На правах рукописи

Абасова Анастасия Михайловна

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА ВНЕДРЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ЦВЕТНОЕ ИЗОБРАЖЕНИЕ НА БАЗЕ МОРФОЛОГИЧЕСКОГО АНАЛИЗА И МОДУЛЯРНОЙ АРИФМЕТИКИ ДЛЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ХИЩЕНИЯ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Специальность 05.13.19 - Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Таганрог - 2018

Работа выполнена на кафедре безопасности информационных технологий Института компьютерных технологий и информационной безопасности Федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет»

Научный руководитель: **Бабенко Людмила Климентьевна**
доктор технических наук, профессор, ФГАОУ ВО «Южный федеральный университет», кафедра Безопасности информационных технологий, профессор

Официальные оппоненты: **Шагрова Галина Вячеславовна**
доктор физико-математических наук, профессор, ФГАОУ ВО «Северо-Кавказский федеральный университет», кафедра Информационных систем и технологий, профессор

Резеньков Денис Николаевич
кандидат технических наук, доцент, ФГБОУ ВО «Ставропольский государственный аграрный университет», кафедра Информационных систем, доцент

Ведущая организация: ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», г. Самара

Защита состоится 1 июня 2018 г. в 12.00 на заседании диссертационного совета Д 212.208.25 при Южном федеральном университете по адресу: 347922, Ростовская область, г. Таганрог, ул. Чехова, 2, ауд. И-409.

С диссертацией можно ознакомиться в Зональной научной библиотеке ЮФУ по адресу: 344090, г. Ростов-на-Дону, ул. Зорге 21-ж.

Диссертация в электронном виде доступна по адресу
http://hub.sfedu.ru/diss/announcements/actions/edit/bce7804f-d41d-4ea4-816c-64ab370a75a5/

Автореферат разослан «24» марта 2018 года

Ученый секретарь
диссертационного совета  Ю.А. Брюхомицкий

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В настоящее время, в связи с развитием цифровых технологий, широким распространением частных издательств, типографий, рекламных агентств, средств массовой информации наблюдается рост нарушений авторских прав, в том числе на изображения (фотографии, рекламные постеры и др.). Авторское право на произведение появляется сразу после его создания, однако когда изображение обнародовано, автор практически теряет контроль над возможным несанкционированным использованием его, так как для злоумышленника не составляет трудности выполнить копирование и распространение данных объектов вне зоны авторского контроля. Копирование цифрового изображения не сказывается на его качестве, что позволяет получить неограниченное количество экземпляров.

В случае нарушения авторских прав у законного владельца есть только два способа решить возникшую проблему – внесудебное решение вопроса (неофициально) либо судебное разбирательство. При разрешении такой ситуации в суде, необходимы особые усилия истца и множество времени. Более того, необходимо доказать авторство и выявить сам факт нарушения авторского права, то есть размещение цифрового изображения без согласия автора в информационной среде. В случае успешного доказательства данных фактов автор имеет право требовать за каждый факт нарушения авторских прав компенсацию, установленную Гражданским кодексом Российской Федерации.

Для закрепления авторских прав не требуется регистрация объекта интеллектуальной собственности – оно возникает по факту его создания. Однако, с учетом практики рассмотрения дел в судах, в качестве доказательной базы и дополнительной защиты автору необходимо обеспечить доказательство наличия авторских прав на конкретный объект на определенную дату, что можно реализовать с помощью организационных или технических методов. Автор или другой обладатель авторских прав оповещает о них, применяя специальный знак охраны авторских прав, который размещается на каждой копии произведения.

В случае если объектом авторского права является изображение, то четкий и ясно видимый знак охраны авторских прав обычно располагается в месте, где он не будет мешать восприятию изображения. Однако в случае его удаления существенные изменения изображения также не произойдут, что создает предпосылки и возможности для его незаконного использования.

В настоящее время активно используется внедрение в изображение невидимых цифровых водяных знаков (далее – ЦВЗ), содержащих информацию о правообладателе. Использование ЦВЗ позволяет сократить потери от угроз хищения, в том числе незаконного копирования, использования изображений,

являющихся объектами интеллектуальной собственности, тем самым обеспечивает защиту авторских прав.

Существенный вклад в развитие и изучение использования стеганографии и ЦВЗ внесли многие российские и зарубежные ученые: М. Барни, Ф. Бартолини, Р. Бергман, В.Г. Грибунин, В.А. Митекин, Н. Мемон, И.Н. Оков, Б.Я. Рябко, И.В. Туринцев, А.Н. Фионов, Дж. Фридрич и др.

Существующие методы встраивания ЦВЗ в цифровое изображение, предложенные и рассмотренные упомянутыми авторами, достаточно эффективны, однако не всегда обеспечивают высокую устойчивость ЦВЗ к широкому спектру деструктивных воздействий с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ.

В связи с вышеизложенным, необходимость в разработке метода внедрения ЦВЗ в изображение, устойчивого к различным деструктивным воздействиям, для повышения эффективности защиты от угроз хищения объектов интеллектуальной собственности является актуальной научной задачей.

Объект исследования. Методы защиты объектов интеллектуальной собственности от угроз хищения.

Предмет исследования. Метод внедрения и структура ЦВЗ для цифрового изображения, как объекта интеллектуальной собственности.

Цель исследования. Повышение эффективности защиты цифрового изображения, как объекта интеллектуальной собственности, от угроз хищения за счет внедрения в него ЦВЗ авторской разработки.

В соответствии с целью были поставлены **задачи диссертационной работы**:

– провести анализ основных правовых аспектов доказательства прав собственности на изображение, решений по противодействию угрозам хищения объектов интеллектуальной собственности, а также существующих деструктивных воздействий на системы ЦВЗ;

– разработать метод защиты цифрового изображения, основанный на внедрении ЦВЗ в изображение, отличающийся новой структурой ЦВЗ и оригинальным алгоритмом внедрения ЦВЗ в изображение, обеспечивающий эффективную защиту изображения от угроз хищения;

– разработать структуру ЦВЗ на основе математического аппарата модулярной арифметики, позволяющую обеспечить его целостность при различных деструктивных воздействиях;

– разработать алгоритм внедрения ЦВЗ в изображение на базе морфологического анализа, позволяющий осуществлять запись бит в значимые области цифрового изображения;

– разработать алгоритм извлечения внедренного ЦВЗ после возможных деструктивных преобразований изображения с ЦВЗ с целью доказательства авторских прав;

– разработать программное обеспечение для реализации предложенного метода внедрения ЦВЗ в изображение и извлечения внедренного ЦВЗ после возможных деструктивных преобразований изображения с ЦВЗ с целью доказательства авторских прав.

Научная новизна работы. В диссертационной работе получены следующие результаты, характеризующиеся научной новизной:

– разработан метод внедрения ЦВЗ в изображение, отличающийся новой структурой ЦВЗ и оригинальным алгоритмом внедрения ЦВЗ в изображение, обеспечивающий более эффективную защиту изображения от угроз хищения;

– разработан новый алгоритм внедрения ЦВЗ, осуществляющий внедрение бит в цифровое изображение, отличающийся от известных использованием морфологического анализа, позволяющий определить значимые области для внедрения на основе стего–ключа – примитива особой сложной формы, а также использующий геометрический центр объекта (центроид) переднего плана как точку отсчета при нелинейном заполнении бит изображения;

– разработан алгоритм извлечения внедренного ЦВЗ после возможных деструктивных преобразований изображения с ЦВЗ с целью доказательства авторских прав;

– разработана структура ЦВЗ, отличающаяся от ранее существующих использованием математического аппарата модулярной арифметики, позволяющего повысить его целостность при различных деструктивных воздействиях.

Теоретическая значимость работы заключается в обосновании применимости математического аппарата модулярной арифметики и морфологического анализа, разработке нового метода внедрения ЦВЗ, структуры ЦВЗ и алгоритмов внедрения и извлечения ЦВЗ, что позволяет повысить эффективность защиты от угроз хищения изображения, являющимся объектом интеллектуальной собственности**.**

Практическая значимость работы. В диссертации получены следующие, характеризующиеся практической значимостью, результаты:

– разработанные метод внедрения ЦВЗ, структура ЦВЗ и алгоритмы внедрения и извлечения ЦВЗ могут использоваться при создании средств защиты авторских прав цифрового изображения как объекта интеллектуальной собственности от угроз хищения;

– разработанное программное обеспечение для реализации предложенного

метода внедрения ЦВЗ в изображение для предотвращения хищения объектов интеллектуальной собственности с целью доказательства авторских прав может использоваться в различных системах обработки и передачи изображений для большинства графических форматов данных PNG, BMP, TIFF и др.

Результаты диссертации использованы в работе ПАО «Совкомбанк» при обеспечении дополнительной защиты авторских прав банка (изображения – разрабатываемые рекламные постеры, в том числе до момента официального опубликования).

Методология и методы исследования.

Методология исследования заключается в поэтапном изучении состояния области научных исследований и разработок в части обеспечения защиты от угроз хищения цифровых изображений - объектов интеллектуальной собственности, в проведении теоретического анализа научной литературы, в разработке научно обоснованного метода внедрения ЦВЗ в изображение, повышающего эффективность защиты от угроз хищения объектов интеллектуальной собственности.

Среди методов исследования выделяются: теория компьютерной стеганографии, математической морфологии, аппараты модулярной арифметики, методы и приемы объектно-ориентированного и логического программирования.

Положения, выносимые на защиту:

– метод внедрения ЦВЗ в изображение, который повышает эффективность защиты от угроз хищения объектов интеллектуальной собственности, отличается новой структурой ЦВЗ, построенной на основе аппарата модулярной арифметики и оригинальным алгоритмом внедрения ЦВЗ в изображение, основанным на морфологической обработке изображения, который позволяет осуществить нелинейное внедрение бит в значимые области цифрового изображения;

– результаты проведенных экспериментальных исследований, выполненных с помощью разработанного программного обеспечения для реализации предложенного метода внедрения ЦВЗ в изображение и извлечения ЦВЗ из изображения, показывают высокую эффективность.

Степень достоверности и апробация результатов. Достоверность исследования подтверждается проведенными экспериментами с помощью разработанного программного обеспечения для реализации предложенного метода внедрения ЦВЗ в изображение и извлечения ЦВЗ из изображения и тестовой группы цифровых изображений.

Основные результаты диссертации были представлены на следующих российских и международных конференциях:

– XVII Всероссийская научно-техническая конференция студентов,

молодых ученых и специалистов «Новые информационные технологии в научных исследованиях» (Рязань, 2012);

– XIII Международная научно-практическая конференция «Информационная безопасность – 2013» (Таганрог, 2013);

– IV Всероссийская молодежная конференция по проблемам информационной безопасности «Перспектива – 2014» (Таганрог, 2014);

– VI Международная научно-техническая конференция «Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6)» (Ставрополь, 2014).

По материалам диссертационной работы опубликовано 7 научных работ, из них 2 статьи в журналах из перечня ведущих рецензируемых научных журналов и изданий, рекомендованных ВАК, получено 2 свидетельства об официальной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, 4 глав, заключения, изложенных на 133 листах машинописного текста, содержит 74 рисунка и 14 таблиц. Список литературы включает 102 наименования.

В приложениях к диссертационной работе приведены свидетельства о государственной регистрации программ для ЭВМ.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы, формулируются цели исследования и основные результаты, которые выносятся на защиту, обосновывается научная и практическая значимость выполненного исследования.

В **первой главе** приводятся основные понятия цифрового изображения, его характеристики, описаны цветовые модели и форматы хранения изображений. Цифровые изображения, а также аудио/видео-произведения обладают повышенным риском нарушения авторского права, т.к. данные объекты интеллектуальной собственности широко представлены в Интернете и для злоумышленника не составляет трудности выполнить копирование и распространение данных объектов вне зоны авторского контроля, в связи с чем целесообразно рассмотреть возможность обеспечения защиты изображения как объекта интеллектуальной собственности от угроз хищения.

Описаны правовые аспекты доказательства прав собственности на изображение. Доказано, что изображение является объектом интеллектуальной собственности, так как является частным случаем аудиовизуального произведения, в котором отсутствует сопровождение звуком. Рассмотрена возможность обеспечить защиту изображения – объекта интеллектуальной собственности от угроз хищения при предоставлении доказательств прав

собственности на изображение, которое можно реализовать с помощью организационных и технических/программных методов.

В главе рассмотрены организационные методы защиты авторских прав, основной целью которых является фиксация даты создания объекта интеллектуальной собственности:

- депонирование объекта в юридической компании;
- получение нотариального удостоверения даты создания объекта;
- отправка готового произведения по почте на собственный адрес.

Однако, данные методы зачастую неприемлемы при регистрации цифровых документов, которые далеко не всегда можно распечатать, а также не фиксируют факт создания объекта интеллектуальной собственности конкретным автором.

Из технических/программных методов были рассмотрены:

- методы, в которых предусматривается наличие подписи, указывающей на автора или правообладателя (использование электронной подписи);
- методы, в которых предусматривается наличие скрытой подписи.

Недостатком использования электронной подписи является сравнительно высокая стоимость сертифицированного программного обеспечения, а также тот факт, что при копировании цифрового изображения электронная подпись может быть легко удалена. Еще одним недостатком является то, что при осуществлении деструктивных воздействий на изображение и при искажении копии электронная подпись может быть не распознана.

Перспективным направлением является использование стеганографии, а именно ЦВЗ за счет сравнительно невысокой стоимости и невидимости самого цифрового знака для злоумышленника. В главе проанализированы существующие методы внедрения ЦВЗ, каждый из которых обладает определенным набором недостатков, которые приводят к тому, что применение алгоритмов, обеспечивающих защиту цифрового изображения от угроз хищения, на основе этих методов становится недостаточно эффективным. На основании этого сделан вывод о необходимости разработки новых решений по обеспечению защиты цифрового изображения от угроз хищения интеллектуальной собственности, а именно разработке метода обеспечения внедрения ЦВЗ, повышающего устойчивость к деструктивным воздействиям на системы ЦВЗ с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ (отсутствие необходимости наличия исходного изображения).

Проанализированы деструктивные воздействия на системы ЦВЗ при изменении параметров изображения: изменение яркости и контрастности; смена формата на JPEG, BMP, TIFF, PNG, GIFF; вычеркивание строк и столбцов на изображении, поворот изображения, сдвиг по горизонтали и вертикали, перемещение или замена части изображения; удаление части изображения.

Рассмотрены существующие методы противодействия деструктивным воздействиям для их учета при разработке алгоритма внедрения ЦВЗ. С учетом большого разнообразия видов проанализированных деструктивных воздействий на системы ЦВЗ предложено использовать математический аппарат модулярной арифметики, позволяющий выявлять и корректировать различного рода искажения, возникающие в результате деструктивных воздействий, оказываемых на информацию, при невысокой избыточности, для формирования структуры ЦВЗ независимо от формы его представления, позволяющей распределенно внедрить его в изображение, что делает его извлечение вероятнее и значительно увеличивает шансы извлечения при удалении части изображения.

Рассмотрены методы морфологической обработки изображений, которые, широко и эффективно используются для решения множества аналитических задач, связанных с изображениями и видео контентом, однако до настоящего времени они не применялись для решения задач в области компьютерной стеганографии. С точки зрения вычислительной простоты по сравнению с классическими методами (сегментацией изображения) предложено использовать методы математической морфологии для определения блоков (объектов/группы пикселей) для внедрения ЦВЗ в изображение.

Во **второй главе** разработан метод внедрения ЦВЗ на базе морфологической обработки изображения, в рамках которого предложено для внедрения ЦВЗ использовать пиксели изображения-контейнера, принадлежащие объектам переднего плана. Такое решение обосновано тем, что при умышленном удалении частей изображения, злоумышленник вынужден не затрагивать объекты переднего плана, существенные для правильного визуального восприятия изображения.

Для формирования матрицы с координатами для внедрения ЦВЗ было предложено вычислять маркеры переднего плана изображений с использованием стего–ключа (структурного элемента – примитива особой сложной формы), так как данная операция обладает меньшей вычислительной сложностью, в отличие от сегментации изображения, более того при сегментации обнаруживаются четкие контуры объектов (для разных алгоритмов границы объектов могут отличаться), что позволит злоумышленнику легко обнаружить объект для внедрения ЦВЗ, зная алгоритм.

Пусть $\mathrm{I}(\mathrm{x},\mathrm{y})$ – исходное изображение-контейнер, $\mathrm{I}'(\mathrm{x},\mathrm{y})$ – исходное изображение-контейнер, преобразованное в полутоновое, $\mathrm{b}(\mathrm{x},\mathrm{y})$ – структурный элемент или примитив (размера $g \times h$, причем будем считать, что $g = 2a_1 + 1$ и $h = 2a_2 + 1$, где a_1, a_2 – неотрицательные целые числа), который также является цифровым изображением меньшего чем $\mathrm{I}'(\mathrm{x},\mathrm{y})$ размера, I' и b соотносят значение яркости каждой группе координат.

Полутоновая дилатация I' по структурному элементу b отмечается как $I' \oplus b$ и определяется как:

$$(I' \oplus b)(s,t) = \max\{I'(s-x,t-y) + b(x,y) | (s-x,t-y) \in D_{I'}; (x,y) \in D_b\} \quad (1)$$

где $D_{I'}$, D_b – области определения I', b соответственно, s – сдвиг по координате x равный a_1, t - сдвиг по координате y равный a_2.

Полутоновая эрозия I' по примитиву b, отмечается $I' \ominus b$, определяется как:

$$(I' \ominus b)(s,t) = \min\{I'(s+x,t+y) - b(x,y) | (s+x,t+y) \in D_{I'}; (x,y) \in D_b\}. \quad (2)$$

Ограничение, указывающее, что координатам (s-x) и (t-y) / $(s+x)$ и $(t+y)$ необходимо состоять в области определения I', а x и y - в области определения b, подобно определению двоичной дилатации/эрозии, которое устанавливает, что два множества должны пересекаться хотя бы в одном элементе (для дилатации) или структурный элемент должен находиться внутри исходного множества (для эрозии).

Операции дилатации и эрозии являются ключевыми при выполнении морфологического размыкания и замыкания. На практике размыкание, как правило, применяется для удаления небольших (по сравнению со структурным элементом) светлых деталей, при этом сохраняя общую яркость и крупные яркие детали. Выполняемая на первом этапе эрозия удаляет небольшие объекты, но при этом изображение становится темнее, после чего применяется дилатация, которая восстанавливает общую яркость до прежнего уровня, не восстанавливая объекты, удаленные при эрозии.

На практике замыкание, как правило, применяется для удаления темных объектов на изображении, при небольших изменениях ярких деталей. Выполняемая на первом этапе дилатация удаляет темные объекты, но при этом изображение становится светлее, после чего применяется эрозия, которая уменьшает общую яркость до прежнего уровня, не восстанавливая объекты, удаленные при дилатации.

Полученные маркированные блоки анализируются на предмет их применимости для внедрения информации (ЦВЗ), а именно учитывается их площадь, а также количество. В случае недостаточности количества маркированных блоков переднего плана уменьшается размер структурного элемента, а в случае недостаточности площади маркированных блоков, а именно количества пикселей в данных блоках, размер структурного элемента увеличивается.

ЦВЗ может выступать как последовательность чисел или символов, может быть представлен в виде текста, бинарного изображения с логотипом организации, QR – кода, который может содержать знак охраны авторских прав или ссылку на сайт автора. Независимо от того в каком виде выступает ЦВЗ, он

может быть представлен модулярным кодом так, что при наличии деструктивного воздействия на систему будет возможно обнаружить и скорректировать возникшую ошибку.

Пусть заданы модули - положительные числа, взаимно простые основания системы: $p_1, p_2, \dots, p_i, \dots, p_k$, НОД$(p_1, p_q) = 1$ для $i \neq q$.

Информационный диапазон получившейся системы чисел определяет значение $P = \prod_{i=1}^{k} p_i$. ЦВЗ для текстовых данных это набор чисел, соответствующий каждой цифре/букве/символу согласно выбранной кодировке. Для бинарного изображения/QR-кода это будет матрица чисел, которая получится после преобразования матрицы, состоящей из нулей и единиц в необходимую для обработки форму.

Любой ЦВЗ может быть представлен матрицей положительных целых чисел каждый столбец в которой содержит остатки по соответствующему модулю всех позиционных значений ЦВЗ, а строками являются сами представления позиционных значений в модулярном коде. Каждое неотрицательное целое число A можно описать в виде модулярного кода $A = \{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}$, который содержит натуральные числа, такие что $0 \leq \alpha_i < p_i$, где $i = 1,2, \dots, k$.

Китайская Теорема об остатках, в которой говорится о том, что между целым числом и некоторым множеством целых чисел находится взаимно однозначное соответствие, является фундаментальным положением, которое лежит в основе модулярных вычислений.

Допустим, что основаниями системы будут являться попарно взаимно простые модули $\{p_1, p_2, \dots, p_i, \dots, p_k\}$, и пусть число $A \in Z(P)$, тогда его модулярное представление $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}$ можно определить выражением $\alpha_1 = |A|_{p_i}$, где $i = 1,2, \dots, k$. Отличительной способностью когда, обладающего свойствами обнаружения и исправления ошибок, будет являться присутствие двух диапазонов цифр – информационного $J_A = \{\alpha_1, \alpha_2, \dots, \alpha_i\}$ и контрольного $K_A = \{\alpha_{k+1}, \dots, \alpha_{k+n}\}$. В информационном диапазоне находятся цифры, составляющие числовое значение закодированной величины, а в контрольном диапазоне – цифры, которые введены для обеспечения возможности обнаружения и коррекции ошибок. При этом, контрольный диапазон цифр будет являться избыточным.

Избыточные *R*-коды в остаточных классах с взаимно простыми модулями являются наиболее эффективными и часто используемыми. Избыточный модулярный код (далее – ИМК) может быть задан последовательностью модулей: $\{p_1, p_2, \dots, p_i, \dots, p_{k+1}, p_{k+2}, \dots p_{k+n}\}$, информационным (рабочим) диапазоном P и полным диапазоном с контрольными основаниями $P' = \prod_{i=1}^{k+n} p_i$. В соответствии с тезисами модулярной арифметики, числа должны находиться в диапазоне $[0, P')$. Признаком наличия искажения является выполнение неравенства $A \geq P$.

Ошибкой будем считать какое-либо искажение значения, соответствующего любому из модулей в модулярном представлении числа.

Путем анализа литературных источников для построения системы коррекции искажений в числовом представлении ЦВЗ был выбран способ, основывающийся на методе проекций как наиболее вычислительно простом и эффективном. Алгоритм выявления ошибки заключается в следующем.

1. Вычисление проекции числа $\tilde{A}$ по всем основаниям

$$\widetilde{A_1}, \widetilde{A_2}, \dots, \widetilde{A_i}, \dots, \widetilde{A_k}, \dots, \widetilde{A_{k+2}}. \quad (3)$$

2. Выявление ошибочного (искаженного) основания. Среди данных проекций есть одна $\widetilde{A_i} < \frac{P}{p_{n+1},p_{n+2}}$. Тогда ошибочной является цифра $\widetilde{\alpha_i}$.

3. Исправление ошибочного основания. После того как выявлена ошибочная цифра, ее исправление производится по формуле:

$$\alpha_i = \widetilde{\alpha_i} + \left[\frac{p_i(1+np_{k+1})}{p_{k+1}m_i} - \frac{\tilde{A}}{B_i}\right]. \quad (4)$$

В **третьей главе** разработан алгоритм преобразования ЦВЗ для внедрения в цифровое изображение на основе использования математического аппарата модулярной арифметики для обеспечения целостности ЦВЗ

Входными данными, для работы алгоритма, является ЦВЗ, вне зависимости от формы его представления. Задача, стоящая на начальном этапе, заключается в определении типа ЦВЗ (последовательность чисел или символов/текст/изображение). Далее ЦВЗ преобразуется к виду, пригодному для функционирования алгоритма.

Формируется двоичный массив, группы элементов которого, в зависимости от рабочего диапазона выбранной системы остаточных классов, преобразуются в блоки по *t*-бит. После чего данные блоки подвергаются преобразованию из двоичной системы в десятичную.

На следующем этапе осуществляется процедура преобразования матрицы, элементами которой уже являются цифры в десятичной системе счисления в матрицу, элементами которой являются цифры, представленные избыточным модулярным кодом (далее – ИМК).

В случае если исходной формой ЦВЗ являются текстовые данные, то символы данного вектора могут быть представлены десятичными цифрами в соответствии с заранее определенной кодировкой. В процессе преобразования обязательным критерием вхождения символа в преобразованную матрицу является его принадлежность к рабочему диапазону выбранной системы оснований, то есть принадлежность соответствующего числового значения в десятичной системе счисления диапазону разрешенных значений системы оснований. Как и в случае с изображением, на следующем этапе производится

процедура преобразования матрицы, элементами которой являются цифры в десятичной системе счисления в матрицу, элементами которой будут уже цифры, которые представлены ИМК.

В разработанном программном обеспечении, описанном в главе 4, преобразование из позиционной системы счисления (далее – ПСС) в ИМК будет производиться по шести модулям, два из которых будут избыточными. Для оценки корректирующих способностей кода использовано понятие кодового расстояния, которое обеспечивает связь между избыточностью кодирования и способностью обнаруживать и исправлять ошибки.

Рабочий диапазон выбранной системы равен $P = p_1 p_2 \dots p_n = \prod_{i=1}^{n} p_i = 210$, полный диапазон системы $P' = p_1 p_2 \dots p_n p_{n+1} \dots p_{n+k} = \prod_{i=1}^{n+k} p_i = 30030$, причем $d_{min} = 3$, откуда следует, что обнаруживающая способность кода равна

$$\frac{P'-P}{P} * 100\% = \frac{30030-210}{30030} * 100\% \approx 99{,}3\% . \qquad (5)$$

Таким образом, при наличии двух избыточных оснований возможно обнаружить любые одиночные и двойные ошибки, обнаружить тройные ошибки с вероятностью 99,3% и гарантированно исправить все одиночные ошибки.

Согласно разработанному алгоритму, матрица с элементами ЦВЗ, представленными ИМК, разделяется на n – матриц (в рассматриваемом случае на 6 матриц) для того, чтобы остатки по каждому отдельному модулю (основанию) заносились в отдельный блок изображения, который соответствует определенному основанию системы. При такой организации, информация по каждому из оснований системы является относительно изолированной друг от друга и даже при полном удалении части изображения, которая включает полностью один из блоков переднего плана, ЦВЗ будет гарантировано полностью восстановлен.

Также в третьей главе разработан алгоритм внедрения ЦВЗ на основе морфологической обработки изображений. При выполнении алгоритма, построенного в соответствии с предложенным решением, некоторые неявные блоки переднего плана изображения–контейнера не будут промаркированы. Данное свойство отражается на обработке подобных объектов изображения–контейнера с позиции сегментации, однако данные неявные объекты могут быть изъяты из рассмотрения так как они не являются ключевыми элементами изображения–контейнера.

Представленные данным способом границы объектов переднего плана используются как области для заполнения ЦВЗ. При реализации морфологических функций дилатации и эрозии используется структурный элемент (примитив). Выбор размера и формы структурного элемента (примитива) зависит от особенностей конкретного изображения–контейнера. Примитив может

представлять собой ромбообразный, прямоугольный, диагональный и другой структурный элемент, состоящий из нулей и единиц.

При построении алгоритма учитывались следующие положения:

– злоумышленник обладает полным представлением о функционировании стегосистемы и схеме ее реализации. Единственной информацией, которая остается неизвестна злоумышленнику, является ключевая информация, с помощью которой только ее держатель может выявить факт наличия и содержания ЦВЗ;

– если злоумышленник будет проинформирован о факте существования ЦВЗ это не должно способствовать извлечению похожих ЦВЗ в других изображениях-контейнерах до тех пор, пока ключевая информация хранится в тайне;

– у злоумышленника должно отсутствовать преимущество (в том числе техническое) в раскрытии наличия и содержания ЦВЗ.

В большинстве стегосистем заполнение бит изображения–контейнера осуществляется на основе линейных функций, либо последовательно, что влияет на возможность легкого стегоанализа со стороны злоумышленника и неустойчивость к деструктивным воздействиям.

Для преодоления проблемы последовательного заполнения бит изображения было предложено использовать геометрический центр объекта (центроид) переднего плана как точку отсчета.

В нашем случае в двухмерном пространстве изображения–контейнера первый момент относительно оси x можно вычислить по формуле

$$\bar{x} \iint b(x,y)\,dx\,dy = \iint xb(x,y)\,dx\,dy, \qquad (6)$$

а относительно оси y:

$$\bar{y} \iint b(x,y)\,dx\,dy = \iint yb(x,y)\,dx\,dy, \qquad (7)$$

где $(\bar{x},\bar{y})$ – координаты центроида.

На рисунке 1 в виде блок схемы представлен алгоритм внедрения ЦВЗ в изображение-контейнер. Входными данными, для работы алгоритма является изображение-контейнер I и ЦВЗ, преобразованный к виду, пригодному для функционирования алгоритма. Задача, стоящая на начальном этапе выполнения данного алгоритма, заключается в определении блоков переднего плана, непосредственно в которые будет вноситься информация.

При морфологической обработке действия производятся с полутоновым изображением, поэтому исходное изображение-контейнер I преобразуется в полутоновое по формуле $Y = 0{,}299R + 0{,}587G + 0{,}114B$, где Y – значение ярковсти, R, G, B – значение красной, зеленой, синей компоненты в данной точке исходного изображения-контейнера.

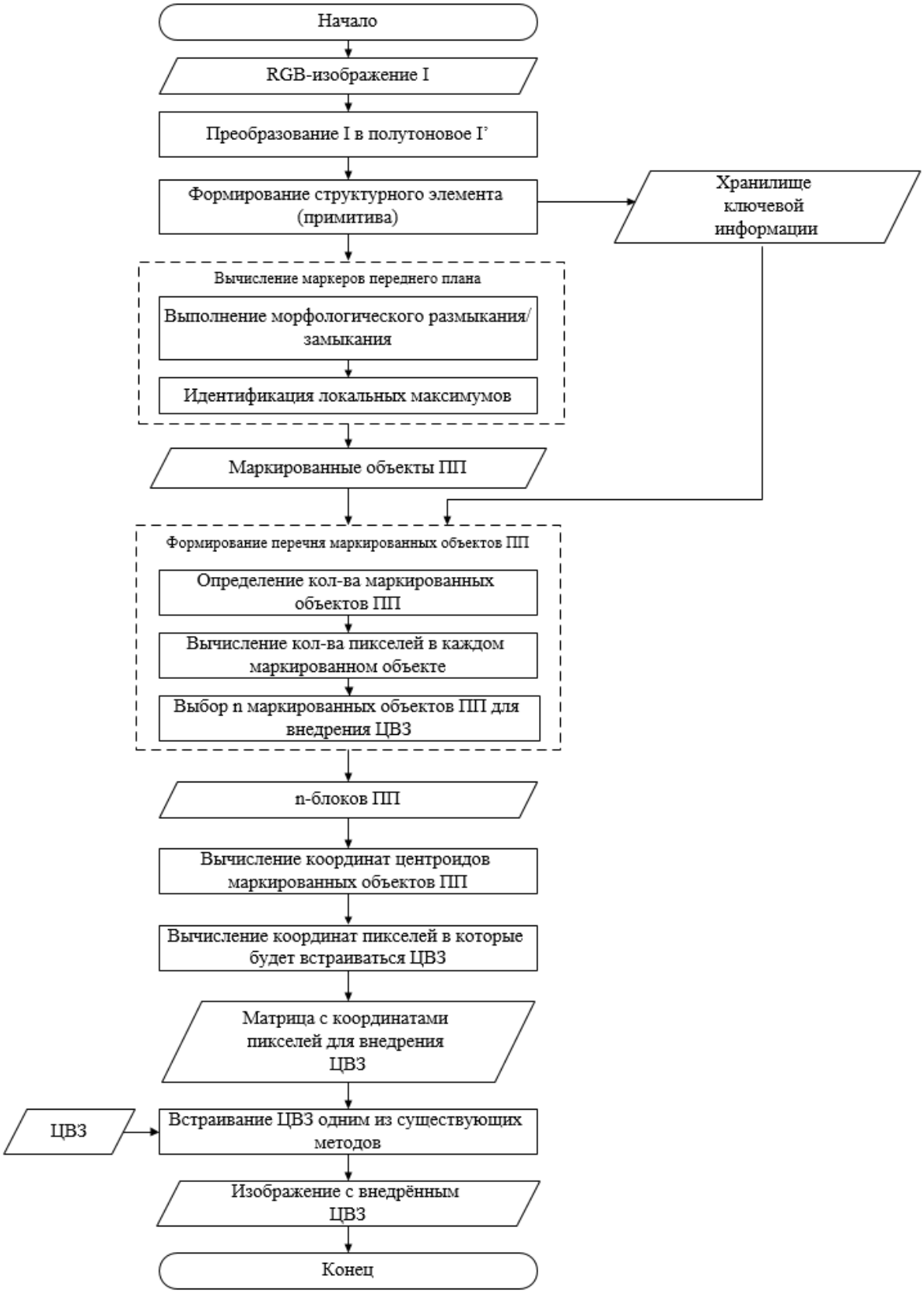

Рисунок 1 – Алгоритм внедрения ЦВЗ в изображение-контейнер

Затем формируется структурный элемент (примитива), который будет являться стего-ключом и находиться в хранилище ключевой информации.

На следующем этапе вычисляются маркеры переднего плана по заданному ранее структурному элементу. Для этого выполняются операции морфологического размыкания/замыкания с учетом формул (1,2), а также идентификация локальных максимумов. На выходе после выполнения указанных операций будем иметь перечень маркированных объектов переднего плана.

Однако не все полученные объекты могут подойти для встраивания ЦВЗ по причине недостаточного размера или неподходящего расположения на изображении-контейнере, поэтому на следующем этапе необходимо определить, какие из объектов переднего плана подойдут для встраивания информации.

Для этого необходимо произвести вычисление количества пикселей, из которых состоит каждый объект переднего плана, а также учесть расположение самих объектов и их удаленность от края изображения. После выполнения данных операций имеем m блоков переднего плана, подходящих для встраивания информации.

В случае если количество блоков переднего плана оказалось меньше требуемого количества блоков n то производится корректировка структурного элемента (примитива) и процедура поиска маркированных объектов переднего плана повторяется.

В случае если количество блоков переднего плана оказалось больше требуемого количества блоков n (на практике данная ситуация наиболее вероятна) то маркированные объекты могут выбираться исходя из условий, которые также указываются в ключевой информации. Этим условием может быть выбор самых больших n блоков, либо n блоков, наиболее удаленных от края изображения и т.п.

На следующем этапе производится вычисление координат центроидов маркированных объектов переднего плана. Данные вычисления производятся с использованием формул (6,7).

Далее происходит выбор пикселей, в которые будет встраиваться ЦВЗ с учетом того, что начальной точкой отсчета в каждом маркированном блоке переднего плана будет являться координата центроида. На выходе на данном этапе будем иметь матрицу с координатами пикселей, в которые будет встраиваться ЦВЗ.

Координаты пикселей также будут зависеть от самого метода встраивания, так как есть методы, в которых для встраивания ЦВЗ недопустимо использование рядом находящихся пикселей (например в методе Куттера-Джордана-Боссена).

На последнем этапе происходит встраивание ЦВЗ в изображение-контейнер одним из известных методов. Встраивание будет происходить таким образом, что n матриц, содержащих значения ЦВЗ по каждому модулю, будут встраиваться в n маркированных блоков переднего плана, где каждому модулю будет

соответствовать свой маркированный объект переднего плана.

Количество маркированных объектов переднего плана должно быть не менее количества модулей $\{p_1, p_2, \dots, p_i, .., p_{k+1}, p_{k+2}, \dots p_{k+n}\}$, по которым будет представляться ЦВЗ. В разработанных программных продуктах будет осуществляться внедрение данных шести матриц с остатками по шести модулям в шесть блоков переднего плана, соответствующих им.

Представленный на рисунке 1 алгоритм применим к существующим методам встраивания ЦВЗ для повышения устойчивости к деструктивным воздействиям.

В третьей главе также представлена модификация метода встраивания ЦВЗ путем замены младшего бита (LSB) на основе описанных выше алгоритмов. Встраивание ЦВЗ будет происходить в цифровое изображение I, представленное в виде файлов формата bmp, png, tiff и др.

Изображение I цветового пространства RGB представляет собой трехмерный массив со значениями компонентов, отвечающих за красную (Red) M_R, зеленую (Green) M_G и синюю (Blue) M_B составляющую цвета элемента изображения I. Встраивание ЦВЗ будет осуществляться в два последних младших бита пикселей способом, представленным на рисунке 2, где x_c, y_c – координаты центроидов.

				$x_{c+\frac{n}{4}}, y_c$				
				...				
				x_{c+2}, y_c				
				x_{c+1}, y_c				
$x_c, y_{c-\frac{n}{4}}$	...	x_c, y_{c-2}	x_c, y_{c-1}	x_c, y_c	x_c, y_{c+1}	x_c, y_{c+2}	...	$x_c, y_{c+\frac{n}{4}}$
				x_{c-1}, y_c				
				x_{c-2}, y_c				
				...				
				$x_{c-\frac{n}{4}}, y_c$				

Рисунок 2 – Последовательность окружающих центроид точек для внедрения ЦВЗ

Для представления ЦВЗ в модулярный код достаточно найти остатки по модулям $p_1, p_2, \dots, p_i, \dots, p_{k+1}, p_{k+2}, \dots, p_{k+n}$, определить информационный диапазон P и полный диапазон системы с контрольными основаниями $P' = \prod_{i=1}^{k+n} p_i$. Полученные остатки будут представлены данными размерностью по четыре бит. Данные остатки заносятся в младшие биты матриц M_B, M_R по схеме, представленной на рисунке 3.

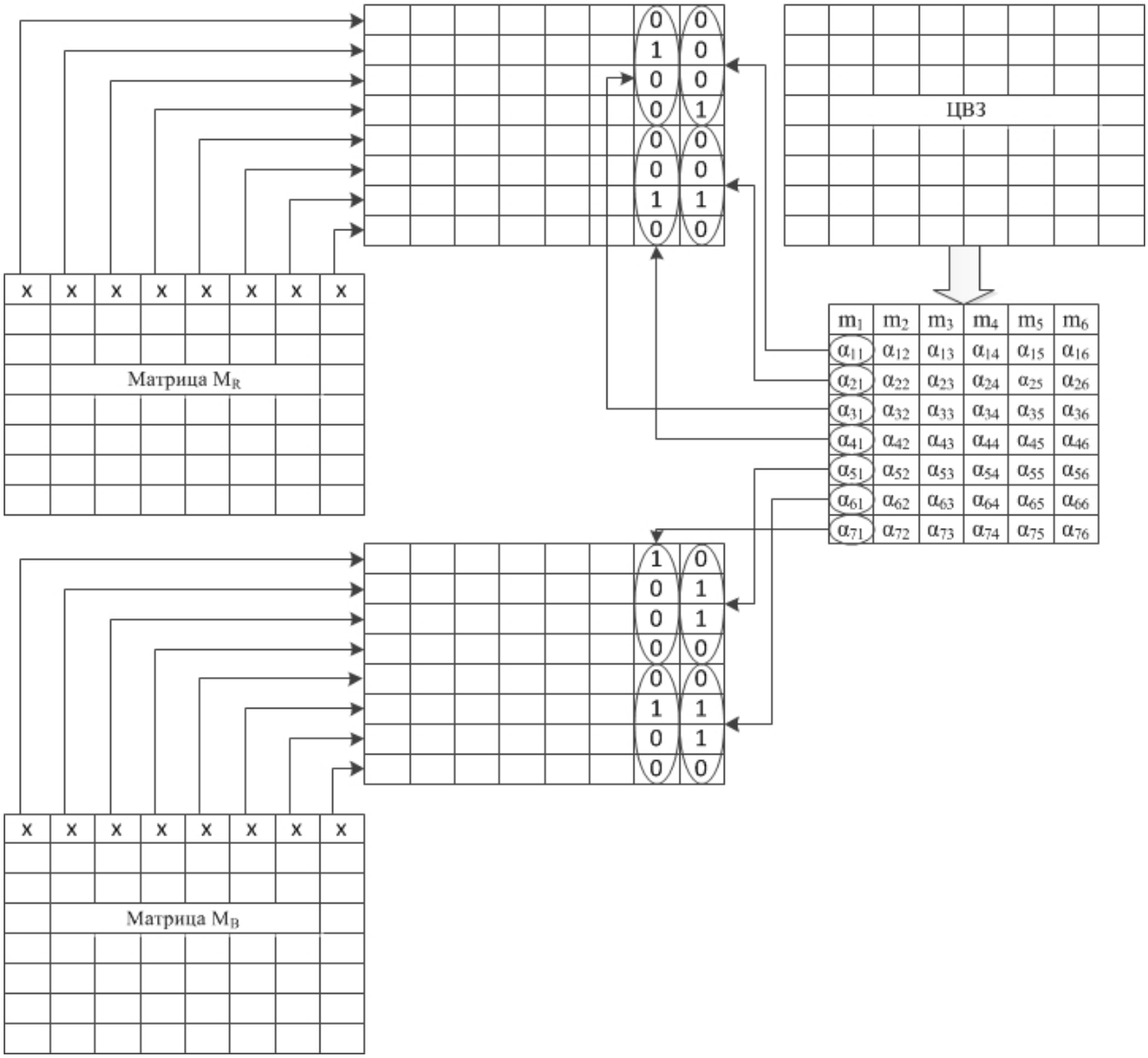

Рисунок 3 – Схема встраивания ЦВЗ

Для извлечения информации, содержащейся в ЦВЗ, производится процедура вычисления координат точек, окружающие центроиды блоков переднего плана с выполнением этапов, указанных ранее. Таким образом, определяются точки, в которых записана информация о ЦВЗ. Эта информация представляет систему чисел $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}$, обладающую свойствами обнаружения и исправления ошибок. Данные подвергаются проверке и в случае если они не подвержены изменению, осуществляется процедура считывания

информации и обратное преобразование ЦВЗ из ИМК в ПСС. В случае если данные подвергнуты изменению, осуществляется процедура коррекции свойствами ИМК, а только затем осуществляется процедура считывания и преобразования информации.

В главе также представлена модификация еще одного метода – Куттера-Джордана-Боссена при изменении яркости синей составляющей цвета элемента изображения I при встраивании разработанного ЦВЗ. На начальном этапе выполнения алгоритма исходное текстовое представление ЦВЗ считывается из файла и преобразовывается к виду, пригодному для преобразования из ПСС в ИМК. Данные из текстового файла подвергаются считыванию в заранее созданный массив. После чего осуществляется процедура преобразования каждого из считанных символов в численное представление с заранее заданной разрядностью, которая типична для заданного вида кодировки.

Встраивание бита s в синюю компоненту пикселя $p = (x, y)$ происходит в результате изменения яркости. Встраивание выполняется согласно формуле:

$$B'(p) = \begin{cases} B(p) + qI(p), & \text{если } s = 0; \\ B(p) - qI(p), & \text{если } s = 1, \end{cases} \quad (8)$$

где $B'(p)$ – модифицированное синее значение пикселя, q – энергия внедряемого сигнала. Так как у получателя нет оригинала изображения-контейнера, то соответственно и нет возможности гарантированно узнать как именно изменилась яркость синего цвета. Поэтому, для извлечения ЦВЗ прогнозируется показатель яркости синего цвета:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i}+B_{x,y-i}+B_{x+i,y}+B_{x-i,y})}{4\sigma}, \quad (9)$$

где $\sigma = 1 \ldots 3$.

Встраивание ЦВЗ будет осуществляться не во все синие компоненты пикселей изображения, сохраненного в цветовой модели RGB, а только в окружающие центроиды маркированных блоков переднего плана, способом, представленным на рисунке 4, где (10,10) – координаты центроида. Темно-синий пиксель – это пиксель, яркость синего цвета которого необходимо предположить, опираясь на пиксели, которые обозначены более светлым цветом.

Основной идеей построения такой схемы встраивания информации является то, что процесс извлечения носит вероятностный характер, следовательно, нельзя производить изменения в пикселях которые будут использованы для прогнозирования яркости измененного пикселя (то есть окрестности данного пикселя) в момент извлечения ЦВЗ.

Для извлечения встроенного ЦВЗ используется формула:

$$s_i = \begin{cases} 1, & \text{при } B^*_{x,y} > \overline{B_{x,y}}; \\ 0, & \text{при } B^*_{x,y} < \overline{B_{x,y}}. \end{cases} \quad (10)$$

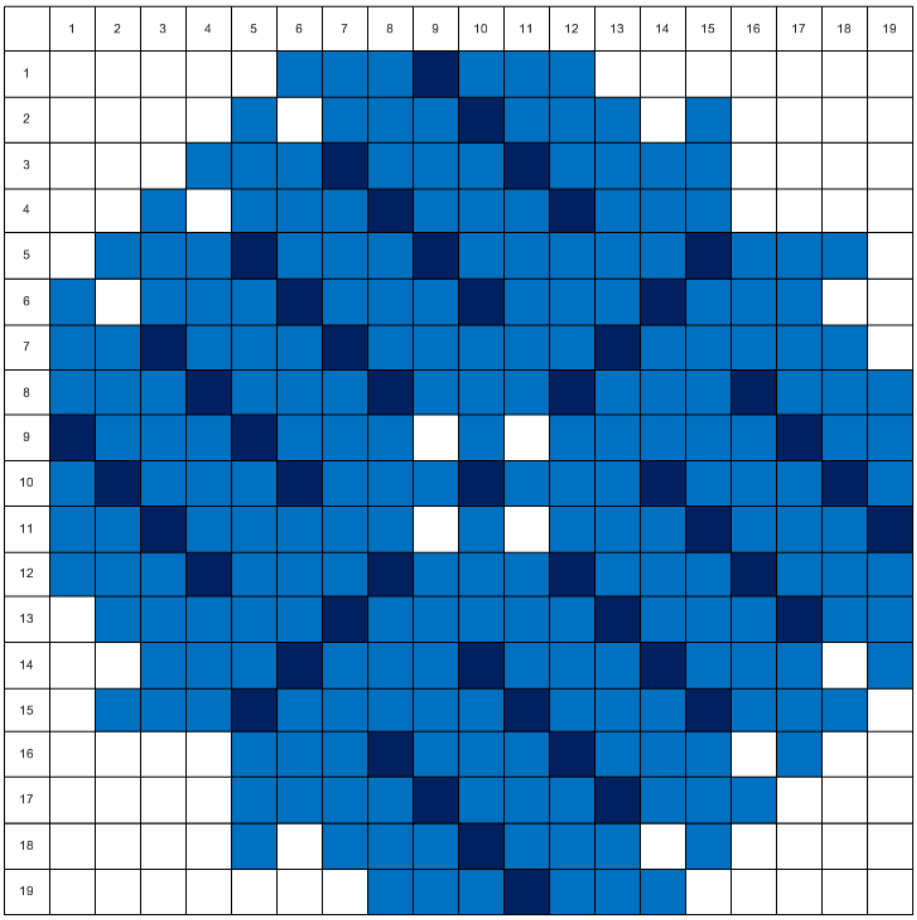

Рисунок 4 – Схема встраивания ЦВЗ

К положительным сторонам использования данного метода встраивания ЦВЗ следует отнести следующее:

– высокая устойчивость к несанкционированному ознакомлению;

– высокая устойчивость к частотному детектированию;

– высокая устойчивость к модификации младших бит контейнера;

– устойчивость к атаке сжатия.

К отрицательным сторонам следует отнести тот факт, что извлечение ЦВЗ носит вероятностный характер, однако использование аппарата модулярной арифметики позволяет избавиться от этого недостатка.

На рисунке 5 в виде блок схемы, представлен обобщенный алгоритм извлечения ЦВЗ из изображения–контейнера.

Обнаружение и коррекция ошибок будет выполняться на основе известных методов ИМК. В первую очередь производится проверка данных на наличие ошибок. Для этого предлагается ИМК перевести в полиадический код.

Разряды полиадического кода $\{z_1, z_2, \dots, z_{n+k}\}$ по основаниям-модулям $p_1. p_2, \dots, p_i, \dots, p_{k+1}, \dots, p_{k+n}$ можно вычислить из ИМК $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}$ с помощью системы:

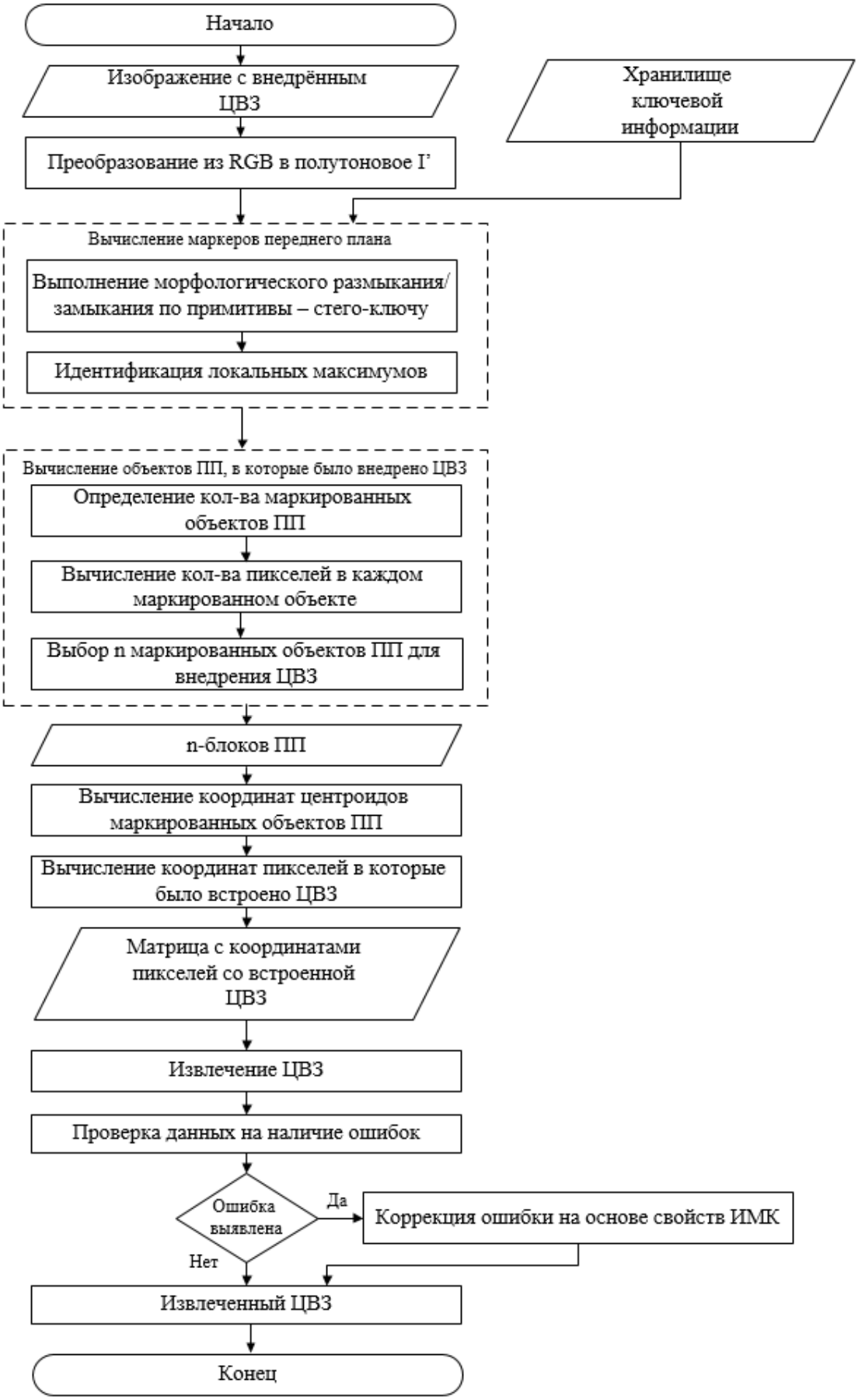

Рисунок 5 – Алгоритм извлечения ЦВЗ из изображения-контейнера

$$\begin{cases} z_1=\alpha_1, \\ z_2=\left||p_1^{-1}|_{p_2}(\alpha_2-z_1)\right|_{p_2}, \\ z_3=\left||p_2^{-1}|_{p_3}(|p_1^{-1}|_{p_3}(\alpha_3-z_1)-z_2)\right|_{p_3} \\ \dots \\ z_n=\left||p_{n-1}^{-1}|_{p_n}\left(|p_{n-2}^{-1}|_{p_n}\left(\dots|p_2^{-1}|_{p_n}(|p_1^{-1}|_{p_n}(\alpha_n-z_1)-z_2)\dots\right)-z_{n-1}\right|_{p_n}\right. \\ \dots \end{cases} . \quad (11)$$

Пусть $A=\{z_1,z_2,\dots,z_{n+k}\}$ – имеющийся результат вычислений. Полученное число A находится в диапазоне разрешенных значений, когда избыточные цифры полиадического кода равны нулю, т.е. $z_{n+r}=0$ для $r=1,2,\dots,k$.. В случае правильности числа A его исходное значение в двоичной форме восстанавливается из полученных коэффициентов обобщенной полиадической системы на основании формулы:

$$A=z_{n+k}p_{n+k-1}p_{n+k-2}\dots p_1+z_3p_2p_1+z_2p_1+z_1. \quad (12)$$

В случае обнаружения искажения его исправление осуществляется на основе метода проекций.

В **четвертой главе** приводится описание программного обеспечения, разработанного на основе метода, описанного во второй главе и алгоритмов, предложенных и описанных в третьей главе диссертационной работы, была произведена серия экспериментальных исследований встраивания ЦВЗ в различные программные продукты с целью выявления устойчивости встроенного ЦВЗ к различным деструктивным воздействиям на цифровое изображение.

В основе первого программного обеспечения ALStego лежит метод встраивания ЦВЗ путем замены младшего бита (LSB). Разработанное в диссертации программное обеспечение позволяет осуществлять внедрение ЦВЗ, представленного в виде логотипа или QR-кода в изображение-контейнер. В результате извлечения ЦВЗ мы имеем QR-код, который может быть легко прочитан с использованием мобильных устройств и онлайн сервисов или логотип.

В основе второго программного обеспечения Astego лежит метод встраивания ЦВЗ Куттера-Джордана-Боссена, который основывается на изменении яркости синей составляющей цвета элемента изображения I. Разработанное в диссертационной работе программное обеспечение позволяет осуществлять внедрение и извлечение ЦВЗ, представленного в виде текста или набора символов в изображение – контейнер.

В главе представлены результаты моделирования различных деструктивных воздействий на цифровое изображение с внедренным ЦВЗ, проведенных с использованием 100 различных цифровых изображений (текстурные, не текстурные, монотонные, многоцветные; пейзажи, рекламные постеры, натюрморты, корреспондентские фото и др.) с ЦВЗ различных видов.

Виды деструктивных воздействий на изображения, а также вероятность

правильного извлечения ЦВЗ для разработанного программного обеспечения и для известных широко используемых программных продуктов для защиты авторских прав (Suresign и DropWaterMark) представлены в таблице 1.

Таблица 1

Вероятность правильного извлечения ЦВЗ при различных деструктивных воздействиях

Программа / Деструктивное воздействие	Suresign	DropWaterMark	ALStego	AStego
Увеличение контрастности на 10%	1	1	0	1
Увеличение контрастности на 50%	1	1	0	1
Уменьшение контрастности на 10 %	1	1	0	1
Уменьшение контрастности на 50 %	1	1	0	1
Увеличение яркости на 10%	1	1	0	1
Увеличение яркости на 50%	1	1	0	0,97
Уменьшение яркости на 10 %	1	1	0	1
Уменьшение яркости на 20 %	1	1	0	1
Смена формата изображения на JPEG (качество 8)	1	1	0	1
Смена формата изображения на JPEG (качество 10)	1	1	0	1
Смена формата изображения на JPEG (качество 12)	1	1	0	1
Смена формата изображения на JPEG (качество 14)	1	1	0	1
Смена формата изображения на BMP	1	1	1	1
Смена формата изображения на TIFF	1	1	1	1
Смена формата изображения на PNG	1	1	1	1
Смена формата изображения на GIF	0,37	0,42	0,3	0,4
Вычеркивание 5 строк шириной 5 пикс	0	0	0,62	1
Вычеркивание 10 строк шириной 1 пикс	0	0	1	1
Вычеркивание 5 столбцов шириной 5 пикс	0	0	0,73	1
Вычеркивание 10 столбцов шириной 1 пикс	0	0	1	1
Вычеркивание 5 строк и 5 столбцов шириной 5 пикс	0	0	0,58	1
Вычеркивание 10 строк и 10 столбцов шириной 1 пикс	0	0	1	1
Поворот изображения на 1°	1	1	1	1
Поворот изображения на 50°	1	1	1	1
Поворот изображения на 50,5°	0	0	0	0
Сдвиг по горизонтали на 10%	0	0	0,8	0,96
Сдвиг по вертикали на 10%	0	0	0,76	0,96
Перемещение 5% части изображения	0	0	0,8	0,98
Перемещение 10% части изображения	0	0	0,72	0,95
Замена 10% изображения	0	0	0,64	0,95
Замена 50% изображения	0	0	0,52	0,6
Удаление 10 крайних пикселей	0	0	1	1
Удаление 50 крайних пикселей	0	0	1	1
Удаление 10% изображения	0	0	0,64	0,95
Удаление 50% изображения	0	0	0,52	0,6

Максимальным значением для разработанного программного обеспечения, при котором получилось извлечь ЦВЗ, являлось удаление 68% изображения.

В результате моделирования было выявлено:

1. Существующие программные продукты Suresign и DropWaterMark показали преимущества к таким деструктивным воздействиям как изменение контрастности, яркости, поворот изображения, смена формата хранения изображения, однако при замене, перемещении, удалении части изображения ЦВЗ было невозможно извлечь, а следовательно доказать наличие знака авторского права.

2. Программное обеспечение ALStego (на базе LSB) показало высокую устойчивость к деструктивным воздействиям, при которых не изменяются все пиксели с внедренным ЦВЗ. Неустойчивость к изменению яркости, контрастности, JPEG сжатию объясняется самим механизмом изменения пикселей при внедрении ЦВЗ и корректирующие способности избыточного модулярного кода при изменении всего ЦВЗ в данном случае работать не будут. Однако при других воздействиях данное программное обеспечение показывает очень высокий результат, что говорит о возможности его практического применения.

3. Программное обеспечение AStego показало высокие показатели ко многим примененным деструктивным воздействиям. Замена и удаление части изображения являются наиболее частыми деструктивными воздействиями при нарушении авторских прав на изображение и результаты при данных воздействиях достаточно высоки для обеих программ, что доказывает высокую эффективность разработанного метода внедрения ЦВЗ в цифровое изображение.

В **заключении** перечислены основные результаты работы и выводы.

В ходе достижения поставленной цели по разработке и исследованию эффективного метода внедрения ЦВЗ для защиты цифрового изображения, как объекта интеллектуальной собственности от угроз хищения **были получены следующие научные и практические результаты:**

– разработан метод внедрения ЦВЗ в изображение, отличающийся новой структурой ЦВЗ и оригинальным алгоритмом внедрения ЦВЗ в изображение, обеспечивающий более эффективную защиту изображения от угроз хищения;

– разработан новый алгоритм внедрения ЦВЗ, осуществляющий внедрение бит в цифровое изображение, отличающийся от известных использованием морфологического анализа, позволяющий определить значимые области для внедрения на основе стего–ключа – примитива особой сложной формы;

– разработан алгоритм извлечения внедренного ЦВЗ после возможных деструктивных преобразований изображения с ЦВЗ с целью доказательства авторских прав, обеспечивший верное извлечение ЦВЗ при удалении 68% одного

из изображений тестовой группы;

– разработана структура ЦВЗ, отличающаяся от ранее существующих использованием математического аппарата модулярной арифметики, позволяющего повысить его целостность при различных деструктивных воздействиях;

– разработано программное обеспечение для реализации предложенного метода внедрения ЦВЗ в изображение для предотвращения хищения объектов интеллектуальной собственности с целью доказательства авторских прав, которое может использоваться в различных системах обработки и передачи изображений для большинства графических форматов данных PNG, BMP, TIFF и др.

В ходе проведенных исследований установлено, что программное обеспечение, разработанное на основе метода и алгоритмов, описанных в диссертационной работе, будет обладать высокими показателями эффективности при наиболее распространенных деструктивных воздействиях при нарушении авторских прав на изображение.

Рекомендации. Для увеличения вероятности гарантированного извлечения ЦВЗ следует использовать для внедрения наиболее большие и удаленные от края изображения области переднего плана, так же этому будет способствовать увеличение количества разрядов представления ЦВЗ в избыточном модулярном коде.

Перспективы дальнейшей разработки темы. Проведение комплекса экспериментальных и теоретических исследований возможностей использования результатов диссертационного исследования, в том числе разработанной структуры ЦВЗ применительно к другим методам встраивания информации в цифровое изображение.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ

Публикации в ведущих рецензируемых изданиях, рекомендуемых ВАК РФ

1. Анкина А.М. (Абасова А.М.) Отказоустойчивый регистратор защищённой информации, функционирующий в классах вычетов / Н.Д. Абасов, А.М. Анкина (А.М. Абасова), Д.И. Ржевский, О.А. Финько // Известия ЮФУ. Технические науки. Информационная безопасность. – 2012. -№12(137). –С.207-211. ISSN 1999-9429.

2. Абасова А.М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение/ А.М. Абасова // Известия ЮФУ. Технические науки. Комплексная безопасность сложных систем. – 2014. -№8(157). –С.75-81. ISSN 1999-9429.

Публикации в других изданиях

3. Анкина А.М. (Абасова А.М.) Синтез структуры отказоустойчивого регистратора защищённой информации, функционирующего в классах вычетов / Н.Д. Абасов, А.М. Анкина (А.М. Абасова) //, Материалы XVII Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Рязанский государственный радиотехнический университет, 2012. – С.30-33.

4. Абасова А.М. Отказоустойчивый регистратор защищённой информации, функционирующий в избыточном модулярном коде / Н.Д. Абасов, А.М. Абасова, С.В. Савин, О.А. Финько // Материалы XIII Международной научно-практической конференции «Информационная безопасность–2013». ФГАОУ ВПО «Южный федеральный университет», 2013. – С.106-113

5. Абасова А.М. Метод преобразование и хранения данных на основе модулярной арифметики, обеспечивающий целостность информации свойствами самовосстановления и контроля / Н.Д. Абасов, А.М. Абасова, О.А. Финько //Информационное противодействие угрозам терроризма. – 2013. –С.89-93.

6. Абасова А.М. Использование методов морфологической обработки изображений для внедрения цифровых водяных знаков / А.М. Абасова // Материалы VI Международной научно-технической конференции «Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6)». Федеральное государственное автономное образовательное учреждение высшего профессионального образования Северо-Кавказский федеральный университет, 2014. –С.199-203. ISSN 2219-293X.

7. Абасова А.М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение / Л.К. Бабенко, А.М. Абасова // Информационное противодействие угрозам терроризма. – 2014. –С.201-205..

СВИДЕТЕЛЬСТВА О РЕГИСТРАЦИИ ПРОГРАММ ДЛЯ ЭВМ

8. Абасова А.М. Программа внедрения информации в изображение на базе морфологического анализа, модулярной арифметики и метода Куттера-Джордана-Боссена (AStego) / А.М. Абасова // Свид. о гос. регистрации программы для ЭВМ. – Федеральная служба по интеллектуальной собственности. – 02.07.2015.

9. Абасова А.М. Программа внедрения информации в изображение на базе морфологического анализа, модулярной арифметики и метода LSB (ALStego) / А.М. Абасова // Свид. о гос. регистрации программы для ЭВМ. – Федеральная служба по интеллектуальной собственности. – 30.06.2015.