

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2019

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Научный руководитель: **Балонин Николай Алексеевич**
доктор технических наук, доцент

Официальные оппоненты: **Фаворская Маргарита Николаевна**
доктор технических наук, профессор, заведующий кафедрой информатики и вычислительной техники федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева»

Круглов Сергей Константинович
кандидат технических наук, доцент, доцент высшей школы программной инженерии института компьютерных наук и технологий федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Ведущая организация: федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук» (СПИИРАН)

Защита состоится «3» марта 2020 г. в 14-00 на заседании диссертационного совета Д 212.233.05 в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» по адресу: г. Санкт-Петербург, ул. Б. Морская, 67, ауд. 53-01.

С диссертацией можно ознакомиться в библиотеке ФГАОУ ВО ГУАП и на сайте www.guap.ru.

Автореферат разослан «23» января 2020 г.

Учёный секретарь диссертационного совета



Овчинников Андрей Анатольевич
к.т.н., доцент

ОБЩАЯ ХАРАКТЕРИТИКА РАБОТЫ

Диссертационная работа посвящена решению части крупной научной проблемы развития и совершенствования теории преобразования данных и сигналов, в том числе в прикладных задачах распределенных видеосистем. Акцент делается на улучшении характеристик процессов дискретных преобразований данных и повышении защищенности и надежности обмена информацией в условиях внешних помех за счет разработки, исследования и применения специальных квазиортогональных 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 цифровой 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. Williamson), Райзер (H. Ryser) и др. 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 работ отечественных ученых Н. А. Балонина, Л. А. Мироновского и М. Б. Сергеева только начиная с 2011 года. Позже к этим исследованиям присоединились такие зарубежные ученые как Дж. Себерри (J. Seberry), Д. Джокович (D. Djoković), Н. Блаунштейн (N. Blaunstein), О. Хадар (O. Hadar) и др.

Примеры применения 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 квазиортогональных 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 покadroвого 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 помехозащищенный обмен ими по открытым коммуникационным каналам.

Предметом исследования являются методы и процессы преобразования цифровых визуальных данных 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 отдельного 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 реализуется программно и аппаратно-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.

Соответствие паспорту специальности. Диссертационная работа соответствует п. 2 «Исследование процессов генерации, представления, передачи, хранения и отображения аналоговой, цифровой, видео-, аудио- и мультимедиа информации; разработка рекомендаций по совершенствованию и созданию новых соответствующих алгоритмов и процедур»; п. 8 «Исследование и разработка новых сигналов, модемов, кодеков, мультиплексоров и селекторов, обеспечивающих высокую надежность обмена информацией в условиях воздействия внешних и внутренних помех»; п. 10 «Исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций» паспорта специальности 05.12.13 - Системы, сети и устройства телекоммуникаций.

Степень достоверности результатов работы обеспечивается корректностью постановки научно-технической задачи исследования, строго обоснованной совокупностью ограничений и допущений, обширным и представительным 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 (РОСПАТЕНТ).

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 об-

работки 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 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).

Помехоустойчивые коды Мерсенна длин 3 и 7 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: модификация метода 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 и орнаменты портретов новых специальных матриц; цепочки квазиортогональных матриц; численные методы и алгоритмы вычисления двуциклических 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 видеок кадров 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, четырех разделов, заключения. Полный объем 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.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, сформулированы её цель, задачи, научная новизна, представлены основные положения, выносимые на защиту, приведены сведения о практическом использовании полученных научных результатов.

В первом разделе работы приведены основные определения ортогональных матриц, матриц Адамара, матриц максимума детерминанта, выделены задачи и вычислительные процедуры, используемые в обработке визуальной информации с применением ортогональных преобразований.

Последовательно рассматриваются задачи:

- покадрового сжатия визуальных данных с использованием матрицы дискретного косинусного преобразования для сокращения объема передаваемых или хранимых данных на примере JPEG;
- помехоустойчивого кодирования изображений с использованием стрип-преобразования для снижения влияния импульсных помех в канале передачи данных на передаваемые изображения;
- покадрового маскирования изображений ортогональными матрицами в канале для исключения их несанкционированного использования и подмены;
- помехоустойчивого кодирования сигналов в открытом коммуникационном канале и выделения полезного сигнала в условиях повышенной помеховой обстановки на примере кода Баркера, используемого в наборе стандартов связи IEEE802.11.

В связи с характеристиками современных цифровых визуальных данных для перечисленных выше задач обосновывается необходимость расширения семейства ортогональных матриц по порядкам их существования, акцентируется внимание на их структурах и других параметрах с целью совершенствования и разработки новых алгоритмов и процедур ортогональных преобразований.

Выделяются квазиортогональные матрицы порядка n как обобщение матриц ортогональных, удовлетворяющие условию

$$\mathbf{A}^T \mathbf{A} = \omega(n) \mathbf{I}, \quad (1)$$

где \mathbf{I} – единичная матрица, $\omega(n)$ – весовая функция. Элементы матриц \mathbf{A} имеют ограничение в виде $|a_{ij}| \leq 1$.

Формулируются требования к специальным квазиортогональным матрицам в рассматриваемом спектре выполняемых ортогональных преобразований. Вводится определение специальных матриц для задач преобразования цифровых изображений как квазиортогональных матриц простых симметричных структур с двумя значениями элементов (уровней), не превышающих по модулю единицы, существующих на четных и нечетных порядках и удовлетворяющих условию (1).

Приводятся классические методы Сильвестра, Пэли, Скарпи и Вильмсона вычисления ортогональных матриц, рассматриваются проблемные порядки вычисления с их помощью двухуровневых ортогональных матриц Адамара, показывается необходимость разработки новых методов и алгоритмов.

Делается вывод о том, что 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.

Второй раздел работы в основном содержит описание малоуровневых квазиортогональных матриц через определение их связей с такими числовыми последовательностями, как $4t - 1$ и $4t - 3$, где t – натуральное число. В свою очередь указанные 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 $2^k - 1$, где k – натуральное число, чисел Ферма $n = 2^{2^k} + 1$ где k – не отрицательное целое число и др.

Приводятся описания малоуровневых квазиортогональных матриц по принадлежности их к матрицам глобального или локального максимумов детерминанта. На основе анализа определений таких матриц впервые вводится новая, более простая классификация, по которой они могут быть отнесены к матрицам Адамара, Мерсенна, Эйлера или Ферма. А именно, в зависимости от остатка r деления порядка n на 4 они классифицируются как матрицы вида:

- $r=0$ – 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.

Введенная классификация открывает возможность понимания того, что требование расширения класса двухуровневых квазиортогональных матриц выполнимо на порядках, вложенных в последовательности $4t - 1$ ($4t + 3$) и $4t - 2$, трехуровневых – на порядках, вложенных в последовательности $4t + 1$ и $4t - 3$ матрицами Зейделя. С использованием понятий вложенности основных числовых последовательностей друг в друга актуализируются определения основных квазиортогональных матриц Мерсенна, Эйлера и Ферма, порядки их существования, зависимости значений элементов от t , приведенные в табл.1.

Таблица 1. Значения элементов квазиортогональных матриц

Обозначение	Порядок n	Матрица	Значения элементов
H	$4t$	Адамара	$1, -1$
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 $q = n - 1 = 4u^2$, $p = q + \sqrt{q}$, $b = \frac{2n - p}{p} = 1 - \frac{2u - 1}{2u + 1} \times \frac{1}{u}$, $s = \frac{\sqrt{nq} - 2\sqrt{q}}{p} = \frac{\sqrt{nu} - 1}{2u + 1} \times \frac{1}{\sqrt{u}}$

Далее рассматриваются взаимосвязи указанных в табл. 1 матриц в виде цепочек, порождаемых матрицами-предикторами. Такое представление позволяет значительно упростить вычисление необходимых для обработки матриц, имея в виду наследование характеристик матриц меньших порядков матрицами порождаемыми.

Так, матрица Адамара \mathbf{H}_{4t} может быть получена путем окаймления матрицы Мерсенна в виде

$$\mathbf{H}_{4t} = \begin{pmatrix} -\lambda & e^T \\ e & \mathbf{M}_{4t-1} \end{pmatrix}, \quad (2)$$

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.

Такая взаимосвязь показывает, что с точностью до знака округленная матрица Мерсенна является ядром (core) нормализованной матрицы Адамара. Приводятся примеры новых матриц Адамара, отличных от матриц основной последовательности, полученные из матриц Мерсенна по выражению (2). Кроме того, каждая из таких матриц Мерсенна является исходной для получения ветви матриц применением описанного выше подхода для нечетных порядков алгоритма Сильвестра. Типичная цепочка взаимосвязанных структурно матриц Мерсенна и Эйлера, например, выглядит как $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \dots$.

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

Далее в работе рассматриваются слои матриц как совокупность матриц различных семейств с известными функциями зависимости значения элемента (уровня) матрицы от ее порядка.

Приведенный в данном разделе материал показывает, что основные определения позволяют классифицировать квазиортогональные матрицы и их характеристики, выделять порядки их существования, принадлежащие известным числовым последовательностям, что призвано облегчить выбор разработчикам систем обработки данных нужных по параметрам квазиортогональных матриц.

Третий раздел работы посвящен рассмотрению специальных структурированных квазиортогональных матриц, описанию их характеристик и преимуществ, а также метода и алгоритмов их вычисления.

Среди структурированных двухуровневых квазиортогональных матриц, относящихся к простейшим, выделяются симметричные и кососимметричные матрицы, обладающие, в отличие от неструктурированных матриц, рядом полезных свойств при их хранении, передаче по коммуникационным каналам. Отдельно рассматриваются квазиортогональные матрицы циклических структур, которые совмещают в себе свойства кососимметричных. Приводятся многочисленные примеры портретов матриц, иллюстрирующих излагаемый материал.

Рассматривается ограничение на симметрию циклических матриц, показывающее, что из них, но больших порядков и не обязательно ортогональных, можно построить бициклические матрицы Адамара, получаемые из двух циклических блоков – матриц \mathbf{A} и \mathbf{B} в виде

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^T & -\mathbf{A}^T \end{pmatrix}. \quad (3)$$

Особый интерес для отдельных задач обработки изображений представляют симметричные конструкции матриц типа Адамара-Уолша, получаемые из классических матриц Мерсенна путем упорядочивания столбцов по частоте (по количеству смены знаков их элементов). В качестве примера приводится матрица Мерсенна-Уолша порядка 31, используемая при построении фильтров.

Рассмотренные основные виды структурированных и неструктурированных двухуровневых квазиортогональных матриц формируют значительно расширенные семейства, предлагаемые для использования в симметричных алгоритмах обработки изображений. Это дает разработчикам алгоритмов более широкие возможности в выборе наиболее удачной матрицы для обработки конкретных изображений, в том числе изображений нестандартных размеров.

Желание получить квазиортогональную матрицу симметричной конструкции не всегда выполнимо, особенно при использовании переборных или эвристических методов. Для циклических ортогональных матриц с симметрией (кососимметрией), согласно гипотезе Райзера, максимальный порядок равен 4. Для бициклических структур, построенных из ортогональных блоков по соотношению (3), в работе формулируется расширение гипотезы Райзера, ограничивающее порядки их существования до 32.

Рассматриваются особенности использования структурированных специальных квазиортогональных матриц в распределенных системах. Приводятся дополнительные аргументы в их пользу при реализации процедур обработки изображений на примере матриц «золотого сечения», существующих на порядках $n=10 \cdot 2^l$.

Далее предлагается метод вычисления бициклических симметричных матриц на основе перекрестных ссылок, гарантирующий их вычисление на порядках до 100 из несимметричных и необязательно ортогональных блоков **A** и **B**. Детально описывается компьютерный поиск бициклических матриц, заключающийся в реализации четырех этапов. Приводится алгоритм оптимизации поиска бициклических матриц и его особенности.

Четвертый раздел работы посвящен вопросам практического применения специальных ортогональных и квазиортогональных матриц в обработке визуальной информации на примере тестовых изображений, а также вопросам помехоустойчивого кодирования сигналов в коммуникационном канале.

Даются расширенные определения процедур маскирования и демаскирования изображения **P**, представляемого совокупностью фрагментов **X** с размерами, кратными порядку маскирующей матрицы n . Рассматривается предлагаемая модификация метода двустороннего матричного преобразования изображений в формате BMP с заданными параметрами в виде $\mathbf{Y} = \mathbf{G}^T \mathbf{X} \mathbf{G}$. Для процедуры маскирования приводится определение особых изображений как изображений, инвариантных к двустороннему матричному преобразованию, переводимых им в то же изображение с точностью до постоянного множителя в виде $\mathbf{G}^T \mathbf{X} \mathbf{G} = \lambda \mathbf{X}$. Приводятся визуализации в формате BMP особых изображений для используемых матриц Мерсенна и Мерсенна-Уолша порядков 7, 15 и 31, для матриц Ферма порядков 3, 5, 17 и 37 и матриц Эйлера порядков 22 и 34.

Приведенные визуализированные результаты преобразований показывают, что метод маскирования с использованием квазиортогональных матриц может быть использован без ограничений, поскольку особые изображения не являются изображениями объектов реального мира, а напоминают лишь портреты указанных матриц. Для примера на рис. 1 приведены полученные возможные визуализации в градациях серого матрицы Ферма порядка 17.

Для тестовых изображений, маскированных матрицами Адамара порядка 12 неструктурированной конструкции, конструкций на основе циклической и симметричной матриц Мерсенна порядка 11, а также симметричной матрицей порядка 32 приведены результаты экспериментов, показывающих улучшение качества маскирования при увеличении порядка структурированной маскирующей матрицы.

Для тех же тестовых изображений приводятся результаты восстановления изображений при потере одного, двух и шести пакетов данных размером 1024 байт каждый, в стрип-преобразованном указанными матрицами изображении, передаваемом по каналу.

Рассматривается возможность замены ДКП в алгоритме JPEG структурированными матрицами.

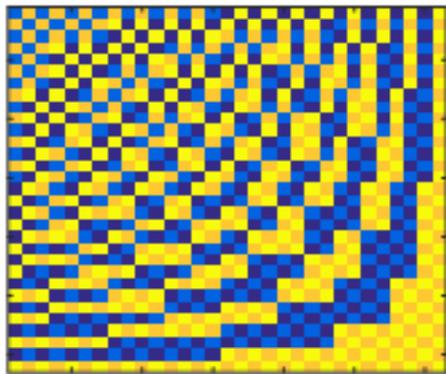


Рис. 2. Портрет модульно двухуровневой матрицы Мерсенна-Уолша порядка 31

Приводятся цветные портреты вычисленных модульно двухуровневых матриц Мерсенна-Уолша порядков 7, 15, 31 (приведена на рис.2) и 63. Приводятся результаты эксперимента по замене ДКП в алгоритме JPEG на матрицу Мерсенна-Уолша порядка 7, в том числе в виде вычисленных метрик PSNR и SSIM восстановленных после сжатия изображений. Результаты получены в разработанной с участием автора среде моделирования, на которую получено свидетельство о регистрации (Роспатент). Пример восстановленных изображений для коэффициента сжатия 3 приведен на рис.3.

Далее рассматривается задача повышения помехоустойчивости передачи информации в открытых каналах. Один из возможных путей, предлагаемых в работе, – ослабление требования к автокорреляционной функции (АКФ) и допущение вторичных пиков, превышающих единицу. Это является приемлемым в случае, когда центральный пик АКФ значительно больше единицы.

Предварительный анализ и проведенные эксперименты показали перспективы получения новых кодов, построенных на основе строк моноциклических квазиортогональных матриц Мерсенна. Однако, у кодовых последовательностей Мерсенна, в отличие от последовательностей Баркера, отрицательный элемент равен $-b$ (табл. 2). С целью определения характеристик сжатия кодовых последовательностей Баркера и Мерсенна в работе были проведены эксперименты для кодов длины 3, 7 и 11. Результаты экспериментов приведены на рис. 4 и в табл. 3.

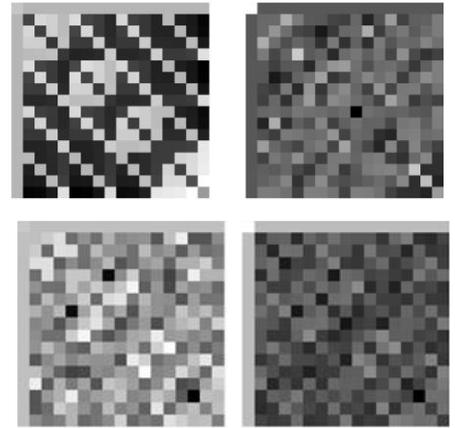


Рис.1 – Особые изображения для матрицы Ферма порядка 17

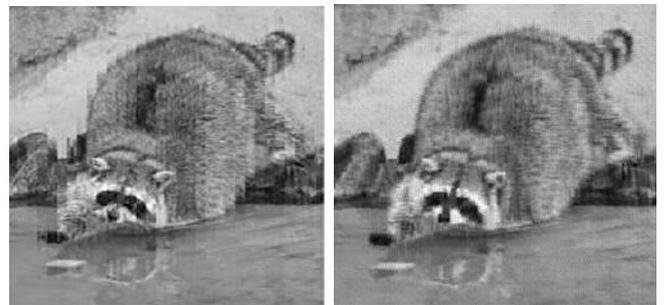
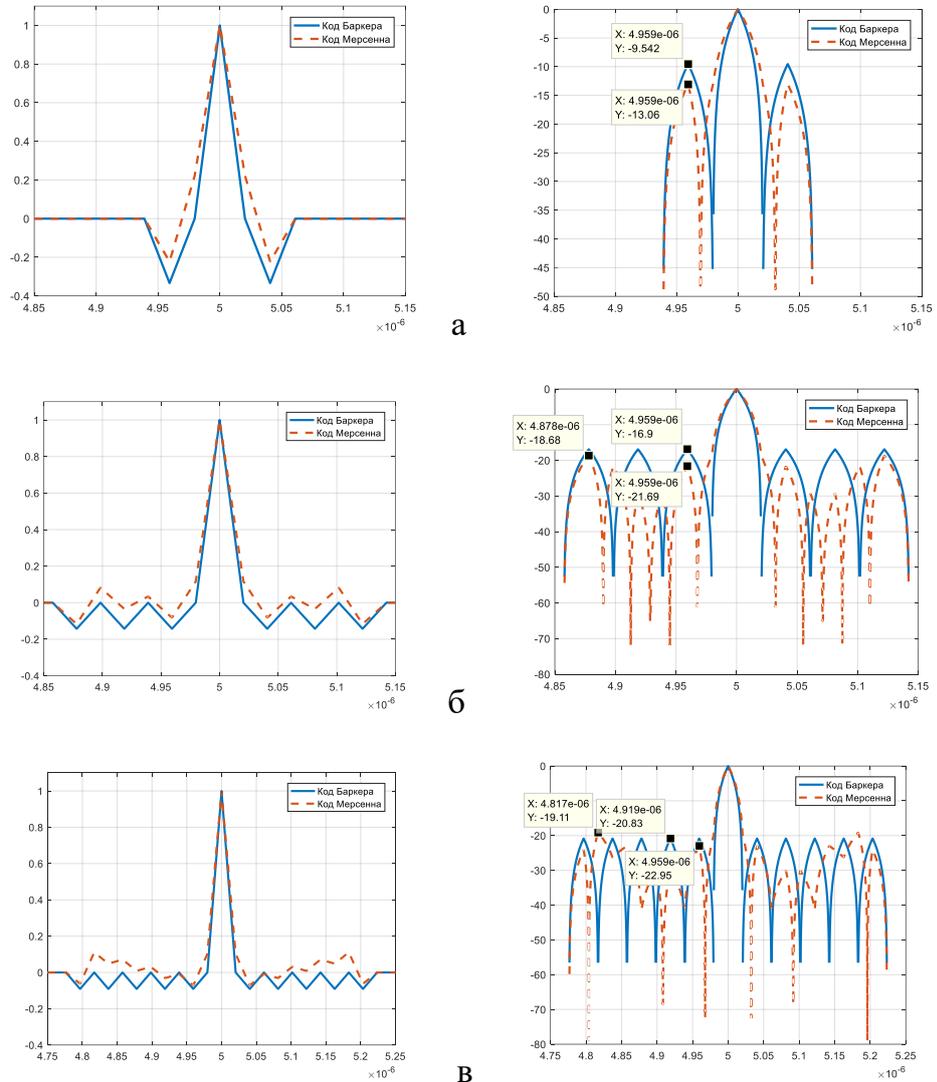


Рис.3. Восстановленные изображения, сжатые с ДКП и с четырехуровневой матрицей Мерсенна-Уолша порядка 7

Таблица 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

Рис. 4. АКФ огибающей при $n=3$ (а), $n=7$ (б) и $n=11$ (в) для кодов Баркера и Мерсенна: слева АКФ нормированная к единице, справа – АКФ в дБ

Полученные в работе характеристики АКФ для кодовых последовательностей Баркера и Мерсенна длин 3, 7 и 11 позволяют сделать вывод о перспективности использования кодов Мерсенна как альтернативы кодам Баркера в радиолокации и при передаче в коммуникационных радиоканалах.

Таблица 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

Сравнение кодовых $\{1, -1\}$ последовательностей Баркера длин 3, 7 и 11 и кодов $\{1, -b\}$ Мерсенна тех же длин из строк циклических матриц, показывает их отличие.

В целом представленные результаты моделирования 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.

Далее формулируется правило формирования вложенных кодов, представляющих собой 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 табл. 4 для комбинаций кодов Баркера и Мерсенна приведены оценки отношения пика автокорреляционной функции к максимальному по модулю боковому лепестку (ОПМБЛ).

Таблица 4. Комбинации вложенных кодов и оценка ОПМБЛ АКФ

<i>nхm</i>	Комбинация кодов							
	Баркер-Баркер		Баркер-Мерсенн		Мерсенн-Баркер		Мерсенн-Мерсенн	
	Оценка ОПМБЛ, 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

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 зашумленного окружения.

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, в том числе в клиент-серверной реализации.

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 строки циклических квазиортогональных матриц с элементами $\{1, -b\}$ или $\{a, -b\}$, отличные от $\{1, -1\}$. 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 ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Монография

1. Сергеев А.М., Востриков А.А. Специальные матрицы: вычисление и применение. СПб: Политехника. 2018. 114 с. ISBN 978-5-7325-1137-6

Статьи, опубликованные в журналах из Перечня ВАК РФ

2. 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.

3. Востриков А.А., Сергеев А. М., Мишура О.В., Чернышев С.А. О выборе матриц для процедур маскирования и демаскирования изображений // *Фундаментальные исследования*. 2015. № 2 (часть 24). С. 5335-5339.
4. 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.
5. Сергеев А. М. О взаимосвязи одного вида квазиортогональных матриц, построенных на порядках последовательностей $4k$ и $4k-1$ // *Известия ЛЭТИ*, 2017. № 7. С. 12 – 17
6. Балонин Ю.Н., Востриков А. А., Капранова Е.А., Сергеев А. М., Сеницына О. И., Чернышев С. А. Цифровое маскирование матрицами Мерсенна и его особые изображения // *Фундаментальные исследования*, 2017, № 4, с. 13-18.
7. Сергеев А.М., Блаунштейн Н.Ш. Ортогональные матрицы симметричных структур для задач обработки изображений // *Информационно-управляющие системы*. 2017. № 6(91). С. 2–8.
8. 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>
9. 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.
10. Ненасhev 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>
11. Востриков А.А., Балонин Ю.Н., Куртяник Д.В., Сергеев А.М., Сеницына О.И. О гибридном методе защиты видеоданных в IP-сетях // *Телекоммуникации*. 2018. № 2. С. 34-39
12. Ненасhev 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.

Статьи в журналах, индексируемых SCOPUS и Web of Science

13. 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
14. 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.
15. 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>
16. 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>.

Публикации в других изданиях

17. 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.

18. 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.

19. Балонин Ю. Н., Егорова И. С., Сергеев А. М. Фильтры Мерсенна-Уолша для видеоданных в IP-сетях. Региональная информатика и информационная безопасность Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 367-371.

20. 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.

21. 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.

22. 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.

23. 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.

24. Сергеев А.М., Куртяник Д.В., Самиков А. В., Семенов А. А. О визуальной оценке результатов вычисления матриц Адамара // Наука. Техника. Технологии (политехнический вестник). 2018. №4. С.19 – 26.

25. 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.

26. 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.

Программное обеспечение, зарегистрированное в РОСПАТЕНТе:

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.