Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное 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 2.3.6. Методы и системы защиты информации, информационная безопасность

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель:

доктор физико-математических наук, профессор

Гуц Александр Константинович

Омск – 2023

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 25% 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.

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 25%. При более низких показателях заполнения вероятность обнаружения наличия СГВ не превышает 30% [124]. 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 [45, 107, 127]. 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 исследования. Методы стегоанализа находятся в постоянном развитии, что, во многом, обусловлено развитием методов стеганографии.

Большой вклад в развитие методов стеганографии внесли: Т. Шарп (T.Sharp), К. Хемпстальк (Hempstalk K.), К. Чжан (X. Zhang), С. Ванг (S. Wang), Л.К. Бабенко, И.С. Вершинин, А.В. Красов, В.Н. Кустов, В.А. Райхлин, М.В. Шакурский и др.

В развитие методов стегоанализа внесли большой вклад: Н. Провос (N. Provos), Д. Фридрич (J. Fridrich), К. Салливан (K. Sullivan), Х. Фарид (H. Farid), Леонов Л.С., Жилкин М.Ю. и пр.

Однако анализ современных исследований в области стеганографического анализа свидетельствует о том, что наряду с имеющимися алгоритмами недостаточно разработаны специализированные алгоритмы для цветных изображений с низким заполнением стегоконтейнера, показывающие высокую эффективность при работе со встраиваниями, выполненными методом LSB-замены или методом Коха-Жао. Кроме того, большинство существующих алгоритмов стегоанализа не решают задачу локализации области встраивания.

Объектом исследования являются изображения с низким уровнем заполнения стегоконтейнера (<25%), встраивания в которые осуществлялись с помощью методов LSB-замены и Коха-Жао.

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

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

Для достижения поставленной цели решались следующие **задачи исследования**:

1. Разработка алгоритма стегоанализа метода LSB-замены при низком заполнении стегоконтейнера на основе анализа битового нулевого слоя на предмет наличия уникальных последовательностей с применением алгоритма решения задачи о наибольшем пустом прямоугольнике.

2. Разработка алгоритма стегоанализа метода LSB-замены при низком заполнении стегоконтейнера на основе сравнительного анализа битового нулевого и первого слоев с использованием моделей попарного сходства, моделей доминирования, моментов изображения, а также задачи о наименьшем пустом прямоугольнике.

3. Разработка алгоритма стегоанализа метода Коха-Жао на основе анализа коэффициентов дискретного косинусного преобразования с выделением их сигнатур и применением алгоритма машинного обучения и кластеризации DBSCAN.

4. Разработка программного обеспечения, реализующего предложенные алгоритмы стегоанализа, и оценка их эффективности.

Методы исследования. Для решения поставленных задач в работе 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.

Научная новизна

1. Предложен алгоритм стеганографического анализа метода LSB-замены и локализации области встраивания при низком заполнении стегоконтейнера, основанный на анализе нулевого слоя на предмет установления областей с уникальными последовательностями пикселей с применением метода решения задачи о наибольшем пустом прямоугольнике, *отличающийся* наличием модуля предварительной обработки изображения, позволяющего выделить области, содержащие уникальные последовательности пикселей, модуля фильтрации шумов и блока автоматического поиска границ встраиваний на базе алгоритма решения задачи о наименьшем пустом прямоугольнике, что дает возможность обнаружить встроенное сообщение, а также определить его положение и размер.

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613002 от 01.03.2022.

2. Предложен алгоритм стеганографического анализа метода LSB-замены и локализации области встраивания при низком заполнении стегоконтейнера, основанный на сравнительном анализе нулевого и первого слоев изображения, *отличающийся* наличием модуля первичной классификации изображения посредством выявления межслойных попарных несовпадений и локализации подозрительных пикселей для определения максимально широкой области возможного встраивания с применением алгоритма решения задачи о наибольшем пустом прямоугольнике с блоком рекурсивного фильтра для нивелирования случайных шумов, а также модулем локализации фактической области встраивания на основе моделей доминирования и соотношения пикселей и использовании моментов изображения для сужения области встраивания посредством последовательного отсечения излишних блоков, что дает

возможность обнаружить встроенное сообщение, а также определить его положение и размер.

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613021 от 01.03.2022.

3. Предложен алгоритм стеганографического анализа метода Коха-Жао и локализации области встраивания, основанный на анализе разниц пар коэффициентов дискретного косинусного преобразования, *отличающийся* присутствием модуля автоматической кластеризации на основании двух сигнатур, определяемых на основе разниц пар коэффициентов ДКП, и использованием алгоритма машинного обучения и кластеризации DBSCAN для выделения кластера, содержащего блоки встраивания, позволяющего определить наличие встраивания, а также его положение и размер.

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613003 от 01.03.2022.

4. Разработан программный комплекс, позволяющий проводить стегоанализ изображений с данными, внедренными методом LSB-вставки и методом Коха-Жао.

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 разработанные алгоритмы и реализованный с их использованием программный комплекс позволяет проводить стегоанализ изображений с данными, встроенными методом LSB-вставки и методом Коха-Жао, при низком заполнении стегоконтейнера (объем вставки составляет, в зависимости от метода, против которого направлен стегоанализ, от 10% до 25% общего объема контейнера).

Разработанный алгоритм стеганографического анализа изображений на предмет обнаружения вставок, выполненных методом замены наименее значащего бита, и локализации области встраивания имеет высокую эффективность в отношении цветных искусственных изображений с градиентной заливкой.

Так, в среднем, эффективность выявления LSB-вставок при малых объемах заполнения стегоконтейнера составляет 98,5% (максимальная эффективность составляет 99% и достигается при работе с 25% уровнем стегонагрузки, при работе с 10% уровнем заполнения стегоконтейнера эффективность составляет 98%), а средняя точность локализации области встраивания составляет 97,53% (98,27% при 25% уровне стегонагрузки и 96,87%при 10% уровне стегонагрузки). При этом алгоритм одинаково эффективен при атаке на встраивание в любую из компонент изображения. Наличие ложных срабатываний при анализе чистых изображений не выявлено.

Разработанный алгоритм стеганографического анализа изображений на предмет обнаружения LSB-вставок, и локализации области встраивания эффективен в отношении цветных фотографических изображений при малых объема заполнения стегоконтейнера. Так, средняя эффективность выявления LSB-вставок составляет 78,8%. При этом максимальная эффективность достигается при работе с 25-% уровнем стегонагрузки и составляет в среднем 88,53%, тогда как при работе с 10 % уровнем заполнения стегоконтейнера, эффективность обнаружения LSB-вставок составляет в среднем составляет 69,07. Средняя точность локализации области встраивания (процент обнаруженных пикселей, содержащих встраивание) составляет 88,92% (92,37% при 25% уровне стегонагрузки и 85,47%при 10% уровне стегонагрузки). При этом алгоритм практически одинаково эффективен при атаке на встраивание в любую из компонент изображения. Процент ложных срабатываний при анализе чистых изображений составляет 3,4%.

Разработанный алгоритм стеганографического анализа цветных изображений на предмет обнаружения вставок, выполненных методом Коха-Жао, и локализации области встраивания также имеет высокую эффективность. При

стегоанализе изображения со встраиванием, выполненным методом Коха-Жао, на примере коллекции BSDS500 показано, что эффективность предложенного алгоритма с точки зрения обнаружения наличия встроенного сообщения практически не зависит от уровня стегонагрузки и варьируется от 98,6% до 98,8%, а его средняя эффективность локализации области встраивания составляет 97,87%, находясь в диапазоне 97,16 – 98,57%. При этом ложные срабатывания алгоритма при работе с чистыми изображениями составляют всего 1,8%.

Результаты диссертационного исследования внедрены в учебный процесс Омского государственного университета им. Ф.М. Достоевского, а также в системы документооборота организаций ООО Строительно-монтажный трест «Стройбетон» и ООО «РЕЙЛСТРОЙ-1520»: 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.

Положения, выносимые на защиту:

1. Алгоритм анализа цветных искусственных цифровых изображений на наличие LSB-вставок и локализации области встраивания на основе анализа нулевого слоя на предмет наличия уникальных последовательностей пикселей с применением задачи о наибольшем пустом прямоугольнике.

2. Алгоритм анализа цветных фотографических цифровых изображений на наличие LSB-вставок и локализации области встраивания на основе сравнительного анализа нулевого и первого слоев изображения на предмет выявления межслойных попарных несовпадений с использованием моделей доминирования пикселей, моментов изображения и применением задачи о наибольшем пустом прямоугольнике.

3. Алгоритм анализа цифровых изображений на наличие вставок методом Коха-Жао и локализации области встраивания на основе анализа разниц пар

коэффициентов дискретного косинусного преобразования с выделением двух сигнатур и применением алгоритма машинного обучения и кластеризации DBSCAN.

4. Программный комплекс, реализующий предложенные алгоритмы.

Степень достоверности результатов работы обусловлена теоретической обоснованностью, отсутствием внутренних и иных противоречий, адекватностью применяемых методов, результатами, полученными в процессе тестирования разработанных алгоритмов, государственной регистрацией программ для ЭВМ, а также внедрением разработанного на основе данных алгоритмов программного комплекса в деятельность организаций ООО Строительно-монтажный трест «Стройбетон» и ООО «РЕЙЛСТРОЙ-1520» для анализа изображений на наличие стеганографических вставок.

Личный вклад соискателя. В диссертации используются результаты, в получении которых основная роль при постановке и решении задач, а также тестировании алгоритмов и обобщении полученных данных принадлежит автору. Ряд публикаций написан в соавторстве с Гуцом А.К.

Апробация результатов работы. Результаты работы проходили обсуждения на таких научных конференциях как: IV Всероссийская научная конференция «Омские научные чтения» (Омск, 2020), XV Международная научно-техническая конференция «Динамика систем, механизмов и машин» (Омск, 2021), IX Международная научная конференция «Математическое и компьютерное моделирование» (Омск, 2021), XI Всероссийская научно-практическая конференция «Молодые учёные России» (Пенза, 2022), IX Научно-практическая конференция с международным участием «Новые горизонты» (Брянск, 2022), XXVI Международная научно-техническая конференция студентов, аспирантов и молодых учёных «Научная сессия ТУСУР – 2022» (Томск, 2022), 23 всероссийский конкурс-конференция студентов и аспирантов SIBINFO-2023, Научная сессия ТУСУР (Томск, 2023).

Соответствие паспорту специальности. Содержание диссертации соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность:

п.6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

Публикации результатов работы. По материалам исследований опубликованы 15 работ, в том числе 3 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК (квартили К2 и К3), 1 статья в научных изданиях, индексируемых международными базами данных, перечень которых определен в соответствии с рекомендациями ВАК, 2 научные работы в изданиях, включенных в базу Scopus, 6 статей в других изданиях. Получено 3 свидетельства о регистрации программ для ЭВМ.

Структура и объем диссертации

Диссертация включает в себя введение, 4 главы, заключение, список литературы и приложения. Основной текст диссертации изложен на 147 страницах, содержит 24 рисунка, 9 таблиц, 6 приложений. Список литературы включает в себя 157 наименований.

Глава 1. Методы стеганографии и стегоанализа

Первая глава диссертационной работы 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.

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 [54]. 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 [122], 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 $\boldsymbol{\Psi}(.)$, 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 $\boldsymbol{Y' \neq Y}$ 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.

Одним из подходов, позволяющих обеспечить высокую эффективность в выполнении вышеизложенных требований, является ассоциативная стеганография [5, 19, 28, 29].

При этом, наряду с проблемами безопасности, вместимости и незаметности [23, 24, 26, 30], в последнее время большое внимание уделяется проблеме устойчивости встраивания к различным деструктивным воздействиям [3, 25].

Следует отметить, что методы стеганографии активно используются не только для незаметной передачи и обмена секретной информации, но и для защиты авторских прав, в том числе авторских прав на изображение, а также отслеживания соблюдения лицензионных соглашений в сфере программного обеспечения. В последнем случае могут быть созданы специальные стеганографические модули, реализующие подобную защиту [33 – 35].

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:

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

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 [118, 143, 153]. 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 [67, 142, 148]. При этом, для целей стегоанализа могут применяться как различные подвиды нейронных (в частности, сверточных нейронных) сетей [87, 149, 150], так и комбинация их с классическими моделями, например пространственной SRM-модели [154].

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 изображение, не содержащее встраивания, было корректно определено как не являющееся стегоконтейнером.

4. Ложно-позитивный (FP) означает, что изображение, не содержащее встраивания, было некорректно определено 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 цветовых компонентов. Так как цветных компонентов в общей сложности три (красный, зеленый и синий), то получается, что в каждом пикселе можно сохранить три бита. В среднем, чтобы скрыть секретное сообщение длиной n бит, количество бит изображения, которые необходимо изменить, определяется как ½ от длины встраиваемого сообщения. Эффективность скрытия встроенного сообщения при таком алгоритме обусловлена тем, что изменения вносятся в наименее значимые биты, которые к тому же, слишком малы для визуального распознания и детекции наличия встраивания. В целом, алгоритмы измененения LSB пикселей могут быть разные, варьируясь от случайного выбора этих пикселей в изображении-стегоконтейнере или выборки пикселей в определенных областях изображения до простого увеличения или уменьшения значения пикселя. При этом, активно разрабатываются в успешно внедряются двухкомпонентные методы встраивания в младшие биты [31, 32].

Метод LSB-совпадений [119] 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 [103] использует пару пикселей в качестве блока внедрения, в котором младший бит первого пикселя несет один бит секретного сообщения, а второй бит встраивания содержится в связке (нечетно-четная комбинация) двух значений пикселей. Это способствует уменьшению интенсивности изменений пикселей на

целых 25% (с 0,5 до 0,375 бит/пиксель – в случае максимальной интенсивности внедрения). В свою очередь, уменьшение интенсивности изменений пикселей уменьшение изменений в исходном изображении при прочих равных условиях, то есть с той же полезной нагрузкой. Такая схема помогает избежать асимметрии LSB-замены, и она должна сделать обнаружение более сложным.

В [79] 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 [123] 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 [123]. 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 [141,147,155], 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 [96] показано, что данные подходы не могут полноценно использовать информацию о границах для скрытия данных. Кроте того, такие подходы являются очень

чувствительными к некоторым статистическим анализам, что означает высокий риск обнаружения встраивания.

В [96] предложен перекрестно-адаптивный стеганографический алгоритм. Данный алгоритм определяет разность LSB-битов, сопоставляя их. Выбор области встраивания осуществляется с учетом размера встраивания и разности LSB-битов двух последовательных пикселей в исходном изображении. Когда интенсивность внедрения возрастает, выделение крайних областей происходит адаптивно. Многие адаптивные стеганографические методы, предложенные в работах [69, 108], 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 качестве основного фокуса как основы детекции наличия встраивания здесь является структурная асимметрия. Впервые алгоритм стегоанализа с использованием статистического метода был предложен в статье [140]. Несомненно, эффективность данного метода гораздо выше по сравнению с простой визуальной детекцией. Метод основан на идентификации и сопоставления пары значений, состоящие из значения пикселей, квантованных коэффициентов

дискретного косинусного преобразования или индексов палитры. Эта концепция парных зависимостей и неизменности общего количества вхождений двух членов пары значений используется для разработки статистического критерия Хи-квадрат для обнаружения скрытых сообщений [72, 140]. Представленные результаты показывают, что указанный метод надежно обнаруживает последовательно встроенные сообщения. Позже этот метод был обобщен для обнаружения беспорядочно рассеянных сообщений [139]. Другим специальным методом стегоанализа для обнаружения LSB- замены в 24-битных цветных изображениях является метод необработанных пар, предложенный в [71]. 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 и высокоэффективно, если количество уникальных цветов в исходном изображении составляет менее 30% от числа пикселей. По сравнению с алгоритмом, приведенным в [140], данный метод стеганографического анализа является более эффективным. Однако, в качестве недостатков данного метода следует выделить невозможность его применения к черно-белым изображениям. В отличие от предыдущего, метод, представленный в [73], использующий чувствительную двойную статистику, полученную из пространственных корреляций в изображениях, неплохо подходит для стегоанализа как цветных, так и черно-белых изображений. Для этого производится непересекающаяся разбивка изображения на группы заранее заданной формы, по каждой из которых определяется среднее абсолютное значение корреляций между пикселями как характеристики степени шума, который появляется при наложении маски и изменении младшего слоя фиксированного набора пикселей внутри каждой группы. В зависимости от направления изменения шума, все группы можно отнести или к сингулярным (при уменьшении шума пикселя), или к регулярным (при увеличении шума пикселя). 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 [41], 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 [64, 65]. 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 [73], но в некоторых случаях средняя абсолютная ошибка становится значимой из-за неравновесности корреляций и неравномерного распределения совместной статистики изображения [114].

Модификация описанного выше подхода предложена в [95]. В этом методе проблема выявления СГВ решается посредством метода наименьших квадратов,

что повышает точность распознавания стего-изображений, доказанную на наборе тестовых изображений. Еще один статистический метод стеганографического анализа, использующий статистику более высокого порядка предложен в [63]. Метод основан на вычислении и оценке подписи как отличительной статистической величины. Указано, что статистика подписи, как функция объема встраивания, зависит от некоторого вектора признаков, чувствительного к этому объему. 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 [156]. 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 и позволяющий произвести успешную атаку на методы последовательной или случайной LSB замены в изображениях и оценки объема встраивания, предложен в [132]. В качестве инструмента статистического анализа метод использует гистограмму разностей изображения, коэффициенты которой являются мерой корреляции между LSB-плоскостью и остальными плоскостями и используются для построения классификатора распознавания стего- и чистых изображений. 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 [74]. 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 [140].

Еще один метод стегоатаки на встраивания, рассеянные случайным образом в нулевом слое цветных или черно-белых изображений, предложен в [91]. Этот метод основан на сборе и проверке набора соответствующих функций изображения из пиксельных групп стегоконтейнера, измерении корреляций и сходств между ними. Эти функции различны при разных отношениях интенсивности встраивания. Для детектирования изображений со СГВ используется векторная регрессия [125]. Метод позволяет распознать наличие СГВ, а также определить их приблизительный размер.

Метод стегоанализа, представленный в [46], 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 [47]. Для обнаружения вставок независимо используются методы поддержки принятия решений и нейронные сети [58, 136]. Предложено несколько алгоритмов генерации деревьев принятия решений [76, 112]. 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 [151]. Этот метод основан на анализе изотропии. Сначала определяется взвешенный стегообраз, из которого выводится формула оценки. Эффективность этого метода с точки зрения обнаружения СГВ и оценки стегонагрузки относительно высока.

Метод стегоанализа, основанный на тестах случайности битовых слоев, предлагается в [57]. Метод использует алгоритм Гильберта и производит сканирование первого и нулевого битового слоев изображения для выделения двух бинарных последовательностей. Случайность этих последовательностей проверяется четырьмя видами тестов – для каждой из последовательностей. В результате выстраиваются опорные вектора, на основе которых выстраивается классификатор. По приведенным в работе результатам тестирования данного метода, можно сделать вывод, что метод эффективен для атаки на встраивания при интенсивности встраивания не менее 0,05 бит на пиксель.

Анализ перечисленных выше результатов показывает, что статистические методы позволяют обнаружить встроенное сообщение и оценить его длину при интенсивности внедрения более 0,05 бит на пиксель. 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 [138]. В основе этой атаки лежит способность человеческого глаза обнаруживать искажения изображения, вызванного встраиванием. Алгоритм анализа пар изображений, предложенный в статьях [20,70] 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 [111,138] 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 [4] 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 [52, 126]. 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 [138]. Работа [21] 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 [27] добавляется, что при наличии предварительно обработанного изображения, указанный метод будет эффективным даже в случае, если контейнер наполнен меньше 40%.

Стеганографический алгоритм F5 [137] 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 [84] 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 [80] предпринята попытка классифицировать атаки стегоанализа для восстановления или удаления сообщения на основе доступной информации. Разработанная методика стегоанализа может обнаруживать несколько вариантов методов скрытия сообщения [101]. Первый метод стегоанализа с использованием вейвлет-разложения был разработан в [124] 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 [129] используется эмпирическая матрица как параметр для стегоанализа. В работе [55] 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 [43]. 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 [75], представляет собой специфический метод стегоанализа для обнаружения данных LSB-замены, скрытых в изображениях. Используя оценки совместной вероятности [102], 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 [46] 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 с максимальной точностью отображать даже небольшие искажения изображения, образуемые при размытии или сжатии изображений, добавления аддитивного шума и т.д. В качества важнейших характеристик показателей качества изображения можно также выделить их последовательность и монотонность.

В статье [42] проведен статистический анализ поведения чувствительности и согласованности 26 показателей качества изображения. Данные показатели были разделены на шесть групп в зависимости от типа используемой ими информации и исследованы на предмет чувствительности и согласованности с кодированием информации, а также аддитивным шумом и уровнем размытия изображения как стегоконтейнера. Значения показателей определялись исходя из разности пикселей, корреляции, краевому спектру и контексту. 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 [104] 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 имеющего 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 [120], 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 [157] 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 [106] 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 [120].

Марковские параметры были расширены до модифицированного Марковского подхода в работе [110]. 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 [68] 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 [98] 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 [99] 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 [144]. 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 [90] 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 [152] 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 [121], 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 [97] 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 [135,144], о чем свидетельствуют результаты компьютерного эксперимента.

В работе [131] 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 [89] 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 [44] 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 [92] 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 [146] 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 [85] 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 [88], 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 [85], 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 [130] 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 [81] изложен метод стегоанализа изображений в градациях сероко 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 [39] 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 [60] 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 [61] 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 [62], 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 [100] 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 [56, 82, 94]. Цифровые изображения, стегоконтейнеры, а также СГВ, анализируются в доменах дискретного косинусного преобразования, дискретного преобразования Фурье и дискретного вейвлет-преобразования.

В статье [109] 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 [145]. 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 [86, 117]. 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 [50, 51] 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 [113]. 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 [78] 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.

Результаты главы опубликованы в работе [5].

Глава 2. Алгоритм выявления и локализации встраиваний, выполненных методом LSB-замены, в цветных искусственных изображениях

Во второй главе диссертационного исследования представлен алгоритм определения в цветных искусственных изображениях наличия и расположения областей встраивания, выполненных методом LSB-замены, на основе анализа нулевого битового слоя. Алгоритм основан на том факте, что в нулевом слое областей равномерной и градиентной заливки исходного изображения-контейнера наблюдаются повторяющиеся, т.е. неуникальные последовательности нулевых и единичных битов, тогда как встраиваемое сообщение изменяет характер последовательности нулевых и единичных битов нулевого слоя, инвертируя их в уникальные, т.е. неповторяющиеся последовательности в области встраивания.

2.1 Введение в проблематику

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.

Поскольку встраивание может быть произведено в любую компоненту, разрабатываемый метод стегоанализа должен равно корректно работать с любой из компонент, поэтапно подвергая анализу красную, зеленую и синюю компоненты.

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 с решением задачи о наибольшем пустом прямоугольнике.

2.2 Постановка задачи анализа нулевого слоя и метод её решения

Чтобы построить алгоритм определения и автоматической локализации 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 или градиентной заливки изображения стегоконтейнера от 10 до 40%.

Необходимо решить задачу по выявлению подменённых битов в условиях, когда стегоконтейнер имеет низкое наполнение, при котором заменены меньше, чем 40% битов нулевого битового слоя. Цель – выявить присутствие области встраивания, ее расположение (локализацию) и размеры автоматически

Представим нулевой слой в виде матрицы, состоящей из 1 и 0. Пример изображения без встраивания, пример СГВ, а также пример этого же изображения

со встраиванием и нулевые слои данного изображения без СГВ и изображения с СГВ, выполненных посредством заменены 25% битов, представлены на Рисунках 2.1 а-д).

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

1. В искусственных изображениях с градиентной заливкой карта битов нулевого слоя представляет собой множество повторяющихся комбинаций единичных и нулевых битов, что представлено на рисунке 2.2 а)

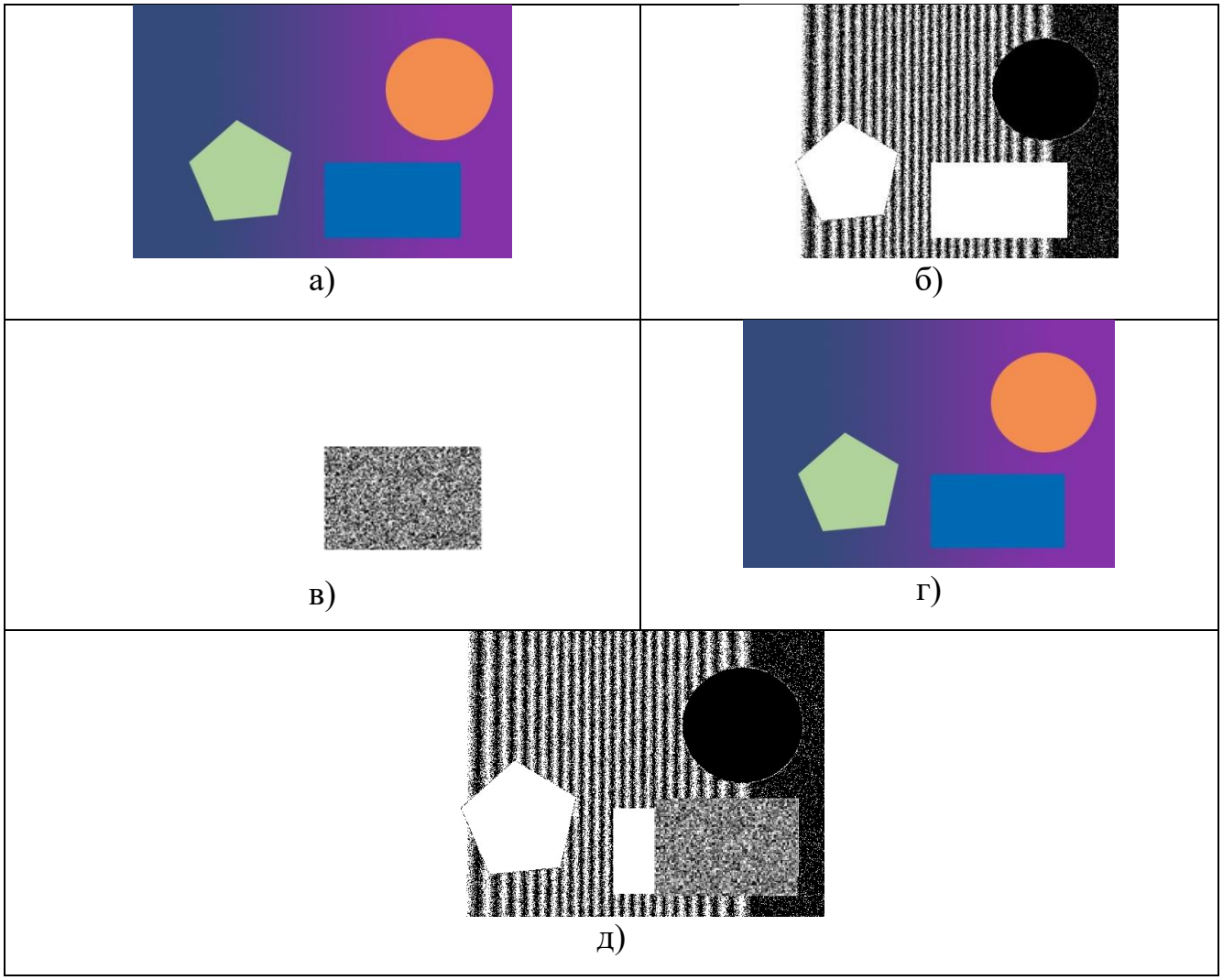
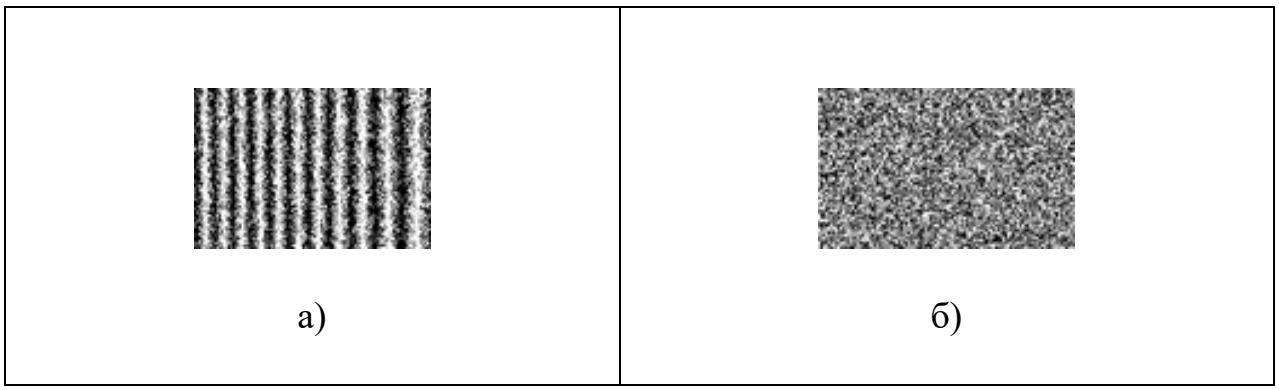


Рисунок 2.1 – Сопоставление нулевых слоев изображения с градиентной заливкой: а) первоначальное изображение, б) нулевой слой первоначального изображения, в) карта встраиваемых пикселей, г) изображение с СГВ, д) нулевой слой изображения с СГВ

2. Очевидно, что LSB замена нарушает установившуюся последовательность комбинаций пикселей, формируя тем самым множество неповторяющихся (т.е. уникальных) комбинаций пикселей, что представлено на рисунке 2.2 б).

3. Анализируя нулевой слой, присутствие СГВ, а также его расположение и размер, можно выявить визуально путем сравнения комбинаций последовательностей и выявление той области, в которой комбинации пикселей (последовательности) преимущественно уникальны.



а) б)

Рисунок 2.2 – Комбинации последовательностей на карте битов нулевого слоя $map(x, y)$ отдельных областей изображения, приведенного на Рисунке 1: а) преимущественно повторяющиеся комбинации последовательностей в области с градиентной заливкой, не имеющей встраивание, б) преимущественно уникальные комбинации последовательностей в области, имеющей встраивание

Таким образом, чтобы решить задачу автоматической локализации области встраивания, необходимо создать алгоритм, который бы позволял путем анализа комбинаций последовательностей карты битов нулевого слоя выявить уникальные комбинации нулевых битов пикселей изображения и установить область их преимущественного сосредоточения.

2.3 Алгоритм обнаружения и локализации области встраивания

Алгоритм обнаружения и локализации области встраивания работает с окнами установленной размерности и состоит из трех этапов. На первом этапе необходимо определить принадлежность каждого пикселя изображения к уникальной (неповторяющейся) или неуникальной (повторяющейся) комбинации битов нулевого слоя. На втором этапе необходимо устранить возможные шумы. На третьем этапе необходимо выделить область с повышенной концентрацией уникальных комбинаций битов нулевого слоя.

Этап 1.

Шаг 1. В первоначальном изображении последовательно выделяются блоки размером 5×5 пикселей таким образом, чтобы исследуемый пиксель являлся центральным для этого блока. Блок 1 имеет следующие координаты: (*1*, 1) – левый верхний угол, (*5*, 5) – правый нижний угол. Блок 2 имеет координаты: (2, 1) – левый верхний угол, (*6*, 5) – правый нижний угол. И так далее. Последний блок, блок N, имеет координаты: (n-4, m-4) – левый верхний угол, (n, m) – правый нижний угол.

Для каждого i-го блока последовательность битов S_i записывается в виде двоичного кода и заносится в структуру, где ключом является последовательность S_i i-го блока, а значением – координаты центрального пикселя исследуемого i-го блока.

На рисунке 2.3 представлен пример фрагмента карты пикселей и выделенных в нем блоков указанной размерностью.

Для каждого из выделенных блоков – блоков 2.3б) – 2.3д) –бинарная запись о содержащейся комбинации последовательностей S_i представлена в таблице 2.1.

Шаг 2. По каждому i -му блоку (где $i = (1; n)$ производится последовательное сравнение содержащейся в блоке комбинации последовательностей S_i с комбинациями последовательностей S_j других блоков

таким образом, что $i \neq j$, и классификация пикселя как пикселя как входящего в уникальную или неуникальную последовательность.

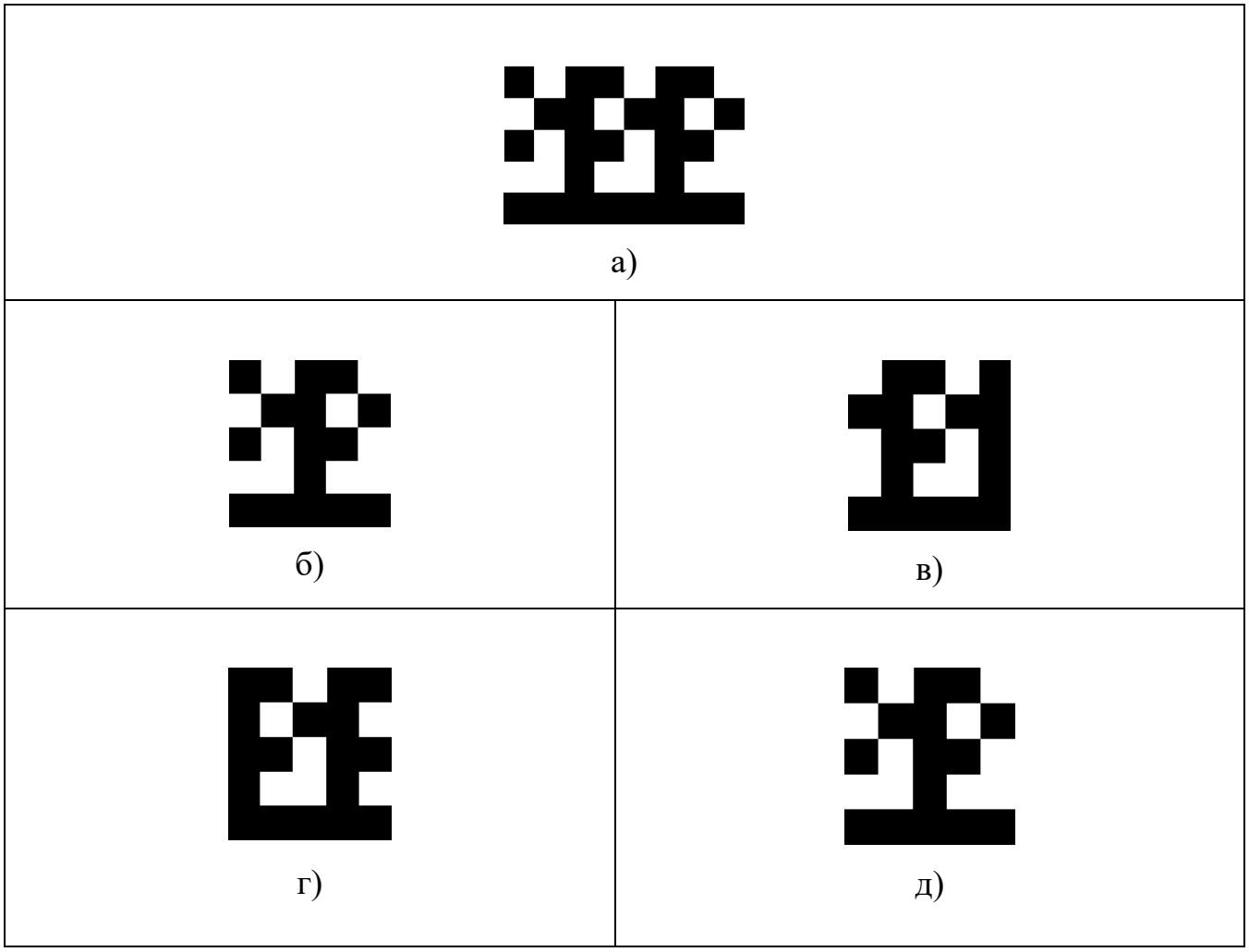


Рисунок 2.3 – Пример фрагмента карты пикселей и выделенных в нем блоков размером 5×5 пикселей: а) исходный анализируемый фрагмент карты пикселей, б-г) блоки 5×5 пикселей, выделенные в приведенном фрагменте

Алгоритм последовательного прогона исследуемого i-го блока выглядит следующим образом:

1. Производится сравнение комбинации последовательностей S_i i-го блока с комбинацией последовательностей S_1 блока 1. Если $S_i = S_1$, блок считается неуникальным, а его центральному пикселю присваивается единичное значение. Иначе – переходим к пункту 2.

Таблица 2.1 – Бинарная запись о содержащейся комбинации последовательностей в блоках, представленных на рисунке 3б) – 3д)

S_1 для блока 3б)	S_2 для блока 3в)	S_3 для блока 3г)	S_N для блока 3д)
1 0 1 1 0	0 1 1 0 1	1 1 0 1 1	1 0 1 1 0
0 1 1 0 1	1 1 0 1 1	1 0 1 1 0	0 1 1 0 1
1 0 1 1 0	0 1 1 0 1	1 1 0 1 1	1 0 1 1 0
0 0 1 0 0	0 1 0 0 1	1 0 0 1 0	0 0 1 0 0
1 1 1 1 1	1 1 1 1 1	1 1 1 1 1	1 1 1 1 1

2. Производится сравнение комбинации последовательностей S_i с комбинацией последовательностей S_j комбинацией последовательностей j -го блока таким образом, что $\mathrm{j}=1+\mathrm{k}$, где k -количество итераций, выполненных ранее для комбинации последовательностей S_i.

Если $S_i = S_j$, блок считается неуникальным, а его центральному пикселю присваивается единичное значение. Иначе – а) если $j < N$ – вновь возвращаемся к пункту 2; б) если $j = N$ – блок считается уникальным, а его центральному пикселю присваивается нулевое значение.

По итогам работы с каждым блоком заполняется еще одна хэш-таблица, где в качестве ключа используется получаемые единичные или нулевые значения, а в качестве значения по-прежнему остаются координаты центрального пикселя исследуемого блока. Таким образом, результатом классификации является матрица M_0, в которой в бинарном виде записана принадлежность пикселя:

- значение 1 – пиксель входит в повторяющуюся последовательность;
- значение 0 – пиксель входит в уникальную последовательность.

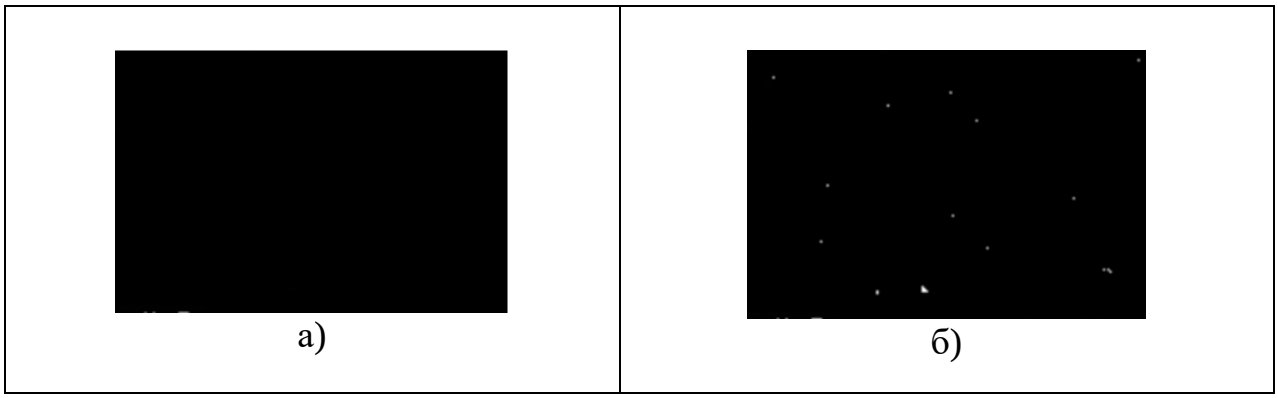
Предполагается, что существует возможность неправильной классификации пикселя. При этом подобная матрица является ключевой для локализации области

встраивания посредством решения задачи о наибольшем пустом треугольнике. Следовательно решение задачи имеет некоторые ограничения, вызванные погрешностью классификации. Снятие ограничений производится на следующем этапе.

Этап 2. Производится обработка значений матрицы M_0 фильтром с целью устранения шумов и снижения погрешности в результатах стеганографического анализа.

В целях проводимого стеганографического анализа LSB-вставок и основываясь на гипотезе обнаружения уникальных комбинаций пикселей как признака наличия в области обнаружения стеганографических вставок, выполненных методом LSB-замены, и исходя из ограничений алгоритма локализации вставок, описание которого будет представлено на шаге 4, шумом следует считать такой пиксель, который был классифицирован как центральный пиксель блока с повторяющейся последовательностью, но при этом расположенный среди пикселей, классифицированных как центральные пиксели блоков с уникальной последовательностью. И наоборот.

Примеры областей встраивания, содержащих и не содержащих шумы, приведены на рисунке 2.4. Так, на рисунке 2.4 а) представлена карта пикселей области встраивания при полном отсутствии шумов, т.е. все пиксели, принадлежащие данному участку изображения охарактеризованы как пиксели, входящие в уникальные последовательности. При этом, на рисунке 2.4 б) представлена карта пикселей области встраивания, где некоторые пиксели являются шумами, т.е. центральными пикселями блоков повторяющихся последовательностей, но при этом расположенные среди пикселей блоков с уникальной последовательностью.



а) б)

Рисунок 2.4 – Карта пикселей области встраивания: а) не содержащая шумы, б) содержащая шумы

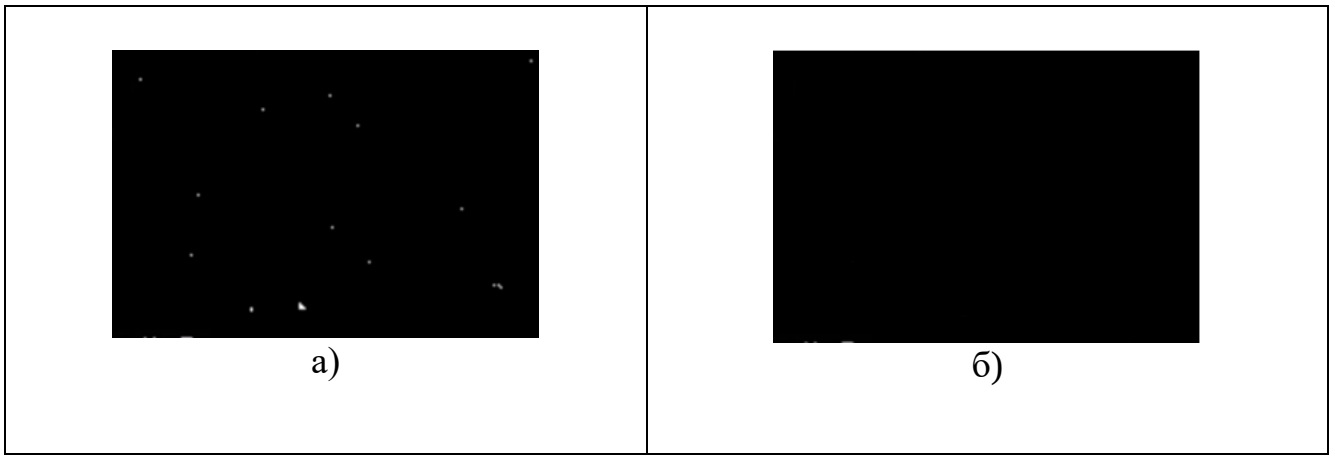
Алгоритм предварительной обработки фильтром значений матрицы значений пикселей M_0 имеет следующий вид.

Шаг 1. В матрице M_0 для каждого пикселя с единичным значением выделяются блоки способом, аналогичным выделению блоков, представленном на этапе 1. Для пикселей первых и последних двух рядов, а также первых и последних двух столбцов блоки выстраиваются частично.

Шаг 2. В каждом из выделенных блоков, производится последовательное сравнение значения исследуемого i-ого пикселя со значениями других пикселей, входящих в этот блок. Если более чем 70% всех пикселей, принадлежащих анализируемому блоку, имеют нулевые значения, исследуемый пиксель считается зашумленным и ему присваивается нулевое значение. Иначе – значение пикселя в матрице остается неизменным, единичным.

На рисунке 2.5 наглядно представлен пример карты пикселей области встраивания до обработки фильтром и после обработки.

В результате, будет сформирована новая матрица M_1, не содержащая шумов и позволяющая с максимальной точностью локализовать область встраивания, т.е. область, содержащую только нулевые значения.



а) б)

Рисунок 2.5 – Карта пикселей области встраивания: а) до обработки фильтром, б) после обработки фильтром

Этап 3. Анализ матрицы M_1 на предмет локализации области встраивания.

Пусть встраиваемое сообщение имеет размеры $X \times Y$. Тогда будем искать прямоугольник, характеризующийся координатами (x_1, y_1) – левый верхний угол, (x_2, y_2) – правый нижний угол.

Значения координат можно найти путем решения задачи о наибольшем пустом прямоугольнике. Задача о наибольшем пустом прямоугольнике – это задача о нахождении такого прямоугольника, площадь которого включает в себя данные массива, обладающими определенными непрерывающимися значениями характеристик. Впервые задача о наибольшем пустом прямоугольнике и ее решение были сформулированы в работе А. Наамад, Д. Ли и В. Шу [105] и были дополнены впоследствии в работах различных авторов [37, 40, 53, 116, 128].

В целях нашего исследования сформулируем задачу следующим образом. Множество пикселей анализируемого искусственного изображения классифицированы либо как пиксели, входящие в уникальные последовательности (в этом случае каждому из таких пикселей присваивается нулевое значение) либо как пиксели, входящие в неуникальные (повторяющиеся) последовательности (в этом случае каждому из таких пикселей присваивается единичное значение). Необходимо извлечь такие пиксели, которые имеют нулевое значение и формируют наибольший непрерывающийся кластер, расположенный в границах

пикселей с единичным значением, т.е. определить наибольший прямоугольник, содержащий только нулевые значения пикселей. Таким образом, область встраивания будет определена в виде прямоугольника с координатами (x_1, y_1) по левому верхнему углу и (x_2, y_2) по правому нижнему углу, все пиксели которого принадлежат только уникальным последовательностям, т.е. объединяющего пиксели, в которые было предположительно осуществлено встраивание.

Алгоритм решения задачи о наибольшем пустом прямоугольнике осуществляется следующий.

Шаг.1 Преобразование исходной матрицы M_1 в рабочую матрицу M_2 с целью определения разрывов.

Преобразование осуществляется по следующим правилам:

- каждому элементу исходной матрицы M_1, имеющему единичное значение, присваивается нулевое значение вне зависимости от того, наблюдаются ли другие элементы с единичными значениями в данной строке, столбце или по диагонали;

- каждый элемент исходной матрицы M_1, имеющий нулевое значение, анализируется по столбцу с присвоением ему значения от 1 до n следующим образом. Значение текущего i-го элемента $A_i^{M_1}$ сравнивается со значением предыдущего элемента исходной матрицы, $A_{i-1}^{M_1}$, расположенного в том же столбце. При этом элементу присваивается значение, равное его порядковому номеру в непрерывной цепочке нулевых значений по столбцу.

В общем виде алгоритм преобразования исходной матрицы M_1, и формирования рабочей матрицы M_2 следующий:

— Если $A_i^{M_1} = 1$, то $A_i^{M_2} = 0$.

— Иначе: если $A_i^{M_1} = A_{i-1}^{M_1}$, то $A_i^{M_2} = A_{i-1}^{M2} + 1$, иначе $A_i^{M_2} = 1$,

где $A_i^{M_1}$ – анализируемый текущий элемент исходной матрицы M_1;

$A_{i-1}^{M_1}$ – предыдущий по столбцу элемент исходной матрицы M_1;

$A_i^{M_2}$ – элемент рабочей матрицы M_2, с координатами, соответствующими анализируемому элементу $A_i^{M_1}$;

$A_{i-1}^{M_2}$ – элемент рабочей матрицы M_2, с координатами, соответствующими анализируемому элементу $A_{i-1}^{M_1}$.

Пример преобразования исходной матрицы M_1 в рабочую матрицу M_2 представлен в таблице 2.2.

Шаг 2. Производится вычисление всех прямоугольников, ограниченных элементами матрицы M_2, содержащими нулевые значения.

Таблица 2.2 – Пример преобразования исходной матрицы M_1 в рабочую матрицу M_2

Исходная матрица M_1	Рабочая матрица M_2
0 0 0 1 0 0	1 1 1 0 1 1
0 0 1 0 0 1	2 2 0 1 2 0
0 1 0 0 0 0	3 0 1 2 3 1
0 0 0 0 0 0	4 1 2 3 4 2
0 0 0 0 0 1	5 2 3 4 5 0
1 0 0 1 0 0	0 3 4 0 6 1

Локализация прямоугольника осуществляется на основании непрерывности элементов с ненулевыми значениями. Вычисление осуществляется в порядке от нижнего ряда к верхнему. Ряд или столбец, содержащий элементы с нулевым значением, определяют границы искомого прямоугольника и не принадлежат ему.

Так для примера, приведенного в таблице 2.2, будут выделены прямоугольники со следующими площадями, измеряемыми в пикселях:

$$\mathrm{H}[6] = \ 0\ 3\ 4\ 0\ 6\ 1\ \rightarrow 6\ (3 * 2)$$

$$\mathrm{H}[5] = \ 5\ 2\ 3\ 4\ 5\ 0\ \rightarrow 10\ (2 * 5)$$

$$H[4] = 4\ 1\ 2\ 3\ 4\ 2 \rightarrow 8\ (2 * 4)$$
$$H[3] = 3\ 0\ 1\ 2\ 3\ 1 \rightarrow 4\ (2 * 2)$$
$$H[2] = 0\ 3\ 4\ 0\ 6\ 1 \rightarrow 4\ (2 * 2)$$
$$H[1] = 1\ 1\ 1\ 0\ 1\ 1 \rightarrow 3\ (1 * 3)$$

Шаг 3. Установление прямоугольной области, имеющей наибольшую площадь.

На данном этапе сравниваются площади найденных на предыдущем шаге прямоугольников и выбирается тот прямоугольник, площадь которого будет наибольшей.

Так для примера, приведенного в таблице 2, прямоугольник, основание которого опирается на ряд $H[5]$, обладает наибольшей площадью – площадью в 10 пикселей.

Следовательно, наибольший выделенный прямоугольник в данном примере имеет следующие координаты – (1, 4) – левый верхний угол, (5, 5) – правый нижний угол.

Шаг 4. Определение наличия встраивания и локализации области встраивания посредством установления прямоугольника, отвечающего заданным параметрам.

В то же время, очевидно, что, поскольку области, не содержащие встраивание, имеют как повторяющиеся, так и уникальные последовательности, то в чистом изображении так же будут выделены прямоугольные области, содержащие пиксели, принадлежащим уникальным последовательностям. Однако, площадь такой области будет сравнительно мала. Проведенные нами эмпирические исследования показали, что площадь области сосредоточения пикселей, входящих в уникальную последовательности, в чистых изображениях не превышает 1% от общей площади анализируемого изображения.

Таким образом, выделенная прямоугольная область считается областью встраивания, если выполняется следующее условие:

$$S_1 \geq 0.01 \times S_0 \tag{5}$$

где S_1 – площадь выделенной прямоугольной области, пиксели;

S_0 – общая площадь анализируемого изображения, пиксели.

2.4 Компьютерный эксперимент и результаты

Апробация алгоритма осуществлена на 100 цветных искусственных изображениях с градиентной заливкой. Поставленные задачи стегоанализа включают определение наличия встраивания, а также локализацию области встраивания.

Встраивание осуществлялось в виде потока бит, которые представляют собой текстовую строку, область встраивания прямоугольная. Для встраивания были поочередно использованы красная, зеленая и синяя компоненты – для каждого изображения. Уровень стегонагрузки составлял 25% и 10% – для каждого изображения и каждой компоненты.

Также, для проверки корректной работы разработанного алгоритма стегоанализа цветных искусственных изображений с градиентной заливкой, каждое из ста изображений подвергалось исследованию при полном отсутствии встраивания (чистые изображения).

Таким образом, в ходе компьютерного эксперимента было произведено 7 прогонов по каждому из исследуемых изображений, а генеральная совокупность составила 700 единиц – 600 стего изображений и 100 чистых изображений.

В 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.

В таблицах 2.3 и 2.4 приведены полученные результаты работы алгоритма стегоанализа метода LSB-замены в цветных искусственных изображениях с градиентной заливкой – точность классификации изображений, т.е. обнаружения встраивания (таблица 2.3) и точность локализации области встраивания (таблица 2.4).

Таблица 2.3 – Результаты работы алгоритма стегоанализа метода LSB-замены цветных искусственных изображений с градиентной заливкой (точность классификации изображений)

<table>
<tr><td rowspan="2">Анализируемая компонента</td><td colspan="3">Уровень стегонагрузки, %</td></tr>
<tr><td>25</td><td>10</td><td>0</td></tr>
<tr><td>Красная компонента</td><td>TP=99%
FN=1%</td><td>TP=98%
FN=2%</td><td rowspan="5">TN=100%
FP=0%</td></tr>
<tr><td>Зеленая компонента</td><td>TP=99%
FN=1%</td><td>TP=98%
FN=2%</td></tr>
<tr><td>Синяя компонента</td><td>TP=99%
FN=1%</td><td>TP=98%
FN=2%</td></tr>
<tr><td>В среднем по компонентам</td><td>TP=99%
FN=1%</td><td>TP=98%
FN=2%</td></tr>
<tr><td>В среднем по коллекции изображений</td><td colspan="2">TP=98,5%
FN=1,5%</td></tr>
</table>

Как представлено в таблице 2.3, средняя эффективность алгоритма стегоанализа метода LSB-замены цветных искусственных изображений с градиентной заливкой составляет 98,5%, что означает, что LSB-вставки были выявлены в 591 случаях из 600.

Таблица 2.4 – Результаты работы алгоритма стегоанализа метода LSB-замены цветных искусственных изображений с градиентной заливкой (точность локализации области встраивания)

Анализируемая компонента	Уровень стегонагрузки, %	
	25	10
Красная компонента	98,27%	96,87%
Зеленая компонента	98,27%	96,87%
Синяя компонента	98,27%	96,87%
В среднем по компонентам	98,27%	96,87%
В среднем по коллекции изображений	97,53%	

При этом, в случае, когда было заменено 25% битов, эффективность алгоритма составила 99% по каждой компоненте, т.е. при прогоне 100 стегоконтейнеров с поочередным встраиванием в одну из компонент (в общем количестве 300 стегоконтейнеров), алгоритм обнаружил наличие встроенного сообщения в 99 стегоконтейнерах в каждой из исследуемых компонент (в общем количестве – 297 единицы) и только 1 контейнер (в общем количестве – 3 единицы) был ошибочно определен как чистый (т.е. был возвращен ложно-негативный результат).

Однако, в случае, когда было заменено 10% битов, эффективность алгоритма составила 98% по каждой компоненте, т.е. при прогоне 100 стегоконтейнеров с поочередным встраиванием в одну из компонент (в общем количестве 300 стегоконтейнеров), алгоритм обнаружил наличие встроенного сообщения в 98 стегоконтейнерах в каждой из исследуемых компонент (в общем количестве – 294 единицы), а 2 контейнера (в общем количестве – 6 единиц) были ошибочно определены как чистые (т.е. по ним был возвращен ложно-негативный результат).

Данные, представленные в таблице 2.4, свидетельствуют также о высокой эффективности разработанного алгоритма в отношении определения областей встраивания.

Так, в среднем по выборке область встраивания, выделенная алгоритмом, составила 97,53%, т.е. меньше действительной на 2,47%.

При этом, в случае, когда было заменено 25% битов, эффективность локализации составила 98,27 % по каждой компоненте, т.е., область встраивания, выделенная алгоритмом, всего на 1,73% меньше фактической области встраивания. В случае, когда было заменено 10% битов, эффективность локализации составила 96,87 % по каждой компоненте, т.е., область встраивания, выделенная алгоритмом, на 3,13% меньше фактической области встраивания.

Т.е. точность локализации при 10% уровне встраивания ниже соответствующего показателя при работе с 25% уровнем встраивания чуть более чем на 1,42% (на 1,4 п.п. в абсолютном выражении).

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. Компьютерный эксперимент показал, что при LSB-замене битов нулевого слоя на 10 – 25% средняя эффективность обнаружения СГВ составляет 98,5%, что превосходит результаты статистических методов при высоком заполнении стегоконтейнера [79, 124] (86% и 90% соответственно).

Помимо этого, разработанный алгоритм может не только устанавливать факт наличия СГВ, но и позволяет определять расположение СГВ и ее размер (а средняя точность локализации области встраивания составляет 97,53%), что можно выделить в качестве главного преимущества разработанного алгоритма.

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 [36] описывается, как алгоритм SD-ROM выявляет с эффективностью 95% поврежденные пиксели, а ложных срабатываний при этом не больше 36%.

Проведенный компьютерный эксперимент, направленный на оценку эффективности разработанного алгоритма, позволил сделать следующие выводы:

1) алгоритм не обнаруживает изменений по точности классификации изображения и локализации области встраивания в зависимости от компоненты, в которую было осуществлено встраивание;

2) алгоритм обнаруживает небольшое снижение его эффективности при работе с 10% уровнем стегонагрузки при сравнении с ситуацией, когда объем заполнения стегоконтейнера составляет 25%.

3) алгоритм обнаруживает незначительное прямо пропорциональное изменение по точности локализации области встраивания в зависимости от размеров маски встраивания, т.е. чем больше площадь маски встраивания, тем больший ее процент выделен и локализован алгоритмом.

Снижение эффективности обнаружения стеговставки по мере уменьшения уровня стегонагрузки, в целом, является хорошо известным явлением, обусловленным снижением количества подмененных битов, в результате чего алгоритм может не иметь достаточно веских оснований для классификации таких областей как стего. При этом в отношении разработанного алгоритма можно утверждать, что снижение эффективности обнаружения встраивания всего на 1 процентный пункт при снижении стегонагрузки на 15 процентных пункта является незначительным.

Анализ точности локализации области встраивания позволил сделать вывод, что недостижение 100%-го охвата области встраивания обусловлено смещением пикселей. При этом, наибольшая потеря точности происходит если обнаруженная область встраивания расположена в крайних областях изображения.

Снижение точности локализации стеговставки по мере уменьшения уровня стегонагрузки обусловлено тем, что чем меньше площадь встраивания, тем больший удельный вес занимает каждый пиксель. Следовательно, его смещение дает некоторую потерю точности.

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 на 25% составляет 99%, а эффективность обнаружения СГВ с заполнением стегоконтейнера всего в 10% составляет 98%, что превышает эффективность статистических методов, применяемых для высоких значений заполнения стегоконтейнера.

2. Применение алгоритма задачи о наибольшем пустом прямоугольнике даёт возможность локализовать область встраивания в автоматическом режиме. При этом для искусственных изображений границы области встраивания могут быть определены с погрешностью, не превышающей 1,73%, для стегоконтейнера в 25%, и 3,13%, для стегоконтейнера в 10%, что означает, что алгоритм способен выявить только, соответственно, 98,27%, и 96,87% пикселей с подмененным младшим битом. Аналогичные алгоритмы определения положения зашумленных пикселей допускают ошибку до 36% [96].

3. Эффективность алгоритма с точки зрения классификации и локализации области встраивания не зависит от компоненты, в которую было произведено встраивания.

Результаты данной главы опубликованы в работах [8, 16, 17, 133].

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ [12].

Глава 3. Алгоритм выявления и локализации встраиваний, выполненных методом LSB-замены, в цветных фотографических изображениях

В третьей главе диссертационного исследования представлен алгоритм определения наличия, размеров и положения областей встраивания, выполненных методом LSB-замены, в цветных фотографических изображениях на основе сравнительного анализа нулевого и первого битового слоев. Алгоритм основан на подтверждаемой гипотезе о том, что закономерности, присутствующие в нулевом слое исходного изображения-контейнера, преимущественно повторяются в первом слое этого изображения.

Для поиска пикселей с замененным нулевым битом анализируется нулевой и первый слои каждой из компонент на предмет наличия межслойного попарного сходства пикселей и их соседей, а также межслойного изменения в моделях доминирования белых пикселей.

Для локализации области встраивания используется гипотеза о сущности встраивания как случайном наборе пикселей с единичными и нулевыми значениями и анализируется нулевой слой выделенной области предполагаемого встраивания на предмет удовлетворения условию равного (или близко к равному) соотношения единиц и нулей.

3.1 Введение в проблематику

В предыдущей главе, было показано, что в нулевом слое цветных искусственных изображении существуют четко выраженные закономерности комбинаций пикселей (их уникальность или не уникальность), поэтому анализ только нулевого слоя является необходимым и достаточным для того, чтобы выявить те пиксели, в которых осуществлена замена младших битов. Однако для эффективного определения стеганографических вставок в цветные фотографические изображения информации только о нулевом слое недостаточно.

Это связано с тем, что в цветных фотографических изображениях пиксели не формируют однозначно определяемые уникальные комбинации в нулевом слое, равно как и в других слоях. Наоборот, в таких изображениях наблюдается высокая вариативность комбинаций пикселей, пример которой приведен на рисунках 3.1 а-в).

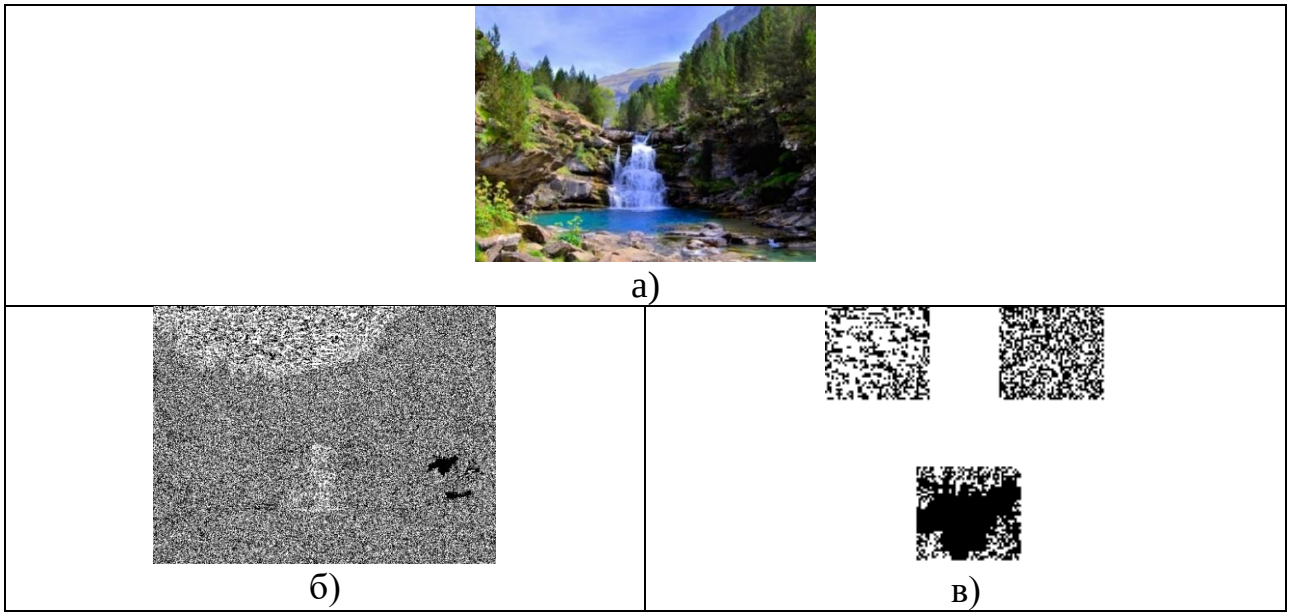


Рисунок 3.1 – Пример вариативности последовательности пикселей нулевого слоя цветного фотографического изображения: а) чистое анализируемое цветное фотографическое изображение, б) нулевой слой анализируемого изображения, в) примеры комбинаций пикселей, встречающихся в нулевом слое чистого анализируемого изображения

При этом, нами установлено, что между комбинациями нулевого и первого слоев существуют определенная инерционность, т.е. схожесть. Следовательно, для повышения эффективности стеганографического анализа необходимо учитывать структуру исходного изображения-контейнера, которая хранится в более высоких битовых слоях, как было указано в первой главе, т.е. проводить их сравнение на основе алгоритмов анализа и принятия решений.

Таким образом в данной главе предлагается алгоритм выявления вставок, выполненных методом замены наименее значащего бита, с помощью метода

анализа иерархий нулевого и первого слоев, и, таким образом, будет учитываться структура нескольких битовых слоев.

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

Сформулируем три предположения:

1. Доподлинно неизвестно есть ли СГВ.

2. Информация о возможном расположении встраиваемых битов отсутствует.

3. Уровень заполнения стегоконтейнера при наличии встраивания не менее 10%.

Следовательно, задачу стегоанализа можно сформулировать следующим образом: необходимо установить, присутствует ли на изображении СГВ, и, если да, то, определить фактическую область встраивания, локализовав, тем самым СГВ.

Для решения данной задачи выдвинем предположение о плавном послойном изменении закономерностей. Таким образом, при анализе ближайших слоев возможно использование одних и тех же закономерностей.

Следовательно, решение поставленной задачи может быть найдено посредством сравнительного анализа нулевого и первого слоев.

Сформулируем четыре этапа стеганографического анализа фотографических цветных изображений, направленного против метода LSB-замены:

1. Установление участков сохранения структуры изображения, т.е. установление сверхсильных комбинаций последовательности пикселей, переносимых между слоями, и разделение блоков изображения на условно чистые (т.е. те, которые однозначно не содержат встраивание) и условные стего (т.е., возможно, содержащие встраивание).

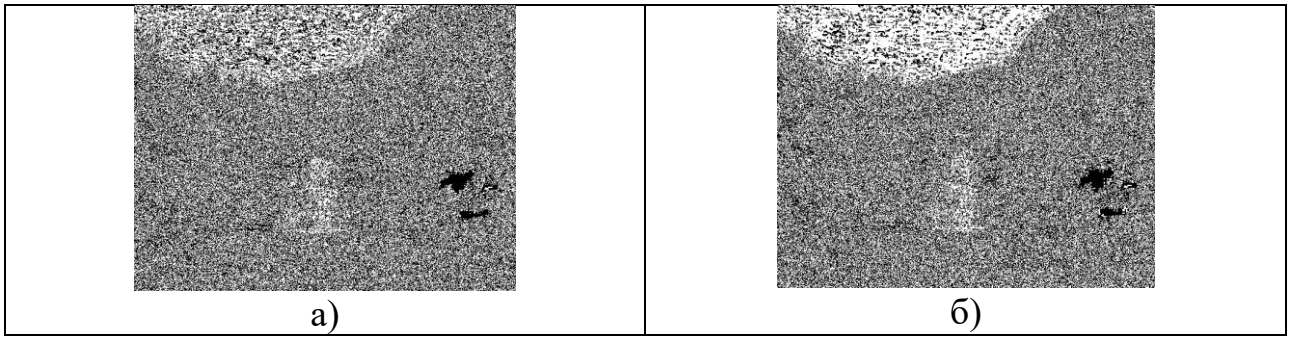
2. Анализ условно чистых блоков рекурсивным фильтром с целью их дополнительной верификации.

3. Выявление максимально широкой области возможного встраивания и окончательная верификация изображения на предмет встраивания.

4. Локализация области встраивания посредством нахождения участков встраивания в установленной области.

3.2 Анализ межслойного сохранения структуры изображения

Так, сравнивая нулевой и первый слой одного и того же изображения, визуально заметно сохранение особенностей структуры изображения на некоторых его участках – пример нулевого и первого слоев изображения представлен на рисунке 3.2 а-б).



а) б)

Рисунок 3.2 – Пример сохранения структуры между слоями изображения: а) нулевой слой изображения, б) первый слой изображения

Этап 1. Анализ сохранения структуры изображения.

Для анализа сохранения структуры изображения между его нулевым и первым слоями введем три сигнатуры:

Сигнатура K_1 – характеризует идентичность или различие между попарными значениями анализируемого бита и его соседа справа. Данный критерий позволяет определить сохранение определенной горизонтальной структуры изображения между слоями или ее межслойного изменения.

Сигнатура K_2 – характеризует идентичность или различие между попарными значениями анализируемого бита и его соседа снизу. Данный критерий позволяет определить сохранение определенной вертикальной структуры изображения между слоями или ее межслойного изменения.

Сигнатура K_3 – характеризует идентичность или различие между попарными значениями анализируемого бита и его соседа по диагонали справа. Данный критерий позволяет определить сохранение определенной диагональной структуры изображения между слоями или ее межслойного изменения.

В качестве критерия классификации блока как чистого или стего используется минимально допустимый удельный вес попарных совпадений ω, определяемый для всего изображения как граница разграничения чистых блоков и блоков, в которых возможно наличие встраивания.

Для достижения максимальной репрезентативности, анализ послойного сохранения структуры изображения проводится поблочно, т.е. последовательно анализируются отдельные блоки изображения размерностью 10x10. Указанная размерность эмпирически найдена как оптимальная, т.к., с одной стороны, является достаточно большой для того, чтобы позволить сделать корректные выводы о межслойном сохранении или изменении структуры изображения, а с другой стороны, является частью изображения, достаточно малой для того, чтобы исключить возможность анализа областей, структуры которых различны сами по себе, что может быть обусловлено особенностью анализируемого.

Таким образом алгоритм анализа межслойного сохранения структуры изображения имеет следующий вид:

Шаг 1. Разделим нулевой слой исследуемого изображения на блоки с окном 10. Полученную последовательность пикселей каждого блока запишем в виде бинарной матрицы $B_{ij}^{(0)}$. Аналогичным образом осуществим разбивку первого слоя изображения, с формированием по каждому блоку бинарной матрицы $B_{ij}^{(1)}$. Установим координаты каждого из пикселей для каждого блока.

Шаг 2. Осуществим строгое закреплений областей сравнения. Т.е. первый блок нулевого слоя сравнивается строго с первым блоком первого слоя и так далее. Иные вариации областей сравнения являются недопустимыми.

Шаг 3. Произведем анализ пикселей попарных блоков по сигнатурам $K_1 - K_3$, начиная с верхнего левого пикселя с координатами (0;0) и заканчивая

предпоследним пикселем предпоследнего ряда предпоследнего столбца с координатами (8;8). Анализ производится на предмет удовлетворения сигнатур нулевого и первого слоев следующему условию:

$$K_1^{(ij)^0} = K_1^{(ij)^1},\ K_2^{(ij)^0} = K_2^{(ij)^1},\ K_3^{(ij)^0} = K_3^{(ij)^1}, \tag{6}$$

где $K_1^{(ij)^0}$ – сигнатура K_1 по пикселю нулевого слоя с координатами (i;j);

$K_1^{(ij)^1}$ – сигнатура K_1 по пикселю первого слоя с координатами (i;j);

$K_2^{(ij)^0}$ – сигнатура K_2 по пикселю нулевого слоя с координатами (i;j);

$K_2^{(ij)^1}$ – сигнатура K_2 по пикселю первого слоя с координатами (i;j);

$K_3^{(ij)^0}$ – сигнатура K_3 по пикселю нулевого слоя с координатами (i;j);

$K_3^{(ij)^0}$ – сигнатура K_3 по пикселю первого слоя с координатами (i;j).

Для каждого блока вводим внутренний счетчик k_i так, что ведется подсчет попарных совпадений по каждому исследуемому пикселю анализируемого блока. Так, для каждого выполнения условия (6) получаем увеличение значения счетчика повторений на единицу:

$$k_i = k_{i-1} + 1 \tag{7}$$

где k_{i-1} – предыдущее значение счетчика попарных совпадений.

Таким образом в результате обработки каждого пикселя счетчик k_i может увеличиться на три единицы максимум.

Шаг 4. Рассчитаем средний удельный вес попарных совпадений $\overline{\partial_i}$ для каждого i-го блока анализируемого изображения:

$$\overline{\partial_i} = \frac{k_i}{3 \times 81} \tag{8}$$

Шаг 5. Вычисляем минимально допустимый удельный вес попарных совпадений ω:

$$\omega = \overline{X} + S \tag{9}$$

где $\overline{X}$ – среднее арифметическое значение по выборке;

S – среднеквадратичное отклонение значений по выборке.

При этом критерием включения блока в выборку является удовлетворение следующего условия:

$$\overline{\partial_i} \leq 0.2 \tag{10}$$

Обоснование условия включения блока в выборку следующее. Исследование множества изображений со встраиванием на предмет среднего удельного веса попарных совпадений $\overline{\partial_i}$ в содержащихся в них чистых блоков и блоков со встраиванием показало, что 97% блоков со встраиванием имеют средний удельный вес попарных совпадений, удовлетворяющих указанному в выражению (10) значению. Графически, пример массива удельных весов попарных совпадений в блоках изображения представлен на рисунке 3.3 (красным цветом обозначены маркеры блоков со встраиванием, зеленым цветом – маркеры блоков без встраивания).

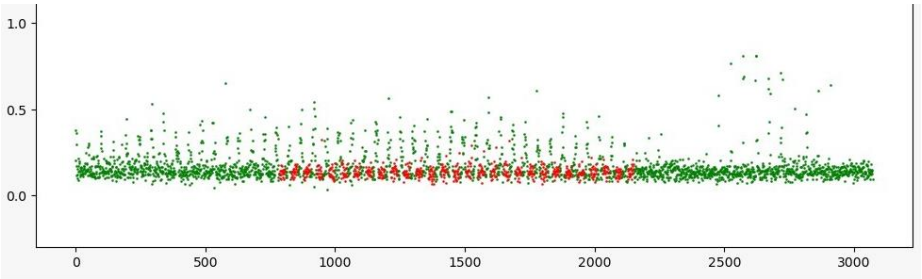


Рисунок 3.3 – Удельный вес попарного сходства пикселей в блоках со встраиванием (красный маркер) и блоков без встраивания (зеленый маркер) для изображения, представленного на рисунке 1

Шаг 6. Прогоняем значения каждого из блоков по обозначенному выше критерию:

- если $\overline{\partial_i} > \omega$, то блок считается условно чистым и имеет значение 1;
- если $\overline{\partial_i} \leq \omega$, то считается, что блок может содержать встраивание (условное стего) и ему присваивается значение 0.

В результате получаем карту блоков изображения, представленную на рисунке 3.4. Для наглядности, обозначим условно чистые блоки как блоки с зеленой заливкой, а блоки, являющимися условными стего, как блоки с бежевой заливкой.

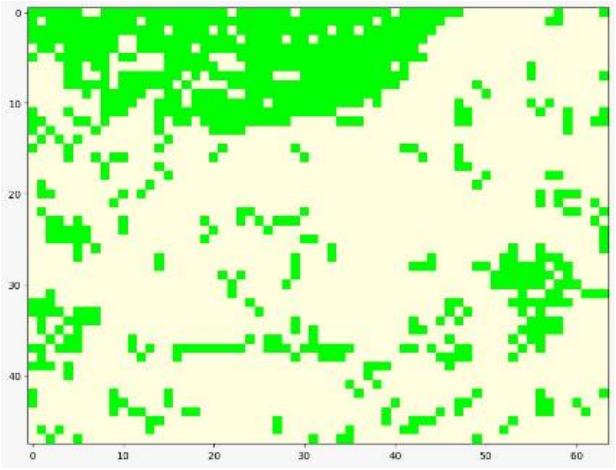


Рисунок 3.4 – Карта блоков изображения

Этап 2. Анализ условно чистых блоков рекурсивным фильтром с целью их дополнительной верификации.

Ранее нами отмечено, что часть блоков, содержащих встраивание, может иметь высокую сохраняемость структуры изображения, в результате чего алгоритм первого этапа может классифицировать данные блоки как условно чистые. Подобная ситуация представлена на рисунке 3.4, в котором представлена карта блоков изображения со встраиванием, объем которого составляет 25%, однако даже невооруженным глазом можно заметить, что на рисунке 3.4 нет ни одной непрерывной области, размеры которой были бы сопоставимы с реальными размерами встраивания.

Таким образом, можно сделать вывод, что блоки, содержащие встраивание, но обнаруживающие высокую сохраняемость структуры изображения, являются ложно негативными, т.е. шумами, препятствующими правильной классификации изображения как стего. При этом, очевидно, что подобные ложно-негативные,

зашумленные, блоки, как правило, имеют случайный, хаотичный характер, тогда как истинно устойчивые сохранения структуры имеют тенденцию к кластеризации.

Так, можно обнаружить, что на рисунке 3.4 блоки, классифицированные как условно чистые, либо формируют четко-различимые кластеры (рисунок 3.5 а), а, следовательно, являются устойчивыми доказательствами сохранения структуры изображения в соответствующих областях, что свидетельствует об отсутствии встраивания, либо существуют обособленно, а потому могут являться ложно-негативными шумами (рисунок 3.5 б).

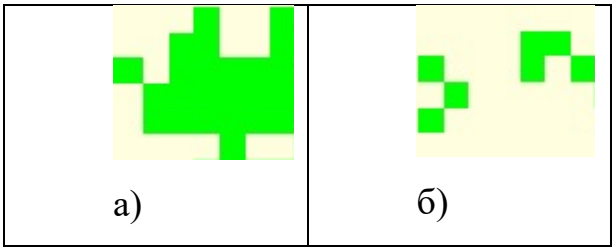


Рисунок 3.5 – Пример блоков первого типа (а) и второго типа (б)

Следовательно, для получения корректных результатов стегоанализа против метода LSB-замены является необходимым применение фильтра, позволяющего избавиться от зашумленных данных и, тем самым, исключить наличие ложно-негативных блоков среди блоков, классифицированных ранее как условно-чистые.

С этой целью нами разработан рекурсивный фильтр, позволяющий осуществить проверку условно-чистых блоков на предмет вхождения их в кластеры и, тем самым, верифицировать их чистоту. Для решения поставленной задачи необходимым и достаточным условием является вхождения исследуемого блока в кластер размерностью не менее 2x2.

Алгоритм рекурсивного фильтра имеет следующий вид:

Шаг 1. Составляем 3 списка:

- список A – список всех блоков, определённых как условно-чистые, т.е. не содержащие встраивание;

- список Б – список всех блоков, определённых как условно-стего, т.е. потенциально содержащие встраивание;
- список В – список блоков, которые следует проанализировать на предмет их вхождения в кластер с заданными параметрами, изначально дублирует список А, и уменьшается по мере работы фильтра.

Шаг 2. Из списка В случайным образом выбирается i-ый блок для анализа.

Шаг 3. Проводится анализ 8 близлежащих соседей выбранного i-го блока:

А) Если ни один из соседствующих блоков не является чистым, значение анализируемого блока инвертируется как блок, потенциально содержащий встраивание, и заносится в список Б, а сам блок исключается из списков В и А.

Б) Если как минимум три соседствующих с ним блока являются чистыми и при этом эти три блока являются соседями между собой, то есть собирается квадрат 2x2 из чистых блоков, то анализируемый блок и все из соседствующих с ним чистых блоков отмечаются как новосформированный кластер. При этом поочередно для каждого из соседствующих блоков запускается рекурсивная функция с аналогичным алгоритмом, а сам блок, являющийся точкой входа, отмечается как блок, обработанный фильтром, и исключается из списка В с целью недопущения его повторного анализа при запуске рекурсивной функции.

Кластер помечается как кластер, содержащий группу блоков с сильной степенью схожести и может быть расширен по мере обработки соседствующих блоков рекурсивной функцией. При этом формирование кластера считается завершенным, если следующий анализируемый блок и его соседи не формируют квадрат 2x2. В этом случае, последний анализируемый блок исключается из списка В, но остается в списке А.

В) Если хотя бы один из соседствующих блоков также является чистым блоком, но при этом условие для формирования кластера не выполняется, рекурсивная функция запускается для найденного чистого соседствующего блока, а сам блок, являющийся точкой входа, отмечается как блок, обработанный фильтром и исключается из списка В с целью недопущения его повторного анализа

при запуске рекурсивной функции. При этом, если рекурсия не обнаруживает ни одного случая выполнения условия кластеризации, значения всей цепочки блоков инвертируются в блоки, потенциально содержащие встраивание. Данные блоки исключаются из списка А и В и включаются в список Б. После чего алгоритм возвращается к шагу 2.

Работа алгоритма завершается при условии отсутствия новой точки входа, т.е. в случае, когда все блоки из списка В обработаны.

На рисунке 3.6 представлена карта блоков изображения после обработки рекурсивным фильтром.

Этап 3. Выявление максимально широкой области возможного встраивания и окончательная верификация изображения на предмет встраивания.

В главе 2 для локализации области встраивания нами был успешно применен метод решения задачи о наибольшем пустом прямоугольнике. Аналогичным методом целесообразно воспользоваться для выявления максимально широкой области возможного встраивания, используя полученную после применения рекурсивного фильтра матрицу чистых блоков и блоков стего.

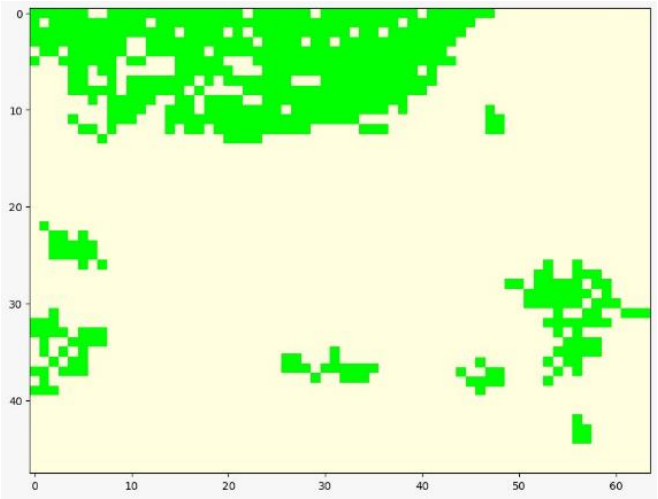


Рисунок 3.6 – Карта блоков изображения после обработки фильтром

Алгоритм выявления максимально широкой области возможного встраивания и окончательной верификации исследуемого изображения на предмет наличия LSB-вставки имеет следующий вид.

Шаг 1. Решение задачи о наибольшем пустом прямоугольнике.

Решение задачи о наибольшем пустом прямоугольнике [37, 40, 53, 105, 116, 128] позволяет выявить наибольший по площади прямоугольный массив условных стего-блоков, заключенный между чистыми блоками, что и является максимально широкой областью возможного встраивания или областью предполагаемого встраивания. Для карты блоков изображения, представленных на рисунке 3.6, предполагаемая область возможного встраивания имеет вид, представленный на рисунке 3.7.

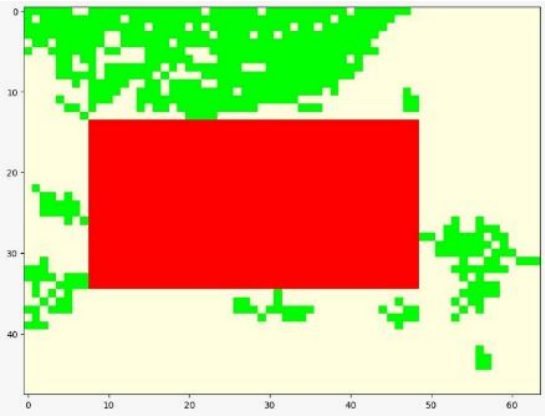


Рисунок 3.7 – Предполагаемая область возможного встраивания

Шаг 2. Верификация изображения на предмет встраивания

В качестве сигнатуры, используемой для окончательной верификации выделенной области используется количество белых пикселей и основанные на них модели доминирования белых/черных пикселей. Последовательно исследуется каждый пиксель предполагаемой области встраивания проводится исследование на предмет моделей доминирования белых пикселей в блоке его вхождения, т.е. блоке, образованным этим пикселем и его 8 окружающими соседями, с последующим расчетом момента изображения.

Таким образом, задача верификации изображения на предмет встраивания может иметь одно из указанных ниже решений:

Yes – выделенная область предполагаемого встраивания верифицирована как содержащая встраивание, а изображение классифицировано как стего.

No – выделенная область предполагаемого встраивания верифицирована как не содержащая встраивание, а изображение классифицировано как чистое.

Верификация изображения на предмет встраивания осуществляется по следующему алгоритму.

Для нулевого слоя предполагаемой области встраивания по каждому пикселю формируется блок вхождения, т.е. блок, образованным этим пикселем и его 8 окружающими соседями. Таким образом размерность блока вхождения составляет 3х3 или 9 пикселей.

В каждом блоке вхождения осуществляется подсчет количества белых пикселей с записью модели их доминирования $\boldsymbol{m_i^0}$. Так, например, $\boldsymbol{m_i^0 = 0}$ означает, что для исследуемого $\boldsymbol{i}$- го пикселя нулевого слоя в блоке вхождения присутствует 0 белых пикселей (по сути, речь идет о доминировании черных пикселей), $\boldsymbol{m_i^0 = 6}$ означает, что для исследуемого $\boldsymbol{i}$- го пикселя нулевого слоя в блоке вхождения присутствует 6 белых пикселей (по сути, речь идет об отсутствии явного доминирования каких либо пикселей), а $\boldsymbol{m_i^0 = 9}$ означает, что для исследуемого $\boldsymbol{i}$- го пикселя нулевого слоя в блоке вхождения присутствует 9 белых пикселей (т.е. наблюдается четкое доминирование белых пикселей)

Результаты выявленных моделей доминирования заносятся в структуру данных, где ключом является выявленная модель доминирования белых пикселей $\boldsymbol{m_i^0}$, а значением – координаты исследуемого $\boldsymbol{i}$-го пикселя.

Аналогичные действия 1-3 выполняются для пикселей первого слоя предполагаемой области встраивания. Модель доминирования белых пикселей в блоке вхождения первого слоя выделенной области предполагаемого встраивания обозначена как m_i^1

По каждому пикселю первого слоя выделенной области предполагаемого встраивания проводится анализ на предмет принадлежности его к одной из моделей типа $m_i^1 = 0$, $m_i^1 = 1$, $m_i^1 = 8$ и $m_i^1 = 9$, в результате чего формируется список, содержащий только пиксели, обнаруживающие модели указанного типа

По каждому пикселю из сформированного ранее списка производится сравнение моделей m_i^0 и m_i^1:

если $(m_i^1 - m_i^0) \leq |З|$, считается, что изменение модели доминирования белых пикселей в блоке вхождения по исследуемому пикселю находится в пределах нормы, обусловленной особенностями межслойного переноса моделей доминирования, а пиксель является неизмененным;

в противном случае считается, что изменение модели доминирования белых пикселей в блоке вхождения по исследуемому пикселю превышает допустимые отклонения, обусловленные особенностями межслойного переноса моделей доминирования, а сам пиксель является измененным.

В результате формируется массив пикселей с изменениями в моделях доминирования, пример графического изображения которого представлен на рисунке 3.8.

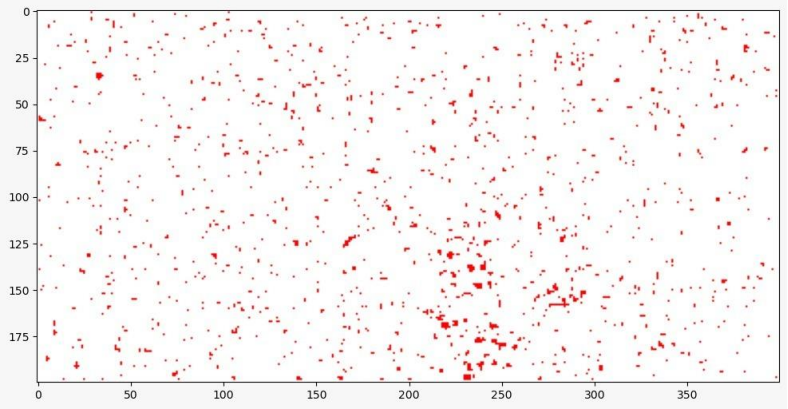


Рисунок 3.8 – Карта пикселей с изменениями в моделях доминирования

Обоснование. На рисунках 3.9 а-в) представлены диаграммы примеров моделей доминирования белых пикселей в соответствующих блоках вхождения первого слоя изображения, а также его чистого нулевого его слоя и нулевого слоя со встраиванием, где по оси абсцисс указан порядковый номер исследуемого пикселя, а по оси ординат указана модель доминирования белых пикселей в блоке вхождения данного пикселя.

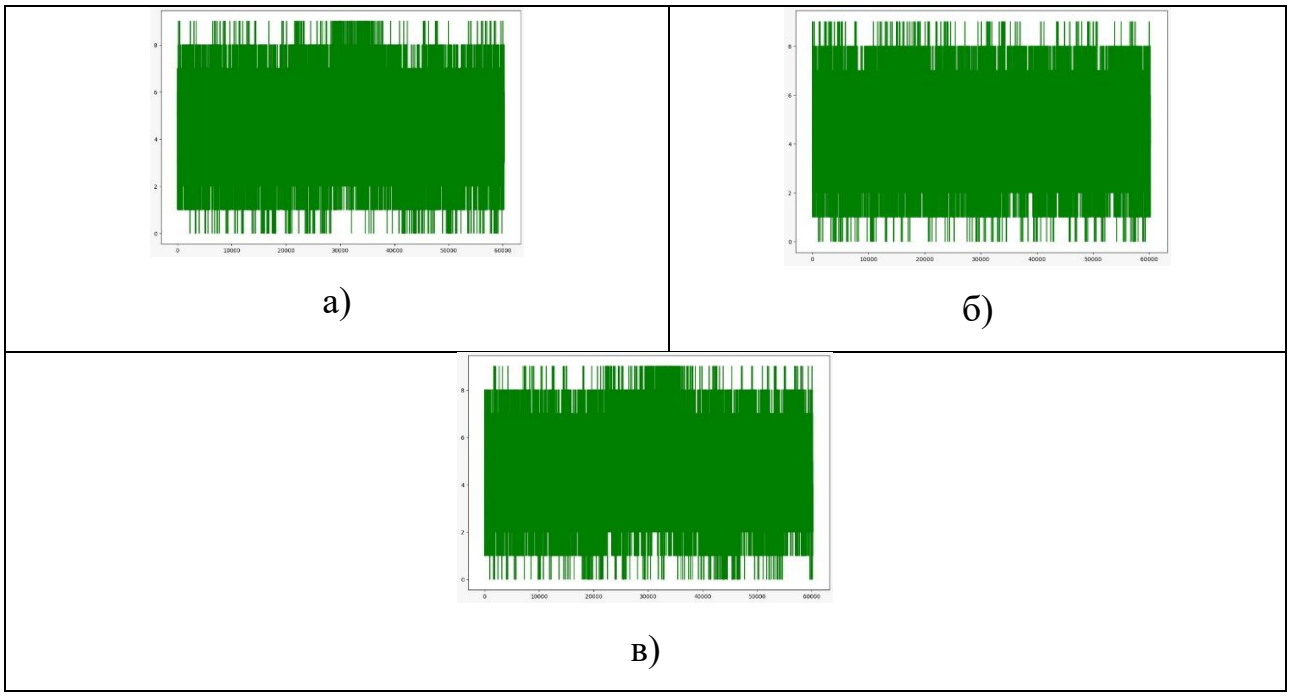


Рисунок 3.9 – Пример моделей доминирования белых пикселей в блоках вхождения области предполагаемого встраивания: а) модели доминирования белых пикселей, выделенные в нулевом слое изображения без встраивания, б) модели доминирования белых пикселей, выделенные в нулевом слое изображения со встраиванием, в) модели доминирования белых пикселей, выделенные в первом слое изображения

Сравнительный анализ поведения моделей доминирования белых пикселей при межслойном переносе, в чистых изображениях и изображениях со встраиванием, проведенный с использованием множества изображений, позволяет сделать следующие выводы:

•при отсутствии встраивания модели доминирования типа $m_i^0 = 0$, $m_i^0 = 1$, $m_i^0 = 8$ и $m_i^0 = 9$ переносятся между слоями в практически неизменном виде, т.е. 80% пикселей, обнаруживающих подобные модели доминирования белых пикселей в нулевом слое, сохраняют эти модели в первом слое либо обнаруживают закономерность типа $(m_i^0 - 3) \le m_i^1 \le (m_i^0 + 3)$,

где m_i^0 – количество белых пикселей в выделенном *i*-ом блоке нулевого слоя;

m_i^1 – количество белых пикселей в выделенном *i*-ом блоке первого слоя.

•при наличии встраивания модели доминирования типа $m_i^0 = 0$, $m_i^0 = 1$, $m_i^0 = 8$ и $m_i^0 = 9$ подвергаются существенным изменениям при переносе между слоями, что обусловлено нарушением структуры изображения в нулевом слое

•для моделей доминирования от типа $m_i^0 = 2$ до типа $m_i^0 = 7$ изменения хаотичны и не обнаруживают четких закономерностей, что говорит об их низкой информативности для целей текущего анализа.

1. Для выделенной области предполагаемого встраивания осуществляется расчет момента изображения MI с использованием массива измененных пикселей, на основании которого осуществляется окончательная верификация на предмет встраивания:

•если координаты момента MI соответствуют центральным координатам исследуемой области в пределах допустимых значений, предположение о наличии встраивания в выделенную область исследуемого изображения считается неподтвержденным, и алгоритм возвращает результат No (изображение не содержит встраивание)

•в противном случае предположение о наличии встраивания в выделенную область исследуемого изображения считается подтвержденным, и алгоритм возвращает результат Yes (изображение содержит встраивание)

Обоснование.

Анализ изменения моделей доминирования белых пикселей и получаемых моментов изображений, проведенный с использованием множества изображений, позволил сделать следующие выводы:

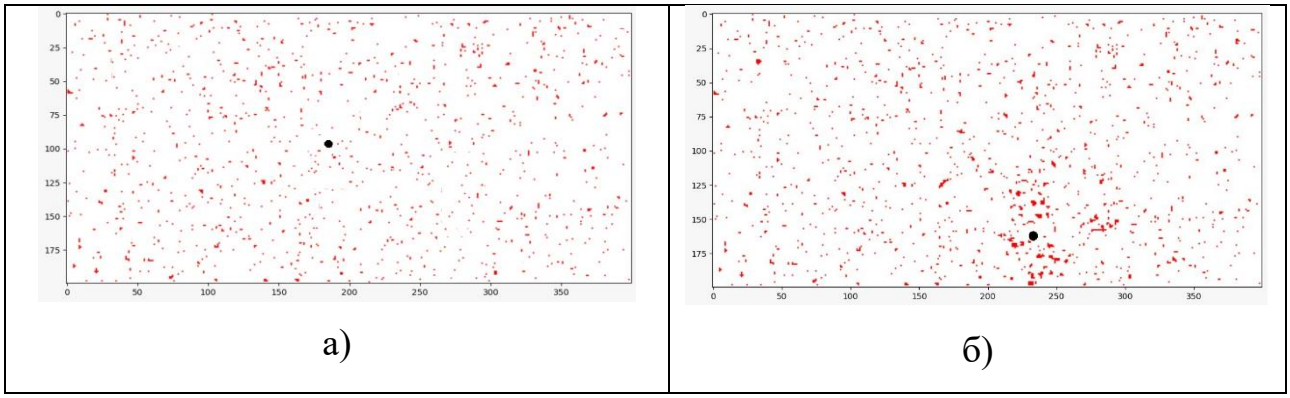
•изменения моделей доминирования белых пикселей при переносе между слоями могут присутствовать как в изображениях со встраиванием, так и в изображениях, не содержащих встраивания;

•в изображениях, не содержащий встраивание, наблюдается отсутствие концентрации пикселей, обнаруживающих изменения моделей доминирования белых пикселей, в одной локальной области, а, наоборот, наблюдается их

относительно равномерное распределение, в результате чего момент изображения находится в диапазоне координат центра изображения;

- в изображениях, содержащий встраивание, наблюдается высокая концентрация пикселей, обнаруживающих изменения моделей доминирования белых пикселей, в одной локальной области, в результате чего момент изображения значительно отклоняется от его центра.

Пример моментов изображений без встраивания и со встраиванием для одной и той же области приведен на рисунках 3.10 а-б).



а) б)

Рисунок 3.10 – Пример моментов изображений для одной и той же области фотографического изображения: (а) момент изображения без встраивания, (б) момент изображения со встраиванием

3.3 Алгоритм выделения области встраивания

Локализация области встраивания производится на основе классификации отдельных ее участков как содержащих и не содержащих встраивание и основывается на особенностях встраивания как случайного набора пикселей со значениями 1 и 0. Таким образом, была выдвинута гипотеза о том, что соотношение 1 и 0 на участках встраивания близко к 0,5. Проведенные эмпирические исследования подтверждают данную гипотезу.

Алгоритм локализации области встраивания имеет следующий вид:

1. Осуществляется разбивка выделенной на предыдущем этапе предполагаемой области встраивания на блоки размерностью 20x20, что достаточно для того, чтобы выборка была признана репрезентативной для целей построения корректных выводов о соотношении нулей и единиц. При этом блок данной размерности позволяет отсекать области без встраивания с минимальными потерями с точки зрения точности определения границ встраивания.

Таким образом, вся исследуемая область формирует массив MS_0 и разбивается на F рядов и G столбцов, а общее количество блоков равно $F \times G$.

2. Для каждого блока рассчитывается показатель плотности единичных значений p. Для этого вычисляем исходный показатель плотности единичных значений p':

$$p'_i = \frac{Q_1}{Q} \tag{11}$$

где Q – общее количество пикселей в исследуемой области, пиксели;

Q_1 – количество пикселей в исследуемой области, имеющих единичное значение, пиксели.

При этом, если значение исходного показателя плотности единиц $p' \leq 0.5$ то $p = p'$. Если значение исходного показателя плотности единиц $p' > 0.5$, то $p_i = 1 - p'_i$

3. По каждому блоку анализируется показатель плотности единичных значений p:

- если $p = 0.5$, блок классифицируется как блок, возможно содержащий встраивание и ему присваивается значение (255,0,0);
- иначе – блок классифицируется как не содержащий встраивание и ему присваивается одно значение (x , 0, 0), где значение x определяется по формуле:

$$x = 255 \times 2 \times p \tag{12}$$

В результате формируется карта блоков выделенной предполагаемой области встраивания для анализируемого изображения, пример которой представлен на рисунке 3.11.

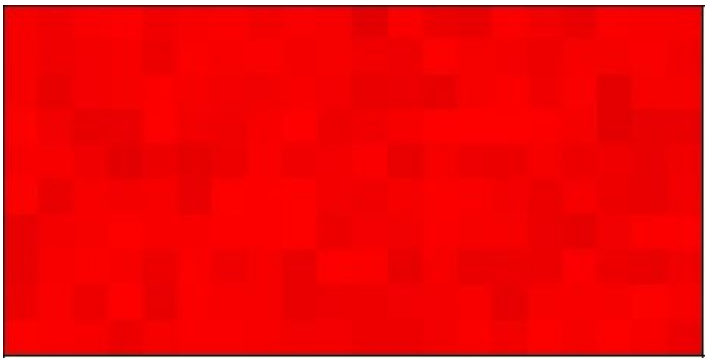


Рисунок 3.11 – Пример карты блоков предполагаемой области встраивания (насыщенность блоков снижается по мере отклонения от равного соотношения нулей и единиц)

4. Для исходного массива рассчитывается средняя плотность блоков $\bar{p}$ по формуле:

$$\bar{p} = \frac{\sum_1^n p_i}{F \times G}, \quad (13)$$

где $F \times G$ – общее количество блоков, которые содержит анализируемая область

5. Используя стандартную функцию, определяется центр масс анализируемой области – *CM* с координатами ($x_{CM}; y_{CM}$). В качестве критерия для вычисления центра масс используем плотность единичных значений p_i в блоках.

6. Координаты центра масс ($x_{CM}; y_{CM}$) сравниваются со значениями центральных координат ($x_0; y_0$).

В случае, когда все блоки выделенной области содержат встраивание, т.е. $p_i \approx 0,5$ по каждому блоку, центр масс будет либо полностью совпадать с центром анализируемой области, либо находиться в ее центральном блоке:

Таким образом, отклонение центра масс изображения от центрального значения означает существование блоков, не содержащих встраивание и имеющих плотность единичных значений p меньше 0,5.

Поскольку ранее в качестве условия встраивания было определено, что встраивание есть прямоугольная область, можно сделать вывод, что допустимо работать с целым рядом или целым столбцом вместо работы с отдельным блоком, принадлежащим этому ряду или столбцу.

Так, можно сделать следующие выводы:

- смещение центра масс по координате *x* к началу координат означает, что блоки одного или нескольких крайних правых столбцов не содержат встраивание;
- смещение центра масс по координате *x* от начала координат означает, что блоки одного или нескольких крайних левых столбцов не содержат встраивание;
- смещение центра масс по координате *y* к началу координат означает, что блоки одного или нескольких крайних верхних рядов не содержат встраивание;
- смещение центра масс по координате *y* от начала координат означает, что блоки одного или нескольких крайних нижних рядов не содержат встраивание.

Таким образом, можно выделить 4 основные стратегии сужения области исследования:

- Стратегия 1 – отсечение по *x* справа;
- Стратегия 2 – отсечение по *x* слева;
- Стратегия 3 – отсечение по *y* снизу;
- Стратегия 4 – отсечение по *y* сверху;

При этом, отклонения значения координат центра масс от центральных значений области осуществляется по формулам:

$$\Delta x = \left| \frac{x_{CM} - x_0}{x_0} \right|, \tag{14}$$

$$\Delta y = \left| \frac{y_{CM} - y_0}{y_0} \right|, \tag{15}$$

Таким образом, на основании проведенных сравнений алгоритмом принимается одно из следующих решений:

- Если $\Delta x = \Delta y = 0$ выделенная область является областью встраивания в полном объеме;
- Иначе:
  - Если $\Delta x > \Delta y$, то: если $\Delta x < 0$, то применяется Стратегия 1; иначе – применяется Стратегия 2;
  - Если $\Delta x < \Delta y$, то если $\Delta y < 0$, то применяется Стратегия 3; иначе – применяется Стратегия 4.

7. Полученный после реализации выбранной стратегии массив MS_i запоминаем как новый массив.

8. Для нового массива MS_i рассчитывается средняя плотность блоков $\overline{p_{MS_i}}$.

9. Производится сравнение средней плотности блоков исходного и нового массивов:

- Если $\overline{p_{MS_i}} > \overline{p_{MS_{i-1}}}$, то принимается решение об использовании нового массива в качестве фокусного, продолжается реализация выбранной стратегии.
- Иначе – в качестве фокусного остается ранее выделенный массив, вновь выполняются шаги 4-9.

3.4 Компьютерный эксперимент

Тестирование алгоритма осуществлено на 500 цветных фотографических изображениях. Поставленные задачи стегоанализа включают определение наличия встраивания, а также локализацию области встраивания. Встраивание осуществлялось в виде потока бит, которые представляют собой текстовую строку, область встраивания прямоугольная. Для встраивания были поочередно использованы красная, зеленая и синяя компоненты – для каждого изображения. Уровень стегонагрузки составлял 25% и 10% – для каждого изображения, по всем трем уровням стегонагрузки для красной, зеленой и синей компонент. Также, для проверки корректной работы разработанного алгоритма стегоанализа цветных

фотографических изображений, каждое из изображений подвергалось исследованию при полном отсутствии встраивания (чистые изображения). Таким образом, в ходе компьютерного эксперимента было произведено 7 прогонов по каждому из исследуемых изображений, а генеральная совокупность составила 3500 единиц – 3000 стего изображений и 500 чистых изображений.

В 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.

В таблицах 3.1 и 3.2 приведены полученные результаты работы алгоритма стегоанализа метода LSB-замены в цветных фотографических изображениях – точность классификации изображений (таблица 3.1) и точность локализации области встраивания (таблица 3.2).

Как представлено в таблице 3.1, средняя эффективность алгоритма стегоанализа метода LSB-замены в цветных искусственных изображениях составляет 78,8 %, т.е. наличие LSB-вставок было успешно выявлено в 2364 случаях из 3000.

При этом, в случае, когда было заменено 25% битов, эффективность по компонентам составила 88,53%, с незначительными отличиями по каждой компоненте (в 1-2 изображения), т.е. при прогоне 500 стегоконтейнеров с поочередным встраиванием в одну из компонент (в общем количестве 1500 стегоконтейнеров), алгоритм обнаружил наличие встроенного сообщения в 432-433 стегоконтейнерах в каждой из исследуемых компонент (в общем количестве – 1298 единицы) и 67-68 контейнер (в общем количестве – 202 единицы) были

ошибочно определены как чистый (т.е. был возвращен ложно-негативный результат).

Таблица 3.1 – Результаты работы алгоритма стегоанализа метода LSB-замены в цветных фотографических изображениях (точность классификации изображений)

<table>
<tr><td rowspan="2">Анализируемая компонента</td><td colspan="3">Уровень стегонагрузки, %</td></tr>
<tr><td>25</td><td>10</td><td>0</td></tr>
<tr><td>Красная компонента</td><td>TP= 88,6%
FN= 11,4%</td><td>TP= 69,2%
FN= 30,8%</td><td rowspan="4">TN= 96,6%
FP= 3,4%</td></tr>
<tr><td>Зеленая компонента</td><td>TP= 88,4%
FN= 11,6%</td><td>TP= 69,0%
FN= 31,0%</td></tr>
<tr><td>Синяя компонента</td><td>TP= 88,6%
FN= 11,4%</td><td>TP= 69,0%
FN= 31,0%</td></tr>
<tr><td>В среднем по компонентам</td><td>TP= 88,53%
FN= 11,47%</td><td>TP= 69,07%
FN= 30,93%</td></tr>
<tr><td>В среднем по коллекции изображений</td><td colspan="2">TP= 78,8%
FN= 21,2%</td><td></td></tr>
</table>

В случае, когда было заменено 10% битов, эффективность алгоритма по компонентам составила 69,07%, с незначительными отличиями по каждой компоненте (в 1 изображения), т.е. при прогоне 500 стегоконтейнеров с поочередным встраиванием в каждую из компонент (в общем количестве 1500 стегоконтейнеров), алгоритм обнаружил наличие встроенного сообщения в 345-346 стегоконтейнерах в каждой из исследуемых компонент (в общем количестве – 1036 единицы), а 155-156 контейнеров (в общем количестве – 464 единиц) были ошибочно определены как чистые (т.е. по ним был возвращен ложно-негативный результат).

Данные, представленные в таблице 3.2, свидетельствуют также о высокой эффективности разработанного алгоритма в отношении определения областей встраивания.

Таблица 3.2 – Результаты работы алгоритма стегоанализа метода LSB-замены в цветных фотографических изображениях (точность локализации области встраивания)

Анализируемая компонента	Уровень стегонагрузки, %	
	25	10
Красная компонента	92,43 %	84,76 %
Зеленая компонента	91,57 %	86,12 %
Синяя компонента	93,01 %	85,54 %
В среднем по компонентам	92,37 %	85,47 %
В среднем по коллекции изображений	88,92%	

Так, в среднем по выборке область встраивания, выделенная алгоритмом, составила 88,92%, т.е. меньше действительной на 11,08%.

При этом, в случае, когда было заменено 25% битов, средняя эффективность локализации по компонентам составляет 92,37 %, т.е., область встраивания, выделенная алгоритмом, меньше фактической области встраивания на 7,63%. В то время как в случае, когда было заменено 10% битов, средняя эффективность локализации по компонентам составила 85,47 %, т.е., область встраивания, выделенная алгоритмом, на 14,53% меньше фактической области встраивания.

Таким образом, можно сделать вывод, что средняя точность локализации при 10% уровне встраивания ниже соответствующего показателя при работе с 25% уровнем встраивания чуть более чем на 8,55% (на 7,9 п.п. в абсолютном выражении).

3.5 Обсуждение результатов

Предложенный в данной главе алгоритм обнаружения вставок методом LSB-замены позволяет обнаруживать встроенное сообщение, и определить область встраивания. Компьютерный эксперимент показал, что при LSB-замене битов нулевого слоя на 25% эффективность обнаружения СГВ по компонентам составляет 88,6% – 88,7%, что превосходит или практически соответствует результатам статистических методов при заполнении стегоконтейнера в 40% и более (86% и 90% соответственно) [79, 124].

Также следует отметить, что эффективность предложенного алгоритма при работе с малым уровнем стегонагрузки превосходит существующие методы стегоанализа цветных изображений с 25% уровнем заполнения стегоконтейнера с привлечением машинного обучения и низкоразмерные методы стегоанализа [50, 51, 81, 117], что свидетельствует об экономичности и является преимуществом предлагаемого алгоритма.

Данные о сравнительной эффективности (по точности классификации) существующих алгоритмов и алгоритма стегоанализа, предлагаемого в данной главе, представлены в таблице 3.3.

Таблица 3.3 – Сравнительная эффективность точности классификации существующих алгоритмов и алгоритма стегоанализа, предлагаемого в данной главе, при низких объемах заполнения стегоконтейнера

Встраиваемая нагрузка	Предлагаемый метод	Существующие методы	
		Ансамблевый SW-стегоанализ	Компактный метод стегоанализа
25%	88,53 %	86,77	74,53
10%	69,07 %	–	–

Помимо этого, разработанный алгоритм может не только устанавливать факт наличия СГВ, но и позволяет определять расположение СГВ и ее размер. Средняя точность локализации области встраивания по компонентам при работе с уровнем стегонагрузки в 10 – 25% также высока и составляет 85,47 – 93,01%, что можно также выделить в качестве преимущества разработанного алгоритма.

Проведенный компьютерный эксперимент, направленный на оценку эффективности разработанного алгоритма, позволил сделать следующие выводы:

1. Алгоритм не обнаруживает большой зависимости точности классификации изображения и локализации области встраивания от компоненты, в которую было осуществлено встраивание. Так эффективность обнаружения LSB-вставок в цветных искусственных изображениях по компонентам при уровне стегонагрузке в 25% варьируется в пределах 0,2 п.п. (т.е. различие в 1 изображение). Аналогичные результаты наблюдаются и для стегоизображений с нагрузкой в 10%.

Подобный разброс значений слишком мал, что объясняется стабильными свойствами межслойной инерционности в отношении нулевого и первого слоев вне зависимости от компоненты. Следовательно, данным разбросом можно пренебречь и сделать вывод о равной эффективности алгоритма в рамках атаки на наличие встраивания в различные компоненты.

2. Алгоритм обнаруживает прямо пропорциональное изменение точности обнаружения встраивания в зависимости от размеров маски встраивания, снижение точности классификации изображения по мере уменьшения уровня стегонагрузки.

Так, наибольшую эффективность алгоритм показывает при работе с контейнером, объем встраивания в котором составляет 25% – в среднем, 88,53%. При работе с контейнером, объем встраивания в котором составляет 10%, алгоритм показывает эффективность, которая на 22% (19,46 п.п.) ниже по сравнению с результативностью при 25% уровне стегонагрузки.

3. Алгоритм обнаруживает прямо пропорциональное изменение по точности локализации области встраивания в зависимости от размеров маски

встраивания, т.е. чем больше площадь маски встраивания, тем больший ее процент выделен и локализован алгоритмом. При этом, зависимость точности локализации области встраивания от ее размеров является менее критичной, чем в случае с точностью обнаружения.

Снижение эффективности обнаружения стеговставки по мере уменьшения уровня стегонагрузки присуще всем существующим алгоритмам. При этом в отношении разработанного алгоритма можно увидеть, что снижение стегонагрузки на 15 (с 25% до 10%) процентных пункта приводит к достаточно большому снижению точности классификации. В отношении разработанного в данной главе алгоритма стегоанализа, это обусловлено тем, что чем меньший размер имеет маска встраивания, тем большая вероятность того, что область встраивания не затронет области максимального межслойного сходства в отношении нулевого и первого слоев.

Следовательно, опираясь на сигнатуры, выбранные в качестве основных, однозначные основания для классификации таких областей как стего могут отсутствовать.

При этом, высокий процент ложных срабатываний является типичным для подобных алгоритмов. Так, в аналогичных алгоритмах [96, 124], решающих задачу поиска поврежденных пикселей, которая значительно проще, процент ложных срабатываний равен 36%.

Анализ точности локализации области встраивания позволил сделать вывод, что недостижение 100%-го охвата области встраивания обусловлено достаточно крупными размерами блоков (20x20), на работу с которыми опирается данный алгоритм, и существование вероятности того, что при разделении первоначально выделенной области на блоки, исходная область не будет обнаруживать четкого деления в размерности 20x20, а, следовательно, в подобных случаях один ряд или столбец области будет захватывать пиксели из чистых областей, что впоследствии приводит к отсечению таких рядов или столбцов по итогам работы с центрами масс изображения и средней плотности пикселей.

При этом, логичным следствием описанного выше эффекта является наибольшая потеря точности в случае более малых размеров маски встраивания, что обусловлено тем, что чем меньше площадь встраивания, тем больший удельный вес занимает каждый пиксель. Следовательно, его последующее отсечение дает большую потерю точности.

Также здесь необходимо отметить, что в данном случае определяется не ошибочное детектирование наличия СГВ, а лишь распознание битов, входящих в область встраивания. Поэтому данная ошибка ложного срабатывания является допустимой.

Выводы по третьей главе

Разработан алгоритм стегоанализа метода LSB-замены в цветных фотографических изображениях на основе анализа нулевого и первого слоев, позволяющий определить наличие LSB-встраивания, а также локализовать область встраивания. При этом:

1. Алгоритм позволяет выявлять СГВ при низком заполнении контейнера. Средняя эффективность обнаружения СГВ с заполнением стегоконтейнера на 25% и 10% по компонентам составляет, соответственно 88,53% и 69,07%, что превышает или сопоставимо с эффективностью существующих методов стегоанализа с привлечением ресурсо-затратного машинного обучения, где подобные высокие результаты описываются только для 25% уровня заполнения стегоконтейнера.

2. Алгоритм даёт возможность локализовать область встраивания в автоматическом режиме. При этом для цветных фотографических изображений границы области встраивания могут быть определены с точностью, в среднем, 92,37%, для стегоконтейнера, заполненного на 25%, и 85,47%, для стегоконтейнера, заполненного на 10%, что означает, что алгоритм оставляет не выявленными всего, соответственно, 7,57%, и 14,53% пикселей с подмененным младшим битом. В

алгоритмах, решающих подобную задачу определения положения зашумленных пикселей процент ложных срабатываний равен 36% [96, 124].

Результаты данной главы опубликованы в работах [6, 9, 17].

По реализации данного алгоритма, выполненного на языке программирования Python, получено Свидетельство о государственной регистрации программ для ЭВМ [13].

Глава 4. Алгоритм выявления и локализации встраиваний, выполненных методом Коха-Жао, в цветных изображениях

В четвертой главе диссертационного исследования представлен алгоритм выявления стеганографических вставок в изображение, встраиваемых с помощью метода Коха-Жао. В диссертации рассмотрен случай, когда осуществляется прерывное встраивание, при этом количество областей встраивания может быть больше одного.

4.1 Введение в проблематику

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 [48] и алгоритм Барни [46, 59]. 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 [83]. 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 [93]. 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 [83]. 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 [83] 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. В целях нашего исследования, мы будем опираться на то, что информация о параметрах имеет минимальный размер. В таком случае можно сформулировать следующие предположения:

1) Осуществляемое встраивание характеризуется как дискретное, т.е. осуществляется в прерывную последовательность блоков.

2) Встраивание осуществляется в среднечастотные компоненты как компоненты, способные максимально скрыть факт наличия встроенного сообщения от визуальной детекции, тем самым, позволяя добиться максимально низкого риска обнаружения.

3) В одном и том же изображении может присутствовать как одна область встраивания, так и несколько отдельных областей встраивания.

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

5) Область встраивания прямоугольная и составляет от 10 до 40%.

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.

Предлагаемый в работе алгоритм стеганографического анализа основан на выявлении коэффициентов 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 блокаB_i $(i = 1, \dots, N)$ рассчитаем коэффициенты ДКП. Результат – совокупность матриц коэффициентов D_i $(i =$

$1, \dots, N$) с размером 8×8. Далее для каждой из матриц необходимо произвести расчет разницы пар коэффициентов ДКП, анализ которых впоследствии будет проводиться предлагаемым алгоритмом.

Выделим те частоты коэффициентов ДКП, которые являются оптимальными для встраивания. В данном случае под оптимальными частотами понимаются те частоты, встраивание в которые вызывает наименьшие искажения изображения, а, следовательно, имеет наименьший риск обнаружения.

Проведем анализ среднечастотных элементов матриц D_i ($i = 1, \dots, N$), встраивание в которые. Введём три последовательности величин ($i = 1, \dots, N$):

$$\begin{aligned} C_i^{(1)} &= ||D_i[3,4]| - |D_i[4,3]||, \\ C_i^{(2)} &= ||D_i[3,5]| - |D_i[5,3]||, \\ C_i^{(3)} &= ||D_i[4,5]| - |D_i[5,4]||. \end{aligned} \tag{16}$$

В результате встраивания СГВ в одной из этих последовательностей возникают изменения. На Рисунке 4.1 изображён пример изменения разниц пар коэффициентов ДКП для изображения с тремя СГВ в компоненты D [3,4] и D [4,3].

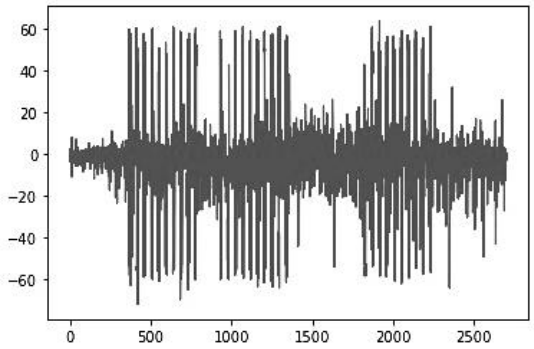


Рисунок 4.1 – Гистограмма последовательности разниц пар коэффициентов ДКП для изображения с тремя СГВ в компоненты D [3,4] и D [4,3]

Нами установлено, что наиболее безопасными для встраивания являются среднечастотные компоненты (3, 4) и (4, 3). Следовательно, разрабатываемый

алгоритм должен осуществлять атаку именно среднечастотных коэффициентов ДКП.

Сформируем последовательность, элементы которой есть разницы пар среднечастотных коэффициентов ДКП.

Анализ массива последовательности разницы пар среднечастотных коэффициентов ДКП для изображений с одной или несколькими СГВ позволяет выявить две основные закономерности в указанных выше последовательностях:

1. Разницы пар коэффициентов ДКП в блоках, в которые было произведено встраивание, имеют значительно большие значения по сравнению с коэффициентами ДКП в блоках, не содержащих встраивание.

2. Разницы пар коэффициентов ДКП в блоках, в которые было произведено встраивание, имеют сравнительно небольшие отклонения между собой в модульном выражении.

Выявленные закономерности позволяют определить сигнатуры, необходимые для осуществления стеганографического анализа, а также сформулировать условие, при котором анализируемый блок последовательности следует считать блоком, в который было произведено встраивание.

В целях нашего исследования, можно утверждать, что необходимыми и достаточными сигнатурами являются следующие:

1. Отклонение P_i модульного значения текущего элемента последовательности (в качестве текущего здесь и далее принимается исследуемый) от максимального модульного значения среди всех элементов анализируемой последовательности:

$$P_i = C^{max} - |C_i| \tag{17}$$

где C^{max} – модульное максимальное значение разницы пар среднечастотных коэффициентов ДКП среди всех элементов анализируемой последовательности;

$|C_i|$– модульное значение разницы пар среднечастотных коэффициентов ДКП текущего (т.е. исследуемого) элемента анализируемой последовательности.

Сигнатура отклонения P_i является основополагающей для отнесения или не отнесения исследуемого блока к блоку-стего, т.е. содержащему встраивание. Общая исследуемого элемента (блока) характеристика с учетом данной сигнатуры имеет следующий вид:

•Исследуемый i -й элемент является блоком, не содержащим СГВ, если значение его отклонения P_i стремится к значению C^{max} всей анализируемой последовательности, т.е. значение разницы пар среднечастотных коэффициентов данного элемента существенно отличается от максимального значения разницы пар среднечастотных коэффициентов всей последовательности;

•Исследуемый i -й элемент является блоком, содержащим СГВ, если значение его отклонения P_i стремится к минимальному значению среди всех значений по анализируемой последовательности, $P_i \to P_{\min}^{j}$ т.е. значение разницы пар среднечастотных коэффициентов данного элемента несущественно отличается от максимального значения коэффициентов ДКП всей последовательности.

2. Отклонение R_i значения разницы пар среднечастотных коэффициентов текущего (в качестве текущего здесь и далее принимается исследуемый) элемента анализируемой последовательности от значения разницы пар среднечастотных коэффициентов последующего элемента указанной последовательности:

$$R_i = C_i - C_{i+1} \tag{18}$$

где C_i – значение разницы пар среднечастотных коэффициентов текущего (т.е. исследуемого) элемента анализируемой последовательности;

C_{i+1}– значение разницы пар среднечастотных коэффициентов последующего элемента анализируемой последовательности.

Сигнатура отклонения R_i осуществляет вспомогательную роль для целей стегоанализа, являясь сигнатурой подтверждения правильности классификации

исследуемого элемента. Также, данная сигнатура позволяет более точно определить границы локализации СГВ.

Общая характеристика данной сигнатуры имеет следующий вид:

•Исследуемый i -й элемент является блоком, являющимся границей встраивания, если значение его R_i-сигнатуры стремится к значению C^{max} всей анализируемой последовательности, т.е. значение разницы пар среднечастотных коэффициентов данного элемента существенно отличается от значения по следующему элементу анализируемой последовательности;

•Исследуемый i -й элемент является блоком, не являющимся границей встраивания, если значение его R_i-сигнатуры стремится к своему минимальному значению среди значений по всей анализируемой последовательности, $R_i \to R_{\min}^j$, т.е. значение разницы пар среднечастотных коэффициентов данного элемента несущественно отличается от значения по следующему элементу анализируемой последовательности.

При этом, в отношении сигнатуры R_i без дополнительного анализа невозможно утверждать, является ли блок со значением $R_i \to C^{max}$ по модулю, блоком, содержащим СГВ, так как близлежащие элементы последовательности, не содержание встраивание так же имеют незначительные отклонения в своих. В то же время, поскольку встраивание дискретное, можно утверждать, что блок со значением $R_i \to C^{max}$ по модулю является блоком, не содержащим СГВ.

Все возможные вариации комбинации значений указанных выше сигнатур можно отнести к одному из представленных ниже варианту развития событий:

А) Значения обоих сигнатур исследуемого элемента стремятся к своим минимальным значениям по анализируемой последовательности:

$$P_i \to P_{\min}^j ; R_i \to R_{\min}^j \qquad (19)$$

Б) Значения обоих сигнатур исследуемого элемента стремятся к максимальным значениям разницы пар среднечастотных коэффициентов по анализируемой последовательности:

$$P_i \to C^{max}; R_i \to C^{max} \quad (20)$$

В) Значение P_i -сигнатуры исследуемого элемента стремится к своему минимальному значению по анализируемой последовательности, тогда как значение R_i -сигнатуры исследуемого элемента стремится к максимальному значению разницы пар среднечастотных коэффициентов по анализируемой последовательности:

$$P_i \to P_{\min}^{j}; R_i \to C^{max} \quad (21)$$

Г) Значение P_i -сигнатуры исследуемого элемента стремится к к максимальному значению разницы пар среднечастотных коэффициентов по анализируемой последовательности, тогда как значение R_i -сигнатуры исследуемого элемента стремится к своему минимальному значению по анализируемой последовательности:

$$P_i \to C^{max}; R_i \to R_{\min}^{j} \quad (22)$$

Исходя из общих характеристик выделенных нами сигнатур, приведенных выше в данном разделе, можно сделать вывод, что элемент содержит СГВ, если одновременно выполняются условия его отнесения к таковому по каждой из сигнатур.

Таким образом, условием отнесения анализируемого элемента исследуемой последовательности к элементу, содержащему встраивание, является следующее условие строгого логического И:

$$P_i \to P_{\min}^j ; R_i \to R_{\min}^j \quad (23)$$

4.4 Алгоритм локализации области встраивания

Локализация области встраивания основана на разделении всех элементов последовательности на кластеры (кластеризация). Поскольку выделенные в предыдущей главе сигнатуры являются необходимыми и достаточными, кластеризация осуществляется в двухмерном пространстве, где каждая их сигнатур соответствует характеристикам одной из осей координат. При этом, в целях проводимого исследования условимся, что сигнатура P_i соответствует характеристикам оси OX, т.е. является абсциссой точки расположения элемента последовательности на плоскости, а сигнатура R_i соответствует характеристикам оси OY, т.е. является ординатой точки расположения элемента последовательности на плоскости.

Кластеризация проводится с использованием алгоритма машинного обучения и кластеризации DBSCAN [77]. Для кластеризации элементов заданной последовательности используются два параметра – плотность расположения соседних элементов (EPS) и минимально допустимое количество соседствующих элементов, расположение которых удовлетворяет условию плотности их расположения, необходимое для группировки их в один кластер (MIN SAMPLES).

Таким образом, алгоритм локализации области встраивания выглядит следующим образом:

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. На основе матрицы коэффициентов, полученных на предыдущем этапе, строится новая последовательность J_i, содержащая модульные значения разниц пар найденных коэффициентов:

$$J_i = \left| |D_i[3,4]| - |D_i[4,3]| \right| \quad (24)$$

4. В последовательности J_i выделяется максимальное модульное значение C^{max}.

5. Вычисляются сигнатуры P_i и R_i для каждого элемента последовательности J_i согласно выражениям (16) и (17) с одновременным выделением их минимальных значений $P_{\min}^{j}$ и $R_{\min}^{j}$.

6. Значения сигнатур подаются на вход алгоритму кластеризации DBSCAN.

7. Задаются параметры EPS и MIN SAMPLES и запускается алгоритм кластеризации DBSCAN.

8. Анализируются выделенные кластеры. Если один или несколько элементов, принадлежащих анализируемому кластеру, удовлетворяют условию:

$$P_i = P_{\min}^{j}; R_i = R_{\min}^{j}, \quad (25)$$

то данный кластер следует считать кластером, в котором сгруппированы блоки, содержащие встраивание, всем блокам кластера присвоить значение 1. Иначе – кластер не содержит коэффициенты, в которые осуществлялось встраивание; всем блокам кластера следует присвоить значение 0.

9. Поскольку в последовательности могут присутствовать шумы, а алгоритм DBSCAN эти шумы отсекает, не включая ни в один из кластеров, необходимо дополнительно провести обработку полученных данных при помощи фильтра,

аналогичному фильтру, представленному в главе 2, что позволит дополнительно выявить блоки изображения, содержащие встраивание.

10. Итоговая локализация области встраивания производиться методом задачи о наибольшем пустом прямоугольнике, решение которой аналогично решению, представленному в главе 2.

При этом:

— если локализованная область составляет не менее 1% от общей площади изображения, изображение классифицируется как изображение классифицируется как стего;

— иначе – изображение классифицируется как чистое.

В качестве примера приведены результаты тестирования фотографического изображения, в который были произведены дискретные встраивания методом Коха-Жао в три различные области. На рисунке 4.2 представлено непосредственно само изображение, в которое было осуществлено встраивание, а также рамочными квадратами выделены три области встраивания.

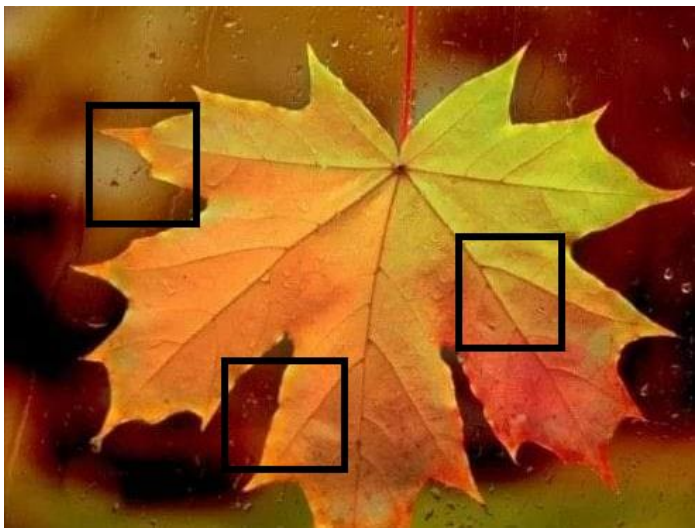


Рисунок 4.2 – Пример фотографического изображения с тремя областями встраивания

Результат прохождения первых двух этапов представленного выше алгоритма можно представить в виде гистограммы полученной последовательности коэффициентов ДКП, графическое изображение такой гистограммы представлено на рисунке 4.3.

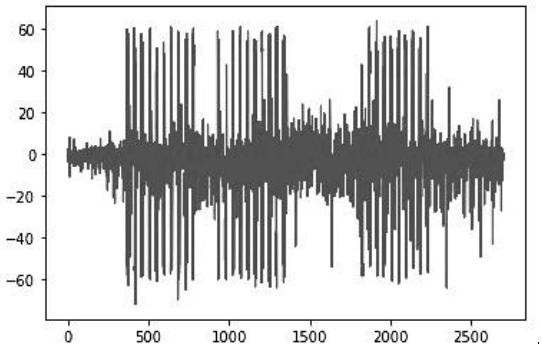


Рисунок 4.3 – Пример гистограммы последовательности коэффициентов ДКП для фотографического изображения с тремя областями встраивания

Результат прохождения этапа 8 с применением алгоритма DBSCAN (этап 8) – множество элементов последовательности разделены на три кластера, что представлено на рисунке 4.5.

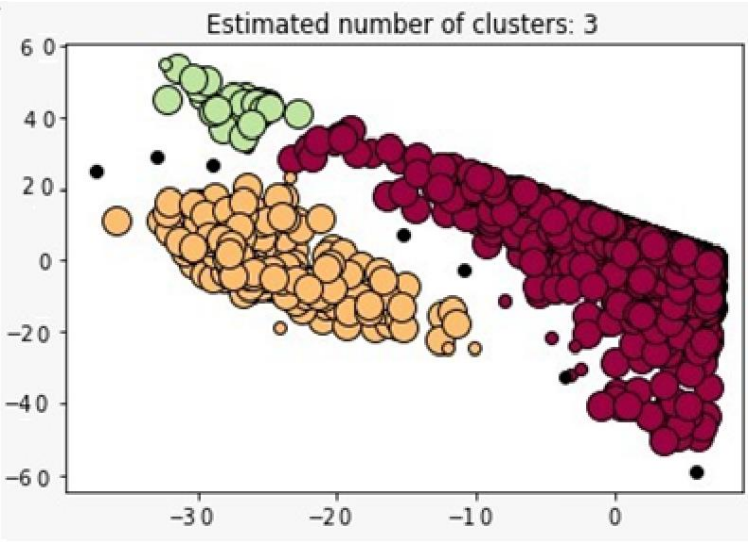


Рисунок 4.5 – Результат инициализации кластеров в исследуемой последовательности посредством алгоритма DBSCAN

На этапе 9 выделен кластер, отвечающим заданным условиям, в результате чего были локализованы области встраивания – соответственно, рисунки 4.6 и 4.7.

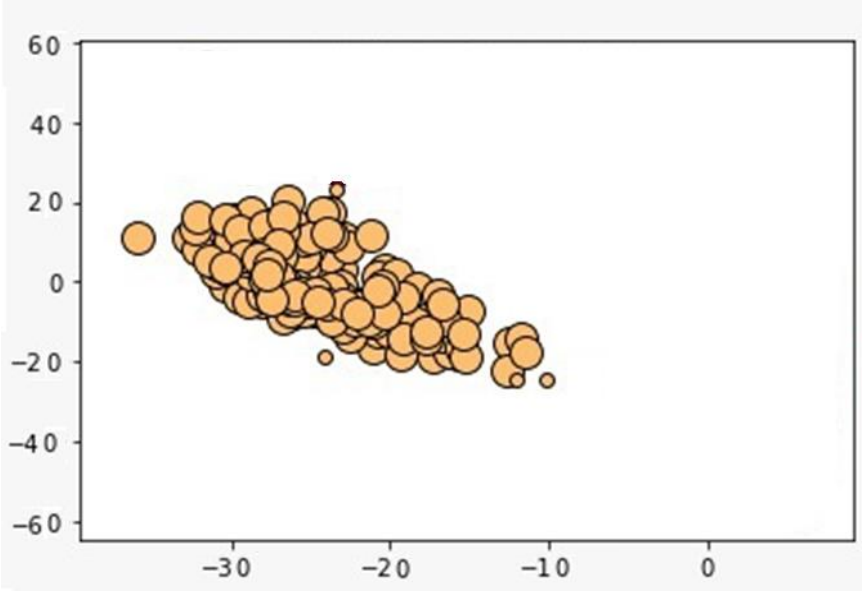


Рисунок 4.6 – Инициализация кластера с блоками, содержащими встраивание

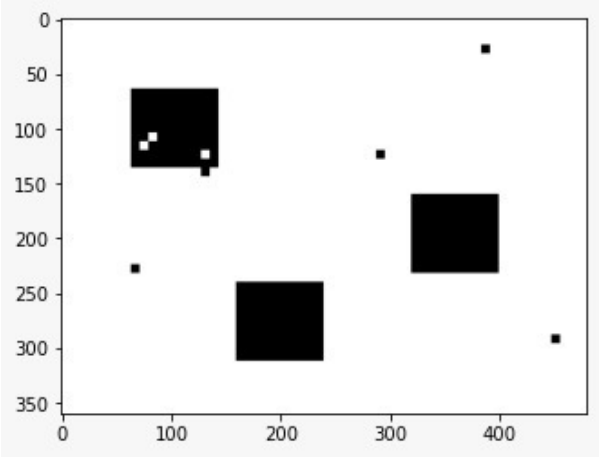


Рисунок 4.7 – Локализация областей встраивания

Исходя из рисунка 4.7 можно сделать вывод, что в выстроенной последовательности коэффициентов ДКП анализируемого фотографического изображения присутствуют шумы. На рисунке 4.7 шумы представлены в виде пяти

отдельно стоящих редких хаотичных черных точек на белом пространстве, а также трех белых точек, локализованных в одном из черном квадрате, являющимся одной из трех областей встраивания.

Обработка данных фильтром позволила нивелировать указанные шумы и получить более точную локализацию областей встраивания, представленную на рисунке 4.8, на котором можно наблюдать четкие границы выявленных (локализованных) областей встраивания. Результаты локализации областей встраивания на анализируемом изображении, приведенном на рисунке 4.2, представлены на рисунке 4.9.

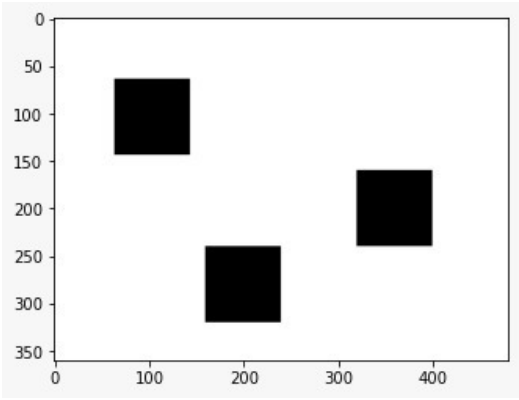


Рисунок 4.8 – Локализация областей встраивания после обработки данных фильтром

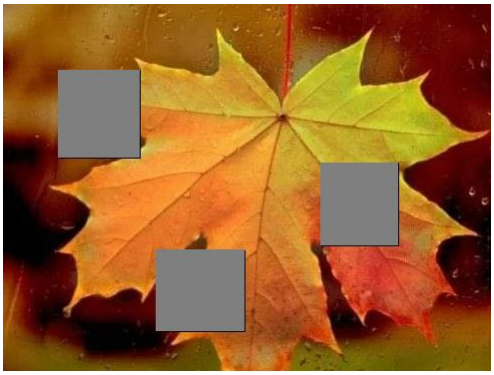


Рисунок 4.9 – Результаты локализации областей встраивания на анализируемом изображении

4.5 Компьютерный эксперимент

В целях оценки работы предлагаемого алгоритма с точки зрения эффективности обнаружения встраивания, а также эффективности локализации областей встраивания, протестируем данный алгоритм с использованием библиотеки изображений Беркли (Berkeley Segmentation Data Set and Benchmarks 500, BSDS500).

Данная коллекция создана для осуществления проверки алгоритмов кластеризации и тем самым оптимально подходит для целей нашего исследования. 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, следует отметить, что именно наличие изображений в формате JPEG делает данную коллекцию изображений пригодными для реализации алгоритма обнаружения и локализации встраиваний, выполненных методом Коха-Жао, что связано с тем, что формат JPEG, так же, как и метод Коха-Жао, базируется на дискретном косинусном преобразовании. Следовательно, при работе с данной коллекцией не придется менять формат файла, что могло бы привести к дополнительными ошибкам.

Таким образом, мы значительно снижаем риск возникновения дополнительных ошибок, что могло бы повлиять на репрезентативность результатов тестирования предложенного в данной главе алгоритма.

В ходе тестирования, на вход алгоритма подавалось каждое изображение вначале без встроенных данных (пустой стегоконтейнер). После этого на вход алгоритма подавалось каждое из изображений со встроенным сообщением (заполненный стегоконтейнер). При этом, прогон стего-изображения осуществлялся с различным количеством областей встраивания и их общим размером:

— первый прогон –тестирование эффективности алгоритма в отношении его способности работать с чистыми стегоконтейнерами;

— второй прогон – тестирование эффективности алгоритма в отношении его способности работать с уровнем стегонагрузкой в 25%;

— третий прогон – тестирование эффективности алгоритма в отношении его способности работать с уровнем стегонагрузкой в 10%.

Таким образом, для каждого изображения было выполнено три прогона (один прогон чистого изображения и два прогона изображения со встраиванием). Общее количество прогонов составило 1500 (500 прогонов чистых изображений и 1000 прогонов изображений со встраиванием).

Следует отметить, что для правильной кластеризации и максимально точной локализации при отстройке алгоритма DBSCAN необходимо правильно выбрать параметры EPS (плотность расположения соседних элементов) и MIN SAMPLES (минимально допустимое количество соседствующих элементов, расположение которых удовлетворяет условию плотности их расположения, необходимое для группировки их в один кластер).

Проведенный компьютерный эксперимент показал, что для получения правдивых результатов кластеризации, отвечающих задачам стеганографического анализа, в качестве плотности расположения EPS достаточным является параметр 0,3 при минимально допустимом количество соседствующих элементов MIN SAMPLES равным 5.

В рамках компьютерного эксперимента по точности классификации, определялись:

FN –ложно-негативные результаты: изображение, содержащее СГВ, было определено как изображение, не имеющее встроенного сообщения.

TN –истинно негативные результаты: изображение, не содержащее СГВ, было корректно определено.

FP –ложно-позитивные результаты: изображение, не содержащее СГВ, было определено как изображение, содержащее СГВ.

TP –истинно позитивные результаты: изображение, содержащее СГВ, было корректно определено как стего.

Результаты тестирования точности классификации и локализации представлены, соответственно, в таблицах 4.1 и 4.2.

Как представлено в таблице 4.1, средняя эффективность алгоритма стегоанализа цветных изображений, направленного против метода Коха-Жао, составляет 98,2%, т.е. встраивания были успешно выявлены в 1483 случаях из 1500, и только 1,13% от общего количества прогонов (17 изображения из 1500) дал ложно-отрицательный результат, т.е. не выявил встраивания.

Таблица 4.1 – Результаты работы алгоритма стегоанализа метода Коха-Жао в цветных фотографических изображениях (точность классификации изображений)

Уровень стегонагрузки	Результаты классификации, шт.	Точность классификации, %
Изображения без встраивания	TN= 491 FP= 9	TN= 98,2 FP= 1,8
25%	TP= 494 FN= 6	TP= 98,8 FN= 1,2
10%	TP= 493 FN= 7	TP= 98,6 FN= 1,4
В среднем по изображениям со встраиванием	TP= 493,5 FN= 6	TP= 98,7 FN= 1,2

При этом, в случае, когда стегонагрузка составляет 25% от общего объема стегоконтейнера, эффективность алгоритма по выявлению встраивания составила 98,8% (494 изображения из 500 были корректно определены как стего). Таким образом, ошибки классификации при работе с 25% уровнем стегонагрузки не превышают 1,2%.

Таблица 4.2 – Результаты работы алгоритма стегоанализа метода Коха-Жао в цветных фотографических изображениях (точность локализации области встраивания)

Уровень стегонагрузки	Точность локализации области встраивания, %
25%	98,57
10%	97,16
В среднем по изображениям со встраиванием	97,87

В случае, когда стегонагрузка составляет 10% от общего объема стегоконтейнера, эффективность алгоритма по выявлению встраивания составила 98,6% (493 изображения из 500 были корректно определены как стего). Таким образом, ошибки классификации при работе с 10% уровнем стегонагрузки составляют 1,4%.

Данные, представленные в таблице 9, свидетельствуют о высокой эффективности разработанного алгоритма в отношении определения областей встраивания.

Так, в среднем по выборке область встраивания, выделенная алгоритмом, составила 97,87%, т.е. что меньше фактической области встраивания всего на 1,69%.

При этом, при общей стегонагрузке в 25%, эффективность локализации составила 98,57%, т.е., выделенная область встраивания меньше фактической на 1,43%. При общей стегонагрузке в 10%, точность локализации составила 97,16%, т.е., выделенная область встраивания меньше фактической на 2,84%.

4.6 Обсуждение результатов

Предложенный в данной главе алгоритм обнаружения встраиваний, выполненных методом Коха-Жао, показывает высокую эффективность и позволяет обнаруживать встроенное сообщение, и определить область встраивания. Компьютерный эксперимент показал, что при работе анализе стегоконтейнеров с низким уровнем заполнения (10 – 25%) эффективность обнаружения СГВ соответственно составляет 98,2 – 98,8%, что значительно превосходит результаты найденных нами алгоритмов стеганографического анализа, работающие с коэффициентами ДКП и сопоставимо низким заполнением стегоконтейнера (74,95 – 78,29%) [86, 117]. Также следует отметить, что, в отличие от существующих методов, использующие классификаторы с большой размерностью и сталкивающиеся с проблемой выбора верного ядра для анализируемых изображений, предлагаемый алгоритм имеет малую размерность, невысокую ресурсоемкость, а также отсутствие необходимости постоянной подстройки параметров алгоритма машинного обучения и классификатора DBSCAN под характеристики анализируемых изображений.

Помимо этого, разработанный алгоритм может не только устанавливать факт наличия СГВ, но и позволяет определять ее расположение и размер. Точность локализации области встраивания при работе с низким уровнем стегонагрузки чрезвычайно высока и составляет 97,16 – 98,57%, что можно также выделить в качестве преимущества разработанного алгоритма.

Проведенный компьютерный эксперимент, направленный на оценку эффективности разработанного алгоритма, позволил сделать следующие выводы:

1. Алгоритм практически не обнаруживает зависимость точности обнаружения встраивания от уровня стегонагрузки, т.е. по мере уменьшения размеров встраивания происходит несущественное снижение точности классификации изображения –потери точности классификации при работе с 10%

уровнем стегонагрузки составляют всего 0,2 п.п. по сравнению с точностью достигаемой при 25% уровне стегонагрузки.

Считаем, что потеря точности классификации на менее чем в один процент при снижении уровня стегонагрузки в 2,5 раза является несущественной, следовательно ею можно пренебречь.

2. Алгоритм обнаруживает прямо пропорциональное изменение по точности локализации области встраивания в зависимости от уровня стегонагрузки, т.е. чем в большее количество блоков произведено встраивание, тем больший процент от их общего количества выделен и локализован алгоритмом:

— наибольшую эффективность алгоритм показывает при работе с изображениями, в которых встраивание произведено в блоки пикселей общим объемом в размере 25% от объема стегоконтейнера – 98,57%;

— при работе с изображениями, в которых отдельная область встраивания составляет 10% от общего объема стегоконтейнера (т.е. размер встраивания в 2,5 раза меньше по сравнению с протестированным ранее уровнем стегонагрузки в 25%), эффективность алгоритма составляет 97,16%, что всего на 1,41 п.п. ниже своего максимального значения.

Недостижение 100%-го обнаружения встраивания обусловлено особенностями сигнатуры R_i, отвечающей за определение границ встраивания и таким образом, допускающая их смещение. При этом, данные проведенного эксперимента позволили сделать вывод, что даже при малых объемах встраивания погрешности определения блоков, содержащих встраивания, будут незначительны. Это обусловлено тем, что алгоритм выявляет конкретные блоки пикселей, содержащих встраивание, и не привязан к конкретной форме выполненной вставки, возвращая непосредственно блоки пикселей со встраиванием без какой-либо привязки их к любым другим блокам пикселей.

Ошибки в работе алгоритма могут быть обусловлены структурой изображения. В пустом изображении-стегоконтейнере возможно наличие пиков в

последовательности разниц коэффициентов дискретного косинусного преобразования, которые могут ложно приниматься за границу СГВ.

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 извлекать СГВ при его обнаружении и практически одинаково хорошо работает с любыми объемами заполнения стегоконтейнера и любым количеством областей встраивания.

3. Тестирование на коллекции изображений показало, что ошибки ложного определения наличия СГВ в пустом стегоконтейнере не превышают 1,8%. Эффективность обнаружения наличия СГВ, в среднем, составляет – 98,7% (фактически варьируется от 98,6% до 98,8%). Эффективность локализации области встраивания, в среднем, составляет 97,87% (фактически варьируется от 97,16% до 98,57%).

Результаты данной главы опубликованы в работах [7, 10, 15, 17, 134].

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ [14].

ЗАКЛЮЧЕНИЕ

Выделим основные результаты, полученные в диссертации:

1. Разработан алгоритм стегоанализа метода LSB-замены в цветных искусственных изображениях 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 небольшой областью градиентной или равномерной заливки на исходном изображении. Так, тестирование предложенного алгоритма показало его высокую эффективность при работе с изображениями, уровень стегонагрузки которых составляет 10 – 25%. Точность определения наличия встраивания составляет 98% при работе с 10% уровнем стегонагрузки и 99% при работе с уровнем стегонагрузки в 25%. При этом, алгоритм способен безошибочно распознать чистое изображение (ложно-положительные результаты отсутствуют). Точность локализации области встраивания составляет 96,87–98,27% с минимальной погрешностью при работе с 25% уровнем стегонагрузки и максимальным при работе с 10% уровне стегонагрузки. Эффективность разработанного алгоритма идентична при атаке на встраивание в любою компоненту как по точности классификации, так и по точности локализации.

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613002 от 01.03.2022.

2. Разработан алгоритм стегоанализа метода LSB-замены в цветных фотографических изображениях на основе анализа нулевого и первого битовых слоев. Предложенный алгоритм позволяет определять наличие СГВ, ее положение и размер и показывает высокую эффективность при работе с изображениями с низким уровнем заполнения стегоконтейнера (10-25%). Так, тестирование алгоритма установило, что средняя эффективность обнаружения LSB-вставок составляет 78,8% (максимальная эффективность в 88,6% достигается при работе со стегоконтейнером, в котором была произведена замена в 25% и более младших

битов; минимальная эффективность наблюдается при работе с 10% уровнем стегонагрузки – 69,07% в среднем). Алгоритм верно выделяет в среднем 88,92% пикселей с замененным младшим битом (от 93,01% при стегонагрузке в 25% до 85,47% при стегонагрузке в 10%). При этом ложные срабатывания при работе с чистыми изображениями составляют всего 3,4%.

Эффективность разработанного алгоритма идентична при атаке на встраивание в любою компоненту как по точности классификации, так и по точности локализации.

По практической реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613021 от 01.03.2022.

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 1,8%. Средняя эффективность обнаружения наличия встроенного сообщения составляет 98,7%. Средняя точность локализации области встраивания составляет 97,87%.

Эффективность разработанного алгоритма практически идентична при атаках на встраивание в изображениях с любым уровнем заполнения стегоконтейнера.

По реализации данного алгоритма на языке программирования Python получено Свидетельство о государственной регистрации программ для ЭВМ №2022613003 от 01.03.2022.

4. Реализован и протестирован программный комплекс, реализующий предложенные алгоритмы.

Перспективы дальнейшей разработки темы исследования заключаются в:

1. Совершенствовании представленных алгоритмов с целью обеспечения высокой эффективности на предмет выявления встраивания и локализации области встраивания при работе со стегонагрузкой, в сумме составляющей 10 – 25%, но разбитой на 2-3 областей встраивания.

2. Совершенствовании представленных алгоритмов с целью обеспечения высокой эффективности на предмет выявления встраивания и локализации области встраивания при работе с общей стегонагрузкой менее 10%, как составляющих единую область встраивания, так и разбитой на 2-3 области встраивания.

3. Разработке алгоритмического обеспечения стеганографического анализа, позволяющего извлекать встроенное сообщение из выделенной области.

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. Бабенко Л.К., Абасова А.М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение // Информационное противодействие угрозам терроризма. 2014. № 23. С. 201-205.
4. Барсуков В.С., Романцов А.П. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации // Специальная Техника. 2000. № 1.
5. Вершинин И.С., Гибадуллин Р.Ф., Пыстогов С.В., Райхлин В.А. Ассоциативная стеганография текстовых сообщений // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2021. № 1. С. 3-14.
6. Вильховский Д.Э. Алгоритм стеганографического анализа в противодействие методу LSB-замены для фотографических изображений с низким уровнем стегонагрузки // В сборнике: Новые горизонты. сборник докладов / под общей редакцией О. М. Голембиовской. – Брянск : БГТУ, 2022. – 653 с.
7. Вильховский Д.Э. Алгоритм стегоанализа цветных изображений в противодействие методу Коха–Жао // В сборнике: Сборник избранных статей научной сессии ТУСУР, Томск, 18–20 мая 2022 г.: в 3 ч. – Томск: В-Спектр, 2022. – Ч. 2. – 248 с.

8. Вильховский Д.Э. Алгоритм стегоанализа цветных искусственных изображений // Молодые учёные России: сборник статей XI Всероссийской научно-практической конференции (Пенза, 12 февраля 2022г.). С. 39–41.
9. Вильховский Д.Э. Метод обнаружения LSB-вставок в цветных фотографических изображениях с низким заполнением стегоконтейнера // Проблемы информационной безопасности. Компьютерные системы. 2022. № 1(49). С. 68–76.
10. Вильховский Д.Э. Метод обнаружения стеганографических вставок, встроенных методом Коха-Жао, в изображениях с низким заполнением стегоконтейнера // Вопросы защиты информации. 2022. №1(136). С. 38–42.
11. Вильховский Д.Э. Обзор методов стеганографического анализа изображений в работах зарубежных авторов // Математические структуры и моделирование. 2020. №4(56). С. 75–102.
12. Вильховский Д.Э. Обнаружение LSB-вставок в искусственных цветных изображениях с градиентной заливкой с низким заполнением стегоконтейнера. / Д.Э.Вильховский // Свид. о гос. рег. программы для ЭВМ 2022613002, 01.03.2022. Заявка № 2022611550 от 07.02.2022.
13. Вильховский Д.Э. Обнаружение LSB-вставок в цветных фотографических изображениях с низким заполнением стегоконтейнера. / Д.Э. Вильховский // Свид. о гос. рег. программы для ЭВМ 2022613021, 01.03.2022. Заявка № 2022611592 от 07.02.2022.
14. Вильховский Д.Э. Обнаружение стеганографических вставок, встроенных методом Коха-Жао, в изображениях с низким заполнением стегоконтейнера. / Д.Э. Вильховский // Свид. о гос. рег. программы для ЭВМ 2022613003, 01.03.2022. Заявка № 2022611548 от 07.02.2022.
15. Вильховский Д.Э. Стеганографический анализ изображений на предмет обнаружения вставок, выполненных методом Коха-Жао // В сборнике: Математическое и компьютерное моделирование. Сборник материалов IX

Международной научной конференции, посвященной 85-летию профессора В.И. Потапова. Омск, 2021. С. 319-321.

16. Вильховский Д.Э. Стеганографический анализ искусственных изображений на предмет обнаружения LSB-вставок // В сборнике: Математическое и компьютерное моделирование. Сборник материалов IX Международной научной конференции, посвященной 85-летию профессора В.И. Потапова. Омск, 2021. С. 316-318.
17. Вильховский Д.Э. Стегоаналитический комплекс для работы с изображениями с низкой стегонагрузкой // Сборник избранных статей научной сессии ТУСУР. 2023. № 1-3. С. 42–46.
18. Вильховский Д.Э., Гуц, А.К. Метод обнаружения LSB-вставок в искусственных цветных изображениях с градиентной заливкой с низким заполнением стегоконтейнера // Вестник УрФО. Безопасность в информационной сфере. 2022. № 1 (43). С. 43-49.
19. Гибадуллин Р.Ф., Вершинин И.С., Райхлин В.А. Стегостойкость и вычислительная стойкость ассоциативной стеганографии // В сборнике: Методы моделирования - VII. Труды Республиканского научного семинара «Методы моделирования». Под редакцией В.А. Райхлина. 2019. С. 23-38.
20. 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.
21. Жилкин М.Ю. Стегоанализ графических данных в различных форматах // Доклады ТУСУРа. 2008. № 2 (18), часть 1. С. 63-64.
22. Загоруйко Н.Г. Прикладные методы анализа данных и знаний // Новосибирск: ИМ СО РАН. 1999. 270 с.

23. Кустов В.Н., Грохотов А.И., Головков Е.В. Имитационная программная модель HUGO стегосистемы // Интеллектуальные технологии на транспорте. 2021. № 4 (28). С. 46-56.
24. Кустов В.Н., Грохотов А.И., Головков Е.В. Программная модель маскировки скрытого сообщения в задачах стеганографии // Интеллектуальные технологии на транспорте. 2022. № 1 (29). С. 45-57.
25. Кустов В.Н., Краснов А.Г. Помехоустойчивое кодирование и высоко необнаруживаемые стегосистемы – успешен ли альянс? // Проблемы информационной безопасности. Компьютерные системы. 2021. № 3. С. 44-54.
26. Кустов В.Н., Процко Д.К. Комплексный подход к стеганографической передаче данных // Защита информации. Инсайд. 2019. № 2 (86). С. 66-73.
27. Монарев В. А. Сдвиговый метод обнаружения скрытой информации // Вестник СибГУТИ. 2012. № 4. С. 62-68.
28. Райхлин В.А., Вершинин И.С., Гибадуллин Р.Ф. Обоснование принципов ассоциативной стеганографии // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2015. Т. 71. № 2. С. 110-119.
29. Райхлин В.А., Вершинин И.С., Гибадуллин Р.Ф. Элементы содержательной теории ассоциативной стеганографии // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2019. № 1. С. 41-47.
30. Рублёв Д.П., Федоров В.М., Макаревич О.Б., Бабенко Л.К. Метод встраивания данных в аудиопоток на основе преобразования фазовых составляющих // Информационное противодействие угрозам терроризма. 2005. № 4. С. 164-170.
31. Шакурский М.В. Двухкомпонентная стеганографическая система встраивания информации в младшие биты звукового сигнала // Проблемы информационной безопасности. Компьютерные системы. 2021. № 4. С. 72-78.

32. Шакурский М.В. Метод встраивания информации в младшие биты растровых изображений без сжатия, использующий двухкомпонентный контейнер // Вопросы защиты информации. 2020. № 2 (129). С. 3-7.
33. Штеренберг С.И., Красов А.В. Разработка методики построения доверенной среды на основе скрытого программного агента. часть 1. Исследование // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 14-20.
34. Штеренберг С.И., Красов А.В. Разработка методики построения доверенной среды на основе скрытого программного агента. часть 2. тестирование и оценка эффективности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 3. С. 3-8.
35. Штеренберг С.И., Красов А.В. Разработка методики построения доверенной среды на основе скрытого программного агента. часть 3. принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 34-40
36. 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.
37. Acharyya A, De M., Subhas C., Pandit S. Variations of largest rectangle recognition amidst a bichromatic point set // Discrete Applied Mathematics. Vol 286. 2020, Pp. 35-50.
38. Adelson E. Digital Signal Encoding and Decoding BApparatus. – U.S. Patent. – No. 4,939515 (1990).
39. 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.

40. Alok A., Subhash S. Fast algorithms for computing the largest empty rectangle // Proc. 3rd Annu. Symposium on Computational Geometry, 1987. Pp. 278–290.
41. Avcibas I., Memon N., Sankur B. Image steganalysis with binary similarity measures // Proceedings of IEEE Int. Conference on Image Processing. 2002. P. 645-648.
42. 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.
43. Avcibas I., Memon N., Sankur B. Steganalysis using image quality metrics // IEEE transactions on Image Processing. 2003. V.12(2). P. 221-229.
44. Avcibaş I., Kharrazi M., Memon N., Sankur B. Image Steganalysis with Binary Similarity Measures // EURASIP Journal on Applied Signal Processing 2005. P. 2749–2757.
45. Bahaghighat M., Motamedi, S.A., Xin, Q. Image Transmission over Cognitive Radio Networks for Smart Grid Applications // Appl. Sci. 2019. *9*. 5498
46. Barni, M. Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications / M. Barni, F. Bartolini. – New York: Marcel Dekker, 2004. – 446 p.
47. 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.
48. 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.
49. 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.

50. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun. 2019. 70. P. 233–245.
51. 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.
52. Chaumont M. Deep learning in steganography and steganalysis // In Digital Media Steganography, Academic Press. 2020. P. 321–349.
53. Chazelle B., Drysdale R. L., Lee D. T. Computing the largest empty rectangle // STACS. Vol. 166. 1984. Pp. 43–54.
54. Cheddad A. Digital image steganography: Survey and analysis of current methods // Signal processing. 2010. V. 90(3). P. 727-752.
55. 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.
56. Chen M, Boroumand M, Fridrich J (2018) Deep learning regressors for quantitative steganalysis // Electron Imaging. 2018. 7. P. 160–161.
57. Chen X. Detect LSB steganography with bit plane randomness tests // Proceedings of IEEE World Congress on Intelligent Control and Automation. 2006. P. 10306-10309.
58. 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]
59. 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.
60. Deng Q.L. The blind detection of information hiding in color image // Computer Engineering and Technology (ICCET). 2010. V. 7. P. 346-348.

61. 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.
62. 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.
63. Dumitrescu S., Wu X. A new framework of LSB steganalysis of Digital Media // IEEE Trans. Signal Processing. 2005. V. 53(10). P. 3936-3947.
64. Dumitrescu S., Wu X. Steganalysis of LSB embedding in multimedia signals // Proceedings of IEEE ICME. 2002, P. 581- 584.
65. 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.
66. 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
67. 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]
68. 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.
69. 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.
70. Fridrich J., and Goljan M. Practical steganalysis of digital images-state of the art // Proceedings of SPIE. 2002. V. 4675.
71. 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.

72. 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.
73. 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.
74. 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.
75. 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.
76. Garna J., Brazdil P. Linear tree // Intelligent Data Analysis. 1999. P. 1-22.
77. Geron A. Hands-on machine learning with Scikit-Learn, Keras, and Tensorflow concepts, tools, and techniques to build intelligent systems. – O'Relly Media, Inc. – 2019. – 1040 p.
78. 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.
79. Hempstalk K. Hiding Behind Corners: Using edges in images for better steganography // Proceedings of Computing Women's Congress. 2006.
80. Johnson N., Jajodia S. Steganalysis: The Investigation of Hidden Information // Proceedings of the IEEE Information Technology Conference. 1998.
81. 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
82. 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]

83. Koch E., Zhao J. Towards robust and hidden image copyright labeling // IEEE Workshop on Nonlinear Signal and Image Processing. 1995. P. 452-455.
84. Kodovsky J., Fridrich J. Quantitative structural steganalysis of Jsteg // IEEE Transactions on Information Forensics and Security. 2010. V. 5(4). 681-693.
85. 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.
86. 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.
87. 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]
88. 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.
89. 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.
90. Lie W., Lin G. A feature based classification technique for blind image steganalysis // IEEE Trans. Multimedia. 2005. V. 7(6). P. 1007-1020.
91. Lin E., Woertz E., Kam M. LSB steganalysis using support vector regression // Proceedings of IEEE, SMC Information Assurance Workshop. 2004. P. 95-100.
92. 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.
93. 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.

94.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.

95.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.

96.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.

97.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.

98.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.

99.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.

100.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).

101.Marvel L., Henz B., Boncelet C. A performance study of±1 steganalysis employing a realistic operating scenario // Military Communications Conference, 2007. MILCOM. IEEE. 2007.

102.Miche Y. A feature selection methodology for steganalysis // International Workshop on Multimedia Content Representation, Classification and Security. Berlin Heidelberg. 2006.

103.Mielikainen J. LSB matching revisited // IEEE Signal Processing Letters. 2006. V. 13(5), P. 285-287.

104.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.

105.Naamad A., Lee D. T., Hsu W.-L. On the Maximum Empty Rectangle Problem // Discrete Applied Mathematics, 1984. Pp. 267–277.

106.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.

107.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.

108.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.

109.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.

110.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).

111.Provos N., Honeyman P. Detecting steganographic content on the internet // Technical Report CITI 01-1a, University of Michigan. 2001.

112.Quinlan J.R. C4.5: Programs for Machine Learning // Morgan Kaufmann, San Mateo, CA. 1993.

113.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.

114.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.

115.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.

116.Sarkar, A., Biswas, A., Dutt, M., Bhattacharya, A. Finding a largest rectangle inside a digital object and rectangularization // Journal of Computer and System Sciences. Vol 95. 2018. Pp. 204-217.

117.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.

118.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]

119.Sharp T. An implementation of key-based digital signal steganography // Proceedings of the 4th Information Hiding Workshop. 2001. V. 2137, P. 13-26.

120.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.

121.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.

122.Simmons G. J. The prisoners' problem and the subliminal channel // Proceedings of CRYPTO'83. 1983. P. 51-67.

123.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.

124.Siwei L.,Farid H. Steganalysis using higher-order image statistics // IEEE transactions on Information Forensics and Security. 2006. V 1(1). P. 111-119.

125.Smola A.J., Scholkopf B. A tutorial on support vector regression // Tech. Rep. NC2-TR-1998 030. 1998.

126.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]

127.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.

128.Subhas C. Nardy, Bhargab B. Bhattacharya. Location of Largest Empty Rectangle among Arbitrary Obstacles // Foundations of Software Technology and Theoretical Computer Science. Vol.880. 1994. Pp.10-28.

129.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.

130.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.

131.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.

132.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.

133. Vilkhovskiy D. E. Steganalysis for LSB inserts in low stego-payload artificial color images // J. Phys.: Conf. Ser. 2022. V 2182. DOI: 10.1088/1742-6596/2182/1/012102.
134. Vilkhovskiy D. E. Steganalysis for DCT inserts with the Koch-Zhao steganographic method in low stego-payload images // J. Phys.: Conf. Ser. *2022. V* 2182. DOI: 10.1088/1742-6596/2182/1/012101.
135. Wang Y., Moulin P. Optimized feature extraction for learning based image steganalysis // IEEE Trans Inf Forensics Security. 2005. V 2(1). P. 262-277.
136. 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.
137. Westfeld A. F5-a steganographic algorithm: high capacity despite better steganalysis // Proceedings of the 4th Information Hiding Workshop. 2001. V. 2137. P. 289-302.
138. 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.
139. Westfield A. Detecting low embedding rates // Proceedings of Int. Workshop on Information Hiding. LNCS 2578. 2003. P. 324-339.
140. Westfield A., Pfitzmann A. Attacks on steganographic systems // Proceedings of Int. Workshop on Information Hiding, LNCS 1768. 2000. P. 61-75.
141. 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.
142. 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.
143. 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.

144.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.

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

146.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.

147.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.

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

149.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.

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

151.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.

152.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.

153.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.

154.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.

155.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.

156.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.

157.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 №2022613002

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022613002

Обнаружение LSB-вставок в искусственных цветных изображениях с градиентной заливкой с низким заполнением стегоконтейнера

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

Автор(ы): ***Вильховский Данил Эдуардович (RU)***

Заявка № **2022611550**
Дата поступления **07 февраля 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***01 марта 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

Приложение 2: Свидетельство о государственной регистрации программы для ЭВМ №2022613021

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022613021

Обнаружение LSB-вставок в цветных фотографических изображениях с низким заполнением стегоконтейнера

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

Автор(ы): ***Вильховский Данил Эдуардович (RU)***

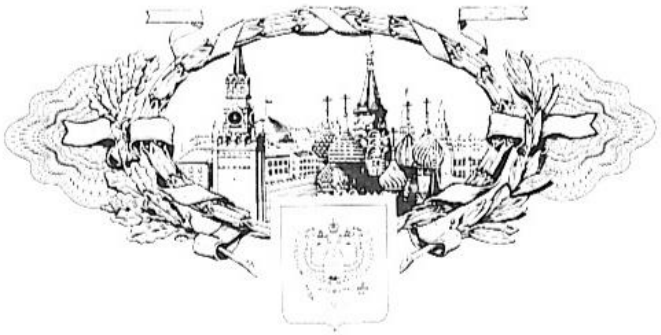
Заявка № **2022611592**
Дата поступления **07 февраля 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***01 марта 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

Приложение 3: Свидетельство о государственной регистрации программы для ЭВМ №2022613003

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022613003

Обнаружение стеганографических вставок, встроенных методом Коха-Жао, в изображениях с низким заполнением стегоконтейнера

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

Автор(ы): ***Вильховский Данил Эдуардович (RU)***

Заявка № **2022611548**

Дата поступления **07 февраля 2022 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***01 марта 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

Приложение 4: Акт о внедрении результатов диссертационного исследования в систему документооборота 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

№ 23 «16» февраля 2022 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 Д.Э. Вильховского «Алгоритмы стеганографического анализа изображений с низким заполнением стегоконтейнера» и разработанный программный комплекс, позволяющий осуществлять стегоанализ изображений на предмет наличия встраиваний, выполненных методом LSB-замены и методом Коха-Жао, а также локализации области встраивания, внедрены во внутреннюю систему документооборота ООО Строительно-монтажный трест «Стройбетон».

Программный комплекс представляет собой веб-приложение с микросервисной архитектурой. Взаимодействует через GET/POST запросы. В качестве входных данных принимает URL изображения или непосредственно изображение, переведенное в формат base64. На выходе возвращает json файл, содержащий следующие данные:

- результат классификации изображения (чистое/стего),
- параметры встраивания и область его локализации,
- извлеченное сообщение,

- модифицированное изображение в формате base64, не содержащее стеганографической вставки.

Интеграция с системой документооборота осуществлена через реализацию хуков приложения, вызов которых осуществляется в следующих случаях:

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

Практическим ценностным результатом внедрения обозначенного выше программного комплекса в систему документооборота ООО Строительно-монтажный трест «Стройбетон» является значительное повышение ее функциональности: добавлена функция стеганографического анализа базы данных изображений, хранящихся в системе.

Внедрение результатов позволило существенно увеличить уровень информационной защиты внутреннего документооборота организации, своевременно и эффективно отслеживать формирование скрытого канала передачи данных, блокировать несанкционированную передачу данных, предназначенных исключительно для внутреннего пользования и затрагивающие информационную и экономическую безопасность организации.

Председатель комиссии _____ Дремов К.В.

Члены комиссии:

_____ Сасин А.С.

_____ Луценко Н.И.

Приложение 5: Акт о внедрении результатов диссертационного исследования в систему документооборота ООО «РЕЙЛСТРОЙ-1520»

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬ «РЕЙЛСТРОЙ-1520»
ИНН/КПП 5504163645/550401001
ЮРИДИЧЕСКИЙ АДРЕС: РОССИЯ, 644024, Г. ОМСК,
УЛ. КУЙБЫШЕВА Д. 56, ПОМЕЩЕНИЕ 9П, ОФИС 4
☎ +7 (3812) 395-002, + 7 (995) 394-25-10
@ SALES@RS-1520.RU

04.02.2022 № 16
На №_____

АКТ
о внедрении результатов диссертационной работы Д.Э. Вильховского,
представленной на соискание ученой степени кандидата технических наук,
в документооборот Общества с ограниченной ответственностью «Рейлстрой-1520»

Настоящий акт составлен в том, что при совершенствовании системы документооборота Общества с ограниченной ответственностью «Рейлстрой-1520» (далее – ООО «Рейлстрой-1520»), были внедрены следующие результаты диссертационной работы Д.Э. Вильховского:

- Алгоритм обнаружения и локализации LSB-вставок в цветных искусственных изображениях с градиентной заливкой с низким заполнением стегоконтейнера;
- Алгоритм обнаружения и локализации LSB-вставок в цветных фотографических изображениях с низким заполнением стегоконтейнера;
- Алгоритм обнаружения и локализации вставок, выполненных методом Коха-Жао в изображениях с низким заполнением стегоконтейнера.

Внедрение указанных выше алгоритмов было осуществлено в виде интеграции в систему документооборота ООО «Рейлстрой-1520» программного комплекса, разработанного Д.Э. Вильховским и реализующего данные алгоритмы.

Значимой особенностью разработанного Д.Э. Вильховским программного комплекса является его быстродействие и возможность проверки фотографических и искусственных изображений как путем непосредственной загрузки изображения в программу, так и путем отправки запроса, содержащего изображений, выполненного из любой другой программы, а также посредством передачи URL изображения.

Также, одним из ценностных аспектов разработанных алгоритмов и созданного на их основе программного комплекса, внедренного и реализуемого в настоящее время в ООО «Рейлстрой-1520», является получение стабильных результатов при сравнительно небольших объемах встраивания. Так, алгоритмы обнаружения LSB-вставок успешно справляются с поставленной задачей при объемах встраивания от 25%, при этом, программный комплекс способен распознать и локализовать область встраивания, выполненного методом Коха-Жао, размер которого составляет всего 10% от общего объема изображения. Данная характеристика говорит о высокой эффективности и надежности программного комплекса, разработанного Д.Э. Вильховским, и является одним из аспектов технико-экономического обоснования целесообразности внедрения данного программного комплекса в систему документооборота ООО «Рейлстрой-1520».

Генеральный директор К.Ю. Щербаков

Исполнитель: Курганов Б.Б.
Тел. + 7 (3812) 395-002 (доб. 704)

Приложение 6: Акт о внедрении в учебный процесс

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования
«**Омский государственный университет им. Ф.М. Достоевского**»

Утверждаю
Проректор по учебной работе
ФГАОУ ВО «Омский государственный университет им. Ф.М. Достоевского»
к.т.н., доц.
_____ Б.Е. Кадлубович
«30» 06. 2022 2022 г.

АКТ

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

Настоящий акт составлен о том, что в учебный процесс Омского государственного университета им. Ф.М. Достоевского (ОмГУ) внедрены и используются следующие результаты диссертационной работы Вильховского Данила Эдуардовича:

1. Алгоритм стеганографического анализа метода LSB-замены в цветных искусственных изображениях с градиентной заливкой с низким заполнением стегоконтейнера, основанный на анализе бинарной матрицы комбинаций пикселей нулевого слоя
2. Алгоритм стеганографического анализа метода LSB-замены в цветных фотографических изображениях с низким заполнением стегоконтейнера, основанный на сравнительном анализе нулевого и первого слоев изображения с применением рекурсивного фильтра и использованием моментов изображения
3. Алгоритм стеганографического анализа метода Коха-Жао в цветных и черно-белых изображениях, основанный на анализе сигнатур, получаемых на основе коэффициентов дискретного косинусного преобразования, с использованием алгоритма машинного обучения DBSCAN

Указанные алгоритмы используются факультетом компьютерных наук ОмГУ при подготовке бакалавров по направлению 10.03.01 «Информационная безопасность» в по дисциплинам «Анализ уязвимостей программного обеспечения», «Компьютерная экспертиза», а также при обучении студентов 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 2021 года.

По реализации каждого из разработанных алгоритмов на языке программирования Python получены Свидетельства о государственной регистрации программ для ЭВМ, правообладателем которых является Омский государственный университет им Ф.М. Достоевского в соответствии с договором об отчуждении права на программы ЭВМ. Номера регистрации (свидетельств), соответственно: №2022613002 от 01.03.2022, №2022613021 от 01.03.2022, №2022613003 от 01.03.2022.

Заведующий кафедрой
информационной безопасности ОмГУ,
к.ю.н., доцент _____ А.И. Горев

100622