

Московский государственный институт электроники и математики
(технический университет)



Пономарев Кирилл Ильич

04201004626

**НЕКОТОРЫЕ МАТЕМАТИЧЕСКИЕ МОДЕЛИ
СТЕГАНОГРАФИИ И ИХ СТАТИСТИЧЕСКИЙ
АНАЛИЗ**

01.01.05 – Теория вероятностей и математическая статистика

Научный руководитель
д.ф.-м.н, профессор
Ивченко Г.И.

Москва 2010

ОГЛАВЛЕНИЕ

Введение.....	5
Глава I. Этапы развития и особенности построения	
стеганографических систем и методов сокрытия в	
них данных.....12	
1.1. <i>Этапы развития стеганографии.....</i>12	
1.1.1. <i>Классическая стеганография.....</i>12	
1.1.2. <i>Компьютерная стеганография.....</i>13	
1.2. <i>Построение стеганографической системы.....</i>19	
1.2.1. <i>Бесключевые стеганосистемы.....</i>24	
1.2.2. <i>Стеганосистемы с секретным ключом.....</i>25	
1.2.3. <i>Стеганосистемы с открытым ключом.....</i>26	
1.2.4. <i>Смешанные стеганосистемы.....</i>27	
1.3. <i>Виды атак на стеганографическую систему.....</i>27	
1.4. <i>Стеганографические методы сокрытия данных.....</i>30	
1.4.1. <i>Сокрытие данных в неподвижных изображениях.....</i>35	
1.4.2. <i>Сокрытие данных в аудио и видеопоследовательностях..</i>40	
Глава II. Математические модели вкрапления скрытой	
информации и их статистический анализ.....45	
2.1. <i>Биномиальная модель вкрапления информации.....</i>45	
2.1.1. <i>Статистический критерий обнаружения вкраплений....</i>46	
2.1.2. <i>Асимптотический вариант критерия</i>	
<i>Неймана-Пирсона.....</i>50	

2.1.3. Схема серии биномиальной модели вкрапления.....	53
2.1.4. Оценивание числа вкраплений.....	55
2.2. Параметрическая модель вкрапления информации	59
2.2.1. Определение модели вкрапления информации.....	59
2.2.2. Проверка гипотезы о наличии вкраплений.....	61
2.2.3. Оценивание интенсивности вкрапления.....	66
2.3. Полиномиальная модель вкрапления и ее статистический анализ.....	70
Заключение.....	75
Литература.....	77

ВВЕДЕНИЕ

Задача надежной защиты авторских прав, прав интеллектуальной собственности и других конфиденциальных данных от несанкционированного доступа является одной из старейших и не до конца решенных до настоящего времени проблем. Поэтому во всем мире постоянно ищут решение вопросов разработки методов защиты информации.

Есть два принципиально различных способа передачи по открытому каналу связи конфиденциальной (секретной) информации. Первый из них, известный как шифрование, состоит в замене (по некоторому алгоритму) символов передаваемой информации другими символами, в результате чего получается шифртекст, который и наблюдается «противником» в канале связи. Наука, которая решает соответствующие проблемы обеспечения безопасности передаваемой таким способом информации, называется *криптографией*.

Второй способ состоит в том, чтобы замаскировать передаваемую секретную информацию, другой, так называемой «шумовой» информацией, которая обычно представляет собой передаваемый по каналу связи некоторый открытый текст. В этом случае секретные символы вкрапляются в открытый текст, то есть некоторые его знаки заменяются на секретные знаки. Такой, видоизмененный открытый текст, несущий в себе секретную информацию, и наблюдается «противником». Соответствующая наука об организации и анализе подобных процедур сокрытия информации называется *стеганографией*.

Надо отметить, что если криптография, как математическая наука, является в настоящее время весьма продвинутой, то такого нельзя сказать

о стеганографии. Здесь на сегодня достаточно хорошо разработаны соответствующие технологические аспекты; что же касается построения и анализа адекватных математических моделей, то эти вопросы еще ждут своего решения.

Криптографическая защита информации не снимает полностью проблему сокрытия конфиденциальной информации, поскольку наличие шифрованного сообщения уже само по себе привлекает внимание «противника», и он, завладев криптографически защищенным файлом, может бросить всю суммарную мощь своей компьютерной базы на дешифрование скрытых данных. Поэтому для передачи конфиденциальной информации широко используют также и *стеганографические методы защиты информации*.

Термин «стеганография» происходит от двух греческих слов – steganos (тайна) и graphy (запись), поэтому ее можно называть тайнописью. Хотя термин «стеганография» появился только в конце XV века, использовать стеганографию начали несколько тысячелетий тому назад.

Стеганография - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Стеганография не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

Стеганография – это метод организации связи. Задачей стеганографии является сокрытие самого факта существования секретных данных при их передаче, хранении или обработке. Иначе говоря, под сокрытием существования информации подразумевается не только невозможность обнаружения в перехваченном сообщении скрытого письма, но и вообще сделать невозможным возникновение любых

подозрений на этот счет. Общей чертой стеганографических методов является то, что скрываемое сообщение встраивается в некий, не привлекающий внимания, объект (контейнер), который затем, открыто, пересыпается адресату. В отличие от криптографии, где «противник» точно может определить, является ли сообщение зашифрованным, методы стеганографии позволяют встраивать секретные сообщения в безобидные файлы так, чтобы нельзя было заподозрить существование тайного послания[1].

На сегодняшний день стеганографическая система или *стегосистема* может рассматриваться как совокупность средств и методов, которые используются для формирования скрытого канала передачи информации. При построении стеганографической системы учитываются следующие положения. Противник имеет полное представление о стеганографической системе. Единственной информацией, которая неизвестна потенциальному «противнику», является ключ, с помощью которого только его держатель может установить факт присутствия сообщения и его содержание. Таким образом, вся секретность системы защиты передаваемых сообщений должна содержаться в ключе – фрагменте информации, предварительно разделенном между адресатами.

Стеганографию можно разделить на 3 раздела [2]:

- *Классическая стеганография* — включает в себя все «некомпьютерные методы».
- *Компьютерная стеганография* — направление классической стеганографии, основанное на особенностях компьютерной платформы и использования специальных свойств компьютерных форматов данных. Примеры: скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д.

- *Цифровая стеганография* — направление компьютерной стеганографии, основанное на сокрытии информации в цифровых объектах, изначально имеющих аналоговую природу, то есть мультимедиа-объекты (изображения, видео, звуки). В связи с развитием аппаратных средств вычислительной техники и огромным количеством каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в файлах, вычислительных сетях и т. п. Например, сокрытие информации в графических либо текстовых файлах путём использования специального программного обеспечения или стандартными средствами [3].

Увеличение количества публикуемых работ и патентуемых решений, связанных с вопросами стеганографии, несомненно указывает на увеличение темпов развития данной науки. Однако, существующие на сегодняшний день методы полностью не удовлетворяют требованиям практических задач. Очевидно, это является сильнейшим стимулом для дальнейшего развития стеганографических систем и методов стеганоанализа.

В первой главе диссертации описаны исторические этапы развития стеганографии и изложены особенности построения стеганографических систем. В ней обсуждаются вопросы взаимосвязи между устойчивостью стеганосистемы и объемом скрываемого сообщения. Рассматриваются некоторые виды атак и общие вопросы надежности стеганографических систем. Данна детальная классификация методов компьютерной стеганографии, в том числе методов сокрытия в мультимедийных файлах. Особое внимание уделяется описанию возможных сфер использования стеганографии.

Вторая глава посвящена построению адекватных математических моделей вкрапления скрытой информации в тексты и изображения и вероятностно-статистическому анализу этих моделей.

Математические аспекты стеганографии на сегодняшний день разработаны еще недостаточно, поэтому построение математических моделей стеганографии и их вероятностно-статистический анализ является, несомненно, актуальной проблематикой и данное диссертационное исследование в определенной степени восполняет этот пробел.

Цель работы

Целью диссертационной работы является построение адекватных математических моделей вкрапления секретной информации при ее хранении или передачи по открытым каналам связи и исследование стойкости стеганосистемы в зависимости от количества вкрапляемой информации и особенностей самого процесса вкрапления. Для достижения этой цели необходимо разработать соответствующие математические модели и провести их вероятностно-статистический анализ.

Методы исследований

В диссертационной работе используются методы математического анализа, теории вероятностей и математической статистики, теории цифровой обработки сигналов и изображений.

Научная новизна

Предложенные в диссертации математические модели являются новыми, вполне адекватными реальным процессам и позволяют

рационально управлять ими. В диссертации получены следующие научные результаты:

- Построена биномиальная модель вкрапления информации, проведен ее вероятностно статистический анализ, включая случай схемы серий, и получена оценка числа допустимых вкраплений, гарантирующее надежное сокрытие факта вкрапления.
- Построена и проанализирована параметрическая модель вкрапления информации, дана оценка допустимой интенсивности вкрапления.
- Исследована полиномиальная модель вкрапления, проведен ее вероятностно-статистический анализ и сформулированы практические рекомендации для обеспечения надежности сокрытия факта вкрапления.
- Обобщены и систематизированы основные методы и положения компьютерной стеганографии, указаны виды атак на нее; показаны возможности использования стеганографических методов как для передачи секретной информации в сетях Internet, так и для защиты авторских прав и прав интеллектуальной собственности.

Теоретическая и практическая значимость

Работа носит теоретический и практический характер. Задачи, рассмотренные в диссертации, позволяют проводить строгий вероятностно-статистический анализ надежности сокрытия факта вкрапления информации в дискретные последовательности в рамках биномиальной и полиномиальной моделей, а также формулировать соответствующие практические рекомендации для организации процесса вкрапления.

Результаты, полученные в диссертации, могут представлять интерес для специалистов, занимающихся приложениями теоретико-вероятностных и статистических методов в различных направлениях компьютерных технологий. Построенные в диссертации модели использованы при разработке ряда конкретных систем защиты информации в локальных вычислительных сетях, что подтверждено актами о внедрении.

Апробация работы

Результаты работы прошли апробацию в виде выступлений на следующих научных конференциях:

- Ежегодная научно-техническая конференция студентов, аспирантов и молодых специалистов МИЭМ (2007), Москва,
- Ежегодная научно-техническая конференция студентов, аспирантов и молодых специалистов МИЭМ (2008), Москва,
- Ежегодная научно-техническая конференция студентов, аспирантов и молодых специалистов МИЭМ (2009), Москва,
- IX Симпозиум «Электротехника 2030», (2007), Московская область.

Результаты диссертации докладывались на заседании научно-исследовательского семинара кафедры «Теория вероятностей и математическая статистика» МИЭМ.

Кроме того, результаты диссертационной работы рассматривались и обсуждались на научно-техническом совете федерального государственного унитарного предприятия «Центр эксплуатации объектов наземной космической инфраструктуры» - филиал «Конструкторское бюро транспортного машиностроения».

Результаты работы использовались при выполнении следующих НИР, выполненных в филиале ФГУП ЦЭНКИ - КБТМ:

- НИР «Инструменты» 2007 год. Тема: «Исследование инструментальных средств реализации концепции «Электронная отрасль» и «Электронное предприятие». Разработка предложений по инструментальной защите данных при их передаче в открытых сетях».
- НИР «PLM-ОНКИ» 2007 год. Тема: «Разработка отладочно-демонстрационно-сертификационного стенда на основе системы InvisiLAN для защиты данных при их передаче в открытых сетях».
- НИР «Поддержка СК» 2008 год. Тема «Исследования структуры, состава и функций элементов системы интегрированной логистической поддержки (ИЛП) объектов наземной космической инфраструктуры»

Публикации

Основные результаты диссертации отражены в 6 работах, 2 из которых опубликованы в изданиях, входящих в утвержденный ВАК перечень ведущих рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертации на соискание ученой степени кандидата наук (см. работы [28-33] в списке литературы).

Структура и объём работы

Работа состоит из введения, двух глав, заключения и списка литературы. Общий объем работы составляет 81 страниц, в том числе 4 рисунка.

Глава I

Этапы развития и особенности построения стеганографических систем и методов сокрытия в них данных.

1.1. Этапы развития стеганографии.

1.1.1. Классическая стеганография.

Первые следы стеганографических методов известны с глубокой древности. Местом зарождения стеганографии многие называют Египет. Хотя «стеганографическими сообщениями» можно назвать и наскальные рисунки древних людей [4].

Первое упоминание о стеганографических методах в литературе приписывается Геродоту, описавшему случай передачи сообщения Демартом, который соскабливал воск с дощечек, писал письмо прямо на дереве, а потом заново покрывал дощечки воском. Таблички выглядели без изменений и поэтому не вызывали подозрений.

XVII - XVIII века известны как эра "черных кабинетов" - специальных государственных органов по перехвату, перлюстрации и дешифрованию переписки. В штат "черных кабинетов", помимо криптографов и дешифровальщиков, входили и другие специалисты, в том числе и химики. Наличие специалистов-химиков было необходимо из-за активного использования так называемых невидимых чернил.

На Руси также использовали симпатические чернила. Так, например, тайные агенты Ивана Грозного писали свои донесения луковым соком: буквы становились видимыми при нагревании бумаги. В России секретные чернила использовали революционеры.

Широкое распространение и применение в стеганографии получил так называемый *метод микроточки*. Под микроточкой понимают уменьшенное более, чем в сто раз, фотоизображение обычного документа. Термин микроточка является дословным переводом немецкого термина Mikrat, введенного ее создателем Эммануилом Голдбергом в 1925 году для обозначения созданного им микроскопического изображения. Такое название она получила за сходство с обычной типографской точкой, диаметр которой составляет порядка 0.8 мм. Английскими специалистами, занимавшимися поиском и обнаружением немецких каналов скрытой связи во время Второй мировой войны, был введен еще один термин - *ультра-микроточка*, обозначающий уменьшение оригинала от четырехсот до двух тысяч раз (менее 0,2 мм в диаметре) [5]. После окончания Второй мировой войны микрофильмы и микроточки активно использовались разведками СССР, США, Японии и других стран.

1.1.2. Компьютерная стеганография.

Основоположником современной компьютерной стеганографии можно считать американского математика Густава Симмонса, который первым стал использовать математические модели для доказательства стеганографических задач.

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях.

Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Это дает возможность говорить о становлении нового быстро развивающегося направления в сфере защиты информации – *компьютерной стеганографии (КС)*. КС – это часть стеганографии, которая занимается вопросами реализации стегосистем с использованием компьютерной техники [6].

Основными исходными положениями современной КС являются:

1. Методы сокрытия должны обеспечивать неизменность и целостность файла.
2. Предполагается, что противнику полностью известны возможные стеганографические методы.
3. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открытого передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа.
4. Даже если факт сокрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу [7].

Существует два основных направления использования КС: связанное с цифровой обработкой сигналов и не связанное с таковой. В первом случае секретные сообщения встраиваются в цифровые данные, которые, как правило, имеют аналоговую природу – речь, изображения, аудио- и видеозаписи. Во втором – конфиденциальная информация размещается в заголовках файлов различных форматов и в текстовых сообщениях. Подавляющее большинство текущих исследований в сфере стеганографии, так или иначе, связано именно с цифровой обработкой сигналов, что позволяет говорить о *цифровой стеганографии (ЦС)*.

КС активно использует как особенности программного обеспечения, протоколов для сокрытия информации, так и приемы, использующие представления информации, предназначенные для восприятия человеческими органами зрения и слуха, в мультимедийном виде.

Несомненный интерес КС представляет для спецслужб, в задачу которых входит либо усиление методов сохранения тайны, либо вскрытие этих методов и доступ к тайне, либо ограничение и контроль за распространением средств сокрытия тайны.

Анализ тенденций развития КС показывает, что в ближайшие годы интерес к развитию методов КС, несомненно, будет усиливаться. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации (ЗИ). С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов ЗИ [7]. И, конечно, сильным катализатором этого процесса является лавинообразное развитие компьютерной сети общего пользования – Internet, в том числе такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

Весьма характерной тенденцией в настоящее время в области ЗИ является внедрение криптографических методов. Однако на этом пути много ещё нерешенных проблем, связанных с разрушительным воздействием на криптосредства таких составляющих информационного оружия как компьютерные вирусы, логические бомбы, автономные репликативные программы и т.п. Объединение методов КС и криптографии явилось бы хорошим выходом из создавшегося положения. В этом случае удалось бы устраниТЬ слабые стороны известных методов

ЗИ и разработать более эффективные новые нетрадиционные методы обеспечения информационной безопасности.

Так как ЦС является молодой наукой, то ее терминология не до конца устоялась. Но все же можно дать неформальное определение. ЦС – это наука о незаметном и надежном скрытии одних битовых последовательностей в других, имеющих аналоговую природу. В этом определении содержатся два главных требования к стеганографическому преобразованию: незаметность и надежность, то есть устойчивость к различного рода искажениям. Упоминание об аналоговой природе цифровых данных подчеркивает тот факт, что встраивание информации выполняется в оцифрованные непрерывные сигналы. Таким образом, в рамках ЦС не рассматриваются вопросы внедрения данных в заголовки IP-пакетов и файлов различных форматов, в текстовые сообщения [8].

В настоящее время можно выделить четыре тесно связанных между собой и имеющих одни и те же корни направления приложений ЦС [9]:

- встраивание информации с целью ее скрытой передачи;
- встраивание цифровых водяных знаков (ЦВЗ)(watermarking);
- встраивание идентификационных номеров (fingerprinting);
- встраивание заголовков (captioning).

ЦВЗ могут применяться, в основном, для защиты от копирования и несанкционированного использования. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами могут являться аудио и видеозаписи. Один из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток - ЦВЗ. Разработки в этой области ведут крупнейшие фирмы во всем мире.

Так как методы ЦВЗ начали разрабатываться недавно, то здесь имеется много нерешенных проблем.

Название этот метод получил от известного всем способа защиты ценных бумаг, в том числе и денег, от подделки. В отличие от обычных водяных знаков ЦВЗ могут быть не только видимыми, но и (как правило) невидимыми. Невидимые ЦВЗ анализируются специальным декодером, который выносит решение об их корректности. ЦВЗ могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию. Наиболее подходящими объектами защиты при помощи ЦВЗ являются неподвижные изображения, файлы аудио и видеоданных.

Довольно большое количество запатентованных решений в области стеганографии посвящено внедрению ЦВЗ. Положительными сторонами методов сокрытия в младших битах и спектре, описанных в патенте The Dice Company “Оптимизированные методы для внедрения, защиты и детектирования цифровых водяных знаков в оцифрованных данных” [10], являются возможность применения кодов, исправляющих ошибки и зависимость псевдослучайного сигнала ЦВЗ не только от ключа, но и от контейнера с целью увеличения стойкости встраиваемых ЦВЗ.

В патенте [11] описан иной способ увеличения стойкости встраиваемых ЦВЗ, который состоит в том, что параметры внедрения ЦВЗ регулируются пользователем, который оценивает искажения, возникающие за счет внедрения ЦВЗ. Таким образом, с учетом достаточной квалификации пользователя возможно внедрение ЦВЗ с максимальной эффективностью без внесения искажений, заметных для человека.

В ряде патентов описаны способы применения методов стеганографии для внедрения и извлечения ЦВЗ [12-15]. Рассмотренные

методы позволяют внедрять ЦВЗ в негативные и позитивные фотографические слайды, а также в фотографии на фотобумаге, и применять детектирование в фотолабораториях с целью обеспечения авторских и имущественных прав на фотографии.

Технология *встраивания идентификационных номеров* производителей имеет много общего с технологией ЦВЗ. Отличие заключается в том, что в первом случае каждая защищенная копия имеет свой уникальный встраиваемый номер (отсюда и название – «отпечатки пальцев»). Этот идентификационный номер позволяет производителю отслеживать дальнейшую судьбу своего детища.

Встраивание заголовков (невидимое) может применяться, например, для подписи медицинских снимков, нанесения легенды на карту и т.д. Целью является хранение разнородно представленной информации в едином целом. Это, пожалуй, единственное приложение стеганографии, где в явном виде отсутствует потенциальный нарушитель.

Несмотря на то, что требования, выдвигаемые к различным направлениям использования стеганографии, во многом имеют общие черты, существуют и отклонения от правил. Так, например, отличие постановки задачи для скрытой передачи данных от постановки задачи встраивания ЦВЗ состоит в том, что в первом случае нарушитель должен обнаружить скрытое сообщение, тогда как во втором случае его существование не скрывается.

Одной из важнейших проблем стеганографии, является проблема устойчивости стеганографических систем. Каждая из указанных выше областей применения стеганографии требует определенного соотношения между устойчивостью встроенного сообщения к внешним влияниям и размером встроенного сообщения. Для большинства современных методов, которые используются для сокрытия сообщений в файлах

цифрового формата, имеет место зависимость надежности системы от объема встраиваемых данных, представленная на рис. 1.

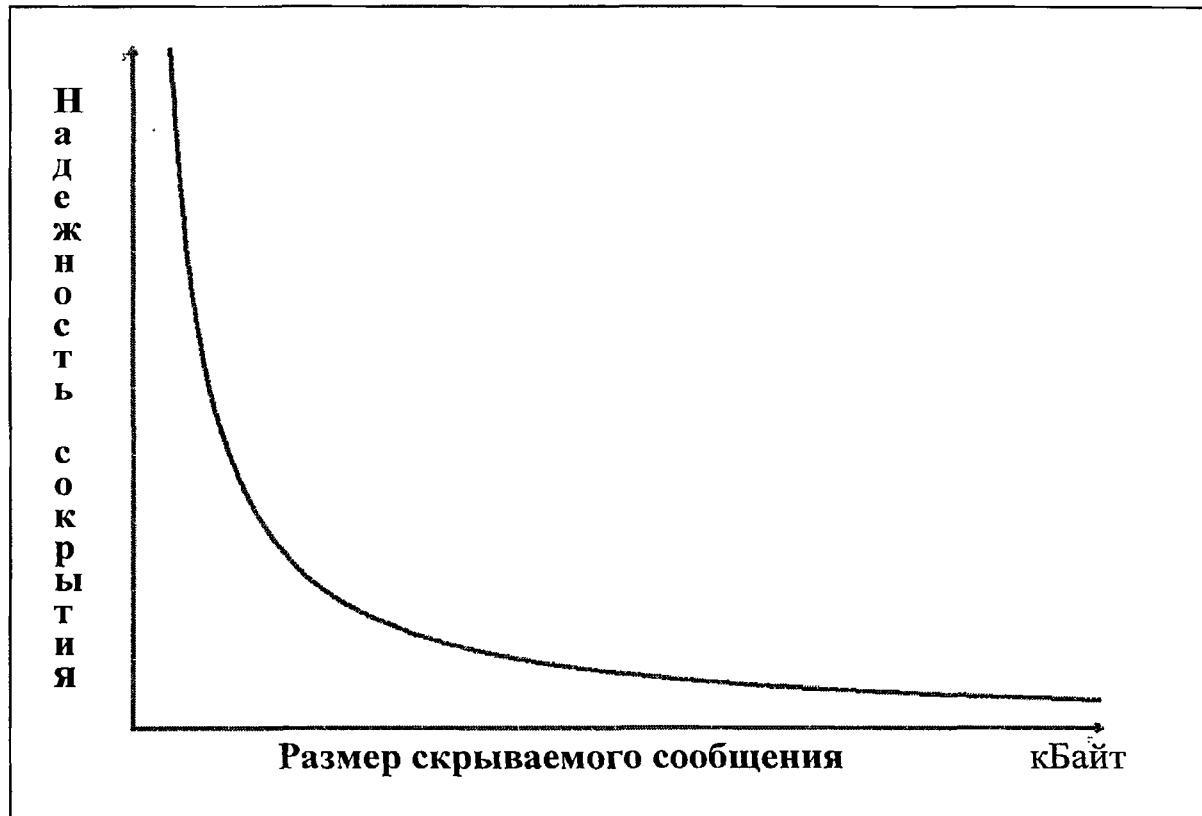


Рис. 1. Взаимосвязь между устойчивостью стеганосистемы и объемом скрываемого сообщения при неизменном размере файла – контейнера.

Из рис. 1 видно, что увеличение объема встраиваемых данных значительно снижает надежность системы. Таким образом, имеется проблема принятия оптимального решения при выборе между количеством (объемом) скрываемых данных и степенью устойчивости (сокрытия) к возможной модификации (анализу) сигнала - контейнера. Путем ограничения степени ухудшения качества контейнера, которые способен воспринимать человек, при стеганографической обработке контейнера можно достичь или высокого уровня (объема) встраиваемых

данных, или высокой устойчивости к модификации (анализу), но никоим образом не обоих этих показателей одновременно, поскольку рост одного из них неизбежно приводит к уменьшению другого.

1.2. Построение стеганографической системы.

Как бы ни отличались направления использования стеганографии, выдвигаемые при этом требования, во многом, остаются неизменными. Так, свойства контейнера должны быть модифицированы настолько, чтобы изменения невозможно было выявить при визуальном контроле. Это требование определяет качество сокрытия внедряемого сообщения: обеспечение беспрепятственного прохождения стегосообщения по каналу связи так, чтобы оно никаким образом не могло привлечь внимание противника [17]. Обобщенная структурная схема стеганосистемы изображена на рис. 2.

Основными стеганографическими понятиями являются *сообщение*, *контейнер* и *ключ*. Термин "контейнер" употребляется в отечественной литературе большинством авторов, поскольку является дословным переводом устоявшегося английского термина "container", обозначающего несекретную информацию, которую используют для сокрытия сообщений. По сути же, контейнер в стеганографической системе является ничем иным как *носителем секретной информации*.

Сообщением называется секретная информация, наличие которой необходимо скрыть.

Ключ представляет собой некоторую секретную информацию, известную только законному пользователю.

Стеганографической системой называют совокупность сообщений, секретных ключей, контейнеров и связывающих их преобразований.

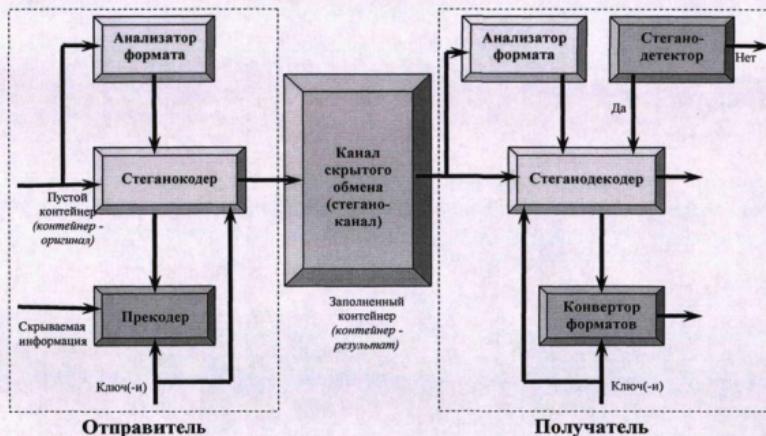


Рис. 2. Структурная схема стеганосистемы как системы связи

В общем случае (Рис.2), в стеганосистему входит: пустой контейнер (или, как еще говорят, *немодифицированный контейнер*), не содержащий секретной информации; заполненный контейнер (или, соответственно *модифицированный контейнер*), содержащий скрытое сообщение; прекодер, с помощью которого производится начальная обработка скрываемой информации; стеганокодер, предназначенный для упаковки сообщения в контейнер, стеганографический канал для передачи модифицированного контейнера; стеганодетектор, определяющий наличие в контейнере скрытых данных; и стеганодекодер, необходимый для выделения секретного сообщения из контейнера.

Существенное влияние на надежность и устойчивость стегосистемы, а также возможность обнаружения факта передачи скрытого сообщения оказывает выбор контейнера. Различают два основных типа контейнеров: *потоковый* и *фиксированный*.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что в кодере неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т.д., то скрываемая информация может идти сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи. Кроме того, потоковый контейнер имеет большое практическое значение. В качестве примера перспективной реализации потокового контейнера можно привести стеганоприставку к обычному телефону. Здесь под прикрытием заурядного, несущественного разговора можно передавать другой разговор, данные и т.п. Не зная секретного ключа, нельзя не только узнать о содержании скрытой передачи, но и о самом факте ее существования.

Наибольшее распространение получил *фиксированный контейнер*, размеры и характеристики которого заранее известны. Это позволяет осуществлять вложение данных оптимальным, в некотором смысле, образом.

Перед тем как выполнить вложение сообщения в контейнер, его необходимо преобразовать с помощью прекодера в определенный, удобный для упаковки, вид. Для повышения защищенности секретной информации, последнюю можно зашифровать достаточно устойчивым криптографическим кодом. Задачу встраивания и выделения сообщения из

другой информации выполняется стеганокодером и стеганодекодером. В большинстве стеганосистем для упаковки и извлечения сообщений используется ключ, который предопределяет секретный алгоритм, определяющий порядок внесения сообщения в контейнер. В качестве секретного алгоритма может быть использован генератор псевдослучайной последовательности (ПСП) битов. Качественный генератор ПСП, ориентированный на использование в системах защиты информации, должен обладать следующими свойствами:

- криптографической стойкостью;
- у нарушителя должны отсутствовать возможности предусмотреть следующий бит на основании известных ему предыдущих с вероятностью, отличной от $\frac{1}{2}$;
- хорошими статистическими свойствами - ПСП по своим статистическим свойствам не должна существенно отличаться от истинно случайной последовательности;
- большим периодом формирования последовательности;
- эффективной аппаратно – программной реализацией.

Алгоритм встраивания сообщения в простейшем случае состоит из двух этапов:

1. Встраивание в стеганокодере секретного сообщения в немодифицированный контейнер.
2. Обнаружение (выделение) в стеганодетекторе (декодере) скрытого сообщения из модифицированного контейнера.

Математическую модель стеганосистемы можно представить в виде двух зависимостей:

$$E : C \times M \rightarrow S, \quad (1.1)$$

$$D : S \rightarrow M, \quad (1.2)$$

где S - множество контейнеров – результатов.

C - множество контейнеров – оригиналов.

M - множество секретных сообщений.

E - алгоритм прямого стеганографического преобразования.

D - алгоритм обратного стеганографического преобразования.

Зависимость (1.1) описывает процесс сокрытия информации, зависимость (1.2) – процесс извлечения сообщения. В общем случае, стеганосистему можно представить как совокупность $\sum(C, M, S, E, D)$.

В стеганографии различают системы с секретным ключом и системы с открытым ключом. В первых – используется один ключ, который должен быть заранее известен авторизованным абонентам до начала скрытого обмена секретными сообщениями (или же переслан защищенным каналом во время указанного обмена). В системах с открытым ключом для встраивания и извлечения скрытой информации используются разные, не выводимые один из другого ключи — открытый и секретный.

Учитывая большое разнообразие стеганографических систем, целесообразно свести их к следующим четырем типам:

- бесключевые стеганосистемы;
- стеганосистемы с секретным ключом;
- стеганосистемы с открытым ключом;
- смешанные стеганосистемы.

1.2.1. Бесключевые стеганосистемы.

Для функционирования бесключевых стеганосистем, кроме алгоритма стегано-графического преобразования, отсутствует необходимость в дополнительных данных, наподобие стеганоключа. Таким образом, безопасность бесключевых стеганосистем базируется только на секретности используемых стеганографических преобразований

E и D . Это не самый лучший подход к системам защиты информации, поскольку стойкость системы зависит только от степени проинформированности нарушителя относительно функций E и D .

Для повышения безопасности бесключевых систем перед началом процесса стеганографического сокрытия предварительно выполняется криптографическое шифрование скрываемой информации. Такой подход увеличивает защищенность всего процесса связи, поскольку усложняет выявление скрытого сообщения. Однако "сильные" стеганосистемы, как правило, способны выполнять возложенные на них функции без предварительной криптографической защиты встроенного сообщения.

1.2.2. Стеганосистемы с секретным ключом.

Безопасность системы должна базироваться на определенном фрагменте секретной информации — ключе, который (как правило, предварительно) разделяется между авторизованными лицами. Отправитель, встраивая секретное сообщение в выбранный контейнер, использует стеганоключ. Если получатель знает данный ключ, то он может извлечь из контейнера скрытое сообщение. Без знания ключа любое постороннее лицо этого сделать не сможет. Данный тип стеганосистем предполагает наличие безопасного (защищенного) канала обмена стеганоключами.

Иногда стеганоключ вычисляют с помощью секретной хэш-функции (hash function), используя некоторые характерные черты контейнера. Если стеганопреобразование E не изменяет в окончательной стеганограмме выбранные особенности контейнера, то получатель также сможет вычислить стеганоключ (хотя и в этом случае защита будет зависеть от секретности хэш-функции). Очевидно, что для достижения адекватного уровня защиты такую особенность в контейнере необходимо выбирать достаточно внимательно.

В некоторых алгоритмах во время извлечения скрытой информации

дополнительно необходимы сведения о первичном (пустом) контейнере или некоторые другие данные, отсутствующие в стеганограмме. Такие системы представляют ограниченный интерес, поскольку они требуют передачи изначального вида контейнера, что эквивалентно традиционной задаче обмена ключами.

1.2.3. Стеганосистемы с открытым ключом.

Стеганография с открытым ключом опирается на достижения криптографии последних 30 лет. Стеганографические системы с открытым ключом не имеют потребности в дополнительном канале ключевого обмена. Для их функционирования необходимо иметь два стеганоключа: один секретный, который необходимо хранить в тайне, а другой — открытый, который может храниться в доступном для всех месте. При этом открытый ключ используется для встраивания сообщения, а секретный — для его извлечения.

Следует отметить, что стеганоключ не шифрует данные, а скрывает место их встраивания в контейнере. Скрытые данные могут быть дополнительно зашифрованы классическим методом, но этот вопрос не касается непосредственно стеганографии.

Стеганосистемы с открытым ключом используют тот факт, что функция извлечения скрытых данных D может быть применена к любому контейнеру, независимо от того, находится в нем скрытое сообщение или нет. Если скрытое сообщение отсутствует, то на выходе будет получена некоторая случайная последовательность. Если эта последовательность статистически не отличается от шифртекста крипtosистемы с открытым ключом, тогда в безопасной стеганосистеме можно скрывать полученный таким образом шифртекст, а не открытый текст.

1.2.4. Смешанные стеганосистемы.

На практике преимущество отдается бесключевым стеганосистемам, хотя последние могут быть раскрыты в случае, если нарушитель узнает о методе стеганопреобразования, который был при этом использован. В связи с этим в бесключевых системах часто используют особенности криптографических систем с открытым или секретным ключом.

Учитывая большое разнообразие форматов, которые могут иметь скрываемые сообщения и контейнеры (текст, звук или видео, которые, в свою очередь, также делятся на подформаты), представляется целесообразным предварительное преобразование сообщения в удобный для встраивания и оптимальный с точки зрения скрытости в заданном контейнере формат. Другими словами, необходимо учитывать как особенности встраиваемого сообщения, так и особенности контейнера, в который планируется его ввести.

1.3. Виды атак на стеганографическую систему.

Стеганосистема считается взломанной, если нарушителю удалось, по крайней мере, доказать существование скрытого сообщения в перехваченном контейнере. Предполагается, что нарушитель способен осуществлять любые типы атак и имеет неограниченные вычислительные возможности. Если ему не удается подтвердить гипотезу о том, что в контейнере скрыто секретное сообщение, то стеганографическая система считается устойчивой. В большинстве случаев выделяют несколько этапов взлома стеганографической системы:

- обнаружение факта присутствия скрытой информации;
- извлечение скрытого сообщения;
- видоизменение (модификация) скрытой информации;
- запрет на выполнение любой пересылки информации, в том числе

скрытой.

Первые два этапа относятся к пассивным атакам на стеганосистему, а последние - к активным (или злонамеренным) атакам. Выделяют следующие виды атак на стеганосистемы (по аналогии с криптоанализом):

Атака на основании известного заполненного контейнера. В этом случае нарушитель имеет в своем распоряжении один или несколько заполненных контейнеров (в последнем случае предполагается, что встраивание скрытой информации выполнялось одним и тем же способом). Задача нарушителя может заключаться в выявлении факта наличия стеганоканала (основное задание), а также в извлечении данных или определении ключа. Зная ключ, нарушитель имеет возможность анализа других стеганосообщений.

Атака на основании известного встроенного сообщения. Этот тип атаки в большей мере характерен для систем защиты интеллектуальной собственности, когда в качестве ЦВЗ, например, используется известный логотип фирмы. Задачей анализа является получение ключа. Если соответствующий скрытому сообщению заполненный контейнер неизвестен, то задача является практически неразрешимой.

Атака на основании выбранного скрытого сообщения. В этом случае нарушитель может предлагать для передачи свои сообщения и анализировать полученные при этом контейнеры - результаты.

Адаптивная атака на основании выбранного сообщения. Эта атака является частным случаем предыдущей. При этом нарушитель имеет возможность выбирать сообщения для навязывания их передачи адаптивно, в зависимости от результатов анализа предшествующих контейнеров-результатов.

Атака на основании выбранного заполненного контейнера. Этот тип атаки более характерен для систем ЦВЗ. У стеганоаналитика есть детектор заполненных контейнеров в виде "черного ящика" и несколько таких

контейнеров. Анализируя продетектированные скрытые сообщения, нарушитель пытается раскрыть ключ.

Кроме того, у нарушителя может существовать возможность применять еще три атаки, не имеющих прямых аналогов в криптоанализе:

Атака на основании известного пустого контейнера. Если последний известен нарушителю, то путем сравнения его с подозреваемым на присутствие скрытых данных контейнером он всегда может установить факт наличия стеганоканала. Несмотря на тривиальность этого случая, в ряде изданий приводится его информационно - теоретическое обоснование. Намного более интересным представляется сценарий, когда контейнер известен приблизительно, с некоторой погрешностью (например, если к нему добавлен шум). В этом случае существует возможность построения устойчивой стеганосистемы.

Атака на основании выбранного пустого контейнера. В этом случае нарушитель способен заставить воспользоваться предложенным им контейнером. Последний, например, может иметь значительные однородные области (однотонные изображения), и тогда обеспечить секретность встраивания будет непросто.

Атака на основании известной математической модели контейнера или его части. При этом атакующий пытается определить отличие подозреваемого сообщения от известной ему модели. Например, можно допустить, что биты в середине определенной части изображения являются коррелированными. Тогда отсутствие такой корреляции может служить сигналом о наличии скрытого сообщения. Задача того, кто встраивает сообщение, заключается в том, чтобы не нарушить статистики контейнера. Отправитель и тот, кто атакует, могут иметь в своем распоряжении разные модели сигналов, тогда в информационно - скрывающем противоборстве победит тот, кто владеет более эффективной (оптимальной) моделью.

Основная цель атаки на стеганографическую систему аналогична цели атак на криптосистему с той лишь разницей, что резко возрастает значимость активных (злонамеренных) атак. Любой контейнер может быть заменен с целью удаления или разрушения скрытого сообщения, независимо от того, существует оно в контейнере или нет. Обнаружение существования скрытых данных ограничивает время на этапе их удаления, необходимое для обработки только тех контейнеров, которые содержат скрытую информацию.

Даже при оптимальных условиях для атаки, задача извлечения скрытого сообщения из контейнера может оказаться очень сложной. Однозначно утверждать о факте существования скрытой информации можно только после ее выделения в явном виде. Иногда целью стеганографического анализа является не алгоритм вообще, а поиск, например, конкретного стеганоключа, используемого для выбора битов контейнера в стеганопреобразовании.

1.4. Стеганографические методы сокрытия данных.

Стеганография представляет собой науку о методах сокрытия информации в контейнерах без нарушения их естественности. Наиболее распространенными типами контейнеров на данный момент являются растровые графические изображения, представленные в цифровой виде различных форматов, а также видеопоследовательности. Это объясняется тем, что подобные контейнеры уже по технологии получения имеют шумовую составляющую, которая маскирует встраиваемое сообщение.

Другим типом контейнеров, являются аудио-сигналы. Этому типу контейнеров в данное время уделяется гораздо меньшее внимание. По видимому, данный факт объясняется как сложностью обработки, так и

более низким, по сравнению с изображениями, коэффициентом использования контейнера.

Опишем современные стеганографические методы сокрытия данных для разных типов информационной среды в качестве стеганоконтейнера. Подавляющее большинство методов КС базируются на двух ключевых принципах [18]:

1. файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и т.д.), могут быть видоизменены (конечно, до определенной степени) без потери своей функциональности;
2. органы чувств человека неспособны надежно различать незначительные изменения в модифицированных таким образом файлах, или отсутствует специальный инструментарий, который был бы способен выполнять данную задачу.

Для существующих методов КС вводят следующую классификацию (Рис. 3) [19].



Рис 3. Классификация методов компьютерной стеганографии

По способу выбора контейнера различают суррогатные, селективные и конструирующие методы стеганографии.

В суррогатных (безальтернативных) методах стеганографии полностью отсутствует возможность выбора контейнера, и для сокрытия сообщения избирается первый попавшийся контейнер, который в большинстве случаев не оптимален для сокрытия сообщения заданного формата.

В селективных методах КС предусматривается, что скрываемое сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое

количество альтернативных контейнеров с последующим выбором наиболее оптимального из них для конкретного сообщения. Особым случаем такого подхода является вычисление некоторой хэш-функции для каждого контейнера. При этом для сокрытия сообщения избирается тот контейнер, хэш-функция которого совпадает со значением хэш-функции сообщения.

В конструирующих методах стеганографии контейнер генерируется самой стеганосистемой. При этом существует несколько вариантов реализации. Так, например, шум контейнера может имитироваться скрываемым сообщением. Это реализуется с помощью процедур, которые не только кодируют скрываемое сообщение под шум, но и сохраняют модель изначального шума. В предельном случае по модели шума может строиться целое сообщение.

По способу доступа к скрываемой информации различают методы для потоковых контейнеров и методы для фиксированных контейнеров.

По способу организации контейнеры, подобно помехоустойчивым кодам, могут быть систематическими и несистематическими. В первых можно указать конкретные места стеганограммы, где находятся информационные биты собственно контейнера, а где — шумовые биты, предназначенные для скрытия информации (как, например, в широко распространенном методе замены наименее значащего бита). В случае несистематической организации контейнера такое разделение невозможно. В этом случае для выделения сокрытой информации необходимо обрабатывать содержимое всей стеганограммы.

По используемому принципу сокрытия методы КС делятся на два основных класса: методы непосредственной замены и спектральные методы. Если первые, используя избыток информационной среды в пространственной (для изображения) или временной (для звука) области, заключаются в замене малозначащей части контейнера битами секретного

сообщения, то другие для сокрытия данных используют спектральные представления элементов среды, в которую встраиваются скрываемые данные.

Основным направлением КС является использование свойств именно избыточности контейнера-оригинала, но при этом следует принимать во внимание то, что в результате сокрытия информации происходит искажение некоторых статистических свойств контейнера или же нарушение его структуры. Это необходимо учитывать для уменьшения демаскирующих признаков.

В особую группу можно также выделить методы, которые используют специальные свойства форматов представления файлов:

- зарезервированные для расширения поля файлов, которые зачастую заполняются нулями и не учитываются программой;
- специальное форматирование данных (сдвиг слов, предложений, абзацев или выбор определенных позиций символов);
- использование незадействованных участков на магнитных и оптических носителях;
- удаление файловых заголовков-идентификаторов и т.д.

В основном, для таких методов характерны низкая степень скрытости, низкая пропускная способность и слабая производительность.

По назначению различают стеганометоды собственно для сокрытой передачи (или скрытого хранения) данных и методы для скрытия данных в цифровых объектах с целью защиты авторских прав на них.

По типам контейнера выделяют стеганографические методы с контейнерами в виде текста, аудиофайла, изображения и видео.

Рассмотрим подробнее стеганографические методы сокрытия данных в неподвижных изображениях, в аудиосигналах и в видеопоследовательностях.

1.4.1. Сокрытие данных в неподвижных изображениях.

Значительная часть исследований в области стеганографии посвящена встраиванию конфиденциальных сообщений и ЦВЗ в статическую графику, которая является одним из наиболее распространенных видов информации. Изначально большое внимание уделялось сокрытию информации в файлах форматов, не использовавших сжатие (примером может служить формат BMP, или Windows Bitmap). В этот период были разработаны не только действенные методы маскирования данных, но и способы атак, позволявших устанавливать факт наличия встроенной информации. Быстрый рост объемов графической информации потребовал создания высокоэффективных алгоритмов сжатия [20]. Таким образом, большинство исследований посвящено использованию в качестве стегоконтейнеров изображений. Это обусловлено следующими причинами:

- актуальностью задачи защиты фотографий, картин, видео от незаконного тиражирования и распространения;
- относительно большим объемом цифрового представления изображений, что позволяет внедрять ЦВЗ большого объема либо повышать устойчивость этого внедрения;
- заранее известным размером контейнера, отсутствием ограничений, накладываемых требованиями реального времени;
- наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и хорошо подходящих для встраивания информации;
- слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержанию в нем шума, искажениям вблизи контуров;
- хорошо разработанными в последнее время методами цифровой обработки изображений.

Надо отметить, что последняя причина вызывает и значительные трудности в обеспечении надежности ЦВЗ: чем более совершенными становятся методы сжатия, тем меньше остается возможностей для встраивания посторонней информации. Развитие теории и практики алгоритмов сжатия изображений привело к изменению представлений о технике внедрения ЦВЗ. Если первоначально предлагалось вкладывать информацию в незначащие биты для уменьшения визуальной заметности, то современный подход заключается во встраивании ЦВЗ в наиболее существенные области изображений, разрушение которых приведет к полной деградации самого изображения. В стегоалгоритмах зачастую используются те же преобразования, что и в современных алгоритмах сжатия. При этом существуют, очевидно, три возможности. Вложение информации может производиться в исходное изображение, либо одновременно с осуществлением сжатия изображения-контейнера, либо в уже сжатое (например, алгоритмом JPEG) изображение.

Привлекательность использования файловых форматов, построенных по схеме сжатия JPEG в целях сокрытия информации, обусловлена их широким распространением при передаче графических изображений, в частности, в сети Интернет.

В патенте [21] приводится метод и схема алгоритма, позволяющего улучшить качество встраивания водяных знаков. А именно, позволяющего сделать их более устойчивыми к таким преобразованиям, как сжатие графических изображений, изменение разрешения, поворот на заданный угол. Примерная схема оптимизации состоит в том, что перед окончательным встраиванием ЦВЗ производится анализ изменений, происходящих после применения тех или иных преобразований к графическому изображению. На основе результатов данного анализа выбирается оптимальный способ встраивания, то есть наиболее

устойчивый ко всем рассмотренным преобразованиям, и производится окончательное встраивание водяных знаков.

Вообще говоря, с точки зрения разработки стеганографических систем важны следующие особенности современных графических форматов:

- наличие в формате сжатия данных,
- наличие в формате сжатия данных с потерями,
- использование в формате палитры цветов.

В том случае, когда формат хранения растровых изображений использует сжатие данных, значительно возрастает сложность разработки стеганографической системы, так как, во-первых, увеличивается сложность анализа формата, а во-вторых, вносимые стеганографической системой в данные изображения изменения приводят к нежелательному ухудшению эффективности сжатия. В случае, когда формат графических изображений использует сжатие с потерями информации, классические методы сокрытия в графических изображениях становятся малоэффективными, так как при потерях информации происходит уничтожение сокрытой информации (в силу малой амплитуды сокрытого сигнала). Поэтому в данном случае необходимо проводить детальный анализ, направленный на поиск этапа сжатия, пригодного для сокрытия, после чего необходима адаптация классических методов сокрытия или разработка новых. Использование в формате хранения графических изображений палитры цветов, также затрудняет применение классических методов сокрытия. К примеру, в данном случае применим метод сокрытия в младших битах. Но не в младших битах данных графического изображения, которые в данном случае являются ссылками на элементы палитры (а следовательно, для сокрытия в младшие биты необходимо, чтобы элементы палитры, отличающиеся лишь младшим битом были

близки по интенсивностям цветовых составляющих, что выполнено далеко не всегда), а в младших битах элементов самой палитры, размер которой не превышает 256 цветов. Конечно же, данные особенности графических форматов важны лишь в случае разработки неформатных методов сокрытия, так как в случае разработки форматных методов основной информацией, необходимой для разработки, является непосредственно сам формат.

В результате детального анализа алгоритма сжатия с потерями JPEG [22], режимов его работы и промежуточных этапов, были разработаны методы, позволяющие производить неформатное сокрытие данных в файлы, форматы которых построены в соответствии со спецификацией JPEG:

- Метод сокрытия в исходных данных изображения;
- Метод сокрытия с использованием таблиц квантования;
- Метод использования ложных таблиц квантования;
- Метод сокрытия в спектре изображения после квантования;
- Метод дописывания данных в конец JPEG файла;
- Метод сокрытия в косвенных данных;
- Метод сокрытия с использованием уменьшенного изображения.

В качестве примера рассмотрим квантованный блок коэффициентов, условимся скрывать биты сообщения в младших битах тех квантованных отсчетов, модуль которых больше 1. Пусть сообщение - это слово "Hell!", в двоичной форме с учетом того, что мы будем скрывать первыми младшие биты оно примет вид: "00010010 10100110 00110110 00110110 10000100".

Блок до сокрытия сообщения:

161, -1, -10, -5, -10, 0, 9, 5,
24, 56, 38, 7, -14, 0, -2, 3,
10, 29, -30, 19, 7, -5, -1, -8,
10, 1, -29, 1, -15, 5, 1, -9,
-12, 4, -5, 9, 0, 0, 3, 4,
8, -16, -4, -1, -2, 0, -6, 10,
3, -1, 1, -3, 3, 2, 0, 3,
5, 8, 0, 0, -5, -1, -6, -1

Блок после сокрытия сообщения (жирным выделены коэффициенты, пригодные для сокрытия, подчеркнуты - измененные в результате сокрытия):

160, -1, -10, **-4**, **-11**, 0, **8**, **4**,
25, **56**, **39**, **6**, **-15**, 0, -2, **2**,
11, **29**, **-30**, **18**, **6**, **-5**, -1, **-9**,
10, 1, -29, 1, -15, **4**, 1, **-8**,
-12, **5**, **-5**, **8**, 0, 0, 3, **5**,
8, **-17**, -4, -1, -2, 0, -6, 10,
3, -1, 1, **-2**, **2**, 2, 0, 3,
5, 8, 0, 0, -5, -1, -6, -1

Использование палитры в графических форматах связано с попыткой уменьшить размер хранимой информации. Вообще говоря, палитра впервые была применена в графических адаптерах для упрощения их устройства и обеспечения большего разрешения при меньшем объеме оперативной памяти графического адаптера. Вслед за этим появились форматы хранения растровых графических изображений, основанные на использовании палитры, некоторые из которых активно используются и в

наши дни. Примером такого формата может служить GIF, который получил широкое распространение в сети Интернет и является неотъемлемой частью дизайна современных веб-страниц и Интернет рекламы. Количество передаваемых по сети файлов в формате GIF более чем в два раза превышает количество передаваемых страниц и писем.

Существует большое количество методов сокрытия информации с использованием палитры, различающиеся как по принципу использования, так и по формату представления данных о палитре в различных форматах графических данных. Приведем некоторые из них:

- *Метод сокрытия с использованием младших бит данных изображения.*
- *Метод сокрытия, основанный на наличии одинаковых элементов палитры.*
- *Метод сокрытия путем перестановки элементов палитры.*

1.4.2. Сокрытие данных в аудио и видеопоследовательностях.

В последние годы появились программные комплексы, обеспечивающие сокрытие информации в цифровых аудио- и видеофайлах с помощью методов стеганографии. Одной из наиболее актуальных и сложных проблем КС является выявление факта такого сокрытия. В этих условиях при отсутствии априорной информации обнаружение скрытого сообщения возможно на основе выявления нарушений естественных зависимостей, присущих натуральному файлу-контейнеру.

При рассмотрении вопросов внедрения информации в аудиосигналы, необходимо определить требования, которые могут быть предъявлены к стегосистемам, применяемым для встраивания информации в аудиосигналы:

- скрываемая информация должна быть стойкой к наличию различных окрашенных шумов, сжатию с потерями, фильтрованию, аналого-цифровому и цифро-аналоговому преобразованиям;
- скрываемая информация не должна вносить в сигнал искажения, воспринимаемые системой слуха человека;
- попытка удаления скрываемой информации должна приводить к заметному повреждению контейнера (для ЦВЗ);
- скрываемая информация не должна вносить заметных изменений в статистику контейнера.

Одним из наиболее перспективных подходов для анализа стеганографического сокрытия является подход, рассматривающий введение в файл скрываемой информации как вмешательство в статистические закономерности, нарушение естественности физического процесса. При данном подходе процесс сокрытия описывается не детерминированным образом, а вероятностным, то есть прогнозируемым с некоторой вероятностью изменением естественных связей.

В качестве мест для внедрения скрываемой информации обычно используются младшие разряды отсчетов, которые принято называть наименее значимыми битами (НЗБ). Проведенные статистические исследования звуковых файлов позволили выявить ряд перспективных для анализа статистик: хи - квадрат, Спирмена и коэффициент корреляции.

Как показывают исследования, эти статистики примерно одинаково реагируют на замену значений НЗБ. Но статистика хи – квадрат требует наименьшего количества вычислительных операций. С помощью функции хи - квадрат, используемой в критерии независимости двух случайных величин, показано [23], что для исходного контейнера НЗБ и остальные разряды статистически зависимы. Показательным является тот факт, что внедрение скрываемого сообщения нарушает естественную природу цифрового аудиоконтейнера, что выражается в уменьшении

значений статистики хи - квадрат, то есть в случае частичного заполнения НЗБ и остальные разряды продолжают оставаться зависимыми, но все же степень зависимости по сравнению с исходной уменьшается. При полном замещении НЗБ становятся независимыми от остальных разрядов. Эти результаты показывают, что изменение значения статистики хи - квадрат является демаскирующим признаком и позволяет выявлять стеганографическое сокрытие информации.

Одним из вопросов при анализе любого метода стеганографического сокрытия данных является вопрос устойчивости внедренной информации, к различного рода искажениям. Очевидно, что метод сокрытия в наименьших значащих битах не в состоянии обеспечить какую либо устойчивость при передаче сигнала по реальным каналам связи. Даже при использовании кодов обнаружения и коррекции ошибок, используемые в реальных цифровых каналах связи алгоритмы сжатия аудио сигнала приведут к потере наименее значащих битов. При передаче по аналоговым линиям неизбежно добавление некоторого шума, как самого канала, так и аппаратуры АЦП и ЦАП, что также приведет к потере информации. Единственной средой передачи, использование которой не приведет к уничтожению передаваемой информации, являются цифровые линии связи или компьютерные сети.

Таким образом, этот метод хорошо подходит для случаев передачи информации между отправителем и получателем в цифровом виде при наличии гарантий, что по пути следования аудио сигнал не будет подвергнут какому либо преобразованию.

Человеческое ухо практически нечувствительно к абсолютному значению фазы гармоник, составляющих аудио сигнал. Основываясь на данном факте, в [24] был предложен алгоритм *внедрения передаваемого сообщения в фазовую часть* аудио сигнала. Суть данного метода состоит в модификации фазы начального сегмента в зависимости от внедряемых

данных. Фаза последующих сегментов согласовывается с новой фазой первого сегмента для сохранения разности фаз. Аудио сигналом - контейнером в данном методе выступает несжатый аудио сигнал, оцифрованный с разрядностью 16 бит на отсчет. Сообщение представляет собой битовую последовательность ограниченной длины.

Метод внедрения передаваемого сообщения в фазовую часть аудио сигнала характеризуется достаточной степенью скрытности, но относительно небольшим коэффициентом использования сигнала-контейнера. Кроме того, на основе анализа непрерывности фазы, можно находить точки начала исходных аудио сигналов, что может быть использовано для построения метода стеганоанализа.

Алгоритм MPEG (Motion Picture Experts Group - Экспертная группа по вопросам движущегося изображения) является наиболее популярным стандартом кодирования видео. Основная идея сжатия по MPEG состоит в том, что из всего потока данных полностью передаются только некоторые кадры, для остальных же передается их отличие от других кадров. Поток видеоданных в MPEG имеет иерархическую синтаксическую структуру. Каждый уровень содержит один или более подчиненных уровней, как это показано на рис. 4. Последовательность видеоданных разделяется на множество групп кадров (ГК), представляющих собой множество видеокадров, непосредственно следующих друг за другом в порядке показа. Далее, кадры подразделяются на слои и макроблоки. Низший уровень, блоковый, состоит из блоков яркости и цветности макроблока.

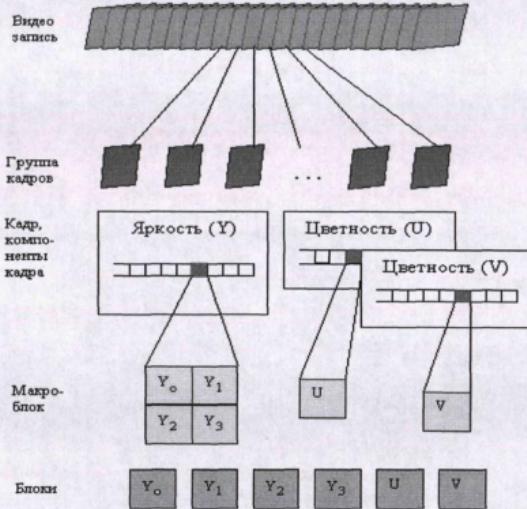


Рис.4. Многоуровневая синтаксическая структура MPEG

В пределах ГК времененная избыточность среди видеокадров уменьшается за счет временного предсказания. Это означает, что одни кадры предсказываются по другим. Затем результирующая ошибка предсказания кодируется.

Метод, позволяющий производить внедрение ЦВЗ в цифровое видео изображение, сжатое с потерями информации с помощью алгоритма MPEG предложен в патенте [25], где в качестве ЦВЗ используются растровые графические изображения.

Глава II

Математические модели вкрапления скрытой информации и их статистический анализ.

2.1. Биномиальная модель вкрапления информации

Теоретико-вероятностная модель скрытого вкрапления передаваемой закрытой информации в мультимедийные файлы имеет следующий вид.

Пусть имеется массив случайных двоичных знаков $\bar{\xi} = (\xi_1, \dots, \xi_n)$ с независимыми в совокупности бернуlliевскими элементами, принимающими значения 1 и 0 с вероятностями соответственно p_0 и q_0 ($p_0 > 0, q_0 > 0, p_0 + q_0 = 1$). Вкрапление закрытой информации осуществляется путем случайного выбора в этом массиве k позиций ($0 < k \leq n$) и заменой на этих позициях исходных элементов ξ другими бернуlliевскими элементами $\bar{\eta} = (\eta_1, \dots, \eta_k)$, независимыми от исходных элементов и между собой и принимающими значения 1 и 0 с некоторыми другими вероятностями p_1 и q_1 ($p_1 > 0, q_1 > 0, p_1 + q_1 = 1$). Этую операцию будем обозначать символом Δ , таким образом, наблюдению доступен массив (последовательность) $\bar{\zeta} = \bar{\xi} \Delta \bar{\eta}$.

Основными задачами анализа такой модели являются:

1. проверка гипотезы H_0 об отсутствие вкраплений, то есть $H_0 : k = 0$, при альтернативе $H_1 : k > 0$ о наличии вкраплений, и
2. оценивание числа k вкраплений (при справедливости альтернативы H_1).

Параметрами описанной модели являются p_0, p_1 и k , и решение этих задач существенно зависит от априорных предположений об этих параметрах. Ниже будут рассмотрены различные варианты конкретизаций нашей модели в терминах этих параметров.

2.1.1. Статистически критерий обнаружения вкраплений.

Рассмотрим сначала случай, когда p_0 и p_1 известны и будем считать, для определенности, что $\Delta p = p_0 - p_1 > 0$.

Для различия гипотез H_0 и H_1 в данном случае будем использовать тестовую статистику ρ_n – число единиц в наблюдаемой последовательности $\bar{\zeta} = (\zeta_1, \dots, \zeta_n)$:

$$\rho_n = \sum_{i=1}^n \zeta_i . \quad (2.1)$$

Очевидно, что при отсутствии вкраплений эта статистика имеет биномиальное распределение

$$\mathcal{L}(\rho_n | H_0) = Bi(n, p_0); \quad (2.2)$$

в частности,

$$\mathbf{E}(\rho_n | H_0) = np_0, \quad \mathbf{D}(\rho_n | H_0) = np_0 q_0. \quad (2.3)$$

Для изучения распределения статистики ρ_n при альтернативе, введем простую альтернативу $H_{1,k}$, фиксирующую число вкраплений $k > 0$. Тогда в рассматриваемой модели при этой альтернативе среди слагаемых в (2.1)

будет присутствовать k бернульиевых элементов η . (обозначим их сумму $|\eta|_k$) и $n-k$ бернульиевых элементов ξ . (обозначим их сумму $|\xi|_{n-k}$). Таким образом, при альтернативе $H_{1,k}$ статистика ρ_n имеет представление

$$\rho_n = |\xi|_{n-k} + |\eta|_k, \quad (2.4)$$

причем слагаемые здесь независимы и имеют соответственно биномиальные распределения $Bi(n-k, p_0)$ и $Bi(k, p_1)$. Следовательно,

$$\mathcal{L}(\rho_n | H_{1,k}) = Bi(n-k, p_0) * Bi(k, p_1) \quad (2.5)$$

(знак * означает операцию свертки).

Из (2.4) и (2.5), в частности, имеем, что

$$\begin{aligned} E(\rho_n | H_{1,k}) &= (n-k)p_0 + kp_1 = np_0 - k\Delta p < np_0, \\ D(\rho_n | H_{1,k}) &= (n-k)p_0 q_0 + kp_1 q_1 = np_0 q_0 - k(p_0 q_0 - p_1 q_1). \end{aligned} \quad (2.6)$$

Из соотношения (2.5) можно также вычислить и распределение тестовой статистики ρ_n при альтернативе $H_{1,k}$ (функцию правдоподобия):

$$\begin{aligned}
L_{n,k}(s) &= \mathbf{P}(\rho_n = s | H_{1,k}) = \mathbf{P}(|\xi|_{n-k} + |\eta|_k = s) = \\
&= \sum_{m=0}^{s \wedge k} \mathbf{P}(|\eta|_k = m) \mathbf{P}(|\xi|_{n-k} = s - m) = \\
&= \sum_{m=0}^{s \wedge k} \binom{k}{m} p_1^m q_1^{k-m} \binom{n-k}{s-m} p_0^{s-m} q_0^{n-k-s+m} = \\
&= p_0^s q_0^{n-k-s} q_1^k \sum_{m=0}^{s \wedge k} \binom{k}{m} \binom{n-k}{s-m} z^m, \quad z = \frac{p_1 q_0}{q_1 p_0}
\end{aligned} \tag{2.7}$$

(здесь $s \wedge k = \min(s, k)$).

При нулевой гипотезе функция правдоподобия есть

$$L_{n,0}(s) = \mathbf{P}(\rho_n = s | H_0) = \binom{n}{s} p_0^s q_0^{n-s},$$

поэтому отношение правдоподобия равно

$$\ell_{n,k}(s) = \frac{L_{n,k}(s)}{L_{n,0}(s)} = \left(\frac{q_1}{q_0} \right)^k \sum_{m=0}^{s \wedge k} \frac{\binom{k}{m} \binom{n-k}{s-m}}{\binom{n}{s}} z^m. \tag{2.8}$$

Эти результаты дают возможность построить критерий Неймана – Пирсона для различения гипотез H_0 и $H_{1,k}$ (см., напр. [27, §4.2]): такой критерий задается критической областью

$$\mathcal{X}_{1,\alpha} = \{s : \ell_{n,k}(s) \geq c_\alpha\}, \tag{2.9}$$

где критическая граница c_α , отвечающая вероятности ошибки первого рода (уровню значимости) α , определяется условием:

$$P(X_{1,\alpha} | H_0) = P(\ell_{n,k}(\rho_n) \geq c_\alpha | H_0) = \alpha. \quad (2.10)$$

Замечание. Отметим, что, с точностью до множителя $(q_1/q_0)^k$, отношение правдоподобия $\ell_{n,k}(s)$ (см.(2.8)) есть производящая функция гипергеометрического распределения в точке $z = \frac{p_1 q_0}{q_1 p_0}$, которую, в свою очередь, можно записать через гипергеометрическую функцию:

$$F(a, b, c; z) = \sum_{m=0}^{\infty} \frac{(a)_m (b)_m}{(c)_m} \frac{z^m}{m!}, \quad (2.11)$$

где $(a)_m = a(a+1)\dots(a+m-1)$, $m = 1, 2, \dots$, $(a)_0 = 1$.

Именно, так как

$$\frac{\binom{k}{m} \binom{n-k}{s-m}}{\binom{n-k}{s}} = \frac{(-k)_m}{m!} \frac{(-s)_m}{(n-k-s+1)_m},$$

то

$$\ell_{n,k}(s) = \left(\frac{q_1}{q_0}\right)^k \frac{\binom{n-k}{s}}{\binom{n}{s}} F(-k, -s, n-k-s+1; z). \quad (2.12)$$

Поскольку функция F- хорошо изученная специальная функция, включая ее асимптотическое поведение в зависимости от роста ее аргументов [26], представление (2.12) может быть использовано при

анализе асимптотического поведения отношения правдоподобия $\ell_{n,k}(s)$, когда $n, k \rightarrow \infty$.

2.1.2. Асимптотический вариант критерия Неймана-Пирсона.

Из выражения (2.8) видно, что точный расчет критерия (2.9)-(2.10) представляет собой трудную вычислительную задачу, поэтому будем рассматривать асимптотический вариант критерия при $n \rightarrow \infty$. Заметим, что асимптотический подход в данной проблематике вполне естественен, поскольку в действительности обычно мы имеем дело с большими массивами данных.

Введем нормированную статистику

$$\rho_n^* = \frac{\rho_n - np_0}{\sqrt{np_0 q_0}}, \quad (2.13)$$

которая при нулевой гипотезе H_0 , согласно теореме Муавра – Лапласа, при больших значениях n имеет асимптотически нормальное распределение $N(0,1)$.

Из формул (2.6) следует, что

$$\begin{aligned} E(\rho_n^* | H_{1,k}) &= -\frac{k \Delta p}{\sqrt{np_0 q_0}}, \\ D(\rho_n^* | H_{1,k}) &= 1 - \frac{k(p_0 q_0 - p_1 q_1)}{np_0 q_0}. \end{aligned} \quad (2.14)$$

Согласно представлению (2.4), при альтернативе $H_{1,k}$ статистика ρ_n^* также будет асимптотически нормальна с параметрами, указанными в (2.14). Отсюда следует, что если число вкраплений k таково, что $\frac{k}{\sqrt{n}} \rightarrow 0$, то гипотезы H_0 и $H_{1,k}$ асимптотически неразличимы (поскольку в этом случае $\mathcal{L}(\rho_n^* | H_{1,k}) \rightarrow \mathcal{N}(0,1)$, как и в случае нулевой гипотезы).

Статистика ρ_n^* будет «чувствительна» лишь к таким альтернативам $H_{1,k}$, для которых $\frac{k}{\sqrt{n}} \rightarrow \lambda > 0$. Для этого случая

$$\mathcal{L}(\rho_n^* | H_{1,k}) \rightarrow \mathcal{N}\left(-\frac{\lambda \Delta p}{\sqrt{p_0 q_0}}, 1\right), \quad (2.15)$$

и в асимптотике задача сводится к различию двух нормальных распределений: $\mathcal{N}(0,1)$ и $\mathcal{N}\left(-\frac{\lambda \Delta p}{\sqrt{p_0 q_0}}, 1\right)$ (по одному наблюдению над тестовой статистикой ρ_n^*).

Соответствующий критерий задается критической областью ([27, с. 188])

$$\mathcal{X}_{1,\alpha}^* = \{\rho_n^* < -t_\alpha\}, \quad \Phi(-t_\alpha) = \alpha, \quad (2.16)$$

где α - заданный уровень значимости, $\Phi(x)$ - стандартная нормальная функция распределения.

Мощность этого критерия, согласно (2.15), удовлетворяет следующему асимптотическому соотношению

$$W_{n,k} = P(\rho_n^* < -t_\alpha | H_{1,k}) \rightarrow \Phi\left(\lambda \frac{\Delta p}{\sqrt{p_0 q_0}} - t_\alpha\right). \quad (2.17)$$

Отметим, что предельная мощность (2.17) является монотонно возрастающей функцией параметра λ (чем больше вкраплений, тем легче этот факт обнаруживается критерием (2.16)).

Замечание. Определенная в (2.16) критическая область $\mathcal{X}_{1,\alpha}^*$ не зависит от параметра λ , характеризующего альтернативу $H_{1,k}$, поэтому эта критическая область максимизирует мощность при любой допустимой альтернативе (в данном случае, согласно (2.14), все альтернативы — левосторонние, то есть при любой из них распределение статистики ρ_n^* сдвинуто влево по отношению к распределению $N(0,1)$). Отсюда следует [27, с. 198], что построенный критерий Неймана — Пирсона является равномерно наиболее мощным критерием проверки гипотезы $H_0 : k = 0$ при сложной альтернативе $H_1 : k > 0$.

Отметим также, что в случае $\frac{k}{\sqrt{n}} \rightarrow \infty$ альтернатива $H_{1,k}$ улавливается критерием (2.16) с вероятностью, стремящейся к 1, то есть против такой альтернативы этот критерий состоятелен.

Подведем итог в виде следующего утверждения.

Теорема 1. В задаче различия гипотез H_0 и H_1 об отсутствии и наличии вкраплений соответственно существует асимптотически (при $n \rightarrow \infty$) равномерно наиболее мощный критерий, задаваемый соотношениями (2.16), (2.13) и (2.1), асимптотическая мощность которого при альтернативах $H_{1,k}$, для которых $k = k(n)$ таково, что $\frac{k}{\sqrt{n}} \rightarrow \lambda > 0$ («пороговый случай»), удовлетворяет соотношению (2.17). При $k = o(\sqrt{n})$ альтернативы $H_{1,k}$ асимптотически от нулевой гипотезы

этим критерием не отличаются, а против альтернатив $H_{1,k}$, для которых $\frac{k}{\sqrt{n}} \rightarrow \infty$, этот критерий состоятелен.

2.1.3. Схема серий биномиальной модели вкрапления

Основной проблемой в стеганографии является скрытие от «противника» самого факта вкрапления передаваемой закрытой информации. С этих позиций для передающей стороны важно организовать процесс вкрапления так, чтобы гипотезы H_0 и H_1 были асимптотически (при $n \rightarrow \infty$) неразличимы. Предыдущий анализ показывает, что если в рассматриваемой модели параметр вкрапления $p_1 (< p_0)$ фиксирован, то сам факт вкрапления надежно маскируется лишь при числе вкраплений $k = o(\sqrt{n})$. Увеличить объем надежно маскируемой вкрапляемой информации (в рамках изучаемой модели) можно путем выбора параметра p_1 , «близкого» к значению параметра p_0 . В этом случае мы должны рассмотреть «схему серий», полагая $p_1 = p_1(n) \rightarrow p_0$ при $n \rightarrow \infty$.

Итак, пусть при $n \rightarrow \infty$ разность $\Delta p = p_0 - p_1 = \Delta_n \rightarrow 0$.

Тогда при таких «близких» (к гипотезе H_0) альтернативах $H_{1,k}$ тестовая статистика ρ_n^* по-прежнему будет иметь асимптотически нормальное распределение:

$$\mathcal{L}(\rho_n^* | H_{1,k}) \sim \mathcal{N}\left(-\frac{k\Delta_n}{\sqrt{np_0q_0}}, 1\right) \quad (2.18)$$

(поскольку $p_0q_0 - p_1q_1 = (q_0 - p_0)\Delta_n - \Delta_n^2 \rightarrow 0$, то в (2.14) $D(\rho_n^* | H_{1,k}) = 1 + o(1)$ при всех $k \leq n$).

Из соотношения (2.18) следует, что факт вкрапления в этих условиях будет надежно

маскироваться, если $\frac{k\Delta_n}{\sqrt{n}} \rightarrow 0$, то есть при $k = o\left(\frac{\sqrt{n}}{\Delta_n}\right)$.

Таким образом, чем меньше величина $\Delta_n = p_0 - p_1$ (чем ближе $p_1 = p_1(n)$ к p_0), тем большее число вкрапляемых символов k можно передать, будучи гарантированно уверенным в том, что факт вкрапления не будет обнаружен. В частности, при $\Delta_n \asymp \frac{1}{\sqrt{n}}$ число вкраплений k может быть достаточно велико: лишь бы выполнялось условие $k = o(n)$. Пороговыми альтернативами в схеме серий являются альтернативы $H_{1,k}$, для которых $\frac{k\Delta_n}{\sqrt{n}} \rightarrow \delta > 0$. Для таких альтернатив критерий (2.16) будет иметь асимптотическую мощность $\Phi\left(\frac{\delta}{\sqrt{p_0 q_0}} - t_\alpha\right)$.

Итак, в схеме серий справедливо следующее заключение.

Теорема 2. Если при $n \rightarrow \infty$ параметр вкрапления p_1 имеет вид $p_1 = p_1(n) = p_0 - \Delta_n$, где $\Delta_n \rightarrow 0$, то при числе вкраплений $k = o\left(\frac{\sqrt{n}}{\Delta_n}\right)$ гипотезы H_0 и H_1 асимптотически не различимы, а при $\frac{k\Delta_n}{\sqrt{n}} \rightarrow \delta > 0$ («пороговый» случай) мощность критерия (2.16) удовлетворяет асимптотическому соотношению

$$W_{n,k} = \mathbf{P}(\rho_n^* < -t_\alpha | H_{1,k}) \rightarrow \Phi\left(\frac{\delta}{\sqrt{p_0 q_0}} - t_\alpha\right). \quad (2.19)$$

2.1.4. Оценивание числа вкраплений.

Предыдущие результаты дают также возможность достаточно просто решить и задачу оценивания числа вкраплений k по наблюдению над статистикой ρ_n (см. (2.1)). Именно, если имел место факт вкрапления (справедлива гипотеза $H_1 = \bigcup_{k>0} H_{1,k}$), то из соотношения (2.6) следует, что

статистика

$$\hat{k}_n = \frac{np_0 - \rho_n}{\Delta p} \quad (2.20)$$

удовлетворяет уравнению несмещенності: для любого $k > 0$

$$\mathbf{E}(\hat{k}_n | H_{1,k}) = \frac{1}{\Delta p} (np_0 - \mathbf{E}(\rho_n | H_{1,k})) = k. \quad (2.21)$$

Таким образом, \hat{k}_n является несмещенной оценкой для k .

Более того, при больших значениях n эта оценка является также асимптотической оценкой максимального правдоподобия. Действительно, как показано в п. 2.1.1, нормированная статистика ρ_n^* (см. (2.13)) при любой гипотезе $H_{1,k}$ имеет асимптотически нормальное распределение

$\mathcal{N}\left(-\frac{k\Delta p}{\sqrt{np_0q_0}}, 1\right)$. Но, как известно (см., напр., [27, §2.4]), для нормального

распределения с неизвестным средним (в данном случае это среднее есть

$-\frac{k\Delta p}{\sqrt{np_0q_0}}$) оценкой максимального правдоподобия по одному наблюдению

над соответствующей случайной величиной является наблюдаемая ее

реализация; следовательно, в данном случае оценкой для $-\frac{k\Delta p}{\sqrt{np_0q_0}}$ является ρ_n^* , и мы приходим к (2.20).

Вычислим еще дисперсию оценки \hat{k}_n . Из (2.6) имеем:

$$\begin{aligned} \mathbf{D}\left(\hat{k}_n \middle| H_{1,k}\right) &= \mathbf{D}\left(\frac{\rho_n}{\Delta p} \middle| H_{1,k}\right) = \\ &= \frac{1}{(\Delta p)^2} [np_0q_0 - k(p_0q_0 - p_1q_1)] = \\ &= \frac{np_0q_0}{(\Delta p)^2} \left[1 - \frac{k}{n} \left(1 - \frac{p_1q_1}{p_0q_0} \right) \right]. \end{aligned} \quad (2.22)$$

Это соотношение показывает, что дисперсия оценки \hat{k}_n с ростом n неограниченно растет, то есть эта оценка не является состоятельной и потому – практически непригодна.

Следовательно, в рассматриваемой задаче нужен другой подход, а именно, оценивать не само число k вкраплений, а, скажем, его долю $\lambda = k/n$. Этот новый параметр нашей модели уже имеет область возможных значений отрезок $[0,1]$ и, как следует из п. 2.1.2., чтобы реально этот параметр был не исчезающе мал при больших значениях n , нужно рассматривать модель в «схеме серий», полагая $p_1 = p_1(n) \rightarrow p_0$ при $n \rightarrow \infty$.

Итак, будем предполагать, что $n \rightarrow \infty$ и параметр вкраплений $p_1 = p_1(n)$ имеет вид

$$p_1 = p_0 + \frac{\tau}{\sqrt{n}}, \tau = \text{const} < 0. \quad (2.23)$$

Тогда, в этих обозначениях соотношение (2.18) принимает вид

$$\mathcal{L}(\rho_n^* | H_{1,k}) \sim \mathcal{N}\left(\lambda \frac{\tau}{\sqrt{p_0 q_0}}, 1\right). \quad (2.24)$$

Отсюда, как и выше, следует, что оценкой максимального правдоподобия параметра $\lambda = \frac{k}{n}$ в условиях (2.23) является статистика

$$\hat{\lambda}_n = \frac{\sqrt{p_0 q_0}}{\tau} \rho_n^* = \frac{\rho_n - np_0}{\tau \sqrt{n}}. \quad (2.25)$$

Для нее выполняется асимптотическое соотношение

$$\mathcal{L}(\hat{\lambda}_n | H_{1,k}) \sim \mathcal{N}\left(\lambda, \frac{p_0 q_0}{\tau^2}\right), \quad (2.26)$$

то есть она является асимптотически несмещенной, но по-прежнему не обладает свойством состоятельности: ее асимптотическая дисперсия не стремится к 0 при $n \rightarrow \infty$.

В то же время проведенный анализ показывает, что свойство состоятельности оценка (2.25) приобретает в ситуации, когда параметр $\tau = \tau(n) \rightarrow -\infty$ при $n \rightarrow \infty$, то есть при $-\tau = (p_0 - p_1)\sqrt{n} = \sqrt{n}\Delta_n \rightarrow \infty$.

Таким образом, справедлив следующий результат.

Теорема 3. Если при $n \rightarrow \infty$ выполняются следующие условия:
 $\Delta_n = p_0 - p_1 \rightarrow 0$, но $\sqrt{n}\Delta_n \rightarrow \infty$, то асимптотически несмещенной и состоятельной оценкой доли $\lambda = \frac{k}{n}$ числа вкраплений является статистика $\hat{\lambda}_n = \frac{np_0 - \rho_n}{n\Delta_n} = \frac{\hat{k}_n}{n}$, где \hat{k}_n определено в (2.20).

Более того, как следует из (2.21), эта оценка является в точности несмещенной, она асимптотически нормальна $\mathcal{N}\left(\lambda, \frac{p_0 q_0}{n \Delta_n^2}\right)$, и тем самым позволяет рассчитать асимптотический доверительный интервал для λ : такой интервал при доверительном уровне γ имеет вид (см. [27, с.144])

$$\left(\hat{\lambda}_n \mp c_\gamma \frac{\sqrt{p_0 q_0}}{\sqrt{n} \Delta_n} \right), \quad c_\gamma = \Phi^{-1} \left(\frac{1+\gamma}{2} \right).$$

Выводы

Итак, с позиции обеспечения надежности сокрытия вкрапляемой информации (а это главная проблема стеганографии) процесс вкрапления (в рамках рассматриваемой модели) должен быть организован так, чтобы выполнялось единственное условие

$$\frac{k \Delta_n}{\sqrt{n}} \rightarrow 0 \text{ при } n \rightarrow \infty,$$

где $\Delta_n = p_0 - p_1 \rightarrow 0$.

В свою очередь, это условие может быть обеспечено двумя способами:

- 1) $k = o(\sqrt{n})$ - тогда параметр вкрапления p_1 может быть любым, но число вкрапляемых символов при этом незначительно;
- 2) $\Delta_n \rightarrow 0$ (то есть $p_1 = p_1(n) \rightarrow p_0$) тогда для числа вкрапляемых символов возможности расширяются до границы $o\left(\frac{\sqrt{n}}{\Delta_n}\right)$, например, при $\Delta_n \sim \frac{1}{\sqrt{n}}$ число k может быть любым вида $o(n)$.

2.2. Параметрическая модель вкрапления информации

В предыдущем параграфе была рассмотрена одна простейшая модель вкрапления, когда в исходную бернуллиевскую последовательность $\bar{\xi} = (\xi_1, \dots, \xi_n)$ независимо вкрапляется некоторое фиксированное число k альтернативных бернуллиевских же элементов. Здесь мы рассматриваем другой вариант вкрапления, когда каждый элемент последовательности $\bar{\xi}$ с некоторой вероятностью $\theta > 0$ заменяется альтернативным бернуллиевским знаком, тем самым число k вкрапляемых знаков в этом случае случайно. Как и раньше, внимание акцентируется на выявление условий на параметры модели, обеспечивающих асимптотическую (при $n \rightarrow \infty$) неразличимость гипотез $H_0: \theta = 0$ (вкрапления отсутствуют) и $H_1: \theta > 0$ (наличие вкраплений). Оказывается, что выводы для обеих моделей «в среднем» аналогичны.

2.2.1. Определение модели вкрапления информации.

Достаточно общая модель вкрапления может выглядеть так: имеются три независимые последовательности из независимых одинаково распределенных случайных величин

$$\bar{\xi}_0 = (\xi_{01}, \xi_{02}, \dots, \xi_{0n}), \quad \bar{\xi}_1 = (\xi_{11}, \xi_{12}, \dots, \xi_{1n}) \text{ и } \bar{\delta} = (\delta_1, \delta_2, \dots, \delta_n),$$

где $\mathcal{L}(\xi_{01}) = F_0$, $\mathcal{L}(\xi_{11}) = F_1$ и $P(\delta_1 = 1) = 1 - P(\delta_1 = 0) = \theta \geq 0$,

а наблюдается последовательность $\bar{\xi} = (\xi_1, \dots, \xi_n)$,

где $\xi_i = I(\delta_i = 0)\xi_{0i} + I(\delta_i = 1)\xi_{1i}$, $i = 1, \dots, n$ ($I(A)$ - индикатор события A).

Последовательность $\bar{\xi}_0$ интерпретируется как исходное открытое сообщение, $\bar{\xi}_1$ - вкрапляемая (в $\bar{\xi}_0$) конфиденциальная информация и $\bar{\delta}$ - механизм вкрапления. Задача состоит в такой организации процесса вкрапления, чтобы по наблюдению последовательности $\bar{\xi}$ «противник» не мог обнаружить факт вкрапления, то есть различить гипотезы $H_0: \theta = 0$ и $H_1: \theta > 0$.

Возможны различные конкретизации и усложнения описанной модели, и далее мы будем рассматривать один ее частный (но близкий к стеганографической практике) вариант, когда $\bar{\xi}_0$ и $\bar{\xi}_1$ - бернульиевские последовательности.

Итак, пусть $\mathcal{L}(\xi_{01}) = Bi(1, p_0)$, $\mathcal{L}(\xi_{11}) = Bi(1, p_1)$ и, для определенности, $\Delta = p_0 - p_1 > 0$. Тогда наблюдаемая последовательность $\bar{\xi} = (\xi_1, \dots, \xi_n)$ - также бернульиевская и

$$p_\theta = \mathbf{P}_\theta(\xi_i = 1) = (1 - \theta)p_0 + \theta p_1 = p_0 - \theta\Delta \in [p_1, p_0]. \quad (2.27)$$

Известно (см., напр., [27]), что для бернульиевской модели $Bi(1, p_\theta)$ полной достаточной статистикой является наблюдаемое число единиц

$$\rho_n = \sum_{i=1}^n \xi_i,$$

при этом

$$\mathcal{L}(\rho_n) = Bi(n, p_\theta) \quad (2.28)$$

($Bi(n, p)$ - биномиальное распределение с параметрами n и p).

Таким образом, в рассматриваемом случае все сводится к получению статистических выводов о параметре θ модели (2.27) – (2.28).

Ниже решаются две основные задачи:

1. проверка гипотезы $H_0: \theta = 0$ (вкрапления отсутствуют) при альтернативе $H_1: \theta > 0$ о наличии вкраплений;
2. оценивание интенсивности вкрапления θ (при справедливости гипотезы H_1).

Замечание. Величина $p_1 = P(\xi_{11} = 1)$, а тем самым и $\Delta = p_0 - p_1$, вообще говоря, также должна рассматриваться как неизвестный параметр модели, но поскольку θ и Δ присутствуют в (2.27) в виде произведения, то фактически рассматриваемая модель зависит лишь от одного параметра $\theta' = \theta\Delta$. В дальнейшем мультипликативный параметр Δ формально можно считать известным и все рассуждения вести в терминах лишь параметра θ .

2.2.2. Проверка гипотез о наличии вкраплений.

Пусть H_θ означает простую гипотезу о наличии вкраплений с заданной интенсивностью вкрапления $\theta > 0$. Запишем отношение правдоподобия L_θ/L_0 в задаче (H_0, H_θ) - различия гипотез H_0 и H_θ :

$$\frac{L_\theta}{L_0} = \frac{p_\theta^{\rho_n} q_\theta^{n-\rho_n}}{p_0^{\rho_n} q_0^{n-\rho_n}} = \varphi^{\rho_n}(\theta) \left(\frac{q_\theta}{q_0} \right)^n, \quad (2.29)$$

где $q_\theta = 1 - p_\theta$, $\varphi(\theta) = \frac{q_0}{p_0} \frac{P_\theta}{q_\theta}$.

Здесь функция $\varphi(\theta)$, $\theta \in [0,1]$, обладает следующими свойствами:

$$\varphi(0) = 1,$$

$$\varphi(1) = \frac{q_0}{p_0} \frac{p_1}{q_1} = \frac{(1-p_0)p_1}{p_0(1-p_1)} < 1 \text{ и (см. (2.27))}$$

$$\varphi'(\theta) = \frac{q_0}{p_0} \frac{-(q_0 + \theta\Delta)\Delta - (p_0 - \theta\Delta)\Delta}{q_\theta^2} = -\frac{q_0\Delta}{p_0 q_\theta^2} < 0.$$

Таким образом, $\varphi(\theta) < 1$ при $\theta > 0$, и поэтому отношение правдоподобия (2.29) монотонно убывает при возрастании ρ_n .

Итак, рассматриваемая модель имеет монотонное отношение правдоподобия, и потому (см.[27, §4.4.1]) в задаче (H_0, H_1) проверки простой гипотезы H_0 при сложной односторонней альтернативе $H_1: \theta > 0$ существует равномерно наиболее мощный (р.н.м.) критерий, который совпадает с критерием Неймана-Пирсона в задаче (H_0, H_θ) с простой альтернативой H_θ .

Последний же задается критической областью вида $L_\theta / L_0 \geq c$ (см.[27, §4.2.3]), что в нашем случае эквивалентно условию $\rho_n \leq t_\alpha$, где критическая граница t_α определяется заданием уровня значимости $\alpha = \mathbf{P}(H_\theta | H_0)$:

$$\alpha = \mathbf{P}_0(\rho_n \leq t_\alpha) = \sum_{j \leq t_\alpha} b_j(n, p_0) \equiv \mathbf{B}(t_\alpha; n, p_0), \quad (2.30)$$

где (см. (2.28))

$$b_j(n, p) = C_n^j p^j q^{n-j}, \quad j = 0, 1, \dots, n.$$

Однако, в силу ступенчатости функции распределения $\mathbf{B}(x; n, p_0) = \mathbf{P}_0(\rho_n \leq x)$ уравнение (2.30) при заданных значениях параметров

n , p_0 и α может не иметь решения. Поэтому в общем случае нужно поступать так [27, §4.2]. Определим при заданном α целое t_α условиями

$$\alpha'' \equiv \mathbf{B}(t_\alpha - 1; n, p_0) < \alpha \leq \mathbf{B}(t_\alpha; n, p_0) \equiv \alpha'. \quad (2.31)$$

Если здесь имеет место знак равенства ($\alpha = \alpha'$), то критерий задается критической областью

$$\mathcal{X}_{1\alpha}^* = \{\rho_n \leq t_\alpha\},$$

которая не зависит от альтернативы H_θ и потому определяет р.н.м. критерий уровня значимости α в задаче (H_0, H_1) . Функция мощности такого критерия вычисляется по формуле

$$W(\mathcal{X}_{1\alpha}^*; \theta) = \mathbf{P}_\theta(\rho_n \leq t_\alpha) = \mathbf{B}(t_\alpha; n, p_\theta). \quad (2.32)$$

Если же в (2.31) $\alpha < \alpha'$, то соответствующий критерий является рандомизированным с критической функцией

$$\varphi_\alpha^*(\rho_n) = \begin{cases} 1 & \text{при } \rho_n \leq t_\alpha - 1, \\ \frac{\alpha - \alpha'}{b_0} & \text{при } \rho_n = t_\alpha, \\ 0 & \text{при } \rho_n \geq t_\alpha + 1, \end{cases}$$

где $b_0 = b_{t_\alpha}(n, p_0)$ (гипотеза H_0 отвергается, если $\rho_n \leq t_\alpha - 1$, и принимается, если $\rho_n \geq t_\alpha + 1$; если же $\rho_n = t_\alpha$, то H_0 отвергается с вероятностью $(\alpha - \alpha')/b_0$ и принимается с дополнительной вероятностью $(\alpha' - \alpha)/b_0$).

Мощность такого критерия при альтернативе H_θ равна

$$W(\varphi_\alpha^*; \theta) = \mathbf{E}_\theta \varphi_\alpha^*(\rho_n) = \mathbf{B}(t_\alpha - 1; n, p_\theta) + (\alpha - \alpha'') \left(\frac{P_\theta}{P_0} \right)^{t_\alpha} \left(\frac{q_\theta}{q_0} \right)^{n-t_\alpha}.$$

На практике мы обычно имеем дело с большими выборками, поэтому вместо точных (и громоздких) формул (2.30)-(2.32) удобно использовать их асимптотический (при $n \rightarrow \infty$) вариант. В рассматриваемом случае из (2.27)-(2.28) следует, что при любом θ при $n \rightarrow \infty$

$$\mathcal{L}_\theta(\rho_n) \sim \mathcal{N}(np_\theta, np_\theta q_\theta), \quad (2.33)$$

поэтому критическую границу $t_\alpha = t_\alpha(n)$ в (2.30) следует выбрать в виде

$$t_\alpha(n) = np_0 + \zeta_\alpha \sqrt{np_0 q_0}, \quad (2.34)$$

где ζ_α есть α -квантиль стандартного нормального распределения $\mathcal{N}(0,1)$:

$$\Phi(\zeta_\alpha) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\zeta_\alpha} e^{-\frac{x^2}{2}} dx = \alpha.$$

Для мощности $W_n(\theta)$ в этом случае из (2.32) будем иметь:

$$\begin{aligned} W_n(\theta) &= \mathbf{P}_\theta \left(\frac{\rho_n - np_\theta}{\sqrt{np_\theta q_\theta}} \leq \sqrt{n} \frac{\theta \Delta}{\sqrt{p_\theta q_\theta}} + \zeta_\alpha \sqrt{\frac{p_0 q_0}{p_\theta q_\theta}} \right) \rightarrow \\ &\rightarrow \begin{cases} \Phi\left(\frac{t}{\sqrt{p_0 q_0}} + \zeta_\alpha\right), & \text{если } \sqrt{n}\theta\Delta \rightarrow t \geq 0, \\ 1 & \text{если } \sqrt{n}\theta\Delta \rightarrow \infty. \end{cases} \end{aligned} \quad (2.35)$$

Итак, справедливо следующее утверждение.

Теорема 4. В задаче проверки гипотезы $H_0: \theta = 0$ при альтернативе $H_1: \theta > 0$ существует р.н.м. критерий, задаваемый при $n \rightarrow \infty$ критической областью $\{\rho_n \leq t_\alpha(n)\}$, где при заданном уровне значимости α граница $t_\alpha(n)$ определяется соотношением (2.34); мощность этого критерия асимптотически имеет вид (2.35).

Из этой теоремы следует, что гипотезы H_0 и H_1 будут асимптотически неразличимы, если выполняется условие

$$\sqrt{n}\theta\Delta \rightarrow 0. \quad (2.36)$$

Это и есть искомое условие для организации (в рамках рассматриваемой модели) процесса вкрапления скрытой информации в передаваемое сообщение: оно означает, что параметры $p_1 = p_0 - \Delta$ и θ должны быть такими, чтобы произведение $\theta\Delta$ было мало в сравнении с $n^{-1/2}$ (при больших n).

В свою очередь, это условие может быть обеспечено двумя способами:

- 1) $\theta\sqrt{n} \rightarrow 0$, то есть $\theta = \theta_n = o(1/\sqrt{n})$, - тогда параметр p_1 может быть любым (напомним, что $p_1 < p_0$), но число вкрапляемых символов k в этом случае имеет среднее $E_\theta k = n\theta = o(\sqrt{n})$, что может быть недостаточным;
- 2) $\Delta = \Delta_n \rightarrow 0$, то есть $p_1 = p_1(n) \rightarrow p_0$ (p_1 мало отличается от p_0), - тогда для $\theta = \theta_n$ получаем условие $\theta_n = o(1/\sqrt{n}\Delta_n)$, и для числа вкрапляемых символов возможности расширяются в среднем до границы

$n\theta_n = o(\sqrt{n}/\Delta_n)$, например, при $\Delta_n \sim \frac{1}{\sqrt{n}}$ эта граница имеет порядок $o(n)$.

Если же условие (2.36) не выполняется, то при $\sqrt{n}\theta\Delta \rightarrow t > 0$ построенный критерий различает гипотезы H_0 и H_θ с ошибками, асимптотически равными α и $1 - \Phi\left(\frac{t}{\sqrt{p_0 q_0}} + \zeta_\alpha\right)$, а при $\sqrt{n}\theta\Delta \rightarrow \infty$ он состоятелен (если альтернатива H_θ имеет место, то этот факт обнаруживается критерием с вероятностью, стремящейся к 1 при $n \rightarrow \infty$).

2.2.3. Оценивание интенсивности вкрапления.

Если в результате тестирования принимается гипотеза H_1 о наличии вкраплений, то желательно иметь информацию о величине интенсивности вкрапления θ , что требует построения приемлемых оценок для этого параметра модели. Прежде всего, рассмотрим вопрос о существовании несмешенной оценки для θ . Из теории полных достаточных статистик [27, §2.3.2] следует, что в нашем случае несмешенная оценка, если она существует, - это такая функция от статистики ρ_n , $\psi(\rho_n)$, которая удовлетворяет уравнению несмешенности

$$\mathbf{E}_\theta \psi(\rho_n) = \theta, \quad \forall \theta. \quad (2.37)$$

Но из (2.27) и (2.29) следует, что

$$\mathbf{E}_\theta \rho_n = np_\theta = n(p_0 - \theta\Delta)$$

или

$$\mathbf{E}_\theta \frac{np_0 - \rho_n}{n\Delta} = \theta. \quad (2.38)$$

Следовательно уравнению (2.37) удовлетворяет функция

$$\psi(\rho_n) = \frac{np_0 - \rho_n}{n\Delta}, \quad (2.39)$$

причем такое решение единствено.

Чтобы принять статистику (2.39) в качестве разумной оценки для θ , необходимо, чтобы ее возможные значения удовлетворяли условию $0 \leq \psi(\rho_n) \leq 1$ (множество значений оценки и оцениваемого параметра должны совпадать). Решая неравенство $\psi(\rho_n) \geq 0$, находим, что $\rho_n \leq np_0$. Из другого неравенства $\psi(\rho_n) \leq 1$ легко получить, что $\rho_n \geq np_1$.

Итак, необходимому условию $\psi(\rho_n) \in [0,1]$ удовлетворяют лишь значения статистики ρ_n в интервале $[np_1, np_0]$. При $\rho_n < np_1$ статистика $\psi(\rho_n) > 1$, а при $\rho_n > np_0$ значение $\psi(\rho_n) < 0$. Таким образом, при $\rho_n \notin [np_1, np_0]$ статистика $\psi(\rho_n)$ не может быть использована в качестве оценки параметра θ . Следовательно, в нашей модели несмещенной оценки для θ не существует.

Базируясь на статистике (2.39), можно предложить следующую естественную оценку θ :

$$\hat{\theta}_n = \begin{cases} 1 & \text{при } \rho_n < np_1, \\ \frac{np_0 - \rho_n}{n\Delta} & \text{при } np_1 \leq \rho_n \leq np_0, \\ 0 & \text{при } \rho_n > np_0. \end{cases} \quad (2.40)$$

Дополнительным обоснованием оценки $\hat{\theta}_n$ является тот факт, что она совпадает с оценкой максимального правдоподобия (ОМП), то есть

она максимизирует функцию правдоподобия L_θ (см. (2.29)).

Действительно, дифференцируя логарифм правдоподобия

$$l(\theta) = \ln L_\theta = \rho_n \ln(p_0 - \theta\Delta) + (n - \rho_n) \ln(q_0 + \theta\Delta),$$

имеем

$$l'(\theta) = -\frac{\rho_n \Delta}{p_0 - \theta\Delta} + \frac{(n - \rho_n)\Delta}{q_0 + \theta\Delta} = \Delta \frac{np_0 - \rho_n - n\Delta\theta}{p_\theta q_\theta}.$$

Если $\rho_n < np_1$, то $np_0 - \rho_n - n\Delta\theta > n\Delta(1 - \theta) > 0$ при $\theta < 1$, то есть функция $l(\theta)$ монотонно возрастает и достигает своего максимума в граничной точке $\hat{\theta}_n = 1$.

Если $\rho_n > np_0$, то $np_0 - \rho_n - n\Delta\theta < -n\Delta\theta < 0$, то есть функция $l(\theta)$ монотонно убывает и потому имеет максимум в другой граничной точке $\hat{\theta}_n = 0$.

Наконец, если ρ_n удовлетворяет условию $np_1 \leq \rho_n \leq np_0$, то $l'(\theta) = 0$ при $\theta = \hat{\theta}_n = (np_0 - \rho_n)/n\Delta$ и в этой точке $l''(\theta) < 0$, то есть это точка максимума функции $l(\theta)$.

Таким образом, в нашей модели принцип максимального правдоподобия приводит к единственному решению и ОМП $\hat{\theta}_n$ имеет указанный в (2.40) вид.

Обсудим теперь вопрос о построении доверительного интервала для параметра θ . Поскольку параметр θ в нашем случае является аргументом параметра p_θ (см. (2.27)) биномиального распределения (2.28), то доверительный интервал для θ можно рассчитать, используя известные методы расчета доверительного интервала для параметра p биномиального распределения $Bi(n, p)$. А именно, если для доверительного уровня γ рассчитан γ -доверительный интервал (p_H, p_B) , то, разрешая

неравенство $p_H < p_\theta < p_B$ с учетом (2.27) относительно θ , получаем γ -доверительный интервал для θ :

$$\frac{p_0 - p_B}{\Delta} < \theta < \frac{p_0 - p_H}{\Delta}.$$

Наконец, рассмотрим еще вопрос об асимптотических свойствах оценки $\hat{\theta}_n$ для больших выборок (при $n \rightarrow \infty$). Из асимптотической нормальности (2.33) статистики ρ_n следует, что события $\{\rho_n < np_1\}$ и $\{\rho_n > np_0\}$ имеют вероятности, стремящиеся к нулю при $n \rightarrow \infty$, следовательно, с вероятностью, стремящейся к 1, оценка $\hat{\theta}_n$ будет иметь вид $(np_0 - \rho_n)/n\Delta$, а эта оценка асимптотически нормальна со средним θ (см. (2.38)) и дисперсией $p_\theta q_\theta/n\Delta^2$, которая стремится к 0 при $n \rightarrow \infty$. Таким образом, оценка $\hat{\theta}_n$ является асимптотически несмещенной и состоятельной, что позволяет рассчитать асимптотический γ -доверительный интервал для параметра θ :

$$\left(\hat{\theta}_n \mp c_\gamma \frac{1}{\Delta} \sqrt{\frac{p_{\hat{\theta}_n} q_{\hat{\theta}_n}}{n}} \right), \quad c_\gamma = \Phi^{-1}\left(\frac{1+\gamma}{2}\right). \quad (2.41)$$

Сформулируем асимптотический вариант оценивания в виде следующего итогового утверждения.

Теорема 5. Пусть $\sqrt{n}\Delta \rightarrow \infty$, тогда принимается гипотеза о наличии вкраплений $H_1: \theta > 0$, и асимптотически несмещенной и состоятельной оценкой параметра θ является статистика $\hat{\theta}_n = (np_0 - \rho_n)/n\Delta$, а асимптотический γ -доверительный интервал для θ имеет вид (2.41).

2.3. Полиномиальная модель вкрапления и ее статистический анализ

В этом разделе мы рассмотрим обобщение предыдущей модели вкрапления на произвольную полиномиальную модель, то есть когда последовательности $\bar{\xi}_0 = (\xi_{01}, \xi_{02}, \dots, \xi_{0n})$ и $\bar{\xi}_1 = (\xi_{11}, \xi_{12}, \dots, \xi_{1n})$ состоят из независимых случайных величин, принимающих значения из некоторого конечного алфавита $A = \{A_1, A_2, \dots, A_N\}$, $N \geq 2$ (механизм вкрапления $\bar{\delta} = (\delta_1, \dots, \delta_n)$ остается прежним).

Пусть $\bar{p}_0 = (p_{01}, \dots, p_{0N})$, $\bar{p}_1 = (p_{11}, \dots, p_{1N})$, где

$$p_{0j} = \mathbf{P}(\xi_{0i} = A_j), \quad p_{1j} = \mathbf{P}(\xi_{1i} = A_j), \quad j = 1, \dots, N, i \geq 1.$$

Тогда наблюдаемая последовательность $\bar{\xi} = (\xi_1, \xi_2, \dots, \xi_n)$, где

$$\xi_i = \mathbf{I}(\delta_i = 0)\xi_{0i} + \mathbf{I}(\delta_i = 1)\xi_{1i}, \quad i = 1, \dots, n,$$

также будет полиномиальной, для которой

$$p_\theta = \mathbf{P}_\theta(\xi_i = A_j) = (1 - \theta)p_{0j} + \theta p_{1j} = p_{0j} - \theta \Delta_j,$$

где $\Delta_j = p_{0j} - p_{1j}$, $j = 1, \dots, N$, $i \geq 1$.

В данном случае правдоподобие данных есть

$$L_\theta(\bar{\xi}) = \prod_{i=1}^n \prod_{j=1}^N p_{\theta_j}^{I(\xi_i = A_j)} = \prod_{j=1}^N p_{\theta_j}^{\nu_j},$$

где $\nu_{nj} = \sum_{i=1}^n \mathbf{I}(\xi_i = A_j)$ - частота символа A_j в последовательности ξ . Тем самым достаточной статистикой в данной модели является вектор частот $\bar{\nu}_n = (\nu_{n1}, \nu_{n2}, \dots, \nu_{nN})$, имеющий полиномиальное распределение:

$$\mathcal{L}_{\theta}(\bar{\nu}_n) = \mathbf{M}(n; \bar{p}_{\theta} = (p_{\theta 1}, \dots, p_{\theta N})).$$

Из теории полиномиального распределения известно (см. [27, §2.4.4 и §3.2.2]), что при $n \rightarrow \infty$ вектор частот $\bar{\nu}_n$ асимптотически нормален с параметрами $n\bar{p}_{\theta}$ и $n\sum(\theta)$, где

$$\sum(\theta) = (\sigma_{ij}(\theta) = p_{\theta j}(\delta_{ij} - p_{\theta}))$$

δ_{ij} - символ Кронекера, и статистика хи-квадрат

$$X_n^2 = \sum_{j=1}^N \frac{(\nu_{nj} - np_{0j})^2}{np_{0j}}$$

имеет при справедливости гипотезы $H_0: \theta = 0$ предельное (при $n \rightarrow \infty$) распределение $\chi^2(N-1)$.

Более того, при любой альтернативе, задаваемой вектором $\bar{p} = (p_1, \dots, p_N)$ появления знаков алфавита A на каждом месте наблюдаемой последовательности ξ ,

$$\mathbf{E}(X_n^2 | \bar{p}) = n \sum_{j=1}^N \frac{(p_j - p_{0j})^2}{p_{0j}} + \sum_{j=1}^N \frac{p_j(1-p_j)}{p_{0j}},$$

то есть в нашем случае (при $\bar{p} = \bar{p}_{\theta}$)

$$\mathbf{E}_\theta X_n^2 = n\theta^2 \sum_{j=1}^N \frac{\Delta_j^2}{p_{0j}} + \sum_{j=1}^N \frac{(p_{0j} - \theta\Delta_j)(1 - p_{0j} + \theta\Delta_j)}{p_{0j}}.$$

Отсюда следует, что если при $n \rightarrow \infty$ выполняется условие

$$\theta\Delta \rightarrow 0, \quad \Delta = \max_{1 \leq j \leq N} |\Delta_j|, \quad (2.42)$$

то

$$\mathbf{E}_\theta X_n^2 = N - 1 + \lambda_n^2 + o(1), \quad (2.43)$$

где

$$\lambda_n^2 = n\theta^2 \sum_{j=1}^N \frac{\Delta_j^2}{p_{0j}}.$$

Далее, если «близкая» альтернатива задается вектором $\bar{p} = \bar{p}(n)$ вида

$$\bar{p}(n) = \bar{p}_0 + \frac{\bar{\beta}}{\sqrt{n}}, \quad (2.44)$$

где $\bar{\beta} = (\beta_1, \dots, \beta_N) \neq \bar{0}$ - фиксированный вектор, задающий отклонение от гипотезы H_0 ($\sum_{j=1}^N \beta_j = 0$), то при $n \rightarrow \infty$

$$\mathcal{L}(X_n^2 | \bar{p}(n)) \rightarrow \chi^2(N-1; \lambda^2),$$

где $\chi^2(N-1; \lambda^2)$ - нецентральное хи-квадрат распределение с $N-1$ степенями свободы и параметром нецентральности

$$\lambda^2 = \sum_{j=1}^N \frac{\beta_j^2}{p_{0j}}. \quad (2.45)$$

В нашем случае альтернативы к нулевой гипотезе $H_0: \theta = 0$, то есть к гипотезе об отсутствии вкраплений, задаются вектором

$$\bar{p}_\theta = (p_{\theta 1}, \dots, p_{\theta N}) = \bar{p}_0 - \theta \bar{\Delta}, \quad \bar{\Delta} = (\Delta_1, \dots, \Delta_N) = \bar{p}_0 - \bar{p}_1$$

(в этом случае мы будем говорить об альтернативе H_θ), поэтому (2.44) будет иметь место, если

$$-\sqrt{n}\theta \bar{\Delta} = \bar{\beta} + o(1). \quad (2.46)$$

В этом случае будет также выполнено условие (2.42) и величина λ_n^2 в (2.43) будет иметь при $n \rightarrow \infty$ предел (2.45).

В итоге имеем следующее утверждение.

Теорема 6. *Если в полиномиальной модели вкрапления «близкие» к гипотезе $H_0: \theta = 0$ альтернативы H_θ задаются условием (2.46), то при $n \rightarrow \infty$*

$$E_\theta X_n^2 = N - 1 + \lambda^2 + o(1)$$

и, более того,

$$\mathcal{L}_\theta(X_n^2) \rightarrow \chi^2(N - 1; \lambda^2),$$

где параметр нецентральности λ^2 указан в (2.45).

Этот результат уже дает возможность дать ответ на вопрос о том, как следует организовать процесс вкрапления, чтобы гипотезы $H_0: \theta = 0$ (отсутствие вкраплений) и $H_1: \theta > 0$ (наличие вкраплений) были

статистически неразличимы, когда наблюдается длинная ($n \rightarrow \infty$) последовательность $\bar{\xi} = (\xi_1, \dots, \xi_n)$, $\xi_i \in A$.

Именно, гипотезы H_0 и H_1 будут асимптотически неразличимы, если в рассматриваемой модели параметры $\theta = \theta(n)$ и $\bar{p}_1 = \bar{p}_1(n) = \bar{p}_0 - \bar{\Delta}(n)$ удовлетворяют при $n \rightarrow \infty$ условию

$$\sqrt{n}\theta(n)\bar{\Delta}(n) \rightarrow \bar{0} \quad (2.47)$$

(в этом случае тестовая статистика X_n^2 будет иметь одно и тоже предельное распределение $\chi^2(N-1)$ как при нулевой гипотезе H_0 , так и при альтернативе H_θ).

Если же выполняется условие (2.46), то в задаче (H_0, H_θ) критерий хи-квадрат, задаваемый критическим множеством

$$\mathcal{X}_{1\alpha} = \left\{ X_n^2 > \chi_{1-\alpha, N-1}^2 \right\} \quad (2.48)$$

(здесь $\chi_{1-\alpha, N-1}^2$ – $(1-\alpha)$ -квантиль распределения $\chi^2(N-1)$), будет различать гипотезы H_0 и H_θ с ошибками, асимптотически равными α (вероятность ошибки 1-го рода) и $F_{N-1}(\chi_{1-\alpha, N-1}^2; \lambda^2)$ (вероятность ошибки 2-го рода), где $F_{N-1}(t; \lambda^2)$ – функция распределения закона $\chi^2(N-1; \lambda^2)$ и λ^2 дано в (2.45).

Наконец, если величина $\lambda_n^2 \rightarrow \infty$ (см.(2.43)), то против таких «далеких» альтернатив H_θ критерий хи-квадрат (2.48) будет состоятельным.

Таким образом, для полиномиальной модели основной вывод оказался вполне аналогичным соответствующему заключению для бернуlliевской модели (сравни условия (2.47) и (2.36)).

ЗАКЛЮЧЕНИЕ

Предложенные в диссертации математические модели являются новыми, вполне адекватными реальным процессам, и позволяют рационально управлять ими. В диссертации получены следующие научные результаты:

- Построена биномиальная модель вкрапления информации, проведен ее вероятностно статистический анализ, включая случай схемы серий, и получена оценка числа допустимых вкраплений, гарантирующего надежное сокрытие факта вкрапления.
- Построена и проанализирована параметрическая модель вкрапления информации, решена задача различения гипотез об отсутствии и наличии вкраплений и дана оценка допустимой интенсивности вкрапления.
- Исследована полиномиальная модель вкрапления, проведен ее вероятностно-статистический анализ и сформулированы практические рекомендации для обеспечения надежности сокрытия факта вкрапления.
- Сформулированы перспективные направления, по которым возможны использование стеганографии, как инструмента защиты информации.
- Рассмотрены принципы, положенные в основу большинства известных стеганографических методов, направленных на сокрытие конфиденциальных данных в компьютерных файлах графического звукового и видео форматов, и изложены проблемы надежности и стойкости произвольной стеганографической системы.
- Обобщены и систематизированы основные методы и положения компьютерной стеганографии, указаны виды атак на нее;

показана возможность использования стеганографических методов как для передачи секретной информации в сетях Internet, так и для защиты авторских прав и прав интеллектуальной собственности.

- Разработанный в процессе выполнения диссертационной работы метод вкрапления закрытой информации использован при выполнении научно-исследовательской работы «*Исследование инструментальных средств реализации концепции «Электронная отрасль» и «Электронное предприятие». Разработка предложений по инструментальной защите данных при их передаче в открытых сетях*». Акт внедрения прилагается.

- Разработанная в процессе выполнения диссертационной работы полиномиальная модель использована при выполнении научно-исследовательской работы «*Разработка отладочно-демонстрационно-сертификационного стенда на основе системы InvisiLAN для защиты данных при их передаче в открытых сетях*». Акт внедрения прилагается.

СПИСОК ЛИТЕРАТУРЫ

1. Digital Scream, журнал Хакер [Электронный ресурс]: Теория стеганографии/Digital Scream. - Электрон. текстовые дан. и граф. дан. – М.: 2003. – Режим доступа:
<http://www.xakep.ru/post/18934/default.asp>, свободный.
2. Свободная Энциклопедия Википедия [Электронный ресурс]: Стеганография/ - Электрон. текстовые дан. и граф. дан. – М.: 2003. – Режим доступа: <http://ru.wikipedia.org/wiki/Стеганография>, свободный.
3. Савельев А.А., Энциклопедический фонд России [Электронный ресурс]: Стеганография/ Савельев А.А. - Электрон. текстовые дан. и граф. дан. – Режим доступа: <http://www.russika.ru/t.php?t=3474>, свободный.
4. Генне О. В., Журнал "Защита информации. Конфидент" [Электронный ресурс], №3, 2000. - Режим доступа:
www.confident.ru/magazine/, свободный.
5. Аграновский А. В., Девягин П. Н., Черемушкин А. В., Хади Р. А., Основы стеганографии, Ростов-На-Дону, 2003.
6. Овсянников В., Журнал "Cio-world" [Электронный ресурс]: Скрытая утечка информации, ч. 2./ Овсянников В., - Электрон. текстовые дан. и граф. дан. - 2003. – Режим доступа: <http://www.cio-world.ru/it-market/e-safety/28763/>, свободный.

7. Барсуков В.С., Романцов А.П., Компьютерная стеганография вчера, сегодня, завтра. Журнал "Специальная Техника" (1998), № 4-5.
8. Васильева Е., Цифровая стеганография [Электронный ресурс]: Цифровая стеганография./ Васильева Е., - Электрон. текстовые дан. - 2006 - Режим доступа:
<http://rain.ifmo.ru/cat/data/theory/coding/steganography-2006/article.pdf>, свободный.
9. Грибунин В.Г., Оков И.Н., Туринцев И.В. *Цифровая стеганография*. Солон-Пресс, Москва, 2002.
10. Moskowitz S.A., Cooperman M.: “Optimization methods for the insertion, protection, and detection of digital watermarks in digitized data”, United States Patent № 5,889,868, March 30, 1999, US Patent & Trademark Office.
11. Moskowitz S.A., Cooperman M.: “Method and system for digital watermarking”, United States Patent № 5,905,800, May 18, 1999, US Patent & Trademark Office.
12. Rhoads G.B.: “Image steganography system featuring perceptually adaptive and globally scalable signal embedding”, United States Patent № 5,748,763, May 05, 1998, US Patent & Trademark Office.
13. Rhoads G.B.: “Steganography methods employing embedded calibration data”, United States Patent № 5,636,292, June 03, 1997, US Patent & Trademark Office.

- 14.Rhoads G.B.: “Photographic products and methods employing embedded information”, United States Patent № 5,822,436, October 13, 1998, US Patent & Trademark Office.
- 15.Rhoads G.B.: “Steganographic methods and media for photography”, United States Patent № 6,111,954, August 29, 2000, US Patent & Trademark Office.
- 16.Moskowitz S.A.: “Z-transform implementation of digital watermarks”, United States Patent № 6,078,664, June 20, 2000, US Patent & Trademark Office.
- 17.Шенон К. *Работы по теории информации и кибернетики*. / Пер. с анг. – Москва: Иностр. литература, 1963 – 829 с.
- 18.Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений. Журнал “Защита информации. Конфидент”, №3, 2000.
- 19.Конахович Г.Ф., Пузыренко А.Ю. *Компьютерная стеганография*, - Киев: МК-Пресс, 2006. – 288 с.
20. Раик Г.А. *Основам информационных технологий*. Белорусский государственный университет. Минск, 2007
- 21.Rhoads G.B.: “Methods for optimizing watermark detection”, United States Patent № 6,307,949, October 23, 2001, US Patent & Trademark Office.

- 22.Быков С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Журнал “Защита информации. Конфидент”, №3, 2000.
- 23.Быков С.Ф. Проведение исследований по оценки влияния факта внедрения случайной информации в контейнер с аудио-, видео-, графической информацией, сжатой с потерями на ее субъективное восприятие человеком. Предложение к НИР “Узор-У”. Москва, 2001.
24. W. Bender, D. Gruhl, N. Morimoto, A. Lu. "Techniques For Data Hiding." IBM Systems Journal Vol. 35, 1996, pp. 313 - 336.
25. Chang Shih-Fu; Meng Jianhao: “Watermarking of digital image data”, WO9922480 (EP1034635), May 06, 1999, World Intellectual Property Organization.
- 26.Бейтмен Г., Эрдейи А. *Высшие трансцендентные функции. Т.1*, Наука, ФМЛ., Москва, 1965.
- 27.Ивченко Г.И., Медведев Ю.И. *Математическая статистика. 2-е изд.*, Высшая школа, Москва, 1992.
- 28.Пономарев К.И. Биноминальная модель вкрапления информации. Научно-техническая конференция студентов аспирантов и молодых специалистов МИЭМ. Тезисы докладов. - М.:МИЭМ, 2007.
29. Пономарев К.И. Статистическая модель вкрапления информации. Научно-техническая конференция студентов аспирантов и молодых специалистов МИЭМ. Тезисы докладов. - М.:МИЭМ, 2008.

30. Пономарев К.И., Путилов Г.П. Стеганография: история и современные технологии. - М. МИЭМ, 2009.
31. Пономарев К.И. Об одной статистической модели стеганографии. - М. Дискретная математика, (2009) 21, №2, 138-145.
32. Пономарев К.И. Полиномиальная модель вкрапления информации. Научно-техническая конференция студентов аспирантов и молодых специалистов МИЭМ. Тезисы докладов. - М.:МИЭМ, 2009.
33. Пономарев К.И. Параметрическая модель вкрапления и ее статистический анализ. - М. Дискретная математика, (2009) 21, №4, 148-157.