

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

Харьковский национальный университет радиоэлектроники

В. В. БАРАННИК, Д. В. БАРАННИК, А. Э. БЕКИРОВ

**ОСНОВЫ ТЕОРИИ
СТРУКТУРНО-КОМБИНАТОРНОГО
СТЕГАНОГРАФИЧЕСКОГО
КОДИРОВАНИЯ**

Монография

Харьков
2017

УДК 004.056.55
ББК 32.97-018.2
Б24

*Рекомендовано ученым советом
Харьковского национального университета радиоэлектроники
Протокол № 13/9-1 от 28.10.2016*

Рецензенты:

Е. В. Василю, доктор техн. наук, профессор, Одесской национальной академии связи; **Г. Ф. Конахович**, доктор техн. наук, профессор, Национального авиационного университета; **А. Г. Окснюк**, доктор техн. наук, профессор, Киевского национального университета им. Т. Г. Шевченко

Баранник В. В.

Б24 Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, А. Э. Бекиров, Д. В. Баранник. – Х. : ХНУРЕ, 2017. – 256 с.

ISBN 000-000-000-000-0

В монографии проводится обоснование необходимости использования стеганографических технологий в комплексных системах защиты информации в интересах обеспечения национальной безопасности. Проводится систематизация показателей комплексной оценки эффективности функционирования стеганографических систем. Строится классификатор стеганографических преобразований с учетом различных ракурсов проблематики встраивания скрываемой информации. Излагаются проблемные аспекты существующих технологий и методов стеганографических преобразований. На основе чего, показывается необходимость создания принципиально новых подходов относительно построения стеганографических систем.

Разрабатываются основные положения теории структурно-комбинаторного стеганографического кодирования. Соответственно формируется базовая концепция стеганографических преобразований на основе неравновесного позиционного синтаксического представления. В обобщенном виде концепция исследований формулируется как синтез систем стеганографического встраивания, осуществляемого в процессе формирования эффективного синтаксического представления видеоконтейнера на основе добавления (привития) скрываемых элементов в одномерное векторное (обобщенное) неравновесно-позиционное пространство с учетом наличия двумерных структурно-комбинаторных закономерностей.

Книга представляет интерес для специалистов в области кибербезопасности, информационных систем, компьютерных наук и телекоммуникационных технологий.

**УДК 004.056.55
ББК 32.97-018.2**

© Баранник В. В., Бекиров А. Е., Баранник Д. В., 2017
ISBN 000-000-000-000-0 © Харьковский национальный университет радиоэлектроники, 2017

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ.....	6
ПРЕДИСЛОВИЕ АВТОРА.....	7
ВСТУПЛЕНИЕ.....	17
Раздел 1. АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	20
1.1. Особенности обеспечения защищенности инфор- мационных ресурсов в современных условиях.....	21
1.2. Аспекты актуальности и значимости стеганогра- фических подходов.....	32
1.3. Классификация стеганографических подходов для реализации скрытного встраивания.....	38
1.4. Классификация методов встраивания информации в изображение-контейнер.....	48
Выводы.....	56
Раздел 2. МЕТОДЫ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ДЛЯ ВИДЕОКОНТЕЙНЕРА.....	59
2.1. Построение базовых методологических аспектов косвенного и непосредственного стеганографиче- ского встраивания.....	60
2.2. Создание системы классификации методов непо- средственного стеганографического встраивания..	69
2.3. Формирование показателей качества функциони- рования стеганографических систем.....	71

2.4. Оценка проблемных недостатков существующих методов стеганографических преобразований.....	91
2.5. Аспекты исследований.....	99
Выводы.....	104
Раздел 3. МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ ТЕХНОЛОГИЙ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ.	
3.1. Обоснование проблемных сторон функционирования технологий непосредственного встраивания.....	109
3.2. Обоснование подхода для построения технологии устранения недостатков непосредственного стеганографического встраивания.....	114
3.3. Разработка технологии функционального преобразования чисел с имплантированными данными на основе неравновесного позиционного кодирования.....	124
Выводы.....	133
Раздел 4. РАЗРАБОТКА МЕТОДА СТРУКТУРНО-КОМБИНАТОРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ.	
4.1. Разработка модели структурно-комбинаторного стеганографического кодирования.....	138
4.2. Разработка концепции стеганографического кодирования неравновесного числа с имплантированным элементом.....	147
4.3. Обоснование появления структурной стеганографической избыточности в процессе стеганографического кодирования.....	151
4.4. Разработка стеганографической системы с маски-	

рованием структурной стеганографической избы- точности.....	156
3.5. Разработка структурно-комбинаторного демаски- рующего декодирования.....	166
Выводы.....	174
Раздел 5. ОЦЕНКА ХАРАКТЕРИСТИК	
ЭФФЕКТИВНОСТИ РАЗРАБОТАННОГО МЕТОДА СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ.....	178
5.1. Оценка стеганографической емкости разработан- ной стеганографической системы.....	179
5.2. Оценка характеристик процесса скрытия встро- енных сообщений в случае неавторизированного доступа.....	185
5.3. Сравнительная оценка эффективности процесса изъятия скрываемой информации авторизирован- ным пользователем.....	197
5.4. Оценка устойчивости скрываемых сообщений к атакам злоумышленника для разработанной стег- нографической системы.....	207
5.5. Оценка стеганографического битрейта разрабо- танной стеганографической системы.....	213
Выводы.....	222
ВЫВОДЫ МОНОГРАФИИ.....	225
ЛИТЕРАТУРА.....	234
Приложение А. Примеры исходных изображений- контейнеров.....	250

СПИСОК СОКРАЩЕНИЙ

ДКП	дискретное косинусное преобразование
ДНК	дезоксирибонуклеиновая кислота
ИК	изображение-контейнер
НЗБ	наименее значимый бит
НПЧ	неравновесное позиционное число
РС	расширение спектра
СКН	системы критического назначения
СМИ	средства массовой информации
СКИ	системы критической инфраструктуры

ПРЕДИСЛОВИЕ АВТОРА

Интерес исследований, касающийся материала, излагаемого в данной книги, относится к построению стеганографических систем на информационном уровне взаимодействия открытых систем согласно модели OSI.

На современном этапе стеганография как наука и ее практические аспекты переживают очередной этап своего развития. Этому способствует целый ряд факторов. С одной стороны это факторы, определяющие актуальность повышения безопасности информационных ресурсов. Сюда следует отнести такие, как:

- наличие, а порой и резкое обострение политической напряженности;
- формирование многогранных и системно-сложных отношений между государствами, отличающихся неопределенностью и противоречивостью позиций и интересов сторон;
- разрастание множества локальных военных конфликтов в разных уголках планеты;
- наращивание фактора наличия террористических угроз, использование его в разыгрывании амбициозных интересов отдельных государств;
- активизация технологий гибридных войн в различных схемах их проявления;
- развитие форм и способов организации информационных войн с элементами информационно-психологического влияния на социум;
- создание новых видов вооружённой борьбы, в том числе кибер-оружия (кибер атаки, кибер вирусы);

- присутствие высокой конкуренции между государственными и коммерческими компаниями различного уровня.

Это диктует необходимость развития и создание новых подходов для обеспечения информационной безопасности (ИБ) как значимой составляющей безопасности государства, общества и личности. Формируется многообразие подходов и методов обеспечения ИБ, в том числе безопасности информации в инфокоммуникационных системах. Значимое место и роль здесь отводится и стеганографическим технологиям. Соответственно факторами, образующими актуальность условий для развития и создания принципиально новых стеганографических систем, использующих в своей основе как новые принципы встраивания в существующие контейнеры, так и принципиально новые системообразующие технологии (физические среды для встраивания и переноски скрытой информации), являются:

- с одной стороны современный высокотехнологичный уровень развития информационных, компьютерных, телекоммуникационных технологий, их взаимное интегрирование;

- с другой стороны наличие необходимого уровня информированности и образованности социума, его интеллектуализация.

В том числе этому способствует высокий уровень наукоемкости и доступности мультимедийных технологий, формирование единой системы электронного документооборота, развитие средств массовой информации. Все это формирует благоприятствующий информационно-технологический климат для развития и создания новых стеганографических технологий.

История развития физических принципов стеганографии как подхода для скрытой передачи (хранения) информации путем сохранения в тайне самого факта такой передачи (хранения) неразрывно связана с уровнем развития общества. Изменилась концепция сфер применения стеганографических технологий, но сама суть использования стеганографии как элемента противоборства остается и поныне!

На современном этапе широкое развитие набирают методы цифровой стеганографии. Современная цифровая стеганография является междисциплинарным научным направлением, и в этом проявляется ее синергетическая суть.

Цифровую стеганографию условно принято делить на два направления. Первое направление относится к сетевой стеганографии. Второе направление формируется как компьютерная стеганография. Основная составляющая компьютерной стеганографии заключается в использовании для скрытия информации компьютерных файлов – контейнеров. Наиболее практически завершенными являются стеганографические системы, использующие в качестве контейнера (переносчика) мультимедийные информационные ресурсы, включая форматы представления статических видеоснимков, потоков динамических видеок кадров, аудиофайлов. Здесь для исключения разнотолков дадим следующее определение.

Видеоcontainer – m -мерные статические (видеокадры) и динамические (видеопотоки) видеоинформационные ресурсы (секретные и несекретные), использующиеся для сокрытия (стеганографического встраивания) скрываемой информации на исходном, промежуточном или конечном этапах построения эффективного синтаксического представления (формата описания видеоинформационного ресурса) с учетом дальней-

шего их хранения и/или передачи в инфокоммуникационном пространстве.

Известные нам методы компьютерной стеганографии можно разделить на два класса. Первый класс составляют методы, организующие встраивание информации в контейнер на основе использования некоторых условий и решающих правил. Такой класс методов в данной книге обозначается как методы косвенного стеганографического преобразования. Для таких методов непосредственное встраивание элементов скрываемого сообщений в контейнер не проводится. Наоборот, второй класс образуют методы, для которых встраивание проводится с учетом значений элементов скрываемых сообщений, а именно: непосредственное встраивание элементов в контейнер или когда такое встраивание проводится с дополнительным учетом некоторых условий. Мы будем называть далее такие методы, как методы непосредственного стеганографического преобразования.

На данный момент вопросу сравнения эффективности функционирования методов двух таких классов уделено ограниченное внимание. Очевидно, что здесь можно найти как преимущества, так и недостатки для методов обоих классов. Сразу определимся, что предметом исследований нашей монографии не является установление факта преимущества методов первого или второго класса. Данный вопрос остается за пределами книги. Основная часть исследований, излагаемых в монографии, касается методов непосредственного стеганографического преобразования.

Монография состоит из пяти разделов. Каждый раздел представляет собой законченное решение одной задачи. Первый раздел рассматривает вопросы, связанные с анализом ак-

туальности и значимости роли и места компьютерной стеганографии для повышения информационной безопасности государства. Во втором разделе разрабатывается классификатор методов *непосредственного* стеганографического преобразования, проводится обоснование проблемных аспектов существующих методов встраивания информации. Соответственно обоснованию подхода относительно создания принципиально нового метода стеганографии и разработке модели стеганографических преобразований уделяется внимание в третьем разделе. Построение метода структурно-комбинаторного стеганографического кодирования излагается в четвертом разделе. Основная часть материалов пятого раздела посвящена оценке эффективности созданной стеганографической системы.

В результате проведенного нами анализа существующих стеганографических систем была установлена тенденция, состоящая в том, что они разрабатываются постфактум для уже созданных видеоформатов. Понятно, что многие из этих форматов строились без учета возможности, использования их в будущем в качестве контейнеров (цифрового переносчика) скрываемой информации. Главная задача, которая ставилась перед разработчиками, состояла в построении эффективного синтаксического представления видеок кадров с позиции сокращения их цифрового объема с допустимыми потерями информации в условиях незначительного влияния с позиции визуального восприятия. И, все! А где же здесь учет особенностей скрытого встраивания информации?

В связи с чем, основное количество подходов по созданию стеганографических систем строится с учетом особенностей разработанных видеоформатов. При этом с одной сторо-

ны системные недостатки таких форматов нередко оказывают сдерживающее влияние на повышение эффективности стеганографических технологий. С другой стороны некоторые форматы в принципе не допускают возможности встраивания информации в условиях ее скрытой передачи (хранения).

Естественным выводом здесь напрашивается аспект относительно создания такого видеоформата (эффективного синтаксического представления видеoinформации), для которого изначально закладывались бы интересы не только с позиции обеспечения эффективности представления информационных ресурсов (степень повышения информационной плотности, устойчивости к ошибкам в канале связи), но и интересы с позиции обеспечения скрытой передачи информации, т.е. стеганографии.

Отсюда вполне обосновано следует формулировка первого аспекта, лежащего в основе создания принципиально нового стеганографического подхода.

***Аспект 1.** Совместное рассмотрение как единого целого в одной системе, как принципов формирования эффективного синтаксического представления контейнера, так и принципов встраивания скрываемой информации.*

Требования стеганографических систем должны учитываться в процессе разработки (синтеза) эффективного синтаксического представления видеоконтейнера (построения формата хранения и передачи видеoinформационных ресурсов), наряду с такими как обеспечения помехоустойчивости, конфиденциальности, условиями семантического анализа.

При этом в процессе создания стеганографических систем важно учитывать то, что существует определенная «плата» за тайнопись. Эта плата касается неопределенно-

сти источника стегано-контейнера, его информационной интенсивности, устойчивости к обнаружению, изъятию и разрушению скрываемой информации, сложности обработки, дополнительных временных затрат на обработку и передачу стеганограммы.

В полне очевидно, что эту плату необходимо учитывать уже на этапе синтеза эффективного синтаксического представления видеоконтейнера.

Безусловно существующие стеганографические методы «стараятся» учитывать особенности как этапов формирования видеоформатов, так и особенности зрительной системы относительно восприятия стеганоконтейнеров (атака путем визуального анализа). В тоже время встраивание информации с использованием видеоконтейнеров происходит фактически путем изменения значений элементов (пикселей) либо для непосредственно самих видеокадров, либо для промежуточных форм их представления. Именно здесь закладывается главный ограничительный механизм, который является по сути системным недостатком, заложенным на этапе формирования фундамента построения стеганографических систем с непосредственным встраиванием информации. Он проявляется в необходимости жесткого учета таких ограничительных принципов как устойчивость к визуальным атакам. Строится механизм, сдерживающий рост удельного объема встраиваемых данных относительно степени вносимых искажений в видеоконтейнер.

Тогда зададимся вопросом. А что, если не изменять значение пикселя? Понятно, что тогда, например, необходимо просто добавлять элемент встраиваемого сообщения в пространство видеоконтейнера.

Законным здесь является формулировка второго ключевого аспекта синтеза стеганографической системы.

Аспект 2. Непосредственное стеганографическое встраивание информации не должно ограничиваться пространством двоичного представления отдельных элементов. Для стеганографического встраивания информации требуется рассматривать пространства больших размерностей.

В том случае, если мы модифицируем значение пикселя, то имеем дело с битовым пространством. В обратном случае для встраивания необходимо использовать пространство более высокой мерности.

Но, что делать с фактом, касающимся учета избыточности в процессе встраивания? В процессе встраивания скрываемой информации происходит повышение степени неопределенности стеганоконтейнера относительно исходного видеоконтейнера (до встраивания информации). Это происходит за счет того, что непосредственное встраивание «отбирает» или использует часть исходного количества избыточности видеоконтейнера для скрытого размещения информации. Тем самым снижая количество избыточности, которое может быть устранено в процессе эффективного синтаксического представления видеоконтейнера.

И вот какой же тип избыточности здесь используется?

А используется в процессе встраивания психовизуальная избыточность. Это как раз тот вид избыточности который с одной стороны обеспечивает для существующих форматов видеок кадров наибольшую эффективность. А с другой стороны напрямую связан с потерями информации. Это объясняется, как отсутствием обоснованного математического аппарата описания зрительной системы, так и универсальной количест-

венной меры определения психовизуальной информативности. Именно этим фактом объясняется наличие такого мощного контраргумента развития компьютерной стеганографии как визуальная атака относительно установления факта наличия встроенной информации.

Но тогда разумно будет предположить, что необходимо основываться дополнительно на учете количества избыточности видеоконтейнеров, связанными с закономерностями отличными от психовизуальной природы. Такими, нам известными закономерностями, являются статистические, структурные и комбинаторные.

Причем как показали проведенные исследования достаточно интересные результаты получаются в случае дополнительного учета структурно-комбинаторных закономерностей.

В связи с чем, доказательно вытекает третий ключевой аспект создаваемой стеганографической системы.

Аспект 3. В процессе стеганографических преобразований не следует ограничиваться учетом наличия только психовизуальной избыточности. Требуется стеганографические преобразования строить с учетом наличия других типов закономерностей видеокадров, не связанных с внесением потери информации. Здесь предлагается учитывать структурно-комбинаторную избыточность.

После чего основываясь на целый спектр трудов [9-16] в области кодирования информации и цифровой обработки изображений логично предложить встраивать скрываемую информацию с учетом наличия структурно-комбинаторной избыточности. Здесь предлагаются подходы, базирующиеся на обобщенных и смешанных позиционных кодовых систем (полиадических кодовых конструкций).

Это определяет формулировку четвертого ключевого аспекта создаваемого стеганографического подхода.

Аспект 4. Осуществлять стеганографическое встраивание информации в процессе сокращения избыточности на этапе формирования эффективного синтаксического представления видеоконтейнера без потери информации на основе полиадических кодовых конструкций (обобщенных и смешанных позиционно-биномиальных кодовых систем).

Таким образом, в обобщенном виде можно выделить следующую формулировку, определяющую направления исследований, изложенных в данной монографии.

Стеганографическое встраивание осуществляется в процессе формирования (принципиально нового) эффективного синтаксического представления видеоконтейнера на основе добавления (привития) скрываемых элементов в одномерное векторное (обобщенное) неравновесно-позиционное пространство с учетом наличия двумерной структурно-комбинаторной избыточности (структурно-комбинаторных закономерностей).

полковник, профессор
В. Баранник

ВСТУПЛЕНИЕ

Опыт функционирования систем критической инфраструктуры в условиях активного противодействия противника обнаружил острую потребность обеспечения необходимого уровня безопасности специальных информационных ресурсов (СИР). С одной стороны это диктуется повышенной значимостью СИР для информационной поддержки процессов принятия решений, в том числе в кризисных ситуациях. С другой стороны повышаются угрозы нарушения конфиденциальности и целостности СИР. В значимой степени это обусловлено ростом оперативно-программных и информационно-технологических возможностей противоборствующей стороны. Поэтому повышение безопасности специальных информационных ресурсов в инфокоммуникационных системах является актуальным направлением *научно-прикладных исследований*.

Отсюда представляет интерес разработка новых путей 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, развитие видеоинформационного поля, наличие привязки служебной информации к конкретному видеоматериалу.

Среди методов стеганографических преобразований отдельный интерес представляют методы непосредственного встраивания информации в изображение-контейнер.

Однако проведенный анализ существующих методов 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 систем критической инфраструктуры (СКИ). Такие требования обусловлены следующими факторами:

- повышение информационной интенсивности донесений в условиях кризисных ситуаций;
- использование в качестве специальных донесений видеоматериалов;
- повышение значимости влияния специальных донесений на результативность функционирования СКИ;
- 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 стеганографические технологии не обеспечивают в полной мере системных требований в кризисных ситуациях в условиях наличия активных противоборствующих сторон.

Для разрешения противоречия в процессе построения стеганографических систем предлагается дополнительно учитывать наличие структурных закономерностей видеоконтейнеров.

Раздел 1

АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В разделе рассмотрены особенности функционирования кризисных систем в современных условиях при наличии угроз. Сформулировано актуальное направление для научно-прикладных исследований, а именно которое заключается в необходимости повышения уровня информационной безопасности специальных информационных ресурсов в системах кризисного назначения.

Проводится анализ аспектов, определяющих актуальность и значимость стеганографических подходов для решения задачи повышения уровня конфиденциальности, целостности и доступности информационного ресурса

Рассматривается вариант классификации существующих стеганографических подходов в зависимости от использования физических принципов при осуществлении встраивания.

1.1. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В СОВРЕМЕННЫХ УСЛОВИЯХ

Развитие инфокоммуникационных технологий, процессы внедрения новейших информационных систем, формирование и развитие современного информационного сообщества определяет важность такого понятия, как информационный ресурс. [2, 34, 35, 36, 81]. В тоже время в информационной среде наблюдаются процессы, которые способствуют появлению дестабилизирующих факторов информационной безопасности. К таким факторам относятся тенденции в политической, экономической, технологической, экологической, правовой и информационной сферах, которые негативно влияют на информационную безопасность (рис.1.1).

На сегодняшний день одними из наиболее значимых дестабилизирующих факторов являются:

1. Дисбаланс существующей концепции коллективной безопасности, которая не всегда способна адекватно реагировать на современные вызовы.
2. Негативные последствия изменений геополитической обстановки для информационной безопасности в различных регионах мира.
3. Информационная экспансия развитых стран по отношению к менее развитым странам с целью получения преимуществ [35, 38, 39].



Рис. 1.1. Дестабилизирующие факторы информационной безопасности

4. Негативные последствия расширения кооперации в сфере развития информационной инфраструктуры и сотрудничества с зарубежными государствами. Уязвимость для информационной безопасности возникает, как следствие предоставления информационных площадок для средств мультимедиа других государств, включая интернет ресурсы.

5. Деструктивные последствия для информационной безопасности обусловлены наличием противоречий между экономическими интересами государств. Обострение противоречий является следствием перехода на рыночные отношения в экономике, появлением на рынке большого количества отечественных и зарубежных коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации, включением информационной продукции в систему товарных отношений [38, 41, 52, 55].

6. Критическое состояние отечественных отраслей промышленности, которая производит средства информатизации, защиты информации, технологии интеллектуальной обработки данных и искусственного интеллекта. Использование импортных технических и программных средств для хранения, обработки и передачи информации. Это может сопровождаться внедрением в аппаратные и программные изделия компонент, реализующих функции, которые не предусмотрены документацией [32, 36].

7. Постоянное развитие информационно-технической базы и повышение доступности средств для осуществления кибернетических атак. Увеличение их производительности при одновременном повышении компактности, в том числе появление новых образцов вирусов, шпионского программного обеспечения, эксплойтов, вредоносных программ.

8. Взаимодействие стран в условиях наличия информационных войн.

9. Уязвимость существующей международной и национальной нормативно-правовой базы в сфере регуляции и обеспечения информационной безопасности. Недостаточная регуляция государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг [43, 70].

10. Борьба между различными идеологическими системами.

11. Негативное воздействие природных и антропогенных факторов на окружающую среду. Это приводит к экологическим изменениям окружающей среды, оказывает влияние на общее состояние защищенности информационной среды.

12. Тенденции к нарастанию противостояния на почве религиозной нетерпимости.

13. Конфронтация на почве стремления к обладанию материальными и человеческими ресурсами.

В рамках исследований угроз безопасности информационных систем наиболее актуальным является вопрос обеспечения безопасности государственного информационного ресурса. В соответствии с Концепцией формирования системы национальных электронных информационных ресурсов (утверждено распоряжением Кабинета Министров Украины от 5 мая 2003 г. №259-р.) Государственный информационный ресурс является объектом права государственной собственности. Безопасность государственного информационного ресурса обеспечивается государственными органами управления (Закон України «Про державну службу спеціального зв'язку та захисту інформації України», ст. 1).

Для обмена и обработки государственной информации, как составляющей национальной безопасности, используются специальные информационные телекоммуникационные системы. Для таких систем важным является вопрос обеспечения заданного уровня информационной безопасности. С одной стороны необходимость защиты исходит из значимости государственной информации. Потеря или подмена даже части такой информации может привести к негативным политическим и экономическим последствиям, нанести ущерб имиджу государства на международной арене, стать причиной потери человеческих и материальных ресурсов. С другой стороны, критичность условий функционирования таких систем обусловлена наличием противоборствующих сторон. Это могут быть государственные или коммерческие структуры или злоумышленники. Потенциальный злоумышленник стремится раскрыть содержание информационного ресурса, а в последствии подменить или разрушить его.

Для анализа особенностей функционирования объектов критической инфраструктуры рассмотрим возможные угрозы информационной безопасности, которые можно разделить, как представлено на рис. 1.2 [3, 29, 40, 70].

Под угрозами конфиденциальности информационного ресурса понимается нарушение гарантии доступности конкретной информации только ограниченному кругу лиц (авторизованным пользователям).

Угроза целостности информационного ресурса подразумевает нарушение исходного вида и содержания информации в процессе обработки, передачи и хранения.

Под угрозой доступности понимается нарушение беспрепятственного доступа и обмена пользователями необходимой

информацией, в том числе не выполнение требований доступа по временным срокам.

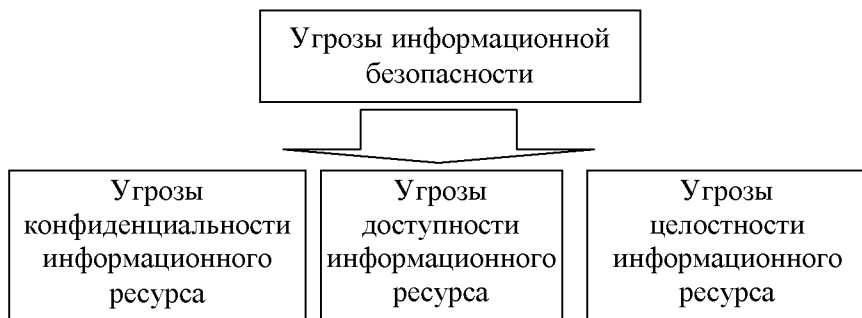


Рис. 1.2. Группы угроз информационной безопасности

Угрозы информационной безопасности в зависимости от источника возникновения делятся на:

- угрозы обусловленные действиями субъекта доступа или антропогенные угрозы;
- угрозы, обусловленные техническими средствами или техногенные угрозы;
- угрозы, обусловленные стихийными источниками или стихийные угрозы.

На рис. 1.3 представлен спектр угроз безопасности на информационную систему. К первой группе угроз относятся умышленные действия и воздействия на процесс обработки и передачи информационного ресурса, а именно:

- намеренное внесение ошибок в процессе обработки и передачи информации;
- перехват информации в каналах передачи данных;



Рис 1.3. Спектр возможных угроз информационной безопасности.

- кража технических средств и средств доступа;
- подмена информации или условий доступа;
- уничтожение (разрушение) программных и технических средств;
- уничтожение паролей и условий доступа;
- нарушение работы средств обработки информации и каналов передачи данных.

Ко второму типу угроз, вызванных техническими средствами, относятся следующие нарушения:

- нарушение условий функционирования системы обработки информации и систем управления;
- нарушение правил доступа;
- уничтожение информационного ресурса, разрушение серверов и хранилищ данных, уничтожение программного обеспечения;
- модификация информационного ресурса, хранилищ данных, программного обеспечения.

Третий тип угроз обусловлен воздействием стихийных источников.

Приведенные угрозы могут способствовать снижению уровня информационной безопасности как независимо друг от друга, так и в комплексе. Для противодействия нарушению безопасности информационного ресурса в кризисных системах организовывается совокупность мероприятий, предназначенных для достижения состояния защищенности при обработке, хранении и распространении информации. Рассмотрим основные направления обеспечения безопасности информации при функционировании кризисных систем:

1. Организационно-правовое обеспечение информационной безопасности. К этому направлению относится норматив-

ная документация, положения, инструкции и руководства которые регулируют взаимоотношения субъектов информационной безопасности, а также комплекс мероприятий, направленных на реализацию и исполнение требований нормативно-правовых актов.

2. Информационно-технологическое направление обеспечения информационной безопасности. Данное направление представлено аппаратными средствами и программными продуктами, функционирующими в рамках информационных систем и препятствующими нарушению конфиденциальности, целостности и доступности информационного ресурса. Также к данному направлению относится информационное и математическое обеспечение, которое необходимо для корректной и успешной организации защиты информации [4].

В рамках данного исследования рассмотрим более подробно технические подходы для обеспечения безопасности информации в кризисных системах. На современном этапе развития технических средств возможно использование различных методов для обеспечения защиты информационного ресурса. Здесь решение задачи обеспечения безопасности информации базируется на основе следующих подходов:

- криптографический подход;
- стеганографический подход;
- маскирование информационных ресурсов.

Криптографические подходы широко используются для защиты данных от несанкционированного доступа (шифрование данных, скремблирование речевых сообщений), модификации данных (хэш-функции, электронная цифровая подпись) и аутентификации (электронная цифровая подпись, протоколы криптографического обмена). Особенностью защиты инфор-

мации на основе криптографических методов является возможность использования открытых каналов для передачи конфиденциальной (критической) информации. При этом на основе криптографических подходов, открытые каналы приобретают основные качества закрытых каналов. Однако в этом случае злоумышленнику известен факт передачи конфиденциальной информации.

Методы маскирования для обеспечения информационной безопасности могут использоваться для скрывания, исключения возможности обнаружения и идентификации объектов и информации. Они применяются для решения следующих основных задач:

- передачи в канале произвольных данных (шум) для скрывания факта и времени передачи истинной информации;
- изменения голоса в речевых и цифровых данных;
- ретуширование важных объектов в статических и динамических изображениях;
- затирание (преобразование) конфиденциальной информации в текстовых данных и базах данных.

Особенностью методов маскирования является то, что такие подходы не всегда позволяют восстановить исходную информацию. В виде варианта обобщения областей применения маскирования, возможно выделить следующие направления:

- маскирование, как действие, направленное на сокрытие (защита, деактивация, обработка) определенных областей комплексного представления информации;
- маскирование, как действие, целью которого является обеспечение невозможности обнаружения, идентификации объектов и их частей.

Третьим направлением обеспечения информационной безопасности являются стеганографические подходы, которые являются некоторым обобщением нескольких подходов, связанных, в том числе и с маскированием информационных ресурсов. Одновременно с реализацией конфиденциальности данных, стеганография дополнительно учитывает вопросы обеспечения таких аспектов, как (рис 1.4):

- целостности информации, что подразумевает гарантии того, что данные будут сохранены в требуемом виде по своему синтаксическому и семантическому содержанию;

- доступности информации, под которой понимается способность обеспечения своевременного беспрепятственного доступа и обмена авторизованных пользователей интересующей их информацией по мере необходимости в установленные временные сроки в независимости от территориальной удаленности источников информации.

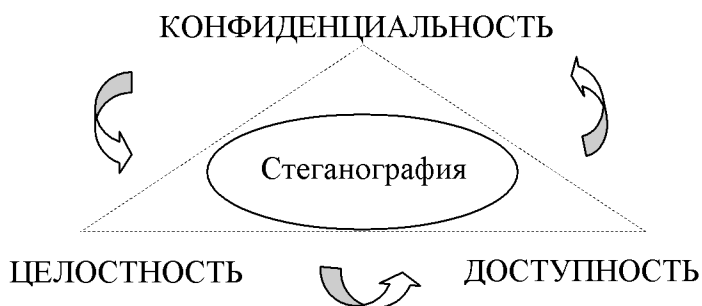


Рис. 1.4. Обеспечение информационной безопасности при стеганографическом подходе

Данные подходы есть суть обеспечения комплексной защиты информационных ресурсов на информационном уровне рассмотрения.

Таким образом, повышение уровня безопасности специальных информационных ресурсов в кризисных системах на основе использования стеганографических подходов является значимым направлением *научно-прикладных исследований* в направлении комплексного обеспечения защиты информации.

В данной книге мы будем рассматривать вопросы, связанные с обеспечением защиты информации на основе использования стеганографических подходов.

1.2. АСПЕКТЫ АКТУАЛЬНОСТИ И ЗНАЧИМОСТИ СТЕГАНОГРАФИЧЕСКИХ ПОДХОДОВ

Для обоснования подхода относительно повышения безопасности специальных информационных ресурсов на основе стеганографических методов необходимо рассмотреть аспекты, которые определяют их актуальность и значимость в кризисных условиях [7, 33, 37, 47, 70, 73, 78, 79] (рис 1.5). Здесь следует выделить такие аспекты актуальности и значимости стеганографических методов:

1. Необходимость повышения уровня конфиденциальности, целостности и доступности специального информационного ресурса. В современных условиях функционирования систем кризисного назначения необходимым условием является обеспечение заданного уровня составляющих информационной безопасности: конфиденциальности, целостности и доступности. Такая необходимость обусловлена с одной стороны повышением значимости информации и необходимо-

стью ее защиты, а с другой стороны возможностями злоумышленника относительно нарушения конфиденциальности, целостности и доступности. При этом необходимо отметить, что повышение уровня одной из составляющих информационной безопасности может быть связана с ухудшением показателей других составляющих. В качестве примера такой зависимости можно привести факт ухудшение показателей доступности специальной информации в условиях функционирования систем кризисного назначения с использованием сложных алгоритмов для обеспечения заданного уровня конфиденциальности.

2. Ограничения при использовании криптографических алгоритмов защиты специальных информационных ресурсов. Такие ограничения могут быть обусловлены следующими причинами:

1) ограничения пропускной способности каналов передачи данных. Данное ограничение обусловлено следующими факторами:

- жесткие требования по своевременности и оперативности доставки специальной информации. Такое условие затрудняет использование криптографических систем защиты для обеспечения требуемого уровня безопасности;

- отсутствие возможности применения компрессионных алгоритмов для учета закономерностей в процессе обработки криптографически преобразованных данных.

2) правовые ограничения на использование криптографических алгоритмов. Данный фактор включает запрет на использование не лицензированных методов защиты в государственных органах.

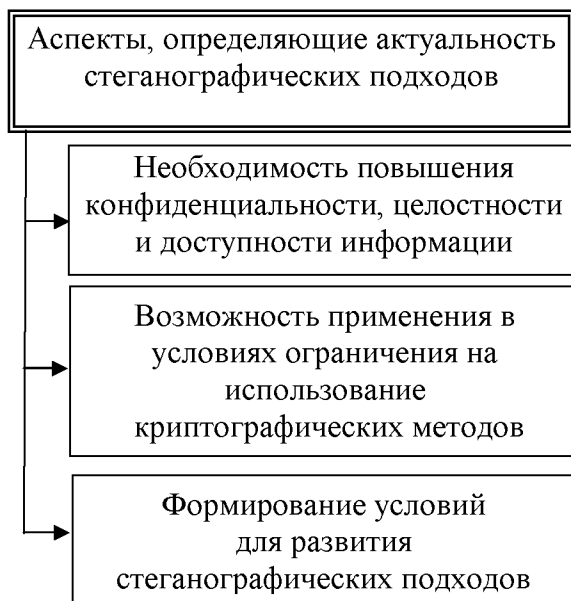


Рис. 1.5. Ограничения при использовании криптографических методов

Также сюда относятся законодательные запреты ряда государств на использование и распространение криптографических алгоритмов, обеспечивающих гарантированную стойкость без возможности обхода системы защиты. Такие средства приравниваются к системам вооружения;

3) ограничения, связанные с использованием вычислительных мощностей. Сложность реализации криптографических методов защиты диктует необходимость обеспечения значительных вычислительных ресурсов при обеспечении оперативности и доступности специальной информации.

Приведенные ограничения при использовании криптографических алгоритмов защиты информации имеют негатив-

ные последствия и могут нанести ущерб политическому и экономическому имиджу государства.

3. Формирование условий для развития стеганографических подходов обеспечения безопасности специальных информационных ресурсов обуславливается следующими позициями:

1) наличием множества различных стеганографических методов скрытного встраивания и передачи информации;

2) развитием телекоммуникационных технологий, использующих открытые каналы передачи данных широкого доступа;

3) отсутствием достаточного количества методов стеганографического анализа для выявления фактов наличия скрытного встраивания специальной информации;

4) широким распространением мультимедийных файлов в инфокоммуникационном пространстве. Это создает базу для формирования контейнеров, используемых при встраивании информации;

5) отсутствием ограниченной в нормативно-правовой базе на использование стеганографических методов защиты информации.

Поэтому в системах комплексной защиты специальных информационных ресурсов требуется также использовать методы стеганографических преобразований [1, 6, 18, 24, 26, 27, 45, 60, 64, 68]. Стеганографические преобразования в отличие от криптографической обработки позволяют скрыть сам факт наличия секретного сообщения. Здесь информация в виде сообщения преобразуется определенным образом и встраивается в некоторый цифровой контейнер, который не привлекает внимания. Функциональная схема реализации скрытой пере-

дачи данных на основе использования стеганографических подходов представлена на рис 1.6 и включает следующие этапы:

1. Стеганографическое встраивание. На этом этапе осуществляется стеганографическое встраивание информации в цифровой контейнер. Встраиваемое сообщение может быть предварительно преобразовано на основе алгоритмов шифрования, компрессионного и помехоустойчивого кодирования. В стеганографическом кодере преобразованное сообщение встраивается в контейнер на основе стеганографического правила и ключевой информации.

В результате стеганографического преобразования формируется стеганограмма.

2. Передача стеганографически преобразованного контейнера (стеганограммы) получателю по каналам передачи данных или размещение стеганограммы в хранилищах. В процессе передачи в инфокоммуникациях стеганограмма может подвергаться активным пассивным воздействиям.

3. Стеганографическое изъятие. На этом этапе авторизованный пользователь проводит стеганографическое декодирование. В этом случае ему известна следующая информация:

- факт наличия встроенной информации в стеганограмме;
- правило стеганографического декодирования;
- ключевая информация.

В результате обратного стеганографического преобразования авторизованный пользователь осуществляет изъятие встроенной информации.

Процесс стеганографического изъятия осуществляется при наличии на приемной стороне ключевой информации.

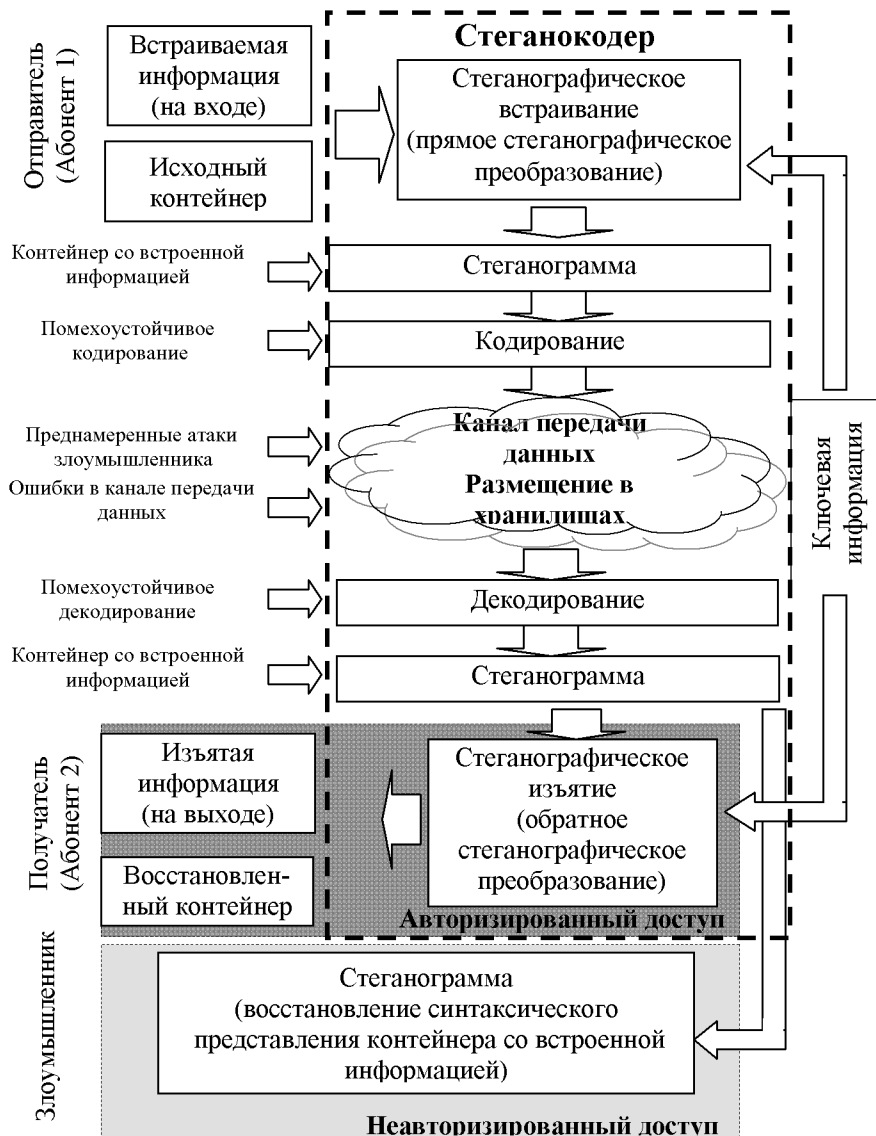


Рис. 1.6. Функциональная схема реализации скрытой передачи данных на основе стеганографического подхода

Теперь рассмотрим случай для неавторизованного доступа. Здесь у злоумышленника отсутствует информация о наличии скрытного встраивания сообщения в конкретной стеганограмме. Даже если злоумышленник осведомлен о том, что в данной стеганограмме присутствует встроенные данные, он не способен их изъять по причине отсутствия у него ключевой информации.

Рассмотрим существующие на сегодняшний день подходы для реализации стеганографического встраивания информации.

1.3. КЛАССИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКИХ ПОДХОДОВ ДЛЯ РЕАЛИЗАЦИИ СКРЫТНОГО ВСТРАИВАНИЯ

Основываясь на публикациях, дошедших до наших дней, можно предположить что стеганография, как термин, впервые был применен Иоганом Третемием (*Johannes Trithemius*) в 1499 году. Первые, сохранные на сегодняшний день записи о практическом использовании методов скрытой передачи сообщений встречаются еще в трактате Геродота «История». Данный трактат описывает греко-персидские войны в 5 веке до н.э.

С тех пор стеганографические подходы нашли широкое применение в самых различных областях жизни и деятельности общества. Основные этапы развития стеганографии представлены на рис 1.7 [125].

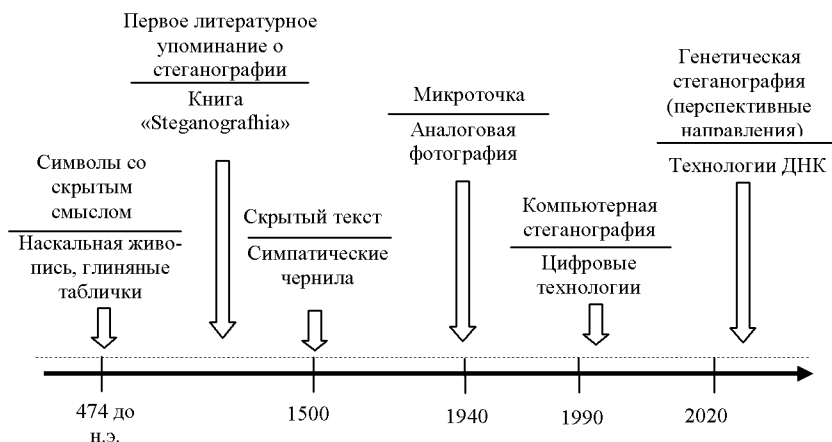


Рис. 1.7. Исторические этапы развития стеганографических подходов

Объединяющим фактором при использовании стеганографии было желание людей скрыть факт передачи сообщений.

Наиболее известным и широко распространенным методом стеганографии, является использование *симпатических чернил*. Например, известен факт использования революционерами декабристами симпатических чернил в письмах к родным и соратникам. Уже позже, в начале 20 века симпатические чернила использовались для составления секретных донесений в период Первой Мировой войны.

Одновременно с тайнописью при помощи симпатических чернил развивалась *графическая стеганография*. Например, графическая тайнопись широко использовалась поэтом классиком А.С. Пушкиным при создании иллюстраций. [31]. Некоторые примеры графической тайнописи представлены на обложке данной книги. В период Второй Мировой войны активно использовался метод скрытной передачи сообщений на

основе формирования микроскопических фотоснимков - *микророточек*.

С распространением компьютерных технологий широкое применение получили методы цифровой стеганографии, которые используют особенности компьютерных платформ и архитектуры сетевых протоколов. Известны случаи, когда методы цифровой стеганографии применялись в интересах специальных разведывательных служб и террористических организаций [126].

Вариант привлечения существующих стеганографических подходов с позиции использования физических процессов при осуществлении встраивания, представлен на рис.1.8.

Более подробно рассмотрим каждый стеганографический подход:

1. Биохимическая стеганография. Данный вид стеганографии сформировался совсем недавно. В работе [83] описан методе биохимической стеганографии на основе модифицирования ДНК существующий клетки или же синтеза новой модифицированной ДНК с целью скрытного встраивания дополнительной информации.

2. Химическая стеганография использует химические свойства некоторых веществ, как правило, для тайнописи. Классическим примером химической стеганографии является применение симпатических чернил, которые не видны и проявляются в процессе обработки специальным химическим веществом – проявителем.

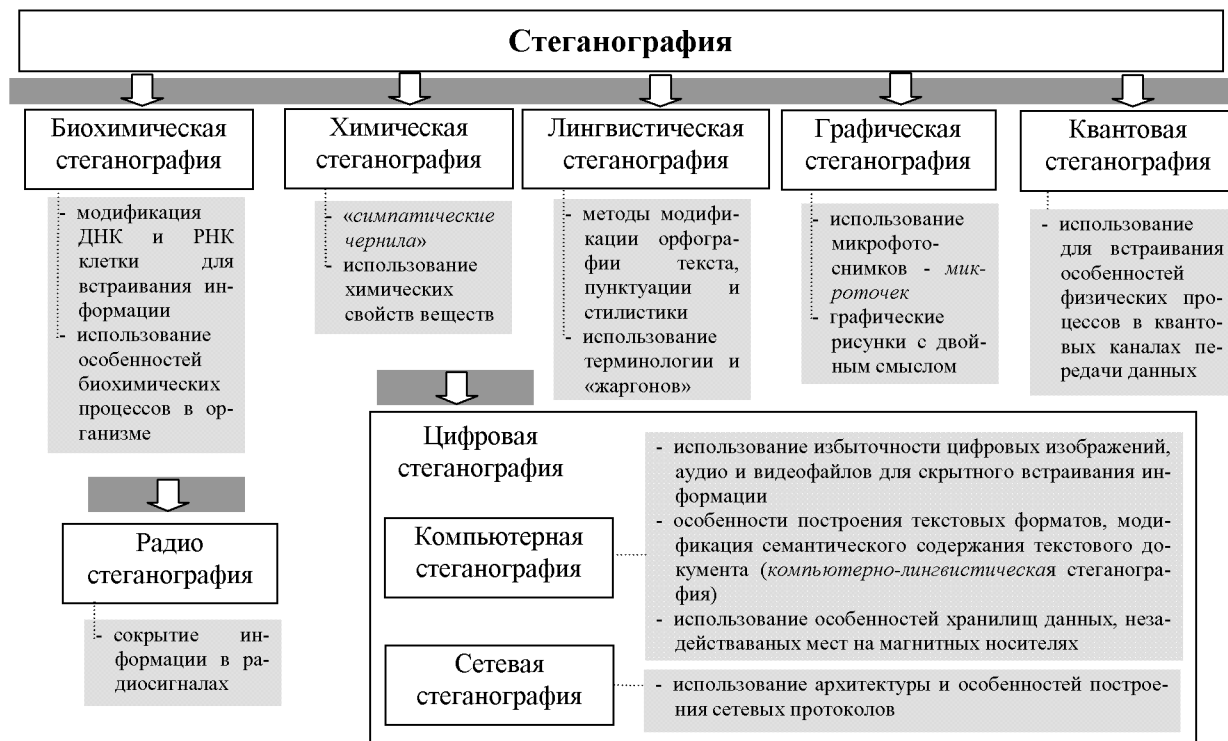


Рис. 1.8. Вариант классификации стеганографических подходов с позиции использования физических процессов при встраивании

3. Лингвистическая стеганография использует семантическую избыточность текста. Намеренное изменение порядка слов, орфографических особенностей текста, стилистики и пунктуации позволяет незаметно встраивать скрываемую информацию.

4. Графическая стеганография предусматривает привлечение микроскопических аналоговых фотоснимков - *микроточек* и реальных рисунков с двойным смыслом.

5. Квантовая стеганография появилась сравнительно недавно. Скрытие и передача информации в методах квантовой стеганографии осуществляется на основе использования особенностей физических процессов, которые протекают в квантовых каналах передачи данных. [51]

6. Радиостеганография использует в качестве контейнера для информации радиосигналы. Методы радиостеганографии подразумевают намеренную модификацию радиоволн на основе закона, который не замечен злоумышленнику и может быть детектирован на приемной стороне.

7. Цифровая стеганография рассматривает реализацию скрытного встраивания на основе компьютерной техники, программного обеспечения, вычислительных и управляющих систем и сетей. Цифровая стеганография на сегодняшний день является наиболее перспективным и развивающимся направлением. На данный момент методы цифровой стеганографии можно классифицировать, как представлено на рис. 1.9.

Сетевая стеганография. Методы сетевой стеганографии используют особенности архитектуры и избыточность сетевых протоколов для скрытной передачи информации.

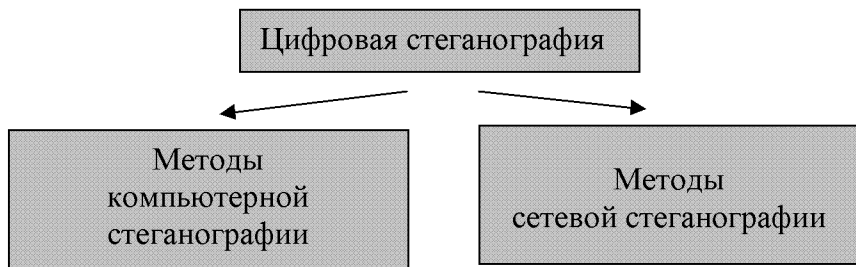


Рис. 1.9. Классификация методов цифровой стеганографии

Компьютерная стеганография представлена следующими методами:

- методы, которые используют специальные незадействованные места жестких дисков и других цифровых носителей информации;
- методы, которые учитывают избыточность и особенности построения форматов для цифровых изображений, аудио и видеофайлов;
- методы, использующие особенности построения текстовых форматов, семантическую избыточность текстового документа (компьютерно-лингвистическая стеганография).

Классификация методов цифровой стеганографии, которые функционируют в рамках сегментов эталонной сетевой модели OSI представлена на рис. 1.10.

При функционировании большинства методов компьютерной стеганографии задействован верхний *прикладной* уровень. Сетевая стеганография представлена на более низких уровнях.

К представленной классификации можно отнести также методы квантовой и радиостеганографии, которые используют физические процессы при обеспечении передачи данных в

инфокоммуникациях, т.е. функционируют в рамках физического уровня.

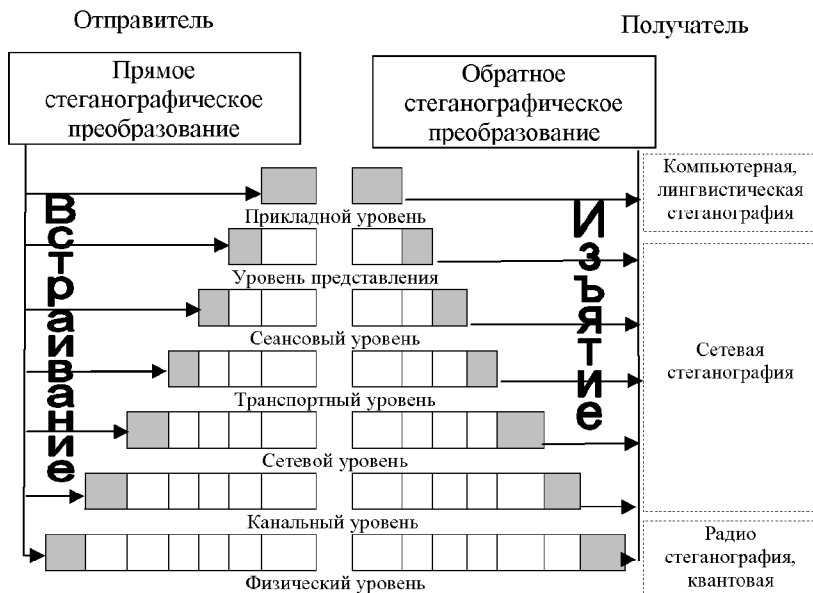


Рис 1.10. Классификация стеганографических методов с позиции модели OSI

Актуальные условия выбора видеoinформационного ресурса в качестве контейнера для методов цифровой стеганографии задаются следующими аспектами, а именно: (рис 1.11) [25, 30, 42, 44, 115, 112, 113, 117, 118]:

- широкое распространения цифровых изображений в открытых сетях общего пользования, в том числе и сети Internet. Развитию стеганографических подходов на основе использования изображения и видео в качестве контейнера способст-

вуют следующие факторы: массивные объемы статического и динамического видеоресурса; популяризация социальных сетей и сайтов видеохостинга, таких как Youtube, Facebook, Instagramm;

- возможность использования в закрытых каналах видеоконференцсвязи для управления в ведомственных организациях. Возможность двухсторонней передачи, обработки и представления интерактивной информации в режиме реального времени позволяет также передавать дополнительно информацию, скрытую в видеоконтейнере;

- относительная простота реализации прямого и обратного стеганографического преобразования, которая связана с особенностью форматов построения видеоконтейнера;

- наличие широких возможностей использования компактных мультимедийных устройств и беспроводных средств в условиях кризисных ситуаций. Это обусловлено постоянным снижением цен и повышением уровня доступности компактных мультимедийных устройств;

- широкое распространение и доступность систем, которые обеспечивают реализацию кибернетических атак на информационные системы;

- создание систем хранилищ на основе новых физических принципов. Данный аспект обусловлен распространением облачных хранилищ и современных накопителей данных, таких как твердотельные накопители (SSD диски) и квантовые хранилища, для хранения и резервного копирования данных.



Рис. 1.11. Обоснование выбора видеoinформационного ресурса в качестве контейнера для скрытой передачи специальной информации

- наличие мультимедийных средств для объекта поиска. Данный аспект обуславливается широким распространением спутниковых навигационных систем (GPS, ГЛОНАСС, Beidou), и отображением локации и маршрутов на цифровых картах, имеющих форматы цифровых изображений;

- широкое использование систем объективного видеонаблюдения и контроля для объектов критической инфраструктуры (контроль и информационное сопровождение мониторинговых миссий, видеоконтроль состояния стратегических объектов, складов вооружения и военной техники);

- наличие обширного видеоинформационного поля для телевизионных новостных служб. Данный аспект характеризуется стремительным развитием цифрового телевидения и интернет видеотрансляций (онлайн WEB камеры, видеостриминговый сервис Periscope и т.д.);

- существование подходов для визуализации вирусных кодов;

- наличие различных видов избыточности для статистического и динамического видеоресурса. Для видеоинформационного ресурса на межкадровом и внутрикадровом пространстве характерны следующие типы избыточности: психовизуальная, вероятностно-статистическая, структурная и комбинаторная;

- наличие четкой привязки специального видеоматериала к соответствующим текстовым пояснениям. Такой материал характерен для медицинской сферы и ведомственных организаций, например Министерства внутренних дел. Примером такой информации могут быть рентгеновские снимки с описанием врача, фотографии злоумышленников и текстовое описание к ним.

Теперь рассмотрим существующие подходы для классификации стеганографических методов встраивания на основе использования изображения-контейнера.

1.4. КЛАССИФИКАЦИЯ МЕТОДОВ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЕ-КОНТЕЙНЕР

Существующие методы компьютерной стеганографии, которые используют в качестве контейнера цифровое изображение можно классифицировать следующим образом:

1. По типу используемого протокола при взаимодействии абонентов стеганографические системы разделяются на [49]:

- *бесключевые*. Для функционирования алгоритма обратного стеганографического преобразования отсутствует необходимость в дополнительных данных, наподобие стеганографического ключа.

- *с секретным ключом*. Безопасность системы базируется на определенном фрагменте секретной информации-ключе, который известен авторизированным пользователям. Без такого ключа осуществить обратное стеганографическое преобразование невозможно.

- *с открытым ключом*. Такие системы используют для функционирования два типа ключей - открытый и секретный. При этом открытый ключ используется для встраивания сообщения, а секретный для извлечений.

- *смешанные системы*. К смешанным системам относятся алгоритмы которые используют различные подходы для выявления и изъятия скрытых данных. В данных системах обратное стеганографическое преобразование базируется как на учете степени корреляции стеганограммы и исходного изо-

бражения-контейнера, так и дополнительной априорной информации о встраивании.

Наибольший интерес для научно-прикладных исследований составляют именно стеганогарфические системы с секретным ключом, т.к. они отвечают требованиям относительно информационной безопасности встраиваемых данных. В данной монографии при разработке метода структурно-комбинаторного стеганографического кодирования будет учитываться условие наличия на приемной стороне секретной ключевой информации, без которой невозможно осуществить изъятие встроженных данных.

2. По типу используемой избыточности алгоритмы делятся на группы, которые учитывают психовизуальную, структурную, вероятностно-статистическую и комбинаторную избыточность (рис 1.12). При этом избыточность может выявляться на внутрикадровом и межкадровом уровнях.

Стеганографическое встраивание, на основе психовизуальной избыточности вызвано нечувствительностью зрительной системы человека к некоторым видам искажений цифрового изображения. Здесь разработчики методов используют преобразования цифровых изображений аналогично тем, что применяются для алгоритмов компрессии (дискретное косинусное преобразование, вейвлет-преобразование, аффинные преобразования и т.д.).

В случае рассмотрения отдельных элементов в качестве комбинаторных объектов, существует возможность выявить *комбинаторную избыточность* и использовать ее для скрывания информации.

Методы, использующие *структурную избыточность* базируются на модификации некоторых форм и взаимных рас-

положений целостных структурных единиц изображения-контейнера. Это обусловлено возможностью на основе правил связать отдельные элементы изображения некоторой структурой и ее математическом описании.



Рис. 1.12. Классификация стеганоалгоритмов по типу используемой избыточности

Вероятностно-статистическая избыточность обусловлена наличием статистических взаимосвязей между элементами изображения.

Для большинства методов стеганографического встраивания характерно использование психовизуальной избыточности. Поэтому, рассмотрим более подробно особенности зри-

тельной системы человека, которая делаются на две группы [15, 16, 46]: низкоуровневые свойства («физиологические») и высокоуровневые свойства («психофизиологические») (рис 1.13).

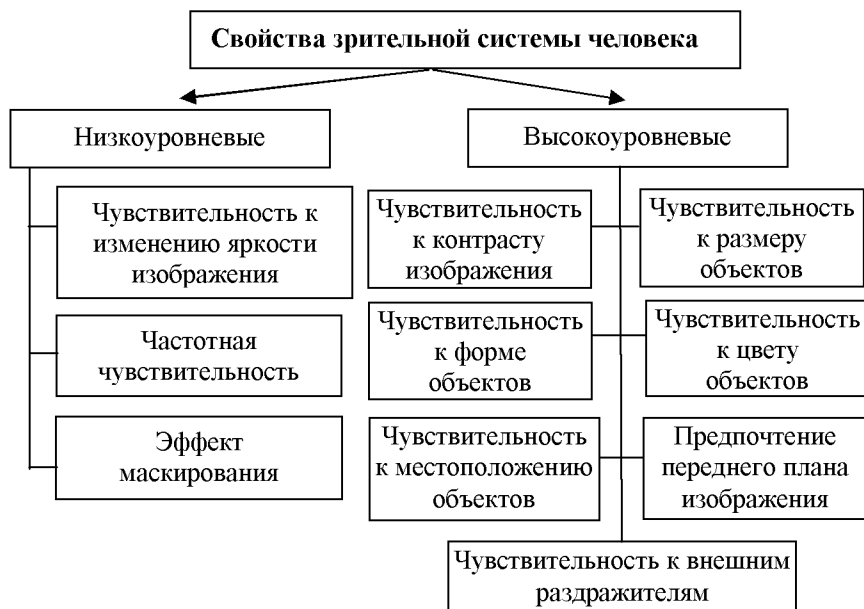


Рис. 1.13. Классификация особенностей человеческого зрения

Чувствительность к изменению яркости имеет следующую зависимость: для среднего диапазона изменения яркости, контраст примерно постоянен, тогда как для малых и больших яркостей значение порога неразличимости возрастает.

Частотная чувствительность человеческого зрения проявляется в том, что человек более восприимчив к низкочастотному, чем к высокочастотному шуму. Это явление связано с

неравномерностью амплитудно-частотной характеристики системы зрения человека.

Эффект маскирования проявляется в увеличении порога обнаружения видеосигнала в присутствии другого сигнала, обладающего аналогичными характеристиками. Каждая составляющая возбуждает нервные окончания глаза через ряд подканалов. Выделяемые глазом компоненты имеют различные пространственные и частотные характеристики, а также различную ориентацию (горизонтальную, вертикальную, диагональную), что и приводит к эффекту маскирования.

Высокоуровневые свойства человеческого зрения проявляются вторично. Обработавший первичную информацию, мозг выдает команды на ее адаптацию под изображение. Основными из этих свойств это:

1) чувствительность к контрасту изображения. Высококонтрастные участки изображения, перепады яркости обращают на себя значительное внимание;

2) чувствительность к размеру объектов изображения. Большие участки изображения более заметны по сравнению с объектами меньших размеров. Причем существует порог насыщения, когда дальнейшее увеличение размера не существенно;

3) чувствительность к форме объектов изображения. Длинные и тонкие объекты вызывают большее внимание, чем круглые однородные;

4) чувствительность к цвету изображения. Некоторые цвета (например, красный) заметнее других. Человеческий глаз менее восприимчив к синему цвету. Этот эффект усиливается, если фон заднего плана отличается от цвета фигур на нем;

5) чувствительность к местоположению. Человек склонен в первую очередь рассматривать центр изображения;

6) человек, в силу особенностей зрительной системы обычно внимательнее к изображениям переднего плана, чем заднего;

7) если на изображении есть люди, в первую очередь человек обратит свое внимание на них. На фотографии человек обращает первоочередное внимание на лицо, глаза, рот, руки.

В данной монографии разрабатываются теоретические основы и методы структурно-комбинаторного стеганографического кодирования. Здесь, соответственно, учитывается при встраивании информации *структурно-комбинаторная* избыточность изображения.

3. По выбору формата контейнера для встраивания:

- встраивание в *стандартизированный контейнер*. Методы, относящиеся к этому типу используют существующие форматы представления цифровых изображений. Например, реализация встраивания может осуществляться на основе платформы JPEG, PNG, JPEG 2000.

- встраивание в *нестандартизированный контейнеры*. Такие методы используют контейнеры, которые формируются на основе принципиально новых подходов.

В данной монографии рассматриваются методы структурнокомбинаторного стеганографического кодирования, которые предусматривают реализацию встраивания в процессе формирования контейнера на основе нового подхода.

4. По способу предобработки встраиваемого сообщения различают формирование компактного представления информационной последовательности, применение шифрования и корректирующих кодов (рис 1.14).

Встраиваемое сообщение можно подвергнуть *компрессионному преобразованию*, вследствие чего оно будет иметь меньший объем. Это позволяет встраивать его в контейнер меньшего объема. Также, такое сообщение будет менее заметным, вследствие меньшего количества измененных данных контейнера.

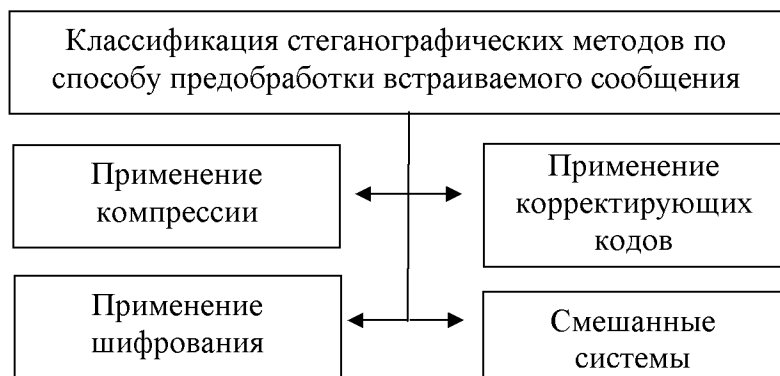


Рис. 1.14. Классификация стеганоалгоритмов по способу предобработки встраиваемого сообщения

В стеганографических системах с предварительным применением *корректирующих кодов* сообщение видоизменяется в преобразованную последовательность чисел для дальнейшего встраивания.

К встраиваемому сообщению также применимо *шифрование*. Такое преобразование усложнит злоумышленнику задачу получения исходного секретного сообщения.

Для *смешанных* систем возможно одновременное применение вышеприведенных способов предобработки к одному и тому же сообщению.

5. По стойкости стегосистемы делятся на [48, 49]:

- устойчивые к атакам разрушения встроенного сообщения;
- устойчивые к геометрическим атакам,
- устойчивые к криптографическим атакам;
- устойчивые к атакам против используемого протокола.



Рис. 1.14. Классификация стеганоалгоритмов по стойкости относительно атакующих воздействий

Стеганосистемы, устойчивые к *атакам, направленным на разрушение встроенного сообщения* не позволяют злоумышленнику разрушить секретное сообщение, встроенное в контейнера.

Устойчивость стеганосистемы к более распространенным *геометрическим атакам* заключается в невозможности на основе атакующих воздействий изменить встроенное в изображения секретное сообщения путем применения к контейнеру аффинных преобразований (масштабирование, изменение пропорций, повороты, сдвиги и усечения).

При наличии у злоумышленника стеганодетектора, он способен подвергнуть систему криптографической атаке. Изучая поведение детектора на различные виды сообщения, злоумышленник способен выяснить алгоритм его работы. Стеганосистемы, устойчивые к такого вида атакам, называются устойчивыми к *криптографическим атакам*.

В стеганосистемах, которые работают без наличия исходного контейнера, возможно применение злоумышленником *атаки против используемого протокола*. Суть атаки заключается в создании атакующим ложного контейнера, в который будет встроено оригинальное секретное сообщение. Стеганосистемы, способные предотвратить такую атаку, называются устойчивыми к атакам против используемого протокола.

В данной монографии рассматриваются методы стеганографического встраивания скрываемой информации, которые используют структурно-комбинаторный вид избыточности на внутрикадровом и межкадровом уровнях в условиях обеспечения устойчивости встроенных данных к активным и пассивным воздействиям злоумышленника.

Выводы

1. Показывается необходимость повышения безопасности специальных информационных ресурсов в кризисных ситуациях. Такая необходимость диктуется, в том числе наличием дестабилизирующих факторов и широкого спектра угроз безопасности информационного ресурса. Повышение значимости специальной информации и возможностей злоумышленника относительно нарушения конфиденциальности, целостности и

доступности специального информационного ресурса обуславливает необходимость обеспечения комплексной защиты информационных ресурсов.

2. Рассмотрены актуальные условия для развития стеганографических подходов. Показывается необходимость использования стеганографических методов в комплексных системах защиты информационных ресурсов. В этом случае закладываются требования по обеспечению доступности и целостности информации.

3. Представлен вариант классификации стеганографических подходов с позиции использования физических процессов при осуществлении встраивания информации. В том числе при классификации учитываются уровни модели OSI. Данный вариант классификации систематизирует знания в области стеганографии и создает целостную картину для понимания наиболее актуальных и распространенных на сегодняшний день направлений для реализации стеганографических преобразований. На основе анализа разработанной классификации выявлено, что на сегодняшний день наиболее развивающимися являются методы цифровой стеганографии. Это обусловлено развитием компьютерной техники и цифровых технологий передачи данных.

4. С учетом особенностей функционирования кризисных систем показана актуальность построения стеганографических систем на основе использования в качестве контейнера видеоинформационных ресурсов. К значимым условиям выбора видеоинформационного ресурса в качестве контейнера при стеганографическом преобразовании относятся:

- широкое распространение статических и динамических изображений для представления информации;

- наличия различных видов избыточности видеоресурса;
- относительная простота реализации прямого и обратного стеганографического преобразования.

5. Создан вариант систематизации классификации стеганографических методов в зависимости от используемого протокола стеганографического обмена, выбора избыточности контейнера в процессе встраивания и изъятия, выбора формата контейнера, способа предобработки сообщения и стойкости стеганосистем к атакам.

Раздел 2

МЕТОДЫ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ДЛЯ ВИДЕОКОНТЕЙНЕРА

В данном разделе проводится анализ существующих методов косвенного и непосредственного стеганографического встраивания.

Рассматривается система классификации для описания и обозначения места разрабатываемого метода структурно-комбинаторного стеганографического кодирования среди существующих подходов непосредственного стеганографического преобразования.

Приводятся различные группы показателей качества стеганографических преобразований. Для учета изменения характеристик компрессионного представления изображений со встроенными данными вводится группа показателей, которые характеризуют стеганографическое преобразования с позиции ухудшения эффективности компрессионных представлений.

Проводится анализ эффективности существующих подходов стеганографических преобразований. Устанавливается противоречие, которое заключается в том, что существующие стеганографические методы не обеспечивают в полной мере системных требований для скрытной передачи специальной информации в условиях наличия противоборства.

Формулируется направление дальнейшего исследования, а именно разработка теоретических основ и методов повышения безопасности специальной информации на основе структурно-комбинаторных стеганографических преобразований.

2.1. ПОСТРОЕНИЕ БАЗОВЫХ МЕТОДОЛОГИЧЕСКИХ АСПЕКТОВ МЕТОДОВ КОСВЕННОГО И НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

Существующие методы цифровой стеганографии для видеоизображений также можно классифицировать по логике встраивания, как показано на рис 2.1.

Чаще всего встраивание информации проводится побитно. В косвенных методах встраивание одного бита сообщения осуществляется путем выявления или создания зависимости между определенными параметрами изображения-контейнера. При этом стеганографический декодер в соответствии с обратным стеганографическим преобразованием устанавливает соответствие между значениями бит "0" или "1" или выявленной зависимостью. Это описывается следующим выражением:

$$B = f_{\text{изв}}(A'),$$

где B - данные, встраиваемые на приемной стороне;

$f_{\text{изв}}$ - функционал, задающий алгоритм обратного преобразования (извлечения встроенных данных);

A' - стеганограмма.

Такая логика встраивания реализована в следующих методах:



Рис. 2.1. Классификация стеганографических методов встраивания в изображение-контейнер

1. Метод относительной замены величин дискретного косинусного преобразования (метод Coch and Zhao) [100, 102, 109]. Один из наиболее распространенных на сегодня методов. В алгоритме метода реализовано разбитие изображения

на блоки 8×8 пикселей для применения к каждому из них дискретного косинусного преобразования (ДКП). В результате данного преобразования получается матрица 8×8 компонент ДКП. Каждый блок используется для скрытия одного бита данных встраиваемого сообщения. Для обеих сторон при организации секретного канала выбираются две конкретные компоненты ДКП с определенными координатами в трансформанте. Непосредственно скрытое начинается со случайного выбора блока изображения, предназначенного для кодирования бита данных. Встраивание происходит такой модификацией компонентов, чтобы при передаче "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 компоненты ДКП. После соответствующей коррекции компонент проводится обратное дискретное косинусное преобразование.

2. Метод Тао (Tao). Данный метод предусматривает косвенное встраивание специальной информации в спектрально-временную область изображения-контейнера. Стеганографическое преобразование осуществляется в два этапа. На первом этапе выполняется классификация блоков по шести категориям в зависимости от степени гладкости и наличия контуров. Для каждого блока на основе ключевого правила вычисляются коэффициенты чувствительности к аддитивному шуму, который имитирует ошибки в канале передачи данных. Второй этап предусматривает упорядочивание блоков в соответствии с полученными коэффициентами. Энергия встраиваемого элемента определяется этими коэффициентами. Обратное стеганографическое преобразование реализуется путем вычитания

прототипа изображения-контейнера из принятой стеганограммы и применения статистических методов проверки гипотез [101, 107].

3. Метод модификации яркости (метод Kutter-Jordan-Bossen) [110, 111, 114]. Встраивание реализуется в канал синего цвета RGB изображения. Данная цветовая компонента выбирается из-за низкой чувствительности человека к изменению значений ее элементов. Секретный ξ -й бит b_ξ скрываемого сообщения встраивается в канал синего цвета путем модификации яркости его i, j -го элемента $B_{i,j}$. Здесь используется выражение:

$$B'_{i,j} = \begin{cases} B_{i,j} - \nu \cdot \lambda_{i,j}, & \text{при } b_\xi = 0 \\ B_{i,j} + \nu \cdot \lambda_{i,j}, & \text{при } b_\xi = 1 \end{cases}$$

или

$$B'_{i,j} = B_{i,j} + (2 \cdot b_\xi - 1) \cdot \nu \cdot \lambda_{i,j}$$

где $B'_{i,j}$ - элемент $B_{i,j}$ после модификации;

ν - величина, которая определяет энергию встраиваемого сигнала, прямо пропорциональна устойчивости встроенной информации к искажениям

$\lambda_{i,j}$ - значение яркости i, j -го элемента изображения-контейнера.

Для извлечения секретного бита получателю необходимо выполнить предсказание значения первичного не модифицированного пикселя на основе значений соседних элементов. Для этого используется «крест» пикселей, расположенных вокруг модифицированного элемента.

4. Метода Бенгама-Мемона-Эо-Юнг (Benham-Memon-Yeo-Yeung) [42, 98]. Встраивание осуществляется в спектральные коэффициенты изображения-контейнера путем их модификации. Для этого в спектральной области выбираются три компонента ДКП, что позволяет уменьшить визуальные искажения. Для встраивания "0" значения компонент изменяются так, чтобы третья компонента стала меньше любой из двух первых. Если необходимо скрыть "1", третья компонента делается большей, чем первая и вторая компонента. Использование трех компонент ДКП вместо двух уменьшает искажения, которые вносятся в результате встраивания скрываемого сообщения.

Некоторые стеганографические методы можно классифицировать как подходы на основе смешанного встраивания. В этом случае прямое стеганографическое преобразование осуществляется с учетом встраиваемого элемента b_{ξ} . Наоборот, изъятие встроенной информации осуществляется на основе косвенного подхода путем сравнения и выявления зависимости. К таким алгоритмам можно отнести следующие методы:

1. Метод Кокса (Cox). Для данного метода встроенное сообщение представляет собой последовательности вещественных чисел с нулевым средним и единичной дисперсией. Для встраивания используются несколько АС - компонент y_i трансформанты ДКП изображения-контейнера с наибольшей энергией. При встраивании осуществляется модификации АС-компонент в соответствии с ключевым правилом встраивания. Такое преобразование задается следующим образом:

$$y'_i = y_i (1 + \alpha b_{\xi}),$$

где α - коэффициент модификации компоненты,

b_{ξ} - ξ -й бит встраиваемого сообщения;

y'_i - i -я модифицированная компонента y_i .

При стеганографическом изъятии осуществляются обратные операции: определяются компоненты ДКП стеганограммы и прототипа изображения-контейнера. После чего находятся разности между соответствующими компонентами наибольшей величины [101, 108].

2. Метод Подильчука (Podilchuk). Для метода характерна предобработка встраиваемого сообщения на основе модуляции вещественным случайным процессом. Следующий этап предусматривает вычисление компонент дискретного косинусного преобразования. Для каждой компоненты дискретного косинусного преобразования определяется значение порога. Порог выбирается таким образом, чтобы изменение компоненты ДКП сверх порога приводило к деградации изображения. Порог деградации изображения выбирается на основе позиции компоненты ДКП в матрице. Кроме того порог обусловлен свойствами самого изображения, а именно контрастностью и яркостью блока. Для встраивания данных анализируются пороги компонент ДКП. Если значение компоненты будет меньше порога, то ее величина не изменяется. В противном случае к компоненте прибавляется произведение порога и значение элемента скрываемого сообщения. Обратное стеганографическое преобразование осуществляется путем сравнения компонент дискретного косинусного преобразования стеганограммы и компонент ДКП прототипа исходного изображения-контейнера [104, 108].

Теперь рассмотрим методы на основе логики непосредственного стеганографического встраивания.

Для таких методов встраивание последовательности B секретного сообщения осуществляется путем замены данных контейнера на значения бит скрываемого сообщения, т.е.

$$A' = f_{стег} (A, B),$$

где A' - стеганограмма;

$f_{стег}$ - правило, определяющее процесс стеганографического встраивания;

A - исходное изображение-контейнер;

B - встраиваемые данные, $B = \{ b_1; \dots; b_g; \dots; b_v \}$

Такая замена возможна непосредственно на элемент встраиваемой информации, либо на бит преобразованного сообщения. Логика непосредственного встраивания реализована в семействах методов, базирующихся на размещении скрываемой информации в наименее значимый бит контейнера. Здесь возможны такие варианты встраивания в элементы:

1) пространственного представления изображения-контейнера (Наименее значимый бит режим 1) [106, 111, 122, 124]. Физика метода заключается в замене младшего значащего бита битом секретного сообщения (рис.2.2).

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 [3, 58, 72, 76, 77]. Среди модификаций данного метода можно выделить метод псевдослучайного интервала, в котором реализовано случайное распределение битов секретного

сообщения в контейнере. В результате чего расстояние между двумя встроенными битами определяется псевдослучайно.

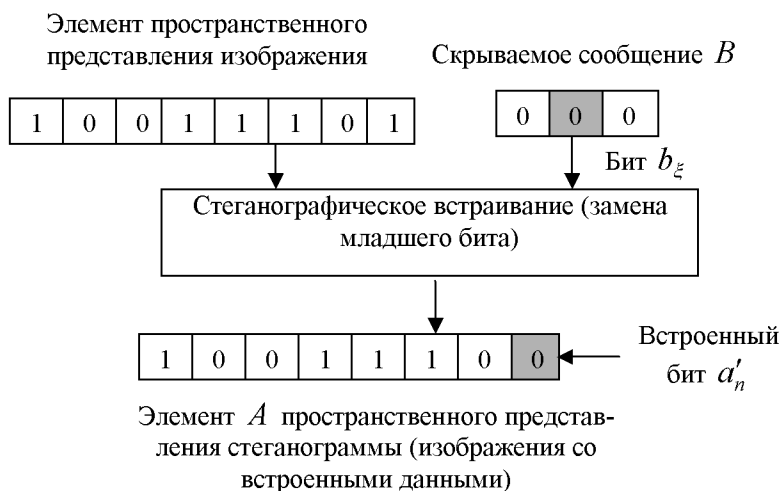


Рис. 2.2. Схема стеганографического встраивания бита скрываемого сообщения в НЗБ элемента пространственного представления изображения-контейнера

Также существует метод псевдослучайной перестановки, в котором биты сообщения встраиваются в псевдослучайные биты контейнера.

2) спектрального представления изображения-контейнера после квантования (Наименее значимый бит режим 2) [14, 50, 59, 9, 65, 71]. Здесь квантование используется, как один из этапов компрессии изображений на основе JPEG-технологий. Его суть заключается в том, что происходит коррекция компонент трансформанты в соответствии с особенностями зрительного восприятия изображения. Чаще всего квантование представляет собой укрупненную дискретизацию в соответст-

вии с заранее заданной матрицей квантования. Значение элементов матрицы квантования зависят от их позиции. Как вариант, матрица квантования строится эмпирическим путем. В этом случае, встраивание бита скрываемого сообщения реализуется путем замены НЗБ элемента спектрального представления изображения контейнера как показано на рис. 2.3.

Другим интересным классом методов непосредственного встраивания являются методы на основе расширения спектра [12, 34, 74, 75]. 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.

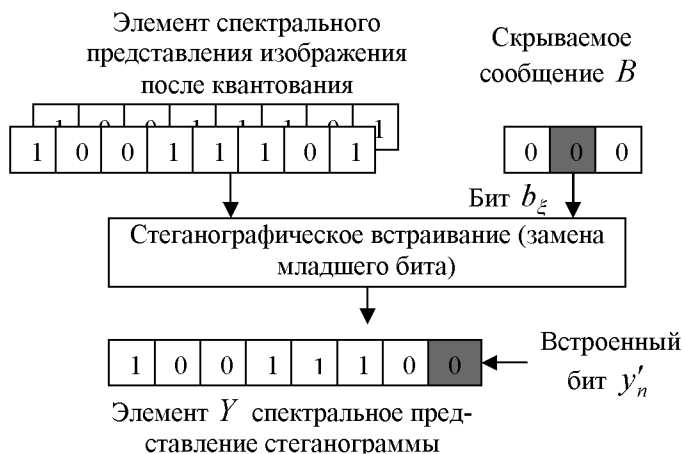


Рис. 2.3. Схема стеганографического встраивания бита скрываемого сообщения в НЗБ элемента спектрального представления изображения-контейнера после квантования

Необходимо отметить, что в данном исследовании не стоит задача сравнения методов непосредственного и косвенного встраивания. Но можно отметить, что при решении определенного класса задач, связанных с встраиванием данных, методы непосредственного стеганографического преобразования имеют некоторые преимущества.

В данном исследовании мы остановимся более подробно на методах непосредственного стеганографического встраивания.

Рассмотрим классификацию методов непосредственного стеганографического встраивания на основе использования видеоизображения в качестве контейнера.

2.2. СОЗДАНИЕ СИСТЕМЫ КЛАССИФИКАЦИИ МЕТОДОВ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

Для позиционирования разрабатываемого метода структурно-комбинаторного стеганографического кодирования среди существующих подходов, авторами предлагается следующая система классификации:

1. По выбору мерности пространства встраивания. Мерность пространства встраивания определяет совокупность элементов, на уровне которых осуществляется непосредственное встраивание (рис.2.4).

При выборе *битовой последовательности* для непосредственного встраивания, стеганографический алгоритм рассматривает двоичное представление компонент изображения контейнера в качестве рабочего пространства для стеганогра-

фического преобразования. Другими словами встраивание осуществляется на битовом уровне представления контейнера.

При выборе *одномерного вектора* в качестве мерности встраивания, стеганографический алгоритм реализует непосредственное стеганографическое встраивание для вектора элементов пространственного представления изображения-контейнера. Такой подход используется в разрабатываемом методе стеганографического кодирования.

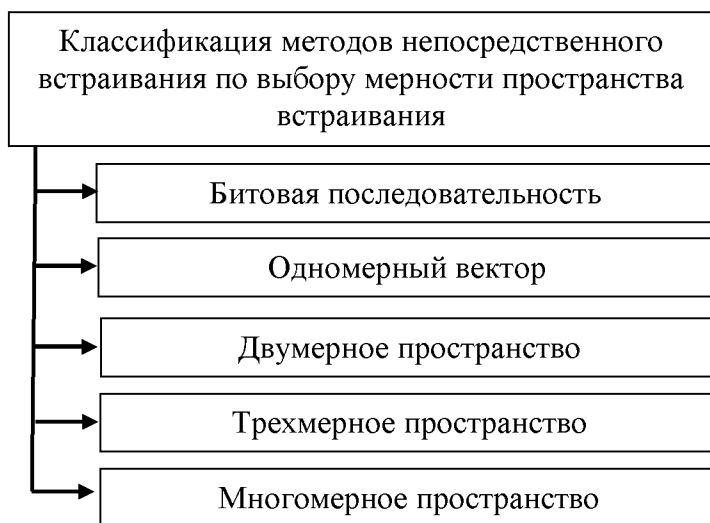


Рис. 2.4. Классификация стеганографических методов по мерности пространства встраивания

При реализации непосредственного встраивания возможно использование *двумерного* и *трехмерного пространства* в качестве рабочей области для стеганографического преобразования.

2. По выбору технологии непосредственного встраивания стеганографические методы можно классифицировать, как показано на рис. 2.5. Здесь выделяются две группы методов.

Технология встраивания на основе *модификации* подразумевает преднамеренное изменение элемента изображения контейнера на элемент стеганографически встраиваемого сообщения. Встраивание на основе модификации может осуществляться *без обратной связи* и с обратной связью (модификация с *размытием*).

В случае модификации без обратной связи стеганографический метод не предусматривает последующее преобразование элемента со встроенными данными. Другими словами стеганографическое встраивание заканчивается на этапе после выполнения непосредственной модификации элемента.

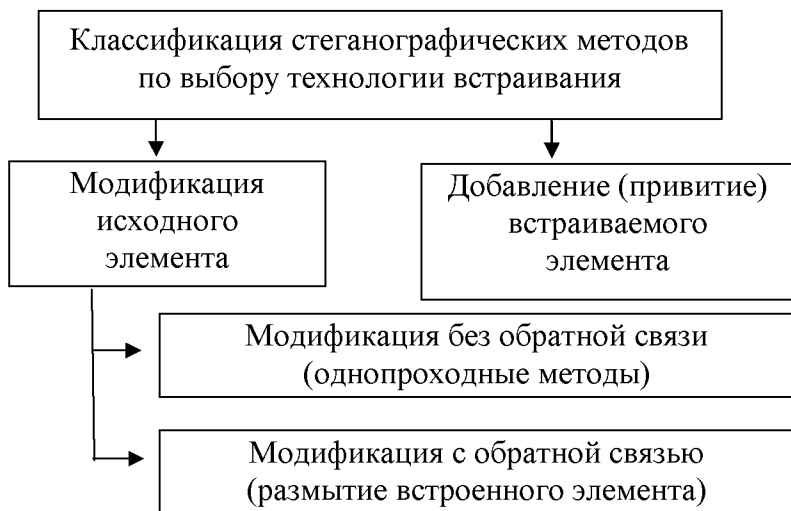


Рис. 2.5. Классификация стеганографических методов по выбору технологии непосредственного встраивания

Наоборот, модификация с обратной связью осуществляется в элементы, полученные после преобразования изображения контейнера. После непосредственной модификации осуществляется обратное преобразование. Искажение, которое было внесено в процессе модификации, *размывается* после обратного преобразования по элементам изображения контейнера. На этом этапе заканчивается этап стеганографического встраивания.

Технология встраивания на основе привития встраиваемого элемента реализовано в разрабатываемом методе стеганографического кодирования. Встраивание осуществляется путем привития встраиваемого элемента к одномерному вектору элементов изображения-контейнера. В отличие от модификации, привитие не вносит искажение непосредственно в исходные элементы.

3. По типу закономерностей, которые учитываются при встраивании на основе методов непосредственного стеганографического преобразования можно разделить на такие, которые учитывают:

- внутриэлементные закономерности, т.е. встраивание осуществляется на двоичном уровне описания элементов контейнера;

- *m* - мерные внутрикадровые закономерности;
- межкадровые закономерности.

4. По выбору этапа представления контейнера для непосредственного встраивания различают (рис 2.6):

- встраивание в *исходное* представление контейнера;
- встраивание в *промежуточную форму* описания представления контейнера. Здесь встраивание осуществляется в

процессе формирования формата представления изображения-контейнера;

- встраивание в элементы *конечной формы* эффективного синтаксического описания контейнера. В этом случае модификации подвергаются элементы формата представления изображения.

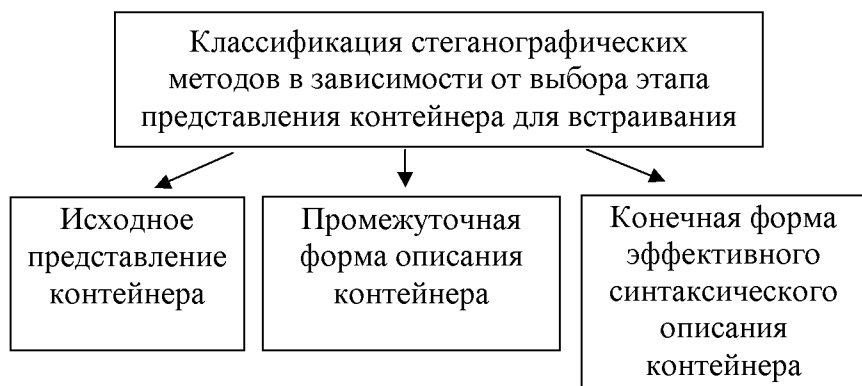


Рис. 2.6. Классификация стеганографических методов по этапам встраивания в процессе построения форматов описания контейнера

На рис 2.7 представлена структурно-функциональная схема обработки и передачи видеоданных в процессе стеганографического преобразования. В данной схеме этап формирования эффективного синтаксического представления объединен с этапом стеганографического преобразования. Это обусловлено тем, что в отличие от существующих стеганографических подходов, встраивание скрываемых данных на основе разработанного метода осуществляется непосредственно в процессе формирования эффективного синтаксического представления контейнера.



Рис 2.7. Структурно-функциональная схема обработки и передачи видеоданных при стеганографическом встраивании

5. По выбору технологии непосредственного изъятия встроенной информации. Здесь различают такие подклассы: считывание и проявление.

В случае, когда непосредственное встраивание осуществляется путем модификации встроенных данных, то процесс изъятия представляет собой *считывание* встроенного элемента с определенной позиции в элементе изображения-контейнера.

Проявление встроенной информации в процессе непосредственного изъятия осуществляется на основе функционального преобразования элемента изображения-контейнера с привитым встроенным элементом. Такая технология изъятия реализуется в разрабатываемом методе стеганографического кодирования.

Для установления позиции методов непосредственного встраивания на основе разработанной классификации предлагается ввести систему классификаторов K :

$$K = \{k_i^{(\gamma_{i,j})}\}, \quad i \in [1; 5]; \quad j \in [1; 4],$$

где $\gamma_{i,j}$ - j -я компонента i -го классификатора;

$k_i^{(\gamma_{i,j})}$ - i -й классификатор системы K по $\gamma_{i,j}$ -му признаку.

В табл. 2.1 представлено соответствие компонент и классификаторов для описания методов непосредственного встраивания.

Например, на основе разработанной системы классификации опишем метод встраивания в наименее значимый бит $K_{нзб}$.

Таблица 2.1

**Соответствие компонент классификатора разработанной
системе классификации**

	Компо- нента	Индекс компо- ненты	Вид классификации
Мерность пространства встраивания	$k_1^{(\gamma_{i,j})}$	$\gamma_{1,1}$	Битовая последова- тельность элементов контейнера
		$\gamma_{1,2}$	Одномерный вектор элементов контейнера
		$\gamma_{1,3}$	Двумерное простран- ство элементов представ- ления контейнера
		$\gamma_{1,4}$	Трехмерное простран- ство элементов пред- ставления контейнера
Техника встраивания данных	$k_2^{(\gamma_{i,j})}$	$\gamma_{2,1}$	Модификация без об- ратной связи
		$\gamma_{2,2}$	Размытие встроенного элемента
		$\gamma_{2,3}$	Привитие (добавление) встроенного элемента

Продолжение таблицы 2.1

Учет закономерности при встраивании	$k_3^{(\gamma_{i,j})}$	$\gamma_{3,1}$	Внутриэлементные закономерности контейнера
		$\gamma_{3,2}$	m - мерные внутрикадровые закономерности контейнера
		$\gamma_{3,3}$	Межкадровые закономерности контейнера
Этап представления контейнера	$k_4^{(\gamma_{i,j})}$	$\gamma_{4,1}$	Исходное представление контейнера
		$\gamma_{4,2}$	Промежуточная форма описания контейнера
		$\gamma_{4,3}$	Конечная форма эффективного синтаксического описания контейнера
Технология изъятия встроенных данных	$k_5^{(\gamma_{i,j})}$	$\gamma_{5,1}$	Считывание встроенных элементов при обратном стеганографическом преобразовании
		$\gamma_{5,2}$	Проявление встроенных элементов при обратном стеганографическом преобразовании

В случае рассмотрения метода встраивания в наименее значимый бит на основе предложенной системы классифика-

торов стеганографических методов непосредственного встраивания, классификатор будет иметь следующий вид:

$$K_{\text{изб}} = \{k_1^{(\gamma_{1,1})}; k_2^{(\gamma_{2,1})}; k_3^{(\gamma_{3,1})}; k_4^{(\gamma_{4,1})}; k_5^{(\gamma_{5,1})}\}.$$

На основе табл. 2.1. можно определить, что при встраивании на основе метода наименее значимого бита:

- встраивание осуществляется в битовую последовательность, $k_1^{(\gamma_{1,1})}$;
- в качестве техники встраивание используется модификация без обратной связи, $k_2^{(\gamma_{2,1})}$;
- при встраивании осуществляется учет внутризlementных закономерностей, $k_3^{(\gamma_{3,1})}$;
- встраивание осуществляется в исходную форму представления контейнера, $k_4^{(\gamma_{4,1})}$;
- изъятие данных осуществляется путем считывания встроенных элементов, $k_5^{(\gamma_{5,1})}$.

Таким образом, разработана классификация методов непосредственного встраивания, которая базируется на особенностях функционирования существующих стеганографических методов и позволяет охарактеризовать существующие методы с позиции:

- мерности пространства контейнера при стеганографическом встраивании;
- технологии стеганографического встраивания данных;
- учета вида закономерности при встраивании;
- выбора этапа построения контейнера при встраивании;

- технологии изъятия встроенных данных при обратном стеганографическом преобразовании.

Разработан вариант системы классификаторов для методов непосредственного встраивания на основе использования цифрового изображения в качестве контейнера. Данный классификатор базируется на разработанной системе классификации.

2.3. ФОРМИРОВАНИЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

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 специальной информации. Рассмотрим основные показатели эффективности стеганографических преобразований [23, 42, 66, 67, 74, 80, 95]:

I. Группа показателей, характеризующих стеганографический метод с позиции скрытности, т.е. стойкости стеганографического преобразования к выявлению факта наличия в изображении скрытного встраивания. Рассмотрение скрытности возможно по таким составляющим:

1. Вероятность $P_{уст}$ установления злоумышленником факта наличия секретного сообщения в изображении. Чем ближе значение величины $P_{уст}$ к нулю, тем выше стойкость стеганографического метода к выявлению факта наличия встроенных данных. При наилучших условиях вероятность

$P_{уст}$ принимает нулевое значение. Такие стеганографические методы исключают вероятность появления у противника утверждения о наличии в конкретной стеганограмме встроенных данных. Вероятность $P_{уст}$ может быть определена:

- качественно;
- количественно.

Качественно вероятность $P_{уст}$ установления злоумышленником факта наличия секретного сообщения в изображении может быть определена при помощи экспертных оценок.

Количественно данная вероятность может быть определена при наличии априорной информации или без нее.

При отсутствии априорной информации вероятность $P_{уст}$ может быть определена при помощи статистического анализа.

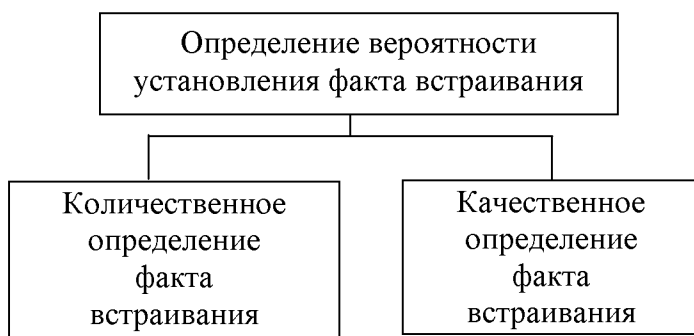


Рис. 2.8. Способы определения вероятности $P_{уст}$

Априорная информация, которая может быть использована для определения наличия факта встроенных данных принимает вид (рис 2.9):

- цифрового водяного знака, встроенного в стеганограмму;
- условий встраивания данных (класс областей изображения, вид компрессионного представления контейнера);
- метода прямого и обратного стеганографического преобразования;
- прототип исходного изображения-контейнера.

При наличии исходного изображения контейнера, стойкость стеганографического метода может быть оценена с помощью количественных разностных и корреляционных показателей.

Эти показатели базируются на вычисление метрики $\varepsilon(A; A')$, которая указывает на степень отличия между контейнером-оригиналом и стеганоизображением. К ним относятся:

1) максимальная разность Q_{MD} (Maximum Difference). Данный показатель характеризует разницу между пустым A и заполненным контейнером A' . Большое значение указывает на низкое качество изображения:

$$Q_{MD} = \max_{i,j} |a_{i,j} - a'_{i,j}|,$$

где $a_{i,j}$ - элемент в i -й строке и j -ом столбце изображения контейнера;

$a'_{i,j}$ - элемент в i -й строке и j -ом столбце изображения со встроенными данными;

2) средняя абсолютная разность Q_{AD} (Average Absolute Difference). Определяет среднее значение модуля разности между пикселями пустого и заполненного контейнеров. Боль-

шое значение средней абсолютной разницы указывает на низкое качество изображения



Рис. 2.9. Способы количественного определения вероятности $P_{уст}$ факта наличия встроенных данных

$$Q_{AD} = \frac{1}{Z_{cmp} Z_{cm\bar{o}}} \cdot \sum_{i=1}^{Z_{cmp}} \sum_{j=1}^{Z_{cm\bar{o}}} |a_{i,j} - a'_{i,j}|.$$

Здесь Z_{cmp} и $Z_{cm\bar{o}}$ - количество элементов соответственно в строке и столбце исходного изображения.

Значение модуля разности между пикселями пустого и заполненного контейнеров также можно представить в виде среднеквадратическое отклонение, которое определяется на основе формулы:

$$\sigma = \sqrt{Q_{AD}},$$

где σ - среднеквадратическое отклонение изображения со встроенными данными относительно изображения-контейнера.

3) качество изображения Q_{IF} (Image Fidelity). Безразмерная величина, которая отображает соответствие пустого контейнера A к заполненному контейнеру A' . Чем ближе это значение к единице, тем больше полученное изображение соответствует прототипу контейнера.

$$Q_{IF} = 1 - \frac{\sum_{i=1}^{Z_{cmp}} \sum_{j=1}^{Z_{cm\bar{o}}} (a_{i,j} - a'_{i,j})^2}{\sum_{i=1}^{Z_{cmp}} \sum_{j=1}^{Z_{cm\bar{o}}} (a_{i,j})^2};$$

5) нормированная взаимная корреляция Q_{NCC} (Normalized Cross-Correlation). Данный показатель характеризует связь между пустым A и заполненным контейнером A' . При высокой подобности изображений нормализованная взаимная корреляция стремится к 1.

$$Q_{NCC} = \frac{\sum_{i=1}^{Z_{cmp}} \sum_{j=1}^{Z_{cmб,}} a_{i,j} - a'_{i,j}}{\sum_{i=1}^{Z_{cmp}} \sum_{j=1}^{Z_{cmб,}} (a'_{i,j})^2}.$$

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

$$h = 20 \lg \left(\frac{255}{\sigma} \right) \text{ (дБ)},$$

где σ - среднеквадратическое отклонение изображения со встроенными данными относительно изображения-контейнера.

2. Вероятность $P_{\text{бл}}$ правильного определения блока изображения со встроенной информацией. Противником могут предприниматься попытки определения блока изображения со встроенными данными. Чем ближе значение величины $P_{\text{бл}}$ к нулю, тем выше стойкость стеганографического метода отно-

сительно правильного обнаружения злоумышленником блока изображения со встроенными данными.

3. Вероятность $P_{стег}$ правильного изъятия встроенного сообщения злоумышленником из стеганограммы. При известном факте наличия информации в изображении, противником может быть предпринята попытка изъятия встроенных данных. При вероятности $P_{стег}$, равной нулю, стеганографический метод является стойким к правильному изъятию скрываемых данных – это идеальные условия.

II. Группа показателей характеризующих метод стеганографического преобразования с позиции объема встраиваемых данных.

Методы стеганографии могут быть оценены по объему встраиваемых данных. Объем встраиваемых данных может быть представлен следующими показателями:

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 в 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. Стеганографический битрейт S_b - величина, определяющая количество пикселей в среднем необходимое для встраивания одного бита информации. Измеряется в битах на пиксель, бит/пиксель. Соответствующая оценка имеет вид:

$$S_b = \frac{w_{встр}}{Z_{min,cmp} Z_{min,cmб}} ,$$

где S_b - стеганографический битрейт, бит/пиксель;

$w_{встр}$ - объем встраиваемой информации, измеряется в битах;

$Z_{min,cmp} Z_{min,cmб}$ - минимально требуемый размер изображения, достаточный для встраивания информации объемом $w_{встр}$ на основе оцениваемого стеганографического алгоритма.

3. Вероятность $P_{из}$ безошибочного изъятия встроенных данных авторизованным пользователем. Данная величина используется для оценки уровня безошибочно изъятых информации при авторизованном 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 изъятых информации, бит.

В случае, когда вероятность $P_{из}$ принимает значение единицы, количество безошибочно изъятых встроенных данных авторизованным пользователем равно 100%. Изъятие проводится без потери скрываемой информации.

III. Группа показателей характеризующих стеганографический метод с позиции временных затрат на реализацию прямого и обратного стеганографического преобразования.

1. Время встраивания $\tau_{(w_{встр})np}$ - временные затраты, необходимые для встраивания информации объемом $w_{встр}$.

2. Время изъятия $\tau_{(w_{встр})обр}$ - время изъятия из стеганограммы информации, объемом $w_{встр}$.

IV. Группа показателей характеризующих стеганографический метод с позиции стойкости к атакам.

Здесь под стеганографическими атаками злоумышленника понимаются преднамеренные действия злоумышленника, направленные на разрушение или модификацию встроенной

информации. При этом учитываются случаи, когда факт наличия встроенной информации не установлен.

Основным показателем является вероятность модификации $P_{\text{мод}}$ встроенных сообщений. Чем ближе величина $P_{\text{мод}}$ к нулю, тем выше стойкость стеганографического преобразования к атакам.

V. Группа показателей характеризующих стеганографические методы с позиции изменения значений показателей эффективности компрессионного представления изображения-контейнера в условиях наличия встроенных данных относительно варианта отсутствия встроенной информации.

В современных телекоммуникационных системах, как правило, используется компрессионное представление изображений. В случае использования компрессионного представления изображений в качестве контейнера появляется необходимость учитывать влияние встроенной информации на показатели эффективности такого описания. Это обусловлено влиянием модификации элементов изображения-контейнера в процессе стеганографического преобразования. Поэтому предлагается ввести следующие показатели оценки влияния стеганографических преобразований на показатели компрессионного представления изображения-контейнера:

1. Степень Δh изменения пикового отношения сигнал-шум, как результат модификации элементов изображения контейнера:

$$\Delta h = |h_{\text{исх}} - h|,$$

где $h_{\text{исх}}$ - пиковое отношение сигнал-шум контейнера-изображения, дБ;

h - пиковое отношение сигнал-шум изображения со встроенной информацией, дБ.

2. Коэффициент Δk снижения степени сжатия изображения со встроенными данными при заданном значении h пикового отношения сигнал-шум. Это что задается формулой:

$$\Delta k = \frac{W_{сж}}{W'_{сж}},$$

где $W_{сж}$ - объем сжатого изображения-контейнера без встраивания;

$W'_{сж}$ - объем сжатого стеганографически преобразованного изображения.

Коэффициент Δk снижения степени сжатия будет принимать значение $0 \leq \Delta k \leq 1$. Наилучший результат $\Delta k = 1$.

3. Степень Δt увеличения суммарного времени обработки, в результате дополнительных временных затрат на прямое и обратное стеганографическое преобразование:

$$\Delta t = \frac{t'_{обр}(Z_{min,cmp}Z_{min,cmб}) - t_{обр}(Z_{min,cmp}Z_{min,cmб})}{t_{обр}(Z_{min,cmp}Z_{min,cmб})} 100\%,$$

где $t'_{обр}(Z_{min,cmp}Z_{min,cmб}) = t_{обр}(Z_{min,cmp}Z_{min,cmб}) + \tau_{(W_{всmp})np} + t_{npд} +$
 $+ \tau_{(W_{всmp})обр};$

$t_{обр}(Z_{min,cmp}Z_{min,cmб})$ - среднее время компрессионной обработки изображения-контейнера размером $Z_{min,cmp}Z_{min,cmб}$;

$\tau_{(W_{встр})np}$ - время встраивания информации в изображение;

$t'_{np\delta}$ - среднее время передачи стеганографически преобразованного изображения в канале передачи данных;

$\tau_{(W_{встр})обр}$ - время изъятия информации из стеганограммы;

$Z_{\min, \text{стр}} Z_{\min, \text{стб}}$ - минимально допустимый размер изображения для встраивания сообщения объемом $W_{встр}$.

Таким образом, в данном параграфе разработано пять групп показателей для оценки эффективности стеганографических методов с различных позиций, а именно:

- группа показателей, которые характеризуют стеганографический метод с позиции стойкости к атакам, направленным на выявления факта наличия скрытного встраивания;

- группа показателей, на основе которых проводится оценка стеганографических преобразований с позиции объема встраиваемых данных;

- группа показателей, характеризующих стеганографический метод с позиции временных затрат на реализацию прямого и обратного стеганографического преобразования;

- группа показателей, которые позволяют оценить стеганографический метод с позиции стойкости к атакам злоумышленника.

Для учета влияние стеганографического встраивания на показатели эффективности компрессионных представлений изображения-контейнера разработана группа показателей, характеризующих стеганографический метод с позиции изменения характеристик эффективности компрессионных показателей изображения со встроенными данными.

2.4. ОЦЕНКА ПРОБЛЕМНЫХ НЕДОСТАТКОВ СУЩЕСТВУЮЩИХ МЕТОДОВ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Проведем анализ эффективности данных стеганографических методов. При этом необходимо учитывать возможность применения злоумышленником активных и пассивных атак. Возможный спектр воздействий на стеганографическую систему, приведенных в табл. 2.2., а именно атаки [28, 54, 56, 61, 63, 94, 99, 103, 106], направленные на:

Таблица 2.2

Спектр основных пассивных и активных атак на стеганографическую систему

	Цель осуществления атаки		
	Выявление факта наличия встраивания	Разрушение встроенного сообщения	Изъятие (раскрытие) встроенного сообщения
Пассивные (непреднамеренные)	Визуальная атака	Шумы в канале передачи данных	-
Активные (преднамеренные)	При наличии априорной информации: - корреляционные методы. При отсутствии априорной информации (стеганографический анализ): - метод хи-квадрат; - RS-метод; - анализ пар значений; - анализ гистограмм частот переходов; - анализ числа переходов значений	Постановка помех. Компрессионные атаки. Геометрические (аффинные) атаки: - повороты; - масштабирование; - фрагментация. Фильтрация.	Стеганографический анализ

- выявление факта наличия встраивания в изображении специальной информации;
- разрушение встроенного сообщения;
- изъятие (раскрытие) встроенного сообщения.

Для выявления проблемных сторон существующих подходов скрытного встраивания информации, 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 $w_{встр}^{(Z_{сmp} Z_{сmb})}$ метода НЗБ в режиме 2 зависит от размера контейнера и определяется на основе следующего выражения:

$$w_{встр}^{(Z_{сmp} Z_{сmb})} = \frac{3 \cdot Z_{сmp} Z_{сmb}}{\omega} \text{ (бит)}, \quad (2.1)$$

где $Z_{сmp} Z_{сmb}$ - размер изображения-контейнера,

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

Выражение для определения относительной стеганографической емкости $w_{отн}^{(Z_{cnp} Z_{ctб})}$ метода НЗБ в режиме 2 имеет вид:

$$w_{отн}^{(Z_{cnp} Z_{ctб})} = \frac{w_{встр}^{(Z_{cnp} Z_{ctб})}}{W_{исх}} \cdot 100 \% . \quad (2.2)$$

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:

$$W_{исх} = 8 \cdot 3 \cdot Z_{cnp} Z_{ctб} = 24 \cdot Z_{cnp} Z_{ctб} \text{ (бит)} \quad (2.3)$$

Перепишем формулу для относительной стеганографической емкости метода с учетом выражений (2.1) и (2.3). Тогда получим:

$$w_{отн}^{(Z_{cnp} Z_{ctб})} = \frac{w_{встр}^{(Z_{cnp} Z_{ctб})}}{W_{исх}} \cdot 100\% = \frac{Z_{cnp} Z_{ctб}}{8 \cdot Z_{cnp} Z_{ctб} \cdot \omega} \cdot 100\% .$$

В этом случае в зависимости от количества элементов ω , необходимых для встраивания относительная стеганографическая емкость $w_{отн}^{(Z_{cmp} Z_{стб})}$ метода НЗБ в режиме 2 примет следующие значения:

- для $\omega = 2$:

$$w_{отн}^{(Z_{cmp} Z_{стб})} = \frac{3 \cdot Z_{cmp} Z_{стб}}{48 \cdot Z_{cmp} Z_{стб}} 100\% = \frac{1}{16} 100\% = 6,25\% ;$$

- для $\omega = 4$:

$$w_{отн}^{(Z_{cmp} Z_{стб})} = \frac{3 \cdot Z_{cmp} Z_{стб}}{96 \cdot Z_{cmp} Z_{стб}} 100\% = \frac{1}{32} \cdot 100\% = 3,1\% .$$

Рассмотрим метод встраивания информации на основе расширения спектра. При встраивании информации на основе метода РС, один бит скрываемого сообщения встраивается в фрагмент изображения, содержащий ω элементов. Абсолютная стеганографическая емкость $w_{встр}^{(Z_{cmp} Z_{стб})}$ для данного метода определяется на основе следующего выражения:

$$w_{встр}^{(Z_{cmp} Z_{стб})} = \frac{3 \cdot Z_{cmp} Z_{стб}}{\omega} \text{ (бит)}. \quad (2.4)$$

Относительная стеганографическая емкость $w_{отн}^{(Z_{cmp} Z_{стб})}$ для данного метода определяется на основе выражения (2.2), а объем $W_{исх}$ исходного изображения-контейнера для метода РС

определяется на основе выражения (2.3). В этом случае формула для определения значения $w_{отн}^{(Z_{cnp} Z_{ctб})}$ относительной стеганографической емкости примет следующий вид:

$$w_{отн}^{(Z_{cnp} Z_{ctб})} = \frac{w_{встр}^{(Z_{cnp} Z_{ctб})}}{W_{исх}} \cdot 100\% =$$

$$= (3 \cdot Z_{cnp} Z_{ctб} / \omega) / 24 \cdot Z_{cnp} Z_{ctб} \cdot 100\%$$

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

$$w_{отн}^{(Z_{cnp} Z_{ctб})} = \frac{3 \cdot Z_{cnp} Z_{ctб} \cdot 4}{24 \cdot Z_{cnp} Z_{ctб} \cdot 64} = \frac{1}{128} \cdot 100\% = 0,78\%$$

В табл. 2.3 представлены значения относительной стеганографической емкости методов НЗБ в режиме 2 и РС для различных классов изображений.

Из анализа значений в табл. 2.3 можно сделать вывод, что значение относительной стеганографической емкости для рассматриваемых методов принимает значение от 0,78 до 6,25 %.

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

Для метода НЗБ в режиме 2 объем $w_{из}^{(Z_{cnp} Z_{ctб})}$ безошибочно изъятых данных в условиях отсутствия активных атак

принимает значение меньше $w_{встр}^{(Z_{стр} Z_{стб})}$ встроенных данных, т.е.

$$w_{из}^{(Z_{стр} Z_{стб})} < w_{встр}^{(Z_{стр} Z_{стб})} .$$

Таблица 2.3

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

Отно- ситель ная ем- кость, %	Метод стега- нографическо- го встраивания		Значение ПОСШ, дБ		
			Сильно- насы- щенное изобра- жение	Средне- насы- щенное изобра- жение	Слабо- насы- щенное изобра- жение
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

Для такого метода вероятность $P_{из}$ безошибочного изъятия встроенных данных может достигать значения $P_{из} = 0,6$.

Теперь рассмотрим вероятность безошибочного изъятия встроенных данных для метода РС. В случае изъятия встроен-

ного бита скрываемого сообщения на основе метода РС, вероятность $P_{из}$ будет достигать уровня 0,5.

На рис. 2.10. 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.

Из анализа рис. 2.10 можно сделать выводы что:

- вероятность безошибочного изъятия встроенных данных для метода НЗБ и РС может принимать значение от 0,5 до 0,6;
- для метода НЗБ в режиме 2 выигрыш относительно метода РС по значению вероятности безошибочного изъятия встроенных данных достигает уровня 0,1.

Проведем оценку вероятности безошибочного изъятия встроенных данных в условиях атаки противника с применением ДКП и квантования. Для этого сравним процентные значения количества $w_{из}^{(Z_{cmp} Z_{ctb})}$ изъятых бит относительно количества $w_{встр}^{(Z_{cmp} Z_{ctb})}$ встроенных бит для метода РС.

Для проверки стойкости стеганографического преобразования к атакующим воздействиям проведем оценку вероятности безошибочного изъятия встроенных данных в условиях атаки противника с применением ДКП и квантования. Для этого сравним процентные значения количества $w_{из}^{(Z_{cmp} Z_{ctb})}$ изъятых бит относительно количества $w_{встр}^{(Z_{cmp} Z_{ctb})}$ встроенных бит для метода РС.

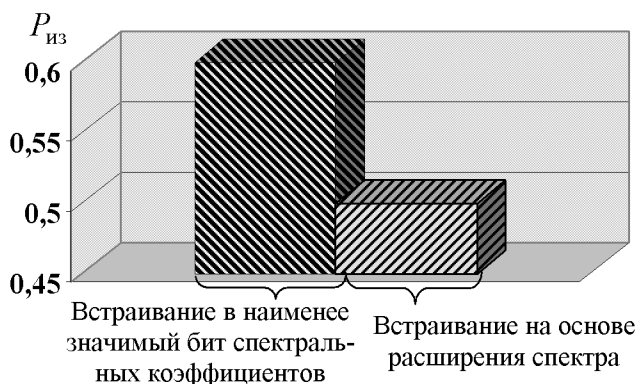


Рис. 2.10. Диаграмма значений вероятности $P_{из}$ для методов НЗБ в режиме 2, РС при условиях отсутствия атак на встроенное сообщение

Для метода НЗБ в режиме 2 и РС количество $w_{из}^{(Z_{cmp} Z_{стб})}$ безошибочно изъятых бит в условиях активных атак может достигать значения до 50%.

На рис. 2.11 представлена диаграмма процентного значения количества безошибочно изъятых бит для методов НЗБ в режиме 2, РС в условиях применения атаки ДКП и квантования с шагом $q = 1; 5$.

Из анализа рис. 2.11 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%.

Из анализа результатов исследований существующих стеганографических систем можно сделать вывод, что методы непосредственного стеганографического встраивания имеют проблемные недостатки относительно значения стеганогра-

фической емкости, пикового отношения сигнал-шум и вероятности безошибочного изъятия встроенных данных.

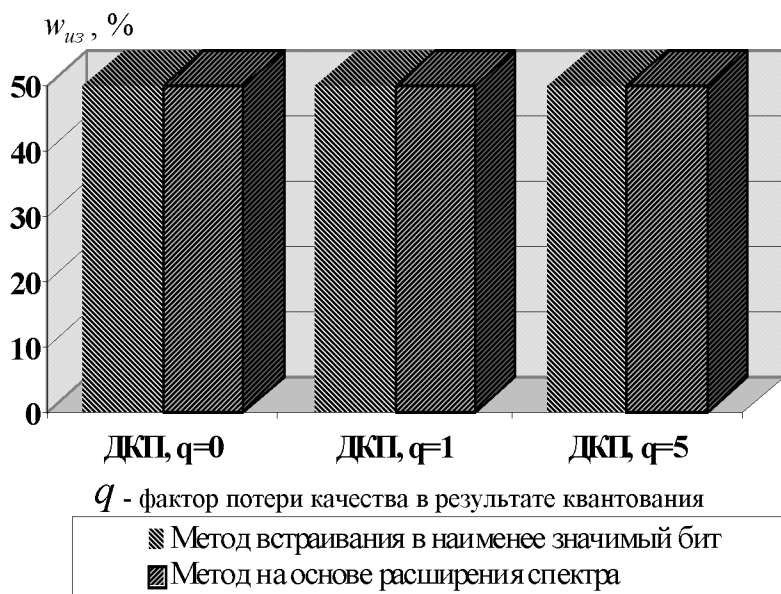


Рис. 2.11. Сравнительная диаграмма величины w_{uz} для методов НЗБ и РС в условиях атак злоумышленника в зависимости от различных значений шага квантования

Значит, существующие методы стеганографических преобразований не обеспечивают в полной мере системных требований по обеспечению информационной безопасности в кризисных ситуациях с активным противостоянием противника.

2.5. АСПЕКТЫ ИССЛЕДОВАНИЙ

Удовлетворение требований к информационному обеспечению кризисных систем связано с повышением эффективно-

сти функционирования существующих стеганографических методов для скрытой передачи специальных информационных ресурсов. В этом случае для существующих стеганографических преобразований выдвигаются следующие требования:

1. Необходимость повышения относительной стеганографической емкости $w_{отн}$ методов встраивания информации. Данное требование диктуется постоянным ростом объемов и увеличением содержательной значимости специальной информации и

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

3. Необходимость увеличения фактора визуальной устойчивости стеганограммы. Для обеспечения стойкости изображения со встроенными данными к визуальным атакам, направленным на установление факта наличия стеганографического встраивания. Данные требования диктуются наличием множества уязвимостей в процессе функционирования кризисных систем [5, 11, 12, 57, 73, 119, 123], а именно:

- использование беспроводных технологий с расширенными возможностями относительно предоставляемых видеослуг;

- развитие информационно-математического и программно-аппаратного обеспечения у злоумышленника включая ме-

тоды стегоанализа, быстроедействия вычислительных комплексов, новейших технологий распределения вычислений.

В тоже время повышаются требования к информационному обеспечению при обмене специальной информацией в кризисных системах. Такие требования обусловлены следующими факторами:

- повышение информационной интенсивности специальных донесений и распоряжений в условиях кризисных ситуаций;

- использование видеоматериалов в качестве донесений для принятия решений;

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

- повышение значимости влияния донесений на результативность функционирования кризисных систем, т.е. от достоверности, целостности и оперативности доведения донесений зависят человеческие жизни, 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 для информационного и информационно-психологического противостояния.

Значит, в процессе использования существующих стеганографических методов для скрытой передачи специальной информации возникает *противоречие* (рис 2.12), которое за-

ключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере новых системных требований в кризисных условиях при наличии дестабилизирующих факторов и противоборствующих сторон.

Для совершенствования существующих и разработки новых методов стеганографических преобразований необходимо использовать *принципиально новые подходы*, которые должны базироваться на современных и перспективных достижениях в области теории информации, кодирования, теории обработки цифровых видеопространств, технологий интеллектуального анализа и методов криптографии. Одним из актуальных направлений является использование структурных преобразований элементов пространственного представления изображения для выявления структурно-комбинаторной избыточности. Такой подход позволит повысить стойкость встроенных данных к активным атакам противника.

Отсюда, *направление исследования* заключается в разработке теоретических основ и методов повышения безопасности специальной информации на основе стеганографического преобразования, задаваемого функционалом $F\{P_{из}, w_{отн}, h\}$ в условиях выполнения следующих ограничений:

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



Рис. 2.12. Структура наличия противоречия при использовании существующих стеганографических методов для обеспечения функционирования кризисных систем

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

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

$h^{(mp)}$ - 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 структурно-комбинаторного стеганографического кодирования для повышения безопасности специальной информации;
- создать метод для локализации структурной стеганографической избыточности для повышения устойчивости относительно атак на выявление факта встроенной информации;
- построить систему встраивания информации с маскированием стеганографической избыточности.

Выводы

1. Систематизированы существующие технологии и методы косвенного и непосредственного стеганографического встраивания на основе использования видеоресурса в качестве контейнера. Для большинства стеганографических подходов косвенного встраивания характерна необходимость использования на приемной стороне прототипов изображения-

контейнера для изъятия встроенной информации. В данной работе для дальнейшего исследования выбраны методы непосредственного стеганографического встраивания.

2. Разработан вариант классификация методов непосредственного встраивания, который позволит обозначить место разрабатываемого метода стеганографического кодирования среди существующих подходов для непосредственного встраивания. Данная классификация дает возможность описать стеганографический метод с позиции:

- мерности пространства встраивания;
- выбора техники непосредственного встраивания;
- виды учитываемых закономерностей при встраивании информации;
- формы описания контейнера в процессе непосредственного встраивания;
- техники изъятия встроенной информации.

Создан классификатор для описания методов на основе предложенной классификации. Данный классификатор используется для позиционирования новых разрабатываемых методов относительно существующих.

3. Для оценки эффективности методов стеганографических преобразований с позиции обеспечения информационной безопасности разработана четырехуровневая система показателей, а именно:

- группа показателей, на основе которых проводится оценка стеганографических методов с позиции стойкости к атакам, направленным на выявления факта наличия скрытного встраивания;

- группа показателей, которые характеризует метод стеганографического преобразования с позиции объема встраиваемых данных;

- группа показателей, характеризующих стеганографический метод с позиции временных затрат на реализацию прямого и обратного стеганографического преобразования;

- группа показателей, которые используются для оценки стеганографических методов с позиции стойкости к атакам злоумышленника.

Разработана новая группа показателей для учета влияние стеганографического встраивания на показатели эффективности компрессионных представлений изображения-контейнера. Такие показатели характеризуют стеганографический метод с позиции изменения характеристик эффективности компрессионных показателей изображения со встроенными данными

4. На основе проведенной оценки методов непосредственного встраивания по относительной стеганографической емкости, вероятности безошибочного изъятия встроенных данных и пиковому отношению сигнал-шум изображения со встроенными данными получены следующие результаты:

- 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 может достигать значения 0,5

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

5. Сформулировано противоречие в процессе функционирования стеганографических методов, которое заключается в том, что существующие технологии стеганографических преобразований не обеспечивают в полной мере системных требований в кризисных условиях с активным противодействием противоборствующих сторон.

6. Обосновано направление для разработки метода встраивания, которое основывается на структурных преобразованиях элементов для выявления структурно-комбинаторной избыточности изображений. Сформулировано направление исследований, которое заключается в разработке метода повышения безопасности специальной информации на основе стеганографического преобразования для систем кризисного назначения.

Раздел 3

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ ТЕХНОЛОГИЙ НЕПОСРЕДСТВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

В разделе рассматриваются системные ограничения для существующих методов непосредственного встраивания. Проводится обобщение недостатков, характерных для стеганографических преобразований для различных позиционных вариантов модификации бит элементов изображения-контейнера.

Предлагается направление для устранения выявленных недостатков, которое заключается в использовании функционального преобразования для числа со встроенным элементом скрываемого сообщения. Формулируются требования к синтезированному функциональному преобразованию и формируется система свойства для разрабатываемого метода стеганографического преобразования.

Разрабатывается технология для функционального преобразования чисел с имплантированными данными. Предлагается в качестве такого функционала использовать кодообразующую функцию для неравновесного позиционного числа. Описываются этапы прямого и обратного стеганографического преобразования на основе неравновесного позиционного кодирования.

3.1. ОБОСНОВАНИЕ ПРОБЛЕМНЫХ СТОРОН ФУНКЦИОНИРОВАНИЯ ТЕХНОЛОГИЙ НЕПОСРЕДСТВЕННОГО ВСТРАИВАНИЯ

Для обоснования направления совершенствования существующих технологий непосредственного встраивания более подробно рассмотрим ограничения при использовании существующих методов. В качестве примера предлагается исследовать алгоритмы непосредственной замены бит элементов представления изображения-контейнера на биты скрываемого сообщения.

Непосредственное встраивание скрываемого сообщения может осуществляться как в пространственно-временную, так и в пространственно-частотную область изображения-контейнера [8, 53, 82, 90, 86, 92, 116]. Как правило, такое встраивание проводится в отдельный элемент текущего представления изображения-контейнера (рис. 3.1), точнее в отдельные биты элемента. В данном случае элемент представляет собой двоичное позиционное число A_2 с основанием равным двум, т.е. $A_2 = [A]_2$.

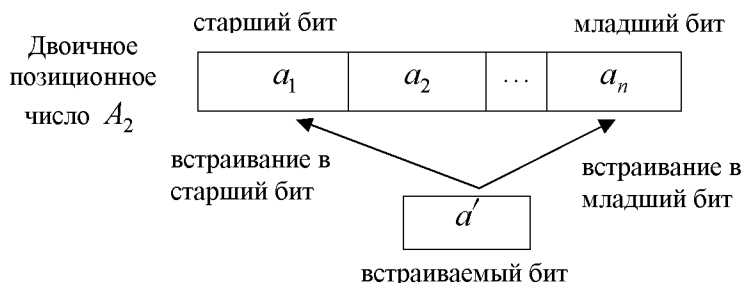


Рис. 3.1. Схема встраивания бита скрываемого сообщения в элемент текущего представления изображения-контейнера

Как пример, в качестве такого элемента может использоваться пиксель пространственно-временного представления изображения или компонента его спектрального представления. В этих случаях элемент, в который осуществляется встраивание бита (группы бит) скрываемого сообщения, 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_c , условия или правила.

В существующих стеганографических методах наиболее проработанные подходы основываются на встраивании информации в наименее значимые младшие (НЗБ) биты. В связи с чем, рассмотрим характеристики таких стеганосистем.

Метод встраивания в наименее значимый бит осуществляет замену младшего бита a_n двоичного позиционного числа A_2 на бит b_ξ встраиваемого сообщения B (рис 3.1). Это описывается следующим выражением:

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

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

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

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:

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

В тоже время данный принцип встраивания отличается низкой устойчивостью стеганографически преобразованного изображения 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.

$$P_{из}(b'_{\xi} = b_{\xi}) \rightarrow 0$$

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

$$\overline{P}_{из}(b'_{\xi} \neq b_{\xi}) \rightarrow 1.$$

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

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

Здесь B_2 , B'_2 - двоичное представление сообщения соответственно до и после встраивания.

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

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

повышает стойкость встроенных данных к трансформации и атакам. Тогда вероятность $P_{из}(b'_\xi = b_\xi)$ того, что элемент b_ξ скрываемого сообщения изъят без ошибок, будет наибольшей, т.е.

$$P_{из}(b'_\xi = b_\xi) \rightarrow 1 ,$$

а вероятность $\overline{P}_{из}(b'_\xi \neq b_\xi)$ того, что элемент b_ξ скрываемого сообщения изъят с ошибкой будет наименьшей

$$\overline{P}_{из}(b'_\xi \neq b_\xi) \rightarrow 0.$$

Здесь A'_2 - число-стеганограмма, содержащее встроенный бит a'_1 скрываемого сообщения, b_ξ - ξ -й элемент встраиваемой двоичной последовательности $B_2 = \{b_1; \dots; b_\xi; \dots; b_\nu\}$, $a'_i \in [0; 1]$; $b_\xi \in [0; 1]$; $i = \overline{1, n}$; $\xi = \overline{1, \nu}$; 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 наибольшим, т.е.

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

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

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

При встраивании бита скрываемого сообщения в старший бит исходного числа наблюдается стойкость встроенных данных при значительных визуальных искажениях. И, наоборот,

встраивание в младший бит характеризуется низкой стойкостью встроенных данных при минимальных визуальных искажениях.

3.2. 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.

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

и устойчивости к трансформации и атакам предлагается синтезировать функционал $f(A')$ от *числа* со встроенной информацией [9, 10, 17, 94, 97]. Такой функционал должен обеспечить следующие требования:

1) взаимнооднозначность прямого $f(A')$ и обратного $f^{(-1)}(C)$ преобразований. В этом случае должен существовать обратный функционал $f^{(-1)}(C)$, позволяющий авторизованному 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 неавторизованным пользователем (злоумышленником), а восстановление изображения осуществляется для стандартных условий $\Psi^{(1)}$, необходимых для достоверной 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.

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

- осуществляется блокировка возможности успешного стеганоанализа и изъятия сообщения.

Условия блокирования изъятия встроенного сообщения задается следующим соотношением

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

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

Второй вариант наоборот, существует для авторизованного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием ключа $\Psi^{(2)}$ или по определенному условию известному авторизованным 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 изображения до встраивания информации (изображением-контейнером) и числом $A(2)''$ соответствующим изображению со встроенной информацией (стеганограммой) принимала наименьшее значение, т.е.

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

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 авторизованным пользователем количественная метрика $\delta(B'_2; B_2)$, указывающая на степень отличия между исходным встраиваемым сообщением B и изъятим на приемной стороне сообщением B' , будет принимать нулевое значение:

$$\delta(B'_2; B_2) = 0.$$

Требование биполярности можно обобщить следующей системой выражений:

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

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

3) функциональное преобразование должно быть инвариантным к атакующим воздействиям (ошибки в канале связи, компрессионные атаки 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-контейнер) и числом A'' соответствующего изображению со встроенной информацией при наличии атакующего воздействия должна быть наименьшей:

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

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 [19, 89, 91]:

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' формиру-

ется 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

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

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 $\Psi^{(1)}$ неавторизованным пользователем

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

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

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

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

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

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. В этом случае стеганограмма определяется на основе следующего выражения:

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

где C_2 - кодовое представление стеганограммы C_2 .

Тогда для реконструкции элементов $A(1)''$ используется формула:

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

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 проис-

ходило встраивание скрываемого сообщения или же принимать значение некоторого симметричного ключа $\Psi^{(2)}$ известного на приемной и передающей 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, чтобы безошибочная реконструкция исходного изображения $A(1)'$ для неавторизованного 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. 3.2. представлена схема стеганографического преобразования на основе использования функционала для числа со встроенными данными [20, 21, 22, 87].

Прямое стеганографическое преобразование включает следующие этапы:

1. Встраивание b_ξ скрываемого сообщения B_2 в число A при помощи оператора встраивания φ . Полученное

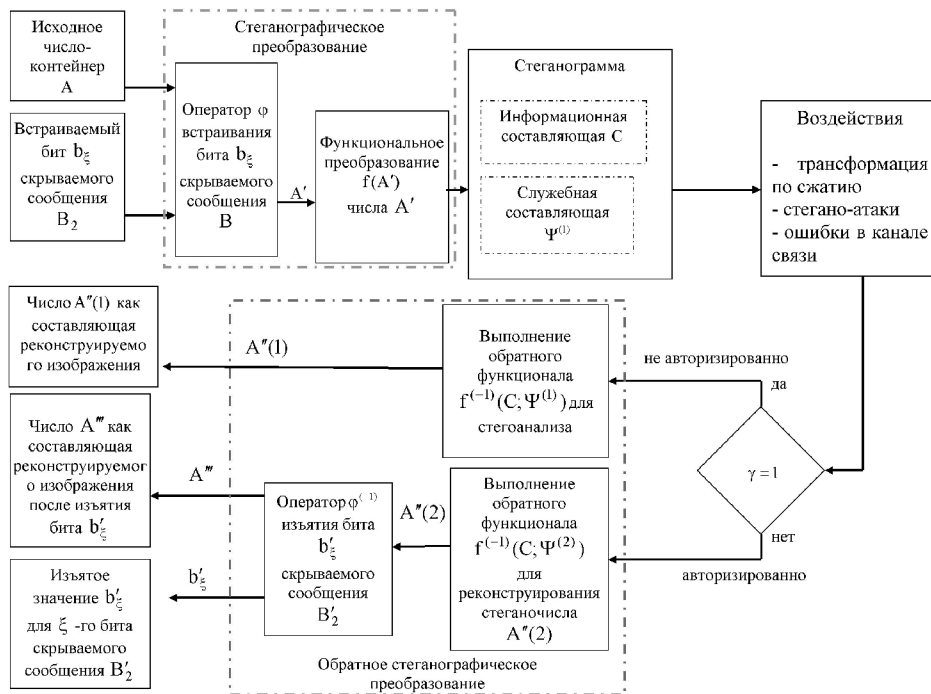


Рис 3.2. Схема стеганографического преобразования на основе использования функционала для числа со встроенными данными

в результате встраивания число A' определяется на основе следующего выражения

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

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

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

Обратное стеганографическое преобразование осуществляется по биполярному принципу для авторизованного и неавторизованного пользователя (стеганографический анализ).

При стеганографическом анализе, 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

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

На основе предложенной технологии необходимо разработать подход, который заключается в использовании стеганографического преобразования чисел с имплантированными данными.

3.3. 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 [13, 23, 84, 85, 93].

В процессе неравновесного позиционного кодирования формируются кодовые комбинации, состоящие из двух частей, а именно: информационная составляющая N и служебная составляющие Ψ (рис. 3.3).

В этом случае исходный элемент изображения рассматривается как неравновесное позиционное числа A , состоящее из m элементов [16], а именно

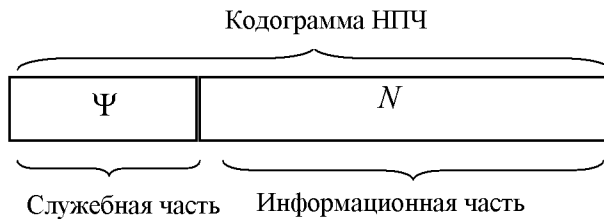


Рис. 3.3. Схема кодограммы для неравновесного позиционного числа

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

Для исходного НП числа (рис 3.4) 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 .

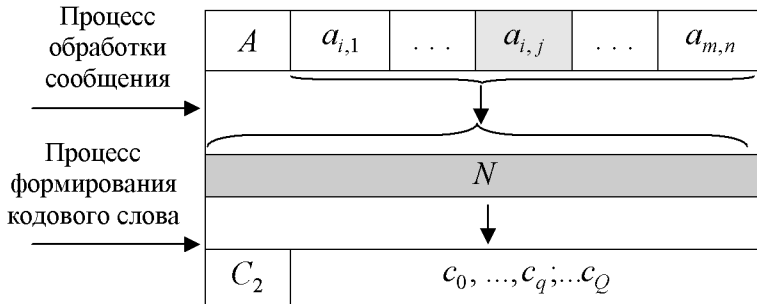


Рис. 3.4. Структурная схема построения кодовых конструкций для неравновесного позиционного числа A

В этом случае получим

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

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 3.5) [12, 21, 25].

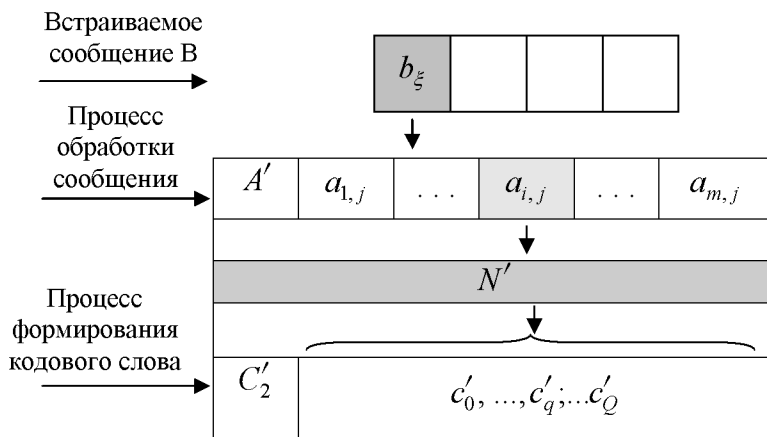


Рис.3.5. Структурная схема построения кодовых конструкций НП числа A' со встроенными данными

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

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

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

После чего, 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 .

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

Первый способ используется неавторизованным 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 метрики $\varepsilon(A; A(1)'')$ было наименьшим

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

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

Второй способ существует для авторизованного 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 авторизованному пользователю безошибочно реконструировать число со встроенными данными, т.е.:

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

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

Изъятие встроенной информации происходит без внесения ошибок вследствие применения оператора изъятия $\phi_c'^{(1)}$ к реконструируемому неравновесному позиционному 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. 3.6. представлена схема стеганографического метода на основе неравновесного позиционного кодирования [13, 88]. Прямое стеганографическое преобразование реализуется в три этапа [15, 20]. 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' , а именно:

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

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:

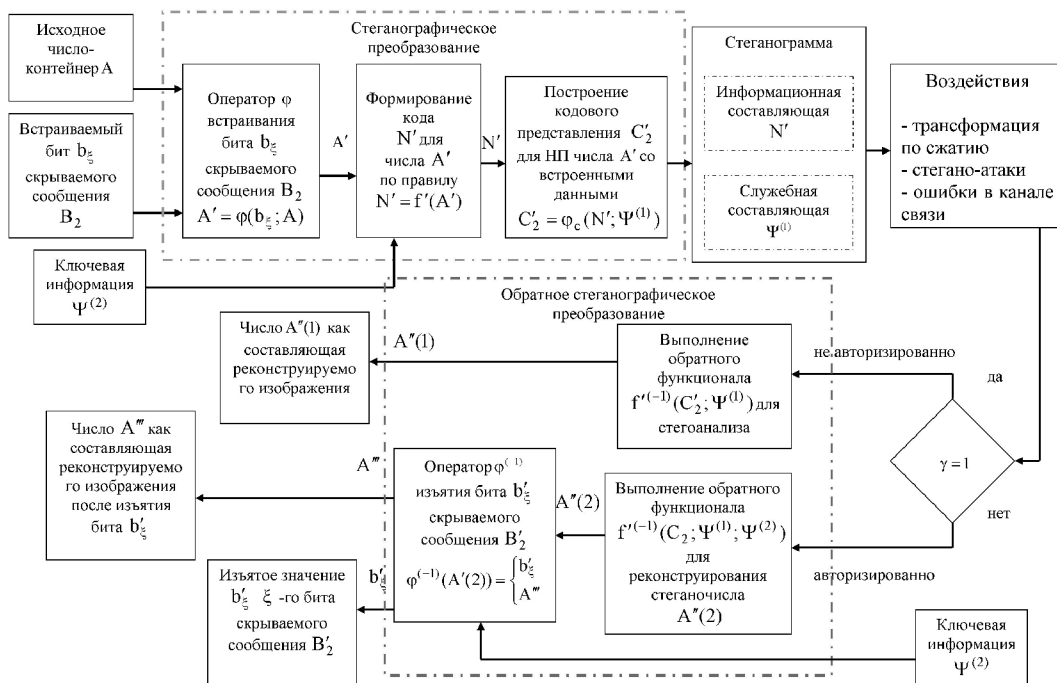


Рис 3.6. Схема стеганографического преобразования на основе неравновесного позиционного кодирования

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

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 неавторизованного пользователя (стеганографический анализ) при условии, что ему известен обратный функционал $f'^{(-1)}$, и авторизованного пользователя. При стеганографическом анализе, по правилу $f'^{(-1)}(\bullet)$ формируется число, записываемое как:

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

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. Это задается таким соотношением:

$$A''(2) = f'^{(-1)}(C'_2; \Psi^{(1)}; \Psi^{(2)}).$$

На втором этапе из реконструированного числа $A''(2)$ происходит изъятие b'_ξ скрываемого сообщения B_2 . В результате применения оператора изъятия $\phi'^{(1)}$ также происходит

реконструкция числа A'' , как составляющего исходного изображения, что описывается выражением

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

Таким образом, разработан подход для проектирования стенографической системы основанный на использовании функционального преобразования для чисел со встроенной информацией.

Выводы

1. Сформулированы ограничения при использовании существующих технологий непосредственного стеганографического встраивания по показателям стойкости и визуальной заметности. Выявлено противоречие между стойкостью встроенных данных и визуальной устойчивостью стеганограммы при встраивании на различные позиции элемента изображения-контейнера. Для устранения такого противоречия предлагается направление, которое заключается в использовании функционального преобразования элемента со встроенными данными в соответствии с синтезированным функционалом.

2. Определены требования к функциональному преобразованию для числа со встроенными данными, а именно:

- должна обеспечиваться взаимоднозначность прямого и обратного функционального преобразований, т.е. должен существовать обратный функционал, позволяющий авторизиро-

ванному 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 авторизованного пользователя и для злоумышленника. Для неавторизованного пользователя восстановление изображения происходит при стандартных условиях, при котором блокируется возможность изъятия встроенного сообщения. Для авторизованного 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, должна обеспечиваться устойчивость встроенных данных к атакующим преобразованиям, а именно компрессионным атакам и воздействиям ошибок в канале связи.

3. Сформулированы свойства, которыми должно обладать функциональное преобразование. 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 предусматривается формирование кодового значения числа со встроенными данными в результате применения функционального преобразования. 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 авторизованного пользователя и реконструированными элементами при неавторизованном доступе не должна превышать порога визуальной незначимости;

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

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

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

4. Обоснован подход совершенствования существующих технологий непосредственного встраивания на основе неравновесного позиционного кодирования. Такой подход предусматривает использование неравновесного позиционного числа в качестве элемента-контейнера, а в качестве функционального преобразования - кодообразующую функции для НПЧ. Данная технология позволяет встраивать бит скрываемого сообщения в исходное неравновесное позиционное число. В результате применения прямого функционального преобразования для исходного числа со встроенной информацией формируется результирующее кодовое представление. Обратное функциональное преобразование будет осуществляться для злоумышленника и для авторизованного пользователя.

При первом способе реконструкция элемента исходного изображения реализуется неавторизованным 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 4

**РАЗРАБОТКА МЕТОДА
СТРУКТУРНО-КОМБИНАТОРНОГО
СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ**

В разделе рассматривается подход для проектирования стеганографической системы, который основан на возможности использования структурно-комбинаторных закономерностей изображения. Предложено использовать кодообразующую функцию для неравновесного позиционного числа.

Разрабатывается концепция стеганографического кодирования неравновесного числа с имплантированным элементом.

Проводится обоснование появления структурной стеганографической избыточности в процессе стеганографического кодирования.

Создается стеганографическая система с маскированием структурной стеганографической избыточности.

Излагаются основные этапы построения структурно-комбинаторного демаскирующего декодирования.

4.1. РАЗРАБОТКА МОДЕЛИ СТРУКТУРНО-КОМБИНАТОРНОГО СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ

Для проектирования стеганосистемы предлагается использовать наличие в изображении-контейнере структурно-комбинаторных закономерностей, обусловленных наличием ограничений на динамический диапазон [10, 11, 15].

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 A представлена на рис. 4.1.

Для удовлетворения требования учета ограничения на динамический диапазон в процессе представления и кодирования предлагается использовать неравновесное представление. [10, 11, 15]. Поэтому предлагается проектировать стеганосистему на основе кодообразующего функционала с учетом неравновесного позиционного базиса [13, 15, 17-19, 21, 22].

В качестве кодообразующего функционального преобразования предлагается использовать кодообразующую функцию для неравновесного позиционного числа. Такая функция обладает свойствами для соответствия требованиям относительно процесса скрытия данных, а именно [10, 15]:

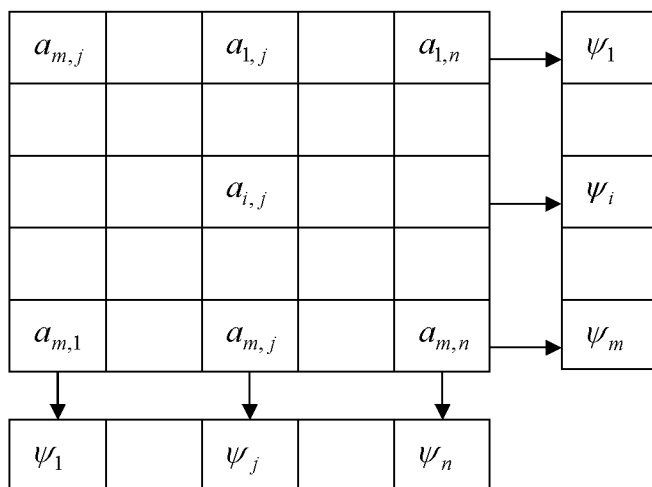


Рис. 4.1. Схема формирования базиса динамических диапазонов для изображения-контейнера A.

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

$$N = f(A'_{cu}).$$

На основе сформированного значения кода N на втором этапе строится результирующее кодовое представление C_2 стеганограммы. Это определяется таким выражением:

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

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 соответствует неавторизированным пользователям. Восстановление изображения происходит при наличии открытой служебной информации $\Psi^{(1)}$, представляющей собой систему неравновесных позиционных базисов оснований числа $A'_{\text{он}}$ 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, чтобы $\Psi^{(2)} \neq \Psi^{(1)}$.

3) стеганограмма C , содержит сведения о векторе служебной информации $\Psi^{(1)}$, при наличии которого возможна реконструкция элементов стеганографического изображения $A(1)''$ при отсутствии информации о наличии встроенного сообщения. Данное свойство задается следующим выражением:

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

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]. Здесь неравновесное позиционное число $A(j)$ без имплантации для j -го столбца массива видеоизображения состоит из m элементов, т.е.

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

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

$$N(j) = f(A(j), V^{(1)}), \quad (4.1)$$

где $V^{(1)}$ - система весовых коэффициентов неравновесного позиционного 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, содер-

жащееся в $(m-i)$ элементах НП числа при выполнении события, 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 неравновесного позиционного числа $A(j)$;

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

В этом случае получим следующую кодограмму:

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

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

$$a_{i,j} = f^{(-1)}(N(j), V_{i,j}, \Psi_{i,j}), \quad (4.2)$$

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

На рис. 4.2. графически отображены этапы формирования кодограммы $C(A(j))$ для кода-контейнера $N(j)$ неравновесного позиционного числа $A(j)$ (прямого неравновесного позиционного преобразования) и его декомпозиции (обратного неравновесного позиционного преобразования).

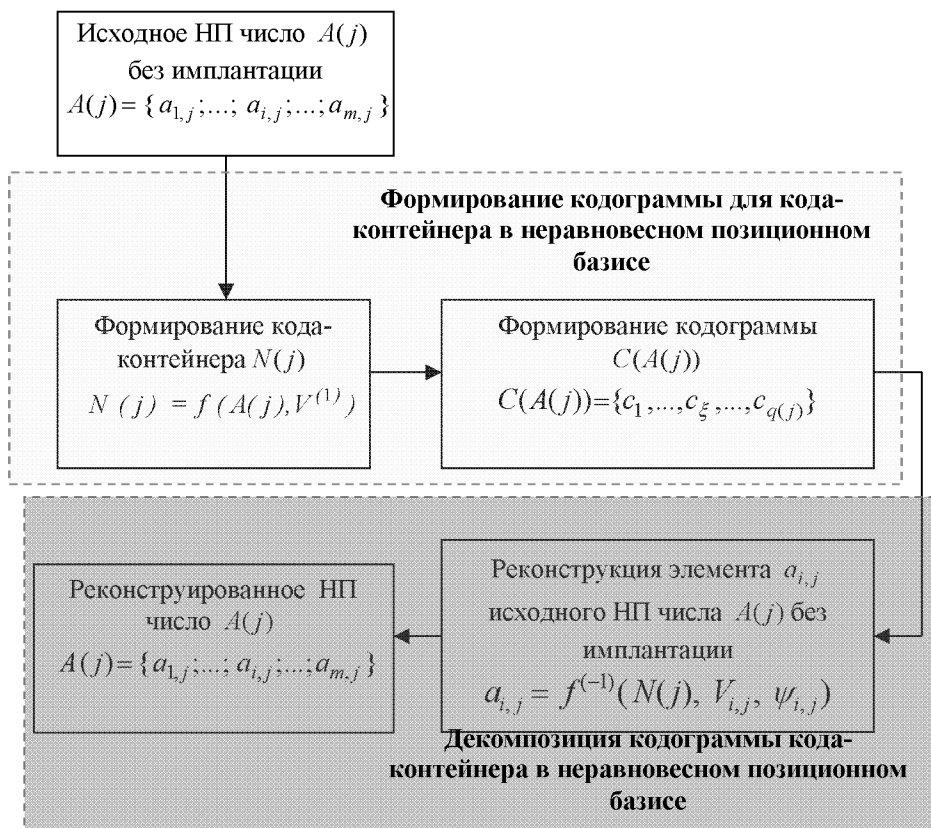


Рис. 4.2. Схема стеганографической системы на основе формирования кода-контейнера в неравновесном позиционном базисе.

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 $\Psi^{(1)} = \{\psi_{i,j}\}$ (рис. 4.3).

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

Рис. 4.3. Структура неравновесного базиса оснований.

Такой подход при формировании базиса оснований для неравновесного позиционного числа позволяет выявить структурно-комбинаторные закономерности на динамический диапазон [10, 13, 15]. Это создает потенциал для установления количества структурно-комбинаторной 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 структурно-комбинаторной 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 фиксированным 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 $N(j)$ неравновесного позиционного 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 на-

копленным произведением $V_{\max}$ оснований элементов неравновесного позиционного числа. Это задается следующим выражением:

$$N(j) \leq V_{\max} = f_{\text{осн}}(\Psi^{(1)}) + 1.$$

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]:

$$q(j) = |C(A(j))| = \lceil \log_2(f_{\text{осн}}(\Psi^{(1)})) \rceil + 1 \text{ (бит)}.$$

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 $R(j)$ структурно-комбинаторной избыточности вычисляется как разность между количеством бит $q(j)$ для двоичного представления кодограммы $C(A(j))$ и количеством бит $q(j)_{\text{исх}}$, необходимых для

двоичного представления числа $A(j)$ исходной видеопоследовательности и описывается выражением

$$R(j) = q(j)_{исх} - q(j) .$$

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

4.2. РАЗРАБОТКА КОНЦЕПЦИИ СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ НЕРАВНОВЕСНОГО ЧИСЛА С ИМПЛАНТИРОВАННЫМ ЭЛЕМЕНТОМ

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

Имплантиацию 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 последова-

тельности $B = \{b_1; \dots; b_\xi; \dots; b_\nu\}$, $b_\xi \in [0; 255]$, $\xi = \overline{1, \nu}$. В этом случае имплантация задается следующей формулой:

$$A(j)' = A(j) \cup b_\xi, \text{ в случае когда } b_\xi = a'_{\gamma,j}. \quad (4.3)$$

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

$$A(j)' = \{a_{1,j}; \dots; a'_{\gamma,j}; \dots; a_{i,j}; \dots; a_{m+1,j}\}, \quad (4.4)$$

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 **стеганокodem**.

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

Определение. Формирование стеганокodem на основе кодирования неравновесного позиционного числа с импланти-

рованным элементом скрываемого сообщения называется **структурно-комбинаторным стеганографическим кодированием в неравновесном позиционном базисе**.

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

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) . \quad (4.5)$$

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

В случае такого встраивания фрагмент исходной видео-последовательности рассматривается, как позиционное число $A(j)' = \{a_{1,j}; \dots; a'_{\gamma,j}; \dots; a_{i,j}; \dots; a_{m+1,j}\}$ 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 $N(j)'$:

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

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

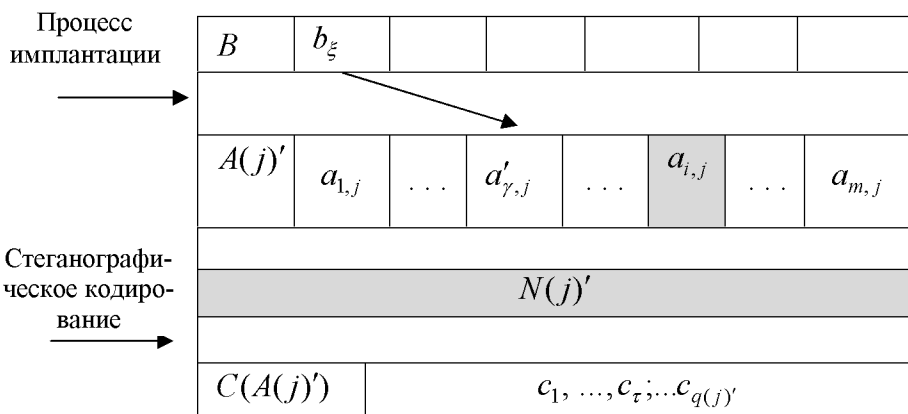


Рис. 4.4. Структурная схема построения кодограммы стеганокода для числа $A'(j)$ с имплантацией

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.

4.3. 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:

$$q(j)' = |N(j)'|_2 = [\log_2 \psi'_{\gamma,j} + \log_2 (f_{осн}(\Psi^{(1)}))] + 1 \text{ (бит)}, \quad (4.6)$$

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:

$$q(j) = |C(A(j))| = [\log_2 (f_{осн}(\Psi^{(1)}))] + 1 \text{ (бит)}. \quad (4.7)$$

Из сравнения выражений (4.9) и (4.10) 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:

$$q(j)' - q(j) = \log_2 \psi_{\gamma,j}. \quad (4.8)$$

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 коде-контейнере), 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 $R(j)_{\text{стег}}$ 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.

$$R(j)_{\text{стег}} = q(j)' - q(j) \geq 0. \quad (4.9)$$

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

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

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

$$R(j)_{\text{ост}} = q(j)_{\text{исх}} - q'(j). \quad (4.10)$$

Графически это можно отобразить, как показано на рис 4.5.

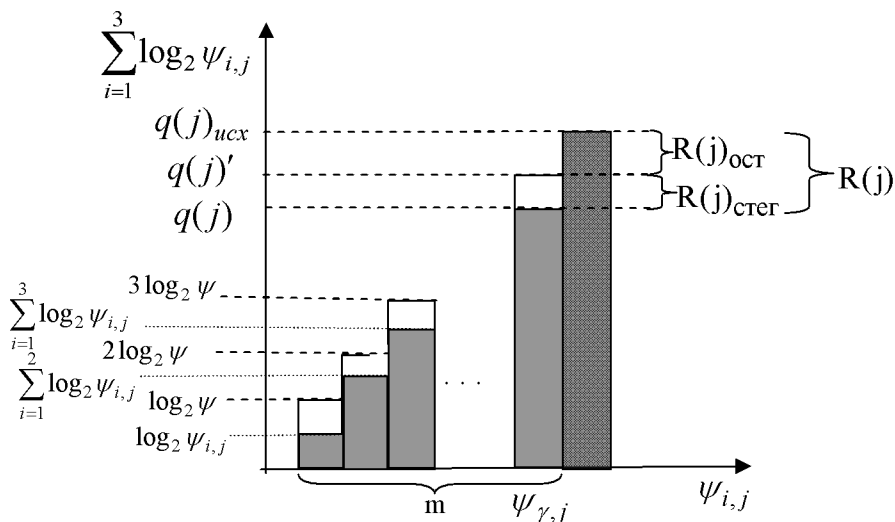


Рис. 4.5. Графическая интерпретация стеганографической избыточности

Очевидно, что возможность встраивания информации в условиях обеспечения ее скрытности будет осуществляться в случае, когда количество структурно-комбинаторной избыточности не будет равно нулю, т.е.

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

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, неавторизованный пользователь име-

ет доступ к базису оснований $\Psi^{(1)}$, на основе которого сформирован стеганокод $N(j)'$. В направлении выявления факта встраивания информации, неавторизованный 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.

$$q(j) = [\log_2 (f_{осн}(\Psi^{(1)}))] + 1 .$$

2. Это позволяет установить предполагаемую длину информационной части текущей кодограммы. В результате чего будет считано значение кода $N(j)''$. Однако, в действительности передается стеганокод $N(j)'$ 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 изъятый

будет восприниматься как первые биты служебной части следующей кодограммы $N(j)''$ (рис 4.6).

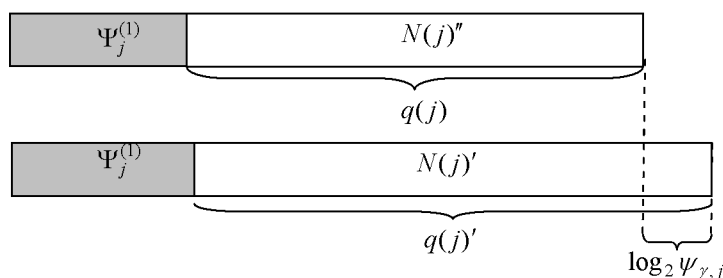


Рис 4.6. Кодограммы для ошибочно изъятых стеганокда $N(j)''$ и стеганокда $N(j)'$

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

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

В этом случае вместо того чтобы отобрать $q(j)'$ бит, неавторизованный 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 стеганокда и кода-контейнера на процесс восстановления элементов исходной видеопоследовательности. Рассмотрим реконструкцию i -го элемента j -й видеопоследовательности. Для этого используем выражение:

$$a_{i,j}'' = f^{(-1)}(N(j)''_i, V_{i,j}, \psi_{i,j}), \quad (4.11)$$

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.

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

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 называть 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 (4.9) 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 $R(j)_{срег}$ в процессе стеганографического кодирования должно выполняться условие:

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

Поэтому для уменьшения уровня искажений стеганокода предлагается встраивать элементы в двоичном представлении, т.е. $b_{\xi} \in [0; 1]$. В этом случае основание встроеного 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:

$$q(j)' = [\log_2 \psi'_{\gamma,j} + \log_2 (f_{осн}(\Psi^{(1)}))] + 1 \text{ (бит)}.$$

Тогда в соответствии с выражением (4.10) можно сделать вывод, что имплантация бита в число $A(j)$ увеличивает длину кодового представления стеганокода относительно кода-контейнера на один бит. Количество $R(j)_{\text{стег}}$ 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:

$$C_j''' = [N(j)''']_2 = [N(j)' / 2]_2. \quad (4.12)$$

Такой вариант локализации стеганографической избыточности заключается в использовании свойств устойчивости структурных характеристик и структурно-комбинаторной 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:

$$q(j)'' = [(\log_2 \psi'_{\gamma,j} + \log_2 (f_{\text{осн}}(\Psi^{(1)}))) / 2] + 1 = q(j).$$

Как показывает анализ выражения (4.12) искажения в значение стеганокода все равно будут вноситься. Причем наи-

большим 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:

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

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

$$B = \{b_1; \dots; b_{\xi}; \dots; b_{\nu}\}; \quad b_{\xi} \in [0; 1], \quad \xi = \overline{1, \nu};$$

$(m+1)$ - 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.

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

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

На рис 4.7 схематично отображено образование минимальной структурно-комбинаторной стеганографической избыточности для кодограммы стеганокodem относительно кодограммы кода-контейнера при встраивании двоичного элемента на позицию старшего элемента неравновесного позиционного числа.

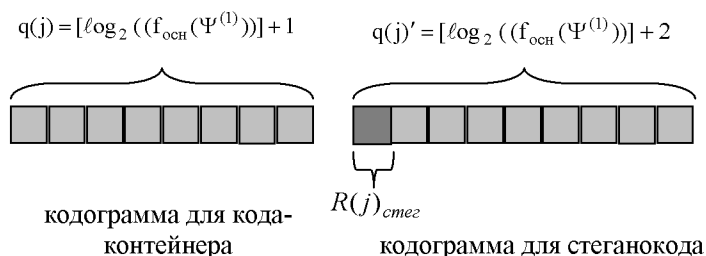


Рис 4.7. Кодограмма кода-контейнера и стеганокodem

Рассмотрим этапы функционирования стеганографической системы с маскированием стеганографической избыточности рис 4.8. 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 авторизованного и неавторизованного пользователя.

Стеганографическая система включает в себя следующие базовые составляющие:

1. Стеганографическое кодирование с маскированием структурной стеганографической избыточности.
2. Структурно-комбинаторное демаскирующее декодирование.

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

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

$$A(j)' = A(j) \cup b_\xi, \text{ для } b_\xi = a'_{1,j} \in [0, 1]. \quad (4.13)$$

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

$$A(j)' = \{ a'_{1,j}; \dots; a_{i,j}; \dots; a_{m+1,j} \}, \quad (4.14)$$

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:

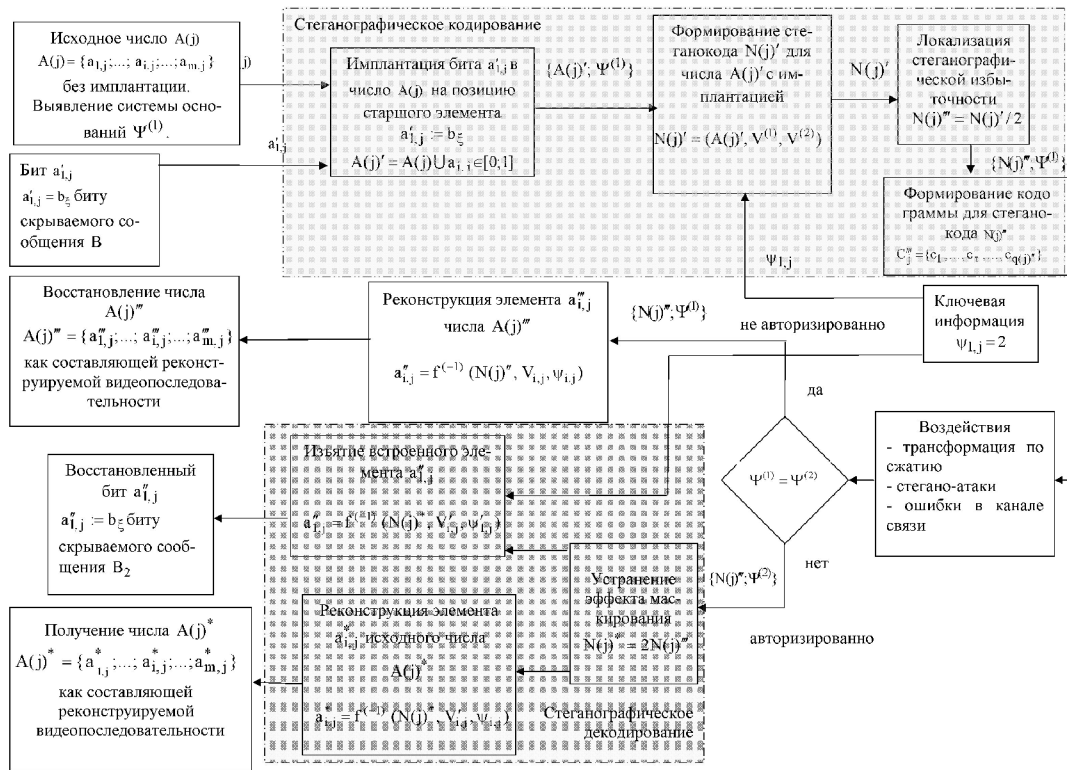


Рис. 4.8 Структурная схема стеганографической системы на основе имплантации скрываемого двоичного элемента на старшую позицию НПЧ с последующим кодированием и маскированием

$$N(j)' = (A(j)', V^{(1)}, V^{(2)}) . \quad (4.15)$$

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 $N(j)''$ этого используется следующее выражение:

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

На рис 4.9 схематически отображены этапы стеганографического кодирования.

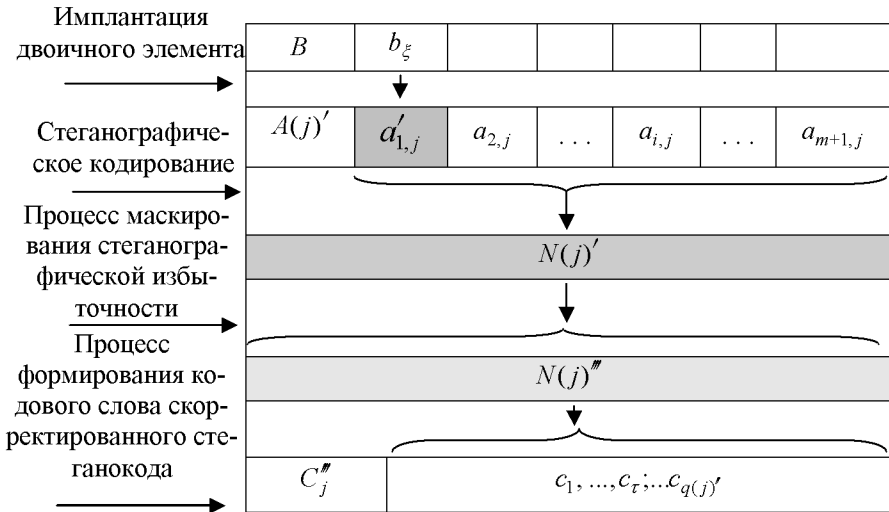


Рис 4.9. Структурная схема построения кодограммы скорректированного стеганокода для числа $A'(j)$ с имплантацией

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

$$C_j'' = \{c_1, \dots, c_\tau, \dots, c_{q(j)'}\},$$

где $q(j)''$ - длина кодограммы C_j'' , равная $q(j)'' = [(\log_2 \psi'_{\gamma,j} + \log_2 (f_{\text{осн}}(\Psi^{(1)}))) / 2] + 1$.

Теперь необходимо рассмотреть вторую базовую составляющую разработанной стеганографической системы - стеганографическое декодирование.

4.5 РАЗРАБОТКА СТРУКТУРНО-КОМБИНАТОРНОГО 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 *структурно-комбинаторным стеганографическим декодированием в неравновесном позиционном базисе*.

Процесс стеганографического декодирования в данном случае осуществляется по *биполяльному принципу* для авто-

ризованного пользователя и злоумышленника (неавторизованный пользователь) [13, 15, 17-19, 22].

В случае неавторизованного 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:

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

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

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

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

1) позиция стеганокода в сжатом представлении изображения;

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

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

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, равный нулю. Значение восстановленного стеганокода $N(j)^*$ определяется по формуле:

$$N(j)^* = N(j)'' / 2.$$

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 изъятых битов 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 авторизованном доступе.

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

- 1) изображение «Снимок аэропорта»;
- 2) изображение «Фотоснимок».

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 неавторизованного пользователя представлены соответственно на рис 4.10 и рис 4.11.

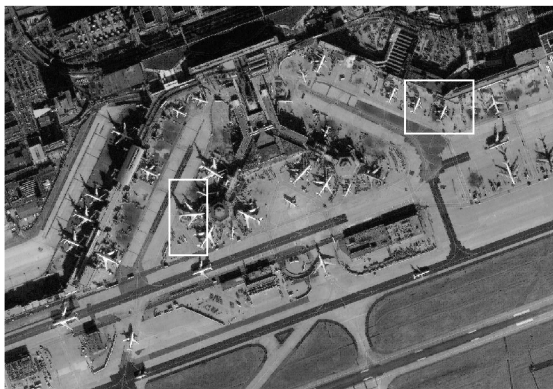


Рис 4.10. Изображение «Снимок аэропорта», декодированное злоумышленником.



Рис 4.11. Изображение «Фотоснимок», декодированное неавторизованным пользователем.

Из анализа изображений декодированных при неавторизованном доступе можно заключить что:

1. Изображения «Снимок аэропорта» и «Фотоснимок» содержат незначительные визуальные искажения, а именно: размытие краев, мозаичный эффект,

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. Неавторизованный пользователь при декодировании использует скорректированное значение стеганокода $N(j)''$.

Восстановление исходных значений изображения контейнера происходит с ошибками.

Реализация демаскирующего стеганографического декодирования для авторизованного пользователя рассматривается на примере реконструкции изображений «Снимок аэропорта» и «Фотоснимок» представленных соответственно на рис 4.12 и рис 4.13.

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

1. Вся встроенная информация изымается без ошибок.
2. Реконструированные изображения имеют незначительные визуальные искажений, которые вызваны коррекции длин при стеганорафическом декодировании.



Рис 4.12. Изображение «Снимок аэропорта» полученное в результате стеганографического декодирования для авторизованного пользователя.



Рис 4.13. Изображение «Фотоснимок» - полученное в результате стеганографического декодирования для авторизованного пользователя.

Коррекции 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», декодированных неавторизованным пользователем, соответственно на 24 дБ и 32 дБ.

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

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

2. Реконструированные изображения при неавторизованном доступе содержат незначительное количество визуальных коррекций.

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 авторизованном доступе, так и для неавторизованного 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 структурно-комбинаторного стеганографического кодирования и декодирования.

Первое базовое концептуальное отличие созданной стеганографической системы. Впервые спроектирована стеганографическая система на основе непосредственного встраивания скрываемого элемента в видеопоследовательность. В отличие 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 встраивание скрываемой информации на основе учета количества структурно-комбинаторной избыточности фрагментов видеоизображений.

2. Обосновано наличие структурно 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 структурно-комбинаторное 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.

Второе базовое концептуальное отличие созданной стеганографической системы. Впервые разработано структурно-комбинаторное стеганографическое 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 выявления злоумышленником факта наличия встроенной информации (локализовать атаку выявления факта наличия встроенной информации).

4. ***Создано правило*** встраивания информации для структурно-комбинаторного 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) структурно-комбинаторное стеганографическое декодирование, обеспечивающее восстановление неравновесного позиционного числа с имплантированным элементом;

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

Третье базовое концептуальное отличие созданной стеганографической системы. Впервые разработано демаскирующее стеганографическое декодирование. В отличие от существующих методов изъятие скрываемой информации и восстановления неравновесного позиционного числа проводится на основе реконструкции стеганокода по ***биполяльному 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 неавторизованном 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 5

ОЦЕНКА ХАРАКТЕРИСТИК ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ РАЗРАБОТАННОГО МЕТОДА СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ

В разделе рассматриваются вопросы, посвященные оценке эффективности функционирования разработанного метода структурно-комбинаторного стеганографического кодирования.

Строится оценка стеганографической системы по показателям объема встраиваемой информации для разработанного метода по величине относительной стеганографической емкости.

Разрабатывается метод оценки характеристик процесса скрытия встроенных сообщений. Для разработанного стеганографического метода проводится оценка характеристик процесса скрытия встроенных сообщений в случае неавторизованного доступа.

Излагается оценка эффективности процесса изъятия встроенной информации для разработанного метода при авторизованном доступе

На основе разработанного метода проводится оценка устойчивости скрываемых сообщений к атакам злоумышленника.

5.1. ОЦЕНКА СТЕГАНОГРАФИЧЕСКОЙ ЕМКОСТИ РАЗРАБОТАННОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

Разработанный метод стеганографического кодирования позволяет встраивать информацию в цифровое изображение-контейнер на основе структурно-комбинаторных особенностей [19, 20]. Этапу стеганографического кодирования предшествует имплантация данных скрываемого сообщения на позицию старшего элемента неравновесного позиционного числа $A(j)$ длиной m (рис 5.1).

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 $B = \{b_1; \dots; b_\xi; \dots; b_\nu\}$, $b_\xi \in [0; 255]$, $\xi = \overline{1, \nu}$.

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

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

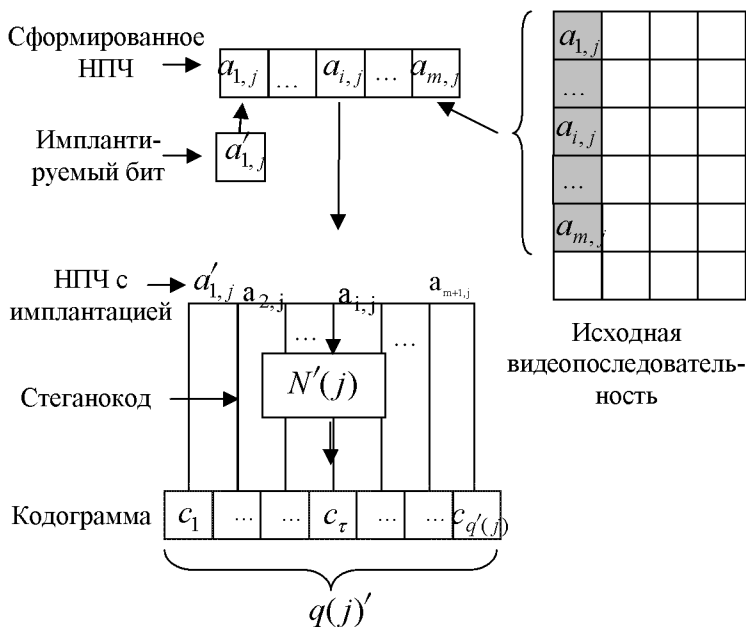


Рис. 5.1 Схема имплантации бита в неравновесное позиционное число

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:

$$w_{отн}^{(m)} = \frac{w_{встр}^{(m)}}{W_{исх}} = \frac{3 \cdot Z_{стр} Z_{стб}}{m \cdot W_{исх}},$$

где $Z_{стр} Z_{стб}$ - размер изображения-контейнера.

Физический смысл данной величины заключается в 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:

$$w_{отн}^{(m)} = \frac{w_{встр}^{(m)}}{W_{исх}} 100\% = \frac{3 \cdot Z_{стр} Z_{стб}}{m \cdot W_{исх}} \cdot 100\%. \quad (5.1)$$

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

$$w_{встр}^{(m)} = L = \frac{3 \cdot Z_{стр} Z_{стб}}{m}, \quad (5.2)$$

где L - количество сформированных неравновесных позиционных чисел.

Оценим объем $W_{исх}$ исходного изображения. Значение объема $W_{исх}$ исходного изображения будет равно произведе-

нию общего количества L сформированных неравновесных позиционных чисел по трем цветовым компонентам изображения-контейнера на количество бит $q(j)_{исх}$, необходимое для двоичного представления неравновесного позиционного числа длиной m элементов:

$$W_{исх} = L \cdot q(j)_{исх} \text{ (бит)}. \quad (5.3)$$

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

$$q(j)_{исх} = 8 \cdot m \text{ (бит)}. \quad (5.4)$$

Перепишем формулу (5.3) с учетом выражения (5.4):

$$W_{исх} = L \cdot m \cdot 8 \text{ (бит)}. \quad (5.5)$$

Теперь преобразуем формулу (5.5) учитывая выражения (5.2) и (5.5). В этом случае получим:

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

Диаграмма зависимости значения $w_{отн}^{(m)}$ относительной стеганографической емкости стеганографического алгоритма

от различной длины $m = 2; 3; 4; 6$ сформированных НЧ представлена на рис 5.2.

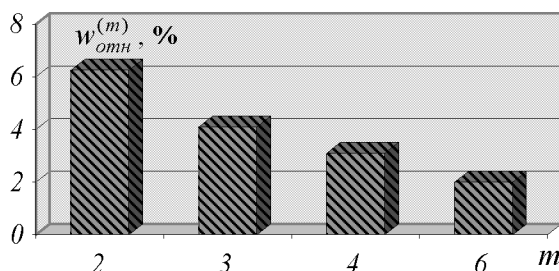


Рис. 5.2. Зависимость значения $w_{отн}^{(m)}$ относительной стеганографической емкости стеганографического алгоритма от длины m НПЧ

Из анализа рис. 5.2 можно сделать вывод, состоящий в том, что в случае формирования неравновесного позиционного числа 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%. Отсюда следует, что для обеспечения максимального значения относительной стеганографической емкости при проектировании стеганографической системы на основе разработанного метода необходимо обеспечить формирование неравновесных позиционных чисел с наименьшей длиной в условиях достижения требуемого уровня эффективного синтаксического представления.

Проведем сравнительную оценку относительной стеганографической емкости $w_{отн}^{(m)}$ для разработанного стеганографического метода и существующих 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).

В табл. 5.1 представлены значения относительной стеганографической емкости методов НЗБ, РС и разработанного метода и значения пикового отношения сигнал-шум для изображений различной насыщенности.

Таблица 5.1

Зависимость значения $w_{отн}$ от ПОСШ для изображений различной насыщенности

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
	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

Из анализа оценки относительной стеганографической емкости в табл.5.1 можно сделать следующие выводы:

1) при одинаковых значениях относительной стеганографической емкости выигрыш для разработанного метода относительно метода НЗБ в режиме 2 по величине пикового отношения сигнал-шум 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 %;

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).

5.2. ОЦЕНКА ХАРАКТЕРИСТИК ПРОЦЕССА СКРЫТИЯ ВСТРОЕННЫХ СООБЩЕНИЙ В СЛУЧАЕ НЕАВТОРИЗИРОВАННОГО ДОСТУПА

Для разработанного стеганографического метода встраивания информации на позицию старшего элемента неравновесного позиционного числа 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 $\gamma = 1$; основание встроенного элемента $\psi'_\gamma = 2$.

Экспериментально оценим визуальные характеристики процесса 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 (приложение «А»):

- 1) сильнонасыщенное изображение «Снимок аэропорта»;
- 2) средненасыщенное изображение «Фотоснимок»;
- 3) слабонасыщенное изображение «Самолет на фоне неба».

Результаты эксперимента в условиях выбора неравновесного позиционного числа длиной $m = 2$ представлены на примере следующих изображений, декодированных неавторизованным пользователем:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 5.3),



Рис 5.3. Изображение «Снимок аэропорта», декодированное неавторизованным пользователем при длине НПЧ $m = 2$

- средненасыщенное декодированное изображение «Фотоснимок» (рис. 5.4);



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

- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 5.4).



Рис 5.5. Изображение «Самолет на фоне неба», декодированное неавторизованным пользователем при длине НПЧ $m = 2$

Из анализа изображений, декодированных при неавторизованном доступе можно сделать вывод, что значения пикового отношения сигнал шум рассмотренных изображений 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 экспериментов в условиях выбора неравновесного позиционного числа длиной $m = 3$ представлены на

примере следующих изображений, декодированных при неавторизованном доступе:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 5.6),
- средненасыщенное декодированное изображение «Фотоснимок» (рис. 5.7);
- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 5.8).



Рис 5.6. Изображение «Снимок аэропорта», декодированное неавторизованным пользователем при длине НПЧ $m = 3$

Анализ полученных изображений показал, что величина пикового отношения сигнал-шум для декодированных изображений относительно исходных изображений при неавторизованном доступе составляет:

- для сильнонасыщенного изображения «Снимок аэропорта»- 39,074 дБ;
- для средненасыщенного изображения «Фотоснимок»- 35,058 дБ;



Рис 5.7. Изображение «Фотоснимок», декодированное неавторизованным пользователем при длине НПЧ $m = 3$



Рис 5.8. Изображение «Самолет на фоне неба», декодированное неавторизованным пользователем при длине НПЧ $m = 3$

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

Теперь рассмотрим результаты экспериментов в условиях выбора неравновесного позиционного числа, длиной $m = 4$. Результаты представлены на примере следующих изображений, декодированных при неавторизованном доступе:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис.5.9),
- средненасыщенное декодированное изображение «Фотоснимок» (рис. 5.10);
- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 5.11).



Рис 5.9. Изображение «Снимок аэропорта», декодированное неавторизованным пользователем при длине НПЧ $m = 4$

Из анализа изображений следует, что значение пикового отношения сигнал-шум для изображений, декодированных

при неавторизованном доступе относительно исходных изображений составляет:



Рис 5.10. Изображение «Фотоснимок», декодированное неавторизованным пользователем при длине НПЧ $m = 4$



Рис 5.11. Изображение «Самолет на фоне неба», декодированное неавторизованным пользователем при длине НПЧ $m = 4$

- 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.

Следующий этап оценки изображений, декодированных при неавторизированном доступе проводился в условиях выбора неравновесного позиционного числа, длиной $m = 6$. Результаты оценки представлены на примере следующих изображений:

- сильнонасыщенное декодированное изображение «Снимок аэропорта» (рис. 5.12),
- средненасыщенное декодированное изображение «Фотоснимок» (рис. 5.13);
- слабонасыщенное декодированное изображение «Самолет на фоне неба» (рис. 5.14).



Рис 5.12. Изображение «Снимок аэропорта», декодированное неавторизованным пользователем при длине НПЧ $m = 6$



Рис 5.13. Изображение «Фотоснимок», декодированное неавторизованным пользователем при длине НПЧ $m = 6$



Рис 5.14. Изображение «Самолет на фоне неба», декодированное неавторизованным пользователем при длине НПЧ $m = 6$.

Проведенный анализ декодированных изображений показал, что значения 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. 5.15 представлены обобщенные результаты по оценке значения пикового отношения сигнал-шум для декодированных изображений при неавторизированном доступе.

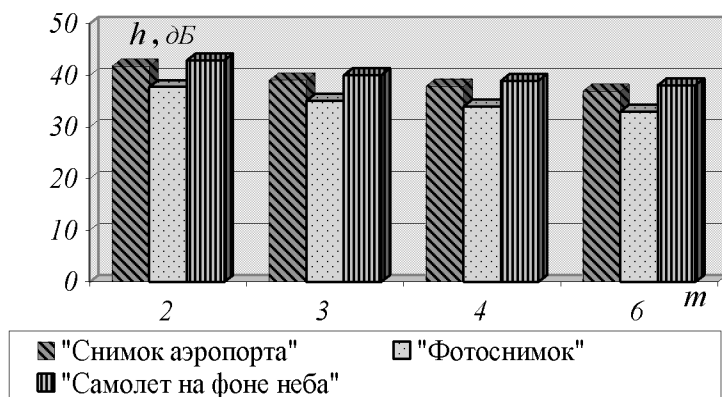


Рис. 5.15. Значения ПОСШ h для декодированных изображений при различных значениях длины m сформированных НПЧ

Из анализа рис. 5.15 можно сделать следующие выводы:

1. Для разработанного метода стеганографического кодирования визуальные искажения, вносимые в изображение при неавторизованном 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 пикового отношения сигнал-шум для средненасыщенного изображения «Фото-снимок» меньше значения пикового отношения сигнал-шум 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 устойчивостью (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 пикового отношения сигнал-шум для изображений, декодированных при неавторизованном доступе, для различных m принимает значения от 38.1 до 42.9 дБ.

4. Величина пикового отношения сигнал-шум для всех типов изображения принимает наибольшее значение в случае встраивания в неравновесное позиционное число 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 от 2,725 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.

Можно утверждать, что учитывая незначительные изменения ПОСШ для декодированных изображений различной насыщенности, в процессе проектирования стеганографической системы отсутствует необходимость в предварительной селекции контейнеров для встраивания.

5.3. СРАВНИТЕЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ПРОЦЕССА 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 эффективном синтаксическом представлении изображения;

- позиция $\gamma = 1$ встроенного элемента $a'_{1,j}$;
- основание $\psi'_\gamma = 2$ 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:

$$N(j)^* = N(j)'' / 2.$$

В этом случае кодограмма стеганокода $N(j)''$ будет иметь следующий вид:

$$C_j''' = \{C'_j; 0\} = \{c_1, \dots, c_\tau, \dots, c_{q(j)'} - 1, 0\},$$

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.

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

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

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

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

Оценим вероятность $P_{из}$ безошибочного изъятия встроенных данных авторизованным 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 авторизованным пользователем принимает максимальное значение. Для этого должно выполняться следующее неравенство:

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

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

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

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

$\psi'_{1,j}$ - 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.

$$N^*(j) = N(j)'. \quad (5.6)$$

Для этого будем учитывать формулу для для стеганокода:

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

Тогда с учетом следующих соотношений:

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

или

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

будет выполняться равенство:

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

Отсюда в случае, когда выполняется равенство

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

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

$$P_{\text{из}} = 1.$$

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 (5.6) с учетом формулы для стеганокода, а именно:

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

Тогда учитывая следующие соотношения

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

или

$$\begin{aligned} \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{V'_{1,j}} &= 0, \quad \frac{1}{V'_{1,j}} = 0; \\ \left[\frac{a'_{1,j} V'_{1,j}}{\psi'_{1,j} V'_{1,j}} + \frac{\sum_{i=2}^{m+1} a_{i,j} V'_{i,j}}{\psi'_{1,j} V'_{1,j}} \right] \psi'_{1,j} &= 0, \end{aligned}$$

будет выполняться равенство:

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

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

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.

$$P_{из} = \frac{w_{из}^{(m)}}{w_{встр}^{(m)}} = 1.$$

Сравним значения вероятностей $P_{из}$ безошибочного изъятия встроенных данных для разработанного стеганографического метода и методов встраивания в наименее значимый бит, расширения спектра.

Для метода НЗБ объем $w_{из}^{Z_{cmp} Z_{ctb}}$ безошибочно изъятых данных в условиях отсутствия активных атак принимает значение меньше $w_{встр}^{Z_{cmp} Z_{ctb}}$ встроенных данных, т.е.

$$w_{из}^{Z_{cmp} Z_{ctb}} < w_{встр}^{Z_{cmp} Z_{ctb}} .$$

Для такого метода вероятность безошибочного изъятия встроенных данных может достигать следующего значения $P_{из} = 0,6$.

Теперь рассмотрим вероятность безошибочного изъятия встроенных данных для метода на основе расширения спектра. В случае встраивания бита скрываемого сообщения на основе метода РС, вероятностью $P_{из}$ изъятия встроенных данных может принимать значение 0,5.

На рис. 5.16. представлена сравнительная диаграмма значений вероятности $P_{из}$ безошибочного изъятия встроенных данных для методов наименее значимого бита, расширения спектра и разработанного метода в условиях отсутствия атак на встроенное сообщение.

Из анализа рис. 5.16 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;

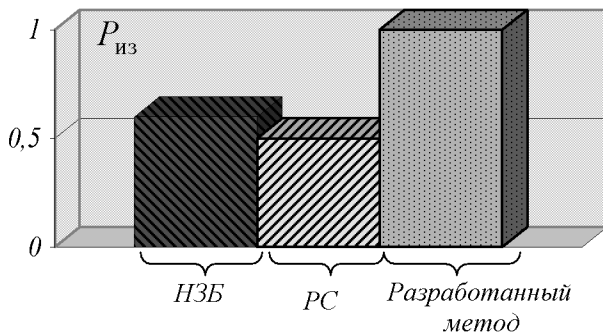


Рис. 5.16. Диаграмма значений вероятности $P_{из}$ для методов НЗБ, РС и разработанного метода в условиях отсутствия атак на встроенное сообщение

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 скрывания информации в кризисных системах.

5.4. ОЦЕНКА УСТОЙЧИВОСТИ СКРЫВАЕМЫХ СООБЩЕНИЙ К АТАКАМ ЗЛОУМЫШЛЕННИКА ДЛЯ РАЗРАБОТАННОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

Оценим устойчивость процесса встраивания данных на основе разработанного стеганографического кодирования в условиях применения противником активной атаки, направленной на разрушение встроенного сообщения.

Такая оценка предусматривает проверку эффективности 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:

а) сильнонасыщенное изображение «Снимок аэропорта» (рис. 4.3);

б) средненасыщенное изображение «Фотоснимок» (рис. 4.4);

в) 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 неравновесных позиционных чисел проводится для трех цветовых компонент исследуемого изображения;

3) имплантация одного бита информации осуществляется на старшую позицию $\gamma = 1$ каждого неравновесного позиционного числа, т.е.:

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

4) значение коэффициента квантования выбирается равным $q = 1; 2; 5; 10$.

Таблица 5.2

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

В табл. 5.2 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.

Проанализировав значения в табл. 5.2 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 неравновесных позиционных чисел;

2) для разработанного метода в условиях атаки дискретного косинусного преобразования с квантования с шагом $q = 10$ наименьший процент 74,1 % по количеству $w_{из}^{(m)}$ правильно изъятых бит достигается для сообщения встроенного в неравновесное позиционное число, 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 неравновесное позиционное число длиной $m = 6$.

В табл. 5.3 представлены процентные значения $w_{из}^{(m)}$ количества безошибочно изъятых бит стеганографически встроенного сообщения в изображение «Фотоснимок» в условиях атак.

Проанализировав значения в табл. 5.3 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 неравновесных позиционных чисел;

Таблица 5.3

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

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 неравновесное позиционное число, длиной $m = 6$.

В табл. 5.4 представлены процентные значения $w_{из}^{(m)}$ количества безошибочно изъятых бит стеганографически встроенного сообщения в изображение «Самолет на фоне неба» в условиях атак.

Проанализировав значения в табл. 5.4 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 неравновесных позиционных чисел;

Таблица 5.4

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

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 $w_{из}^{(z_{cnp}z_{ctb})}$ изъятых бит относительно количества $w_{встр}^{(z_{cnp}z_{ctb})}$ встроенных бит для метода расширения спектра, наименее значимого бита и разработанного метода.

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

На рис. 5.17 представлена диаграмма процентного значения количества безошибочно изъятых бит для методов НЗБ, РС и разработанного метода в условиях применения атаки ДКП и квантования с шагом $q = 0; 1; 5$.

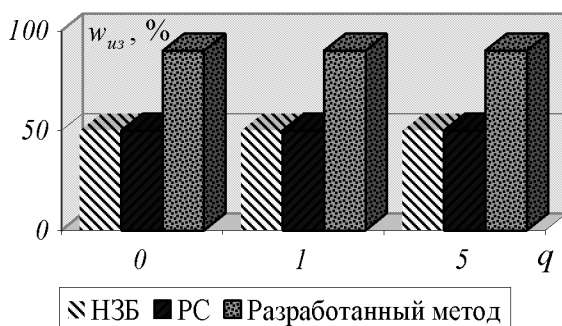


Рис. 5.17 Диаграмма значений величины $w_{uz}^{(m)}$ для метода НЗБ, РС и разработанного метода в зависимости от типа атак

Из анализа рис. 5.17 можно сделать следующие выводы:

- 1) для исследуемых значений коэффициентов квантования количество $w_{uz}^{(m)}$ безошибочно изъятых бит для разработанного метода принимает значения не менее 90 %;
- 2) в условиях применения активных атак выигрыш для разработанного метода относительно методов НЗБ и РС по количеству безошибочно изъятых данных составляет 40 %.

5.5. ОЦЕНКА СТЕГАНОГРАФИЧЕСКОГО БИТРЕЙТА РАЗРАБОТАННОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

Для разработанной системы непосредственного встраивания оценим величину стеганографического битрейта S_b , который определяется на основе следующего выражения:

$$S_b = \lim_{\substack{P_{из} \rightarrow 1 \\ h \rightarrow \infty}} (f(w_{встр}, Z_{стр} Z_{стб}, P_{из}, h)),$$

где $f(\bullet)$ - функциональное преобразование, которое используется для определения стеганографического битрейта;

$w_{встр}$ - величина абсолютной стеганографической емкости, т.е. максимальный объем сообщения, которое можно встроить в изображение, измеряется в битах;

$Z_{стр} Z_{стб}$ - минимально требуемый размер изображения, достаточный для встраивания информации объемом $w_{встр}$ на основе оцениваемого стеганографического алгоритма;

$P_{из}$ - вероятность безошибочного изъятия встроенных данных;

h - величина пикового отношения сигнал-шум.

Физический смысл стеганографического битрейта S_b заключается в том, что данная величина характеризует количество пикселей, которое необходимо для встраивания одного бита скрываемого сообщения. Стеганографический битрейт измеряется в битах на пиксель (бит/пиксель). На практике используется следующее выражение для определения стеганографического битрейта:

$$S_b = \frac{w_{встр}}{Z_{стр} Z_{стб}}, \quad (5.7)$$

где $w_{встр}$ - величина абсолютной стеганографической емкости, т.е. максимальный объем сообщения, которое можно встроить в изображение, измеряется в битах;

$Z_{cmp}Z_{cm\bar{o}}$ - минимально требуемый размер изображения, достаточный для встраивания информации объемом $w_{встр}$ на основе оцениваемого стеганографического алгоритма.

Оценим величину стеганографического битрейта $S_b^{(m)}$ для разработанной стеганографической системы. Для этого необходимо оценить величину $w_{встр}^{(m)}$ абсолютной стеганографической емкости. Учитывая, что разработанная стеганографическая система позволяет встраивать 1 бит скрываемого сообщения в одно неравновесное позиционное число, то величина $w_{встр}^{(m)}$ абсолютной стеганографической емкости будет определяется на основе следующего выражения:

$$w_{встр}^{(m)} = L = \frac{3 \cdot Z_{cmp}Z_{cm\bar{o}}}{m}, \quad (5.8)$$

где L - количество сформированных неравновесных позиционных чисел;

m - длина сформированного неравновесного позиционного числа для встраивания бита скрываемого сообщения.

Перепишем выражение (5.7) с учетом формулы (5.8). В этом случае получим следующее выражение для определения величины стеганографического битрейта для разработанной стеганографической системы:

$$S_b^{(m)} = \frac{w_{\text{встр}}^{(m)}}{Z_{\text{стр}} Z_{\text{стб}}} = \frac{3 \cdot Z_{\text{стр}} Z_{\text{стб}}}{Z_{\text{стр}} Z_{\text{стб}} \cdot m} = \frac{3}{m} \text{ (бит/пиксель)}.$$

На рис. 5.18 представлена диаграмма зависимости величины $S_b^{(m)}$ стеганографического битрейта разработанной стеганографической системы от различной длины $m = 2; 3; 4; 6$ сформированных неравновесных позиционных чисел.

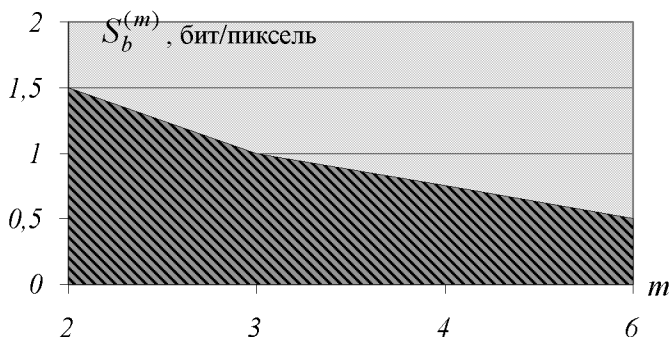


Рис. 5.18 Зависимость величины $S_b^{(m)}$ стеганографического битрейта разработанного метода от длины m НПЧ

Из анализа диаграммы на рис. 5.18 можно сделать вывод, состоящий в том, что в случае формирования неравновесного позиционного числа длиной $m = 2$, величина $S_b^{(m)}$ пропускной способности разработанной системы принимает наибольшее значение, равное 1,5 бит на пиксель. Наоборот, при формировании НПЧ длиной $m = 6$ стеганографическая система обладает наименьшей пропускной способностью – 0,5 бит на пиксель.

Теперь проведем сравнительную оценку величины стеганографического битрейта $S_b^{(m)}$ для разработанного стеганографической системы и существующих методов непосредственного встраивания в изображение-контейнер. Сравнительную оценку будем проводить для следующих методов:

1. Метод встраивания информации в наименее значимый бит элемента спектрального представления контейнера после квантования.

2. Метод встраивания информации на основе расширения спектра.

Для оценки пропускной способности метода встраивания в наименее значимый бит, рассмотрим абсолютную стеганографическую емкость $w_{встр}^{(НЗБ)}$ данного метода. Значение $w_{встр}^{(НЗБ)}$ определяется на основе следующего выражения:

$$w_{встр}^{(НЗБ)} = \frac{3 \cdot Z_{стр} Z_{стб}}{\omega} \text{ (бит)}, \quad (5.9)$$

где ω - количество элементов спектрального представления изображения-контейнера, необходимое для встраивания 1 бита скрываемого сообщения.

Для определения значения $S_b^{(НЗБ)}$ стеганографического битрейта для метода НЗБ перепишем выражение (5.7) с учетом формулы (5.9) для абсолютной стеганографической емкости $w_{встр}^{(НЗБ)}$. В этом случае получим:

$$S_b^{(НЗБ)} = \frac{w_{встр}^{(НЗБ)}}{Z_{стр} Z_{стб}} = \frac{3 \cdot Z_{стр} Z_{стб}}{Z_{стр} Z_{стб} \cdot \omega} = \frac{3}{\omega} \text{ (бит/пиксель)}.$$

Значения стеганографического битрейта для метода НЗБ в зависимости от количество элементов ω , необходимых для встраивания, составляет:

- для $\omega = 2$:

$$P_b^{(НЗБ)} = \frac{3}{2} = 1,5 \text{ (бит/пиксель);}$$

- для $\omega = 4$:

$$P_b^{(НЗБ)} = \frac{3}{4} = 0,75 \text{ (бит/пиксель);}$$

Рассмотрим теперь стеганографический битрейт метода встраивания на основании расширения спектра. Абсолютная стеганографическая емкость $w_{встр}^{(PC)}$ метода на основе расширения спектра определяется на основе следующего выражения:

$$w_{встр}^{(PC)} = \frac{3 \cdot Z_{стр} Z_{стб}}{\omega} \text{ (бит),} \quad (5.10)$$

Перепишем выражения для определение стеганографического битрейта $S_b^{(PC)}$ метода РС с учетом выражения (5.10). В этом случае выражение (5.11) примет вид:

$$S_b^{(PC)} = \frac{w_{всп}^{(PC)}}{Z_{сmp} Z_{сmb}} = \frac{3 \cdot Z_{сmp} Z_{сmb}}{Z_{сmp} Z_{сmb} \cdot \omega} = \frac{3}{\omega}, \text{ (бит/пиксель)}$$

Тогда в случае встраивания 4 бит скрываемого сообщения в блок размером 8×8 пикселей, стеганографический битрейт метода РС примет следующее значение:

$$S_b^{(PC)} = \frac{3 \cdot Z_{сmp} Z_{сmb} \cdot 4}{Z_{сmp} Z_{сmb} \cdot 16} = \frac{12}{16} = 0,75 \text{ (бит/пиксель)}$$

На рис.5.19 – 5.21 представлены диаграммы зависимости величины S_b значения и величины h пикового отношения сигнал шум изображений различной насыщенностью для методов наименее значимого бита, расширения спектра и разработанного метода.

Из анализа из анализа диаграмм на рис рис.5.19 – 5.21. можно сделать следующие выводы:

1) для разработанного метода наибольшее значение стеганографический битрейт принимает в случае формирования неравновесных позиционных чисел длиной $m = 2 - 1,5$ бита на пиксель, и наоборот наименьшее значение величины S_b наблюдается для неравновесных позиционных чисел длиной $m = 6 - 0,5$ бита на пиксель;

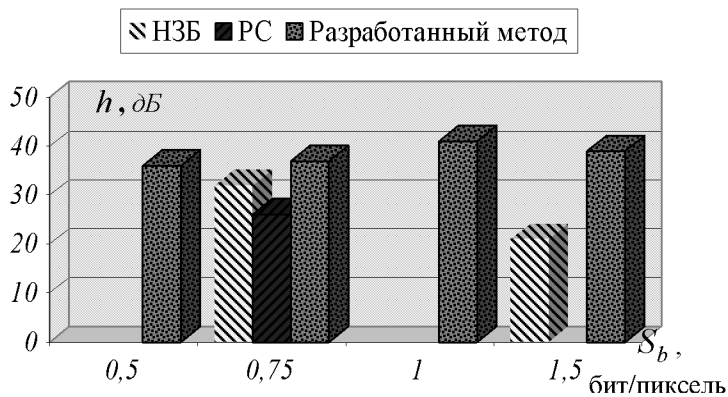


Рис. 5.19 Диаграмма значений величины S_b и h для сильнонасыщенного изображения, декодированного на основе метода H3B, PC и разработанного метода

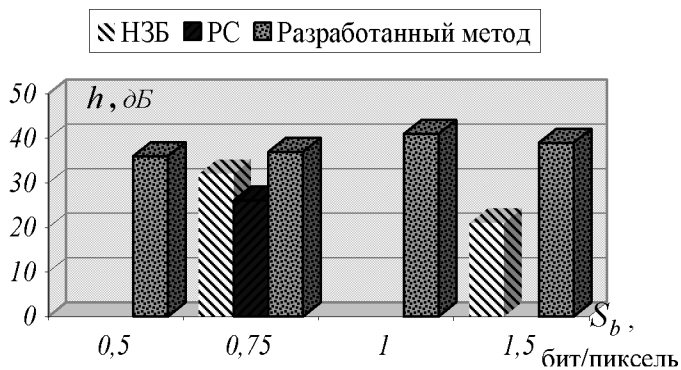


Рис. 5.20 Диаграмма значений величины S_b и h для средненасыщенного изображения, декодированного на основе метода H3B, PC и разработанного метода

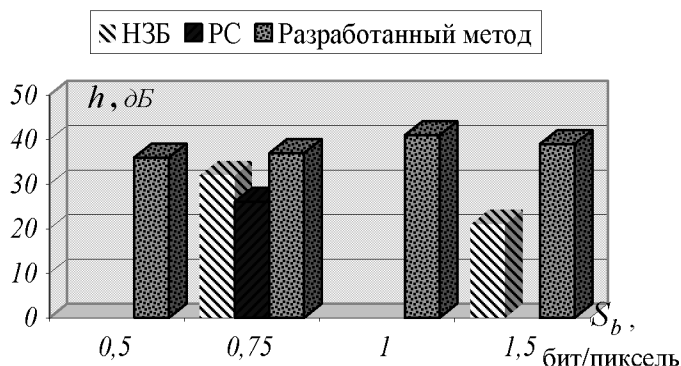


Рис. 5.21 Диаграмма значений величины S_b и h для слабонасыщенного изображения, декодированного на основе метода НЗБ, РС и разработанного метода

Из анализа из анализа диаграмм на рис рис.5.19 – 5.21. можно сделать следующие выводы:

1) для разработанного метода наибольшее значение стеганографический битрейт принимает в случае формирования неравновесных позиционных чисел длиной $m = 2 - 1,5$ бита на пиксель, и наоборот наименьшее значение величины S_b наблюдается для неравновесных позиционных чисел длиной $m = 6 - 0,5$ бита на пиксель;

2) выигрыш для разработанного метода относительно метода НЗБ и РС по величине стеганографического битрейта:

- для метода НЗБ в среднем до 25 %;
- для метода РС в среднем до 25 %.

Выводы

1. Разработан метод оценки емкости стеганографической системы. 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 наименее значимого бита и метода на основе расширения спектра. При этом получены следующие результаты:

1) при одинаковых значения стеганографической емкости $w_{отн}^{(m)}$ выигрыш для разработанного метода относительно метода наименее значимого бита по величине пикового отношения сигнал-шум составляет в среднем от 8 до 20 дБ;

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

2. Разработан метод оценки характеристик процесса скрытия встроенных сообщений. Для разработанного метода проведена оценка характеристик процесса скрытия встроенных сообщений в случае неавторизованного доступа.

Величина пикового отношения сигнал-шум для всех типов изображения принимает максимальное значение в случае встраивания в неравновесное позиционное число длиной $m = 2$. При этом выигрыш в значении ПОСШ относительно встраивания в неравновесное позиционное число 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 4,79 дБ.

При одинаковых условиях стеганографического кодирования наибольшими коррекциями обладают реалистичные яркие декодированные изображения средней насыщенности. Наоборот наименьшее количество искажений вносится при встраивании в слабонасыщенные затемненные изображения.

3. Разработан метод оценки эффективности процесса изъятия встроенной информации при авторизированном доступе. Проведена оценка эффективности процесса изъятия встроенной информации для разработанного метода при авторизированном доступе. Доказано, что вероятность безошибочного изъятия при авторизированном доступе принимает значение 1.

Проведенный 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. Проведенная оценка устойчивости скрываемых сообщений к атакам злоумышленника показал, что для различных значений коэффициента квантования наибольшей устойчивостью обладают данные, стеганографически встроенные в неравновесное позиционное число длиной $m = 6$. Наоборот наименьшей стойкостью обладают данные стеганографически встроенные в неравновесное позиционное число 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%.

5. Разработан метод оценки стеганографического битрейта стеганографического метода. Проведена оценка стеганографического битрейта разработанного метода.

Проведенный сравнительный анализ разработанного метода относительно методов НЗБ и РС по величине стеганографического битрейта показал, что выигрыш для разработанного метода относительно существующих методов составляет: для метода НЗБ – до 25 %; для метода РС – до 25 %.

ВЫВОДЫ МОНОГРАФИИ

В процессе проведения научно прикладных исследований получены следующие результаты:

1. Обосновано направление повышения безопасности специальных информационных ресурсов в кризисных системах на основе использования стеганографических методов. Показывается необходимость использования стеганографических подходов в комплексных системах защиты. В этом случае закладываются требования по обеспечению доступности и целостности информации.

Представлен вариант классификации стеганографических подходов с позиции использования физических процессов при встраивании. Показана актуальность построения стеганографических систем на основе использования в качестве контейнера видеоинформационного ресурса.

2. Систематизированы существующие методы косвенного, непосредственного и смешанного стеганографического встраивания. Разработан вариант классификации, который позволит обозначить место разрабатываемого метода стеганографического кодирования среди существующих подходов для непосредственного встраивания.

Создан классификатор для описания методов на основе предложенной классификации. Данный классификатор используется для позиционирования новых разрабатываемых методов относительно существующих.

Для оценки эффективности стеганографических преобразования с позиции обеспечения информационной безопасности разработана система показателей. В отличие от существующих, данная система в том числе позволяет оценить влия-

ние встраивания информации на показатели эффективности компрессионных представления изображения-контейнера.

На основе проведенной оценки существующих методов непосредственного встраивания сформулировано противоречие, которое заключается в том что существующие технологии стеганографических преобразования не обеспечивают в полной мере системных требований в кризисных системах с активным противостоянием противнику.

3. Обосновано направление для разработки метода стеганографического встраивания. Данное направление базируется на преобразовании числа со встроенными данными на основе функционального преобразования. Определены требования к функциональному преобразованию для числа со встроенными данными, а именно:

- должна обеспечиваться взаимоднозначность прямого и обратного функционального преобразования, т.е. должен существовать обратный функционал, позволяющий авторизованному 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 авторизованного пользователя и для злоумышленника. Для неавторизованно пользователя восстановление изображения происходит при стандартных условиях, при котором блокируется возможность изъятия встроенного сообщения. Для авторизованного 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.

4. 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 контейнера, полученными при обратном преобразовании в случае для авторизованного пользователя и элементами, реконструированными при неавторизованном 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 (неавторизованный пользователь) возможно только при известном ключе, даже при наличии у него информации о встраивании данных;

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

5. 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 результирующее кодовое представление. Обратное функциональное преобразование будет осуществляться для злоумышленника (не авторизованный доступ) и для авторизованного пользователя. При первом способе реконструкция элемента исходного изображения реализуется неавторизованным 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.

6. 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 структурно-комбинаторного стеганографического кодирования и декодирования.

7. Разработано структурно-комбинаторное стеганографическое кодирование с маскированием, базирующееся на следующих этапах:

- формирование неравновесного позиционного базиса для фрагмента изображения;
- структурно-комбинаторное стеганографическое кодирование в неравновесном базисе оснований;
- маскирование структурной стеганографической избыточности путем ее локализации на основе коррекции длины стеганограммы.

8. Создано правило встраивания информации для структурно-комбинаторного 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.

9. 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) структурно-комбинаторное стеганографическое декодирование, обеспечивающее восстановление неравновесного позиционного числа с имплантированным элементом;
- 3) изъятие элемента скрываемого сообщения со старшей позиции неравновесного позиционного числа.

Научная новизна обусловлена решением научно-прикладной задачи повышения безопасности специальных информационных ресурсов на основе использования технологии структурно-комбинаторного 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 структурно-комбинаторной избыточности фрагментов видеоизображений.

2. Впервые разработан метод структурно-комбинаторного стеганографического кодирования с маскированием. В отличие от других методов обеспечивается встраивание скрывае-

мой 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 структурно-комбинаторное 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.

Основные практические результаты.

Разработан метод повышения безопасности специальных информационных ресурсов в системах критического назначения на основе структурно-комбинаторного стеганографиче-

ского кодирования, доведенный до программно – аппаратных реализаций. На основе чего получены такие результаты:

1. Проведенный сравнительный анализ значений относительной стеганографической емкости разработанного метода относительно методов наименее значимого бита и расширения спектра показал, что:

1) при одинаковых значения стеганографической емкости выигрыш для разработанного метода относительно метода НЗБ по величине пикового отношения сигнал шум составляет в среднем от 8 до 20 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 неавторизованного доступа позволяет заключить, что величина ПОСШ для всех типов изображения принимает максимальное значение в случае встраивания в неравновесное позиционное число 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 4,79 дБ.

3. Проведенный 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 наименее значимого бита и расширения спектра 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 неравновесное позиционное число 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%.

5. Оценка стеганографического битрейта разработанного метода встраивания позволяет сделать вывод что наибольшее значение стеганографический битрейт принимает в случае формирования неравновесных позиционных чисел длиной $m = 2 - 1,5$ бита на пиксель, и наоборот наименьшее значение пропускной способности наблюдается для неравновесных позиционных чисел длиной $m = 6 - 0,5$ бита на пиксель. При этом выигрыш для разработанного метода относительно существующих методов составляет:

- для метода НЗБ – до 25 %;
- для метода РС – до 25 %.

Полученные научные результаты являются вкладом в развитие теории информационной безопасности относительно обеспечения безопасности специальных информационных ресурсов в критических системах.

Л И Т Е Р А Т У Р А

1. 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.

2. 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.

3. Андреев А. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 7. – С.19 – 25.

4. Андреев А.. Применение видеоконференцсвязи в Вооружённых силах иностранных государств / А.Андреев, В.Аржанов, К.Семёнов // Зарубежное военное обозрение. – 2008. – № 8. – С.16 – 22.

5. Анин Б. Защита компьютерной информации / Б.Анин. - СПб.: БХВ-Петербург, 2000. - 384 с.

6. Артехин Б.В. Стеганография / Артехин Б.В. // Журнал «Защита информации. Конфидент». – 1996. - № 4 -

7. 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.

8. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Э. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.

9 Баранник Д.В. Стеганографическая система на основе неравновесного позиционного кодирования / Д.В. Баранник, В.В. Баранник, А.Э. Бекиров // Радіоелектроніка та інформатика. - 2014. - №4. - С. 37 – 46.

10. Баранник Д.В. Метод локализации потери целостности информации на основе слот-технологии [Текст] / Д.В. Баранник, В.В. Баранник, С.А. Подлесный // Радиоелектроника и информатика. – Х, ХНУРЭ. - 2015. - Вип. 4. - С. 32 - 41.

11. Баранник Д.В. Обоснование подхода для формирования квантованного описания трансформанты сегмента аэрофотоснимка / Д.В. Баранник, С.Ю. Стасев, Д.О. Медведев // АСУ и приборы автоматики. – 2015. - №173. – С. 63 – 67.

12. Бараннік Д.В. Метод криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі / Д.В. Бараннік, С.А. Сидченко // Наукоємні технології. – 2017. - №1. – С. 00 – 00.

13. Баранник Д.В. Метод криптокомпрессионного представления изображений на основе двухкаскадного обобщенного позиционного кодирования в базисе по верхним границам / Д.В. Баранник, В.В. Баранник, С.А. Сидченко // Радиоелектроника и информатика.– 2016. – № 3. – С. 62 – 68.

14. Баранник В.В. Анализ возможности использования маскирования при выявлении областей для стеганографического встраивания / В.В. Баранник, А.Е. Бекиров, Д.В. Баранник // Наукоємкіе технології в інфокомунікаціях: обробка інформації, кібербезпека, інформаційна боротьба: колективна монографія [под редакцією В.В. Баранника, В.М.Безрука]. – Х.: ТОВ «Видництво «Лідер»», 2017. – С. 375 - 389.

15. Баранник В.В. Структурно-комбинаторное представ-

ление данных в автоматизированных система управления / В.В. Баранник, Ю.В. Стасев, Н.А. Королева - Х.: ХУПС, 2009. – 252 с.

16. Баранник В.В. Метод формування функціонала стеганографічного кодування стійкого до стегано-атак / В.В. Баранник, А.Е. Бекіров // АСУ та прилади автоматики. - 2013. - Вип.165. - С. 34 – 43.

17. Баранник В.В. Метод функционального преобразования чисел со встроенной информацией для стеганосистем / В.В. Баранник, А.Э. Бекиров, А.В. Хаханова // Радиоелектроніка та інформатика. - 2013. - №4. С. 69 – 73.

18. Баранник В.В. Обоснование значимых угроз безопасности видеoinформационного 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.

19. 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.

20. Баранник В.В. Технология неравновесного позиционного кодирования для функционального преобразования чисел со встроенной информацией / В.В. Баранник, Ю.Н. Рябуха, А.Э. Бекиров // Радиоэлектронные и компьютерные системы. – 2014. - №4. - С. 32 - 39.

21. 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.

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. Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники. – 2000. - №2. – С.31-40.

24. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем // Озброєння та військова техніка. – 2015. - №1 - С. 29 – 36.

25. 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.

26. Біла книга - 2016. Збройні Сили України. - К. : Пресса України, 2016. – 111 с.

27. Білінський Й.Й. Методи обробки зображень в комп'ютеризованих оптико-електронних системах. Вінниця: ВНТУ, 2010. - 272 с.

28. Бобок И.И. Метод детектирования стеганосообщения, сформированного посредством модификации наименьшего значащего бита / И.И. Бобок, А.А. Кобозева // Інформаційна

безпека. – 2001.-С.56-63.

29. Богуш В.М. Інформаційна безпека держави /В.М. Богуш, О.К. Юдин. – К.: МК–Прес, 2005. – 432 с.

30. 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.

31. Валерий Чудинов Тайнопись в рисунках А.С. Пушкина

32. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.

33. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений/ А.В. Галицкий. – М.: ДМК Пресс, 2005. –616 с.

34. Генне О.В. Основные положения стеганографии / Генне О.В.// «Защита информации. Кофидент» - 2000 - №3. с 45.

35. Голубев В.О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубев, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжний. - Запоріжжя : Просвіта, 2001. - 252 с.

36. Голубев В.О. Проблемні питання протидії кіберзлочинам у системі інформаційної безпеки держави / В. О. Голубев // Вісник Запорізького юридичного інституту. 1999 р. №4(9). - 1999. - С. 286-300

37. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1073 с.

38. 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.

39. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Окон И.Н., Туринцев И.В. – СПб.: Солон-Пресс, 2002.- 272 с.

40. Гургенидзе А.Т., Корше В.И. Мультисервисные сети и услуги широкополосного доступа. – СПб., 2003. – 434 с.

41. Державна програма розвитку Збройних Сил України на період до 2020 року Затвержена указом Президента України від 29.12.2016 №73/2017.

42. 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.

43. Жилкин М.Ю. Стегоанализ графических данных в различных форматах / М.Ю. Жилкин // Доклады ТУСУРа, №2 (18), часть 1, 2008. – С.63-64.

44. 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.

45. Задирака В.К. Новые подходы к разработке алгоритмов скрытия информации / В.К. Задирака, Л.Л. Никитенко // Штучный інтелект.-2008. - №4. – С.353-357.

46. 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.

47. Кобозева А.А. Аналіз захищеності інформаційних систем / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К.: ДУКІТ, 2010. – 316 с.

48. Кобозева А.А. Применение сингулярного и спек-

трального розложення матриць в стеганографічних алгоритмах / А.А. Кобозева // Вісник Східноукраїнського національного університету ім. В.Даля. – 2006. - №9 (103), ч. 1. – С.74-83.

49. 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.

50. Конахович Г.Ф. Оценка эффективности методов стеганографического встраивания информации в спектральную область изображений / Г.Ф. Конахович // АСУ та прилади автоматизації. - 2014. - Вип.168. - С. 23 - 29.

51. Конахович Г.Ф. Сучасні методи квантової стеганографії / Г.Ф. Конахович, О.В. Шевченко, В.М. Кінзеревий, Ю.Е. Хохлачова // Захист інформації – №2 (51), 2011.- С.5-9.

52. Державна програма розвитку Збройних Сил України на період до 2020 року Затвержена указом Президента України від 29.12.2016 №73/2017.

53. 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.

54. Корольов В.Ю. RS-стеганоанализ. Принципы работы, недостатки та концепція методу його обходу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко // Вісник Вінницького політехнічного інституту. – 2010. - №6. – С.66-71.

55. 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.

56. Крук Б.И. Телекоммуникационные системы и сети. Том 1, 2, 3 / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов. - М.: Го-

рячая линия-Телеком, 2003. – 647 с.

57. Куш А.В. Использование алгоритмов стеганографии при проведении компьютерно-технической экспертизы / А.В. Куш // VI Всероссийская межвузовская конференция молодых ученых – СПб. СПбГУ ИТМО, 2009.

58. Лидовский В.В. Теория информации / В.В. Лидовский. – М.: Компания Спутник+, 2004. – 111 с.

59. 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.

60. Михайличенко О.В. Повышение устойчивости стега-ноалгоритмов 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. – вып. 2(60). – С.102-104.

61. 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.

62. 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.

63. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).

64. Пузыренко А.Ю. Оценка качества реализации стегано-

графических 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.

65. Пузыренко О.Ю. Представлення і прогнозування ефективності нового протоколу оцінки якості реалізації розроблюваних алгоритмів комп'ютерної стеганографії / О.Ю. Пузыренко, Д.О. Навроцький, Л.П. Дюжаєв // Радіотехніка. Радіоапаратобудування: Зб. наук. пр. – Вип. 34. – К.: НТУУ «КПІ», 2007. – С.150-156.

66. 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.

67. 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.

68. 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.

69. 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.

70. Стратегія національної безпеки України: Указ Президента України від 26 травня 2016 № 287/1015.

71. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М: Техносфера, 2004. – 368 с.

72. Тропченко А.Ю. Методы сжатия изображений, аудио-сигналов и видео / А.Ю. Тропченко, А.А. Тропченко // Учебное пособие – СПб: СПбГУ ИТМО, 2009. – 108 с.

73. Фисенко В.Т. Компьютерная обработка и распознавание изображений: учебн. пособие / В.Т. Фисенко, Т.Ю. Фисенко. – СПб.: СПбГУ ИТМО, 2008. – 192 с.

74. Хорошко В.А. Методы и средства защиты информации. / Хорошко В.А., Чекатов А.А. –К.: Юниор, 2003. – 501с.

75. Хорошко В.А. Введение в компьютерную стеганографию /Хорошко В.А., Шелест М.Е., Яремчук Ю.Е. – Вінниця: ВДТУ, 2003. – 143 с.

76. Хорошко В.О. Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов / Азаров О.Д., Шелест М.Э - Винница: ВДТУ, 2003.-143 с.

77. 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.

78. Шеннон К. Работы по теории информации и кибернетики. – М.: Изд – во иностр. лит – ры, 1963. – 793 с.

79. 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.

80. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник / О.К. Юдін. – К.: НАУ, 2011. – 640с.

81. Юдін О.К. Концептуальний аналіз уразливості державних інформаційних ресурсів / О.К.Юдін, С.С.Бучик // Наукоємні технології. – 2013. - № 3 (19). – С. 299 – 304.

82. Alimpiev, A The video information resources integrity concept by using binomial slots / Alimpiev, A., Barannik, V., Podlesny, S., Suprun, O. and Bekirov A. // 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH 2017), Lviv, 2017, pp. 193-196.

83. Bancroft F.C., Clelland C: DNA-based steganography W00068431. November 16, World Intellectual Property Organization.

84. Barannik V.V. Structural slotting with uniform redistribution for enhancing trustworthiness of information streams./ Barannik, V.V., Ryabukha, Yu.N., Podlesnyi, S.A.// Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017. №76 (7), pp.607.

85. Barannik V. The ensuring the integrity of information streams under the cyberattacks action / Barannik, V., Podlesny, S., Krasnorutskyi, A., Musienko, A., Himenko, V. // Proceedings of 2016 IEEE East-West Design and Test Symposium, EWDTs 2016, Yerevan, 2016, pp. 1-5.

86. Barannik V. The method of increasing accessibility of the dynamic video information resource / Barannik, V., Shulgin, S.S. // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Proceedings of the 13th International Conference on TCSET 2016 Lviv, 2016, pp.621.

87. Barannik V. The analysis of the use of technologies of error resilient coding at influence of an error in the codeword. / Barannik, V., Podlesny, S.A., Yalivets, K., Bekirov, A. // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Proceedings of the 13th International Conference on TCSET 2016, Lviv, 2016, pp. 52-54.

88. Barannik V. Model intelligent processing of aerial photographs with a dedicated key features interpretation / Barannik, V.,

Krasnorutskiy, A., Ryabukha, Y.N., Okladnoy, D.E // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Proceedings of the 13th International Conference on TCSET 2016, Lviv, 2016, pp. 736

89. Barannik V.V. Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding / Barannik, V.V., Ryabukha, Yu.N., Tverdokhlebov, V.V., Barannik, D.V. // 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 - Proceedings, pp.188.

90. Barannik V. Dynamic coding of transforms of the images in two-level polyadic space / Barannik, V., Hahanova, I., Kulbakova, N. // Modern Problems of Radio Engineering, Telecommunications and Computer Science - International Conference, TCSET 2008; Lviv-Slavsko; Ukraine; 19 February 2008 - 23 February 2008; pp. 320-325.

91. Barannik V.V. Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component / Barannik, V.V., Komolov, D., Musienko, A.P., Tarnopolov, R.V. // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016, pp.739.

92. Barannik V. Method of effective syntactic description of frames using the contour information to improve the integrity of the video information resource / Barannik, V., Ryabukha, Y., Krasnorutskiy, A. // 2015 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015 - Conference Proceedings, pp.253.

93. Barannik V.V. The methodological base of cryptocompression presentation of videoinformation resources / Barannik,

V.V., Sidchenko, S.A., Larin, V.V. // 2013 12th International Conference: The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM 2013 ,pp.27

94. 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.

95. 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.

96. Barannik V. Functional transformation for direct embedding steganographic methods / Vladimir Barannik, Ali Bekirov, Roman Tarnopolov // International Symposium «IEEE East-West Design & Test», (Kiev, Ukraine, September 26–29, 2014).

97. 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 (Zakarpattia), Ukraine).

98. Bohme R. Advanced Statistical Stegoanalysis. – Berlin: Springer-Verlag, 2010. – 300 p.

99. 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.

100. Chen B. An Information-Theoretical Approach to the Design of Robust Digital Watermarking Systems / B. Chen, G.W. Wornell // Proceeding Int. Conf. on Acoustics, Speech and Signal Processing. 1999.

101. Cox I.J. Digital watermarking and steganography. / I.J Cox, M.L. Bloom, J.A. Fridrick, and T. Kalkert. // USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

102. 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.

103. Fortrini M Steganography and digital watermarking: A global view / M. Fortrini // University of California, Davis. Available:

<http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf> [June 2011].

104. Fridrich J. Stegoanalysis of LSB encoding in color image / J. Fridrich, R. Du, M. Long // ICME, 2000.

105. Fridrich J. New blind steganalysis and its implication / J. Fridrich, G. Miroslov // Proc. SPIE Elec-tronic Imaging, 2006.

106. Fridrich J. Steganalysis of LSB encoding of Color Images / Fridrich J., Du R., Long M. // Proceedings of ICME 2000, New York City, July 31 – August 2, New York, USA.

107. Granrath D.J. The role of human visual models in image processing, // Proceedings of the IEEE, Vol. 67, 1981. - pp. 552-561.

108. Gonzales R.C. Digital image processing / R.C. Gonzales, R.E. Woods. - Prentice Inc. Upper Saddle River, New Jersey 2002. – 779 p.

109. Hui T. An M-Sequence Based Steganography Model for

Voice over IP / T. Hui, et al. // Communications, 2009. ICC'09. IEEE International Conference on 2009.

110. 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.

111. Kutter M. Digital Image Watermarking: Hiding Information in Images. PhD, Thesis. // Swiss Federal Institute of Technology, Lausanne, Switzerland, 1999.

112. Lin C. Watermarking and digital Signature Techniques for Multimedia Authentication and Copyright Protection // PhD Thesis, Columbia University, 2000.

113. Marvel L. Image Steganography for Hidden Communication. PhD Thesis. University of Delaware, 1999. 115p.

114. 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.

115. Petitcolas F. Attacks on Copyright Marking Systems / F. Petitcolas., R. Anderson, M. Kuhn // Lecture notes in Computer Science. 1998. P. 218-238.

116. Provos N/ Hide and Seek: An Introduction to Steganography / N. Provos, P. Honeyman // The IEEE Computer Security, 2003.

117. Petrou M. Image Processing The Fundamentals, John Wiley & Sons, Inc. – 1999. – 355 p.

118. Ramkumar M. Data Hiding in Multimedia. PhD Thesis // New Jersey Institute of Technology, 1999, 68 p.

119. 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.

120. 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.

121 Smith J. Modulation and Information hiding in Image / J. Smith, B. Comiskey // Information hiding: First Int. Workshop “InfoHiding’96”, Springer as Lecture Notes Computing Science, vol 1174. 1996. – pp.207-227.

122. 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.

123. 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.

124. Wallace G.K. The JPEG Still Picture Compression Standard // Communication in ACM. – 1991. – V34 – №4. – P.31 – 34.

125. <http://www.bnti.ru/showart.asp?aid=643&lv1=04.03.07>.

126. United States Department of Justice. Criminal complaint by Special Agent Ricci against alleged Russian agents.

ПРИЛОЖЕНИЕ А

Примеры исходных реалистичных изображений



Исходное изображение-контейнер «Снимок аэропорта»



Исходное изображение-контейнер «Фотоснимок»



Исходное изображение-контейнер «Самолет на фоне неба»

ДЛЯ ЗАПИСЕЙ

Монография

Баранник Владимир Викторович
Баранник Дмитрий Владимирович
Бекиров Али Энверович

**ОСНОВЫ ТЕОРИИ
СТРУКТУРНО-КОМБИНАТОРНОГО
СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ**

Монография

Дизайн обложки В. В. Баранник, В. В. Твердохлеб

Редактор Л. М. Шевченко
Технический редактор Т. В. Василенко
Корректор Н. К. Гур'ева

Подп. к печати 00.00.2017. Формат 60 × 84/16. Бумага офсетная.
Гарнитура Times New Roman. Печать ризографическая. Ус. печ. арк. 26,27.
Тираж 500 пр. Зам. № 0-253.

Издатель и подготовитель
Харьковский национальный университет радиоэлектроники
61000, м. Харьков, пр. Науки, 14
Свидетельство субъекта издательского дела
ДК № 2535 от 22.06.2006