Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный университет им. Ф.М. Достоевского»

На правах рукописи

ВИЛЬХОВСКИЙ Данил Эдуардович

АЛГОРИТМЫ СТЕГАНОГРАФИЧЕСКОГО АНАЛИЗА ИЗОБРАЖЕНИЙ С НИЗКИМ ЗАПОЛНЕНИЕМ СТЕГОКОНТЕЙНЕРА

Специальность 05.13.19 — Методы и системы защиты информации, информационная безопасность

Диссертация на соискание учёной степени кандидата технических наук

Научный руководитель
доктор физико-математических наук,
профессор Гуц А.К.

Омск – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования

Проблема выявления стеганографических вставок (СГВ), получившая название стеганографического анализа или стегоанализа, является важной составляющей построения комплексной системы защиты информации, так как решает сразу несколько задач построения защищенных информационных систем. Прежде всего, стеганографические методы передачи информации используются для скрытой передачи данных в различных файлах, обладающих избыточностью. Наибольшее распространение в качестве контейнеров получили медиафайлы. В качестве медиафайлов могут быть использованы аудиофайлы, видеофайлы, или изображения. Однако последние представляют наибольший интерес для нашего исследования, поскольку обмен изображениями имеет значительно большую частоту по сравнению с обменом других аудиофайлов. Так, например, пользователи активно пересылают друг другу изображения в различных мессенджерах и социальных сетях. Кроме того, контент, который выкладывается на страницах веб-сайтов, содержит помимо текстовой части именно изображения как один из мощных триггеров и факторов привлечения внимания.

Обнаружение стеганографических вставок позволяет выявлять скрытые каналы передачи информации. Кроме этого, на стеганографических алгоритмах основаны методы внедрения цифровых водяных знаков. Цифровые водяные знаки используются для подтверждения авторства документа и обнаружения несанкционированного копирования данных. Методы стегоанализа позволяют тестировать скрытость и устойчивость цифровых водяных знаков, а также определять области изображений, встраивание в которые позволяет повысить устойчивость цифрового водяного знака.

Основным требованием к СГВ является скрытность и устойчивость. Под скрытностью понимается невозможность обнаружения встроенных данных без дополнительной информации о параметрах встраивания. В избыточный медиафайл

встраивается сообщение таким образом, что сам файл, являющийся обложкой для передаваемого скрытого сообщения, не претерпевает изменений, влияющих на его визуальное отображение (для изображений и видеофайлов) или аудио восприятие (для аудиофайлов). В данном случае речь идет о том, что контейнер по-прежнему выполняет свое функциональное предназначение без изменения своих внешних свойств, а встроенное изображение не подлежит детекции ни визуально ни на слух.

Основной целью стеганографического анализа (стегоанализа) является оценка уровня скрытности сообщения.

Перед стегоанализом ставятся три задачи. Первая задача состоит в установлении факта встраивания или отсутствия встраивания информации. Большинство современных алгоритмов стегоанализа решает именно эту задачу.

Алгоритмы стегоанализа можно разделить на общие и специализированные. Общие алгоритмы предназначены для обнаружения факта встраивания без уточнения метода встраивания. Общие алгоритмы основываются на некоторых предположениях о статистических характеристиках исходного изображения, которые изменяются при внедрении СГВ. Современные общие алгоритмы стегоанализа эффективны, если объем СГВ составляет не менее 40% от максимально возможного. Это вызвано объективными закономерностями, когда большее заполнение стегоконтейнера влечет за собой большее изменение статистических характеристик, что позволяет стегоанализу преодолеть порог статистической погрешности используемого алгоритма и, следовательно, получать более достоверные результаты при классификации изображения. В данном случае речь идет, прежде всего, о снижении числа ложно-негативных значений, когда стего-изображение ошибочно классифицируется как чистое, а ошибки классификации вызваны тем фактом, что выявленное изменение статистических характеристик анализируемого медиафайла определяется как статистически незначимое.

Большой вклад в развитие методов стегоанализа внесли: Н. Провос (N. Provos), Д. Фридрич (J. Fridrich), К. Салливан (K. Sullivan), Х. Фарид (H. Farid), Р.

Андерсон (R. Anderson), К. Качин (C. Cachin), А.Н. Фионов, И.В. Туринцев, Б.Я. Рябко, И.Н. Оков, В.Г. Грибунин, и пр.

Специализированные алгоритмы стегоанализа жестко привязаны к методу встраивания. В этом случае сначала делается предположение об используемом стеганографическом методе, после чего выполняется проверка наличия встроенных данных.

Вторая и третья задачи стеганографического анализа состоят в определении параметров алгоритма встраивания и извлечении встроенного сообщения с максимальной точностью. Решение третьей задачи тесно связано с и невозможно без решения второй задачи. Определение параметров алгоритма встраивания позволяет выявить области встраивания с большей степени точности, чем простое угадывание, и тем самым обеспечить успешное извлечение скрытого сообщения минимизировав потери, вызванные неполным захватом области встраивания. Следует отметить, что для второй и третьей задач стегоанализа невозможно построение общих алгоритмов. На сегодняшний день для большинства методов стеганографического встраивания не разработаны специализированные алгоритмы, решающие вторую и третью задачи. Существующие же алгоритмы обладают невысокой точностью. В связи с чем разработка новых специализированных алгоритмов стегоанализа является актуальной.

Как было отмечено ранее, существующие алгоритмы стегоанализа основаны на статистических методах и эффективны только при заполнении стегоконтейнера более чем на 40%. При более низких показателях заполнения вероятность обнаружения наличия СГВ не превышает 30% [104]. Этот недостаток обусловлен предположением о существенном изменении статистических свойств изображения при встраивании сообщения. Если заполнение стегоконтейнера не превышает 25%, то статистические характеристики изображения со СГВ отличаются от исходного изображения не более чем на 7%, что сопоставимо с погрешностями используемого метода [25, 88, 107]. Данный недостаток существующих методов стегоанализа активно используются в стеганографии в целях повышения уровня скрытности как

одного из требований ко стеганографическим вставкам, в результате чего наблюдается тенденция к снижению уровня рабочей нагрузки при встраивании сообщения как способ противостояния стего-атакам. При этом использование всего 10 – 30% от общего объема стегоконтейнера свободно компенсируется увеличением количества используемых медиафайлов, что позволяет, в конечном итоге передавать большие объемы информации.

Кроме этого, статистические методы не позволяют определять положение области встраивания на изображении и ее размер. Следовательно, вторая и третья задачи стегоанализа остаются нерешенными. Однако, в рамках повышения информационной безопасности важным является не только предотвращение факта передачи данных, но и отслеживание центров фокусного внимания как наиболее частых векторов атак, что невозможно без знания того, какие конкретно данные содержит встроенное сообщение. Таким образом, задача разработки алгоритмов стегоанализа является актуальной для изображений с низким заполнением стегоконтейнера, а также алгоритмов, определяющих положение и размеры СГВ.

Существует достаточно большое количество алгоритмов стеганографического встраивания как в пространственную, так и в частотную области изображения.

Являясь исторически первым методом стеганографии и обладая относительной простотой и высокой производительностью алгоритмов, наибольшее распространение для пространственной области встраивания получили алгоритмы, основанные на методе замены наименее значащего бита (LSB-замены). Эти методы используются при выборе изображения-стегоконтейнера в растровом формате, например, BMP или PNG. При этом, поскольку LSB-замена может быть достаточно простой для обнаружения современными инструментами стегоанализа, а следовательно, в целом, скрытность встраиваемой информации недостаточно высока для данного метода, низкое заполнение стегоконтейнера является одним из наиболее активных мер,

используемых для повышения уровня скрытности СГВ как простая альтернатива разработки более сложных алгоритмов встраивания.

Для частотной области встраивания наиболее распространены алгоритмы с использованием дискретного косинусного преобразования, основанные на алгоритме Коха-Жао. Данные алгоритмы обеспечивают наибольшую скрытность встраиваемой информации, что обуславливает их высокую распространенность при передаче информации. Эти методы совместимы с изображениями в формате JPEG. В то же время, низкое заполнение стегоконтейнера также активно используется для алгоритмов, основанных на дискретном косинусном преобразовании в целях достижения максимальной степени скрытности и предотвращения тем самым обнаружения стеганографических вставок. В связи с этим актуальной является задача стеганографического анализа этих двух базовых алгоритмов (LSB-замены и Коха-Жао) при условии низкого заполнения стегоконтейнера.

Степень разработанности темы

Большой вклад в развитие методов стегоанализа внесли: Н. Провос (N. Provos), Д. Фридрич (J. Fridrich), К. Салливан (K. Sullivan), Х. Фарид (H. Farid), Р. Андерсон (R. Anderson), К. Качин (C. Cachin), А.Н. Фионов, И.В. Туринцев, Б.Я. Рябко, И.Н. Оков, В.Г. Грибунин, и пр. Однако анализ современных исследований в области стеганографического анализа говорит о том, что, наряду с имеющимися алгоритмами, недостаточно разработаны специализированные алгоритмы для изображений с низким заполнением стегоконтейнера.

Цель работы

Целью диссертации является повышение эффективности работы методов стеганографического анализа для изображений с низким заполнением стегоконтейнера.

Для достижения поставленной цели были решены **задачи**:

1. Разработка алгоритма стегоанализа метода LSB-замены при низком заполнении стегоконтейнера на основе анализа битового нулевого слоя с применением алгоритма таксономии.
2. Разработка алгоритма стегоанализа метода LSB-замены при низком заполнении стегоконтейнера на основе сравнительного анализа нескольких битовых слоев с применением метода анализа иерархий.
3. Разработка алгоритма стегоанализа метода Коха-Жао на основе анализа коэффициентов дискретного косинусного преобразования.
4. Программная реализация разработанных алгоритмов и их тестирование.

Объект исследования

Объект исследования – изображения с низким уровнем заполнения стегоконтейнера (<40%), встраивания в которые осуществлялись с помощью методов LSB-замены и Коха-Жао.

Предмет исследования

Предметом исследования являются алгоритмы обнаружения и извлечения сообщений, встроенных в изображения методами LSB-замены и Коха-Жао, при низком заполнении стегоконтейнера.

Методы исследования

Чтобы решить данный комплекс задач, использовались методы поддержки принятия решений, численные методы исследования функций, методы таксономии. Также использовались методы математической статистики и теории вероятностей, теории информационной безопасности и защиты информации.

Основные положения, выносимые на защиту

1. Алгоритм анализа нулевого слоя цифрового изображения на наличие LSB-вставок с использованием метода таксономии.
2. Алгоритм анализа цифрового изображения на наличие LSB-вставок с использованием метода анализа иерархий.
3. Алгоритм анализа цифрового изображения на наличие вставок методом Коха-Жао на основе анализа коэффициентов дискретного косинусного преобразования.

4. Программный комплекс, реализующий предложенные алгоритмы.

Научная новизна

1. Предложен алгоритм стеганографического анализа методом LSB-замены при низком заполнении стегоконтейнера, основанный на анализе нулевого слоя с применением метода таксономии, *отличающийся* наличием модуля предварительной обработки изображения (линейное преобразование), позволяющего выделить области градиентной заливки, и блока автоматического поиска границ встраиваний на базе алгоритма таксономии FOREL, что дает возможность не только обнаружить встроенное сообщение, но и определить его положение и размер.

2. Предложен алгоритм стеганографического анализа метода LSB-замены при низком заполнении стегоконтейнера, основанный на сравнительном анализе нескольких слоев изображения с помощью метода анализа иерархий, *отличающийся* тем, что выделенные критерии принятия решения представляют возможность учитывать структуру исходного изображения-контейнера, которая хранится в более высоких битовых слоях, и за счет этого представляется возможным сформировать карту подозрительных пикселей, повышающую эффективность обнаружения встроенного сообщения.

3. Предложен алгоритм стеганографического анализа метода Коха-Жао, основанный на анализе коэффициентов дискретного косинусного преобразования, *отличающийся* присутствием модуля автоматического поиска ступенчатых изменений, который позволяет определить параметры встраивания и извлечь сообщение.

4. Разработан программный комплекс, позволяющий проводить стегоанализ изображений с внедренными данными методом LSB-вставки и методом Коха-Жао. Программный комплекс имеет Свидетельства о государственной регистрации программ для ЭВМ №2017661544 от 16.10.2017, №2018617635 от 03.08.2018, №2018617407 от 28.08.2018.

Практическая и научная значимость результатов

Научная значимость результатов заключается в создании новых алгоритмов стеганографического анализа цифровых изображений, позволяющих определять параметры встраивания для стеганографических методов LSB-вставки и Коха-Жао при низком заполнении стегоконтейнера.

Практическая значимость результатов заключается в том, что разработанный программный комплекс позволяет проводить стегоанализ изображений с данными, встроенными методом LSB-вставки и методом Коха-Жао, при низком заполнении стегоконтейнера (менее чем 40% битов нулевого битового слоя). При стегоанализе изображения со встраиванием методом LSB факт наличия стеганографической вставки определяется с эффективностью 95% при заполнении стегоконтейнера от 10% до 30%. Разработанный алгоритм даёт возможность определять в среднем 91% заменённых битов для искусственных изображений, у которых градиентная и равномерная заливка. При этом ложных срабатываний не больше 1%.

При обработке фотографических изображений предлагаемым алгоритмом ложных срабатываний было порядка 37%, при этом было правильно обнаружено 89% пикселей (у найденных пикселей была произведена замена младшего бита).

При стегоанализе изображения со встраиванием методом Коха-Жао на коллекции BSDS500 показано, что ошибки ложного определения наличия СГВ в пустом стегоконтейнере составляют 23%. Эффективность обнаружения наличия встроенного сообщения составляет 85,5%.

Результаты диссертационного исследования внедрены в учебный процесс Омского государственного университета им. Ф.М. Достоевского, а также в деятельность ООО Строительно-монтажный трест «Стройбетон»: добавлена функция анализа базы данных изображений, хранящихся в системе, на наличие стеганографических вставок, что позволило существенно повысить уровень информационной защищенности внутреннего документооборота организации за счет возможности отслеживания наличия скрытого канала передачи данных при обработке изображений.

Апробация работы

Результаты работы проходили обсуждения на таких научных конференциях как: IV международная конференция «Математическое и компьютерное моделирование» (Омск, 2016), Всероссийская научная конференция «Анализ данных и моделирование» (Омск, 2016), V международная конференция «Математическое и компьютерное моделирование» (Омск, 2017), Всероссийская научная конференция «Данные, моделирование и безопасность» (Омск, 2017), IX Межрегиональная научно-практическая конференция «Информационная безопасность и защита персональных данных. Проблемы и пути их решения» (Брянск, 2017), Международная конференция «Динамика систем, механизмов и машин» (Омск, 2017), X Международная школа-конференция студентов, аспирантов и молодых ученых «Фундаментальная математика и ее приложения в естествознании» (Уфа, 2018).

Исследования поддержаны грантом молодых ученых ОмГУ им. Ф.М. Достоевского в 2018 году.

Соответствие паспорту специальности

Содержание диссертации соответствует пункту 6 паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» – Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

Степень достоверности результатов работы

Обоснованность полученных результатов состоит в адекватности используемых методов: они имеют подтверждение данными, которые были получены в ходе тестирования алгоритмов, государственной регистрацией программ для ЭВМ, а также внедрением в деятельность ООО Строительно-монтажный трест «Стройбетон» для анализа базы данных изображений, хранящихся в системе, на наличие стеганографических вставок.

Личный вклад соискателя

В диссертации используются результаты, в получении которых основная роль при постановке и решении задач, а также обобщении полученных данных принадлежит автору. В соавторстве с Белимом С.В написан ряд публикаций.

Публикации

Материалы диссертации опубликованы в 14 изданиях, из них 6 статей в журналах из перечня, рекомендованного ВАК, 4 статьи в изданиях, индексируемых в базе Scopus, 4 публикации в материалах конференций и 3 свидетельства о регистрации программ для ЭВМ.

Структура и объем диссертации

Диссертация содержит: введение, 4 главы, заключение, библиографический список и 5 приложений. Общий объем диссертации 135 страниц. Библиографический список состоит из 134 источников.

Во **введении** обосновывается актуальность выбранной темы диссертационного исследования, характеризуется степень её разработанности, определяются цели и задачи, осуществляется выбор предмета и объекта исследования, определяются методологические основания исследования, теоретическая и практическая значимость результатов исследования.

Первая глава носит обзорный характер, в ней приведены основные методы и алгоритмы стеганографического анализа изображений. Показаны основные численные характеристики методов стеганографического анализа, их основные преимущества и недостатки.

Во **второй главе** представлен алгоритм определения наличия, размеров и положения областей при стеганографическом встраивании в изображения методом LSB-замены на основе анализа нулевого и первого битового слоев. Алгоритм основан на том факте, что встраивание сообщения изменяет распределение нулевых и единичных битов в нулевом слое, которое наиболее заметно на областях равномерной и градиентной заливки.

В третьей главе представлен алгоритм выявления пикселей изображения, в которых произведена подмена наименее значащего бита при стеганографическом встраивании сообщения, на основе метода анализа иерархий. При построении алгоритма делается предположение о том, что закономерности, присутствующие в одном слое исходного изображения-контейнера, должны с высокой вероятностью повторяться в близлежащих слоях. Для поиска пикселей с замененным нулевым битом анализируется нулевой слой и ближайшие к нему три слоя синей компоненты.

В **четвертой главе** представлен алгоритм выявления стеганографических вставок в изображение, встраиваемых с помощью метода Коха-Жао. В диссертации рассмотрен случай, когда встраивание производится в непрерывную область изображения и для всех блоков используется одинаковое значение M_0.

В **заключении** подводятся итоги диссертационного исследования, излагаются его основные выводы и обобщающие результаты.

ГЛАВА 1. МЕТОДЫ СТЕГАНОГРАФИИ И СТЕГОАНАЛИЗА

1.1 Стеганографические методы встраивания данных в изображения

Стеганография определяется как скрытое вложение данных в цифровые изображения. Стеганография позволяет скрывать информацию в любом из цифровых медиа, однако цифровые изображения являются самыми популярными стеганографическими контейнерами из-за их частого использования в Интернете [37]. Поскольку размер файла изображения достаточно велик, то объем встраиваемой информации также может быть большим. Визуально человеческий глаз не может легко отличить нормальное изображение от изображения со скрытыми данными. Цифровые изображения природы обычно содержат большое количество избыточных бит, что делает их наиболее популярными контейнерами для стеганографического встраивания.

Общая схема стеганографического встраивания может быть описана в терминах криптографических протоколов. Базовой моделью стеганографии и стегоанализа является проблема заключенного [102], в которой участвует три стороны: Алиса и Боб – двое заключенных, сотрудничающие для составления плана побега, при этом их связь контролируется начальником Венди. Используя метод встраивания данных $\boldsymbol{\Psi}(.)$, секретная информация $\boldsymbol{m}$ прячется Алисой в сообщение $\boldsymbol{X}$ с использованием ключа k_1. Передаваемое сообщение со встроенным сообщением $\boldsymbol{Y}$ можно описать как:

$$\boldsymbol{Y} = \Psi(\boldsymbol{X}, \boldsymbol{m}, k_1). \quad (1)$$

Боб получает сообщение Y' и использует метод извлечения данных $\Phi(.)$ для получения m' с использованием ключа k_2. Процесс извлечения данных может быть описан как:

$$m' = \Phi(Y', k_2). \quad (2)$$

Стеганографическая схема должна обеспечивать выполнение следующего равенства:

$$\boldsymbol{m'} = \boldsymbol{m}. \quad (3)$$

Хотя стеганографическая схема с публичными ключами рассматривается в некоторых источниках, стеганографическая схема с закрытыми ключами, где предполагается что $k_1 = k_2$, остается наиболее распространенным сценарием в стеганографической системе. Венди может быть активной или пассивной по изучению средств передачи информации. Если она внесет изменения и сделает $\boldsymbol{Y'} \neq \boldsymbol{Y}$ для предотвращения возможности скрытого общения Алисы и Боба, то она называется активным начальником. Если она принимает меры только тогда, когда $\boldsymbol{Y}$ выглядит подозрительным, она является пассивным надзирателем. В случае пассивного надзирателя, если Венди может отличить $\boldsymbol{Y}$ от $\boldsymbol{X}$, то стеганографический метод считается нарушенным.

Оценивать эффективность различных видов стеганографических методов принято на основе трех общих требований: безопасность, вместимость и незаметность.

Безопасность. Стеганографическая схема может подвергаться большому количеству активных или пассивных атак. Если существование секретного сообщения может быть оценено только с вероятностью, не превышающей случайное угадывание, то стеганографическая схема может считаться безопасной.

Вместимость. Схема передачи секретного сообщения будет эффективной, если она позволяет передавать большое количество скрытых данных. Вместимость может оцениваться как в абсолютном значении (размер секретного сообщения), так и в относительном (бит на пиксель, бит на ненулевой коэффициент дискретного косинусного преобразования или отношение встроенного сообщения к контейнеру).

Незаметность. Изображения со встроенными данными не должны иметь заметных визуальных изменений. При одинаковом уровне безопасности и вместимости, чем выше незаметность изображения, тем лучше. Если

результирующее изображение выглядит достаточно безобидным, можно полагать, что это требование выполнено при условии отсутствия оригинального изображения для сравнения.

1.2 Стегоанализ изображений

Под стегоанализом принято понимать методы определения наличия встроенных данных. Цель стегоанализа состоит в выработке методов, определяющих уязвимости стеганографических схем. Анализ угроз безопасности скрытой информации может принимать несколько форм, таких как обнаружение, извлечение или уничтожение скрытой информации. Злоумышленник может также вставлять противоречивую информацию по существующим скрытым данным. Эти подходы различаются в зависимости от методов, используемых для встраивания информации в контейнер. Изменения изображения-контейнера могут быть аномальными, что позволяет получить подсказку о скрытой информации. Без знания методов встраивания процесс поиска скрытой информации представляет значительную трудность. Некоторые из стеганографических методов имеют характеристики, которые действуют как их сигнатуры. Для стегоанализа используются различные методы обработки изображений, такие как обрезка, фильтрация и т.д. Пассивный стегоанализ просто повреждает изображение при возникновении какого-либо подозрения. Активный стегоанализ пытается найти алгоритм, чтобы выявить информацию и попытаться получить сообщение.

Проблема стегоанализа может быть математически сформулирована следующим образом. Обозначим $s(k)$ как сообщение контейнера, а через $w(k)$ – встраиваемое сообщение. Стегоконтейнер со встроенным сообщением:

$$y = s(k) + aw(k), k = 1,2, \dots, N \quad (4)$$

Если предположить, что $s(k)$ и $w(k)$ являются образцами из стационарного случайного вектора, то целью стегоанализа является найти оценки $s(k)$ и $w(k)$ для данной $y(k)$.

Алгоритм стегоанализа может как зависеть, так и не зависеть от стеганографического алгоритма. Исходя из этого, алгоритмы стегоанализа разделяются на два вида:

1. Конкретный стегоанализ

2. Общий или универсальный стегоанализ

Конкретный стегоанализ: стеганографический алгоритм известен и используется при проектировании алгоритма стегоанализа. Этот тип стегоанализа основан на анализе статистических свойств изображения, которые изменяются после внедрения. Преимущество использования конкретного стегоанализа заключается в точности результатов. Конкретный стегоанализ ограничен одним алгоритмом внедрения. Поэтому он не применим для всех типов алгоритмов. И он также не поддерживает все форматы изображений.

Общий, или универсальный, стегоанализ не зависит от алгоритма стеганографического встраивания. По сравнению с конкретным стегоанализом, универсальность является общей и менее эффективной. Тем не менее, универсальный стегоанализ широко используется. Универсальный стегоанализ включает в себя две фазы – выделение параметров изображения и классификация изображений в две разные группы.

Выделение параметров изображения — это процесс создания набора различных статистических атрибутов изображения. Параметры изображения должны быть чувствительны к объектам внедрения и метрикам качества изображения, а также к вейвлет-разложениям, моменту статистических гистограмм изображения, матрице эмпирического перехода Маркова, статистическим моментам изображения в пространственной и частотной областях, матрице совпадения и т.д.

Классификация изображений — это способ категоризации изображений в классы в зависимости от значений их признаков. Контролируемое обучение является одним из основных методов классификации в стегоанализе. В рамках стегоанализа ставится задача классификации изображений на чистые и содержащие СГВ. В основном используется обучение с учителем. Обучающий набор, включающий в себя параметры изображения, используется в качестве входных данных для обучения классификатора. После обучения определяется класс изображения исходя из его характеристик. В стегоанализе нашли применение следующие классификаторы: многомерная регрессия, линейный дискриминант Фишера (FLD), метод опорных векторов (SVM), искусственные нейронные сети (ANN).

Метод многомерной регрессии для классификации изображений использует регрессионный эффект. На этапе обучения коэффициенты регрессии прогнозируются с использованием минимальной среднеквадратической ошибки. Этот алгоритм эффективен, когда имеется в наличии большое количество образцов изображений для формирования обучающего множества.

Линейный дискриминант Фишера — это линейная комбинация функций, которая максимизирует значение разности между изображениями. В методе классификации многомерные функции проектируются в линейное пространство. Поскольку данный алгоритм использует линейный метод во время извлечения элементов и извлечения содержимого, то при его применении извлечение и сопоставление функций будут выполняться эффективно.

Метод опорных векторов— это популярный алгоритм контролируемого процесса обучения по набору образцов, то есть обучающему множеству. В этом алгоритме происходит обучение, после чего появляется возможность распознавать и назначать метки классов на основе заданного набора функций и объектов. В общем случае, SVM сводится к проблеме выбора разделяющей гиперплоскости.

Искусственные нейронные сети также широко используются для выделения изображений со СГВ [98, 120, 130]. Для обучения нейронных сетей используются

методы прямого и обратного распространения ошибки. Процесс классификации изображений разбивается на два этапа – обучение и тестирование. На этапе обучения нейронная сеть связывает выходы с заданными шаблонами ввода, изменяя веса входных аксонов. На этапе тестирования идентифицируется входной шаблон, и определяются весовые коэффициенты на выходе нейросети [50, 119, 125]. При этом, для целей стегоанализа могут применяться как различные подвиды нейронных (в частности, сверточных нейронных) сетей [11, 69, 126, 127], так и комбинация их с классическими моделями, например пространственной SRM-модели [131].

Квантовые протоколы являются перспективным направлением в стеганографии, их обзор представлен в статье [13].

При проведении стегоанализа подозрительного изображения возможны четыре случая:

1. Истинно положительный (TP) означает, что непустой стегоконтейнер был корректно определен.

2. Ложно-негативный (FN) означает, что непустой стегоконтейнер был определен как контейнер, который не содержит секретного послания.

3. Истинно негативный (TN) означает, что пустой контейнер был корректно определен.

4. Ложно-позитивный (FP) означает, что пустой контейнер был некорректно определен как стегоконтейнер.

Таким образом, современные методы стегоанализа, основанные на статистических признаках изображения, требуют использования классификаторов, параметры которых определяются с помощью обучающего множества. Причем обучающее множество должно быть достаточно большим. Эти требования существенно ограничивают область применимости указанных методов стегоанализа, так как позволяют выявлять только закономерности, характерные для обучающего множества. Если в качестве контейнера будет использовано оригинальное изображение, то статистический подход к стегоанализу может

обладать низкой эффективностью обнаружения вставок и высоким процентом ложных срабатываний.

1.3 Стеганографический алгоритм LSB-замены

Большое, если не сказать массовое, распространение получил метод по встраиванию стеганографических вставок – метод LSB-замещение (подмена самых незначащих бит). Данный метод использует некоторые особенности сетчатки наших глаз, а именно тот факт, что изменения в синей компоненте для глаз остаются почти что незаметными. Указанный метод осуществляет замену младших битов (1-4 бита) в байтах синей компоненты пикселей изображения. На текущий момент разработано огромное количество алгоритмов для осуществления встраивания в различные типы файлов и медиа данных, но метод LSB замещения является первым. Задача по выявлению наличия СГВ является важной и актуальной потому, что все методы стеганографического встраивания производят такие незначительные изменения в изображениях, что визуально человеческим глазом их определить невозможно. В связи с этим и появляется скрытый канал передачи информации.

При использовании 24-битного цветного изображения можно использовать один бит каждого из красных, зеленых и синих цветовых компонентов, поэтому в каждом пикселе можно сохранить в общей сложности 3 бита. В среднем, чтобы скрыть секретное сообщение длиной n бит, изменяется только $n/2$ бит в изображении. Результирующие изменения, внесенные в наименее значимые биты, слишком малы, чтобы их можно было распознать человеческим глазом, поэтому сообщение эффективно скрыто. Некоторые алгоритмы изменяют LSB пиксели, выбранные в результате случайного блуждания, другие изменяют пиксели в определенных областях изображения или вместо того, чтобы просто изменять последний бит, увеличивают или уменьшают значение пикселя.

Метод LSB-совпадений [99] является незначительной модификацией метода LSB. Если изменяемый бит, не равен биту исходного изображения, то к значению пикселя случайным образом добавляется + 1 или –1. Вероятность увеличения или уменьшения значения пикселя одинакова. Вследствие этого эффекта асимметрия не проявляется, а методы стегоанализа, предназначенные для обнаружения LSB-замены, неэффективны для LSB- совпадений.

В отличие от двух предыдущих методов, которые изменяют младшие биты различных пикселей независимо друг от друга, метод инверсного LSB-совпадения [85] использует пару пикселей в качестве блока внедрения, в котором младший бит первого пикселя несет один бит секретного сообщения, и связь (нечетно-четная комбинация) двух значений пикселей несет еще один бит секретного сообщения. Таким образом, интенсивность изменения пикселей может уменьшаться с 0,5 до 0,375 бит/пиксель (bpp) в случае максимальной интенсивности внедрения, что означает меньшее количество изменений в исходном изображении с той же полезной нагрузкой. Такая схема помогает избежать асимметрии LSB-замены, и она должна сделать обнаружение более сложным.

В [61] предложена схема встраивания на основе замены наименее значащих битов исходного изображения с помощью разности значений между пикселем и четырьмя ближайшими соседями. Несмотря на то, что использование данного метода может осуществлять встраивание важных данных по краям изображения и приводить к визуально заметным эффектам, требования безопасности выполняются. Поскольку метод модифицирует только наименее значимые биты пикселей изображения при скрытии данных, его можно легко обнаружить с помощью существующих алгоритмов стегоанализа.

В [103] предложен метод внедрения, который для выявления границ сначала использует оператор Лапласа на каждом неперекрывающемся блоке 3×3 внутри исходного изображения, а затем встраивает данные в блоки с наиболее резкими границами, превышающими пороговое значение. Максимальная емкость внедрения такого метода относительно низкая [103]. Кроме того, порог является

предопределенным и, следовательно, не может изменяться адаптивно в соответствии с содержимым изображения и встраиваемым сообщением. Схемы разнесения значений пикселей, описанные в [118,124,132], образуют еще один метод привязки границ, в котором количество встроенных бит ограничено и определяется разницей между пикселем и его соседом. Чем больше разница, тем больше количество секретных бит может быть встроено. Обычно подходы, основанные на определении границ, могут обеспечить большую емкость вложения (в среднем более 1 bpp). Однако на основании обширных экспериментов [78] показано, что данные подходы не могут полноценно использовать информацию о границах для скрытия данных, а также плохо противодействуют некоторым статистическим анализам.

В [78] предложен перекрестно-адаптивный стеганографический алгоритм, основанный на сопоставлении наименее значимых битов. Этот метод выбирает области внедрения в зависимости от размера секретного сообщения и разности между двумя последовательными пикселями в исходном изображении. Когда интенсивность внедрения возрастает, выделение крайних областей происходит адаптивно. Многие адаптивные стеганографические методы, предложенные в работах [52, 89], изменяют область встраивания в зависимости от содержимого изображения или методов стегоанализа, чтобы избежать обнаружения. Поскольку обнаружение никогда не может дать гарантию нахождения всей скрытой информации, оно может использоваться вместе с методами устранения стеганографических вставок, для минимизации возможности скрытой связи.

Таким образом, метод LSB-замены, оставаясь наиболее распространенным, претерпел ряд изменений, направленных на противодействие стегоанализу. Основные методы сокрытия факта встраивания связаны с выбором области встраивания сообщения. Поэтому нужно совершенствовать методы стегоанализа направленные на обнаружение области встраивания.

1.4 Стеганографический анализ метода LSB-замены

В методе LSB-замены биты в плоскости наименее значимых битов заменяются битами секретного сообщения в детерминированной или случайной последовательности. В результате вводится некоторая структурная асимметрия, которая может быть использована стегоанализом. Первый статистический стегоанализ был предложен в статье [117]. Данный подход специфичен для метода LSB-замены и является первым методом, основанном на статистическом анализе, а не визуальном осмотре. Указанная методика идентифицирует пары значений, состоящие из значения пикселей, квантованных коэффициентов дискретного косинусного преобразования или индексов палитры, которые сопоставляются друг с другом при изменении битов младшего слоя. После встраивания сообщений, общее количество вхождений двух членов пары значений остается неизменным. Эта концепция парных зависимостей используется для разработки статистического критерия Хи-квадрат для обнаружения скрытых сообщений [55, 117]. Представленные результаты показывают, что указанный метод надежно обнаруживает последовательно встроенные сообщения. Позже этот метод был обобщен для обнаружения беспорядочно рассеянных сообщений [116]. Другим специальным методом стегоанализа для обнаружения LSB- замены в 24-битных цветных изображениях является метод необработанных пар, предложенный в [54]. Метод основан на анализе близких пар цветов, созданных LSB встраиванием. Было показано, что отношение близких цветов к общему количеству уникальных цветов значительно увеличивается, когда сообщение выбранной длины вложено в естественное, а не искусственное изображение. Метод работает надежно, если количество уникальных цветов в исходном изображении составляет менее 30% от числа пикселей. Этот метод имеет более высокую эффективность обнаружения, чем метод, приведенный в [117], но не может применяться к изображениям в оттенках серого. Более сложный метод представлен в [56] для обнаружения LSB-замены в цветных изображениях и изображениях в оттенках серого. Этот метод

использует чувствительную двойную статистику, полученную из пространственных корреляций в изображениях. Изображение делится на непересекающиеся группы фиксированной формы. В пределах каждой группы шум измеряется средним абсолютным значением корреляций между пикселями.

Указанные группы, можно отнести или к сингулярным, или к регулярным. Это будет зависеть от того, как меняется шум пикселя внутри группы (уменьшается или увеличивается). Данный шум появляется после того, как был изменён младший слой фиксированного набора пикселей внутри каждой группы с применением маски. Доля сингулярных и регулярных групп образует кривые, квадратичные по количеству сообщений, внедренных методом LSB-замены – на это указывают эксперименты и теоретический анализ.

Метод стегоанализа, предложенный в [21], специфичен для алгоритмов внедрения LSB. Этот метод рассматривает 1-ю и 0-ю битовые плоскости изображения и вычисляет несколько бинарных мер сходства. Предложенный подход основан на том факте, что корреляция между смежными битовыми плоскостями, а также бинарные характеристики текстуры в битовых плоскостях изменяются после того, как сообщение встраивается в изображение. Для обнаружения эффекта, созданного алгоритмами встраивания, вычисляются несколько значений. На основе отмеченных особенностей, а также при использовании меры сходства двоичных изображений применяется многомерная регрессия для определения наличия или отсутствия встроенных данных.

Другой подход к стегоанализу метода LSB-вставок, называемый методом пары образов, представляет собой обобщенный случай алгоритмов, приведенных в [47, 48]. В этих работах было показано, что статистика выборочных пар значения сигнала очень чувствительна к внедрению методом LSB-замены. Этот метод основан на применении конечного автомата, состояния которого определяются несколькими наборами пар образов, называемых множествами трассировки. Поведение множеств трассировки в рамках операций встраивания моделируется конечным автоматом. Структура этого конечного автомата используется для

создания квадратных уравнений, которые оценивают длину встроенных сообщений. Метод точно измеряет длину встроенного сообщения, даже когда скрытые сообщения являются очень короткими относительно размера изображения. Этот метод является немного более точным, чем метод, приведенный в [56], но в некоторых случаях средняя абсолютная ошибка становится значимой из-за неравновесности корреляций и неравномерного распределения совместной статистики изображения [95].

Модификация описанного выше подхода предложена в [77]. В этом методе проблема выявления СГВ решается посредством метода наименьших квадратов. На наборе тестовых изображений было показано, что эта методика повышает точность оценки. В статье [46] предложен еще один подход, использующий статистику более высокого порядка для получения уравнений обнаружения и оценки скрытой длины сообщения путем измерения некоторой статистической величины подписи (отличительной статистики). Статистика подписи идентифицируется как функция длины скрытого сообщения, зависящая от некоторого вектора признаков, чувствительного к длине скрытого сообщения. Характеристическая функция, полученная из вектор-функции, приводит к кубическим уравнениям от длины скрытого сообщения. Этот метод является надежным и эффективным как для цветных изображений, так и для изображений в оттенках серого.

Метод детектирования градиентной энергии обтекания предложен в [133]. Основу этого метода обнаружения стеговставок составляет связь между длиной встроенного сообщения и энергией градиента. В этом методе рассчитывается энергия градиента изображения стегоконтейнера. После вычисления энергии градиента выполняется встраивание с различными частотами опрокидывания младшего бита и рассчитывается полученная энергия градиента изображения после каждого встраивания. Для оценки длины сообщения кривая энергии градиента аппроксимируется линейной функцией. Этот метод надежно обнаруживает присутствие секретного сообщения при интенсивности встраивания более 0,05 бит на пиксель.

Другой метод стегоанализа, специфичный для изображений в оттенках серого, предложен в [111]. В качестве инструмента статистического анализа метод использует гистограмму разностей изображения. Коэффициенты гистограммы определяются как мера корреляции между плоскостью младших битов и остальными плоскостями. Эти коэффициенты используются для построения классификатора, отличающего изображения со СГВ от чистых изображений. Этот алгоритм может обнаружить наличие скрытых сообщений, внедренных с использованием последовательной или случайной LSB замены в изображениях, а также может оценить объем скрытых сообщений. Алгоритм характеризуется высокой производительностью и скоростью вычислений для изображений с коэффициентом внедрения более 50%.

Метод стегоанализа для палитр изображений, известный как анализ пар, был предложен в [57]. Этот подход идеально подходит для 8-битных изображений формата GIF, в которых биты сообщений встроены в младшие разряды индексов упорядоченной палитры. Изображение сначала разбивается на цветовые срезы. Далее осуществляется просмотр изображения и подборка пикселей, попадающих в одну из пар значений (0, 1), (2, 3) и т.п. В один поток объединяются цветовые срезы и измеряются однородностью младшего слоя. После этого снова оценивается однородность для альтернативных пар значений (255, 0), (1, 2), (3, 4), и т.д. Эта однородность представляется как квадратичная функция длины секретного сообщения и, следовательно, служит оценкой неизвестной длины встроенного сообщения. Этот метод более эффективен, чем хи-квадрат [117].

Схема детектирования сообщений, случайным образом рассеянных в нулевом слое как цветных изображений, так и изображений в градациях серого, предложена в [73]. Этот метод основан на сборе и проверке набора соответствующих функций изображения из пиксельных групп изображения со СГВ. Особенности схемы состоят в измерении корреляций и сходств между группами пикселей. Эти функции различны при разных отношениях интенсивности встраивания. Для детектирования изображений со СГВ

используется векторная регрессия [105]. Этот подход обнаруживает существование скрытых сообщений, а также их размер.

Метод стегоанализа, представленный в [32], основан на изменениях кривых интенсивности искажений вследствие встраивания сообщения. Алгоритм основан на том факте, что стеганографические алгоритмы нарушают базовую статистику сигнала и, следовательно, изменяют характеристики интенсивности искажения сигнала. Механизм обнаружения LSB-вставок использует статистические нарушения, вызванные встраиванием. Для обнаружения стохастического встраивания используются схемы сжатия с потерями. В качестве показателей искажения используются среднеквадратическая ошибка, средняя абсолютная ошибка и взвешенная среднеквадратическая ошибка как измененных, так и исходных изображений. Элементы изображения используются для обучения байесовского классификатора. Затем этот классификатор используется для классификации чистых изображений и изображений со СГВ.

Метод мягких вычислений для реализации стегоанализа, специфичного для метода LSB-замены, предложен в [31]. Для обнаружения вставок независимо используются методы поддержки принятия решений и нейронные сети [41, 113]. Предложено несколько алгоритмов генерации деревьев принятия решений [59, 93]. Цель этого метода состоит в принятии решения о наличии или отсутствии скрытых данных, а не в оценке вероятности внедрения.

Практически все методы стегоанализа, приведенные выше, специфичны для стеганографического метода LSB-замены в случае одного изменяемого слоя и не могут быть распространены на случай нескольких слоев. Первый способ стегоанализа LSB-замены для случая нескольких изменяемых слоев предложен в [128]. Этот метод основан на анализе изотропии. Сначала определяется взвешенный стегообраз, из которого выводится формула оценки. Для этого метода точность обнаружения скрытой информации и оценка коэффициента внедрения скрытых сообщений в изображениях относительно высока.

Метод стегоанализа, основанный на тестах случайности битовой плоскости, предлагается в [40]. Две бинарные последовательности получаются путем сканирования первой и нулевой битовой плоскости изображения с помощью алгоритма Гильберта. Случайность этих двух последовательностей проверяется индивидуально четырьмя видами тестов. Результаты этих тестов образуют вектор и используются для построения классификатора на основе метода опорных векторов, который различает изображения со СГВ и чистые изображения. Результаты показывают, что метод эффективен для стеганографии при интенсивности внедрения более 0,05 bpp.

Анализ перечисленных выше результатов показывает, что статистические методы позволяют обнаружить встроенное сообщение и оценить его длину при интенсивности внедрения более 0,05 bpp. Данная интенсивность достигается в методе LSB-замены при подмене битов нулевого слоя не менее чем на 40%. При более низкой интенсивности внедрения эффективность обнаружения существенно падает, а длина встроенного сообщения определяется с большими погрешностями.

1.5 Общие методы стегоанализа

Простейшей атакой, позволяющей обнаружить СГВ, является визуальное исследование изображения [115]. В основе этой атаки лежит способность человеческого глаза обнаруживать искажения изображения, вызванного встраиванием. Алгоритм анализа пар изображений, предложенный в статьях [12,53] ориентирован на обнаружение встраивания, методом LSB-замены.

Любой из алгоритмов стегоанализа который есть на сегодняшний день предназначен для определения того факта, что изображение содержит или не содержит СГВ.

В статьях из [92,115] рассматривается процесс стеганографического анализа с помощью критерия Хи-квадрат. В основе этого метода лежит предположение о том, что при встраивании распределение младших битов будет равномерным, а в

изначальном изображении такое распределение не будет выполняться ввиду особенностей структуры изображения. Если подобное встраивание было осуществлено во всем стегоконтейнере, то благодаря критерию Хи-квадрат можно добиться неплохих результатов, однако если для замены младших битов использовалась случайная подборка пикселей, то результаты будут достаточно слабыми. Работа [2] посвящена методу, который основывается на визуальном выявлении наличия СГВ, для этого цветовые срезы рассматриваемых изображений сравниваются между собой. Так, если изображение имеет сплошную заливку на больших полях, то можно получить неплохие результаты. Материалы работы [3] содержат информацию о стегоанализе, в котором используются цепи Маркова, при этом выполняется сравнение младших битов в соседних байтах. Для определения наличия СГВ можно использовать принципы глубокого изучения и искусственные нейронные сети [36, 106]. В [1] утверждается, что при наличии необходимого объём обучающей выборки, то нейронная сеть выявит присутствие такой СГВ, а погрешность будет до 15%.

Следует отметить, что на эффективность методов стегоанализа относительно метода LSB-замещения влияет наполнение соответствующего контейнера, оно должно быть от 50% – об этом говорится в [115]. Работа [15] посвящена применению алгоритмов сжатия информации для определения наличия встроенной информации. Концепция данного метода базируется на том явлении, что, если сравнивать с упорядоченными данными, случайные сжимаются слабее. И даже если контейнер заполнен только от 40%, то можно получить хорошие результаты. А в [17] добавляется, что при наличии предварительно обработанного изображения, указанный метод будет эффективным даже в случае, если контейнер наполнен меньше 40%.

Стеганографический алгоритм F5 [114] встраивает биты в сообщения, используя матричное кодирование, что позволяет минимизировать количество изменений квантованных коэффициентов. Матричное кодирование в алгоритме F5 можно представить в виде набора трех параметров (P,Q,R). Параметр P показывает

количество коэффициентов и в большинстве случаев изменяется при встраивании. Параметр Q показывает количество коэффициентов, участвующих во встраивании k-битового сообщения. В процессе внедрения сообщение делится на сегменты длиной R бит для встраивания в группу из n случайно выбранных коэффициентов. В алгоритме F5 квантованные коэффициенты изменяют хэш-значение группы, не соответствующей битам сообщения, поэтому значения гистограммы коэффициентов дискретного косинусного преобразования изменяются. Изменения в гистограмме коэффициентов дискретного косинусного преобразования могут быть использованы для обнаружения наличия скрытого сообщения.

В статье [66] разработан метод стегоанализа, основанный на этом процессе для обнаружения внедрения вставок алгоритмом LSB-замены в цветные и полутоновые изображения. Для проверки изображения определяются регулярные группы (G) и сингулярные группы (H) пикселей в зависимости от некоторых свойств. Затем с помощью относительных частот этих групп на изображении, полученном из исходного с перевернутыми LSB, и изображением, полученным рандомизацией LSB исходного изображения, предпринимается попытка предсказать уровень встраивания.

В работе [62] предпринята попытка классифицировать атаки стегоанализа для восстановления или удаления сообщения на основе доступной информации. Разработанная методика стегоанализа может обнаруживать несколько вариантов методов скрытия сообщения [83]. Первый метод стегоанализа с использованием вейвлет-разложения был разработан в [104] и показал, что это изменение пропорционально уровню встраивания. Также показано, что если изображение обрезается 4 строками и 4 столбцами, то можно получить оригинальную гистограмму дискретного косинусного преобразования. Основное предположение состоит в том, что квантованные коэффициенты дискретного косинусного преобразования устойчивы к малым искажениям, и после обрезки вновь вычисленные коэффициенты дискретного косинусного преобразования не будут отображать кластеры из-за квантования. Кроме того, поскольку обрезанное

изображение со СГВ визуально похоже на исходное изображение, многие макроскопические характеристики исходного изображения будут примерно совпадать с изображением со СГВ. Сравнение изображения со СГВ с изображением после сглаживания позволяет рассчитать длину скрытого сообщения. В статье [108] используется эмпирическая матрица как параметр для стегоанализа. В работе [38] статистические моменты с дополнительными признаками применяются для стегоанализа изображения в формате JPEG.

Наиболее известный метод для обнаружения LSB-замены – это хи-квадрат. Он позволяет эффективно обнаруживать LSB-замену в коэффициентах формата JPEG. Другая схема обнаружения LSB-замены позже была предложена в [23]. В этой работе использованы двоичные показатели сходства между 1-ой битовой плоскостью и 0-ой (наименее значимой) битовой плоскостью. Предполагается, что существует естественная корреляция между битовыми плоскостями, которая нарушается при использовании LSB. Эта схема не может регулироваться автоматически на основе изображения, вместо этого она калибруется на обучающем наборе исходных изображений и изображений со СГВ. Данная схема работает лучше, чем общая схема стегоанализа, но не так хорошо, как современный стегоанализ LSB.

Схема, предложенная в [58], представляет собой специфический метод стегоанализа для обнаружения данных LSB-замены, скрытых в изображениях. Используя оценки совместной вероятности [84], удается увеличить эффективность обнаружения стегановставок. Используются локальные оценки на основе пиксельных кварталов, чтобы улучшить обнаружение LSB-вставок. Этот метод предназначен для типичных распределений значений цветов пикселей. Далее эти оценки используются для обучения байесовского многовариантного классификатора, различающего изображения со встроенным сообщением и без него. Автором статьи выполнены тесты на изображениях RGB, используя комбинированный центр масс каждой цветовой плоскости. В работе [32] используются кривые искажения для обнаружения скрытия LSB-вставок. В этих

работах отмечается, что вложение данных обычно увеличивает энтропию изображения. С другой стороны, сжатие предназначено для уменьшения энтропии изображения. Поэтому разность между изображением со СГВ и его сжатой версией больше, чем разность между исходным изображением и ее сжатой формой. Показатели искажения, такие как среднеквадратичное отклонение и взвешенное среднеквадратичное отклонение, показывают абсолютную ошибку. Эти методы используются для измерения разницы между изображением и сжатой версией изображения. Для обучения классификатора используется вектор признаков, состоящий из этих показателей искажения для нескольких разных степеней сжатия (с использованием JPEG2000). Ложные срабатывания и показатели пропущенных обнаружений составляют около 18%.

Из изложенного материала видно, что общие методы стегоанализа ориентированы только на факт обнаружения скрытого сообщения и не позволяют определять ни его размер, ни положение на изображении. Общие методы стегоанализа обнаруживают СГВ с ошибкой не более 15% лишь в том случае, если наполнение контейнера составляет не меньше половины. Общие методы стегоанализа, основанные на дискретном косинусном преобразовании, ориентированы на исследование статистических свойств коэффициентов преобразования, а не на их детальное изучение.

1.6 Методы стегоанализа, основанные на классификаторах

Для отделения пустого изображения-стегоконтейнера от заполненного необходимо ввести параметры, анализ значений которых позволяет выполнять классификацию. Параметры должны быть чувствительны к методу скрытия данных. Значения параметров должны отличаться для исходного изображения и для изображения с встроенным сообщением. Чем больше разница в значении параметров, тем лучше осуществлен выбор параметров. Кроме выбора отдельных параметров, в ряде случаев необходимо построение многомерного вектора

параметров. Проблема построения классификатора — это второй шаг стегоанализа, близкий по постановке к задаче распознавания образов.

Рассмотрим некоторые подходы к выбору параметров, применяемых для стегоанализа изображений.

Показатели качества изображения и сигнатуры

Показатели качества изображений должны быть выбраны таким образом, чтобы отображать искажения изображения вследствие размытости, сжатия, аддитивного шума и т.д. Кроме этого, показатели качества изображения должны быть точными, последовательными и монотонными.

В статье [22] был проведен статистический анализ поведения чувствительности и согласованности объективных показателей качества изображения. Двадцать шесть показателей качества изображения были разделены на шесть групп в зависимости от типа используемой ими информации. Значения показателей определялись исходя из разности пикселей, корреляции, краевому спектру и контексту. Были исследованы их чувствительность и согласованность с кодированием, а также аддитивным шумом и уровнем размытия. Было обнаружено, что показатели, основанные на измерениях спектра и краевой устойчивости, наиболее чувствительны к кодированию и размытию деталей изображения, тогда как среднеквадратическая ошибка более применима для аддитивного шума.

Распространенным также является стегоанализ несжатого изображения на основе сигнатур изображения. Так, в работе [86] представлен метод стегоанализа с использованием сигнатуры близкой цветовой пары, где производится сравнение соотношения близких цветовых пар и уникальных цветов. Поскольку обозначенное соотношение у изображения, не имеющее встроенного сообщения всегда имеет большее значение чем у изображения-контейнера, в анализируемое изображение необходимо осуществить тестовое встраивание какого-либо сообщения, после чего анализировать сигнатуру близкой цветовой пары в исходном изображении и изображении, полученном после намеренного встраивания. Если оба изображения

не показывают значительной разницы в соотношениях близких цветовых пар и уникальных цветов, можно сделать вывод, что анализируемое изображение содержит скрытое сообщение.

Марковские параметры

Марковские процессы были использованы для разработки метода стегоанализа [100], направленного на эффективное обнаружение расширенного стеганографического встраивания в изображения формата JPEG. Для обнаружения факта встраивания были использованы различия в двумерных массивах JPEG в горизонтальном, вертикальном и диагональном направлениях. После этого был использован Марковский процесс для моделирования этих разностных отношений и вычисления статистики второго порядка для стегоанализа. В качестве классификатора был использован метод опорных векторов. Этот метод стегоанализа был протестирован для обнаружения стеганографического встраивания, осуществленного с помощью алгоритмов F5, Outguess и MB1.

В статье [134] для построения показателей качества изображения были использованы методы прогнозирования на основе Марковских процессов. Значение пикселей изображения прогнозируется исходя из значений соседних пикселей, а величина ошибки прогнозирования вычисляется путем вычитания значения предсказания из значения пикселя. Затем происходит сравнение с заданным пороговым значением. Эмпирическая матрица перехода по горизонтальному, вертикальному и диагональному направлениям служит в качестве параметров для классификатора. Для классификации был использован метод опорных векторов с линейным и нелинейным ядром. Было показано, что метод опорных векторов с нелинейным ядром характеризуется более высокой эффективностью по сравнению с линейным ядром. Данный метод тестировался для изображений с различными объемами встроенного сообщения. Параметры изображения, использующие моделирование с помощью Марковских цепей, получили название Марковских параметров.

Параметры изображения на основе Марковских цепей были также рассмотрены в статье [87] для исходных, разностных и вторых разностных массивов формата JPEG. Марковские параметры, основанные на исходном массиве формата JPEG, фиксируют характеристики распределения коэффициентов дискретного косинусного преобразования, в то время как Марковские параметры, основанные на разностях и вторых разностях JPEG-массивов, фиксируют различия между соседними коэффициентами. Объединение этих трех Марковских параметров позволяет улучшить результаты работы системы стегоанализа. В качестве классификатора использовалась искусственная нейронная сеть. Экспериментальные результаты для различных баз данных изображений, полученные в указанной работе, показывают более высокую эффективность по сравнению с [100].

Марковские параметры были расширены до модифицированного Марковского подхода в работе [91]. Параметры извлекались из внутриблочного домена дискретного косинусного преобразования и межблочного домена дискретного косинусного преобразования. После этого извлекались параметры из горизонтальных и вертикальных разностных массивов вдоль поддиапазонов приближения дискретного преобразования Фурье. Для повышения точности обнаружения были введены калибровочные функции. Для определения наличия СГВ использовался классификатор на основе искусственной нейронной сети. Алгоритм тестировался для стеганографических методов MB1, MB2, JSTEG и F5.

Вейвлет-преобразования

В работе [51] для извлечения объектов из изображений в оттенках серого было использовано разложение, основанное на сепарабельных квадратурных зеркальных фильтрах. Для этого была разработана статистическая модель, состоящая из вычисления среднего, дисперсии, эксцесса, перекоса коэффициентов поддиапазонов и статистики ошибок на основе оптимального линейного прогнозирования коэффициентов. После этого для разделения исходных и

измененных изображений был использован линейный дискриминантный анализ Фишера.

В статье [80] данная модель расширена и использует статистику вейвлет-преобразования первого и более высокого порядков, а также статистику цветов. Для обнаружения встроенных сообщений в цифровых изображениях используется однокомпонентный метод опорных векторов. Предложенный подход протестирован для стеганографических методов JSteg, Outguess, F5, Jphide и Steghide применительно к базе изображений в формате JPEG.

Этими же авторами [81] построенная ранее модель была расширена с помощью включения дополнительной фазовой статистики, что позволило построить 432-мерную вектор-функцию параметров. Для классификации изображений использовался метод опорных векторов. Результаты компьютерного эксперимента показали более высокую эффективность расширенной модели при обнаружении стеганографических вставок.

Метод стегоанализа, основанный на выявлении множества особенностей изображения, представлен в статье [121]. В нем используются первые три момента разложения по вейвлетам Хаара, что приводит к 39-мерным векторам параметров. Для классификации тестовых изображений используется классификатор Байеса. Тестирование осуществлялось на коллекции из 1096 изображений CorelDraw. Для встраивания использовался метод LSB-вставок. Эффективность обнаружения стеганографических вставок в среднем составляет 86%.

В статье [72] для обнаружения стеганографических вставок предложен набор из двух функций изображения: энергия градиента и статистическая дисперсия параметров Лапласа. Предлагаемая система эффективна при обнаружении любой технологии внедрения СГВ и обеспечивает эффективность обнаружения до 90%.

Для изображений в градациях серого в статье [129] предложен метод, основанный на дискретном двумерном вейвлет-разложении до четвертого порядка, что позволяет получить статистическую модель, основанную на среднем значении, дисперсии, асимметрии и эксцессе. В результате формируется 36-

мерный вектор параметров. Еще один набор из 36 элементов может быть получен из статистики ошибок оптимального линейного предиктора. Для определения чувствительности этих данных вейвлет-статистики к наличию скрытого сообщения выполняется анализ дисперсии. Для тестирования предложенного подхода были использованы методы сокрытия данных Steguide, Hide4pgp и S-tools.

Метод, предложенный в работе [101], получает на входе одноуровневое вейвлет-разложение изображения на основе вейвлетов Хаара и делит его на горизонтальные, вертикальные и диагональные окна. Затем записывается система уравнений для каждого окна, которая решается с помощью псевдообращения Мура-Пенроуза. После этого вычисляется ошибка линейного прогноза для всех поддиапазонов. Параметры извлекаются из векторов ошибок, полученных для поддиапазонов, и классифицируются с использованием метода опорных векторов.

В статье [79] изображение раскладывается на три составляющие с использованием вейвлет-преобразования. В результате получается 85 коэффициентов, на основе которых формируются параметры, использующие многозначные характерные функциональные гистограммы моментов. После нормализации полученных параметров они объединятся с 255-мерным вектором параметров, описанным в предыдущей работе. Для классификации изображений применяется нейронная сеть с обратным распространением ошибки. Этот метод имеет более высокую среднюю точность обнаружения по сравнению с [112,121], о чем свидетельствуют результаты компьютерного эксперимента.

В работе [110] также предложена классификация с использованием нейронной сети на основе характеристик, извлеченных из моментов трехуровневых подблоков вейвлет-преобразования, включая коэффициенты разложения первого диагонального поддиапазона. Далее эта работа расширяется в сторону анализа эффективности использования векторов признаков. Расстояние между векторами признаков вычисляется с помощью евклидовой метрики. В статье [71] используется анализ основных компонентов для уменьшения размерности

векторов признаков и метод опорных векторов в качестве классификатора. Точность обнаружения улучшается благодаря уменьшенному набору параметров.

В статье [24] разработан метод стегоанализа, основанный на бинарных методах сходства. Основная идея этой методики заключалась в том, что существует сильная корреляция между 1-м и 0-м битовыми плоскостями. Если происходит стеганографическое встраивание, то бинарные характеристики текстуры в этих битовых плоскостях будут отличаться. Эта разности используются в качестве входных данных для классификатора на основе метода опорных векторов. Был проведен компьютерный эксперимент на базе 1800 естественных изображений. Использовался стеганографический алгоритм LSB-замены, в котором значения пикселя увеличиваются или уменьшаются на 1. Кроме этого, использовались алгоритмы F5 и Outguess для изображений в формате JPEG. Для каждого изображения были построены различные 18-мерные бинарные оценки сходства. Затем эти векторы использовались для обучения и тестирования классификатора на базе метода опорных векторов.

В статье [74] аналогичным образом сравнивались первая и нулевая битовые плоскости ненулевых коэффициентов дискретного косинусного преобразования в изображениях формата JPEG. На основе двоичных показателей подобия вычислялись 14 признаков изображения. Для классификации также использовался метод опорных векторов.

В работе [123] при проведении стеганографического анализа изображений в градациях серого используется метод комбинирования пространственного и вейвлет фильтров посредством простого голосования. Пространственный остаток получается в результате фильтрации по значениям четырех соседних пикселей. Вейвлет остаток вычисляется с использованием 8-ступенчатого фильтра Добеши. После чего обе полученные дискриминантные функции объединяются для получения оценочной матрицы модификаций. Метод показывает высокую эффективность обнаружения стеганографических вставок даже при рабочей

нагрузке в 10%, а также позволяет решить вторую и третью задачи стегоанализа, определив местоположение вставки.

Матрица совпадений

В работе [67] разработаны 7850-мерные векторы параметров, которые вычисляются из совпадений матриц пар коэффициентов дискретного косинусного преобразования. Поскольку данные параметры представляют как внутриблочные, так и межблочные зависимости, метод стегоанализа позволяет эффективно обнаруживать скрытые данные в изображениях формата JPEG. Для классификации изображений использованы линейные дискриминанты Фишера, обучающиеся в случайных подпространствах малого размера. Окончательное решение о наличии СГВ принимается на основе отдельных линейных дискриминантов Фишера с помощью мажоритарной стратегии голосования. Таким образом, обеспечивается как хорошая эффективность классификации, так и удовлетворительная вычислительная сложность.

Схема стегоанализа, предложенная в статье [70], состоит из двух этапов: выделение параметров на основе признаков и анализ изображений с помощью байесовского классификатора. Набор параметров состоит из двух частей: первая часть генерируется из матриц совпадений коэффициентов, позволяющих получить 7850 параметров, предложенных в [67], а вторая часть вычисляется из матриц совпадений разностей коэффициентов. Для стегоанализа используется в общей сложности 15700 параметров. Данные параметры используются для работы ряда подклассификаторов, которые интегрированы с байесовским классификатором. При построении каждого дополнительного классификатора 15700 параметров используются для обучения набора линейных дискриминантов Фишера. В данной работе используется 201 субклассификатор. Данный подход тестировался для метода встраивания F5. Использование двух наборов параметров увеличивает эффективность выявления СГВ на 2%.

В статье [109] для получения трехсторонних дифференциальных отображений естественного изображения вычисляется прямая разность в трех

направлениях: горизонтальном, вертикальном и диагональном между соседними пикселями. Для удаления избыточной информации дифференциальные отображения сравниваются с заранее заданным пороговым значением. В качестве признаков стегоанализа используются матрицы совпадений пороговых дифференциальных отображений. В качестве классификатора применяется метод опорных векторов.

В статье [63] изложен метод стегоанализа изображений в градациях серого с использованием матрицы совпадения изображений и функции плотности вероятности. Данный метод основан на вычислении всего 12 характеристик, из которых четыре вычисляются непосредственно из матрицы совместной встречаемости, четыре вычисляются из функции плотности вероятности, а оставшиеся четыре связаны с разностной матрицей смежности, а также разницы значений соседних пикселей при 4- и 8- связной смежности. Метод использует алгоритм машины опорных векторов и показывает высокую эффективность при больших объемах заполнения стегоконтейнера, снижаясь до 64-75% при заполнении стегоконтейнера на ¼.

В работе [20] описывается метод стеганографического анализа изображения в градациях серого с использованием матрицы совпадений на основе 22 признаков, включающих корреляцию между левым и правым полубайтами, а также энтропию правых полубайтов, коэффициент вариации правых полубайтов и разницу между последовательно идущими правыми полубайтами. Метод показывает практически равновысокую эффективность при пятидесяти и двадцати пяти процентном уровне заполнения стегоконтейнера. В качестве классификатора используется метод опорных векторов.

Особенности гистограммы

В статье [43] предложен вектор признаков, вычисляющийся из 18 двухмерных гистограмм, полученных для данного цветного изображения. В этот набор входят 9 двумерных гистограмм смежности трехстороннего дифференциального отображения и 9 двумерных гистограмм дифференциальных

отображений для трех цветных плоскостей. После этого рассчитываются двухмерные гистограммы дискретного преобразования Фурье, в результате получается набор из 54 параметров. В качестве классификатора применяется метод опорных векторов. В работе [44] дополнительно выделены признаки дискретного преобразования Фурье на основе гистограммы дифференциального отображения. Из гистограммы самого отображения и трех гистограмм разности в трех направлениях – горизонтальном, вертикальном и диагональном по отношению к соседним пикселям – получают четыре гистограммы: одну из гистограммы самого изображения и три фокальных дифференциальных отображения. Затем параметры делятся на полосы низких и высоких частот. В качестве классификатора применяется метод опорных векторов.

Функции длины прогона, предложенные в [45], используют характеристики гистограмм изображений. Вычисляются первые три момента для каждой гистограммы. Далее используются разные отображения: квантованное изображение, разностное изображение и оригинальное изображение с четырьмя направлениями (горизонтальные, вертикальные, малые и основные диагонали). В итоге получается 36-мерный вектор параметров. В статье [82] был представлен слепой метод стегоанализа с использованием гистограммы и дискретного преобразования Фурье. Был получен 24-мерный вектор параметров, а затем для разграничения исходных изображений и изображений со СГВ использовался метод опорных векторов. Этот алгоритм был протестирован на стеганографическом методе S-Tool. Метод обеспечивал очень хорошую эффективность обнаружения даже при уровне внедрения менее 50%.

Стегоанализ, основанный на использовании нейронной сети, представлен в работах [39, 64, 76]. Цифровые изображения, стегоконтейнеры, а также СГВ, анализируются в доменах дискретного косинусного преобразования, дискретного преобразования Фурье и дискретного вейвлет-преобразования.

В статье [90] предложен новый набор параметров для стегоанализа изображений формата JPEG, который состоит из 193 параметров дискретного

косинусного преобразования и учитывает межблочные и внутриблочные зависимости коэффициентов дискретного косинусного преобразования. Далее к Марковским особенностям параметров применяется калибровка, что позволяет дополнительно уменьшить их размерность в 4 раза. В результате получается 81 параметр. Результирующие наборы параметров объединяются, создавая 274-мерный вектор параметров. Новый набор параметров используется для создания мультиклассификатора, способного распознавать пять популярных стеганографических алгоритмов – F5, OutGuess, JP, Hide & Seek и Steghide. Предложенный набор параметров обеспечивает значительно более надежные результаты, однако изображения, подвергающиеся двойному сжатию, имеют высокую вероятность ошибочной классификации.

Многодоменные функции используются для универсального стегоанализа в работе [122]. Параметры изображения вычисляются на основе разности градиента в пространственной области, коэффициента корреляции в домене дискретного косинусного преобразования, среднего и стандартного отклонения матрицы разностных значений в домене дискретного вейвлет-преобразования. Тестирование осуществлялось базе BMP-изображений.

Из приведенного обзора методов выделения параметров изображения, которые можно применять для выявления встраивания, видно, что для достижения высокой эффективности набор параметров должен быть достаточно большим. Вследствие чего увеличивается вычислительная трудоемкость стегоанализа. Увеличение количества параметров приводит к повышению эффективности выявления СГВ только до определенного предела, после чего добавление новых параметров не значительно влияет на результат. Так, удвоение количества параметров с 7500 до 15000 приводит к повышению эффективности всего на 2%.

Комбинация подходов

В последние несколько метод появились комбинированные методы стеганографического анализа, позволяющие существенно повысить результативность обнаружения СГВ.

Стегоанализ изображений формата JPEG на основе 165 признаков, извлеченных из двойной, глобальной и индивидуальной гистограмм, 81 Марковских признаков, дополненных 28 признаками второго порядка, полученными с использованием матрицы совместной встречаемости, предложен в работах [68, 97]. Для достижения наилучшей чувствительности используется SVM-PSO классификатор, объединяющий алгоритмы машины опорных векторов (SVM) и оптимизации роя частиц (PSO), и мультиквадратичное ядро, показывающее значительно лучшие результаты по сравнению с такими ядрами как полиномиальное, ядро ANOVA, ядро DOT и другими ядрами. Метод показывает эффективность до 71% при минимальной (10%) рабочей нагрузке, однако характеризуется высокой разрядностью и, следовательно, высокой вычислительной трудоемкостью.

В работах [34, 35] предложен ансамблевый метод SW-анализа цветных изображений, основанный на вычислении весов подобий пикселей (PSW) и весов подобий цветовых каналов (CSW). Таким образом, эффективность PSW-анализа, достигаемая при высоких уровнях заполнения стегоконтейнера, дополняется эффективностью CSW-анализа при низком заполнении стегоконтейнера. Для достижения максимальной чувствительности, ядро классификатора на основе алгоритма машины опорных векторов, является также ансамблевым, с использованием гауссово распределения, правила трех сигм и стандартного отклонения от среднего как наиболее значащих статистических функций.

Интересным также представляется метод стегоанализа изображений в градациях серого с применением топологических данных, предложенный в работе [94]. Для целей анализа определяется последовательность Rips SC однородных локальных двоичных шаблонов (кодов ULBP), содержащих три или шесть единиц значений пикселей, с извлечением шести восьмимерных векторов признаков. Эффективность метода, протестированная при 100% полезной нагрузке, составляет 90%.

Еще одной разновидностью комбинированных методов стегоанализа на основе классификаторов является расширение ранее созданных аналитических алгоритмов. Так, например, в работе [60] классическая SRM-модель для проведения стеганографического анализа цветных изображений, количество признаков которой (размерность модели) составляло 12 753, дополнена 4 704 дополнительными характеристиками, формирующимися из остаточных значений шума и включающими остатки, вычисленные по трем цветовым каналам. Данный метод стегоанализа использует ансамблевый классификатор на основе линейного дискриминанта Фишера.

Выводы по первой главе

Проведенный анализ известных методов стегоанализа позволил выявить следующие недостатки:

1. Подавляющее большинство методов стегоанализа основано на предположении об изменении статистических свойств изображения при встраивании в него скрытого сообщения. Как следствие, данные методы не применимы для случая низкого заполнения стегоконтейнера, не превышающего 40% от максимально возможного. Поэтому нужно развивать методы стегоанализа, ориентированные на исследование структуры изображения.

2. Основное направление развития статистических методов стегоанализа, связанное с увеличением количества параметров, используемых для выделения изображений со СГВ, практически исчерпало себя. Увеличение количества параметров в два раза приводит к незначительному повышению эффективности. Поэтому нужно развивать алгоритмы, использующие не глобальные параметры изображения как целого, а некоторые локальные характеристики областей, в которых может быть осуществлено встраивание.

3. Общие методы стегоанализа обладают невысокой эффективностью, особенно в случае низкого заполнения стегоконтейнера, поэтому нужно развивать

специализированные методы стегоанализа, ориентированные на конкретные алгоритмы стеганографического встраивания.

4. Статистические методы стегоанализа позволяют только решать задачу установления факта присутствия СГВ. Для определения размера, положения и содержимого СГВ необходимо развитие алгоритмов стегоанализа, основанных на анализе параметров изображения, используемых для встраивания. В случае метода LSB-замены необходимо развивать методы анализа нулевого битового слоя и сравнительного анализа нулевого и близлежащих битовых слоев. Для методов стеганографии, основанных на дискретном косинусном преобразовании, необходимо проводить поиск и исследование коэффициентов преобразования, используемых при встраивании сообщения.

5. Методы стегоанализа, основанные на использовании классификаторов изображений требуют достаточно большого обучающего набора однотипных изображений и не применимы в случае одного уникального изображения. При этом эффективность обнаружения зависит от баз данных и выборки, применяемых для обучения классификаторов.

ГЛАВА 2. СТЕГОАНАЛИЗ МЕТОДА LSB-ЗАМЕНЫ НА ОСНОВЕ АНАЛИЗА ДВУХ МЛАДШИХ СЛОЕВ

2.1 Введение

Как было показано в предыдущей главе, встраивание сообщения в наименее значащие биты нулевого слоя приводит к изменению его статистических характеристик. В частности, данное изменение проявляется как увеличение или уменьшение плотности единичных значений. Также в первой главе было показано, что обнаружение сообщения, встроенного методом LSB-вставки, возможно только для областей равномерной заливки. Для областей с большим количеством границ и изменений цветов встраивание сообщения не может быть обнаружено ни визуально, ни статистическими методами, так как энтропия нулевого слоя остается неизменной.

В данной главе будем исходить из предположения о том, что изображение-контейнер содержит большие области градиентной либо равномерной заливки. Градиентная заливка, так же, как и равномерная, обладает некоторыми закономерностями распределения единичных и нулевых битов и может быть выявлена явным образом.

В распределении единичных и нулевых битов при встраивании сообщения появляется изменение, которое можно определить автоматически либо визуальным способом. Так как для того, чтобы скрыть сообщения, используют синюю компоненту из-за её малозаметности для человеческих глаз, то и анализировать будем именно её. Однако, все прочие компоненты также можно проанализировать, при этом общность метода не утратится. Опираться будем на следующие предположения. Первое можно сформулировать так: доподлинно неизвестно есть ли СГВ. Второе: СГВ может быть в определённой области прямоугольной формы, но её расположение и размеры неизвестны.

Второе предложение усложняет задачу, потому что необходимо будет дополнительно устанавливать ту область, в которой есть СГВ. К тому же, может возникнуть ситуация, когда подменены будут все младшие пиксели. Поэтому предположим также, что на нулевом слое произведена была неполная замена.

В данной главе предлагается алгоритм, с помощью которого можно выявить пиксели, в которых была осуществлена подмена нулевого бита при встраивании сообщения. Алгоритм основан на автоматическом анализе нулевого слоя изображения.

2.2 Постановка задачи анализа нулевого слоя и метод её решения

Для того чтобы понять, что такое нулевой слой, представим его в виде матрицы, состоящей из 1 и 0. Если не было встраивания, то закономерности распределения нулей и единиц зависят от особенностей изображения, которые определяются его структурой, но если было встраивание, то в нулевом слое меняется плотность распределения нулей и единиц. Таким образом, необходимо решить задачу по выявлению подменённых битов в условиях, когда стегоконтейнер имеет низкое наполнение, при котором заменены меньше, чем 40% битов нулевого битового слоя. Изображения с нулевым слоем без СГВ, изображения с нулевым слоем с СГВ представлены на Рисунках 1-х. Представлены фотографические изображения как искусственные, так и с равномерной заливкой. В нулевом слое заменены 25% битов. Анализируя нулевой слой, присутствие СГВ, а также его расположение и размер можно выявить визуально. Установим цель – выявить присутствие области встраивания, расположение и размеры.

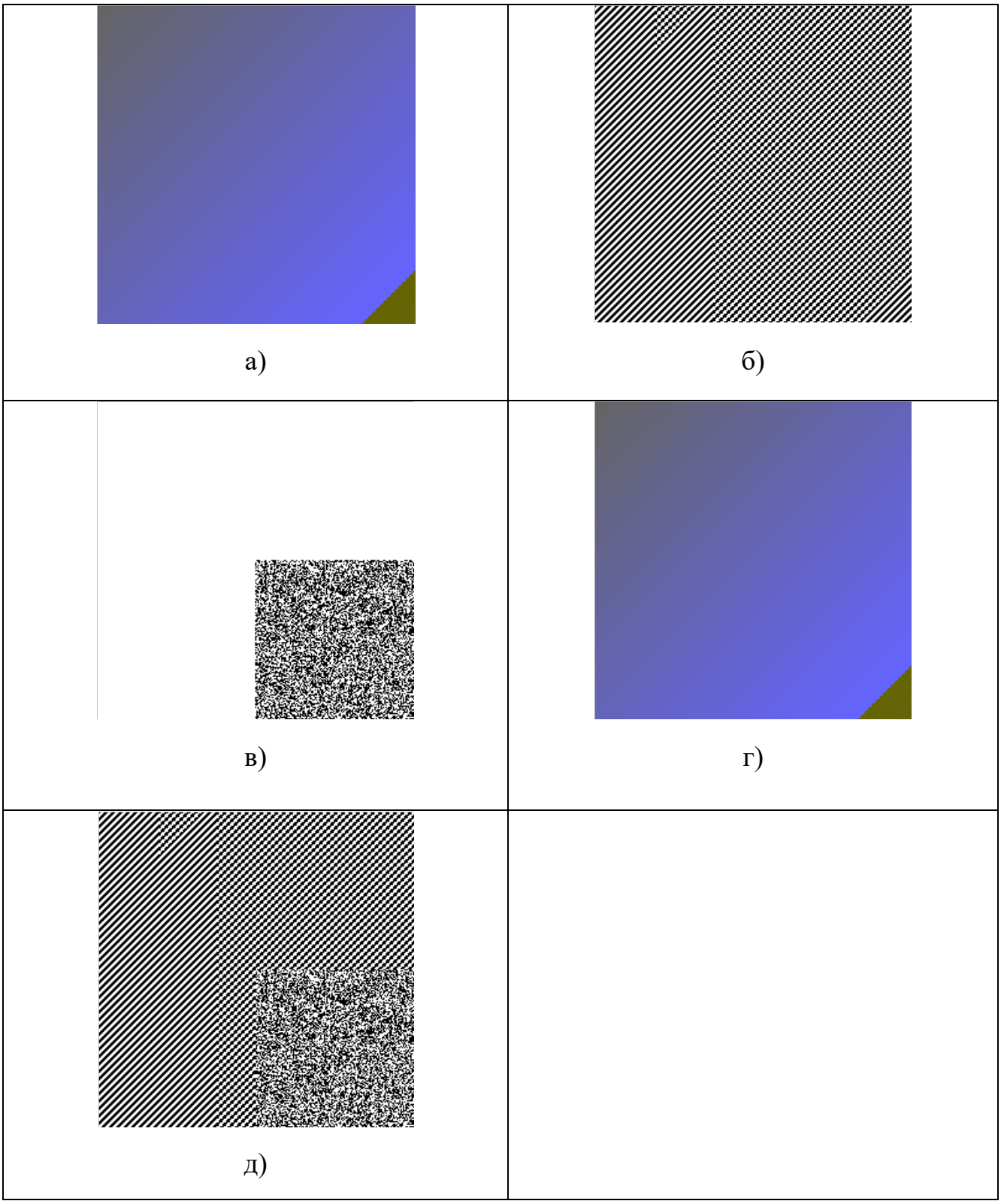


Рисунок 1 – Сопоставление нулевых слоев изображения с градиентной заливкой: а) первоначальное изображение, б) нулевой слой первоначального изображения, в) карта встраиваемых пикселей, г) изображение с СГВ, д) нулевой слой изображения с СГВ

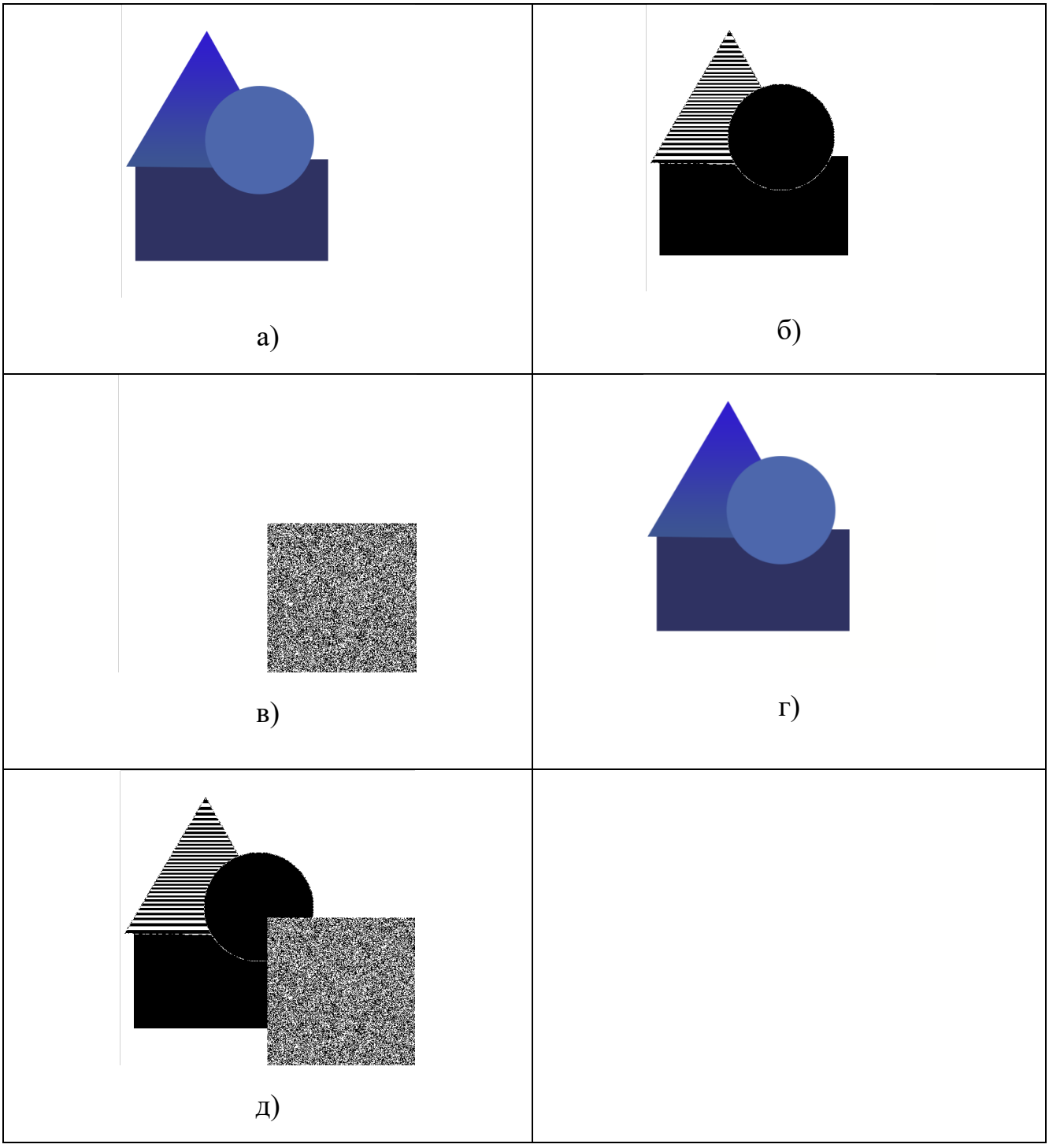
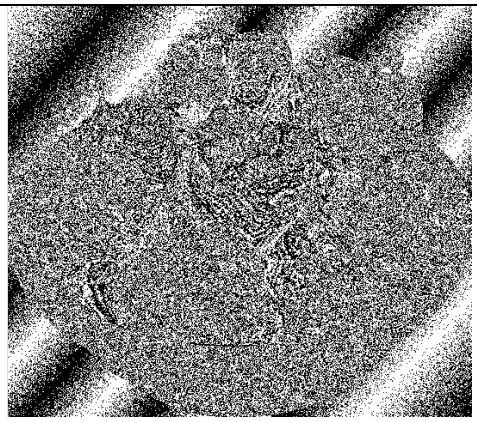
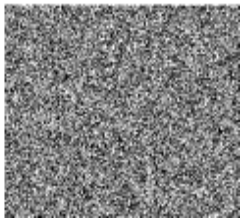


Рисунок 2 – Сопоставление нулевых слоев искусственного изображения: а) первоначальное изображение, б) нулевой слой первоначального изображения, в) карта встраиваемых пикселей, г) изображение с СГВ, д) нулевой слой изображения с СГВ

а)

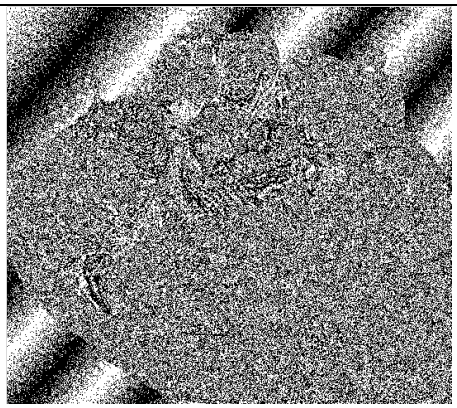


б)



в)

г)



д)

Рисунок 3 – Сопоставление нулевых слоев фотографического изображения: а) первоначальное изображение, б) нулевой слой первоначального изображения, в) карта встраиваемых пикселей, г) изображение с СГВ, д) нулевой слой изображения с СГВ

Чтобы построить алгоритм определения и автоматического выделения области встраивания сообщения в нулевой слой, предположим следующее:

1. Встраиваемое сообщение – это поток битов с распределением единиц и нулей, близким к равномерному.

2. Стороны изображения стегоконтейнера параллельны сторонам прямоугольной области встраивания.

3. У прямоугольной области встраивания есть пересечение с областью равномерной заливки изображения стегоконтейнера не меньше, чем на 25%.

Визуальный анализ нулевого слоя позволяет зафиксировать некоторые нюансы изменения распределения единичных и нулевых битов:

1. Область равномерной заливки на начальном изображении не будет совпадать с областью равномерной заливки на нулевом слое.

2. Встроенное сообщение формирует прямоугольную область, у которой равномерное распределение единичных битов.

То есть, чтобы выделить области встраивания, нужно проанализировать нулевой слой и выделить те области, которые будут соответствовать одинаковому значению плотности единичных значений битов. По своей постановке такая задача совпадает с задачей таксономии точек на плоскости. Но классические алгоритмы таксономии могут выделять только те области, которые ограничены окружностями. В нашем случае требуется усовершенствовать алгоритмы таксономии, принимая во внимание априорную информацию о том, что области встраивания имеют прямоугольную форму. Для построения алгоритма таксономии применим метод последовательных приближений.

Постоянная смена цвета изображения может добавить определённые сложности, с этим можно столкнуться, если присутствует у искусственных изображений градиентная заливка. Визуальным проявлением подобной смены цвета изображения является наличие полос одинаковых значений на нулевом слое.

Данную проблему можно устранить только посредством предварительной обработки изображений.

2.3 Алгоритм предварительной обработки изображений

Нулевой слой изображения, имеющий градиентную заливку – это полосы из 0 и 1. Используя линейное преобразование, данное утверждение можно записать следующим образом:

$$d(x,y) = ax + by - e, \quad (5)$$

где $a = c(x+1,y) - c(x,y), b = c(x,y+1) - c(x,y)$, $c(x,y)$ – значения цвета пикселя, а (x,y) – координаты расположения пикселя. На множестве всех пикселей изображения зададим параметр e как наименьшее значение $c(x,y)$. $d(x,y) = const$ для случая, когда цвет изображения достигается при помощи заливки с постоянным градиентом.

К функции $d(x,y)$ можно применить алгоритм принятия решений об изменении пикселя. К фотографическим изображениям также можно применить линейное преобразование. Однако это становится возможным только после определения области градиентной заливки. Для функции $c(x,y)$ вычислим вторые производные, а также области с нулевыми значениями. Принимая во внимание, что области идеальной градиентной заливки на фотографических изображениях – крайне редкое явление, запишем следующее неравенство:

$$\left|\frac{\partial^2 c(x,y)}{\partial x^2}\right| \leq 2, \left|\frac{\partial^2 c(x,y)}{\partial y^2}\right| \leq 2, \left|\frac{\partial^2 c(x,y)}{\partial x \partial y}\right| \leq 2. \quad (6)$$

Данное условие позволяет сохранить встроенные биты и учесть небольшие отклонения – дано нестрогое неравенство.

Следующим шагом является определение коэффициентов функции $d(x,y)$; в этом случае метод наименьших квадратов – идеальный инструмент.

Теперь создадим карты, чтобы найти области встраивания $map(x,y)$:

1. Если точка (x, y) находится в области градиентной заливки, то $map(x, y) = d(x, y)$.

2. Для всех прочих точек $map(x, y) = 0$.

Алгоритм поиска областей встраивания сообщений для $map(x, y)$.

Возможность уменьшения влияния границ областей изображения на результаты работы алгоритма позволяет нам присваивать нулевые значения $map(x, y)$ в точках, находящихся вне областей градиентной заливки.

На Рисунке 4 отображены карты $map(x, y)$ для изображений, представленных на Рисунках 1-3.

2.4 Алгоритм выделения области встраивания

Единичные значения на карте пикселей возникают как вследствие встраивания, так и по причине наличия резких границ на исходном изображении. Однако биты, измененные вследствие встраивания, присутствуют только в нулевом слое, тогда как биты, характерные для самого изображения, присутствуют и в более высоких слоях. Поэтому вычтем из нулевого битового слоя первый битовый слой. Это не приведет к полному устранению особенностей изображения контейнера, но снизит плотность единичных битов. Результаты подобного вычитания для изображения, отображенного на Рисунке 3, приведены на Рисунке 5, на котором можно увидеть, что часть области, в которую производилось встраивание, пересекающаяся с областью градиентной заливки изображения контейнера, имеет более высокую плотность единичных значений. Построим алгоритм, который автоматически выделяет эту область и по ней восстанавливает прямоугольник стеганографического встраивания.

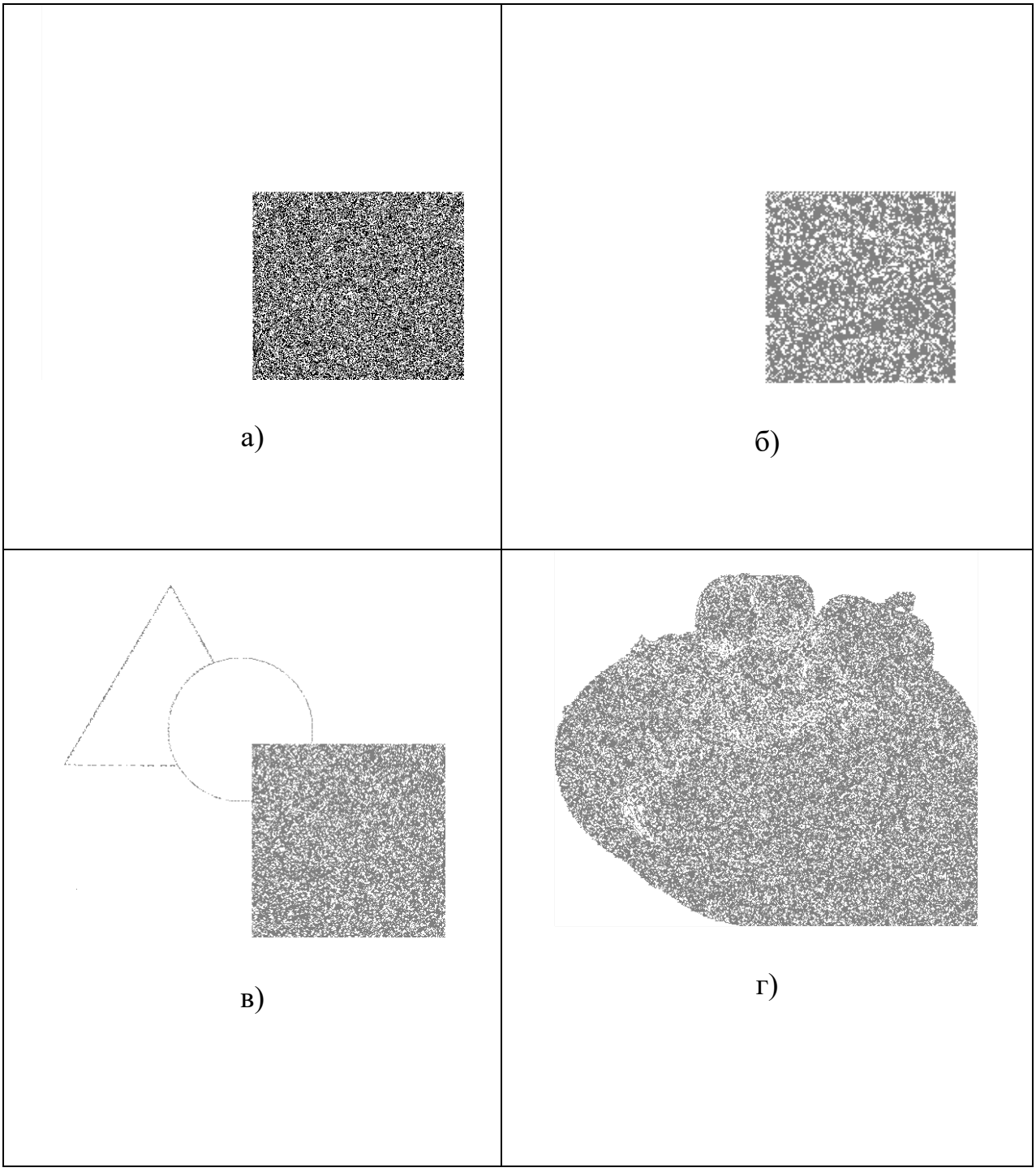


Рисунок 4 – Карты $map(x, y)$ для изображений, приведенных на Рисунках 1-3: а) исходная карта встраивания пикселей, б) градиентная заливка фона, в) искусственное изображение, г) фотографическое изображение

Проблема выделения области сосредоточения точек на плоскости относится к задачам таксономии. Используя алгоритм таксономии FOREL [16], разработаем алгоритм автоматического выделения области встраивания. В нашем случае таксоны будут иметь прямоугольную форму.

Алгоритм состоит из двух этапов. На первом этапе необходимо выделить прямоугольную область, полностью заполненную точками для того, чтобы отделить пустые области, в которые точно не производилось встраивание. На втором этапе внутри полученного прямоугольника необходимо выделить область с повышенной концентрацией точек. Добавим параметр p, характеризующий плотность единичных значений; формула для его вычисления выглядит следующим образом:

$$p = P_1/P, \tag{7}$$

где P – размер некой области, P_1 – количество пикселей, которые имеют единичное значение в этой области.

После чего нужно выделить на плоскости область, у которой самая высокая плотность точек.

Пусть изображение имеет размеры $M \times N$. Будем искать прямоугольник, характеризующийся координатами (x_1, y_1) – левый верхний угол, (x_2, y_2) – правый нижний угол. В начале работы алгоритма полагаем $x_1=0$, $y_1=0$, $x_2=M$, $y_2=N$. Вычисляем общее количество единичных битов P_0 внутри этого прямоугольника. Изменять размеры координат прямоугольника будем с шагом h. Значение h является параметром алгоритма. Оптимальный выбор значения h осуществлялся в рамках компьютерного эксперимента.

Этап 1.

Шаг 1. Вычисляем $x_{11}=x_1-h$. Находим количество единичных битов P внутри прямоугольника (x_{11}, y_1) - (x_2, y_2).

Шаг 2. Если $P=P_0$, то $x_1=x_{11}$ и переходим к шагу 1, иначе – к шагу 3.

Шаг 3. Проделываем то же самое для координат x_2, y_1, y_2.

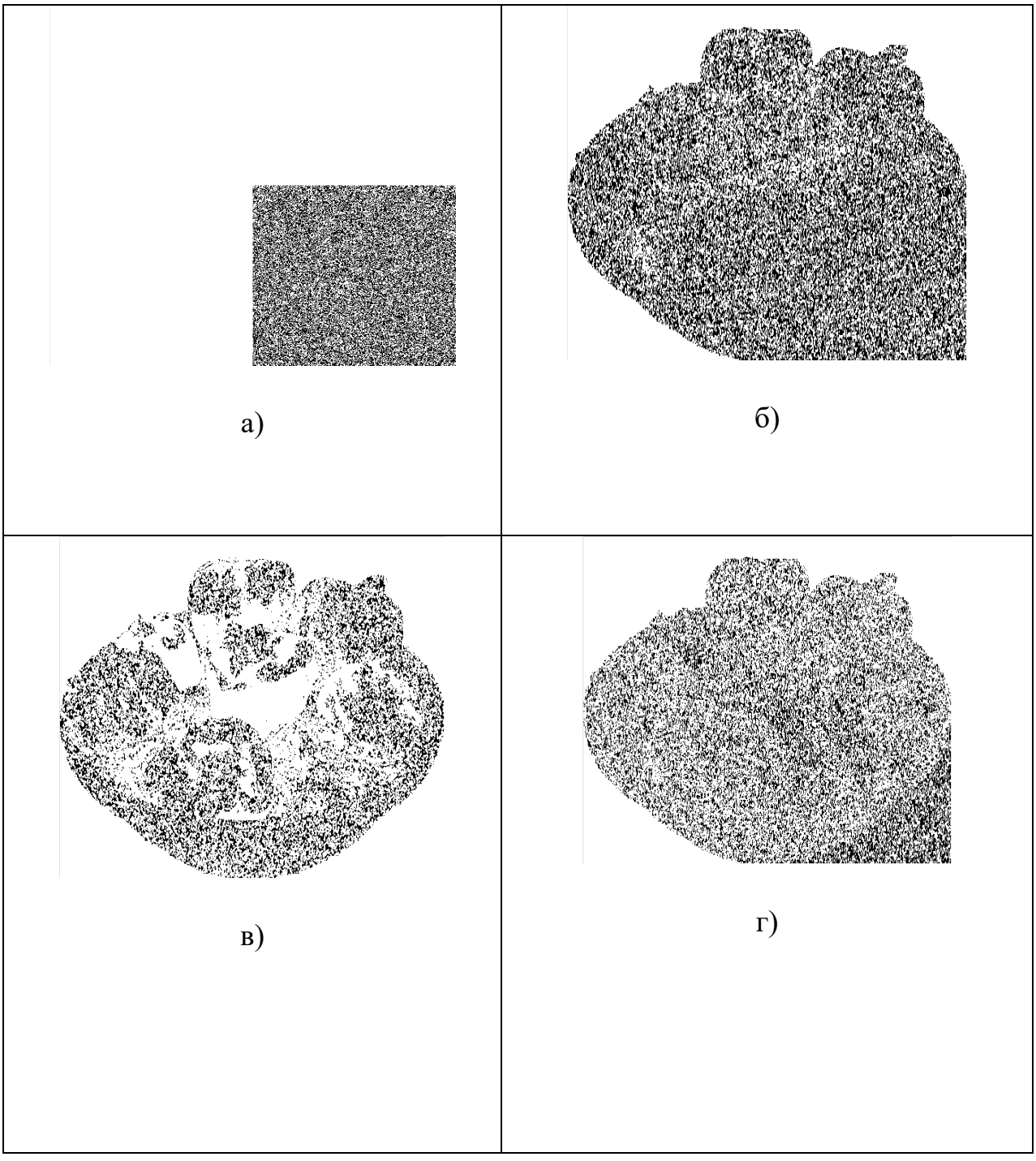


Рисунок 5 – Результат вычитания карты первого битового слоя из карты нулевого слоя для изображения, приведенного на Рисунке 3: а) исходная карта встраивания пикселей, б) нулевой битовый слой после градиентного преобразования, в) первый битовый слой после градиентного преобразования, г) результат вычитания первого битового слоя из нулевого битового слоя

После выполнения первого этапа будет локализована область, в которой есть единичные биты.

Этап 2.

Шаг 1. Вычисляем плотность единичных битов внутри прямоугольника (x_1, y_1)-(x_2, y_2):

$$p_0 = P/((y_2 - y_1)(x_2 - x_1)). \quad (8)$$

Шаг 2. Берем $x_{11}=x_1-h$. Вычисляем значение плотности единичных битов p для прямоугольника (x_{11}, y_1)-(x_2, y_2).

Шаг 3. Если $p>p_0$, то $x_1=x_{11}$, $p_0=p$ и переход на шаг 2, иначе – шаг 4.

Шаг 4. Выполняем те же шаги для x_2, y_1, y_2.

На выходе получаем координаты вершин прямоугольника (x_1, y_1), (x_2, y_2).

2.5 Компьютерный эксперимент и результаты

Апробация алгоритма осуществлена на 70 искусственных и фотографических изображениях. Локализация области подмененных бит является одной из задач, которая ставится перед стегоанализом. Встраивание осуществлялось в виде потока бит, которые представляли собой текстовую строку. Компонента синего цвета была выбрана для встраивания.

Во всех случаях выполнялось преобразование, устраняющее влияние градиентной заливки на первый и нулевой битовые слои. После чего выполнялось вычитание первого битового слоя из нулевого битового слоя. Далее выполнялся поиск таксонов.

Компьютерный эксперимент проводился при значениях шага алгоритма таксономии h=1, 2, 3, 4, 5, 10, 15, 20. Определялись координаты левого верхнего угла прямоугольника и правого нижнего угла. После этого вычислялась относительная погрешность ошибки определения координат точек как отношение разности координат к общей длине изображения контейнера по соответствующей оси:

$$\begin{aligned} \Delta x_1 &= |x_{10} - x_1|/M, \\ \Delta x_2 &= |x_{20} - x_2|/M, \\ \Delta y_1 &= |y_{10} - y_1|/N, \\ \Delta y_2 &= |y_{20} - y_2|/N, \end{aligned} \tag{9}$$

где (x_{10}, y_{10}), (x_{20}, y_{20}) – координаты углов прямоугольника, в который выполняется встраивание.

Эксперименты со встраиванием в фотографические изображения осуществлялись с двумя положениями прямоугольной области встраивания. В первом случае прямоугольная область встраивания имела большую площадь пересечения с областью градиентной заливки изображения-контейнера. Во втором случае площадь такого пересечения была маленькой.

В таблице 1 приведены средние ошибки определения координат прямоугольника встраивания в зависимости от значения величины шага h.

Таблица 1 – Средние ошибки определения координат прямоугольника встраивания при различных значениях шага h

h	Δx_1(%)	Δy_1(%)	Δx_2(%)	Δy_2(%)
Искусственные изображения				
1	0,56	0,21	0,19	0,21
2	0,56	0,42	0,56	0,42
3	0,74	1,25	0,93	0,63
4	0,93	1,67	0,93	0,83
5	1,30	1,04	2,41	1,04
10	3,15	8,33	2,41	2,08
15	4,07	9,38	4,26	3,13
20	6,85	16,67	17,22	4,17
Фотографические изображения (первый случай)				
1	14,26	10,83	0,37	0,42
2	5,93	7,92	0,74	0,83
3	3,33	8,13	1,67	1,25

4	4,07	7,50	2,22	0,83
5	3,70	7,29	1,85	1,04
10	5,56	6,25	3,70	2,08
15	5,56	6,25	2,78	3,13
20	5,56	4,17	3,70	4,17
Фотографические изображения (второй случай)				
1	20,37	6,25	1,30	6,25
2	9,07	2,08	10,56	17,50
3	9,26	1,88	13,15	17,50
4	8,70	1,67	12,78	26,67
5	8,89	1,04	13,52	27,08
10	0,56	0,00	13,52	27,08
15	1,48	0,00	15,37	37,50
20	0,56	4,17	8,70	45,83

Если посмотреть на данные из таблицы 1, то видно, что для искусственных изображений возможно достаточно точное определение области встраивания. Причем наилучших результатов удается достичь при малых значениях шага h. Для фотографических изображений, в силу особенностей строения нулевого слоя, оптимальным является шаг близкий к значению 5. На Рисунке 6 приведены результаты выделения области встраивания для искусственных изображений при различном значении шага. Аналогичные результаты для двух случаев встраивания в фотографическое изображение приведены на Рисунках 7 и 8.

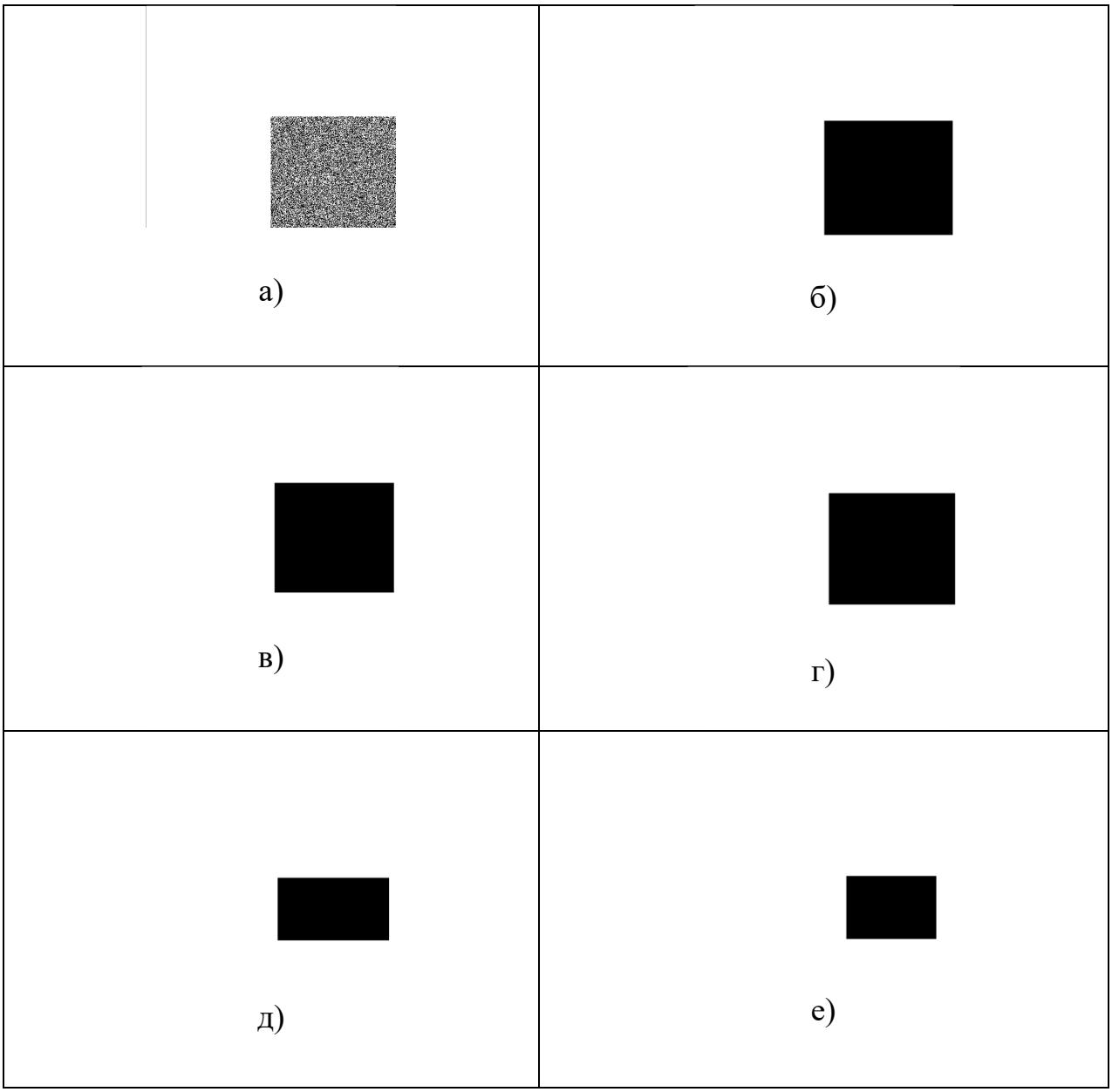


Рисунок 6 – Результаты работы алгоритма по выделению областей встраивания для искусственного изображения, приведенного на Рисунке 1: а) маска встраивания, б) $h = 1$, в) $h = 5$, г) $h = 10$, д) $h = 15$ е) $h = 20$

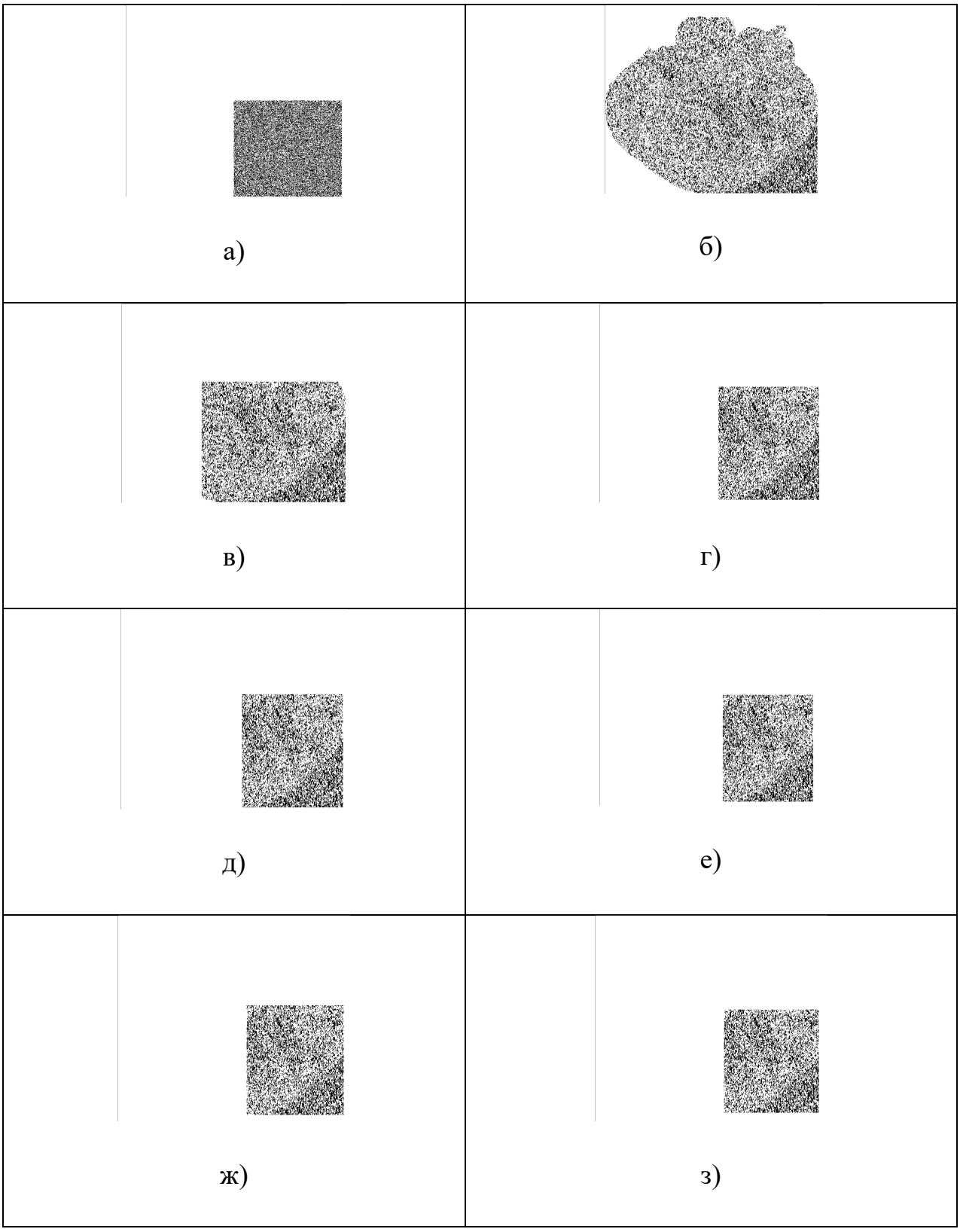


Рисунок 7 – Результаты работы алгоритма по выделению областей встраивания для фотографического изображения, рисунок 3 (первый случай):
а) маска встраивания, б) разность нулевого и первого битовых слоев, в) $h = 1$, г) $h = 3$, д) $h = 5$, е) $h = 10$, ж) $h = 15$, з) $h = 20$

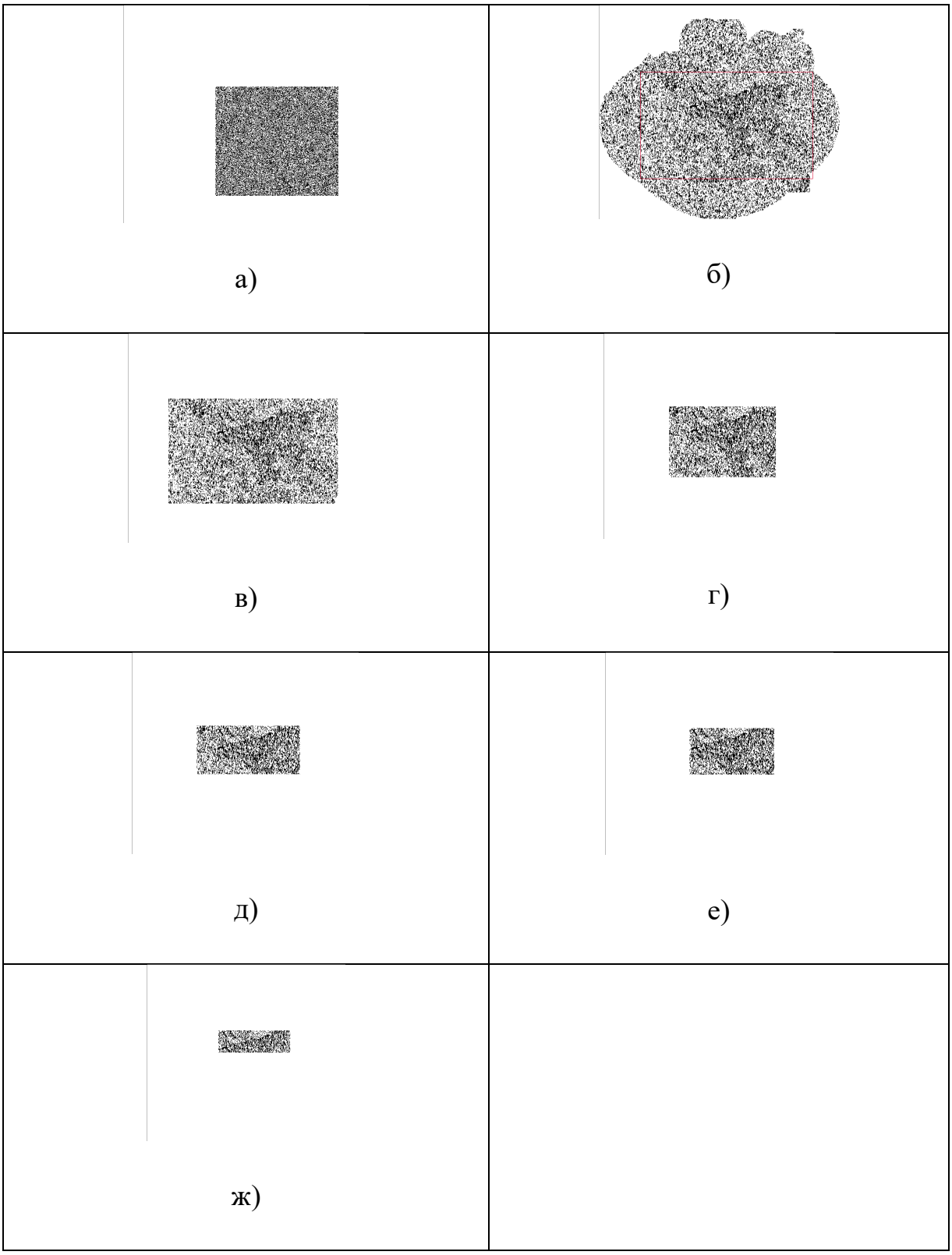


Рисунок 8 – Результаты работы алгоритма по выделению областей встраивания для фотографического изображения, рисунок 3 (второй случай):
а) маска встраивания, б) разность нулевого и первого битовых слоев, в) $h = 1$, г) $h = 3$, д) $h = 5$, е) $h = 10$, ж) $h = 15$

2.6 Обсуждение результатов

Предложенный в данной главе алгоритм обнаружения вставок методом LSB-замены позволяет обнаруживать встроенное сообщение, если область встраивания имеет пересечение с областями градиентной либо равномерной заливки на изображении. Следует отметить, что подобная зависимость от структуры изображения-стегоконтейнера наблюдается для всех методов стегоанализа. Компьютерный эксперимент на коллекции изображений показал, что при LSB-замене битов нулевого слоя менее чем на 25% эффективность обнаружения СГВ составляет 91%, что сопоставимо с результатами статистических методов при высоком заполнении стегоконтейнера [61,104] (86% и 90% соответственно).

Помимо этого, разработанный алгоритм может не только устанавливать факт наличия СГВ, но и позволяет определять расположение СГВ и ее размер. Разработанный алгоритм досконально исследует каждый пиксель; подобный механизм расширяет возможности его использования. Если в областях встраивания не присутствуют области равномерной заливки, то процесс встраивания сообщения не окажет влияния на статистические характеристики изображения.

Изображения, у которых «средние» характеристики, можно достаточно успешно обрабатывать статистическими методами. Однако, в случае наличия ряда особенностей у структуры изображения, применение статистических методов окажется малоэффективным. Необходимо отметить, что использование метода одиночного анализа пикселей показывает высокую эффективность не для всех изображений. Данный факт вызван тем, что наличие пересекающихся области встраивания и большой области градиентной заливки на первоначальном изображении является здесь обязательным условием. Подобное условие является достаточно распространенным, так его предъявляют и прочие методы выявления СГВ.

К главному преимуществу разработанного алгоритма стоит отнести возможность устанавливать положение и размер СГВ. Очень сильно на

эффективность работы разработанного алгоритма оказывает влияние количество мелких деталей, присутствующих на изображении. Поскольку информация о существовании научных работ подобной направленности отсутствует, определено, что наиболее близкой задачей является поиск пикселей, которые повреждены импульсным шумом. Однако, следует отметить низкий уровень сложности данной задачи по сравнению с исследуемой в данной работе. Основанием для подобного утверждения является большая величина изменений, которым подвергается изображение. В [18] описывается, как алгоритм SD-ROM выявляет с эффективностью 95% поврежденные пиксели, а ложных срабатываний при этом не больше 36%

Выводы по второй главе

Предложенный в данной главе алгоритм анализа нулевого слоя стегоконтейнера даёт возможность определить наличие стеганографического встраивания методом LSB-вставок. Вместе с тем:

1. Алгоритм даёт возможность выявлять СГВ при относительном низком заполнении контейнера. Эффективность обнаружения СГВ с заполнением стегоконтейнера ниже 25% составляет 91%, что сопоставимо с эффективностью статистических методов, применяемых для высоких значений заполнения стегоконтейнера.

2. Применение алгоритма таксономии даёт возможность локализовать область встраивания в автоматическом режиме. При этом для искусственных изображений границы области встраивания могут быть определены с ошибкой, не превышающей 2%. Для фотографических изображений ошибка определения границ области встраивания составляет 21%, что является приемлемым результатом. Аналогичные алгоритмы определения положения зашумленных пикселей [97] допускают ошибку до 37%.

Результаты данной главы опубликованы в работах [8,27].

ГЛАВА 3. ВЫЯВЛЕНИЕ LSB-ВСТАВОК С ПОМОЩЬЮ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

3.1 Введение

Как было показано в предыдущей главе, анализ только нулевого слоя позволяет выявлять часть пикселей, в которых осуществлена замена младших битов. Однако информации только о нулевом слое недостаточно для эффективного определения стеганографических вставок. Для повышения эффективности стеганографического анализа необходимо учитывать структуру исходного изображения-контейнера, которая хранится в более высоких битовых слоях, как было указано в первой главе.

Простое вычитание значения битов первого слоя из битов нулевого слоя, выполненное во второй главе, позволяет уменьшить процент ложных срабатываний, вызванных мелкими деталями исходного изображения. Однако удается удалить далеко не все особенности, что сказывается на итоговых результатах стегоанализа. Для повышения эффективности обнаружения подмененных пикселей необходимо не просто вычитать один слой из другого, а проводить их сравнение на основе алгоритмов анализа и принятия решений.

В данной главе предлагается алгоритм выявления подмененных пикселей, встраивание в которые осуществлялось в наименее значимый бит, с помощью метода анализа иерархий, и, таким образом, будет учитываться структура нескольких битовых слоев.

Проведём анализ изображений, в которые встраивалась информация в виде стеганографических вставок.

Сформулируем два предположения:

1. Доподлинно неизвестно есть ли СГВ.

2. Нет информации ни о количестве встроенных битов, ни об их расположении.

Следовательно, задача формулируется как: необходимо установить, присутствует ли на изображении СГВ, и, если да, то, в какое количество пикселей была осуществлена подмена младших битов синей компоненты. Данную задачу усложняет второе предположение. Это связано с тем, что может возникнуть ситуация, когда у синей компоненты все младшие пиксели будут подменены. В подобном случае проведение анализа нулевого слоя может оказаться бесполезным или, по крайней мере, неизвестно заранее какова эффективность (и есть ли она) этого анализа.

Значит, необходимо анализировать более высокие слои. Для этого выдвинем предположение о плавном послойном изменении закономерностей. Таким образом, при анализе ближайших слоев возможно использование одних и тех же закономерностей. Для этого отдельно проанализируем нулевой слой и три слоя вблизи нулевого. В дальнейшем построим схему для принятия решения.

С целью получения наилучших результатов, осуществим предварительную обработку изображения, в ходе которой должны быть исключены равномерная и градиентная заливки. В дальнейшем работа сводится к взаимодействию с картой преобразованных пикселей.

В виде бинарной матрицы цветов $B_{ij}^{(k)}$ зададим k-ый слой синей компоненты первоначального изображения. Через матрицу R_{ij} установим координаты встраиваемой информации. Если была замена, то $R_{ij} = 1$, если нет, то $R_{ij} = 0$. При встраивании происходит формирование матрицы $A_{ij}^{(0)}$ вместо нулевого слоя $B_{ij}^{(0)}$. В результате, решаемая задача сводится к максимальному восстановлению матрицы R_{ij} из анализа матриц $A_{ij}^{(0)}$, $B_{ij}^{(1)}$, $B_{ij}^{(2)}$, $B_{ij}^{(3)}$.

3.2 Применение метода анализа иерархий для выявления стеганографических вставок

Метод анализа иерархий [96] дает возможность принять решение о наличии или отсутствия факта подмены бита. Сформулируем те альтернативные решения, из которых будет выбрано окончательное решение. Кроме того, определим критерии отбора для сформулированных альтернативных решений.

Таким образом, задача имеет единственное решение:

Y – при условии наличия факта подмены младшего бита в данном пикселе.

N – при условии отсутствия факта подмены младшего бита в данном пикселе.

Для определения замененных битов следует сформировать систему аналитического состояния нулевого слоя посредством последовательного анализа каждого из младших битов на предмет выявления наличия или отсутствия различий значений анализируемого бита и его близлежащих соседей.

Для осуществления данного анализа следует использовать три основных критерия:

Критерий K_1 – характеризует идентичность или отклонения между значениями анализируемого бита и соседних по сторонам битов. Данный критерий позволяет определить принадлежность (или отсутствие принадлежности) анализируемого бита к определенной вертикальной или горизонтальной структуре, присутствующей на изображении.

Критерий K_2 – характеризует идентичность или отклонения между значениями анализируемого бита и соседних по углам битов. Данный критерий позволяет определить принадлежность (или отсутствие принадлежности) анализируемого бита к определенной диагональной структуре, присутствующей на изображении.

Критерий K_3 – характеризует идентичность или отклонения между значениями анализируемого бита и среднего значения окружающих 8 битов. Данный критерий позволяет определить принадлежность (или отсутствие

принадлежности) анализируемого бита к определенной области градиентной или равномерной заливки.

Таким образом критерии K_1 и K_2 позволяют определить протяженные области изображения одного цвета, а критерий K_3 – установить области с градиентной заливкой. Принятие решения R о наличии или отсутствии замены младшего бита осуществляется с использованием двухуровневого иерархического дерева альтернатив, представленное на Рисунке 9.

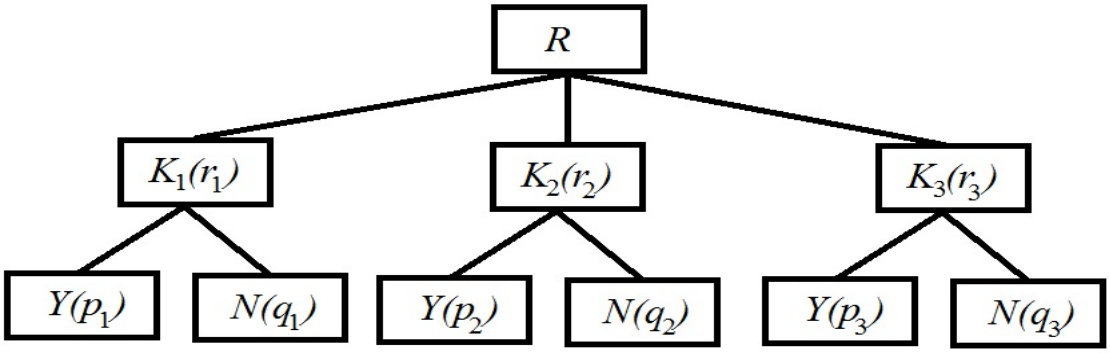


Рисунок 9 – Иерархия критериев для установления подмены бита из анализа нулевого слоя

Использование двухуровневого иерархического дерева альтернатив предполагает необходимость определения относительного веса критериев r_i ($i = 1,2,3$), и веса решений в рамках одного критерия p_i и q_i ($i = 1, 2, 3$). Определим иерархическую взаимосвязь посредством установления степени значимости всех трех критериев относительно друг друга следующим образом: K_1значимее K_2 в n раз, K_2 значимее K_3 в k раз, а K_1 значимее K_3 в nk раз. В результате получаем следующую матрицу:

	K_1	K_2	K_3
K_1	1	n	kn
K_2	$1/n$	1	k
K_3	$1/(kn)$	$1/k$	1

Посредством классических способов [18], из получившейся матрицы определяются весовые коэффициенты:

$$r_1 = \frac{nk}{nk+k+1}, r_2 = \frac{k}{nk+k+1}, r_3 = \frac{1}{nk+k+1} \quad (10)$$

Одним из недостатков классического алгоритма анализа иерархий является использование экспертных оценок в качестве опоры для принятия решений. Данный подход не позволяет раскрыть все широкие возможности данного метода, что связано, прежде всего с тем, что экспертные оценки не являются в полной мере объективными и позволяют получить только парные сравнения.

Однако подобное ограничение можно достаточно легко преодолеть воспользовавшись объективными показателями. В целях нашего анализа, такими объективными показателями являются соотношения степеней значимости n и k. Анализ простейших примеров позволит сузить диапазон искомых значений, выделив объективные ограничения значений данных параметров, а проведение компьютерного эксперимента впоследствии позволит установить их оптимальные значения, равно как и оптимальные значения параметра l.

Следующим шагом здесь является определение весовых коэффициентов критериев K_1, K_2 и K_3.

Для определения веса решений по первому критерию K_1, необходимо сформировать матрицу парных сравнений, получаемую при сопоставлении значений анализируемого бита и четырех соседних по сторонам битов. Если соблюдается условие абсолютной идентичности значений всех пяти битов, то, следовательно, можно сделать вывод, что анализируемый бит является исходным (не заменённым), а решение N имеет значительно больший вес по сравнению с весом решения Y. Кратность значимости веса решения N в таком случае составляет $\frac{x}{4-x}$ раз. В итоге, после проведения необходимых преобразований вычисляем следующие значения коэффициентов:

$$p_1 = \frac{4-x}{4}, q_1 = \frac{x}{4}. \quad (11)$$

Аналогичным образом определим вес решений по второму критерию K_2, для чего сформируем матрицу парных сравнений, получаемую при сопоставлении значений анализируемого бита и четырех соседних по углам битов (битов с угловым соприкасанием). Предположим, что значения y битов совпадают со значением анализируемого бита, то значения весовых коэффициентов по критерию K_2 будут следующие:

$$p_2 = \frac{4-y}{4},\ q_2 = \frac{y}{4}. \tag{12}$$

Для определения значения весов по критерию K_3 обозначим что значение анализируемого бита равно c, а среднее значение восьми окружающих его битов будет равно c_0. Далее предположим, что решение N имеет значительно больший вес по сравнению с весом решения Y в a раз, где величина a находится в зависимости от абсолютного значения отклонения значения бита c от среднего значения окружающих битов c_0 ($dc = |c - c_0|$). Весовые коэффициенты:

$$p_3 = \frac{1}{a+1},\ q_3 = \frac{a}{a+1} \tag{13}$$

Опишем предельные случаи. Если значение рассматриваемого бита равно среднему значению окружающих битов ($dc = 0$), то примем, что он не заменён. В таком случае у коэффициентов значения будут следующими: $p_3 = 0$, $q_3 = 1$. Если бит максимально отличается от окружающих ($dc = 1$), то примем его однозначно заменённым, т.е. $p_3 = 1$, $q_3 = 0$. Значит, при $dc = 0$ должно быть $a \to \infty$. При значении $dc = 1$ необходимо, чтобы $a = 0$. Обозначенным условиям будет удовлетворять:

$$a = \frac{1}{dc} - 1. \tag{14}$$

При этом значения для весовых коэффициентов:

$$p_3 = dc\ , q_3 = 1 - dc. \tag{15}$$

Для окончательного принятия решения нужно определить величины:

$$P(Y) = r_1 p_1 + r_2 p_2 + r_3 p_3,\ P(N) = r_1 q_1 + r_2 q_2 + r_3 q_3. \tag{16}$$

Если $P(Y) > P(N)$, то принимается решение Y, т.е. бит является заменённым, в ином случае, когда $P(Y) \leq P(N)$, принимается решение N, т.е. бит не заменён.

Для вычисления всех вероятностей и коэффициентов в программном комплексе применялся тип данных с плавающей точкой.

Для проведения иерархического анализа исследуемого бита, следует расширить описанный выше метод так, чтобы было возможным его применение для целей сравнительного анализа нулевого и трех вышележащих слоев. Для этого следует в качестве объекта сравнения использовать окно в каждом из анализируемых слоев, т.е. бит, который расположен над анализируемым совместно с окружающими его восьмью битами.

Рассмотрим 3 главные конструкции на изображении: горизонтальные и вертикальные линии, диагональные линии, области градиентной либо равномерной заливки. Указанные конструкции имеют определенные закономерности распределения битов на нулевом слое и нескольких более высоких слоях, расположенных непосредственно над ним. В целях повышения точности анализа и выявления стеганографических вставок указанные конструкции необходимо дополнить специальными критериями решений. Подобная необходимость вызвана наличие вероятности нарушения анализируемым битом существующей закономерности в структуре и статистике изображения. Таким образом, предложенные ниже критерии призваны установить наличие или отсутствие нарушений закономерностей при проведении анализа k-го слоя ($k = 1,2,3$):

$K_1^{(k)}$ – в окне k-го слоя наблюдается идентичность или отклонения между значениями анализируемого бита и соседних по сторонам битов. В рамках данного критерия проводится проверка: вписывается ли рассматриваемый бит в нулевом слое в вертикальные и горизонтальные линии на изображении. При этом наличие вертикальных и горизонтальных линий устанавливается по более высоким битовым плоскостям.

$K_2^{(k)}$ – в окне k-го слоя наблюдается идентичность или отклонения между значениями анализируемого бита и соседних по углам битов. Целевым назначением данного критерия является проверка наличия согласованности, а следовательно, и соблюдения необходимых закономерностей, значений

анализируемого бита нулевого слоя и значений битов трех вышележащих слоев в диагональном разрезе, т.е. по диагональным линиям этих слоев.

$K_3^{(k)}$ – отклонение значения бита в нулевом слое от среднего значения битов окна в k-ом слое. Здесь устанавливается, соответствует ли значение бита в нулевом слое окружающей области градиентной либо равномерной заливки. Иерархическое дерево, состоящее их трёх уровней, представлено на Рисунке 10. R – это окончательное решение. Если происходит встраивание сообщения, то меняется нулевой слой.

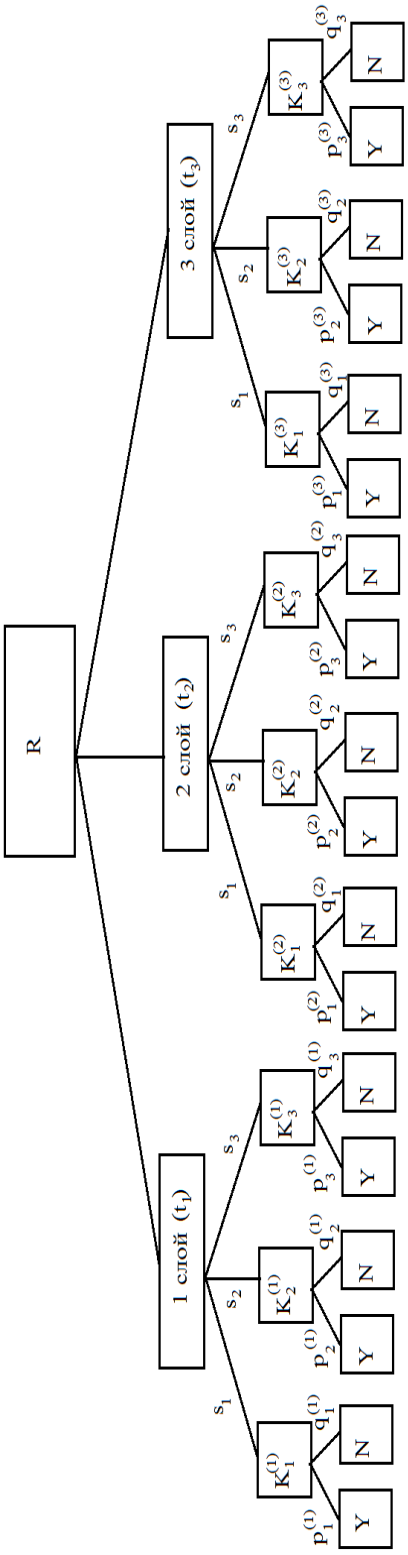


Рисунок 10 – Иерархия критериев для выявления замены бита из анализа вышележащих слоев

Следовательно, нарушаются закономерности следования битов. Выделение первоначальных закономерностей производится при перекрестном сравнении битов нулевого слоя. Кроме того, поскольку анализ включает также три слоя более высокого уровня, а именно, первого, второго и третьего, то сравнительный анализ битов указанных слоев с битами нулевого слоя также позволяет выявить такие закономерности. Результирующим здесь является решение об абсолютной равнозначности анализируемых слоев, и, следовательно, весовые коэффициенты могут быть признаны равными:

$$t_1 = t_2 = t_3 = \frac{1}{3}. \tag{17}$$

Линии в вертикальном, горизонтальном и диагональном направлениях, на фотографических изображениях, встречаются с равной вероятностью. Помимо этого, подменяемый бит с равной вероятностью может попасть как на область градиентной или равномерной заливки, так и на границу изображения. Поэтому, в рамках одного слоя, все три критерия равнозначны:

$$s_1 = s_2 = s_3 = \frac{1}{3}. \tag{18}$$

Методология установления весовых коэффициентов, примененная ранее в рамках анализа нулевого слоя, является универсальной и может быть применена для установления весовых коэффициентов по двум решениям в рамках одного критерия без каких либо дополнительных модификаций.

Таким образом, веса по 1-му критерию имеют вид:

$$p_1^{(k)} = \frac{4-x^{(k)}}{4},\ q_1^{(k)} = \frac{x^{(k)}}{4}, \tag{19}$$

где $x^{(k)}$ – количество соседних по сторонам бит, обладающих идентичными значениями в окне k-слоя.

Весовые коэффициенты по 2-му критерию имеют вид:

$$p_2^{(k)} = \frac{4-y^{(k)}}{4},\ q_2^{(k)} = \frac{y^{(k)}}{4}, \tag{20}$$

где $y^{(k)}$ – количество соседних по диагонали бит, обладающих идентичными значениями в окне k-слоя.

Наконец, весовые коэффициенты по 3-му критерию имеют вид:

$$p_3^{(k)} = dc^{(k)},\ q_3^{(k)} = 1 - dc^{(k)}, \quad (21)$$

где $dc^{(k)}$ – отличие значения бита от среднего значения битов окна в k-ом слое.

Основная суть предлагаемого алгоритма принятия решения в рамках стегоанализа может быть описана следующим образом. Осуществляется последовательное прохождение каждого из пикселей изображения и их анализ на предмет подтверждения или опровержения факта замены младшего бита по каждому из них. Положительное (обнаружена замена) или отрицательное (замена не обнаружена) решения основывается на сравнении значений бита анализируемого пикселя и значений соседних с ним битов. В результате прохождения всех пикселей формируется перечень тех пикселей, для которых было принято положительное решение, что означает обнаружение факта LSB-замены, т.е. в данные пиксели было встроено какое-либо сообщение.

Одним из преимуществ предлагаемого алгоритма является его линейная трудоемкость, обусловленная единственным проходом с конечным и заранее определенным количеством шагов. Также к преимуществам алгоритма можно отнести легкость его распараллеливания посредством простого разделения изображения на несколько областей, обусловленная узкой локализацией данных вокруг анализируемого пикселя, на основе которых принимается конечное решение

На выходе данный алгоритм позволяет сформировать матрицу решений R. Данная матрица состоит из единиц и нулей и обладает размерами, идентичными с размерами изображения, где единица соответствует решению Y (младший бит пикселя заменен), а нуль – решению N (младший бит пикселя не заменен). Графически полученная матрица может быть представлено в виде однобитного черно-белого изображения, где 1 – черные точки, 0 – белые точки.

3.3 Алгоритм выделения области встраивания

На базе алгоритма таксономии FOREL [16] был создан алгоритм для выделения области встраивания. Алгоритм таксономии FOREL объединяет точки в таксоны, располагающиеся внутри окружности. У нас таксон будет прямоугольной формы.

Введём показатель плотности единичных значений p. В случае, если в некоторой области изображения присутствует N пикселей, и из них у N_1 будет единичное значение, то $p = N_1/N$.

Будем искать прямоугольные области с плотностью единичных значений величины p_0. В качестве входного параметра алгоритма установим параметр R_0 – начальный размер таксона.

Алгоритм состоит из шагов:

Шаг 1. Выбирается исходное значение размера таксона $R = R_0$.

Шаг 2. Случайным образом выбирается точка с координатами (x_1, y_1), выполняющая центра таксона. Строится квадрат, у левого верхнего угла которого координаты равны $(x_1 - R, y_1 - R)$, а правый нижний угол имеет координаты $(x_1 + R, y_1 + R)$.

Шаг 3. Осуществляем поиск координаты центра масс точек, находящейся внутри построенного квадрата (x_2, y_2).

Шаг 4. Если точки (x_1, y_1) и (x_2, y_2) будут совпадать, то следует перейти к Шагу 5, в противном случае $x_1 = x_2$, $y_1 = y_2$ и переход к Шагу 2.

Шаг 5. Вычисляем показатель плотности единичных значений p.

Шаг 6. Если $p > p_0$, то $R := 1.1R$ и переход к Шагу 3.

Шаг 7. Если $p < p_0$, то $R := 0.9R$ и переход к Шагу 3.

Шаг 8. Если $\mathrm{p} = p_0$, то переход к Шагу 2.

Выполнения алгоритма осуществляется до тех пор, пока не будет произведено объединение всех точек нулевого слоя в соответствующие таксоны.

В качестве областей возможного встраивания сообщения следует выбрать таксоны с размером от 10% начального изображения.

3.4 Компьютерный эксперимент и результаты

Компьютерный эксперимент проводился для изображений двух типов: фотографические и искусственные. В качестве задачи стегоанализа ставилось определение области с располагающимися в ней подменёнными битами. Области встраивания представляли собой прямоугольную область с размером $\frac{1}{4}$ от максимальной области стегоконтейнера изображения. В синюю компоненту изображений встраивалась текстовая строка.

На Рисунке 11 отображены результаты работы алгоритма для изображения, которое представляет собой изображение с равномерной заливкой.

Из Рисунка 11 видно: в результате работы алгоритма на искусственном изображении с равномерной заливкой достаточно точно выявляется область встраивания. Разделение начального прямоугольника на группу прямоугольников обусловлено распределением нулевых и единичных битов внутри самого сообщения.

На Рисунке 12 отображены результаты работы алгоритма на основе метода анализа иерархий для искусственного изображения с равномерной заливкой.

Результаты работы алгоритма для фотографических изображений представлены на Рисунке 13.

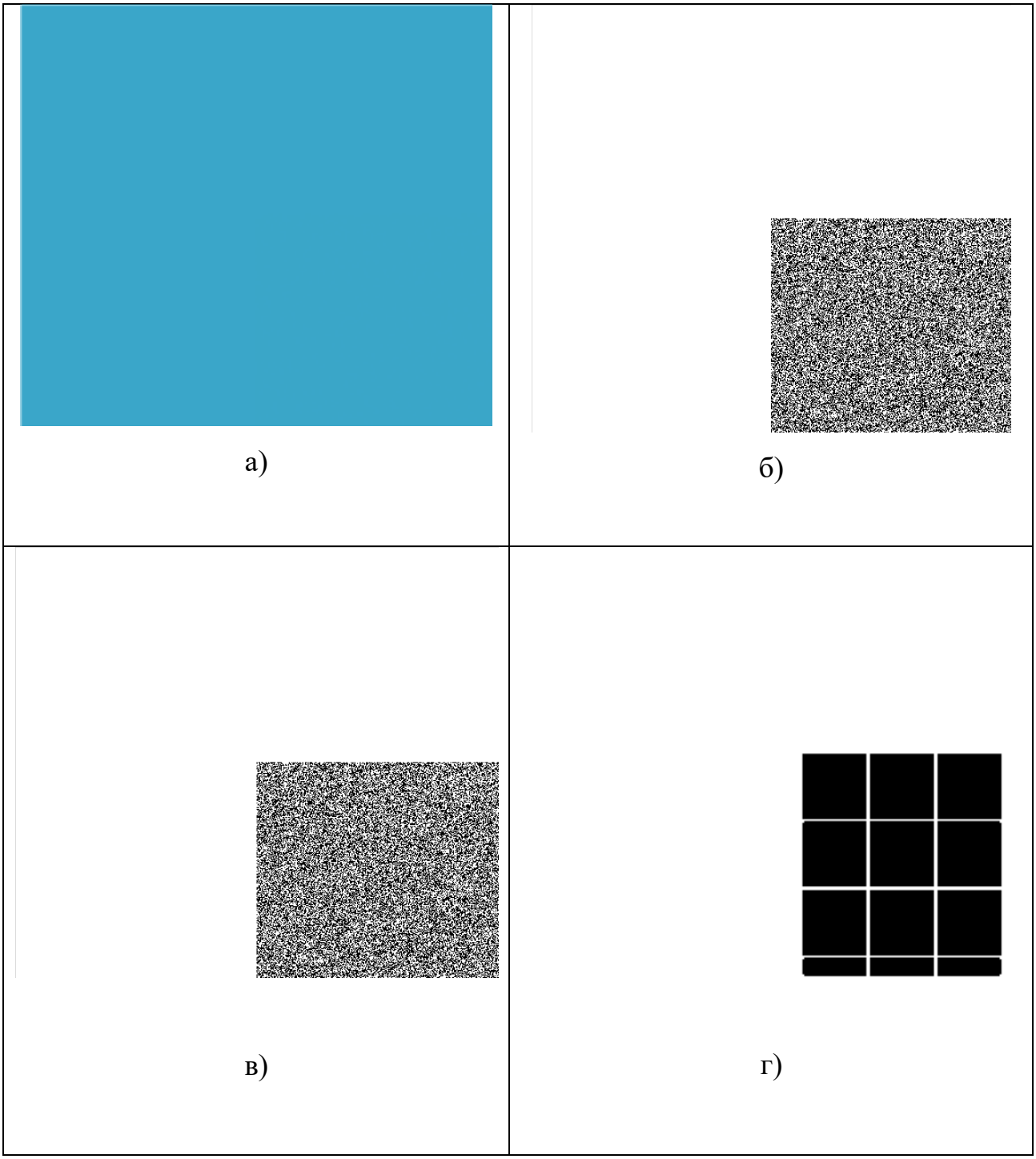
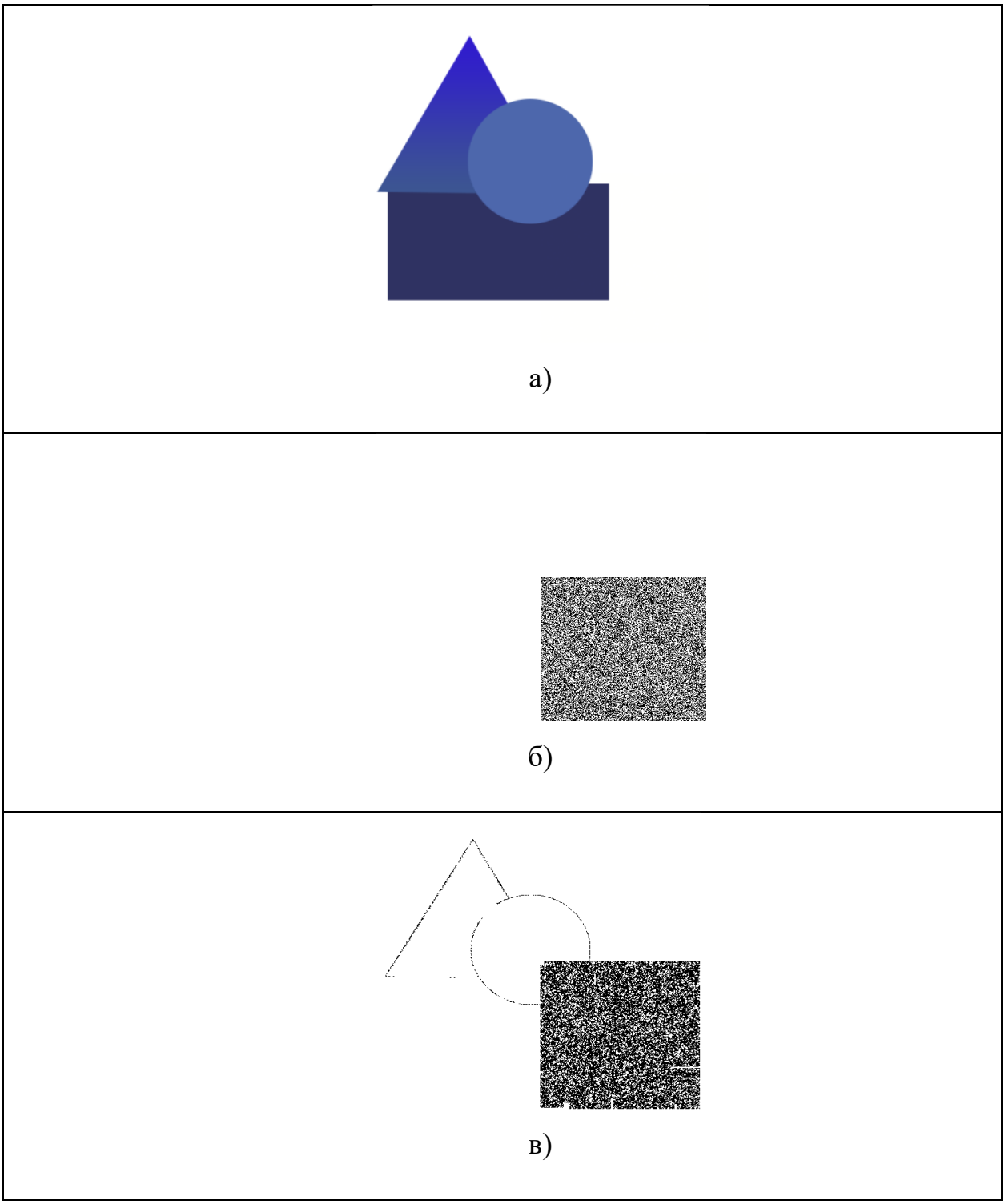


Рисунок 11 – Результаты работы алгоритма по автоматическому выделению области встраивания для изображения с равномерной заливкой: а) изображение со встроенной СГВ, б) карта встроенных пикселей, в) нулевой слой, г) автоматически выделенная область встраивания при $p = 0.5$



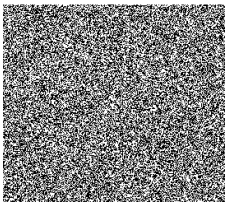
а)

б)

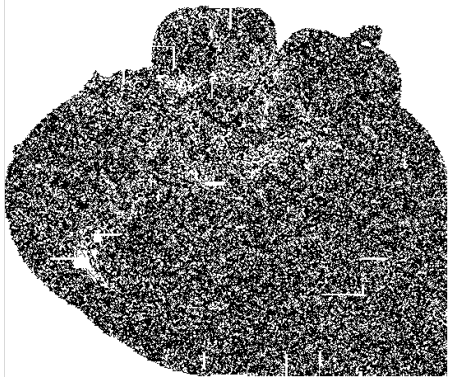
в)

Рисунок 12 – Визуализация матрицы решений R для искусственного изображения: а) изображение со встроенной СГВ, б) карта измененных пикселей (черным цветом выделены пиксели, значения которых изменены при встраивании), в) визуализированная матрица решений *R*

а)



б)



в)

Рисунок 13 – Визуализация матрицы решений R для фотографического изображения: а) изображение со встроенной СГВ, б) карта измененных пикселей (черным цветом выделены пиксели, значения которых изменены при встраивании), в) визуализированная матрица решений R

Как видно из этих двух рисунков, предложенный алгоритм позволяет визуализировать измененные пиксели в области равномерной или градиентной заливки, однако для областей, содержащих мелкие детали, происходят ложные срабатывания. Объяснение ошибочного срабатывания алгоритма состоит в том, что резкие границы и быстрые изменения цвета не могут быть устранены алгоритмом предварительной обработки. Однако сравнение рисунков 13а и 13в позволяет делать выводы о наличии в изображении встроенного сообщения и его расположении в правом нижнем углу.

Чтобы локализовать области встраивания для карт подозрительных пикселей, применим алгоритм таксономии. От выбора параметров R_0 и p зависят результаты работы алгоритма таксономии. Начальный размер таксона определяет первый параметр. В результате проведенного компьютерного эксперимента можно сделать вывод что, окончательный размер таксона незначительно отличается от исходного. На Рисунках 14-17 приведены результаты компьютерного эксперимента для изображений, которые отображены на Рисунках 11-13.

Было экспериментально установлено, что хорошие результаты получаются, если у показателяpзначения находятся в диапазоне от 0.50 – 0.60. Конкретное значение p будет зависеть от структуры изображения. Для искусственных изображений лучшие результаты получаются при более низких значениях p, а для фотографических изображений стоит выбирать значение p ближе к 0.60, так как это даёт возможность убрать лишние детали.

Из рисунков 14-17 видно: алгоритм таксономии не дает возможность выделить в виде одной прямоугольной области область встраивания СГВ. Посредством внутренних особенностей распределения битов выполняется разделение области на прямоугольные области меньшего размера. Для выявления одной области встраивания использовались два различных подхода.

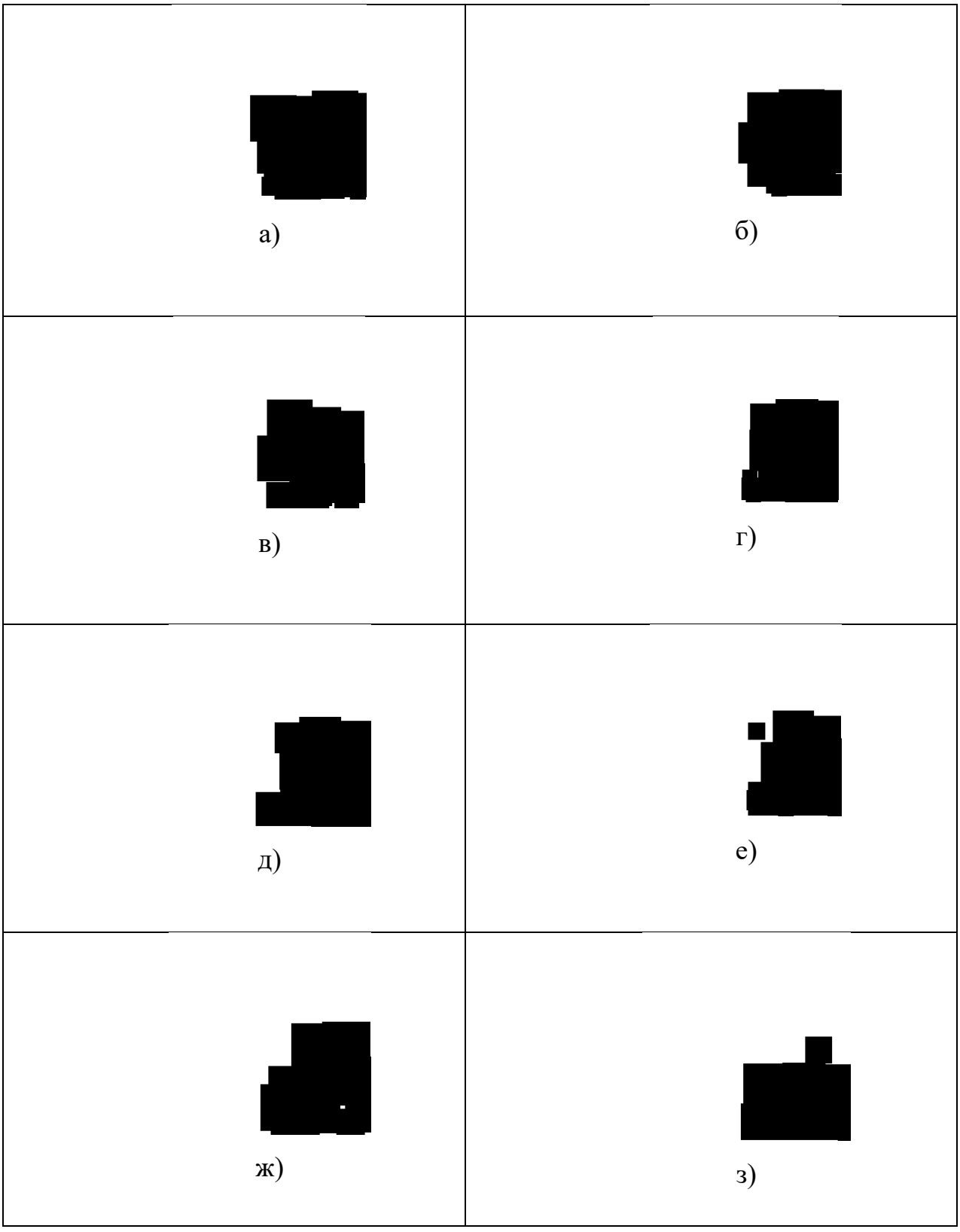


Рисунок 14 – Результаты автоматического выделения области встраивания для изображения, приведенного на Рисунке 12, для $R_0 = 30$: а) $p = 0.52$, б) $p = 0.53$, в) $p = 0.54$, г) $p = 0.55$, д) $p = 0.56$ е) $p = 0.57$ ж) $p = 0.58$ з) $p = 0.60$

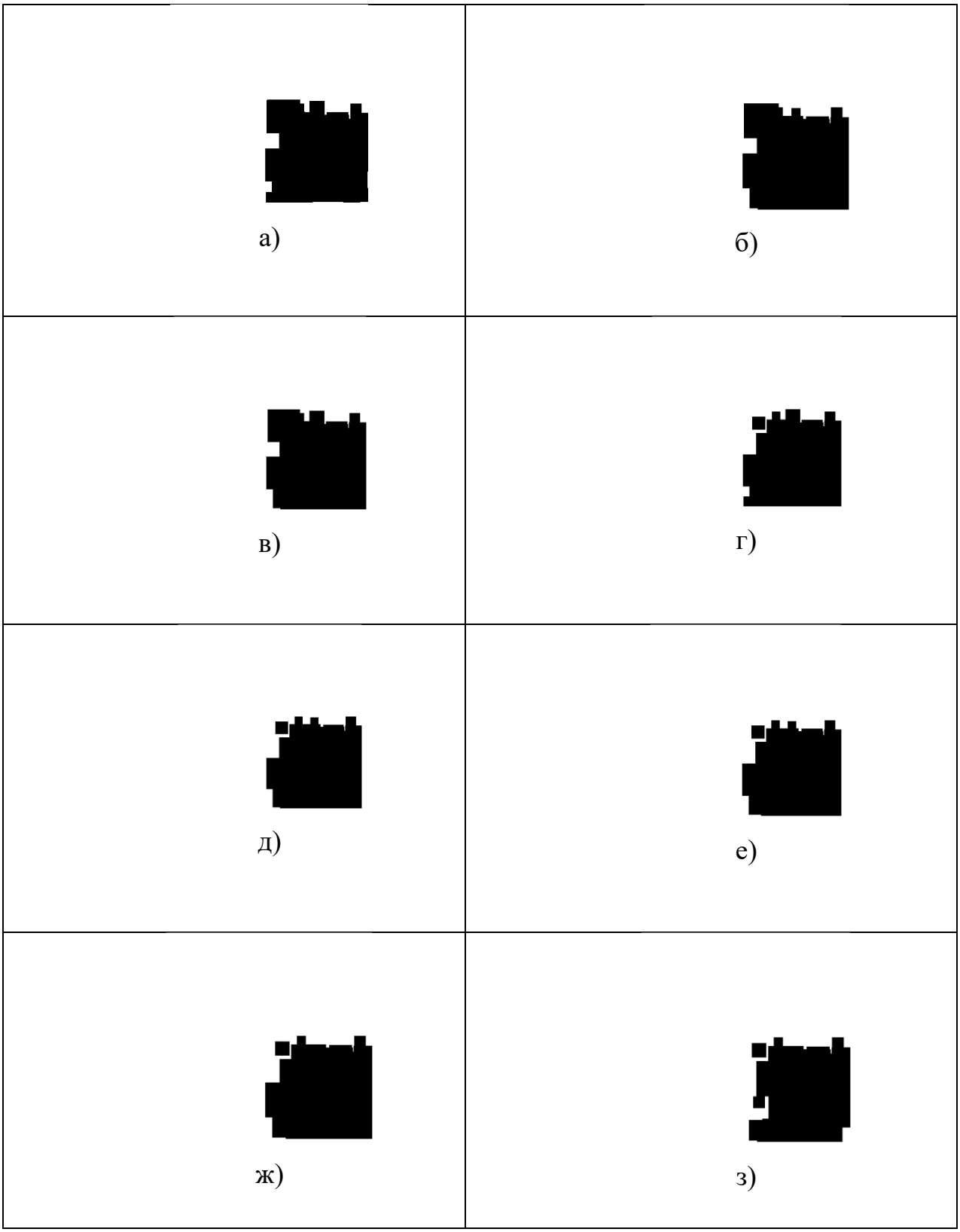


Рисунок 15 – Результаты автоматического выделения области встраивания для изображения, приведенного на Рисунке 12, для $R_0 = 40$: а) $p = 0.52$, б) $p = 0.53$, в) $p = 0.54$, г) $p = 0.55$, д) $p = 0.56$ е) $p = 0.57$ ж) $p = 0.58$ з) $p = 0.60$

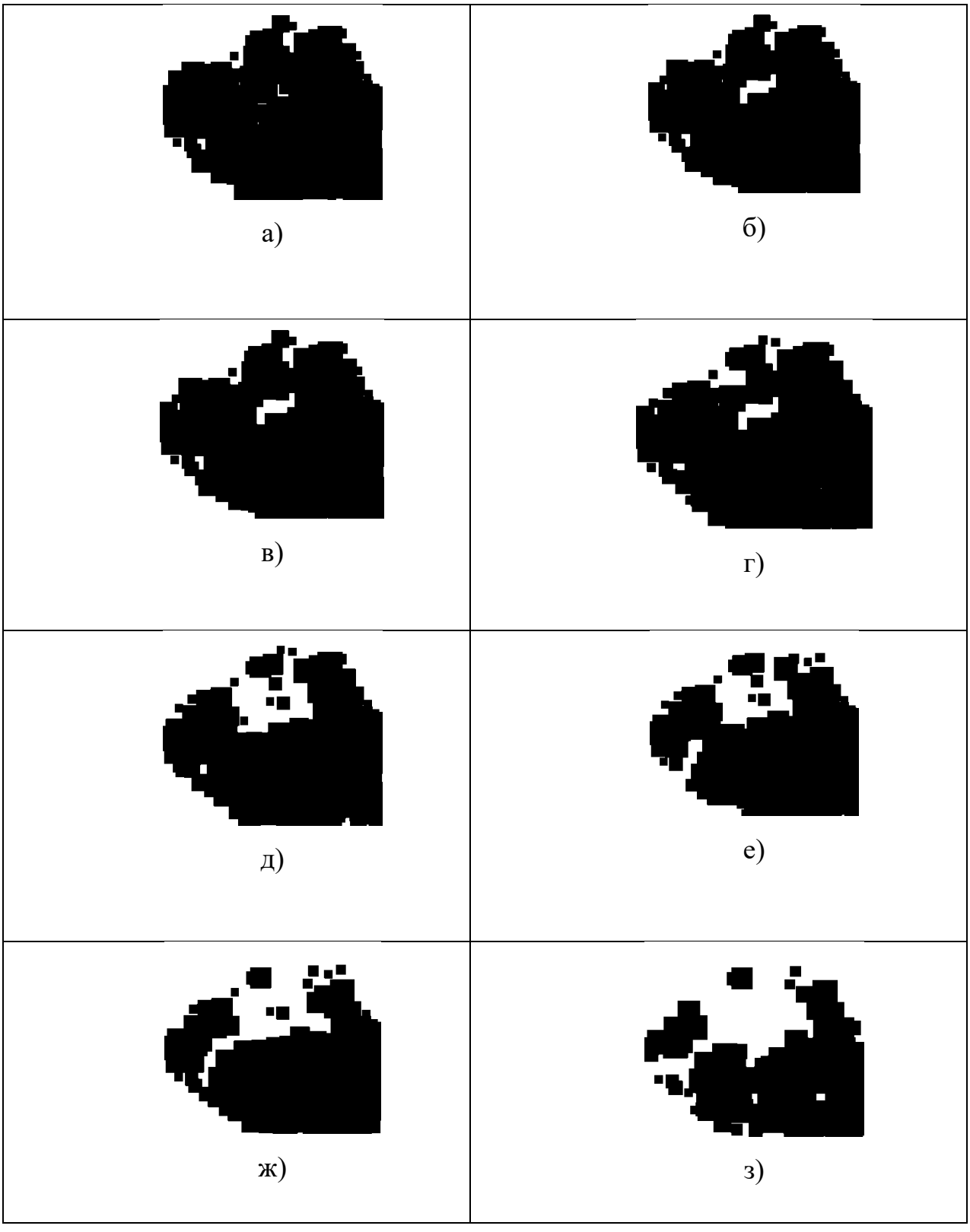


Рисунок 16 – Результаты автоматического выделения области встраивания для изображения, приведенного на Рисунке 13, для $R_0 = 30$: а) $p = 0.52$, б) $p = 0.53$, в) $p = 0.54$, г) $p = 0.55$, д) $p = 0.56$ е) $p = 0.57$ ж) $p = 0.58$ з) $p = 0.60$

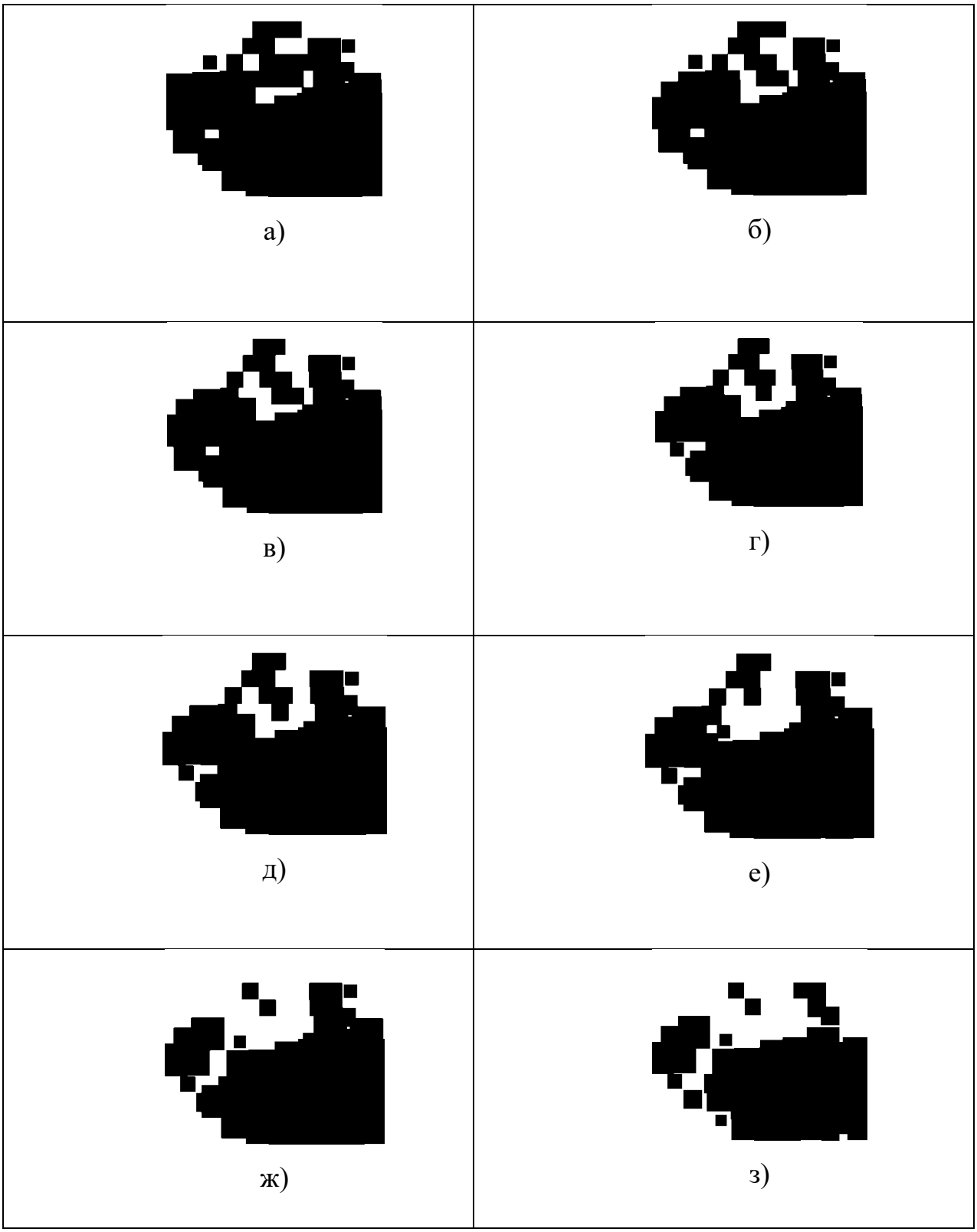


Рисунок 17 – Результаты автоматического выделения области встраивания для изображения, приведенного на Рисунке 13, для $R_0 = 40$: а) $p = 0.52$, б) $p = 0.53$, в) $p = 0.54$, г) $p = 0.55$, д) $p = 0.56$ е) $p = 0.57$ ж) $p = 0.58$ з) $p = 0.60$

Первый подход заключается в построении минимального прямоугольника, который включал бы в себя выделенные прямоугольные небольшие области. При этом подобных областей на изображении может быть несколько. Такой подход даёт возможность выделить на изображении наиболее вероятные области встраивания. На Рисунке 18 приведен пример выделения подобных областей на основе прямоугольных областей, выделенных на Рисунке 17.

Сопоставление изображений на Рисунке 18 позволяет сделать заключение о том, что прямоугольник 18.а) достаточно точно совпадает с областью встраивания на Рисунке 13.б)

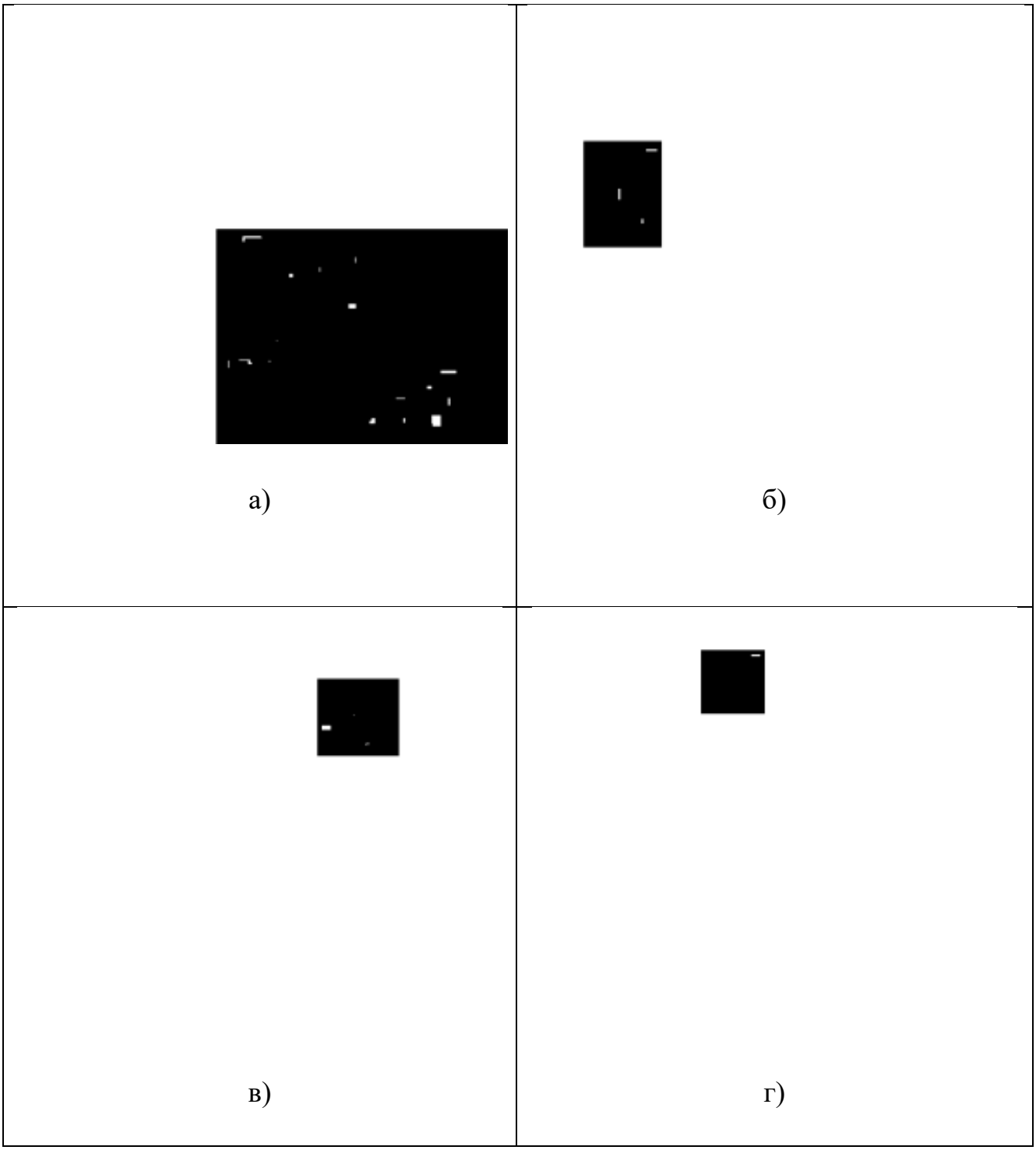


Рисунок 18 – Результаты выделения вписанных прямоугольных областей в контур, приведённый на Рисунке 13.з)

3.5 Обсуждение результатов

Таким образом, предложенный в данной главе алгоритм выявления СГВ позволяет с высокой вероятностью определять наличие СГВ, встроенного методом LSB. Факт наличия СГВ для тестируемой коллекции определялся с эффективностью 95%. Для искусственных изображений с равномерной и градиентной заливкой предлагаемый алгоритм дает возможность определить в среднем 91% подмененных битов, при этом ложных срабатываний не больше 1%. При этом визуализация матрицы решений даёт возможность с высокой точностью определить положение и размеры области встраивания СГВ. Для фотографических изображений предлагаемый алгоритм верно выделяет в среднем 89% пикселей с подмененным младшим битом, а ложных срабатываний в среднем – 37%. Положение встроенных битов может быть установлено исходя из сопоставления матрицы решений с первоначальным изображением. Высокий процент ложных срабатываний является типичным для подобных алгоритмов. В аналогичных алгоритмах [78, 104], решающих задачу поиска поврежденных пикселей, которая значительно проще, процент ложных срабатываний равен 36%. Необходимо отметить, что в данном случае определяется не ошибочное детектирование наличия СГВ, а битов, входящих в область встраивания. Поэтому данная ошибка ложного срабатывания является допустимой. В таблице 2 приведены результаты определения границ встроенной области.

Как видно из таблицы 2, и сравнении ее с аналогичными результатами из главы 2, учет информации не только о первом слое, но и о втором и третьем, позволяет повысить точность определения границ встраивания в среднем на 13%. Трудоемкость вычислений при этом возрастает. Хорошие результаты получаются при p=0,55-0,57. При практическом использовании наилучшей стратегией является поиск области встраивания при различных p с дальнейшим усреднением.

Таблица 2 – Средние ошибки определения координат прямоугольника встраивания при различных значениях шага граничной плотности *p*

p	Δx_1(%)	Δy_1(%)	Δx_2(%)	Δy_2(%)
Искусственные изображения				
0,52	0,74	0,41	0,37	2,71
0,53	0,83	0,46	0,33	2,83
0,54	0,77	0,51	0,47	0,21
0,55	0,71	0,42	0,44	0,83
0,56	0,79	0,45	0,34	0,91
0,57	0,83	6,25	0,39	2,56
0,58	0,87	8,58	0,38	2,69
0,59	0,91	9,53	0,43	2,81
0,6	0,94	9,25	2,59	2,63
Фотографические изображения (первый случай)				
0,56	1,67	1,04	0,37	14,17
0,57	3,89	0,42	0,19	3,13
0,58	5,01	1,46	0,21	1,67
0,59	7,04	2,08	9,44	25,83
0,6	7,22	1,25	8,52	19,79
Фотографические изображения (второй случай)				
0,56	11,11	3,96	5,19	28,54
0,57	11,48	3,15	5,31	15,21
0,58	7,07	2,09	9,47	25,83
0,59	7,22	1,26	8,52	19,93
0,6	5,19	1,68	3,54	10,63

Предлагаемый алгоритм, в отличие от разработанных ранее алгоритмов, эффективен при малых размерах СГВ. Если прочие методы, описанные во введении, наиболее эффективны при заполнении контейнера более чем на 50%, то

предлагаемый алгоритм показывает хорошие результаты даже тогда, когда стегоконтейнер заполнен на 10–30%.

Выводы по третьей главе

Разработан алгоритм стегоанализа метода LSB-замены на основе анализа нескольких слоев. При этом:

1. Факт встраивания СГВ определяется с эффективностью 95% при заполнении стегоконтейнера от 10% до 30%.

2. Для искусственных изображений с градиентной и равномерной заливкой предлагаемый алгоритм даёт возможность определять в среднем 91% заменённых битов, при этом ложных срабатываний не больше 1%. К тому же, визуализация матрицы решений даёт возможность с высокой точностью установить размеры и расположение области встраивания сообщения.

3. Предлагаемый алгоритм для фотографических изображений верно выделяет порядка 89% пикселей с подмененным младшим битом, а ложных срабатываний – 37%. Расположение встроенных битов можно определить на основе сопоставления матрицы решений с исходным изображением.

Результаты данной главы опубликованы в работах [4,7,9,29,30].

ГЛАВА 4. СТЕГОАНАЛИЗ АЛГОРИТМА КОХА-ЖАО

4.1 Введение

Кроме алгоритмов встраивания СГВ непосредственно в битовые плоскости изображения, большое распространение получили стеганографические методы, использующие частотную составляющую. Их применение состоит в том, что к изображению применяется какое-либо из частотных преобразований: дискретное преобразование Фурье, дискретное косинусное преобразование или вейвлет-преобразование. После преобразования сообщение встраивается с помощью изменения коэффициентов преобразования. Изображение со СГВ формируется путем обратного преобразования. Преимущество такого метода встраивания состоит в том, что обратное преобразование обеспечивает равномерное распределение изменений вследствие сокрытия данных по всей пространственной области изображения. Данное свойство распределения изменений повышает устойчивость частотных методов встраивания к традиционным методам стеганографического анализа, базирующихся на исследовании изменения энтропии пространственной области изображения. В связи с этим необходимо развитие новых специализированных методов стеганографического анализа, ориентированных на анализ частотных компонент различных преобразований.

Методы встраивания СГВ в частотную область получили распространение в связи с развитием форматов изображений, использующих различные преобразования. Это обстоятельство позволяет достаточно органично использовать методы стеганографического встраивания в процессе преобразования к новому формату. Так стандарт JPEG для изображений и стандарт MPEG для видеофайлов включают в себя дискретное косинусное преобразование как один из этапов.

Основная идея методов, основанных на дискретном косинусном преобразовании, состоит в том, что встраивание производится не в пиксели изображения, а в коэффициенты дискретного косинусного преобразования. Простейший подход состоит в добавлении к коэффициентам дискретного косинусного преобразования битов сообщения. К таким методам можно отнести алгоритм Кокса [32] и алгоритм Барни [26,42]. По сути, эти методы аналогичны LSB-замене, но выполняется в частотной области. Стегоанализ для этих методов встраивания осуществляется методами, аналогичными тем, которые применяются для метода LSB-замены, но в частотной области. Модификация коэффициентов дискретного косинусного преобразования не является устойчивой к малым изменениям формата изображения и не гарантирует однозначного извлечения СГВ. Кроме этого, данные методы встраивания нелегко поддаются статистическому стегоанализу. Для противодействия простейшим статистическим методам используются алгоритмы, реализованные в программных комплексах, таких как F5, Outguess, JPHide, Jsteg и др. Однако данные алгоритмы неустойчивы к статистическим методам стегоанализа, которые используют большое количество параметров изображения с применением классификаторов.

Более устойчивым к изменению формата является метод встраивания, основанный на алгоритме Коха-Жао [65]. В этом случае канал передачи скрытых сообщений характеризуется низкой пропускной способностью, и применение к нему статистических методов приводит к низкой эффективности обнаружения. Для повышения устойчивости метода Коха-Жао к преобразованиям формата изображения разработан алгоритм, который использует дополнительно различные методы кодирования [75]. Однако основной принцип изменения пары коэффициентов дискретного косинусного преобразования, заложенный в методе Коха-Жао, остается общим для всех алгоритмов, основывающихся на нем. В связи с этим рассмотрение базового алгоритма и выработка для него методов стегоанализа является актуальной задачей. Таким образом, стегоанализ

алгоритмов, базирующихся на методе Коха-Жао, может быть проведен на основе тех же принципов, но с учетом модификаций, внесенных в алгоритм встраивания.

Цель данной главы заключается в разработке алгоритма определения СГВ в изображении, встраиваемых посредством метода Коха-Жао.

4.2 Алгоритм встраивания и постановка задачи

В качестве объекта исследования рассмотрим цифровое изображение, о котором нет информации об отсутствии или наличии СГВ. Известно только, что используется метод встраивания Коха-Жао [65]. Сформулируем три задачи:

1. Нужно установить факт наличия или отсутствия СГВ.
2. При наличии СГВ, определить его положение в изображении-контейнере и размеры.
3. Требуется максимально точно определить СГВ, при его наличии, без априорной информации.

Стеганографический метод Коха-Жао [65] базируется на двумерном дискретном косинусном преобразовании (ДКП). Алгоритм встраивания сообщения состоит из шагов:

1. Первоначальное изображение разбивается на блоки размером 8×8 пикселей.

2. К каждому блоку применяется ДКП, результат – матрицы коэффициентов D_i ($i = 1, \dots, N$; N – количество блоков) размером 8×8.

3. Выбирается последовательность блоков, в которые будет осуществляться встраивание. В каждый блок записывается 1 бит информации.

4. Выбираются два коэффициента ДКП в каждом блоке, расположенные в среднечастотной области коэффициентов, симметричные относительно главной диагонали ($D_i[3,4]$ и $D_i[4,3]$, $D_i[3,5]$ и $D_i[5,3]$, $D_i[4,5]$ и $D_i[5,4]$).

5. Для передачи бита 0 необходимо, чтобы разница модулей пары коэффициентов ДКП была больше положительной величины M_0; для передачи

бита 1 разница должна быть меньшей $-M_0$. То есть, при передаче 0 увеличиваем модуль первого коэффициента и уменьшаем модуль второго. При передаче 1 уменьшаем модуль первого коэффициента и увеличиваем модуль второго.

6. Проходим по каждому блоку и выполняем пункты 4 и 5.

7. Для каждого блока выполняем обратное ДКП.

Выбор среднечастотных коэффициентов ДКП связан с необходимостью минимизации воздействия встраивания на визуальные свойства измененного изображения. Выбор высокочастотных или низкочастотных коэффициентов приводит к появлению эффектов, заметных визуально.

При извлечении СГВ считается, что пары изменяемых коэффициентов ДКП известны. Алгоритм извлечения:

1 – 4 пункта алгоритма совпадают с алгоритмом встраивания, представленным выше.

5. Вычисляем разность значений модулей для пар коэффициентов, в которые производилось встраивание.

6. Если разность больше M_0, то был встроен бит 0. Если разность значений меньше, чем $-M_0$, то был встроен единичный бит.

7. Последовательно извлекаем биты, встроенные во все блоки.

Анализ алгоритмов встраивания и извлечения говорит нам о том, что для успешного осуществления атаки на стеганографический метод Коха-Жао нужно установить блоки, в которые было осуществлено встраивание СГВ, пороговое значение M_0 и индексы изменяемых коэффициентов ДКП.

Для того чтобы корректно извлечь сообщения у отправляющей и принимающей сторон, обязательно должна быть общая секретная информация о параметрах встраивания. Будем опираться на то, что информация о параметрах имеет минимальный размер. В таком случае можно сформулировать следующие три предположения:

1) Встраивание осуществляется в непрерывную последовательность блоков.

2) Для всех блоков применяются одни и те же пары коэффициентов ДКП.

3) Для всех блоков применяется одно и тоже значение M_0.

Любые отклонения от указанных предположений повышают объём секретной информации.

4.3 Алгоритм стеганографического анализа

Для определения параметров СГВ воспользуемся тем фактом, что у параметра M_0 обязано быть большое значение, которое позволяет принимающей стороне из любого изображения без потерь извлекать СГВ. Если M_0 выбрать недостаточно большим, то в извлекаемой СГВ могут быть ошибки, которые связаны с особенностями изображения-контейнера.

В первую очередь, следует определить коэффициенты ДКП, в которые осуществлялось встраивание. Для этого, как и в алгоритме встраивания, разделим изображение на блоки B_i ($i = 1, \dots, N$) размером 8×8 пикселей. Для каждого блока B_i ($i = 1, \dots, N$) воспользуемся ДКП. Результат – совокупность матриц коэффициентов D_i ($i = 1, \dots, N$) с размером 8×8. Проведем анализ среднечастотных элементов матриц D_i ($i = 1, \dots, N$). Введём три последовательности величин ($i = 1, \dots, N$):

$$\begin{aligned} C_i^{(1)} &= ||D_i[3,4]| - |D_i[4,3]||, \\ C_i^{(2)} &= ||D_i[3,5]| - |D_i[5,3]||, \\ C_i^{(3)} &= ||D_i[4,5]| - |D_i[5,4]||. \end{aligned} \tag{22}$$

В результате встраивания СГВ в одной из этих последовательностей возникают изменения. Построим гистограммы зависимости $C_i^{(j)}$ ($j = 1,2,3$; $i = 1, \dots, N$) от номера блока i. Встраивание СГВ меняет одну из последовательностей в виде появления «ступени» высотой M_0. На Рисунках 19–24 изображён пример подобного изменения.

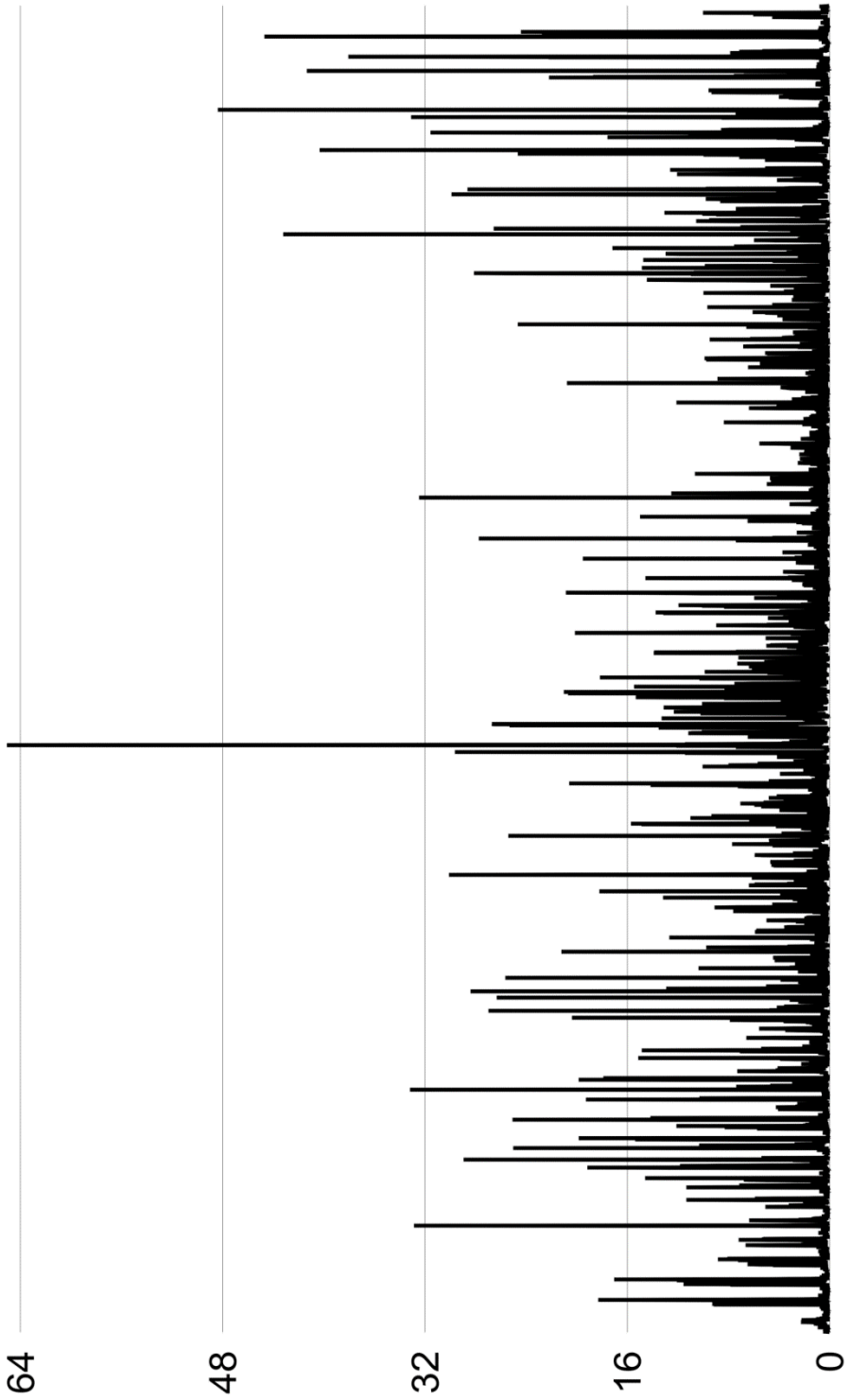


Рисунок 19 – Гистограмма зависимости $C_i^{(1)}$ от номера блока i для изображения без СГВ

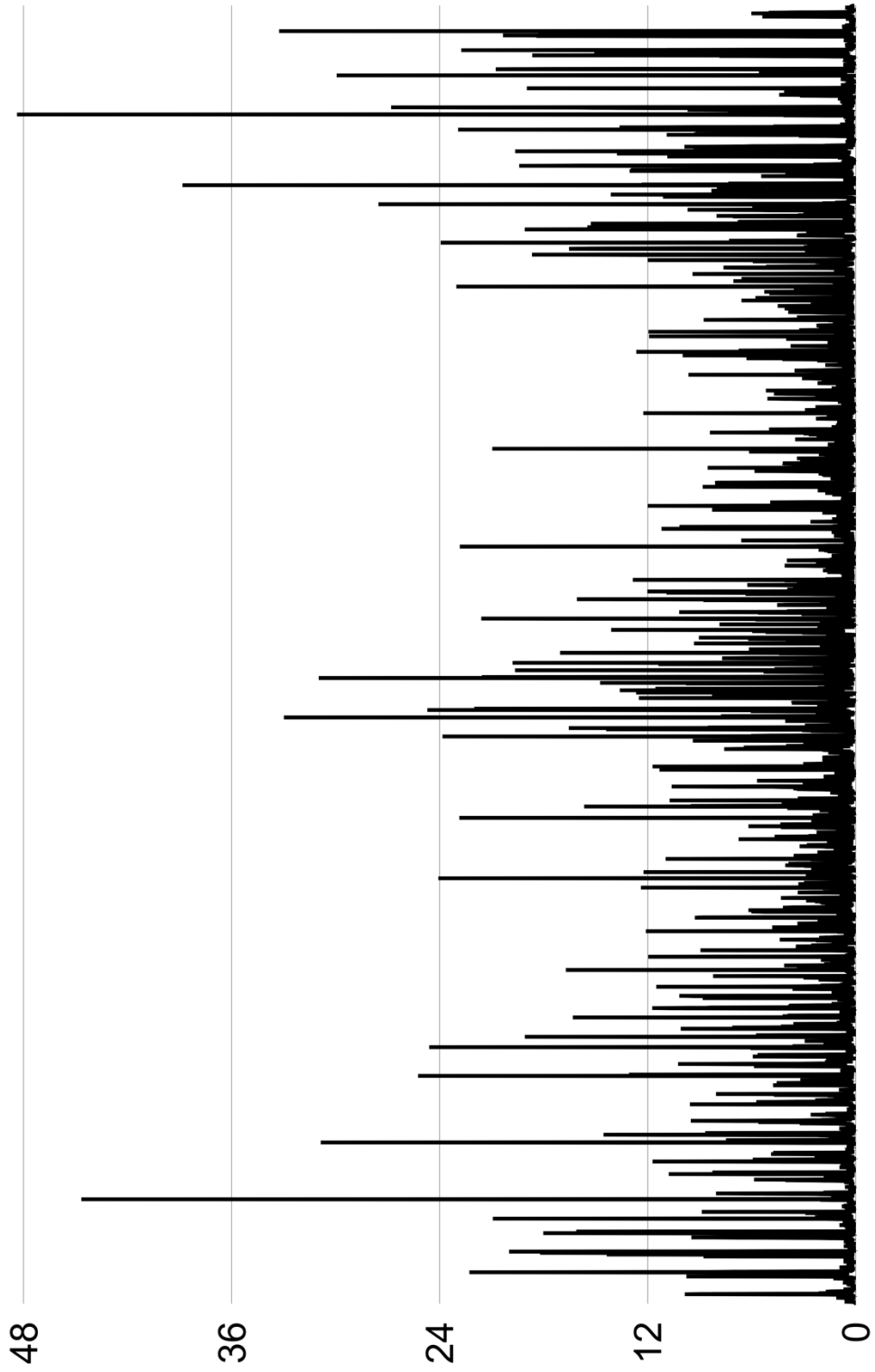


Рисунок 20 – Гистограмма зависимости $C_i^{(2)}$ от номера блока i для изображения без СГВ

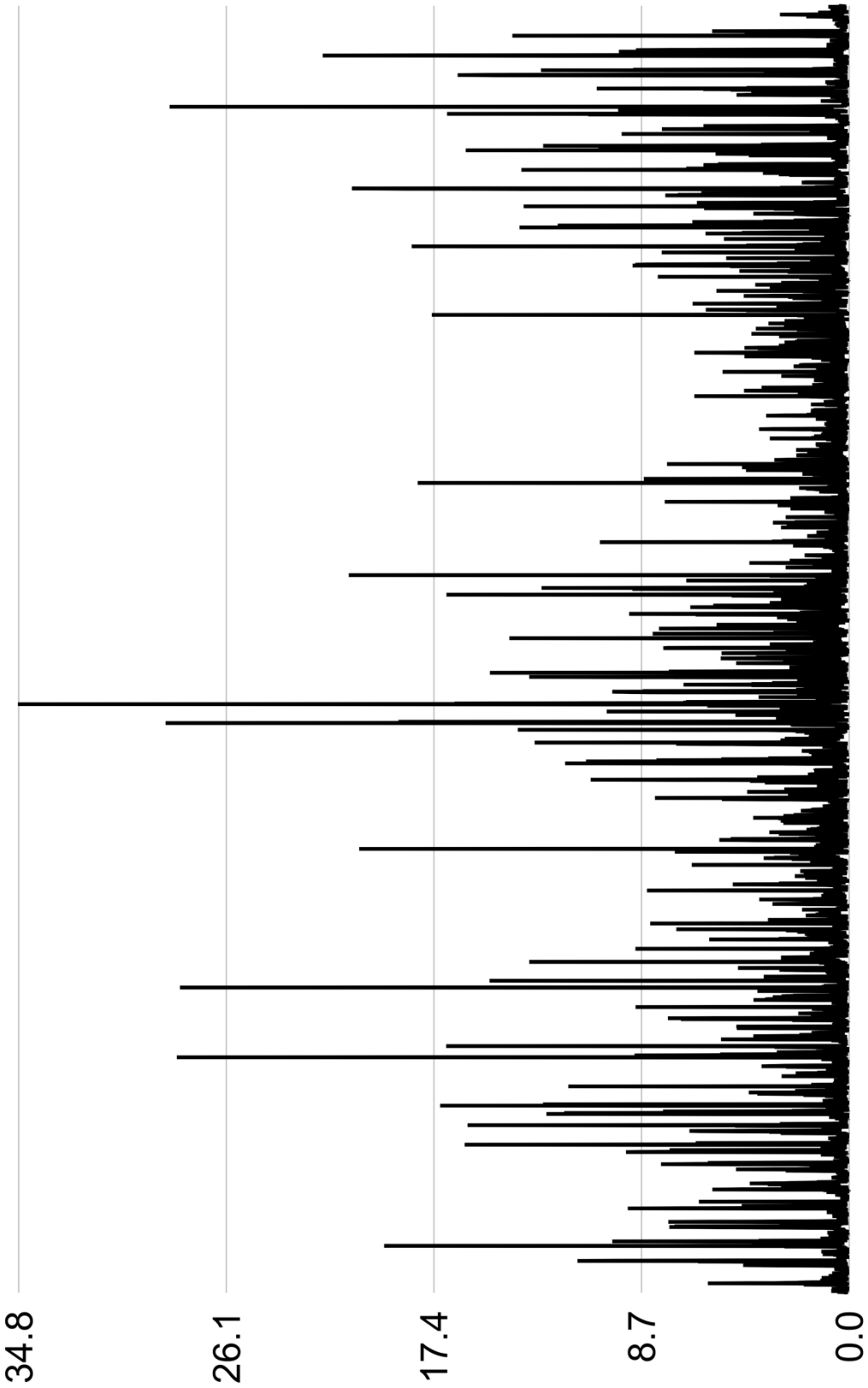


Рисунок 21 – Гистограмма зависимости $C_i^{(3)}$ от номера блока i для изображения без СГВ

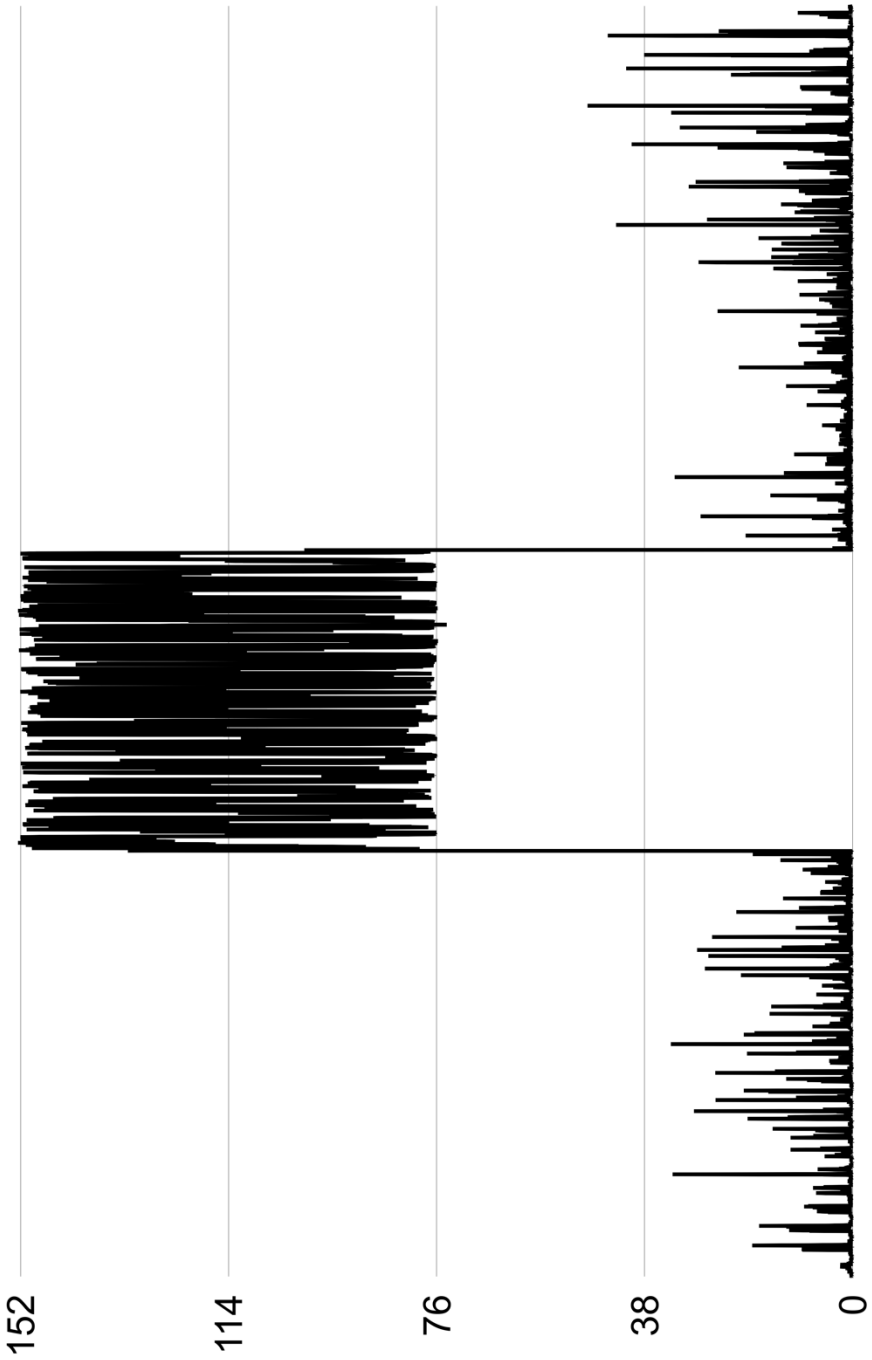


Рисунок 22 – Гистограмма зависимости $C_i^{(1)}$ от номера блока i для изображения со СГВ в компоненты $D[3,4]$ и $D[4,3]$

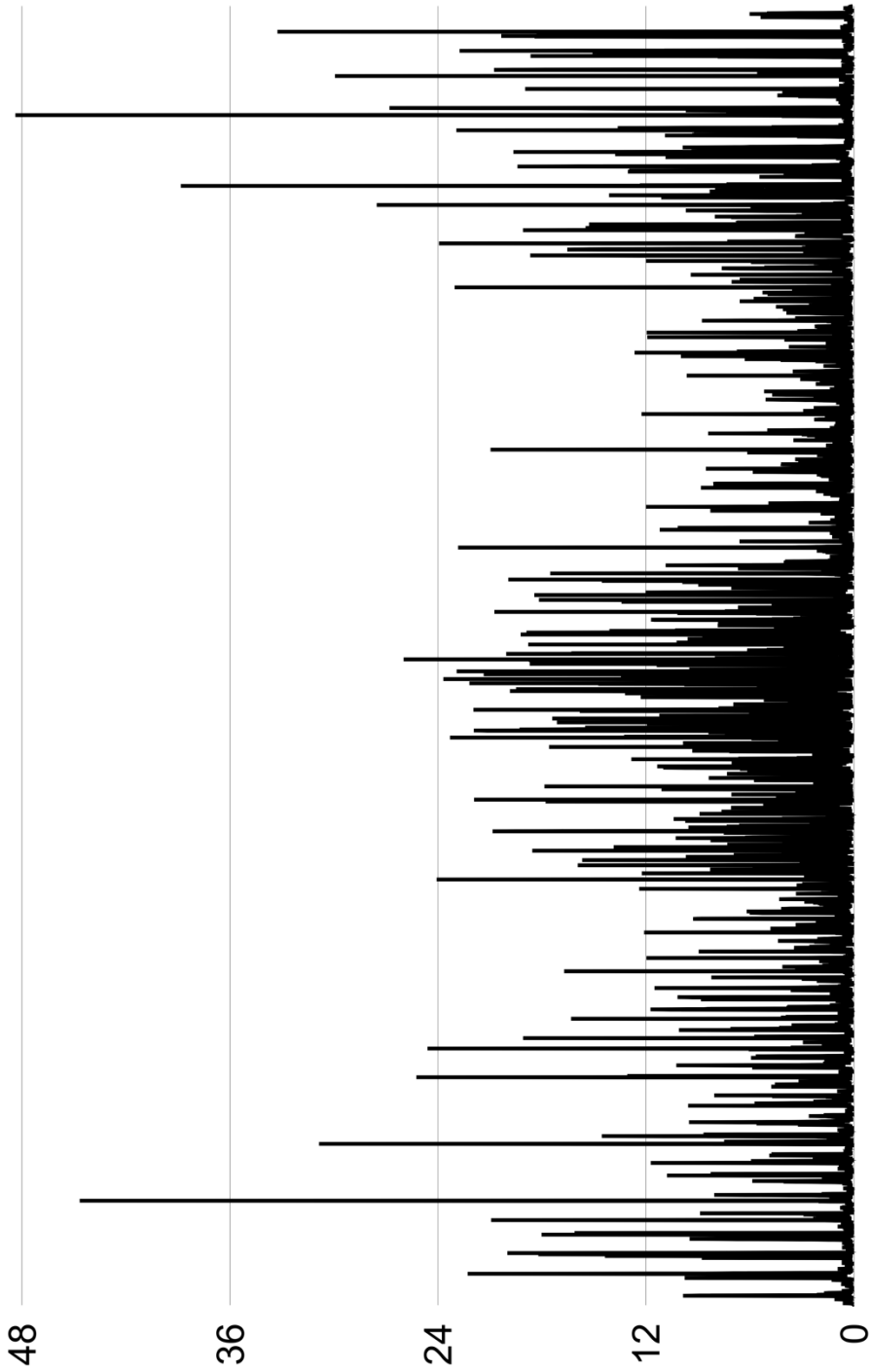


Рисунок 23 – Гистограмма зависимости $C_i^{(2)}$ от номера блока i для изображения со СГВ в компоненты $D[3,4]$ и $D[4,3]$

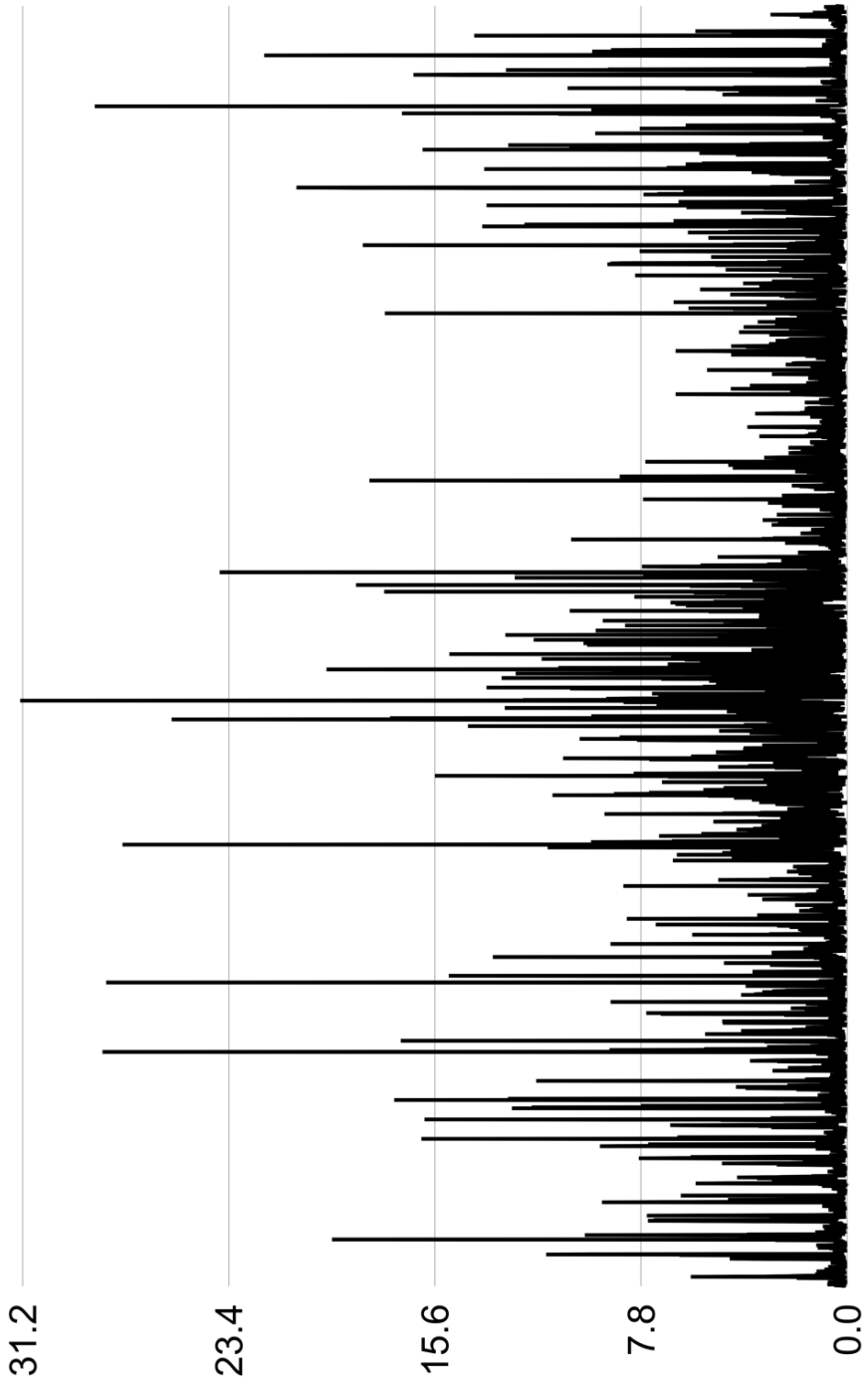


Рисунок 24 – Гистограмма зависимости $C_i^{(3)}$ от номера блока i для изображения со СГВ в компоненты D[3,4] и D[4,3]

Проблему выявления СГВ можно свести к анализу зависимостей $C_i^{(j)}$ ($j = 1,2,3$; $i = 1, \dots, N$) от номера блока i и поиску ступенчатых изменений. На гистограмме границы ступеней можно выявить при помощи численного дифференцирования опираясь на разностные схемы. Произведём численное дифференцирование зависимости $C_i^{(j)}$ ($j = 1,2,3; i = 1, \dots, N$) по i:

$$dC_i^{(j)} = C_i^{(j)} - C_{i-1}^{(j)}. \quad (23)$$

Ступенчатые изменения после данной операции дадут высокие пики, которые позволяют установить границы СГВ. На Рисунках 25–27 приведена зависимость $dC_i^{(j)}$ от номера блока i для зависимости, изображённой на Рисунках 22–24.

Для автоматического определения границы СГВ для каждого массива $d\mathrm{C}^{(j)}$ определим величины: O_j – среднеквадратичное отклонение для элементов массива $d\mathrm{C}^{(j)}$, N_j – среднее значение элементов массива $d\mathrm{C}^{(j)}$, M_j – максимальное значение элементов массива $d\mathrm{C}^{(j)}$. Определим:

$$R_j = N_j + O_j. \quad (24)$$

Введем величину Y_j , находящуюся в пределах значений от R_j до M_j . Подберём значение Y_j так, чтобы было ровно 2 значения $C_{i1}^{(j)} > Y_j$ и $C_{i2}^{(j)} > Y_j$. Значения i_1 и i_2 – границы СГВ. Для определения значения M_0 нужно определить наименьшее значение $C_i^{(j)}$ на пределах от i_1 до i_2

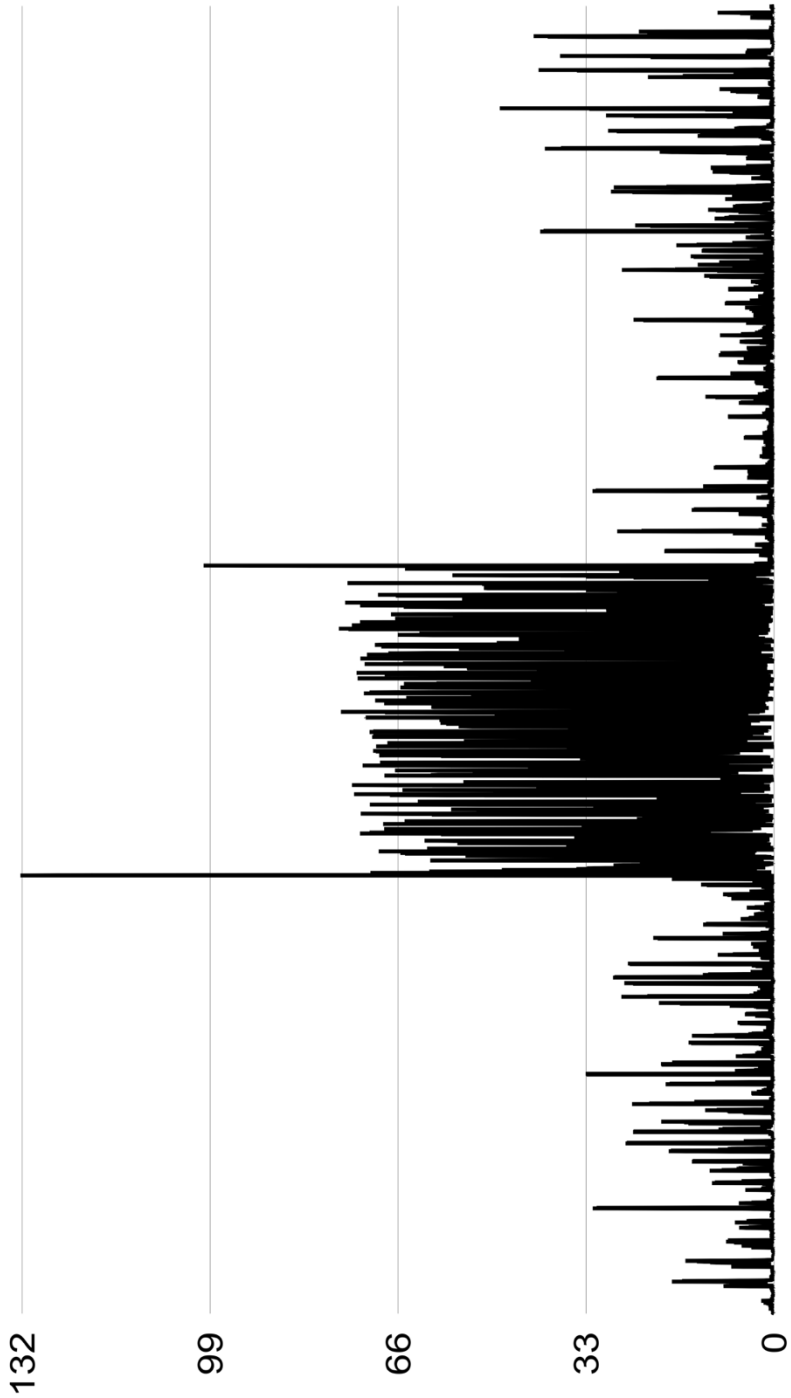


Рисунок 25 – Гистограмма зависимости $dC_i^{(1)}$ от номера блока i при встраивании в компоненты D [3,4] и D[4,3]

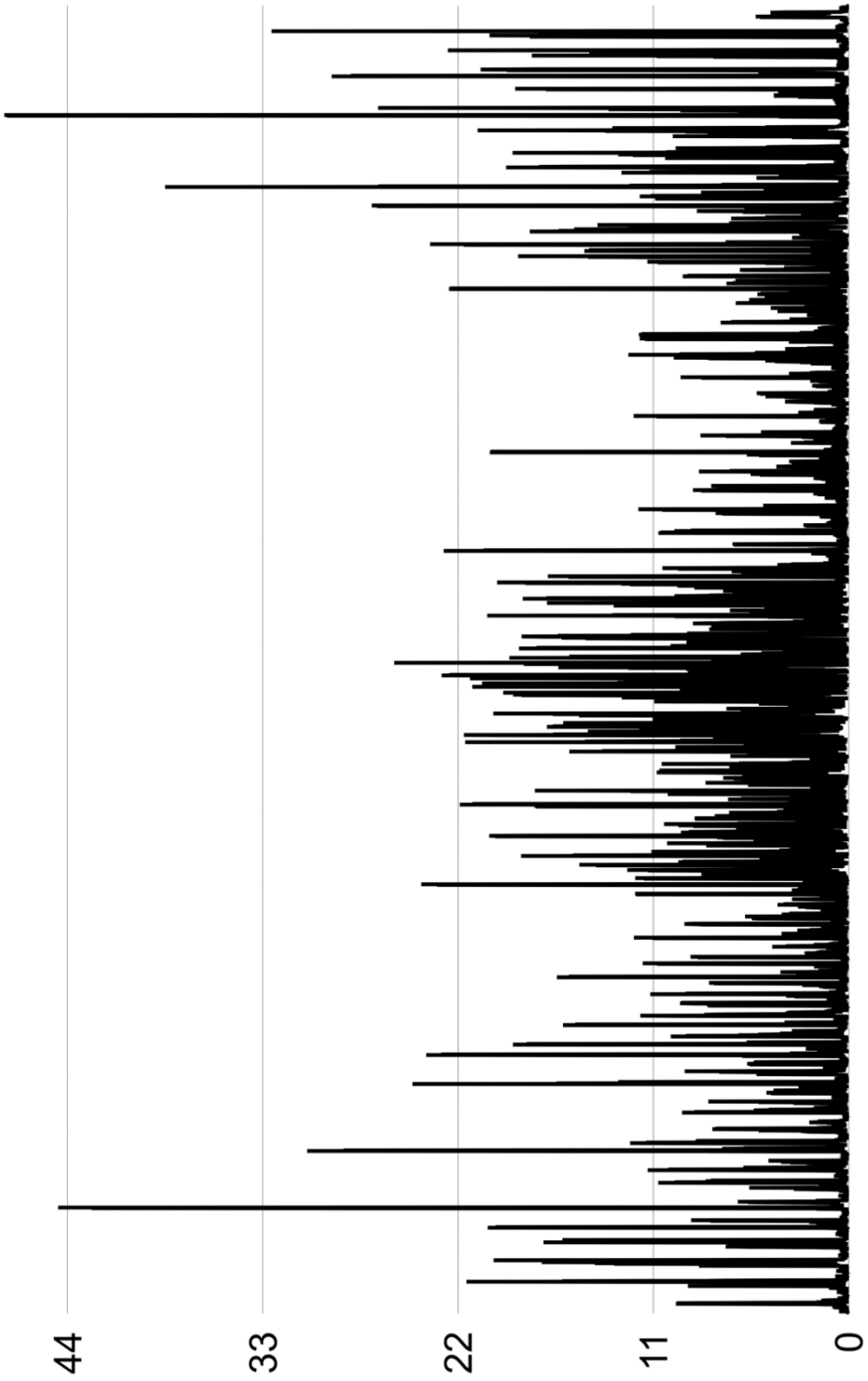


Рисунок 26 – Гистограмма зависимости $dC_i^{(2)}$ от номера блока i при встраивании в компоненты D [3,4] и D[4,3]

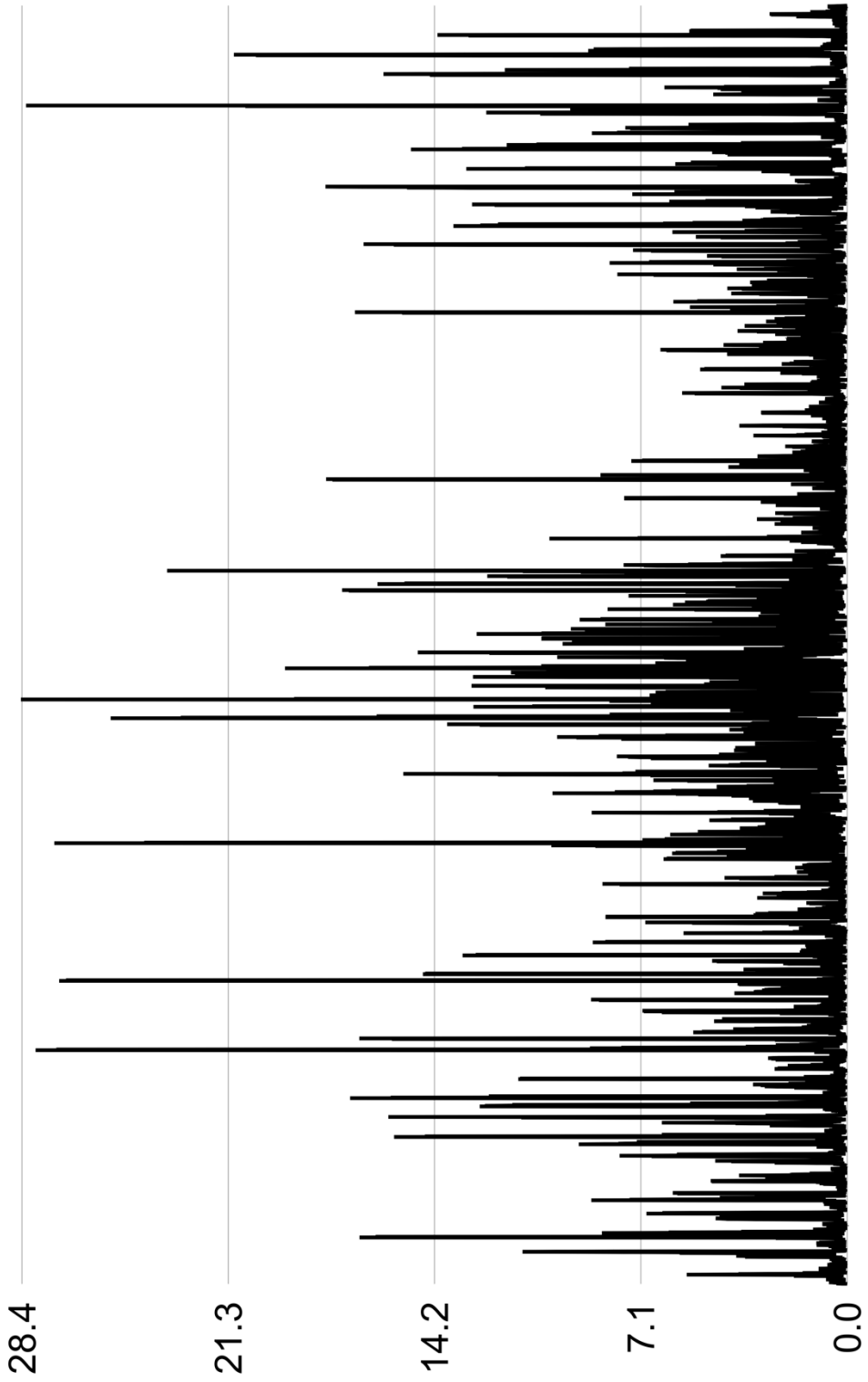


Рисунок 27 – Гистограмма зависимости $dC_i^{(3)}$ от номера блока i при встраивании в компоненты D[3,4] и D[4,3]

Представим алгоритм по шагам:

1. Разделим изображение на блоки B_i размером 8×8пикселей.
2. К каждому блоку B_i применим дискретное косинусное преобразование. Результат – матрицы коэффициентов ДКП D_i размером 8×8.
3. Построим три последовательности величин ($i = 1, \dots, N$):

$$C_i^{(1)} = ||D_i[3,4]| - |D_i[4,3]||,$$
$$C_i^{(2)} = ||D_i[3,5]| - |D_i[5,3]||, \quad (25)$$
$$C_i^{(3)} = ||D_i[4,5]| - |D_i[5,4]||.$$

4. Выполним численное дифференцирование $C_i^{(j)}$ ($j = 1,2,3$; $i = 1, \dots, N$) по i:

$$dC_i^{(j)} = C_i^{(j)} - C_{i-1}^{(j)}. \quad (26)$$

5. Вычислим: M_j – наибольшее значение элементов массива $d\mathrm{C}^{(j)}$,N_j – среднее значение элементов массива $d\mathrm{C}^{(j)}$, O_j – среднеквадратичное отклонение для элементов массива $d\mathrm{C}^{(j)}$. Определим:

$$R_j = N_j + O_j. \quad (27)$$

6. Осуществим перебор величин Y_j в диапазоне от R_j до M_j, шаг dY. Найдем значение Y_j так, чтобы было ровно 2 значения $C_{i_1}^{(j)} > Y_j$ и $C_{i_2}^{(j)} > Y_j$. Если подобное значение невозможно определить, то сократим шаг dY. Установим i_1 и i_2.
7. Определим минимальное значение $C_i^{(j)}$в интервале от i_1 до i_2. Присвоим M_0 найденное значение.
8. Используя найденные параметры, извлечём СГВ.

4.5 Компьютерный эксперимент

Чтобы определить эффективность работы предлагаемого алгоритма, протестируем его результаты на основе библиотеки изображений Беркли (Berkeley

Segmentation Data Set and Benchmarks 500, BSDS500). Данная коллекция создана для осуществления проверки алгоритмов кластеризации. В коллекции присутствует набор из 500 изображений в формате JPEG. Данная коллекция была выбрана для тестирования предложенного метода, потому что в ней есть изображения с разным содержимым и разными типами областей заливки. Помимо этого, формат JPEG, так же как и метод Коха-Жао, базируется на дискретном косинусном преобразовании, что при изменении формата файла изображения устраняет дополнительные ошибки.

В ходе тестирования, на вход алгоритма подавалось каждое изображение вначале без встроенных данных (пустой стегоконтейнер), а после чего со встроенным сообщением (заполненный стегоконтейнер). Нужно подчеркнуть, что при $M_0 > 54$ предложенный алгоритм эффективен. Но применение алгоритма Коха-Жао при более низких значениях порога M_0 сталкивается со значительными сложностями при извлечении встроенных данных. Помимо этого, если алгоритм выявляет встроенное сообщение, то он может его однозначно извлечь.

На основе обработки 500 изображений коллекции BSDS500B, рамках компьютерного эксперимента, определялись:

FN – процент ложно-негативных результатов: изображение, содержащее СГВ, было определено как изображение, не имеющее встроенного сообщения.

TN – процент истинно негативных результатов: изображение, не содержащее СГВ, было корректно определено.

FP – процент ложно-позитивных результатов: изображение, не содержащее СГВ, было определено как изображение, содержащее СГВ.

TP – процент истинно положительных результатов: изображение, содержащее СГВ, было корректно определено и сообщение извлечено верно.

Предложенный алгоритм показал:

$$TP = 85{,}5\%, FN = 14{,}5\%, TN = 77\%, FP = 23\%.$$

Как видно из статистических данных, предлагаемый алгоритм с достаточно высокой эффективностью устанавливает наличие СГВ. Ошибки в работе алгоритма обусловлены структурой изображения. В пустом изображении-стегоконтейнере возможно наличие пиков в последовательности коэффициентов дискретного косинусного преобразования, которые могут ложно приниматься за границу СГВ. К ложно-позитивным результатам приводит наличие 2-х ложных границ. Наличие больше 2-х ложных границ приводит к тому, что определить фактические границы СГВ невозможно.

Интересны, с точки зрения защиты информации, такие изображения, для которых стегоанализ не позволяет определить факт встраивания.

На Рисунке 28 представлены примеры изображений, для которых наблюдаются ложно-позитивные результаты. То есть они позволяют ввести в заблуждение злоумышленника и заставить его анализировать пустой стегоконтейнер. На Рисунке 29 приведены примеры изображений, для которых наблюдаются ложно-негативные результаты. Эти изображения позволяют скрыто передавать СГВ.

На Рисунке 30 приведены примеры изображений, для которых наблюдаются истинно положительные и истинно негативные результаты. Эти изображения не рекомендуется использовать для передачи скрытых сообщений, так как они легко поддаются стегоанализу.

Рисунок 28 – Примеры изображений, для которых наблюдаются ложно-позитивные результаты

Рисунок 29 – Примеры изображений, для которых наблюдаются ложно-негативные результаты.

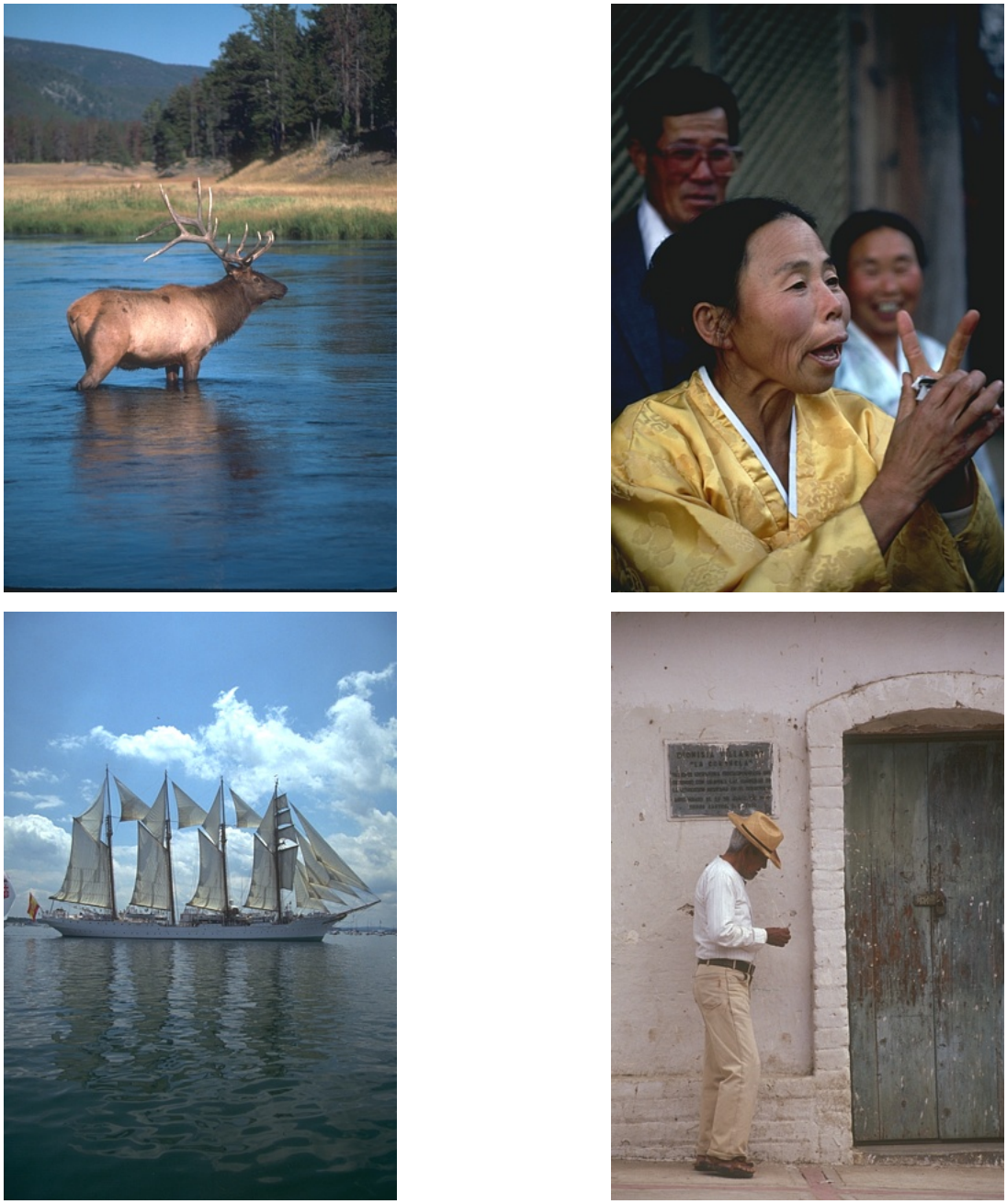


Рисунок 30 – Примеры изображений, для которых наблюдаются истинно положительные и истинно негативные результаты

Выводы по четвертой главе

Разработан алгоритм стегоанализа метода Коха-Жао на основе анализа коэффициентов дискретного косинусного преобразования. При этом:

1. Показано, что стеганографический алгоритм Коха-Жао не является устойчивым к атаке анализа коэффициентов ДКП.

2. Предлагаемый алгоритм позволяет абсолютно точно извлекать СГВ при его обнаружении.

3. Тестирование на коллекции изображений показало, что ошибки ложного определения наличия СГВ в пустом стегоконтейнере не превышают 23%. Эффективность обнаружения наличия СГВ – 85,5%.

Результаты данной главы опубликованы в работах [5,10,14,28].

ЗАКЛЮЧЕНИЕ

В заключение выделим основные результаты, полученные в диссертации:

1. Разработан алгоритм стегоанализа метода LSB-замены на основе анализа нулевого слоя. Предложенный алгоритм позволяет определять наличие СГВ, ее положение и размер. Данный алгоритм эффективен при наличии пересечения области встраивания с достаточно большой областью градиентной или равномерной заливки на исходном изображении. Это требование является необходимым и для иных методов стегоанализа. Предложенный алгоритм позволяет верно определить положение в среднем 88% встроенных пикселей, при уровне ложных срабатываний не более 27%.

2. Разработан алгоритм стегоанализа метода LSB-замены на основе анализа нескольких слоев. Для искусственных изображений с равномерной и градиентной заливкой предложенный алгоритм позволяет выявлять в среднем 91% подмененных битов, тогда как ложные срабатывания составляют не более 1%. При этом визуализация матрицы решений позволяет с высокой точностью определить положение и размеры области встраивания сообщения. Для фотографических изображений предложенный алгоритм верно выделяет в среднем 89% пикселей с замененным младшим битом, при этом ложные срабатывания в среднем составляют 37%. Положение встроенных битов может быть определено на основе сравнения матрицы решений с исходным изображением. Предложенный алгоритм эффективен при заполнении стегоконтейнера от 10% до 30%.

3. Разработан алгоритм стегоанализа метода Коха-Жао на основе анализа коэффициентов дискретного косинусного преобразования. Показано, что стеганографический алгоритм Коха-Жао не является устойчивым к атаке анализа коэффициентов ДКП. Предложенный в данной главе алгоритм позволяет абсолютно точно извлекать встроенное сообщение при его обнаружении. Тестирование на коллекции изображений показало, что ошибки ложного

определения наличия СГВ в пустом стегоконтейнере составляют 23%. Эффективность обнаружения наличия встроенного сообщения составляет 85,5%.

4. Разработан и протестирован программный комплекс, реализующий предложенные алгоритмы, получившие свидетельства о государственной регистрации программ для ЭВМ и внедренные в ряде организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Абденов А.Ж., Леонов Л.С. Использование нейронных сетей в слепых методах обнаружения встроенной стеганографической информации в цифровых изображениях // Ползуновский Вестник. 2010. № 2. С. 221-225.
2. Алиев А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки // Вестник ДГТУ. – Ростов-на-Дону. 2004. Т. 4, № 4 (22). С. 454-460.
3. Барсуков В.С., Романцов А.П. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации // Специальная Техника. 2000. № 1.
4. Белим С.В., Вильховский Д.Э Выявление LSB-вставок на основе анализа младшего слоя // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы XI Межрегиональной научно-практической конференции. под ред. О. М. Голембиовской, М.Ю. Рытова. – Брянск: БГТУ, 2019. – С. 24-26.
5. Белим С.В., Вильховский Д.Э Стегоанализ алгоритма Коха-Жао // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы XI Межрегиональной научно-практической конференции. под ред. О. М. Голембиовской, М.Ю. Рытова. – Брянск: БГТУ, 2019. – С. 20-23.
6. Белим С.В., Вильховский Д.Э. Алгоритм выявления стеганографических вставок типа LSB-замещения на основе анализа слоя младших битов // Информатика и системы управления, 2017, №4(54), С. 3-11.
7. Белим С.В., Вильховский Д.Э. Алгоритм выявления стеганографических вставок типа LSB-замещения на основе метода анализа иерархий // Вестник компьютерных и информационных технологий. 2018. № 4 (166). С. 25-33.
8. Белим С.В., Вильховский Д.Э. Выявление стеганографических вставок типа LSB-замещения в растровых изображениях // В сборнике: Математическое и

компьютерное моделирование Сборник материалов V Международной научной конференции, посвященной памяти Р.Л. Долганова. Ответственный за выпуск И.П. Бесценный. 2017. С. 183-185.

9. Белим С.В., Вильховский Д.Э. Использование метода анализа иерархий для выявления стеганографических вставок в изображениях // В книге: Математическое и компьютерное моделирование сборник материалов IV Международной научной конференции. отв. за вып. И. П. Бесценный. 2016. С. 119-121.
10. Белим С.В., Вильховский Д.Э. Стеганоанализ алгоритма Коха-Жао // Математические структуры и моделирование 2018. № 4(48). С. 112–118
11. Вильховский Д.Э. Обзор методов стеганографического анализа изображений в работах зарубежных авторов // Математические структуры и моделирование. 2020. №4(56). С. 75–102.
12. Гиголаев А.В., Тярт Н.А., Швечкова О.Г. Модификация стеганографического метода LSB для повышения секретности передачи сообщения // В сборнике: Современные технологии в науке и образовании - СТНО-2018 Сборник трудов международного научно-технического форума: в 11 томах. Под общ. ред. О.В. Миловзорова. 2018. С. 43-47.
13. Гуц А.К., Вильховский Д.Э. Протоколы квантовой стеганографии // Математические структуры и моделирование 2020. № 2(54). С. 100–128.
14. Гуц А.К., Вильховский Д.Э. Стегоанализ цветных изображений с низким заполнением стегоконтейнера с использованием программного комплекса // Математические структуры и моделирование. 2020. №4(56). С. 103–111.
15. Жилкин М.Ю. Стегоанализ графических данных в различных форматах // Доклады ТУСУРа. 2008. № 2 (18), часть 1. С. 63-64.
16. Загоруйко Н.Г. Прикладные методы анализа данных и знаний // Новосибирск: ИМ СО РАН. 1999. 270 с.
17. Монарев В. А. Сдвиговый метод обнаружения скрытой информации // Вестник СибГУТИ. 2012. № 4. С. 62-68.

18. Abreu E., Lightstone M., Mitra S.K., Arakawa S.K. A new efficient approach for the removal of impulse noise from highly corrupted images // IEEE Transactions on Image Processing, IEEE Transactions on. 1996. V.5, P. 1012-1025.
19. Adelson E. Digital Signal Encoding and Decoding Apparatus. – U.S. Patent. – No. 4,939515 (1990).
20. Al-Jarrah M., Al-Taei Z., Aboarqoub A. Steganalysis using LSB-focused statistical features // In Proceedings of ICFNDS'17. Cambridge, United Kingdom, 2017. July 19-20. P. 1–5.
21. Avcibas I., Memon N., Sankur B. Image steganalysis with binary similarity measures // Proceedings of IEEE Int. Conference on Image Processing. 2002. P. 645-648.
22. Avcibas I., Memon N., Sankur B. Steganalysis of watermarking techniques using image quality metrics // In Proceedings of the SPIE, Security and Watermarking of Multimedia Contents II. 2000. V. 4314. P. 523–531.
23. Avcibas I., Memon N., Sankur B. Steganalysis using image quality metrics // IEEE transactions on Image Processing. 2003. V.12(2). P. 221-229.
24. Avcibaş I., Kharrazi M., Memon N., Sankur B. Image Steganalysis with Binary Similarity Measures // EURASIP Journal on Applied Signal Processing 2005. P. 2749–2757.
25. Bahaghighat M., Motamedi, S.A., Xin, Q. Image Transmission over Cognitive Radio Networks for Smart Grid Applications // Appl. Sci. 2019. *9*. 5498
26. Barni, M. Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications / M. Barni, F. Bartolini. – New York: Marcel Dekker, 2004. – 446 p.
27. Belim S.V., Vilkhoskiy D.E. Detection the Stego-Insertions Like LSB-Substitution in Bitmap Images // CEUR Workshop Proceedings. 2017. V.1965. [Электронный ресурс]. Режим доступа: http://ceur-ws.org/Vol-1965/paper11.pdf

28. Belim S.V., Vilkhoskiy D.E. Method of detecting hidden data transmission via the Koch-Zhao steganographic algorithm // Journal of Physics: Conf. Series. 2019. V. 1210. P. 012012(1-5).
29. Belim S.V., Vilkhoskiy D.E. Steganalysis Algorithm Based on Heirarchy Analysis Method // CEUR Workshop Proceedings. 2016. V.1732. [Электронный ресурс] Режим доступа: http://ceur-ws.org/Vol-1732/paper7.pdf.
30. Belim S.V., Vilkhoskiy D.E. Usage of analytic hierarchy process for steganographic inserts detection in images // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines"(Dynamics). 2016. [Электронный ресурс]. Режим доступа: http://ieeexplore.ieee.org/document/7818977/
31. Benton R., Chu H. Soft computing approach to steganalysis of LSB embedding in digital images // Proceedings of Int. Conference on Information Technology, Research, and Education. 2005. P. 105-109.
32. Bloom, J.A. Rotation, scale and translation resilient public watermarking for images / J.A. Bloom, I.J. Cox, M.L. Miller, C.Y. Lin, Y.M. Lui, M. Wu // Proc. SPIE Security Watermarking Multimedia Contents II. – 2000. – Vol. 3971. – P. 90-98.
33. Celik M.U., Sharma G., Tekalp A.M. Universal image steganalysis using rate-distortion curves // Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Con-tents VI. 2004. V. 5306. P. 19-22.
34. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun. 2019. 70. P. 233–245.
35. Chaeikar. S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // In Proceedings of the 10th International Conference on Computer Modeling and Simulation. Sydney, Australia. 8 January 2018. P. 14–18.
36. Chaumont M. Deep learning in steganography and steganalysis // In Digital Media Steganography, Academic Press. 2020. P. 321–349. [5]

37. Cheddad A. Digital image steganography: Survey and analysis of current methods // Signal processing. 2010. V. 90(3). P. 727-752.
38. Chen C., Shi Y.Q. JPEG image steganalysis utilizing both intrablock and interblock correlations // Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on. IEEE. 2008. P. 3029-3032.
39. Chen M, Boroumand M, Fridrich J (2018) Deep learning regressors for quantitative steganalysis // Electron Imaging. 2018. 7. P. 160–161. [6]
40. Chen X. Detect LSB steganography with bit plane randomness tests // Proceedings of IEEE World Congress on Intelligent Control and Automation. 2006. P. 10306-10309.
41. Cogranne R., Giboulot Q., Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis // Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. 2019. P. 125–137. [7]
42. Cox I.J. Secure Spread Spectrum Watermarking for Multimedia [Article] // IEEE transactions on image processing. - [s.l.] : IEEE, 1997. - 12 : Vol. 6. - pp. 1673-1687.
43. Deng Q.L. The blind detection of information hiding in color image // Computer Engineering and Technology (ICCET). 2010. V. 7. P. 346-348.
44. Deng Q.L., Lin J.J., A Universal Steganalysis Using Features Derived from the Differential Image Histogram in Frequency Domain // Image and Signal Processing. 2009. P. 1 – 4.
45. Dong J., Tan T. Blind Image Steganalysis Based on Run-Length Histogram Analysis // National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, ICIP. 2008. P. 2064-2067.
46. Dumitrescu S., Wu X. A new framework of LSB steganalysis of Digital Media // IEEE Trans. Signal Processing. 2005. V. 53(10). P. 3936-3947.
47. Dumitrescu S., Wu X. Steganalysis of LSB embedding in multimedia signals // Proceedings of IEEE ICME. 2002, P. 581- 584.

48. Dumitrescu S., Wu X., Memon N. On steganalysis of random LSB embedding in continuous-tone images // Proceedings of IEEE International Conference on Image Processing. 2002. V.3. P. 324-339.
49. Dumitrescu S., Wu X., Wang Z. Detection of LSB steganography via sample pair analysis// IEEE Trans. on Signal Processing. 2003. V. 51(7). P. 1995-2007
50. Eslam Mustafa M., Elshafey Mohamed A., Fouad Mohamed M. Enhancing CNN-based Image Steganalysis on GPUs // Journal of Information Hiding and Multimedia Signal Processing. 2020. 11(3). P. 138-150. [10]
51. Farid H. Detecting hidden messages using higher-order statistical models // In Proceedings of IEEE Int. Conf. Image Process., Rochester, NY, vol. 2, September 2002, P. 905–908.
52. Filler T., Fridrich J. Design of Adaptive Steganographic Schemes for Digital Images // Proceedings of SPIE, Media Watermarking, Security & Forensics of Multimedia III. 2011. V. 7880.
53. Fridrich J., and Goljan M. Practical steganalysis of digital images-state of the art // Proceedings of SPIE. 2002. V. 4675.
54. Fridrich J., Du R., Meng L. Steganalysis of lsb encoding in colour images // Proceedings of IEEE Int. conference on Multimedia and Expo. 2000. P. 1279-1282.
55. Fridrich J., Goljan M. Practical steganalysis of digital images-state of the art // Proceedings of SPIE, Security and Watermarking of Multimedia Contents IV. 2002. V. 4675. P. 1-13.
56. Fridrich J., Goljan M., Du R. Detecting LSB steganography in color and grey-scale images // Magazine of IEEE multimedia, Special Issue on Security. 2001. V. 8(4). P. 22-28.
57. Fridrich J., Goljan M., Soukal D. Higher-order statistical steganalysis of palette images // Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. 2003. V. 5020. P. 178-190.

58. Fridrich, J., Long M. Steganalysis of LSB encoding in color images // Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on. Vol. 3. IEEE. 2000.
59. Garna J., Brazdil P. Linear tree // Intelligent Data Analysis. 1999. P. 1-22.
60. Goljan, M., Fridrich, J., & Cogranne, R. Rich model for steganalysis of color images // In Information Forensics and Security (WIFS). IEEE International Workshop. 2014. P. 185- 190.
61. Hempstalk K. Hiding Behind Corners: Using edges in images for better steganography // Proceedings of Computing Women's Congress. 2006.
62. Johnson N., Jajodia S. Steganalysis The Investigation of Hidden Information // Proceedings of the IEEE Information Technology Conference. 1998.
63. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography // 5th International Workshop on Biometrics and Forensics (IWBF). 2017. P. 1 – 6
64. Kim J, Park H, Park J-I. CNN-based image steganalysis using additional data embedding // Multimed Tools Appl. 2020. 79 (1–2). P. 1355–1372. [23]
65. Koch E., Zhao J. Towards robust and hidden image copyright labeling // IEEE Workshop on Nonlinear Signal and Image Processing. 1995. P. 452-455.
66. Kodovsky J., Fridrich J. Quantitative structural steganalysis of Jsteg // IEEE Transactions on Information Forensics and Security. 2010. V. 5(4). 681-693.
67. Kodovsky J., Fridrich J., Holub V. Ensemble classifier for steganalysis of digital media // IEEE Trans. Inf. Forensics Security, April 2012. V. 7(2). P. 432–444.
68. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image using SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019. Vol 8. P. 1239 – 1246.
69. Li B., Wei W., Ferreira A, Tan S. ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis // IEEE Signal Process Lett. 2018. 25(5). P. 650–654. [25]

70. Li F., Zhang X., Chen B., Feng G. JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier // IEEE signal processing letters. March 2013. V. 20(3). P. 233-236.
71. Li H., Sun Z., Zhou Z. An image steganalysis method based on characteristic function moments and PCA // Control Conference (CCC), 30th Chinese Publication. 2011. P. 3005 – 3008.
72. Lie W., Lin G. A feature based classification technique for blind image steganalysis // IEEE Trans. Multimedia. 2005. V. 7(6). P. 1007-1020.
73. Lin E., Woertz E., Kam M. LSB steganalysis using support vector regression // Proceedings of IEEE, SMC Information Assurance Workshop. 2004. P. 95-100.
74. Lin J-Q, Zhong S-P. JPEG Image Steganalysis Method Based on Binary Similarity Measures // Proceedings of Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009. P. 2238-2243.
75. Lin, C.Y. Rotation, scale, and translation resilient watermarking for images / C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller, Y.M. Lui // IEEE Trans on Image Processing. – 2001. – N 10(5). – P. 767-782.
76. Liu S., Yao H., Goa W. Neural network based steganalysis in still images // Proceedings Int. Conf. on Multimedia and Expo, ICME2003. 2003. V. 2. P. 509–512.
77. Lu P., Luo X., Tang Q., Shen L. An improved sample pairs method for detection of LSB embedding // Proceedings of Int. liVorkshop on Information Hiding, LNCS 3200. 2004. P. 116-127.
78. Luo W., Huang F., Huang J. Edge Adaptive Image Steganography Based on LSB Matching Revisited // IEEE Trans. Information Forensics & Security. 2010. V. 5(2). P. 201-214.
79. Luo X., Liu F., Chen J., Zhang Y. Image universal steganalysis based on wavelet packet transform // Multimedia Signal Processing, IEEE 10th Workshop on Digital. 2008. P. 780 – 784.

80. Lyu S., Farid H. Steganalysis using color wavelet statistics and one-class vector support machines // In Proceeding of SPIE, Security, Steganography, Watermarking of Multimedia Contents. 2004. V. 5306. P. 35–45.
81. Lyu S., Farid H. Steganalysis using higher order image statistics // In Proceedings of IEEE Trans. Information Forensics and Security. 2006. V. 1(1). P. 111-119.
82. Manjula Devi T.H., Manjunatha Reddy H.S., Raja Venugopal K.B., Patnaik L.M. Detecting Original Image Using Histogram, DFT and SVM // International Journal of Recent Trends in Engineering. 2009. V. 1(1).
83. Marvel L., Henz B., Boncelet C. A performance study of±1 steganalysis employing a realistic operating scenario // Military Communications Conference, 2007. MILCOM. IEEE. 2007.
84. Miche Y. A feature selection methodology for steganalysis // International Workshop on Multimedia Content Representation, Classification and Security. Berlin Heidelberg. 2006.
85. Mielikainen J. Lsb matching revisited // IEEE Signal Processing Letters. 2006. V. 13(5), P. 285-287.
86. Mitra S., Roy T., Mazumdar D., Saha A.B. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis // IITKHACK. 2014. 24 Feb. P. 11–14.
87. Ng W.W.Y., He Z-M., Chan P.P.K, Yeung D.S. Blind Steganalysis with High Generalization Capability for different Image Databases L-GEM // Proceedings of the 2011 International Conference on Machine Learning and Cybernetics. Guili. 2011. P. 1690-1695.
88. Noriega J. A. M., Kurkoski B. M., Miyatake M. N. and Meana H. P.. Image Authentication and Recovery Using BCH Error-Correcting Codes // INTERNATIONAL JOURNAL OF COMPUTERS, 2011. Issue 1, Vol. 5. P. 26-33.
89. Pevny T., Filler T., Bas P. "Using high dimensional Image models to perform highly undetectable steganography," In P.W.L. Fong, R. Bohme, and Rei

Safaviaini, editors // Proceedings of Information Hiding Workshop, LNCS 6387. 2010. P. 161-177.

90. Pevny T., Fridrich, J. Merging markov and dct features for multiclass jpeg steganalysis // IS and T/SPIE EI 2007, Lecture Notes in Computer Science. 2007. V. 6505.
91. Priya R.L., Eswaran P., Kamakshi S.L.P. Blind Steganalysis with Modified Markov Features and RBFNN // IJERT. e-ISSN 2278-0181. 2013. V(5).
92. Provos N., Honeyman P. Detecting steganographic content on the internet // Technical Report CITI 01-1a, University of Michigan. 2001.
93. Quinlan J.R. C4.5: Programs for Machine Learning // Morgan Kaufmann, San Mateo, CA. 1993.
94. Rashid R. D., Asaad A., Jassim S. Topological data analysis as image steganalysis technique // Mobile Multimedia/Image Processing, Security, and Applications. 2018. Vol. 10668. P. 17 – 26.
95. Roue B., Bas P., Chassery J. Improving LSB steganalysis using marginal and joint probabilistic distributions // Proceedings of ACM Vlorkshop on M'ultimedia 8 Security. 2004. P. 275- 287.
96. Saaty T.L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process // Review of the Royal Spanish Academy of Sciences, Series A, Mathematics, 2008, V.102 (2), P. 251–318.
97. Shankar D.D., Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO // Multimedia Tools and Applications. 2020. DOI: 10.1007/s11042-020-09820-7.
98. Sharifzadeh M., Agarwal C., Aloraini M., Schonfeld D. Convolutional neural network steganalysis’s application to steganography // IEEE Visual Communications and Image Processing. 2017. 12. P. 1-4. [32]

99. Sharp T. An implementation of key-based digital signal steganography // Proceedings of the 4th Information Hiding Workshop. 2001. V. 2137, P. 13-26.
100. Shi Y. Q., Chen C., Chen W. A Markov process based approach to effective attacking jpeg steganography // Proceedings of the 8th Information Hiding Workshop. 2006. V. 4437. P. 249-264.
101. Shojaei-Hashemi A., Ghaemmaghami S., Soltanian-Zadeh H., Universal Steganalysis based on Local Prediction Error in Wavelet Domain // Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2011. P. 165-168.
102. Simmons G. J. The prisoners' problem and the subliminal channel // Proceedings of CRYPTO'83. 1983. P. 51-67.
103. Singh K.M., Singh L.S., Singh A.B., Devi K.S. Hiding secret message in edges of the image // Proceedings of Int. Con-ference on Information and Communication Technology. 2007. P. 238-241.
104. Siwei L.,Farid H. Steganalysis using higher-order image statistics // IEEE transactions on Information Forensics and Security. 2006. V 1(1). P. 111-119.
105. Smola A.J., Scholkopf B. A tutorial on support vector regression // Tech. Rep. NC2-TR-1998 030. 1998.
106. Soto R.T., Ramos-Pollan R., Isazad G., et al. Digital media steganalysis // Digital Media Steganography: Principles, Algorithms, and Advances. 2020. P. 259-293. [33]
107. Stoyanova, Veselka T.: Steganography System Using LSB Methods // Proceedings of the ENTRENOVA. ENTerprise REsearch InNOVAtion Conference, Split. Croatia, IRENET – Society for Advancing Innovation and Research in Economy, Zagreb. 6–8 September 2018. Vol. 4. P. 381–387.
108. Sullivan K., Madhow U., Chandrasekaran S., Manjunath B.S. Steganalysis for Markov cover data with applications to images // IEEE Transactions on Information Forensics and Security. 2006. V. 1(2). P. 275-287.

109.Sun Z., Hui M., Guan C. Steganalysis Based on Cooccurrence Matrix of Differential Image // Intelligent Information Hiding and Multimedia Signal Processing, Aug. 2008. P.1097 – 1100.

110.Sun Z., Li H., Wu Z., Zhou Z. An Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands // Artificial Intelligence and Computational Intelligence. 2009. P. 291 – 295.

111.Tao Z., Xijian P. Reliable detection of lsb steganography based on the difference image histogram // Proceedings of IEEE ICAAP, Part III. 2003. P. 545-548.

112.Wang Y., Moulin P. Optimized feature extraction for learning based image steganalysis // IEEE Trans Inf Forensics Security. 2005. V 2(1). P. 262-277.

113.Wang Z., Chen M., Yang Y. Joint multi-domain feature learning for image steganalysis based on CNN // EURASIP Journal on Image and Video Processing. 2020 (1). DOI: 10.1186/s13640-020-00513-7. [34]

114.Westfeld A. F5-a steganographic algorithm: high capacity despite better steganalysis // Proceedings of the 4th Information Hiding Workshop. 2001. V. 2137. P. 289-302.

115.Westfeld A., Pfitzmann A. Attacks on steganographic systems-breaking the steganographic utilities ezstego, jsteg, steganos, and s-tools-and some lessons learned // Proceedings of the 3rd Information Hiding Workshop. 1999. V. 1768. P. 61-76.

116.Westfield A. Detecting low embedding rates // Proceedings of Int. Workshop on Information Hiding. LNCS 2578. 2003. P. 324-339.

117.Westfield A., Pfitzmann A. Attacks on steganographic systems // Proceedings of Int. Workshop on Information Hiding, LNCS 1768. 2000. P. 61-75.

118.Wu D.C., Tsai W.H. A steganographic method for images by pixel-value differencing // Pattern Recognition Letters. 2003. V. 24(9-10). P. 1613-1626.

119.Xu G., Wu H. Z., Shi Y. Q. Structural design of convolutional neural networks for steganalysis // IEEE Signal Process. 2016. 23(5). P. 708–712. [38]

120.Xu G., Wu H-Z., and Shi YQ. Ensemble of CNNs for steganalysis: An empirical study // Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. 2016. P. 103–107. [39]

121.Xuan G. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions // Proceedings of Int. Conference on Information Hiding, LNCS 3727. 2005. P. 262-277.

122.Yan Y., Li L., Zhang Q. Universal Steganalysis method based on Multi- Domain Features // Journal of Information & Computational Science. 2013. P. 2177-2185.

123.Yang C., Wang J. Lin C. Chen H., Wang W. Locating steganalysis of LSB matching based on spatial and wavelet filter fusion // CMC-Comput. Mat. Contin. 2019. 60(2). P. 633–644.

124.Yang C.H., Weng C.Y., Wang S. J., Sun H.M. Adaptive data hiding in edge areas of images with spatial LSB domain systems // IEEE Trans. Information Forensics and Security. 2008. V. 3(3). P. 488-497.

125.Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Security. 2017. 12(11). P. 2545–255. [41]

126.Yedroudj M., Comby F., Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2018. P. 2092–2096. [42]

127.You W, Zhang H., ZhaoX. A Siamese CNN for Image Steganalysis // IEEE Transactions on Information Forensics and Security. 2020. Vol. 16. P. 291-306. [43]

128.Yu X., Tan T., Wang Y. Isotropy-based detection and estimation: A general framework of LSB steganalysis // IEEE Trans. Image Processing, vol. 14, no. 5. 2005. P. 509-517.

129.Zhan S-H, Zhang H-B, Blind Steganalysis using Wavelet Statistics and ANOVA // Machine Learning and Cybernetics, International Conference on Volume 5, August 2007. P. 2515 – 2519.

130. Zhang R., Zhu F., Liu J., Liu G. Efficient feature learning and multi-size image steganalysis based on CNN. 2018. – https://www.researchgate.net/publication/326696542_Efficient_feature_learning_and_multi-size_image_steganalysis_based_on_CNN. [45]
131. Zhang T, Zhang H, Wang R, Wu Y. A new JPEG image steganalysis technique combining rich model features and convolutional neural networks // Math Biosci Eng. 2019. 16(5). P. 4069–4081. [46]
132. Zhang X., Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security // Pattern Recognition Letters. 2004. V. 25(3). P. 331-339.
133. Zhi L., Fen S., Xian Y. A LSB steganography detection algorithm // Proceedings of IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communication. 2003. P. 2780-2783.
134. Zou D., Shi Y.Q., Su W., Xuan G. Steganalysis based on Markov model of threshold prediction-error image // Proceedings of IEEE ICME. 2006. P. 1365-1368.

Приложение 1: Свидетельство о государственной регистрации программы для ЭВМ №2017661544

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2017661544

Программа выявления стеганографических вставок типа LSB-замещения на основе метода анализа иерархий

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского» (RU)***

Авторы: ***Белим Сергей Викторович (RU),***
Вильховский Данил Эдуардович (RU)

Заявка № **2017614324**
Дата поступления **10 мая 2017 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***16 октября 2017 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

Приложение 2: Свидетельство о государственной регистрации программы для ЭВМ №2018660624

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018660624

Определение наличия стеганографических вставок на основе дискретного косинусного преобразования

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского» (RU)***

Авторы: ***Вильховский Данил Эдуардович (RU),***
Белим Сергей Викторович (RU)

Заявка № **2018617407**
Дата поступления **16 июля 2018 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***28 августа 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

Приложение 3: Свидетельство о государственной регистрации программы для ЭВМ №2018619350

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018619350

Извлечение сообщения, встроенного в изображение методом Коха-Жао

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского» (RU)***

Авторы: ***Вильховский Данил Эдуардович (RU),***
Белим Сергей Викторович (RU)

Заявка № **2018617635**
Дата поступления **18 июля 2018 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***03 августа 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

Приложение 4: Акт о внедрении ООО СМТ «Стройбетон»

Общество с ограниченной ответственностью
Строительно-монтажный трест
«Стройбетон»

646973 Омская область, Кормиловский р-н, с. Михайловка
ул.Советская д.3
р/с 40702810800000002421 ОА «ИТ Банк» к/сч
30101810900000000731
Контактные телефоны: 21-78-43,21-78-35
Телефон-факс : 21-78-46
Поч. Адрес:644065 г.Омск ул. Заводская д.15

ИНН 5517200848
КПП 551701001
БИК 045209731
ОКПО 09480042
ОГРН 1125543050588
ОКОГУ 4210014

№ 126 «16» октября 2020 г.

АКТ
о внедрении результатов диссертационной работы Д.Э. Вильховского «Алгоритмы стеганографического анализа изображений с низким заполнением стегоконтейнера»

Комиссия в составе: председатель Дремов К.В. (начальник информационного отдела), члены комиссии: Сасин А.С. (первый заместитель генерального директора), Луценко Н.И. (заместитель генерального директора по вопросам строительного надзора и качества), составили настоящий акт о том, что результаты диссертационной работы «Алгоритмы стеганографического анализа изображений с низким заполнением стегоконтейнера» и разработанный программный комплекс , позволяющий проводить стегоанализ изображений с внедренными данными методом LSB-вставки и методом Коха-Жао. (Свидетельства о государственной регистрации программ для ЭВМ №2017661544 от 16.10.2017, №2018617635 от 03.08.2018, №2018617407 от 28.08.2018) были внедрены во внутреннюю систему документооборота ООО Строительно-монтажный трест «Стройбетон».

Программный комплекс представляет собой веб-приложение с микросервисной архитектурой. Взаимодействует через GET/POST запросы. Принимает на вход либо URL изображения, либо изображение, переведенное

в формат base64, на выходе возвращает json файл содержащий следующие данные:

- Ответ касательно наличия или отсутствия стеганографической вставки
- Параметры встраивания
- Извлеченное сообщение
- Модифицированное изображение в формате base64, не содержащее стеганографической вставки.

Интеграция с системой документооборота осуществлена через реализацию хуков приложения, которые вызываются в следующих случаях:

- при загрузке файла на сервер
- при добавлении, обновлении строк в таблицах базы данных (реализовано на уровне ORM моделей приложения)

Практическим результатом является повышение функциональности информационной системы документооборота: добавлена функция анализа базы данных изображений, хранящихся в системе, на наличие стеганографических вставок.

Внедрение результатов позволило существенно повысить уровень информационной защищенности внутреннего документооборота организации за счет возможности отслеживать наличия скрытого канала передачи данных при обработке изображений.

Председатель комиссии _____ Дремов К.В.

Члены комиссии:

_____ Сасин А.С.

_____ Луценко Н.И.

Приложение 5: Акт о внедрении в учебный процесс

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Омский государственный университет им. Ф.М. Достоевского»

Утверждаю
Проректор по учебной работе
ФГБОУ ВО «Омский государственный
университет им. Ф.М. Достоевского»
д.и.н., проф.

Т.Б. Смирнова
«__» _____ 2020 г.

А К Т

о внедрении результатов диссертационной работы Вильховского Д.Э.
«Алгоритмы стеганографического анализа изображений с низким заполнением стегоконтейнера» в учебный процесс университета

Настоящий акт составлен в том, что результаты диссертационной работы Вильховского Данила Эдуардовича, а именно:

1. Алгоритм стеганографического анализа метода LSB-замены при низком заполнении стегоконтейнера, основанный на анализе нулевого слоя с применением метода таксономии
2. Алгоритм стеганографического анализа метода LSB-замены при низком заполнении стегоконтейнера, основанный на сравнительном анализе нескольких слоев изображения с помощью метода анализа иерархий
3. Алгоритм стеганографического анализа метода Коха-Жао, основанный на анализе коэффициентов дискретного косинусного преобразования

используются факультетом компьютерных наук Омского государственного университета им. Ф.М. Достоевского в учебном процессе при подготовке бакалавров по специальности 10.03.01 «Информационная безопасность» по дисциплинам «Анализ уязвимостей программного обеспечения», «Компьютерная экспертиза», а также при подготовке специалистов по специальности 10.05.01 «Компьютерная безопасность» по дисциплинам «Анализ уязвимостей программного обеспечения», «Основы цифровых расследований» при чтении курсов лекций, проведении практических и лабораторных работ с 1 сентября 2017 года.

И.о. заведующего кафедрой
информационной безопасности ОмГУ,
к.ю.н., доцент

А.И. Горев