ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

На правах рукописи

Чернышев Станислав Андреевич

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА МАТРИЧНОГО МАСКИРОВАНИЯ ВИДЕОИНФОРМАЦИИ В ГЛОБАЛЬНО РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Специальность 05.12.13 –
«Системы, сети и устройства телекоммуникаций»

Диссертации на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук, профессор
Сергеев Михаил Борисович

Санкт-Петербург – 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность работы. Видео- и фото-информация используются сегодня в самых разных видах производственной деятельности человека, а также в повседневной его 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, учитывающее 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 по криптографии таких ученых как T. ElGamal, R. L. Rivest, Sh. McEliece, А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, В. И. Нечаев и др.

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 для защиты визуальной информации, рассматриваемой как особая цифровая информация, используются не криптографические методы.

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/демаскирова-ния 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 результатов 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.

1 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ. КЛАССИФИКАЦИЯ СУЩЕСТВУЮЩИХ МЕТОДОВ МАСКИРОВАНИЯ

В настоящем разделе описываются основные характеристики современных цифровых распределенных систем видеонаблюдения. Анализируется современное состояние теории маскирования. Формулируется расширенное определение процедуры маскирования фото- и видеоизображений. Анализируются и выделяются основные типы и форматы изображений, подлежащих маскированию. Оцениваются возможности реализации матричных преобразований в ПЛМ (FPGA) и процессорах ЦОС (DSP).

1.1 Области использования и основные характеристики цифровых распределенных систем видеонаблюдения

Цифровые распределенные системы видеонаблюдения применяются при мониторинге и регистрации чрезвычайных ситуаций (МСР™), анализе дорожно-транспортной обстановки, фиксации событий в местах проведения массовых мероприятий, в беспилотной авиации, в охранной деятельности, при наблюдении за распределенными объектами и др.

Использование распределенных систем видеонаблюдения позволяет осуществлять поддержку при принятии решений, повышает эффективность управления технологическими процессами, их надежность и результативность. Обычно, видеоинформация, передаваемая в большинстве перечисленных распределенных систем, является не секретной, у неё малый срок актуальности, однако она не желательна для массового распространения и использования.

Поскольку перечисленные распределенные системы видеонаблюдения строятся, в основном, на основе использования незащищенных IP-сетей общего пользования, трансляция по ним изображений и видеоданных требует защиты.

Системы видеонаблюдения можно разделить на цифровые и аналоговые. Использование аналоговых систем в современных условиях становится не рентабельным, так как связано с большими затратами и их сложностью, а порой и невозможностью функционирования. Построение систем видеонаблюдения с применением IP-технологий обеспечивает гибкость построения системы и ее реконфигурируемость, возможность установки камер в труднодоступных местах, высокую надежность передачи видеоданных и их помехоустойчивость. Основной минус таких систем видеонаблюдения – открытость инфраструктуры сетей и доступность IP-камер, находящихся вне зоны охраны.

К основным характеристикам современных видеокамер цифровых распределенных систем видеонаблюдения относятся [1]:

- формат видеоматрицы (размер диагонали матрицы в дюймах) – определяет угол зрения при использовании объектива с разным фокусным расстоянием;
- разрешение (пикс) – характеризует детальность изображения, при большем разрешении проще детектировать мелкие, значимые детали на передаваемом видеоизображении;
- чувствительность (люкс) – характеризует минимальный уровень освещенности, при котором камера выдает распознаваемый видеосигнал;
- отношение сигнал-шум (дБ).
- электронный затвор (с) – элемент матрицы, который позволяет регулировать время накопления электрического заряда;
- компенсация заднего света (BLC) – функция видеокамеры, позволяющая управлять автоматической регулировкой усиления и электронным затвором не по всей площади экрана, а по его центральной части для компенсации излишек освещения, мешающих восприятию изображения;

- цифровая обработка видеосигнала (DSP) – позволяет значительно увеличить функциональные возможности видеокамеры, например, детектировать наличие движений в кадре и т.д.;
- тип установки видеокамер (обычная или скрытная);
- условия работы видеокамер (помещение, улица и т.д.).

В таблице 1.1 приведены некоторые технические характеристики трех современных КМОП-матриц компании Aptina Imaging (Micron Technology Inc.) [2].

Таблица 1.1 − Технические характеристики КМОП-матриц Micron

Модель	MT9V024	MT9M032	MT9J003
Разрешение	752 x 480	1440 x 1080	3856 x 2764
Формат	1/3"	1/4.5"	1/2.3"
Размер пикселя, мкм	6.0 x 6.0	2.2 x 2.2	1.6 x 1.6
Частота кадров	60 Гц	30 Гц	15 Гц
Затвор	кадровый	строковый / полукадровый	строковый / полукадровый
Выходной интерфейс	последовательный / параллельный 8/10 бит	последовательный 12 бит	последовательный / параллельный 10бит
Цвет/ЧБ	цвет, ЧБ	цвет, ЧБ	цвет, ЧБ

IP-камера является цифровым устройством, проводящим видеосъемку, оцифровку, регистрацию звука и синхронизацию его с видеосигналом, сжатие, формирование пакетов и их передачу по сети.

IP-камера включает в себя следующие элементы [3]:

- ПЗС/КМОП-матрицу;
- объектив и оптический фильтр;
- плату видеозахвата;
- блок управления компрессией (сжатием) видеоизображения;
- основной процессор и встроенный IP-сервер;
- оперативную память, флэш-память;
- сетевой интерфейс;

– последовательные порты вывода данных;
– входы/выходы оповещающих сигналов.

На рисунке 1.1 представлена укрупненная структурная схема IP-камеры:

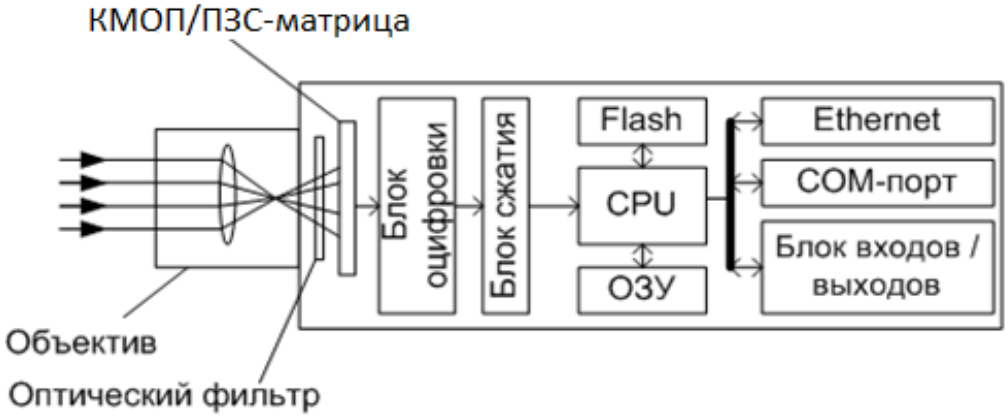


Рисунок 1.1 − Структурная схема IP-камеры

При маскировании предварительное сжатие оцифрованного изображения, поступающего на CPU (DSP, FPGA) не осуществляется.

К основным преимуществам использования IP-видеонаблюдения относится [4]:

– высокое качество съемки;
– возможность передачи видеоданных по сети Internet и локальной сети, что позволяет установить систему IP-видеонаблюдения на уже готовую сеть;
– легкая масштабируемость и конфигурирование;
– широкий спектр применения;
– передача сигнала в сжатом виде;
– неограниченные сетевые возможности.

Основным недостатком является возможность сетевого взлома и зависания в процессе работы.

На рисунке 1.2 представлена схема канала передачи распределенной IP-системы видеонаблюдения и список рисков, связанных с передачей данный по сети Internet:

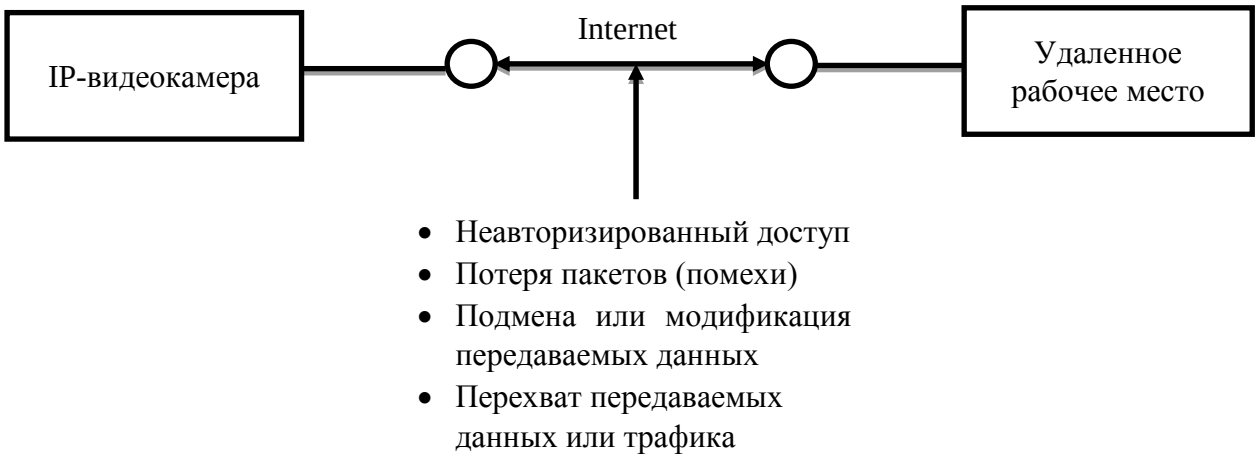


Рисунок 1.2 − Схема канала передачи распределенной IP-системы видеонаблюдения

Использование криптографических методов для сокрытия передаваемой по сети Internet исходной видеоинформации в видеокамерах современных цифровых распределенных систем видеонаблюдения в режиме реального времени затруднительно. Это связано с необходимостью использования ключей большой длины для полного «сокрытия» объектов на изображении, а для этого требуются значительные вычислительные ресурсы из-за больших объемов самой видеоинформации. В тоже время на сами камеры возлагаются всё более интеллектуальные и ресурсоемкие задачи, такие как: поиск объекта, трекинг, анализ изменений в кадре и т.д.

1.2 Современное состояние теории маскирования. Расширенное определение процедуры маскирования

Термин «маскирование» в настоящее время используется в различных областях человеческой деятельности, таких как биология [5], военное дело [6], химия [7], психология [8,9], технологии управления базами данных [10,11],

обработка фотографических изображений [12], цифровая обработка изображений [13].

В то же время на протяжении последних 8 лет данный термин используется в области защиты от несанкционированного доступа к цифровым изображениям, имеющим малое время актуальности.

Основные определения, дополняющие перечисленные выше известные и относящиеся к области защиты цифровых фото- и видеоданных, сформулированы в работах [14, 15].

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 визуальной информацией или маскированным изображением.

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

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

Первые упоминания о необходимости замены шифрации видеоданных для задач передачи видеоизображений в глобальных распределенных сетях встречаются в работе [16]. В ней приведено обоснование того, что использование известных криптографических алгоритмов в задачах защиты визуальной информации проблематично, поскольку ограниченный вычислительный ресурс встраиваемых систем, какими являются IP-камеры, позволяет использовать их лишь с небольшой длиной ключа. При использовании такого ключа на преобразованном изображении остаются контуры, характерные светлые или

темные области и др., что позволяет идентифицировать передаваемое изображение или даже полностью наблюдать сценарий происходящих на видеопоследовательности событий, действий. Объясняется это тем, что человеческое зрение представляет собой лучшую систему распознавания образов, а изображения и видеоинформация – особый вид информации, плохо разрушаемый на уровне визуализации, и требующий для своей защиты особых подходов и специальных методов [16].

Пример результатов применения поточного шифра RC4 с ключом различной длины к различным изображениям представлен на рис. 1.3 [17]:

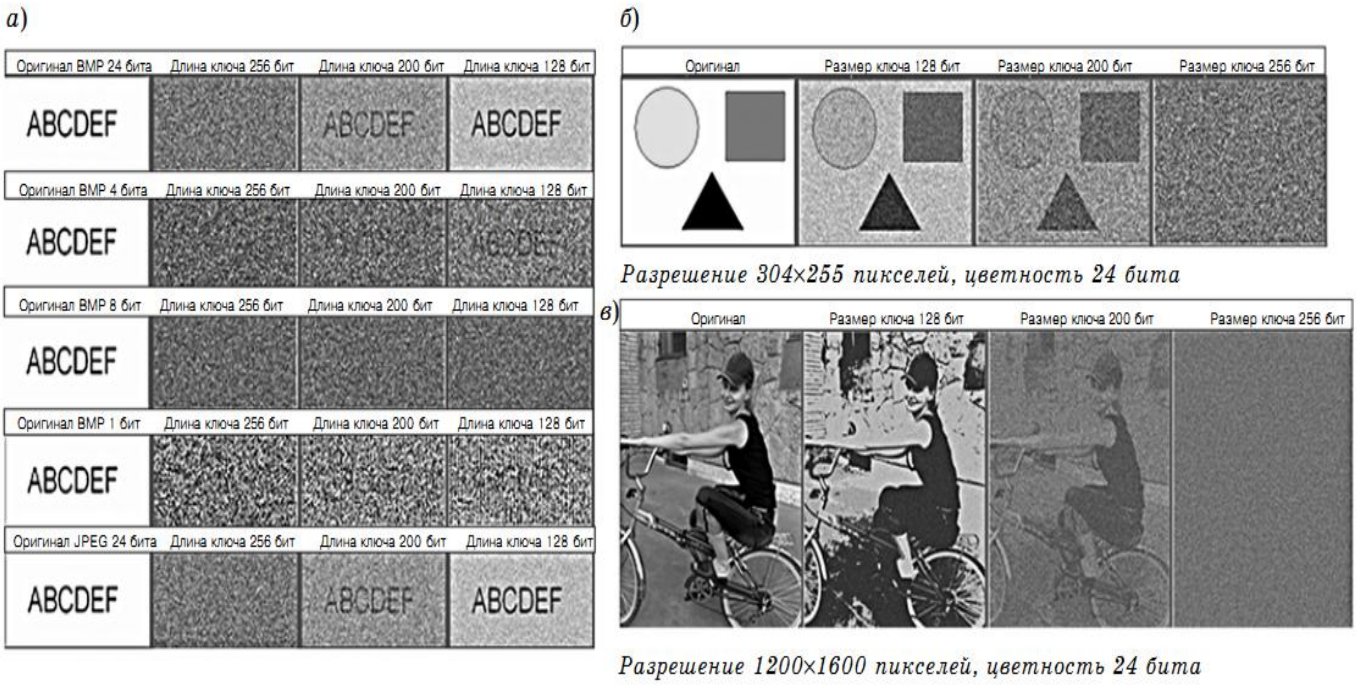


Рисунок 1.3 − Пример использования поточного шифра RC4 для изображения с текстом (а), цветного рисунка (б) и фотографии (в)

Существующие методы цифрового маскирования изображений можно разделить на два вида:

- криптографическое маскирование или маскирование с использованием криптографических примитивов;
- матричное маскирование.

Определение 4. Криптографическое маскирование – вычислительная процедура прямого преобразования цифровых или аналоговых изображений с

применением элементов криптографических методов, разрушающая их до вида, воспринимаемого визуально как шум.

Определение 5. Криптографическое демаскирование – вычислительная процедура обратного преобразования с использованием элементов криптографических методов, восстанавливающая исходное цифровое или аналоговое изображение из маскированного.

К криптографическим методам маскирования или методам с использованием криптографических примитивов можно отнести следующие методы.

Метод, предложенный в диссертации М. Ю. Литвинова [18], реализует для маскирования видеоинформации процесс преобразования изображения в теле кадра к «шумоподобному» виду. Для преобразования видеоинформации используются криптографические примитивы. Литвиновым М. Ю. введены понятия первичной и вторичной информации при передаче маскированных изображений. Под первичной информацией понимается структура сцены на изображении. Под вторичной информацией понимается характер передаваемого видеоизображения (статичная/динамичная сцена, контрастная/темная сцена и т.п.) и указывается, что данную информацию третья сторона может получить, используя размер перехватываемого кадра.

В работе [19] предложен метод маскирования передаваемого видеопотока с учетом его особенностей, которые обусловлены его форматом. Маскирование производится за счет разрушения синхроимпульсов видеосигнала в канале передачи. Метод демонстрирует хороший результат, но применим для маскирования только аналогового видеопотока.

Метод маскирования цифровой визуальной информации с помощью кватернионов или Quaternion Encryption Scheme (QES) [20], основанный на Cipher Block Chaining (CBC), являющийся одним из режимов шифрования для симметричного блочного шифра с использованием механизма обратной связи. Кватернионы – гиперкомплексные числа четвертого ранга. Для шифрования изображения используется вращение векторов данных, представленных в виде

кватернионов в трехмерном пространстве вокруг другого кватерниона, который является ключом. Данный метод используется для шифрования видеоизображения и для подтверждения подлинности видеоизображения на приемной стороне распределенной видеосистемы. Для представления маскированного изображения в виде «шума» необходимо произвести несколько циклов маскирования.

Определение 6. Матричное маскирование – вычислительная процедура преобразования цифровых изображений с использованием матричных операций, разрушающая его до вида, воспринимаемого визуально как шум.

Определение 7. Матричное демаскирование – вычислительная процедура обратного преобразования с использованием матричных операций, восстанавливающая исходное цифровое изображение из маскированного.

К матричным методам маскирования можно отнести следующие.

Метод, предложенный профессором И. Л. Ерошем [16], в котором матричные преобразования изображения осуществляются умножением вектор-столбцов фрагментов изображений на особенные матрицы над полем GF(2) – матрицы с определителем, равным 1. Этот метод работоспособен при выполнении ряда указанных ниже требований:

- пиксели с одинаковой яркостью должны преобразовываться в пиксели с разной яркостью, что обеспечит разрушение контуров изображения;
- характерные области на исходном изображении должны попадать в различные области в преобразованном изображении.

Недостатками этого метода являются, во-первых, огромная сложность нахождения матриц с определителем 1 в поле GF(2) с элементами {0, 1}, а во-вторых, ограниченность количества таких матриц.

В качестве основы метода матричного маскирования можно рассматривать стрип-преобразование, предложенное Л. А. Мироновским и В. А. Слаевым в работе [21]. Преобразование предназначено для помехоустойчивого кодирования изображений при передаче по каналам связи с импульсными помехами, искажающими изображение. Оно основано на матричных операциях и

обеспечивает ослабление амплитуды импульсной помехи на изображении за счет её равномерного распределения по всему изображению. В стрип-преобразовании используются матрицы Адамара. Они являются широко известными, особенно матрицы малых порядков, и находятся в общем доступе в сети Интернете, что не позволяет рассматривать преобразование как метод матричного маскирования.

В работе [22] рассматривается и описывается метод маскирования изображений с использованием матричной модели перестановок с матрично-битоворазрядной декомпозицией. К достоинствам этого метода относится то, что матрицы для маскирования можно генерировать на стороне встраиваемого устройства, маскирующее преобразование является симметричным. Маскирующие матрицы в данном методе являются матрицами поворота. Недостаток – не представляется возможным использовать метод для маскирования видеоряда, поскольку по-битовый срез предполагает, что исходное изображение, например, при разрешении 128x128 (в градации серого) преобразуется к виду 1024x1024 и такого же размера должна быть одна из маскирующих матриц. При увеличении разрешения маскируемого изображения рост временных затрат на маскирующее преобразование будет существенно увеличиваться.

1.3 Основные типы и форматы изображений, подлежащих маскированию

Основной вид изображений, рассматриваемый в настоящей работе, – исходное растровое изображение, представляющие собой двумерный массив, элементы которого называются пикселами и содержат информацию о цвете.

Обычно цифровую обработку применяют к растровым изображениям следующих типов [23]:

- бинарное изображение, элементы которого принимают только два значения {0, 1}. Бинарные (бинаризованные) изображения в основном получаются в результате обработки полноцветных, палитровых или полутоновых изображений методами бинаризации. При бинаризации изображений используется фиксированный или адаптивный порог бинаризации.
- полутоновое изображение, элементы которого принимают одно из значений интенсивности какого-либо одного цвета. Данный тип изображения является одним из самых распространенных при проведении различных исследований. Самая распространенная глубина цвета на элемент изображения – 8 бит.
- палитровое изображение, элементы которого представляют собой ссылку на ячейки карты цветов (палитру). Палитра – двумерный массив, в столбцах которого расположены интенсивности цветовых составляющих одного цвета.
- полноцветное изображение, элементы которого непосредственно хранят информацию о яркостях цветовых составляющих.

Основными типами растровых изображений для маскирования являются полутоновое и полноцветное. В настоящей работе рассматривается маскирование применительно к полутоновым изображениям. Однако он применим и к цветным изображениям и кадрам, представляемым, например, в RGB, отдельно к каждой составляющей.

Основной формат маскируемых цифровых изображений – Bitmap Picture (BMP), разработанный Microsoft для хранения растровых изображений. Он непосредственно хранит значения пикселей изображений с переменной глубиной цвета, полученных непосредственно с видеоматрицы. Изображения формата BMP не используются для передачи по сетям из-за большого размера файлов. Формат файла BMP способен хранить цифровые изображения произвольной ширины, высоты и разрешения. Форматом также предусмотрено сжатие без потерь, обычно не используемое. Формат BMP в диссертационной работе является основным для

изображений, подлежащих маскированию и исследованию параметров маскирования.

1.4 Перспектива реализации матричных преобразований в ПЛИС и процессорах ЦОС

Матрицы и операции над ними широко используются при математическом моделировании разнообразных явлений, процессов и систем. Они являются основой для большинства инженерных и научных расчетов. Матричные вычисления трудоемки, но в тоже время представляют собой классическую область применения параллельных вычислений, ориентированных на высокоскоростные преобразования. Именно матричные операции дают прекрасную возможность для демонстрации многих приемов и методов параллельного программирования [24].

При распараллеливании вычислений с матрицами имеется возможность увеличить производительность (скорость) вычислений на таких устройствах как многоядерный процессор, графический ускоритель, процессор ЦОС и структура на ПЛИС.

Процессор ЦОС оптимизирован для выполнения повторяющихся операций (умножение с суммированием), а также поддерживает векторные операции и матричные вычисления. ПЛИС позволяет реализовать специализированный вычислитель с требуемой конфигурацией и параллельной структурой. В виду этого, процессоры ЦОС и ПЛИС идеально подходят для матричных операций, а, следовательно, и для реализации матричного маскирования.

Маскированное изображение может быть представлено в двух видах: в формате массива целочисленных данных или данных с плавающей запятой. Для маскирования изображений, представляющих собой матрицу с целочисленными элементами, наиболее предпочтительны структурные реализации вычислителя на ПЛИС. Процессоры ЦОС подходят для реализации на них процедуры

маскирования изображений, представленных матрицей с элементами в виде чисел с плавающей запятой.

В тоже время, процессоры ЦОС не столь специализированы как ПЛИС, они менее эффективны для обеспечения на матричных операциях максимальной скорости. Однако, их плюсом является гибкость и простота программирования. Для процессоров ЦОС программист не должен детально вникать в аппаратную архитектуру, так как она скрыта от пользователя, что нельзя сказать о процессе программировании на ПЛИС. Приложение, написанное для ПЛИС может обеспечить максимальную производительность, если надлежащим образом распараллелена его архитектура [116].

Типичная архитектура на ПЛИС для параллельного умножения двух матриц A (n x m) и B (m x n) представлена на рисунке 1.4 [115]. Строка матрицы A с индексом 0 хранится в блоке памяти RAM A0, строка с индексом 1 хранится в блоке памяти RAM A1 и т.д. Столбец матрицы B с индексом 0 хранится в блоке памяти RAM B0 и т.д. Самое важное преимущество такой архитектуры – это то, что требуется только $n + m$ блоков памяти (на выходе каждого блока необходимо множество арифметических модулей). Это очень важно, так как во многих приложениях на ПЛИС для встраиваемых систем емкость памяти ограничивает уровень параллелизма.

В зарубежной печати опубликован ряд работ, где представлены различные улучшения типичной архитектуры для параллельного умножения матриц на ПЛИС [113 – 118] и способы распараллеливания/ускорения матричного умножения на процессорах ЦОС [119 – 121]. Это позволяет говорить о реализуемости метода матричного маскирования в системах встраиваемого типа на процессорах ЦОС для маскирования изображений, представляемых матрицей с элементами в виде чисел с плавающей запятой, и ПЛИС для маскирования изображений, представляемых матрицей с целочисленными элементами.

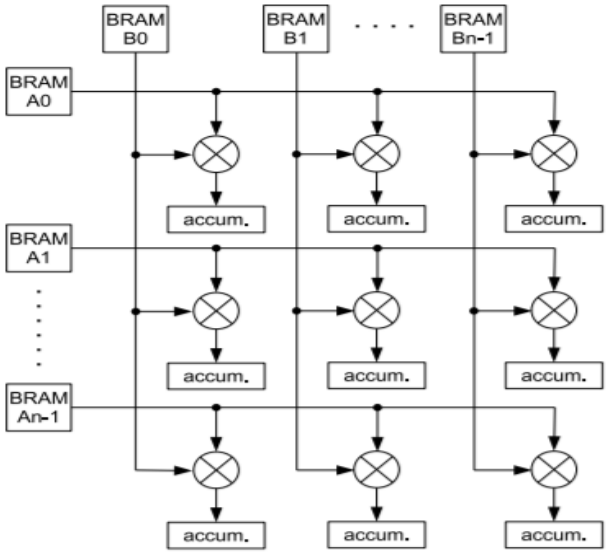


Рисунок 1.4 – Типичная архитектура на ПЛИС для параллельного умножения двух матриц

Проведенный анализ известных методов матричного маскирования позволяет сформулировать основные требования к ним при реализации в рассматриваемых распределенных видеосистемах с открытым коммуникационным каналом.

Во-первых, метод маскирования должен требовать минимальный вычислительный ресурс, обеспечивающий эффективную реализацию в оптико-электронных модулях встраиваемых систем.

Во-вторых, маскирующее и демаскирующее преобразования должны быть симметричными, т.е. должны выполняться преобразования во взаимно обратной последовательности.

В-третьих, маскирующее преобразование должно обеспечивать адаптируемость процедуры маскирования/демаскирования к разрешению матриц цифровых видеокамер.

В-четвертых, метод должен обеспечить устойчивость маскированной информации к помехам и потерям в коммуникационном канале, к преднамеренным искажениям.

В-пятых, метод должен обеспечить возможность определения наличия изменений в маскированных изображениях при передаче по открытым коммуникационным каналам или при хранении.

1.5 Выводы

В настоящем разделе рассмотрены области применения цифровых распределенных систем видеонаблюдения и их основные характеристики. Введено расширенное понятие маскирования цифровых изображений, а также проведена классификация маскирования, включающая криптографическое и матричное маскирование.

Проведенный анализ видов маскирования позволил выделить их основные особенности и имеющиеся недостатки. Показаны основные недостатки классических методов шифрования на визуализированных результатах их применений к изображениям.

Для маскирования выделен, как основной тип, растровое полутоновое изображение в формате BMP.

Анализ работ в области распараллеливания и ускорения матричного умножения на ПЛИС и процессорах ЦОС показал возможность реализуемости матричного маскирования в реальном масштабе времени, при представлении элементов матриц числами с плавающей запятой и целыми числами.

Выполнение сформулированных к методам маскирования требований обеспечит достижение поставленной в диссертации цели в телекоммуникационных системах за счет использования простых матричных преобразований.

2 ОБЗОР МЕТОДОВ МАСКИРОВАНИЯ. ВЫБОР МАСКИРУЮЩЕГО МАТРИЧНОГО БАЗИСА

В данном разделе рассмотрены методы маскирования изображений. Показано, что методы матричного маскирования могут более эффективно использоваться по сравнению с другими известными методами.

Основой таких методов служит модифицированный стрип-метод в совокупности с переходом к использованию уникальных квазиортогональных матриц.

Показано, что класс двухуровневых квазиортогональных матриц значительно шире класса ортогональных матриц Адамара, а классификация показывает существование базиса малоуровневых (двухуровневых) матриц на порядках, соответствующих практически всему ряду натуральных чисел.

Рассматриваются в качестве основных матриц для процедуры маскирования/демаскирования матрицы Мерсенна, наиболее близкие по своим свойствам к матрицам Адамара.

2.1 Обзор реализаций методов маскирования

Процедура маскирования изображений и кадров видеопоследовательности М. Ю. Литвинова**,** представленная в работе [18], осуществляет маскирование видеоинформации с использованием криптографических примитивов. В ней используется несимметричный алгоритм маскирования видеоинформации, основу которого составляют коды, исправляющие ошибки. Метод является улучшенным вариантом системы Мак-Элиса [25-29], который модифицирован алгоритмом Rao-Nam [30-32] и позволяет устранить недостатки исходной системы.

При использовании системы Мак-Элиса изображение кодируется некоторым кодом Гоппы [33]. На полученный результат производится наложение ошибок, веса которых не превышают корректирующей способности кода. Передающее устройство хранит информацию об открытом ключе. Такая реализация имеет два положительных эффекта:

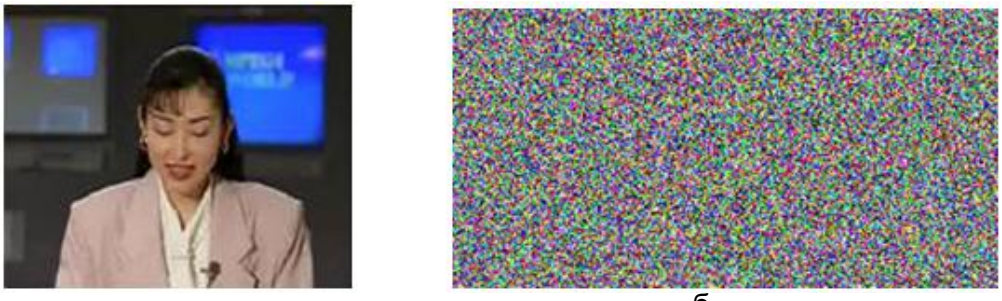
– нет необходимости синхронизировать приемное и передающее устройства;
– передающее устройство не содержит конфиденциальной информации.

Усовершенствованная система Мак-Элиса с модифицированной схемой Rao-Nam позволяет избежать хранения массива кодовых слов на передающей и приемной сторонах для их использования в качестве секретного ключа. Для достижения данного эффекта используется хэш-функция:

$$c = (\mathbf{P} \oplus f) \cdot \mathbf{G}' + e \cdot \mathbf{N},$$

где f=hash(e), e – случайный вектор ошибки длины n, **P** – исходная информация, **G**’– матрица, составляющая открытый ключ, **N –** случайная перестановочная матрица $n \times n$.

На рис. 2.1 приведены исходное цветное изображение и полученное маскированное изображение после реализации модифицированной схемы Мак-Элиса, взятые из работы [18].



а б

Рисунок 2.1 – Пример применения модифицированной схемы Мак-Элиса для цветного изображения (а – исходное изображение, б – маскированное изображение)

Основные недостатки рассмотренного метода – большая вычислительная сложность и значительное увеличение объема кадра [18].

Метод маскирования, предложенный И. Л. Ерошем и описанный в работе [16], разработан для маскирования видеоизображений в системах встраиваемого класса и использует матричные преобразования – умножение в поле GF(2) неособенных матриц с элементами {0, 1}, имеющих определитель, равный 1, на вектор-столбцы фрагментов изображений. Маскирование и демаскирование изображений осуществляется с использованием сложения по модулю 2.

Рассматриваемый метод маскирования изображений хорошо совместим с применением корректирующих кодов, что позволяет защитить маскированное изображение как от ошибок в коммуникационном канале, так и от несанкционированного доступа к передаваемой информации [17]. Например, для маскирования исходного изображение матрицей **M** размерностью 7x7 в поле GF(2), исходное изображение необходимо разбить на 7 фрагментов и в соответствии с единицами матрицы **M** складывать фрагменты по модулю 2.

В общем виде процедура маскирования и демаскирования изображений с использованием матриц с определителем, равным 1, в поле GF(2) представляется как:

$$\mathbf{Z} = \mathbf{M} \times \mathbf{P}$$

$$\mathbf{P} = \mathbf{M}^{-1} \times \mathbf{Z},$$

где **M** – маскирующая матрица с определителем 1 в поле GF(2), $\mathbf{M}^{-1}$ – матрица обратная матрице **M** для демаскирования изображения, **P** – исходное изображение, **Z** – маскированное изображение.

Данный метод позволяет маскировать, кроме изображений, широкий спектр сообщений, таких как команды и тексты без смены маскирующей матрицы.

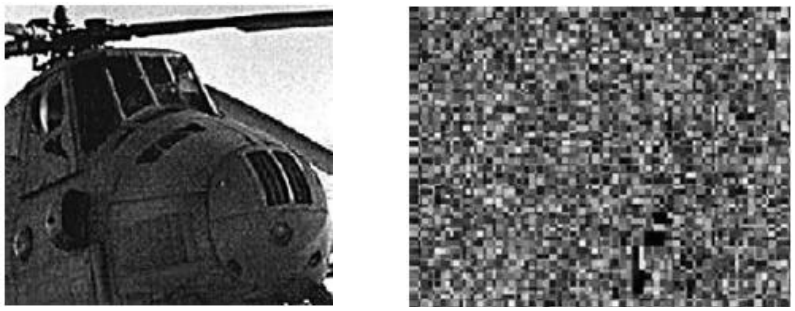
Матрицам с определителем, равным 1, в поле GF(2) присущи следующие свойства:

- результат произведения двух матриц M_1 и M_2 размера (n, n) есть матрица с определителем, равным 1, в поле GF(2);
- перестановка любых строк (и столбцов) матрицы не меняет ее определителя в поле GF(2). Порядок циклической группы, порождаемой этой матрицей, меняется.

– замена любой строки на линейную комбинацию (сложение по модулю 2) этой строки с любыми строками матрицы не меняет определителя матрицы, однако меняет порядок циклической группы, порождаемой этой матрицей.

В случае, когда необходимо повысить степень защиты изображения можно использовать две или три маскирующие матрицы.

На рис. 2.2 представлен результат маскирования изображения рассматриваемым методом, взятый из [16]:



а б

Рисунок 2.2 – Маскирование изображения (а – исходное изображение, б – маскированное изображение)

Преимуществом рассмотренного метода является использование логических, а не арифметических операций при обработке изображений, что обеспечивает высокую скорость преобразований. Программная, а также аппаратная реализации метода совместимы с корректирующими кодами.

Достоинством метода является огромная сложность нахождения необходимых для маскирования матриц **M**. Однако это может расцениваться и как недостаток – таких матриц к настоящему времени найдено мало и почти все они известны [16].

Quaternion Encryption Scheme (QES) – метод поблочного маскирования изображений основан на применении кватернионов – гиперкомплексных чисел 4-го ранга имеющих скалярную и векторную часть, которая является обычным вектором в трехмерном пространстве [20].

Для маскирования на основе кватерниона составляется матрица поворота ($\mathbf{B}_{\text{rot}}$). Метод маскирования и демаскирования данных на основе кватерниона представляется как

$$\mathbf{B}_{\text{rot}} = q \cdot \mathbf{B} \cdot q^{-1}$$
$$\mathbf{B} = q^{-1} \cdot \mathbf{B}_{\text{rot}} \cdot q,$$

где q – кватернион.

Можно вычислить матрицу поворота, чтобы получить кватернионы высокого порядка, которые рассматриваются как последующие ключи шифрования и, следовательно, повышают безопасность данных. Количество вычисленных кватернионов-ключей высшего порядка равно $3n$, где n – порядок.

На рис. 2.3 приведена схема реализации метода поблочного маскирования изображения в градации серого с использованием кватернионов.

Рисунок 2.3 – Реализация метода поблочного маскирования изображения в градации серого с использованием кватернионов

Для улучшения защищенности в рассматриваемом методе введена зависимость между блоками. Для этого используется метод шифрования Cipher Block Chaining (CBC) – используется поразрядное двоичное добавление данных матриц **B** и матриц $\mathbf{B}_{\text{rot}}$, которые были получены на предыдущих этапах. В первом шаге инициализации (на рисунке обозначен как (1)) используется случайная

матрица IM. Эта матрица такого же размера, как все матрицы **B**. В результате получается новая матрица $\mathbf{B}_{mod}$, имеющая такую же размерность, как матрицы **B**, но значения элементов данной матрицы рандомизированы.

Элементы матриц $\mathbf{B}_{rot}$ хранятся в виде чисел с плавающей точкой. В связи с этим при демаскировании возможно отличие восстановленных значений пикселей на ± 3.

На рис. 2.4 приведен пример зависимости блоков при маскировании:

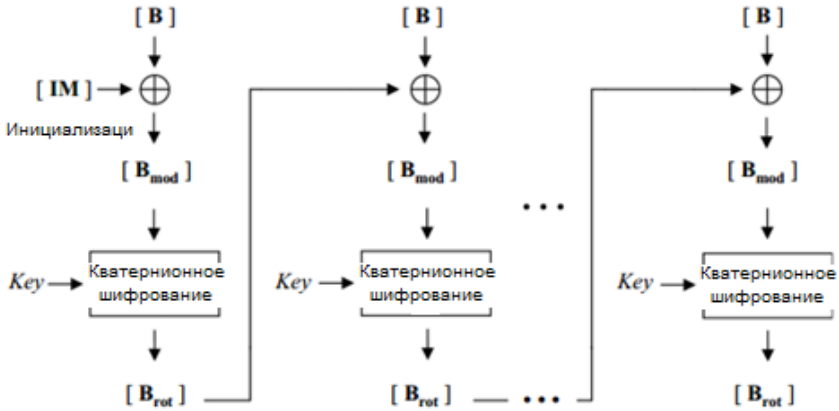


Рисунок. 2.4 – Пример зависимости блоков при маскировании

На рис. 2.5 приведен пример маскирования изображения рассматриваемым методом, взятый из работы [20]:

а б в г

Рисунок 2.5 – Пример маскирования методом QES (а – исходное изображение, б – маскированное изображение, в – восстановленное изображение, г – разностное изображение между (а) и (б))

Для получения более «шумоподобного» вида маскированного изображения процедуру QES необходимо выполнить итерационно несколько раз, что значительно увеличивает время преобразования.

2.2 Стип-метод как маскирующее преобразование изображений

Стрип-метод [21] изначально разрабатывался для помехоустойчивого кодирования изображений. Основу метода составляют матричные преобразования, обеспечивающие ослабление амплитуды импульсной помехи на передаваемом в канале изображении за счет равномерного её распределения по всему изображению. Для максимального ослабления амплитуды помехи на выходе канала используются, как правило, ортогональные матрицы Адамара с двумя возможными значениями (уровнями) элементов {1, -1} такие, что

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

где **H** – матрица Адамара, **I** – единичная матрица.

Из существующих двух модификаций стрип-метода для преобразования изображений – одностороннего и двухстороннего – основной интерес представляет вторая, обеспечивающая более полное «перемешивание» фрагментов изображения, результат которого может рассматриваться как его маскирование.

Под двусторонним стип-преобразованием изображения в общем случае понимается преобразование вида

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

где $\mathbf{A}_1$ и $\mathbf{A}_2$ – ортогональные матрицы размера *nxn*; исходное изображение в виде матрицы **P** размера *nxn*, **Z** – маскированное изображение размера *nxn*, полученное в результате преобразования.

Под обратным двусторонним стип-преобразованием понимается преобразование вида

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

Реально в двустороннем стип-преобразовании изображений используются матрицы $\mathbf{A}_1 = \mathbf{A}_2$ [21], поскольку это упрощает вычисления и экономит память. Таким образом, уравнение (2.1) имеет вид

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

где **A** – ортогональная матрица.

Поскольку матрица **A** является ортогональной, то $\mathbf{A}^{-1} = \mathbf{A}^{T}$. Следовательно, максимальные элементы у матриц **A** и $\mathbf{A}^{-1}$ одинаковы. Оптимальная матрица преобразования **A** должна быть ортогональной с минимально возможным по модулю элементом.

В отличие от представленного в работе [21] способа, результирующее изображение будет более «шумоподобным» при преобразованиях вида

$$\mathbf{Z} = \mathbf{APA}^{T},$$

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

которые предлагаются в настоящей работе.

Рассмотрим представление изображения при стрип-преобразовании. Размер матрицы **A** для одностороннего преобразования равен $n^2 \times n^2$, а для двустороннего $- n \times n$. Например, для изображения размером 300x300 пикселей при одностороннем преобразовании потребуется матрица **A** размера 90000x90000 и 300x300 для двухстороннего (двумерного) стрип-преобразования. Применение таких преобразований на практике потребует больших вычислительных ресурсов. При этом передаваемое изображение зачастую оказывается значительно больше исходного.

Для устранения этих проблем изображение можно разбить на одинаковые по размеру прямоугольные фрагменты, то есть произвольное исходное изображение представляется в виде блочной матрицы **P** так, чтобы она была квадратной (см. рис. 2.6).

В результате разбиения изображения на фрагменты получается блочно-квадратная матрица размера *n*x*n* блоков. Элементы блочной матрицы в общем случае являются прямоугольными и имеют размер XxY. Все фрагменты имеют одинаковый размер. В тех случаях, когда число пикселей в строке или столбце матрицы исходного изображения не делится нацело на *n*, соответственно справа или снизу изображения добавляются пиксели (столбцы или строки). Добавляемые пиксели не должны искажать или излишне контрастировать с основным изображением.

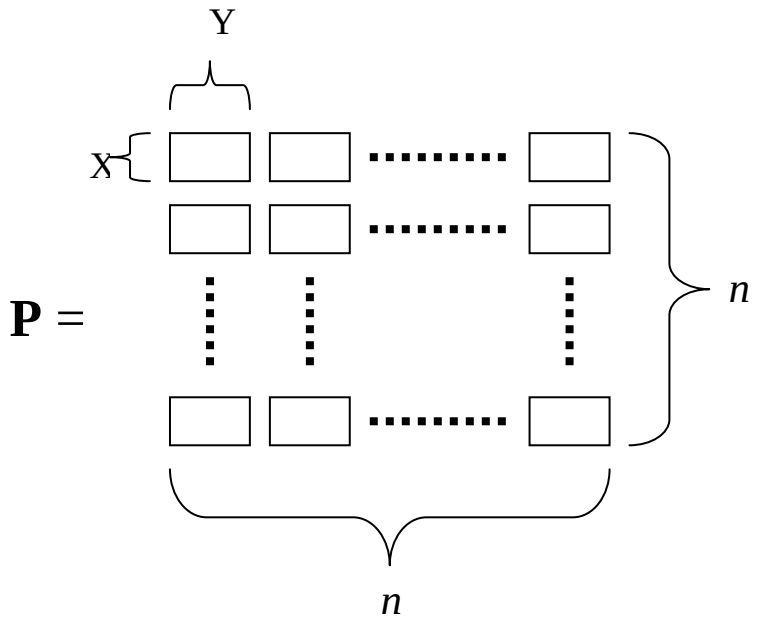


Рисунок 2.6 – Представление изображения в виде блочной матрицы **P**

При этом матрица преобразования **A** выбирается не блочной. В случае использования одностороннего преобразования блочная матрица преобразуется в вектор путем последовательного размещения строк исходной блочной матрицы друг за другом.

Например: пусть необходимо передать по коммуникационному каналу изображение размером 300x300 пикселей с использованием двустороннего преобразования. Матрица преобразования **A** имеет размер 8x8. Разобьем матрицу изображения **P** на фрагменты так, чтобы в блочном представлении матрица имела размер 8x8. Дополнив изображение пикселями до размера 304x304 разделим его на 64 одинаковых блока размером 8x8. Каждый блок имеет размер 38x38 пикселей. Будем выполнять преобразования над блочной матрицей **P** с помощью матрицы **A** размера 8x8. Умножение матриц производится по-блочно.

Для проведения с блочными матрицами преобразований, указанных в примере выше, используется несколько операций:

- сложение отдельных блоков (фрагментов) матриц – операция производится путем суммирования соответствующих элементов блоков, она аналогична сложению двух матриц одинакового размера;

– умножение фрагмента на число – операция производится путем умножения каждого пикселя фрагмента на число, при этом изменяется яркость фрагмента в целом. Операция аналогична умножению матрицы на число;
– умножение блочной матрицы на матрицу – производится как обычное перемножение матриц с учетом использования первых двух операций.

Деление изображения на фрагменты позволяет значительно сократить вычислительные затраты. Матрица преобразования **A** может быть выбрана гораздо меньшего размера, чем изображение. Размер блока (фрагмента) изображения выбирается исходя из ожидаемого размера импульсной помехи, то есть линейных размеров искажаемого участка изображения. Наилучшим вариантом является выбор размера фрагмента, равного размеру помехи. Это позволяет максимально равномерно распределить помеху по изображению на выходе системы. Выбранный размер фрагмента определяет размеры матрицы преобразования, так при перемножении матриц число строк и столбцов должно соответствовать правилам перемножения.

Двухстороннее (двумерное) стрип-преобразование изображений можно продемонстрировать приведенным на рис. 2.7 примером [21].

Рисунок 2.7 –Двухстороннее стрип-преобразование (а – исходное изображение, б – преобразованное изображение, в – восстановленное изображение с использованием стрип-преобразования, д –изображение после передачи в канале с помехой без использования стрип-преобразования)

Приведенный на рис. 2.7 пример стрип-преобразования реализован с использованием матрицы Адамара размера 4x4, а однократная помеха соответствует прямоугольнику пикселей размером 30x30.

Стрип-преобразование с использованием матрицы Адамара размера 12x12 и однократной помехой в канале как в предыдущем примере приведено на рис. 2.8 [21].

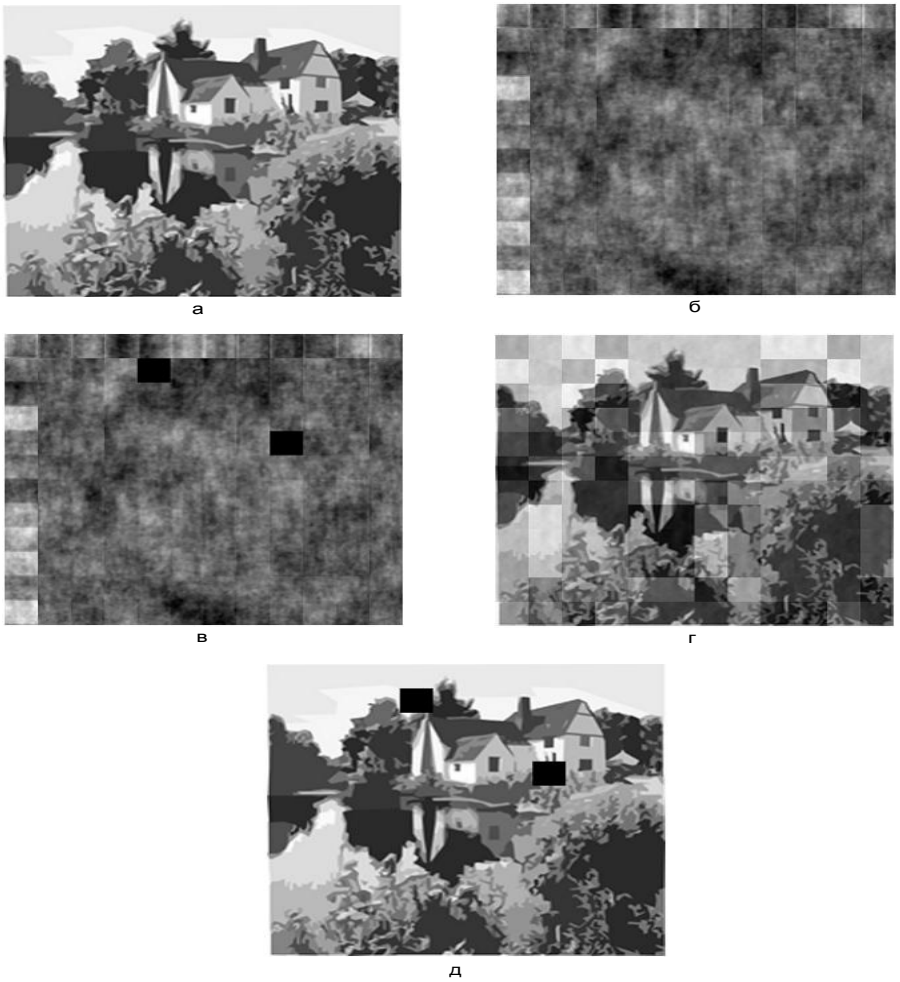


Рисунок 2.8 – Двухстороннее стрип-преобразование (а – исходное изображение, б – преобразованное изображение, в – преобразованное изображение с внесенной помехой, г – восстановленное изображение с использованием стрип-преобразования, д – изображение после передачи в канале с помехой без стрип-преобразования)

2.3 Современные стандартные разрешения и форматы видео кадров

Требования к качеству видеоинформации и ее разрешению постоянно возрастают – это является современной тенденцией, реализуемой как производителями матриц видеокамер, так и производителями дисплеев. Сегодня выделяют стандартные разрешения и форматы видео кадров, представленные в табл. 2.1, на которые ориентируются производители компьютерной и видеотехники.

Таблица 2.1 − Стандартные разрешения и форматы видео информации

Поколение	Тип	Разрешение (в пикселях)	Соотношение сторон	Формат	Кадр фактический (в пикселях)
SD – Standard Definition (стандартная чёткость)	SD	720x576 (704x576)	4:3	576i	720x288 (704x288)
				576p	720x576 (704x576)
	SD	640x480	4:3	480i	640x240
				480p	640x480
HD – High Definition (высокая чёткость)	HD	1280x720	16:9	720p	1280x720
	Full HD	1920x1080	16:9	1080i	1920x540
				1080p	1920x1080
UHD – Ultra High Definition (ультравысокая чёткость)	4K UHD	3840x2160	16:9	2160p	3840x2160
	8K UHD	7680x4320	16:9	4320p	7680x4320

Индексы i и p в форматах видео означают режимы: чересстрочный (interlaced) и прогрессивный (progressive). Прогрессивный режим является режимом более качественного представления видео, поскольку каждый его кадр имеет полный размер. В чересстрочном режиме кадр видео разбивается на два полукадра, строки в которых представлены через одну. Однако и в том и другом форматах общий объем информации для обработки одинаков.

Важным параметром видео, который не отображен в таблице, является частота кадров в секунду. Самые распространенные значения этого параметра –

25, 30, 50, 60, 100, 120 и др. В большой степени требования к производительности алгоритмов и методам маскирования предъявляются именно значением этого параметра.

На рис. 2.9 приведено сравнение размеров кадров из табл.2.1.

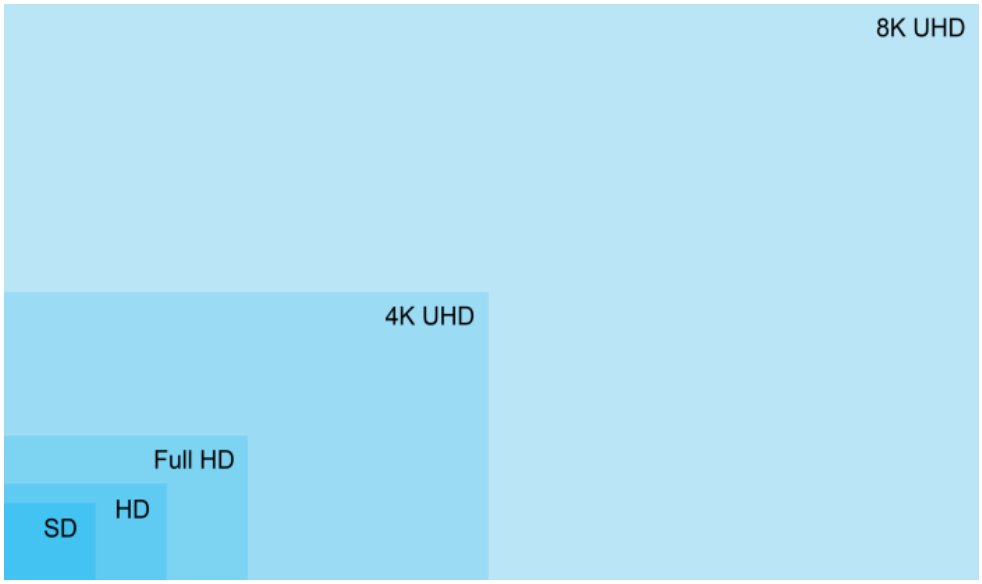


Рисунок 2.9 – Сравнение стандартных разрешений видео

Как видно, разница в разрешении (размерах) стандартных форматов видео очень существенна. Чем выше разрешение, частота кадров, тем больше требуется времени на их обработку, маскирование и демаскирование. Данное обстоятельство можно скорректировать использованием возможности распараллеливания вычислений. Для маскирования фото- и видеоизображения, с учетом распараллеливания процедуры ее выполнения, идеально подходит матричное маскирование. При этом желательно иметь широкий базис матриц, которые, с учетом необходимости обеспечения симметричности преобразований, должны быть ортогональными.

Еще больше требует расширения базиса ортогональных матриц появившаяся возможность выделения на изображении с видеоматрицы «окна интереса» (Quality box) произвольного размера.

Таким образом, можно кратко сформулировать требования к матрицам, используемым в матричном маскировании:

- они должны быть ортогональными для обеспечения симметричности процедур маскирования/демаскирования;
- порядки должны соответствовать возможно большему количеству чисел натурального ряда для того, чтобы можно было выбирать соответствующие матрицы (или кратно их использовать) для приведенных в табл. 2.1 разрешений, а также для реализаций маскирования «окон интереса»;
- для каждого порядка должно существовать более одной ортогональной матрицы для возможности ее смены в сеансах передачи видеопотока по коммуникационным каналам;
- количество возможных значений элементов (уровней) не должно превышать двух для оптимизации объема памяти для хранения матриц и упрощения вычислительных процедур.

Известно, что существование матриц Адамара ограничено порядками $4k$, где k – натуральные числа, что существенно ограничивает возможности их применения для изображений произвольного разрешения. Несмотря на использование в различных областях обработки информации множества других ортогональных матриц [35-63], для маскирования изображений и видеокадров преимущественными являются ортогональные матрицы с двумя значениями элементов, как и у матриц Адамара.

Указанным требованиям в полной мере отвечают квазиортогональные матрицы, являющиеся естественным обобщением ортогональных.

2.4 Квазиортогональные матрицы и метод маскирования

Квазиортогональная матрица – квадратная матрица **A** порядка n, у которой элементы каждого из столбцов приведены к единице максимумами модулей и удовлетворяет квадратичному условию

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

где **I** – единичная матрица; ω – вес матрицы.

Квазиортогональные матрицы весьма близки к ортогональным, которые получаются из **A** нормированием их столбцов, при этом максимальный по модулю элемент (m-норма) уменьшается до $m< 1$ для порядков $n> 1$. Класс квазиортогональных матриц более широк и включает в себя ортогональные матрицы.

Минимаксные квазиортогональные **M**-матрицы – матрицы, обладающие глобальным или локальным минимумом m-нормы на классе квазиортогональных матриц порядка n. При этом порядки таких матриц могут быть как четными, так и нечетными [64, 65].

В процессе поиска квазиортогональных матриц нечетных порядков, которые были бы близки по своим свойствам к матрицам Адамара, одним из первых был выделен класс малоуровневых **M**-матриц [64-73], которые получили название обобщенных матриц Адамара-Мерсенна или матриц Мерсенна. Эти матрицы впервые были обнаружены на порядках $n=2^k-1$, где k – натуральное число, принадлежащих последовательности чисел Мерсенна, в связи с чем и получили свое название. На сегодня сформулирована гипотеза о существовании таких матриц на всех нечетных порядках $4k-1$, имеющая четко сформулированное обоснование [73].

Уникальность малоуровневых матриц Мерсенна в том, что они допускают взаимно-однозначное преобразование в матрицы Адамара. Например, окаймлением матрицы Мерсенна (добавлением соответствующих верхней строки и левого столбца) можно получить матрицу Адамара порядка $4k$.

Следует отметить, что работы по исследованию квазиортогональных матриц локального максимума детерминанта, альтернативных матрицам Адамара, начали активно проводиться лишь с 2011 г. [66].

В работе [71] сформулировано определение квазиортогональных матриц Мерсенна, которое приведено ниже.

Определение. Квазиортогональными матрицами Мерсенна **M** называются двухуровневые матрицы порядков n=4k-1 со значениями элементов {1, -b}, где |b|< 1, удовлетворяющие квадратичному уравнению связи

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

где **I** – единичная матрица; $\omega(n) = \frac{(n+1)+(n-1)b^2}{2}$ - переменный вес, b=1/2 при n=3, в других случаях $b = \frac{q+\sqrt{4q}}{q-4}$, где $q = n + 1$.

В качестве примера на рис. 2.10 приведены портреты матриц Мерсенна порядков 7, 15, 31 и 255. Здесь белый квадрат соответствует элементу матрицы со значением 1, а черный — отрицательному элементу –b.

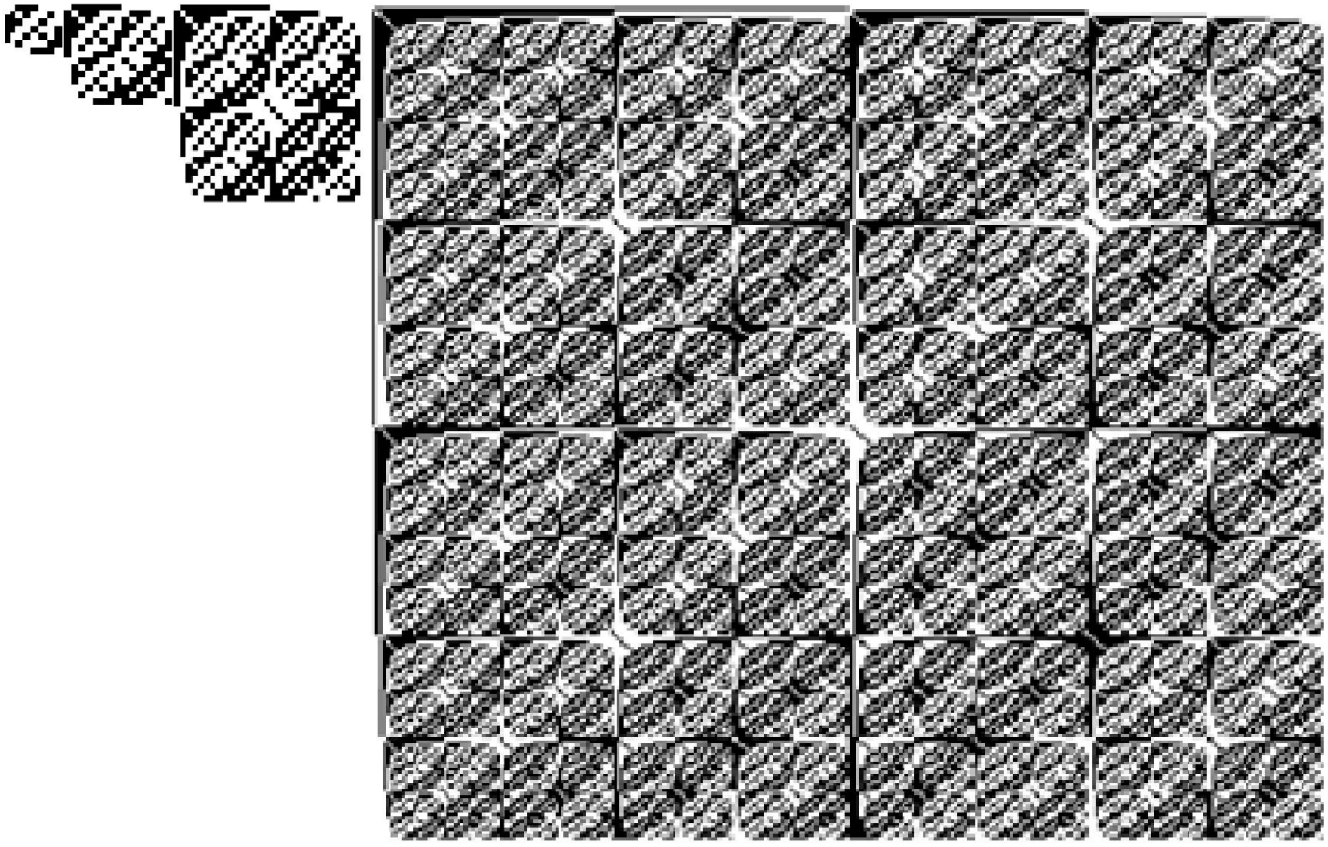


Рисунок 2.10 – Портреты матрицы Мерсенна порядков 7, 15, 31 и 255

Приведенные на рис.2.10 портреты матриц Мерсенна демонстрируют свойства геометрических фракталов – являются самоподобными структурами. Это облегчает их построение для различных порядков, сосредоточившись на

вычислении только значения элемента матрицы b и выборе начальной структуры матрицы.

Более полный каталог матриц Мерсенна можно найти на [http://mathscinet.ru].

За последнее время класс квазиортогональных матриц существенно расширился. В работе [72] предложена классификация, учитывающая, что возможны всего четыре варианта квазиортогональных матриц с малым числом уровней. В зависимости от остатка r деления порядка матрицы n на 4 выделяются:

при $r = 0$ – матрицы Адамара, включающие матрицы последовательности Сильвестра;

при $r = 1$ – матрицы Ферма (**F**), включающие матрицы порядков последовательности чисел Ферма;

при $r = 2$ – матрицы Эйлера (**E**), замещающие не существующие, согласно критерию Эйлера-Ферма, матрицы Белевича (**C**);

при $r = 3$ – матрицы Мерсенна (**M**), включающие матрицы порядков последовательности чисел Мерсенна.

Таким образом, в данном классе матриц последовательности Сильвестра и Мерсенна являются системообразующими.

Следует отдельно отметить, что маскирование призвано защитить информацию, передаваемую по открытым телекоммуникационным каналам, по открытым сетям, являющимся основой распределенных видеосистем. С этой точки зрения важным является то, что в двухуровневых матрицах Мерсенна элемент $-b$ является иррациональным числом, и, если принять элемент b в качестве «ключа», то сложность его подбора методом перебора будет равна 2^N, где N – длина b в битах. Расчет, представленный в работе [96], показывает, что количество операций для подбора самой матрицы Мерсенна порядка n будет соизмеримо с $2^N n!/2$.

Таким образом, метод маскирования цифровых изображений, с учетом приведенных выше основной схемы двустороннего матричного преобразования и

представления изображений, с использованием матриц Мерсенна можно представить как

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

где **M** – квазиортогональная матрица Мерсенна.

Демаскирование является симметричным обратным преобразованием.

В диссертационной работе использованы исключительно матрицы Мерсенна. Однако, как следует из классификации квазиортогональных матриц [72, 73], они составляют базис матриц различных порядков, значительно превышающий по количеству базис известных матриц Адамара, и обеспечивают большую гибкость в вопросе адаптации матриц преобразования к возможным размерам изображений.

2.5 Выводы

Модификация стрип-метода двустороннего преобразования изображений в совокупности с использованием двухуровневых квазиортогональных матриц позволяет реализовать преобразование изображений к «шумоподобному» виду.

Класс квазиортогональных матриц значительно шире класса ортогональных матриц Адамара и вместе они составляют ортогональный базис малоуровневых (в основном двухуровневых) матриц, существующих на порядках, соответствующих практически всему ряду натуральных чисел. Это облегчает выбор для различных размеров изображений наиболее подходящих матриц из такого базиса.

Метод двустороннего матричного маскирования на основе модифицированного стрип-метода в совокупности с использованием базиса уникальных квазиортогональных матриц имеет преимущества по сравнению с другими известными, в том числе матричными, методами.

3 ПОКАДРОВОЕ МАСКИРОВАНИЕ ИЗОБРАЖЕНИЙ

В данном разделе рассматривается и описывается алгоритм маскирования фото и видеоинформации с использованием уникальных квазиортогональных матриц Мерсенна.

Предлагается алгоритм приведения в соответствие разрешения маскируемого изображения и порядка маскирующей матрицы. Приводятся схемы прямых и обратных преобразований. Классифицируются шумы в цифровой обработке изображений и анализ, позволяющий отнести маскированные цифровые изображения по гистограмме к одному из них.

Оценивается качество восстановленного изображения при отсутствии и при наличии помех в коммуникационном канале с использованием объективных метрик PSNR, MSE, SSIM, MSSIM.

3.1 Алгоритм маскирования изображений

Процедура маскирования в распределенных видеосистемах является симметричной: на передающей стороне выполняется прямое преобразование, на приемной – обратное, симметричное прямому преобразованию. Под прямым преобразованием будет пониматься процедура маскирования, а под обратным – демаскирования.

Процедура маскирования в целом состоит из нескольких этапов [81-83]:

- выбор маскирующей матрицы;
- приведение в соответствие разрешения маскируемого изображения и порядка маскирующей матрицы;
- двустороннее матричное преобразование выбранного изображения с заданными параметрами;
- хранение и передача маскированного изображения;

– восстановление (демаскирование) маскированного изображения.

Выбор маскирующей матрицы. На этом этапе необходимо выбрать/сгенерировать уникальную квазиортогональную матрицу Мерсенна. Следует учитывать, что чем меньше порядок используемой для маскирования матрицы, тем меньше времени потребуется на процедуру маскирования. Однако существует вероятность распознавания маскируемого изображения. В другом случае: чем больше порядок используемой для маскирования матрицы, тем больше времени потребуется на процедуру маскирования, но исходное изображение более «качественно» преобразуется в шум.

Приведение в соответствие разрешения маскируемого изображения и порядка маскирующей матрицы. Главное условие на данном этапе – кратность высоты и ширины маскируемого изображения порядку матрицы, т.е должны выполнятся равенства

$$W_i \bmod n = 0, \tag{3.4}$$

$$H_i \bmod n = 0, \tag{3.5}$$

где n – порядок маскирующей матрицы, W_I - ширина маскируемого изображения в пикселях, H_I - высота маскируемого изображения в пикселях.

В тех случаях, когда условия (3.4) и (3.5) не выполняются, существует ряд решений:

– подобрать такую маскирующую матрицу, порядок которой будет удовлетворять условиям (3.4) и (3.5), т.е. сгенерировать новую маскирующую матрицу;
– дополнить маскируемое изображение пустыми или содержащими среднее значение строками/столбцами, чтобы оно удовлетворяло условиям равенств (3.4) и (3.5);
– обрезать (уменьшить количество) у маскируемого изображения количество строк/столбцов, чтобы оно удовлетворяло условиям (3.4) и (3.5).

Самым объективным является первый и второй из описанных подходов, так как не происходит умышленного обрезания областей изображения, которые могут содержать критически важные сведения.

Двустороннее матричное преобразование изображения с заданными параметрами. Маскирование и демаскирование может производиться над двумя типами изображений, где значения пикселей представлены в виде числа и фиксированной [109, 110] или плавающей точкой [111, 112]. При использовании представления пикселей в виде числа с фиксированной точкой перед процедурой маскирования выполняется перевод значений элементов маскирующей матрицы из вещественных чисел (с плавающей точкой) в числа с фиксированной точкой.

Маскирование изображения включает в себя следующие действия:

– из всех значений матрицы исходного изображения вычитается 128 для сдвига начала отсчёта в область нуля:

$$\mathbf{K} = \mathbf{P} - 128,$$

где **P** – исходное изображение, **K** – изображение, полученное в ходе вычитания;

– перемножение исходного изображения с маскирующей матрицей, в виде $\mathbf{Z} = \mathbf{M}\,\mathbf{K}\,\mathbf{M}^{\mathrm{T}}$, где **Z** – маскированное изображение, **M** – матрица Мерсенна;

– квантование. Ввиду специфики применяемых квазиортогональных матриц матрица квантования не применятся, а происходит простейшая операция сдвига вправо при представлении пикселей в виде числа с фиксированной точкой, или операция деления при представлении пикселей в виде числа с плавающей точкой на некоторый коэффициент q:

$$\mathbf{Z_{qfix}} = \mathbf{Z} \gg q$$

$$\mathbf{Z_{qfloat}} = \mathbf{Z}/q,$$

где $\mathbf{Z_{qfix}}$ – маскированное изображение с представлением пикселей в виде числа с фиксированной точкой после квантования, $\mathbf{Z_{qfloat}}$ – маскированное изображение с представлением пикселей в виде числа с плавающей точкой после квантования, q – коэффициент квантования.

В FPGA, например, операция сдвига не требует времени на выполнение (во время перемещения данных по шинам можно просто «терять» младшие разряды), что дает существенный выигрыш в обработке больших (4K, 8K) видеоизображений;

– перевод значений пикселей в байтовые последовательности для дальнейшей передачи или хранения маскированного изображения. В случае использования чисел с плавающей точкой производится преобразование из типа float (32 бита) в 4 числа типа байт. При использовании представления пикселей в виде числа с фиксированной точкой производится преобразование из типа long long (64 бита) в 8 чисел типа байт. Тем самым пропорционально увеличивается размер маскированного изображения с WxH до 4WxH или 8WxH, где W – ширина маскированного изображения, а H – высота.

Хранение и передача маскированного изображения. Для хранения (записи на носитель) и передачи маскированных изображений и последовательностей кадров предлагается использовать три формата: PNG, zmi (Zip Masked Image) или RAW (формат без сжатия). При представлении маскированного изображения в формате PNG осуществляется информационное сжатие без потерь, а кроме этого, упрощается задача воспроизведения полученной матрицы в виде плоского изображения, поскольку формат PNG широко используется распространенными пользовательскими пакетами программ. Это позволяет покадрово производить анализ маскированной видеопоследовательности.

При представлении маскированного изображения в формате zmi (Zip Masked Image) сжатие маскированного изображения осуществляется алгоритмом Deflate [84] (он же является основой PNG) с использованием библиотеки zlib [87], являющейся комбинацией алгоритмов сжатия без потерь LZ77 [85] и алгоритма Хаффмана [86]. Помимо этого, в заголовок файла записываются данные для последующего демаскирования – разрешение исходного изображения.

Восстановление (демаскирование) маскированного изображения. Обратное преобразование (демаскирование) выполняется в следующем порядке:

- загрузка сохраненного (или прием переданного) маскированного изображения;
- восстановление значений пикселей при их представлении в виде чисел с фиксированной или плавающей точкой;
- квантование: операция сдвига влево при представлении пикселей в виде числа с фиксированной точкой; операция умножения при представлении пикселей в виде числа с плавающей точкой на некоторый коэффициент q:

$$\mathbf{Z} = \mathbf{Z_{qfix}} \ll q$$

$$\mathbf{Z} = \mathbf{Z_{qfloat}} * q$$

- обратное симметричное преобразование в виде $\mathbf{K} = \mathbf{M}^{\mathrm{T}}\mathbf{Z}\,\mathbf{M}$;
- ко всем значениям матрицы восстанавливаемого изображения прибавляется 128 (**P** = **K** + 128);
- восстановление исходного размера изображения;
- сохранение/отображение восстановленного (исходного) изображения.

3.2 Классификация шумов на изображениях

Маскирование цифровых фото и видеоизображений подразумевает, что исходное изображение разрушается до вида, который воспринимается визуально как шум. Обычно наличие шума на изображении говорит о наличии катастрофических изменений в процессе передачи изображения по каналам связи, что приводит к частичному или полному «разрушению» исходного изображения. Но, поскольку процедура маскирования предназначена для осознанного разрушения изображения до шума, то становится необходимым классифицировать полученное маскированное изображение в процессе преобразования.

Само по себе изображение является двумерной функцией $f(x, y)$, где x и y – плоские координаты, а амплитуда f в любой паре данных координат называется градацией серого или интенсивностью изображения в этой точке. Цифровые изображения состоят из конечного числа элементов, называемых пикселями.

Снимки, сделанные с помощью цифровой камеры, могут содержать шум из-за случайных вариаций параметров элементов в матрице датчиков. Шум представляет собой нежелательные явления, ухудшающие качество изображения. Наличие шума в коммуникационных сетях может иметь катастрофические последствия для передаваемых данных.

В обработке цифровых изображений различают следующие типы шумов [78,80].

Импульсный шум, при котором на изображении появляются изолированные точки, значения амплитуды f в которых существенным образом отличаются от значений окружающих их пикселей (точек). Примером такого типа шума является шум «соль и перец». Импульсный шум описывается как

$$g(x, y) = (1 - p) * f(x, y) + p * i(x, y), \qquad (3.1)$$

где $g(x, y)$ – зашумленное изображение, $i(x, y)$ – модель импульсного шума, p – бинарный параметр (0 или 1).

Аддитивный шум, получаемый при суммировании элементов исходного изображения с аддитивной помехой, не зависящий от сигнала шум. Он имеет гауссовское (или другое) распределение функции плотности вероятности и описывается как

$$g(x, y) = f(x, y) + \mu(x, y), \qquad (3.2)$$

где $g(x, y)$ – зашумленное изображение, $f(x, y)$ – исходное изображение, $\mu(x, y)$ – аддитивный шум.

Мультипликативный шум, наблюдаемый на изображениях, полученных при помощи ультразвука, радиолокационных изображениях и на фотопленочных изображениях при ее зернистости. Мультипликативный шум описывается как

$$g(x, y) = f(x, y) * \mu(x, y). \qquad (3.3)$$

Шум квантования, зависящий от сигнала и характеризуемый выбранным шагом квантования. При наличии шума квантования на исходном изображении возможно появление нежелательных артефактов, таких как ложные контуры вокруг объектов или устранение низкоконтрастных деталей на изображении;

Спекл-шум, зависящий от сигнала изображения. В случаях, когда изображение имеет низкое разрешения спекл-шум для такого изображения является мультипликативным шумом. Основной пример возникновения спекл-шума – получение цифровых изображений с помощью оптического сканера.

Наиболее распространенными типами шумов в и цифровой обработке изображений являются импульсный и аддитивный шумы.

Для анализа, типов шумов на изображении часто используется метод гистограмм [80]. Гистограмма цифрового изображения – некоторая дискретная функция $H(K) = N_K$, которая характеризует распределение пикселей изображения по уровням яркости (для изображения в градации серого $0 \leq K \leq 255$) где K – яркость, а N_K – число пикселей в изображении, с яркостью K.

Таким образом, при наличии импульсного шума на изображении на гистограмме этого изображения будет присутствовать несколько или один импульс в граничных пределах данной гистограммы. То есть в области значений яркости 0 или 255 (но не обязательно). А при наличии аддитивного шума на изображении на гистограмме этого изображения яркости пикселей будут иметь равномерное распределение.

Данные определения типов шумов будут использоваться при анализе, относящем маскированное изображение к одному из приведенных типов шумов.

3.3 Анализ маскированных изображений

Для исследования процедуры маскирования/демаскирования была собрана база изображений из открытых источников, предоставляющих тестовые наборы изображений для их обработки [88-93], включающая в себя более 1000 цифровых

изображений различных разрешений. Для демонстрации характеристик процедуры маскирования был подобран ряд наиболее показательных тестовых изображений, приведенных на рис. 3.1:

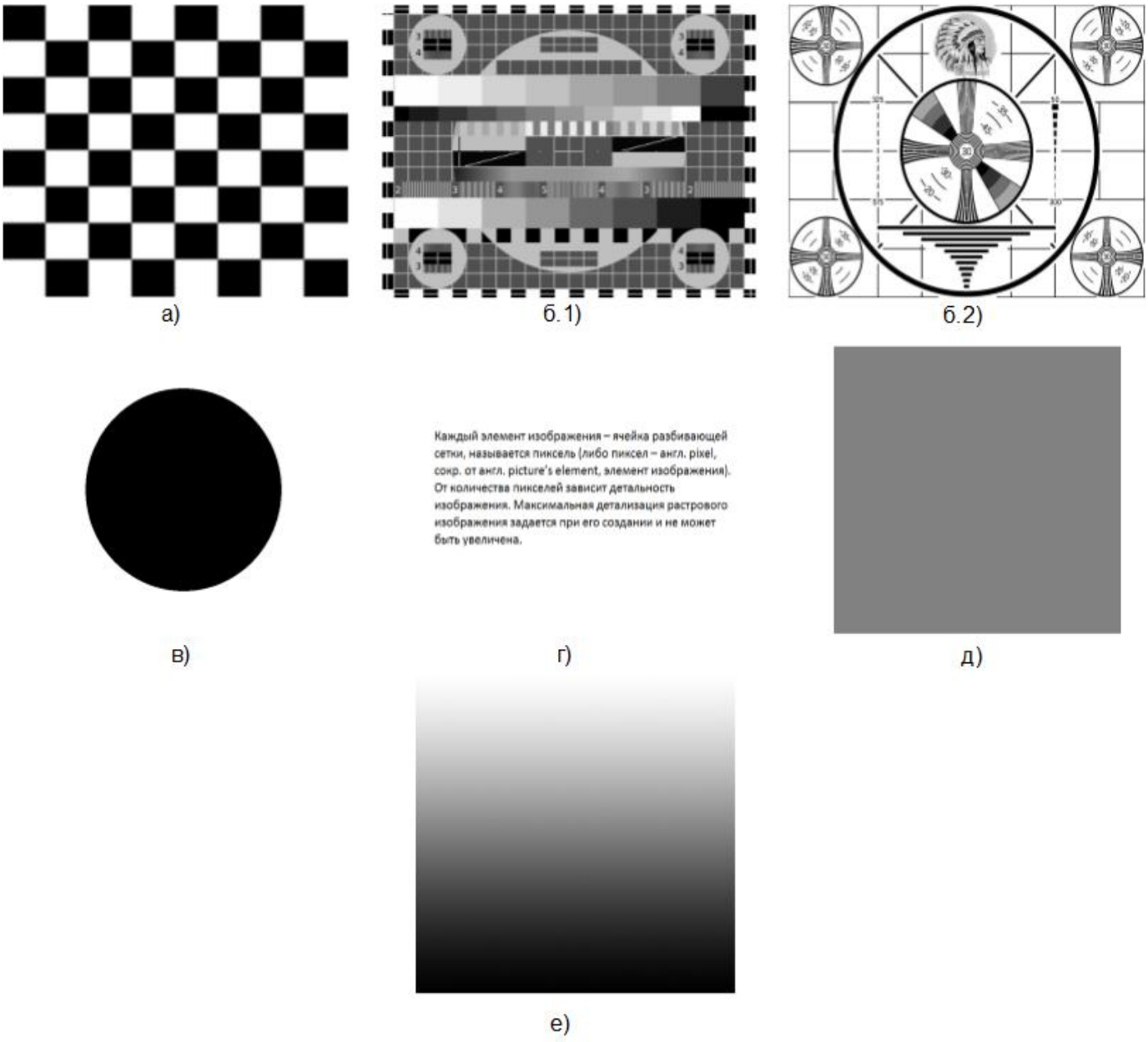


Рисунок 3.1 – Набор тестовых изображений

Набор тестовых изображений включает в себя:

- изображение «Шахматная доска»;
- два изображения телевизионной испытательной таблицы (ТИТ);
- изображение черного круга на белом фоне;

– изображение текста на белом фоне;
– изображение, содержащее только серый цвет;
– изображение, содержащие градиент в градации серого.

Для демонстрации маскирования/демаскирования изображений была использована матрица Мерсенна порядка 15 ($\mathbf{M}_{15}$). На рис. 3.2 представлено маскированное изображение «Шахматная доска» с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой.

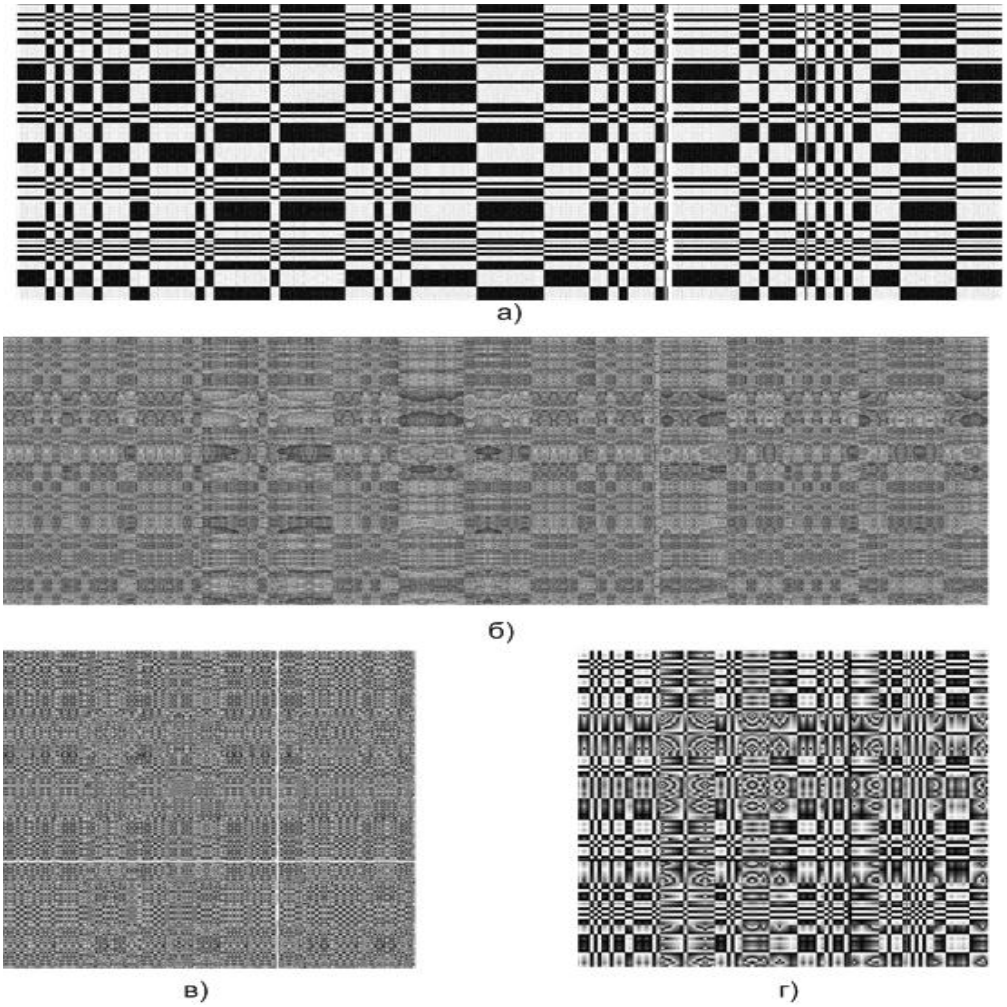


Рисунок 3.2 – Маскированное изображение «Шахматная доска» (а, в – фиксированная точка; б, г – плавающая точка)

При представлении значений пикселей как чисел с фиксированной точкой осуществлялся сдвиг вправо на 20, при представлении значений пикселей как чисел с плавающей точкой осуществлялось деление на 8192 на этапе квантования. Также представлены их визуализации (в, г) – воспроизводимые изображения,

если числовое представление пикселей маскированного изображения не переводится в байты.

На рис. 3.3 представлены демаскированные (восстановленные) изображения:

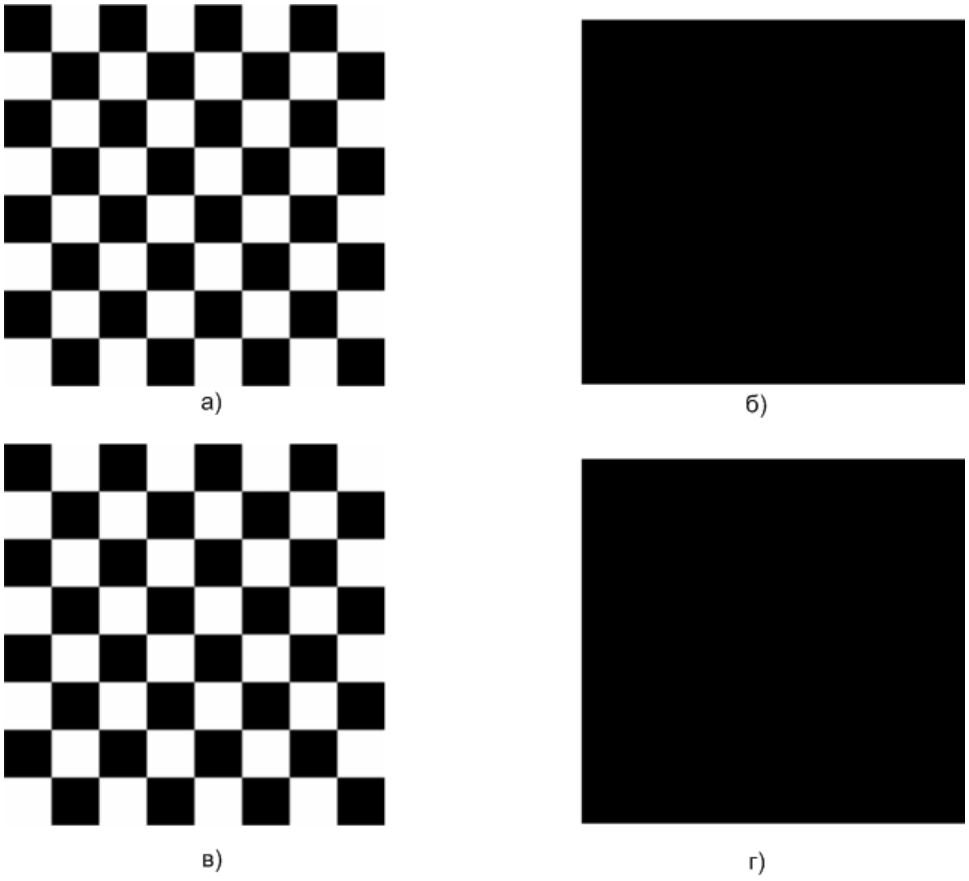


Рисунок 3.3 − Демаскированные (восстановленные) изображения (а, б – преобразования выполнялись с фиксированной точкой, где а) – восстановленное изображение, б) – разность исходного и восстановленного изображения; в, г – преобразования выполнялись с плавающей точкой, где в) – восстановленное изображение, а г) – разность исходного и восстановленного изображения)

При анализе маскированных изображений следует учитывать, что в процедуре маскирования на сохраняемое или передаваемое изображение накладывается шум квантования. На рис. 3.4 представлены гистограммы маскированных изображений.

а)

б)

Рисунок.3.4 − Гистограмма маскированного изображения (а – преобразования с фиксированной точкой; б – преобразования с плавающей точкой)

Анализ гистограмм на рис.3.4, показывает, что в случае а) при представлении чисел с фиксированной точкой и после наложения шума квантования результат маскирования представляет собой импульсный шум, в случае б) при представлении чисел с плавающей точкой получается шум, подобный аддитивному.

В последующих примерах буквенное обозначение маскированных изображений остается таким же, как и в приведенном на рис. 3.4.

На рис.3.5 представлено маскированное изображение первой из телевизионных испытательных таблиц, а также их визуализации (в, г).

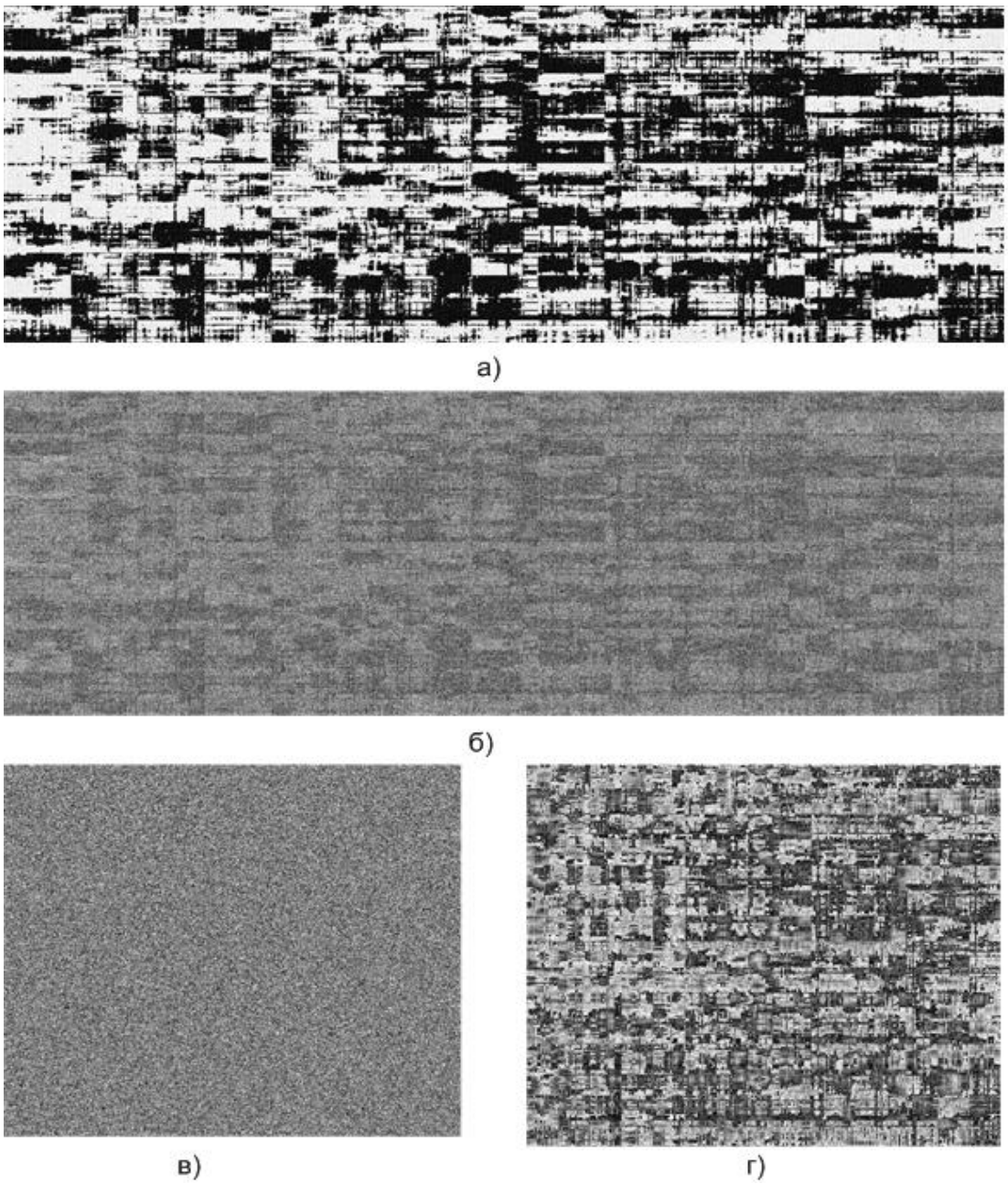


Рисунок 3.5 – Маскированное изображение телевизионной испытательной таблицы (а, в – фиксированная точка; б, г – плавающая точка)

На рис. 3.6 и 3.7 представлены демаскированные (восстановленные) изображения и гистограммы маскированных изображений соответственно.

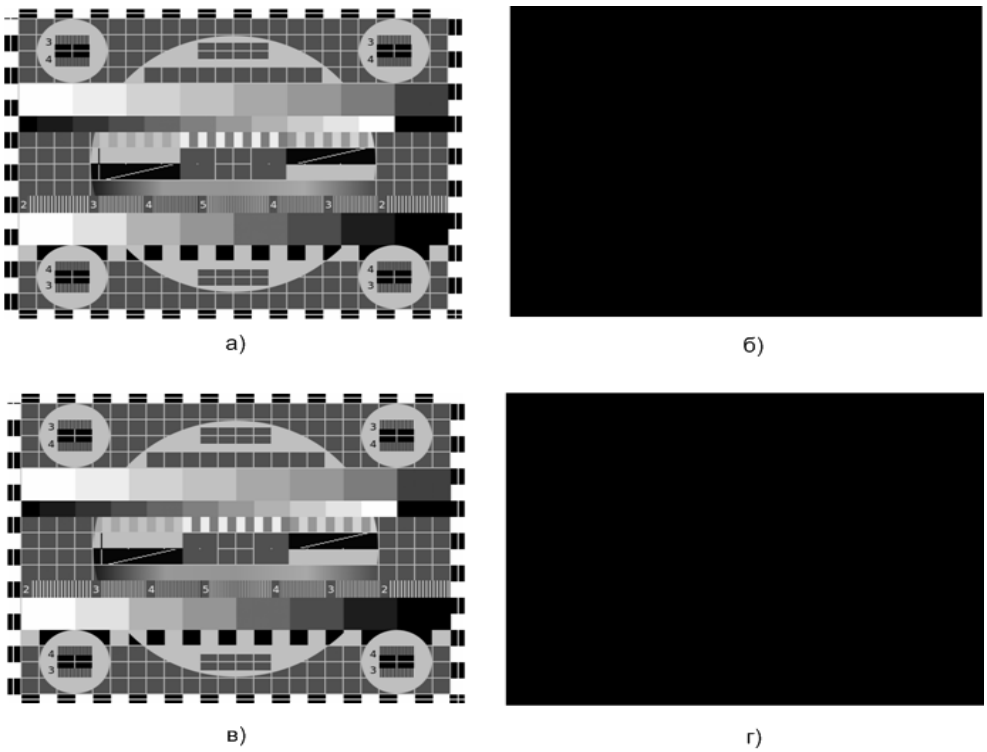


Рисунок 3.6 − Демаскированные (восстановленные) изображения (а, в) и их разностное представление с исходным изображением

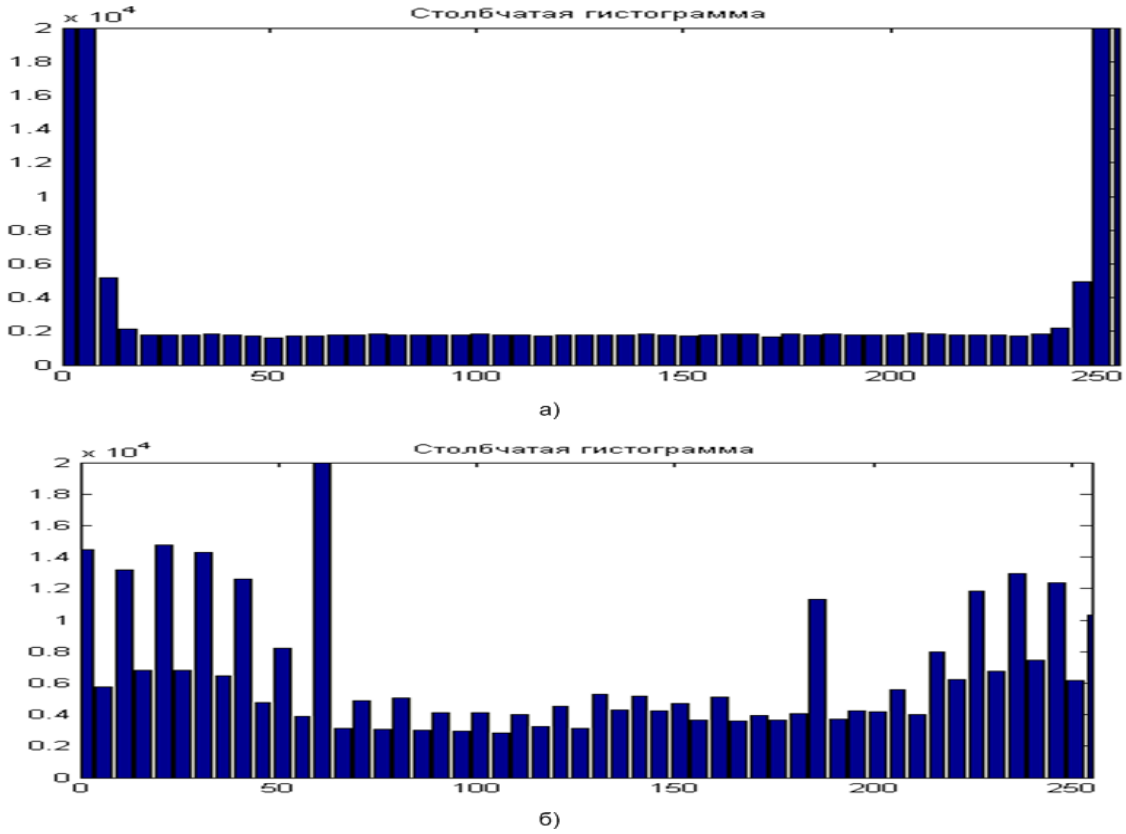


Рисунок 3.7 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

Анализ гистограммы на рис. 3.7, показывает, что в случае (а) при представлении чисел с фиксированной точкой получается импульсный шум. В то же время в случае (б), при представлении чисел с плавающей точкой, получается шум, подобный аддитивному, но с импульсным скачком по яркости.

На рис. 3.8 представлено маскированное изображение второй из телевизионных испытательных таблиц (с изображением головы индейца) с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой, а также их визуализации (в, г).

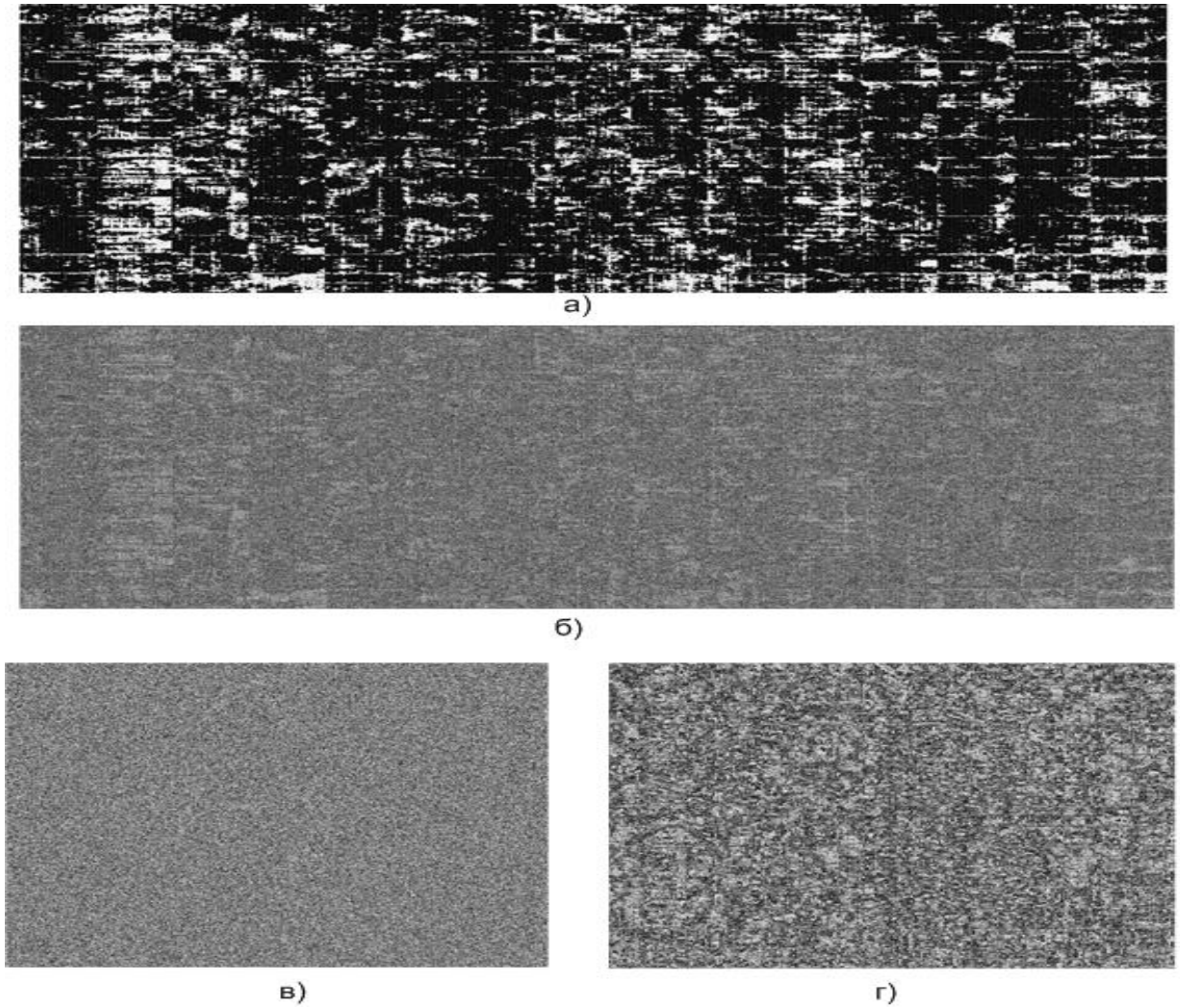


Рисунок 3.8 – Маскированное изображение телевизионной испытательной таблицы (а,в – фиксированная точка; б,г – плавающая точка)

На рис. 3.9 представлены демаскированные (восстановленные) изображения, из которого видно (б), что при использовании чисел с фиксированной точкой произошла потеря данных. Это связано с этапом

квантования, заключающимся в сдвиге коэффициентов маскированного изображения на 20 бит вправо и приведении числа с фиксированной точкой, после восстановления маскированного изображения, к целочисленному значению.

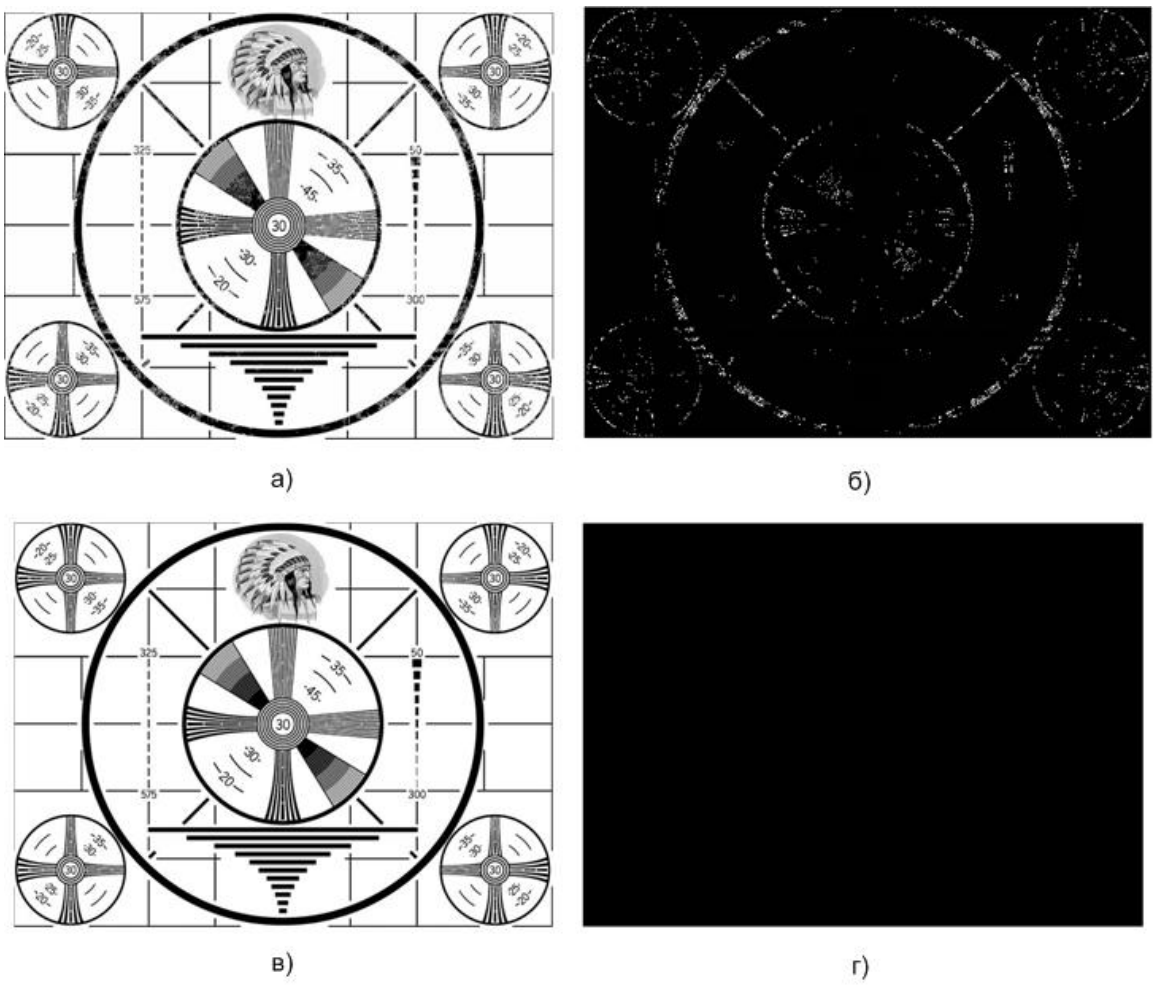


Рисунок 3.9 − Демаскированные (восстановленные) изображения (а,в) и их разностное представление с исходным изображением (б,г)

Если коэффициент квантования при восстановлении уменьшить на единицу (q=19), то потерь удастся избежать и изменится вид маскированного изображения. Восстановленное изображение тогда будет «тусклым». Гистограммы маскированного изображения представлены на рис. 3.10.

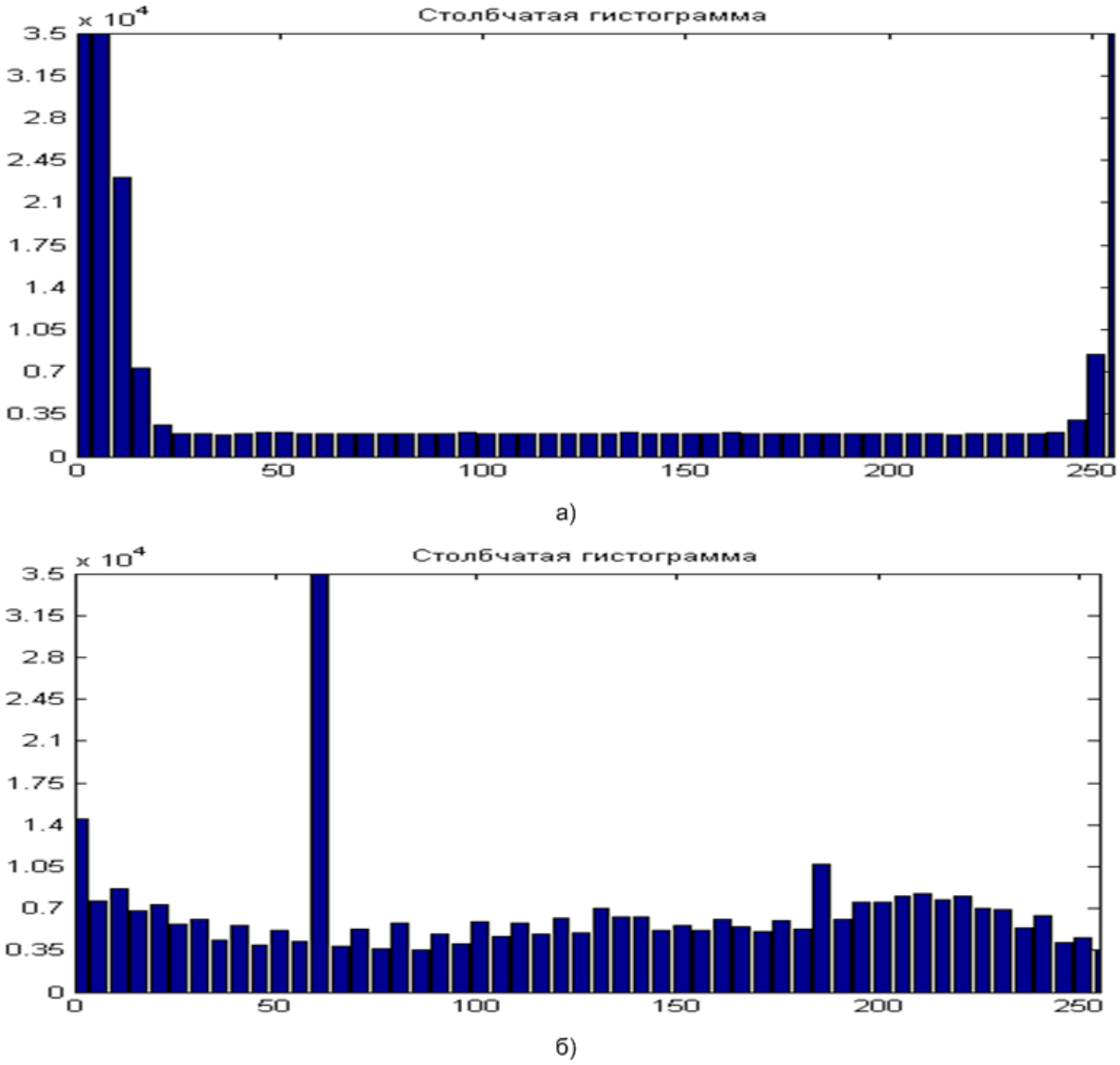


Рисунок 3.10 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

По гистограммам на рис. 3.10 можно сделать вывод, что при представлении пикселей в виде чисел с фиксированной и плавающей точкой получается импульсный тип шума.

На рис. 3.11 представлено маскированное изображение черного круга на белом фоне с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой, а также их визуализации (в, г).

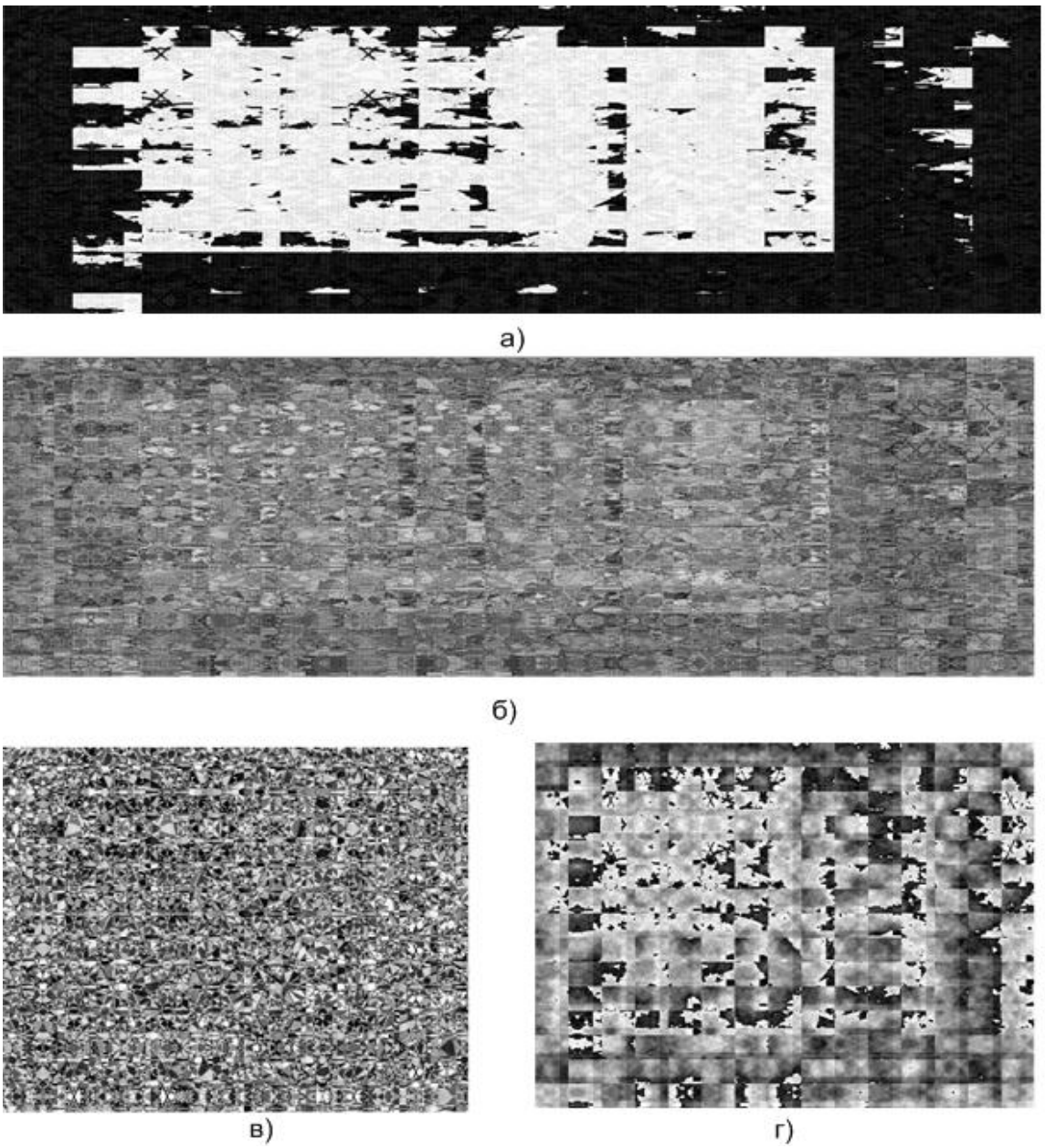


Рисунок 3.11 – Маскированное изображение черного круга на белом фоне (а, в – фиксированная точка; б, г – плавающая точка)

На рис.3.12 представлены демаскированные (восстановленные) изображения. Гистограммы маскированного изображения представлены на рис. 3.13.

По гистограммам на рис. 3.13, можно сказать, что при представлении пикселей в виде чисел с фиксированной и плавающей точкой результирующее изображение представляет собой импульсный шум.

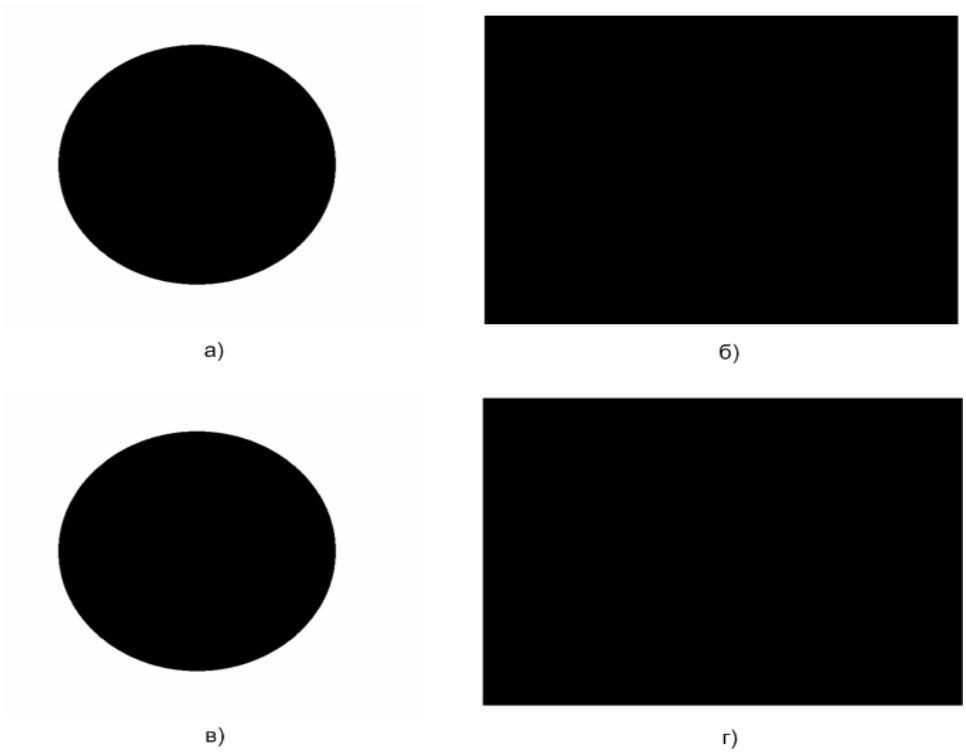


Рисунок 3.12 − Демаскированные (восстановленные) изображения (а,в) и их разностное представление с исходным изображением (б,г)

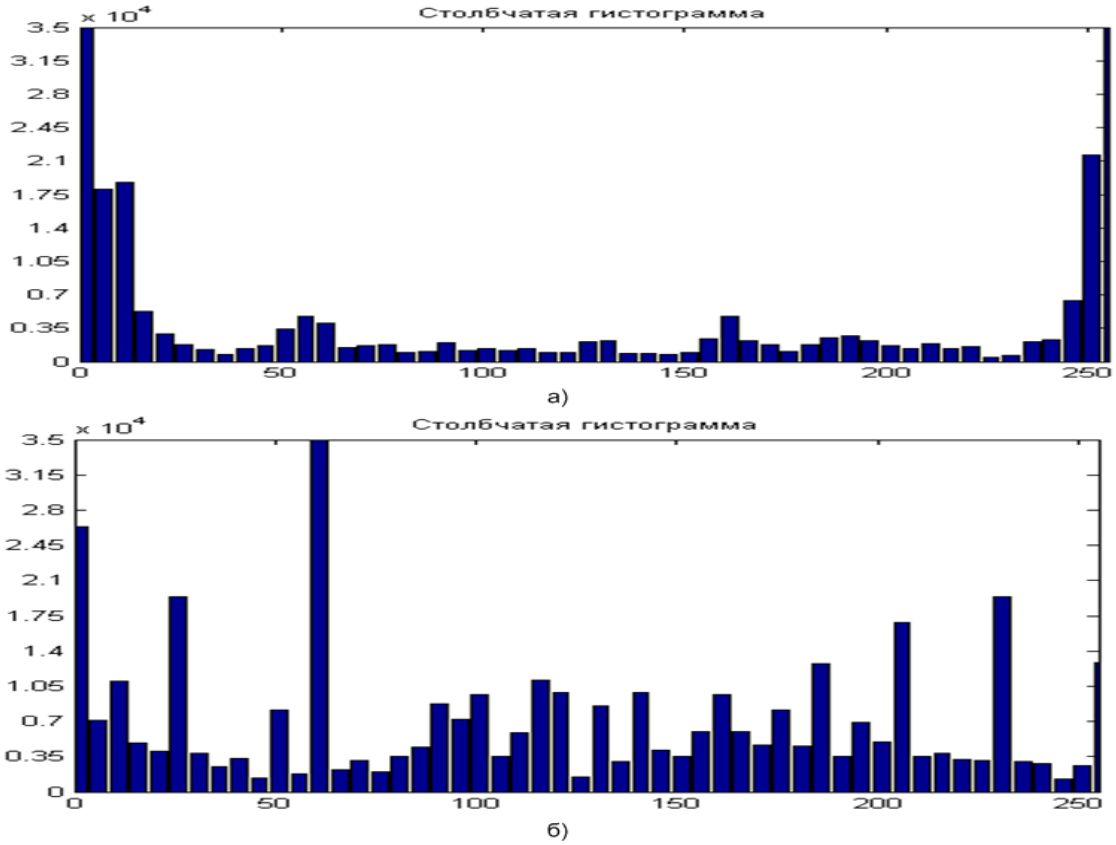


Рисунок 3.13 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

На рис. 3.14 представлено маскированное изображение градиента в градации серого с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой, а также их визуализации (в, г).

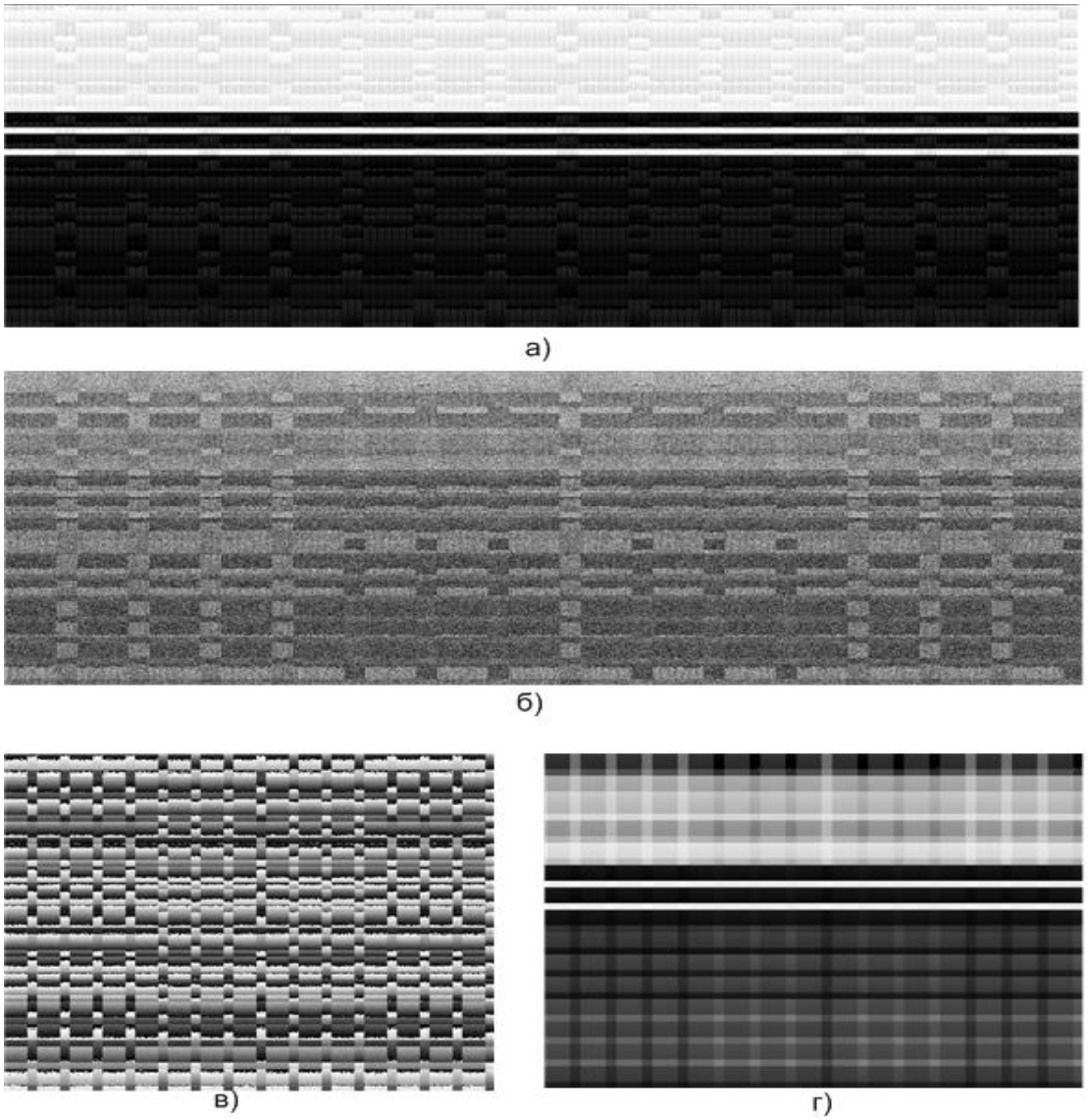


Рисунок 3.14 – Маскированное изображение градиента в градации серого (а,в – фиксированная точка; б,г – плавающая точка)

На рис.3.15 представлены демаскированные (восстановленные) изображения. Гистограммы маскированного изображения представлены на рисунке 3.16.

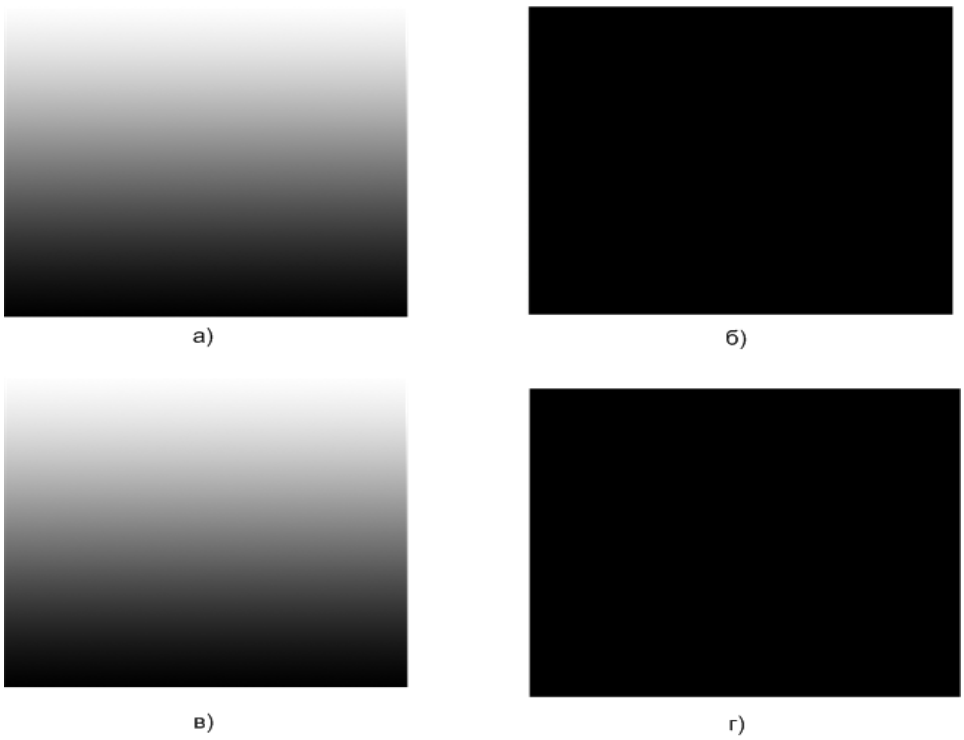


Рисунок 3.15 − Демаскированные (восстановленные) изображения (а,в) и их разностное представление с исходным изображением (б,г)

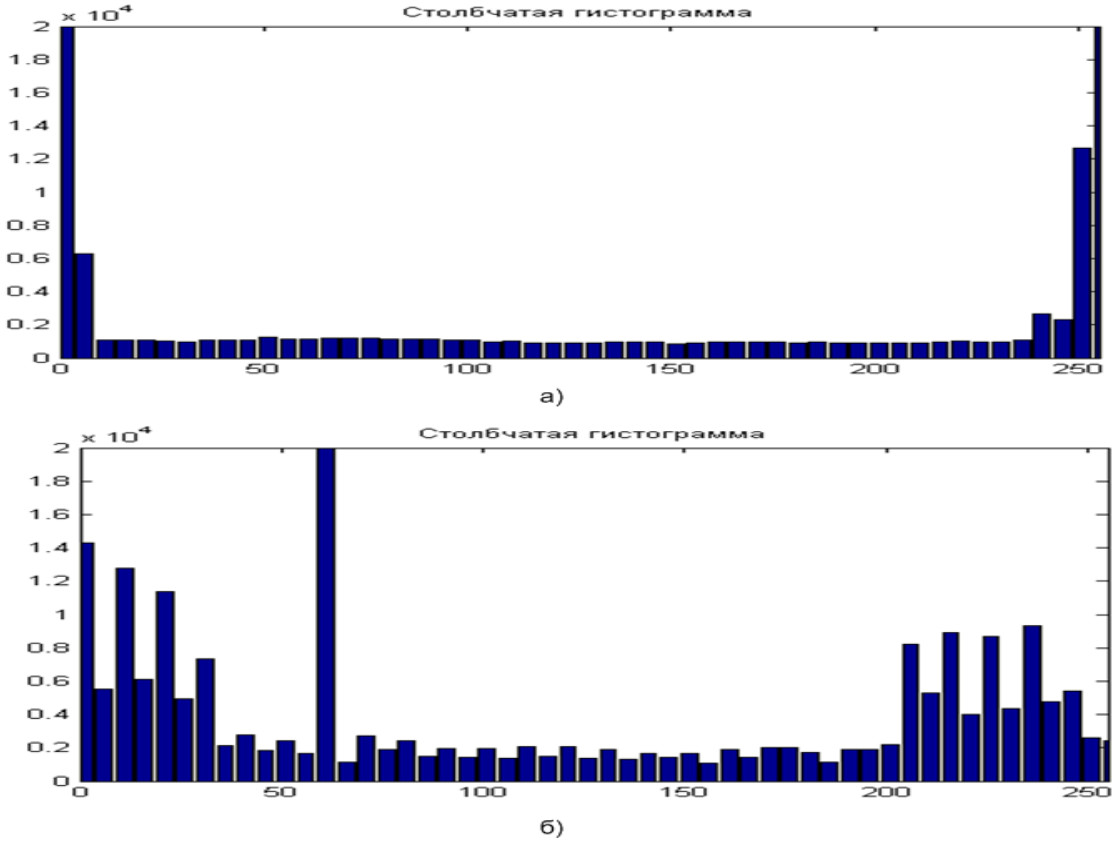


Рисунок 3.16 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

По гистограммам на рис. 3.16, можно сказать, что при представлении пикселей в виде чисел с фиксированной и плавающей точкой получается импульсный шум.

На рис. 3.17 представлено маскированное изображение, содержащее только серый цвет с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой, а также их визуализации (в, г).

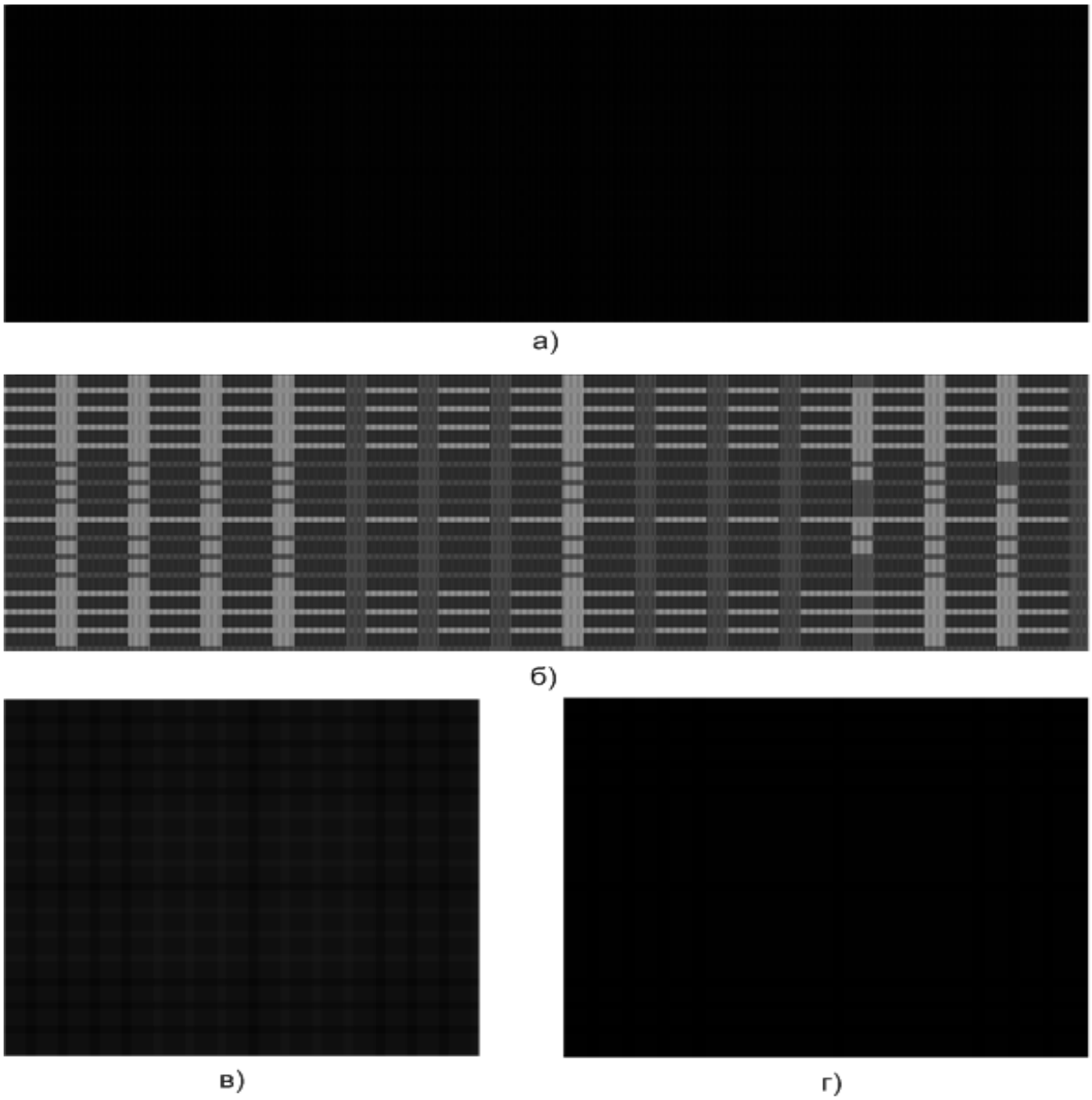


Рисунок 3.17 – Маскированное изображение содержащее только серый цвет (а,в – фиксированная точка; б,г – плавающая точка)

На рис. 3.18 представлены демаскированные (восстановленные) изображения.

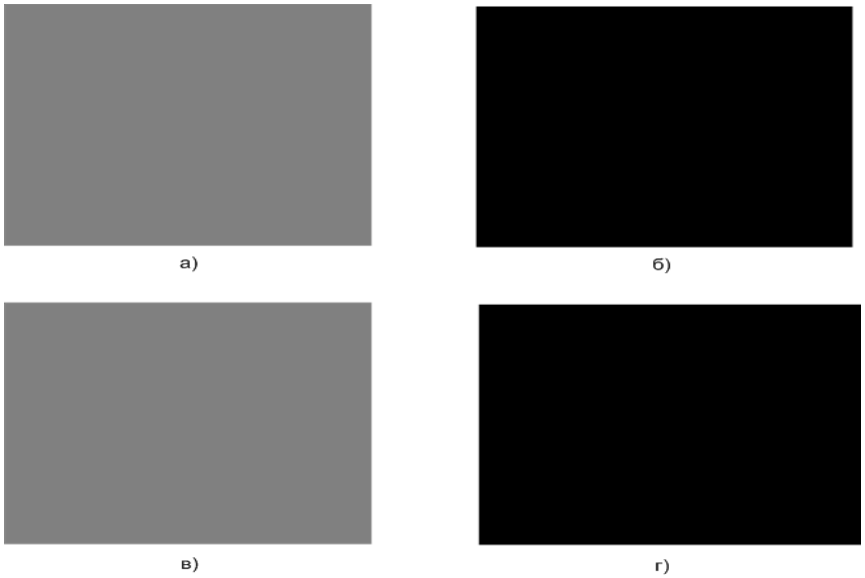


Рисунок 3.18 − Демаскированные (восстановленные) изображения (а,в) и их разностное представление с исходным изображением (б,г)

Гистограммы маскированного изображения представлены на рисунке 3.19:

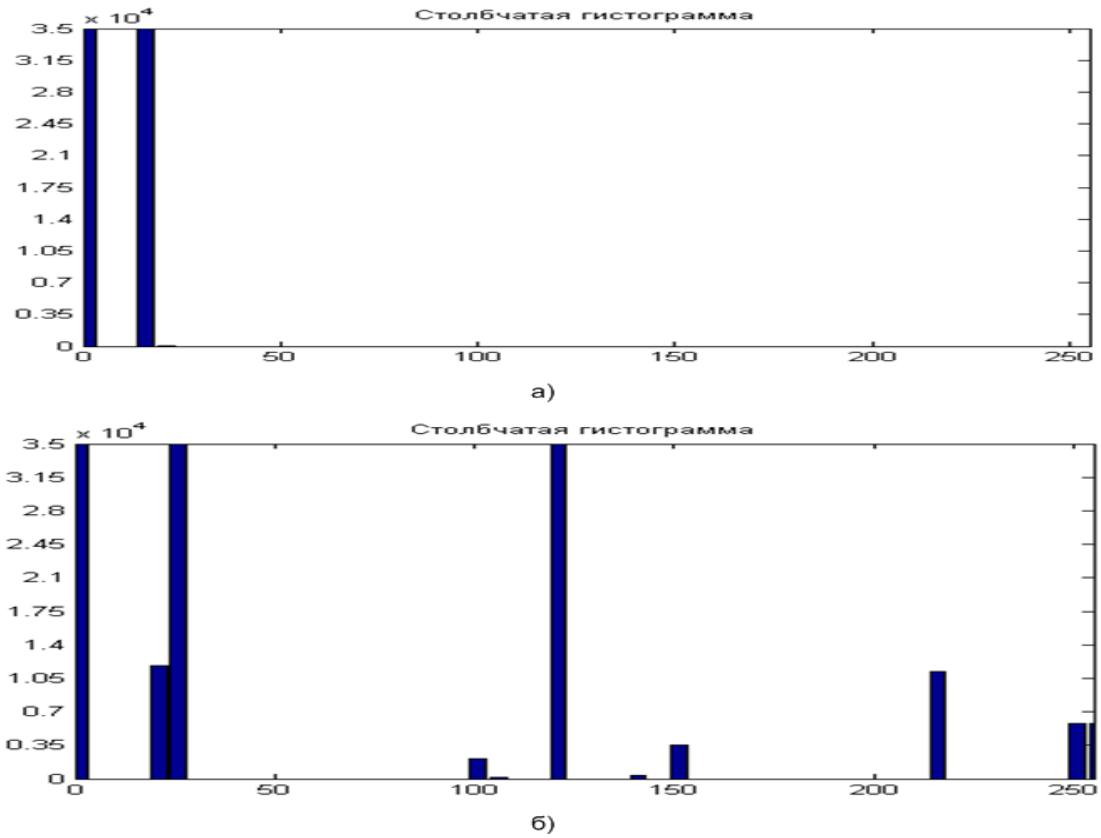


Рисунок 3.19 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

По гистограммам на рис. 3.19 можно сделать вывод, что при представлении пикселей в виде чисел с фиксированной и плавающей точкой получается импульсный шум.

На рис. 3.20 представлено маскированное изображение черного текста на белом фоне с представлением пикселей изображения в виде числа с фиксированной (а) и плавающей (б) точкой, а также их визуализации (в, г).

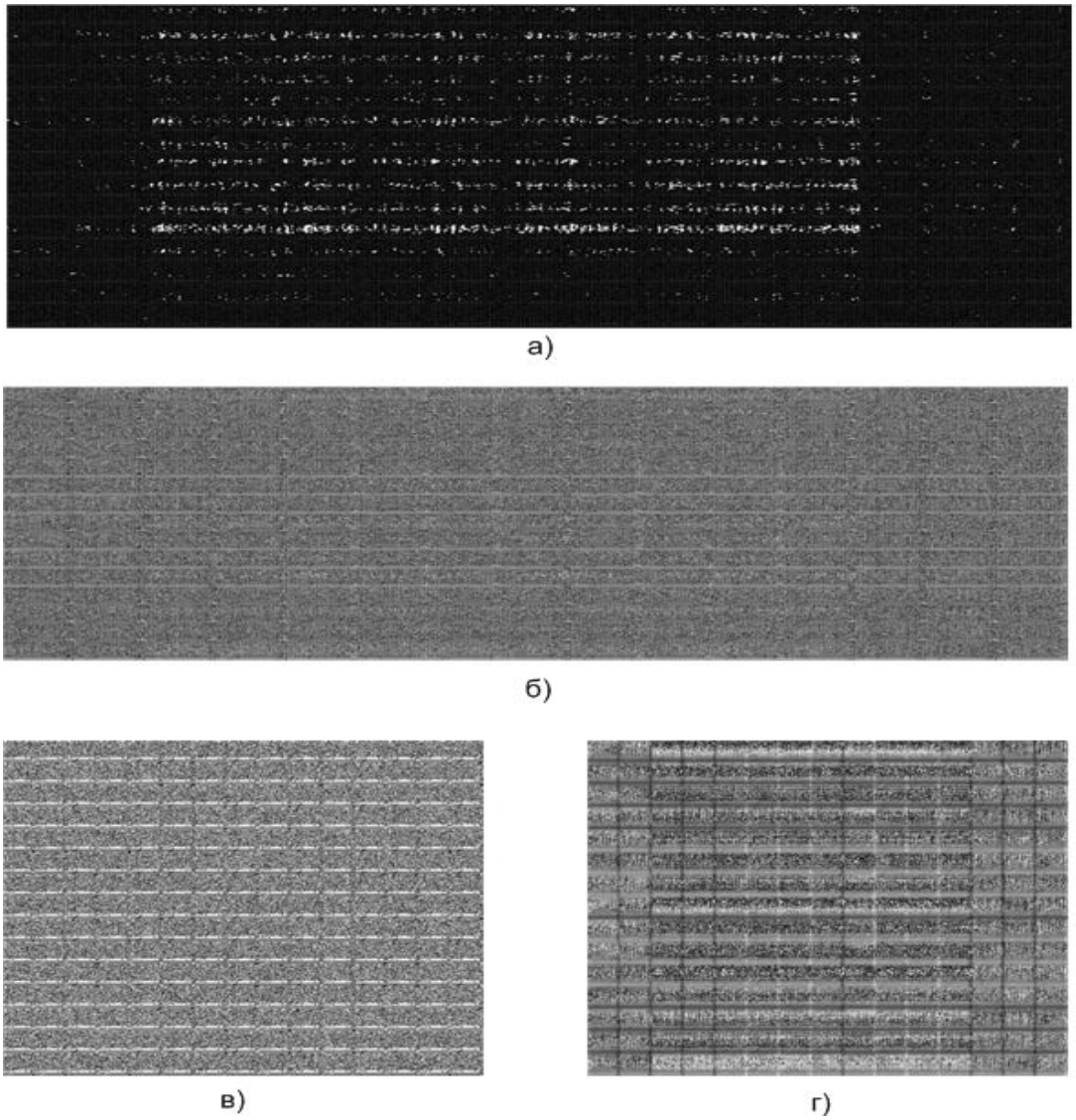


Рисунок 3.20 – Маскированное изображение черного текста на белом фоне (а,в – фиксированная точка; б,г – плавающая точка)

На рис. 3.21 представлены демаскированные (восстановленные) изображения:

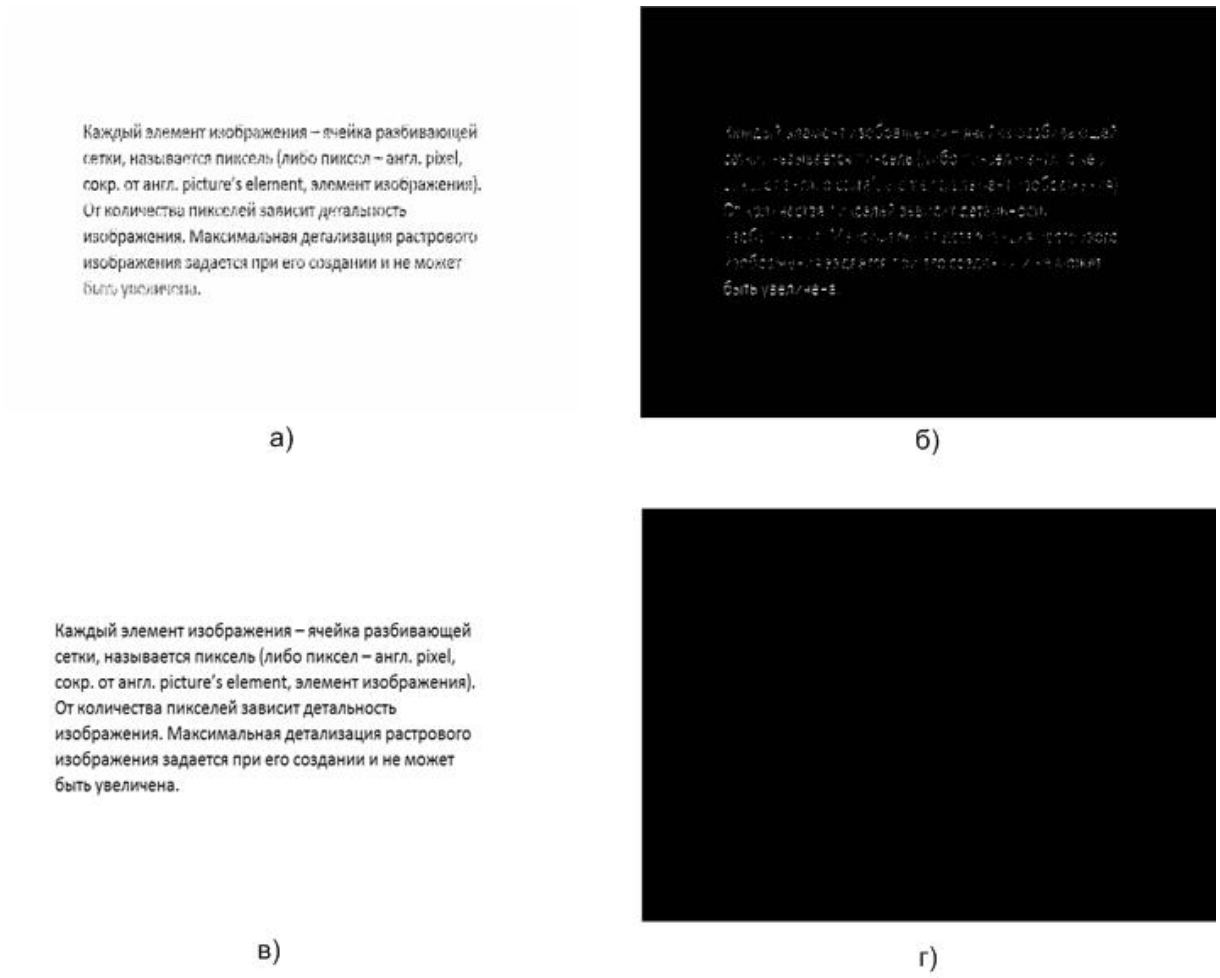


Рисунок 3.21 − Демаскированные (восстановленные) изображения (а,в) и их разностное представление с исходным изображением

На рис. 3.21 (б) видно, что при использовании чисел с фиксированной точкой произошла потеря данных. Это связано с этапом квантования, заключающемся в сдвиге коэффициентов маскированного изображения на 20 бит и приведении числа с фиксированной точкой, после восстановления маскированного изображения, к целочисленному значению.

Гистограммы маскированного изображения представлены на рис. 3.22.

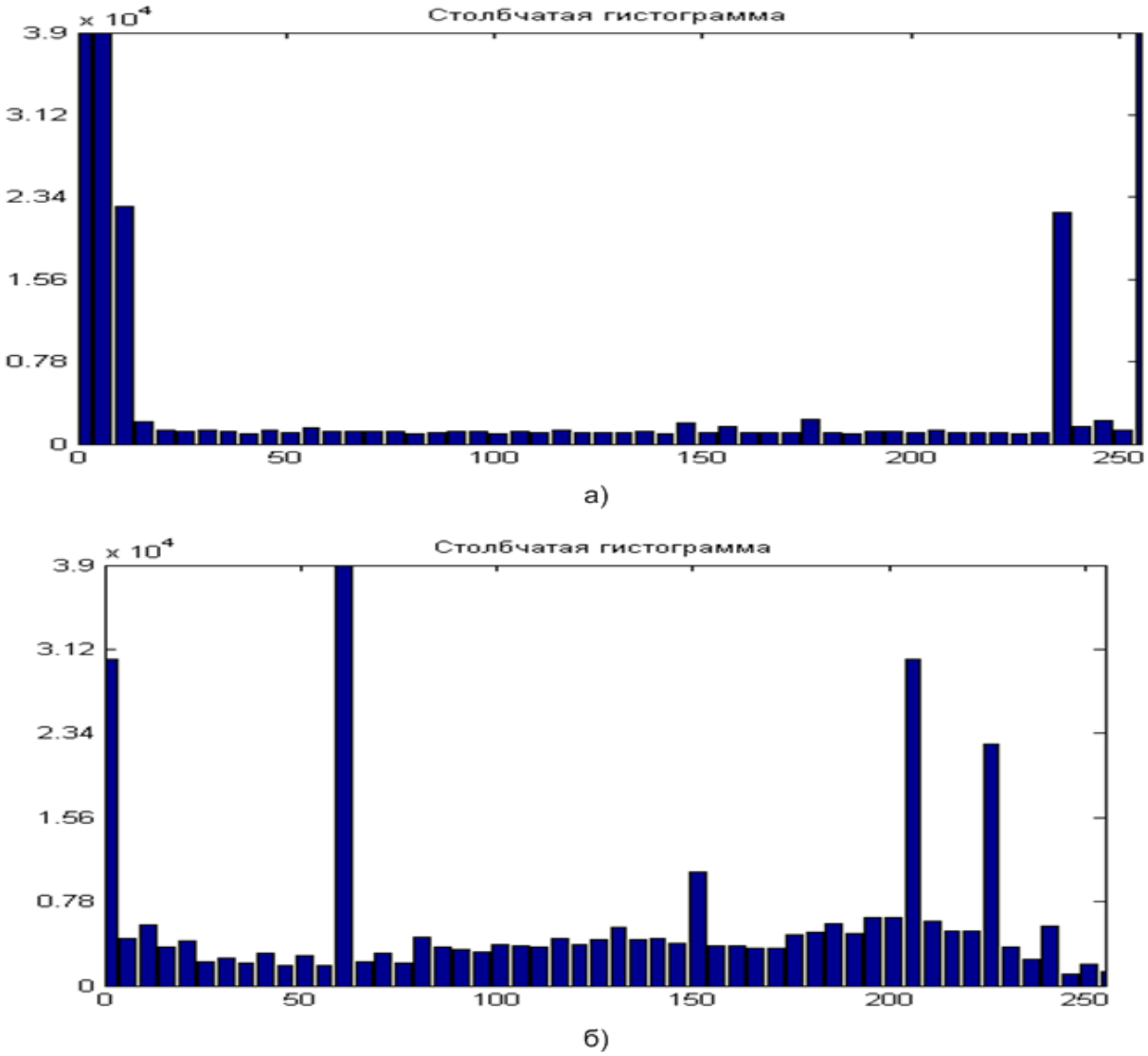


Рисунок 3.22 − Гистограмма маскированного изображения (а – фиксированная точка; б – плавающая точка)

По гистограммам на рис. 3.22, можно сказать, что при представлении пикселей в виде чисел с фиксированной и плавающей точкой получается импульсный шум.

Оценка качества восстановленных маскированных изображений. Для оценки качества изображений после демаскирования, относительно исходных, будем использовать несколько известных метрик, которые скалярно оценивают соответствие восстановленного изображения исходному изображению, а именно метрики PSNR, MSE [78], SSIM [77], MSSIM [76].

В табл. 3.1 представлены числовые значения оценок качества восстановленных маскированных изображений, с представлением значений пикселей в виде чисел с фиксированной точкой.

Таблица 3.1 – Оценки качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 3.1 (а)	51.1339	0.5008	1	1
Рис. 3.1 (б.1)	50.9848	0.5183	0.9999	1
Рис. 3.1 (б.2)	18.5996	897.6804	0.9397	0.9770
Рис. 3.1 (в)	50.2090	0.6197	1	1
Рис. 3.1 (г)	21.1026	504.4501	0.9682	0.9705
Рис. 3.1 (д)	48.1308	1	1	1
Рис. 3.1 (е)	50.8999	0.5286	0.9998	0.9999

Из табл. 3.1 видно, что в большинстве случаев, кроме рис. 3.1(б.2) и 3.1 (д), качество изображений не изменилось.

В табл. 3.2 представлены числовые значения оценок качества восстановленных маскированных изображений, с представлением значений пикселей в виде чисел с плавающей точкой.

Таблица 3.2 – Оценки качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 3.1 (а)	51.1411	0.5	1	1
Рис. 3.1 (б.1)	51.4682	0.4637	0.9993	0.9998
Рис. 3.1 (б.2)	68.2706	0.0097	1	1
Рис. 3.1 (в)	60.5386	0.0574	0.9999	0.9999
Рис. 3.1 (г)	Inf	0	1	1
Рис. 3.1 (д)	Inf	0	1	1
Рис. 3.1 (е)	51.1595	0.4979	0.9983	0.9999

Из табл. 3.2 видно, что качество восстановленных изображений, согласно метрикам, претерпело незначительное изменение и лежит в пределах нормы данных метрик.

Таким образом, маскирование изображений не вносят в восстановленное изображение относительно исходного изображения критических артефактов и изменений.

3.4 Особые изображения двустороннего матричного маскирования

Пусть исходное изображение разбито на N одинаковых матриц $\mathbf{X}$ размером $n \times n$. Поставим задачу найти изображения, которые инвариантны к преобразованию маскирования и переводятся им в то же изображение с точностью до постоянного множителя – $\mathbf{M}^T\mathbf{X}\mathbf{M} = \lambda\mathbf{X}$. Такие изображения называют собственными, корневыми или особыми изображениями преобразования [21, 108, 122]. 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.

Ортогональные матрицы $\mathbf{M}$ с собственными значениями $|\lambda| = 1$ не усиливают изображения. При умножении на $\mathbf{M}$ слева поиск особых изображений сводится к стандартной задаче определения перестановочных друг с другом матриц $\mathbf{XM} = \mathbf{MX}$ (или $\mathbf{XM} = -\mathbf{MX}$).

Из матричной алгебры известно, что матрицы перестановочны (коммутируемы), если они построены на одинаковом наборе собственных векторов. Для симметричных матриц $\mathbf{M}$ собственные числа вещественны, а собственные векторы – ортогональны. В частности, коммутируема сама с собой матрица $\mathbf{X} = \mathbf{M}$, поскольку она, безусловно, построена на том же наборе собственных векторов, что и преобразующая матрица, и $\mathbf{M}^T\mathbf{X} = \mathbf{I}$ – единичная матица. Иными словами, наиболее беззащитны изображения, похожие на преобразующую матрицу, и для успешного маскирования ей самой выгодно выглядеть хаотичной. Это качество разделяют между собой все матрицы семейства Мерсенна.

Для маскирования фрагментов изображения **P** будем использовать матрицы Мерсенна, визуализованные «портреты» порядков 7, 15, 31 и 255 которых приведены в разделе 2.4 на рис. 2.10.

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

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) 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***, т.е. не меняется. Отсюда следует алгоритм построения особых изображений, состоящий в вариации матрицы собственных чисел ортогональной матрицы **M** и ее реконструкции $\mathbf{P}^* = \mathbf{VD^*V}^{-1}$.

На рис. 3.23 приведены по два «портрета» вычисленных корневых изображений **P*** для приведенных на рис. 2.10 матриц. 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, можно смело утверждать, что матричное двустороннее маскирование матрицами Мерсенна может быть использовано в системах без каких-либо ограничений, вносимых изображениями, инвариантными к преобразованию $\mathbf{M}^{\mathrm{T}}\mathbf{PM}$.

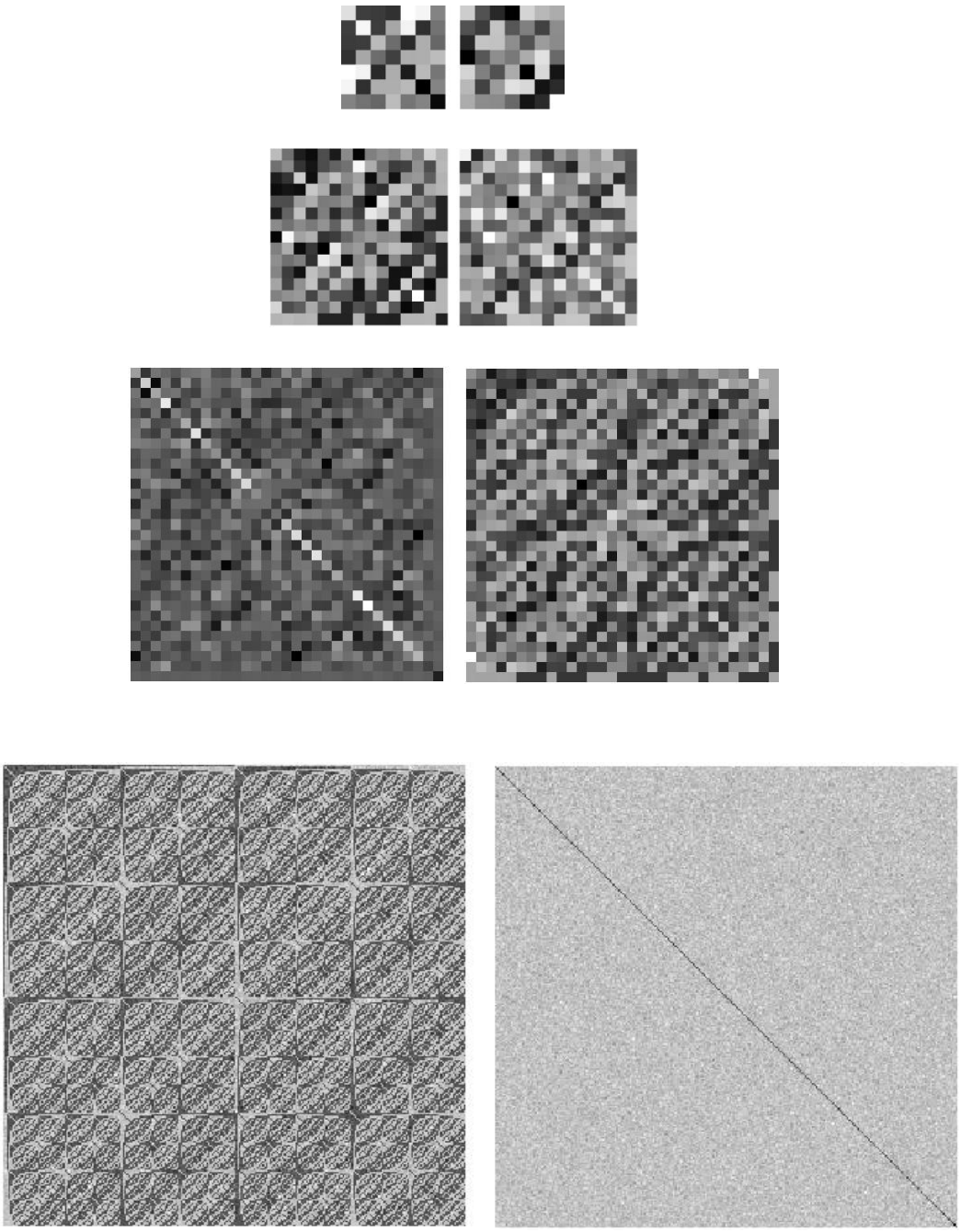


Рисунок 3.23 – «Портреты» особых изображений для матриц Мерсенна порядков 7, 15, 31 и 255

3.4 Восстановление маскированного изображения при потере части данных в коммуникационном канале

В работах [94 - 96] приведены примеры искажения и восстановления маскированных изображений при передаче по коммуникационным каналам. Данные исследования проводились на фотографиях, а не на наборе тестовых изображений. Поскольку на фотографиях, использованных в эксперименте, имеется больший разброс по яркостям, чем у тестовых изображений, маскирующее преобразование при восстановлении «дефектного» (с потерей части данных/пакета) маскированного изображения распределяет ошибки по всему восстановленному изображению в случае потери пакетов. Это происходит при условии, что значения пикселей представляются как число с плавающей запятой.

Стоит отметить, что такая потеря пакетов не является критичной, если передается не сжатое маскированное изображение и не теряется первый пакет, который содержит заголовок и данные для приема последующих частей кадра. В случае, когда произошла потеря данных при передаче маскированного изображения в «контейнере», то восстановить исходное изображение не представляется возможным.

Разработка собственного «контейнера» (формата), который не критичен к потере небольшой части пакетов является одним из приоритетных направлений при дальнейших исследованиях в теории маскирования.

Ниже представлены результаты восстановления маскированного изображения при потере части данных – изменению подверглась небольшая часть маскированного изображения. Приведенные результаты актуальны и для случаев, когда в маскированное изображение преднамеренно внесли искажения.

На рис.3.24 приведен пример восстановленного изображения телевизионной испытательной таблицы, на котором значения пикселей представлены в виде чисел с фиксированной (а) и плавающей (в) точками.

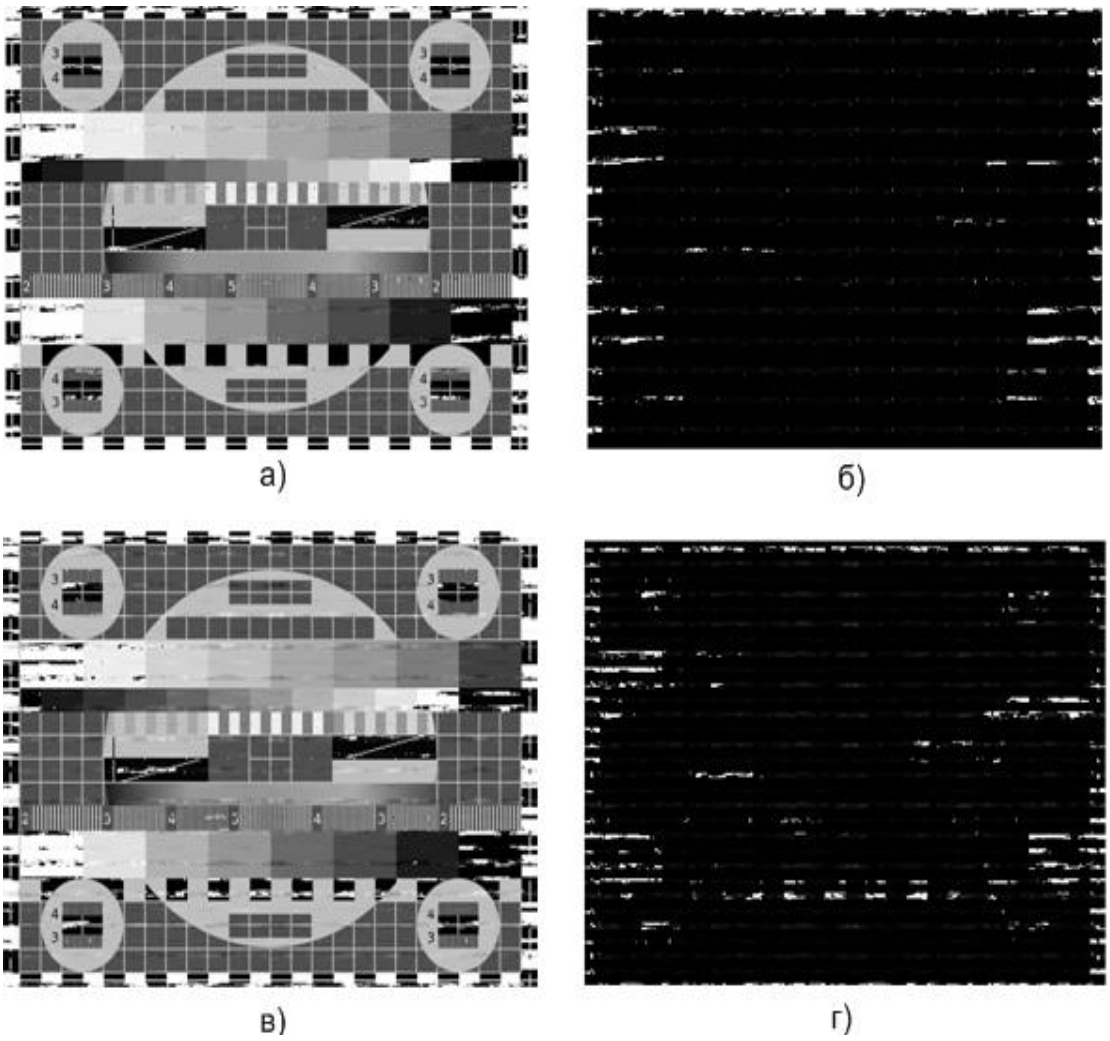


Рисунок 3.24 – Пример восстановленного маскированного изображения после потери части исходных данных (а, в – восстановленное маскированное изображение с внесенными изменениями; б, г – разность восстановленного и исходного изображения)

На рис. 3.25 приведен пример восстановленного изображения градиента в градации серого, где значения пикселей представлены в виде чисел с фиксированной (а) и плавающей (в) точкой.

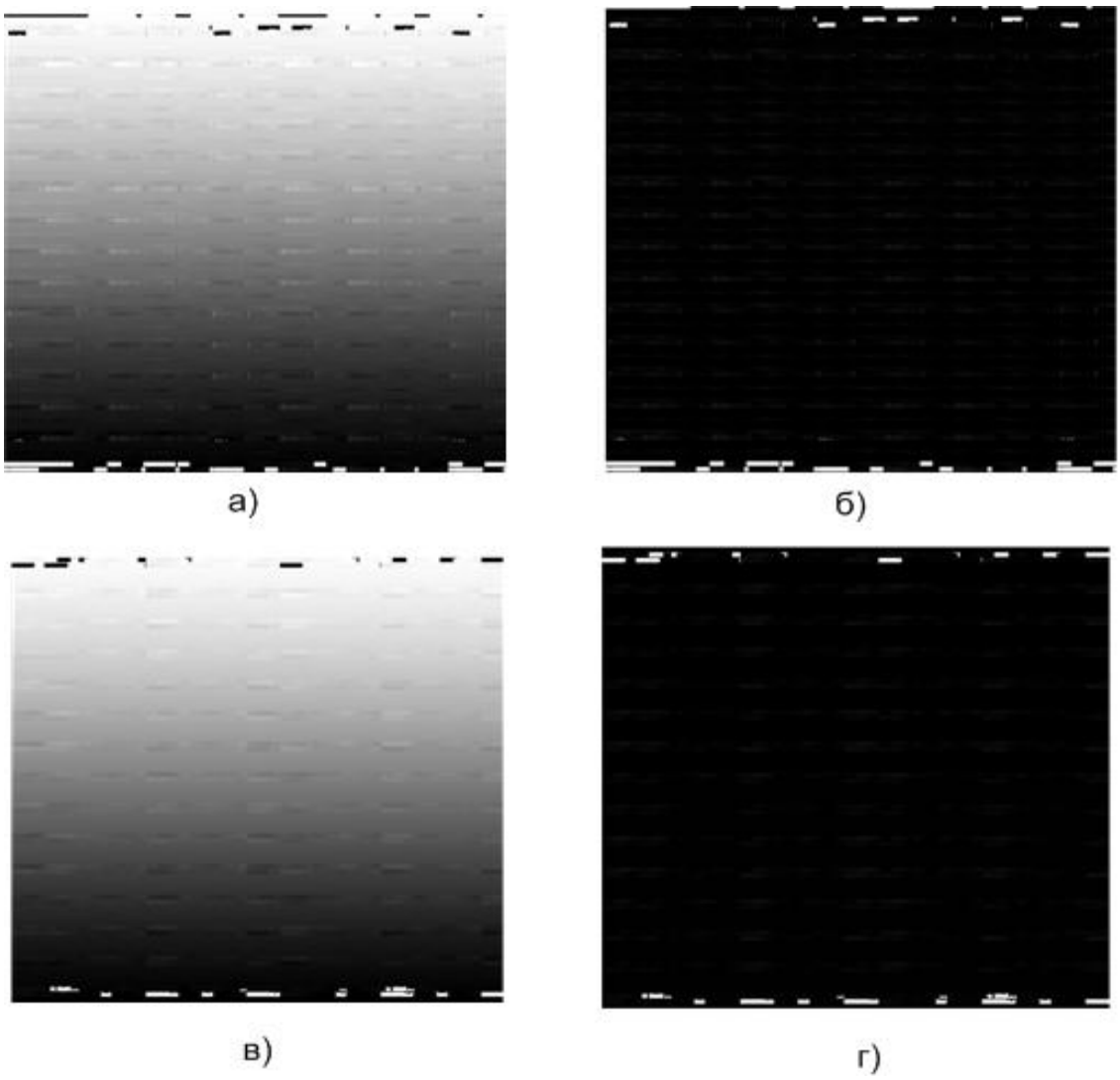


Рисунок 3.25 – Пример восстановленного маскированного изображения после потери части исходных данных (а, в – восстановленное маскированное изображение с внесенными изменениями; б, г – разность восстановленного и исходного изображения)

На рис. 3.26 приведен пример восстановленного изображения, содержащего текст, где значения пикселей представлены в виде чисел с фиксированной (а) и плавающей (б) точкой:

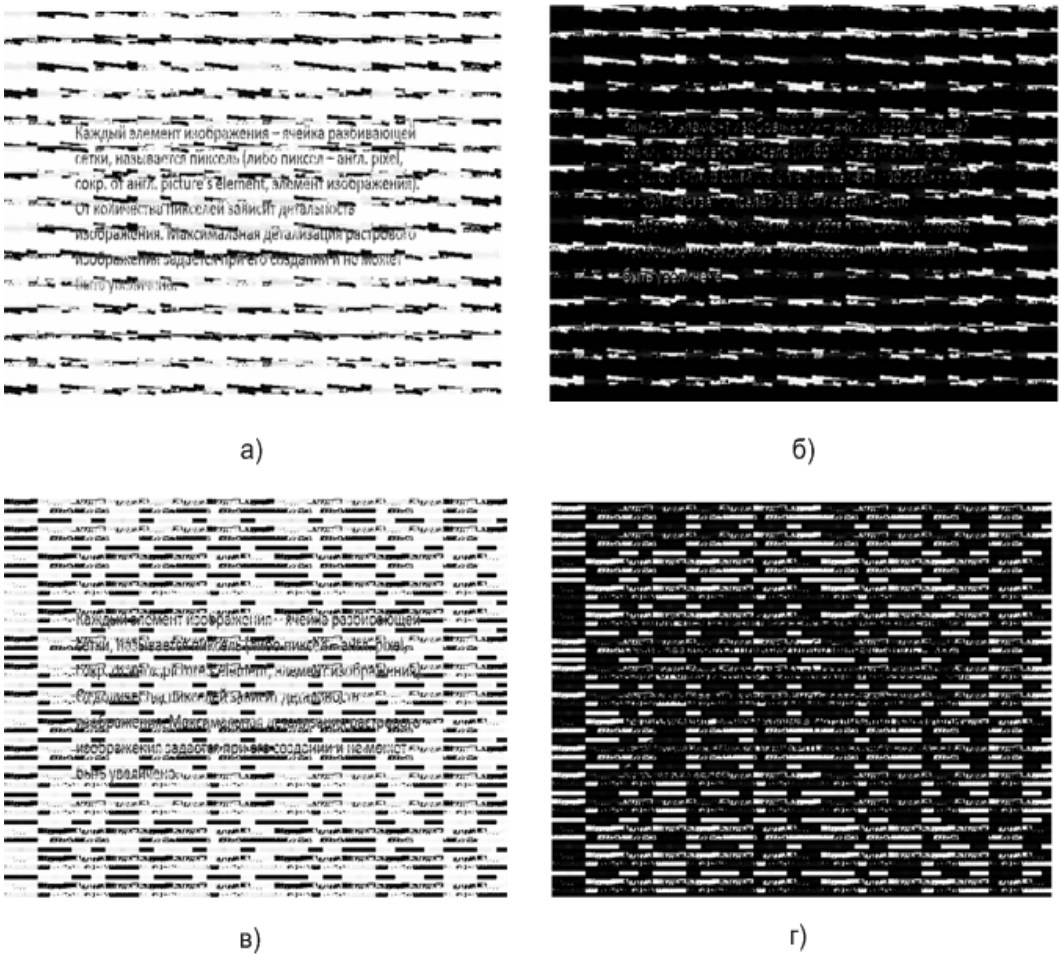


Рисунок 3.26 – Пример восстановленного маскированного изображения после потери части исходных данных (а, в – восстановленное маскированное изображение с внесенными изменениями; б, г – разность восстановленного и исходного изображения)

Анализ рис. 3.24 – 3.26 показал, что внесение небольших изменений в маскированное изображение приводит в возникновению большого количества артефактов на восстановленном изображении. Это связано со спецификой базовой операции – стрип-преобразования, а также с тем, что на тестовых изображениях имеется множество блоков с одинаковой яркостью. Такое свойство предложенного метода маскирования способствует быстрому обнаружению проблем в канале передачи.

Оценка качества восстановленных маскированных изображений. В табл. 3.3 представлены числовые значения оценок качества восстановленных

маскированных изображений с представлением значений пикселей в виде чисел с фиксированной точкой (рис. 3.24 (а) – 3.26 (а)).

Таблица 3.3 – Оценки качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 3.24 (а)	17.6707	1.1118e+003	0.8863	0.9297
Рис. 3.25 (а)	19.5756	717.0016	0.8687	0.8752
Рис. 3.26 (а)	9.2157	7.7895e+003	0.5556	0.3281

Из табл. 3.3 видно, что качество восстановленных изображений, согласно значениям метрик, претерпело значительное изменение.

В табл. 3.4 представлена оценка качества восстановленных маскированных изображений с представлением значений пикселей в виде чисел с плавающей точкой (рисунок 3. 24 (в) – 3. 26 (в)).

Таблица 3.4 – Оценки качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 3.24 (в)	16.1717	1.5700e+003	0.8370	0.8793
Рис. 3.25 (в)	21.5433	455.7713	0.9316	0.9310
Рис. 3. 26 (в)	6.6537	1.4051e+004	0.2222	0.2546

Анализ результатов в табл. 3.3 – 3.4 показывает, что при изменении данных (внесении помех) в маскированное изображение при восстановлении появляются артефакты. По их наличию, как и ранее, можно судить о проблемах в коммуникационном канале. Это связано со спецификой маскирования и 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 свойственно для маскированных изображений, у которых значения яркостей пикселей представлены в виде чисел с плавающей точкой. Если значения яркости пикселей

представлены в виде чисел с фиксированной точкой, то возникающие артефакты становятся более заметными.

3.5 Выводы

Метод маскирования/демаскирования цифровых изображений позволяет выявлять по демаскированным изображениям наличие помех в коммуникационном канале, что подтверждается оценками качества восстановленных (демаскированных) изображений с использованием объективных метрик.

При двустороннем матричном маскировании изображений матрицами Мерсенна характерно наличие особых изображений, которые инвариантны по отношению к маскирующему преобразованию. Полученные и визуализированные особые изображения для матриц Мерсенна позволяют утверждать, что разработанный метод маскирования может быть использован без ограничений – особые изображения не являются портретами объектов реального мира. Поскольку основной целью метода является сокрытие информации на маскированном изображении, то «синтетическая» природа особых изображений опасности не несет и такие изображения не требуют дополнительного исследования.

Предложенный метод маскирования непосредственно применим только к монохромным изображениям, поскольку только они представляются в виде матрицы, состоящей из числовых значений отдельных пикселей. Однако при представлении цветных изображений трехслойной матрицей RGB маскированию будет подвергаться отдельно каждый из трех слоев матрицы изображения.

4 СРАВНИТЕЛЬНЫЙ АНАЛИЗ МАТРИЧНОГО МАСКИРОВАНИЯ С КЛАССИЧЕСКИМ АЛГОРИТМОМ ШИФРОВАНИЯ

В данном разделе представлены результаты сравнения метода маскирования, с применением уникальных ортогональных базисов, с методами шифрации с коротким ключом.

Приводятся результаты по времени матричного маскирования и возможности его ускорения.

Оценивается дальнейшего развития направления маскирования фото и видеоизображений.

4.1 Выбор алгоритма симметричного шифрования для сравнительного анализа результирующего изображения с процедурой маскирования

Для сравнения метода шифрования с методом маскирования было проведено исследование, которое показало, что использованные алгоритмы шифрования [98 -107] относительно тестовых изображений повели себя примерно одинаково. В исследовании использовались такие алгоритмы, как:

- DES;
- RC2;
- RC5;
- ГОСТ 28147-89;
- AES (Advanced Encryption Standard);
- IDEA (International Data Encryption Algorithm);
- ThreeWay;
- DES_EDE3;
- Blowfish.

В качестве библиотеки, для проведения данного исследования была выбрана криптографическая библиотека Crypto++ 5.6.2 для языка программирования C++, которая предоставляет оптимизированные реализации всех приведенных в списке выше алгоритмов шифрования.

Для сравнения результатов шифрования с результатами маскирования шифрованию подверглись изображения с тестового набора, представленные на рисунке 3.1.

На основе проведенного исследования для сравнения с процедурой маскирования был выбран один из алгоритмов симметричного шифрования – DES (Data Encryption Standard).

4.2 Шифрация тестовых изображений и сравнение результатов

Шифрация тестовых изображений алгоритмом шифрования DES. На приведенных ниже рисунках представлены результаты шифрования тестового набора изображений алгоритмом симметричного блочного шифрования DES с максимальной длиной ключа – 56 бит.

Как можно заметить из рис. 4.1, после шифрования исходного изображения можно определить, какое именно изображение было подвергнуто шифровано. Это связано с тем, что шифрование осуществляется блоками, а последовательность пикселей исходного изображения повторяется в каждой строке. Из-за такого строения исходного изображения, которое имеет резкие переходы, классический алгоритм шифрования неспособен сокрыть «смысл» изображения. По гистограмме можно судить, что шифрованное изображение можно отнести к импульсному шуму.

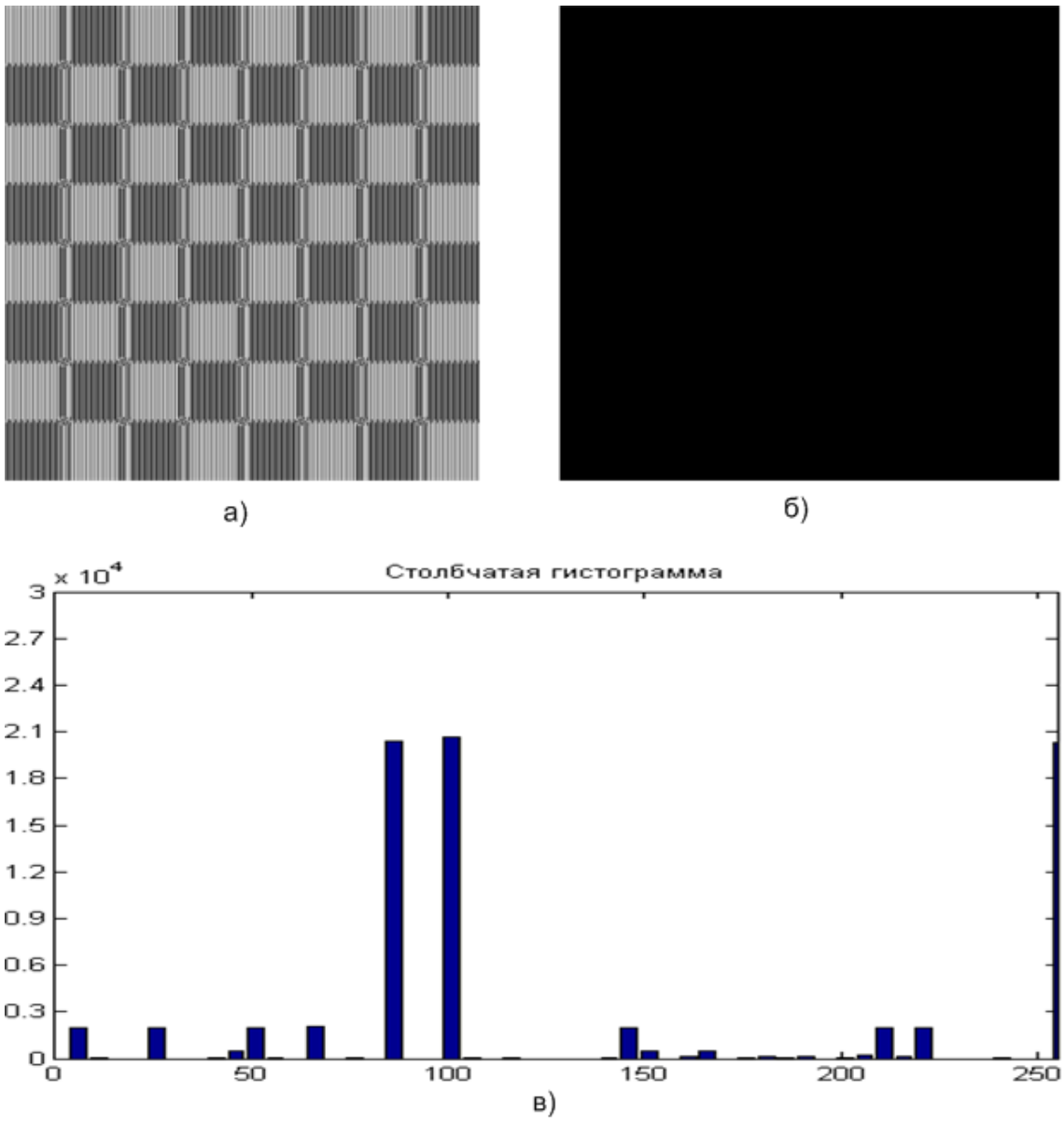


Рисунок 4.1 – Шифрованное изображение «Шахматная доска» (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

На рис. 4.2 видно, что после шифрования исходного изображения, как и в предыдущем случае, можно определить, что за изображение было зашифровано. На исходном изображении, как и в предыдущем случае, присутствуют резкие переходы и блоки с постоянными значениями пикселей, из-за их наличия классический алгоритм шифрования не способен скрыть «смысл» исходного изображения. Гистограмма показывает, что шифрованное изображение можно отнести к аддитивному типу шума.

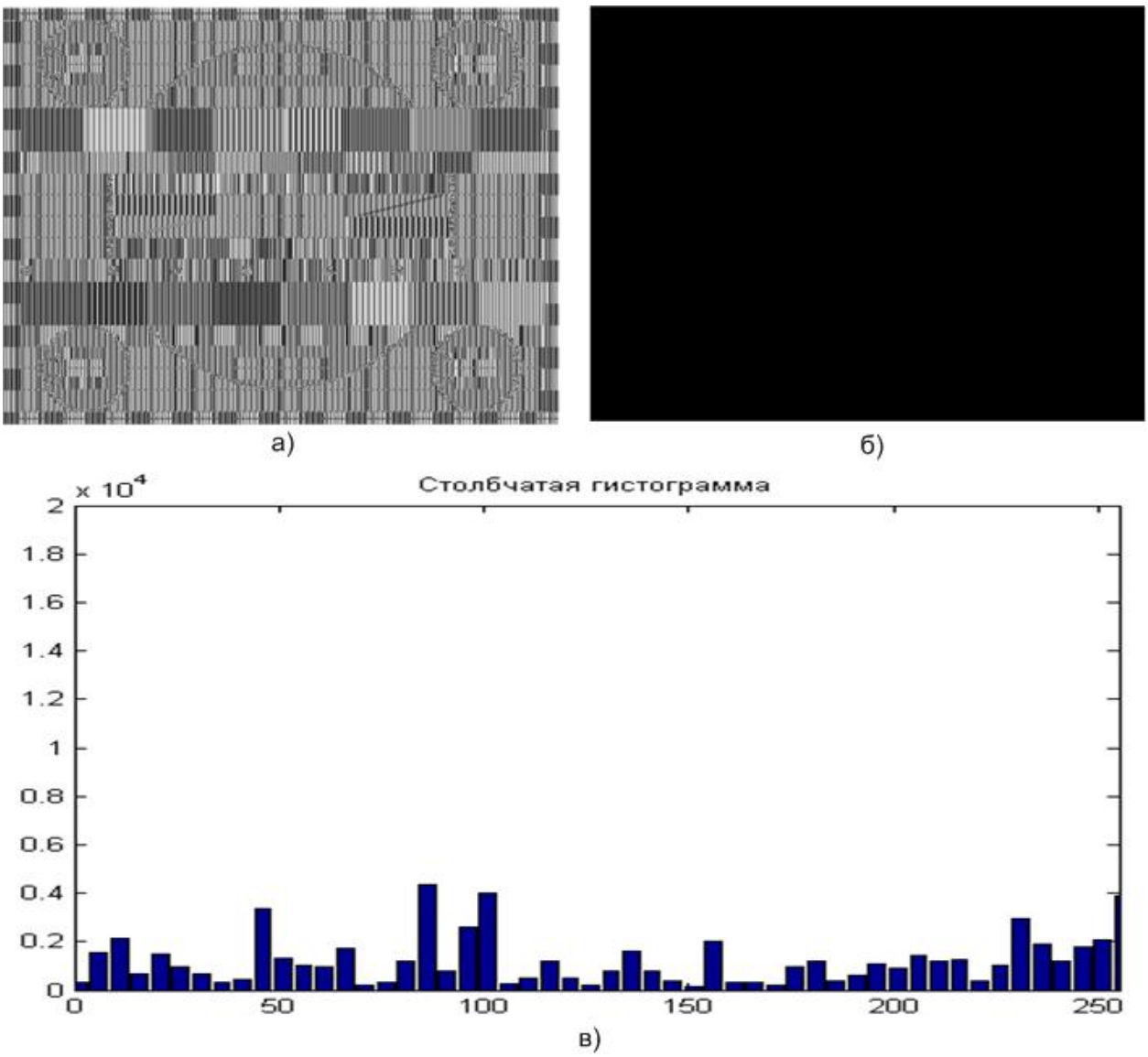


Рисунок 4.2 – Шифрованное изображение телевизионной испытательной таблицы (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

На рис. 4.3 видно, что после шифрования, как и в предыдущих случаях, просматривается исходное изображение. Исходное изображение, как и в предыдущем случае, характеризуется резкими перепадами яркостей, что влияет на сокрытие его «смысла». Гистограмма показывает, что шифрованное изображение относится к аддитивному типу шума.

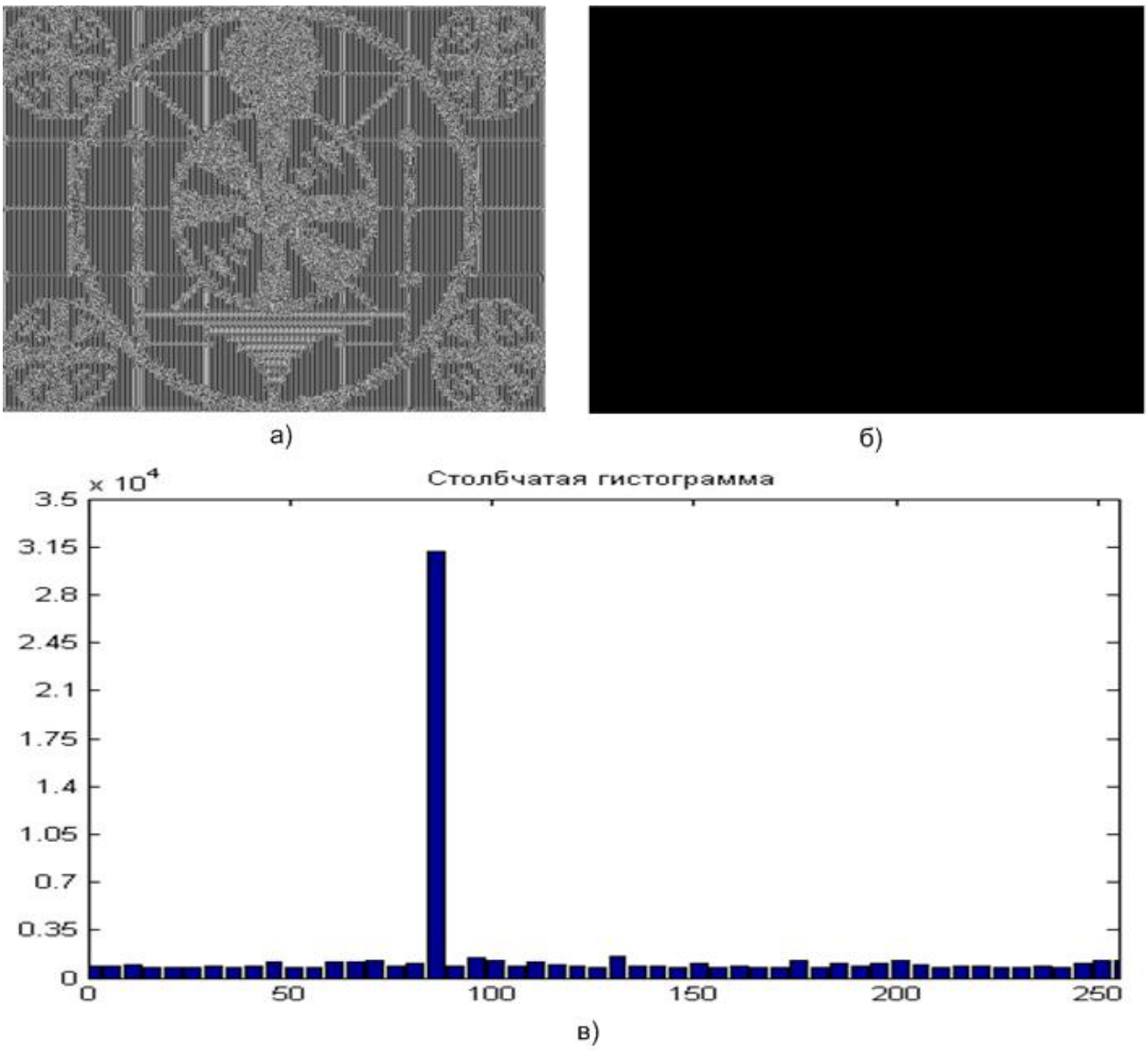


Рисунок 4.3 – Шифрованное изображение телевизионной испытательной таблицы (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

На рис. 4.4, на котором представлен результат шифрования градиента серого, поведение алгоритма шифрования объясняется следующим образом: каждая строка исходного изображения имеет свою постоянную яркость, тем самым осуществляется «сдвиг» текущей выходной зашифрованной строки относительно предыдущей и создается вид «шума» на шифрованном изображении. По гистограмме можно судить, что шифрованное изображение можно отнести к аддитивному типу шума.

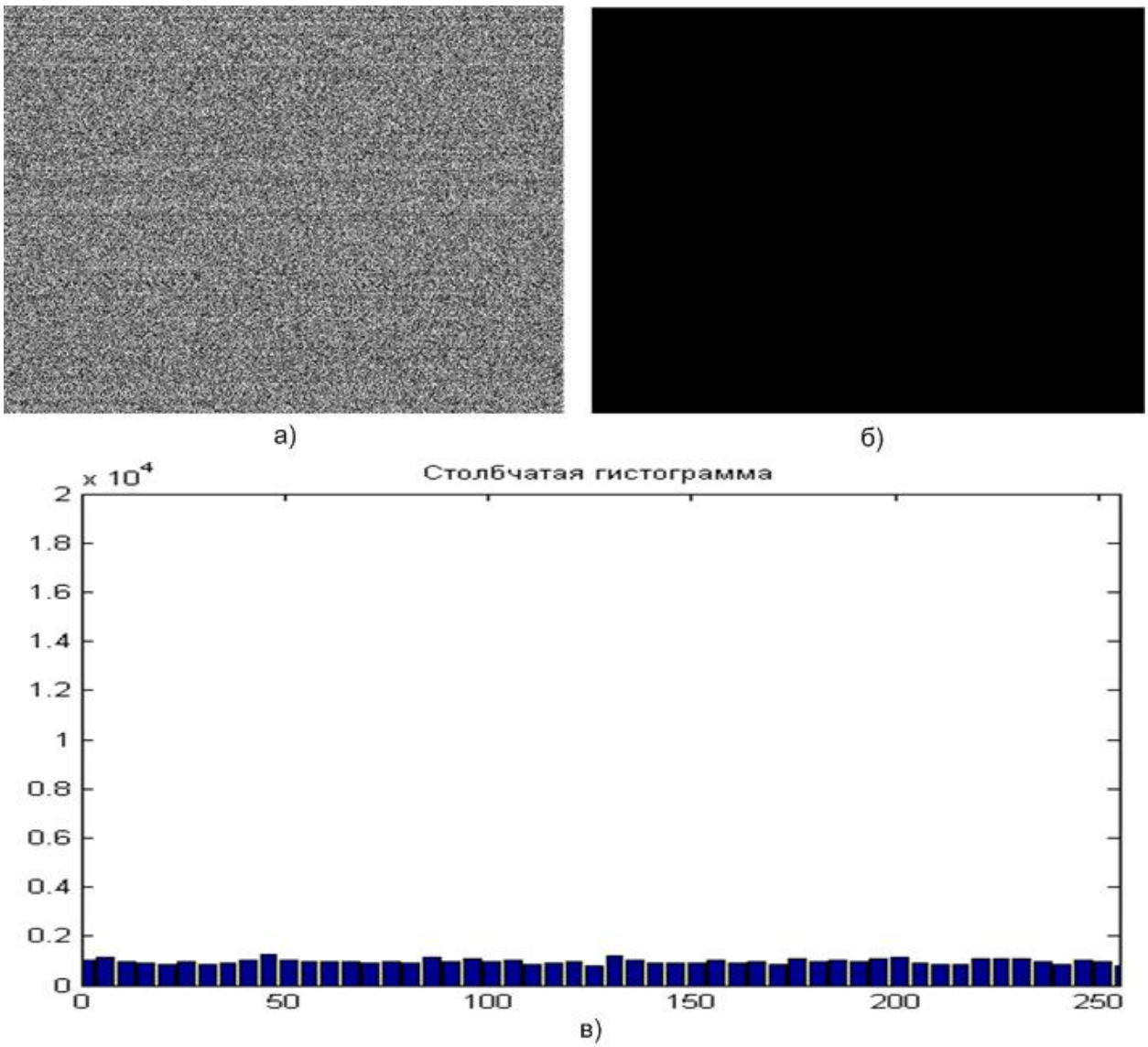


Рисунок 4.4 – Шифрованное изображение градиента в градации серого (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

Рис. 4.5, представляющий результат шифрования просматривающегося исходного изображения круга, демонстрирует тот факт, что шифрование, осуществляемое блоками над блоками с постоянной яркостью пикселей и наличием резких переходов по яркости на изображении, не приводит к желаемому результату. По гистограмме можно судить о том, что шифрованное изображение относится к импульсному типу шума.

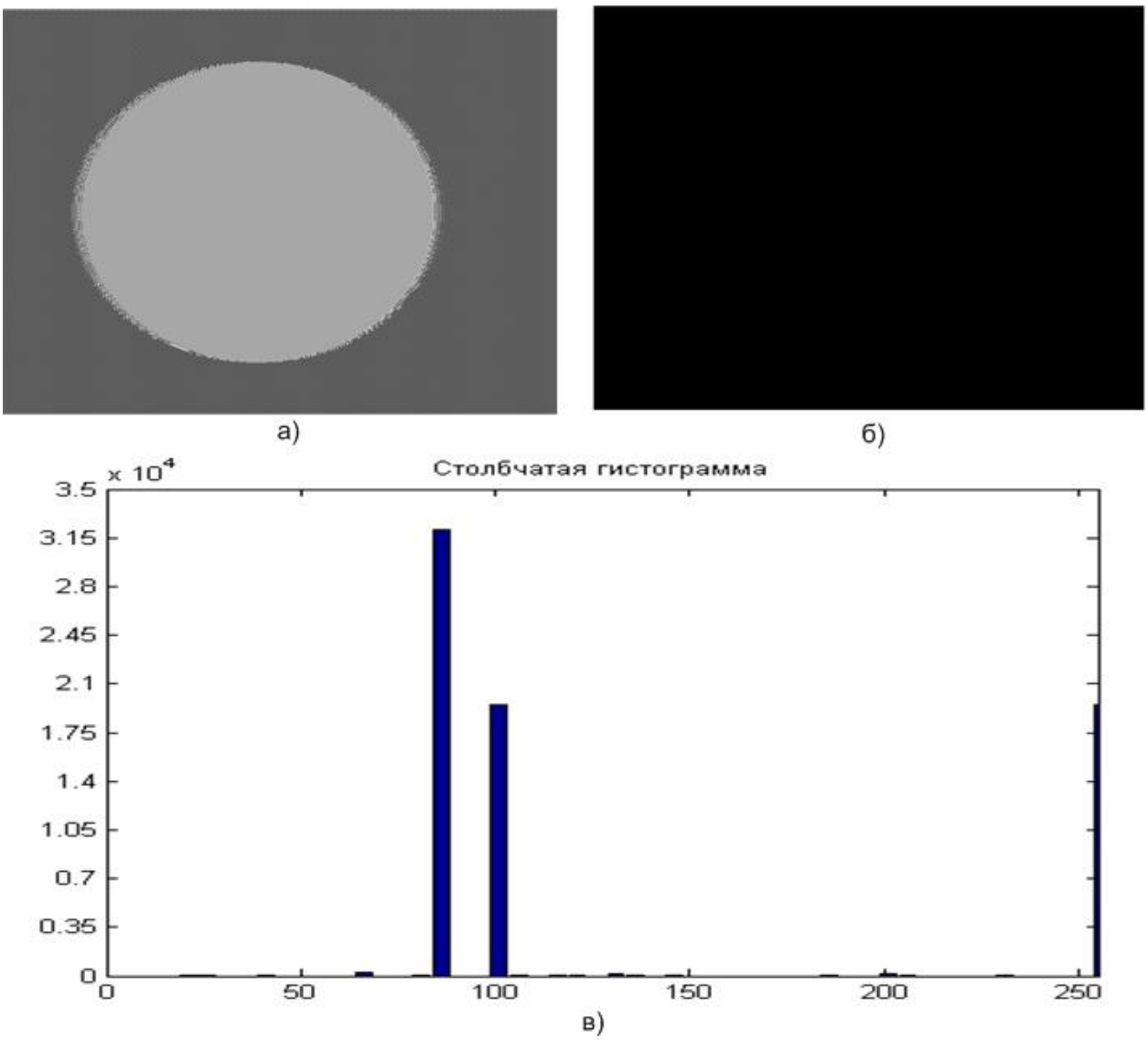


Рисунок 4.5 – Шифрованное изображение черного круга на белом фоне (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

На шифрованном изображении (рис. 4.6) можно наблюдать повторяющуюся блочную структуру, из чего следует, что наличие блоков с постоянной яркостью или резкими перепадами на исходном изображении для рассматриваемого метода шифрования не желательно. По гистограмме можно судить, что шифрованное изображение можно отнести к импульсному типу шума.

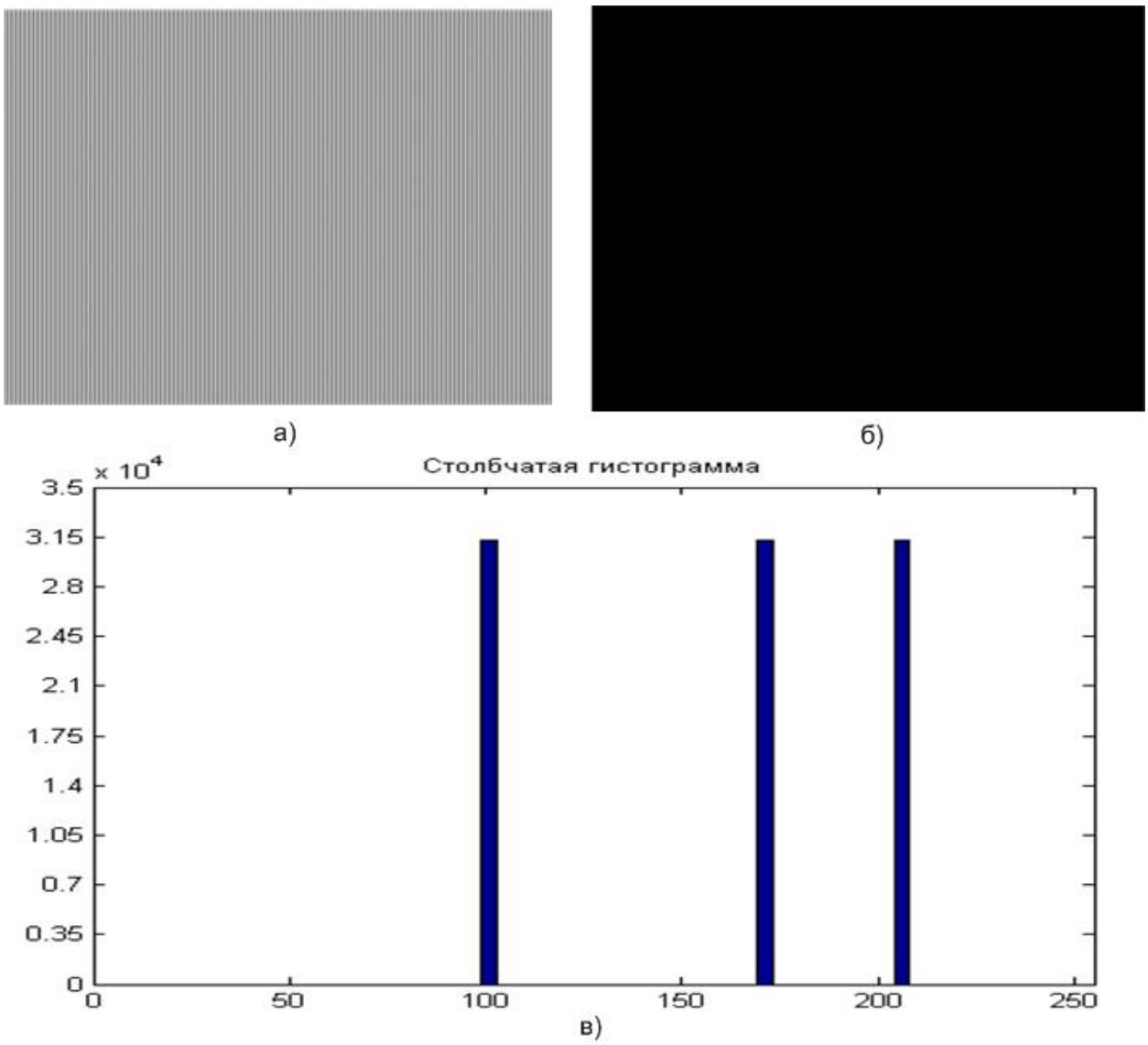


Рисунок 4.6 – Шифрованное изображение с постоянным серым цветом (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

Как можно заметить из рис. 4.7, после шифрования исходного изображения можно определить, что на исходном изображении был текст, но невозможно его прочитать. По гистограмме видно, что шифрованное изображение относится к импульсному типу шума.

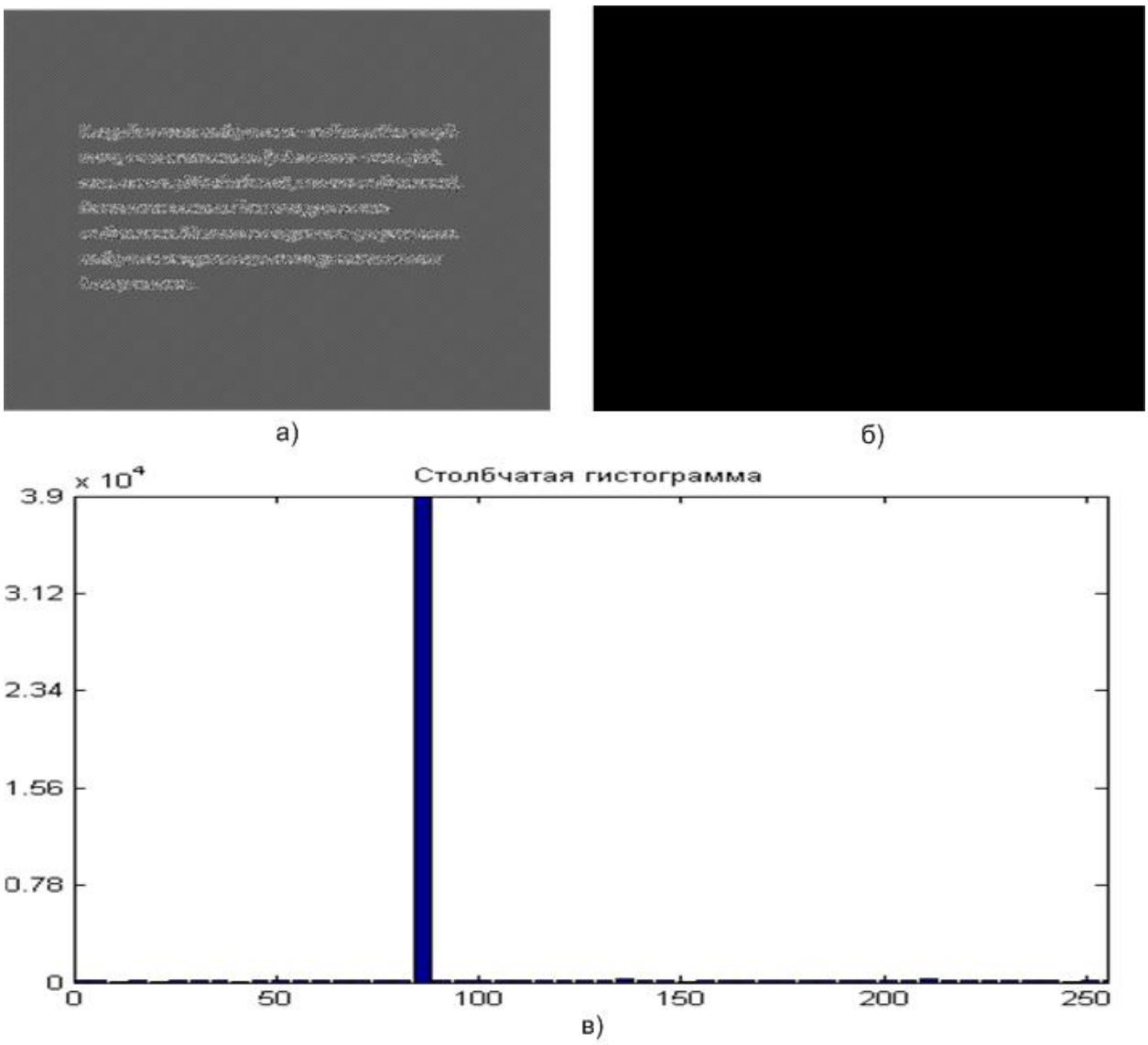


Рисунок 4.7 – Шифрованное изображение черного текста на белом фоне (а – шифрованное изображение, б – разность исходного и восстановленного изображения, в – гистограмма шифрованного изображения)

Оценка качества восстановленных шифрованных изображений. Для оценки качества восстановленных шифрованных изображений в сравнении с исходными, использовался тот же набор метрик, что и для оценки качества восстановленных маскированных изображений.

В табл. 4.1 представлена оценка качества восстановленных изображений, шифрованных алгоритмом DES, по значениям метрик.

Таблица 4.1 – Оценка качества восстановленных изображений

Обозначение исходного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 3.1 (а)	Inf	0	1	1
Рис. 3.1 (б.1)	84.0965	2.5318e-004	1	1
Рис. 3.1 (б.2)	104.9432	2.0833e-006	1	1
Рис. 3.1 (в)	45.4304	1.8623	1	1
Рис. 3.1 (г)	45.3700	1.8883	1	1
Рис. 3.1 (д)	50.8675	0.5325	1	1
Рис. 3.1 (е)	102.1102	4.0000e-006	1	1

Из табл. 4.1 видно, что качество восстановленных изображений, согласно метрикам, претерпело незначительное изменение.

Таким образом (по результатам оценки метрик из табл. 3.1, 3.2 и табл. 4.1) шифрование и маскирование изображений не вносят в восстановленное изображение, по сравнению с исходным, критических артефактов и изменений.

4.3 Восстановление исходного изображения из шифрованного при потере части данных при передаче и сравнение результатов

Восстановление шифрованного изображения при потере части исходных данных. Рассмотрим, что происходит при восстановлении шифрованного с использованием алгоритма DES изображения при потере пакетов (части данных) во время передачи изображения (без сжатия) или при внесенных изменениях в любом графическом редакторе при его хранении.

На рис. 4.8 приведен пример восстановленного и шифрованного изображения телевизионной испытательной таблицы (рис.4.2 с внесенной потерей части исходных данных).

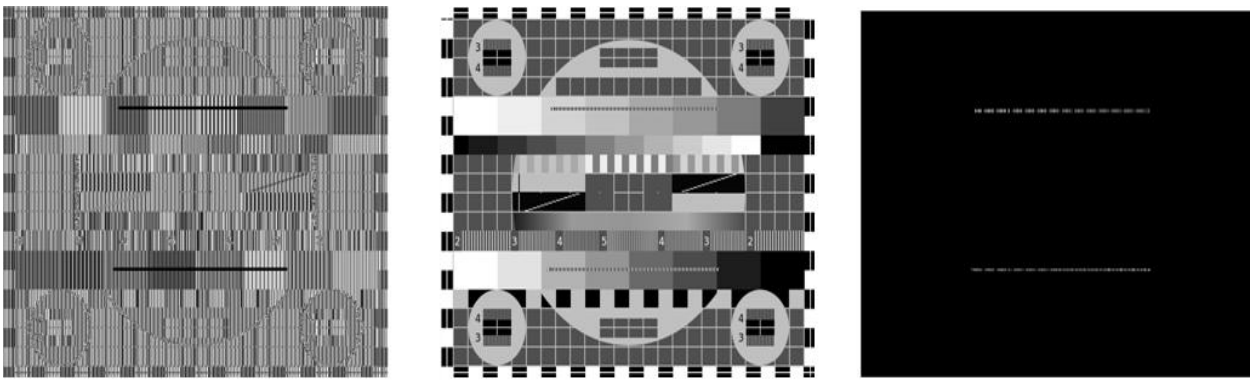


Рисунок 4.8 – Пример восстановленного шифрованного изображения после потери части исходных данных (а –шифрованное изображение с внесенными изменениями, б – восстановленное изображение, в – разность восстановленного и исходного изображения)

Как видно из рис. 4.8 пострадали только блоки, в которые были внесены изменения, структура восстановленного изображения относительно исходного, в целом, не претерпела изменений.

На рис. 4.9 приведен другой пример восстановленного и шифрованного изображения градиента в градации серого (рис.4.4 с внесенной потерей части исходных данных).

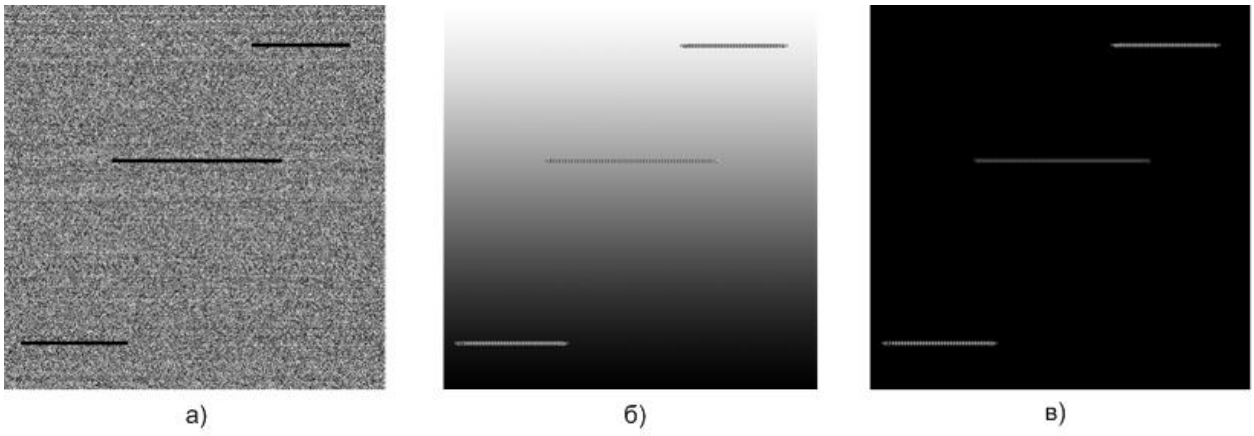
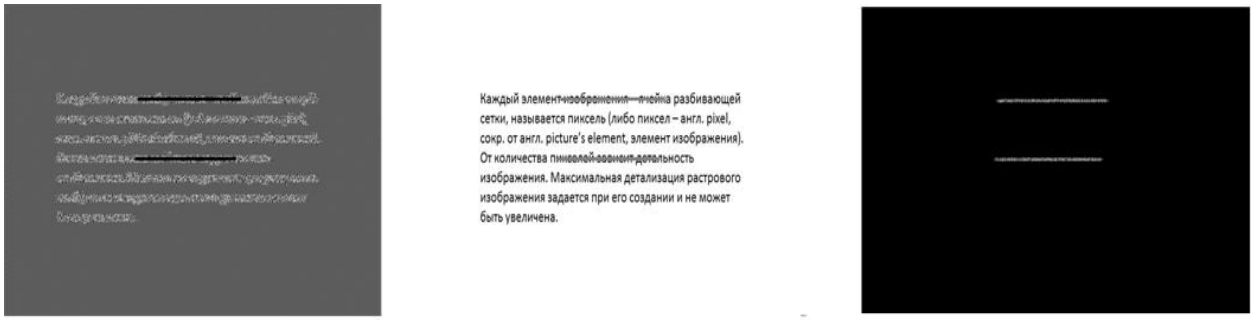


Рисунок 4.9 – Пример восстановленного шифрованного изображения после потери части исходных данных (а –шифрованное изображение с внесенными

изменениями, б – восстановленное изображение, в – разность восстановленного и исходного изображения)

Из рис. 4.9 видно, что, как и в предыдущем случае, пострадали блоки, в которые были внесены изменения. Структура восстановленного изображения относительно исходного, в целом, не претерпела изменений.

На рис. 4.10 приведен пример восстановленного и шифрованного изображения текста (рис. 4.7 с внесенной потерей части исходных данных).



а) б) в)

Рисунок 4.10 – Пример восстановленного шифрованного изображения после потери части исходных данных (а –шифрованное изображение с внесенными изменениями, б – восстановленное изображение, в – разность восстановленного и исходного изображения)

По изображениям, представленным на рис. 4.8 – 4.10 можно определить, в какой области шифрованного изображения были внесены изменения. Если изменения внесены в один пиксель 8-ми байтного блока, то данный блок восстановится некорректно. Внесение небольших изменений в маскированное изображение приводит в возникновению большого количество артефактов на восстановленном изображении. С одной стороны, в изображении, восстановленном из шифрованного, меньше артефактов, но менее заметен факт, что был потерян пакет при передаче или были внесены изменения в шифрованное изображение, что более отчетливо наблюдается в восстановленных маскированных изображениях на рис. 3.9 – 3.11.

Оценка качества восстановленных шифрованных изображений. В табл. 4.2 представлена оценка качества восстановленных изображений, приведенных на рис. 4.8 – 4.10, по значениям метрик.

Таблица 4.2 – Оценка качества восстановленных изображений

Обозначение восстановленного изображения	Вычисленные значения метрик			
	PSNR	MSE	SSIM	MSSIM
Рис. 4.8	30.4906	58.0788	0.9809	0.9761
Рис. 4.9	27.2689	121.9515	0.9729	0.9317
Рис. 4.10	27.8186	107.4535	0.9937	0.9962

Из этой таблицы, согласно значениям метрик, видно, что качество восстановленных изображений претерпело незначительное изменение. Таким образом, при внесении погрешностей в шифрованное изображение при его восстановлении появляются артефакты в тех областях (кратных блоку шифрования), где были внесены погрешности.

4.4 Оценка времени маскирования

Для оценки времени маскирования использовался ПК с процессором Intel® Core™ i7-2630QM с 8Гб оперативной памяти, ОС – Windows 8.1 с программным обеспечением, написанным на языке программирования C++.

В табл. 4.3 и 4.4 представлены результаты времени маскирования/шифрования и демаскирования/дешифрования изображений. Столбец fix обозначает маскирование/демаскирование с представлением пикселей числами с фиксированной точкой, а float – представление пикселей маскируемого/демаскируемого изображения числами с плавающей точкой.

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.

Таблица 4.3 – 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

Таблица 4.4 – 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

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 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.

Напомним, что процедура маскирования направлена на её реализацию в системах встраиваемого класса на процессорах ЦОС и ПЛИС. Например, на тестовых наборах использовалась матрица Мерсенна $\mathbf{M}_{15}$, что позволит на ПЛИС ускорить процедуру маскирования не менее чем в 15 раз, при наличии достаточного количества ее внутренних ресурсов. Помимо этого, алгоритмам сжатия без потерь необходимо построить словарь на основе которого и будет производиться уменьшение размера файла.

Перемножение элементов матрицы Мерсенна и маскируемого изображения можно оптимизировать, используя поиск по хэш-таблице. Поскольку матрицы Мерсенна двухуровневые (со значениями 1 и $-b$), это значительно сокращает количество возможных вариантов при перемножении, а, следовательно, размер таблицы и время поиска результата.

Хеш-таблица – структура данных, реализующая интерфейс ассоциативного массива и позволяющая хранить пары вида «ключ-значение» и выполнять три операции: добавление (вставка), поиск и удаление пары по ключу.

Таким образом, хеш-таблица в реализации метода маскирования – массив, формируемый в определенном порядке хеш-функцией [97].

Считается, что «хорошая» хеш-функция должна удовлетворять следующим условиям:

- быть простой (с вычислительной точки зрения);
- распределять наиболее равномерно ключи в хеш-таблице;
- не отображать какую-либо связь между значениями ключей в связь между значениями адресов;
- минимизировать число коллизий (ситуаций, когда разным ключам соответствует одно значение хеш-функции).

Не смотря на то, что операции поиска, добавления и удаления в среднем выполняются за время O(1), такая оценка не учитывает возможные аппаратные

затраты на перестройку индекса хеш-таблицы, когда увеличивается значение размера массива и в хеш-таблицу добавляется новая пара.

Самая простейшая организация таблицы, обеспечивающая быстрый поиск – таблица прямого доступа. К сожалению, не смотря на их эффективность область применения таких таблиц весьма ограничена.

Замена умножения на поиск по хэш-таблице позволит сократить время маскирования, так как операция умножения более дорогостоящая, чем поиск по таблице. Для данной реализации предлагается создать специализированную хэш-таблицу, в которой будет осуществляться поиск по ключевой паре – «значение яркости пикселя изображения – значение элемента маскирующей матрицы».

Во время маскирования, если результат в хэш-таблице не найден, осуществляется вычисление текущей пары «ключ-значение» и результат записывается в таблицу. В момент старта данная таблица является пустой и перестраивается под каждую смену маскирующей матрицы, т.е. хранится в энергозависимой памяти и стирается при отключении устройства.

Таким образом, при старте устройства будут задержки, связанные с необходимостью заполнить хэш-таблицу. Чем больше времени будет производится маскирование изображения с использованием одной маскирующей матрицы, тем меньше раз, от начала работы, будет необходимо производить запись в хэш-таблицу.

Приведенные выше факты являются основанием для дальнейшего исследования и модификации процедуры маскирования с целью сокращения временных затрат на нее при реализации.

4.5 Внедрение результатов диссертационной работы

Различные аспекты результатов проведенных в диссертационной работе исследований имеют внедрения, что подтверждено актами о внедрении, приведенными в приложении.

Универсальное программное обеспечение на языке C++, защищенное свидетельствами о государственной регистрации программного обеспечения для ЭВМ [109 – 112, 123], используется в учебном процессе Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» в дисциплинах, связанных с процедурами обработки цифровой визуальной информации и проектированием систем обработки информации на ПЛИС.

Несмотря на то, что эти реализации используют принципы распараллеливания вычислений на центральном процессоре ПК, «чистой» параллельной реализации процедуры маскирования получить не возможно, поскольку в операционной системе, обычно, запущено множество фоновых процессов (либо запущены другие приложения), что загружает часть вычислительных ресурсов процессора. Однако, несмотря на это, разработанное программное обеспечение позволяет проводить моделирование и исследование процедур маскирования/демаскирования с матрицами Мерсенна различных порядков на любых наборах изображений с различным представлением пикселей маскируемого/демаскируемого изображения (фиксированная и плавающая точка).

На рис. 4.11 приведен пример графического пользовательского интерфейса программного обеспечения Mask Pro v3 для маскирования и демаскирования изображений с представлением пикселей в виде чисел с фиксированной точкой.

Программно-аппаратная реализация разработанного метода в виде алгоритма, адаптированного для DSP процессора BlackFin, использована в рамках опытно-конструкторской работы, проведенной ООО «АСК Лаборатория», при создании опытного образца специализированного видеорегистратора событий. Full-HD видеорегистратор с беспроводным интерфейсом Wi-Fi и функцией геолокации используется в качестве конечного мобильного модуля распределенной видео системы. Процедура маскирования видеоизображения в данном устройстве реализуется на процессоре ADSP-BF523KBCZ фирмы Analog Devices в режиме реального времени и используется при передаче и записи

видеоизображения с разрешением Full-HD на информационный носитель типа microSD с фиксацией местоположения (геолокация в системах GPS и GLONASS). Доступ к настройкам и выполненным записям, а также получение регистрируемого видео-аудио потока в реальном масштабе времени, осуществляется через беспроводной сетевой интерфейс Wi-Fi.

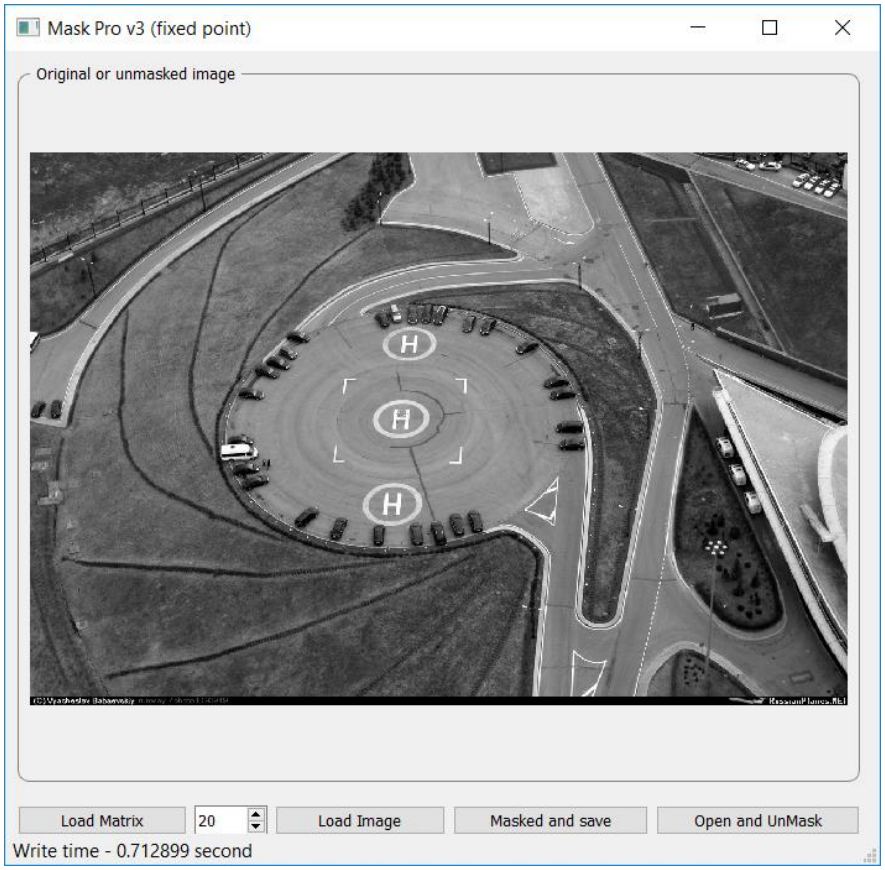


Рисунок 4.11 – Пользовательский интерфейс программного обеспечения для маскирования и демаскирования изображений с применением квазиортогональных матриц

Встроенный датчик ускорений позволяет автоматически переводить устройство в режимы работы, соответствующие текущему состоянию объекта, и фиксировать ситуации, требующие немедленной архивации записи (удары, столкновения). Видеорегистратор оснащается супер-конденсатором или литий-полимерным аккумулятором для корректного завершения записи в случае внезапного отключения питания.

На рис. 4.12 приведен внешний вид сборки разработанного Full-HD видеорегистратора, а в табл. 4.5 – его основные технические характеристики.

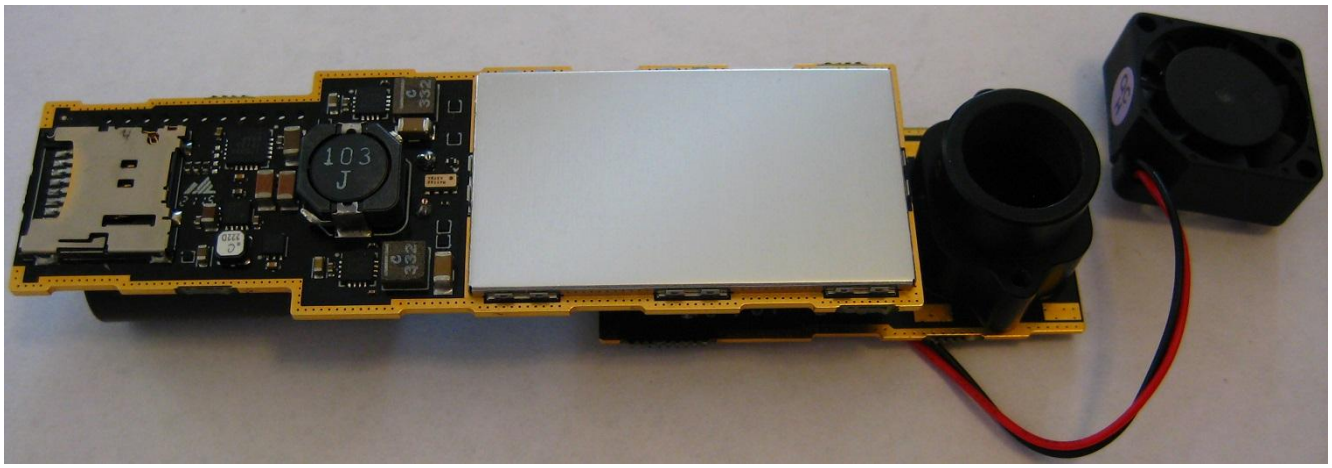


Рисунок 4.12 – Внешний вид сборки видеорегистратора

Таблица 4.5 – Основные технические характеристики видеорегистратора

Характеристики видеоизображения	Full-HD 1920x1080 (60 к/с) Full-HD 1920x1080 (30 к/с) HD 1280x720 (60 к/с) HD 1280x720 (30 к/с)
Свойства светочувствительной матрицы	3+ Mpix, RGB, режим WDR
Способ защиты изображений при записи и передаче по Wi-Fi (IEEE 802.11b/g/n)	Маскирование матричное
Формат файла	MJPEG
Режимы записи	линейный или «по кольцу»
Режима работы	«нормальный», «стоянка», «по событию»
Носитель информации	microSD (16Gb/32Gb/64Gb)
Геолокационный приёмник	GPS/GLONASS
Датчик ускорений	3-осевой, измен. чувств-ть
Беспроводной сетевой интерфейс	Wi-Fi (IEEE 802.11b/g/n), поддержка MIMO
Потребляемая мощность, не более, Вт	5.5
Диапазон рабочих температур, °С	- 40 ÷ +50
Габаритные размеры, мм	80x30мм (диам.) (определяется конструктивным исполнением)

4.6 Выводы

Рассмотренные в данном разделе результаты шифрации с коротким ключом тестовых изображений показали их несостоятельность для сокрытия изображений, передаваемых по открытым коммуникациям. В большинстве случаев после шифрации изображения не разрушаются и визуально идентифицируются.

Предложенный в работе метод маскирования цифровых изображений более устойчив к искажениям информации в телекоммуникационном канале передачи информации, что демонстрируется значениями объективных метрик.

Замена перемножения элементов матрицы Мерсанна и пикселей маскируемого изображения на поиск по хэш-таблице является значительным резервом ускорения выполнения процедуры маскирования/демаскирования изображений при программной реализации разработанного метода.

ЗАКЛЮЧЕНИЕ

В диссертационной работе рассмотрено матричное маскирование фото- и видеоизображений с использованием уникальных квазиортогональных матриц Мерсенна. Основное внимание уделено тому, 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, так как человеческое зрение представляет собой лучшую систему распознавания образов. Ввиду этого представление и визуализация защищенных изображений требуют особых подходов при маскировании изображений.

Время актуальности передаваемой видеоинформации в системах встраиваемого класса мало, что позволяет отказаться от шифрации видеопотока с использованием более длинных ключей, заменив ее матричным маскированием.

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-метода 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.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Основные характеристики камер видеонаблюдения [Электронный ресурс]. – Режим доступа – http://www.microvideo.ru/ articles/article1/.
2. КМОП-матрицы Aptina [Электронный ресурс] – Режим доступа – http://www.npk-photonica.ru/content/products/cmos-sensors-aptina.
3. Принцип работы IP видеонаблюдения: устройство и преимущества [Электронный ресурс] – Режим доступа – http://nabludau.ru/printsip-raboty-ip-videonablyudeniya-ustrojstvo-i-preimushhestva/.
4. IP видеонаблюдение: принцип, устройства, преимущества [Электронный ресурс] – Режим доступа – http://www.pogar-bezopasnost.ru/materials-11/bezopasnost/apr2013/918-princip-raboty-ip-vidjeonabljudjenija.
5. Гиляров, М. С. Биологический энциклопедический словарь. 2-е изд., исправл. / М. С. Гиляров, А. А. Бабаев, Г. Г. Винберг, Г. А. Заварзин и др. — М.: Сов. Энциклопедия, 1986 – 863 с.
6. Плехов, А. М. Словарь военных терминов. / А. М. Плехов, С. Г. Шапкин. — М.: Воениздат, 1988 – 335 с.
7. Кнунянц И. Л. Химическая энциклопедия. В 5 томах / гл. ред. И. Л. Кнунянц — М.: Советская энциклопедия, 1988 – 3355 с.;
8. Ребер, А. Оксфордский толковый словарь по психологии. В 2-х тт: Т.1 / Под ред. А. Ребера, Пер. с англ. Е.Ю Чеботарева. — М.: Вече АСТ, 2003. — 592 с.
9. Мещеряков, Б. Г. Большой психологический словарь / Б.Г. Мещеряков, В.П. Зинченко — М.: Прайм-ЕВРОЗНАК, 2003 – 816 с.
10. Статья «IBM представила ПО для маскировки закрытых данных» [Электронный ресурс] – Режим доступа – http://www.securitylab.ru/news/301841.php.
11. Официальный сайт компании Oracle [Электронный ресурс] – Режим доступа – http://www.oracle.com.
12. Справка по Photoshop [Электронный ресурс] – Режим доступа – http://helpx.adobe.com/ru/photoshop/using/masking-layers.html.

13. Гонсалес, Р. «Цифровая обработка изображений». / Р. Гонсалес, Р. Вудс – М.:Техносфера, 2005. – 1072 с.
14. 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;
15. Востриков, А.А. Маскирование цифровой визуальной информации: термин и основные определения/ А.А. Востриков, М.Б. Сергеев, М.Ю. Литвинов // Информационно-управляющие системы, Выпуск № 5 (78) // 2015, стр 116 - 123
16. Ерош, И. Л. О защите цифровых изображений при передаче по каналам связи / И. Л. Ерош, М. Б. Сергеев, Г. П. Филатов // Информационно-управляющие системы. 2007. № 5. С. 20–22.
17. Ерош, И. Л. Скоростное шифрование разнородных сообщений/ И. Л. Ерош, М. Б. Сергеев // Вопросы передачи и защиты информации: Сб. ст. / СПбГУАП. СПб., 2006. С. 133–155.
18. Литвинов, М.Ю. Алгоритмы маскирующих преобразований видеоинформации / М.Ю. Литвинов // Автореф. дис. канд. техн. Наук – ГУАП. СПб., 2009. – 23 с.
19. Железняк, В.К. Маскирование видеосигнала адаптивным видеошумовым сигналом с разрушением синхроимпульсов / В.К. Железняк, А. В. Барков // Международная научно-техническая конференция, приуроченная к 50-летию МРТИ-БГУИР : материалы конф. В 2 ч. Ч. 1. - Минск, 2014. - С. 422-423
20. Czaplewski, B. Digital Fingerprinting Based on Quaternion Encryption Scheme for Gray-Tone Images/ B. Czaplewski, M. Dzwonkowski, R. Rykaczewski // Journal of Telecommunications and Information Technology (JTIT) 2/2014 p. 3 – 11
21. Мироновский, Л. А. Стрип-метод преобразования изображений и сигналов / Л. А. Мироновский, В. А. Слаев // Монография. СПб: Политехника, 2006 - 163 с.
22. Красиленко, В. Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією

та їх моделювання/ В. Г. Красиленко, В. М. Дубчак // Вісник Хмельницького національного університету. Технічні науки, 2014. - № 1. - С. 74-79;

23. Журавель, И.М. «Краткий курс теории обработки изображений» [Электронный ресурс] – Режим доступа – http://matlab.exponenta.ru/imageprocess/book2/0.php .
24. Учебный курс «Высокопроизводительные вычисления для многопроцессорных многоядерных систем» [Электронный ресурс] – Режим доступа – http://www.hpcc.unn.ru/?doc=489.
25. Литвинов, М.Ю Использование помехоустойчивых кодов для шифрации видеоинформации/ М.Ю. Литвинов, С.В. Беззатеев, Б.К. Трояновский // Информационно-управляющие системы – 2004, № 5(30). – С. 23 – 26
26. McEliece, R.J. A public-key cryptosystem based on algebraic coding theory/ R.J. McEliece // DSN Progress Report, Jet Propulsion Laboratory, Pasadena, CA, Jan/Feb, 1978. – pp. 114 - 116.
27. Krouk, E. A new public-key cryptosystem/ E. Krouk // Proceedings of the 6-th Joint Swedish-Russian International Workshop on Information Theory, 1993. – pp. 285 – 286.
28. Gabidulin, E.M. Public-key cryptosystem based on linear codes/ E.M. Gabidulin // Designs, Codes and Cryptography, № 6(1), 1995. - pp. 37 - 45.
29. Jian-feng, M.A. A novel encryption method with its application in the copyright protection of digital data / M.A. Jian-feng, C. Teechye, K. Chichung Alex // Journal of Software, vol. 13, № 3, 2002. – pp. 330-334.
30. Rao, T.R.N. Private-key algebraic-code encryptions / T.R.N. Rao, Kil-Myun Nam //IEEE Trans. on Information Theory, vol.35, no. 4, 1989. – pp. 829 – 833.
31. Bezzateev, S.V. Converted Transformation of the Image with the Structure Destroying/ S.V. Bezzateev, M.Y. Litvinov, E.A. Krouk, G.P. Philatov // XI International Symposium on Problems of Redundancy in Information and Control Systems: Proceeding, SUAI, 2007. – p.173.
32. Фам, С. Н., Модификации алгоритма МакЭлис для повышения показателей качества радиосистем передачи информации/ С. Н. Фам // Диссертация на соискание ученой степени кандидата технических наук: спец. 05.12.04

Рязань, Рязанский государственный радиотехнический университет, 2007. – 168 с.

33. Гоппа, В.Д. Новый класс линейных помехоустойчивых кодов/ В.Д. Гоппа // Проблемы передачи информации, т.6 , №3, 1970. - С. 24 – 30.
34. Стандартные разрешения и форматы видео [Электронный ресурс] – Режим доступа – http://pctuner.ru/page-id-2127.html.
35. Delsarte, Ph. Orthogonal polynomial matrices on the unit circle / Ph. Delsarte, Y. Genin and Y. Kamp // IEEE Trans. Circuits Systems 25 (3) (1978) 149-160.
36. Dur/m, A.J. Orthogonal matrix polynomials and higher order recurrences / A.J. Dur/m and W. Van Assche // Linear Algebra Appl. 219 (1995) 261-280.
37. Geronimo, J.S. Matrix orthogonal polynomials on the unit circle/ J.S. Geronimo // J. Math. Phys. 22 (7) (1981) 1359-1365.
38. Espafiol, F. M. A class of matrix orthogonal polynomials on the unit circle / F. M. Espafiol, I. R. Gonz/flez // Linear Algebra Appl. 121 (1989) 233-241.
39. Guterman, A. New matrix partial order based on spectrally orthogonal matrix decomposition/ A. Guterman, A. Herrero, N. Thome, // Linear and Multilinear Algebra 64(3):1-13 · May 2015
40. Шеремет, И.А. Обработка изображений с помощью целочисленных ортогональных преобразующих матриц/ И.А. Шеремет, В.Д. Лебедев, А.П. Рукин, // Цифровая обработка сигналов. 2014. № 4. С. 45-52.
41. Мазурова, Т.А. О генерации ортогональных матриц произвольной силы / Т.А. Мазурова, А.Г. Чефранов, // Известия ЮФУ. Технические науки, №1 (24) 2002г., стр.: 81-82
42. Shepard, R. The Representation and Parametrization of Orthogonal Matrices/ R. Shepard, S. R. Brozell, G. Gidofalvi // The Journal of Physical Chemistry A 119(28) · May 2015
43. Hoffman, D. K. Generalization of Euler Angles to N- Dimensional Orthogonal Matrices/ D. K. Hoffman, R. C. Raffenetti, K. Ruedenberg // Journal of Mathematical Physics 13(4), April 1972, pp:528-533.
44. Lee, M. H. A new reverse Jacket transform and its fast algorithm/ M. H. Lee // IEEE Transactions on circuits and systems II, 47(2000). pp. 39-47.

45. Lee, M. H. Jacket Matrices: Constructions and Its Applications for Fast Cooperative Wireless Signal Processing/ M. H. Lee // LAP LAMBERT Publishing, Germany, 2012.
46. Lee, M. H. Simple systolic array for hadamard trans-form / M. H. Lee, Y. Yasuda, // Electron. Lett., vol. 26, no. 18, pp. 1478–1480, Aug. 30, 1990.
47. Lee, M. H. Jacket Matrices constructed from Hadamard Matrices and Generalized Hadamdrd Matrices/ K. Finlayson, M. H. Lee, J. Seberry, M. Yamada // Australasian Journal of Combinatorics, 35 (2006). pp.83-87.
48. Frank, J H. G-matrices, J-orthogonal matrices, and their sign patterns/ Frank J Hall, R. Miroslav // Czechoslovak Mathematical Journal 66(3), September 2016, pp:653-670.
49. Fiedler, M. More on G-matrices/ M. Fiedler, T. L. Markham // Linear Algebra and its Applications 438(1), January 2013, pp:231–241.
50. RozložnÍk, M. Cholesky-Like Factorization of Symmetric Indefinite Matrices and Orthogonalization with Respect to Bilinear Forms/ M. RozložnÍk, F. Okulicka-DŁużewska, A. Smoktunowicz // SIAM Journal on Matrix Analysis and Applications 36(2), April 2015, pp:727-75.
51. Fiedler, M. G-matrices/ M. Fiedler, F. J. Hall //Linear Algebra and its Applications 436(3) · February 2012.
52. Higham, N. J. J-Orthogonal Matrices: Properties and Generation / N. J. Higham // SIAM Review 45(3) · September 2003
53. Shepard, R. The Representation and Parametrization of Orthogonal Matrices / R. Shepard, S. R. Brozell, G. Gidofalvi //The Journal of Physical Chemistry A 119(28) · May 2015
54. Khan, F. H. Hill Cipher Key Generation Algorithm by using Orthogonal Matrix / F. H. Khan, R. Shams, F. Qazi, // International Journal of Innovative Science and Modern Engineering (IJISME), Volume-3 Issue-3, February 2015, p: 5-7
55. Liu, R. Two Types of Special Bases for Integral Lattices / R.Liu, Y. Pan, // Information Security Applications, January 2016, pp.87-95
56. Khan, F. H. Advance Procedure Of Encryption And Decryption Using Transposition And Substitution / F. H. Khan, F. Qazi // Journal of Computer

Science of Newports Institute of Communications and Economics Volume 6, Issue-2015, p: 39-51

57. Gupta, K. C. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications/ K. C. Gupta, I. G. Ray // Cryptography and Communications 7(2) · June 2015
58. Kumar, A. S. A Three Factor Authentication System for Smartcard Using Biometric / A. S. Kumar, K. P. Girish // Visual Cryptography and OTP, Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, January 2015, pp.673-679,
59. Cariow, A. An algorithm for discrete fractional Hadamad transform with reduced arithmetical complexity / A. Cariow, D. Majorkowska-Mech // Przeglad Elektrotechniczny R88(11a/2012), September 2013, pp:70-76
60. Xu, Z. On the provably secure CEW based on orthogonal decomposition / Z. Xu, L.Xiong, X. Yanyan // Signal Processing Image Communication 29(5) · January 2013
61. Song, W. Quasi-Orthogonal Space-Time Block Codes Designs Based on Jacket Transform / W. Song, M. H. Lee, M. M. Matalgah, Y. Guo // Journal of Communications and Networks 12(3), June 2010, pp:240-245.
62. Zhang, I. Nearest orthogonal matrix representation for face recognition/ I. Zhang, J. Yang, J. Qian, J. Xu // Neurocomputing 151(1), March 2015,pp:471–480
63. Defez, E. Computing Hyperbolic Matrix Functions Using Orthogonal Matrix Polynomials/ E. Defez, J. S. Martínez, J. J. Ibáñez, P. A. Ruiz // Progress in Industrial Mathematics at ECMI 2012, pp.403-407
64. Балонин, Н. А. М-матрицы / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2011. № 1(50). С. 14–21.
65. Балонин, Ю. Н. Алгоритм и программа поиска и исследования М-матриц / Ю. Н. Балонин, М. Б. Сергеев // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3(64). С. 82–86.
66. Балонин, Ю. Н. М-матрица 22-го порядка/ Ю. Н. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2011. № 5(54). С. 87–90.

67. Балонин, Н. А. Вычисление матриц Адамара — Мерсенна / Н. А. Балонин, М. Б. Сергеев, Л. А. Мироновский // Информационно-управляющие системы. 2012. № 5(60). С. 92–94.
68. Балонин, Н. А. Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2013. № 5(66). С. 97–98.
69. Балонин, Н. А. Матрица золотого сечения G10 / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2013. № 6(67). С. 2–5.
70. Балонин, Н. А. О существовании матриц Мерсенна 11-го и 19-го порядков / Н. А. Балонин // Информационно-управляющие системы. 2013. № 2(63). С. 89–90.
71. Балонин, Н. А. К вопросу существования матриц Мерсенна и Адамара / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.
72. Балонин, Н.А. Матрицы локального максимума детерминанта / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2014. №1 (68). С.2-15
73. Сергеев, А. М. Обобщенные матрицы Мерсенна и гипотеза Балонина / А. М. Сергеев // Автоматика и вычислительная техника. 2014. № 4. С. 35–43.
74. Балонин, Н. А. Вычисление матриц Адамара — Ферма / / Н. А. Балонин, М. Б. Сергеев, Л. А. Мироновский // Информационно-управляющие системы. 2012. № 6(61). С. 90–93.
75. Балонин, Н. А. О двух способах построения матриц Адамара — Эйлера / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. 2013. № 1(62). С. 7–10.
76. Wang, Z. Image Quality Assessment: From Error Visibility to Structural Similarity/ Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, // IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, pp. 600-612, APRIL 2004
77. Wang, Z. MULTI-SCALE STRUCTURAL SIMILARITY FOR IMAGE QUALITY ASSESSMENT / Z. Wang, E. P. Simoncelli, A. C. Bovik // 37th IEEE

Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, Nov. 9-12,2003

78. Thyagarajan, K. S. Still Image and Video Compression with MATLAB / K. S. Thyagarajan // Wiley, 2011, 428s
79. Bhelke, G. P. Detection of noise in degraded Images by efficient noise detection algorithm: A Survey / G. P. Bhelke, M. V. Sarode, H. B. Nadiyana // International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 2, Issue 4, April 2013, p. 359 – 363.
80. Приоров, А.Л. Цифровая обработка изображений: учебное пособие / А.Л. Приоров, И.В. Апальков, В.В. Хрящев // гос. ун-т. – Ярославль: ЯрГУ, 2007. – 235 с.
81. 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.
82. Чернышев, С.А. Исследование влияния порядка маскирующей матрицы на эффективность сжатия изображения матрицы / А.А. Востриков, С.А. Чернышев // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2013. – с. 109-112.
83. Chernyshev, S. A. Implementation of Novel Quasi-Orthogonal Matrices for Simultaneous Images Compression and Protection / A. A. Vostrikov, S. A. Chernyshev // Smart Digital Futures 2014. Intelligent Interactive Multimedia Systems and Services (IIMSC-2014), IOS Press, 2014. pp. 451–461.
84. Salomon, D. Handbook of Data Compression / D. Salomon, G. Motta // N.Y., Springer-Verlag, 2010, pp. 399–410.
85. Ziv, J. A Universal Algorithm for Sequential Data Compression / J. Ziv, A. Lempel. // IEEE Transactions on Information Theory, 23(3), pp.337-343, May 1977.
86. Huffman, D.A. A Method for the Construction of Minimum-Redundancy Codes / D.A. Huffman // Proc. I.R.E, 1965, pp. 1098-1101.
87. Zlib Software [Электронный ресурс] – Режим доступа – http://www.zlib.net/.
88. Databases or Datasets for Computer Vision Applications and Testing [Электронный ресурс] – Режим доступа – http://datasets.visionbib.com/.

89. The Berkeley Segmentation Dataset and Benchmark [Электронный ресурс] – Режим доступа – https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/bsds/.
90. Test Image [Электронный ресурс] – Режим доступа – http://decsai.ugr.es/cvg/dbimagenes/.
91. Apollo 16 Image Library [Электронный ресурс] – Режим доступа – https://www.hq.nasa.gov/alsj/a16/images16.html.
92. Image Databases [Электронный ресурс] – Режим доступа – http://www.imageprocessingplace.com/root_files_V3/image_databases.htm.
93. The USC-SIPI Image Database [Электронный ресурс] – Режим доступа – http://sipi.usc.edu/database/.
94. Чернышев, С.А. О восстановлении маскированного изображения при возникновении информационных потерь в процессе передачи/ А.А. Востриков, С.А. Чернышев // Научная сессия ГУАП: сб. докл.: В 3 ч. Ч. II. Технические науки / СПб СПб.:ГУАП., 2014. – с. 185-190.
95. Чернышев, С.А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами/ А.А. Востриков, С.А. Чернышев // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99-103.
96. 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.;
97. Алгоритмы хеширования данных, Академия Microsoft: Структуры и алгоритмы компьютерной обработки данных [Электронный ресурс] – Режим доступа – http://www.intuit.ru/studies/courses/648/504/lecture/11467.
98. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер // Триумф, 2002 г. - 816 стр.
99. Стандарт шифрования данных – Data Encryption Standard [Электронный ресурс] – Режим доступа – http://protect.htmlweb.ru/des.htm.
100. RC2 [Электронный ресурс] – Режим доступа – https://en.wikipedia.org/wiki/RC2.

101. RC5 [Электронный ресурс] – Режим доступа – https://en.wikipedia.org/wiki/RC5.
102. ГОСТ 28147-89 [Электронный ресурс] – Режим доступа – http://www.certisfera.ru/uploads/28147-89.pdf.
103. Advanced Encryption Standard [Электронный ресурс] – Режим доступа – https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard.
104. Алгоритм шифрования данных IDEA [Электронный ресурс] – Режим доступа – http://protect.htmlweb.ru/idea.htm.
105. Daemen, J. A New Approach to Block Cipher Design, Fast Software Encryption (FSE) / J. Daemen; R. Govaerts; J. Vandewalle, // Springer-Verlag. 1993, pp. 18–32.
106. Triple DES [Электронный ресурс] – Режим доступа – https://ru.wikipedia.org/wiki/Triple_DES.
107. Blowfish (cipher) [Электронный ресурс] – Режим доступа – https://en.wikipedia.org/wiki/Blowfish_(cipher).
108. Чернышев, С.А. Цифровое маскирование матрицами Мерсенна и его особые изображения / Ю.Н. Балонин, А.А. Востриков, Е.А. Капранова, А.М. Сергеев, О.И. Синицына, С.А. Чернышев // Фундаментальные исследования. – 2017. – № 4-1. – С. 13-18;
109. 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.
110. Свидетельство о государственной регистрации программы для ЭВМ № 2015611310 от 27 января 2015 г. «Специальное программное обеспечение для демаскирования изображений методом матричных целочисленных преобразований в квазиортогональных базисах» // А. А. Востриков, Н.В. Соловьев, М.Б. Сергеев, С. А. Чернышев, 2015 г.
111. 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.

112. 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 квазиортого-нальных матриц» // А. А. Востриков, Н. А. Балонин, М.Б. Сергеев, С. А. Чернышев, 2015 г.
113. Jang Ju-Wook Energy- and Time-Efficient Matrix Multiplication on FPGAs / Ju-Wook Jang, S. B. Choi, V. K. Prasanna // IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 13, NO. 11, NOVEMBER 2005 p. 1305 – 1319
114. Lee Tai-Chi Matrix Multiplication on FPGA-Based Platform / Tai-Chi Lee, M. White, M. Gubody // Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I
115. Jamro, E. The algorithms for fpga implementation of sparse matrices multiplication / E. Jamro, T. Pabi´s, P. Russek, K. Wiatr // Computing and Informatics, Vol. 33, 2014, 667–684
116. Qasim, S. M. FPGA Design and Implementation of Matrix Multiplier Architectures for Image and Signal Processing Applications / S. M. Qasim, A. A. Telba, A. Y. AlMazroo // IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010, p. 168 – 176
117. Qasim, S. M. A Proposed FPGA-based Parallel Architecture for Matrix Multiplication / S. M. Qasim, S. A. Abbasi, B. Almashary // Circuits and Systems, 2008. APCCAS 2008. IEEE Asia Pacific Conference on, p.1763 – 1766
118. Tiwari, S. Efficient Hardware Design for Implementation of Matrix Multiplication by using PPI-SO / S. Tiwari , N. Meena // International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2013 p. 1020 - 1024
119. Sohl, J. Large Matrix Multiplication on a Novel Heterogeneous Parallel DSP Architecture / J. Sohl, J. Wang, D. Liu // International Workshop on Advanced Parallel Processing Technologies 2009: Advanced Parallel Processing Technologies pp 408-419

120. Wunderlich, R. E. Accelerating Blocked Matrix-Matrix Multiplication using a Software-Managed Memory Hierarchy with DMA / R. E. Wunderlich, M. Püschel, J. C. Hoe // Signal and Image Processing (SIP 2003), Proceedings of the IASTED International Conference, August 13-15, 2003, Honolulu, HI, USA
121. Petrinovic, D. Implementation of sparse matrix arithmetic on a dsp processor / D. Petrinovic, I. Lukacevic, D. Petrinovic // Signal and Image Processing (SIP 2003), Proceedings of the IASTED International Conference, August 13-15, 2003, Honolulu, HI, USA
122. Chernyshev, S. Digital masking using Mersenne matrices and its special images / A. Vostricov, M. Sergeev, N. Balonin, S. Chernyshev // Procedia Computer Science. Volume 112, Elsivier, 2017, Pages 1151-1159
123. 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» // Д. В. Бодня, А. А. Востриков, Ю. Н. Балонин, С. А. Чернышев, А. М. Сергеев, 2017

ПРИЛОЖЕНИЕ А

АКТЫ О ВНЕДРЕНИИ

"У Т В Е Р Ж Д А Ю "

Генеральный директор
ООО «АСК Лаборатория»
канд. техн. наук, доцент

Востриков А.А.
"01" августа 2017 г.

А К Т

об использовании результатов диссертационной работы
Чернышева Станислава Андреевича, представляемой на соискание ученой степени кандидата технических наук.

Комиссия в составе:
главного инженера Чудиновского Юрия Геннадьевича
ведущего инженера Анисимова Андрея Леонидовича
инженера-программиста Егоровой Ирины Сергеевны

составила настоящий акт об использовании результатов диссертационной работы Чернышева С.А. в рамках опытно-конструкторской работы, выполняемой по договору №1/14 от 14.01.2014г. на создание опытных образцов электронных модулей видеорегистратора специального назначения.

Разработанные автором диссертационной работы технические решения применяются в настоящее время Заказчиком работы для серийного производства специализированных видеорегистраторов, обеспечивающих удаленный мониторинг поступающего видеосигнала и беспроводной съём выполняемых видеозаписей на подвижных объектах.

Предложенный автором метод матричного преобразования кадров видео последовательности реализован программно в системе-на-кристалле с DSP-сопроцессорами (ADSP-BF523KBCZ и других).

Проведенные исследования показали, что метод и выбранный для него квазиортогональный базис при беспроводной передаче в условиях существования активных помех позволяют эффективно обнаруживать потери

блоков данных, а также значительно снизить их влияние на содержимое кадров видеопоследовательности, что существенно повышает устойчивость функционирования видеосистем, построенных на базе предложенного технического решения.

Члены комиссии

Егорова И.С.

Чудиновский Ю.Г.

Анисимов А.Л.

«У Т В Е Р Ж Д А Ю»

Проректор по учебно-
воспитательной работе ГУАП
доктор юридических наук, профессор

_____ В.М. Боер
"15" _____ 2017 г.

А К Т

об использовании результатов диссертационной работы
Чернышева Станислава Андреевича, представляемой на соискание ученой степени кандидата технических наук.

Комиссия в составе:
доктор технических наук, доцент, профессор кафедры вычислительных систем и сетей Балонин Николай Алексеевич;
кандидат технических наук, доцент, доцент кафедры вычислительных систем и сетей Соловьев Николай Владимирович;
кандидат технических наук, доцент, доцент кафедры безопасности информационных систем Овчинников Андрей Анатольевич

составила настоящий акт о том, что результаты диссертационной работы Чернышева С.А. «Разработка и исследование метода матричного маскирования видеоинформации в глобально распределенных системах», выполненной на кафедре вычислительных систем и сетей федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», внедрены в учебный процесс:

1) на кафедре вычислительных систем и сетей в дисциплинах, включенных в программы подготовки по направлению «Информатика и вычислительная техника» (бакалавриат – 09.03.01 и магистратура – 09.04.01):

- «Проектирование систем обработки и передачи информации» (Лабораторная работа «Реализация матричных операций в ПЛИС для обработки визуальной информации»);
- «Цифровая обработка изображений» (Лабораторная работа «Матричные способы обработки изображений»);
- «Специализированные микропроцессорные системы» (Лабораторная работа «Эффективная реализация матричных операций в программно-управляемых вычислителях»).

2) на кафедре безопасности информационных систем в лекционном курсе дисциплины «Технологии стеганографии в системах инфокоммуникаций», включенной в программу подготовки по направлениям 10.03.01 – «Информационная безопасность» и 11.04.02 – «Инфокоммуникационные технологии и системы связи».

Члены комиссии

Н. А. Балонин

Н. В. Соловьев

А. А. Овчинников

ПРИЛОЖЕНИЕ Б

СВИДЕТЕЛЬСТВА

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015611308

Специальное программное обеспечение для маскирования изображений методом матричных целочисленных преобразований в квазиортогональных базисах

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

Авторы: ***см. на обороте***

Заявка № **2014662299**
Дата поступления **01 декабря 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 января 2015 г.***

Врио руководителя Федеральной службы по интеллектуальной собственности

Л.Л. Кирий

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015611309

Специальное программное обеспечение демаскирования изображений матричными преобразованиями в формате с плавающей запятой с использованием квазиортогональных матриц

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

Авторы: ***см. на обороте***

Заявка № **2014662301**
Дата поступления **01 декабря 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 января 2015 г.***

Врио руководителя Федеральной службы по интеллектуальной собственности

Л.Л. Кирий

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015611310

Специальное программное обеспечение для демаскирования изображений методом матричных целочисленных преобразований в квазиортогональных базисах

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

Авторы: ***см. на обороте***

Заявка № **2014662302**
Дата поступления **01 декабря 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 января 2015 г.***

Врио руководителя Федеральной службы по интеллектуальной собственности

Л.Л. Кирий

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015611311

Специальное программное обеспечение маскирования изображений матричными преобразованиями в формате с плавающей запятой с использованием квазиортогональных матриц

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

Авторы: ***см. на обороте***

Заявка № **2014662305**
Дата поступления **01 декабря 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***27 января 2015 г.***

Врио руководителя Федеральной службы по интеллектуальной собственности

Л.Л. Кирий

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2017616795

Специальное программное обеспечение для приема по беспроводному каналу, декодирования, демаскирования с использованием квазиортогональных матриц, декомпрессии и воспроизведения видеоизображений с малым временем актуальности

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

Авторы: ***см. на обороте***

Заявка № **2017613820**
Дата поступления **24 апреля 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***14 июня 2017 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Авторы: ***Бодня Дмитрий Викторович (RU), Востриков Антон Александрович (RU), Балонин Юрий Николаевич (RU), Чернышев Станислав Андреевич (RU), Сергеев Александр Михайлович (RU)***