ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

На правах рукописи

БЕКИРОВ АЛИ ЭНВЕРОВИЧ

УДК 621.391.2: 004.056

МЕТОД ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ В КРИТИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ СТРУКТУРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ

21.05.01 – информационная безопасность государства

Диссертация на соискание ученой степени кандидата
технических наук

Научный руководитель
доктор технических наук, профессор
БАРАННИК Владимир Викторович

Харьков – 2015

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СИР	–	специальные информационные ресурсы
ВКС	–	видеоконференцсвязи
МО	–	Министерство Обороны
СМИ	–	средства массовой информации
ДКП	–	дискретное косинусное преобразование
СС	–	скрываемое сообщение
НПЧ	–	неравновесное позиционное число
НЗБ	–	наименее значимый бит
ИК	–	изображение-контейнер
СКН	-	системы критического назначения

ВВЕДЕНИЕ

Актуальность темы. Опыт функционирования систем критического назначения в условиях активного противодействия противника обнаружил острую необходимость обеспечения необходимого уровня безопасности специальных информационных ресурсов, как составной части государственной информации. Такая необходимость с одной стороны диктуется повышенной значимостью СИР для информационной поддержки функционирования систем критического назначения, в том числе в условиях кризисных ситуаций. С другой стороны повышаются угрозы нарушения конфиденциальности и целостности СИР, что обусловлено оперативно-программными и информационно-технологическими возможностями противника. Поэтому повышение безопасности специальных информационных ресурсов в инфокоммуникационных системах является актуальной ***научно-прикладной задачей***.

Для решения сформулированной задачи необходимо разработать новые пути обеспечения безопасности СИР. Одним из направлений является использование стеганографических методов встраивания информации в изображение-контейнер. Базой для реализации такого подхода являются системы видеоконференцсвязи, широкое использование мультимедийных средств, наличие широкого видеоинформационного поля, наличие привязки служебной информации к конкретному видеоматериалу.

Среди методов стеганографических преобразований наиболее проработанными и используемыми на практике являются методы непосредственного встраивания информации в изображение-контейнер. Данные методы характеризируются простотой реализации встраивания, большим значением стеганографической емкости и небольшими значениями временных затрат на реализацию прямого и обратного стеганографических преобразований.

Однако проведенный анализ существующих методов стеганографических преобразований выявил следующие проблемные недостатки:

- недостаточное значение относительной стеганографической емкости;

- недостаточное значение устойчивости встроенных данных к атакам противника;

- значительные визуальные искажения стеганограммы.

Такие недостатки обусловлены тем, что в процессе стеганографических преобразований в основном учитываются психовизуальные закономерности. При этом изъятие встроенной информации осуществляется с использованием корреляционных зависимостей, которые нарушаются в результате нелинейной обработки стеганограммы.

В тоже время повышаются требования к информационному обеспечению функционирования кризисных систем. Такие требования обусловлены следующими факторами:

- повышение объемов доведения донесений в условиях кризисных ситуаций;

- использование в качестве специальных донесений видеоматериалов;

- повышение значимости влияния специальных донесений на результативность функционирования критических систем;

- повышение требований относительно достоверности и наглядности донесений;

- необходимость оперативной доставки скрытых сообщений в ограниченные временные промежутки сеанса связи;

- необходимость обеспечения и контроля использования пропагандистского поля противостояния.

Значит, в процессе использования существующих стеганографических систем для скрытой передачи специальной информации возникает ***противоречие***, которое заключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере системных требований в критических условиях с активным противостоянием противнику.

В связи с чем, для разрешения противоречия при построения стеганографических систем предлагается использовать механизмы выявления струк-

турных закономерностей. Таким образом, тема научно-прикладных исследований, которая связана с разработкой метода повышения безопасности специальных информационных ресурсов в системах критического назначения, на основе структурного стеганографического кодирования является актуальной.

Связь работы с научными программами, планами, темами. Диссертационные исследования выполнены в рамках заданий: Закона Украины «О Концепции Национальной программы информатизации» от 04.02.1998 № 75/98-ВР, «Об информации» от 02.10.1992 № 2657-XII, «О государственной тайне» от 21.01.1994 №3855-XII, «О научно-технической информации» от 25.06.1993 №3322-XII, Концепции технической защиты информации в Украине от 08.10.1997.№1126, Концепции (основы государственной политики) национальной безопасности Украины от 16.01. 1997 №3 / 97-ВР, Концепции национальной безопасности Украины, Концепции развития связи Украины, Комплексной программы развития и реформирования Вооруженных Сил Украины на период до 2017 года, Национальной космической программы Украины от 30.09.2008 N 608-VI. Основные результаты диссертационной работы отражены в отчете по НИР «Технологии создания интегрированных информационных систем на основе сетей цифрового мобильной связи» (№ 0113U000360), в которой автор диссертации был исполнителем.

Цель исследований. Цель диссертационной работы заключается в разработке метода повышения безопасности специальной информации для инфокоммуникационных систем критического назначения на основе стеганографических преобразований.

Для достижения сформулированной цели необходимо решить следующие задачи:

1. Обосновать подход для совершенствования методов непосредственного встраивания информации в цифровое изображение-контейнер.

2. Разработать метод структурного стеганографического кодирования для повышения безопасности специальной информации.

3. Создать метод для локализации структурной стеганографической избыточности для повышения стойкости к атакам на выявление факта встроенной информации.

4. Построить структурную стеганографической систему с маскированием стеганографической избыточности.

5. Разработать программную реализацию и провести оценку эффективности разработанной стеганографической системы.

Объект исследования. Процессы повышения безопасности специальных информационных ресурсов в инфокоммуникационных системах.

Предмет исследования. Методы повышения безопасности специальной информации на основе технологии стеганографического встраивания в изображение-контейнер.

Методы исследования. Проведенные исследования базируются на методах теории функционирования сложных систем, положениях теории цифровой обработки сигналов, методах защиты информации, положениях теории стеганографических преобразований и теории информации.

Научная новизна обусловлена решением научно-прикладной задачи повышения безопасности специальных информационных ресурсов на основе использования технологии структурного стеганографического кодирования.

Научная новизна результатов исследований заключается в том, что:

1. Впервые разработана стеганографическая система на основе непосредственного встраивания скрываемой информации в видеопоследовательность. В отличие от других стеганосистем обеспечивается одновременное встраивание и извлечение скрытой информации соответственно в процессе формирования и реконструкции кода-контейнера в базисе оснований неравновесного позиционного числа. Это обеспечивает встраивание скрытой информации на основе учета количества структурной избыточности фрагментов видеоизображений.

2. Впервые разработан метод структурного стеганографического кодирование с маскированием. В отличие от других методов обеспечивается

встраивание скрываемой информации в процессе неравновесного позиционного кодирования с последующей локализацией стеганографической избыточности. Это позволяет снизить возможность обнаружения злоумышленником факта наличия встроенной информации.

3. Впервые разработано метод демаскирующего стеганографическое декодирования. В отличие от существующих методов извлечение скрытой информации и восстановление неравновесного позиционного числа проводится на основе реконструкции стеганокода по биполярному принципу с демаскированием стеганографической избыточности. Это позволяет повысить эффективность извлечения скрываемой информации и локализовать атаки злоумышленника на выявление факта наличия скрытой информации.

4. Получили дальнейшее усовершенствование методы повышения безопасности государственной информации на основе применения стеганографических систем. В отличие от других систем используется структурное стеганографическое маскирующее и демаскирующее преобразование. Это позволяет повысить скрытность и целостность встроенной информации.

Новизна полученных результатов подтверждается отсутствием разработанных методов в существующих стандартах цифровой обработки изображений и стеганографического кодирования.

Обоснованность и достоверность полученных научных результатов базируются на:

- всестороннем анализе недостатков существующих технологий стеганографических преобразований для обеспечения условий повышения безопасности специальных информационных ресурсов;

- корректном использовании методов структурного кодирования.

Достоверность результатов диссертационных исследований подтверждается адекватностью результатов экспериментальных и теоретических исследований относительно стеганографической емкости и визуальной стойкости стеганограмм к атакам злоумышленника на выявления факта наличия встраивания, полученными на основе программной реализации и математи-

ческой модели; отсутствием противоречия полученных результатов методам структурного кодирования.

Практическое значение полученных результатов исследований заключается в том, что:

1. При одинаковых значениях стеганографической емкости выигрыш для разработанного метода относительно метода наименее значимого бита по величине пикового отношения сигнал-шум составляет в среднем от 8 до 32 дБ.

2. Для разработанного метода выигрыш в значении стеганографической емкости относительно метода на основе расширения спектра составляет от 1,22 до 5,47%.

3. Для разработанного метода выигрыш в значении вероятности безошибочного изъятия относительно метода наименее значимого бита и метода на основе расширения спектра составляет:

- для метода наименее значимого бита 40%;

- для метода на основе расширения спектра 50%.

4. Для различных значений коэффициента квантования наибольшей устойчивостью обладают данные, стеганографически встроенные в неравновесное позиционное число длиной шесть элементов. Наоборот наименьшей устойчивостью обладают данные, стеганографически встроенные в неравновесное позиционное число длиной, равной двум элементам. Количество безошибочно изъятых бит в условиях применения противником атак для разработанного метода в среднем принимает значение 90%.

5. Выигрыш для разработанного метода относительно метода на основе расширения спектра и метода наименее значимого бита по количеству безошибочно изъятых данных в условиях применения противником активных атак составляет:

- относительно метода наименее значимого бита - 40%,

- относительно метода на основе расширения спектра - 40%.

Практическая значимость полученных результатов диссертации подтверждается их применением при выполнении опытно-конструкторских работ в Научно-техническом специальном бюро «ПОЛИСВИТ» (акт реализации от 23.03.2014) и ГНИИ МВД Украины (акт реализации от 23.01.2015).

Личный вклад автора диссертационной работы в публикации, выполненные в соавторстве, заключается в следующем: в статьях [10; 12] - разработан подход для улучшения характеристик непосредственного стеганографического встраивания информации в изображение-контейнер; в статье [11] - определено количество бит, которые потрачены на представление одного блока и макроблока для всех составляющих цветной модели при кодировании; в статье [13] - проанализированы возможности злоумышленника относительно атак на видеоинформационный ресурс в информационно-телекоммуникационных сетях; в статье [14] - сформулирована концепция структурного стеганографического кодирования на основе неравновесного кодирования; в статье [15] - обоснована возможность использования неравновесного кодирования в качестве функционального преобразования для стеганографического встраивания; в статье [16] - разработана стеганографическая система с маскированием стеганографической избыточности; в статье [21] - обоснована необходимость повышения безопасности информационных ресурсов в системах специального назначения; в статье [22] - определена зависимость суммарного количества операций от количества типовых операций обработки изображений по выявлению значимых компонент трансформант; в статье [89] – разработана стеганографическая система на основе формирования кода-контейнера в неравновесном позиционном базисе.

Апробация результатов диссертации. Основные результаты диссертации докладывались и были одобрены на: двенадцатой международной конференции «TCSET'2014», Львов-Славское, 25 февраля - 1 марта; на Шестой Международной научно-практической конференции «Проблемы и перспективы развития IT - индустрии», Харьков, 17 - 18 апреля 2014 г.; на Четвертой международной научно-практической конференции «ITSEC», Киев,

20 - 23 мая 2014 г.; на Четвертой международной научно-практической конференции «Информационные технологии и компьютерная инженерия», Винница, 28 - 30 мая 2014 г.; International Symposium «IEEE East-West Design & Test», Kiev, Ukraine, 26-29 September 2014г; на Научно-методической конференции «Современные проблемы связи и подготовка специалистов в области телекоммуникаций – 2014», Львов, 1-4 ноября 2014г, на Третьей международной научно-технической конференции «Проблемы информатизации», Киев, 11 - 13 декабря 2014 г.; на XIII международной конференции CADSM'2015, Polyana-Svalyava (Zakarpattya), 24-27 February 2015; на научно-технической конференции «Информационная безопасность Украины», Киев, 12-13 марта 2015 г.

Публикации. Основные положения и результаты диссертационной работы опубликованы в 20 научных трудах, среди которых 11 статей, две из которых входят в международные научно-метрические базы и одна единоличная статья. Апробация результатов диссертации отражена в 9 тезисах докладов на международных научно-технических и научно-практических конференциях. В частности три апробации на конференциях, которые входят в состав международной организации IEEE.

РАЗДЕЛ 1
ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ В СИСТЕМАХ КРИТИЧЕСКГО НАЗНАЧЕНИЯ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В разделе обоснована необходимость повышения безопасности специальных информационных ресурсов в системах критического назначения, которая заключается в использовании методов цифровой стеганографии.

Обоснованы преимущества использование в качестве контейнера цифрового изображения.

Рассмотрены основные показатели эффективности стеганографических преобразований которые позволяют провести оценку успешности использования стеганографических методов для скрытого встраивания информации.

Проведена оценка методов непосредственного встраивания по относительной стеганографической емкости, вероятности безошибочного изъятия встроенных данных авторизированным пользователем и пиковому отношению сигнал-шум.

Сформулировано противоречие, которое заключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере системных требований в критических условиях с активным противостоянием противнику.

Сформулировано цель исследований, которая заключается в разработке метода повышения безопасности специальной информации на основе стеганографического преобразования для систем критического назначения.

1.1. Исследование характеристик функционирования систем критического назначения в условиях противодействия

Развитие инфокоммуникационных технологий, процессы внедрения новейших информационных систем, формирование и развитие современного информационного сообщества определяет важность информационного ресурса при обеспечении работы различных систем [34, 35, 36]. В настоящее время невозможно представить функционирование систем критического назначения без применения инфокоммуникационных систем. Это обусловлено тем, что все ведомственные организации государства задействуют инфокоммуникационные системы для оперативности обмена данными, организации управления и обеспечения информационной поддержки [34, 38, 40, 41, 43, 50].

Для систем критического назначения существует необходимость повышения безопасности специальных информационных ресурсов, которые являются составной частью государственной информации, в условиях функционирования с активным противодействием противника [53, 60, 69, 80]. Такая необходимость обусловлена несколькими явлениями (рис 1.1):

1. Развитие беспроводных технологий передачи данных. Данный аспект обусловлен использованием существующих и внедрением перспективных телекоммуникационных технологий для обеспечения обмена информацией в ведомственных организациях [45, 61, 83, 86]. С одной стороны широкое применение существующих беспроводных телекоммуникационных технологий при обеспечении обмена специальными информационными ресурсами обеспечивает простоту и оперативность функционирования СКН. Но с другой стороны у противника возникает упрошенный доступ к каналам передачи данных [12, 51,66, 88]. Это обусловлено использованием электромагнитного излучения в качестве носителя информации в пространстве.

В табл. 1.1 приведены основные беспроводные технологии, которые используются для информационной поддержки специальных операций.

Таблица 1.1

Основные характеристики беспроводных телекоммуникационных технологий, используемых в СКН

<table>
<tr><td colspan="5">Тип сети (системы)</td><td>Макс. скорость передачи данных</td></tr>
<tr><td rowspan="7">Беспроводные сети</td><td rowspan="4">Wi-Fi</td><td>802.11a</td><td>100 м.</td><td>54 Мбит/с</td></tr>
<tr><td>802.11b</td><td>100 м.</td><td>11 Мбит/с</td></tr>
<tr><td>802.11g</td><td>100 м.</td><td>54 Мбит/с</td></tr>
<tr><td>802.11n</td><td>100 м.</td><td>600 Мбит/с</td></tr>
<tr><td rowspan="3">WiMax</td><td>802.16d</td><td>6-10 км.</td><td>75 Мбит/с</td></tr>
<tr><td>802.16e</td><td>1-5 км.</td><td>40 Мбит/с</td></tr>
<tr><td>802.16m (перспектива)</td><td>н/д</td><td>100 Мбит/с
1 Гбит/с</td></tr>
<tr><td rowspan="3">Модемное соединение</td><td colspan="3">УПС ТЧ АТ-3002М</td><td>9,6 Кбит/с</td></tr>
<tr><td colspan="3">для коммутируемых линий</td><td>56 Кбит/с</td></tr>
<tr><td colspan="3">для выделенных линий</td><td>128 Кбит/с</td></tr>
<tr><td colspan="4">Цифровая транкинговая радиосвязь TETRA</td><td>36 Кбит/с</td></tr>
<tr><td colspan="4">Радиорелейные станции (на расстояние до 55 км без ретрансляции)</td><td>2 – 155 Мбит/с</td></tr>
<tr><td rowspan="11">Мобильная радиосвязь</td><td colspan="3">Tetrapol</td><td>7,8 Кбит/с
(2,4 - 7,2 Кбит/с)</td></tr>
<tr><td colspan="3">GSM (GSM-R), APCO 25, EDACS</td><td>9,6 Кбит/с</td></tr>
<tr><td colspan="3">GPRS</td><td>171,2 Кбит/с
(85 Кбит/с)</td></tr>
<tr><td rowspan="8">CDMA2000</td><td rowspan="2">1XEV-DO Rev 0</td><td>Down</td><td>2,4 Мбит/с</td></tr>
<tr><td>Up</td><td>153 Кбит/с</td></tr>
<tr><td rowspan="2">1XEV-DO Rev A</td><td>Down</td><td>3,1 Мбит/с</td></tr>
<tr><td>Up</td><td>1,8 Мбит/с</td></tr>
<tr><td rowspan="2">1XEV-DO Rev B (перспектива)</td><td>Down</td><td>4,9 Мбит/с</td></tr>
<tr><td>Up</td><td>2,4 Мбит/с</td></tr>
<tr><td rowspan="2">15 частотных каналов (перспектива)</td><td>Down</td><td>73,5 Мбит/с</td></tr>
<tr><td>Up</td><td>27 Мбит/с</td></tr>
<tr><td colspan="4">Космические аппараты (спутники)</td><td>665,4 Кбит/с
15,3 или 61,44 Мбит/с
370 – 550 Мбит/с</td></tr>
</table>

2. Появление большого количества информационно-технических средств для проведения атак. Появление новых подходов для обеспечения информационной безопасности сопровождается стремление противника к поиску методов и способов нарушения конфиденциальности и целостности специального ресурса [6, 80]. При этом важным аспектом является развитие

существующих и разработка новых технических средств для осуществления атак на специальный информационный ресурс.

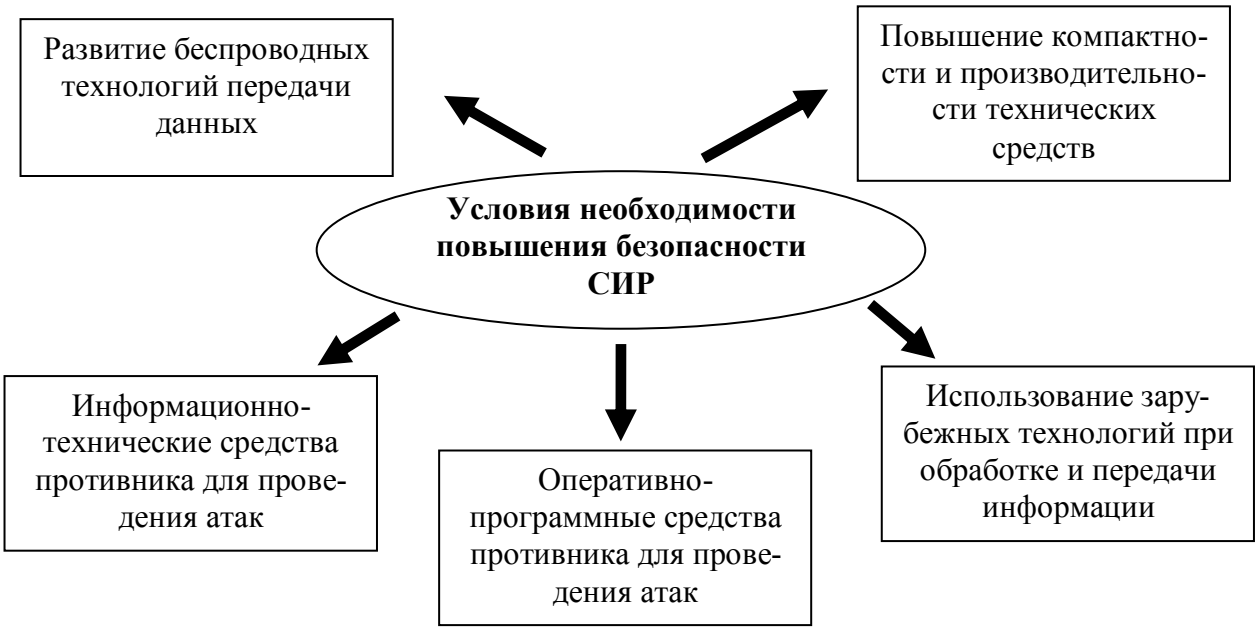

Рис. 1.1. Обоснование необходимости повышения безопасности специальных информационных ресурсов в системах критического назначения

3. Повышение оперативно-программных возможностей противника. Корректная работа аппаратных средств для осуществления атаки на специальный информационный ресурс во многом зависит от программного обеспечения их функционирования [3, 74]. Поэтому среди актуальных направлений деятельности противника является разработка новых программных средств для решения задачи проведения атаки на специальный информационный ресурс за минимальный период времени.

4. Повышение компактности и производительности технических средств для осуществления атак. Развитие технологических возможностей в направлении уменьшения размеров средств осуществления атак одновременно сопровождается увеличением их производительности. Это дает потенциальную возможность противнику для оперативного и скрытного использования таких средств в непосредственной близости к функционирующим СКН.

5. Использование зарубежных технологий для организации обработки и передачи данных. Отсутствие отечественных программных пакетов и аппаратных технологий для осуществления информационной поддержки функционирования СКН диктует необходимость использования зарубежных средств. Такой подход негативно влияет на обеспечения безопасности специальных информационных ресурсов. Это обусловлено возможностью злоумышленника скрытно использовать программы для нарушения конфиденциальности и целостности специальной информации.

Одновременно с повышением угроз относительно специальных информационных ресурсов в СКН постоянно повышается значимость такой информации. Это обусловлено тем, что нарушение безопасности СИР влечет за собой значительные потери человеческого и материальных ресурсов, имеет негативные информационно-пропагандистские последствия и наносит ущерб политическому и экономическому имиджу государства.

К актуальным направлениям для обеспечения безопасности специальных информационных ресурсов относится (рис 1.2):

1. Обеспечение документирования в базах данных ведомственных организаций. Для ведомственных баз данных характерно широкое использование мультимедийных данных совместно с текстовой информацией. В данном случае текстовая информация используется в качестве дополнительного материала к цифровым изображениям и видеоматериалам, представляющим собой специальный информационный ресурс [31, 56].

2. Информационная поддержка в условиях критических ситуаций [63, 74]. Актуальность данного аспекта заключается в том, что успешность функционирования СКН зависит от оперативного и точного информационного обеспечения. В то же время значимость такой информации вынуждает злоумышленника искать способы для нарушения ее конфиденциальности и целостности. Отсюда возникает необходимость повышения безопасности информационного ресурса в условиях критических ситуаций.

Рис. 1.2. Актуальные направления для обеспечения повышения безопасности специальных информационных ресурсов

3. Информационная поддержка систем контроля и мониторинга в критических условиях. Одним из инструментов урегулирования кризисных ситуаций являются международные мониторинговые миссии. Неудовлетворительный уровень объективности и достоверности результатов мониторинга имеет негативные последствия для государства. Это обуславливает значимость и необходимость повышения безопасности данного информационного ресурса.

4. Передача указаний в системах видеоконференцсвязи ведомственных организаций. Системы ВКС являются одной из базовых компонент организации управления подчиненными подразделениями и позволяет решить следующие задачи [4, 5, 16, 20-22, 55-57]:

- оценка состояния объектов управления и процессов функционирования;

- оперативное отображение информации о состоянии процессов организации и ведения боевых действий;

- оперативное отображение информации о состоянии объектов управления;

- подготовка данных и организация обмена между смежными (соседними) и вышестоящими уровнями системы управления;

- сбор, прием, передача, обработка, обобщение, хранение, анализ и отображение информации о состоянии объектов контроля и управления.

С одной стороны использование ВКС обеспечивает своевременное и необходимое качество управления подразделениями с выполнением объективного контроля решения поставленных задач. С другой стороны общедоступность алгоритмов, которые используются при организации ВКС, повышает потенциальную возможность противника относительно осуществления атаки на специальный информационный ресурс в системе ВКС.

5. Контроль и использование информационных каналов СМИ в критических условиях. Повышенный интерес СМИ к кризисным ситуациям сопровождается активным сбором информации. Для такой информации существует потенциальная возможность использование таких каналов злоумышленником для скрытой передачи данных.

6. Информационная поддержка поисковых операций в критических условиях. Актуальность данного аспекта обусловлена необходимостью оперативной и своевременной информационной поддержки поисковых действий в условиях кризисных ситуаций.

Значит для критических систем с одной стороны повышается важность информации для корректного функционирования и принятия решений. Но с другой стороны повышаются возможности для злоумышленника относительно нарушения конфиденциальности и целостности специального информационного ресурса.

Таким образом, повышение безопасности специальных информационных ресурсов в инфокоммуникационных системах является актуальной ***научно-прикладной задачей***.

Для критических систем повышение безопасности специальных информационных ресурсов заключается:

1) в уменьшении вероятности $P_{из}$ правильного восстановления специальной информации противником, что задается следующим выражением:

$$P_{вост} \rightarrow 0;$$

2) в уменьшении времени $T_{пр}$, которое необходимо для выявления и правильной реконструкции информации, что задается следующим образом:

$$T_{пр} \rightarrow \max.$$

Отсюда, для решения научно-прикладной задачи необходимо разработать подход для повышения безопасности специальных информационных ресурсов в системах критического назначения в условиях активного противодействия противника.

1.2. Обоснование необходимости повышения безопасности СИР на основе стеганографических технологий

При обосновании подхода для повышения безопасности СИР необходимо рассмотреть факторы, влияющие на снижение уровня информационной безопасности при функционировании СКН [8, 36, 49, 53, 80, 86, 87]. К основным факторам относятся следующие (рис 1.3):

1) Повышение возможностей противника для успешного криптоанализа. Развитие существующих и разработка новых аппаратных и программных средств для осуществления криптоанализа противником сопровождается необходимостью повышения безопасности специальных информационных ресурсов.

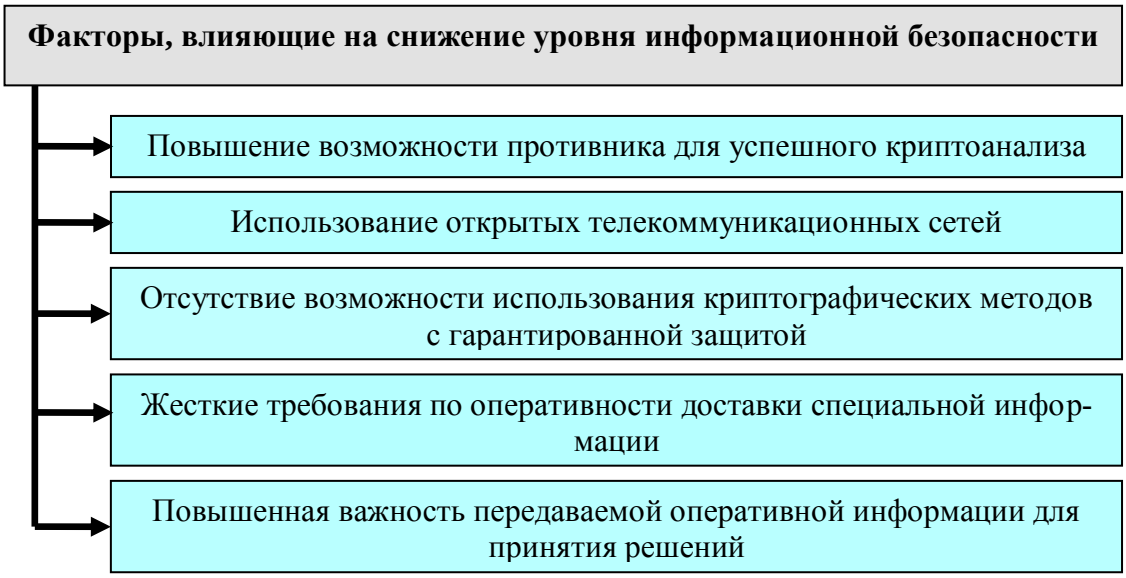

Рис. 1.3. Ограничения при использовании криптографических методов

2) Использование открытых телекоммуникационных сетей для передачи специальной информации [73].

3) Отсутствие возможности использования криптографических методов с гарантированной защитой. Данный фактор объясняется необходимо-

стью значительных аппаратных и программных затрат для обеспечения гарантированной защиты СИР, что не всегда возможно обеспечить в условиях функционирования СКН.

4) Жесткие требования по оперативности доставки специальной информации. Для информационного обеспечения достаточно остро стоит вопрос оперативности и своевременности доставки специальной информации. Такое условие затрудняет использование сложных систем защиты для обеспечения требуемого уровня безопасности СИР.

5) Повышенная важность передаваемой оперативной информации для принятия решений. Важность результатов успешного функционирования критических систем сопровождается повышением значимости информационного обеспечения. Данный факт в свою очередь, диктует необходимость обеспечения гарантированного уровня безопасности СИР.

Это влечет за собой значительные потери человеческих и материальных ресурсов, имеет негативные информационно-пропагандистские последствия, и наносит ущерб политическому и экономическому имиджу государства.

Поэтому наряду со сложными методами защиты специальных информационных ресурсов требуется использовать методы компьютерной стеганографии [2, 7, 23, 29, 54, 64, 67, 76]. В отличие от криптографии, стеганография позволяет скрыть факт наличия секретного сообщения. Информация в виде сообщения преобразуется определенным образом и встраивается в некоторый цифровой контейнер, который не привлекает внимания. Функциональная схема реализации скрытой передачи данных на основе использования компьютерной стеганографии представлена на рис 1.4 и включает следующие этапы:

1. Стеганографическое встраивание. На этом этапе осуществляется встраивание преобразованной специальной информации в цифровой контейнер. При этом используется стеганографическое правило. В процессе реализации встраивания специальной информации в цифровой контейнер

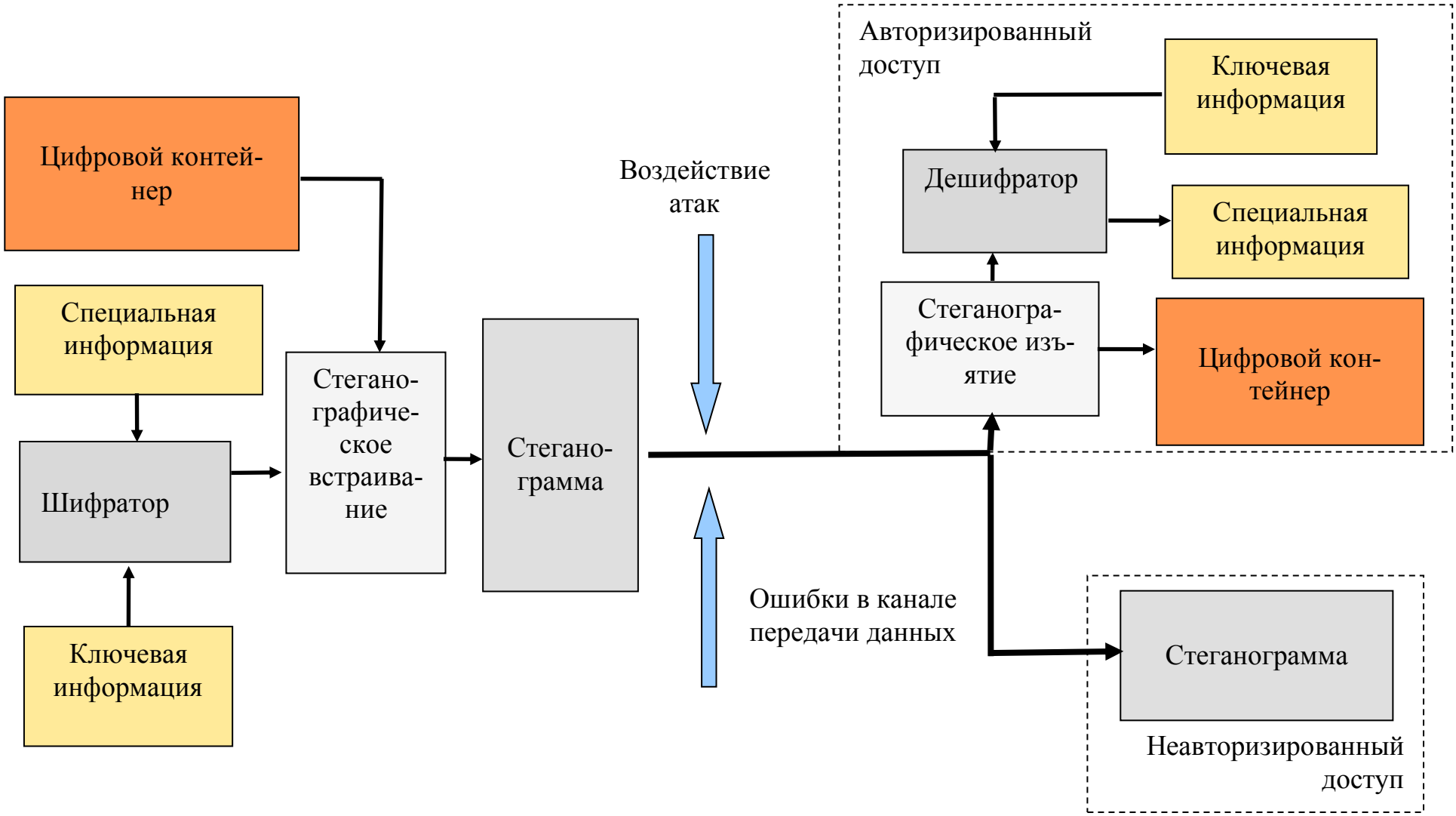

Рис. 1.4. Функциональная схема реализации скрытой передачи данных на основе подхода цифровой стеганографии

формируется стеганограмма, которая передается через канал передачи данных получателю.

2. Стеганографическое изъятие. На этом этапе авторизированный пользователь проводит стеганографическое декодирование. При этом ему известна следующая информация:

- факт наличия встроенной информации в стеганограмме;
- правило стеганографического декодирования;
- правило обратного преобразования изъятой информации.

В результате обратного стеганографического преобразования авторизированный пользователь осуществляет изъятие встроенной преобразованной информации с последующим дешифрированием. Также существует возможность использования цифровой контейнер в качестве полезной информации.

В случае авторизированного доступа появляется возможность избежать прямых атак на встроенную информацию, поскольку злоумышленнику не известен факт наличия встраивания в стеганограмме.

Компьютерная стеганография представлена методами встраивания информации в различные цифровые носители. Среди существующих методов стеганографии большое количество исследований посвящено использованию в качестве стеганографического контейнера цифровых изображений [7, 24, 33, 44, 46, 47, 48, 54, 58, 65, 79,82]. Это обусловлено рядом причин, среди которых можно выделить следующие:

- широкое распространение и использование цифровых изображений и видеопоследовательностей в самых различных областях деятельности человека [14, 77];
- большой объем мультимедийного файла для встраивания скрываемой информации [28, 119,];

- наличие в изображении обширных областей с психовизуальной избыточностью, которая потенциально может быть использована для скрытого встраивания [30, 42, 68, 75, 79, 103, 117].

Актуальность направления повышения безопасности специальных информационных ресурсов в системах критического назначения на основе стеганографического встраивания в изображение контейнера обусловлено рядом причин, среди которых присутствуют и явные достоинства использования цифровых изображений в качестве контейнера для встраивания СИР представлены на рис 1.5.

К преимуществам выбора методов стеганографического встраивания в изображение-контейнер для повышения безопасности СИР относятся следующие аспекты [24, 33, 44, 46, 111, 108, 109, 113, 114]:

- возможность использования в закрытых каналах видеоконференцсвязи для управления в ведомственных организациях;

- наличие широких возможностей использования компактных мультимедийных устройств и беспроводных средств в условиях кризисных ситуаций;

- наличие мультимедийных средств для объекта поиска;

- широкое использование видеоинформационного контента для мониторинга миссий ОБСЕ в системах объективного контроля;

- наличие обширного видеоинформационного поля для телевизионных новостных служб;

- наличие четкой привязки служебной информации к соответствующему видеоматериалу.

Рис. 1.5. Обоснование выбора видеоинформационного ресурса в качестве контейнера для скрытой передачи специальной информации

Существующие методы цифровой стеганографии для изображений можно классифицировать, как показано на рис 1.6.

В непосредственных методах информационная последовательность секретного сообщения встраивается путем замены данных контейнера на данные сообщения по формуле:

$$A' = f_{стег}\ (A,\ B\ ),$$

где A' - стеганограмма;

$f_{стег}$ - правило стеганографического встраивания;

A - исходное изображение-контейнер;

B -встраиваемые данные.

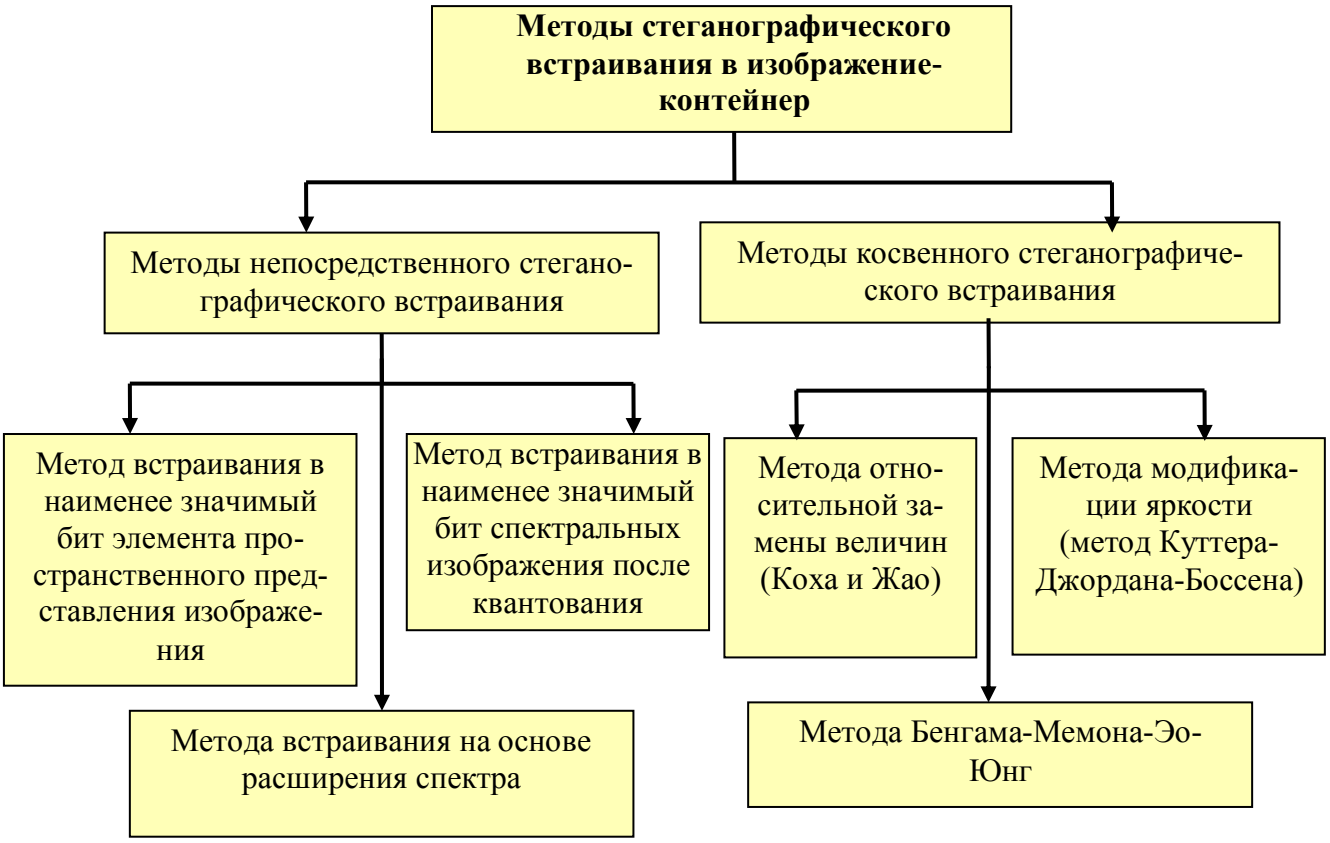

Рис. 1.6. Классификация стеганографических методов встраивания в изображение-контейнер

В непосредственных методах информационная последовательность секретного сообщения встраивается путем замены данных контейнера на данные сообщения по формуле [98, 119]:

$$A' = f_{стег}\ (A,\ B\ ),$$

где A'- стеганограмма;

$f_{стег}$ - правило стеганографического встраивания;

A - исходное изображение-контейнер;

B -встраиваемые данные.

Такая замена возможна непосредственно на бит встраиваемой информации, либо на бит преобразованного сообщения. Непосредственная логика встраивания реализована в семействах методов встраивания в наименее значимый бит данных:

1) пространственного представления изображения-контейнера (НЗБ режим 1) [82, 116, 120]. Физика метода заключается в замене младшего значащего бита битом секретного сообщения рис.1.7.

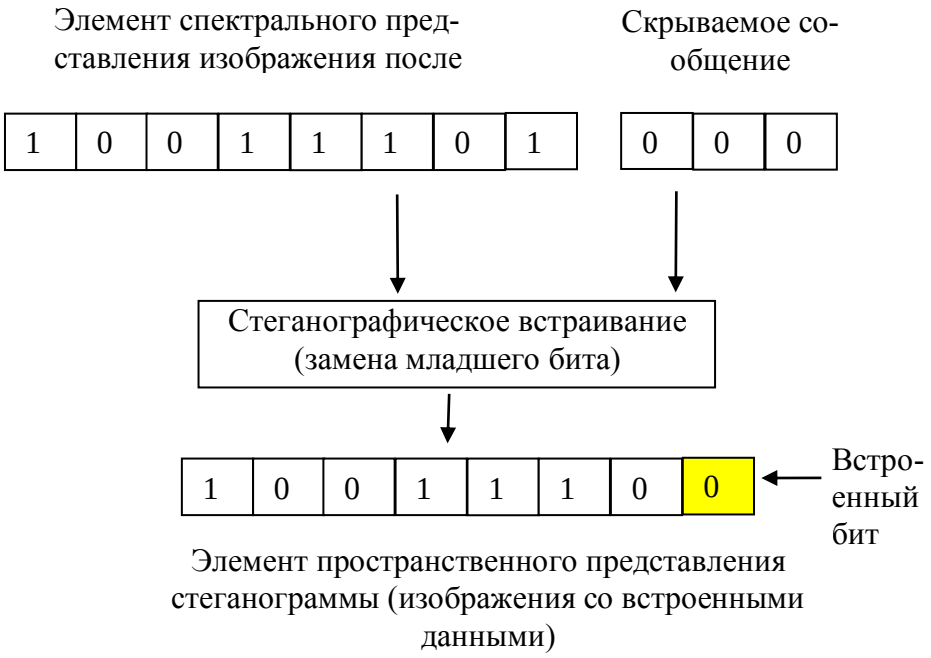

Рис. 1.7. Стеганографическое встраивание бита скрываемого сообщения в НЗБ элемента пространственного представления изображения-контейнера

Человек, в силу особенностей своих органов чувств не способен заметить изменений в данном бите. Фактически НЗБ - это шум, поэтому это позволяет использовать его в качестве замены [78, 84, 102]. Среди модификаций данного метода, можно выделить метод псевдослучайного интервала, в котором реализовано случайно распределение битов секретного сообщения в контейнере, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Также существует метод псевдослучайной пе-

рестановки, в котором биты сообщения встраиваются в псевдослучайные биты контейнера.

2) спектрального представления изображения-контейнера после квантования (НЗБ режим 2) [23, 52, 65, 9]. Встраивание бита скрываемого сообщения реализуется путем замены НЗБ элемента спектрального представления изображения контейнера как показано на рис. 1.8.

Рис. 1.8. Стеганографическое встраивание бита скрываемого сообщения в НЗБ элемента спектрального представления изображения-контейнера после квантования

Также непосредственное встраивание реализуется в методах на основе расширения спектра [2, 23, 81, 82]. В таких методах встраиваемое сообщение в двоичном представлении преобразуется на основе модуляции сигналом специального вида. Полученные значения преобразованного сообщения встраиваются путем модификации элементов пространственного представления изображения.

В косвенных методах встраивание одного бита сообщения осуществляется созданием зависимости между определенными параметрами изображения-контейнера, при которой стеганографический декодер, в соответствии с

обратным стеганографическим преобразованием, выделяет 0 или 1 бита встроенной информации. Это описывается следующим выражением:

$$B = f_{изв}(A'),$$

где B - встраиваемые данные;

$f_{изв}$ - алгоритм обратного преобразования (извлечения);

A' - стеганограмма.

Такая логика встраивания реализована в следующих методах:

1. Метод относительной замены величин ДКП (метод Коха и Жао) [97, 99, 105]. Один из наиболее распространенных на сегодня методов. В алгоритме метода реализовано разбитие изображения на блоки 8*8 пикселей для применения к каждому из них ДКП. В результате данного преобразования получается матрица 8*8 коэффициентов ДКП. Каждый блок используется для скрытия одного бита данных. Для обеих сторон при организации секретного канала, выбираются два конкретных коэффициента ДКП, с определенными координатами в массиве коэффициентов. Непосредственно скрытее начинается со случайного выбора блока изображения, предназначенного для кодирования бита данных. Встраивание происходит такой модификацией коэффициентов, чтобы при передачи «0» их разница превышала некоторую положительную величину, а для «1» эта разница делается меньшей по сравнению с некоторой отрицательной величиной. Таким образом, первичное изображение модифицируется за счет внесения изменения в коэффициенты ДКП. После соответствующей коррекции коэффициентов проводится обратное дискретное косинусное преобразование.

2. Метод модификации яркости (метод Куттера-Джордана-Боссена) [106, 107, 110]. Встраивание реализуется в канал синего цвета RGB изображения. Цвет был выбран из-за низкой чувствительности человека к его изме-

нению. Секретный бит M_i встраивается в канал синего цвета путем модификации яркости $\lambda_{x,y} = 0.29890 \cdot R_{x,y} + 0{,}58662 \cdot G_{x,y} + 0.11448 \cdot B_{x,y}$:

$$B'_{x,y} = B_{x,y} - \upsilon \cdot \lambda_{x,y}, \quad \text{при} \quad m_i = 0$$

и

$$B'_{x,y} = B_{x,y} - \upsilon \cdot \lambda_{x,y}, \quad \text{при} \quad m_i = 1,$$

где υ- величина, которая определяет энергию встраиваемого сигнала, прямо пропорциональна устойчивости встроенной информации к искажениям.

Для извлечения секретного бита, получателю необходимо выполнить предсказание значения первичного не модифицированного пикселя, используя значения соседних пикселей. Авторы метода использовали «крест» пикселей размером 7*7.

3. Метода Бенгама-Мемона-Эо-Юнг [39, 95, 44]. Встраивание осуществляется в спектральные коэффициенты изображения-контейнера путем их модификации. Для этого в спектральной области выбираются три коэффициента ДКП, что позволяет уменьшить визуальные искажения. Для встраивания «0», эти коэффициенты изменяются таким образом, что бы третий коэффициент стал меньше любого из двух первых. Если необходимо скрыть «1», он делается большим, чем первый и второй коэффициенты. Использование трех коэффициентов ДКП вместо двух уменьшает искажения, которые вносятся в результате встраивания скрываемого сообщением.

Для приведенных стеганографических методов встраивания в изображение-контейнер важно оценить успешность их функционирования для скрытого встраивания специальной информации.

1.3 Оценка недостатков существующих методов стеганографических преобразований

Для сравнения и оценки существующих стеганографических систем рассмотрим показатели эффективности их функционирования. Такое оценивание должно давать полную картину успешности использования оцениваемых стеганографических методов для скрытой передачи СИР. Рассмотрим основные показатели эффективности стеганографических преобразований [23, 44, 62, 70, 91]:

1. Относительная стеганографическая емкость $w_{отн}$ стеганографической системы. Значение относительной стеганографической емкости показывает процентное отношение объема $w_{встр}$ встраиваемой информации относительно объема $W_{исх}$ изображения-контейнера. Данная величина используется для оценки эффективности стеганографической системы по удельному объему встраиваемой информации относительно объема изображения-контейнера. Величина $w_{отн}$ относительной стеганографической емкости системы определяется на основе следующей формулы:

$$w_{отн} = \frac{w_{встр}}{W_{исх}} .$$

Физический смысл данной величины заключается том, что проводится оценка количества бит исходного изображения-контейнера приходящегося на один бит встроенного сообщения.

В процентах значение относительной стеганографической емкости системы оценивается на основе следующего выражения:

$$w_{отн} = \frac{w_{встр}}{W_{исх}} \cdot 100\% .$$

2. Вероятность $P_{из}$ безошибочного изъятия встроенных данных авторизированным пользователем. Данная величина используется для оценки безошибочно изъятой информации при авторизированном доступе. Вероятность $P_{из}$ определяется на основе следующего выражения:

$$P_{из} = \frac{w_{из}}{w_{встр}},$$

где $w_{встр}$ - объем встраиваемой информации, бит;

$w_{из}$ - объем безошибочно изъятой информации, бит.

В случае, когда вероятность $P_{из}$ принимает значение единицы, количество безошибочно изъятых встроенных данных авторизированным пользователем равно 100%.

3. Пиковое отношение сигнал-шум h изображения со встроенными данными при неавторизированном доступе. Данная величина характеризует визуальные искажения, которые вносятся в изображение-контейнер в процессе встраивания, и определяется на основе следующей формулы:

$$h = 20\log_{10}(255/СКО) \text{ (дБ)}$$

где СКО - среднеквадратическое отклонение изображения со встроенными данными относительно изображения-контейнера и определяется на основе следующей формулы:

$$СКО = \sqrt{\sum_{i=1}^{z_{строк}} \sum_{j=1}^{z_{столб}} (a_{i\,j} - a'_{i\,j})^2 / z_{строк}\ z_{столб}} .$$

Здесь a_{ij}, a'_{ij} - элементы соответственно исходного и стеганографически преобразованного изображений, $z_{строк}$ $z_{столб}$ - размер изображения-контейнера.

Чем больше значение пикового отношения сигнал шум, тем меньше визуальных искажений вносится в изображение в процессе встраивания. В случае, когда $СКО = 0$, значение $h \to \infty$ - идеальные условия.

По этим показателям предпочтительными являются методы непосредственного встраивания специальной информации [115, 118]. Для решения задач скрытого встраивания данных методы непосредственного встраивания имеют ряд преимуществ, которые представлены на рис 1.9.

В сравнении с методами косвенного встраивания алгоритмы непосредственного встраивания характеризуются:

- простотой реализации алгоритма;

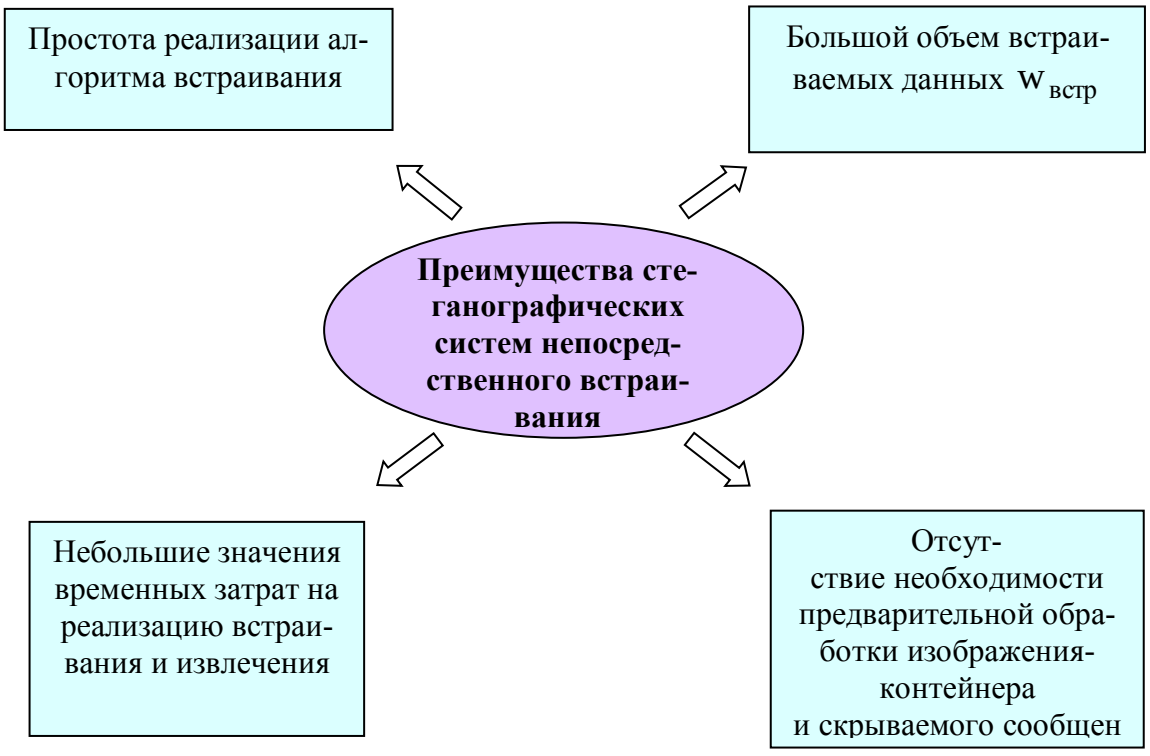

Рис. 1.9. Преимущества стеганографических систем непосредственного встраивания

- большим объемом встраиваемых данных $w_{встр}$;

- небольшими значениями временных затрат на реализацию встраивания и извлечения, при которых время встраивания и время изъятия являются наименьшими;

- отсутствием необходимости предварительной обработки изображения-контейнера и скрываемого сообщения.

Среди методов непосредственного встраивания наиболее широко используемыми на практике являются методы встраивания в наименее значимый бит и методы на основе расширения спектра.

Проведем анализ эффективности данных стеганографических методов. При этом необходимо учитывать возможность применения злоумышленником активных и пассивных атак в условиях проведения специальных операций, приведенных в табл. 1.2.

Таблица 1.2

Спектр основных атак на стеганографическую систему

	Цель осуществления атаки		
	Выявление факта наличия встраивания	Разрушение встроенного сообщения	Изъятие (раскрытие) встроенного сообщения
Активные (преднамеренные)	Визуальная атака	Шумы в канале передачи данных	
Пассивные (непреднамеренные)	Стеганографический анализ	Постановка помех, компрессионные атаки	Стеганографический анализ

В этом случае противник может применить атаки [59, 71, 94, 96, 100], направленные на: выявление факта наличия встраивания в изображении специальной информации; разрушение встроенного сообщения; изъятие (раскрытие) встроенного сообщения.

Проведем оценку относительной стеганографической емкости $w_{отн}^{(m)}$ для следующих методов:

- метод встраивания информации в наименее значимый бит элемента спектрального представления контейнера после квантования (режим 2 НЗБ);

- метод встраивания информации на основе расширения спектра (РС).

Рассмотрим режим 2 для метода НЗБ. Этот режим предусматривает непосредственную замену бит двоичного представления элемента спектрального представления изображения-контейнера после квантования на значения бит скрываемой информации. Другими словами, данный режим метода НЗБ позволяет встраивать 1 бит скрываемой информации в ω элементов спектрального представления изображения после квантования. Абсолютная стеганографическая емкость $w_{встр}^{(z_{строк}\, z_{столб})}$ метода НЗБ в режиме 2 зависит от размера контейнера и определяется на основе следующего выражения:

$$w_{встр}^{(z_{строк}\, z_{столб})} = \frac{3 \cdot z_{строк}\ z_{столб}}{\omega} \text{ (бит)}, \qquad (1.1)$$

где $z_{строк}\, z_{столб}$ - размер изображения-контейнера,

ω - количество элементов спектрального представления, необходимых для встраивания 1 бита скрываемой информации.

Выражение для определения относительной стеганографической емкости $w_{отн}^{z_{строк}\, z_{столб}}$ метода НЗБ в режиме 2 имеет вид:

$$w_{отн}^{z_{строк}\, z_{столб}} = \frac{w_{встр}^{z_{строк}\, z_{столб}}}{W_{исх}} \cdot 100\ \%. \qquad (1.2)$$

Объем $W_{исх}$ исходного изображения для метода НЗБ в режиме 2 определяется, как произведение общего количества элементов спектрального представления изображения-контейнера на количество бит, необходимое для

двоичного представления одного элемента (8 бит). В этом случае объем $W_{исх}$ исходного изображения определяется по формуле:

$$W_{исх} = 8 \cdot 3 \cdot z_{строк}\ z_{столб} = 24 \cdot z_{строк}\ z_{столб}\ (бит) \qquad (1.3)$$

Перепишем формулу для относительной стеганографической емкости метода с учетом выражений (1.1) и (1.3). Тогда получим:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{w_{встр}^{z_{строк}\ z_{столб}}}{W_{исх}} \cdot 100\% = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot \omega} \cdot 100\%.$$

В этом случае в зависимости от количества элементов ω, необходимых для встраивания относительная стеганографическая емкость $w_{отн}^{z_{строк}\ z_{столб}}$ метода НЗБ в режиме 2 примет следующие значения:

- для $\omega = 2$:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot 2} \cdot 100\% = \frac{1}{16} \cdot 100\ \% = 6{,}25\ \%;$$

- для $\omega = 4$:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot 4} \cdot 100\% = \frac{1}{32} \cdot 100\ \% = 3{,}1\ \%.$$

Рассмотрим метод встраивания информации на основе расширения спектра. При встраивании информации на основе метода PC, 1 бит скрываемого сообщения встраивается в фрагмент изображения, содержащий ω эле-

ментов. Абсолютная стеганографическая емкость $w_{встр}^{z_{строк}\, z_{столб}}$ для данного метода определяется на основе следующего выражения:

$$w_{встр}^{z_{строк}\, z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{\omega} \text{ (бит).} \qquad (1.4)$$

Рассмотрим теперь метод встраивания информации на основе расширения спектра. Относительная стеганографическая емкость $w_{отн}^{z_{строк}\, z_{столб}}$ для данного метода определяется на основе выражения (1.2), а объем $W_{исх}$ исходного изображения-контейнера для метода РС определяется на основе выражения (1.3). В этом случае формула для определения значения $w_{отн}^{z_{строк}\, z_{столб}}$ относительной стеганографической емкости примет следующий вид:

$$w_{отн}^{z_{строк}\, z_{столб}} = \frac{w_{встр}^{z_{строк}\, z_{столб}}}{W_{исх}} \cdot 100\% =$$

$$= (3 \cdot z_{строк}\ z_{столб} / \omega) / 24 \cdot z_{строк}\ z_{столб} \cdot 100\ \%$$

Тогда в случае встраивании 4 бит скрываемого сообщения в блок размером 8×8 относительная пропускная способность для метода РС примет следующее значение:

$$w_{отн}^{z_{строк}\, z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб} \cdot 4}{24 \cdot z_{строк}\ z_{столб} \cdot 64} = \frac{1}{128} \cdot 100\ \% = 0{,}78\ \%.$$

В табл. 1.3 представлены значения относительной стеганографической емкости методов НЗБ в режиме 2 и РС для различных классов изображений.

Таблица 1.3

Зависимость значения $w_{отн}$ от ПОСШ для методов НЗБ и РС для различных классов изображений

Относительная емкость, %	Метод стеганографического встраивания		Значение ПОСШ, дБ		
			«Снимок аэропорта»	«Фото снимок»	«Самолет на фоне неба»
6,25	НЗБ режим 2	$q = 1$	14,67	14,12	14,62
		$q = 2$	11,17	12,03	11,13
		$q = 4$	8,69	9,11	8,79
3,1	НЗБ режим 2	$q = 1$	32,12	33,42	31,43
		$q = 2$	26,43	22,15	20,45
		$q = 4$	18,54	18,27	18,03
0,78	РС	$\omega = 16$	16,93	13,019	18,121

Из анализа значений в табл.1.3 можно сделать вывод, что значение относительной стеганографической емкости для рассматриваемых методов принимает значение от 0,78 до 6,25 %.

Теперь проведем оценку значения вероятность $P_{из}$ безошибочного изъятия встроенных данных для методов встраивания НЗБ и РС.

Для метода НЗБ в режиме 2 объем $w_{из}^{z_{строк}\ z_{столб}}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение меньше $w_{встр}^{z_{строк}\ z_{столб}}$ встроенных данных, т.е.

$$w_{из}^{z_{строк}\ z_{столб}} < w_{встр}^{z_{строк}\ z_{столб}}.$$

Для такого метода вероятность безошибочного изъятия встроенных данных буде равно $P_{из} = 0{,}6$.

Теперь рассмотрим вероятность безошибочного изъятия встроенных данных для метода РС. В случае встраивания бита скрываемого сообщения

на основе метода РС, его изъятие будет осуществляться с вероятностью $P_{из} = 0{,}5$.

На рис. 1.10. представлены диаграммы значений вероятности $P_{из}$ безошибочного изъятия встроенных данных для методов НЗБ в режиме 2 и РС в условиях отсутствия атак на встроенное сообщение.

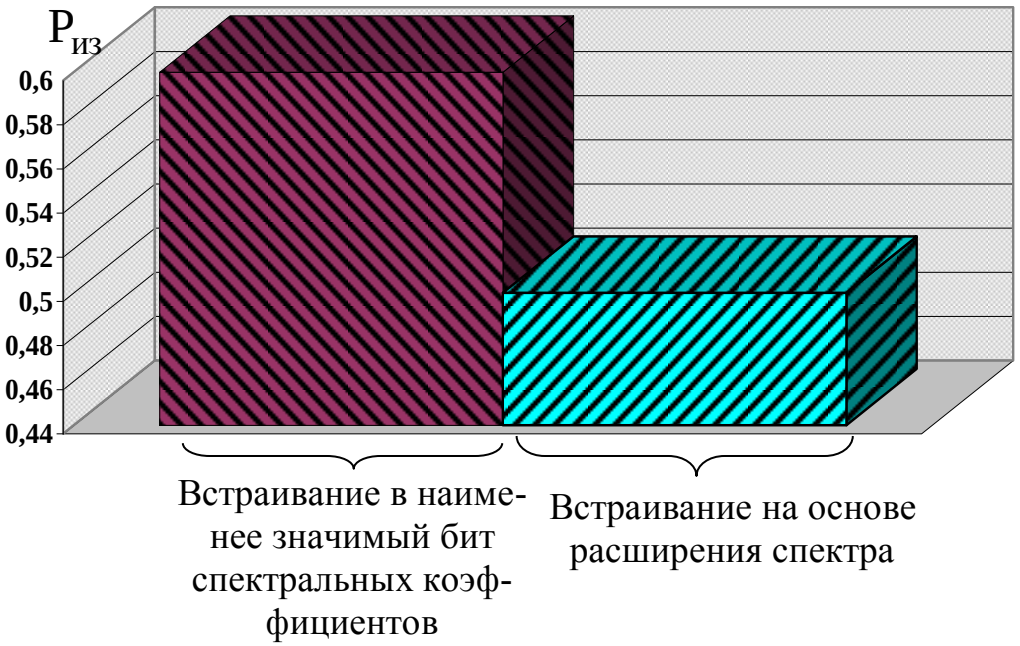

Рис. 1.10. Диаграмма значений вероятности $P_{из}$ для методов НЗБ в режиме 2, РС условиях отсутствия атак на встроенное сообщение

Из анализа рис. 1.10 можно сделать выводы что:

- вероятность безошибочного изъятия встроенных данных для метода НЗБ и РС принимает значение от 0,5 до 0,6;

- для метода НЗБ в режиме 2 выигрыш относительно метода РС по значению вероятности безошибочного изъятия встроенных данных составляет 0,1.

Теперь проведем оценку вероятности безошибочного изъятия встроенных данных в условиях атаки противника с применением ДКП и квантования. Для этого сравним процентные значения количества $w_{из}^{(z_{строк} z_{столб})}$ изъ-

ятых бит относительно количества $w_{встр}^{(z_{строк}z_{столб})}$ встроенных бит для метода РС.

Для метода НЗБ в режиме 2 и РС количество $w_{из}^{(z_{строк}z_{столб})}$ безошибочно изъятых бит в условиях активных атак составляет 50%.

На рис. 1.11 представлена диаграмма процентного значения количества безошибочно изъятых бит для методов НЗБ в режиме 2, РС в условиях применения атаки ДКП и квантования с шагом $q = 1; 5$.

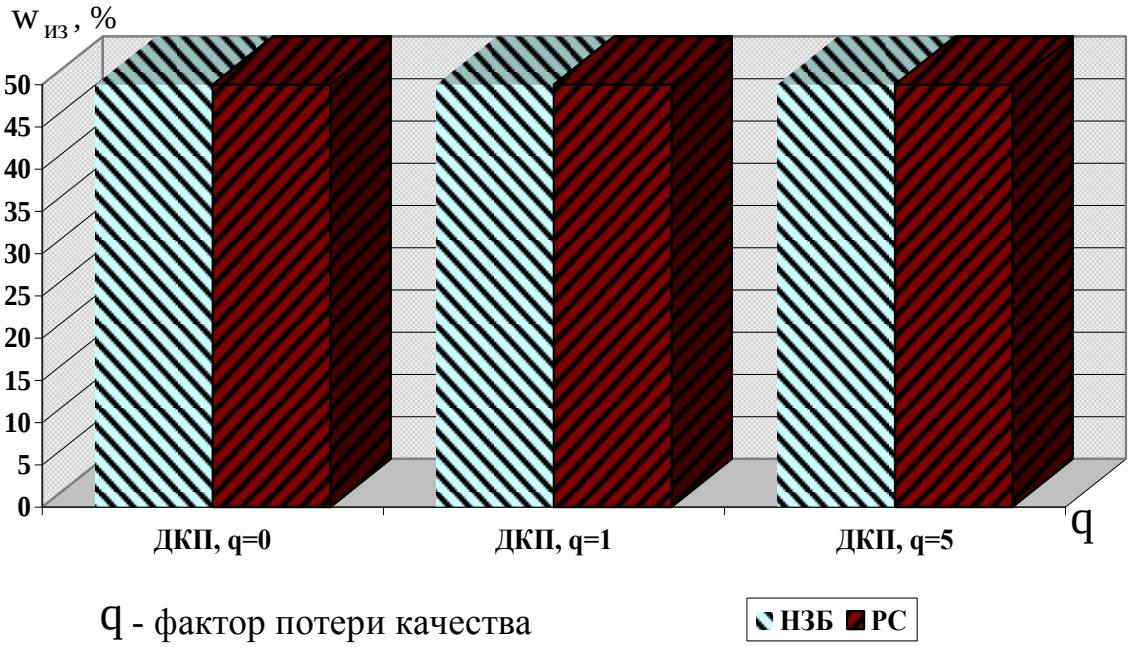

Рис. 1.11. Сравнительная диаграмма значений $w_{из}$ безошибочно изъятых данных для методов НЗБ и РС в условиях атак

Из анализа рис. 1.11 можно сделать вывод, что для различных коэффициентов квантования количество $w_{из}^{(m)}$ безошибочно изъятых бит для методов НЗБ в режиме 2 и РС принимает значение 50%.

Результаты исследований существующих стеганографических систем показали, что методы непосредственного стеганографического встраивания имеют недостатки относительно значения стеганографической емкости, пикового отношения сигнал-шум и вероятности безошибочного изъятия встроенных данных.

1.4 Постановка задачи на исследование

Удовлетворение требований к информационному обеспечению критических систем связано с повышением требований относительно характеристик функционирования существующих стеганографических методов для крытой передачи СИР. В этом случае для существующих стеганографических преобразований появляется следующие требования:

1. Необходимость повышения относительной стеганографической емкости стеганографической системы $w_{отн}$. Данное требование диктуется постоянным ростом объемов и увеличением содержательной значимости СИР.

2. Необходимость повышения вероятности $P_{из}$ изъятия встроенных данных в условиях применения активных атак. Наличие обширных возможностей злоумышленника относительно атак, направленных на разрушение и модификацию встроенных данных, сопровождается повышенными требованиями к стеганографическим методам относительно безошибочного изъятия встроенных данных.

3. Необходимость увеличения пикового отношения сигнал шум изображения со встроенными данными h. Для обеспечения стойкости изображения со встроенными данными к визуальным атакам, направленным на установление факта наличия стеганографического встраивания.

Данные требования диктуются особенностями условий, в которых функционируют критические системы [6, 38, 53, 60, 69, 80], а именно:

- использование беспроводных технологий с расширенными возможностями относительно предъявляемых видеоуслуг;

- развитие информационно-математического и программно-аппаратного обеспечения у злоумышленника включая методы стегоанализа, быстродействия вычислительных комплексов, новейших технологий распределения вычислений;

- повышение значимости для злоумышленника в доступе к специальной информации в условиях функционирования критических систем, что сопровождается ростом скрываемой информации;

- возможность применения злоумышленником нестандартных технологий несанкционированного доступа к скрываемой информации.

В тоже время повышаются требования к информационному обеспечению при обмене СИР в критических системах. Такие требования обусловлены следующими факторами:

- повышение объемов доведения специальных донесений и распоряжений в условиях кризисных ситуаций;

- использование видеоматериалов в качестве донесений;

- использование для информационного обеспечения новейших информационно-вычислительных средств и технологий (фото и видеоаппаратура);

- повышение значимости влияния донесений на результативность функционирования критических систем, т.е. от достоверности, целостности и оперативности доведения донесений зависят жизни людей, политический и экономический имидж государства;

- повышение требований относительно достоверности и наглядности донесений (полнота и качество наглядности специальной информации);

- необходимость оперативной доставки скрытых сообщений в ограниченные временные промежутки сеанса связи;

- необходимость обеспечения и контроля использования пропагандистского поля противостояния.

Значит, в процессе использования существующих стеганографических систем для скрытой передачи специальной информации возникает ***противоречие*** (рис 1.12), которое заключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере

Рис. 1.12. Структура наличия противоречия при использовании существующих стеганографических методов для обеспечения функционирования критических систем

системных требований в критических условиях с активным противостоянием противнику.

Для совершенствования существующих и разработки новых методов стеганографических преобразований необходимо использовать альтернативные источники избыточности изображения. Актуальным направлением является использование структурных преобразований элементов пространственного представления изображения для выявления структурной избыточности. Такой подход позволит повысить стойкость встроенных данных к активным атакам противника.

Отсюда, ***цель исследований*** заключается в разработке метода повышения безопасности специальной информации на основе стеганографического преобразования, задаваемого функционалом $F\{ P_{из},\ w_{отн},\ h \}$ в условиях выполнения следующих ограничений:

$$\begin{cases} P_{из} \geq P_{из}^{(тр)}; \\ w_{отн} \geq w_{отн}^{(тр)}; \\ h \geq h^{(тр)}; \end{cases}$$

где $F\{ P_{из},\ w_{отн},\ h \}$ - функционал, который реализует стеганографический метод встраивания специальной информации;

$w_{отн}^{(тр)}$ - требуемое значение относительной стеганографической емкости системы;

$h^{(тр)}$ - требуемое значение пикового отношения сигнал-шум

Таким образом, для достижения поставленной цели необходимо решить следующие задачи:

- обосновать подход для совершенствования методов непосредственного встраивания информации в цифровое изображение-контейнер;
- разработать метод структурного кодирования для повышения безопасности специальной информации;

- создать метод для локализации структурной стеганографической избыточности для повышения устойчивости относительно атак на выявление факта встроенной информации;
- построить структурную стеганографическую систему с маскированием стеганографической избыточности;
- разработать программную реализацию и провести оценку эффективности разработанной стеганографической системы.

Выводы

1. Обоснована необходимость повышения безопасности специальных информационных ресурсов в системах критического назначения. Такая необходимость диктуется повышенной значимостью СИР для информационной поддержки функционирования систем критического назначения, а также повышением угрозы их конфиденциальности и целостности.

2. Предложен подход для повышения безопасности СИР, который заключается в использовании методов цифровой стеганографии для скрытой передачи информации. Для этого обоснованы преимущества использование в качестве контейнера цифрового изображения.

3. Проведена классификация стеганографических методов по логике встраивания. Рассмотрены методы непосредственного стеганографического встраивания информации в изображение-контейнер, а именно:

- метод встраивания в наименее значимый бит коэффициентов спектрального представления изображения после квантования;

- метод встраивания на основе расширения спектра.

4. Рассмотрены основные показатели эффективности стеганографических преобразований. К основным показателям относятся следующие:

- относительная стеганографическая емкость системы;

- вероятность безошибочного изъятия встроенных данных;

- пиковое отношение сигнал-шум изображения со встроенными данными.

Сравнение и оценка существующих стеганографических методов на основе приведенных показателей позволяют проанализировать успешность их использования для скрытой передачи специальной информации.

5. Проведена оценка методов непосредственного встраивания по относительной стеганографической емкости, вероятности безошибочного изъятия встроенных данных и пиковому отношению сигнал-шум изображения со встроенными данными. На основании полученных результатов можно заключить следующее:

- значение относительной стеганографической емкости методов НЗБ в режиме 2 и РС принимает значение от 0,78 до 6,25 %;

- значение вероятности безошибочного изъятия встроенных данных в условиях отсутствия атак для методов НЗБ в режиме 2 и РС принимает значение от 0,5 до 0,6

- количество безошибочно изъятых бит в условиях применения противником атак для методов НЗБ в режиме 2 и РС принимает значение 50 %.

5. Сформулировано противоречие, которое заключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере системных требований в критических условиях с активным противостоянием противнику.

6. Обосновано направления для разработки метода встраивания, которое основывается на структурных преобразованиях элементов для выявления структурной избыточности изображений. Сформулировано цель исследований, которая заключается в разработке метода повышения безопасности специальной информации на основе стеганографического преобразования для систем критического назначения.

РАЗДЕЛ 2

ОБОСНОВАНИЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ТЕХНОЛОГИЙ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

В разделе проведено обоснование направления для устранения недостатков существующих методов непосредственного встраивания.

Показано, что методы встраивания на позицию младшего бита характеризуется низкой устойчивостью встроенных данных к активным атакам противника и минимальным значением вносимых визуальных искажений. Наоборот встраивание старший бит обладает большим уровнем стойкости встроенных данных к атакующим воздействиям. Но в этом случае в процессе встраивания вносятся значительные визуальные искажения.

Для устранения выявленных недостатков предлагается подход в виде функционального преобразования числа со встроенными данными. Формулируются требования для синтезированного функционального преобразования. Строится структурная схема стеганографического преобразования на основе функционала от числа со встроенными данными.

Обосновывается необходимость использования в качестве функционала для числа со встроенными данными кодообразующей функции для неравновесного позиционного числа. Разрабатывается структурная схема стеганографической системы на основе неравновесного позиционного кодирования.

2.1. Обоснование проблемных сторон функционирования технологий непосредственного стеганографического встраивания

Рассмотрим класс методов непосредственного встраивания скрываемой информации в изображение-контейнер.

По логике встраивания, современные стеганографические системы разделяются на алгоритмы непосредственного встраивания и алгоритмы косвенного встраивания.

В методах непосредственного встраивания бит информационной последовательности скрываемого сообщения заменяется на бит данных изображения контейнера. Непосредственная логика встраивания реализована в семействах методов встраивания в значения элементов представления изображения-контейнера [115, 118]. Также непосредственное встраивание осуществляется в коэффициенты ДКП и в величины таблицы квантования компрессионного алгоритма JPEG (рис 2.1.) [82, 116, 120].

Встраивание бита информационной последовательности скрываемого сообщения в косвенных методах осуществляется путем создания зависимости между некоторыми параметрами изображения контейнера по определенному алгоритму. Благодаря тому, что данный алгоритм заранее известен на приемной стороне, стегодекодер выделяет логический 0 или 1 бит встроенной информационной последовательности. Современные алгоритмы косвенного встраивания представлены спектральными методами встраивания, методами модификации яркости и методами замены палитры.

Для решения задач скрытого встраивания данных методы непосредственного встраивания имеют ряд преимуществ. В сравнении с методами косвенного встраивания алгоритмы непосредственного встраивания характеризуются:

- простотой реализации алгоритма;

- большим объемом встраиваемых данных $w_{встр}$;

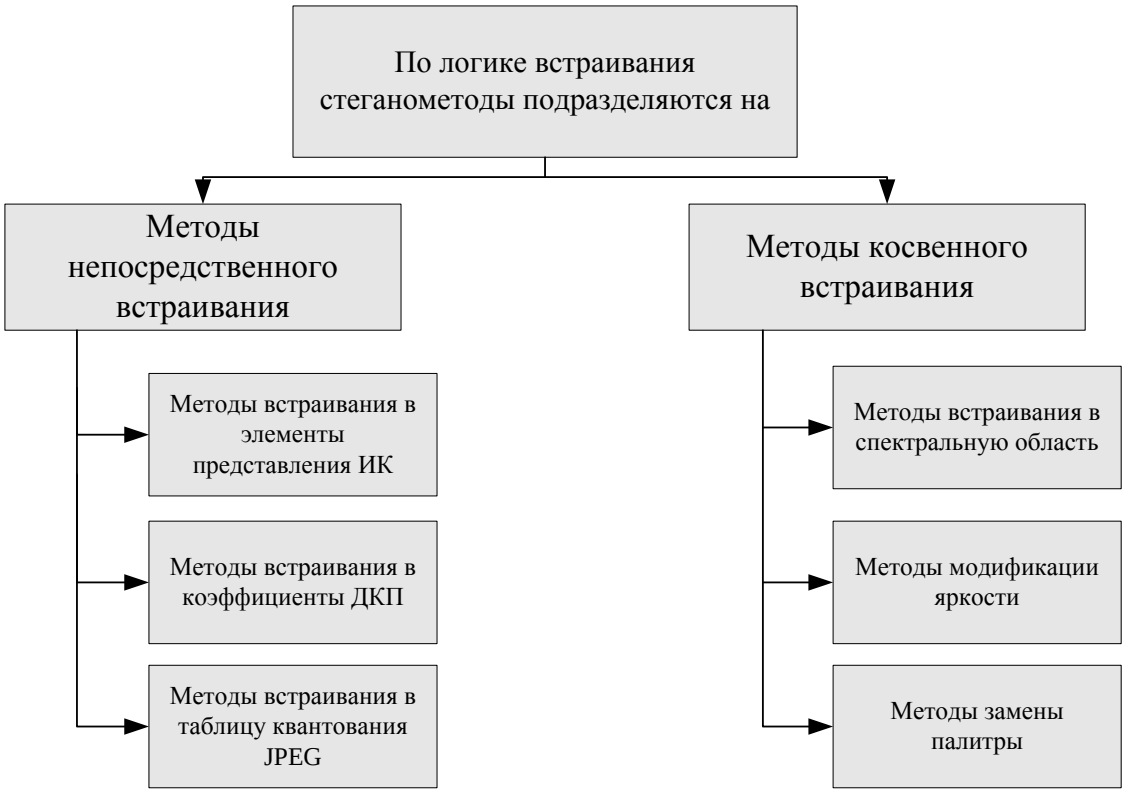

Рис. 2.1. Классификация стеганографических алгоритмов по логике встраивания

- небольшими значениями временных затрат на реализацию встраивания и извлечения, при которых время встраивания $\tau_{(W_{встр})пр}$ и время изъятия $\tau_{(W_{встр})обр}$ являются наименьшими;

- отсутствием необходимости предварительной обработки изображения-контейнера и скрываемого сообщения.

Непосредственное встраивание СС может осуществляться как в пространственно-временную, так и в пространственно-частотную область изображения-контейнера [23, 52, 65, 82, 90, 116, 120]. Как правило, такое встраивание проводится в отдельный элемент текущего представления ИК (рис. 2.2), точнее в отдельные биты элемента. В данном случае элемент представляет собой двоичное позиционное число A_2 с основанием равным двум, т.е. $A_2 = [A]_2$.

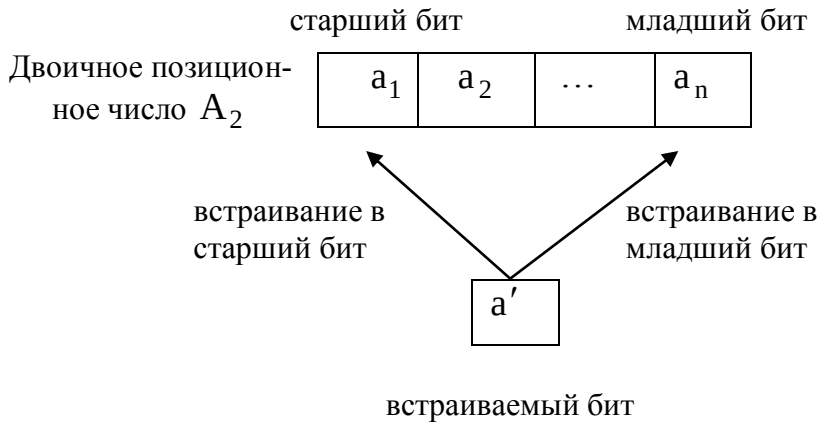

Рис. 2.2. Схема встраивания бита СС в элемент текущего представления ИК

Это может быть пиксель пространственно-временного представления изображения или компонента его спектрального представления. В этих случаях элемент, в который осуществляется встраивание бита (группы бит) СС, называется загруженным (модифицируемым, стегано-преобразованным) элементом изображения-контейнера.

Процесс непосредственного встраивание фактически представляет собой замену одного бита исходного элемента-контейнера на бит скрываемого сообщения с использованием некоторого функционала φ_2, условия или правила.

В существующих стегнаографических методах наиболее проработанные подходы, основываются на встраивании информации в наименее значимый младший (НЗБ) бит. В связи с чем, рассмотрим характеристики таких стеганосистем.

Метод встраивания в наименее значащий бит осуществляет замену младшего бита a_n двоичного позиционного числа A_2 на бит b_ξ встраиваемого сообщения B (рис 2.2). Это описывается следующим выражением:

$$a'_n = b_\xi, \quad A'_2 = \{a_1, a_2, ..., a_{n-1}, a'_n\},$$

где A'_2 - число, содержащее встроенный бит a'_n скрываемого сообщения.

Здесь b_ξ - ξ-й элемент, встраиваемой двоичной последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$, $a'_i \in [0;1]$; $b_\xi \in [0;1]$, $i = \overline{1,n}$; $\xi = \overline{1,\nu}$.

Такой подход для встраивания скрываемой информации характеризуется тем, что количественная метрика $\varepsilon(A;A')$, указывающая на степень отличия между значением элемента A исходного изображением до встраивания информации (изображение-контейнер) и значением A' этого же элемента изображения со встроенной информацией (стеганограммой) будет наименьшей:

$$\varepsilon(A;A') \to 0.$$

В тоже время данный принцип встраивания отличается низкой устойчивостью стеганограммы относительно трансформирующих и атакующих воздействий. В этом случае вероятность $P_{из}$ того, что элемент b_ξ скрываемого сообщения будет изъят без ошибок стремится к нулю, т.е.

$$P_{из}(b'_\xi = b_\xi) \to 0$$

или соответственно вероятность $\overline{P}_{из}$ того, что элемент b_ξ скрываемого сообщения изъят с ошибкой будет наибольшей

$$P_{из}(b'_\xi \neq b_\xi) \to 1.$$

Здесь b'_ξ- значение ξ-го элемента скрываемого сообщения, который изымается при наличии трансформирующего или атакующего воздействия; $(b'_\xi = b_\xi)$- событие, состоящее в том, что значения b_ξ элемента скрываемого сообщения до атаки и полученного b'_ξ после атаки будут равными;

$(b'_\xi \neq b_\xi)$ - событие, состоящее в том, что значение элемента скрываемого сообщения до атаки b_ξ и полученного после атаки b'_ξ будут неравными.

Другими словами, если использовать количественную метрику $\delta(B'_2; B_2)$, указывающую на степень отличия между исходным сообщением B_2 и изъятым на приемной стороне сообщением B'_2, то будет выполняться соотношение

$$\delta(B'_2; B_2) \to \max.$$

Наоборот метод встраивания элемента скрываемого сообщения в старший бит исходного числа A_2, т.е.

$$A'_2 = \{a'_1, a_2, a_n\}; \quad a'_1 := b_\xi,$$

повышает стойкость встроенных данных к трансформации и атакам. Тогда вероятность $P_{из}$ того, что элемент b_ξ скрываемого сообщения изъят без ошибок, будет наибольшей, т.е.

$$P_{из}(b'_\xi = b_\xi) \to 1,$$

а вероятность $\overline{P}_{из}$ того, что элемент b_ξ скрываемого сообщения изъят с ошибкой будет наименьшей

$$P_{из}(b'_\xi \neq b_\xi) \to 0.$$

Здесь A'_2 - число-стеганограмма, содержащее встроенный бит a'_1 скрываемого сообщения, b_ξ - ξ-й элемент встраиваемой двоичной последова-

тельности $B_2 = \{b_1;...;b_\xi;...;b_\nu\}$, $a'_i \in [0;1]$; $b_\xi \in [0;1]$; $i = \overline{1,n}$; $\xi = \overline{1,\nu}$; b'_ξ - элемент сообщения, изъятый при наличии атакующего воздействия.

Однако такое встраивание вносит существенные искажения с позиции визуального восприятия изображения-контейнера. Здесь значение количественной метрики $\varepsilon(A;A')$ будет наибольшей, т.е.

$$\varepsilon(A;A') \to \max.$$

Обобщенно недостатки непосредственного встраивания бита СС в элемент-контейнер задаются следующим соотношением:

$$a'_\tau := \begin{cases} b_\xi \ \& \ P_{из}(b'_\xi = b_\xi) \to 0 \ \& \ \varepsilon(A;A') \to 0 \ \& \ \delta(B'_2;B_2) \to \max, \ \tau \to n; \\ b_\xi \ \& \ P_{из}(b'_\xi = b_\xi) \to 1 \ \& \ \varepsilon(A;A') \to \max \ \& \ \delta(B'_2;B_2) \to 0, \ \tau \to 1. \end{cases}$$

При встраивании бита СС в старший бит исходного числа наблюдается стойкость встроенных данных при значительных визуальных искажениях и наоборот, встраивание СС в младший бит характеризуется низкой стойкостью встроенных данных при минимальных визуальных искажениях.

2.2. Обоснование подхода для построения технологии устранения недостатков непосредственного стеганографического встраивания

Для устранения выявленных недостатков, т.е. обеспечения визуальной устойчивости стеганограммы, при которой значение количественной метрики $\varepsilon(A;A')$ будет наименьшим, т.е.

$$\varepsilon(A;A') \to 0$$

и устойчивости к трансформации и атакам предлагается синтезировать функционал $f(A')$ от ***числа*** со встроенной информацией [13]. Такой функционал должен обеспечить следующие требования:

1) взаимооднозначность прямого $f(A')$ и обратного $f^{(-1)}(C)$ преобразований. В этом случае должен существовать обратный функционал $f^{(-1)}(C)$, позволяющий авторизированному пользователю получить скрываемое сообщение без потери информации, т.е. количественная метрика $\delta(B_2';B_2)$, указывающая на степень отличия между исходным сообщением B_2 и изъятым на приемной стороне сообщением B_2', будет принимать нулевое значение

$$\delta(B_2';B_2) = 0$$

2) возможность осуществлять обратное преобразование (реконструкцию) по биполярному принципу. Биполярность заключается в том, что для функционала $f(A')$ существует два варианта обратного преобразования. Первый вариант является стандартным. Он используется неавторизированным пользователем (злоумышленником), а восстановление изображения осуществляется для стандартных условий $\Psi^{(1)}$, необходимых для достовер-

ной реконструкции элементов $A(1)''$ изображения-контейнера (позиционного числа)

$$A(1)'' = f^{(-1)}(C;\Psi^{(1)}).$$

Для такого варианта должно обеспечиваться отсутствие визуальных искажений в реконструируемом изображении, что задается условием, при котором:

- значение количественной метрика $\varepsilon(A;A(1)'')$ будет наименьшим, т.е.

$$\varepsilon(A;A(1)'') \to 0, \quad \text{где} \quad A(1)'' = f^{(-1)}(C;\Psi^{(1)}),$$

- осуществляется блокировка возможности успешного стеганоанализа и изъятия сообщения.

Условия блокирования изъятия встроенного сообщения задается следующим соотношением

$$\delta(B_2'';B_2) \to \max.$$

Здесь B_2'' - скрываемое сообщение, полученное при декодировании неавторизированным пользователем.

Второй вариант наоборот, существует для авторизированного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием ключа $\Psi^{(2)}$ или по определенному условию известному авторизированным пользователям, так что $\Psi^{(2)} \neq \Psi^{(1)}$, т.е.

$$A(2)'' = f^{(-1)}(C;\Psi^{(2)}).$$

В процессе чего формируется число $A(2)''$ со встроенными данными, так чтобы выполнялись следующие условия:

- обеспечивалось безошибочное изъятие по известному оператору $\varphi^{(-1)}$ (оператору выборки элемента) встраиваемого элемента b'_ξ скрываемого сообщения, т.е.

$$b'_\xi = \varphi^{(-1)}(A(2)'') \quad \text{и} \quad \delta(B'_2; B_2) = 0;$$

- метрика $\varepsilon(A; A(2)'')$, указывающая на степень отличия между числом A, составленным для исходного изображением до встраивания информации (изображением-контейнером) и числом $A(2)''$ соответствующего изображению со встроенной информацией (стеганограммой) принимала наименьшее значение, т.е.

$$\varepsilon(A; A(2)'') \to 0.$$

Процесс изъятия элемента b'_ξ скрываемого сообщения B' описывается соотношением

$$b'_\xi = \varphi^{(-1)}(f^{(-1)}(C)).$$

Здесь $\varphi^{(-1)}$ - оператор изъятия.

Формула, которая описывает реконструкцию числа $A(2)''$ на приемной стороне по известной стеганограмме и ключевой информации имеет вид:

$$A(2)'' = f^{(-1)}(C; \Psi^{(2)}).$$

При изъятии встроенной информации авторизированным пользователем количественная метрика $\delta(B_2'; B_2)$, указывающая на степень отличия между исходным встраиваемым сообщением B и изъятым на приемной стороне сообщением B', будет принимать нулевое значение:

$$\delta(B_2'; B_2) = 0.$$

Требование биполярности можно обобщить следующей системой выражений:

$$A(\gamma)'' = f^{(-1)}(C;\ \Psi^{(\gamma)}),$$

$$\delta(B'; B) \to \begin{cases} \max, \to \gamma = 1\ \ \& \ \ \Psi = \Psi^{(1)}, \\ 0, \quad \to \gamma = 2\ \ \& \ \ \Psi = \Psi^{(2)}; \end{cases}$$

3) функциональное преобразование должно быть инвариантным к атакующим воздействиям (ошибки в канале связи, пережатие ДКП с квантованием). Должна обеспечиваться устойчивость скрываемого сообщения, т.е. возможность его достоверного (целостного) изъятия в случае последующего сжатия, проведения атак и воздействия ошибок канала связи. Другими словами, количественная метрика $\alpha(A;\ A'')$, указывающая на степень отличия между числом A составленного для исходного изображения при отсутствии атакующего воздействия (изображение-контейнером) и числом A'' соответствующего изображению со встроенной информацией при наличии атакующего воздействия должна быть наименьшей:

$$\alpha(A;\ A'') \to 0.$$

Далее обоснуем свойства функционалов, которыми они должны обладать для соответствия требованиям относительно устойчивости процесса скрытия сообщений.

Для соответствия требованиям визуальной устойчивости числа A' со встроенными данными, устойчивости к трансформированию и атакам, синтезированный функционал $f(A')$ должен обладать следующими свойствами [13]:

1) формирование стеганограммы C с использованием стеганообразующего функционала должно осуществляться по интегральному принципу в два этапа. На первом этапе как результат применения функционала $f(A')$ к числу A' формируется кодовое значение N, содержащее информацию об элементах числа A', т.е.

$$N = f(A').$$

На основе сформированного значения N на втором этапе строится результирующее кодовое представление C стеганограммы

$$C_2 = \varphi_c(N).$$

Здесь φ_c - оператор, обеспечивающий построение двоичного кода C_2 для кодового значения N. В этом случае получим

$$C_2 = \{c_1;...;c_q;...;c_Q\}, \quad c_q \in \{0; 1\},$$

где Q - количество бит на представления стеганограммы C_2.

2) количественная метрика $\varepsilon(A(1)'';A(2)'')$ указывающая на степень отличия числа $A(1)''$, восстановленного при стандартных условиях $\Psi^{(1)}$ неавторизированным пользователем

$$A(1)'' = f^{(-1)}(C;\Psi^{(1)})$$

и числа $A(2)''$, реконструированного авторизированным пользователем с использованием ключа $\Psi^{(2)}$

$$A(2)'' = f^{(-1)}(C;\Psi^{(2)}),$$

не должна превышать значения порога визуальной незначимости μ, т.е.

$$\varepsilon \in 0..\mu.$$

3) стеганограмма C, должна содержать сведения о векторе служебной информации $\Psi^{(1)}$, при наличии которой возможна реконструкция элементов $A(1)''$ изображения контейнера при отсутствии информации о наличии встроенного сообщения

$$C_2 = \varphi_c(N, \Psi^{(1)}) \qquad A(1)'' = f^{(-1)}(C;\Psi^{(1)}).$$

4) извлечения элемента b'_ξ скрываемого сообщения B'_2 противником, при наличии у него информации о наличии встраивания, возможно только при известном ключе $\Psi^{(2)}$(ключевой информации). Такая ключевая информация может представлять собой условия, с учетом которых происходило встраивание скрываемого сообщения или же принимать значение некоторого симметричного ключа $\Psi^{(2)}$ известного на приемной и передающее стороне. Выражение, описывающее выполнение обратного функционала будет иметь вид:

$$A(2)'' = f^{(-1)}(C; \Psi^{(2)}).$$

5) Служебная составляющая $\Psi^{(1)}$ должна иметь определяющее значение при формировании кодограммы таким образом, что бы безошибочная реконструкция исходного изображения $A(1)''$ для неавторизированного пользователя достигалась только при наличии полных сведений о векторе служебных данных, т.е. если $\Psi^{(1)'} \neq \Psi^{(1)}$, то

$$C_2' = \varphi_c(N, \Psi^{(1)'}) \text{ и } A(1)'' \neq f^{(-1)}(C; \Psi^{(1)'}) \text{ где } C_2 \neq C_2'.$$

Здесь C_2' - значение двоичного кодового слова, восстановленного в результате использования вектора $\Psi^{(1)'}$ служебных данных, декодированных с ошибкой.

На рис. 2.3. представлена схема стеганографического преобразования на основе использования функционала для числа со встроенными данными [13, 15, 17-19].

Прямое стеганографическое преобразование включает следующие этапы:

1. Встраивание b_ξ скрываемого сообщения B_2 в число A при помощи оператора встраивания φ. Полученное в результате встраивания число A' определяется на основе следующего выражения

$$A' = \varphi(b_\xi; A).$$

2. Функциональное преобразование числа A' с имплантацией по правилу $f(A')$.

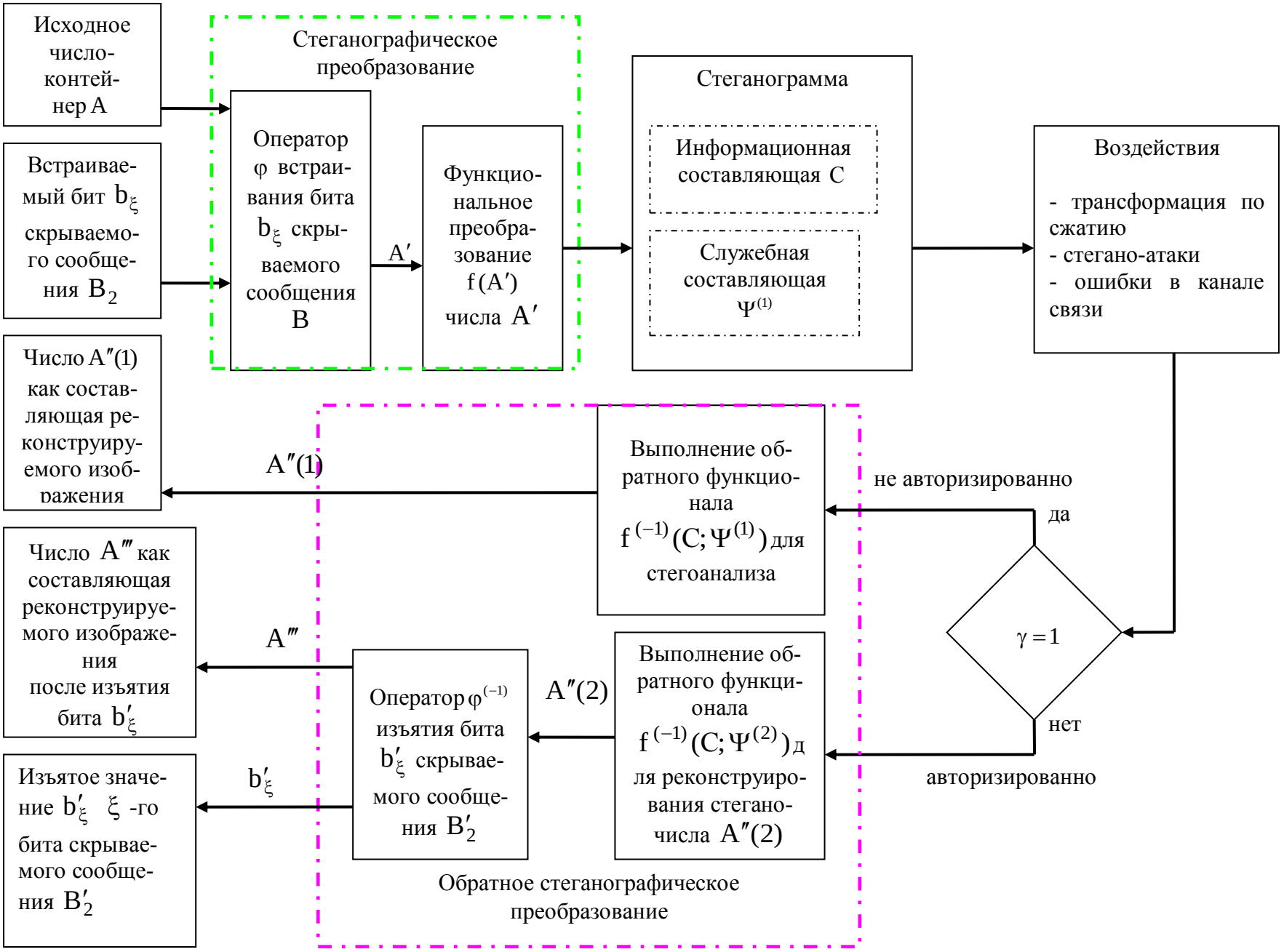

Рис 2.3. Схема стеганографического преобразования на основе использования функционала для числа со встроенными данными

Полученная стеганограмма, содержащая в себе информационную составляющую C и служебную составляющую $\Psi^{(1)}$, подвергается атакующим воздействиям.

Обратное стеганографическое преобразование осуществляется по биполярному принципу для авторизированного и неавторизированного пользователя (стегоанализ).

При стегоанализе, по правилу $f'^{(-1)}(\bullet)$ формируется число

$$A''(1) = f'^{(-1)}(C'; \Psi^{(1)}).$$

Здесь $A''(1)$ - число, как составляющая реконструируемого изображения, полученное в результате стегоанализа.

Для авторизованного пользователя обратное стеганографическое преобразование происходит в два этапа:

1. На первом этапе по правилу $f'^{(-1)}(\bullet)$ и с учетом ключевой информации $\Psi^{(2)}$ происходит реконструкция числа с имплантацией

$$A''(2) = f'^{(-1)}(C; \Psi^{(2)}).$$

2. На втором этапе в результате применения оператора изъятия $\varphi^{(-1)}$ из реконструированного числа $A''(2)$ со встроенными данными происходит изъятие b'_ξ скрываемого сообщения B_2 и реконструкция числа A''', как составляющего исходного изображения, что описывается выражением

$$\varphi^{(-1)}(A'(2)) = \begin{cases} b'_\xi \\ A''' \end{cases}.$$

2.3. Разработка технологии функционального преобразования чисел с имплантированными данными на основе неравновесного позиционного кодирования

В качестве преобразующего функционала, обладающего свойствами для соответствия требованиям относительно процесса скрытия данных предлагается использовать кодообразующую функцию для неравновесного позиционного числа (НПЧ кодирование), а в качестве элемента-контейнера предлагается использовать неравновесное позиционное число [10, 11, 12, 18, 19, 89].

В процессе неравновесного позиционного кодирования формируются кодовые комбинации, состоящие из двух частей, а именно: информационная составляющая N и служебная составляющие Ψ (рис. 2.4).

Рис. 2.4. Схема кодограммы для неравновесного позиционного числа

В этом случае исходный элемент изображения рассматривается как неравновесное позиционное числа A, состоящее из m элементов [10, 11, 12], а именно

$$A = \{a_{1,j};...; a_{i,j};...;a_{m,j}\}.$$

Для исходного НП числа (рис 2.5): A значения кода определяется по формуле:

$$N = f'(A),$$

где N- код исходного неравновесного позиционного числа A.

На втором этапе для сформированного значения кода N строится результирующее кодовое представление C_2 неравновесного позиционного числа A:

$$C_2 = \varphi_c(N, \Psi)$$

Здесь φ_c - оператор, обеспечивающий построение двоичного кода C_2 для кодового значения N и служебных данных Ψ .

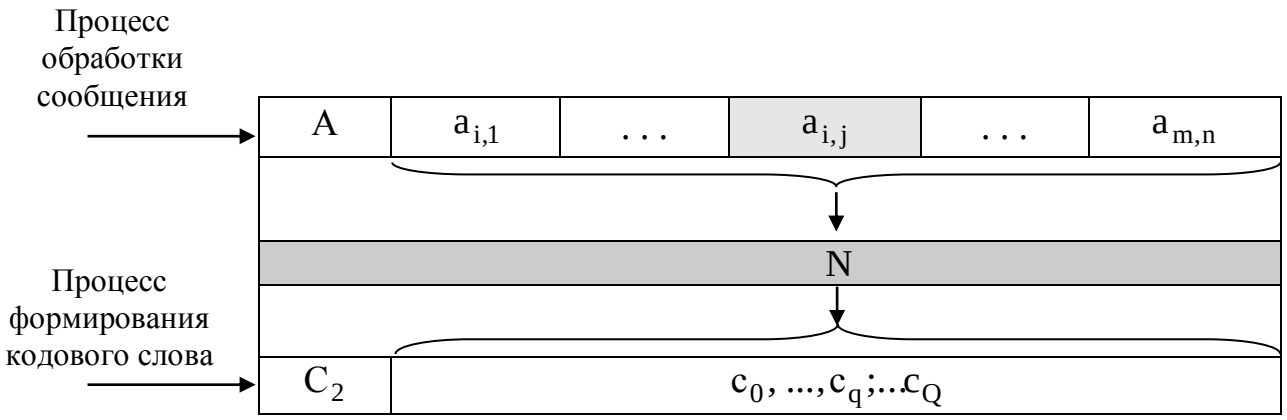

Рис. 2.5. Структурная схема построения кодовых конструкция для неравновесного позиционного числа A

В этом случае получим

$$C_2 = \{c_1; ...; c_q; ...; c_Q\}, \quad c_q \in \{0; 1\},$$

где Q - количество бит на представления НП числа C_2.

Служебная составляющая включает в себя информацию о системе оснований неравновесного позиционного числа $\Psi = \{\psi_{i,j}\}$.

В случае такого подхода для формирования кодового представления C_2 неравновесного позиционного числа A, оператор обратного функционального преобразования $f^{(-1)'}(\bullet)$ позволит получить исходное НП число A при наличии служебной информации Ψ. Выражение, которое описывает обратное функциональное преобразование имеет вид:

$$A = f^{(-1)'}(C_2; \Psi).$$

Для такого подхода принцип встраивания предлагается выбирать следующим образом (рис 2.6) [12, 21, 25].

В исходное неравновесное позиционное числа A при помощи оператора φ' встраивается бит b_ξ скрываемого сообщения В таким образом, что

$$A' = \varphi'(A; b_\xi).$$

Здесь A'- неравновесное позиционное число с встроенным битом b_ξ (НПЧ с встраиванием).

Затем определяется код N' для числа A':

$$N' = f'(A').$$

На третьем этапе для сформированного значения кода N' строится результирующее кодовое представление C_2' неравновесного позиционного числа A' со встраиванием:

$$C_2' = \varphi_c(N', \Psi^{(1)})$$

Здесь φ_c- оператор, обеспечивающий построение двоичного кода C_2'.

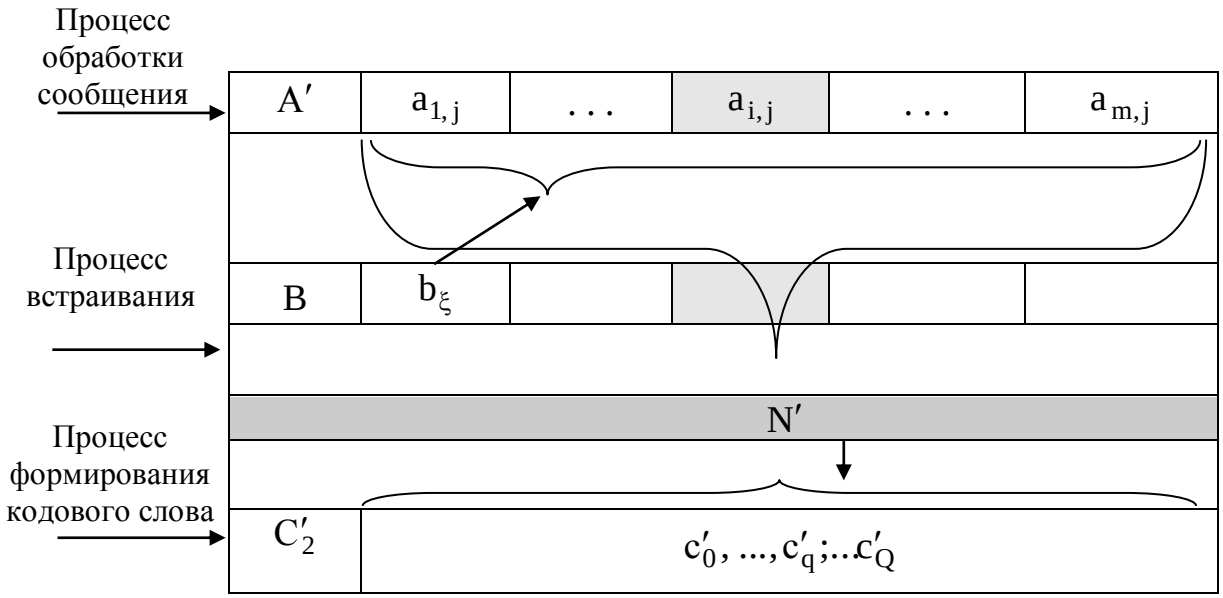

Рис.2.6. Структурная схема построения кодовых конструкция НП числа A' со встроенными данными

Обратное стеганографическое преобразование будет выполняться по биполярному принципу для авторизированного (при наличии ключа $\Psi^{(2)}$) и неавторизированного пользователя (злоумышленника) при стандартных условиях.

Первый способ используется неавторизированным пользователем. Восстановление изображения происходит при наличии открытой служебной информации $\Psi^{(1)}$, представляющей собой систему оснований НП числа A'. Такое обратное преобразование позволяет достоверно реконструировать элемент $A''(1)$ по формуле:

$$A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)})$$

так, чтобы значение количественной метрика $\varepsilon(A; A(1)'')$ была наименьшим

$$\varepsilon(A; A(1)'') \to 0.$$

Здесь $A''(1)$ - элемент, реконструированный при стандартных условиях.

Второй способ существует для авторизированного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием открытой служебной информации $\Psi^{(1)}$ и ключа $\Psi^{(2)}$. В данном случае значение ключа $\Psi^{(2)}$ представляет собой заранее известное значение основания встроенного элемента так, что бы $\Psi^{(2)} \neq \Psi^{(1)}$. Обратное функциональное преобразование позволит авторизированному пользователю безошибочно реконструировать число со встроенными данными, т.е.

$$A(2)'' = f'^{(-1)}(C_2; \Psi^{(1)}; \Psi^{(2)}) \qquad \text{и} \qquad A(2)'' = A',$$

где $A(2)''$ - НП число со встроенными данными, полученное при обратном функциональном преобразовании авторизированным пользователем.

Изъятие встроенной информации происходит без внесения ошибок вследствие применения оператора изъятия φ_c^{-1} к реконструируемому НП числу $A(2)''$ при котором также возможно безошибочное восстановление числа A''' как элемента исходного изображения, так что:

$$\varphi'^{(-1)}(A''(2)) = \begin{cases} b'_\xi, & b'_\xi = b_\xi; \\ A''', & A''' = A. \end{cases}$$

Здесь b'_ξ - изъятый элемент скрываемого сообщения B'_2.

На рис. 2.7. представлена схема стеганографического метода на основе неравновесного позиционного кодирования [13, 15, 89]. Прямое стеганографическое преобразование реализуется в три этапа [15 ,29]. На первом этапе при помощи оператора встраивания φ бит b_ξ скрываемого сообщения B_2

встраивается на различную позицию НП числа A. Полученное вследствие загрузки бита b_ξ неравновесное позиционное A' определяется выражением

$$A' = \varphi(b_\xi; A).$$

На втором этапе для стеганочисла A' по правилу $f(A')$ формируется код N':

$$N' = f'(A').$$

Формирование кода происходит с учетом ключевой информации $\Psi^{(2)}$, подразумевающей под собой основание встроенного элемента.

На третьем этапе строится результирующее кодовое представление C'_2 числа A' со встроенными данными. Это описывается выражением:

$$C'_2 = \varphi_c(N'; \Psi^{(1)}).$$

Полученная стеганограмма C, содержащая в себе информационную составляющую N' и служебную составляющую $\Psi^{(1)}$, подвергается атакующим воздействиям.

Обратное стеганографическое преобразование включает в себя случай для неавторизированного пользователя (стегоанализ) при условии, что ему известен обратный функционал $f'^{(-1)}$, и авторизированного пользователя. При стегоанализе, по правилу $f'^{(-1)}(\bullet)$ формируется число

$$A''(1) = f'^{(-1)}(C'_2; \Psi^{(1)}).$$

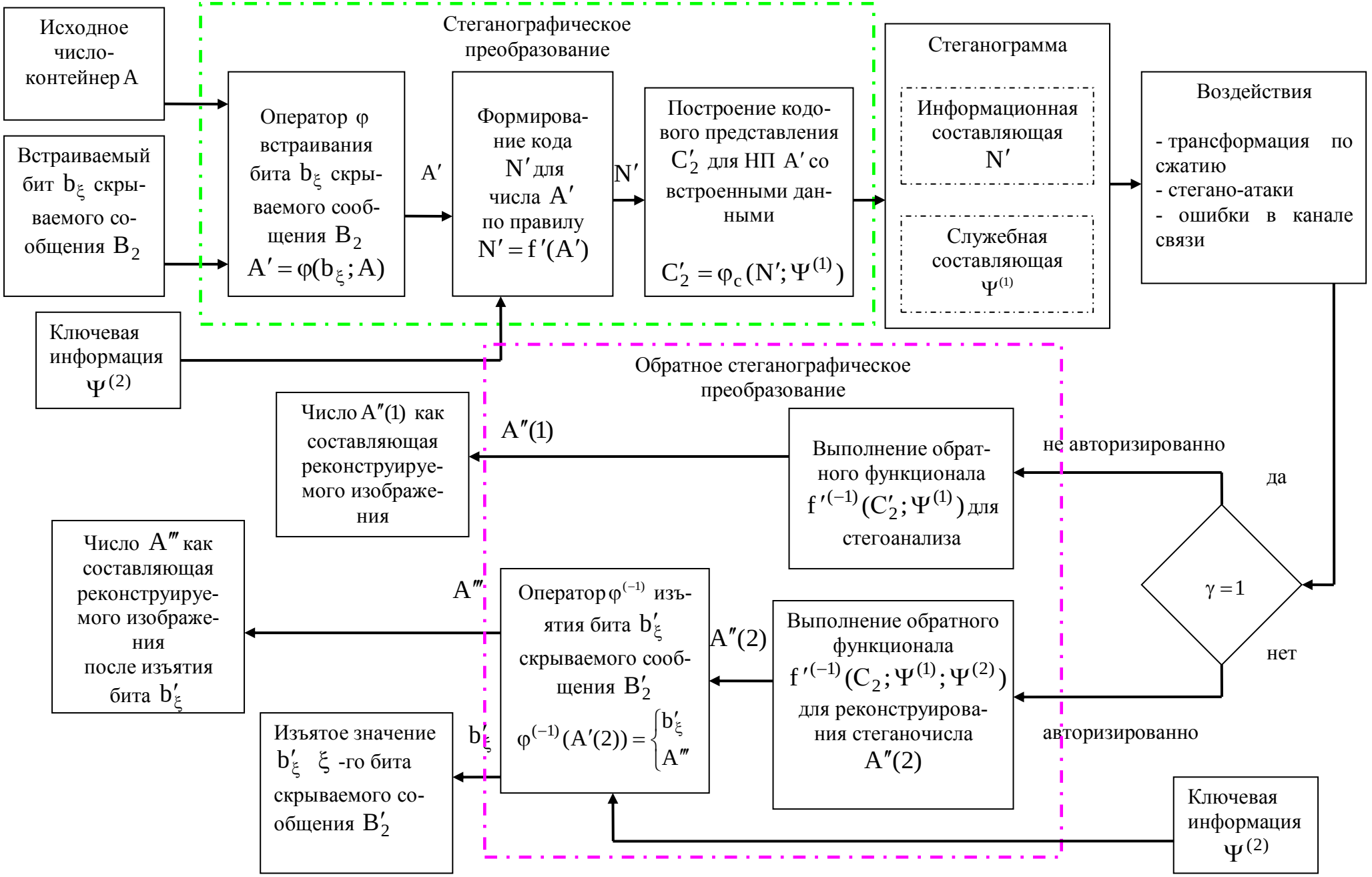

Рис 2.7. Схема стеганографического преобразования на основе неравновесного позиционного кодирования

Здесь $A''(1)$- число, как составляющая реконструируемого изображения, полученное в результате стегоанализа.

Для авторизованного пользователя обратное стеганографическое преобразование происходит в два этапа. На первом этапе по правилу $f'^{(-1)}(\bullet)$ и с учетом ключевой информации $\Psi^{(2)}$ происходит реконструкция числа со встроенными данными

$$A''(2) = f'^{(-1)}(C_2'; \Psi^{(1)}; \Psi^{(2)}).$$

На втором этапе из реконструированного числа $A''(2)$ происходит изъятие b_ξ' скрываемого сообщения B_2. В результате применения оператора изъятия $\varphi^{(-1)}$ также происходит реконструкция числа A''', как составляющего исходного изображения, что описывается выражением

$$\varphi^{(-1)}(A'(2)) = \begin{cases} b_\xi' \\ A''' \end{cases}.$$

Выводы

1. Проанализированы существующие методы непосредственного стеганографического встраивания в изображение-контейнер. Методы непосредственного встраивания в элементы пространственного представления ИК обладает рядом преимуществ в сравнении с другими методами. Однако существует противоречие между стойкостью встроенных данных и визуальной устойчивостью стеганограммы при встраивании на различные позиции элемента ИК. Для устранения такого противоречия предлагается проводить преобразование элемента со встроенными данными в соответствии с синтезированным функционалом.

2. Определены требования к функционалу от числа со встроенными данными:

- должна обеспечиваться взаимооднозначность прямого и обратного функционального преобразований, т.е. должен существовать обратный функционал, позволяющий авторизированному пользователю получить скрываемое сообщение без потери информации;

- обратное функциональное преобразование должно осуществляться по биполярному принципу. Биполярность заключается в существовании для функционала двух вариантов обратного преобразования: для авторизированного пользователя и для злоумышленника. Для неавторизированного пользователя восстановление изображения происходит при стандартных условиях, при котором блокируется возможность изъятия встроенного сообщения. Для авторизированного пользователя обратное преобразование реализуется при наличии ключа, и при этом возможно безошибочное изъятие встроенных данных;

- функциональное преобразование должно быть инвариантным к атакующим воздействиям. Другими словами, должно обеспечиваться достоверное изъятие встроенного сообщения после подвергания стеганограммы атакам, сжатию и при наличии ошибок в канале связи.

3. Сформулирована система свойств для функционального преобразования. Для соответствия требованиям визуальной устойчивости к трансформированию и атакам, синтезируемый функционал должен обладать следующими свойствами:

- формирование стеганограммы с использованием функционала должно осуществляться по интегральному принципу в два этапа. На первом этапе применения функционала к числу с встраиванием формируется кодовое значение, содержащее информацию элементах исходного числа. На втором этапе на основе кодового значения строится результирующее кодовое представление стеганограммы.

- количественная метрика, указывающая на степень отличия между элементами ИК полученными при обратном преобразовании в случае для авторизированного пользователя и реконструированными элементами при неавторизированном доступе, не должна превышать порога визуальной незначимости;

- стеганограмма, полученная вследствие функционального преобразования, должна содержать сведения о векторе служебной информации, при наличии которой возможно реконструкция элементов изображения контейнера;

- извлечение встроенного бита скрываемого сообщения неавторизированным пользователем возможно только при известном ключе, даже при наличии у него информации о встраивании данных;

- реконструкция исходного изображения для неавторизированного пользователя реализовалась только при наличии у него полных сведений о векторе служебных данных.

4. Обоснован подход на основе неравновесного позиционного кодирования, где в качестве элемента-контейнера предлагается использовать НПЧ, а в качестве функционального преобразования используется кодообразующая функция для НПЧ. При таком подходе предусматривается встраивание бита секретного сообщения в исходное неравновесное позиционное число. В результате применения прямого функционального преобразования для исходного числа со встроенной информацией формируется результирующие кодовое представление. Обратное функциональное преобразование будет осуществляться для злоумышленника и для авторизированного пользователя. При первом способе реконструкция элемента исходного изображения реализуется неавторизированным пользователем с учетом открытой служебной информации. Второй способ позволяет, при наличии служебной информации и закрытого ключа, изъять бит встроенных данных и безошибочно реконструировать

исходный элемент изображения-контейнера.

РАЗДЕЛ 3

РАЗРАБОТКА МЕТОДА СТРУКТУРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ

В разделе разрабатывается метод структурного стеганографического кодирования с маскированием и метод демаскирующего стеганографического декодирования.

Проводится обоснование необходимости использования структурных закономерностей изображения-контейнера для стеганографического встраивания информации. Разрабатывается модель структурного стеганографического кодирования на основе использования функционального преобразования для неравновесного позиционного кодирования.

Разрабатывается метод стеганографического кодирования неравновесного позиционного числа с имплантированным элементом.

Обосновывается появление структурной стеганографической избыточности в процессе стеганографического кодирования неравновесного позиционного числа с имплантированным элементом.

Разрабатывается стеганографическая система с маскирование структурной стеганографической избыточности для устранения потенциальной возможности для выявления факта наличия встроенной информации.

Разрабатывается метод демаскирующего стеганографического декодирования. Декодирование осуществляется по биполярному принципу для авторизированного и неавторизированного пользователя.

3.1. Разработка модели структурного стеганографического кодирования

Для проектирования стеганосистемы предлагается использовать наличие в изображении-контейнере структурных закономерностей, обусловленных наличием ограничений на динамический диапазон [10, 11, 12].

Величина ψ_i динамического диапазона строки массива изображения-контейнера $A = \{a_{i,j}\}$ определяется на основе следующего выражения:

$$\psi_{i,j} = \min(\psi_i;\ \psi_j).$$

Схема формирования базиса динамических диапазонов для изображения-контейнера А представлена на рис. 3.1.

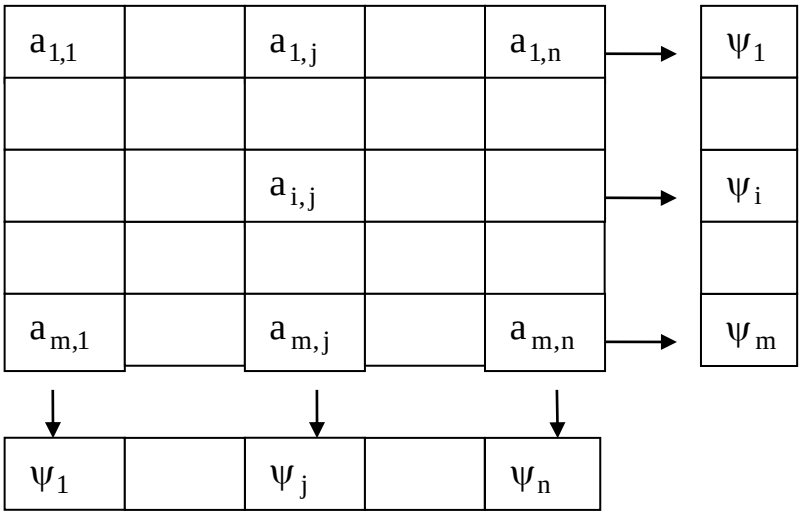

Рис. 3.1. Схема формирования базиса динамических диапазонов для изображения-контейнера А

Свойствами учитывать ограничений на динамический диапазон, в процессе представления и кодирования, обладает неравновесное (НП) представ-

ление [10, 11, 12]. Поэтому предлагается проектировать стеганосистему на основе кодообразующего функционала с учетом НП базиса [13, 15, 17-19, 21, 25, 27].

В качестве кодообразующего функционала, обладающего свойствами для соответствия требованиям относительно процесса скрытия данных, предлагается использовать кодообразующую функцию для неравновесного позиционного числа (НП кодирование), которая обладает следующими свойствами [10, 11, 12]:

1) формирование стеганограммы C с использованием кодообразующего функционала для НП числа осуществляется по интегральному принципу в два этапа. На первом этапе для исходного НП числа, как результат применения функционала $f(A'_{си})$ к числу с имплантацией $A'_{си}$, формируется кодовое значение N, содержащее информацию об элементах числа $A'_{си}$, т.е.

$$N = f(A'_{си}).$$

На основе сформированного значения кода N на втором этапе строится результирующее кодовое представление C_2 стеганограммы

$$C_2 = \varphi_c(N).$$

Здесь φ_c - оператор, обеспечивающий построение двоичного кода C_2 для кодового значения N.

2) обратное преобразование выполняется по биполярному принципу для авторизированного (при наличии ключа $\Psi^{(2)}$) и неавторизированного пользователя (злоумышленника) при стандартных условиях.

Первый способ используется неавторизированным пользователем. Восстановление изображения происходит при наличии открытой служебной ин-

формации $\Psi^{(1)}$, представляющей собой систему НП базисов оснований числа $A'_{ди}$ до осуществления имплантации.

Второй способ существует для авторизированного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием открытой служебной информации $\Psi^{(1)}$ и ключа $\Psi^{(2)}$. В данном случае значение ключа $\Psi^{(2)}$ представляет собой заранее известное значение основания встроенного элемента так, что бы $\Psi^{(2)} \neq \Psi^{(1)}$.

3) стеганограмма C, содержит сведения о векторе служебной информации $\Psi^{(1)}$, при наличии которого возможна реконструкция элементов стеганоизображения $A(1)''$ при отсутствии информации о наличии встроенного сообщения

$$C=\varphi_c(N,\Psi^{(1)}) \qquad A(1)'' = f^{(-1)}(C;\Psi^{(1)}).$$

В процессе реализации функционального преобразование на основе неравновесного позиционного кодирования область исходного изображения, содержащая совокупность видеопоследовательностей, рассматривается как множество неравновесных позиционных чисел $\{A(j)\}$ [10, 11, 12, 15, 26]. Здесь неравновесное позиционное число $A(j)$ без имплантации для j-го столбца массива видеоизображения состоит из m элементов, т.е.

$$A(j)=\{a_{1,j};...;a_{i,j};...;a_{m,j}\}.$$

На данном этапе структурная избыточность еще не сокращается. Устранение структурной избыточности осуществляется на втором этапе в процессе кодирования НПЧ $A(j)$ без имплантации. Правило $f(A(j))$ предусматривает формирование кода-контейнера $N(j)$ для неравновесного позиционного числа $A(j)$ без имплантированного элемента по формуле:

$$N(j) = f(A(j), V^{(1)}), \qquad (3.1)$$

где $V^{(1)}$ - система весовых коэффициентов НП числа $A(j)$ без имплантации в коде-контейнере, которая определяется при помощи системы оснований $\Psi^{(1)}$.

Физический смысл весового коэффициента $V_{i,j}$ можно интерпретировать как условное количество информации, содержащееся в $(m-i)$ элементах НП числа при условии, когда значение i-го элемента равно $a_{i,j}$.

На этом этапе фактически будет заканчиваться процесс встраивания информации.

Кодограмма $C(A(j))$ для кода-контейнера $N(j)$ неравновесного позиционного числа без имплантации $A(j)$ формируется на третьем этапе при помощи оператора выделения разрядов $\varphi_c(\bullet)$ по формуле:

$$C(A(j) = \varphi_c(N(j), \Psi^{(1)}) = \varphi_c(A(j); \Psi^{(1)}; V),$$

где $\Psi^{(1)}$ - ключевая составляющая, содержащая систему оснований НПЧ $A(j)$;

$V^{(1)}$ - значения весовых коэффициентов элементов НПЧ $A(j)$.

В этом случае получим следующую кодограмму:

$$C(A(j))=\{c_1,...,c_\xi,...,c_{q(j)}\},$$

где $q(j)$ - длина двоичной кодограммы $C(A(j))$;

c_ξ - ξ-й двоичный разряд кодограммы $C(A(j))$.

Процесс реконструкции элемента $a_{i,j}$ для неравновесного позиционного числа $A(j)$ без встроенной информации на основе кода-контейнера $N(j)$ выполняется по формуле

$$a_{i,j} = f^{(-1)}(N(j), V_{i,j}, \psi_{i,j}), \qquad (3.2)$$

где $V_{i,j}$ - весовой коэффициент элемента $a_{i,j}$.

На рис. 3.2. графически отображены этапы формирования кодограммы $C(A(j))$ для кода-контейнера $N(j)$ НП числа $A(j)$ (прямого неравновесного позиционного преобразования) и его декомпозиции (обратного неравновесного позиционного преобразования).

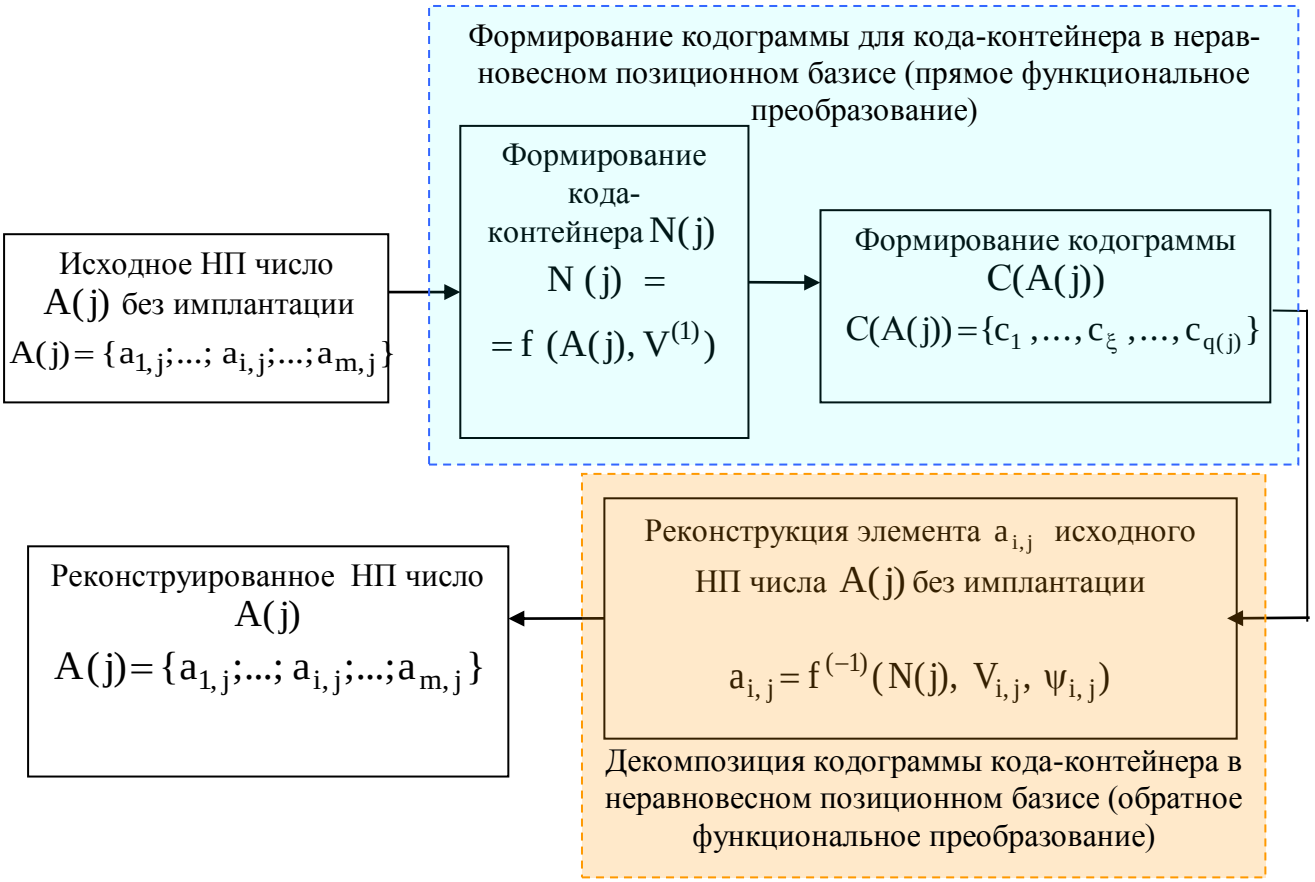

Рис. 3.2. Схема стеганографической системы на основе формирования кода-контейнера в неравновесном позиционном базисе

Ключевая составляющая $\Psi^{(1)}$ включает в себя информацию о системе оснований $\Psi^{(1)}=\{\psi_{i,j}\}$ неравновесного позиционного числа без имплантации. Основание $\psi_{i,j}$ определяется как минимальное значение из двух динамических диапазонов строки ψ_i и столбца ψ_j, на пересечении которых он расположен, т.е. $\psi_{i,j}=\min(\psi_i;\psi_j)$. На основе полученных значений оснований строится неравновесный базис оснований $\Psi^{(1)}=\{\psi_{i,j}\}$ (рис. 3.3).

$\psi_{1,1}$		$\psi_{1,j}$		$\psi_{1,n}$
		$\psi_{i,j}$		
$\psi_{m,1}$		$\psi_{m,j}$		$\psi_{m,n}$

Рис. 3.3. Структура неравновесного базиса оснований

Такой подход при формировании базиса оснований для НП числа позволяет выявить структурные закономерности на динамический диапазон [13]. Это создает потенциал для установления количества структурной избыточности, которую можно будет использовать для скрытого встраивания информации.

Проведем обоснование, что в этих условиях обеспечивается возможность скрыть встраиваемую информацию в коде-контейнере.

Необходимо оценить величину структурной избыточности, которая потенциально может быть использована для встраивания информации в код-контейнер. Для этого сравним количество бит $q(j)_{исх}$ необходимое для двоичного представления числа $A(j)$ исходной видеопоследовательности с фик-

сированным динамическим диапазоном и количество бит $q(j)$ необходимое для представления кодограммы $C(A(j))$.

Значения яркости элемента пространственно-временного представления изображения-контейнера в системе RGB может принимать значения $a_{i,j} \in [0; 255]$, Другими словами, для каждого i-го элемента числа $A(j) = \{a_{i,j}\}$ исходной видеопоследовательности величина динамического диапазона будет равна 256. Тогда $q(j)_{исх}$ будет описываться выражением:

$$q(j)_{исх} = m \cdot \log_2 256 = 8 \cdot m \text{ (бит).}$$

Определим количество бит $q(j)$ необходимые для представления кодограммы $C(A(j))$, полученной в процессе формирования кода-контейнера $N(j)$ НП числа $A(j)$. На основе использования свойства неравновесных позиционных чисел $A(j)$ можно заключить, что для заданного базиса оснований $\Psi^{(1)}$ максимально возможное значение кода-контейнера $N(j)$ будет ограничено сверху накопленным произведением V_{max} оснований элементов НП числа. Это задается следующим выражением:

$$N(j) \le V_{max} = f_{осн}(\Psi^{(1)}) - 1.$$

Здесь $f_{осн}(\Psi^{(1)})$ - преобразование для получения накопленного произведения оснований НПЧ.

Другими словами, величина V_{max} определяет количество различных кодов-контейнеров, которые могут быть сформированы для заданной системы оснований $\Psi^{(1)}$.

Отсюда, длина $q(j)$ кодограммы информационной части кода-контейнера $N(j)$ определяется на основе следующего выражения [10,11,12, 15,18, 21]:

$$q(j) = |C(A(j))| = [\ell og_2 (f_{осн} (\Psi^{(1)}))]+1 \text{ (бит).}$$

Необходимо учитывать, что основание элементов пространственно-временного представления исходной видеопоследовательности принимают значения $\psi_{i,j} \in [1;256]$. Тогда количество бит $q(j)$ необходимое для двоичного представления кодограммы $C(A(j))$ кода-контейнера $N(j)$ примет значение:

$$q(j) = C(A(j)) \in [0; 8 \cdot m] \text{ (бит).}$$

С учетом чего количество $R(j)$ структурной избыточности вычисляется как разность между количеством бит $q(j)$ для двоичного представления кодограммы $C(A(j))$ и количеством бит $q(j)_{исх}$, необходимых для двоичного представления числа $A(j)$ исходной видеопоследовательности и описывается выражением

$$R(j) = q(j)_{исх} - q(j).$$

Здесь $R(j)$ - структурная избыточность, возникающая в процессе функционального преобразования на основе формирования кода-контейнера НП числа $A(j)$. Другими словами, это избыточность, возникающая в процессе формирования кода-контейнера $N(j)$ для НП числа $A(j)$ в результате формирования неравновесного базиса оснований относительно кодового представления исходной видеопоследовательности.

3.2. Разработка концепции стеганографического кодирования неравновесного числа с имплантированным элементом

Для реализации выявленной потенциальной возможности относительно встраивания информации на основе структурных характеристик ***предлагается*** подход в виде формирования стеганокода для числа с имплантированными данными в неравновесном позиционном базисе [13, 15,17, 89].

Имплантацию в число $A(j)$ ***предлагается*** проводить поэлементно, т.е. один элемент b_ξ на позицию γ-го разряда числа $A(j)$. Здесь b_ξ - ξ-й элемент встраиваемой последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0; 255]$, $\xi = \overline{1, \nu}$. В этом случае имплантация задается следующей формулой:

$$A(j)' = A(j) \cup b_\xi, \quad b_\xi = a'_{\gamma,j} \ . \tag{3.3}$$

В результате имплантации, число $A(j)'$ примет следующий вид:

$$A(j)' = \{ a_{1,j};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j}\}, \tag{3.4}$$

где $A(j)'$ - число с имплантированным элементом $a'_{\gamma,j}$ в γ-й разряд числа;

$(m+1)$ - количество элементов в числе с имплантацией.

На следующем этапе число $A(j)'$ с имплантированным элементом кодируется. На этом этапе проводится встраивание скрываемой информации в код-контейнер. В связи с чем, сформулируем следующее определение.

Определение. Процесс одновременного встраивания информации и построения кода-контейнера, т.е. когда встраивание информации осуществляется в процессе формирования кода-контейнера, называется ***стеганографическим кодированием***.

Определение. Значение кода-контейнера, содержащее скрываемую информацию, называется ***стеганокодом***.

Другими словами стеганокод это кодовое значение, формирующееся в процессе стеганографического кодирования.

Определение. Формирование стеганокода на основе кодирования неравновесного позиционного числа с имплантированным элементом скрываемого сообщения называется ***структурным стеганографическим кодированием в неравновесном позиционном базисе***.

Значения стеганокода $N(j)'$ для НП числа с имплантацией определяется по следующей формуле:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) ; \qquad (3.5)$$

Здесь $V^{(2)}$ - весовой коэффициент имплантированного элемента $a'_{\gamma,j}$.

В случае такого встраивания фрагмент исходной видеопоследовательности рассматривается, как позиционное число $A(j)' = \{ a_{1,j};...;a'_{\gamma,j};...;a_{i,j};...;a_{m+1,j} \}$ с имплантированным элементом $a'_{\gamma,j}$, $i=\overline{1,m+1}$. Для числа $A(j)'$ кодовое представление $C(A(j)')$ его стеганокода $N(j)'$ в неравновесном позиционном базисе формируется в два этапа (рис 3.4).

Первый этап включает в себя вычисление значения стеганокода $N(j)'$, как взвешенного суммирования величин $a_{i,j} V'_{i,j}$ и величины $a'_{\gamma,j} V'_{\gamma,j}$. Кодограмма $C(A(j)')$ стеганокода формируется на втором этапе для значения величины $N(j)'$:

$$C(A(j))'=\{c_1,...,c_\tau,...,c_{q(j)'}\},$$

где $q(j)'$ - длина кодограммы $C(A(j)')$.

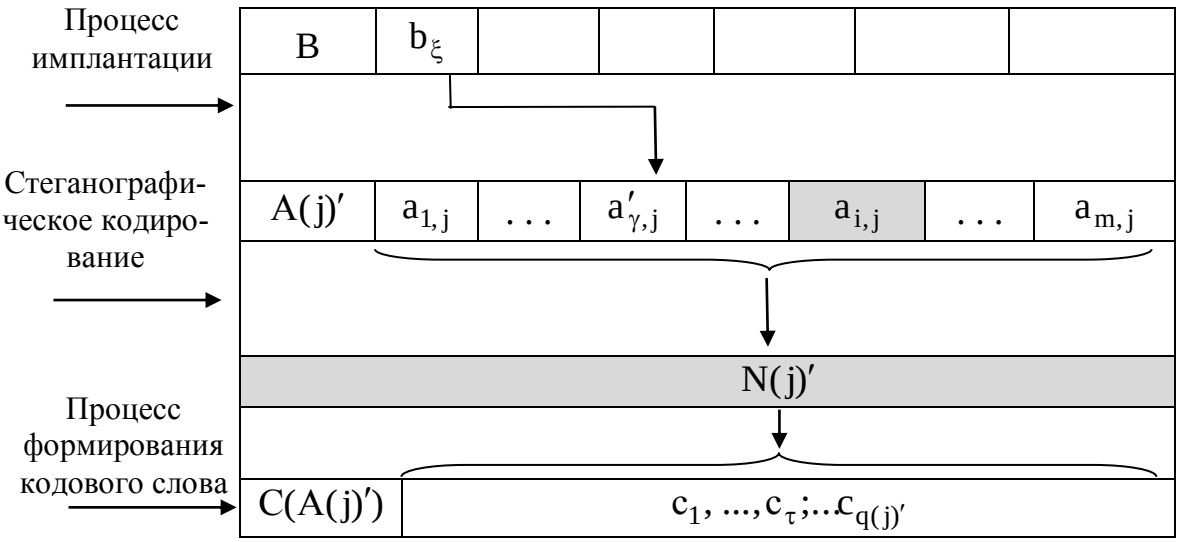

Рис 3.4. Структурная схема построения кодограммы стеганокода для числа $A'(j)$ с имплантацией

В результате стеганографического кодирования формируются кодовые комбинации, состоящие из двух частей: служебной $\Psi^{(1)}$ и информационной $N(j)'$ (значение стеганокода). В связи с чем сформулируем следующее определение:

Определение. Кодовую комбинацию, которая содержит служебную часть $\Psi^{(1)}$ (система оснований) и информационную часть (кодовое представление стеганокода $N(j)'$) будем называть стеганограммой.

Значит, встраивания элемента в неравновесное позиционное число осуществляется в результате кодирования в два этапа. На первом этапе для НПЧ с имплантацией формируется стеганокод. Второй этап предусматривает формирование кодограммы для значения стеганокода. В результате стеганографического преобразования формируется стеганограмма, содержащая служебную и информационную части.

3.3 Обоснование появления структурной стеганографической избыточности в процессе стеганографического кодирования

Для сформированной стеганограммы оценим длину $q(j)'$ кодограммы стеганокода $N(j)'$ для числа $A(j)'$ с имплантацией. Значение $q(j)'$ с учетом того, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j}$, будет определяться по формуле:

$$q(j)' = |N(j)'|_2 = [\ell og_2\, \psi'_{\gamma,j} + \ell og_2\, (f_{осн}(\Psi^{(1)}))]+1 \ \text{(бит)}, \qquad (3.6)$$

где $|N(j)'|_2$ - длина стеганокода $N(j)'$.

Сравним значение $q(j)'$ с длиной $q(j)$ кодограммы кода-контейнера $N(j)$ числа $A(j)$ без имплантированного элемента. Значение $q(j)$ определяется на основе следующего выражения:

$$q(j) = |C(A(j))| = [\ell og_2\, (f_{осн}(\Psi^{(1)}))]+1 \ \text{(бит)}. \qquad (3.7)$$

Из сравнения выражений (3.6) и (3.7) можно сделать вывод, что имплантация бита в число $A(j)$, увеличивает длину кодового представления на величину, равную $(\log_2 \psi'_{\gamma,j})$ бит. Это описывается выражением:

$$q(j)' - q(j) = \log_2 \psi_{\gamma,j}. \qquad (3.8)$$

Отсюда можно заключить, что в процессе формирования стеганокода для числа $A(j)'$ с имплантированным элементом относительно варианта до встраивания вносится избыточность. В связи с чем сформулируем следующее определение.

Определение. Избыточность, которая возникает в результате стеганографического кодирования, т.е. встраивания информации относительно выявляемых закономерностей до встраивания (количества информации в кодеконтейнере), будем называть стеганографической избыточностью.

Применительно к предложенному подходу для построения стеганографической системы необходимо определить структурную избыточность в рамках выявляемых структурных закономерностей в виде ограничения на динамический диапазон в фрагменте изображения.

В этом случае вводим понятие структурной стеганографической избыточности.

Определение. Под структурной стеганографической избыточностью будем понимать такую стеганографическую избыточность, которая формируется в результате введения избыточности по системе оснований. В нашем случае это соответствует добавлению одного основания соответствующего встраиваемому элементу.

Структурная стеганографическая избыточность $R(j)_{стег}$ определяется как разность длины $q(j)'$ кодограммы стеганокода числа $A(j)'$ с имплантацией и длины $q(j)$ кодограммы кода-контейнера для числа $A(j)$ без встроенной информации, т.е.

$$R(j)_{стег} = q(j)' - q(j) \geq 0 \qquad (3.9)$$

Теперь оценим величину остаточной структурной избыточности $R(j)_{ост}$, которая образуется в результате формирования стеганокода для числа с имплантацией в неравновесном базисе оснований относительно кодового представления исходной видеопоследовательности. Для этого оценим длину $q(j)_{исх}$ кодового представления исходной видеопоследовательности. Длина $q(j)_{исх}$ кодового представления числа $A(j)$ с постоянным основанием $\psi = 256$ определяется по формуле:

$$q(j)_{исх} = m \cdot \log_2 256 = 8 \cdot m \text{ (бит).}$$

Сравним длину $q(j)'$ кодограммы стеганокода $N(j)'$ для числа $A(j)'$ с имплантацией с длиной $q(j)_{исх}$ кодового представления числа $A(j)$ с постоянным основанием $\psi = 256$ без имплантированного элемента. Это описывается выражением:

$$R(j)_{ост} = q(j)_{исх} - q'(j). \qquad (3.10)$$

Графически это можно отобразить, как показано на рис 3.5.

Очевидно, что возможность встраивания информации в условиях обеспечения ее скрытности будет обеспечиваться, когда количество структурной избыточности не будет равно нулю, т.е.

$$R(j)_{ост} = q(j)_{исх} - q(j)' \neq 0$$

Проведем оценку того, как влияет появление стеганографической избыточности на возможность выявления факта встраивания информации. В этом случае необходимо учитывать, что стеганограмма содержит как информационную часть (значение стеганокода $N(j)'$) так и служебную (систему оснований $\Psi^{(1)}$). Отсюда, неавторизированный пользователь имеет доступ к базису оснований $\Psi^{(1)}$, на основе которого сформирован стеганокод $N(j)'$.

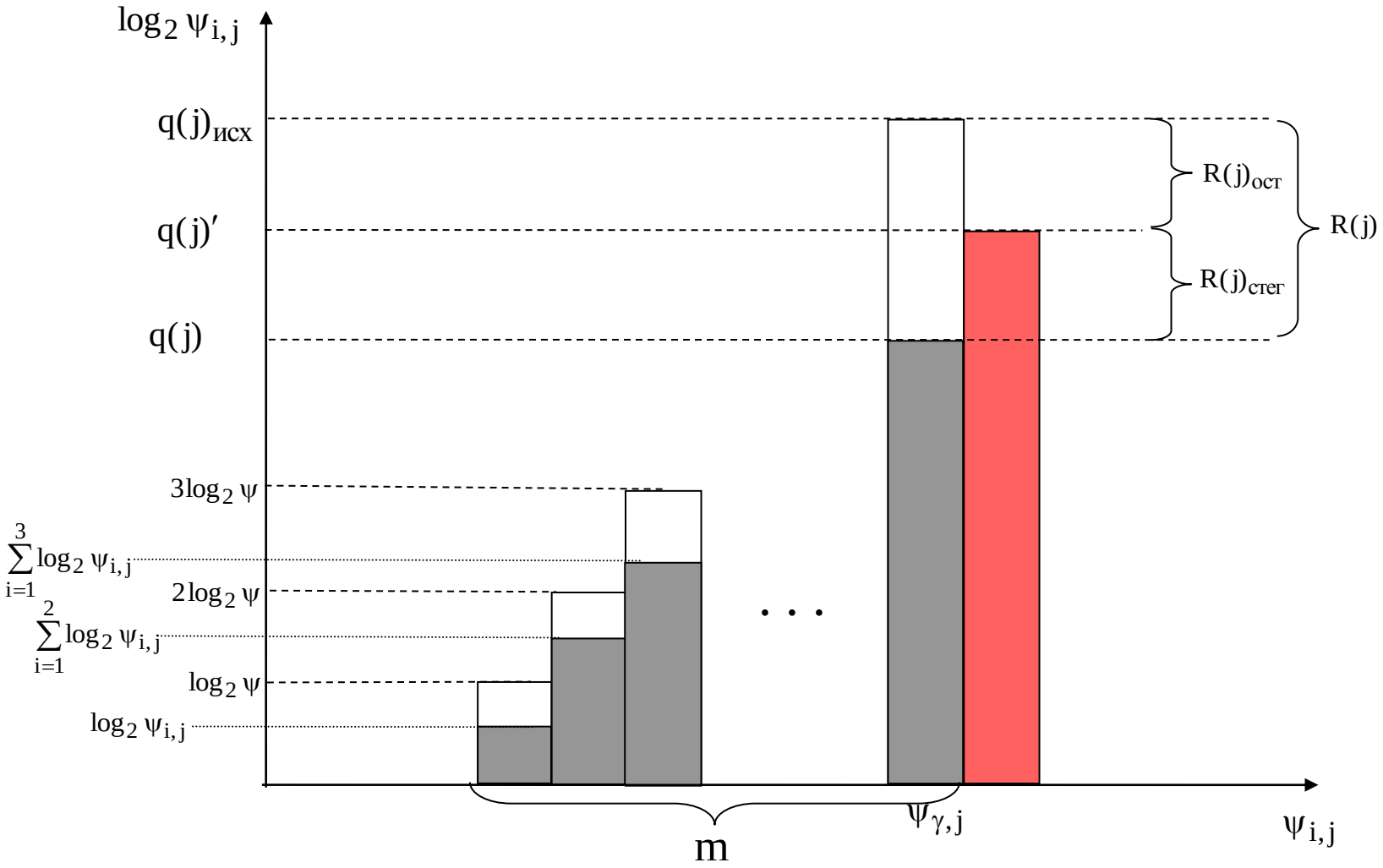

Рис 3.5. Графическая интерпретация стеганографической избыточности

Очевидно, что возможность встраивания информации в условиях обеспечения ее скрытности будет обеспечиваться, когда количество структурной избыточности не будет равно нулю, т.е.

$$R(j)_{ост} = q(j)_{исх} - q(j)' \neq 0$$

Проведем оценку того, как влияет появление стеганографической избыточности на возможность выявления факта встраивания информации. В этом случае необходимо учитывать, что стеганограмма содержит как информационную часть (значение стеганокода $N(j)'$) так и служебную (систему оснований $\Psi^{(1)}$). Отсюда, неавторизированный пользователь имеет доступ к базису оснований $\Psi^{(1)}$, на основе которого сформирован стеганокод $N(j)'$. В направлении выявления факта встраивания информации, неавторизированный пользователь может предпринять следующее:

1. На основе имеющейся в кодограмме системы оснований $\Psi^{(1)}$ существует возможность вычислить значение длины $q(j)$ кодограммы для кода контейнера $N(j)$, т.е.

$$q(j) = [\ell og_2 (f_{осн}(\Psi^{(1)}))]+1$$

2. Это позволяет установить предполагаемую длину информационной части текущей кодограммы. В результате чего будет считано значение кода $N(j)''$. Однако, в действительности передается стеганокод и величина $q(j)$ не будет равна $q(j)'$. Длина кодового представления стеганокода превышает длину исходного кода-контейнера. Поэтому в общем случае считанное значение $N(j)''$ в информационной части кодограммы будет отличаться от исходного значения кода-контейнера, а именно:

$$N(j)'' \neq N(j).$$

Это приводит к тому, что:

1) реконструкция элементов в исходной видеопоследовательности будет проводиться с ошибками;

2) разница между длинами кодовых представлений стеганокода $q(j)'$ и кодограммы $q(j)$, которая остается не изъятой будет восприниматься как первые биты служебной части следующей кодограммы $N(j)''$ (рис 3.6).

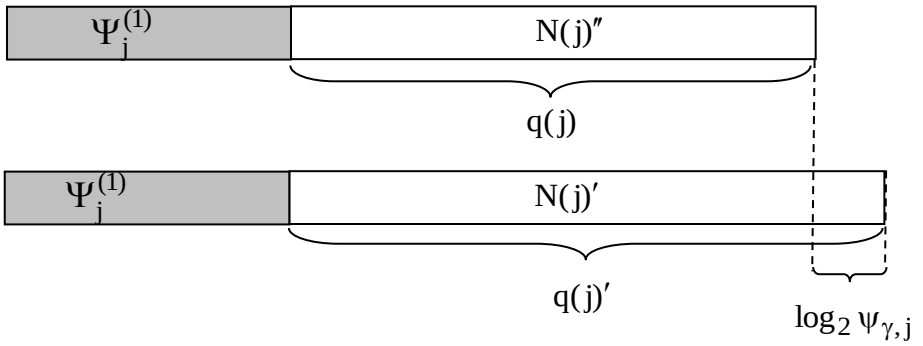

Рис 3.6. Кодограммы для ошибочно изъятого стеганокода $N(j)''$ и стеганокода $N(j)'$

Поэтому можно заключить, что появление структурной стеганографической избыточности $R(j)_{стег}$ приводит к тому, что изображение будет декодироваться с наличием существенных искажений. Это позволит злоумышленнику установить факт наличия встроенной информации.

3.4 Разработка стеганографической системы с маскированием структурной стеганографической избыточности

Рассмотрим как влияет ошибочное значение $N(j)''$ кода-контейнера, считанное из информационной части кодограммы в условиях, когда:

- с одной стороны в реальности передается стеганокод $N(j)'$;

- с другой стороны неавторизированный пользователь будет считывать значение кода-контейнера $N(j)$.

В этом случае вместо того чтобы отобрать $q(j)'$ бит, неавторизированный пользователь выбирает $q(j)$ бит.

Рассмотрим процесс реконструкции элементов исходной видеопоследовательности, представленных как неравновесные позиционные числа в условиях использования ошибочного значения кода-контейнера $N(j)''$. Другими словами проведем оценку влияния несоответствия длины стеганокода и кода-контейнера на процесс восстановления элементов исходной видеопоследовательности. Рассмотрим реконструкцию i- го элемента j- й видеопоследовательности. Для этого используем выражение:

$$a''_{i,j} = f^{(-1)}\left(N(j)''_i, V_{i,j}, \psi_{i.j}\right) \qquad (3.11)$$

где $a''_{i,j}$- i-й элемент реконструированной видеопоследовательности;

$N(j)''_i$ - остаточное значение кода неравновесного позиционного числа для декодирования очередного i-го элемента.

Из анализа этого выражения в условиях, когда

$$N(j)'' > N(j)',$$

следует что как минимум начиная с некоторой β-й позиции, элементы видеопоследовательности будут обнуляться, т.е.

$$a''_{i,j} = 0, \quad \text{для} \quad i = \overline{\beta; m+1}.$$

Значит, ошибочно установленная злоумышленником длина информационной части $N(j)''_i$ будет приводить к появлению искажений в процессе восстановления видеоизображения. Данные визуальные искажения могут служить дополнительным источником для стегоанализа.

Поэтому для устранения влияния стеганографической избыточности на возможность проведения атаки злоумышленником, в том числе установления факта наличия встроенной информации, необходимо разработать подход для устранения стеганографической избыточности. Вначале дадим следующее определение.

Определение. Процесс локализации количества избыточности, возникающей в процессе стеганографического кодирования, будем назвать структурным стеганографическим маскированием или маскированием структурной стеганографической избыточности.

Локализацию структурной стеганографической избыточности в процессе формирования стеганокода в неравновесном базисе предлагается осуществлять на основе коррекции длины кодограммы $C(A(j)')$ стеганокода $N(j)'$. Процесс коррекции предусматривает приведение длины кодограммы стеганокода $q(j)'$ к значению длины $q(j)$. В физическом плане, реализация коррекции кодограммы заключается в отбрасывании $(\log_2 \psi'_{\gamma,j})$ наименее значимых бит кодограммы $C(A(j)')$, т.е.

$$C'''_j = [N(j)''']_2 = [N(j)' / \psi'_{\gamma,j}]_2,$$

где $N(j)'''$ - значение стеганокода, скорректированное в процессе маскирования структурной стеганографической избыточности;

$[N(j)''']_2$ - двоичное значение скорректированного стеганокода $N(j)'''$;

C'''_j - кодограмма кодового представления скорректированного стеганокода $N(j)'''$.

Как следует из выражения (3.9) степень локализации значения стеганокода, а значит и уровень его искажений, будет зависеть от значения основания $\psi'_{\gamma,j}$ встраиваемого элемента. Тогда для обеспечения появления минимального значения $R(j)_{стег}$ в процессе стеганографического кодирование должно выполняться условие:

$$(\log_2 \psi'_{\gamma,j}) \to \min .$$

Поэтому для уменьшения уровня искажений стеганокода предлагается встраивать элементы в двоичном представлении, т.е. $b_\xi \in [0;1]$. В этом случае основание встроенного элемента будет равно $\psi'_{\gamma,j} = 2$.

Определим длину $q(j)'$ кодограммы стеганокода $N(j)'$ числа $A(j)'$ с имплантацией двоичного элемента. Учитывая, что имплантированный элемент $a'_{\gamma,j}$ имеет основание $\psi'_{\gamma,j} = 2$, то величина $q(j)'$ будет определяться по формуле:

$$q(j)' = [\ell og_2 \psi'_{\gamma,j} + \ell og_2 (f_{осн}(\Psi^{(1)}))]+1 \ \text{(бит)}$$

Тогда в соответствии с выражением (3.7) можно сделать вывод, что имплантация бита в число $A(j)$ увеличивает длину кодового представления стеганокода относительно кода-контейнера на один бит. Количество $R(j)_{стег}$ структурной избыточности будет равно:

$$R(j)_{\text{стег}} = q(j)' - q(j) = 1 \text{ (бит)}.$$

Следовательно, встраивание двоичного элемента позволяет минимизировать степень несоответствия между значениями стеганокода и кода – контейнера. В этом случае правило локализации будет иметь вид:

$$C_j''' = [N(j)''']_2 = [N(j)'/2]_2. \qquad (3.12)$$

Такой вариант локализации стеганографической избыточности заключается в использовании свойств устойчивости структурных характеристик и структурной избыточности кодов относительно обработки искаженных значений кодов неравновесного позиционного числа. После локализации стеганографической избыточности длина $q(j)''$ кодограммы скорректированного стеганокода $N(j)'''$ будет вычисляться с помощью следующей формулы:

$$q(j)'' = [(\ell og_2 \psi'_{\gamma,j} + \ell og_2 (f_{\text{осн}}(\Psi^{(1)})))/2] + 1 = q(j)$$

Как показывает анализ выражения (3.12) искажения в значение стеганокода все равно будут вноситься. Причем наибольшим искажениям будут подвергаться младшие элементы неравновесного позиционного числа. Поэтому для повышения устойчивости встроенных данных предлагается размещать один бит скрываемой информации на позицию старшего элемента неравновесного позиционного числа.

Вследствие такого встраивания число $A(j)'$ примет следующий вид:

$$A(j)' = \{a'_{1,j}; a_{2,j}; ...; a_{i,j}; ...; a_{m+1,j}\},$$

где $A(j)'$ - число с имплантированным битом $a'_{1,j}$ на позиции старшего элемента;

$a'_{1,j}$ - имплантированный бит на позиции старшего элемента числа $A(j)'$, равный

$$a'_{1,j} = b_\xi, \quad a'_{1,j} \in [0;1],$$

где b_ξ - ξ-й элемент встраиваемой последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$;

$b_\xi \in [0;1]$, $\xi = \overline{1,\nu}$;

$(m+1)$ - количество элементов в числе $A(j)'$ с имплантацией.

В этом случае вес встраиваемого элемента $V'_{\gamma,j}$ в неравновесном позиционном числе будет наибольшим, т.е.

$$V'_{\gamma,j} = V'_{1,j} = \max_{1\le i\le m+1}.\{V'_{i,j}\}.$$

Следовательно, встраиваемый элемент будет более устойчив к преобразованиям со стеганокодом. В тоже время встраивание скрываемого элемента на старшую позицию в числе обеспечивает исключение влияния его оснований на реконструкцию элементов исходной видеопоследовательности.

На рис 3.7 схематично отображено образование минимальной структурной стеганографической избыточности для кодограммы стеганокода относительно кодограммы кода-контейнера при встраивании двоичного элемента на позицию старшего элемента неравновесного позиционного числа.

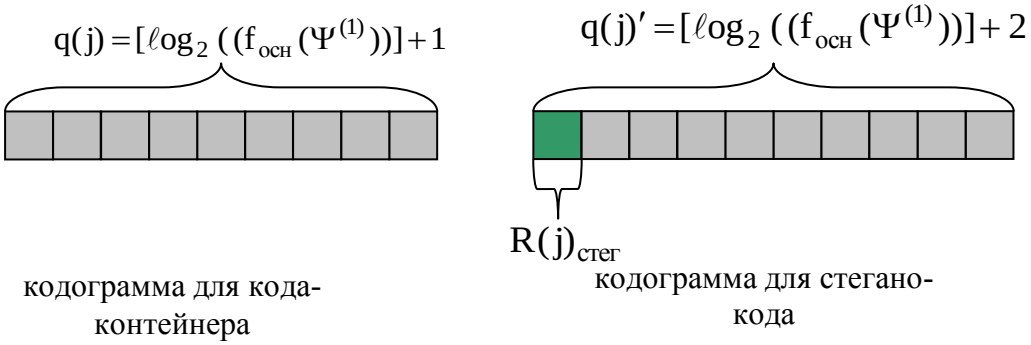

Рис 3.7. Кодограмма кода-контейнера и стеганокода

Рассмотрим этапы функционирования стеганографической системы с маскирование стеганографической избыточности рис 3.8. Данная система позволяет встроить бит скрываемого сообщения на старшую позицию неравновесного позиционного числа в процессе стеганографического кодирования. Полученная в результате такого кодирования стеганограмма состоит из служебной и информационной частей. Реализация извлечения встроенных данных происходит по биполярному принципу: для авторизированного и неавторизированного пользователя.

Стеганографическая система включает в себя следующие базовые составляющие:

Стеганографическое кодирование с маскированием структурной стеганографической избыточности.

Рассмотрим процесс стеганографического кодирования. Данный этап включает в себя следующие действия:

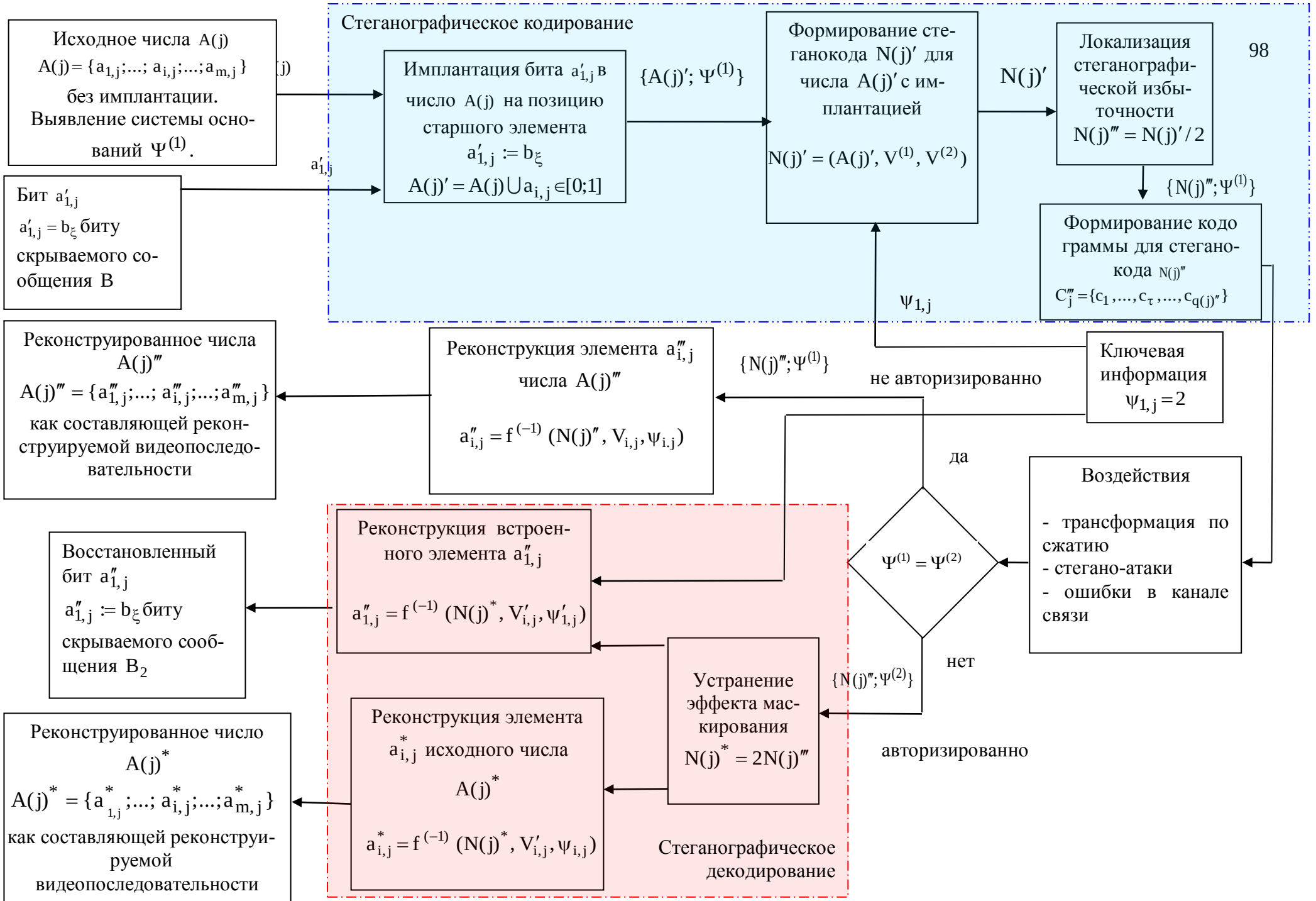

Рис. 3.8. Структурная схема стеганографической системы на основе имплантации скрываемого двоичного элемента на старшую позицию НПЧ с последующим кодированием и маскированием

1. Имплантацию элемента b_ξ на позицию старшего элемента числа $A(j)$. Здесь b_ξ - ξ-й элемент встраиваемой последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0;1]$, $\xi = \overline{1,\nu}$. Имплантация задается следующей формулой

$$A(j)' = A(j) \cup b_\xi, \quad b_\xi = a'_{1,j} \in [0,\ 1]. \tag{3.13}$$

В результате имплантации, число $A(j)'$ примет следующий вид:

$$A(j)' = \{ a'_{1,j};...;a_{i,j};...;a_{m+1,j}\}, \tag{3.14}$$

где $A(j)'$ - число с имплантированным на старшую позицию элементом $a'_{1,j}$.

2. Формирование стеганокода $N(j)'$ для числа $A(j)'$ с имплантированным элементом $a'_{1,j}$. Учитывая механизм локализации количества структурной стеганографической избыточности, выражения для формирования стеганокода $N(j)'$ будет иметь вид:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)})\ ; \tag{3.15}$$

3. Маскирование структурной стеганографической избыточности. Осуществление такого маскирования происходит путем коррекции стеганокода $N'(j)$, а именно уменьшением длины его двоичного представления на один бит. Для получения значения скорректированного стеганокода $N(j)'''$ используется следующее выражение:

$$N(j)''' = N(j)'/2,$$

4. Формирование кодограммы C'''_j для кодового представления скорректированного стеганокода $N(j)'''$:

$$C'''_j = \{c_1, ..., c_\tau, ..., c_{q(j)''}\}$$

где $q(j)''$ - длина кодограммы C'''_j, равная $q(j)'' = [(\ell og_2\, \psi'_{\gamma,j} + \ell og_2\, (f_{осн}(\Psi^{(1)})))/2] + 1$.

На рис 3.9 схематически отображены этапы стеганографического кодирования.

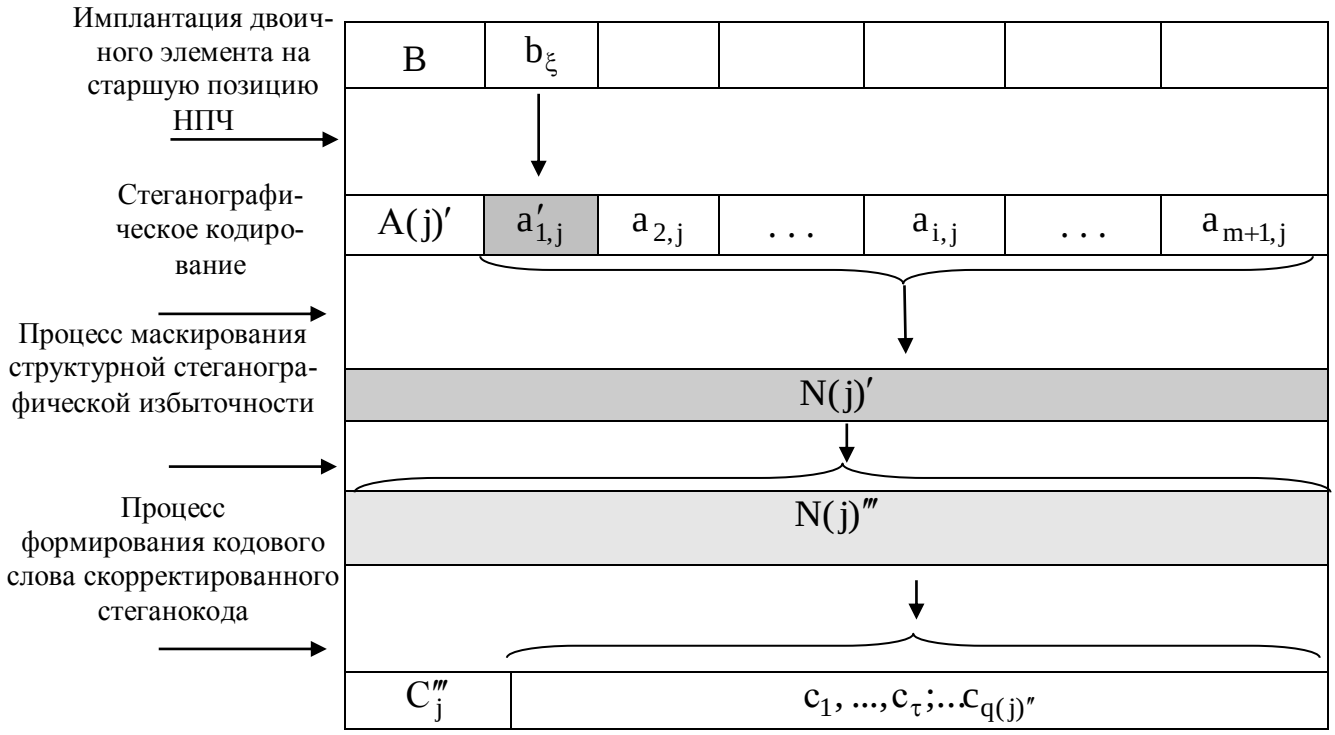

Рис 3.9. Структурная схема построения кодограммы скорректированного стеганокода для числа $A'(j)$ с имплантацией

3.5 Разработка структурного демаскирующего декодирования

Рассмотрим процесс извлечения данных, содержащихся в стеганограмме. Для этого введем следующее определение.

Определение. Процесс изъятия скрываемой информации, осуществляемый одновременно с процессом реконструкции кода-контейнера, называется ***стеганографическим декодированием***.

Определение. Процесс одновременного изъятия скрываемой информации и восстановления неравновесного позиционного числа на основе реконструкции стеганокода называется ***структурным стеганографическим декодированием в неравновесном позиционном базисе***.

Процесс стеганографического декодирования в данном случае осуществляется по ***биполярному принципу*** для авторизированного пользователя и злоумышленника (неавторизированный пользователь) [13, 15, 17-19, 25, 29].

В случае неавторизированного доступа, когда у злоумышленника нет информации о позиции стеганокода в сжатом представлении изображения и позиции встроенного элемента, процесс декодирования осуществляется на основе следующих этапов:

1. Извлечение из кодограммы C_j''' скорректированного стеганокода $N(j)'''$ при помощи системы оснований $\Psi^{(1)}$.

2. Восстановление элементов исходной видеопоследовательности по формуле:

$$a_{i,j}''' = f^{(-1)}(N(j)''', V_{i,j}, \psi_{i.j}),$$

где $a_{i,j}'''$- i-й элемент реконструируемого числа $A(j)'''$, как составляющей реконструируемой j-й видеопоследовательности при неавторизированном доступе.

3. Оценка качества визуального восприятия реконструируемого изображения, т.е. проведение атаки относительно факта наличия встроенной информации.

Наоборот, когда проводится стеганографическое декодирование авторизированным пользователем, то ему доступна следующая информация:

1) позиция стеганокода в сжатом представлении изображения;

2) позиция встроенного элемента $a'_{1,j}$;

3) основание встроенного элемента. $a'_{1,j}$.

В этом случае стеганографическое декодирование будет содержать следующие этапы:

1. Извлечение из кодограммы C'''_j скорректированного стеганокода $N(j)'''$. Такое извлечение осуществляется на основе системы оснований $\Psi^{(1)}$, которая содержится в служебной части стеганограммы.

2. Проведение демаскирования стеганокода (устранение эффекта маскирование). Для этого введем следующее определение.

Определение. Стеганографическое декодирование с учетом демаскированной структурной стеганографической избыточности будем называть демаскирующим стеганографическим декодированием.

Для этого к двоичному представлению стеганокода $N(j)'''$, извлеченного из кодограммы C'''_j добавляется один бит (ноль). Значение восстановленного стеганокода $N(j)^*$ определяется по формуле:

$$N(j)^* = N(j)''' \cdot 2.$$

3. Восстановление встроенного элемента $a'_{1,j}$. Данный этап реализуется на основе информации о позиции стеганокода в сжатом изображении, о позиции встроенного элемента и его основания $\psi'_{1,j} = 2$. Для этого используется следующая формула:

$$a''_{1,j} = f^{(-1)}\,(N(j)^*,\, V_{1,j}, \psi'_{1,j}).$$

Здесь $a''_{1,j}$ - значение изъятого бита встроенной информации $b_\xi := a''_{i,j}$.

4. Восстановление остальных элементов $a^*_{i,j}$ исходной видеопоследовательности проводится на основе использования системы оснований $\Psi_j^{(1)}$. При этом применяется выражение:

$$a^*_{i,j} = [\,N(j)^* / V'_{i,j}\,] - [\,N(j)^* / (\psi_{i,j}\, V'_{i,j})\,]\,\psi_{i,j},$$

где $a^*_{i,j}$- i-й элемент числа $A(j)^*$, как составляющей реконструируемой исходной j-й видеопоследовательности при авторизированном доступе.

Рассмотрим пример использования разработанного стеганографического метода для встраивания скрываемой информации. В качестве исходных изображений используем следующие:

1) изображение «Снимок аэропорта» (рис А1);

2) изображение «Фотоснимок» (рис А2).

Эксперимент проводится в следующих условиях:

1) формируются неравновесные позиционные числа длиной $m = 4$;

2) имплантация одного бита информации $b_\xi = 1$ осуществляется на старшую позицию каждого неравновесного позиционного числа.

Результаты обработки изображений «Снимок аэропорта» и «Фотоснимок» для неавторизированного пользователя представлены соответственно на рис 3.10 и рис 3.11.

Рис 3.10. Изображение «Снимок аэропорта», декодированное неавторизированным пользователем

Рис 3.11. Изображение «Фотоснимок», декодированное неавторизированным пользователем

Из анализа изображений декодированных при неавторизированном доступе можно заключить что:

1. Изображения «Снимок аэропорта» и «Фотоснимок» содержат визуальные искажения.

2. Значение пикового отношения сигнал-шум относительно исходного изображения-контейнера составляет: для изображения «Снимок аэропорта»- 37,94 дБ, для изображения «Фотоснимок»- 33,978 дБ.

Искажения, которые появились в процессе декодирования, объясняются влиянием локализации структурной стеганографической избыточности. Неавторизированный пользователь при декодировании использует скорректированное значение стеганокода $N(j)'''$.

Восстановление исходных значений изображения контейнера происходит с ошибками.

Реализация демаскирующего стеганографического декодирования для авторизированного пользователя рассматривается на примере реконструкции изображений «Снимок аэропорта» и «Фотоснимок» представленных соответственно на рис 3.12 и рис 3.13.

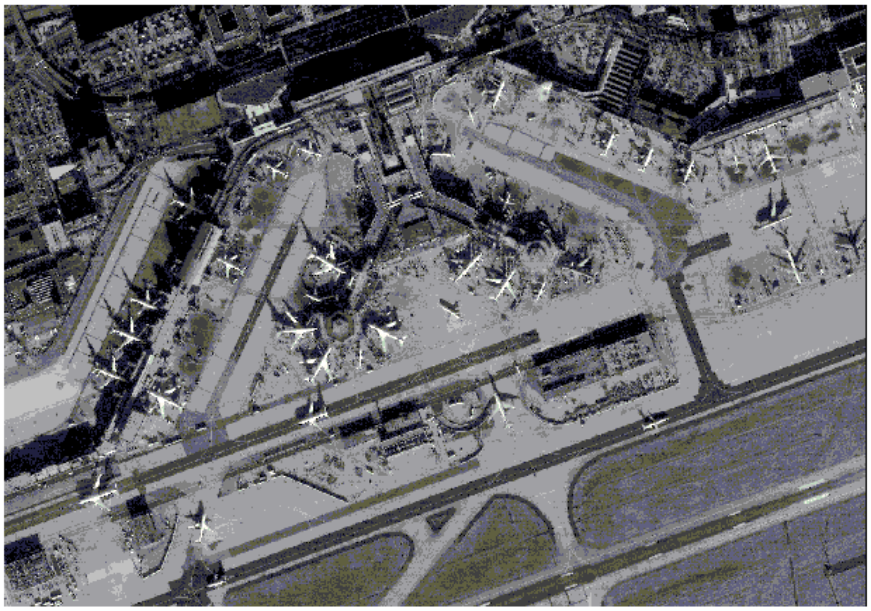

Рис 3.12. Изображение «Снимок аэропорта» полученное в результате стеганографического декодирования для авторизированного пользователя

Рис 3.13. Изображение «Фотоснимок» - полученное в результате стеганографического декодирования для авторизированного пользователя

Из анализа изображений, полученных в процессе стеганографического декодирования с демаскированием (авторизированный доступ) можно заключить следующее:

1. Вся встроенная информация изымается без ошибок.

2. Реконструированные изображения имеют незначительные визуальные искажений, которые вызваны ошибками при стеганографическом декодировании. Искажения в виде ошибочно изъятых элементов расположены равномерно, по всему изображению независимо от насыщенности изображения.

3. Пиковое отношение сигнал-шум относительно изображения-контейнера для стеганографически декодированного изображения «Снимок аэропорта» составляет 61,489 дБ, а для изображения «Лена» 61,399 дБ. Отсюда, наблюдается увеличение значения пикового отношения сигнал шум относительно изображений «Снимок аэропорта» и «Фотоснимок», декодиро-

ванных неавторизированным пользователем, соответственно на 24 дБ и 32 дБ.

На основе проведенных экспериментов для разработанной стеганографической системы можно сделать следующие выводы:

1. Восстановление встроенной информации при стеганографическом декодировании составляет 100%.

2. Реконструированные изображения при неавторизированном доступе содержат незначительное количество визуальных искажений.

3. Появляется возможность использования изображений, изъятых при демаскирующем стеганографическом декодировании, в качестве полезной информации.

4. Для насыщенных изображений оценка пикового отношения сигнал-шум дает лучшие показатели в сравнении с менее насыщенными изображениями, как при авторизированном доступе, так и для неавторизированного пользователя.

Выводы

1. Разработана стеганографическая система на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающая встраивание и изъятие скрываемой информации на основе соответственно структурного стеганографического кодирования и декодирования.

Научная новизна. Впервые спроектирована стеганографическая система на основе непосредственного встраивания скрываемого элемента в видеопоследовательность. В отличии от других стеганосистем обеспечивается одновременное встраивание и изъятие скрываемой информации соответственно в процессе формирования и реконструкции кода-контейнера в неравновесном позиционном базисе оснований. Это обеспечивает встраива-

ние скрываемой информации на основе учета количества структурной избыточности фрагментов видеоизображений.

2. Обосновано наличие структурной стеганографической избыточности в кодовом представлении стеганокода, образуемой на основе имплантации скрываемой информации в неравновесное позиционное число. Это создает дополнительную возможность для злоумышленника относительно установления факта наличия встроенной информации.

3. Разработано структурное стеганографическое кодирование с маскированием, базирующееся на следующих этапах:

- формирование неравновесного позиционного базиса для фрагмента изображения;

- структурное стеганографическое кодирование в неравновесном базисе оснований;

- маскирование структурной стеганографической избыточности путем ее локализации на основе коррекции длины стеганограммы.

Научная новизна. Впервые разработано структурное стеганографическое кодирование с маскированием. В отличии от других методов обеспечивается встраивание скрываемой информации в процессе неравновесного позиционного кодирования с последующей локализацией стеганографической избыточности. Это позволяет снизить возможность выявления злоумышленником факта наличия встроенной информации (локализовать атаку выявления факта наличия встроенной информации).

4. ***Создано правило*** встраивания информации для структурного стеганографического кодирования, заключающееся в том, что:

1) один бит скрываемого сообщения встраивается на старшую позицию неравновесного позиционного числа;

2) локализация стеганографической избыточности достигается на основе отсечения младшего бита стеганограммы.

На основе правила построено маскирующее стеганографическое кодирование для встраивания одного бита на старшую позицию неравновесного

позиционного числа. Это обеспечивает встраивание скрываемой информации в условиях:

1) повышения устойчивости скрываемой информации;

2) обеспечение восстановления элементов исходной видеопоследовательности независимо от наличия встроенной информации;

3) снижения количество структурной стеганографической избыточности.

5. Разработано демаскирующее стеганографическое декодирование для извлечения имплантированного на старшую позицию бита с одновременной реконструкцией элементов исходного неравновесного позиционного числа. Механизм демаскирующего стеганографического декодирования предусматривает предусматривает:

1) восстановление исходной длины для скорректированного в процессе маскирования стеганокода.

2) структурное стеганографическое декодирование, обеспечивающее восстановление неравновесного позиционного числа с имплантированным элементом;

3) изъятие элемента скрываемого сообщения со старшей позиции неравновесного позиционного числа

Научная новизна. Впервые разработано демаскирующее стеганографическое декодирование. В отличии от существующих методов изъятие скрываемой информации и восстановления неравновесного позиционного числа проводится на основе реконструкции стеганокода по ***биполярному принципу*** с демаскированием стеганографической избыточности. Это позволяет повысить эффективность изъятия скрываемой информации и локализацию атаки злоумышленника относительно выявления факта наличия скрываемой информации.

6. Проведены эксперименты по обработке насыщенных реалистичных изображений с использованием разработанной стеганографической системы

для встраивания информации на старшую позицию неравновесного позиционного числа. В результате чего получены следующие результаты:

1) 100% встроенной информации извлекается без ошибок;

2) для декодированных изображений при неавторизированном доступе количество визуальных искажений увеличивается, а пиковое отношение сигнал-шум уменьшается в сравнении с стеганографически декодированными изображениями;

3) изображения восстанавливаются с незначительными погрешностями и в случае необходимости существует возможность использования таких изображений в качестве полезной информации;

4) значения пикового отношения сигнал-шум для изображений «Снимок аэропорта» и «Фотоснимок» составляет соответственно 37,94 дБ и 33,978 дБ, т.е. оценка пикового отношения сигнал-шум для насыщенных изображений дает лучшие показатели в сравнении с менее насыщенными изображениями.

РАЗДЕЛ 4

ОЦЕНКА ХАРАКТЕРИСТИК ЕФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ РАЗРАБОТАННОГО МЕТОДА СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ

В разделе проведена оценка характеристик эффективности разработанного стеганографического метода для скрытого встраивания специальной информации.

Проводится оценка значений абсолютной и относительной стеганографической емкости. Определяется зависимость объема стеганографически встроенных данных от длины сформированных неравновесных чисел. Проводится сравнительный анализ разработанного стеганографического метода и существующих методов по значению стеганографической емкости.

Для разработанного метода оцениваются характеристики скрытия встроенных сообщений в случае неавторизированного доступа. Такая оценка соответствует визуальной атаке, направленно на выявления факта наличия встраивания.

Проводится сравнительная оценка эффективности изъятия скрываемой информации для разработанного стеганографического метода и существующих методов.

Рассматривается и анализируется целостность исходного изображения-контейнера после изъятия встроенных данных.

Проводится сравнительная оценка значения стойкости встроенных данных для разработанного метода и существующих стеганографических методов по количеству безошибочно изъятых встроенных данных в условиях атаки злоумышленника.

4.1 Оценка стеганографической емкости разработанной стеганографической системы

Разработанный метод стеганографического кодирования позволяет встраивать скрываемую информацию в цифровое изображение-контейнер на основе структурных особенностей [13, 15, 19, 21, 25]. Этапу стеганографического кодирования предшествует имплантация данных скрываемого сообщения на позицию старшего элемента неравновесного позиционного числа $A(j)$ длиной m (рис 4.1).

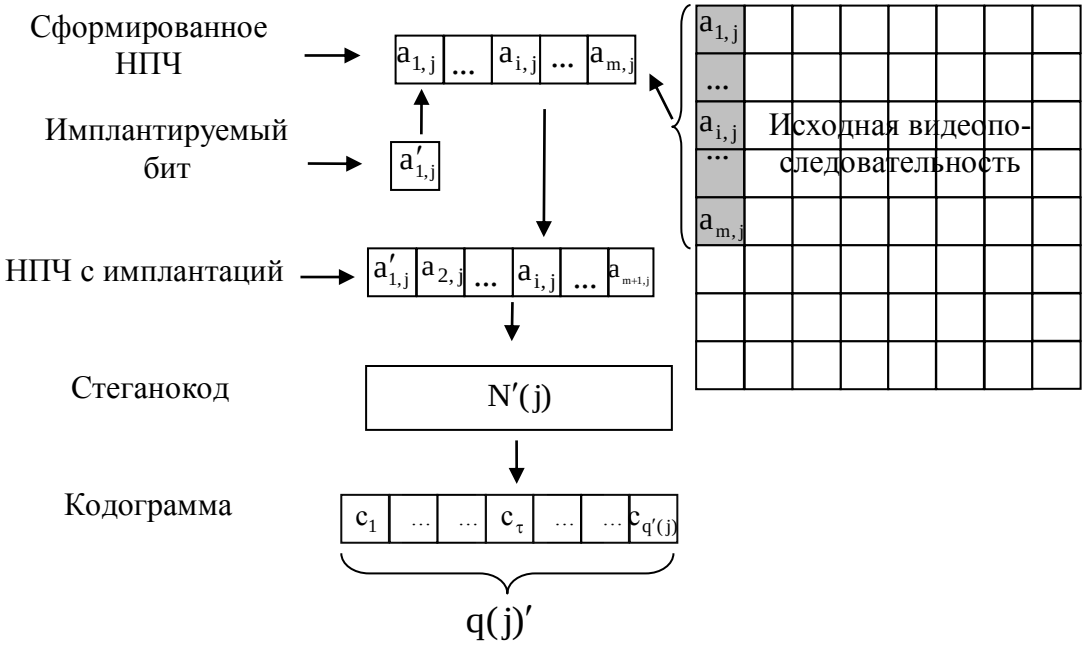

Рис. 4.1 Схема имплантации бита в неравновесное позиционное число

Множество неравновесных позиционных чисел $\{A(j)\}$ длиной m формируется отдельно для каждой цветовой составляющей изображения-контейнера.

Имплантация задается следующей формулой $A(j)' = A(j) \cup b_\xi$, $b_\xi = a'_{1,j}$.

Здесь $A(j)'$ - число с имплантированным битом $a'_{1,j}$ на позицию старшего элемента; b_ξ - ξ-й элемент встраиваемой последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$, $b_\xi \in [0; 255]$, $\xi = \overline{1, \nu}$.

В результате имплантации, число $A(j)'$ примет следующий вид $A(j)' = \{a'_{1,j};...;a_{2,j};...;a_{i,j};...;a_{m+1,j}\}$.

В процессе стеганографического кодирования для числа с имплантацией $A(j)'$ формируется стеганокод $N'(j)$. Затем для значения стеганокода $N'(j)$ формируется кодограмма $C(A(j)')$: $C(A(j)') = \{c_1, \ldots, c_\tau, \ldots, c_{q(j)'}\}$, где $q(j)'$ - длина кодограммы $C(A(j)')$.

Оценку объема встраиваемой информации будем проводить с позиции относительной стеганографической емкости $w_{отн}^{(m)}$ системы.

Значение относительной стеганографической емкости показывает процентное отношение объема $w_{встр}^{(m)}$ встраиваемой информации относительно объема $W_{исх}$ изображения-контейнера. Данная величина используется для оценки эффективности стеганографической системы по удельному объему встраиваемой информации относительно объема изображения-контейнера.

Величина $w_{отн}^{(m)}$ относительной стеганографической емкости системы определяется на основе следующей формулы:

$$w_{отн}^{(m)} = \frac{w_{встр}^{(m)}}{W_{исх}} = \frac{3 \cdot z_{строк}\ z_{столб}}{m \cdot W_{исх}},$$

где $z_{строк}\ z_{столб}$ - размер изображения-контейнера.

Физический смысл данной величины заключается том, что проводится оценка количества бит исходного изображения-контейнера приходящегося на один бит встроенного сообщения.

В процентах значение относительной стеганографической емкости системы оценивается на основе следующего выражения:

$$w_{отн}^{(m)} = \frac{w_{встр}^{(m)}}{W_{исх}} \cdot 100\% = \frac{3 \cdot z_{строк}\ z_{столб}}{m \cdot W_{исх}} \cdot 100\%. \qquad (4.1)$$

Формула для абсолютной стеганографической емкости разработанной системы будет иметь следующий вид:

$$w_{встр}^{(m)} = L = \frac{3 \cdot z_{строк}\ z_{столб}}{m}, \qquad (4.2)$$

где L - количество сформированных неравновесных чисел

Оценим объем $W_{исх}$ исходного изображения. Значение объема $W_{исх}$ исходного изображения будет равно произведению общего количества L сформированных неравновесных позиционных чисел по трем цветовым компонентам изображения-контейнера на количество бит $q(j)_{исх}$ необходимое для двоичного представления НПЧ длиной m элементов

$$W_{исх} = L \cdot q(j)_{исх} \text{ (бит)}. \qquad (4.3)$$

Учитывая, что для двоичного представления одного элемента НПЧ необходимо 8 бит, количество $q(j)_{исх}$ бит, необходимое для двоичного представления НПЧ длиной m элементов определяется на основе следующей формулы:

$$q(j)_{исх} = 8 \cdot m \text{ (бит)}. \qquad (4.4)$$

Перепишем формулу (4.3) с учетом выражения (4.4):

$$W_{\text{исх}} = L \cdot m \cdot 8 \text{ (бит)}. \qquad (4.5)$$

Теперь преобразуем формулу (4.5) учитывая выражения (4.2) и (4.5). В этом случае получим:

$$w_{\text{отн}}^{(m)} = \frac{L}{L \cdot m \cdot 8} \cdot 100\% = \frac{1}{8 \cdot m} \cdot 100\%.$$

Диаграмма зависимости значения $w_{\text{отн}}^{(m)}$ относительной стеганографической емкости стеганографического алгоритма от различной длины $m = 2; 3; 4; 6$ сформированных НЧ представлена на рис 4.2.

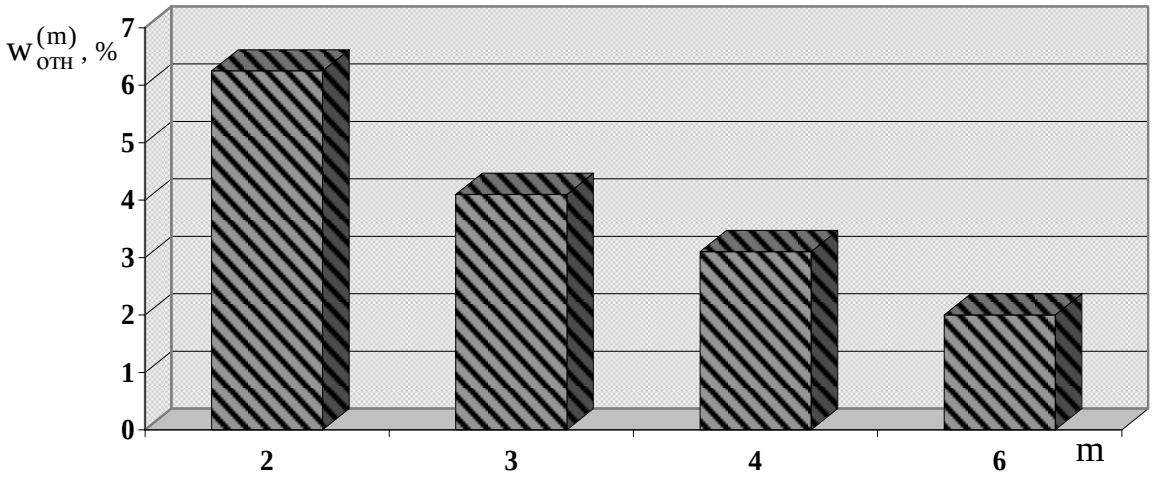

Рис. 4.2. Зависимость значения $w_{\text{отн}}^{(m)}$ относительной стеганографической емкости стеганографического алгоритма от длины m НПЧ

Из анализа рис. 4.2 можно сделать вывод, состоящий в том, что в случае формирования НПЧ длиной $m = 2$, относительная стеганографическая емкость разработанной системы принимает значение, равное 6,25 %. Наоборот, при формировании НПЧ длиной $m = 6$ стеганографическая система обладает наименьшей относительной емкостью- 2%.

Проведем сравнительную оценку относительной стеганографической емкости $w_{отн}^{(m)}$ для разработанного стеганографического метода и существующих стеганографических методов непосредственного встраивания информации в изображение-контейнер. Сравнительную оценку будем проводить для следующих стеганографических методов:

- метод встраивания информации в наименее значимый бит элемента спектрального представления контейнера после квантования (режим 2 НЗБ);

- метод встраивания информации на основе расширения спектра (РС).

Выражение для определения относительной стеганографической емкости $w_{отн}^{z_{строк}\ z_{столб}}$ метода НЗБ имеет вид:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{w_{встр}^{z_{строк}\ z_{столб}}}{W_{исх}} \cdot 100\ \%. \qquad (4.6)$$

Объем $W_{исх}$ исходного изображения для метода НЗБ определяется, как произведение общего количества элементов спектрального представления изображения-контейнера на количество бит, необходимое для двоичного представления одного элемента (8 бит). В этом случае объем $W_{исх}$ исходного изображения определяется по формуле:

$$W_{исх} = 8 \cdot 3 \cdot z_{строк}\ z_{столб} = 24 \cdot z_{строк}\ z_{столб}\ (бит) \qquad .(4.7)$$

Объем $w_{встр}^{(z_{строк}\ z_{столб})}$ встраиваемой информации для метода НЗБ зависит от размера контейнера и определяется на основе следующего выражения:

$$w_{встр}^{(z_{строк}\ z_{столб})} = \frac{3 \cdot z_{строк}\ z_{столб}}{\omega}\ (бит), \qquad (4.8)$$

где $z_{строк}\ z_{столб}$ - размер изображения-контейнера,

ω - количество элементов спектрального представления, необходимых для встраивания 1 бита скрываемой информации.

Перепишем формулу для относительной стеганографической емкости метода с учетом выражений (4.7) и (4.8). Тогда получим:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{w_{встр}^{z_{строк}\ z_{столб}}}{W_{исх}} \cdot 100\% = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot \omega} \cdot 100\%.$$

В этом случае в зависимости от количества элементов ω, необходимых для встраивания относительная стеганографическая емкость $w_{отн}^{z_{строк}\ z_{столб}}$ метода НЗБ в режиме 2 примет следующие значения:

- для $\omega = 2$:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot 2} \cdot 100\% = \frac{1}{16} \cdot 100\ \% = 6{,}25\ \%;$$

- для $\omega = 4$:

$$w_{отн}^{z_{строк}\ z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{24 \cdot z_{строк}\ z_{столб} \cdot 4} \cdot 100\% = \frac{1}{32} \cdot 100\ \% = 3{,}1\ \%.$$

Рассмотрим теперь метод встраивания информации на основе расширения спектра. Относительная стеганографическая емкость $w_{отн}^{z_{строк}\ z_{столб}}$ для данного метода определяется на основе следующего выражения

$$w_{встр}^{z_{строк}\ z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб}}{\omega}\ \text{(бит)}, \qquad (4.9)$$

а объем $W_{исх}$ исходного изображения-контейнера для метода РС определяется на основе выражения (4.7). В этом случае формула для определения значения $w_{отн}^{z_{строк}\, z_{столб}}$ относительной стеганографической емкости примет следующий вид:

$$w_{отн}^{z_{строк}\, z_{столб}} = \frac{w_{встр}^{z_{строк}\, z_{столб}}}{W_{исх}} \cdot 100\% =$$

$$= (3 \cdot z_{строк}\ z_{столб} / \omega) / 24 \cdot z_{строк}\ z_{столб} \cdot 100\ \%$$

Тогда в случае встраивании 4 бит скрываемого сообщения в блок размером 8×8, относительная пропускная способность для метода РС примет следующее значение:

$$w_{отн}^{z_{строк}\, z_{столб}} = \frac{3 \cdot z_{строк}\ z_{столб} \cdot 4}{24 \cdot z_{строк}\ z_{столб} \cdot 64} = \frac{1}{128} \cdot 100\ \% = 0{,}78\ \%.$$

В табл. 4.1 представлены значения относительной стеганографической емкости методов НЗБ, РС и разработанного метода и значения ПОСШ для изображений «Снимок аэропорта», «Фотоснимок» и «Самолет на фоне неба».

Из анализа оценки относительной стеганографической емкости в табл.4.4 можно сделать следующие выводы:

1) при одинаковых значениях относительной стеганографической емкости выигрыш для разработанного метода относительно метода НЗБ в режиме 2 по величине ПОСШ для различных классов изображений составляет:

- для шага квантования $q = 1$ от 5% до 66 %;

- для шага квантования $q = 2$ от 35% до 75 %;

- для шага квантования $q = 4$ от 47% до 80 %;

Таблица 4.1

Зависимость значения $w_{отн}$ от ПОСШ для изображения «Снимок аэропорта»

Относительная емкость, %	Метод стеганографического встраивания		Значение ПОСШ, дБ		
			«Снимок аэропорта»	«Фотоснимок»	«Самолет на фоне неба»
6,25	НЗБ режим 2	$q = 1$	14,67	14,12	14,62
		$q = 2$	11,17	12,03	11,13
		$q = 4$	8,69	9,11	8,79
	РМ	$m = 2$	41,799	37,768	42,911
4,1	РМ	$m = 3$	39,074	35,058	40,052
3,1	НЗБ режим 2	$q = 1$	32,12	33,42	31,43
		$q = 2$	26,43	22,15	20,45
		$q = 4$	18,54	18,27	18,03
	РМ	$m = 4$	37,94	33,978	38,973
2	РМ	$m = 6$	36,931	33,019	38,121
0,78.	РС	$\omega = 16$	16,93	13,019	18,121

2) для разработанного метода выигрыш относительно метода РС по относительной стеганографической емкости составляет от 1,22 до 5,47 %, а по величине ПОСШ от 60 до 70% (что соответствует от 20 до 25 дБ)

4.2 Оценка характеристик скрытия встроенных сообщений в случае неавторизированного доступа

Для разработанного стеганографического метода встраивания информации на позицию старшего элемента НПЧ оценим характеристики скрытия встроенных данных при неавторизированном доступе. **В данном случае такая оценка будет соответствовать визуальной атаке противника, направленной на выявление факта наличия встроенной информации.** При этом у противника будет отсутствовать следующая информация: позиция встроенного элемента $a'_{1,j}$; основание встроенного элемента $a'_{1,j}$.

Экспериментально оценим визуальные характеристики скрытия данных для разработанного стеганографического алгоритма. Эксперимент проводится в следующих условиях:

1) в процессе встраивания на этапе имплантации длина неравновесных позиционных чисел выбирается равной $m = 2; 3; 4; 6$;

2) имплантация одного бита информации осуществляется на старшую позицию $\gamma = 1$ каждого неравновесного позиционного числа;

3) процесс декодирования осуществляется без устранения эффекта маскирования (неавторизированный доступ);

В качестве исходных изображений будем использовать:

1) сильнонасыщенное изображение «Снимок аэропорта» (рис А1);

2) средненасыщенное изображение «Фотоснимок» (рис А2);

3) слабонасыщенное изображение «Самолет на фоне неба» (рис А3).

Результаты эксперимента в условиях выбора НПЧ длиной $m = 2$ представлены на примере следующих изображений, декодированных неавторизированным пользователем:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 4.3),

Рис 4.3. Изображение «Снимок аэропорта», декодированное неавторизированным пользователем при длине НПЧ $m = 2$

Рис 4.4. Изображение «Фотоснимок», декодированное неавторизированным пользователем при длине НПЧ $m = 2$

- средненасыщенное декодированное изображение «Фотоснимок» (рис. 4.4);

- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 4.4).

Рис 4.5. Изображение «Самолет на фоне неба», декодированное неавторизированным пользователем при длине НПЧ $m = 2$

Значения оценки пикового отношения сигнал шум для изображений, декодированных в случае неавторизированного пользователя, относительно исходных изображений-контейнеров составляет:

- для сильнонасыщенного изображения «Снимок аэропорта»- 41,799 дБ;

- для средненасыщенного изображения «Фотоснимок»- 37.768 дБ;

- для слабонасыщенного изображения «Самолет на фоне неба»- 42.911 дБ.

Результаты эксперимента в условиях выбора НПЧ длиной $m = 3$ представлены на примере следующих изображений, декодированных при неавторизированном доступе:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 4.6),

- средненасыщенное декодированное изображение «Фотоснимок» (рис. 4.7);

- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 4.8).

Рис 4.6. Изображение «Снимок аэропорта», декодированное неавторизированным пользователем при длине НПЧ $m = 3$

Рис 4.7. Изображение «Фотоснимок», декодированное неавторизированным пользователем при длине НПЧ $m = 3$

Рис 4.8. Изображение «Самолет на фоне неба», декодированное неавторизированным пользователем при длине НПЧ $m = 3$

Значения оценки пикового отношения сигнал шум для изображений, декодированных при неавторизированном доступе относительно исходных изображений-контейнеров составляет:

- для сильнонасыщенного изображения «Снимок аэропорта»- 39,074 дБ;

- для средненасыщенного изображения «Фотоснимок»- 35,058 дБ;

- для слабонасыщенного изображения «Самолет на фоне неба»- 40,052 дБ.

Результаты эксперимента в условиях выбора НПЧ, длиной $m = 4$ представлены на примере следующих изображений, декодированных при неавторизированном доступе:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис.4.9),

- средненасыщенное декодированное изображение «Фотоснимок» (рис. 4.10);

- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 4.11).

Рис 4.9. Изображение «Снимок аэропорта», декодированное неавторизированным пользователем при длине НПЧ $m = 4$

Рис 4.10. Изображение «Фотоснимок», декодированное неавторизированным пользователем при длине НПЧ $m = 4$

Рис 4.11. Изображение «Самолет на фоне неба», декодированное неавторизированным пользователем при длине НПЧ $m = 4$

Значения оценки пикового отношения сигнал шум для изображений, декодированных при неавторизированном доступе относительно исходных изображений-контейнеров составляет:

- для сильнонасыщенного изображения «Снимок аэропорта»- 37,94 дБ;
- для средненасыщенного изображения «Фотоснимок»- 33,978 дБ;
- для слабонасыщенного изображения «Самолет на фоне неба»- 38,973 дБ.

Результаты эксперимента в условиях выбора НПЧ длиной $m = 6$ представлены на примере следующих изображений, декодированных при неавторизированном доступе:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 4.12),
- средненасыщенное декодированное изображение «Фотоснимок» (рис. 4.13);
- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 4.14).

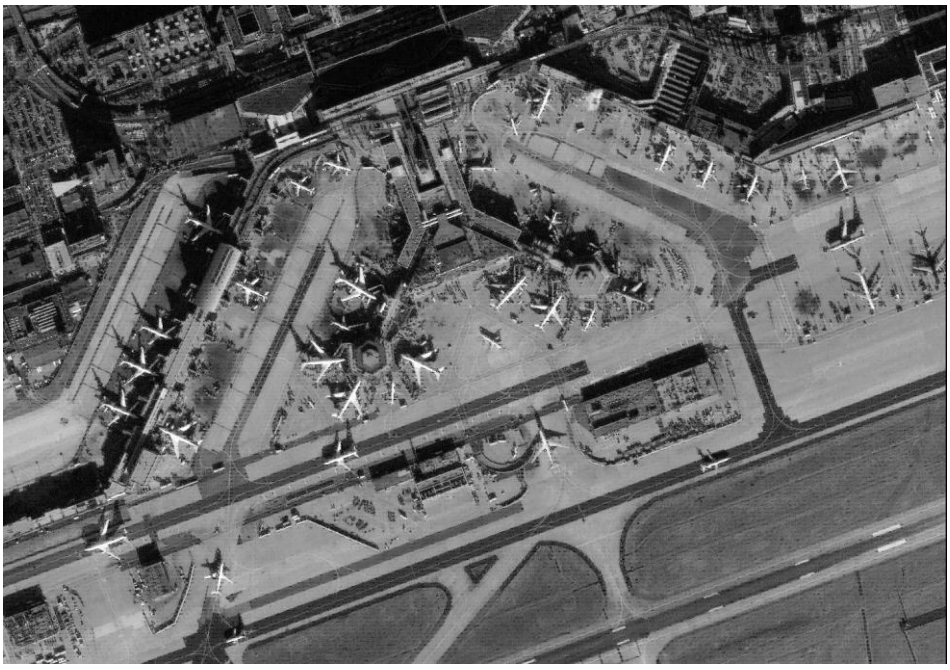

Рис 4.12. Изображение «Снимок аэропорта», декодированное неавторизированным пользователем при длине НПЧ $m = 6$

Рис 4.13. Изображение «Фотоснимок», декодированное неавторизированным пользователем при длине НПЧ $m = 6$

Рис 4.14. Изображение «Самолет на фоне неба», декодированное неавторизированным пользователем при длине НПЧ $m = 6$

Значения оценки пикового отношения сигнал шум для изображений, декодированных при неавторизированном доступе, относительно исходных изображений-контейнеров составляет:

- для сильнонасыщенного изображения «Снимок аэропорта»- 36,931 дБ;
- для средненасыщенного изображения «Фотоснимок»- 33.019 дБ;
- для слабонасыщенного изображения «Самолет на фоне неба»- 38.121 дБ.

На рис. 4.15 представлены обобщенные результаты по оценке значения пикового отношения сигнал-шум для декодированных изображений при неавторизированном доступе.

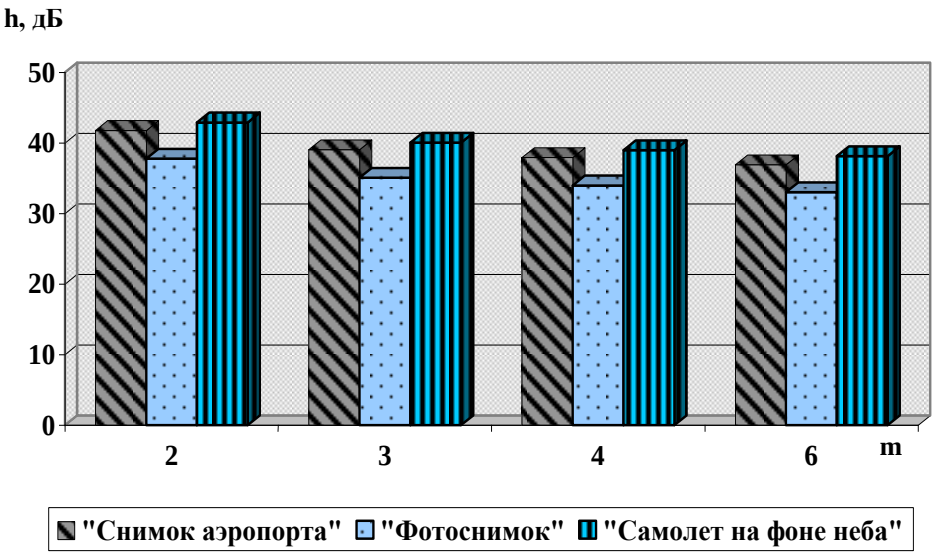

Рис. 4.15. Значения ПОСШ для декодированных изображений при различных значениях длины сформированных НПЧ

Из анализа рис. 4.15 можно сделать следующие выводы:

1. Для разработанного метода стеганографического кодирования визуальные искажения, вносимые в изображение при неавторизированном доступе, являются незначительными как с позиции зрительного восприятия, так и с позиции машинной обработки. Это позволяет использовать разработанный метод для скрытого встраивания информации.

2. При одинаковых условиях стеганографического кодирования наибольшие искажениями наблюдаются для реалистичных изображений с повышенной яркостью и средней насыщенностью мелкими деталями. Значение ПОСШ для средненасыщенного изображения «Фотоснимок» меньше значения ПОСШ для сильнонасыщенного изображения «Снимок аэропорта» на 10-11 % (3,8-4 дБ). Значение ПОСШ для средненасыщенного изображения «Фотоснимок» меньше значения ПОСШ для сильнонасыщенного изображения «Самолет на фоне неба» на 13 % (5 дБ).

3. Наилучшей визуальной устойчивость (наименьшей уязвимостью) к визуальной атаке, направленной на выявления факта наличия встраивания обладает разработанная стеганографическая система в случае встраивания данных в слабонасыщенное изображение «Снимок самолета на фоне неба». Для разработанного метода величина ПОСШ для изображений, декодированных при неавторизированном доступе, для различных m принимает значения от 38.1 до 42.9 дБ.

4. Величина ПОСШ для всех типов изображения принимает наибольшее значение в случае встраивания в НПЧ длиной $m = 2$. При этом ***выигрыш*** в значении ПОСШ относительно встраивания в НПЧ с длиной $m = 3; 4; 6$ будет соответственно равен:

- для сильнонасыщенного изображения «Снимок аэропорта» от 7 до 13%, что составляет от2,725 дБ до 4,86 дБ;

- для средненасыщенного изображения «Фотоснимок» от 7 до 14%, что составляет от 2,71 дБ до 4,79 дБ;

- для слабонасыщенного изображения «Самолет на фоне неба» от 7,1 до 12,5%, что составляет от 2,85 дБ до 4,79 дБ.

4.3 Сравнительная оценка эффективности изъятия скрываемой информации авторизированным пользователем

Рассмотрим процесс извлечения стеганографически встроенных данных для разработанного метода. Необходимо учитывать, что для авторизированного пользователя скрываемое сообщение является полезной информацией. Поэтому при авторизированном доступе объем изъятых данных должен составлять 100 % от объема встроенных данных. Для разработанного метода, изъятие бита скрываемого сообщения осуществляется при наличии следующей информации (авторизированный доступ):

- позиция стеганокода в сжатом представлении изображения;
- позиция встроенного элемента $a'_{1,j}$;
- основание встроенного элемента. $a'_{1,j}$.

В этом случае демаскирующее стеганографическое декодирование предусматривает устранения эффекта локализации структурной стеганографической избыточности. Проведение демаскирования стеганокода $N'''(j)$ осуществляется путем приведения его длины к значению длины исходного стеганокода $N^*(j)$. Это происходит вследствие добавления младшего нулевого бита к двоичному содержанию стеганокода $N(j)'''$ и описывается следующим выражением:

$$N(j)^* = N(j)''' \cdot 2, \quad C'''_j = \{C'_j; 0\} = \{c_1,...,c_\tau,...,c_{q(j)'-1}, 0\},$$

Восстановление встроенного элемента $a'_{1,j}$ реализуется на основе информации о позиции стеганокода в сжатом изображении, о позиции встроенного элемента и его основания $\psi'_{1,j} = 2$. Для этого используется следующая формула:

$$a''_{1,j} = f^{(-1)}(N(j)^*, V'_{1,j}, \psi'_{1,j}),$$

где $V'_{1,j}$ - вес встроенного элемента $a'_{1,j}$.

Как видно из формулы, восстановление встроенного элемента $a'_{1,j}$ осуществляется на основе значения стеганокода $N^*(j)$ после устранения эффекта маскирования. Однако в этом случае необходимо учитывать, что значение стеганокода $N^*(j)$ после устранения эффекта маскирования не всегда принимает значения исходного стеганокода.

Возможны случаи, когда значение скорректированного стеганокода $N(j)^*$ будет отличаться от исходного значения стеганокода $N(j)'$ значением младшего бита, т.е.

$$c'_{q(j)'} \neq c^*_{q(j)'} .$$

В этом случае значения исходного $N(j)'$ и демаскированного $N(j)^*$ стеганокодов будут отличаться на единицу, т.е.

$$\text{если } N(j)^* \neq N(j)', \text{ то } \quad N(j)' - N(j)^* = 1.$$

Для разработанной стеганографической системы погрешность в значении демаскированного стеганокода $N^*(j)$ относительно исходного значения стеганокода $N(j)'$ не влияет на восстановление элемента $a''_{1,j}$. Безпогрешное изъятие встроенного элемента достигается за счет имплантации на позицию старшего элемента НПЧ. В этом случае вес встраиваемого элемента $V'_{1,j}$ в неравновесном позиционном числе будет наибольшим, т.е.

$$V'_{1,j} = \max_{1 \le i \le m+1} .\{V'_{i,j}\}.$$

Следовательно, встраиваемый элемент будет более устойчив к прямым и обратным преобразованиям в стеганографических системах.

Оценим вероятность $P_{из}$ безошибочного изъятия встроенных данных авторизированным пользователем. Такая вероятность $P_{из}$ показывает отношение количества $w_{из}^{(m)}$ безошибочно изъятых бит на количество $w_{встр}^{(m)}$ встроенных бит и описывается следующим выражением:

$$P_{из} = \frac{w_{из}^{(m)}}{w_{встр}^{(m)}}.$$

В случае, когда стеганографическая система позволяет безошибочно изъять 100% значение вероятности $P_{из}$ будет равна единице, т.е.

$$P_{из} = 1.$$

Докажем что для разработанной стеганографической системы, вероятность $P_{из}$ безошибочного изъятия встроенных данных авторизированным пользователем принимает максимальное значение. Для этого должно выполняться следующее неравенство:

$$a''_{1,j} = f^{(-1)}(N(j)^*, V'_{1,j}, \psi'_{1,j}),$$

где $a''_{1,j}$ - значения восстановленного элемента;

$a'_{1,j}$ - значение встроенного элемента;

$N(j)^*$ - восстановленное значение стеганокода;

ψ'_{1j} - значение основания встроенного элемента $a'_{1,j}$;

$V'_{1,j}$ - весовой коэффициент встроенного элемента $a'_{1,j}$.

Рассмотрим первый случай, когда значения стеганокода $N^*(j)$ после устранения эффекта маскирования принимает значение исходного стеганокода $N(j)'$, т.е.

$$N^*(j) = N(j)'.$$

Для этого будем учитывать формулу для для стеганокода:

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) .$$

Тогда с учетом следующих соотношений:

:

$$\frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} < 1, \quad \frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} < 1, \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}} < 1$$

или

$$\frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} = 0, \quad [\frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} + \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}}] \cdot \psi'_{1,j} = 0$$

будет выполняться равенство:

$$a''_{1,j} = [\frac{a'_{1,j} V'_{1,j}}{V'_{1,j}} + \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}}] - [\frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} + \frac{\sum_{i=1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}}] \cdot \psi'_{1,j} = a'_{1,j}.$$

Отсюда в случае, когда выполняется равенство

$$N^{*}(j) = N(j)'$$

значение встроенного элемента $a'_{1,j}$ восстанавливается без ошибок. Тогда вероятность $P_{из}$ безошибочного изъятия будет равна единице, т.е.

$$P_{из} = 1.$$

Рассмотрим второй случай, когда значение стеганокода $N^{*}(j)$ после устранения эффекта маскирования будет отличаться от значения исходного стеганокода $N(j)'$ на единицу, т.е.

$$N^{*}(j) = N(j)' - 1.$$

Для этого перепишем выражение (4.10) с учетом формулы для стеганокода:

$$N(j)^{*} = (A(j)', V^{(1)}, V^{(2)}) - 1.$$

Тогда учитывая следующие соотношения

$$\frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} < 1, \quad \frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} < 1, \quad \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}} < 1, \quad \frac{1}{V'_{1,j}} < 1$$

или

$$\frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} = 0, \quad \frac{1}{V'_{1,j}} = 0, \quad [\frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} + \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}}] \cdot \psi'_{1,j} = 0$$

будет выполнятся равенство:

$$a''_{1,j} = [\frac{a'_{1,j} V'_{1,j}}{V'_{1,j}} + \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} - \frac{1}{V'_{1,j}}] -$$

$$-[\frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} + \frac{\sum_{i=1}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}} - \frac{1}{V'_{1,j}}] \cdot \psi'_{1,j} = a'_{1,j}.$$

Отсюда погрешность в определении значения стеганокода $N^*(j)$ в результате демаскирования не влияет на восстановление встроенного элемента $a'_{1,j}$. При этом значение восстановленного элемента $a''_{1,j}$ будет равно значению встроенного элемента $a'_{1,j}$.

Учитывая то, что в обоих случаях встроенный элемент $a'_{1,j}$ изымается без ошибок, можно заключить, что для разработанного стеганографического алгоритма вероятность $P_{из}$ безошибочного изъятия будет равна единице, т.е.

$$P_{из} = \frac{w^{(m)}_{из}}{w^{(m)}_{встр}} = 1.$$

Сравним значения вероятность $P_{из}$ безошибочного изъятия встроенных данных для разработанного стеганографического метода и методов встраивания НЗБ и расширения спектра.

Для метода НЗБ объем $w_{из}^{z_{строк}\ z_{столб}}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение меньше $w_{встр}^{z_{строк}\ z_{столб}}$ встроенных данных, т.е.

$$w_{из}^{z_{строк}\ z_{столб}} < w_{встр}^{z_{строк}\ z_{столб}}.$$

Для такого метода вероятность безошибочного изъятия встроенных данных буде равно $P_{из} = 0{,}6$.

Теперь рассмотрим вероятность безошибочного изъятия встроенных данных для метода РС. В случае встраивания бита скрываемого сообщения на основе метода РС, его изъятие будет осуществляться с вероятностью $P_{из} = 0{,}5$.

На рис. 4.16. представлена сравнительная диаграмма значений вероятности $P_{из}$ безошибочного изъятия встроенных данных для методов НЗБ, РС и разработанного метода в условиях отсутствия атак на встроенное сообщение.

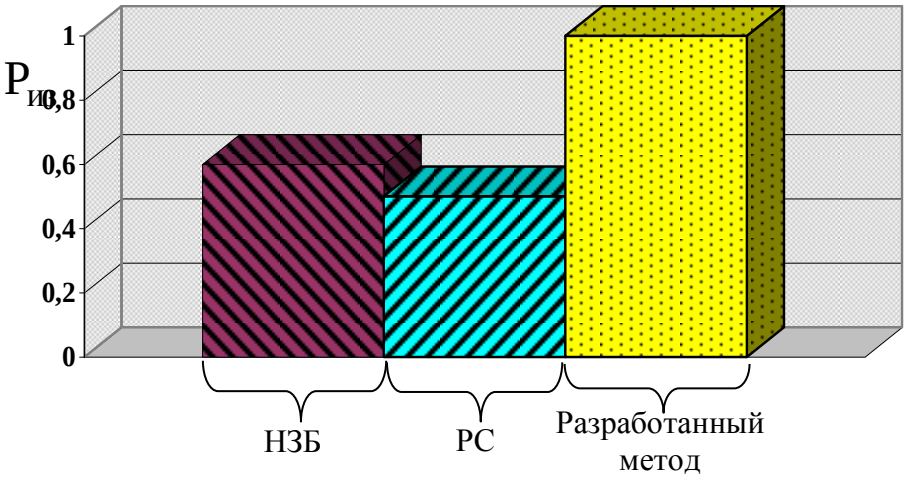

Рис. 4.16. Диаграмма значений вероятности $P_{из}$ для методов НЗБ, РС и разработанного метода в условиях отсутствия атак на встроенное сообщение

Из анализа рис. 4.16 можно сделать следующие выводы:

1) для разработанного стеганографического метода вероятность $P_{из}$ безошибочного изъятия встроенных данных в условиях отсутствия атак на встроенное сообщение равна единице;

2) выигрыш для разработанного метода относительно метода НЗБ по значению вероятности $P_{из}$ безошибочного изъятия в условиях отсутствия атак на встроенное сообщение составляет 40%;

3) выигрыш для разработанного метода относительно метода РС по значению вероятности $P_{из}$ безошибочного изъятия в условиях отсутствия атак на встроенное сообщение составляет 50%;

4) наличие для разработанного метода возможности безошибочного изъятия встроенных данных в условиях отсутствия атак позволяет использовать его для успешного скрытия информации в специализированных критических системах.

4.4 Оценка устойчивости скрываемых сообщений к атакам злоумышленника для разработанной стеганографической системы.

Оценим устойчивость данных встроенных на основе разработанного стеганографического кодирования в условиях применения противником активной атаки, направленной на разрушение встроенного сообщения.

Для оценки устойчивости встроенных данных рассмотрим пример использования разработанного стеганографического алгоритма в условиях применения злоумышленником следующих атак:

1. Выполнение прямого и обратного дискретного косинусного преобразования с последующим округлением вещественного значения.

2. Прямое и обратное квантование с различными факторами потери качества.

Атакам подвергаются значения стеганокодов, сформированных для изображений различных типов, а именно:

1) сильнонасыщенное изображение «Снимок аэропорта» (рис 4.3);

2) средненасыщенное изображение «Фотоснимок» (рис 4.4);

3) слабонасыщенное изображение «Снимок самолета на фоне неба» (рис 4.5).

Эксперимент проводится в следующих условиях:

1) в процессе встраивания на этапе имплантации длина неравновесных позиционных чисел выбирается равной $m = 2;3;4;6$;

2) формирование НПЧ проводится для трех цветовых компонент исследуемого изображения;

3) имплантация одного бита информации осуществляется на старшую позицию $\gamma = 1$ каждого неравновесного позиционного числа:

$$A(j) = \{a_{1,j};\ldots;a_{i,j};\ldots;a_{m,j}\} \bigcup b_{\xi} = A'(j) = \{a_{1,j};a'_{2,j}\ldots;a_{i,j};\ldots;a_{m+1,j}\}.$$

4) значение коэффициента квантования выбирается равным $q = 1; 2; 5; 10$.

В табл. 4.2 представлены значения процентного соотношения количества $w_{из}^{(m)}$ безошибочно изъятых бит относительно количества $w_{встр}^{(m)}$ встроенных бит для разработанной стеганографической системы в условиях атак.

Таблица 4.2

Процентное соотношение $w_{из}^{(m)}$ безошибочно изъятых бит встроенного сообщения для изображения «Снимок аэропорта» в условиях атак

Условия атаки	Количество $w_{из}^{(m)}$ безошибочно изъятых бит встроенного сообщения, %			
	$m = 2$	$m = 3$	$m = 4$	$m = 6$
Без атаки	100	100	100	100
ДКП	98,3	99,3	99,7	99,9
$q = 1$	80,4	91,9	96,8	99,4
$q = 2$	78,5	91	96,4	99,3
$q = 5$	75,6	90	95,9	99,3
$q = 10$	74,1	89,1	95,4	99,2

Проанализировав значения в табл. 4.2 можно сделать вывод, что:

1) для разработанного стеганографического кодирования количество $w_{из}^{(m)}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение 100% независимо от длины сформированных НПЧ;

2) для разработанного метода в условиях атаки ДКП и квантования с шагом $q = 10$ наименьший процент 74,1 % по количеству $w_{из}^{(m)}$ правильно изъятых бит достигается для сообщения встроенного в НПЧ длиной $m = 2$;

3) наибольший процент 99,2 % по количеству $w_{из}^{(m)}$ правильно изъятых бит в условиях атаки ДКП и квантования с шагом $q = 10$ для разработанного

метода достигается для стеганографически встроенного сообщения в НПЧ длиной $m = 6$.

В табл. 4.3 представлены процентные значения $w_{из}^{(m)}$ количества безошибочно изъятых бит стеганографически встроенного сообщения в изображение «Фотоснимок» в условиях атак.

Таблица 4.3

Процентное соотношение $w_{вост}$ безошибочно изъятых бит встроенного сообщения для изображения «Фотоснимок»

Условия атаки	Количество $w_{из}^{(m)}$ безошибочно изъятых бит встроенного сообщения, %			
	$m = 2$	$m = 3$	$m = 4$	$m = 6$
Без атаки	100	100	100	100
ДКП	98	99,1	99,9	99,9
$q = 1$	76,9	89,4	94,2	98,3
$q = 2$	75,2	88,4	93,8	98,3
$q = 5$	73,4	87,4	93,3	98,2
$q = 10$	72,9	87,2	93,1	98,2

Проанализировав значения в табл. 4.3 можно сделать вывод, что:

1) для разработанного стеганографического кодирования количество $w_{из}^{(m)}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение 100% независимо от длины сформированных НПЧ;

2) для разработанного метода в условиях атаки ДКП и квантования с шагом $q = 10$ наименьший процент 72,9 % по количеству $w_{из}^{(m)}$ правильно изъятых бит достигается для сообщения, стеганографически встроенного в НПЧ длиной $m = 2$;

3) наибольший процент 98,2 % по количеству $w_{из}^{(m)}$ правильно изъятых бит в условиях атаки ДКП и квантования с шагом $q=10$ для разработанного метода достигается при встраивании сообщения в НПЧ длиной $m=6$.

В табл. 4.4 представлены процентные значения $w_{из}^{(m)}$ количества безошибочно изъятых бит стеганографически встроенного сообщения в изображение «Самолет на фоне неба» в условиях атак.

Таблица 4.4

Процентное соотношение $w_{из}^{(m)}$ безошибочно изъятых бит встроенного сообщения для изображения «Самолет на фоне неба» в условиях атак

Условия атаки	Количество $w_{из}^{(m)}$ безошибочно изъятых бит встроенного сообщения, %			
	$m=2$	$m=3$	$m=4$	$m=6$
Без атаки	100	100	100	100
ДКП	97,7	99,2	99,7	99,9
$q=1$	78,2	89,8	97,2	99,8
$q=2$	74,6	89,1	96,9	99,8
$q=5$	69,6	88,1	96,6	99,7
$q=10$	68,7	87,8	96,5	99,8

Проанализировав значения в табл. 4.4 можно сделать вывод, что:

1) для разработанного стеганографического кодирования количество $w_{из}^{(m)}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение 100% независимо от длины сформированных НПЧ;

2) для разработанного метода в условиях атаки ДКП и квантования с шагом $q=10$ наименьший процент 68,7 % по количеству $w_{из}^{(m)}$ правильно изъятых бит достигается для стеганографически встроенного сообщения в НПЧ длиной $m=2$;

3) в условиях атаки ДКП и квантования с шагом $q=10$ наименьший процент 99,8 % по количеству $w_{из}^{(m)}$ правильно изъятых бит достигается для сообщения встроенного на основе разработанного метода в НПЧ длиной $m=6$.

Сравним процентные значения количества $w_{из}^{(z_{строк}z_{столб})}$ изъятых бит относительно количества $w_{встр}^{(z_{строк}z_{столб})}$ встроенных бит для метода РС, НЗБ и разработанного метода.

Для метода НЗБ и РС количество $w_{из}^{(z_{строк}z_{столб})}$ безошибочно изъятых бит в условиях активных атак составляет 50%.

На рис. 4.17 представлена диаграмма процентного значения количества безошибочно изъятых бит для методов НЗБ, РС и разработанного метода в условиях применения атаки ДКП и квантования с шагом $q=1;5$.

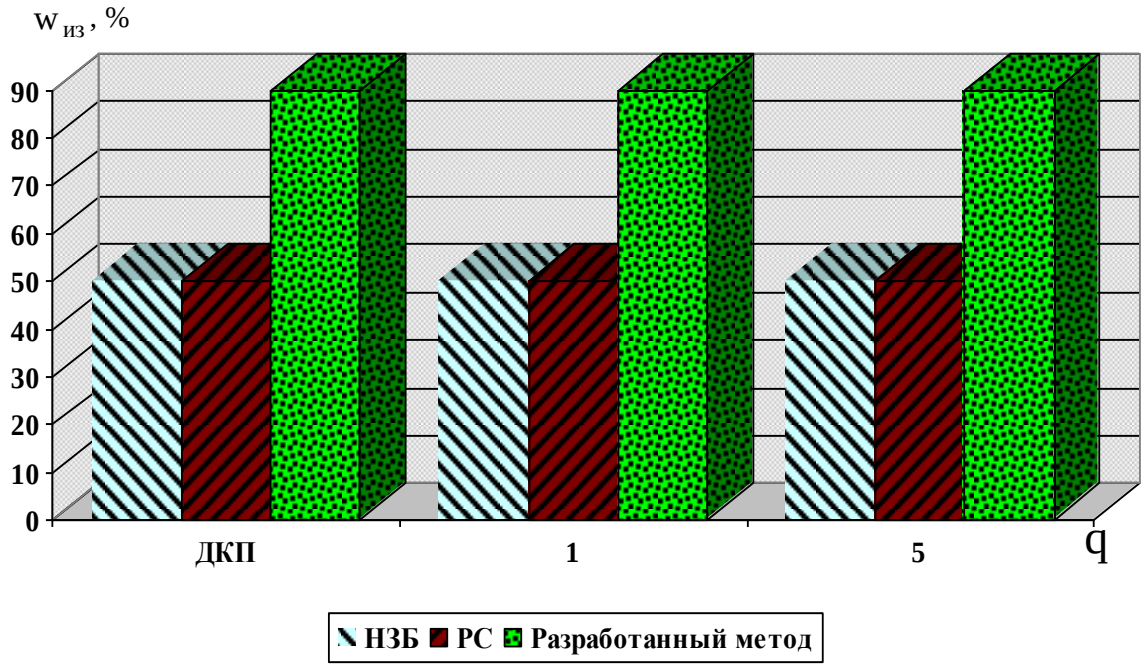

Рис. 4.17 Диаграмма значений величины $w_{из}^{(m)}$ для метода НЗБ, РС и разработанного метода в зависимости от типа атак

Из анализа рис. 4.17 можно сделать следующие выводы:

1) для различных коэффициентов квантования количество $w_{из}^{(m)}$ безошибочно изъятых бит для разработанного метода принимает значения 90 %;

2) в условиях применения активных атак выигрыш для разработанного метода относительно методов НЗБ и РС по количеству безошибочно изъятых данных составляет 40 %.

Выводы

1. Разработан метод оценки объема встраиваемых данных. Проведена оценка объема встраиваемых данных для разработанного метода с позиции относительной стеганографической емкости системы.

Проведен сравнительный анализ значений абсолютной и относительной стеганографической емкости разработанного метода относительно методов НЗБ и РС. При этом получены следующие результаты:

1) при одинаковых значения стеганографической емкости $w_{отн}^{(m)}$ выигрыш для разработанного метода относительно метода НЗБ по величине ПОСШ составляет в среднем от 8 до 32 дБ;

2) для разработанного метода выигрыш в значении стеганографической емкости относительно метода РС составляет от 1,22 до 5,47 %.

2. Разработан метод оценки характеристик скрытия встроенных сообщений. Для разработанного метода проведена оценка характеристик скрытия встроенных сообщений в случае неавторизированного доступа.

Величина ПОСШ для всех типов изображения принимает максимальное значение в случае встраивания в НПЧ длиной $m = 2$. При этом выигрыш в значении ПОСШ относительно встраивания в НПЧ с длиной $m = 3; 4; 6$ будет равен:

- для сильнонасыщенного изображения «Снимок аэропорта» от 2,725 дБ до 4,86 дБ;

- для средненасыщенного изображения «Фотоснимок» от 2,71 до 4,79 дБ;

- для слабонасыщенного изображения «Самолет на фоне неба» от 2,85 до 4,79дБ.

При одинаковых условиях стеганографического кодирования наибольшими искажениями обладают реалистичные яркие декодированные изображения средней насыщенности. Наоборот наименьшее количество искажений вносится при встраивании в слабонасыщенные затемненные изображения.

3. Разработан метод оценки эффективности изъятия встроенной информации при авторизированном доступе. Проведена оценка эффективности изъятия встроенной информации для разработанного метода при авторизированном доступе. Доказано, что вероятность безошибочного изъятия при авторизированном доступе принимает значение 1.

Проведен сравнительный анализ разработанного метода относительно методов НЗБ и РС по вероятности безошибочного изъятия встроенных данных. При этом выигрыш в значении вероятности безошибочного изъятия относительно методов НЗБ и РС составляет:

- для метода НЗБ - 40 % ;
- для метода РС - 50 %.

4. Проведена оценка устойчивости скрываемых сообщений к атакам злоумышленника. Для различных значений коэффициента квантования наибольшей устойчивостью обладают данные, стеганографически встроенные в НПЧ длиной $m = 6$. Наоборот наименьшей стойкостью обладают данные стеганографически встроенные в НПЧ длиной $m = 2$. Количества $w_{из}^{(m)}$ безошибочно изъятых бит в условиях применения противником атак для разработанного метода в среднем принимает значение 90 %. Выигрыш для разработанного метода относительно методов РС и НЗБ по количеству безошибочно изъятых данных составляет: относительно метода НЗБ- 40 %; относительно

метода РС – 40%.

ВЫВОДЫ

В диссертационной работе решена научно-прикладная задача, состоящая в повышении безопасности специальных информационных ресурсов в инфокоммуникационных системах. В диссертации разработан метод повышения безопасности специальных информационных ресурсов в критических системах на основе структурного стеганографического кодирования. Созданная технология стеганографического встраивания базируется на основе неравновесного позиционного кодирования числа с имплантированным двоичным элементом на старшую позицию неравновесного позиционного числа с последующей локализацией стеганографической избыточности.

Опыт функционирования критических систем в условиях активного противодействия противника обнаружил острую необходимость обеспечения необходимого уровня безопасности специальных информационных ресурсов. Такая необходимость с одной стороны диктуется повышенной значимостью СИР для информационной поддержки функционирования систем критического назначения, в том числе в условиях решения конфликтных ситуаций. С другой стороны повышаются угрозы нарушения конфиденциальности и целостности СИР, что обусловлено оперативно-программными и информационно-технологическими возможностями противника. Поэтому повышение безопасности специальных информационных ресурсов в инфокоммуникационных системах является актуальной ***научно-прикладной задачей***.

Вариантом обеспечения требуемого уровня информационной безопасности является направление, основанное на использовании технологий стеганографического встраивания информации в изображение-контейнер. В тоже время в процессе использования существующих технологий стеганографического встраивания для решения сформулированной научно-прикладной задачи выявил следующие проблемные недостатки:

- недостаточное значение относительной стеганографической емкости;

- недостаточное значение устойчивости встроенных данных к атакам противника;

- значительные визуальные искажения стеганограммы.

Наличие перечисленных недостатков обусловлено тем, что в процессе стеганографических преобразований в основном учитываются психовизуальные закономерности. Изъятие встроенной информации осуществляется с использованием корреляционных зависимостей, которые нарушаются в результате нелинейной обработки стеганограммы. Поэтому необходимо использовать для построения стеганографических систем механизмы выявления структурных закономерностей. Таким образом, тема научно-прикладных исследований, которая связана с разработкой метода повышения безопасности специальных информационных ресурсов в системах критического назначения на основе структурного стеганографического кодирования является актуальной.

В процессе проведения диссертационных исследований были разработаны следующие ***научно-прикладные результаты***:

1. Обосновано направление для разработки метода стеганографического встраивания. Данное направление базируется на преобразовании числа со встроенными данными на основе функционального преобразования. Определены требования к функционалу от числа со встроенными данными:

- должна обеспечиваться взаимооднозначность прямого и обратного функционального преобразования, т.е. должен существовать обратный функционал, позволяющий авторизированному пользователю получить скрываемое сообщение без потери информации;

- обратное функциональное преобразование должно осуществляться по биполярному принципу. Биполярность заключается в существовании для функционала двух вариантов обратного преобразования: для авторизированного пользователя и для злоумышленника. Для неавторизированно пользователя восстановление изображения происходит при стандартных условиях,

при котором блокируется возможность изъятия встроенного сообщения. Для авторизированного пользователя обратное преобразование реализуется при наличии ключа, и при этом возможно безошибочное изъятие встроенных данных;

- функциональное преобразование должно быть инвариантным к атакующим воздействиям. Другими словами, должно обеспечиваться достоверное изъятие встроенного сообщения после подвергания стеганограммы атакам, сжатию и при наличии ошибок в канале связи.

2. Сформулирована система свойств для функционального преобразования. Для соответствия требованиям визуальной устойчивости к трансформированию и атакам, синтезируемый функционал должен обладать следующими свойствами:

- формирование стеганограммы с использованием функционала должно осуществляться по интегральному принципу в два этапа. На первом этапе применения функционала к числу с встраиванием формируется кодовое значение, содержащее информацию об элементах исходного числа. На втором этапе на основе кодового значения строится результирующее кодовое представление стеганограммы;

- количественная метрика, указывающая на степень отличия между элементами ИК полученными при обратном преобразовании в случае для авторизированного пользователя и элементами, реконструированными при неавторизированном доступе, не должна превышать порога визуальной незначимости;

- стеганограмма, полученная вследствие функционального преобразования, должна содержать сведения о векторе служебной информации, при наличии которой возможно реконструкция элементов изображения контейнера;

- извлечение встроенного бита скрываемого сообщения злоумышленником (неавторизированный пользователь) возможно только при известном ключе, даже при наличии у него информации о встраивании данных;

- реконструкция исходного изображения для неавторизированного пользователя реализовалась только при наличии у него полных сведений о векторе служебных данных.

3. Обоснован подход на основе неравновесного позиционного кодирования, где в качестве элемента-контейнера предлагается использовать неравновесное позиционное число, а в качестве функционального преобразования используется кодообразующая функция для неравновесного позиционного числа. При таком подходе предусматривается встраивание бита секретного сообщения в исходное неравновесное позиционное число. В результате применения прямого функционального преобразования для исходного числа со встроенной информацией формируется результирующие кодовое представление. Обратное функциональное преобразование будет осуществляться для злоумышленника (не авторизированный доступ) и для авторизированного пользователя. При первом способе реконструкция элемента исходного изображения реализуется неавторизированным пользователем с учетом открытой служебной информации. Второй способ позволяет, при наличии служебной информации и закрытого ключа, изъять бит встроенных данных и безошибочно реконструировать исходный элемент изображения-контейнера.

4. Разработана стеганографическая система на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающая встраивание и изъятие скрываемой информации на основе соответственно структурного стеганографического кодирования и декодирования.

5. Разработано структурное стеганографическое кодирование с маскированием, базирующееся на следующих этапах:

- формирование неравновесного позиционного базиса для фрагмента изображения;

- структурное стеганографическое кодирование в неравновесном базисе оснований;

- маскирование структурной стеганографической избыточности путем ее локализации на основе коррекции длины стеганограммы.

6. ***Создано правило*** встраивания информации для структурного стеганографического кодирования, заключающееся в том, что:

1) один бит скрываемого сообщения встраивается на старшую позицию неравновесного позиционного числа;

2) локализация стеганографической избыточности достигается на основе отсечения младшего бита стеганограммы.

На основе правила построено маскирующее стеганографическое кодирование для встраивания одного бита на старшую позицию неравновесного позиционного числа. Это обеспечивает встраивание скрываемой информации в условиях:

1) повышения устойчивости скрываемой информации;

2) обеспечение восстановления элементов исходной видеопоследовательности независимо от наличия встроенной информации;

3) снижения количество структурной стеганографической избыточности.

7. Разработано демаскирующее стеганографическое декодирование для извлечения имплантированного на старшую позицию бита с одновременной реконструкцией элементов исходного неравновесного позиционного числа. Механизм демаскирующего стеганографического декодирования предусматривает:

1) восстановление исходной длины для скорректированного в процессе маскирования стеганокода;

2) структурное стеганографическое декодирование, обеспечивающее восстановление неравновесного позиционного числа с имплантированным элементом;

3) изъятие элемента скрываемого сообщения со старшей позиции неравновесного позиционного числа.

Основные практические результаты.

Разработан метод повышение безопасности специальных информационных ресурсов в системах критического назначения на основе структурного стеганографического кодирования, доведенный до программно – аппаратных реализаций. На основе чего получены такие результаты:

1. Проведенный сравнительный анализ значений относительной стеганографической емкости разработанного метода относительно методов НЗБ и РС показал, что:

1) при одинаковых значения стеганографической емкости $w_{отн}^{(m)}$ выигрыш для разработанного метода относительно метода НЗБ по величине ПОСШ составляет в среднем от 8 до 32 дБ.

2) для разработанного метода выигрыш в значении стеганографической емкости относительно метода РС составляет от 1,22 до 5,47 %.

2. Оценка характеристик скрытия встроенных сообщений в случае неавторизированного доступа позволяет заключить, что величина ПОСШ для всех типов изображения принимает максимальное значение в случае встраивания в НПЧ длиной $m = 2$. При этом выигрыш в значении ПОСШ относительно встраивания в НПЧ с длиной $m = 2; 3; 4; 6$ будет равен:

- для сильнонасыщенного изображения «Снимок аэропорта» от 2,725 дБ до 4,86 дБ;

- для средненасыщенного изображения «Фотоснимок» от 2,71 до 4,79 дБ;

- для слабонасыщенного изображения «Самолет на фоне неба» от 2,85 до 4,79дБ.

3. Проведеный сравнительный анализ разработанного метода относительно методов НЗБ и РС по вероятности безошибочного изъятия встроенных данных показал, что выигрыш в значении вероятности безошибочного изъятия относительно методов НЗБ и РС составляет:

- для метода НЗБ - 40 % ;

- для метода РС - 50 %.

4. Оценка устойчивости скрываемых сообщений к атакам злоумышленника позволяет заключить, что для различных значений коэффициента квантования наибольшей устойчивостью обладают данные, стеганографически встроенные в НПЧ длиной $m = 6$. Наоборот наименьшей стойкостью обладают данные стеганографически встроенные в НПЧ длиной $m = 2$. При этом выигрыш для разработанного метода относительно методов РС и НЗБ по количеству безошибочно изъятых данных составляет:

- относительно метода НЗБ- 40 %;
- относительно метода РС – 40%.

Полученные научные результаты являются вкладом в развитие теории информационной безопасности относительно обеспечения безопасности специальных информационных ресурсов в критических системах.

Научные и практические результаты диссертации использовались при выполнении исследовательских и конструкторских работ в Научно-техническом специальном конструкторском бюро «ПОЛИСВИТ» (акт реализации от 23.03.2014 г.) и в Государственном научно-исследовательском институте МВД Украины (акт реализации от 23.01.2015 г.).

Обоснованность и достоверность полученных научных результатов базируются на: всестороннем анализе недостатков существующих технологий стеганографического встраивания в изображение-контейнер; корректном использовании методов неравновесного позиционного кодирования.

Достоверность результатов относительно показателей эффективности функционирования разработанного стеганографического метода подтверждается адекватностью результатов, полученных на основе аналитических выражений, с результатами, полученными в ходе натурного эксперимента с реальными видовыми изображениями.

Результаты диссертационной работы целесообразно использовать:

- при обеспечении информационной безопасности специальных информационных ресурсов в информационно-телекоммуникационных системах;

- при создании скрытых каналов передачи указаний и распоряжений в системах видеоконференцсвязи ведомственных организаций;

- при изучении учебных дисциплин по информационной безопасности, теории стеганографического кодирования и цифровой обработке изображений для подготовки специалистов в ВУЗах Украины.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Абламейко С.В., Лагуновский Д.М. Обработка изображений: технология, методы, применение. - Минск: Амалфея, 2000. – 303 с.

2. Аграновски А.В. Стеганография, цифровые водяные знаки и стегоанализ [Тест]: учеб. пособие для вузов / А.В. Аграновски, А.В. Балакин, В.Г. Грибунин. – М.:Вузовская книга, 2009. – 220 с.

3. Алфёров А. П. Основы криптографии: учебное пособие / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

4. Андреев А. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 7. – С.19 – 25.

5. Андреев А.. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 8. – С.16 – 22.

6. Анин Б. Защита компьютерной информации / Б.Анин. - СПб.: БХВ-Петербург, 2000. - 384 с.

7. Артехин Б.В. Стеганография / Артехин Б.В. // Журнал «Защита информации. Конфидент». – 1996. - № 4 -

8. Бабенко В. Г. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення / В.Г. Бабенко, С.В. Рудницький // Системи обробки інформації : зб. наук. праць. – № 9 (107). – Х. : ХУПС ім. І. Кожедуба, 2012. – С. 163–168.

9. Бабенко В.Г. Метод вбудовування стегоповідомлення на основі ключового елементу / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 37 - 44.

10. Баранник В.В. Структурно-комбинаторное представление данных в автоматизированных система управления / В.В. Баранник, Ю.В. Стасев, Н.А. Королева - Х.: ХУПС, 2009. – 252 с.

11. Баранник В.В. Кодирование трансформированных изображений в инфокоммуникационных системах / В.В. Баранник, В.П. Поляков - Х.:

ХУПС, 2010. – 234 с.

12. Баранник В.В. Кодирование трехмерных моделей видеокадров в инфотелекоммуникационных системах / В.В. Баранник, В.П. Поляков, А.В. Слободянюк // Каменец-Подольский-Харьков: Вид-во Каліграф, 2011. – 210 с.

13. Баранник В.В. Метод формування функціонала стеганографічного кодування стійкого до стегано-атак / В.В. Бараннік, А.Е. Бекіров // АСУ та прилади автоматики. - 2013. - Вип.165. - С. 34 – 43.

14. Баранник В.В. Методологическая база управления битовой скоростью при формировании предсказанных кадров / В.В. Баранник, Н.А. Харченко, А.Э. Бекиров // Радіоелектроніка та інформатика. - 2013. - №3. - С. 12 – 17.

15. Баранник В.В. Метод функционального преобразования чисел со встроенной информацией для стеганосистем / В.В. Баранник, А.Э. Бекиров, А.В. Хаханова // Радіоелектроніка та інформатика. - 2013. - №4. С. 69 – 73.

16. Баранник В.В. Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов, С.А. Сидченко, А.Э. Бекиров // Информационно-управляющие системы на ЖД транспорте. – 2014. - №3. - С. 24 – 31.

17. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Е. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.

18. Баранник В.В. Технология неравновесного позиционного кодирования для функционального преобразования чисел со встроенной информаций / В.В. Баранник, Ю.Н. Рябуха, А.Э. Бекиров // Радиоэлектронные и компьютерные системы. – 2014. - №4. - С. 32 - 39.

19. Баранник В.В. Стеганографическая система на основе неравновесного позиционного кодирования / В.В. Баранник, А.Э. Бекиров, Д.В. Баранник // Радіоелектроніка та інформатика. - 2014. - №4. - С. 00 – 00.

20. Бараннік В.В. Технологія кодування кортежів трансформованих зображень в інфокомунікаційних системах / В.В. Бараннік, С.В. Туренко, В.В. Твердохлеб, А.Е. Бекіров // IV Міжнародна науково-практична конференція [″International Scientific Conference, «ITSEC»″], (Київ, 20 - 23 травня 2014 р.) / Національний авіаційний університет, Київ, 2014. – С. 59.

21. Баранник В.В. Метод повышения безопасности видеоинформационного ресурса / В.В. Баранник, Ю.Н. Рябуха, А.Е. Бекиров // Третя міжнародна науково-технічна конференція ″Проблеми інформатизації″, (Киев, 11 - 13 грудня 2014 г.) / Державний університет телекомунікацій, Київ, 2014. – С. 9.

22. Баранник В.В. Анализ действий кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях / В.В. Баранник, Ю.Н. Рябуха, С.А. Подлесный, А.Э. Бекиров // Науково-технічна конференція ["Інформаційна безпека України″] / Київський національний університет імені Тараса Шевченка, 12-13 березня 2015 р. - С. 34.

23. Барсуков В.С. Компьютерная стеганография: вчера, сегодня, завтра. / Барсуков В.С., Романцов А.И. Технологии информационной безопасности XXI века. – материалы Internet-ресурса «Специальная техника» (http://st. ess.ru/).

24. Барсуков В.С. Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники. – 2000. - №2. – С.31-40.

25. Бекиров А.Э. Пути повышения безопасности информационных ресурсов в системах специального назначения / А.Э. Бекиров, К.Ю. Трифоненко // Наука і техніка Повітряних Сил України. - 2014. - №2(15). – С. 139-143.

26. Бекиров А.Э. Метод оценки вычислительной сложности обработки изображений с выявлением значимых компонент трансформант / В.Н. Кривонос, А.Э. Бекиров // Сучасна спеціальна техніка. – 2014. - №3. – С. 22 – 29.

27. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем // Озброєння та військова техніка. – 2015. - №1 - С. 29 – 36.

28. Бекіров А.Е. Спосіб компресії зображень в інфокомунікаціях на основі кодування кортежів / А.Е. Бекіров, В.В. Бараннік, С.В. Туренко, Д.І. Комолов // VI Международной научно-практической конференции [″Проблеми і перспективи розвитку ІТ-індустрії ″], (Харьков, 17 - 18 апреля 2014 р.) / Харьковский национальный экономический университет, Харьков, 2014. – С. 233.

29. Бекиров А.Э. Пути повышения информационной безопасности ресурсов в системах специального назначения / В.В. Баранник, Ю.Н. Рябуха, А.Е. Бекиров, Д.И. Комолов // Четверта міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Вінниця, 28 - 30 травня 2014 р.) / Вінницький національний технічний університет, Вінниця, 2014. – С. 151.

30. Бекиров А.Э. Способ обработки потока кадров с предсказанием для систем телекоммуникаций / А.Э. Бекиров, Н.А. Харченко, Д.И. Комолов // Науково-методична конференція ["Сучасні проблеми телекомунікації і підготовка фахівців в галузі телекомунікацій - 2014″] / Національний університет "Львівська політехніка", - 1-4 листопада 2014р. - С. - 117-118.

31. Біла книга - 2013. Збройні Сили України. - К. : Військо України, 2014. – 76 с.

32. Білинський Й.Й. Методи обробки зображень в комп'ютеризованих оптико-електронних системах. Вінниця: ВНТУ, 2010. - 272 с.

33. Бобок И.И. Метод детектирования стеганосообщения, сформированного посредством модификации наименьшего значащего бита / И.И. Бобок, А.А. Кобозева // Інформаційна безпека. – 2001.-С.56-63.

34. Богуш В.М. Інформаційна безпека держави /В.М. Богуш, О.К. Юдин. – К.: МК–Прес, 2005. – 432 с.

35. Бурячок В.Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В.Л. Бурячок, Г.М. Гулак, В.О. Хорошко // Наука і оборона. -

2011. - № 3. - С. 35-42.

36. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.

37. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин – М.: ДИАЛОГ – МИФИ, 2003. – 384с.

38. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений/ А.В. Галицкий. – М.: ДМК Пресс, 2005. –616 с.

39. Генне О.В. Основные положення стеганографии / Генне О.В.// «Защита информации. Кофидент» - 2000 - №3. с 45.

40. Голубєв В.О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжний. - Запоріжжя : Просвіта, 2001. - 252 с.

41. Голубєв В.О. Проблемні питання протидії кіберзлочинам у системі інформаційної безпеки держави / В. О. Голубєв // Вісник Запорізького юридичного інституту. 1999 р. №4(9). - 1999. - С. 286-300

42. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1073 с.

43. Горбулін В.П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В.П. Горбулін, М.М. Биченок, П.М. Копка // Матер.міжнар. наук.-практ. конф. “Форми та методи забезпечення інформаційної безпеки держави”. – К.: Національна академія СБ України, 2008.– С. 79 – 85.

44. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Окон И.Н., Туринцев И.В – СП.б.: Солон-Пресс, 2002.- 272 с.

45. Гургенидзе А.Т., Корше В.И. Мультисервисные сети и услуги широкополосного доступа. – СПб., 2003. – 434 с.

46. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах / М.А. Дрюченко // Вест. Воронеж. гос. ун. Системный анализ и информационные технологии. – 2007. -№1. – С.21-30.

47. Жилкин М.Ю. Стегоанализ графических данных в различных форматах / М.Ю. Жилкин // Доклады ТУСУРа, №2 (18), часть 1, 2008. – С.63-64.

48. Задирака В.К.Статистический анализ систем с цифровыми водяными знаками / В.К. Задирака, Н.В. Кошкина, Л.Л. Никитенко // Штучный інтелект.-2008. - №3. – С.315-324.

49. Задирака В.К. Новые подходы к разработке алгоритмов скрытия информации / В.К. Задирака, Л.Л. Никитенко // Штучный інтелект.-2008. - №4. – С.353-357.

50. Ільяшов О.А. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу / О.А. Ільяшов, В.Л. Бурячок // Наука и оборона. – 2010. – №4. – С.35 – 41.

51. Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К.: ДУКІТ, 2010. – 316 с.

52. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах / А.А. Кобозева // Вісник Східноукраїнського національного університету ім. В.Даля. – 2006. - №9 (103), ч. 1. – С.74-83.

53. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчик, С.М. Паук, В.Г. Потапов. – К.: МК – Пресс, 2005. – 288 с.

54. Конахович Г.Ф Оценка эффективности методов стеганографического встраивания информации в спектральную область изображений / Г.Ф. Конахович // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 23 - 29.

55. Концепція національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 № 3/97-ВР// ВВР. – 1997. – №10. – С.85.

56. Концепция реформирования и развития Вооруженных Сил Украины на период до 2017 года. / Рішення Ради національної безпеки і оборони України від 29 грудня 2012 року.

57. Комплексна програма розвитку і реформування Збройних Сил України на період до 2017 року. / Затверджена указом Президента України від 02.09.2013 №479/2013.

58. Королев В.Ю. Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В.Ю. Королев, В.В. Полиновский, В.А, Герасименко // Управляющие системы и машины. – 2011. - №4. – С.187-196.

59. Корольов В.Ю. RS-стеганоаналіз. Принципи роботи, недоліки та концепція методу його обходу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко // Вісник Вінницького політехнічного інституту. – 2010. - №6. – С.66-71.

60. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г Корченко, Є.В. Васілу, С.О. Гнатюк // Науково-технічний журнал «Захист інформації». – 2010, №1. – С.77-89.

61. Крук Б.И. Телекоммуникационные системы и сети. Том 1, 2, 3 / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов. - М.: Горячая линия-Телеком, 2003. – 647 с.

62. Кущ А.В. Использование алгоритмов стеганографии при проведении компьютерно-технической экспертизы / А.В. Кущ // VI Всероссийская межвузовсткая конференция молодых ученных – Спб. СПбГУ ИТМО, 2009.

63. Лидовский В.В. Теория информации / В.В. Лидовский. – М.: Компания Спутник+, 2004. – 111 с.

64. Михайличенко О.В. Применение стеганографических методов сокрытия информации в неподвижных изображениях / О.В. Михайличенко, А.Г. Коробейникова, С.Ю. Каменева // Труды международных научно-технических конференций «Интеллектуальные системы (IEEE AIS’06) и «Интеллектуальные САПР (CAD-2006)»: в 3 т. М.: Физмалит, 2006. Т.2. – С.511-515.

65. Михайличенко О.В. Повышение устойчивости стеганоалгоритмов частотной области на основе дискретного косинусного преобразования к внешним воздействиям / О.В. Михайличенко, Н.Н. Прохожев, А.Г. Коробейников // Научно-технический вестник СПб ГУ ИТМО – СПб.: СПб ИТМО, 2009. – вип. 2(60). – С.102-104.

66. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999р., №22.

67. Паламарчук С.А. Стеганографічні методи приховування інформації

в зображеннях / С.А. Паламарчук, І.В. Бабич // Бизнес и и безопасность. – К.: 2011. – Вип.3. – С.35-37.

68. Поляков П.Ф. Метод восстановления изображений с контролируемой погрешностью / П.Ф. Поляков, В.В. Баранник, А.В. Яковенко // Системи управління, навігації та зв'язку. – ЦНДІ НіЗ. – 2008. – № 4. – С. 44 – 47.

69. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

70. Пузыренко А.Ю. Оценка качества реализации стеганографических алгоритмов // В.П. Бабак, Г.Ф. Конахович, А.Ю. Пузыренко // Безопасность информации в ИТКС-2006: XI міжнар. наук.-практ. конф., 17-19 травня 2006 р.: тези доп.-К.: - НИЦ – Тезис, 2006.- С.18.

71. Пузиренко О.Ю. Представлення і прогнозування ефективності нового протоколу оцінки якості реалізації розроблюваних алгоритмів комп'ютерної стеганографії / О.Ю. ПУзиренко, Д.О. Навроцький, Л.П. Дюжаєв // Радіотехніка. Радіоапаратобудування: Зб. наук. пр. – Вип. 34. – К.: НТУУ «КПІ», 2007. – С.150-156.

72. Садов В.С. Обнаружение стеганографического канала передачи данных путем анализа однобитного шума изображения / В.С. Садов, И.Л. Чваркова // Известия Белорусской инженерной академии, №1 (19)/2, 2005, с. 75-78.

73. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2006. – 958 с.

74. Рудницький В.М. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Зб. наук. пр. Харківського університету Повітряних Сил. – Харків: ХУПС. – 2011. – Вип. 3(29). – С. 145-150.

75. Соколов А.Ю. Методы формирования параметров пространственного движения объекта на основе обработки визуальной информации / А.Ю. Соколов, Ватик М.Хуссейн // Радіелектроні і комп'ютерні системи, 2009. - №3 (37). - с.104 -

107.

76. Стасюк О.І. Сучасні стеганографічні методи захисту інформації / Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. // Захист інформації. – 2011. - №1(50). – С.56-63.

77. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М: Техносфера, 2004. – 368 с.

78. Тропченко А.Ю. Методы сжатия изображений, аудиосигналов и видео / А.Ю. Тропченко, А.А. Тропченко // Учебное пособие – СПб: СПбГУ ИТМО, 2009. – 108 с.

79. Фисенко В.Т. Компьютерная обработка и распознавание изображений: учебн. пособие / В.Т. Фисенко, Т.Ю. Фисенко. – СПб.: СПбГУ ИТМО, 2008. – 192 с.

80. Хорошко В.А. Методі и средства защиты ифнормации. / Хорошко В.А., Чекатов А.А. –К.: Юниор, 2003. – 501с.

81. Хоршко В.А. Введение в компьютерную стеганографию /Хорошко В.А., Шелест М.Е., Яремчук Ю.Е. – Вінниця: ВДТУ, 2003. – 143 с.

82. Хорошко В.О. Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов / Азаров О.Д., Шелест М.Э - Винница: ВДТУ, 2003.-143 с.

83. Хорошко В.О. Термінологічний довідник з питань технічного захисту інформації. / Хорошко В.О., Огарков І.М., Чирков Д.В., Голего А.Г., Горохова Т.Б.// За ред. проф. Хорошко В.О. 3 вид., доп. і перероб. – К.: ТОВ «ПоліграфКонсалтинг» - 2003.-286 с.

84. Цифровая обработка изображений в информационных системах / И.С. Грузман, В.С. Киричук и др. – Новосибирск: Изд-во НГТУ, 2002. – 352 с.

85. Шеннон К. Работы по теории информации и кибернетики. – М.: Изд – во иностр. лит – ры, 1963. – 793 с.

86. Юдін О.К. Захист інформації в мережах передачі даних: підручник / Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с.

87. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпе-

чення: підручник / О.К. Юдін. – К. : НАУ, 2011. – 640с.

88. Юдін О.К. Концептуальний аналіз уразливості державних інформаційних ресурсів / О.К.Юдін, С.С.Бучик // Наукоємні технології. – 2013. - № 3 (19). – С. 299 – 304.

89. Barannik V.V. Design of steganographic system on the basis of a code container in nonequilibrium positional base / V.V. Barannik, A.E. Bekirov, A.V. Hahanova // Radioelectronics & informatics. – 2013. - №1. - С. 49 – 53.

90. Barannik V. The Positional Structural-Weight Coding of the Binary View of Transformants / Barannik V., Hahanova A. // International Symposium [″IEEE East-West Design & Test″], (Kharkov, Ukraine, September 18-21, 2012) / Kharkov: 2012. – P. 490 – 494.

91. Vladimir Barannik. Quality indicators for steganographic transformations of images / Vladimir Barannik, Ali Bekirov, Konstantin Tryfonenko // XIIth International Conference [“Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET’2014”], (Lviv-Slavske, Ukraine, February 25 – March 1, 2014) / Lviv-Slavske: 2014. – P. 533.

92. Barannik V. Functional transformation for direct embedding steganographic methods / Bladimir Barannik, Ali Bekirov, Roman Tarnopolov // International Symposium «IEEE East-West Design & Test», (Kiev, Ukraine, September 26–29, 2014).

93. Barannik V. Design of steganographic system on the basis of a code container in nonequilibrium positional base / V. Barannik, A. Bekirov, S. Sidchenko, V. Larin // The XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics CADSM’2015 (24-27 February 2015 Polyana-Svalyava (Zakarpattya), Ukraine).

94. Bohme R. Advanced Statistical Stegoanalysis. – Berlin: Springer-Verlag, 2010. – 300 p.

95. Chae J.J. Robust Techniques for Data Hiding in Image and Video. PhD Thesis // Department for Electrical and Computing Engineering, University of California, Santa Barbara, CA, USA, 1999.

96. Chen B. An Information-Theoretical Approach to the Design of Robust Digital Watermarking Systems / B. Chen, G.W. Wornell // Procceding Int.

Conf. on Acoustics, Speech and Signal Processing. 1999.

97. Cox I.J. Digital watermarking and steganography. / I.J Cox, M.L. Bloom, J.A. Fridrick, amd T. Kalkert. // USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

98. Cox I.J., Miller M.L., McKellips A.L. Watermarking as Communication with Side Information // Proceeding IEEE, Special Issue on Identification and Protection of Multimedia Information. 1999. Vol. 87. №. 7. P. 1127-1141.

99. Fortrini M Steganography and digital watermarking: A global view / M. Fortrini // University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progretti00/fortini/project.pdf [June 2011].

100. Fridrich J. Stegoanalysis of LSB encoding in color image / J. Fridrich, R. Du, M. Long // ICME, 2000.

101. Fridrich J. New blind steganalysis and its implication / J. Fridrich, G. Miroslav // Proc. SPIE Elec-tronic Imaging, 2006.

102. Granrath D.J. The role of human visual models in image processing, // Proceedings of the IEEE, Vol. 67, 1981. - pp. 552-561.

103. Gonzales R.C. Digital image processing / R.C. Gonzales, R.E. Woods. - Prentice Inc. Upper Saddle River, New Jersey 2002. – 779 p.

104. Hui T. An M-Sequence Based Steganography Model for Voice over IP / T. Hui, et al. // Communications, 2009. ICC'09. IEEE International Cinference on 2009.

105. Husrev T. Sencar Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia / Husrev T. Sencar, Mahalinggam Pamkumar // ELSEIVER science and technology books, 2004. 364 p.

106. Kutter M. Digital Image Watermarking: Hiding Information in Images. PhD, Thesis. // Swiss Federal Institute ofTechnology, Lausanne, Switzerland, 1999.

107. Lin C. Watermarking and digital Signature Techniques for Multimedia Authentication and Copyright Proytction // PhD Thesis, Columbia University, 2000.

108. Marvel L. Image Steganography for Hidden Communication. PhD

Thesis. University of Delavare, 1999. 115p.

109. Medeni M.B. A novel Steganographic Protocol from Error-correcting Codes / M.B. Medeni, El.M Soudi // Journal of Information Hiding and Multimedia Signal Processing. – 2010. –P.339-343.

110. Petitcolas F. Attacks on Copyright Marking Systems / F. Petricolas., R. Anderson, M. Kuhn // Lecture notes in Computer Science. 1998. P. 218-238.

111. Provos N/ Hide and Seek: An Introduction to Steganography / N. Provos, P. Honeyman // The IEEE Computer Security, 2003.

112. Petrou M. Image Processing The Fundamentals, John Wiley & Sons, Inc. – 1999. – 355 p.

113. Ramkumar M. Data Hiding in Multimedia. PhD Thesis // New Jersey Institute of Technology, 1999, 68 p.

114. Rybko B. Information-Theoretical Approach to Steganographic Systems / B. Rybko, D. Ryabko // Proc. IEEE International Symposium on Information Theory, Nice, France, 2007. P.2461-2464.

115. S. P. Mohanty A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management // Elsevier Journal of Systems Architecture (JSA) – October-December 2009 – Volume 55, Issues 10-12. – P. 468-480.

116. Smith J. Modulation and Information hiding in Image / J. Smith, B. Comiskey // Information hiding: First Int. Workshop “InfoHidding’96”, Springer as Lecture Notes Computing Science, vol 1174. 1996. – pp.207-227.

117. Wang Z., Bovik A.C., Sheikh H.R. Image quality assessment: From error visibility to structural similarity. / Z. Wang, A.C. Bovik, H.R. Sheikh // IEEE Transaction on Image Processing. – 2004. – Vol. 13, 4,. pp. 309-312.

118. Wang X., Zhang X.P. Generalized trellis coded quantization for data hiding // In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) – Honolulu, Hawaii, USA, April 2007 – vol. 2 – P. 269-272.

119. Wallace G.K. The JPEG Still Picture Compression Standard // Communication in ACM. – 1991. – V34 – №4. – P.31 – 34.

120. Fridrich J. Steganalysis of LSB encoding of Color Images / Fridrich J., Du R., Long M. // Proccedings of ICME 2000, New York City, July 31 – August 2, New York, USA.

ПРИЛОЖЕНИЕ А

Примеры исходных реалистичных изображений

Рис. А1. Исходное изображение-контейнер «Снимок аэропорта»

Рис. А2. Исходное изображение-контейнер «Фотоснимок»

Рис. А3. Исходное изображение-контейнер «Самолет на фоне неба»

ПРИЛОЖЕНИЕ Б

Элементы программной реализации разработанного метода стеганографического кодирования с маскирование стеганографической избыточности

```
script
clear;                          %очистка ВСЕХ параметров
FileName= '41.bmp';             %имя файла изображения-контейнера
FileDate        = 'r.txt';      %имя текстового файла для стеганографического встраивания
FileDate2       = 'r2.txt';     %имя выходного файла после демаскирования
NPlosk          = 1;            %номер обрабатываемой плоскости
MStR            = 3;            %размерность матрицы кодирования   - строк
MStB            = 3;            %                                  - столбцов
MStR_DCP        = 8;            %размерность матрицы для ДКП       - строк
MStB_DCP        = 8;            %                                  - столбцов
DiscreteTransform = 0;          %Двумерное дискретное косинусное преобразование
                                %1 - Да
                                %0 - Нет
KvantTransform    = 0;          %квантование
                                %1 - Да
                                %0 - Нет
qv1             = 5;            %коэффициент квантования
SaveFig         = 1;            %Запись - плоскости в файл 'fig2.bmp'
                                %  восстановленного изображения в файл 'fig3.bmp'


%-------------------------------------------------------------------------------------------------------

%Считать файл данных для встраивания
fid = fopen(FileDate, 'r');
[MDate,count] = fread(fid,inf,'ubit1');
fclose(fid);
NDate = 0;

%Считать исходное изображение
ISHM=imread(FileName);
NFig=1,figure(NFig),imshow(ISHM);       %Отобразить рисунок

%Информация про файл
INFO=imfinfo(FileName);

%-----------Обработка всех 3-х плоскостей
%for NPlosk=1:3

%Обработка плоскости NPlosk
P1=ISHM(:,:,NPlosk);
NFig=NFig+1,figure(NFig),imshow(P1);     %Отобразить рисунок

%Запись плоскости в файл
if SaveFig == 1
   imwrite(P1,'fig2.bmp');
end
```

```
%-------------------------------------------------------------------------

P1=double(P1)+1;                    %переход в формат двойной точности

if or(Type_M_Transform == 0,M_Transform == 0)
   Rmin=0;
end;

%-------------------------------------------------------------------------

%м-кодирование
if M_Transform == 1

if Type_M_Transform == 0

   for i=1:fix(INFO.Width/MStB)
   for j=1:fix(INFO.Height/MStR)

      %Выбираем массив
      A1=P1(MStR*(j-1)+1:MStR*(j-1)+MStR,MStB*(i-1)+1:MStB*(i-1)+MStB);

      %Определение максимального элемента в строках матрицы (основание)
      for StR=1:MStR
         Mmax(StR)=max(A1(StR,1:MStB))+1;
      end

      %Сохранение максимумов - Переводим в столбец
      for StR=1:MStR                %по строкам
         R(MStR*(j-1)+StR,i)=Mmax(StR);
      end

      %Рассчет V(i)
      V(MStR+1,1)=1;
      for StR=1:MStR
         V(MStR+1-StR,1)=V(MStR+1-StR+1,1)*R(MStR*j-StR+1,i);
      end

      %обнуление
      for StB=1:MStB                %по столбцам
         N(StB)=0;
      end

      %Рассчет N(j)=sum(A(ij)V(i)) - кодирование изображения,
      %где V(i)-вектор-произведение максимальных значений
      for StB=1:MStB                %по столбцам
         for StR=1:MStR             %по строкам
            N(StB)=N(StB)+A1(StR,StB)*V(StR+1,1);
         end
         NDate = NDate +1;
         if MDate(NDate,1) == 1
           N(StB)=N(StB)+V(1,1);        %прибавить вес от дополнительной 1
```

```
                                %если добавляется 0 бит (не 1),
                                %то операция не выполняется
            end
            N(StB)=fix(N(StB)/2);          %отбросил последний бит
        end

        %Переводим трансформанту в столбец
        for StB=1:MStB                  %по строкам
            N1(MStB*(j-1)+StB,i)=N(StB);
        end

    end         %for j=1:fix(INFO.Height/MStR)
    end         %for i=1:fix(INFO.Width/MStB)

else

    for i=1:fix(INFO.Width/MStB)
    for j=1:fix(INFO.Height/MStR)

        %Выбираем массив
        A1=P1(MStR*(j-1)+1:MStR*(j-1)+MStR,MStB*(i-1)+1:MStB*(i-1)+MStB);

        %Определение максимального элемента в строках матрицы
        for StR=1:MStR
            Mmax(StR)=max(A1(StR,1:MStB))+1;
            Mmin(StR)=min(A1(StR,1:MStB));
        end

        %Сохранение максимумов - Переводим в столбец
        for StR=1:MStR                  %по строкам
            R(MStR*(j-1)+StR,i)=Mmax(StR);
            Rmin(MStR*(j-1)+StR,i)=Mmin(StR);
        end

        %Рассчет V(i)
        V(MStR,1)=1;
        for StR=1:(MStR-1)
            V(MStR-StR,1)=V(MStR-StR+1,1)*(R(MStR*j-StR+1,i)-Rmin(MStR*j-StR+1,i));
        end

        %обнуление
        for StB=1:MStB                  %по столбцам
            N(StB)=0;
        end

        %Рассчет N(j)=sum(A(ij)V(i)) - кодирование изображения,
        %где V(i)-вектор-произведение максимальных значений
        for StB=1:MStB                  %по столбцам
            for StR=1:MStR              %по строкам
                N(StB)=N(StB)+(A1(StR,StB)-Rmin(MStR*(j-1)+StR,i))*V(StR,1);
            end
        end
```

```
      %Переводим трансформанту в столбец
      for StB=1:MStB                %по строкам
         N1(MStB*(j-1)+StB,i)=N(StB);
      end

   end          %for j=1:fix(INFO.Height/MStR)
   end          %for i=1:fix(INFO.Width/MStB)
end

else
   N1=P1;
   MStB=1;
   MStR=1;
   R=0;
end


%временно сохранить кодовые комбинации до ДКП
NTemp = N1;


%-------------------------------------------------------------------------

   %Сохранение - Очистка - Восстановление ВСЕХ параметров
   %(Передача изображения)

   %восстановление плоскости после обработки
   for i=fix(fix(INFO.Width/MStB)/MStB_DCP)*MStB_DCP+1:fix(INFO.Width/MStB)
   for j=1:fix(INFO.Height/MStR)*MStR
      N1(j,i)=DCP(j,i);
   end
   end
   for i=1:fix(INFO.Width/MStB)
   for
j=fix(fix(INFO.Height/MStR)*MStR/MStR_DCP)*MStR_DCP+1:fix(INFO.Height/MStR)*MS
tR
      N1(j,i)=DCP(j,i);
   end
   end

else
%-------------------------------------------------------------------------

%Восстановление изображения
%м-кодирование
if M_Transform == 1

if Type_M_Transform == 0

   Q1bmp = 0;
   Q0bmp = 0;
```

```
   MDate = zeros(NDate, 1);
   NDate = 0;

   for i=1:fix(INFO.Width/MStB)
   for j=1:fix(INFO.Height/MStR)

      %Рассчет V(i)
      %V(MStR,1)=1;
      %for StR=1:(MStR-1)
      %    V(MStR-StR,1)=V(MStR-StR+1,1)*R(MStR*j-StR+1,i);
      %end

      %Рассчет V(i)
      V(MStR+1,1)=1;
      for StR=1:MStR
         V(MStR+1-StR,1)=V(MStR+1-StR+1,1)*R(MStR*j-StR+1,i);
      end

      %Рассчет A(ij) - восстановление изображения
      for StB=1:MStB                %по столбцам
         for StR=1:MStR             %по строкам
            A2(StR,StB)=fix(N1(MStB*(j-1)+StB,i)*2/V(StR+1,1))-fix(N1(MStB*(j-
1)+StB,i)*2/(V(StR+1,1)*R(MStR*(j-1)+StR,i)))*R(MStR*(j-1)+StR,i);
         end
         Q1bmp_tmp = fix(N1(MStB*(j-1)+StB,i)*2/V(1,1))-fix(N1(MStB*(j-
1)+StB,i)*2/(V(1,1)*R(MStR*(j-1)+StR,i)))*R(MStR*(j-1)+StR,i);
         NDate = NDate + 1;
         MDate(NDate,1) = Q1bmp_tmp;
         %if Q1bmp_tmp == 1
         %    Q1bmp = Q1bmp +1;
         %else
         %    Q0bmp = Q0bmp +1;
         %end
      end

      %Сохраняем массив
      P2((MStR*(j-1)+1):(MStR*(j-1)+MStR),(MStB*(i-1)+1):(MStB*(i-
1)+MStB))=uint8(round(A2(1:MStR,1:MStB)-1));

   end          %for j=1:fix(INFO.Height/MStR)
   end          %for i=1:fix(INFO.Width/MStB)

else

   for i=1:fix(INFO.Width/MStB)
   for j=1:fix(INFO.Height/MStR)

      %Рассчет V(i)
      V(MStR,1)=1;
      for StR=1:(MStR-1)
         V(MStR-StR,1)=V(MStR-StR+1,1)*(R(MStR*j-StR+1,i)-Rmin(MStR*j-StR+1,i));
      end
```

```
      %Рассчет A(ij) - восстановление изображения
      for StB=1:MStB                %по столбцам
         for StR=1:MStR             %по строкам
            A2(StR,StB)=fix(N1(MStB*(j-1)+StB,i)/V(StR,1))-fix(N1(MStB*(j-
1)+StB,i)/(V(StR,1)*(R(MStR*(j-1)+StR,i)-Rmin(MStR*(j-1)+StR,i))))*(R(MStR*(j-1)+StR,i)-
Rmin(MStR*(j-1)+StR,i))+Rmin(MStR*(j-1)+StR,i);
         end
      end

      %Сохраняем массив
      P2((MStR*(j-1)+1):(MStR*(j-1)+MStR),(MStB*(i-1)+1):(MStB*(i-
1)+MStB))=uint8(round(A2(1:MStR,1:MStB)-1));

   end          %for j=1:fix(INFO.Height/MStR)
   end          %for i=1:fix(INFO.Width/MStB)
end

else
   P2=uint8(round(N1-1));              %перевод в байтовый формат uint8
end

%восстановление плоскости после обработки
%              - черновая обработка
if or (fix(INFO.Width/MStB)*MStB ~= INFO.Width, fix(INFO.Height/MStR)*MStR ~= IN-
FO.Height)
   P2(INFO.Height,INFO.Width)=uint8(0);
end

%NFig=NFig+1,figure(NFig),imshow(P2);      %Отобразить рисунок

%Сохранить файл данных после демаскирования
fid = fopen(FileDate2, 'w');
count = fwrite(fid,MDate,'ubit1');
count = fclose(fid);
```

ЗАТВЕРДЖУЮ
Перший заступник Головного конструктора
ДНВП «Об`єднання Комунар» –
Головний інженер НТ СКБ «ПОЛІСВІТ»
кандидат технічних наук, доцент,
заслужений винахідник України

М.Ф. Сидоренко
"23" березня 2014 року

А К Т
впровадження результатів науково-прикладних досліджень
Бекірова Алі Енверовича

Комісія у складі: голови начальника відділу Євсюкова М.П. та членів комісії начальника лабораторії Сальникова В.В., провідного інженера, кандидата технічних наук Дашкієва В.М. склала дійсний акт, який полягає в тому, що при виконанні дослідно-конструкторських робіт використані наступні результати науково-прикладних досліджень Бекірова Алі Енверовича:

1. Стеганографічна система на основі прямого і зворотного функціонального перетворення для нерівноважного позиційного числа з імплантованим елементом, що забезпечує вбудовування і вилучення прихованої інформації на основі структурного стеганографіческого кодування та декодування.

2. Структурне стеганографічне кодування з маскуванням, яке базується на наступних етапах:

- формуванні нерівноважного позиційного базису для фрагмента зображення;
- структурне стеганографічне кодування в нерівноважному базисі основ;
- маскування структурної стеганографічної надмірності шляхом її локалізації на основі корекції довжини стеганограми.

3. Правило вбудовування інформації для структурного стеганографічного кодування, яке полягає в тому, що:

- один біт приховуваного повідомлення вбудовується на старшу позицію нерівноважного позиційного числа;
- локалізація стеганографічної надмірності досягається на основі відсікання молодшого біта стеганограми.

Впровадження результатів досліджень Бекірова А.Е. в контрольно-перевірочних комплексах КУ560, КУ4560 та в автоматизованій системі відображення інформації АСВІ на основі програмно-апаратних реалізацій дозволило забезпечити:

- приховану передачу службових повідомлень використовуючи в якості контейнеру як статичны так і динамічні відео сцени;
- більш ефективну побудову серверних баз даних стосовно службової інформації з елементом приховання документальних супроводжень відносно фото-відео матеріалів;
- підвищення стійкості прихованих даних до атак зловмисника відносно застосування існуючих методів стегонографічних перетворень досягає 30 – 70 % в залежності від ступеня структурної насиченості відео-контейнерів;
- збільшення стеганографічної ємкості на 40 – 80 % для потрібного рівня стійкості прихованих даних відносно виявлення та знищення.

Голова комісії
Начальник відділу М.П. Євсюков

Члени комісії:
Начальник лабораторії В.В. Сальников

Провідний інженер,
кандидат технічних наук В.М. Дашкієв

ЗАТВЕРДЖЕНО
Начальник ДНДІ МВС України
доктор юридичних наук,
професор,
заслужений працівник освіти

_____ **Проценко Т.О.**
«23» 01 2015 р.

А К Т
впровадження результатів дисертаційного дослідження
Бекірова Алі Енверовича

Комісія у складі:

Голови комісії: заступника начальника ДНДІ МВС України, кандидата юридичних наук Смерницького Д.В.;

Членів комісії:

начальника науково-дослідної лабораторії ДНДІ МВС України, кандидата юридичних наук, старшого наукового співробітника Лопатіна С.І.;

начальника науково-дослідного відділу ДНДІ МВС України, кандидата технічних наук, доцента Циганова О.Г.;

старшого наукового співробітника ДНДІ МВС України, кандидата технічних наук, Марченка О.С.,

склала цей акт про те, що нею розглянуто результати дисертаційного дослідження Бекірова Алі Енверовича, які можуть бути використані в науково-дослідній діяльності під час виконання дослідно-конструкторських робіт ДНДІ МВС України.

Результати науково-практичних досліджень Бекірова Алі Енверовича:

1. Стеганографічна система на основі прямого і зворотнього функціонального перетворення для нерівноважного позиційного числа з імплантованим елементом, що забезпечує вбудовування і вилучення прихованої інформації на основі структурного стеганографічного кодування та декодування.

2. Структурне стеганографічне кодування з маскуванням, яке базується на наступних етапах:

- формування нерівноважного позиційного базису для фрагмента зображення;
- структурне стеганографічне кодування в нерівноважному базисі основ;
- маскування структурної стеганографічної надмірності шляхом її локалізації на основі корекції довжини стеганограми.

3. Правило вбудовування інформації для структурного стеганографічного кодування, яке полягає в тому, що:

- один біт повідомлення, що приховується, вбудовується на старшу позицію нерівноважного позиційного числа;
- локалізація стеганографічної надмірності досягається на основі відсікання молодшого біта стеганограми.

Упровадження результатів досліджень Бекірова А.Е. в практичну діяльність підрозділів МВС України на основі програмно-апаратних реалізацій дозволить забезпечити:

- приховану передачу службових повідомлень з використанням в якості контейнера потоку відеокадрів як у системі відеоконференційного зв'язку, так і в системі електронної переписки;
- більш ефективну побудову серверних баз даних стосовно службової інформації з елементом приховання документальних супроводжень відносно фото - відеоматеріалів;
- підвищення стійкості прихованих даних до атак зловмисника відносно застосування наявних методів стеганографічних перетворень досягає 30–70 % в залежності від ступеня структурної насиченості відеоконтейнерів;
- збільшення стеганографічної ємкості на 40–80 % для потрібного рівня стійкості прихованих даних відносно виявлення та знищення.

Голова комісії:
Заступник начальника ДНДІ МВС України,
кандидат юридичних наук _____ **Смерницький Д.В.**

Члени комісії:
Начальник науково-дослідної лабораторії ДНДІ МВС України,
кандидат юридичних наук,
старший науковий співробітник _____ **Лопатін С.І.**

Начальник науково-дослідного відділу ДНДІ МВС України,
кандидат технічних наук,
доцент _____ **Циганов О.Г.**

Старший науковий співробітник ДНДІ МВС України,
кандидат технічних наук _____ **Марченко О.С.**