На правах рукописи

Чернышев Станислав Андреевич

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА МАТРИЧНОГО МАСКИРОВАНИЯ ВИДЕОИНФОРМАЦИИ В ГЛОБАЛЬНО РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

05.12.13 – Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2018

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

Научный руководитель: доктор технических наук, профессор
Сергеев Михаил Борисович

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»

Зубакин Игорь Александрович
кандидат технических наук, доцент кафедры «Телевидение и видеотехника» Федерального государственного автономного образовательного учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»

Ведущая организация: **Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук»**

Защита состоится 27 марта 2018 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 20 февраля 2018 г.

Учёный секретарь
диссертационного совета  Овчинников Андрей Анатольевич
к.т.н., доцент

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Видео- и фото-информация используются сегодня в самых разных видах производственной деятельности человека, а также в его повседневной жизни. Одними из наиболее актуальных задач, связанных с накоплением и передачей цифровых фото- или видеоизображений в распределенных видеосистемах, таких как охранные, мониторинговые, системы телемедицины и специального назначения, являются задачи их защиты от несанкционированного доступа, а также обнаружение фактов искажения и подмены.

Пакетная передача видео информации по открытой IP-сети как коммуникационному каналу указанных видеосистем является широко распространенной, что, с учетом повсеместного использования беспроводных технологий передачи данных, делает ее доступной для несанкционированного пользователя.

Особую актуальность перечисленные выше задачи приобретают для распределенных систем, реализуемых на основе IP-модулей встраиваемого класса, для которых существуют ограничения по скорости вычислений и свободному вычислительному ресурсу. Кроме того, возрастающие пропускные способности коммуникационных каналов, размеры передаваемых фото и видеоизображений делают актуальной защиту не только предварительно сжимаемой с потерями информации, но и исходной информации с видеоматриц IP-модулей.

Анализ показал, что большинство известных методов защиты фото или видеоинформации являются криптографическими или используют криптографические примитивы, требующие значительных вычислительных ресурсов. В то же время в большинстве случаев в перечисленных выше системах передаваемая видеоинформация является актуальной небольшой отрезок времени и применение таких методов не требуется. Кроме того применение хорошо исследованных и широко применяемых криптографических методов защиты информации зачастую существенно ограничено в системах встраиваемого класса, к которым относятся IP-модули распределенных видеосистем.

В настоящей работе разрабатывается и исследуется метод маскирования как альтернатива криптографическим методам защиты фото и видеоинформации, учитывающий специфику структуры видеокадров (фото), а также алгоритмов их сжатия и протоколов передачи по IP-сети. Использование маскирования в качестве метода защиты фото и видеоинформации с малым временем актуальности связано с решением вопросов генерации маскированных структур данных, их представления, обмена между приемником и передатчиком, хранения и демаскирования информации.

Известно, что кадры (под кадром будем понимать фотоизображение или кадр видеоинформации, представляемой покадрово) представляют собой матрицы пикселей и наиболее органичны для их преобразования матричные операции, хорошо структурированные, регулярные и обеспечивающие распараллеливание вычислений, что эффективно реализуется в системах встраиваемого класса, использующих DSP или FPGA.

Степень разработанности темы. Вопросам защиты информации при её передаче по открытым каналам связи посвящено множество работ таких ученых как Р. Мак-Элис, Х. Нидеррайтер, Е. А. Крук и др. К сожалению фундаментальных

работ, рассматривающих фото и видеоинформацию как особую цифровую информацию с точки зрения ее защиты нет, а в большей части опубликованных работ используются криптографические методы и криптографические примитивы.

Тем не менее, вопросы защиты цифровой визуальной фото и видеоинформации не криптографическими методами с недавнего времени рассматриваются в работах таких российских ученых как И. Л. Ерош, А. В. Сидоренко, М. Ю. Литвинов, М. Б. Сергеев, А. А. Востриков, М.А. Самохина и зарубежных исследователей B. Czaplewski, K. Wong, M. Gschwandtner, В. Г. Красиленко, В. К. Железняк.

Целью диссертационной работы является разработка эффективного метода маскирования цифровой фото- и видеоинформации в телекоммуникационных системах за счет использования простых матричных преобразований.

Для достижения указанной цели в работе рассматриваются основные принципы функционирования систем передачи видеоданных, выявляются особенности наиболее распространенных графических форматов и предлагаются алгоритмы маскирующего матричного покадрового преобразования, хранения и передачи фото и видеоинформации с использованием квазиортогональных базисов.

Объектом исследования в диссертационной работе является процесс обмена цифровой фото- и видеоинформацией по открытым коммуникационным каналам.

Предметом исследования являются алгоритмы матричного преобразования цифровой фото- и видеоинформации с целью ее маскирования.

Задачи исследования

– анализ существующих решений в области защиты цифровой визуальной информации в распределенных видеосистемах с целью выделения методов, эффективно реализуемых в модулях встраиваемого класса;

– разработка метода матричного маскирования изображений с использованием уникальных квазиортогональных матриц;

– исследование влияния процедуры маскирования/демаскирования на качество восстановленного изображения;

– исследование влияния искажений в коммуникационном канале на качество восстановленного изображения;

– получение изображений, инвариантных к матричному маскированию с использованием квазиортогональных матриц.

Методология и методы исследования. При решении поставленных в работе задач использованы методы теории информации, математической статистики, цифровой обработки изображений и линейной алгебры.

Научная новизна работы определяется тем, что в ней:

– расширено существующее понятие маскирования для цифровой фото- и видеоинформации за счет применения простых матричных преобразований;

– разработан и реализован базовый метод раздельного покадрового маскирования и демаскирования цифровой фото- и видеоинформации с использованием уникальных квазиортогональных матриц Мерсенна;

– исследованы качество маскированных изображений, устойчивость метода к потерям информации в канале, качество восстановленных изображений с использованием известных метрик;

– получены особые изображения для использованных в работе маскирующих матриц Мерсенна, инвариантные к двустороннему матричному маскированию.

Теоретическая и практическая значимость работы определяется тем, что

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

– по результатам демаскирования обеспечивается выявление наличия помех в каналах передачи маскированной информации и внесения изменений третьей стороной в передаваемую маскированную информацию;

– предложенные модификации базового метода позволяют обеспечить маскирование цифровой информации в широком классе распределенных 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;

– маскированные изображения обладают устойчивостью к искажениям в коммуникационном канале.

Положения, выносимые на защиту:

1. метод симметричного двустороннего матричного маскирования/демаскирования цифровых фото- и видеоизображений с использованием уникальных квазиортогональных матриц;
2. алгоритмы маскирования и демаскирования цифровых фото и видеоизображений с адаптацией их размеров к порядкам маскирующих матриц, реализуемые в форматах с фиксированной и плавающей запятыми;
3. способ вычисления для матриц Мерсенна особых (корневых) изображений, инвариантных по отношению к матричному маскированию, и их «портреты».

Достоверность 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 алгоритмов, разработанных на основе базового метода, на программные реализации которых получены свидетельства о государственной регистрации программ для ЭВМ.

Апробация работы. Основные научные положения и результаты диссертационной работы докладывались, обсуждались и получили одобрение на научно-методических семинарах кафедры «Вычислительные системы и сети» ГУАП и докладывались на 66-й научной сессии ГУАП (апрель 2013, г. Санкт-Петербург), 67-й научной сессии ГУАП (апрель 2014, г. Санкт-Петербург), International Conference «Intelligent Interactive Multimedia Systems and Services» IIMSS-2014 (18-20 июня 2014, г. Ханья, Греция), 68-й научной сессии ГУАП (апрель 2015, г. Санкт-Петербург), научно-техническом семинаре НИИ информационно-управляющих систем ИТМО (октябрь 2015, г. Санкт-Петербург), 69-й научной сессии ГУАП (апрель 2016, г. Санкт-Петербург), International Conference on Knowledge-based and Intelligent Information & Engineering Systems (6 - 8 сентября 2017, г. Марсель, Франция).

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», «Цифровая обработка изображений», «Специализированные микропроцессорные системы» и при подготовке по направлению «Инфокоммуникационные технологии и системы связи» в дисциплине «Технологии стеганографии в системах инфокоммуникаций».

В виде программной реализации в системе-на-кристалле с DSP-сопроцессорами (ADSP-BF523KBCZ и др.) метод матричного преобразования кадров видео последовательности используется в видеорегистраторах специального назначения, разработанных ООО «АСК Лаборатория» (г. Санкт-Петербург).

На специальное программное обеспечение для маскирования и демаскирования изображений методом матричных целочисленных преобразований в квазиортогональных базисах получены свидетельства о государственной регистрации программ для ЭВМ №2015611308 и №2015611310. На специальное программное обеспечения для маскирования и демаскирования изображений матричными преобразованиями в формате с плавающей запятой с использованием квазиортогональных матриц получены свидетельства о государственной регистрации программ для ЭВМ №2015611311 и №2015611309. 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.

Личный вклад автора диссертационной работы заключается в:

– разработке метода матричного маскирования/демаскирования цифровой визуальной информации;

– выборе для разработанного метода квазиортогональных матриц Мерсенна;

– разработке программного обеспечения для моделирования, обеспечивающего покадровое маскирование фото и видеоизображений с использованием уникальных квазиортогональных матриц для последующей передачи по сетям общего пользования и демаскирования принятого кадра с использованием ПК;

– выборе изображений для проведения экспериментальных исследований и искажающих факторов;

– выполнении моделирования, обработке и обобщении результатов;

– описании исходной информации о способах маскирования изображений;

– предложении сопоставления порядка маскирующей матрицы, применяемой для маскирования, размерам изображений;

– вычислении и визуализации особых изображений для матриц Мерсенна, инвариантных к двустороннему матричному маскированию.

Публикации. Материалы, отражающие основное содержание и результаты диссертационной работы, опубликованы в 9 печатных работах. Из них 3 работы опубликованы в рецензируемых научных журналах, внесенных в перечень ВАК, и 2 работы опубликованы в изданиях, индексируемых в Scopus.

Объем и структура работы. Диссертация состоит из введения, четырёх разделов, заключения. Полный объём диссертации составляет 120 страниц с 52 рисунками и 11 таблицами и приложения, включающего акты внедрения. Список используемых источников содержит 123 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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

В первом разделе работы выделена область использования современных цифровых распределенных систем видеонаблюдения и рассмотрены их основные свойства. Акцентировано внимание на том, что видеоинформация, передаваемая в таких распределенных системах видеонаблюдения не является секретной, но требует защиты от тиражирования, подмены, искажения и несанкционированного использования.

Показано, что использование криптографических методов для преобразования исходной фото- и видеоинформации в видеокамерах современных цифровых распределенных систем видеонаблюдения в режиме реального времени является затруднительным. Во-первых, это требует значительных вычислительных ресурсов из-за больших объемов самой видеоинформации. Во-вторых, невозможно полностью скрыть исходную информацию путем её шифрования с малым ключом, а только такое шифрование может быть реализовано в реальном времени. Ввиду этого представление и визуализация защищенных изображений требуют особых подходов.

Время актуальности передаваемой видеоинформации в рассматриваемых видеосистемах мало, что позволяет отказаться от шифрации видеопотока с использованием более длинных ключей, заменив ее более простым в реализации маскированием.

Определение 1. Маскирование – процесс преобразования цифровой визуальной информации с малым сроком актуальности к шумоподобному виду с целью защиты от несанкционированного ознакомления.

Определение 2. После выполнения маскирования полученный массив информации называется маскированной цифровой визуальной информацией или маскированным изображением.

Определение 3. Демаскирование – процесс обратного преобразования маскированной визуальной информации путём применения операций, являющихся обратными к маскирующими операциями, с целью восстановления исходного изображения.

Для современных способов маскирования фото- и видеоинформации, которые используют криптографические примитивы и матричные преобразования, сформулированы определения, согласно которым классифицированы рассматриваемые в работе методы и алгоритмы.

Приводятся методы маскирования, известные из открытых литературных источников, используемые для маскирования как аналоговой, так и цифровой информации, в том числе методы, основанные на использовании матричных операций с уникальными матрицами.

Рассмотрены и выделены основные типы и форматы цифровых изображений, к которым может применяться маскирование. Рассмотрены перспективы реализации матричного маскирования в системах встраиваемого класса с использованием DPS или FPGA.

Сформулированы требования к матричному маскированию, заключающиеся в обеспечении:

- минимальных затрат вычислительного ресурса для встраиваемых систем;
- симметричности маскирующего и демаскирующего преобразований;
- адаптируемости маскирования к разрешению матриц цифровых видеокамер;
- устойчивости маскированной информации к помехам и потерям в коммуникационном канале;
- возможности определения наличия изменений в маскированных изображениях при хранении или передаче по открытым коммуникационным каналам.

Второй раздел работы в основном содержит анализ методов, используемых сегодня для маскирования изображений. Рассматривается метод, предложенный в диссертационной работе «Алгоритмы маскирующих преобразований видеоинформации» (М. Ю. Литвинов) и использующий криптографические примитивы, способ маскирования видеопотоков путем разрушения синхроимпульсов видеосигнала в канале передачи, а также метод преобразования данных с помощью кватернионов – Quaternion Encryption Scheme (QES), основанный на реализации Cipher Block Chaining (CBC). Рассматриваются и анализируются методы маскирования, основанные на применении матричных преобразований. В частности, метод, использующий умножение неособенных матриц над полем GF(2) на вектор-столбцы фрагментов изображений (И. Л. Ерош), стрип-метод, предназначенный для помехоустойчивой передачи изображений в каналах с помехами за счет ослабления амплитуды импульсной помехи на цифровом изображении (Л. А. Мироновский и В. А. Слаев), метод маскирования изображений с использованием матричной модели перестановок с матрично-битоворазрядной декомпозицией (В. Г. Красиленко и В. М. Дубчак).

Как основа для разрабатываемого в диссертации метода детально рассматривается двустороннее стрип-преобразование вида

$$\mathbf{Z} = \mathbf{A}_1 \mathbf{P} \mathbf{A}_2,$$

где $\mathbf{P}$ – исходное цифровое изображение размера $n \times n$, $\mathbf{Z}$ – результат маскирования размера $n \times n$, $\mathbf{A}_1$ и $\mathbf{A}_2$ – ортогональные матрицы Адамара размера $n \times n$ с коэффициентами {1, -1}, для которых выполняется $\mathbf{A}^T\mathbf{A} = n\mathbf{I}$, где $\mathbf{I}$=diag(1,1…,1).

При демаскировании выполняется обратное двустороннее стип-преобразование вида

$$\mathbf{P} = \mathbf{A}_1^{-1} \mathbf{Z} \mathbf{A}_2^{-1}.$$

В отличие от рассмотренного выше в диссертационной работе предлагается двустороннее преобразование вида

$$\mathbf{Z} = \mathbf{A} \mathbf{P} \mathbf{A}^T,$$

которое обеспечивает более «шумоподобный» результат маскирования – цифровое маскированное изображение.

Рассмотрены и выделены основные типы и форматы современных цифровых видеокадров, способы их представления, показано возрастание разрешений видеоинформации.

Описываются особенности квазиортогональных матриц Мерсенна, близких по свойствам к матрицам Адамара, но отличающихся от них тем, что, во-первых, они существуют на порядках $n = 4k - 1$ (k – натуральное число), во-вторых, имеют значения коэффициентов $\{1, -b\}$, где $b = f(n)$, в-третьих, отдельные структуры этих матриц фрактальны. В результате предлагаемый в работе метод реализуется в виде:

маскирование $\mathbf{Z} = \mathbf{M}\,\mathbf{P}\,\mathbf{M}^{\mathrm{T}}$,

демаскирование $\mathbf{P} = \mathbf{M}^{\mathrm{T}}\,\mathbf{Z}\,\mathbf{M}$,

где **M** – квазиортогональная матрица Мерсенна.

Матрицы Мерсенна — не целочисленные матрицы, элемент b является иррациональным числом. Однако с ростом n значения коэффициентов стремятся к {1,–1}, характерным для матриц Адамара. Приняв элемент b в качестве «ключа», сложность его подбора перебором можно оценить как 2^N, где N – длина b в битах. С учетом структуры матрицы Мерсенна количество операций перебора оценивается как $2^N n!/2$, где n – порядок маскирующей матрицы.

Третий раздел диссертационной работы посвящен описанию алгоритмов маскирования/демаскирования цифровых изображений и кадров видео с использованием двустороннего матричного преобразования с уникальными квазиортогональными матрицами Мерсенна, а также анализу результатов вычислительных экспериментов.

Процедура маскирования/демаскирования состоит из пяти этапов.

На первом этапе выбирается/генерируется уникальная квазиортогональная матрица Мерсенна. При этом должно учитываться то обстоятельство, что порядок используемой для маскирования матрицы и качество маскирования являются взаимосвязанными.

На втором этапе проверяется условие кратности размеров маскируемого изображения порядку матрицы, т.е анализируется выполнения равенства:

$$W_i \bmod n = 0,$$

$$H_i \bmod n = 0,$$

здесь n – порядок маскирующей матрицы Мерсенна, W_i - ширина маскируемого изображения в пикселях, H_i - его высота.

Для тех случаев, когда условие не выполняется, применимы следующие решения:

– подбор/генерация маскирующей матрицы, порядок которой будет удовлетворять условию;

– дополнение маскируемого изображения/кадра пустыми или содержащими среднее значение по строкам/столбцам;

– обрезание (уменьшение размера) у маскируемого изображения строк/столбцов.

Преимущественными являются первое и второе из описанных решений как не приводящие к потере областей изображения, которые могут содержать критически важную информацию.

На третьем этапе маскирование может производится над двумя типами изображений, для которых значения пикселей представлены в виде чисел с фиксированной или плавающей точками.

Этап включает в себя следующие действия:

– вычитание из всех значений матрицы исходного изображения 128 для сдвига начала отсчёта в область нуля;

– двухстороннее умножение исходного изображения на маскирующую матрицу;

– ввиду специфики используемых квазиортогональных матриц Мерсенна квантование не применятся, но выполняется сдвиг вправо при представлении пикселей числами с фиксированной точкой, и деление на коэффициент q при представлении числами с плавающей точкой.

В результате выполнения этапа значения пикселей переведены в байтовые последовательности для дальнейшей передачи или хранения маскированного

изображения. Для представления пикселов числами с плавающей точкой производится преобразование из типа float (32 бита) в 4 числа типа байт, при представлении числами с фиксированной точкой – преобразование из типа long long (64 бита) в 8 чисел типа байт. Таким образом пропорционально увеличивается размер маскированного изображения с WxH до 4WxH или 8WxH.

На четвертом этапе для хранения и передачи маскированных изображений и последовательностей кадров используются три формата: PNG, zmi (Zip Masked Image) или RAW (формат без сжатия).

При представлении маскированного изображения в формате PNG реализуется информационное сжатие без потерь, упрощается задача воспроизведения полученной матрицы в виде плоского изображения. Поскольку PNG широко используется пользовательскими пакетами программ, можно по-кадрово производить анализ маскированной видеопоследовательности.

При представлении маскированного изображения в формате zmi его сжатие осуществляется по алгоритму Deflate, являющемуся комбинацией сжатия без потерь LZ77 и алгоритма Хаффмана.

На пятом этапе, после передачи данных по сети или после чтения с носителя информации выполняется демаскирование – симметричное преобразование, заключающееся в выполнении описанных выше действий в обратном порядке.

Для демонстрации процедуры маскирования/демаскирования были подобраны тестовые изображения (см. рис. 1), включающие в себя: «шахматную доску»; две телевизионные испытательные таблицы (ТИТ); черный круг на белом фоне; черный текст на белом фоне; серое поле; градиент в градации серого. В общей сложности исследование над процедурой маскирования/демаскирования проводилось на выборке из открытых источников, включающую в себя более 1000 цифровых изображений различных разрешений.

Для демонстрации метода маскирования в эксперименте была выбрана матрица $\mathbf{M}_{15}$. Для примера на рис. 2а и 2б представлены маскированные изображения ТИТ с двумя видами представления его пикселей. На рис. 2в и 2г представлены их визуализации, если числовое представление пикселей маскированного изображения не переводить в байтовые значения.

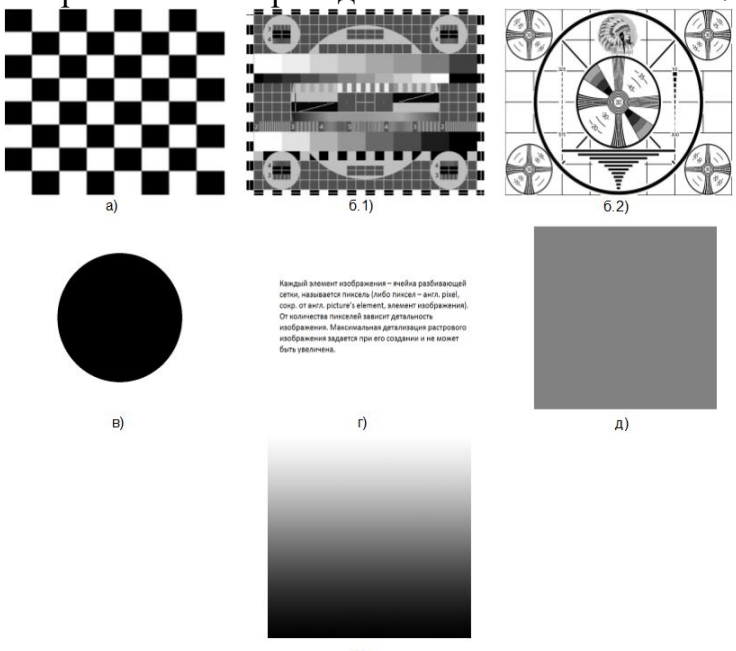


Рисунок 1 – Набор тестовых изображений

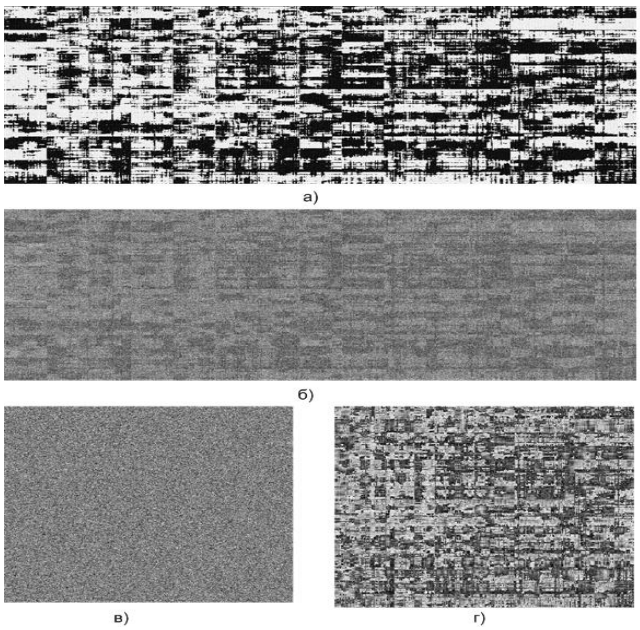


Рисунок 2– Маскированное изображение телевизионной испытательной таблицы (а,в – представление пикселов числами с фиксированной точкой; б,г – числами с плавающей точкой)

На рис. 3 представлены демаскированные (восстановленные) изображения ТИТ и результаты их вычитания из исходного изображения.

Для оценки качества восстановленных изображений, относительно исходных, используются известные метрики, которые скалярно оценивают соответствие восстановленного изображения исходному изображению, а именно: PSNR, MSE, SSIM, MSSIM.

В табл. 1 представлены результаты оценки качества по значениям метрик восстановленных после маскирования изображений с представлением значений пикселей числами с фиксированной точкой. В табл. 2 – результаты оценки качества восстановленных маскированных изображений, с представлением значений пикселей числами с плавающей точкой.

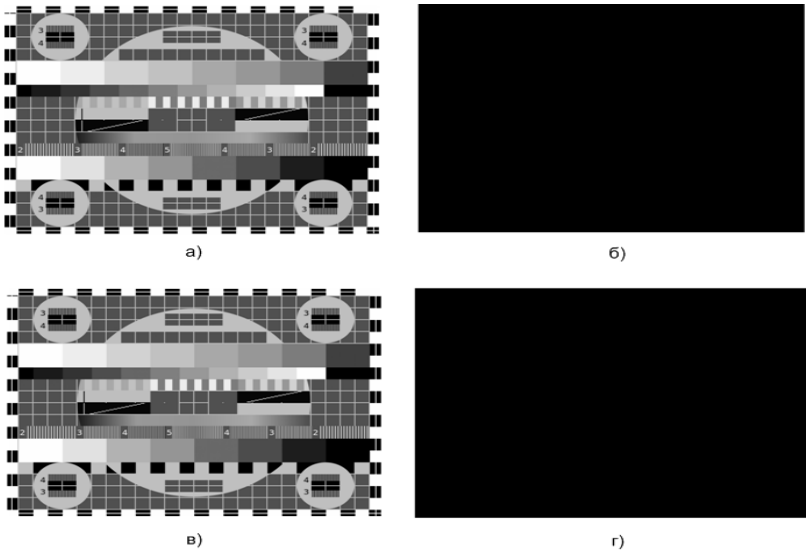


Рисунок 3 - Демаскированные (восстановленные) изображения (а,в) и представление их разностей с исходным изображением (б,г)

Таблица 1 – Оценка качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 1 (а)	51.1339	0.5008	1	1
Рис. 1 (б.1)	50.9848	0.5183	0.9999	1
Рис. 1 (б.2)	18.5996	897.6804	0.9397	0.9770
Рис. 1 (в)	50.2090	0.6197	1	1
Рис. 1 (г)	21.1026	504.4501	0.9682	0.9705
Рис. 1 (д)	48.1308	1	1	1
Рис. 1 (е)	50.8999	0.5286	0.9998	0.9999

Из приведенных таблиц значений метрик видно, что качество восстановленных изображений претерпело незначительное изменение. Однако анализ визуализаций восстановленных изображений демонстрирует отсутствие критических артефактов и изменений относительно исходного изображения.

В разделе решается задача поиска изображений **X**, которые инвариантны к преобразованию маскирования и переводятся им в то же изображение с точностью до постоянного множителя – $\mathbf{M}^{\mathrm{T}}\mathbf{X}\mathbf{M} = \lambda\mathbf{X}$. Такие изображения называют *собственными*, *корневыми* или *особыми*, а число λ – соответствующим особым или корневым числом. Если исходное изображение совпадет с особым изображением используемого преобразования, то маскированное изображение совпадет с исходным и эффект маскирования достигнут не будет. Для используемых в методе ортогональных матриц **M** с собственными значениями $|\lambda| = 1$ при умножении на них слева поиск особых изображений сводится к задаче определения перестановочных друг с другом матриц **XM** = **MX** (или **XM** = – **MX**).

Таблица 2 – Оценка качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 1 (а)	51.1411	0.5	1	1
Рис. 1 (б.1)	51.4682	0.4637	0.9993	0.9998
Рис. 1 (б.2)	68.2706	0.0097	1	1
Рис. 1 (в)	60.5386	0.0574	0.9999	0.9999
Рис. 1 (г)	Inf	0	1	1
Рис. 1 (д)	Inf	0	1	1
Рис. 1 (е)	51.1595	0.4979	0.9983	0.9999

Умножение на матрицу **M** можно рассматривать как умножение на ортогональную матрицу $\mathbf{V}^{-1}$ (поворот изображения), собственно кодирование при помощи знакопеременной матрицы **D** = diag(1, -1, 1, -1, …,1) и обратный поворот **V**. Особое изображение индифферентно к этому процессу, если состоит (частично) из инверсных операций: обратного поворота, любой диагональной матрицы **D*** и поворота. При двустороннем преобразовании матрица **DD*D** = **D*** не изменяется. Отсюда реализован алгоритм построения особых изображений, состоящий в вариации матрицы собственных чисел ортогональной матрицы **M** и ее реконструкции $\mathbf{X}^* = \mathbf{V}\mathbf{D}^*\mathbf{V}^{-1}$.

В процессе выполнения работы для маскирования изображений и их фрагментов использовались матрицы $\mathbf{M}_7$, $\mathbf{M}_{15}$, $\mathbf{M}_{31}$ и $\mathbf{M}_{255}$. В качестве примера на рис. 4, 5 и 6 приведены по два «портрета» (а и б) вычисленных корневых изображений **X*** для матриц порядков 7, 31 и 255. Квадраты различного оттенка серого соответствуют визуализированным пикселям реального изображения.

Представленные изображения инвариантны по отношению к рассматриваемому преобразованию с использованием матриц Мерсенна. Они являются «портретами» объектов, которые не имеют отношения к множеству объектов реального мира – объектов, изображения которых передаются в рассматриваемых в работе видеосистемах. Следовательно, справедливо утверждение о том, что матричное двустороннее маскирование матрицами Мерсенна может быть использовано в системах без каких-либо ограничений, вносимых изображениями, инвариантными к преобразованию $\mathbf{M}^T\mathbf{P}\mathbf{M}$.

Наибольший вклад в искажение демаскированного изображения могут внести потери пакетов при передаче маскированного изображения по телекоммуникационным каналам, обеспечивающим функционирование распределенных видеосистем. Ниже представлены результаты восстановления маскированного изображения, характерные при потере части передаваемых в канале данных или при их преднамеренном искажении. Изменению подверглась лишь часть маскированного изображения.

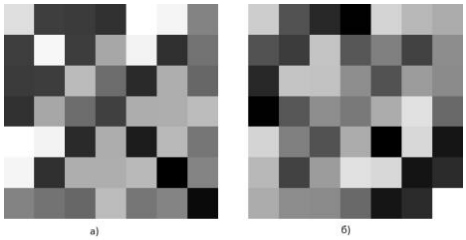


Рисунок 4 – Корневые изображения для матрицы $\mathbf{M}_7$

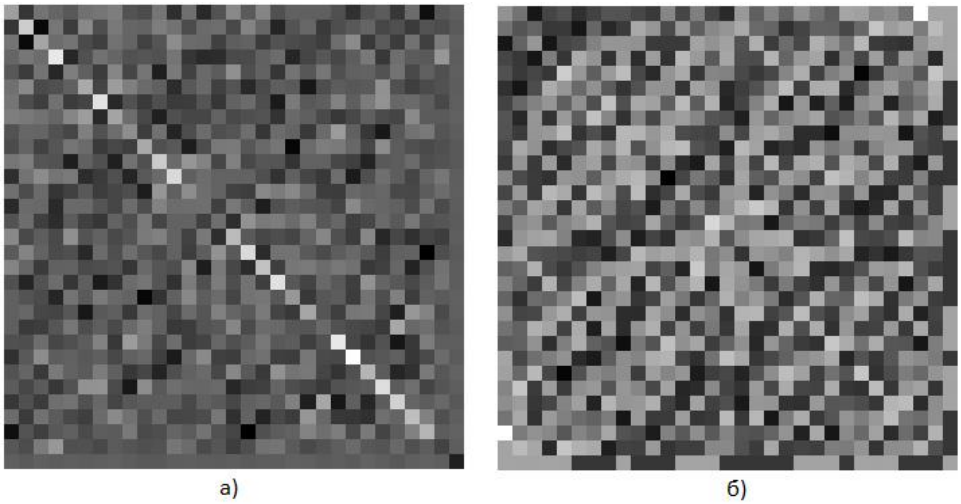


Рисунок 5 – Корневые изображения для матрицы $\mathbf{M}_{31}$

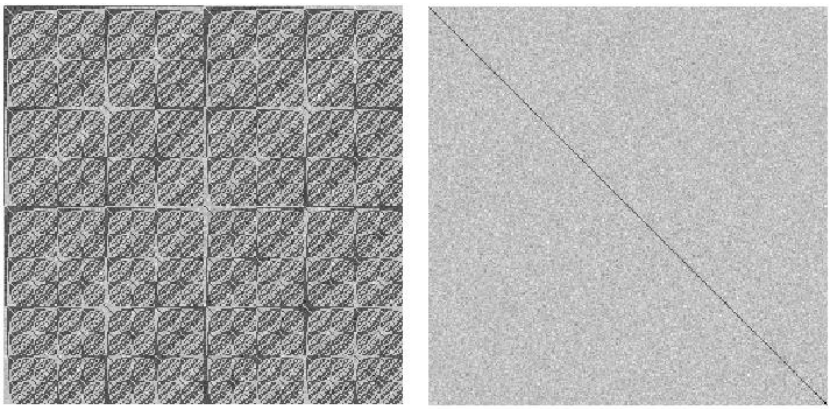


Рисунок 6 – Корневые изображения для матрицы $\mathbf{M}_{255}$

На рис. 7 приведен пример восстановленных изображений ТИТ с искажениями, произошедшими в канале, для которых значения пикселей представлены в виде чисел с фиксированной (а) и плавающей (в) точками.

В таблице 3 представлена оценка качества восстановленных маскированных изображений (рис. 7) по значениям метрик.

Таблица 3 – Оценка качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 7 (а)	17.6707	1.1118e+003	0.8863	0.9297
Рис. 7 (в)	16.1717	1.5700e+003	0.8370	0.8793

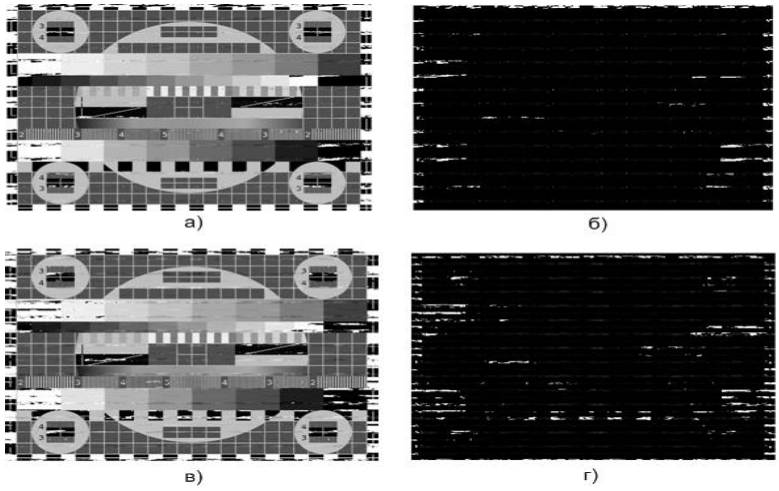


Рисунок 7 –Восстановленные маскированные изображения ТИТ (а, в – восстановленные маскированные изображения с внесенными в канале искажениями; б, г – разности восстановленного и исходного изображения)

Из табл. 3 видно, что при изменении данных (внесении искажений в канале) в демаскированном изображении при восстановлении появляются артефакты. Это связано со спецификой разработанного метода и с тем, что на тестовых изображениях имеется множество блоков с одинаковой яркостью. В тоже время, при внесении помех в реальные маскированные изображения, где на исходное изображение накладывается шум и т.д., при восстановлении артефакты будут

«размазываться» по всему изображению. Это действительно для маскированных изображений, где значения яркостей пикселей представлены в виде чисел с плавающей точкой. Если значения яркостей пикселей представлены числами с фиксированной точкой, то артефакты более заметны.

В четвертом разделе проводится сравнение результатов маскирования набора тестовых изображений и их шифрования симметричным алгоритмом DES. В качестве криптографической библиотеки выбрана Crypto++ 5.6.2 для языка программирования C++, которая имеет оптимизированную реализацию алгоритма DES. Сравнение проводилось как на основе анализа показателей качества, так и результатов оценки времени преобразования изображений.

На рис. 8 в качестве примера представлен результат шифрования исходного изображения, из которого видны резкие переходы и блоки с постоянными значениями пикселей не обеспечивающие сокрытие «смысла» исходного изображения.

Для оценки качества восстановленных шифрованных изображений в сравнении с исходными применялся тот же набор метрик, что и для оценки качества восстановленных маскированных изображений. В табл. 4 представлена оценка качества восстановленных изображений, преобразованных алгоритмом DES, по значениям таких метрик. Из таблицы видно, что качество восстановленных изображений изменилось незначительно. Из приведенных в табл. 1, 2 и 4 результатов следует, что шифрование и маскирование изображений не вносят критических артефактов и изменений.

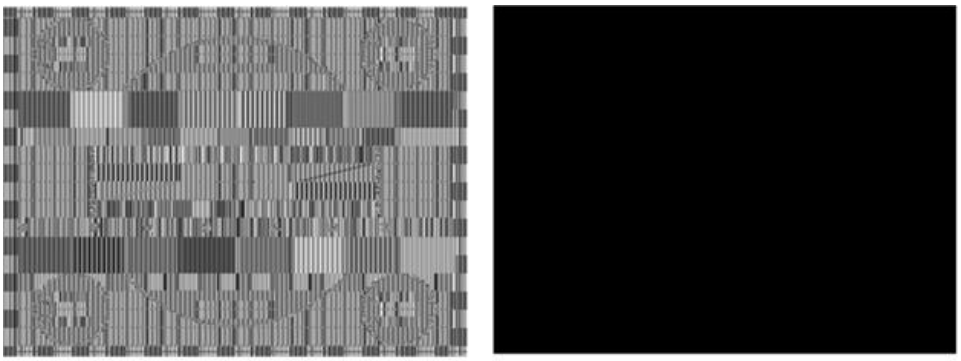


Рисунок 8 – Изображение телевизионной испытательной таблицы (а – шифрованное изображение, б – разность исходного и восстановленного изображения)

Таблица 4 – Оценка качества восстановленных изображений (алгоритм DES)

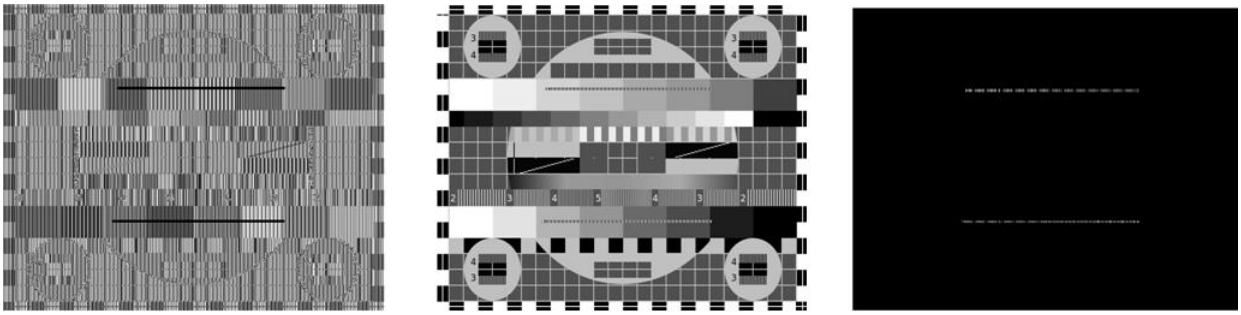
Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 1 (а)	Inf	0	1	1
Рис. 1 (б.1)	84.0965	2.5318e-004	1	1
Рис. 1 (б.2)	104.9432	2.0833e-006	1	1
Рис. 1 (в)	45.4304	1.8623	1	1
Рис. 1 (г)	45.3700	1.8883	1	1
Рис. 1 (д)	50.8675	0.5325	1	1
Рис. 1 (е)	102.1102	4.0000e-006	1	1

Далее описываются результаты моделирования влияния потерь пакетов (блоков данных) и внесения умышленных искажений при хранении на качество восстановления шифрованного алгоритмом DES изображения..

На рис. 9 в качестве примера приведено восстановленное изображение телевизионной испытательной таблицы из шифрованного, показывающее, что его качество претерпело изменение. Этот пример демонстрирует тот факт, что при потере части пакетов в процессе передачи шифрованного изображения на восстановленном изображении появляются артефакты в областях, кратных блоку шифрования. Результаты эксперимента подтвердились на всех тестовых изображениях.

Для оценки времени шифрования изображений использовалась та же библиотека Crypto++ 5.6.2, оптимизированная для работы на процессорах семейства Intel. Поэтому численный эксперимент проводился на ПК с процессором Intel® Core™ i7-2630QM с 8Гб оперативной памяти, ОС – Windows 8.1.

Время маскирования и шифрования изображений в эксперименте включает процедуру сжатия без потерь и, следовательно, чем проще структура сжимаемого файла, тем быстрее производится сжатие и распаковка. Немаловажную роль играет вид представления пикселей: при шифровании на один пиксель отводится один байт, а при маскировании при представлении пикселей числами с фиксированной точкой на один пиксель приходится 8 байт. При представлении пикселей числами с плавающей точкой – 4 байта.



а) б) в)

Рисунок 9 – Восстановление изображения при потере части исходных данных:а) – шифрованное изображение с внесенными изменениями, б) – восстановленное изображение, в) – разность восстановленного и исходного изображения.

Таблица 5 – Время маскирования и шифрования тестовых изображений

Обозначение исходного изображения	Время маскирования/шифрования (мс)				
	DES (сохранение в PNG)	Маскирование			
		Со сжатием gzip		Сохранение в PNG	
		fix	float	fix	float
Рис. 1 (а)	35	128	87	116	70
Рис. 1 (б.1)	42	382	152	106	61
Рис. 1 (б.2)	43	425	166	133	71
Рис. 1 (в)	34	126	91	102	67
Рис. 1 (г)	35	235	110	111	58
Рис. 1 (д)	36	63	28	60	41
Рис. 1 (е)	35	177	85	99	43

В табл. 5 представлены результаты измерения времени маскирования и шифрования изображений. В столбце fix представлены результаты для маскирования изображений с представлением в формате с фиксированной точкой, а float – с плавающей точкой.

В табл. 6 представлены результаты измерения времени демаскирования и дешифрования изображений. Очевидно, что результаты проведенных экспериментов не в полной мере раскрывают преимущества разработанного в диссертационной работе метода. Во-первых, реализованная для исследования программа маскирования/демаскирования не обеспечивает полного распараллеливания реализации матричных вычислений, составляющих его основу. Во-вторых, маскирование производится с использованием кронекеровского преобразования, которое в смысле вычислений является трудоемким. В эксперименте для метода маскирования не производился выбор оптимальной маскирующей матрицы Мерсенна для конкретного типа изображений.

Обозначенные моменты, влияющие на время маскирования, являются предметом дальнейших исследований и модификации метода с целью оптимизации времени преобразований, в том числе и при его аппаратной реализации в системах встраиваемого класса. Немаловажной при этом является задача разработки и собственного «контейнера» (формата), который был бы не критичен к потере небольшой части пакетов и обеспечивал бы одновременно приемлемое сжатие маскированной информации.

Таблица 6 – Время демаскирования и дешифрования тестовых изображений

Обозначение исходного изображения	Время демаскирования/дешифрования (мс)				
	DES (сохранение в PNG)	Маскирование			
		Со сжатием gzip		Сохранение в PNG	
		fix	float	fix	float
Рис. 1 (а)	41	49	31	77	42
Рис. 1 (б.1)	35	52	39	87	33
Рис. 1 (б.2)	38	71	38	124	39
Рис. 1 (в)	40	47	27	78	47
Рис. 1 (г)	37	50	28	70	39
Рис. 1 (д)	34	27	17	51	27
Рис. 1 (е)	35	30	24	44	29

В заключении приводятся основные результаты, полученные в диссертационной работе.

Приложение содержит документы, подтверждающие внедрение и государственную регистрацию программных реализаций алгоритмов на основе разработанного метода.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Основные результаты диссертационной работы могут быть сформулированы следующим образом:

1. Проведено исследование существующих методов маскирования, которые было предложено разделить на криптографические и матричные. Показано, что из-за избыточности фото- и видеоизображения невозможно «скрыть» исходную информацию путем её шифрования с малым ключом. Особенно это критично

для систем встраиваемого класса, где использование длинного ключа для шифрования приведет к задержкам в канале передачи. Сформулированы требования для матричного маскирования.

2. Предложен новый метод на основе модификации стрип-преобразования изображений с использованием уникальных квазиортогональных матриц Мерсенна порядков $n=4k-1$ (где k – натуральное число) для покадрового маскирования изображений. Элементы матриц Мерсенна с ростом значений k стремятся к значениям {1, –1}, свойственным матрицам Адамара, что позволяет сохранить помехоустойчивость базового метода. Предложен алгоритм адаптации маскируемого изображения к порядку маскирующей матрицы.
3. Для использованных в работе матриц Мерсенна получены особые изображения, инвариантные к двустороннему матричному преобразованию – основе разработанного метода.
4. Исследованы устойчивость предлагаемого метода к потерям информации в канале и внесению изменений третьей стороной в передаваемую маскированную информацию, а также качество маскирования и влияние маскирующего преобразование на качество восстановленного изображения.
5. Проведен сравнительный анализ предлагаемого метода маскирования с алгоритмом симметричного шифрования DES. Было выявлено влияние особенностей изображений на результат их шифрования с использованием короткого ключа.
6. Внедрение результатов диссертационной работы в виде программной реализации в системе-на-кристалле с DSP-сопроцессорами (ADSP-BF523KBCZ и др.) в видеорегистраторах специального назначения показало возможность реализации матричного маскирования в системах встраиваемого класса в реальном масштабе времени.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых научных изданиях

1. Чернышев, С.А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами / С.А. Чернышев, А.А. Востриков // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99-103.
2. Чернышев, С.А. О выборе матриц для процедур маскирования и демаскирования изображений / С.А. Чернышев, А.А. Востриков, О.В. Мишура, А.М. Сергеев // Фундаментальные исследования. – 2015. – № 2–24. – С. 5335-5339.
3. Чернышев, С.А. Цифровое маскирование матрицами Мерсенна и его особые изображения / С.А. Чернышев, Ю.Н. Балонин, А. А. Востриков, Е.А. Капранова, А. М. Сергеев, О. И. Синицына //Фундаментальные исследования, № 4, 2017. С.13 - 18

В изданиях, входящих в систему цитирования Scopus

4. Chernyshev, S. A. Implementation of Novel Quasi-Orthogonal Matrices for Simultaneous Images Compression and Protection / S. A. Chernyshev, A. A. Vostrikov // Frontiers in Artificial Intelligence and Applications. 2014. T. 262. C. 451-461. DOI: 10.3233/978-1-61499-405-3-451

5. Chernyshev, S. Digital masking using Mersenne matrices and its special images / S. Chernyshev, A. Vostricov, M. Sergeev, N. Balonin, // Procedia Computer Science. Vol. 112, Elsivier, 2017, P. 1151-1159.
   DOI: https://doi.org/10.1016/j.procs.2017.08.156

В других изданиях

6. Чернышев, С.А. О восстановлении маскированного изображения при возникновении информационных потерь в процессе передачи / С.А. Чернышев, А.А. Востриков // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2014. – с. 185-190.
7. Чернышев, С.А. Исследование влияния порядка маскирующей матрицы на эффективность сжатия изображения матрицы / С.А. Чернышев, А.А. Востриков // // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2013. – с. 109-112.
8. Чернышев, С.А. Исследование устойчивости маскированного изображения к атакам путем подбора ключевой М-матрицы/ С.А. Чернышев // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2014. – с. 282-287.
9. Чернышев, С.А. Первая реализация фильтра Мерсенна с регулируемым квантованием уровней/ С.А. Чернышев // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2013. – с. 172-175.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2015611308 от 27 января 2015 г. «Специальное программное обеспечение для маскирования изображений методом матричных целочисленных преобразований в квазиортогональных базисах» // А. А. Востриков, Ю. Н. Балонин, М. Б. Сергеев, С. А. Чернышев, 2015 г.
11. Свидетельство о государственной регистрации программы для ЭВМ № 2015611310 от 27 января 2015 г. «Специальное программное обеспечение для демаскирования изображений методом матричных целочисленных преобразований в квазиорто-гональных базисах» // А. А. Востриков, Н.В. Соловьев, М.Б. Сергеев, С. А. Чернышев, 2015 г.
12. Свидетельство о государственной регистрации программы для ЭВМ № 2015611311 от 27 января 2015 г. «Специальное программное обеспечение маскирования изображений матричными преобразованиями в формате с плавающей запятой с использованием квазиортогональных матриц» // Востриков А. А., Балонин Ю. Н., Сергеев М.Б., Чернышев С. А., 2015 г.
13. Свидетельство о государственной регистрации программы для ЭВМ № 2015611309 от 27 января 2015 г. «Специальное программное обеспечение демаскирования изображений матричными преобразованиями в формате с плавающей запятой с использованием квазиортогональных матриц» // А. А. Востриков, Н. А. Балонин, М.Б. Сергеев, С. А. Чернышев, 2015 г.
14. Свидетельство о государственной регистрации программы для ЭВМ № 2017616795 от 14 июня 2017 г. «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., Чернышев С. А., Сергеев А. М., 2017 г.