

Федеральное государственное бюджетное
учреждение науки
Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук
(СПИИРАН)

14 линия, д. 39, Санкт-Петербург, 199178
Телефон: (812) 328-33-11, факс: (812) 328-44-50
E-mail: spiiiran@iias.spb.su, http://www.spiiiran.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ
Директор СПИИРАН
доктор технических наук,
профессор РАН

А. Л. Ронжин

« 12 » 02 2020 г.

« 12 » февраля 2020 г. № 60-01-01-147

На № _____



ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационную работу Сергеева Александра Михайловича на тему: «Методы преобразования изображений и кодирования сигналов в каналах распределенных систем на основе использования специальных квазиортогональных матриц», представленную на соискание ученой степени кандидата технических наук по специальности 05.12.13 — «Системы, сети и устройства телекоммуникаций».

Актуальность темы диссертации

Диссертационная работа Сергеева А. М. посвящена актуальной задаче повышения защищенности цифровой визуальной информации, передаваемой по открытым каналам IP-коммуникаций распределенных видеосистем. К ним относятся такие системы как охранные, мониторинговые, системы регистрации событий и чрезвычайных ситуаций, телемедицины, специального назначения и др.

Для решения поставленной задачи автором предлагаются подходы для маскирования данных ограниченного доступа, сжатия видеоданных, а также защиты от помех при беспроводных коммуникациях за счет расширения аппарата традиционно применяемых для этого двухуровневых и малоуровневых ортогональных матриц, элементы которых принимают два-три или более значений из заданного набора.

Актуальность диссертации определяется необходимостью создания специализированных аппаратных и программно-аппаратных решений, направленных на реализацию специализированных задач обработки и передачи изображений в сетях телекоммуникаций, выполняемых в масштабе реального времени. Это требует теоретических исследований, обеспечивающих создание быстрых алгоритмов.

ГИАИОД	Документ зарегистрирован
	« 13 » 02 2020 г.
	Вх. № 71-40/20

Отметим, что развиваемое научное направление диссертационного исследования согласуется с аналогичным направлением СПИИРАН по исследованию определенного класса матриц Адамара с порядком, совпадающим со степенями двойки (патент СССР № 1799274 от 1990 г.) и ориентировано на:

-обобщение аддитивного эрмитова разложения оператора на симметрично-кососимметричные части;

-формализацию понятия матричной зеркальной симметрии, построение симметричных матриц Адамара для любой степени двойки, а также обобщение векторного произведения.

Тема диссертационной работы Сергеева А. М., по существу, относится к междисциплинарным исследованиям на стыке прикладной математики и ее технических приложений, что усиливает актуальность исследования.

Особую актуальность решаемая в диссертации задача приобретает в беспроводных коммуникациях распределенных систем с IP-модулями встраиваемого класса с ограничениями вычислительной мощности и свободного ресурса.

Краткий анализ диссертации

Диссертационная работа состоит из введения, четырех глав, заключения, списка литературы (150 наименований, из которых более половины ссылок на работы сторонних авторов) и двух приложений: описания разработанной с участием автора среды моделирования и копий актов о внедрении полученных в результате выполнения диссертации результатов. Работа хорошо структурирована. Разделяется на две части — три первых главы раскрывают способы построения двухуровневых и малоуровневых ортогональных матриц, а в четвертой главе (и разделе 3.3 третьей главы) рассматриваются практические приложения. Формулы точно, последовательно и понятно для программирования отражают содержание диссертации. Словесные комментарии, местами, выходят за рамки дублирования формул и выполнены в несколько вольном стиле. Нестандартные понятия везде поясняются при первом употреблении. Материал соразмерно распределен по главам. Наибольший объем занимает 4 глава, которой придается наибольшее значение для раскрытия положений, выносимых на защиту. В конце каждой главы имеются выводы по представленным научным результатам. Объем работы составляет 153 страницы.

Во введении определяются цель и задачи диссертации и формулируются основные положения, выносимые на защиту. Автор раскрывает актуальность исследуемой темы, формулирует научные положения, результаты, обосновывает теоретическую и практическую значимость.

В первом разделе представлены основные понятия и термины, относящиеся к рассматриваемой в диссертации области, анализируются основные ортогональные преобразования и матрицы, применяемые в задачах сжатия, помехозащищенного кодирования, маскирования изображений и модуляции

сигналов в каналах коммуникаций. Формулируются требования к семействам матриц для современных задач обработки и передачи информации.

Особенностью первого раздела является то, что в ней традиционный обзор оформлен в виде комментариев к десятку «определений», в качестве которых вводятся основные обсуждаемые понятия. При этом указанные определения в максимально доступной форме раскрывают поисковый характер исследования и его место среди других исследований, а также эффективно подготавливают читателя к восприятию содержания последующих разделов.

С методической точки зрения, первый раздел диссертации Сергеева А. М. может использоваться в качестве образца удачного оформления обзорной части диссертационного исследования.

Во втором разделе исследуется расширенное множество матриц Адамара. В расширенное множество входят не только ортогональные матрицы, состоящие из ± 1 , но и ортогональные матрицы из элементов, множество значений которых отличается от $+1$ и -1 . При этом порядок исследуемых матриц может отличаться от кратного четырем, и открываются дополнительные возможности построения матриц за счет изменения их размера, например, на единицу. Рассматриваемые ортогональные матрицы можно охарактеризовать как «квазиадамаровы», но в авторской терминологии школы ГУАП они именуется «квазиортогональными».

Исследования мотивируются гипотезой Адамара о существовании матриц Адамара для всех порядков, кратных четырем. В диссертации ставится обобщенная задача построения примеров «квазиортогональных» матриц различных порядков, вероятно, при разумном ограничении размера целевых матриц, например, в пределах актуальных размеров обрабатываемых изображений. Задача построения «квазиортогональных» матриц для каждого размера анализируется на уровне гипотез, но не решается. Рассматриваются порядки матриц, связываемые с известными числовыми последовательностями Мерсенна, Эйлера, Ферма и др. Для краткости соответствующие «квазиортогональные» матрицы именуется матрицами Мерсенна, Эйлера, Ферма и др. вопреки сложившейся традиции присваивать имена авторов однозначно понимаемым классам матриц и другим математическим объектам, созданным данными авторами.

Основными «квазиортогональными» матрицами, обсуждаемым в данном разделе, являются «матрицы Мерсенна» порядка 2^k-1 , который, в сравнении с остальными, плотнее заполняет числовую ось возможных порядков. Наиболее достоверным и значимым результатом является предложенный автором диссертации способ увеличения порядка «квазиортогональных» матриц за счет добавления строк и столбцов в процедуре «окаймления» матрицы по определенному алгоритму. При этом по «матрице Мерсенна» вычисляется матрица Адамара порядка 2^k . Обсуждаемые «матрицы Мерсенна» иллюстрируются в диссертации на стр. 57 посредством рис. 2.5 – «Портреты квазиортогональных матриц M_3 , M_7 , M_{15} ». Получение из каждой из матриц M_3 , M_7 , M_{15} матрицы

Адамара порядка ближайшей степени двойки сводится к добавлению строки и столбца из одних только черных полей, обозначающих в диссертации значения -1 .

Характерно, что с точностью до замены -1 на 1 и наоборот, именно «матрицы Мерсенна», представленные на рис. 2.5, предложены в составе классов матриц по патенту СССР №1799274, в котором они получаются из нормализованных матриц Адамара размером 2^k вычеркиванием строки и столбца из одних только 1 . При этом множества строк (столбцов) обсуждаемых матриц Адамара относительно почленного умножения строк (столбцов) образуют абелевы группы с элементами второго порядка. При $k=3$ и порядке 8 имеется ровно 15 различных наборов строк, составляющих «матрицы Мерсенна». Из них 7 наборов отличаются тем, что имеют симметричные строки, как в центральной матрице на рис. 2.5.

Отмеченное частичное совпадение результатов с известными ни в коем случае не умаляет новизны способа «окаймления» матриц, так как сравниваемые способы преобразования матриц являются противоположными, и способ Сергеева А. М. является более общим (см. рис. 3.2 – «Портреты матрицы H_{12} на основе ядра – циклической матрицы M_{11} (а), и матрицы H_{12} на основе ядра – симметричной матрицы M_{11} (б)). Напротив, частичное совпадение результатов, полученных независимо друг от друга, свидетельствует об их достоверности, необходимости и значимости.

В разделе представлены также соображения по поводу вычисления «квазиортогональных матриц» любого порядка. Идея состоит в классификации избранных авторами числовых последовательностей Мерсенна, Эйлера, Ферма и др. посредством вычисления остатка от деления чисел из указанных последовательностей на четыре (Таблица 2.1 – «Значения элементов семейств матриц»). В контексте приложений к обработке сигналов идея приветствуется, но в теории матриц подобные соображения будут работать, вероятно, после того, как гипотеза Адамара станет теоремой или будет опровергнута.

В третьем разделе обсуждается проблема получения, так называемых, «специальных» матриц, под которыми согласно Определению 11 на стр. 34 понимаются «квазиортогональные матрицы простых симметричных структур с двумя значениями уровней, не превышающими по модулю единицы, существующие на четных и нечетных порядках». Проще говоря, речь идет о построении двухуровневых симметричных матриц, прежде всего, матриц Адамара. Основным аргументом в пользу применения симметричных матриц при обработке сигналов является то, что в вычислениях удастся исключить процедуру транспонирования матрицы.

В разделе рассматривается построение симметричных «квазиортогональных» матриц увеличенного размера традиционными операциями кронекерова произведения, трансляции, перебором и др. Предлагаются авторские

модификации способов получения симметричных ортогональных малоуровневых матриц ограниченного размера.

Основной упор в разделе делается на сложность построения симметричных матриц Адамара и установления ограничений их размера, достижимого конкретными методами. В качестве результата построения симметричных ортогональных матриц максимального размера указываются блочные регулярные матрицы "в форме Пропус" размером до 212.

В контексте обсуждения симметрии в данном разделе было бы уместно вернуться к матрицам по рис. 2.5, указанные матрицы примечательны тем, что:

(а) обладают максимальной *перестановочной симметрией*, то есть свойством сохранять симметрию при перестановках строк или столбцов. Например, центральная симметричная матрица на рис. 2.5 сохраняет симметрию при 28 перестановках строк;

(б) обладают групповым свойством *скрытой симметрии*, при которой набор строк в матрице по чередованию ± 1 совпадает с набором столбцов, но сами строки чередуются не обязательно в том же порядке, что столбцы. При этом перестановкой строк центральной симметричной матрицы рис. 2.5 можно получить 168 симметричных и несимметричных матриц со скрытой симметрией;

(с) легко строятся для любого порядка, образуя нормализованные матрицы Адамара размера 2^k при добавлении строки и столбца черных полей.

"Специальные" симметричные нормализованные матрицы Адамара по рис. 2.5 с любым размером, равным степени двойки, строятся и даже перечисляются по тривиальным алгоритмам. Тем не менее, в настоящее время, исследования в СПИИРАН ограничены приложениями обсуждаемых матриц размером только 4 и 8. Возможно, специалисты ГУАП получают эффект от применения симметричных нормализованных матриц Адамара для размерностей, скажем, 1024 или 2048, что было бы интересно в перспективе продолжения работ.

В **четвертом разделе** автором описывается метод двустороннего матричного маскирования изображений, который реализуется проще известных методов и обеспечивает лучшее сокрытие визуальной информации в коммуникационном канале. Для метода маскирования вычисляются и визуализируются особые изображения, инвариантные к двустороннему матричному умножению при использовании «матриц Мерсенна», «матриц Эйлера» и «матриц Ферма» различных порядков до 37. Приводятся результаты маскирования тестовых изображений специальными матрицами, стрип-преобразования с потерей одного, двух и шести пакетов данных при передаче в коммуникационном канале, замены матрицы дискретного косинусного преобразования на «матрицу Мерсенна-Уолша» порядка 7. Предлагается способ формирования кодов из строк циклических «матриц Мерсенна» для фазовой модуляции сигналов в канале с несимметричным представлением. Исследуются автокорреляционные функции полученных кодов длины три, семь и одиннадцать, а также отношения пика автокорреляционной

функции к максимальному боковому лепестку. Для корректного сравнения выбраны аналогичные характеристики кодов Баркера тех же длин. Приводятся результаты моделирования вложенных кодов на комбинации кодов Баркера и Мерсенна.

В **заключении** приведены основные результаты работы и выводы, подтверждающие достижение цели работы.

В **приложении 1** описывается разработанная с участием автора среда моделирования, использованная для проведения ряда экспериментов. В **приложении 2** представлены копии актов внедрения и использования результатов диссертационной работы.

Научная новизна полученных результатов

К основным научным результатам диссертационной работы можно отнести:

1. Расширение класса ортогональных матриц специальными «квазиортогональными» матрицами. Увеличение видов и количества симметричных «квазиортогональных» матриц с двумя значениями элементов позволяет расширить область применимости ортогональных преобразований и способствует совершенствованию известных и разработке новых процедур преобразования данных и кодирования сигналов в открытом канале.

2. Метод симметричного двустороннего матричного маскирования/демаскирования цифровых визуальных данных с использованием специальных «квазиортогональных» матриц. В отличие от существующих методов, предложенный метод обеспечивает математически более простую защиту визуальных данных от несанкционированного доступа.

3. Новые двухуровневые несимметричные $\{1, -b\}$ кодовые последовательности длин 3 и 7 на основе использования строк «матриц Мерсенна», используемые для фазовой модуляции сигналов в радиоканале. Допущение несимметрии позволяет указанным кодам иметь лучшие автокорреляционные характеристики, чем у кодов Баркера той же длины.

4. Вложенные кодовые последовательности, построенные на комбинации пар кодовых последовательностей Баркера и Мерсенна длин 3 и 7. Указанные последовательности обеспечивают повышение помехозащищенности сигналов в радиоканале.

Теоретическая и практическая значимость полученных автором диссертации результатов

Теоретическую значимость диссертационной работы, во-первых, составляют предлагаемый новый класс специальных «квазиортогональных» матриц, ориентированных на преобразование визуальных данных и сигналов в коммуникационных каналах, и показанная возможность практического совершенствования и развития теории ортогональных преобразований цифровой информации.

Во-вторых, впервые предложенная классификация экстремальных малоуровневых «квазиортогональных» матриц и выявленная связь структур таких матриц, построенных на порядках последовательностей $4t$ и $4t-1$.

В-третьих, расширенное семейство ортогональных матриц, используемых для обработки цифровых данных, за счет введения новых двухуровневых и модульно двухуровневых бициклических симметричных матриц.

В-четвертых, новый подход к формированию кодовых последовательностей для фазовой модуляции сигналов в коммуникационном канале за счет использования строк «квазиортогональных матриц Мерсенна».

Практическая значимость работы определяется показанными улучшениями характеристик процессов дискретных преобразований визуальных данных и повышением защищенности и надежности обмена информацией по радиоканалу в условиях внешних помех при программной и аппаратно-программной реализации в реальном масштабе времени в системах встраиваемого класса на основе DSP и FPGA.

Метод маскирования может быть использован для защищенного хранения визуальных данных на цифровых носителях информации.

Достоверность, обоснованность основных научных положений, выводов и рекомендаций

Все положения, формулируемые в диссертационной работе Сергеева А. М., доказываются с использованием аппарата линейной алгебры, цифровой обработки изображений, теории модуляции и кодирования сигналов. Эффективность разработанного метода и алгоритмов подтверждается посредством компьютерных экспериментов.

Обоснованность полученных в работе результатов подтверждается внедрением в рамках опытно-конструкторской работы в мобильный видеорегистратор, разработанный ООО «АСК Лаборатория» (г. Санкт-Петербург), в учебный процесс федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» (по направлению «Информатика и вычислительная техника» в дисциплинах «Проектирование систем обработки и передачи информации» и «Цифровая обработка изображений», по направлению «Инфокоммуникационные технологии и системы связи» в дисциплине «Технологии стеганографии в системах инфокоммуникаций»).

Результаты использованы при разработке перспективных радиолокационных станций в АО «Концерн «Гранит-Электрон» (г. Санкт-Петербург), в НИР «Оптико-электронный модуль мобильного применения» гос. рег. № 117032810028-3 (2018 г.) и НИР «Поиск и исследование экстремальных квазиортогональных матриц для обработки информации» гос. рег. № АААА-А17-117042710042-9 (2017-2019 гг.).

По теме диссертационной работы у автора имеется 7 свидетельств о государственной регистрации программ для ЭВМ, в том числе № 2017616795 на

специальное программное обеспечение для приема по беспроводному каналу, декодирования, демаскирования с использованием квазиортогональных матриц, декомпрессии и воспроизведения видеоизображений с малым временем актуальности, № 2017616930 на специальное программное обеспечение для маскирования с использованием квазиортогональных матриц, помехоустойчивого кодирования, сжатия и беспроводной передачи видеоизображений с малым временем актуальности.

Публикация и апробация результатов исследования

По теме диссертации автором опубликовано 26 печатных работ, из них одна монография, 11 статей в журналах, включенных в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, а также четыре статьи в зарубежных изданиях, индексируемых в Scopus.

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).

Рекомендации по использованию результатов и выводов, приведенных в диссертации. Результаты диссертационной работы рекомендуется применять при разработке систем обработки изображений и передачи данных, а также использованы в учебном процессе в ИТМО и СПбГУТ.

В качестве потребителей предложенных в диссертационном исследовании алгоритмов могут выступать производители видеокамер, видеорекордеров, систем кодирования и передачи видеоданных ООО «ЭВС», АО «НИИ телевидения», ЗАО «Элекард Девайсез».

Правильность оформления диссертации и автореферата, соответствие автореферата содержанию диссертации

Диссертация и автореферат оформлены в соответствии с принятыми для научных квалификационных работ нормами и требованиями. Диссертационная работа хорошо структурирована и иллюстрирована. Автореферат диссертации в полной мере соответствует работе и включает ее основные результаты.

Замечания по диссертационной работе.

1. Введение А.М. Сергеевым «гипотезы Балонина (Balonin conjecture)» о предложенных Н.А. Балониным «матрицах Мерсенна» представляется неудачным, т.к. указанная гипотеза, скорее всего, окажется тривиальным следствием доказанной или опровергнутой гипотезы Адамара.

2. В диссертации имеется ряд утверждений, в которых слово "гипотеза" употребляется в смысле "теорема". Указанные утверждения было бы полезно просто исключить.

3. Числа Ферма имеют вид $2^{2^k} + 1$, а размер "матрицы Ферма" имеет вид " $2^k + 1$, при четных значениях k ". Не понятно, какое отношение имеют, так называемые, "матрицы Ферма" к этому великому ученому.

4. Термин "кососимметричная матрица" употребляется в диссертации неправильно: "На рис. 3.3 приведены конструкции матриц M_{15} , найденные двумя характерными для поиска матриц Адамара методами. Первая матрица симметрична, вторая – кососимметрична." (стр. 66) — Кососимметричных матриц нечетного порядка не бывает.

5. При описании решения задач повышения помехоустойчивости в каналах связи не рассматривается случай многократного применения помехи к каналу и соответствующая оценка эффективности предлагаемого подхода в таком случае.

6. При рассмотрении задачи сжатия изображений автор не приводит общую схему такого сжатия и не обосновывает выбор каждого из этапов в этой схеме.

Выводы

1. Диссертация Сергеева Александра Михайловича является законченной научно-квалификационной работой, в которой содержатся новые научные результаты и положения, а также рекомендации по их использованию на практике. По своей актуальности, достоверности и обоснованности результатов, теоретической и практической значимости диссертационная работа соответствует требованиям п. 9 «Положения о присуждении ученых степеней», утвержденной Постановлением Правительства от 24 сентября 2013 г. № 842 (ред. от 01.10.2018).

2. В диссертационной работе содержится решение актуальной научной задачи повышения защищенности передачи цифровой информации в телекоммуникационных каналах распределенных систем, имеющей значение для развития этих систем.

3. Соискатель Сергеев Александр Михайлович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Отзыв составлен главным научным сотрудником лаборатории автоматизации научных исследований, д.т.н. Кулешовым Сергеем Викторовичем и старшим научным сотрудником лаборатории технологий больших данных социкиберфизических систем, к.т.н. Хариновым Михаилом Вячеславовичем.

Отзыв обсужден и утвержден на расширенном заседании лаборатории автоматизации научных исследований СПИИРАН (протокол № 1 от «04» февраля 2020 г.).

Главный научный сотрудник
лаборатории автоматизации научных исследований,
доктор технических наук

Кулешов С.В.

Старший научный сотрудник лаборатории
технологий больших данных социкиберфизических систем,
кандидат технических наук, доцент

Харинов М.В.

Сведения об организации:

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

199178, Россия, Санкт-Петербург, 14 линия, дом 39;
+7(812)-328-34-11; spiiran@iias.spb.su; ww.spiiras.nw.ru