связаны между собой и ассоциированные с ними матрицы.

В работах [78 – 80] раскрываются выявленные взаимосвязи матриц, приведенных в таблице 2.1 и их структур.

Взаимосвязь 1. Матрица $\mathbf{H}_{4t}$ вычисляется путем окаймления матрицы Мерсенна в виде

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

с заменой элементов $-b$ образующей ее матрицы на –1. Здесь λ, e – собственное число и собственный вектор округленной целочисленной матрицы $\mathbf{M}_{4t-1}$ соответственно [80].

Возможен и обратный ход этого алгоритма, когда усечением нормированной матрицы Адамара (с изменением по знаку) и изменением отрицательных значений ее элементов до расчетного значения уровня $-b$, вычисляемого по формулам, приведенным в определении 14, формируется матрица Мерсенна.

Такая взаимосвязь показывает, что с точностью до знака округленная матрица Мерсенна является ядром (core) нормализованной матрицы Адамара. В качестве примера матриц Адамара, отличных от матриц основной последовательности, на рис. 2.3 и 2.4 приведены портреты матриц Адамара $\mathbf{H}_{12}$ с инвертированным по знаку ядром, чтобы обеспечить должное значение $-\lambda$, и ядра – матрицы Мерсенна $\mathbf{M}_{11}$, соответственно.

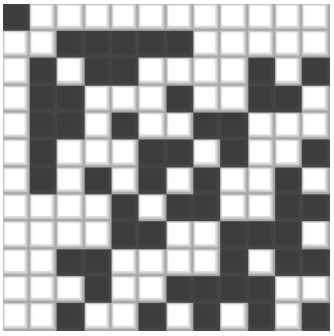


Рисунок 2.3 – Портрет матрицы $\mathbf{H}_{12}$

Следовательно, матрица Мерсенна, включая порядки, отличные от чисел Мерсенна, может быть найдена посредством матрицы Адамара (и наоборот). Каждая из таких матриц Мерсенна является исходной для получения ветви матриц применением описанного выше и модифицированного для нечетных порядков алгоритма Сильвестра.

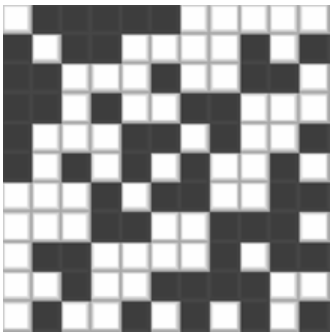


Рисунок 2.4 – Портрет матрицы $\mathbf{M}_{11}$

В публикациях матрицы Мерсенна и Ферма представлены самостоятельно, отдельно друг от друга. Однако существуют некоторые общие структуры квазиортогональных матриц четного и нечетного порядков.

Взаимосвязь 2. Матрица Ферма $\mathbf{F}_{4u^2+1}$, где u – целое число, может быть получена путем окаймления регулярной матрицы Адамара в виде

$$\mathbf{F}_{4u^2+1}=\begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{H}_{4u^2} \end{pmatrix},$$

где λ, e – соответственно собственное число и собственный вектор регулярной матрицы Адамара $\mathbf{H}_{4u^2}$ (суммы строк и столбцов одинаковы), у которой отрицательные элементы заменены значениями, характерными для матриц Ферма из определения 16.

Элемент –1 матрицы Адамара следует принять равным значению $-b$, $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u}$, элементы $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}$ собственного вектора являются элементами ($a < s \le b$) каймы матриц Ферма, $q=n-1=4u^2$ (порядок регулярной матрицы Адамара), $p=q+\sqrt{q}$.

Как и в предыдущем случае возможен обратный ход алгоритма вычисления вложенной матрицы Адамара по матрице Ферма. Отличие матриц Ферма от матриц Мерсенна состоит в том, что первые существуют только для значений порядков, равных числам Ферма, а также расширенных

порядков, равных числам вида $n = 4u^2 + 1$, где u – натуральное число, имеем: 3, 5, 17, 37, 65, 101, 145, 197, 257, ….

Матрица Адамара после нормализации (операции, при которой знаки элементов ее первого столбца и строки совпадают) дальнейшим усечением ее с пересчетом уровня переводится сначала в матрицу Мерсенна, а потом усечением – в матрицу Эйлера [61] четного порядка с модулем уровня $b = \frac{q - \sqrt{8q}}{q - 8}$, $q = n + 2$, $n = 4t - 2$.

Матрицы Эйлера сходны с матрицами Адамара в том, что они существуют на четных порядках и для них справедливо следующее разложение на квадратные блоки

$$\mathbf{E}_{2n} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix},$$

а верхние блоки образуются, в частности, из матриц Мерсенна $\mathbf{A} = \mathbf{B} = \mathbf{M}_n$. Расширение этого простого частного случая на матрицы с не совпадающими блоками даст весь набор порядков $n = 4t - 2$ матриц с указанными уровнями.

Матрицы Мерсенна существуют для всех значений $n = 4t - 1$ без исключения. Матрицы Эйлера удобны для технических приложений тем, что они существуют, соответственно, для всех $n = 4t - 2$. Они удачным образом заполняют известные пробелы порядков 22 [82], 34, 58 и т. п. среди квазиортогональных матриц Белевича. Объясняется это тем, что матрицы Эйлера могут быть иррациональны, тогда как целочисленные матрицы Белевича существуют только для порядков, на которых $n - 1$ разложимо на сумму квадратов целых чисел.

2.4 Матрицы Мерсенна как предикторы цепочек квазиортогональных матриц

Представленные ранее и другие взаимосвязи квазиортогональных матриц рассмотрены в работе [78] и уточнены в работе [81].

Особенность взаимосвязи квазиортогональных матриц состоит в том, что по каждой матрице Мерсенна нечетного порядка можно построить матрицу Эйлера удвоенного четного порядка. На порядках $n = 1$ и $n = 2$ формы этих двух типов матриц не имеют развитых отличительных признаков, а, соответственно, не ясно, первична матрица Мерсенна или Эйлера.

Нельзя утверждать, что матрицы Мерсенна являются предикторами матриц Эйлера, поскольку существует правило перехода от любой матрицы Эйлера $\mathbf{E}_n$ к матрице Мерсенна $\mathbf{M}_{n+1}$ на единицу большего значения порядка.

Типичная цепочка взаимосвязанных структурно матриц Мерсенна и Эйлера выглядит как $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$. Цепочка таких последовательно вычисляемых матриц может начинаться и с матрицы Эйлера. В работе [61] доказывается, что порядок матриц Эйлера четен и равен $n = 4t - 2$, здесь, как и ранее, t – натуральное число. Поэтому на основе матриц Мерсенна порядков $n = 4t - 1$, принимающих значения 3, 7, 11, 15 … и отличающихся на 4 (характерный период для всех типов матриц семейства Адамара) строятся матрицы Эйлера порядков 6, 14, 30….

Таким образом, имеется неопределенность относительно нахождения матриц Эйлера, когда половинное значение их порядка не равно порядку матриц Мерсенна. Это характерно, например, для существующей матрицы $\mathbf{E}_{10}$ [83]. До сих пор в статьях при описании взаимосвязи матриц Мерсенна и Эйлера порождающая матрица для такого случая не определялась.

Помимо асимметричных циклических матриц Мерсенна порядков $n = 4t–1$ используем во многом похожие на них симметричные циклические матрицы Зейделя $\mathbf{S}_n$ порядков $n = 4t + 1$.

Матрицы Мерсенна и Зейделя имеют нечетный порядок и могут использоваться при вычислении четных двуциклических матриц Эйлера.

В первом случае матрица Эйлера строится на основе асимметричных составляющих, во втором – симметричных.

Матрицы Эйлера можно вычислить по правилу Сильвестра, общему для всех адамаровых матриц, по матрицам Мерсенна в виде [81]

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & -\mathbf{M}_{n/2} \end{pmatrix},$$

где $\mathbf{M}_{n/2}$ –матрица Мерсенна.

В то же время матрицы Мерсенна связаны с матрицами Эйлера дополнением их строкой и столбцом (каймой) в виде [81]

$$\mathbf{M}_{n+1} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{E}_n^* \end{pmatrix},$$

где $\lambda = –a$ – собственное число, а e – собственный вектор «сопряженной» матрицы

$$\mathbf{E}_n^* = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & \mathbf{M}_{n/2}^* \end{pmatrix},$$

блок $\mathbf{M}_{n/2}^*$ получатся из $\mathbf{M}_{n/2}$ взаимной заменой элементов 1 и $–b$ и пересчетом уровня $b = \dfrac{q - \sqrt{4q}}{q - 4}$, где $q = n + 2$ (порядок матрицы Адамара).

Содержательная сторона формул состоит в том, что матрицы Мерсенна и Эйлера рассчитываются на основе друг друга, образуя возрастающие по порядкам цепочки.

Это обобщает правило Сильвестра – расчет возрастающих по порядку матриц Адамара.

Приведенное модифицированное правило Сильвестра обобщает правило Пэли вычисления матриц Адамара по матрицам Белевича, опираясь на взаимно однозначную связь матриц Адамара, Мерсенна и Эйлера.

Рассмотрим алгоритмы построения квазиортогональных матриц заданных порядков, а также произведем оценку сложности таких процедур. Заметим, что в итерационных алгоритмах вычисления матриц Мерсенна нет необходимости вычислять собственные числа и собственные векторы $\mathbf{S}_{2n}$.

Для уменьшения трудоемкости решение этой задачи, служащее источником определения уровней, ищется аналитически: половину элементов собственного вектора e матрицы $\mathbf{S}_{2n}$ составляют элементы $-b$, остальную половину – элементы a, что дает возможность быстрого вычисления матриц требуемых семейств в виде

$$\mathbf{M}_{2n+1} = \begin{pmatrix} 1 & e^{\mathrm{T}} \\ e & \mathbf{S}_{2n} \end{pmatrix}.$$

Пример. Итерации вычисления матриц Мерсенна основной последовательности $n = 2^k - 1$ начинаются с матрицы [74]

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix},$$

причем

$$\mathbf{M}_3^* = \begin{pmatrix} -b & a & -b \\ a & -b & -b \\ -b & -b & a \end{pmatrix}.$$

Как было принято ранее, a=1 и тогда модуль второго элемента $b = \dfrac{t}{t+\sqrt{t}}$ будет иметь значение 0,5 при t = 1 (порядок $n = 4t - 1 = 3$) и растет до $b = 2 - \sqrt{2} = 0{,}5858\ldots$ при t = 1 (порядок n = 7).

Учитывая выписанное выше выражение, расчетная матрица Мерсенна $\mathbf{M}_7 = \begin{pmatrix} 1 & e^{\mathrm{T}} \\ e & \mathbf{S}_6 \end{pmatrix}$ при e = (*-b*, *-b*, *-b*, 1, 1, 1)$^{\mathrm{T}}$ также квазиортогональна, а итерации можно продолжить до бесконечности.

На рис. 2.5 приведены первые три матрицы Мерсенна $\mathbf{M}_3$, $\mathbf{M}_7$, $\mathbf{M}_{15}$ этого бесконечного, согласно гипотезе Балонина [74], семейства.

Приведенные выше формулы, как видно, несложно компьютеризировать, получая цепочки ортогональных по столбцам матриц Мерсенна нечетных порядков $2^k - 1$, столь же легко, как и цепочки матриц Адамара четных порядков 2^k, содержащих элементы 1 и –1.

Число уровней матриц Мерсенна – два, причем с ростом порядка значение модуля уровня второго элемента $b = \frac{t}{t + \sqrt{t}}$ стремится к 1, т.е. эти две цепочки матриц сближаются друг к другу по значениям их элементов при $n \to \infty$.

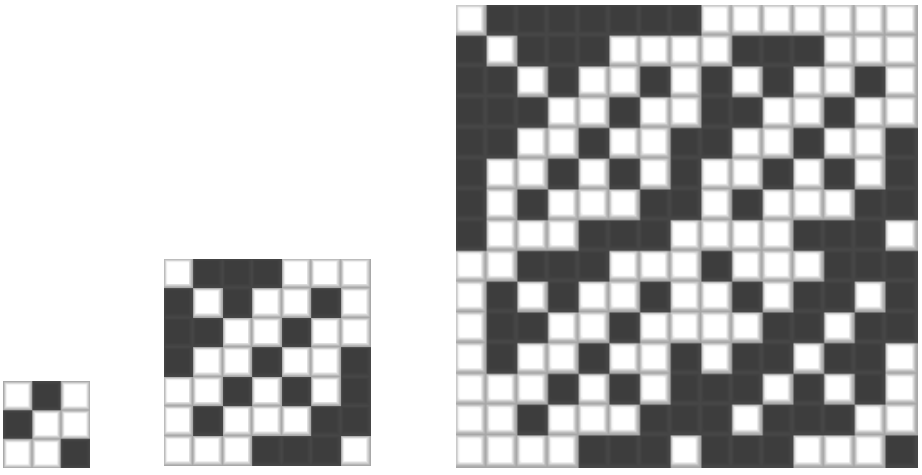


Рисунок 2.5 – Портреты квазиортогональных матриц $\mathbf{M}_3$, $\mathbf{M}_7$, $\mathbf{M}_{15}$

Алгоритм вычисления матриц Эйлера четных порядков использует алгоритм вычисления матриц Мерсенна, т.е. не превосходит его по трудоемкости:

$$\mathbf{E}_{2n} = \begin{pmatrix} \mathbf{M}_n & \mathbf{M}_n \\ \mathbf{M}_n^{\mathrm{T}} & -\mathbf{M}_n^{\mathrm{T}} \end{pmatrix}.$$

В работе [74] показано, что цепочка последовательно вычисляемых матриц может начинаться непосредственно с матрицы Эйлера, если соответствующей ей по порядку матрицы Белевича нет.

Отдельно следует отметить, что в ряде случаев предпочтительным вариантом для обработки информации действительно является матрица Мерсенна с фиксацией значения уровня a=1 и вычислением второго уровня элементов -b по представленным выше зависимостям от n.

В то же время для других преобразований предпочтительно отсутствие такой фиксации и построение матриц Мерсенна с обоими вычисляемыми уровнями a и b, что демонстрируется в разделе 4 при реализации процедуры сжатия с матрицей Мерсенна, отсортированной по Уолшу, используемой вместо матрицы ДКП.

2.5 Слои квазиортогональных матриц

Перечисленные семейства матриц обладают сходными свойствами, вместе они образуют расширенное семейство матриц типа Адамара, и могут использоваться в прикладных алгоритмах, расширяя их возможности.

Определение 19. Слоем матриц семейства Адамара будем называть «…совокупность квазиортогональных матриц с известными функциями зависимости значений элементов (уровней) матриц слоя от заданных показателем j значений порядков».

Матрицы Адамара, Мерсенна и Эйлера, согласно [3, 57, 59], образуют слои для $n = 4k - l$, для $l = 0, 1, 2$ соответственно. Матрицы Ферма такого непрерывного слоя не образуют, поскольку для них функции уровня определены на узком множестве значений $n = 2^k + 1$ при четных k [60].

Балонин Н. А. и Сергеев М. Б. в своих работах утверждают, что «…следствием такого подхода к классификации матриц семейства Адамара является представление о том, что все названные выше матрицы являются проявлением одного широчайшего матричного базиса, данного совокупностью слоев и сечений – матриц соседних слоев для заданных показателем k значений порядков. Нахождение любой матрицы сечения автоматически влечет за собой нахождение всех остальных, поскольку они отражают одно и то же: матрицы сечения взаимно зависимы. Например, матрицы Адамара $\mathbf{H}_4$ получается из приведенной выше матрицы Мерсенна $\mathbf{M}_3$ округлением ее отрицательных элементов до значения –1 с добавлением каймы в виде строки и столбца с отрицательными элементами для соблюдения баланса положительных и отрицательных элементов».

В заключение проиллюстрируем зависимости от порядка n детерминантов матриц трех выделенных слоев: Эйлера, Мерсенна, Адамара, добавив к ним ветви выборочно проявляющих себя матриц Ферма и Белевича.

Поскольку график детерминанта $|\det(\mathbf{A})|=n^{n/2}/h^n$ быстро растет, для иллюстрации достаточно, избавившись от степеней, вывести график делителя − адамаровой нормы $h(n)$.

Определение 20. Адамаровой нормой h (h-нормой) квазиортогональной матрицы называют $h = m\sqrt{n} \geq 1$ [5, 58].

Адамарова норма квазиортогональной матрицы удобнее m-нормы при контроле завершения вычисления адамаровых матриц, поскольку для них (и только для них) она равна 1. Это инвариант матриц Адамара. У всех остальных матриц h >1.

Если делитель стремится к единице, а он стремится к ней у всех рассмотренных матриц, то такие матрицы с ростом порядка почти ничем не отличаются от матриц Адамара с их максимально большим определителем. Графики h-норм рассмотренных в разделе матриц приведены на рис. 2.6 [58].

Здесь инвариант виден по *h*-нормам связанных друг с другом матриц Мерсенна и Эйлера (удвоенного порядка). Данные инварианты описывают равновеликие по *h*-нормам особенности единого математического объекта и обобщают правило, использованное Пэли для увеличения числа найденных им матриц Адамара.

Подводя итог рассмотренного в настоящем разделе материала отметим, что приведенные основные определения позволяют классифицировать квазиортогональные матрицы и их характеристики, выделять порядки их существования, принадлежащие известным числовым последовательностям. С использованием понятий вложенности основных числовых последовательностей друг в друга актуализируются определения основных квазиортогональных матриц Мерсенна, Эйлера, Ферма и порядки их существования.

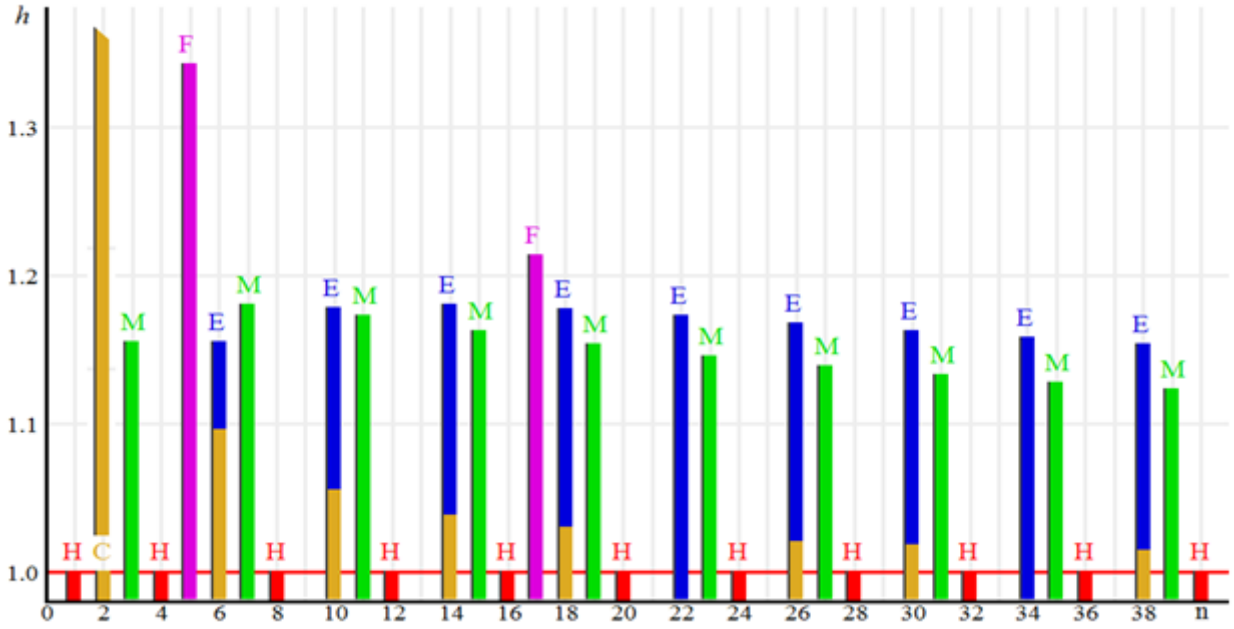


Рисунок 2.6 – *h*-нормы матриц Эйлера (**E**), Белевича (**C**), Мерсенна (**M**), Адамара (**H**) и Ферма (**F**)

2.6 Выводы по разделу 2

В настоящем разделе предложена классификация квазиортогональных матриц, порядки которых соответствуют известным последовательностям чисел. Это значительно развивает теорию квазиортогональных матриц, позволяя выявлять взаимосвязи структур и получать как отдельные матрицы, не вычисляемые классическими методами Сильвестра, Пэли, Скарпи и др., так и строить семейства матриц.

Показано, что двухуровневые квазиортогональные матрицы Мерсенна обобщают матрицы Адамара, существующие на соседних с ними порядках $4k - 1$. Матрицы Мерсенна являются ядром матриц Адамара при их окаймлении слева и сверху. Эта выявленная в работе связь гарантирует существование матриц Адамара неизвестной ранее структуры «ядро с окаймлением» на всех порядках $4k$, поскольку матрицы Мерсенна, согласно гипотезе Балонина, существуют.

Выделены цепочки взаимосвязанных значениями уровней и структурами квазиортогональных матриц с различными матрицами-предикторами. Приведенные цепочки позволяют вычислять или получать объединением блоков матрицы на различных порядках, используя результаты вычислений в качестве комбинаций ядра матрицы предшественника с каймой или удвоением порядка.

Квазиортогональных матриц больше, чем ортогональных, известных до настоящего времени, что обеспечивает расширение базиса для процессов преобразования изображений.

3 Специальные матрицы и методы их вычисления

3.1 Симметрии в структурах квазиортогональных матриц

В практике применения ортогональных матриц большое значение имеет не только их двухуровневость, но и максимальная простота структуры. В разделе 1 отмечалось, что это определяет, во многом, затраты памяти для хранения матриц или время на их генерацию, если система обработки информации предполагает такой способ получения матриц.

Для примера на рис. 3.1 приведены портреты двух матриц Адамара порядка 12. Первая матрица не имеет выраженной структурной организации, вторая – строго структурирована.

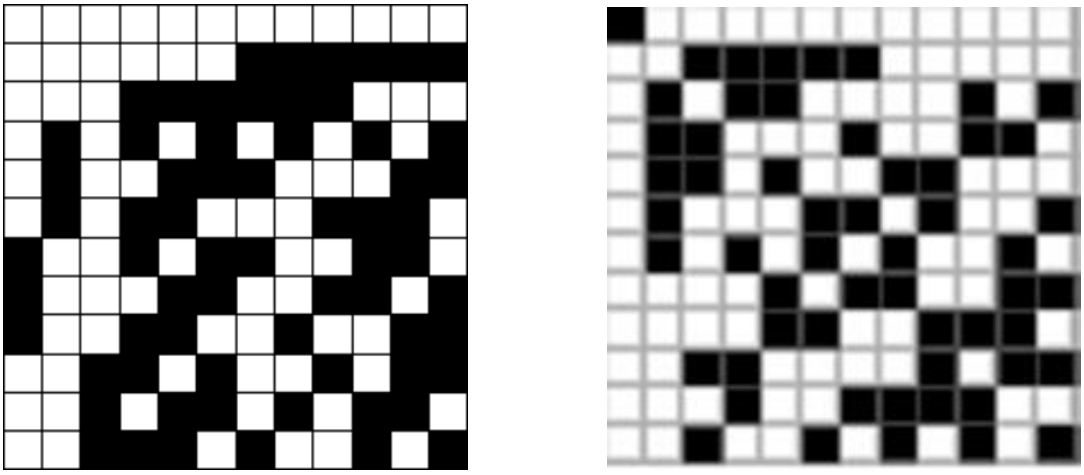


Рисунок 3.1 – Портреты неструктурированной и структурированной матриц Адамара порядка 12

Среди структурированных квазиортогональных матриц, относящихся к простейшим, можно выделить симметричные и симметричные относительно побочной диагонали, обладающие, в отличие от неструктурированных матриц Адамара, рядом полезных свойств.

Название матриц связано с тем, что одинаковые элементы таких матриц расположены симметрично относительно главной или побочной

диагонали. Для хранения таких матриц требуется всего $(n^2 + n)/2$ их элементов.

Отметим, что умножение на симметричные матрицы реализуется достаточно просто [1], поэтому симметрия в целом выгодна как при их хранении, так и при обработке изображений [56].

Циклические ортогональные матрицы представляют собой еще более простую структуру, задаваемую хранимой первой строкой n ее элементов. Все последующие строки получаются последовательным сдвигом предыдущей вправо с размещением вытесняемого элемента слева [1], как это показано ниже на примере матрицы **A.**

$$\mathbf{A} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \ldots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \ldots & a_1 \end{pmatrix}. \qquad (3.1)$$

В общем случае циклическая матрица чаще может быть симметричной относительно побочной диагонали.

В ряде конструкций свойство симметрии используется для получения симметричных матриц элементарным зеркальным отражением элементов относительно центральной осевой линии. Преимущество очевидно: вместо $(n^2 + n)/2$ элементов симметричной матрицы необходимо хранить лишь n элементов развернутого блока, который дает, помимо экономии памяти, еще и экономию при выполнении умножения на него [56].

Ограничение на симметрию циклических матриц не означает, что из них, но больших порядков и не обязательно ортогональных, нельзя построить бициклические матрицы Адамара, получаемые из двух циклических блоков-матриц **A** и **B** в виде

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}, \qquad (3.2)$$

где $\mathbf{B}^T$ – транспонированная матрица **B**, а $-\mathbf{A}^T$ – транспонированная **A** с инверсными знаками элементов.

Для хранения симметричных матриц в бициклической форме необходимо хранить только блоки **A** и **B,** что составит половину количества ее элементов $2(n/2)^2$, а в бициклической форме, даже не принимая во внимание симметрию, потребует только n.

Двухблочную конструкцию обобщает массива Вильямсона из четырех циклических блоков **A**, **B**, **C** и **D** в виде:

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \end{pmatrix} \tag{3.3}$$

Поскольку блоки **A**, **B**, **C** и **D** являются циклическими, то для хранения матрицы Адамара порядка n в этой форме понадобится не более n элементов, по $n/4$ для каждого из четырех блоков. Однако нет гарантии того, что вычисленная таким способом матрица Адамара будет симметричной.

Существующая модификация массива Вильямсона в форме Пропус [84, 85], базирующейся на трехблочных массивах Балонина-Себерри [86], позволяет хранить только по одной строке каждого из блоков **A**, **B** и **D**, что составляет $3n/4$ элементов.

В работах [87, 88] высказана гипотеза, что матрицы Пропус симметричны на всех порядках, на которых существуют. Экспериментально предположение доказано вплоть до порядка 212 [64, 85, 89], при этом вычислены 5 симметричных матриц этого порядка.

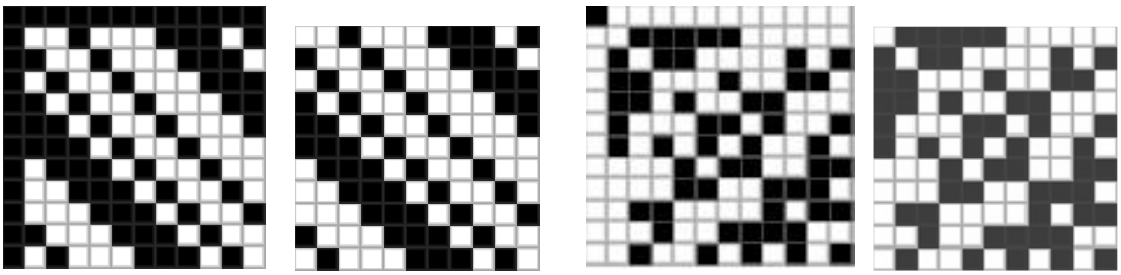
Помимо циклических и бициклических форм блоков симметричных матриц, существует негациклическая форма [90], отличающаяся от циклической лишь операцией инверсии знака размещаемых ниже диагонали элементов.

Подводя итог, отметим, что для хранения несимметричных матриц порядка n, если они не цикличные, потребуется n^2 элементов. Это количество можно вдвое уменьшить (не считая диагонали), опираясь на симметрию. У блочных матриц решающее значение имеет размер симметричной клетки и конфигурация массива клеток. Объем в размере $3n/4$ элементов можно еще уменьшить, учитывая возможную симметрию блоков.

Рассмотренные в разделе 2 двухуровневые матрицы Мерсенна (**M**) нечетных порядков $n = 4t - 1$, имеют, как и матрицы Адамара, два значения элементов. Однако в отличие от пары {1, -1} это пара значений элементов {1, $-b$}. Как было отмечено ранее, именно послабление в виде отступления от целочисленности одного из элементов квазиортогональных матриц позволяет им существовать и на нечетных порядках

В работе [80] сформулирована гипотеза о существовании таких матриц на всех порядках, соседствующих с порядками матриц Адамара $4t$. Однако, в [91] и в разделе 2 показано, что это не простое соседство, а матрицы Мерсенна являются ядром (core) матриц Адамара соответствующей конструкции.

Для получения матрицы Адамара достаточно ядро окаймить слева и сверху, а элементы $-b$ заменить на -1. На рис. 3.2 приведены, в отличие от рис. 1.1, две конструкции матрицы H_{12} , полученные таким образом.



а б

Рисунок 3.2 – Портреты матрицы $\mathbf{H}_{12}$ на основе ядра – циклической матрицы $\mathbf{M}_{11}$ (а), и матрицы $\mathbf{H}_{12}$ на основе ядра – симметричной матрицы $\mathbf{M}_{11}$ (б)

Для матриц Мерсенна характерны не только методы поиска как и для матриц Адамара, но также и разнообразие их конструкций. На рис. 3.3 приведены конструкции матриц $\mathbf{M}_{15}$, найденные двумя характерными для поиска матриц Адамара методами. Первая матрица симметрична, вторая – кососимметрична. Вторая матрица, как и матрица $\mathbf{M}_{11}$ на рис. 3.2, может быть сделана симметричной применением операции флип-инверсии, и в этом ее отличие от бициклической формы матрицы $\mathbf{H}_{20}$.

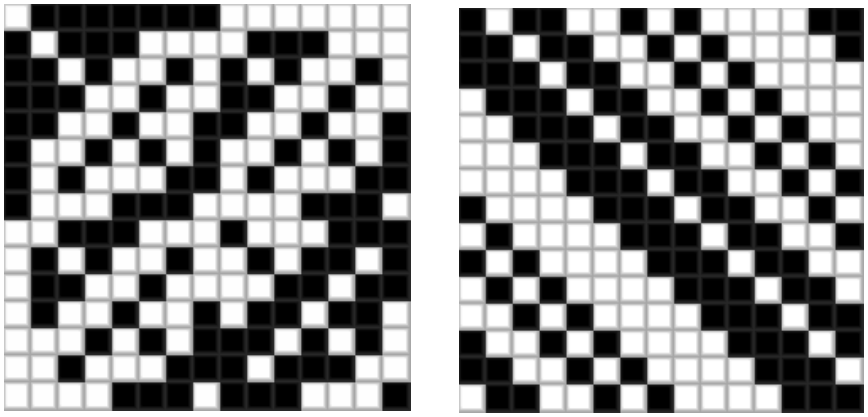


Рисунок 3.3 – Портреты матриц $\mathbf{M}_{15}$, найденных методом Сильвестра (слева) и методом Пэли (справа)

Если порядок матрицы – степень простого числа, то матрица Мерсенна состоит из циклических блоков размеров, равных простому числу.

В работе [92] приведено структурное исключение, подтверждающее общее правило – когда порядок $n = 4t - 1$ равен произведению пар близких простых чисел, матрица Мерсенна будет циклической.

Особый интерес для отдельных задач обработки изображений представляют симметричные конструкции матриц Адамара-Уолша, получаемые из классических матриц Адамара путем упорядочивания столбцов по частоте (по количеству смены знаков их элементов).

Упорядоченные матрицы Адамара-Уолша могут быть получены и из матриц Мерсенна-Уолша [93, 94] путем инвертирования знаков элементов и добавления каймы.

На рис. 3.4 для примера приведен портрет симметричной матрицы Мерсенна-Уолша порядка 31, полученной упорядочиванием матрицы $\mathbf{M}_{31}$.

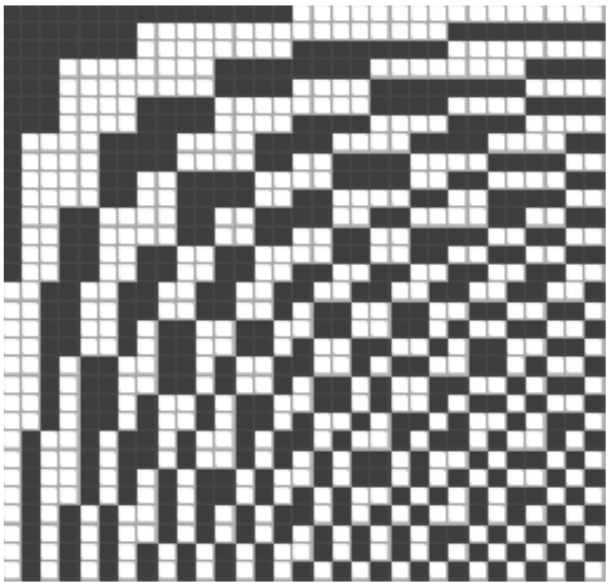


Рисунок 3.4 – Портрет матрицы Мерсенна-Уолша
(взято из статьи [93])

Рассмотренные в настоящем разделе основные виды структурированных и неструктурированных двухуровневых квазиортогональных матриц формируют значительно расширенные семейства, предлагаемые для использования в симметричных алгоритмах обработки изображений при их передаче в распределенных системах на основе IP-сетей [94].

Это дает разработчикам алгоритмов более широкие возможности в выборе наиболее удачной матрицы для обработки конкретных изображений, в том числе изображений нестандартных размеров.

3.2 Границы существования симметричных конструкций

Желание получить матрицу Адамара симметричной конструкции не всегда выполнимо, особенно при использовании переборных или эвристических методов.

Ограничение для циклических ортогональных матриц в виде симметрии (кососимметрии), согласно гипотезе Ризера (Ryser) [95], существенно ограничивает возможность их существования – последняя из циклических симметричных матриц Адамара имеет порядок 4. Очевидно, применение таких матриц весьма ограничено, а вопрос хранения или их вычисления не является для такого порядка принципиальным.

Бициклические матрицы, являясь по конструкции блочно-симметричными, могут одновременно иметь симметричные блоки и быть симметричными в целом. Примеры приведены на рис. 3.5.

Однако в работе [97] автором сформулирована гипотеза, расширяющая гипотезу Райзера о существовании симметричных бициклических матриц Адамара на симметричных блоках порядков, не выше 32. Гипотеза эта проверена и на сегодня имеет подтверждение, изложенное в работах [97, 98].

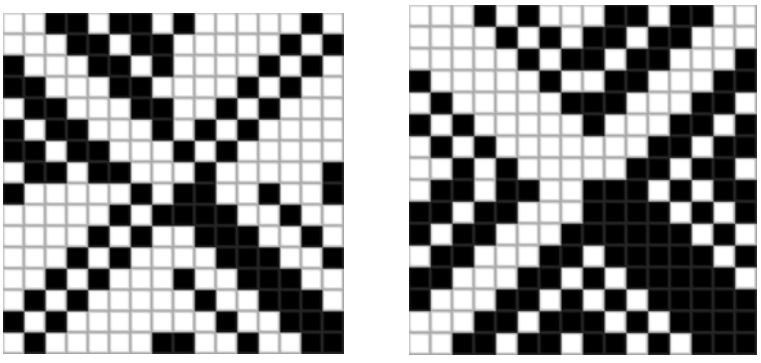


Рисунок 3.5 – Портреты матриц Адамара порядка 16
с симметричными блоками

Особенность симметричных четырехблочных конструкций Вильямсона заключается в том, что они могут базироваться как на четырех симметричных, так и отчасти несимметричных блоках, дающих в результате симметричную матрицу Адамара. Из работы [99] следует, что не существует, например, симметричных матриц порядка 35 для массива Вильямсона, дающих матрицу $\mathbf{H}_{140}$. Однако такая матрица построена на основе одного симметричного и трех несимметричных циклических блоков. Ее портрет приведен на рис. 3.6.

Как отмечалось ранее, при равенстве блоков **B** и **C** симметричная конструкция матрицы Адамара может быть построена на трех фактических блоках **A**, **B** и **D.** Такие матрицы получили название матриц Адамара в форме Пропус (**P**) [84, 100, 101].

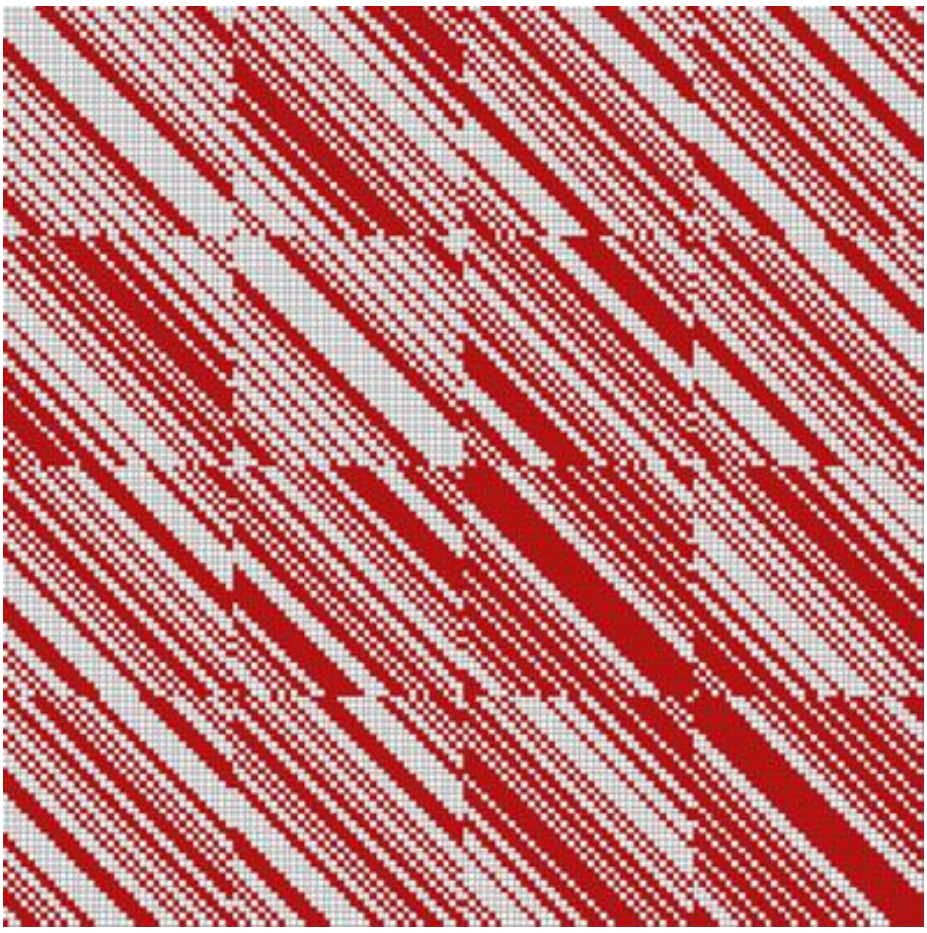


Рисунок 3.6 – Портрет симметричной матрицы $\mathbf{H}_{140}$

Матрицы Пропусы могут быть реализованы в двух конфигурациях $\mathbf{P}_1$ и $\mathbf{P}_2$ [84, 85, 102], представленных как

$$\mathbf{P}_1 = \begin{pmatrix} \mathbf{A} & \mathbf{B}=\mathbf{C} & \mathbf{C}=\mathbf{B} & \mathbf{D} \\ \mathbf{C} & \mathbf{D} & -\mathbf{A} & -\mathbf{B} \\ \mathbf{B} & -\mathbf{A} & -\mathbf{D} & \mathbf{C} \\ \mathbf{D} & -\mathbf{C} & \mathbf{B} & -\mathbf{A} \end{pmatrix},$$

$$\mathbf{P}_2 = \begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ \mathbf{CR} & \mathbf{D}^{\mathrm{T}}\mathbf{R} & -\mathbf{A} & -\mathbf{B}^{\mathrm{T}}\mathbf{R} \\ \mathbf{BR} & -\mathbf{A} & -\mathbf{D}^{\mathrm{T}}\mathbf{R} & \mathbf{C}^{\mathrm{T}}\mathbf{R} \\ \mathbf{DR} & -\mathbf{C}^{\mathrm{T}}\mathbf{R} & \mathbf{B}^{\mathrm{T}}\mathbf{R} & -\mathbf{A} \end{pmatrix}.$$

В отличие от массива Вильямсона, обладающего сходной конфигурацией, новый массив с симметричными блоками или одним симметричным блоком $\mathbf{A}$ в случае $\mathbf{P}_2$ всегда симметричен, что обеспечивается реверсной единичной матрицей $\mathbf{R}$. Примеры таких массивов приведены на рис. 3.7.

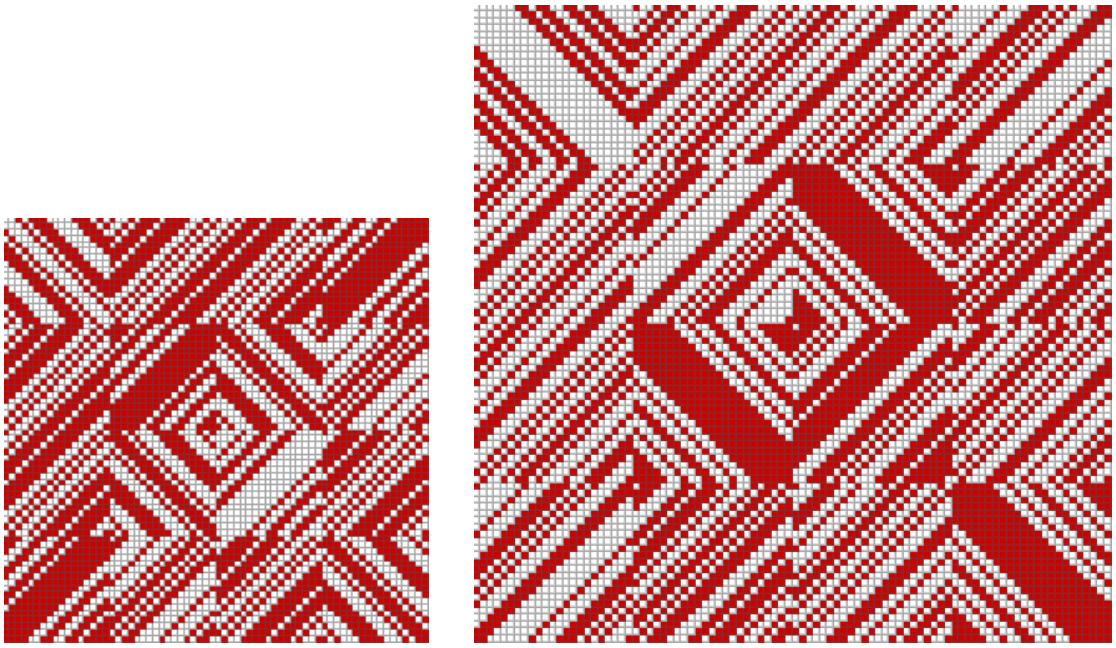


Рисунок 3.7 – Портреты симметричных матриц $\mathbf{H}_{68}$ и $\mathbf{H}_{92}$ в форме Пропус

Таким образом, вычислить симметричную матрицу Адамара возможно на порядках до 32 в бициклической форме, для порядков выше – в форме Пропус [98].

3.3 Использование структурированных специальных матриц в приложениях распределенных систем

Как было отмечено в [19], трафик передаваемого «видео на заказ» в IP-системах удваивается ежегодно. В самом простом случае такие системы представляют собой связанные через структуру коммуникаций сети Интернет два объекта – приемник и передатчик [21].

Ранее было показано, что возможность вычислять квазиортогональные матрицы различных порядков, в том числе и нечетных, обеспечена отходом от классического целочисленного подхода за счет введения иррациональности значений элементов матриц – уровней.

Для рассматриваемых в работе задач на передающей и принимающей сторонах должны быть использованы одинаковые малоуровневые иррациональные матрицы [18, 31, 103]. Иррациональность уровней, во-первых, существенное препятствие для стороннего демаскирования; во-вторых, «…сохранение принципиальной возможности сжатия маскируемой информации, например, адаптацией процедуры фильтрации к структурным особенностям ортогонального базиса. Это способствует неразличимости маскированного и немаскированного видеопотоков в каналах связи». В-третьих, необычная матрица или ключ маскирования в виде вектора перестановки строк и столбцов, неизвестные третьей стороне, способствуют, как показало исследование [104], надежному сокрытию видеоизображения от перехвата и подмены.

Разнообразие порядков специальных симметричных матриц, соответствующих ряду целых чисел вплоть до высоких значений, позволяет выбирать матрицы не только на замену матрицы в алгоритме сжатия, но и адаптировать преобразования к размеру обрабатываемого изображения. Это важно при маскировании изображений произвольных размеров, определяемых во многих IP-камерах функцией «quality box» [105]. Значительное число возможных перестановок строк и столбцов, позволяют одновременно с устранением избыточности в видеоизображении осуществлять его защиту маскированием.

Отдельно стоит отметить класс квазиортогональных матриц, порядки которых пропорциональны размерам кадров видеопоследовательности. При построении этих матриц использована золотая пропорция [83, 106]. Такими являются оригинальные **G**-матрицы «золотого сечения», у которых всего два значения элементов a и g. Однако с учетом знака – матрица четырехуровневая.

Пример такой матрицы порядка 10 в форме бицикла, взятый из [106], приведен ниже.

$$\mathbf{G}_{10} = \begin{pmatrix} g & a & -g & -g & a & -a & a & g & g & a \\ a & g & a & -g & -g & a & -a & a & g & g \\ -g & a & g & a & -g & g & a & -a & a & g \\ -g & -g & a & \mathrm{g} & a & g & g & a & -a & a \\ a & -g & -g & a & g & a & g & g & a & -a \\ -a & a & g & g & a & -g & -a & g & g & -a \\ a & -a & a & g & g & -a & -g & -a & g & g \\ g & a & -a & a & g & g & -a & -g & -a & g \\ g & g & a & -a & a & g & g & -a & -g & -a \\ a & g & g & a & -a & -a & g & g & -a & -g \end{pmatrix}.$$

G-матрицы, как показано в работе [106], «…существуют на порядках имеют порядки $n=10\cdot 2^k$, где k – натуральное число, занимающих особое место в алгоритмах обработки изображений: 10, 20, 40, 80, 160, 320, 640».

Все приведенные отличия квазиортогональных матриц от известных ортогональных, позволяя реализовать гибридную обработку видеокадров при сжатии, существенно усложняют задачу демаскирования кадров видеопотока третьей стороной.

Некоторые дополнительные аргументы в пользу квазиортогональных матриц. Дополнительный аргумент рациональности использования квазиортогональных базисов, построенных на последовательностях чисел [59–61], среди которых матрицы Мерсенна [57, 59] и Мерсенна-Уолша [93], отличает их близость к матрицам Адамара. Алгоритм построения матриц Мерсенна фрактален, и при определенной его реализации вычисляемые матрицы обладают повышенной чувствительностью к изменению разрядной сетки процессора и начальным данным.

Разнообразие начальных условий в методах вычисления квазиортогональных матриц [81, 107] позволяет получать структурированные циклические, бициклические, негациклические, бинегациклические и другие формы матриц [108, 109]. Для примера на рис.3.8 приведены портреты матриц Мерсенна, где слева расположена матрица порядка 19 циклическая симметричная относительно побочной диагонали, справа – матрица порядка 19 неструктурированная симметричная.

Перечисленные формы привычны при поиске ортогональных матриц Адамара на порядках $n=4k$, где k – целое, обладающих глобальным максимумом детерминанта [107]. Однако это могут быть квазиортогональные негациклические матрицы [108, 109], матрицы локального максимума детерминанта на порядках, отличных от адамаровых [5, 110], в том числе

структурированные. Пример двухуровневых структурированных матриц Мерсенна, отсортированных по Уолшу [93] приведен на рис.3.9.

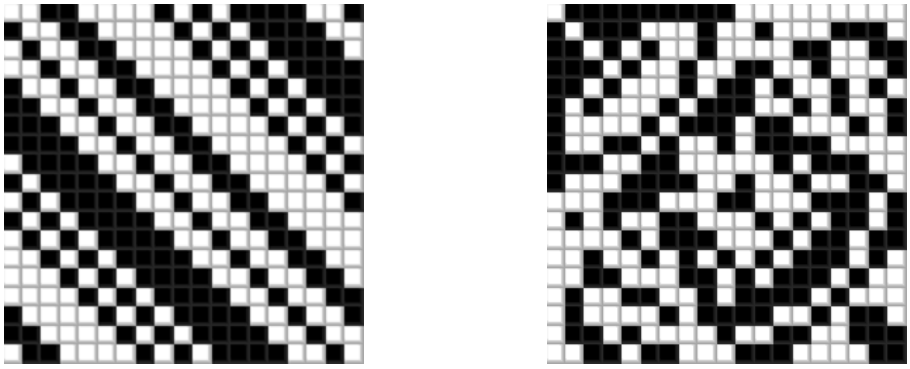


Рисунок 3.8 – Портреты матриц Мерсенна

При реализации процедуры маскирования или гибридной обработки видеокадров в системах встраиваемого класса критичными параметрами являются объем хранимой информации и свободная вычислительная мощность процессора. В этом смысле заранее структурированные квазиортогональные матрицы наиболее предпочтительны, поскольку для их хранения, в зависимости от полученной формы матрицы, может использоваться от $n^2/2$ до n ячеек памяти вместо n^2.

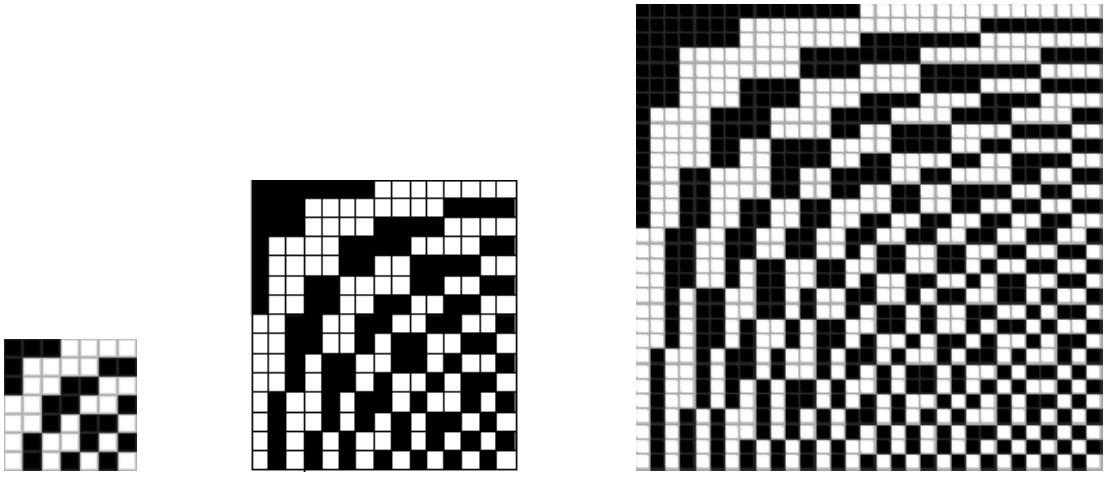


Рисунок 3.9 – Портреты структурированных матриц Мерсенна-Уолша порядков 7, 15 и 31 (взята из [93])

При использовании уникальных, например, **G**-матриц «золотого сечения» на передающей и принимающей сторонах могут храниться лишь ключи, определяемые порядком таких матрицы.

Задачи маскирования видеоизображений, а, следовательно, и демаскирования их третьей стороной, может быть значительно усложнена тем, «…что матрица квазиортогонального преобразования может не вычисляться заранее, а являться результатом работы алгоритма» [62]. В этом случае по открытому каналу в качестве ключа передаются только настройки для ее вычисления. Не менее важны при этом и существующие рекурсивные процедуры увеличения порядка матриц, обычные для адамаровых матриц [81].

3.4 Метод поиска бициклических симметричных матриц Адамара

Известные алгоритмы позволяют вычислять матрицы Адамара порядков общей последовательности $4t$, но различаемые по внешнему виду – их «портретам» [6, 7], на которых два значения (уровня) элементов, как и ранее, представлены клетками разного цвета.

Для поиска матриц Адамара сегодня известны классические методы, приведенные в разделе 1 и дающие матрицы увеличенного порядка на основе существующих матриц. Там же приведены проблемные (невычислимые) порядки, определяемые логикой этих методов.

При реализации классических методов симметричность результирующих матриц не гарантируется в силу того, что исходные матрицы (предикторы) не симметричны.

Поиск симметричных матриц – задача сложная, требующая отдельного подхода. Например, ортогональную матрицу порядка 100 найти практически невозможно [5, 111].

Для эффективного поиска матриц полезно ограничивать как область назначаемых параметров, опираясь на какие-либо закономерности, но и структуру блоков [90, 112].

Можно задать циклическую структуру, образованную сдвигом строки (моноциклы). Она просто вычислима, но, согласно гипотезе Райзера, циклических ортогональных матриц с двумя значениями элементов не существуют выше порядка 4. Циклические матрицы слишком просты, чтобы существовать на больших порядках. И такой подход не годится.

Заметно лучшие результаты дает парная конструкция с циклическими блоками **A**, **B** (бициклические матрицы), т. к. бициклов существует много [97], но поиск их значительно усложнен [113].

Структура бициклической матрицы Адамара представлена формулой (1.1), которая в явном виде просматривается на представленном на рис. 3.10 портрете.

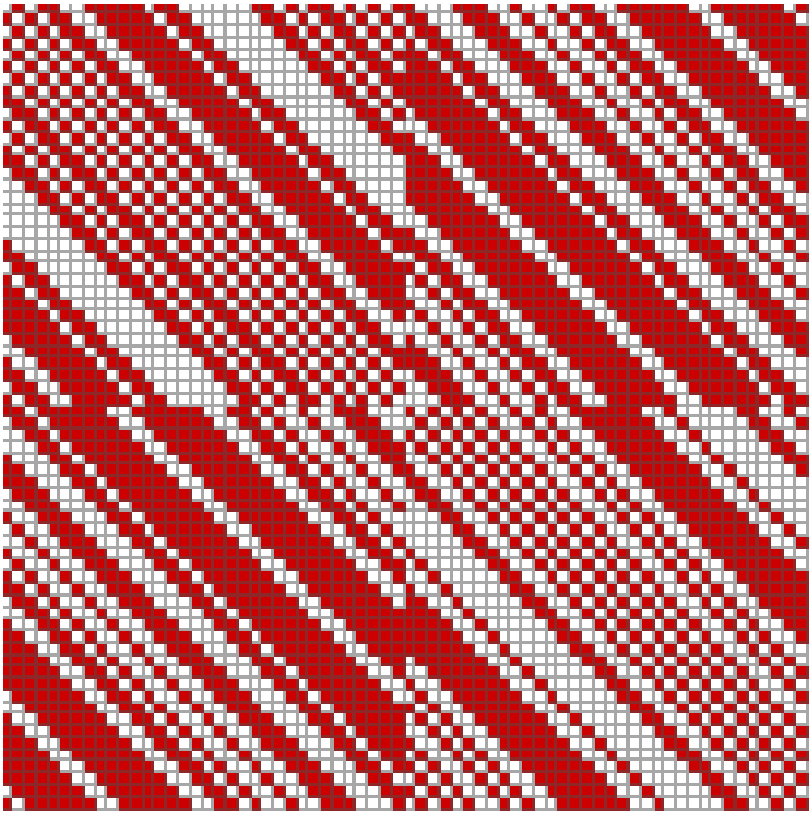


Рисунок 3.10 – Бициклическая матрица Адамара порядка 68

Как видно, здесь бицикл Адамара состоит из двух моноциклов, иными словами – блоки **A** и **B** состоят из циклически смещаемых первых строк **a** и **b** каждого блока соответственно.

Поиск матриц методом перекрестных ссылок. Перед поиском ортогональных матриц в предлагаемом в диссертации методе предусмотрено указание количества отрицательных элементов в строках двух блоков [113].

В табл. 3.1, например, показана зависимость числа отрицательных элементов в левом (k_1) и правом (k_2) плечах [113] в зависимости от порядка матрицы n. Такое предварительное задание ускоряет процесс поиска.

Наиболее эффективный метод, помогающий искать очень редкие матрицы, связан с таблицей перекрестных ссылок [114]. Каждый левый элемент такой таблицы представляет собой сгенерированное компьютером плечо **A** матрицы Адамара, справа расположены элементы, представляющие правое плечо **B**.

Таблица 3.1. Количество отрицательных элементов для матриц

Порядок матрицы n	Количество отрицательных элементов	
	k_1	k_2
8	1	1
16	4	2
20	4	3
32	6	6
40	9	7
52	11	10
64	16	12
68	16	13
80	18	16
100	22	21

Каждый левый элемент сравнивается с правым на предмет возможности образования с ним ортогональной пары, дающей нужную

матрицу. Если такая пара образуется, то перебор заканчивается. Иначе таблица должна быть пересчитана для продолжения поиска.

Генератор элементов 1 и –1 векторов-строк **a** и **b** необходимо настраивать так, чтобы сгенерированные строки содержали заранее известные количества k_1 и k_2 отрицательных значений [62, 70].

Условие ортогональности $\mathbf{H}^T\mathbf{H}=\mathbf{H}\mathbf{H}^T=n\mathbf{I}$ сводится к выполнению уравнения для блоков $\mathbf{A}\mathbf{A}^T+\mathbf{B}\mathbf{B}^T=n\mathbf{I}$. Его можно упростить до выражения $\mathbf{A}\mathbf{a}+\mathbf{B}\mathbf{b}=ne$, где $e = (1, 0, 0, \ldots, 0)^T$, а правые множители **a** и **b** – транспонированные вектор-строки размера $v=n/2$.

Запоминанию подлежат не только сами последовательности, но и произведения **Aa** и **Bb**, поскольку условие ортогональности выражено через них, и необходимую пару без них не сравнить.

Заметим, что произведение циклического блока на вектор легко вычислить без явного построения блока, поскольку элементы каждой его строки повторяются со смещением, которое пропорционально номеру строки.

В табл. 3.2 показан пример последовательностей **a**, **b** и их произведений на циклические матрицы.

Поскольку $\mathbf{H}^T\mathbf{H}$ симметрично, то достаточно фиксировать равенство усеченных произведений [**Aa**]=–[**Bb**], где скобками выделена половина всех элементов кроме первого, который не отличается знаком и равен v. Очевидно, компьютерный поиск бициклов, если не принимать во внимание всегда возможную оптимизацию детерминанта, сводится к составлению таблицы строк **a**, **b** совместно с отмеченными усеченными произведениями [**Aa**], [**Bb**] [115–117].

Таблица 3.2. Примеры последовательностей и их произведений

n	**a**	**Aa**	**Bb**	**b**
4	(–1 1)	(2 | –2)	(2 | 2)	(1 1)
8	(–1 1 1 1)	(4 | 0 0 0)	(4| 0 0 0)	(–1 1 1 1)
16	...	(8 | ...)	(8 | ...)	...

Таблица в *ms*=1000 строк допускает 1000×1000 = 1000000 попарных сравнений усеченных последовательностей [**Aa**] и –[**Bb**]. В настоящее время таким образом разрешимы порядки 2, 4, 8, 16, 20, 32, 40, 52, 64, 68, 80, 100. Однако, сложно находится уже бициклическая матрица порядка 68. К вычислению матрицы порядка 80 есть подход через меньшие порядки, но он мало актуален, а порядок 100 относится к числу сложно вычисляемых. Минимальный известный порядок пока не найденной бициклической матрицы – 180.

Компьютерный поиск бициклов. Алгоритм работы программ поиска бициклических матриц на основе перекрестных ссылок [118, 119] состоит в реализации четырех этапов [120].

Этап 1. Резервирование памяти для массивов.

Этап 2. Формирование колонки векторов **a** и **b** случайной генерацией последовательности из элементов 1 и –1. Если количество элементов –1 в ней совпадает с коэффициентом k_1, она вставляется в список для последовательностей **a**; если совпадает с коэффициентом k_2 – в список для последовательностей **b**; если не совпадает ни с тем, ни с другим коэффициентами – последовательность отбрасывается. Повторение осуществляется до полного заполнения зарезервированной для обоих векторов памяти.

Этап 3. Для каждого элемента списка вычисляется произведение исходного вектора (**a** или **b**) на полученную из него циклическую матрицу (**A** или **B**) и полученные усеченные произведения также запоминаются в списке.

Этап 4. После построения списков в двойном цикле перебираются попарно все элементы. Если сумма сохраненных в таблице произведений [**Aa]** и [**B*b***] дает нулевой вектор, значит вектор-строки **a** и **b** формируют бициклическую ортогональную матрицу.

Описывая особенности компьютерного поиска бициклических матриц обратим внимание на то, что резервирование памяти компьютера рассчитано

обычно на некоторый фиксированный объем данных и прибавление строк в наращиваемую большую таблицу вызывает их потерю. Компилятор не проверяет эту ситуацию, поскольку до использования размер таблицы не задан.

Предлагаемый выход состоит в том, чтобы перед размещением очередной порции данных обращаться к операционной системе с тем, чтобы она расширила, если нужно, размер выделяемой области.

В Delfi Pascal за выделение дополнительной памяти отвечает оператор GetMem(), с указанием дополнительно требуемого объема, как показано на рис. 3.11 [113, 120].

Этот момент слабо документируется в самой системе программирования, поскольку инструмент создавался задолго до возникновения современных компьютеров с их расширенными возможностями.

Интерфейс программы, реализующей метод перекрестных ссылок, и пример найденной этой программой матрицы порядка 64 показан на рис. 3.12.

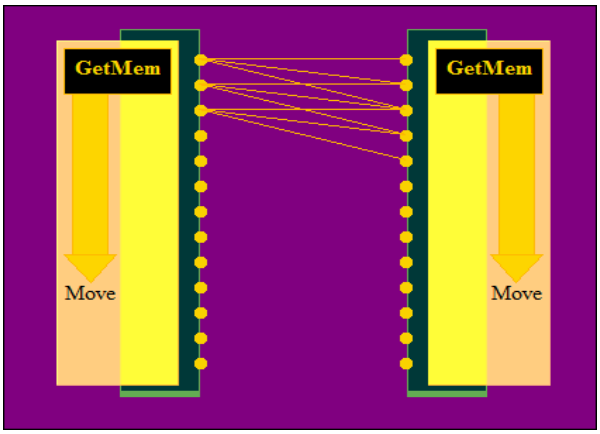


Рисунок 3.11 – Иллюстрация расширения зоны поиска для последовательностей

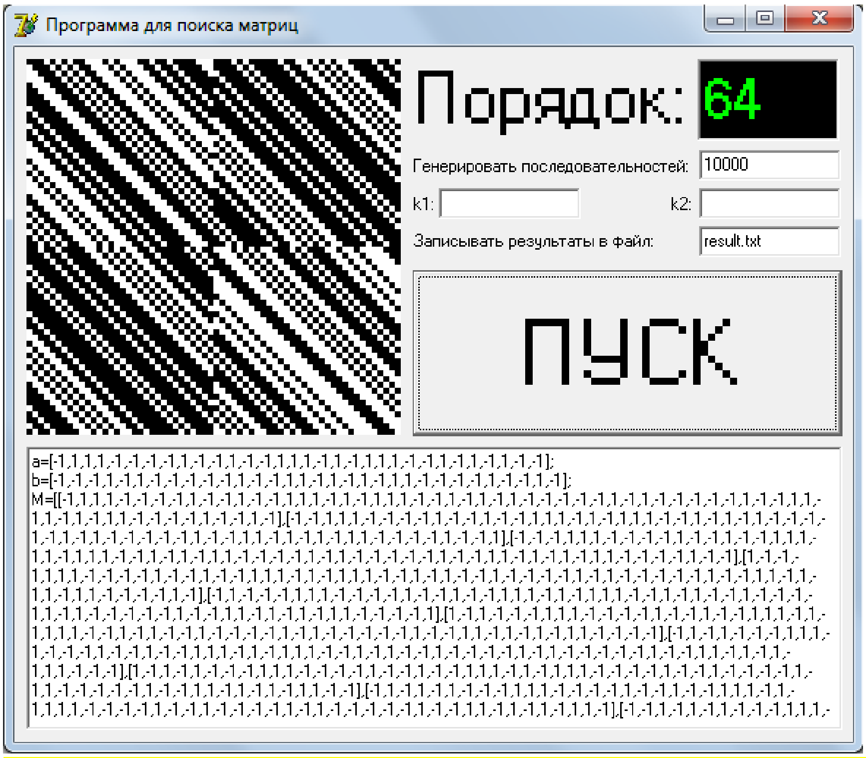


Рисунок 3.12 – Интерфейс программы и пример найденной ею матрицы порядка64

Оптимизация алгоритма поиска матриц. Скорость алгоритма поиска бициклической матрицы и требуемый объем памяти в большой степени зависят от типа представления векторов **a** и **b**, состоящих из значений элементов 1 и –1. При этом количество элементов, имеющих значение -1, заранее определено. При представлении векторов в виде двоичных чисел, считая единицу нулем, а минус единицу единицей, объем памяти для хранения одного вектора будет равен восьми байтам даже для порядка бициклической матрицы $2n = 100$.

Таким образом, числа a и b будут хранить информацию о расположении элементов со значениями 1 и –1 в векторах. Информация о размере n вектора должна храниться отдельно.

Представление векторов в виде целых двоичных чисел не только сокращает объем памяти, но и позволяет упорядочить множество векторов

[120]: у каждого вектора появляется свой номер, который является десятичным, полученным по двоичному преставлению вектора. Номера располагаются в порядке возрастания, но шаг между соседними номерами не является величиной постоянной. Опорными точками здесь являются те номера, в двоичной записи которых единицы расположены подряд друг за другом.

Например, пусть вектор имеет размер n = 8. При этом количество k элементов – 1 в нем фиксировано и равно 3. Начальная опорная точка будет иметь вид вектора

0	0	0	0	0	1	1	1

Следующая опорная точка получается сдвигом всех единиц на одну позицию влево:

0	0	0	0	1	1	1	0

Переход между соседними опорными точками будем называть октавой. Она соответствует удвоению номера вектора. Каждая опорная точка вычисляется по формуле $O_k^p = (2^k - 1)\,2^p$, где число k есть число единиц в двоичном представлении вектора, а число p – нижний номер октавы.

Число p может изменяться в пределах от нуля до значения $n - k$. Количество номеров векторов внутри октавы не постоянно – оно зависит как от числа единиц в преставлении вектора, так и от нижнего номера p. Чем выше номер p, тем больше мощность октавы – больше номеров располагается внутри нее. Общее количество номеров векторов при заданных числах n и k – это число сочетаний

$$V = C_n^k = \frac{n!}{k!(n-k)!}.$$

Число V назовем мощностью вектора. Так как в формировании бициклической матрицы участвуют два вектора одинакового размера, то при

поиске правильных решений учитываются все комбинации номеров векторов. Отсюда возникает понятие мощности поля решений, представимого как:

$$P=V_{\mathbf{a}}V_{\mathbf{b}}\ .$$

Мощность поля решений – это число всевозможных комбинаций векторов **a** и **b**. Естественно, оно равно произведению мощностей векторов. Если последовательность номеров векторов делится на октавы, то поле решений можно разделить на квадраты октав. Каждый квадрат «весит» на определенное число комбинаций номеров векторов. Мощности квадратов распределены неравномерно по всему полю. Наибольшей мощностью обладают квадраты с высокими номерами октав (рис. 3.13).

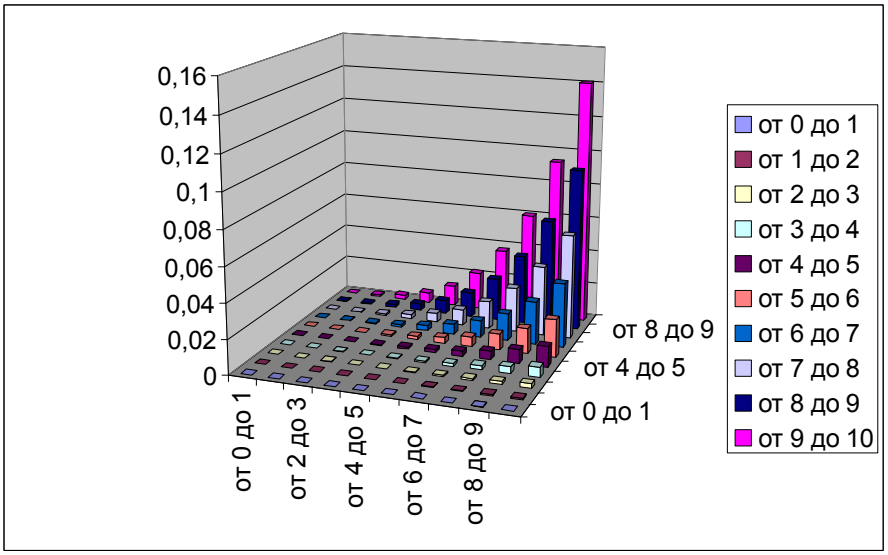


Рисунок 3.13 – Распределение мощностей квадратов.

На рис. 3.14 показан принт-скрин результатов вычисления относительного распределения мощностей квадратов по всему полю решений для размера бициклической матрицы $2n$=32. По вертикали на рисунке отложено отношение мощности квадрата ко всей мощности поля решений.

Экспериментально было установлено, что решения локализуются именно в квадратах октав. В квадрате может быть либо одно «правильное» сочетание, приводящее к построению бициклической матрицы, либо решений вообще нет.

октавы вектора B	октавы вектора A										
		от 0 до 1	от 1 до 2	от 2 до 3	от 3 до 4	от 4 до 5	от 5 до 6	от 6 до 7	от 7 до 8	от 8 до 9	от 9 до 10	
	от 0 до 1	5,614E-07	1,965E-06	5,24E-06	1,179E-05	2,358E-05	4,323E-05	7,41E-05	0,0001204	0,0001873	0,00028106	6
	от 1 до 2	1,965E-06	6,877E-06	1,834E-05	4,126E-05	8,252E-05	0,0001513	0,0002594	0,0004215	0,0006556	0,00098372	21
	от 2 до 3	5,24E-06	1,834E-05	4,89E-05	0,00011	0,0002201	0,0004034	0,0006916	0,0011239	0,0017483	0,00262325	56
	от 3 до 4	1,179E-05	4,126E-05	0,00011	0,0002476	0,0004951	0,0009077	0,0015561	0,0025287	0,0039336	0,00590231	126
	от 4 до 5	2,358E-05	8,252E-05	0,0002201	0,0004951	0,0009903	0,0018155	0,0031123	0,0050574	0,0078671	0,01180463	252
	от 5 до 6	4,323E-05	0,0001513	0,0004034	0,0009077	0,0018155	0,0033284	0,0057058	0,009272	0,0144231	0,02164182	462
	от 6 до 7	7,41E-05	0,0002594	0,0006916	0,0015561	0,0031123	0,0057058	0,0097814	0,0158948	0,0247253	0,03710026	792
	от 7 до 8	0,0001204	0,0004215	0,0011239	0,0025287	0,0050574	0,009272	0,0158948	0,0258291	0,0401786	0,06028793	1287
	от 8 до 9	0,0001873	0,0006556	0,0017483	0,0039336	0,0078671	0,0144231	0,0247253	0,0401786	0,0625	0,09378122	2002
	от 9 до 10	0,0002811	0,0009837	0,0026233	0,0059023	0,0118046	0,0216418	0,0371003	0,0602879	0,0937812	0,14071867	3004
		6	21	56	126	252	462	792	1287	2002	3004	

Рисунок 3.14 – Распределение мощностей для порядка $2n = 32$

Естественно было бы предположить, что наличие «правильного решения» зависит от мощности квадрата, то есть от числа комбинаций номеров векторов в нем. Однако это не совсем так. Общая тенденция именно такова, однако, граница между «правильными» квадратами и квадратами, где нет решений, проходит не по линии равных мощностей квадратов. Она, скорее, определяется произведением нижних номеров октав для данного квадрата. Но даже и эта зависимость не является строгой.

Использование двоичного представления базовых векторов **a** и **b** позволяет сократить количество используемой в алгоритме поиска памяти, упорядочить векторы по номерам. Отпадает необходимость формирования вектора случайным образом, что занимает довольно длительное время. Отметим по пунктам особенности, вносимые оптимизацией и сформулированные в работе [113].

1. Порядок следования номеров векторов логарифмический по

степеням двойки. Базовыми точками можно считать те номера, где единицы двоичного представления расположены друг за другом. Расстояние между двумя ближайшими точками – октава.

2. Формирование бициклической матрицы на базе двух векторов приводит, таким образом, к понятию поля номеров векторов или поля решений.

3. Поле решений делится на октавные квадраты, мощности которых неравномерны. В каждом квадрате либо есть «правильное решение», либо нет никакого решения. «Правильные решения» тяготеют к квадратам с большими номерами октав.

4. Граница между «правильными» квадратами и квадратами, где нет решений, приближенно определяется произведениями нижних номеров октав по векторам **a** и **b**.

3.5 Выводы по разделу 3

Специальные квазиортогональные матрицы симметричных структур имеют различные конструкции, но все они имею преимущества при хранении или их генерации при использовании в телекоммуникационных системах.

Специальные квазиортогональные матрицы симметричных структур в форме Пропус всегда существуют (на всех их порядках). Они всегда вычислимы.

Бициклические матрицы имеют границу симметрии на порядке 32. Однако бициклические специальные матрицы не симметричной структуры границы не имеют.

Предложенный метод вычисления бициклических матриц обеспечивает на основе накопленных последовательностей быстрое нахождение квазиортогональных матриц.

Предлагаемый алгоритм поиска бициклических матриц гарантирует поиск симметричных матриц на основе блочной схемы Вильямсона с двумя равными блоками – массива Балонина-Себерри.

4 Практические применения специальных матриц в обработке изображений и помехоустойчивом кодировании

4.1 Маскирование цифровой визуальной информации

В разделе 1 отмечалось, что перспективный подход в защите цифровой визуальной информации от несанкционированного доступа в открытых коммуникациях заключается в использовании методов их двустороннего цифрового матричного маскирования на передающей стороне с последующим восстановлением (демаскированием) – на приемной.

Действительно, на протяжении уже 10 последних лет термин «маскирование» используется в области защиты от несанкционированного доступа к цифровой визуальной информации, имеющей малое время актуальности [14, 23, 31].

Здесь цифровая визуальная информация – это сохранённые и передаваемые статические изображения (данные, представляемые в виде двумерного массива значений яркости) или видеоизображения (последовательно сменяющие друг друга во времени статические кадры видеопоследовательности).

Приведем уточненные определения терминов, приведенные в работе [31], которыми будем оперировать далее.

Определение 21. Матричное маскирование – «…вычислительная процедура преобразования цифровых изображений с использованием матричных операций, разрушающая его до вида, воспринимаемого визуально как шум».

Определение 22. Матричное демаскирование – «… вычислительная процедура обратного преобразования с использованием матричных операций, восстанавливающая исходное цифровое изображение из маскированного».

Хотя к матричным методам маскирования относятся методы, изложенные в работах [14, 54, 55] и др., но наиболее перспективным в смысле простоты реализации и обеспечения качества маскирования, является метод двустороннего матричного маскирования, описанный и исследованный в работах [18, 54, 55].

Основной формат маскируемых цифровых изображений – Bitmap Picture (BMP) используемый для хранения растровых изображений, получаемых непосредственно с видеоматрицы. Формат файла BMP способен хранить цифровые изображения произвольной ширины, высоты и разрешения. Он непосредственно хранит значения пикселей изображений с переменной глубиной цвета, полученных с матрицы чувствительных элементов.

В настоящем разделе будут приведены результаты преобразований изображений в градации серого. Маскирование цветных изображений выполняется отдельно над каждой составляющей цифрового представления изображения. Восстановление выполняется аналогично в обратном порядке ввиду симметричности преобразования. Пример оригинального черно-белого изображения и результата его «идеального» маскирования (данные в коммуникационном канале) приведен на рис. 4.1, взятом из [121].

В качестве маскирующих матриц, очевидно, могут быть использованы не только [27] рассматриваемые в диссертации квазиортогональные матрицы, но и другие [122], в том числе, например, жакетные матрицы [123, 124], построенные на основе матриц Адамара [125], либо дискретное вейвлет-преобразование [126]. Однако анализ показывает либо ограниченное число таких матриц, либо их многоуровневость – элементы матриц имеют более двух значений.

Дополнительный аргумент рациональности использования семейств специальных квазиортогональных матриц, построенных на последовательностях чисел [56, 78, 80, 91, 103], среди которых матрицы

Мерсенна [57, 59] и Мерсенна-Уолша [93,94], отличает их близость к матрицам Адамара.

Рисунок 4.1 – Оригинальное и «идеально» маскированное изображения

Алгоритм построения матриц Мерсенна фрактален, и при определенной его реализации вычисляемые матрицы обладают повышенной чувствительностью к изменению разрядной сетки процессора и начальным данным, что существенно затрудняет их поиск третьей стороной [18, 27].

Задача демаскирования третьей стороной может быть значительно усложнена тем, что матрица квазиортогонального преобразования может не вычисляться заранее, а являться результатом работы алгоритма [27]. В этом случае по открытому каналу в качестве ключа передаются настройки для программы ее вычисления. Примерами таких программ являются [127 – 130] и специальное программное обеспечение [131, 132], включающее их.

4.2 Метод двустороннего матричного маскирования и его особые изображения

Классический стрип-метод [9] предполагает двустороннее кронекерово умножение (×) на ортогональные матрицы **A** и **B** вида:

$$\mathbf{Y} = \mathbf{A}\times\mathbf{X}\times\mathbf{B}.$$

В предположении, что максимальный по модулю элемент таких матриц должен быть минимальным, а именно это приводит к равномерному «размазыванию» амплитуды помехи по изображению [9, 17], в качестве матриц выбираются нормированные матрицы Адамара с элементами {1, −1} или матрицы Белевича с элементами {0, 1, −1} [17]. Однако использование кронекерова умножения, приводящего к увеличению объема преобразованного (маскированного) изображения пропорционально размеру матриц **A** и **B**, определяет не высокий порядок таких матриц для маскирования – 4 или 8.

Метод двустороннего матричного маскирования [18], разработанный с участием автора диссертации [27, 133], построенный на основе стрип-метода, реализуется в отличном от стрип-метода виде (1.1), а именно с квазиортогональными матрицами Мерсенна **M**:

$$\mathbf{Y} = \mathbf{M}^{\mathrm{T}} \times \mathbf{X} \times \mathbf{M}.$$

Вычислительные эксперименты с различными тестовыми изображениями и квазиортогональными матрицами показали, что простое матричное умножение, заменяющее в стрип-методе кронекерово, вполне приводит к более лучшим результатам [18, 27] и при этом могут быть использованы матрицы более высоких порядков, что не «утяжеляет» цифровое маскированное изображение. В диссертационной работе максимальный порядок матрицы Мерсенна – 31.

Поскольку целью маскирования, в отличие от стрип-метода, является сокрытие изображения, а не борьба с импульсными помехами, то в данной диссертационной работе предлагается модернизировать метод маскирования [18], отказавшись полностью от идеи разрезания на полоски. При этом заменяется не только кронекерово умножение на обычное матричное умножение справа и слева, но и используется широкий набор маскирующих матриц, условно обозначаемых как **G** в виде:

$$\mathbf{Y} = \mathbf{G}^{\mathrm{T}}\mathbf{X}\mathbf{G}.$$

При этом возникает ряд вопросов, относящихся к изображениям (их фрагментам), которые инвариантны к такому преобразованию [133, 134].

При реализации метода исходное изображение разбивается на N одинаковых матриц $\mathbf{X}$ размера $n \times n$, равного размеру матрицы маскирования.

Определение 23. Изображения, инвариантные к преобразованию маскирования и переводимые им в то же изображение с точностью до постоянного множителя называются особыми (корневыми).

Поставим задачу найти изображения, которые инвариантны к преобразованию маскирования и для которых выполняется условие $\mathbf{G}^{\mathrm{T}}\mathbf{X}\mathbf{G} = \lambda\mathbf{X}$ **[**133, 134**].** Здесь число λ – называется соответствующим особым (корневым) числом.

Иными словами, «…если исходное изображение совпадет с особым изображением используемого преобразования, то маскированное изображение совпадет с исходным изображением и эффект маскирования не будет достигнут» [133].

В работе [133] показано, что «…матрицы $\mathbf{G}$ с собственными значениями $|\lambda| = 1$ не усиливают изображения. При умножении на $\mathbf{G}$ слева поиск особых изображений сводится к задаче определения перестановочных друг с другом матриц $\mathbf{XG} = \mathbf{GX}$ (или $\mathbf{GM} = -\mathbf{GX}$)».

Из линейной алгебры [1, 2] известно, что «…матрицы перестановочны (коммутируемы), если они построены на одинаковом наборе собственных векторов. Для симметричных матриц $\mathbf{G}$ собственные числа вещественны, а собственные векторы – ортогональны». В частности, коммутируема сама с собой матрица $\mathbf{X} = \mathbf{G}$, поскольку она, безусловно, построена на том же наборе собственных векторов, что и преобразующая матрица, и $\mathbf{G}^{\mathrm{T}}\mathbf{X} = \mathbf{I}$ является единичной матицей.

Иными словами, и это показано в работе [133], «…наиболее беззащитны при маскировании изображения, похожие на преобразующую матрицу, и для успешного маскирования ей самой выгодно выглядеть хаотичной. Это качество разделяют между собой все матрицы семейства Мерсенна».

Каноническое разложение нормированной матрицы **G** на матрицу собственных векторов **V** и диагональную матрицу собственных значений имеет вид $\mathbf{G}=\mathbf{VDV}^{-1}$. Собственные значения ортогональных матриц равны 1 или –1.

В работе [133] показано, что умножение на матрицу **G** можно рассматривать как:

– умножение на ортогональную матрицу $\mathbf{V}^{-1}$ (поворот изображения);

– собственно кодирование при помощи знакопеременной матрицы **D** = diag(1, –1, …, 1);

– обратный поворот **V**.

Особое изображение индифферентно к этому процессу, если формируется (частично) инверсными операциями: обратным поворотом, любой диагональной матрицей **D*** и поворотом. При двустороннем преобразовании матрица **DD*D** = **D***, т.е. не меняется. Отсюда следует алгоритм, позволяющий получить особые изображения, состоящий в вариации матрицы собственных чисел квазиортогональной матрицы **G** и ее реконструкции в виде $\mathbf{P}^* = \mathbf{VD}^*\mathbf{V}^{-1}$ [133, 134].

Пример. Для маскирования фрагментов **X** изображения **P** используются матрицы Мерсенна порядков 7, 15 и 31, портреты которых приведены в разделе 2 на рис. 2.5 и на рис. 4.2.

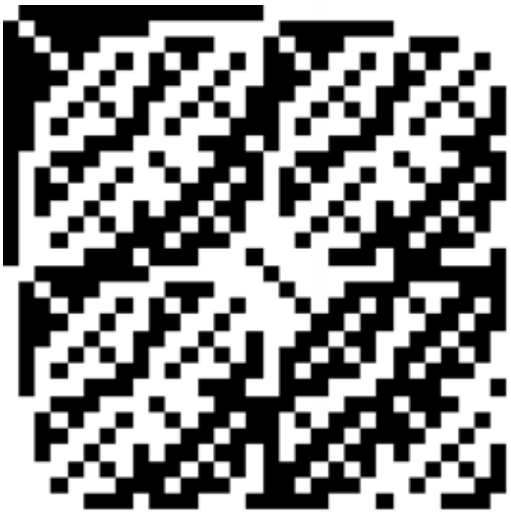


Рисунок 4.2 – Портер матрицы Мерсенна порядка 31

На рис. 4.3 – 4.5 приведены особые изображения для указанных матриц, визуализированные в формате BMP.

В отличие от ранее демонстрированных портретов матриц при их анализе с условно представленными элементами матриц цветными или полутоновыми квадратами [134], на указанных рисунках (и далее) представлены реальные визуализации изображений матриц, на которых квадраты соответствуют пикселам особых изображений.

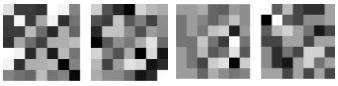


Рисунок 4.3 – Особые изображения для матрицы Мерсенна порядка 7

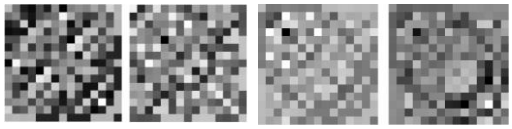


Рисунок 4.4 – Особые изображения для матрицы Мерсенна порядка 15

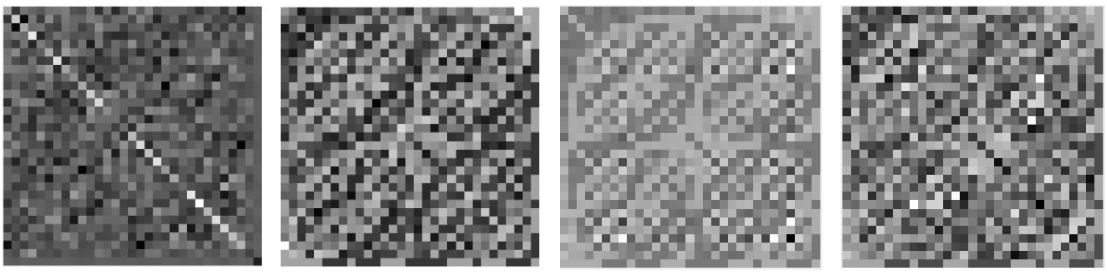


Рисунок 4.5 – Особые изображения для
матрицы Мерсенна порядка 31

Пример. Для маскирования фрагментов **X** изображения **P** используются матрицы Мерсенна-Уолша тех же порядков 7, 15 и 31, портреты которых приведены на рис. 4.6.

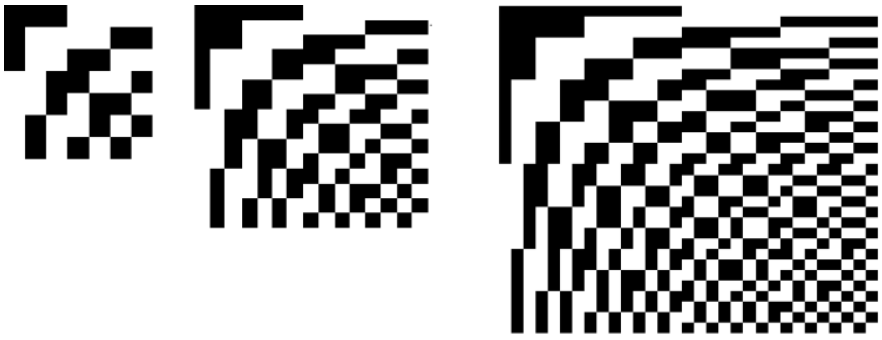


Рисунок 4.6 – Портреты матриц Мерсенна-Уолша

На рис. 4.7 – 4.9 приведены особые изображения для указанных матриц, визуализированные в формате BMP.

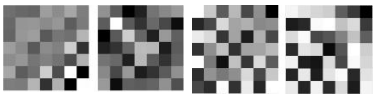


Рисунок 4.7 – Особые изображения для матрицы
Мерсенна-Уолша порядка 7

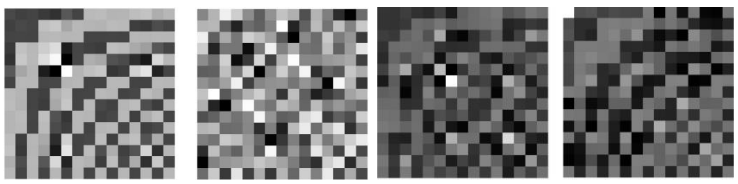


Рисунок 4.8 – Особые изображения для матрицы
Мерсенна-Уолша порядка15

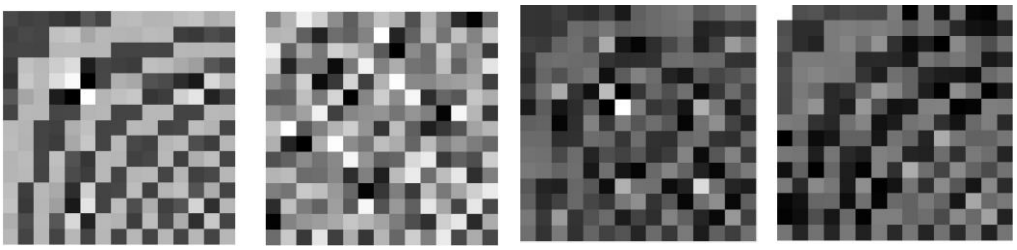


Рисунок 4.9 – Особые изображения для матрицы
Мерсенна-Уолша порядка 31

Пример. Для маскирования фрагментов **X** изображения **P** используются матрицы Ферма порядков 3, 5, 17 и 37, портреты которых приведены на рис. 4.10.

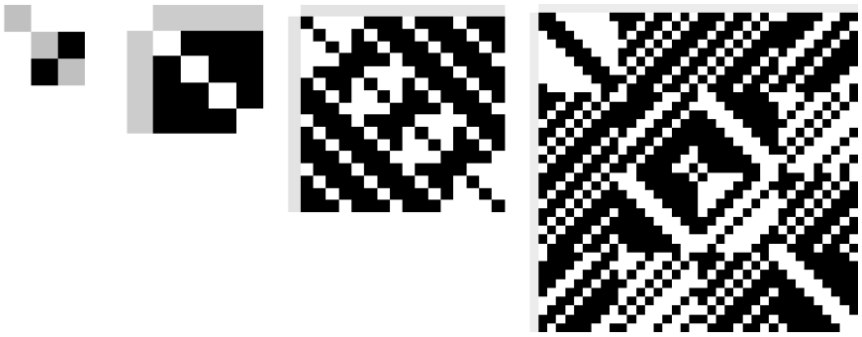


Рисунок 4.10 – Портреты матриц Ферма порядков 3, 5, 17 и 37

Особые изображения, визуализированные в формате BMP, для приведенных матриц Ферма представлены на рис. 4.11 – 4.14 соответственно.

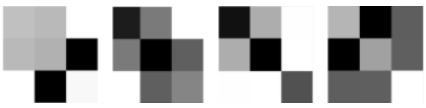


Рисунок 4.11 – Особые изображения для матрицы $\mathbf{F}_3$

Рисунок 4.12 – Особые изображения для матрицы $\mathbf{F}_5$

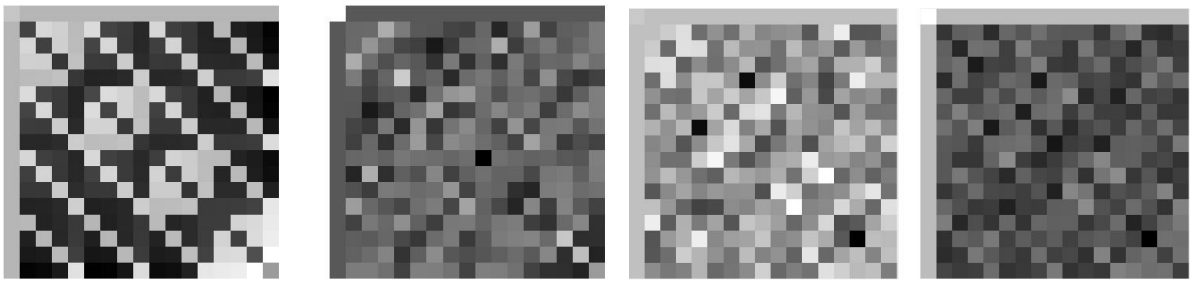


Рисунок 4.13 – Особые изображения для матрицы $\mathbf{F}_{17}$

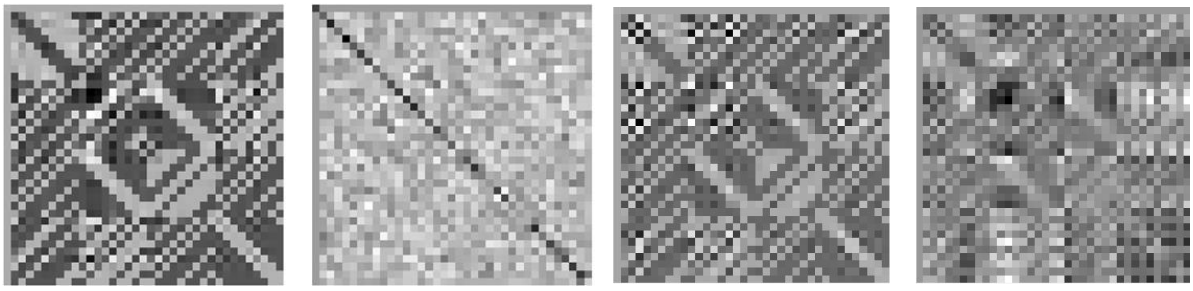


Рисунок 4.14 – Особые изображения для матрицы $\mathbf{F}_{37}$

Пример. Для маскирования используются матрицы Эйлера порядков 22 и 34, портреты которых приведены на рисунке 4.15

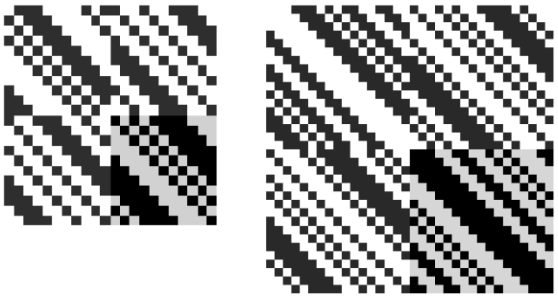


Рисунок 4.15 – Портреты матриц Эйлера

Особые изображения, визуализированные в формате BMP, для приведенных матриц Эйлера приведены на рис. 4.16 и 4.17.

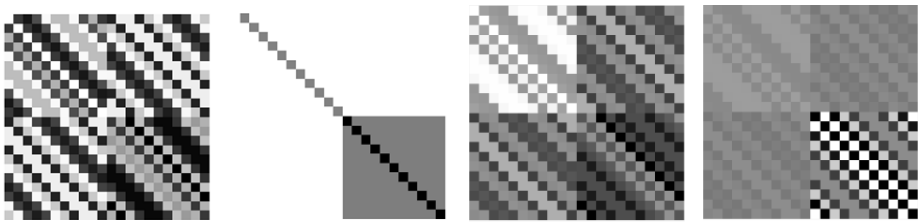


Рисунок 4.16 – Особые изображения для матрицы $\mathbf{E}_{22}$

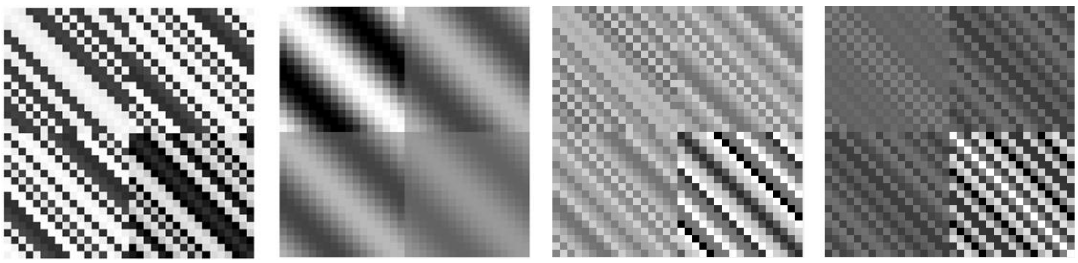


Рисунок 4.17 – Особые изображения для матрицы Эйлера $\mathbf{E}_{34}$

Приведенные визуализированные результаты преобразований позволяют утверждать, что метод маскирования с использованием квазиортогональных матриц может быть использован без ограничений, поскольку особые изображения, инвариантные к двустороннему матричному преобразованию, не являются изображениями объектов реального мира, а напоминают лишь портреты указанных матриц.

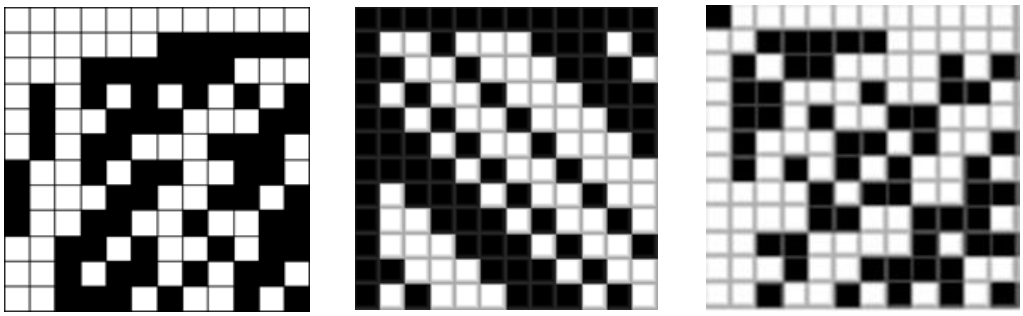
4.3 Маскирование специальными матрицами

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 [25, 104].

В качестве примера для двух тестовых изображений («Лена» и «Танк») с разрешением 512×512 пикселов, приведенных на рис. 4.18, приведем результаты некоторых экспериментов.

Рисунок 4.18 – Тестовые изображения для эксперимента

На рис. 4.19 представлены портреты использованных для экспериментов трех матриц Адамара. Неструктурированная матрица, вычисленная самим Адамаром, представлена на рис. 4.19а. Матрица Адамара, вычисленная на основе циклической матрицы Мерсенна порядка11, представлена на рис. 4.19б, а вычисленная на основе симметричной матрицы Мерсенна порядка 11 – на рис. 4.19в. Обе матрицы вычислены в процессе исследований.



а б в

Рисунок 4.19 – Портреты матриц Адамара порядка 12

Представленные далее визуализации маскированного изображения, передаваемого в теле IP-пакета в коммуникационном канале, получена с использованием библиотеки Open CV, которая не делает выравнивания вещественных значений пикселей в диапазон от 0 до 255.

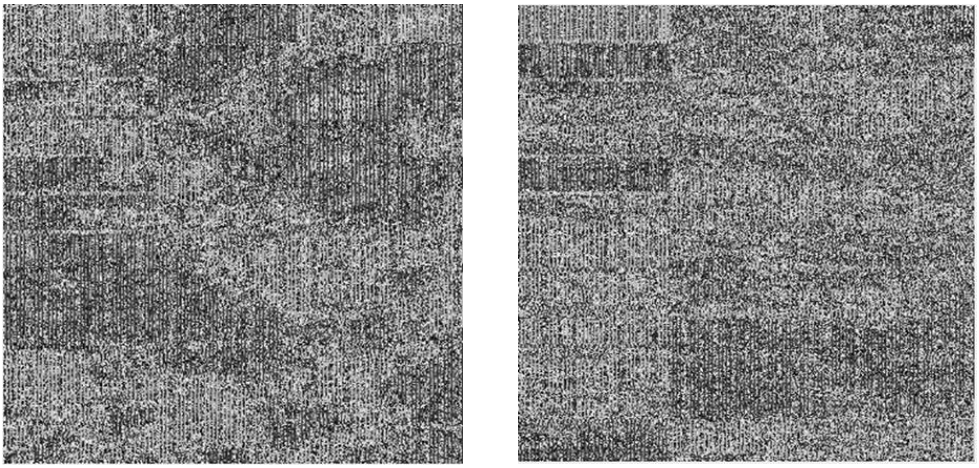


Рисунок 4.20 – Тестовые изображения, маскированные неструктурированной матрицей Адамара порядка 12

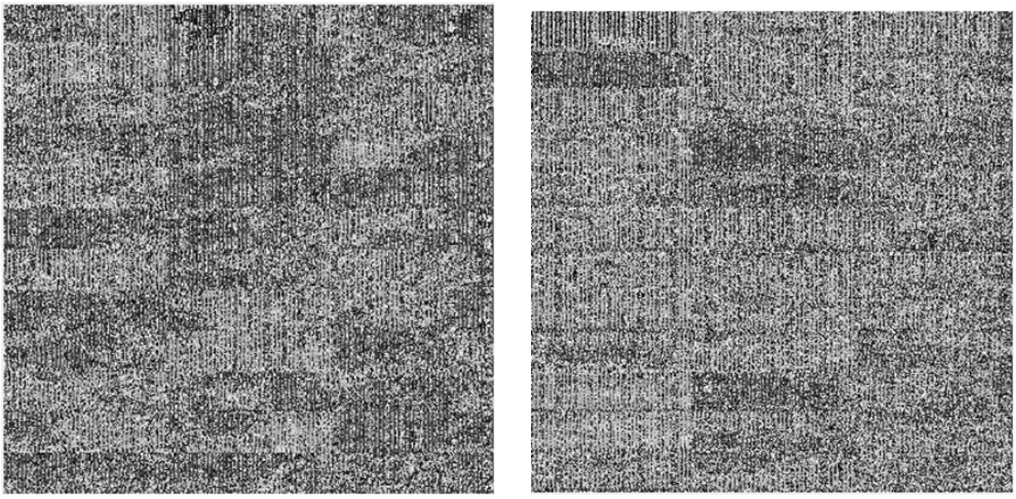


Рисунок 4.21 – Тестовые изображения, маскированные симметричной матрицей Адамара порядка 12

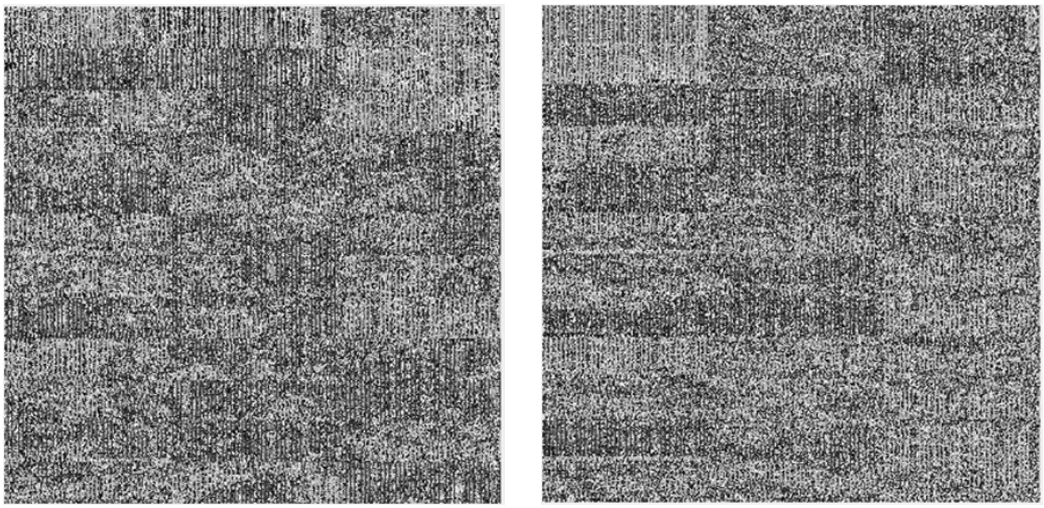


Рисунок 4.22 – Тестовые изображения, маскированные несимметричной матрицей Адамара порядка 12

Визуализации маскированных изображений, представленных на рис. 4.20 – 4.22, отличаются друг от друга, но их гистограммы показывают близость характеристик. С точки зрения решения задачи маскирования – сокрытия передаваемого изображения или контуров объектов на изображении – они практически равнозначны.

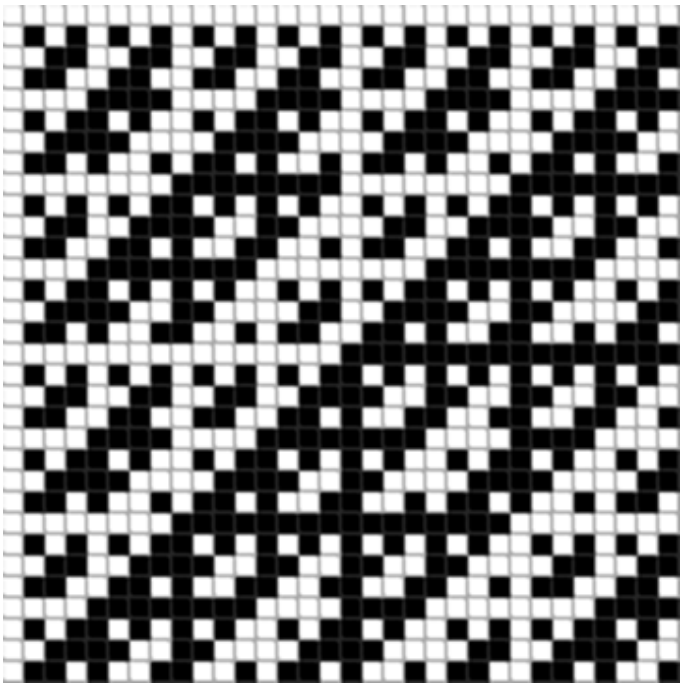


Рисунок 4.23 – Портрет симметричной матрицы
Адамара порядка 32

При использовании матрицы Адамара порядка 32, портрет которой представлен на рис. 4.23, получен наилучший результат маскирования, приведенный на рис. 4.24.

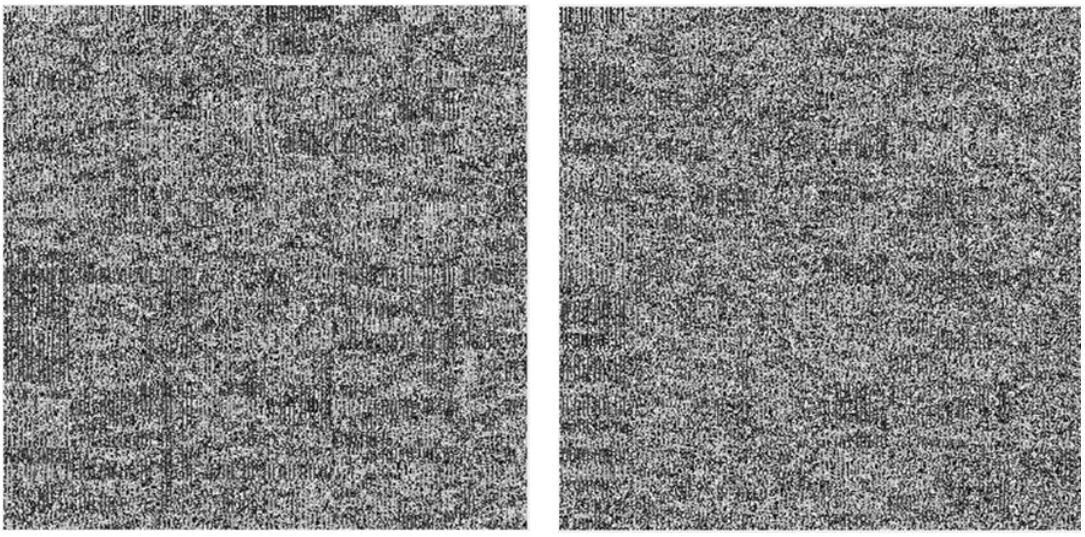


Рисунок 4.24 – Тестовые изображения, маскированные симметричной матрицей Адамара порядка 32

Эксперименты со специальными матрицами симметричных структур более высоких порядков показали еще более качественное маскирование изображений.

4.4 Стрип-преобразование с циклическими и симметричными матрицами Адамара

Для приведенных на рис. 4.19 матриц были проведены эксперименты для оценки влияния выбора структуры специальной матрицы на модифицированное стрип-преобразование тех же тестовых изображений (рис. 4.18). Отличие от классического [9] заключается в отказе от кронекерова умножения.

Восстановленные изображения на приемном конце распределенной IP-системы соответствуют случаям потери в коммуникационном канале одного, двух и шести пакетов данных размером 1024 байт каждый. Местоположение потерь на преобразованном изображении можно представить наложением темных полос на поле изображения (рис. 4.25).

Результаты восстановления изображений с потерей пакетов в канале приведены на рис.4.26.

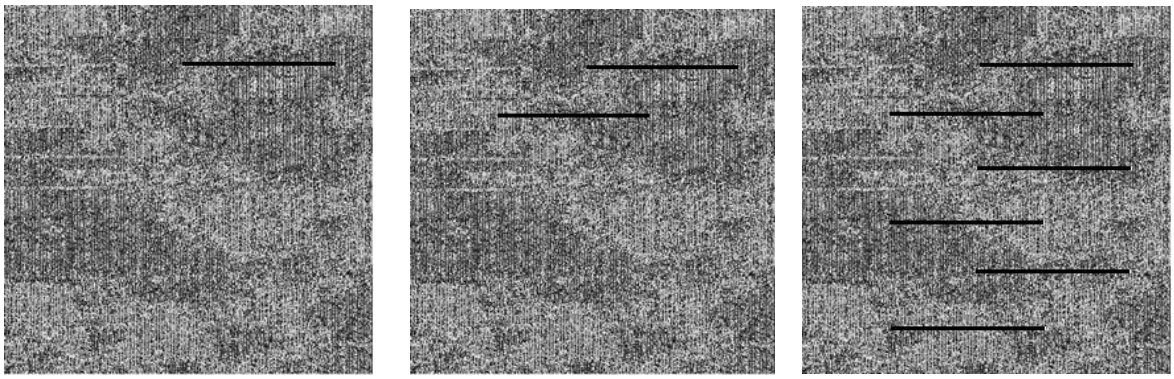


Рисунок 4.25 – Места потерь одного, двух и шести пакетов на маскированном изображении «Лена» в канале

а

б

в

Рисунок 4.26 – Восстановленные изображения при потере одного (а), двух (б) и шести (в) пакетов в маскированном изображении, передаваемом по каналу.

4.5 Эксперименты по замене ДКП в алгоритме сжатия изображений специальными матрицами

Проведение экспериментов по замене ДКП на специальные квазиортогональные матрицы проводилось в среде моделирования (ПРИЛОЖЕНИЕ 1), разработанной с участием автора, в которой был реализован плагин сжатия по алгоритму JPEG [135].

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.

Как отмечалось в работах [12, 13 и др.], «…в практике применения ортогональных матриц большое значение имеет максимальная простота их структуры». В процессе работы рассматривался вопрос расширения семейства специальных матриц для обработки изображений, включая матрицы не только больших размеров, неизвестных до настоящего времени, но и матрицы нечетных порядков.

Общие уточненные требования к формируемому семейству специальных матриц были сформулированы в разделе 1 (см. п.1.3).

Приведенным выше требованиям в полной мере отвечает семейство специальных квазиортогональных матриц, являющихся естественным обобщением ортогональных матриц [57, 121, 136].

Особый интерес для отдельных задач обработки изображений [93, 94, 137, 138] представляют симметричные конструкции матриц Мерсенна и Адамара-

Уолша, получаемые из классических матриц Адамара путем упорядочивания столбцов по частоте (по количеству смены знаков их элементов), либо вычисляемые по рассмотренному в разделе 3 методу со случайной генерацией последовательностей для формирования таких матриц [139].

Известно, что процедура сжатия с потерями, как наиболее перспективная, позволяет получить высокие коэффициенты сжатия, по сравнению со сжатием без потерь. При этом, используя сжатие с потерями, возможно достичь компромисса между предъявляемыми требованиями к качеству изображения и степенью сжатия, что позволяет разработать алгоритм сжатия для конкретной прикладной задачи.

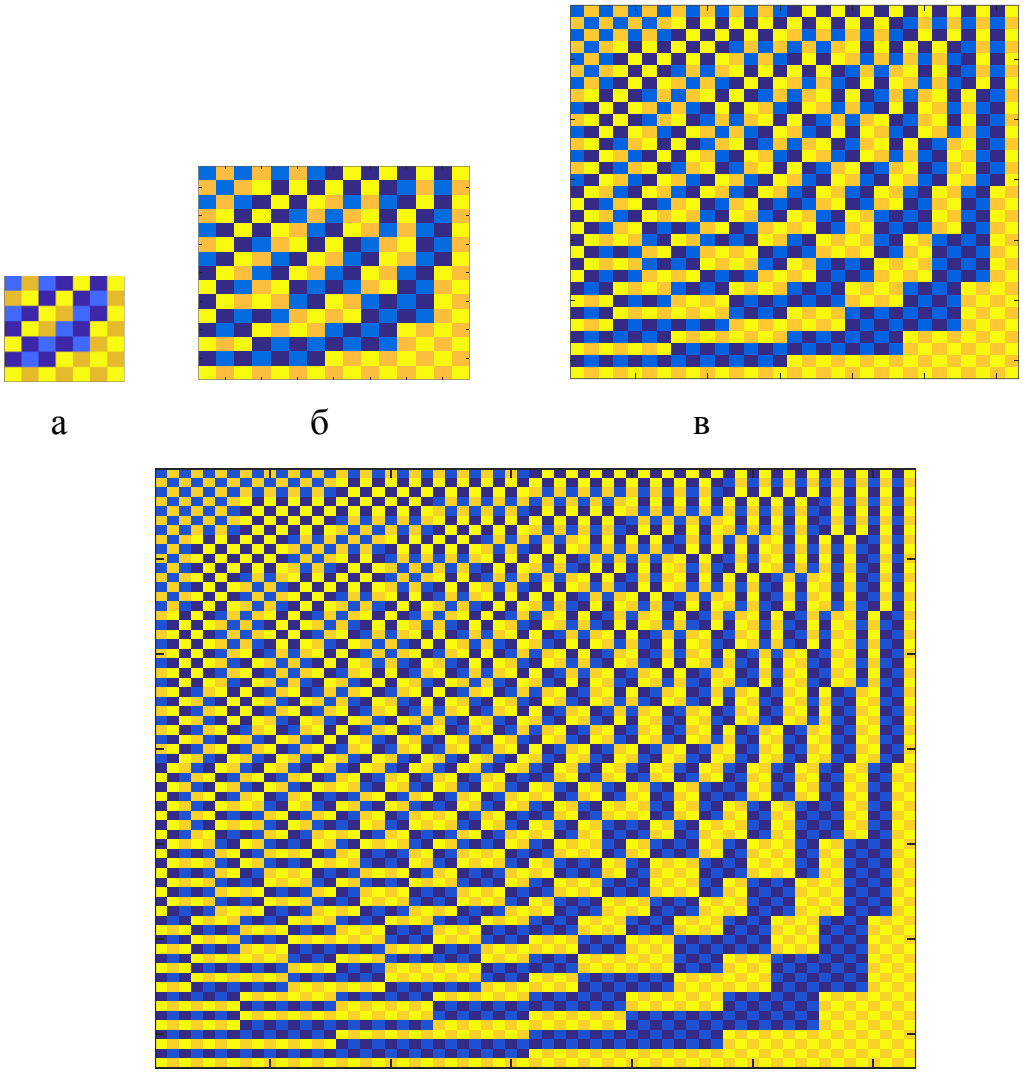
На этапе препроцессинга в алгоритме JPEG изображение переводится из растрового представления в цветоразностное и яркостное, что позволяет добиться больших результатов сжатия при меньших визуальных потерях. На следующем этапе изображение подвергается ДКП. Результатом является матрица, в которой элементы в левом верхнем углу связаны с низкочастотными составляющими изображения, а в правом нижнем – высокочастотными. В упрощенном виде это преобразование представимо как уже известное двустороннее матричное умножение.

Поиск и последующее удаление нулей и элементов матрицы, вклад которых в формирование изображения минимален, приводят при выставленном пороге значения коэффициента сжатия к сокращению объема данных – сжатию.

В диссертационной работе рассматривается возможность замены ДКП в цепочке преобразований на ортогональное преобразование со специальными матрицами [138, 140, 141]. Однако, в отличие от использования двухуровневых симметричных матриц Мерсенна [28], предлагается использование модульно двухуровневых (четырехуровневых) матриц [140, 141], при поиске которых по формулам, приведенным в определении 14, для коэффициентов не фиксируется значение a в виде $a = 1$.

В проведенных экспериментах [140, 141] именно такие модульно двухуровневые квазиортогональные матрицы Мерсенна, отсортированные по Уолшу, а именно – симметричные четырехуровневые матрицы Мерсена-Уолша, показали себя лучше.

На рис. 4.27 представлены цветные портреты таких матриц порядков 7, 15, 31 и 63. Очевидно, что при их применении в преобразовании изображений, в отличие от ДКП, низкие частоты оказываются в правом нижнем углу, а высокие – в левом верхнем. В связи с этим в алгоритме сжатия меняется порядок обхода матрицы после квантования.



а б в

г

Рисунок 4.27 – Портреты четырехуровневых матриц Мерсена-Уолша порядков 7 (а), 15 (б), 31 (в), 63 (г)

Для эквивалентности экспериментов по сжатию изображений с ДКП и матрицами Мерсенна-Уолша задавались одинаковые коэффициенты сжатия, величина которых связана с порогом квантования. Следовательно, фильтрация в том и другом случаях производилась по правилу «все, что ниже порога обнуляется, все что выше – остается неизменным».

В качестве примера на рис. 4.28 приведено восстановленное после сжатия при различных коэффициентах тестовое изображение «Енот» для преобразования с ДКП и с приведенной на рис. 4.28 матрицей Мерсенна-Уолша порядка 7. Визуально эти результаты, как и ряд других с различными тестовыми изображениями показывают, что уже при сжатии в 3 раза при применении матрицы Мерсена-Уолша восстановленное после сжатия изображение в большей степени соответствует исходному изображению.

В теории цифровой обработки изображений сегодня нет метода оценки качества, полностью соответствующего визуальному восприятию человека. Для объективного сравнения изображений обычно используются метрики, две наиболее показательные и широко используемые из которых – PSNR и SSIM [142].

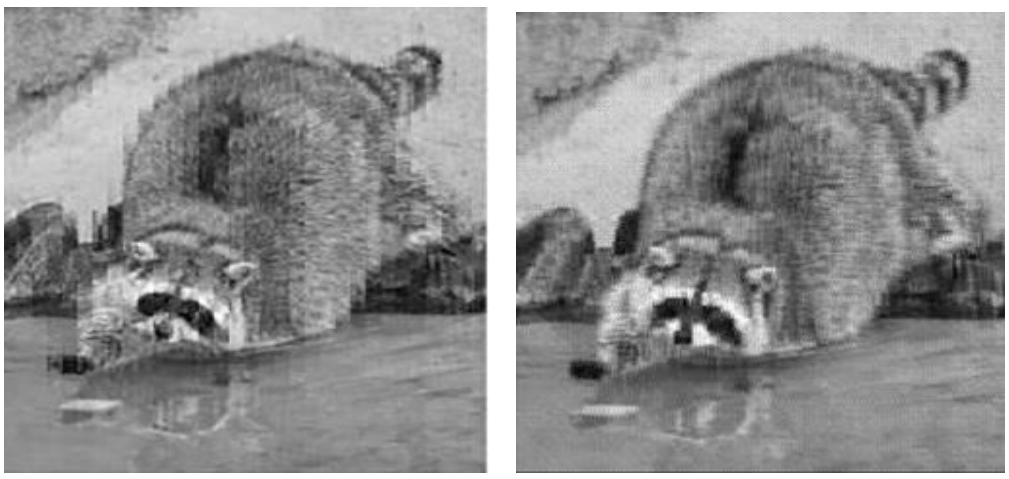
В таблице 4.1 для тестового изображения «Енот» приведены значения этих метрик при сравнении качества сжатия/восстановления изображений, приведенных на рис. 4.28.

Таблица 4.1. Метрики восстановленных изображений после сжатия

Преобразование	Вычисленные значения метрик					
	PSNR			SSIM		
	Коэффициент сжатия					
	1,5	2	3	1,5	2	3
Дискретное косинусное	33,3501	31,0116	25,613	0,9551	0,9197	0,8112
Квазиортогональное	21,3865	20,9127	20,3842	0,7886	0,7056	0,6097

а

б



в

Рисунок 4.28– Восстановленные после сжатия изображения: слева с ДКП, справа – с четырехуровневой матрицей Мерсенна-Уолша для коэффициентов сжатия 1,5 (а), 2 (б) и 3 (в)

С использованием приведенных реализаций алгоритмов сжатия и маскирования, описанного ранее, было реализовано специальное программное обеспечение [131, 132] для системы передачи видео на регистрирующее устройство в системе дистанционной передачи данных по радиоканалу в ООО «АСК Лаборатория»

Замена ДКП на преобразование со специальными матрицами при внедрении ЦВЗ в изображения (операция маркирования изображений) отдельно в данной диссертационной работе не исследовалась. Однако эффективность внедрения была исследована и показана в диссертационной работе Григоряна А. К. [32]. Результаты экспериментов были получены при использовании программных утилит [143, 144], разработанных с участием автора.

Следует лишь отметить, что указанные утилиты позволили не только внедрять и извлекать ЦВЗ в изображения, но и более точно определять возможное место искажения изображения, случайного или преднамеренного.

4.6 Повышение помехоустойчивости при передаче информации в открытых каналах

Анализ кодовых последовательностей Баркера длины 3, 7 и 11 показал, что они являются кодовыми последовательностями мерсеннова типа. Код Баркера длины 11, используемый в стандарте IEEE802.11, соответствует части строки матрицы максимума детерминанта порядка 41, вычисленной Гвидо Барба [145].

С целью поиска новых, более эффективных кодовых последовательностей целесообразно проработать и дополнить общую теорию кодов, комбинаций кодовых последовательностей и провести сравнительный анализ параметров автокорреляционных функций.

В диссертационной работе предлагается один из возможных путей реализации исследований в такой постановке, состоящий в том, чтобы несколько ослабить требования к АКФ и допустить значения вторичных пиков, превышающих единицу. Это было бы приемлемым в том случае, когда центральный пик АКФ значительно больше единицы.

Кроме того, поиск новых последовательностей должен осуществляться с учетом следующих требований:

– функция взаимной корреляции любой пары из группы последовательностей одинаковой длины должна быть минимизирована;

– количество вариантов для маскирования кодовой последовательности одной длины должно быть максимальным в целях затруднения возможности их радиоразведки;

– длина кода должна быть произвольной;

– уровень максимальных по модулю боковых лепестков автокорреляционной функции должен быть не хуже, чем у кода *m*-последовательности.

Предварительный анализ и проведенные эксперименты показали перспективы получения новых кодов, построенных на основе строк моноциклических квазиортогональных матриц Мерсенна. Работа в этом направлении позволит расширить общую теорию кодирования и удовлетворить в совокупности требованиям, предъявляемым в современных системах обнаружения и в телекоммуникационных каналах.

На основании исследованных в работе [121] матриц Мерсенна [57, 74], существующих на порядках $n=4t-1$, где t – натуральное число, и имеющих в одном из вариантов представления два фиксированных значения элементов $\{1, -b\}$ и в каждой их строке (столбце) количество единичных значений на единицу больше отрицательных значений, предложены новые коды.

Указанные матрицы, являясь ядром матриц Адамара и обобщая их, имеют, как и они, различные конструкции, в том числе моноциклические и симметричные [56, 91].

Сравнение кодовых последовательностей Баркера длин 3, 7 и 11 и строк циклических матриц Мерсенна этих же порядков, приведенное в таблице 4.2, показывает, что хотя они и отличаются, но являются кодовыми последовательностями одного типа – мерсеннова, и сформированы на основе строк матриц Мерсенна моноциклической конструкции [74, 112].

Однако, у кодовых последовательностей Мерсенна, получаемых из строк циклической матрицы Мерсенна, в отличие от последовательностей Баркера, отрицательный элемент равен $-b$ [112]. Интересен тот факт, что для этих матриц $b = f(n)$, и с ростом порядка $-b \rightarrow -1$. Это делает близкими получаемые на их основе коды с существующими кодами, но отличаемыми по форме модулированного ими сигнала в канале. Именно $-b$ является тем послаблением, которое приводит к новым результатам в генерации кодов и обеспечивает лучшие параметры кодированных сигналов.

Таким образом, при $n = 3$ значение $b = 1/2$, в остальных случаях $b = \dfrac{s \pm \sqrt{4s}}{s-4}$, где $s = n + 1$.

Таблица 4.2 – Кодовые последовательности Баркера и Мерсенна

Длина кода n	Коды Баркера	Коды Мерсенна
3	1 1 –1	$-b$ 1 1
7	1 1 1 –1 –1 1 –1	$-b$ $-b$ 1 $-b$ 1 1 1
11	1 1 1 –1 –1 –1 1 –1 –1 1 –1	$-b$ 1 $-b$ $-b$ $-b$ 1 1 1 $-b$ 1 1

На рис. 4.29 приведены портреты матриц Мерсенна, на которых белое поле, как и ранее, соответствует элементу матрицы со значением 1, черное поле – элементу со значением $-b$.

Сами же конструкции последовательности Мерсенна могут быть получены [121] для всех простых чисел длинной $p=4t-1$ с помощью вычисления последовательности Лежандра [78].

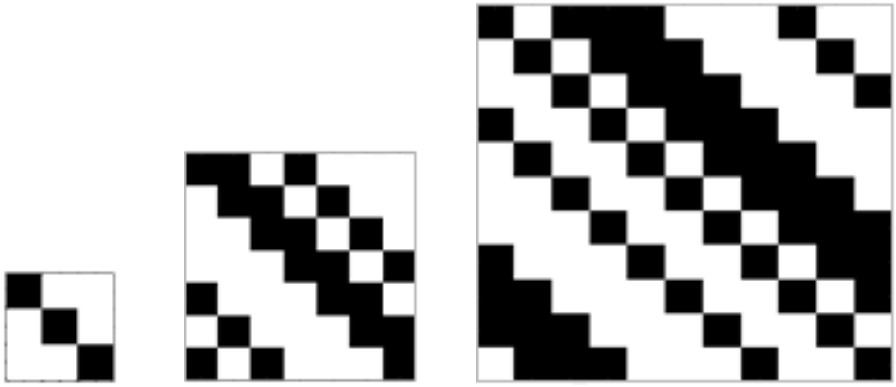


Рисунок 4.29 – Портреты моноциклических квазиортогональных матриц Мерсенна порядков 3, 7 и 11

Эти последовательности формируются через вычисления «квадратичных символов» (символы Лежандра), определенных на $1 \le a \le p-1$ по выражению:

$$\left(\frac{a}{p}\right)=\begin{cases}-1, & \text{если } x^2=a \bmod p \\ 1- & \text{в остальных случаях,}\end{cases}$$

где p – длина последовательности; x – номер позиции последовательности от 1 до p; $\left(\frac{a}{p}\right)$ – вычисленные позиции отрицательных и положительных элементов последовательности.

Таким образом, имеется возможность получить кодовые последовательности Мерсенна, аналогичные по своим свойствам кодовым последовательностям Баркера. Однако, с целью оценки характеристик АКФ, следует провести сравнительный анализ этих кодовых последовательностей.

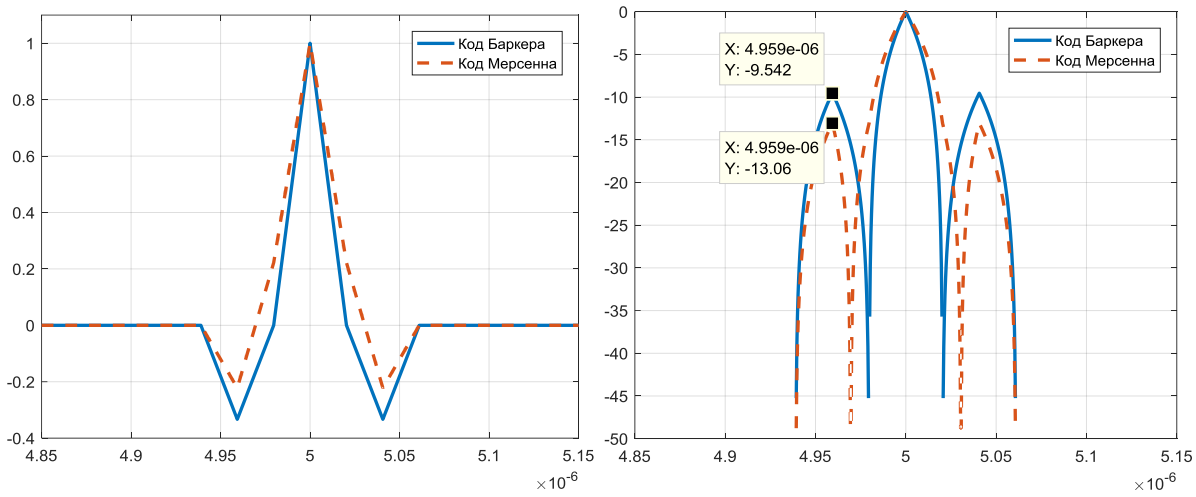
С целью определения характеристик сжатия кодовых последовательностей Баркера и Мерсенна в работе были проведены эксперименты для кодов длины 3, 7 и 11. Результаты экспериментов опубликованы в работах [49, 147, 148] и приведены на рис. 4.29, где сравнивались АКФ их огибающих и оценивалось ОПМБЛ.

На рис. 4.30а результаты получены для $n = 3$, на рис. 4.29б – для $n = 7$, на рис. 4.29в – для $n = 11$. Слева – нормированная к единице, справа – АКФ в децибелах.

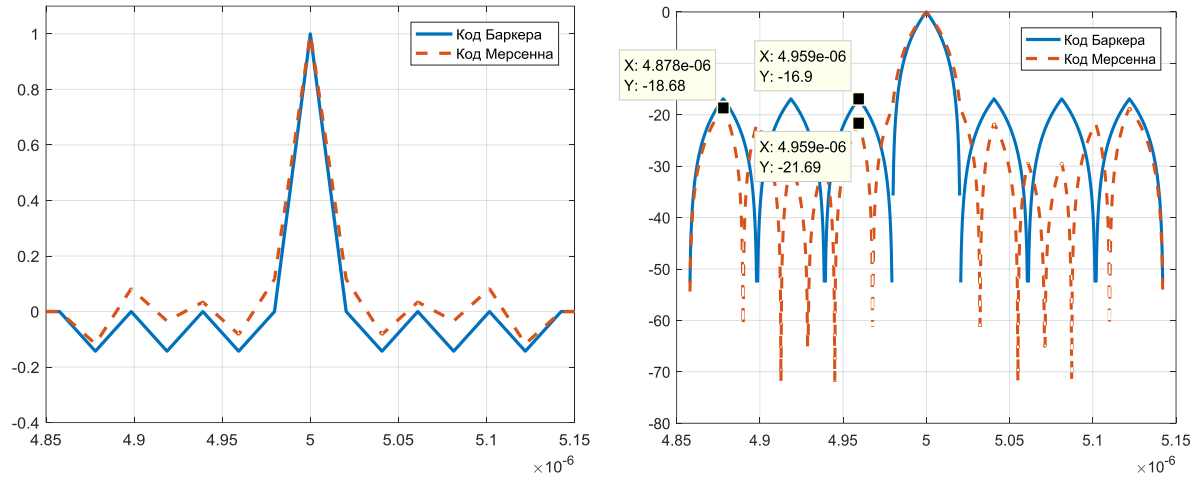
Результаты оценки характеристики АКФ для кодовых последовательностей Баркера и Мерсенна, приведенных в таблице 4.3 показывают, что ОПМБЛ АКФ для кодовой последовательности Мерсенна при $n = 7$ составляет –18,68 дБ, что на 1,78 дБ ниже уровня боковых лепестков, чем у аналогичного кода Баркера (см. рис. 4.30б). Особый интерес представляет результат, приведенный на рис. 4.30а, где ОПМБЛ АКФ кода Мерсенна при $n = 3$ превышает аналогичную оценку для кода Баркера на 3,52 дБ.

Для кодовой последовательности Мерсенна длины 11 оценка ОПМБЛ АКФ получилась хуже, чем у кода Баркера на 1,72 дБ, однако максимальный боковой лепесток находится на достаточном удалении от главного лепестка АКФ, что может рассматриваться как отдельный аргумент в пользу кода Мерсенна.

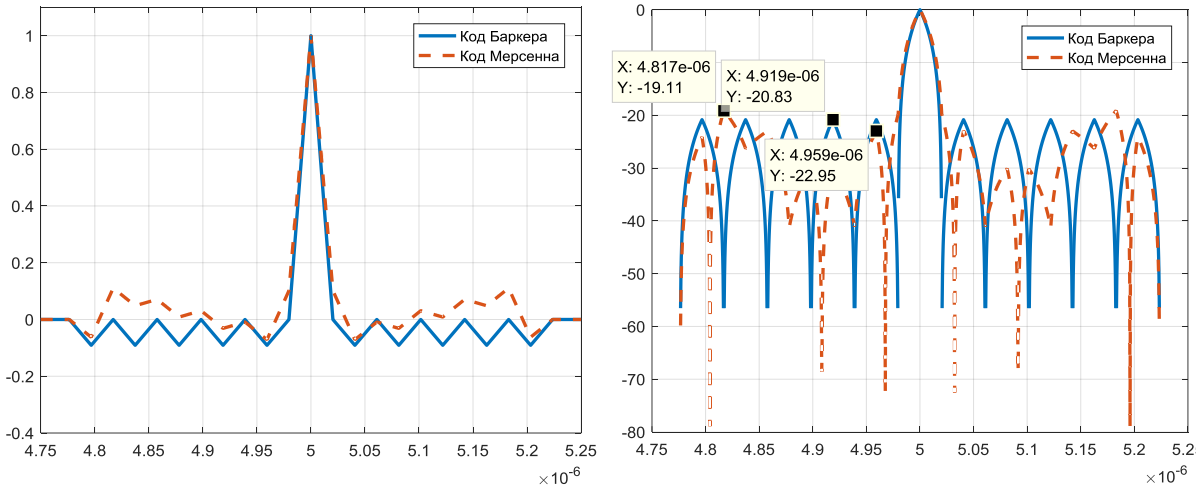
Полученные в работе характеристики АКФ для кодовых последовательностей Баркера и Мерсенна длин 3, 7 и 11 позволяют сделать вывод о перспективности использования кодов Мерсенна и аналогичных, полученных по предлагаемой стратегии их построения, как альтернативы кодам Баркера в радиолокации и при передаче в коммуникационных радиоканалах [146].



а



б



в

Рисунок 4.30 – АКФ огибающей кодов Баркера и Мерсенна

Таблица 4.3 – Оценка характеристик АКФ

Длина кода, n	Код Мерсенна	Код Баркера	Выигрыш кода Мерсенна
ОПМБЛ, дБ			
3	–13,06	–9,54	3.52
7	–18,68	–16,90	1.78
11	–19,11	–20,83	–1.72

Нерешенным пока остается вопрос несимметричности элементов кодовой последовательности Мерсенна. Однако, решение возможно как с использованием специального аппарата синтеза сигналов, модулированных кодами Мерсенна, так и новых подходов к сжатию этих сигналов.

Коды, превосходящие коды Баркера по характеристикам, для длин 2 и 4 в процессе выполнения работы найдены не были. Указанные длины кодов в теории квазиортогональных матриц соответствуют их порядкам 2 и 4 и являются исключениями. Единственная известная моноциклическая матрица Адамара, согласно гипотезе Райзера [95], имеет порядок 4. Ее элементы всегда строго симметричны относительно главной и побочной диагоналей. Порядку n=2 соответствует моноциклическая матрица Белевича. Однако для этих матриц отход от существующего представления кодов в паре {1, –1} и использование для кодирования предлагаемых в работе несимметричных пар $\{1, -b\}$ или $\{a, -b\}$ невозможен.

В целом результаты моделирования, впервые представленные в работе [49] и изложенные выше, имеют теоретическое и практическое значения при исследованиях, связанных с:

– помехоустойчивостью зондирующего сигнала в радиолокационных каналах,

– выбором характеристик сигналов РЛС в условиях сложной электромагнитной обстановки,

– помехоустойчивостью систем передачи данных.

4.7 Вложенные кодовые последовательности и сравнительный анализ их АКФ

Изложенный выше материал и обнадеживающие расчетные результаты для новых кодов, тем не менее, могут быть улучшены в части ОПМБЛ АКФ при решении задач обнаружения и обеспечения помехоустойчивости в открытых радиоканалах. Для улучшения ОПМБЛ АКФ таких кодов можно рассмотреть комбинации из последовательно вложенных кодов Баркера и Мерсенна, а также оценить характеристики их АКФ.

Известны комбинации двух кодовых последовательностей Баркера, называемых «несущая» длины n_1 и «модулирующая» длины n_2, приводящих к последовательности длины n_1 n_2 [149, 150]. В нашем случае будем использовать разные комбинации пар кодовых последовательностей Баркера и Мерсенна различных длин.

Определение 24. Вложенным кодом будем называть комбинацию кодовых последовательностей такую, в которой одна является последовательностью (или внешним кодом) верхнего уровня, а вторая, вложенная в каждый элемент ее кода, – последовательностью нижнего уровня (или внутренним кодом).

В качестве примера на рис. 4.31 представлен вложенный код из последовательностей Баркера длины 4 и длины 5. Здесь огибающая сигнала на нижнем уровне, модулированная кодом Баркера длины 5, а на верхнем – кодом Баркера длины 4.

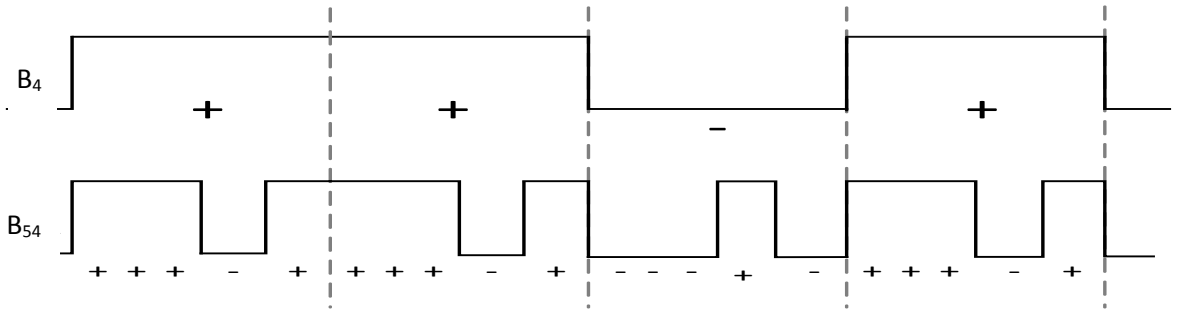


Рисунок 4.31 – Код Баркера 5×4 (сверху) и огибающая сигнала этим кодом (снизу)

Таким образом, получаем код Баркера длины 4, в каждый элемент которого «вложен» код Баркера длиной 5 с учетом знака последовательности на верхнем уровне. Таким образом, реализуется принцип вложенности кодов.

Для формирования АКФ комбинированного кода длиной $m \times n$ применяется двойное последовательное сжатие в два этапа. На первом этапе сначала сжимают код нижнего уровня (код Баркера длины 5), на втором этапе применяется сжатие последовательности, полученной на первом этапе – осуществляется сжатие на верхнем уровне. Таким образом, формируется АКФ вложенного кода.

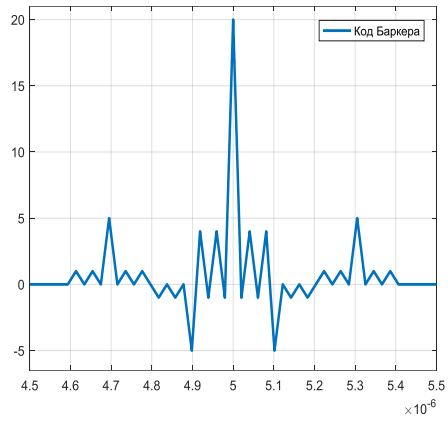
Анализ полученных в процессе исследований результатов показал, что целесообразно внешний код брать меньшей длины, чем внутренний.

На рис. 4.32 представлены АКФ для вложенного кода Баркера комбинации 5×4 для двух видов кода Баркера длины 4.

Пример формирования вложенного кода из комбинации кода Баркера и кода Мерсенна приведен на рис. 4.33. Поскольку оценка ОПМБЛ новых найденных кодов превышает аналогичную оценку кода Баркера, то их совмещение предполагает улучшение показателей новых вложенных последовательностей.

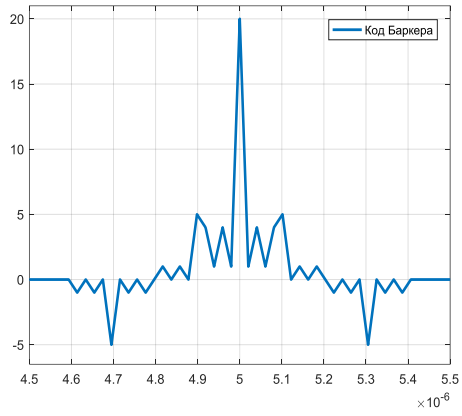
В таблице 4.4 приведены возможные комбинации вложенных кодов и оценки их ОПМБЛ. В качестве кода Мерсенна в расчетах использовался

новый код, сформированный на основе квазиортогональной циклической матрицы.



B_{54}= [B_5 –B_5 B_5 B_5]

B_5=[1 1 1 –1 1]



B_{54}=[B_5 –B_5 –B_5 –B_5]

B_5=[1 1 1 –1 1]

Рисунок 4.32 – АКФ вложенного кода Баркера длины 5×4

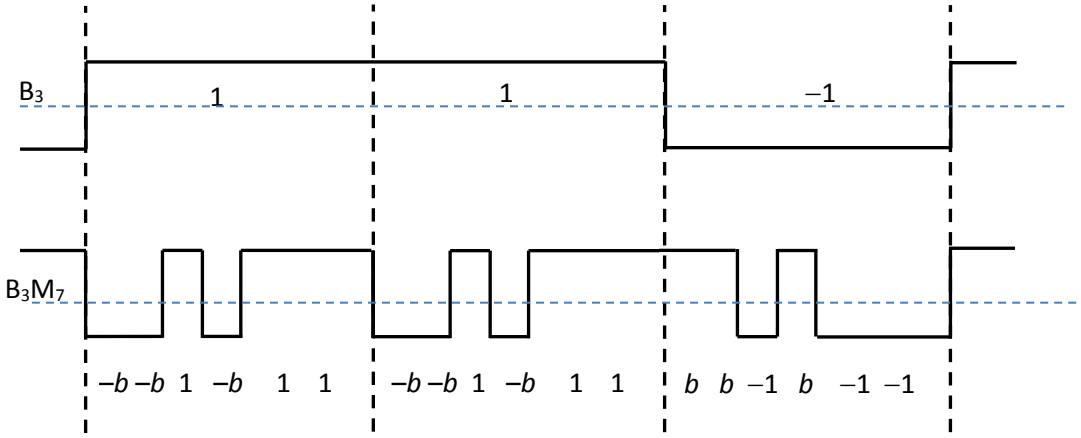


Рисунок 4.33 – Код Баркера-Мерсенна 5×4 (сверху) и огибающая сигнала этим кодом (снизу)

4.8 Выводы по разделу 4

Двустороннее матричное маскирование может реализоваться не только с двух, но и трехуровневых специальных матриц. При этом найденные особые изображения симметричных матриц Мерсенна-Уолша, Ферма и

Эйлера высоких порядков показывают, что они могут быть использованы без ограничений в качестве маскирующих матриц.

Таблица 4.4 – Комбинации вложенных кодов и оценка ОПМБЛ АКФ

*n*x*m*	Комбинация кодов							
	Баркер-Баркер		Баркер-Мерсенн		Мерсенн-Баркер		Мерсенн-Мерсенн	
	Оценка ОПМБО, дБ							
	«+»	«-»	«+»	«-»	«+»	«-»	«+»	«-»
3x3	-19.2285	-9.6855	-22.6062	-9.5424	-13.2575	-9.6531	-13.0643	-13.3065
3x7	-26.8826	-9.5424	-21.6835	-9.6687	-13.0636	-13.1873	-13.0636	-13.3205
3x11	-31.7564	-9.6857	-26.1265	-9.6857	-13.0646	-13.3537	-13.0646	-13.0646
7x3	-26.4444	-9.6863	-29.9619	-13.2081	-18.6753	-9.6813	-18.6753	-14.1401
7x7	-33.8039	-16.9020	-21.6849	-16.9020	-18.6758	-17.0282	-18.6758	-19.7519
7x11	-37.7298	-17.1910	-26.3775	-17.0453	-18.6759	-21.3468	-18.6759	-18.3863
11x3	-30.3703	-9.5424	-33.8917	-13.0646	-26.2338	-9.5424	-26.2176	-13.1062
11x7	-37.7298	-17.1910	-21.6853	-19.2649	-34.6170	-17.1991	-21.7279	-17.7125
11x11	-42.0939	-20.9712	-26.1275	-18.0017	-39.8083	-18.0131	-26.2401	-17.7156

Стрип-преобразование может использовать все матрицы, образующие семейство специальных. Достигнутый на сегодня эффект заключается в том, что для преобразования можно использовать матрицы четных и нечетных порядков, упрощенную схему двустороннего матричного умножения, особые изображения используемых матриц не представляют идентифицируемые объекты реального мира.

Эксперименты по применению специальных четырехуровневых квазиортогональных матриц Мерсенна в алгоритме сжатия JPEG позволяют надеяться на эффект от их использования. Первые полученные результаты показали, что в перспективе совершенствование алгоритма сжатия с использованием указанных матриц следует проводить с усреднением значений ниже порога и с применением специальных алгоритмов их сжатого

представления. Это должно повысить качество восстановленных изображений и снизить появление артефактов на них.

Основным результатом исследования, дающим мотивацию к развитию теории кодирования в части разработки основ построения новых помехоустойчивых кодов и вложенных кодовых комбинаций, является предложенный отход от существующего представления кодов в паре значений {1, –1} и использование для кодирования пар {1, $-b$} и {a, $-b$}. Код длины 11, сформированный на основе строки циклической матрицы Мерсенна с приведением значения элементов $-b$ к –1, обеспечивает лучшую АКФ по сравнению с кодом Баркера. Отношение центрального и боковых лепестков гарантируют безошибочную передачу данных, модулированных этим кодом либо на большие расстояния, либо в условиях более зашумленной среды.

ЗАКЛЮЧЕНИЕ

Результаты диссертационной работы направлены на развитие и совершенствование основ преобразования изображений и кодирования сигналов в коммуникационных каналах, в том числе в прикладных задачах распределенных видеосистем, за счет расширения базиса ортогональных матриц специальными квазиортогональными матрицами.

Предложено расширение гипотезы Райзера, позволяющее ограничить поиск симметричных бициклических квазиортогональных матриц на порядках не выше 32. Для их поиска разработан и исследован специальный метод на основе перекрестных ссылок.

Предлагаемое расширение базиса позволяет не только использовать матрицы в известных процедурах обработки изображений, но и способствует пересмотру самих процедур с ориентацией на свойства таких матриц. В частности, в работе предложена модификация метода маскирования, в которой значительно упрощена реализация классического метода; предложен новый подход к фильтрации изображений и квантованию в алгоритме сжатия, показывающий перспективы использования предлагаемых модульно двухуровневых квазиортогональных матриц.

Предложен один из возможных путей конструирования новых кодовых последовательностей на основе свойств матриц Мерсенна, состоящий в ослаблении требований к АКФ и допущении значения ее вторичных пиков, превышающих единицу при условии, что центральный пик значительно больше единицы. При этом для фазовой (амплитудной) модуляции сигналов используются отличные от $\{1, -1\}$ строки циклических квазиортогональных матриц с элементами $\{1, -b\}$ или $\{a, -b\}$. Практическая значимость такого предложения заключается в развитии подходов к разработке и совершенствованию сложных кодо-модулированных сигналов в

радиолокационных системах и телекоммуникационных каналах, работающих в условиях сложной помеховой обстановки.

Наиболее интересными прикладными результатами работы, подтверждающими теоретические, являются реальные программные модули, реализующие поиск структурированных квазиортогональных матриц, помехозащищенный маскированный обмен в распределенной видеосистеме с мобильными видеорегистраторами, а также новые амплитудно несимметричные коды Мерсенна, использованные при разработке перспективных моделей радиолокаторов.

СПИСОК ЛИТЕРАТУРЫ

1. Воеводин В. В., Кузнецов Ю. А. Матрицы и вычисления. М.:Наука, 1984. 320 с.
2. Гантмахер Ф. Р. Теория матриц. М.:Физматлит , 2010. 560 с.
3. Hadamard J. Resolution d’une question relative aux determinants. Bulletin des Sciences Mathematiques. 1893. Vol. 17. pp. 240–246.
4. Silvester J. J. Thoughts on Inverse Orthogonal Matrices, Simultaneous Sign Successions and Tessellated Pavements in Two or More Colours with Applications to Newton's Rule Ornamental Tile-Work and the Theory of Numbers / J. J. Silvester // Philosophical Magazine. 1867. Vol. 34. P. 461–475.
5. Балонин Н.А., Сергеев М.Б. Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1. С. 2 – 15.
6. Jenny Seberry suggests we create a gallery of maths pictures. Available at: http://mathscinet.ru/catalogue/files/Judy-AnneOsborne_JennysIdea_VisHadamard.pdf (accessed 02 December 2018).
7. Сергеев А. М., Куртяник Д.В., Самиков А. В., Семенов А. А.О визуальной оценке результатов ычисления матриц Адамара // Наука. Техника. Технологии (политехнический вестник). 2018. №4. С.19 - 26
8. D'Angeli D., Donno A. Shuffling matrices, Kronecker product and Discrete Fourier Transform. arXiv.org. 2016
9. Мироновский Л. А., Слаев В. А. Стрип-метод преобразования изображений и сигналов. СПб.: Политехника, 2006. 163 с.
10. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.:Диалог-МИФИ. 2002. 384 с.
11. Ахмед Н., Рао К. Р. Ортогональные преобразования при обработке цифровых сигналов. Пер. с англ./ Под ред. И. Б. Фоменко, М.: Связь, 1980, С. 130 –132.

12. Mahafza B. R. Radar Systems Analysis and Design using MATLAB. Chapman&Hall/CRC. 2000. 532 p.
13. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge University Press. 2010. 504 p.
14. Ерош И.Л., Филатов Г.П., Сергеев А.М. О защите изображений при передаче по каналам связи // Информационно-управляющие системы. 2007. № 5(30). С. 20 – 22.
15. Сергеев М.Б., Сергеев А.М., Литвинов М.Ю., Филатов Г.П. Problems on Formation Protected Digital Images // XI International Symposium on Problems of Redundancy in Information and Control Systems: Proceeding/ Saint-Petersburg State University of Aerospace Instrumentation (SUAI). 2007. P.202.
16. Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник. – М.: Горячая линия-Телеком, 2004. – 247 с.
17. Рассохина А. А. Исследование стрип-метода обработки сигналов и изображений // System Informatics (Системная информатика). 2013. № 1. С. 97 – 106.
18. Чернышев С. А. Разработка и исследование метода матричного маскирования видеоинформации в глобально распределенных системах: дис….канд. техн. наук: защищена 27.03.2018: утв. 13.08.2018 / Чернышев Станислав Андреевич. СПб, 2018. 120 с.
19. http://local.com.ua/story/Prognozi-Cisco-po-rostu-obemov-IP-trafika/ (дата обращения: 10.01.2016)
20. Cai L., Shen X., Mark J. W. Multimedia Services in Wireless Internet // Modeling and Analysis. June 2009. P. 52–57.
21. Астапкович А. М., Востриков А. А., Сергеев М. Б., Чудиновский Информационно-управляющие системы на основе Internet // Информационно-управляющие системы. 2002. № 1. С. 12-18.

22. Беззатеев С.В., Литвинов М.Ю., Трояновский Б.К., Филатов Г.П. Выбор алгоритма преобразования, обеспечивающего изменение структуры изображений // Информационно-управляющие системы. 2006. № 6(25). С. 2-6.
23. Литвинов М. Ю. Алгоритмы маскирующих преобразований видеоинформации: автореф. дис. … канд. техн. наук / ГУАП. СПб., 2009. – 23 с.
24. Разинков Е. В., Латыпов Р. Х. Встраивание цифрового водяного знака в изображение с использованием комплексного преобразования Адамара // Материалы II международной научной конференции по проблемам безопасности и противодействия терроризму. М.: МЦНМО, 2007. С. 509–514.
25. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images // Intelligent Interactive Multimedia Systems and Services. Smart Innovations, Systems and Technologies 40. Springer, 2015. Pp. 161 – 168. DOI 10.1007/978-3-319-19830-9_15
26. Балонин Ю. Н., Востриков А. А., Сергеев М. Б. О прикладных аспектах применения М-матриц // Информационно-управляющие системы. 2012. № 1 (56). С. 92 - 93.
27. Востриков А. А., Мишура О. В., Сергеев А. М., Чернышев С. А. О выборе матриц для процедур маскирования и демаскирования изображений // Фундаментальные исследования. 2015. № 2-24. С. 5335-5339.
28. Vostrikov A., Chernyshev S. Implementation of novel quasi-orthogonal matrices for simultaneous images compression and protection. Frontiers in Artificial Intelligence and Applications. Volume 262: Smart Digital Futures 2014, pp. 451 – 461.
29. Востриков А. А., Балонин Ю. Н. Матрицы Адамара-Мерсенна как базис ортогональных преобразований в маскировании видеоизображений //

Известия высших учебных заведений. Приборостроение. 2014, т. 57, № 1, С.15–19.

30. Красиленко В. Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельницького національного університету. Технічні науки. 2014. № 1. С. 74-79.
31. Востриков А. А. Маскирование цифровой визуальной информации: термин и основные IP / А. А. Востриков, М. Б. Сергеев, М. Ю. Литвинов // Информационно-управляющие системы. 2015, № 5 (78). С. 116 – 123.
32. Григорьян А. К. Разработка и исследование метода преобразования видеоданных для определения их подлинности и подтверждения целостности: дис….канд. техн. наук: защищена 20.03.2012: утв. 12.11.2012 / Григорьян Амаяк Карэнович. СПб, 2012. 120 с.
33. Favorskaya M. N., Savchina E. I., Jain L. C. Perceptually tuned Watermarking using non-subsampled shearlet transform // Intelligent Systems Reference Library. 2018. T. 136. C. 41-69.
34. Ho A.T.S., Shen J., Chow A.K.K., Woon J. Robust digital image-in-image watermarking algorithm using fast Hadamard transform // Proc. IEEE International Symposium on Circuits and Systems. 2003. V. 3. P. III826-III829.
35. Saryazdi S., Nezamabadi-pour H. A blind digital watermark in Hadamard domain // International Journal of Computer, Information, Systems and Control Engineering. 2007. V. 1. N 3. P. 784–787.
36. Bhatnagar G., Raman B. Robust watermarking in multiresolution Walsh-Hadamard transform // IEEE International Advance Computing Conference (IACC 2009). Patiala, Infia, 2009. Art. 4809134. P. 894–899.
37. Patra J. C., Phua J. E., Bornand C. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression

// Digital Signal Processing: A Review Journal. 2010. V. 20. № 6. P. 597–1611.

38. Maity S. P., Kundu M. K. DHT domain digital watermarking with low loss in image informations // AEU – International Journal of Electronics and Communications. 2010. V. 64. № 3. P. 243–257.
39. Maity S. P., Kundu M. K. Perceptually adaptive spread transform image watermarking scheme using Hadamard transform // Information Sciences. 2011. V. 181. № 3. P. 450–465.
40. Shabanali Fami E., Samavi S., Rezaee Kaviani H., Molaei Radani Z. Adaptive watermarking in Hadamard transform coefficients of textured image blocks // 16th International Symposium on Artificial Intelligence and Signal Processing. Shiraz, Iran, 2012. V. 2012. Art. 6313799. P. 503–507.
41. Wu X., Sun W. Robust copyright protection scheme for digital images using overlapping DCT and SVD // Applied Soft Computing Journal. 2013. V. 67. № 2. P. 1170–1182.
42. Sarker I. H., Iqbal S. Content-based image retrieval using Haar wavelet transform and color moment // Smart Computing Review. 2013. V. 3. N 3. P. 155–165.
43. Радиолокационные системы многофункциональных самолетов. Т. 1: РЛС – информационная основа боевых действий многофункциональных самолетов. Системы и алгоритмы первичной обработки радиолокационных сигналов / под ред. А. И. Канащенкова и В. И. Меркулова. М.: Радиотехника, 2006. 656 с.
44. Моделирование алгоритма сжатия ФМ-сигнала при влиянии активной помехи для решения задач помехоустойчивости / А. П. Шепета, А. Ю. Каплин, В. А. Ненашев, И. А. Юдин / Свидетельство о государственной регистрации программы для ЭВМ № 2016618938 от 10.08.2016 г.
45. Barker R. H. Group synchronizing of binary digital system // Communication theory. – London, 1953. – 273 p.

46. Современная радиолокация. Анализ, расчет и проектирование / под ред. Ю. В. Кобзарева. М.: Сов. радио, 1969. 704 с.
47. Ненашев В. А. Исследование влияния индустриальных помех на характеристики сжатия фазоманипулированных сигналов в первичных РЛС / В. А. Ненашев, В. А. Синицын, С. А. Страхов // Инновационные технологии и технические средства специального назначения: тр. IX общерос. науч.-практ. конф.: в 2 т. Балтийский государственный технический университет «Военмех» им. Д. Ф. Устинова. 2017. С. 351–355.
48. Трухачев А. А. Радиолокационные сигналы и их применения. М.: Воениздат, 2005. 320 с.
49. Ненашев В. А., Сергеев А. М., Капранова Е. А Исследование и анализ автокорреляционных функций кодовых последовательностей, сформированных на основе моноциклических квазиортогональных матриц // Информационно-управляющие системы. 2018. №3. С. 9 – 14. https://doi.org/10.31799/1684-8853-2018-4-9-14
50. Справочник по радиолокации / под. ред. М. И. Скольника. Пер. с англ. под общей ред. В. С. Вербы. Москва: Техносфера, 2015. 680 с.
51. Осипов Л. А. Помехоустойчивость беспроводной связи // Наука и техника транспорта. 2010. № 2. С. 52 – 56.
52. Балонин Н.А., Сергеев М.Б. О расширении ортогонального базиса в задачах сжатия видеоизображений // Вестник компьютерных и информационных технологий. 2014, № 2. С. 11 - 18.
53. 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
54. Vostrikov A. Expansion of the Quasi-Orthogonal Basis to Mask Images / A. Vostrikov, M. Sergeev // Smart Innovation, Systems and Technologies. 2015. T. 40. P. 161-168.

55. Balonin N. Construction of Transformation Basis for Video and Image Masking Procedures / N. Balonin, M. Sergeev // Frontiers in Artificial Intelligence and Applications. 2014. Т. 262. С. 462-467.
56. Сергеев А. М., Блаунштейн Н. Ш. Ортогональные матрицы симметричных структур для задач обработки изображений // Информационно-управляющие системы. 2017. № 6(91). С. 2–8.
57. 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.
58. Балонин Н. А., Сергеев М. Б. Нормы обобщенных матриц Адамара // Вестник Санкт-Петербургского университета. Сер. 10: Прикладная математика. Информатика. Процессы управления. 2014. № 2. С. 5–12.
59. Балонин Н. А. Вычисление матриц Адамара-Мерсенна / Н. А. Балонин, М. Б. Сергеев, Л. А. Мироновский // Информационно-управляющие системы. 2012. № 5(60). С. 92–94.
60. Балонин Н.А., Сергеев М.Б., Мироновский Л.А. Вычисление матриц Адамара-Ферма // Информационно-управляющие системы. 2012. № 6 (61). С. 90-93.
61. Балонин Н. А. О двух способах построения матриц Адамара-Эйлера / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2013. № 1(62). С. 7–10.
62. Балонин Ю.Н., Сергеев М.Б. Алгоритм и программа поиска и исследования М-матриц // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3 (85). С. 82 – 86.
63. Olivia Di Matteo Methods for parallel quantum circuit synthesis, fault-tolerant quantum RAM, and quantum state tomography. A thesis presented to the University of Waterloo in fullment of the thesis requirement for the degree

of Doctor of Philosophy in Physics - Quantum Information. Waterloo, Ontario, Canada, 2019. 98 p.

64. Balonin N.A. Dokovic D.Z. Symmetric Hadamard Matrices of Orders 268, 412, 436 and 604 // Информационно-управляющие системы. 2018. № 4. С. 2 – 8.
65. Paley R. E. A. C. On orthogonal matrices // Journal of mathematics and physics. 1933. Vol. 12. P. 311–320.
66. Baumert L. D., Golomb S. W. and Hall M. 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.
67. Baumert L. D. and Hall M. Jr. A new construction for Hadamard matrices // Bull. Amer. Math. Sot. 71 (1965), 169-170.
68. Baumert L. D. Hadamard matrices of orders 116 and 232 // Bull. Amer. Math. Soc. 72 (1966), no. 2. P.237.
69. Scarpis U. Sui determinanti di valore Massimo // Rendiconti della R. Istituto Lombardo di scienze e lettere. 1898. No. 31. P. 1441–1446.
70. Балонин Н.А., Джокович Д. Симметрия двуциклических матриц Адамара и периодические пары Голея // Информационно-управляющие системы. 2015. № 3 (76). С. 2-16.
71. Williamson J. Hadamard’s Determinant Theorem and the Sum of Four Squares // Duke Math. J. 1944. № 11. P. 65–81.
72. Horadam K. J. Hadamard matrices and their applications: Progress 2007–2010 // Cryptography and Communications. 2010. Volume 2. Issue 2. Pp 129–154.
73. Yang Y.X., Niu X.X., Xu C.Q.: Theory and Applications of Higher-Dimension Hadamard Matrices, 2nd edn. Chapman and Hall. 2010. 437 p.
74. Sergeev A. Generalized Mersenne Matrices and Balonin’s Conjecture // Automatic Control and Computer Sciences, 2014, Vol. 48, No. 4, pp. 214–220. DOI: 10.3103/S0146411614040063

75. Belevitch V. Theorem of 2n-terminal Networks with Application to Conference Telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
76. Seidel J. J. Strongly Regular Graphs with (–1, 1, 0) Adjacency Matrix Having Eigenvalue 3 // Lin. Alg. Appl. 1968. Vol. 1. P. 281–298
77. Балонин Н.А. О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 89 - 90.
78. Балонин Ю.Н., Востриков А.А., Егорова И.С., Сергеев А. М. О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел // Труды СПИИРАН, 2017. Вып. 50. С. 209-223. DOI: http://dx.doi.org/10.15622/sp.50.9
79. Балонин Н. А. Динамические генераторы квазиортогональных матриц семейства Адамара / Н. А. Балонин, М. Б. Сергеев, В. С. Суздаль // Труды СПИИРАН. 2017. Вып. 5(54). С. 224–243.
80. Сергеев А. М. О взаимосвязи одного вида квазиортогональных матриц, построенных на порядках последовательностей 4k и 4k – 1 / А. М. Сергеев // Известия ЛЭТИ. 2017. № 7. С. 12–17.
81. Balonin N. A., Vostrikov A. A. and Sergeev M. B. On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices // Automatic Control and Computer Sciences. 2015. Vol. 49. No. 3. Pp. 153–158.
82. Балонин Ю.Н., Сергеев М.Б. М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5 (54). С. 87-90.
83. Балонин Н. А., Сергеев М. Б. Матрица золотого сечения G10 // Информационно-управляющие системы. 2013. № 6(67). С. 2–5.
84. Балонин Н.А., Сергеев М.Б. Матрицы Пропус 92 и 116 // Информационно-управляющие системы. 2016. № 2 (81). С. 101-103.
85. Construction of Symmetric Hadamard Matrices / Н. А.Балонин, Ю. Н. Балонин, Д. Ж. Джокович и др. // Информационно-управляющие системы 2017. № 5(90). С. 2–11.

86. Seberry J., Balonin N.A. Two Infinite Families of Symmetric Hadamard Matrices // Australasian Journal of Combinatorics. 2017. Т. 69. № 3. С. 349-357.
87. Seberry J., Yamada M. Hadamard matrices, sequences, and block designs // Contemporary design theory: A collection of surveys, J. H. Dinitz and D. R. Stinson. eds., John Wiley and Sons, Inc. 1992. P. 431–560.
88. Colbourn Charles J. Handbook of combinatorial designs. Discrete mathematics and its applications. 2nd ed. / Charles J. Colbourn, Jeffrey H. Dinitz eds. Chapman and Hall/CRC, 2006. 1000 p.
89. Balonin N. A., Djokovic D. Z., Karbovskiy D. A. Construction of symmetric Hadamard matrices of order 4v for v=47, 73, 113 // Special matrices. 2018. Vol. 6. P. 11–22.
90. Balonin N.A., Djokovic D.Z. Negaperiodic Golay Pairs and Hadamard Matrices // Информационно-управляющие системы. 2015. № 5 (78). С. 2-17.
91. Сергеев А.М., Востриков А.А. Специальные матрицы: вычисление и применение. СПб: Политехника. 2018. 112 с.
92. Hall, M. A Survey of Difference Sets // Proc. Amer. Math. Soc. 7. 1956. P. 975–986.
93. Вычисление матриц Месенна-Уолша / Н. А. Балонин, Ю. Н. Балонин, А. А. Востриков, М. Б. Сергеев // Вестник компьютерных и информационных технологий. 2014. № 11(125). С. 51–56.
94. Балонин Ю. Н., Сергеев А. М., Егорова И. С. Фильтры Мерсеннна-Уолша для видеоданных в IP-сетях / Региональная информатика и информационная безопасность сб. тр. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 367–371.

95. 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.
96. Балонин Н. А., Сергеев М. Б. Расширение гипотезы Райзера на двуциклические структуры и разрешимость матриц Адамара орнаментом в виде бицикла с двойной каймой // Информационно-управляющие системы. 2017. № 1. С. 2–10.
97. Balonin Yu. N., Sergeev A. M. Two-Circulant Hadamard Matrices, Weighing Matrices, and Ryser's Conjecture // Информационно-управляющие системы. 2018. № 3. С. 2 – 9. doi:10.15217/issn1684-8853.2018.3.2
98. Балонин Ю.Н., Сергеев А.М. Эффект чередования матриц Адамара и взвешенных матриц и граница их симметрии. В сборнике: Научная сессия ГУАП. Сборник докладов. В 3-х частях. Ч. II. Технические науки. 2018. С. 224-227.
99. Djokovic D. Z. Good Matrices of Orders 33, 35 and 127 // JCMCC. 1993. № 14. P. 145–152.
100. Seberry J., Balonin N. The Propus Construction for Symmetric Hadamard Matrices // arXiv:1512.01732 [math.co].
101. Di Matteo, O. Symmetric Hadamard Matrices of Order 116 and 172 Exist / O. Di Matteo, D. Z. Djokovic, I. S. Kotsireas // Special Matrices. 2015. Vol. 31. P. 227–234.
102. Карбовский Д. А. Поиск симметричных матриц Адамара в форме трехцикла Пропус порядков 96, 104 // сб. докл.: Научная сессия ГУАП: Технические науки Ч. II /СПб.: ГУАП. СПб., 2017. С. 247–249.
103. Востриков А. А., Балонин Ю. Н., Куртяник Д. В., Сергеев А. М., Синицына О. И. О гибридном методе защиты видеоданных в IP-сетях // Телекоммуникации. 2018. № 2. С. 34-39
104. Востриков А. А., Чернышев С. А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-

технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99-103.

105. Астапкович А. М., Востриков А. А., Касаткин А. А., Чудиновский Ю. Г. Опыт использования информационно-управляющих сетевых систем для передачи видеоизображений // Информационно-управляющие системы для подвижных объектов. Семинары ASK Lab 2001 / Под общ. ред. М.Б. Сергеева. – СПб: Политехника, 2002. С. 180–197.
106. Balonin N. A., Vostrikov A. A., Sergeev M. B. Two-Circulant Golden Ratio Matrices // Информационно-управляющие системы. 2014. № 5(72). С. 5–11.
107. Балонин Н. А., Сергеев М. Б. О значении матриц начального приближения в алгоритме поиска обобщенных взвешенных матриц глобального и локального максимума детерминанта // Информационно-управляющие системы. 2015. № 6(79). С. 2–9.
108. Балонин Ю. Н., Егорова И. С., Сергеев А. М. Алгоритм преобразования циклических матриц в негациклические. Научная сессия ГУАП:сб.докл.:в 3 ч. Ч II. Технические науки / СПб.: ГУАП, СПб., 2016. С. 132-134.
109. Балонин Ю.Н., Егорова И. С., Сергеев А. М. Негациклические матрицы и фильтры Мерсенна // Вестник информационных и компьютерных технологий. 2016. № 11, с. 20 – 24. DOI: 10.14489/vkit.2016.11.pp.020-024
110. Balonin N., Sergeev M. Quasi-orthogonal Local Maximum Determinant Matrices. Applied Mathematical Sciences, 2015, vol. 9, no. 6, pp. 285–293. DOI 10.12988/ams.2015.4111000
111. Balonin N. A., Seberry J. Remarks on Extremal and Maximum Determinant Matrices with Moduli of Real Entries ≤ 1 // Informatsionno-upravliaiushchie sistemy [Information and Control Systems]. 2014. No. 5 (71). P. 2–4.
112. Балонин, Н. А., Сергеев М. Б. Матрицы Мерсенна и Адамара // Информационно-управляющие системы. 2016. № 1(80). С. 2–15.

113. Балонин Ю. Н., Клюковкин В. Р., Сергеев А. М. Численный алгоритм эффективного поиска бициклических матриц на основе таблицы перекрестных ссылок. Научная сессия ГУАП:сб.докл.: В 3 ч. Ч.II. Технические науки/СПб.:ГУАП. СПб, 2017. С. 179-184.
114. Rokicki T. New records for maximal determinants, based on pairs of circulant matrices. http://tomas. rokicki.com/newrec.html.
115. Балонин Н. А., Марлей В. Е., Сергеев М. Б. Новые возможности математической сети для коллективных исследований и моделирования в Интернете // Информационно-управляющие системы. 2014. № 3 (70). С. 40–46.
116. Балонин Н. А., Сергеев М. Б. Двуциклическая М-матрица 22-го порядка // Информационно-управляющие системы. 2014. № 2 (69). С. 109–111.
117. Балонин Н. А., Сергеев М. Б. Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационно-управляющие системы. 2013. № 5 (66). С. 97–98.
118. Программный комплекс поиска бициклических матриц на основе таблицы перекрестных ссылок / Ю. Н. Балонин, А. М. Сергеев / Свидетельство о государственной регистрации программы для ЭВМ № 2018616390 от 01.06.2018 г.
119. Программный комплекс клиент-серверного поиска бициклических матриц Адамара в реальном масштабе времени / Ю. Н. Балонин, А. М. Сергеев / Свидетельство о государственной регистрации программы для ЭВМ № 2018617112 от 19.06.2018 г.
120. Балонин Ю.Н., Сергеев А.М Алгоритм накопления последовательностей для таблицы перекрестных ссылок. – В сборнике: Научная сессия ГУАП. Сборник докладов. В 3-х частях. Ч. II. Технические науки. 2018. С. 221-223.

121. Исследование связей семейств квазиортогональных матриц порядков, принадлежащих известным последовательностям чисел, и разработка методов их поиска: отчет о НИР (промежуточный) / Санкт-Петербургский гос.университет аэрокосмического приборостроения (ГУАП); рук. М. Б. Сергеев; № ГР АААА-А17-117042710042-9. СПб., 2017. 110 с.
122. 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.
123. Lee, M. H. A new reverse Jacket transform and its fast algorithm 91 / M. H. Lee // IEEE Transactions on circuits and systems II, 47(2000). P. 39-47.
124. Lee, M. H. Jacket Matrices: Constructions and Its Applications for Fast Cooperative Wireless Signal Processing / M. H. Lee / LAP LAMBERT Publishing, Germany, 2012.
125. Finlayson K., Lee M. H., Seberry, J. Yamada M. Jacket Matrices constructed from Hadamard Matrices and Generalized Hadamdrd Matrices. Australasian Journal of Combinatorics, 35 (2006). pp.83-87
126. Фаворская М. Н., Савчина Е. И. Улучшение контраста изображений на основе статистического анализа вейвлет-коэффициентов // DSPA: Вопросы применения цифровой обработки сигналов. 2018. Т.8. № 4. С. 147 – 151.
127. Программный комплекс клиент-серверного поиска бициклических матриц Адамара в реальном масштабе времени / Ю. Н. Балонин, А. М. Сергеев / Свидетельство о государственной регистрации программы для ЭВМ № 2018617112 от 19.06.2018 г.
128. Программный комплекс поиска бициклических матриц на основе таблицы перекрестных ссылок / Ю. Н. Балонин, А. М. Сергеев / Свидетельство о государственной регистрации программы для ЭВМ № 2018616390 от 01.06.2018 г.

129. Программный комплекс поиска матриц локального максимума детерминанта с самомасштабированием / Ю. Н. Балонин, А. М. Сергеев, О. И. Синицина / Свидетельство о государственной регистрации программы для ЭВМ № 2018616389 от 01.06.2018 г.
130. Программа вычисления структурированных квазиортогональных матриц Мерсенна / Востриков А.А., Сергеев А.М., Куртяник Д.В., Ненашев С.А., Григорьев Е.К. / Свидетельство о государственной регистрации программы для ЭВМ № 2019612775 от 27.02.2019 г.
131. Специальное программное обеспечение для приема по беспроводному каналу, декодирования, демаскирования с использованием квазиортогональных матриц, декомпрессии и воспроизведения видеоизображений с малым временем актуальности / Бодня Д. В., Востриков А. А., Балонин Ю. Н., Сергеев А. М., Чернышев С. А. / Свидетельство о государственной регистрации программы для ЭВМ № 2017616795. Зарегистрировано в реестре программ для ЭВМ от 14 июня 2017 г.
132. Специальное программное обеспечение для маскирования с использованием квазиортогональных матриц, помехоустойчивого кодирования, сжатия и беспроводной передачи видеоизображений с малым временем актуальности / Бодня Д.В., Востриков А. А., Егорова И.С., Сергеев А. М., Капранова Е.А., Синицына О.И. / Свидетельство о государственной регистрации программы для ЭВМ № 2017616930. Зарегистрировано в реестре программ для ЭВМ от 20 июня 2017 г.
133. Цифровое маскирование матрицами Мерсенна и его особые изображения / Ю. Н. Балонин, А. А. Востриков, Е. А. Капранова, Сергеев А. М. и др. // Фундаментальные исследования. 2017. № 4-1. С. 13-18.

134. Digital masking using Mersenne matrices and its special images / A. Vostricov, M. Sergeev, N. Balonin, S. Chernyshev // Procedia Computer Science. 2017. Vol. 112. P. 1151-1159.
135. Среда моделирования этапов обработки фото- и видеоизображений. Плагин маскирования / Чернышев С.А., Сергеев А.М., Куртяник Д.В. / Свидетельство о государственной регистрации программы для ЭВМ № 2018664105 от 12 ноября 2018 г.
136. Балонин Ю. Н., Егорова И. С., Сергеев А. М. Исследование соответствия структур и порядков матриц Мерсенна. Научная сессия ГУАП:сб.докл.:в 3 ч. Ч II. Технические науки / СПб.: ГУАП, СПб., 2016. С. 134-138.
137. Беззатеев С.В., Крук Е.А., Литвинов М.Ю., Сергеев А.М. Converted Transformation of the Image with the Structure Destroying // XI International Symposium on Problems of Redundancy in Information and Control Systems: Proceeding/ Saint-Petersburg State University of Aerospace Instrumentation (SUAI). 2007. - P.173.
138. Соловьев Н. В., Сергеев А. М. Особенности применения ортогональных (квазиортогональных) матриц для сжатия растровых изображений // Научная сессия ГУАП: сб. докл.: в 3 ч. Ч. II. Технические науки / СПб.: ГУАП, 2018. С. 402-404.
139. Balonin Y., Abuzin L., Sergeev A., Nenashev V. The Study of Generators of Orthogonal Pseudo-Random Sequences // Smart Innovation, Systems and Technologies. Volume 143. Springer, 2019. P.125 – 133. https://doi.org/10.1007/978-981-13-8303-8.
140. Ненашев В.А., Сергеев А.М., Капранова Е.А., Рыжов К.Ю. Эксперименты по замене ДКП квазиортогональным преобразованием в алгоритмах сжатия изображений. В сборнике: Научная сессия ГУАП Сборник докладов. В 3-х частях. Ч. II. Технические науки. 2018. С. 369-373.

141. Kapranova, E. Compression and coding of images for satellite systems of Earth remote sensing based on quasi-orthogonal matrices / E. Kapranova, V. Nenashev, M. Sergeev // Proceedings of SPIE Vol. 10789, Image and Signal Processing for Remote Sensing XXIV, 1078923.
142. Косткин, И.В. Исследование взаимосвязи объективных и субъективных критериев качества мультимедийных изображений / И. В. Косткин // Молодежный научный вестник. 2016. № 5. С. 55 – 64.
143. Утилита внедрения ЦВЗ в изображения/Image DWM Embed Tool / Григорьян А.К., Литвинов М.Ю., Сергеев А.М. / Свидетельство о государственной регистрации программы для ЭВМ № 2011618156. Зарегистрировано в реестре программ для ЭВМ 18 октября 2011. Заявка № 2011616481 от 22 августа 2011.
144. Утилита извлечения ЦВЗ из изображений/ Image DWM Detect&Extract Tool / Григорьян А.К., Литвинов М.Ю., Сергеев А.М. / Свидетельство о государственной регистрации программы для ЭВМ № 2011618157. Зарегистрировано в реестре программ для ЭВМ 18 октября 2011. Заявка № 2011616482 от 22 августа 2011 г.
145. Barba, G. Intorno al Teorema di Hadamard sui Determinanti a Valore Massimo / G.Barba // Giorn. Mat. Battaglini. 1933. Vol. 71. P. 70–86.
146. Ненашев В. А., Сергеев А. М., Сергеев М. Б. Вложенные кодовые конструкции Баркера-Мерсенна-Рагхаварао // Информационно-управляющие системы. 2019. № 3. С. 63-73. doi: 10.31799/1684-8853-2019-3-63-73.
147. 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. https://doi.org/10.1007/978-981-13-8303-8.
148. Поиск и классификация симметричных квазиортогональных матриц и их применение в задачах обработки и передачи информации в открытых

радиоканалах: отчет о НИР (промежуточный, 2 этап) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Сергеев А. М. [и др.]. СПб., 2018. 111 с. – № ГР АААА-А17-117042710042-9.

149. Волынская А. В. Результаты математического моделирования процесса поиска кодовых последовательностей с заданными корреляционными свойствами // Вестник Уральского государственного университета путей сообщения. 2009. № 3-4. С. 64 – 71.
150. Волынская А.В., Калинин П.М. Новые помехоустойчивые сигналы для интеллектуального канала телемеханики // Фундаментальные исследования. 2012. № 11. С.922 – 926.

ПРИЛОЖЕНИЕ 1. Среда моделирования

Разработанная среда моделирования этапов обработки изображений (кадров видеопоследовательностей) позволяет автоматизировать процесс разработки и моделирования алгоритмов их преобразования с возможностью прослеживания изменений на каждом этапе. В среде для удобства отладки процессов преобразования обеспечивается пошаговый анализ разрабатываемых алгоритмов.

Выбранная архитектура программного обеспечения позволяет разработчикам реализовывать и подключать собственные плагины с блоками обработки видео- и фото-информации для его дополнения. Использование при разработке библиотеки OpenCV делает возможным как реализацию собственных методов обработки изображений, так и использование уже готовых решений из данной библиотеки.

Моделирование этапов обработки изображений в имитационной среде. Известно, что процедуры компрессии и декомпрессии, защитного кодирования и декодирования симметричны. Это является основанием использования в данных процедурах ортогональных преобразований.

Среда имитационного моделирования изначально ориентирована на академическое сообщество. Важной ее особенностью является возможность создания собственных расширений (плагинов). Если в предоставляемом базовом комплекте нет реализации некоторых методов обработки изображений или разрабатывается свой уникальный, то разработчик сможет добавлять реализацию существующих алгоритмов цифровой обработки изображений в уже разработанные плагины – данная среда моделирования является Open Source проектом и исходные коды будут выложены на GitHub.

При разработке среды моделирования использовался следующий стек технологий:

– язык программирования – C++;

– библиотека компьютерного зрения OpenCV;

– кроссплатформенный фреймворк Qt.

Использование OpenCV позволило значительно ускорить разработку среды моделирования, поскольку в ней имеется реализация большинства алгоритмов цифровой обработки изображений, и она не исключает возможность реализовывать новые алгоритмы обработки.

Qt как кроссплатформенный фреймворк для разработки программного обеспечения, позволяет быстро и эффективно проектировать, разрабатывать, выпускать и сопровождать программные продукты, обеспечивающие единый UX среди всех используемых платформ.

Плагинная архитектура разработанной среды позволяет вести разработку не одной группе разработчиков, поскольку нет необходимости вносить изменения в исходные коды основной программы, а только придерживаться предлагаемой архитектуры для разрабатываемых плагинов.

На рисунке П.1 приведен общий вид архитектуры разработанной среды моделирования:

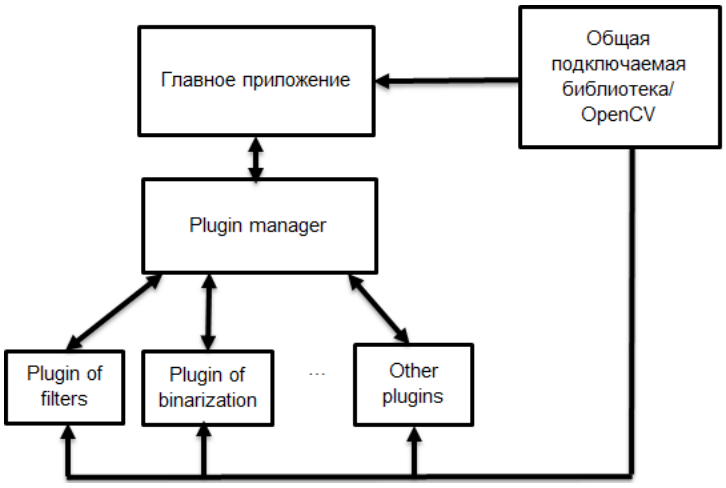


Рисунок П.1 – Общий вид архитектуры среды моделирования

Это совокупность основного программного обеспечения, общей библиотеки и плагинов, перечисленных на рис. П.1. На плагины получены

свидетельства о государственной регистрации программ для ЭВМ (РОСПАТЕНТ).

Графический пользовательский интерфейс (GUI) программного обеспечения представлен на рис. П.2, где для примера использована цепочка с блоками: «Image In», «Rotate», «Threshold», «ROI».

В блоке «Image In» задается входное изображение и частота его отправки по цепочке блоков. В блоке «Rotate» задается коэффициент скалирования изображения, угол поворота, и координаты, относительно которых осуществляется поворот. Блок «Threshold» отвечает за бинаризацию изображения. В блоке «ROI» осуществляется «вырезание» региона интереса из входного изображения.

После двойного клика манипулятором «мышь» по любому из блоков появляется виджет для его настройки. На рис. П.3 приведены виджеты для блока «Image In» (а), «Rotate» (б), «Threshold» (в), «ROI» (г).

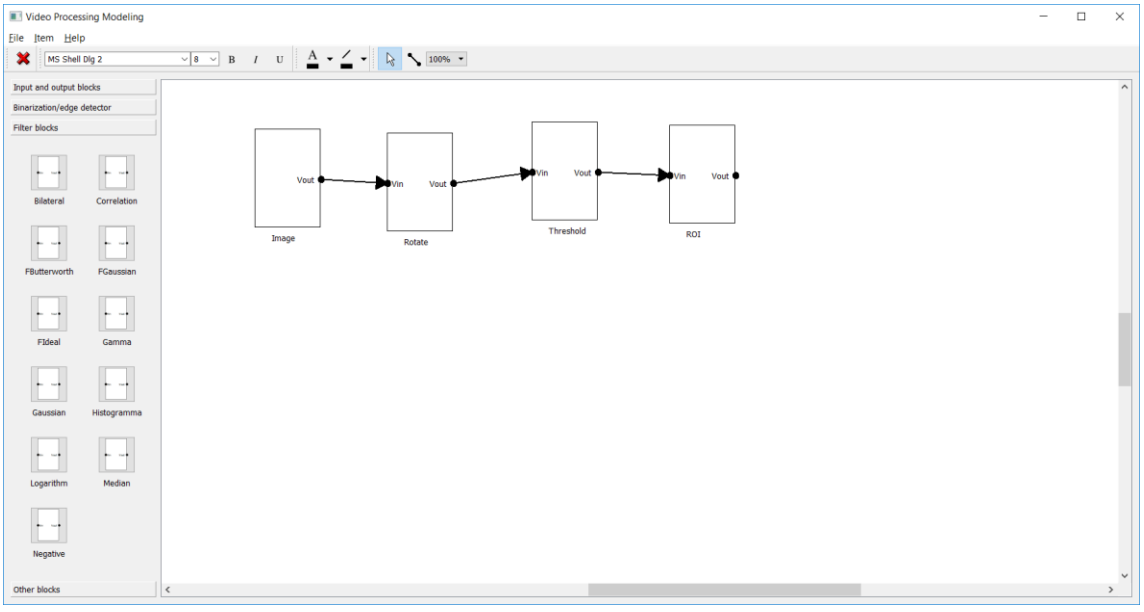


Рисунок П.2 – GUI программного обеспечения

В качестве первых алгоритмов, отработанных в разработанной среде моделирования, были не только манипуляции с изображениями, описанные

выше, но и процедура их маскирования в реальном масштабе времени, описанная в диссертационной работе.

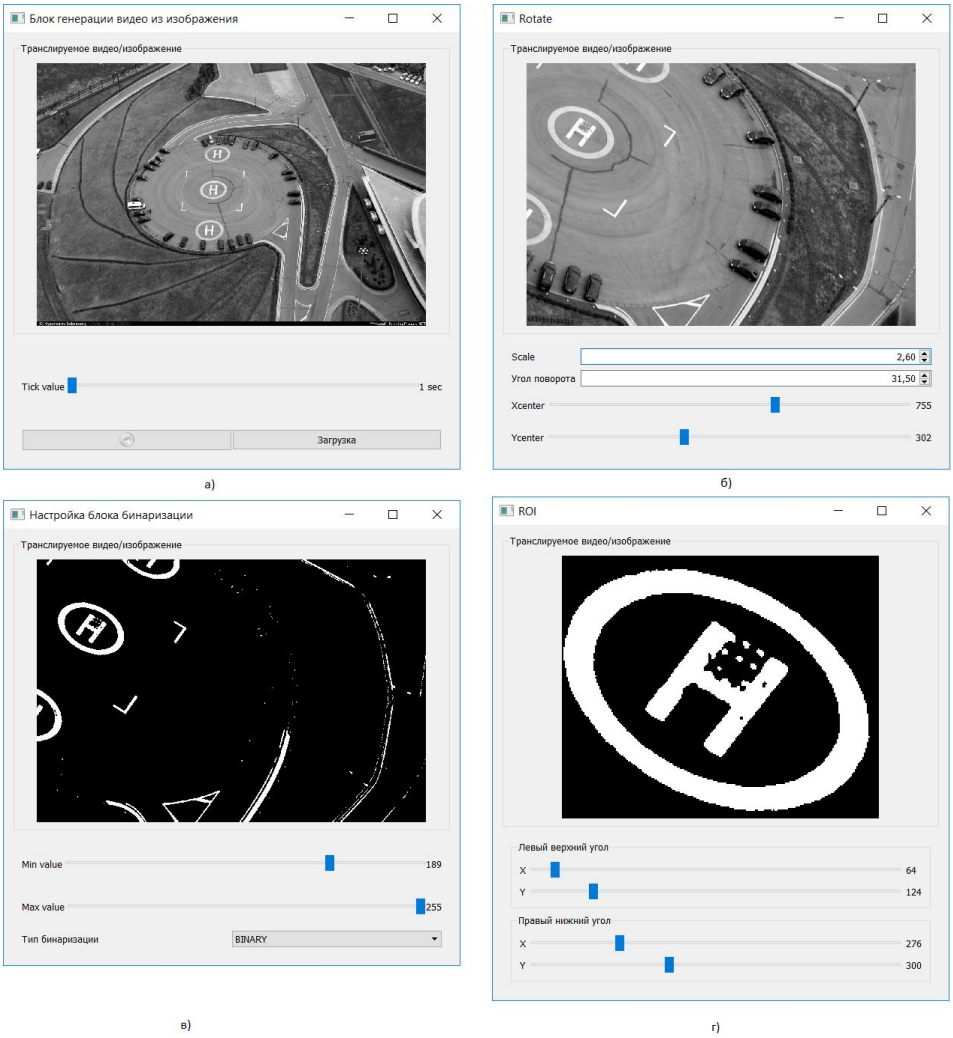


Рисунок П.3 – Пример виджетов настройки блоков обработки изображений

Среда моделирования предусматривает формирование библиотеки квазиортогональных матриц, таких как матрицы Адамара симметричных конструкций, матрицы Мерсенна-Уолша, Адамара-Уолша, Мерсенна, Ферма, Эйлера и др., и предоставляет возможность отработки этапов маскирования и сжатия изображений, включая совмещения их в одном плагине.

ПРИЛОЖЕНИЕ 2. Акты внедрения

ASK Lab
АСК Лаборатория

ООО «АСК Лаборатория»
ИНН 7801396519, КПП 780101001
ОГРН 1057813226020, ОКПО 79716262
р/с 40702810222070000602
в филиале «Санкт-Петербургская дирекция ОАО «УралСиб»
к/с 30101810800000000706, БИК 044030706

"У Т В Е Р Ж Д А Ю "
Генеральный директор
ООО «АСК Лаборатория»
канд. техн. наук, доцент
_____ А. А. Востриков
" 24 " апреля 2019 г.

А К Т
об использовании результатов диссертационной работы
Сергеева Александра Михайловича
“Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц”,
представляемой на соискание ученой степени кандидата технических наук.

Комиссия в составе:
Чудиновского Юрия Геннадьевича, главного инженера
Анисимова Андрея Леонидовича, ведущего инженера
Гончарова Александра Андреевича, инженера-системотехника
составила настоящий акт об использовании результатов диссертационной работы Сергеева А. М. в опытно-конструкторской работе, выполненной по договору №1/14 от 14.01.2014 г. с Заказчиком на создание опытных образцов электронных модулей видеорегистратора мобильного назначения.

Разработанные автором диссертационной работы технические решения применяются в настоящее время Заказчиком работы при серийном производстве мобильных видеорегистраторов, обеспечивающих защищенный беспроводный дистанционный съём выполняемых видеозаписей на подвижных объектах по каналам, реализуемым через WiFi и на частоте 868 МГц.

Предложенная автором модификация метода, включающего матричное маскирование последовательности кадров квазиортогональными матрицами и помехоустойчивое кодирование в радиоканале, используется в программе электронного модуля на системе-на-кристалле с DSP-сопроцессорами ADSP-BF523KBCZ.

Опыт использования разработанных электронных модулей показал, что метод и выбранное для него семейство квазиортогональных матриц как основа маскирования и помехоустойчивого кодирования при беспроводной передаче в условиях активных помех, позволяют значительно снизить их влияние на содержимое кадров, а также эффективно обнаруживать потери блоков данных. Это существенно повышает устойчивость функционирования распределенных видеосистем, в том числе мобильными видеорегистраторами, построенных на базе предложенного технического решения.

Члены комиссии _____ Ю. Г. Чудиновский
_____ А. Л. Анисимов
_____ А. А. Гончаров

199034, г. Санкт-Петербург, В.О., 16 линия, д. 7
тел./факс: (812) 448-53-52; e-mail: mail@ask-lab.com; www.ask-lab.com
Лицензия УФСБ РФ по СПб и ЛО №0004612 от 02.11.2011 г.

АКЦИОНЕРНОЕ ОБЩЕСТВО
"Концерн "Гранит-Электрон"
ФЕДЕРАЛЬНЫЙ НАУЧНО-ПРОИЗВОДСТВЕННЫЙ ЦЕНТР
Россия, 191014, Санкт-Петербург, Госпитальная ул., 3, факс: +7-812-274 63 39, +7-812-274 03 06, тел.: +7-812-271 45 85, e-mail: cri-granit@peterlink.ru

_____ № _____

УТВЕРЖДАЮ

Первый заместитель
генерального директора
АО «Концерн «Гранит-Электрон»
по науке
доктор технических наук, профессор

Ю.Ф. Подоплекин
28 мая 2019 г.

АКТ

об использовании результатов диссертационной работы

Сергеева Александра Михайловича,

представляемой на соискание ученой степени кандидата технических наук.

Комиссия в составе

Председателя Селивохина О.С. – Главного научного сотрудника НИЛ 5032

Членов комиссии:

Ямщикова Ю.А. – начальника ОРПНР

Ицковича Ю.С. – ведущего научного сотрудника НИЛ-5032

Мальцева О.И. – начальника НИЛ-8312

составила настоящий акт об использовании результатов диссертационной работы Сергеева А. М., а именно – помехоустойчивых

кодов Мерсенна в опытно-конструкторских работах АО "Концерн "Гранит-Электрон" по проектированию перспективных РЛС.

Предложенные автором коды на основе моноциклических квазиортогональных матриц Мерсенна применимы при амплитудной модуляции сверхширокополосного сигнала и фазовой модуляции широкополосного сигнала как альтернатива кодам Баркера, а разработанные технические решения по генерации, синтезу и обработке – в современных системах обнаружения и выделения сигнала на фоне шумов естественного и искусственного происхождения.

Проведенные в рамках ОКР испытания показали, что оценка уровня боковых лепестков автокорреляционной функции, предложенных автором кодов Мерсенна, длины 3 и 7, ниже на 3,52 дБ и 1,78 дБ, соответственно, чем у аналогичных кодов Баркера. На основе этих кодов были синтезирован кодо-модулированные сигналы и вложенные сигнально-кодовые конструкции, позволяющие значительно улучшить характеристики обнаружения полезного сигнала в условиях сложной электромагнитной обстановки.

Применение указанных результатов диссертационной работы позволило повысить ТТХ перспективных изделий и имеет существенное значение для развития исследований в области помехоустойчивого кодирования.

Главный научный сотрудник НИЛ 5032 Селивохин О.С.
Начальник ОРПНР Ямщиков Ю.А.
Ведущий научный сотрудник НИЛ-5032 Ицкович Ю.С.
Начальник НИЛ-8312 Мальцев О.И.

Подписи председателя и членов комиссии: главного научного сотрудника НИЛ 5032 Селивохина Олега Сергеевича, начальника ОРПНР

Ямщикова Юрия Алексеевича, ведущего научного сотрудника НИЛ-5032 Ицковича Юрия Соломоновича, начальника НИЛ-8312 Мальцева Олега Григорьевича заверяю.

Ученый секретарь
АО «Концерн «Гранит-Электрон» Васильевский А.С.

ГУАП

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

Большая Морская ул., д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057,
E-mail: common@aanet.ru; http://www.guap.ru; ОКПО 02068462; ОГРН 1027810232680; ИНН/КПП 7812003110/783801001

_____ № _____

На № _____ от _____

«УТВЕРЖДАЮ»
Проректор ГУАП по
образовательным технологиям и
инновационной деятельности
д-р техн. наук, профессор

_____ В. Ф. Шишлаков

«26» сентября 2019 г.

АКТ

внедрения научных результатов диссертационной работы Сергеева Александра Михайловича, выполненной на тему «Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц» и представляемой на соискание ученой степени кандидата технических наук

Комиссия в составе

Рабина Алексея Владимировича, кандидата технических наук, доцента, директор центра координации научных исследований,
Соловьева Николая Владимировича, кандидата технических наук, доцента кафедры вычислительных систем и сетей,
Чернышева Станислава Андреевича, кандидата технических наук, старшего преподавателя кафедры вычислительных систем и сетей

составила настоящий акт о том, что научные результаты, полученные лично Сергеевым Александром Михайловичем, а именно:

- модифицированный метод матричного маскирования изображений с набором специальных бициклических квазиортогональных матриц;
- алгоритмы маскирования и кодирования визуальных данных с использованием специальных квазиортогональных матриц;
- алгоритм декодирования и демаскирования визуальных данных с использованием специальных квазиортогональных матриц

были использованы в программном обеспечении:

Специальное программное обеспечение для приема по беспроводному каналу, декодирования, демаскирования с использованием квазиортогональных матриц, декомпрессии и воспроизведения видеоизображений с малым временем актуальности / Бодня Д.В., Балонин Ю. Н., Сергеев А. М. и др. / Свидетельство о государственной регистрации программы для ЭВМ № 2017616795 от 14.06.2017,

Специальное программное обеспечение для маскирования с использованием квазиортогональных матриц, помехоустойчивого кодирования, сжатия и беспроводной передачи видеоизображений с малым временем актуальности / Бодня Д.В., Востриков А. А., Сергеев А. М. и др. / Свидетельство о государственной регистрации программы для ЭВМ № 2017616930 от 20.06.2017,

разработанном при выполнении научно-исследовательской работы

Оптико-электронный модуль мобильного применения: отчет о НИР / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Сергеев А. М. [и др.]. СПб., 2018. 56 с. – гос. рег. № 117032810028-3

Директор центра координации научных исследований ГУАП, канд. техн. наук, доцент — А. В. Рабин

Доцент кафедры вычислительных систем и сетей, канд. техн. наук — Н. В. Соловьев

Старший преподаватель кафедры вычислительных систем и сетей, канд. техн. наук — С. А. Чернышев

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

Большая Морская ул., д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057,
E-mail: common@aanet.ru; http://www.guap.ru; ОКПО 02068462; ОГРН 1027810232680; ИНН/КПП 7812003110/783801001

_____ № _____

На № _____ от _____

«УТВЕРЖДАЮ»
Проректор ГУАП
по учебной деятельности
канд. техн. наук, доцент
_____ В. А. Матьяш
"11" 09 2019 г.

А К Т

об использовании результатов диссертационной работы Сергеева Александра Михайловича на тему «Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц», представляемой на соискание ученой степени кандидата технических наук.

Комиссия в составе:

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

доктор технических наук, профессор, профессор кафедры проблемно-ориентированных вычислительных комплексов Шепета Александр Павлович

кандидат технических наук, доцент, заведующий кафедрой безопасности информационных систем Овчинников Андрей Анатольевич

составила настоящий акт о том, что результаты диссертационной работы Сергеева А. М., 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):
   - «Проектирование систем обработки и передачи информации» (Лабораторная работа «Реализация матричных операций в ПЛИС для обработки визуальной информации»);
   - «Цифровая обработка изображений» (Лабораторная работа «Матричные способы обработки изображений»);
2) на кафедре безопасности информационных систем в лекционном курсе дисциплины «Технологии стеганографии в системах инфокоммуникаций», включенной в программу подготовки по направлениям 10.03.01 – «Информационная безопасность» и 11.03.02 – «Инфокоммуникационные технологии и системы связи».

Члены комиссии  А. В. Гордеев

А. П. Шепета

А. А. Овчинников

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

Большая Морская ул., д. 67, лит. А, Санкт-Петербург, 190000, Тел. (812) 710-6510, факс (812) 494-7057,
E-mail: common@aanet.ru; http://www.guap.ru; ОКПО 02068462; ОГРН 1027810232680; ИНН/КПП 7812003110/783801001

_____ № _____

На № _____ от _____

«УТВЕРЖДАЮ»
Проректор ГУАП по
образовательным технологиям и
инновационной деятельности
д-р техн. наук, профессор

_____ В. Ф. Шишлаков

«26» сентября 2019 г.

АКТ

внедрения научных результатов диссертационной работы
Сергеева Александра Михайловича на тему «Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц», представляемой на соискание ученой степени кандидата технических наук

Комиссия в составе

Рабина Алексея Владимировича, кандидата технических наук, доцента, директора центра координации научных исследований,
Ненашева Вадима Александровича, кандидата технических наук, доцента кафедры вычислительных систем и сетей,
Чернышева Станислава Андреевича, кандидата технических наук, старшего преподавателя кафедры вычислительных систем и сетей

составила настоящий акт о том, что научные результаты, полученные лично Сергеевым Александром Михайловичем, а именно:

1) классификация малоуровневых квазиортогональных матриц порядков, отвечающих известным числовым последовательностям $4t$, $4t-1$, $4t-2$, $4t-3$,

2) выявленная связь структур квазиортогональных матриц, построенных на порядках последовательностей $4t$ и $4t-1$, обеспечивающая гарантированное вычисление матриц Адамара нового вида – «ядро с окаймлением»,

3) численный метод поиска квазиортогональных матриц симметричных бициклических структур на основе таблицы перекрестных ссылок,

4) метод маскирования изображений на основе двустороннего умножения их фрагментов на квазиортогональные матрицы соответствующего порядка,

5) особые изображения для матриц Мерсенна, Мерсенна-Уолша, Эйлера, Ферма, инвариантные к двустороннему матричному преобразованию при их маскировании для передачи в IP-сетях,

6) двухуровневые несимметричные $\{1, -b\}$ кодовые последовательности Мерсенна длин 3, 7 и 11 для фазовой (амплитудной) модуляции сигналов в радиоканале,

7) конструкции вложенных кодов с использованием комбинаций последовательностей Баркера и Мерсенна

использованы в отчетах о научно-исследовательской работе «Поиск и исследование экстремальных квазиортогональных матриц для задач обработки информации», выполняемой при поддержке Минобрнауки РФ в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/4.6:

Исследование связей семейств квазиортогональных матриц порядков, принадлежащих известным последовательностям чисел, и разработка методов их поиска: отчет о НИР (промежуточный, 1 этап) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Сергеев А. М. [и др.]. СПб., 2017. 110 с. – № ГР АААА-А17-117042710042-9.

Поиск и классификация симметричных квазиортогональных матриц и их применение в задачах обработки и передачи информации в открытых радиоканалах: отчет о НИР (промежуточный, 2 этап) / Санкт-Петербургский гос. университет аэрокосмического приборостроения (ГУАП); рук. Сергеев М. Б.; исполн.: Сергеев А. М. [и др.]. СПб., 2018. 111 с. – № ГР АААА-А17-117042710042-9.

Директор центра координации научных исследований ГУАП, канд. техн. наук, доцент — А. В. Рабин

Доцент кафедры вычислительных систем и сетей, канд. техн. наук — В. А. Ненашев

Старший преподаватель кафедры вычислительных систем и сетей, канд. техн. наук — С. А. Чернышев