Оглавление

Введение

Настоящее пособие, по существу, развивает первичные материалы раздела «Обнаружение и распознавание сигналов», посвященного стеганографическим методам сокрытия сообщений. Совместно с опубликованными в 2011 году работами студентов, посвященным конкретным исследованиям с использованием среды MathCad, эти материалы могут быть полезными для студентов, принявших решение выполнить домашнее задание по выбору. Методическое пособие, как часть учебной дисциплины по дисциплине «Обнаруженние и распознавание сигналов» в виде электронного учебного издания (ЭУИ), подготовлено на основе Государственного образовательного стандарта Российской Федерации по образованию студентов технических вузов, а также в соответствии с учебными планами МГТУ им. Н.Э. Баумана. Пособие содержит основные положения соответствующего раздела учебного курса по основным положениям и тенденциям развития стеганографии.

Новизну предлагаемого учебного издания составляют вопросы, специфика которых недостаточно освещается в известных публикациях. Темы раздела учебного курса дополнены ссылками и непосредственно приведенными методическими материалами. К числу таких материалов относятся, в частности, листинги программ в среде MathCad, результаты выполнения которых иллюстрируют отдельные теоретические положения. Учитывается еще и то, что публикации в рассматриваемой предметной области весьма разрознены и единственное отечественное издание, систематизирующее сведения по стеганографии, в практической области уже не совсем актуально. Речь идет о книге: Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.

Методической особенностью публикации является то, что оно содержит ссылки на некоторые положения, содержащиеся в «Электронной энциклопедии» кафедры ИУ-8, активно используемой студентами в процессе самостоятельной работы при подготовке к практическим занятиям, выполнении домашних заданий и проектов, а также при

подготовке к зачетам и экзаменам. Материалы данного издания позволяют более наглядно представить изучаемый материал, приблизить его к практическим вопросам.

Рекомендовано преподавателям, аспирантам и студентам технических факультетов и НУК МГТУ им. Н. Э. Баумана для учебного процесса и при подготовке к текущим занятиям, зачетам, экзаменам, для обсуждения на семинарских занятиях, в курсовых, дипломных и диссертационных работах, а также для самостоятельной внеаудиторной работы.

Раздел 1. Стеганография: Основные положения

УЧЕБНЫЕ ЦЕЛИ РАЗДЕЛА 1.

1) Раскрыть понятие стеганографии.

2) Определить основную терминологию.

3) Провести краткий исторический обзор.

4) Провести классификацию методов и средств стеганографии.

Тема 1. Стеганография: Принятая терминология, исторический обзор и классификация методов и средств.

Вопросы для самостоятельного изучения и обсуждения на семинаре.

1) Исторически сложившиеся методы сокрытия данных.

2) Отличие и сходство стеганографии с криптографией.

3) Теоретические положения с учетом принятой терминологии.

Литература для изучения темы.

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с
2. Rotation scale and translation invariant spread spectrum digital image watermarking. IEEE Int. Conf. on Image Processing, 1998. P. 4.
3. Pereira S., Joseph J., Deguillaume F. Template Based recovery of Fourier-Based Watermarks Using log-polar and Log-log Maps. IEEE Int. Conf on Multimedia Computing and Systems, 1999. P. 5.

1.1 Историческая справка. Принятая терминология

Скрыть сообщение можно разными способами, например, зашифровать. Правда, в этом случае противник знает, что вы передаете некоторое секретное сообщение, но не может его прочитать (криптография). Во многих случаях достаточно и самого факта передачи для получения сведений о каком-то событии, особенно если рассматривать и сопоставлять все факты вместе - на этом основана разведка по материалам из открытых источников. Другой способ состоит в том, чтобы скрыть не только сообщение, но и сам факт его передачи. Такой способ скрытия данных и сообщений называется стеганографией.

Исторически стеганография предшествовала появлению криптографии. Этимология слова «стеганография» уходит в далекое прошлое. В переводе с греческого «стеганография» означает «тайнопись». Стеганография, так же как когда-то и криптография, превращается постепенно из технического искусства в отдельную область научных исследований и постепенно приобретает статус самостоятельной прикладной науки, изучающей способы и методы сокрытия секретных сообщений.

В 1996 году, на первом открытом симпозиуме в Кембридже, официально посвященном проблематике сокрытия данных, были подведены итоги терминологическим дискуссиям. Обсуждением руководил сподвижник стеганографии в Массачусетском институте технологии Росс Андерсон (*Ross Anderson),* известный своими научными результатами и в криптографии. Результат обсуждения был зафиксирован Биргитом Пфитцманом. С этого момента опубликованный в трудах симпозиума набор терминов можно считать устоявшимся, по крайней мере, в западной литературе.

Русская стеганографическая терминология на данный момент не имеет подобного кембриджскому документу. Учитывая, что после появления большого количества разнородных открытых материалов по криптографии в криптографическую терминологию было внесено много путаницы, и она еще долго будет испытывать трудности из-за неточного определения многих терминов, к вопросу о стеганографической терминологии следует подходить чрезвычайно деликатно.

Как видно, терминология и математические модели стеганографии во многом сходны с понятиями и моделями, знакомыми нам из криптографии, однако они имеют иную смысловую окраску. В стеганографических системах сегодня часто используются методы криптографического преобразования данных, поэтому важно верно определять смысл соответствующих терминов исходя из контекста.

Одним из таких «скользких» терминов является понятие секретной компоненты стеганографической системы — ключа, который является параметром как стеганографических, так и криптографических систем.

Однако в разных системах термин «ключ» имеет различный смысл. Поэтому в случае, когда в стеганографической системе присутствуют еще и криптографические преобразования, важно различать используемые ключи по их предназначению и способу использования.

Стеганография изучает способы сокрытия данных и сообщений. Поэтому она является одним из направлений достаточно широкой области исследований, в которой изучаются способы сокрытия данных *(information hiding).*

Строго говоря, стеганография изучает способы, с помощью которых производится сокрытие самого факта передачи информации. Чтобы более точно понять очертить данное направление, попробуем описать разные подходы к сокрытию информации.

Проще всего возможные способы сокрытия информации рассмотреть на примере абстрактной модели канала скрытой передачи сообщений. Пусть имеется некоторый канал связи для передачи скрываемых данных, включающий отправителя, получателя и использующий конкретный способ передачи. Способ передачи должен быть выбран с учетом имеющейся ситуации, оговорен заранее и фиксирован. Отправитель и получатель также должны договориться о едином способе представления информации в виде сообщений, так как в противном случае получатель не сможет понять ни одного полученного сообщения. Информация скрывается от третьего лица, которого будем называть противником. В зависимости от конкретного приложения противником может быть также не один человек, а группа лиц. Противник может ставить перед собой различные цели, в том числе:

- обнаружение факта передачи скрытых данных и сообщений,
- ознакомление со скрываемыми данными,
- уничтожение скрытых данных,
- подделка (искажение) передаваемых сообщений,
- навязывание ложных данных.

В зависимости от ситуации и возможностей противника возможны различные постановки задач и методы их решения. Перечислим некоторые возможные подходы к

сокрытию передаваемой информации, упорядочив их по степени возрастания возможностей противника.

1) Попытаться скрыть сам факт передачи и, в частности,

- скрыть канал связи,
- скрыть отправителя,
- скрыть получателя,
- скрыть способ передачи,
- скрыть способ представления информации в виде сообщений.

2) Попытаться в открытом канале связи создать трудности для перехвата передаваемых сообщений, например, путем использования современных трудно доступных для противника технологий (микроточки, сверхскоростной способ передачи, использование скачков частоты, скремблирование и т.д.)

3) Попытаться в открытом канале связи, доступном для перехвата, спрятать скрытые данные в передаваемых открытых сообщениях так, чтобы они не могли быть обнаружены без специальных средств, например, химических, оптических и т.п.

4) Попытаться в открытом канале связи, доступном для перехвата, спрятать скрытое сообщение в протоколе, т.е. в порядке выбора и последовательности передачи открытых сообщений.

5) В открытом канале связи, доступном для перехвата и обнаружения наличия скрытых сообщений, попытаться затруднить возможность противника по обнаружению скрытых данных в передаваемых сообщениях, в частности, путем использования особенностей человеческого восприятия.

6) В открытом канале связи, доступном для перехвата и обнаружения противником наличия скрытых сообщений, попытаться затруднить возможность противника по ознакомлению с содержанием скрытых данных в передаваемых сообщениях, например, путем использования:

- кодов,
- шифрования сообщений.

7) В открытом канале связи, доступном для перехвата, обнаружения наличия и ознакомления с содержанием крытой информации, попытаться затруднить возможность

противника по пониманию смысла передаваемых сообщениях путем использования таких методов, как:

- дезинформация,
- многозначное толкование.

Данный перечень, как и всякая классификация, далеко не исчерпывает всех возможных подходов к сокрытию данных. Он как бы фиксирует уровни, на которых решается задача обеспечения надежности сокрытия.

1.2 Основные понятия и определения стеганографии

Попробуем отделить круг вопросов, который решает стеганография, от области применения других методов. Как было сказано выше, стеганографическая техника является одним из разделов общего направления по сокрытию данных. Но помимо стеганографии существуют и другие направления, изучающие методы сокрытия. Это — криптография, всевозможные сигнальные системы и условные знаки, маскировка и введение в заблуждение, наконец, различные толкования одних и тех же фраз и др.

В отличие от криптографии, которая также изучает методы сокрытия данных для хранения или передачи, причем данные преобразуются в форму сообщения, которое специально не скрывается, и допускается возможность его анализа противником, цель классической стеганографии состоит в том, чтобы скрыть секретные данные в других открытых наборах или потоках данных таким способом, который не позволяет обнаружить, что в них имеется какая-то скрытая составная часть, и тем самым выделить эти сообщения среди остальных. Поэтому можно было бы сказать, что стеганография — это искусство и наука о способах передачи (хранения) сообщений, скрывающих факт существования скрытого канала связи (скрываемых данных). Вместе с тем, такое определение было бы не совсем полным.

Дело в том, что к кругу задач, решаемых стеганографическими методами, помимо собственно скрытой передачи сообщений *(secret communication)* непосредственно примыкают направления, связанное со вставкой в передаваемые данные специальных скрытых меток — цифровых водяных знаков *(digital copyright watermarking)* и цифровых отпечатков пальцев *(digital fingerprinting & traitor tracing).* Так как данные метки служат для установления и защиты авторских прав, а также для контроля за нелегальным распространением, то их наличие в исходной информации, как правило, не составляет

секрета, и факт их присутствия не скрывается. Более того, средства для проверки данной вложенной информации легко доступны и, как правило, встроены в приемные устройства. Вместе с тем, сам способ вставки информации должен быть неизвестен, чтобы ее нельзя было извлечь либо обнаружить ее месторасположение. Главным же требованием к этому способу внедрения скрытой информации является стойкость к ее удалению и изменению, даже при выполнении определенных преобразований над исходной информацией.

Существуют также технологии внесения в исходные сообщения специальных вставок *(feature tagging, captioning).* Так, в изображения могут вставляться заголовки, аннотации, временные метки и другие описательные элементы, например имена изображенных людей на фото или названия мест на карте. Такие вставки могут нести и служебные сведения. Например, вставленные в изображения ключевые слова можно использовать для проведения быстрого поиска в базе данных изображений. Спрятанные во фрагменты видеоизображений временные метки могут быть полезными для синхронизации со звуком. Понятно, что сам факт наличия скрытых данных в данном случае также общеизвестен.

Стеганографию следует отличать и от сигнальных систем. С древних времен применяется метод сокрытия данных, основанный на построении некоторой сигнальной системы с использованием «условных знаков», т.е. не привлекающих внимание знаков и сообщений, смысл которых оговорен заранее и держится в секрете. С их помощью одна из сторон может передавать другой короткие сообщения о ходе событий или интересующих объектах, а также информировать другую сторону о том, какой способ поведения необходимо выбрать в данный момент.

Подобные «условные знаки», стоящие в передаваемом тексте, могут применяться для указания того, в каком смысле следует понимать этот текст и как к нему следует относиться.

В разное время стеганография использовала различные технологии. Каждый новый способ передачи информации порождал и новые подходы к созданию скрытых каналов.

Классическая документальная стеганография использует целый ряд методов сокрытия информации в передаваемых и хранимых документах. Это невидимые чернила, микроточки, акростих, трафареты и т.д. Это направление потеряло актуальность и в настоящих материалах не рассматривается.

С появлением радиосвязи было разработано много методов сокрытия сообщений в различных аналоговых потоках: широкополосные шумоподобные сигналы *(spread spectrum)*, включение сигналов в радиосообщения и музыку, передача с использованием прыгающих частот и т.д. Это направление можно назвать *радиоэлектронной стеганографией.* Вопросы скрытой передачи сообщений по радиоканалам, а также оптико-электронным и акустоэлектронном каналах детально рассматриваются в конспекте дисциплины «Обнаружение и распознавание сигналов» [https://gir.bmstu.ru].

В последнее время с развитием цифровых систем передачи данных появилось много исследований в области цифровой стеганографии. Под *цифровой стеганографией* понимается сокрытие информации в потоках оцифрованных (т.е. преобразованных в дискретную форму) сигналов, имеющих непрерывную аналоговую природу.

Компьютерная стеганография изучает способы сокрытия в компьютерных данных, представляющих собой различные файлы, программы, пакеты протоколов и т.п. С учетом общей компьютеризации всех областей человеческой деятельности в настоящее время очень трудно провести различие между цифровой и компьютерной стеганографией. Подобно тому, как в системах связи аналоговые сигналы (аудио, видео) преобразуются в форму дискретных последовательностей или потоков, которые разбиваются на пакеты и передаются по сети, компьютерные данные, соответствующие изображениям, звуковым или видеофрагментам, представляются в виде файлов или передаются в виде пакетов по компьютерной сети.

На самом деле с компьютерами связано множество различных направлений сокрытия информации, которые не стоит относить к стеганографии. Например, существует много способов, позволяющих обеспечить анонимность работы с маскировкой адресов и имен по открытым сетям и защитить (точнее замаскировать) трафик от анализа *(anonymity & traffic analysis).* Данное направление включает вопросы организации анонимных ремейлеров, позволяющих скрывать обратные адреса, создания цифровых псевдонимов, принятия мер по маскировке получателя путем отправки широковещательных сообщений. Возможно также использование изменяемых форм запросов, поддельных сообщений, изменение активности передач или скрытие пауз.

Кроме того, в литературе изучаются методы создания скрытых каналов *(covert channals)* для организации съема информации с компьютерных систем. Например, «Оранжевая книга», посвященная критериям оценки безопасности компьютерных систем

(Trusted Computer System Evaluation Criteria, TCSEC), определяет два типа скрытых каналов, позволяющих осуществлять съем информации с компьютерных систем: по памяти и по времени [9]. Можно использовать также программные способы управления режимами монитора, которые, будучи встроенными в лицензионные программные продукты, позволяют, например, снимать серийные номера используемого ПО с помощью простых приемников и тем самым контролировать правомерность их использования.

Традиционно из вышеперечисленных направлений сокрытия информации к стеганографии относят передачу (хранение) информации с использованием *стеганографического контейнера.* Это такие способы сокрытия информации в другом сообщении *(data hiding),* когда сначала выбирается сообщение-контейнер (coverf, *host data, message, container),* потом в нем каким-либо образом прячется скрываемая информация, которая затем с помощью сообщения-контейнера передается или хранится в нем.

Определение 1. *Стеганография* — это искусство и наука о способах передачи (хранения) скрытых сообщений, при которых скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации, причем для этой цели могут использоваться такие приемы, как:

- полное сокрытие факта существования скрытого канала связи,
- создание трудностей для обнаружения, извлечения или модификации передаваемых скрытых сообщений внутри открытых сообщений-контейнеров,
- маскировки скрытой информации в протоколе.

В настоящее время наблюдается большой интерес именно к компьютерной стеганографии. Появляется множество открыто распространяемых и коммерческих программных продуктов, использующих стеганографическую технику. Это объясняется многими причинами. Во-первых, использование криптографических средств приводит к появлению сообщений, которые по своим статистическим свойствам близки к случайным равновероятным последовательностям и поэтому легко обнаруживаются в канале связи. Наличие таких сообщений всегда служит настораживающим признаком. Во-вторых, распространение криптографических продуктов регулируется законодательно и имеет множество ограничений при экспорте. В то же время для использования и распространения стеганографических средств законодательных ограничений ни в одной стране пока не имеется. В-третьих, методы цифровой и компьютерной стеганографии стали мощным средством решения задач по созданию различных систем контроля над

соблюдением авторских прав на рынке цифровой фото-, аудио-, видеопродукции и при распространении программных продуктов (водяные знаки, подписи, защита от подделки, вставка заголовков в оцифрованные аналоговые сигналы и т.д.). Последний факт является серьезным стимулом для финансирования исследований в этой области со стороны крупных производителей.

Основными стеганографическими понятиями являются *сообщение* и *контейнер.* 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 ни чем иным как *носителем сокрытой информации,* поэтому вполне возможно использование и такого термина. В некоторых источниках термин контейнер также заменяют названием «стего», который также является производным от английского сокращения *«stego»* (полное название *«stegano»).*

Определение 2. *Контейнером* (носителем) b (где $b \in B$ — множеству всех контейнеров) называют несекретные данные, которые используют для сокрытия сообщений.

В компьютерной стеганографии в качестве контейнеров могут быть использованы различные оцифрованные данные: растровые графические изображения, цифровой звук, цифровое видео, всевозможные носители цифровой информации, а также текстовые и другие электронные документы.

Определение 3. *Сообщением m* будем называть секретную информацию, наличие которой в контейнере необходимо скрыть. Всевозможные сообщения объединяются в пространство сообщений *M* (естественно, что ему также принадлежит и наше m).

Определение 4. Ключом *K* называют секретную информацию, известную только законному пользователю, которая определяет конкретный вид алгоритма сокрытия.

Через *K* обозначается множество всех допустимых секретных ключей. Заметим, что в работах по стеганографии ключ понимается как в широком, так и в узком смысле. В широком смысле стеганографический ключ — это сам неизвестный противнику способ сокрытия информации. В узком смысле по аналогии с криптографией под стеганографическим ключом понимается секретный параметр применяемого

стеганографического алгоритма, без знания которого извлечение скрытой информации должно быть невозможным. Поэтому будем различать бесключевые стеганографические системы, в которых применяется одно и то же неизвестное противнику стеганографическое преобразование, и системы, в которых стеганографический ключ присутствует. При этом необходимо отличать стеганографический ключ от криптографического, который также может присутствовать в системе и использоваться для предварительного криптографического закрытия внедряемой информации.

В общем случае в качестве сообщений, контейнеров и ключей могут быть использованы объекты произвольной природы. В компьютерной стеганографии в качестве сообщений, контейнеров и секретных ключей используют, как правило, двоичные последовательности, т.е. $M = Z_2^n$ для некоторого фиксированного целого *n*, $B = Z_2^q$ и $K = Z_2^p$, при этом $q >> n$.

Определение 5. *Пустой контейнер* (или, еще говорят, *немодифицированный контейнер)* — это некоторый контейнер *b*, не содержащий сообщения.

Определение 6. *Заполненный контейнер* (или соответственно *модифицированный контейнер)* — это контейнер *b*, содержащий сообщение *m,* в дальнейшем обозначаемый как $b_{m,k}$ (или b_m для случая бесключевой системы).

Определение 7. *Стеганографическим алгоритмом* принято называть два преобразования: прямое стеганографическое преобразование $F: M \times B \times K \to B$ и обратное стеганографическое преобразование $F^{-1} : B \times K \to M$, сопоставляющие соответственно тройке (сообщение, пустой контейнер, ключ) контейнер-результат и паре (заполненный контейнер, ключ) — исходное сообщение, причем

$$F(m,b,k) = b_{m,k}; \quad F^{-1}(b_{m.k},k) = m,$$

где $m \in M$; $b, b_{m,k} \in B$; $\kappa \in K$.

Определение 8. Под *стеганографической системой* будем понимать систему $S = (F, F^{-1}, M, B, K)$, представляющую собой совокупность сообщений, секретных ключей, контейнеров и связывающих их преобразований.

Отметим, что помимо приведенного определения стеганографической системы существует еще одно, в котором определена более ранняя (классическая) схема [8],

являющаяся частным случаем данной схемы. Ее отличительной особенностью является отсутствие зависимости от секретного ключа, т.е.

$$F(m,b) = b_m; \quad F^{-1}(b_m) = m,$$

где $m \in M;\ b, b_m \in B$.

Определение 9. Под *внедрением (сокрытием)* сообщения с помощью системы S в контейнер b понимают применение прямого стеганографического преобразования F к конкретным m, b, и $к$.

Определение 10. *Извлечение* сообщения есть не что иное, как применение обратного стеганографического преобразования с теми же значениями аргументов.

Определение 11. По аналогии с криптографией сторону, пытающуюся раскрыть стеганографическую систему передачи информации и определить наличие сообщения, называют *стеганоаналитиком,* или, по аналогии с английскими источниками, *стегоаналитиком* (что с точки зрения этимологии является менее предпочтительным, поскольку слово «стего» есть не что иное, как сленговое сокращение от полного названия «стегано»).

Соответственно, попытку определить наличие сообщения и его смысл называют атакой на стеганографическую систему. Задача стеганоаналитика состоит в раскрытии стеганографической системы и определении тайно переданного сообщения. В отличие от криптографии, под *раскрытием (взломом)* стеганографической системы принято понимать нахождение такой ее конструктивной либо иной уязвимости, которая позволяет определить факт сокрытия информации в контейнере, и возможность доказать данное утверждение третьей стороне с высокой степенью достоверности. Учитывая это, аналогично криптографическим атакам, атаки на стеганографические системы можно разделить на классы:

• *атаки со знанием только модифицированного контейнера* — аналог криптографической атаки со знанием шифртекста. Стеганоаналитик в этом случае обладает только модифицированным контейнером, по которому он пытается определить наличие сокрытого сообщения. Данный вид стеганографических атак — базовый из всех, по которым оцениваются стеганосистемы;

• *атаки со знанием немодифицированного контейнера* возможны в случае, когда

стеганоаналитик также обладает способностью узнавать, какой именно немодифицированный контейнер был использован для сокрытия сообщения. Данная атака определяет возможность определения факта сокрытия сообщений в дальнейшем, в зависимости от наличия однажды перехваченного контейнера и раскрытого сообщения;

• об *атаках с выбором сообщения* говорят, когда стеганоаналитик имеет возможность указывать, какие именно сообщения будут сокрыты, но при этом не имеет возможности указать контейнер, который будет для этого использоваться. Стойкость к данной атаке характеризует стойкость системы к перехвату и отслеживанию сообщений, посланных с использованием одного и того же контейнера. Данный вид атак иногда также позволяет определить тип примененной стеганографической системы;

• *атаки с выбором контейнера,* аналогично предыдущим, позволяют определить стойкость стеганосистемы к раскрытию в случае повторного использования одного и того же сообщения с различными контейнерами;

• *атаки по подмене и имитации* не призваны определить факт наличия сообщения или извлечь его, их применяют для модификации скрытой информации, либо имитации такой передачи;

• *атаки по противодействию передаче информации* используют для уничтожения сокрытой информации и снижения пропускной способности каналов скрытой передачи данных.

При проведении анализа стеганографической системы следует по аналогии с криптографией учитывать необходимость применения правила Керкгоффа, которое заключается в том, что стойкость секретной системы должна определяться только секретностью ключа.

Сам процесс стеганоанализа контейнера можно разделить на два различных по сути действия:

• определение наличия сообщения в контейнере;

• извлечение содержания сокрытого сообщения.

Стеганоаналитик, перед которым стоит задача первого или второго типа, является, по сути, *пассивным нарушителем,* поскольку он не модифицирует доступные ему для анализа данные. С другой стороны, стеганоаналитик, который может вносить изменения в передаваемые по каналу данные, носит название *активный нарушитель (активный противник).* Атаки по подмене, имитации и противодействию характерны только для

активного нарушителя, в то время как остальные виды атак присущи только пассивным нарушителям.

Устоявшимся является использование термина *активный стеганоанализ* для описания действий активного нарушителя, что несколько противоречит смысловому содержанию понятия стеганоанализа. В дальнейшем, для того чтобы не вносить путаницу, использование термина «активный стеганоанализ» будет максимально сокращено. При этом смысл термина будет оговариваться отдельно в каждом случае.

Для удобства введем еще несколько понятий, связанных с эффективностью стеганосистем.

Пусть B — контейнер, а M — скрываемое сообщение, и соответственно $|B|$ — объем контейнера, а $|M|$ — размер сообщения.

Определение 12. *Пространством сокрытия* (ПС) будем называть те участки контейнера (биты, поля и т.д.), в которых стеганосистема может сокрыть информацию.

Определение 13. *Используемое пространство сокрытия* (ИПС) представляет собой совокупность областей пространства сокрытия, в которых действительно произошло сокрытие в процессе работы стеганосистемы. Обозначив для удобства файл, содержащий контейнер через *File,* получим цепочку соотношений, которой связаны эти величины:

$$|M| \le |ИПС| \le |ПС| \le |B| \le |File|.$$

Обычно файл *File* помимо контейнера содержит некоторые дополнительные данные. Вследствие того, что в большинстве случаев размер этих данных существенно меньше объема контейнера, мы можем пренебречь разницей и считать, что $|B| = |File|$.

Определение 14. *Коэффициент сокрытия* определяется соотношением КС = |M|/|B| и пригоден для предварительного определения объема контейнера *B,* который должен быть обработан для передачи сообщения размером $|M|$.

Определение 15. По аналогии с коэффициентом сокрытия, *коэффициент использования контейнера (КЭ или коэффициент эффективности)* — это отношение

размера наибольшего сообщения, которое возможно скрыть в контейнере, к объему контейнера:

$$КЭ(B) = \frac{|M_{\max}(B)|}{|B|}$$

Можно также определить информационную емкость контейнера как

$$И(B) = \frac{|ПС|}{B}$$

Очевидно, что значения коэффициентов КЭ и И зависят не только от выбранного контейнера, но также и от используемого стегано-графического метода.

Для систем скрытого обмена информацией, безусловно, желательно использовать контейнеры с возможно большей информационной емкостью. Однако применение таких контейнеров чревато их высокой уязвимостью к обнаружению наличия скрытой информации. Поэтому, как правило, предпочтение отдается большей защищенности, чем высокой скорости передачи.

Для систем цифровых водяных знаков, наоборот, информационная емкость не играет никакой важной роли, поскольку объем скрываемой информации, как правило, намного меньше объема контейнера. С другой стороны, для обеспечения невозможности удаления водяного знака его следует разнести по всему пространству сокрытия, чтобы он содержался в каждом фрагменте файла-контейнера.

Заметим, что данные оценки являются очень грубыми и не учитывают таких свойств информации, содержащейся в контейнере, как избыточность, наличие разнородных участков, применяемый алгоритм сжатия и т.д. Вместе с тем, даже при таком общем подходе проявляется основное отличие стеганографических систем от криптографических, а именно, зависимость всех свойств системы от конкретного контейнера.

1.3 Общая схема стеганографической системы

Рассмотрим общую схему стеганографической системы, используемой для передачи данных при наличии как пассивного, так и активного противника. Согласно данной схеме, на передающей стороне сообщение скрывается в контейнере при помощи прямого стеганографического преобразования. Затем полученный модифицированный

контейнер по открытым каналам связи отправляется принимающей стороне, где после его получения при помощи обратного стеганографического преобразования извлекается исходное сообщение (рис. 1.).

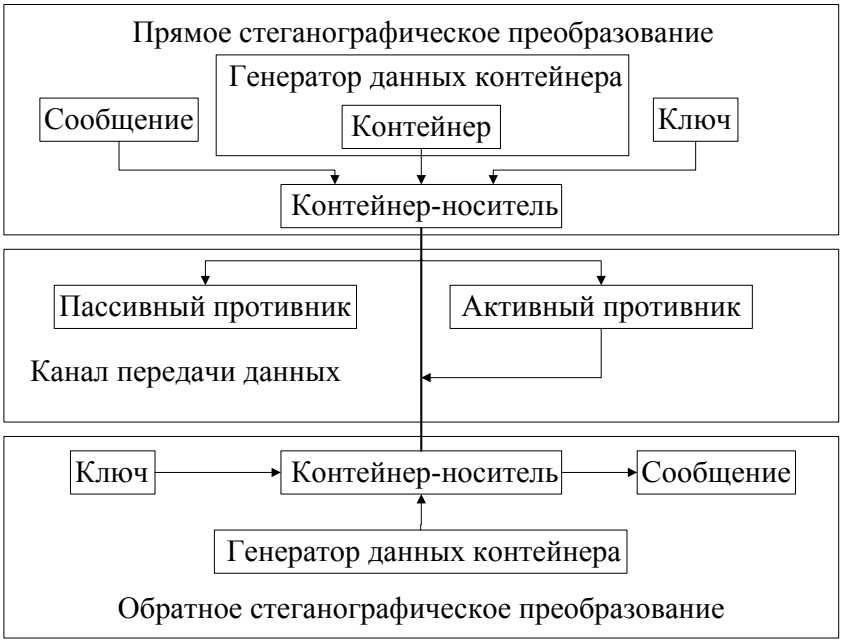

Рис. 1. Обобщенная структура стеганографической системы.

Как было сказано выше, задача пассивного противника состоит в определении факта наличия в контейнере сокрытых данных, при этом делается допущение о том, что он может перехватывать все посланные контейнеры и анализировать их как по отдельности, так и в совокупности. В случае если пассивному противнику удалось верно определить факт наличия скрытого сообщения в контейнере, он может пытаться извлечь его с целью ознакомления с его содержанием. Однако, как правило, перед сокрытием сообщение шифруется, и поэтому, даже если противнику удастся извлечь сообщение, то для ознакомления с его содержимым будет необходимо его дешифровать. Если же пассивный противник не сможет определить факт наличия сообщения, то попытки извлечь сообщение ни к чему не приведут в силу того, что эта задача будет иметь огромное множество решений, выбрать верное из которых практически невозможно.

Активный противник может вносить изменения в передаваемый по каналам связи контейнер, при этом предполагается, что ни на принимающей, ни на передающей стороне не знают, какой контейнер был изменен во время передачи, а какой нет. На этот вопрос должно верно отвечать обратное стеганографическое преобразование. Самая простая задача активного противника — это уничтожение сокрытой информации без определения

факта наличия сообщения. Если же перед активным противником стоит задача изменения сокрытого сообщения, то перед ее выполнением он должен проанализировать контейнер, чтобы удостовериться, что в контейнере действительно содержится сообщение, которое он должен изменить.

Очевидно, что стеганографическая система, предназначенная для передачи данных, в первую очередь должна быть стойкой к попыткам определить факт ее использования. Но если при этом она не будет стойкой к попыткам уничтожить скрытое с ее помощью сообщение, т.е. к попыткам понизить пропускную способность канала скрытой передачи (а в идеале — не допустить никакой скрытой передачи, даже той, наличие которой неизвестно), то эффективность ее практического использования при наличии активного противника может достигнуть нуля. Поэтому стойкость к таким атакам пассивного и активного противника — это и есть основное требование, которое предъявляется к стеганографической системе.

Впервые схема стеганографической системы для передачи данных с наличием только пассивного противника была подробно описана в работе Густава Симмонса в 1983 году. Представим себе, что Алиса и Боб находятся в тюрьме и хотят разработать план побега. Все их послания друг другу просматриваются противником (в данном случае это надзиратель Ева, которая желает разрушить их план и переведет их в тюрьму более строгого режима, как только поймет, что в их посланиях содержится скрытая от нее информация). Задача, стоящая перед Алисой и Бобом, состоит в том, чтобы разработать такой способ обмена информацией, при использовании которого Ева ничего не смогла заподозрить.

Раздел 2. Компьютерная стеганография.

УЧЕБНЫЕ ЦЕЛИ РАЗДЕЛА 2.

1) Раскрыть понятие компьютерной стеганографии.

2) Определить структуру модели компьютерной стеганографической системы.

3) Провести классификацию методов и средств компьютерной стеганографии.

4) Провести краткий сопоставительный анализ методов и средств компьютерной стеганографии.

5) Ознакомиться с примером известной системы.

Тема 2. Компьютерная стеганография: классификация, сопоставительный анализ методов и средств.

Вопросы для самостоятельного изучения и обсуждения на семинаре.

1) Структура стеганографической системы.
2) Сопоставительный анализ основных методов и средств компьютерной стеганографии.
3) Изучение свободно распространяемых продуктов.

Литература для изучения темы.

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.
2. Lin Ch-Y., Chang Sh.-F. Distortion Modeling and Invariant Extraction for Digital Image Print-and Scan Process. International Symposium on Multimedia Information Processing, 1999. P. 10.
3. Lin Ch-Y., Chang Sh.-F. Public Watermarking Surviving General Scaling and Cropping: An Application for Print-and-Scan Process. Multimedia and Security Workshop at ACM Multimedia, 1999.

2.1 Методы компьютерной стеганографии (КС).

Результаты сопоставительного анализа методов КС приведены в таблице 1

Таблица 1.

Методы КС	Краткая характеристика методов	Недостатки	Преимущества
1. Методы использования специальных свойств компьютерных форматов данных			
1.1. Методы использования зарезервированных для расширения полей компьютерных форматов данных	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Низкая степень скрытности, передача небольших объемов информации	Простота использования
1.2. Методы			

специального форматирования текстовых файлов:			
1.2.1. Методы использования известного смещения слов, предложений, абзацев	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	1.Слабая производительность метода,передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)		
1.2.3. Методы использования специальных свойств полей форматов, не отображаемых на экране	Методы основаны на использовании специальных "невидимых", скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)		
1.3. Методы скрытия в неиспользуемых местах гибких дисков	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	1. Слабая производительность метода, передача небольших объемов информации	Простота использования. Имеется опубликованное программное

		2. Низкая степень скрытности	обеспечение реализации данного метода
1.4. Методы использования имитирующих функций (mimic-function)	Метод основан на генерации текстов и является обобщением акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	1. Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Результирующий текст не является подозрительным для систем мониторинга сети
1.5. Методы удаления идентифицирующего файл заголовка	Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок,оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю	Простота реализации. Многие средства (White Noise Storm, S-Tools), обеспечивают реализацию этого метода с PGP шифроалгоритмом
2. Методы использования избыточности аудио и визуальной информации			
2.1. Методы использования избыточности цифровых фотографии, цифрового звука и цифрового видео	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого

	восприятия, что и дает возможность скрытия конфиденциальной информации	компрометирующих признаков требуется коррекция статистических характеристик	изображения товарной марки, регистрационных номеров и т.п

Как видно из таблицы 1, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. На основании анализа материалов можно сделать вывод, что основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации. Как показывает предварительный анализ, применение стеганографических методов для решения задач, поставленных в ТЗ, принципиально возможно. Однако все проанализированные методы обладают следующими недостатками:

- Множество возможных реализаций в КС счетно и конечно, что позволяет реализовать атаки простым перебором методов, хотя это требует значительных вычислительных затрат.

- Не все реализации отвечают требованию возможности аппаратной реализации.

2.2 Новые разработки в области компьютерной стеганографии

2.2.1 Система StegFS.

StegFS - стеганографическая файловая система, способная преодолевать указанные выше недостатки, предлагая владельцам данных возможность отрицания существования этих данных. StegFS надежно скрывает файлы, выбранные пользователем, в файловой системе таким образом, что, без соответствующих ключей, взломщик не сможет угадать их существование, даже если он хорошо знаком с файловой системой и имеет к ней полный доступ.

Контроль доступа пользователей и шифрование – стандартные механизмы защиты данных в текущих продуктах, таких, как Encrypting File System (EFS). Эти механизмы позволяют администратору ограничить доступ пользователей к тем или иным фалам и папкам. Однако, контроль доступа и шифрование могут не помочь в случаях, когда речь

идет об очень ценных данных. Само присутствие зашифрованного файла или папки является свидетельством того, что на компьютере присутствуют ценные данные.

Чтобы защитить данные в таких ситуациях, необходимо разработать файловую систему, которая предоставляет доступ к данным только при правильно введенном пароле. Без этого взломщик не сможет получить даже данных о том, существуют ли данные.

Таким образом, пользователи, находящиеся под давлением, смогут отрицать само существование информации. Он может раскрыть наименее ценную информацию (например, адресную книгу, переписку), но сохранить самую ценную, например, финансовую информацию. Неавторизованные пользователи и даже администраторы не смогут получить доступ к такой информации.

В последние годы было несколько решений для стеганографической файловой системы. В этих решениях было множество ограничений и недостатков, связанных с огромным увеличением операций ввода/вывода, малоэффективным использованием свободного пространства и даже вероятностью потерять данные. Такие ограничения не позволили этим решениям выйти на массовый рынок.

Новая система StegFS позволяет пользователю выборочно скрыть файлы и папки таким образом, что взломщик даже не догадается об их существовании. Чтобы гарантировать свою практичность, StegFS разработана с учетом трех требований:

1) она не должна терять или повреждать данные
2) она должна позволять владельцам информации отрицать ее существование
3) должна минимизировать вычислительные затраты и затраты на пространство

StegFS исключает скрытые папки и файлы из центральной директории файловой системы. Вместо этого, метаданные скрытой информации хранятся в заголовке непосредственно самого объекта. Весь объект, включая заголовок и данные, зашифрован, чтобы сделать его неотличимым от неиспользуемых блоков для наблюдателя. Только авторизованный пользователь с корректным ключом может получить местоположение заголовка и доступ к самой информации через заголовок.

StegFS была реализована в операционной системе Linux, и многочисленные эксперименты подтвердили, что StegFS на самом деле качественно увеличивает такие

показатели, как производительность и использование дискового пространства, по сравнению с существующими схемами.

2.2.2 Архитектура файловой системы StegFS.

Рисунок 3 дает краткий обзор файловой системы StegFS. Дисковое пространство разбивается на блоки стандартного размера и битовый массив отслеживает, свободен ли каждый блок или был зарезервирован – нулевой бит указывает на то, что соответствующий блок свободен; бит = 1 – на используемый блок. Доступ ко всем простым файлам осуществляется через центральную директорию, которая смоделирована через inode таблицу в Unix. Скрытые файлы не зарегистрированы в центральной директории, хотя блоки, занимаемые ими, отделены в битовом массиве, чтобы защитить пространство от перераспределения.

После того, как файловая система создана, произвольно сгенерированные шаблоны записываются во все блоки таким образом, что оно не отличаются от свободных блоков. Кроме того, некоторые произвольно выбранные блоки отброшены, при помощи включения соответствующих им бит в битовый массив. Эти блоки необходимы для того, чтобы предотвратить любую попытку найти скрытые данные при просмотре блоков, которые помечены в битовом массиве, но не входят в центральную директорию. Чем выше число отброшенных блоков, тем труднее достичь цели при таком исследовании « в лоб». Однако, это необходимо согласовать с необходимостью правильно использовать дисковое пространство. На практике, число отброшенных блоков может определяться администратором или произвольно устанавливаться StegFS.

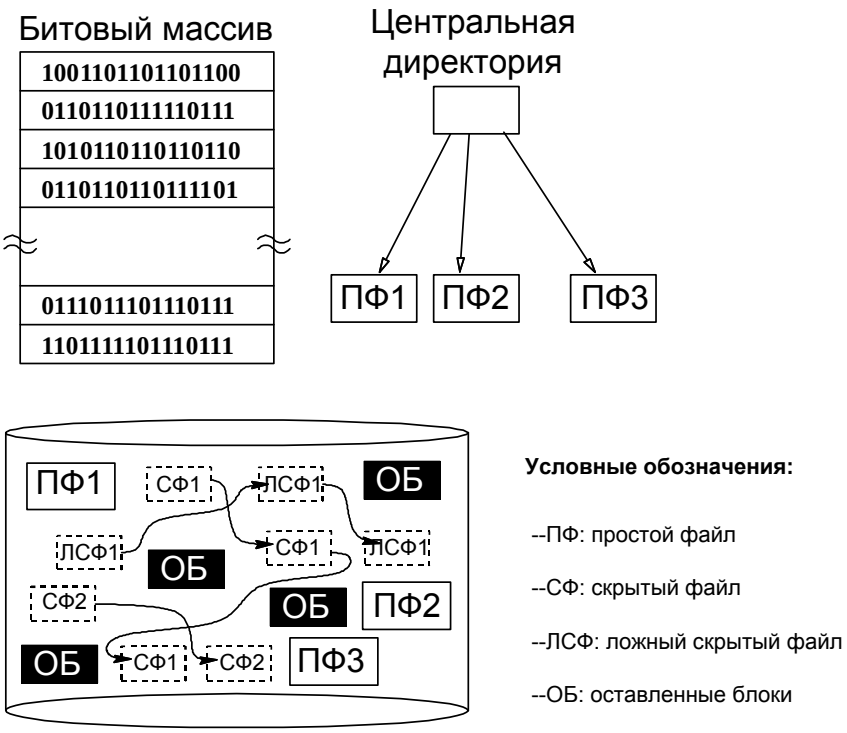

Рис. 2. Обзор стеганографической файловой системы StegFS

StegFS дополнительно поддерживает один или более ложные скрытые файлы, которые она периодически обновляет. Это необходимо для того, чтобы удержать взломщика от предположения, что блоки, размещенные в битовом массиве и не принадлежащие ни одному простому файлу, должны содержать скрытые данные. Число таких файлов также может выставляться вручную или автоматически.

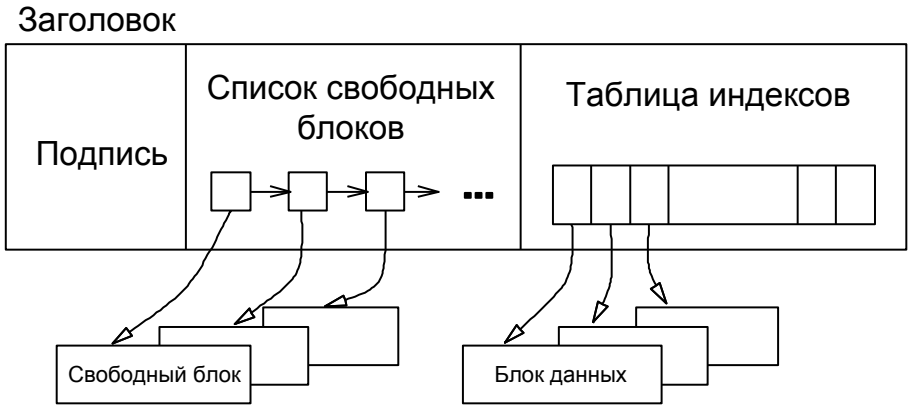

Рис. 3. Структура скрытого файла

В примере на рисунке 2 в файловой системе находится два скрытых пользовательских файла, один ложный скрытый файл и 3 простых файла, каждый из

которых состоит из одного или более дисковых блоков. Кроме того, в системе также присутствуют отброшенные блоки.

Структура скрытого файла показана на рисунке 3. Доступ к каждому скрытому файлу осуществляется через его собственный заголовок, который состоит из 3-х структур данных:

1) Ссылка на inode таблицу, которая адресует все блоки данных в файле
2) Подпись, которая уникальным образом идентифицирует файл
3) Присоединенный список указателей на свободные блоки, занимаемые файлом

Все компоненты файла, включая заголовок и данные, зашифрованы при помощи ключа, чтобы сделать их неотличимыми от отброшенных блоков и ложных файлов.

Поскольку скрытые файлы не записываются в центральную директорию, StegFS должна иметь возможность найти заголовок файла, используя только имя файла и ключ. Во время создания файла StegFS использует хэш-значение, вычисленное из имени файла и ключа для генератора случайных номеров блоков. Затем, каждый успешно сгенерированный блок она просматривает в битовом массиве до тех пор, пока не найдет свободный блок, чтобы сохранить в него заголовок. После того, как заголовок сохранен, последующие блоки могут быть назначены произвольно, согласуясь с битовым массивом, и затем присоединены к inode таблице файла. Чтобы избежать перезаписи файла из-за того, что различные пользователи используют одно и то же имя файла и пароль, физическое имя файла получается при помощи сложения идентификатора пользователя с полным путем к файлу.

Чтобы восстановить скрытый файл, StegFS снова вводит хэш-значение, полученное из имени файла и ключа, просматривает в битовом массиве первый блок, помеченный в качестве используемого и соответствующего файловой подписи. Первые номера блоков, выданные генератором, могут не содержать правильного заголовка, т.к. во время создания файла они были не доступны. Таким образом, подпись, полученная из имени и ключа, наиболее важна при получении местоположения необходимого заголовка. Чтобы избежать неправильные соответствия, файловая подпись должна быть длинной строкой. Хэш-функция генерируется таким образом, что взломщик не сможет получить ее из имени файла и ключа.

Другой особенностью скрытого файла является то, что он может держаться за свободные блоки. Целью этого является удержание злоумышленника, который начинает

просмотр файловой системы сразу после того, как она была создана и который, следовательно, имеет возможность убрать отброшенные блоки из рассмотрения, от отслеживания местонахождения ложных скрытых файлов. Такой нарушитель, возможно, сможет выделить часть блоков, выделенных для хранения скрытого файла. Поддерживая внутренний пул свободных блоков в скрытом файле, StegFS препятствует взломщику в отделении ценных данных от свободных блоков. Когда создается скрытый файл, StegFS напрямую выделяет для данного файла несколько блоков. Эти блоки, отслеженные через связанный список указателей в заголовке файла, выбираются произвольно из свободного пространства в файловой системе. Таким образом, увеличивается трудность определения принадлежности блоков к данному файлу и порядка между ними. В процессе расширения файла, блоки в произвольном порядке берутся из присоединенного списка для хранения данных или inodes, до тех пор, пока число свободных блоков не превысит некоторую границу. Наоборот, когда файл уменьшается, свободные блоки добавляются в пул до тех пор, пока их число не превысит некоторое пороговое значение и тогда эти блоки возвращаются в файловую систему.

2.2.3 Поддержка директорий

Хотя StegFS имеет несколько инструментов, сохраняющих файлы, скрытые пользователем, наиболее эффективной она оказывается в мультипользовательской системе. Происходит это потому, что когда много блоков, выделено для скрытых файлов, взломщик может оценить размеры ценной информации в этих файлах, но точно оценить, сколько информации принадлежит тому или иному пользователю не представляется возможным. Таким образом, пользователь, действующий под давлением, имеет дополнительные возможности отрицания того, что существует какая-либо ценная информация, принадлежащая ему.

Естественным требованием к мультипользовательской системе является необходимость совместного использования скрытых файлов. Т.к. пользователь может захотеть совместно использовать лишь выбранные им файлы, StegFS защищает каждый скрытый файл произвольно сгенерированным ключом доступа к файлу (FAK), а не ключом пользователя, так, что пользователи могут обмениваться именами файлов и ключами.

Рисунок 3 показывает структуру директорий, которую применяет StegFS, чтобы помочь пользователям отслеживать их скрытые файлы. StegFS позволяет пользователю иметь несколько пользовательских ключей доступа (UAK). Для каждого UAK StegFS

поддерживает директорию из пар значений (имени файла и FAK) для всех скрытых файлов, к которым можно иметь доступ при помощи этого UAK.

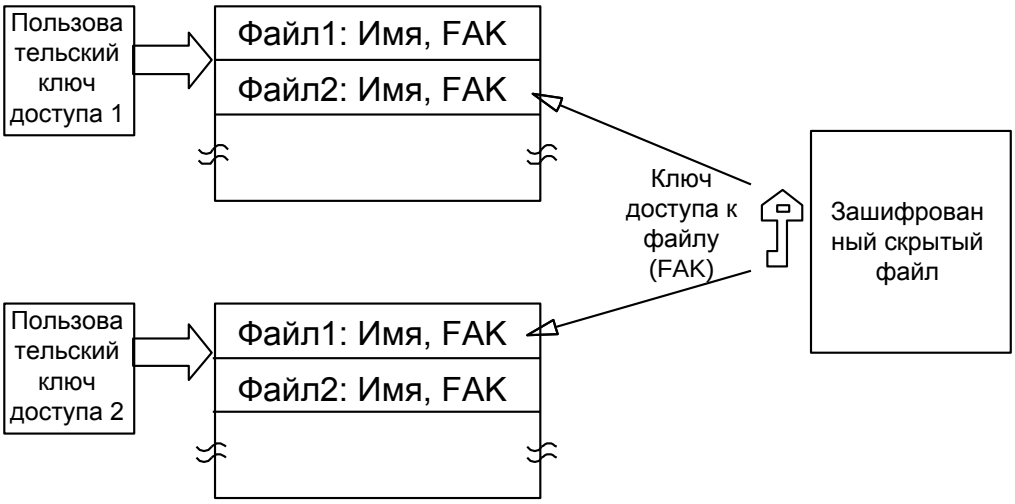

Рис. 4. Структура директорий в StegFS

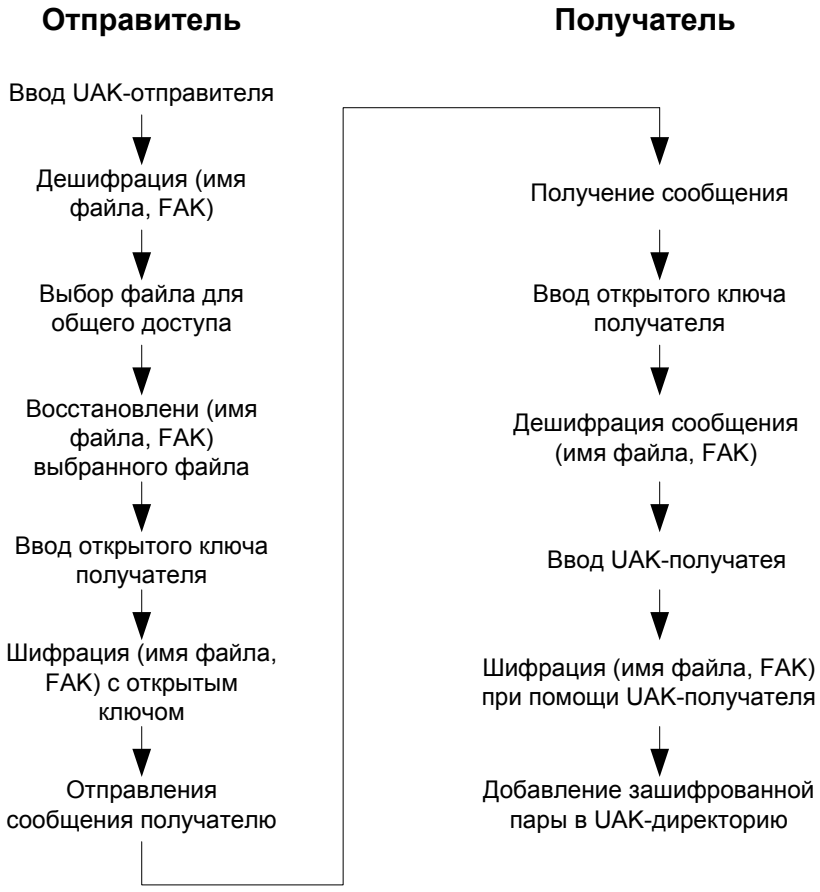

Рис. 5. Совместное использование файлов в StegFS

Вся директория зашифрована при помощи UAK и хранится в виде скрытого файла в файловой системе. UAKи могут управляться независимо, например, храниться на независимых картах для большей защищенности. Чтобы сделать файловую систему более дружественной к пользователю, UAKи, принадлежащие пользователю могут быть организованы в виде иерархии линейного доступа таким образом, что когда пользователь подписывается на данный уровень доступа, все скрытые файлы, связанные с данным UAKом на этом уровне или ниже становятся видимыми. Таким образом, под давлением пользователь может выборочно раскрыть только подмножество своих UAKов. Не зная, как много UAKов у пользователя, взломщик не сможет предположить, что пользователь удерживает часть UAKов.

Чтобы обмениваться скрытыми файлами между пользователями, владелец должен передать пару (имя файла, FAK) получателю. Т.к. ни владелец, ни StegFS не имеют UAK получателя, обмен файлов не может быть автоматическим. Вместо этого, информация о файле шифруется с открытым ключом получателя, и результирующее сообщение посылается получателю, например, по электронной почте. Используя утилиту StegFS, получатель дешифрует сообщение при помощи своего закрытого ключа и ассоциирует скрытый файл со своим собственным UAKом, в это время информация в файле добавляется в директорию UAK и сообщение уничтожается. Практика передачи информации в файле – относительно слабое место в StegFS, т.к. зашифрованное сообщение может предупредить взломщика о существовании скрытого файла. Однако, т.к. у каждого скрытого файла имеется FAK, обнаруженное сообщение не подставляет другие скрытые файлы в StegFS. Механизм обмена файлами показан на рисунке 4.

Наконец, когда владелец скрытого файла решает отменить права общего пользования файлом, StegFS сначала делает новую копию с новым FAK и возможно с другим именем файла, затем удаляет исходный файл, чтобы отменить старый FAK. Просроченный FAK будет удален из директорий других пользователей после следующей загрузки.

Раздел 3. Цифровая стеганография: Основные положения и анализ методов и средств.

УЧЕБНЫЕ ЦЕЛИ РАЗДЕЛА 1.

1) Раскрыть понятие цифровой стеганографии.

2) Определить основную терминологию.

3) Провести обзор классификацию методов и средств цифровой стеганографии.

4) Провести сопоставительный анализ средств цифровой стеганографии.

Тема 3. Цифровая стеганография: Принятая терминология, классификация и сопоставительный анализ методов и средств.

Вопросы для самостоятельного изучения и обсуждения на семинарах.

1) Исторически сложившиеся методы сокрытия данных. Структура цифровой стеганографической системы.
2) Принятая терминология.
3) Теоретические положения цифровой стеганографии с учетом принятой терминологии.
4) Сопоставительный анализ средств цифровой стеганографии.

Литература для изучения темы.

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.
2. Kutter M. Watermarking Resisting to Translation, Rotation, and Scaling. Signal Processing Laboratory, 1998. P. 10.
3. Kutter M. Digital Signature of Color Images using Amplitude Modulation. Signal Processing Laboratory, 1997. P. 9.
4. Herrigel A., Pereira S., Petersen H. Secure Copyright Protection Techniques for Digital Images. International Workshop on Information Hiding, 1998. P. 22.
5. Ramkumar M. Data Hiding in Multimedia – Theory and Applications. New Jersey Institute of Technolog, 1999. P. 70.
6. Bender W. Applications for Data Hiding. IBM Systems Journal, 2000. P. 22.
7. Chae J., Manjunath B. A Robust Data Hiding Technique using Multidimensional Lattices. Proc. IEEE Conference on Advances in Digital Libraries, 1998. P. 8.
8. Chae J., Manjunath B. A Technique for Image Data Hiding and Reconstruction without Host Image. Proceedings of the SPIE - The International Society for Optical Engineering. 1999, P.
9. Cuche E., Marquet P., Spatial filtering for zero-order and twin-image elimination in digital off-axis holography. Applied Optics V.39, 2000. P. 4070–4075

3.1Структура цифровой стеганографической системы.

В настоящем разделе для краткости принято обозначать стеганографическое сообщение, как цифровой водяной знак (ЦВЗ). Рассмортрим структуру цифровой стеганографической системы.

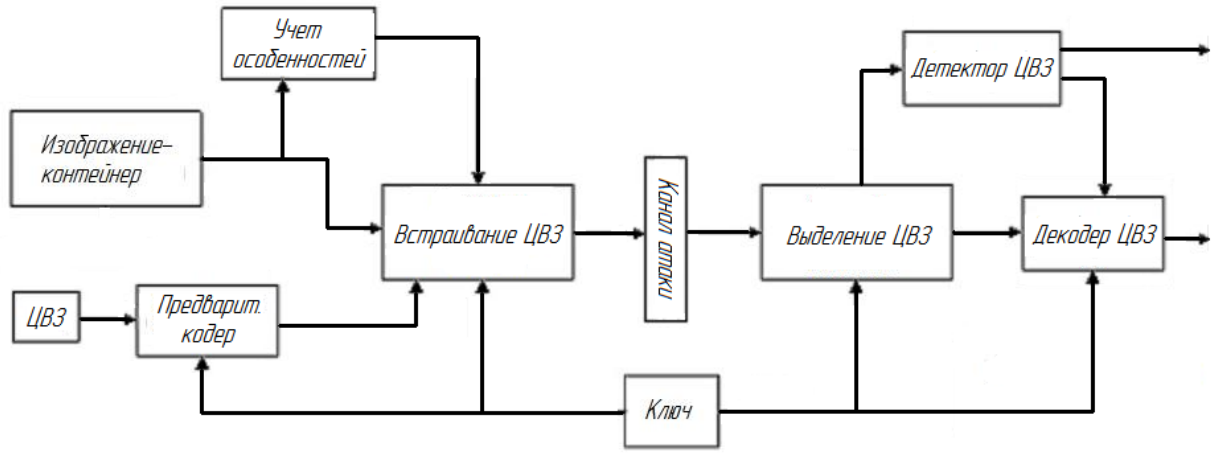

Рис.6 Структурная схема типичной цифровой стегосистемы

Стегосистема, представленная на рис.6, выполняет задачу встраивания и выделения цифровых водяных знаков (ЦВЗ) из изображения-контейнера. Предварительный кодер - устройство, предназначенное для преобразования скрываемого водяного знака к виду, удобному для встраивания в контейнер. Устройство встраивания ЦВЗ предназначено для осуществления встраивания (вложения) скрытого ЦВЗ в изображение-контейнер. В стегосистеме происходит объединение двух типов информации так, чтобы они могли быть различимы двумя принципиально разными детекторами. В качестве одного из детекторов выступает система выделения ЦВЗ, в качестве другого – человек. Предварительная обработка часто выполняется с использованием ключа для повышения секретности встраивания. Далее ЦВЗ «вкладывается» в контейнер, например, путем модификации младших значащих бит коэффициентов. Этот процесс возможен благодаря особенностям системы восприятия человека. Хорошо известно, что изображения обладают большой психовизуальной избыточностью. Глаз человека подобен низкочастотному фильтру, пропускающему мелкие детали. Особенно незаметны искажения в высокочастотной области изображений. В стегодетекторе (Детектор ЦВЗ) происходит обнаружение ЦВЗ в (возможно измененном) защищенном ЦВЗ изображении. Это изменение может быть

обусловлено влиянием ошибок в канале связи, операций обработки сигнала, преднамеренных атак нарушителей.

Различают стегодетекторы, предназначенные для обнаружения факта наличия ЦВЗ и устройства, предназначенные для выделения этого ЦВЗ (стегодекодеры, Декодер ЦВЗ). В первом случае возможны детекторы с жесткими (да/нет) или мягкими решениями. Решение о наличии или отсутствии ЦВЗ выносится либо на основании расстояния по Хэммингу, либо на основании взаимной корреляции между имеющимся сигналом и оригиналом (при отсутствии которого, используются статистические методы).

В зависимости от того, какая информация требуется детектору для обнаружения ЦВЗ, стегосистемы ЦВЗ делятся на три класса:

- открытые;
- полузакрытые;
- закрытые системы.

Существуют 2 типа закрытых систем: в первом типе, детектору требуется и исходный контейнер и исходный ЦВЗ, а на выходе система выдает решение о наличии или отсутствии ЦВЗ (такие стегосистемы имеют наибольшую устойчивость по отношению к внешним воздействиям); во втором типе детектору нужен только исходный контейнер, а на выходе система выдает восстановленный ЦВЗ. В полузакрытых системах детектору требуется исходный ЦВЗ, на выходе выдается решение о наличии или отсутствии ЦВЗ. Наибольшее применение имеют открытые стегосистемы ЦВЗ, так как они аналогичны системам скрытой передачи данных, и в них детектору не нужны ни исходный контейнер, ни исходный ЦВЗ, а на выходе система выдает восстановленный из контейнера ЦВЗ.

Встраивание сообщения в контейнер может производиться при помощи ключа, одного или нескольких. Ключ - псевдослучайная последовательность (ПСП) бит, порождаемая генератором, удовлетворяющим определенным требованиям (криптографически безопасный генератор). Числа, порождаемые генератором ПСП, могут определять позиции модифицируемых отсчетов (пикселей на изображении). Скрываемая информация внедряется в соответствии с ключом в те отсчеты, искажение которых не приводит к существенным искажениям контейнера. Эти биты образуют стегопуть. Под существенным искажением можно понимать искажение, приводящее как к неприемлемости для человека-адресата заполненного контейнера, так и к возможности выявления факта наличия скрытого сообщения после стегоанализа.

Встраиваемые ЦВЗ могут быть трех типов:

- робастные;
- хрупкие;
- полухрупкие.

Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стегоконтейнер. Робастные ЦВЗ могут быть 3-х типов. Это ЦВЗ, которые могут быть обнаружены всеми желающими, хотя бы одной стороной, либо это могут быть ЦВЗ которые трудно модифицировать или извлечь контента (контейнера) (ЦВЗ для аутентификации).

Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера и применяются для аутентификации сигналов (изображений). Отличие от средств электронной цифровой подписи заключается в том, что хрупкие ЦВЗ все же допускают некоторую модификацию контента. Это важно для защиты мультимедийной информации, так как законный пользователь может, например, пожелать сжать изображение. Другое отличие заключается в том, что хрупкие ЦВЗ должны не только отразить факт модификации контейнера, но также вид и местоположение этого изменения.

Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Вообще говоря, все ЦВЗ могут быть отнесены к этому типу. Однако полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми по отношению к определенного рода операциям. Например, они могут позволять выполнять сжатие изображения, но запрещать вырезку из него или вставку в него фрагмента.

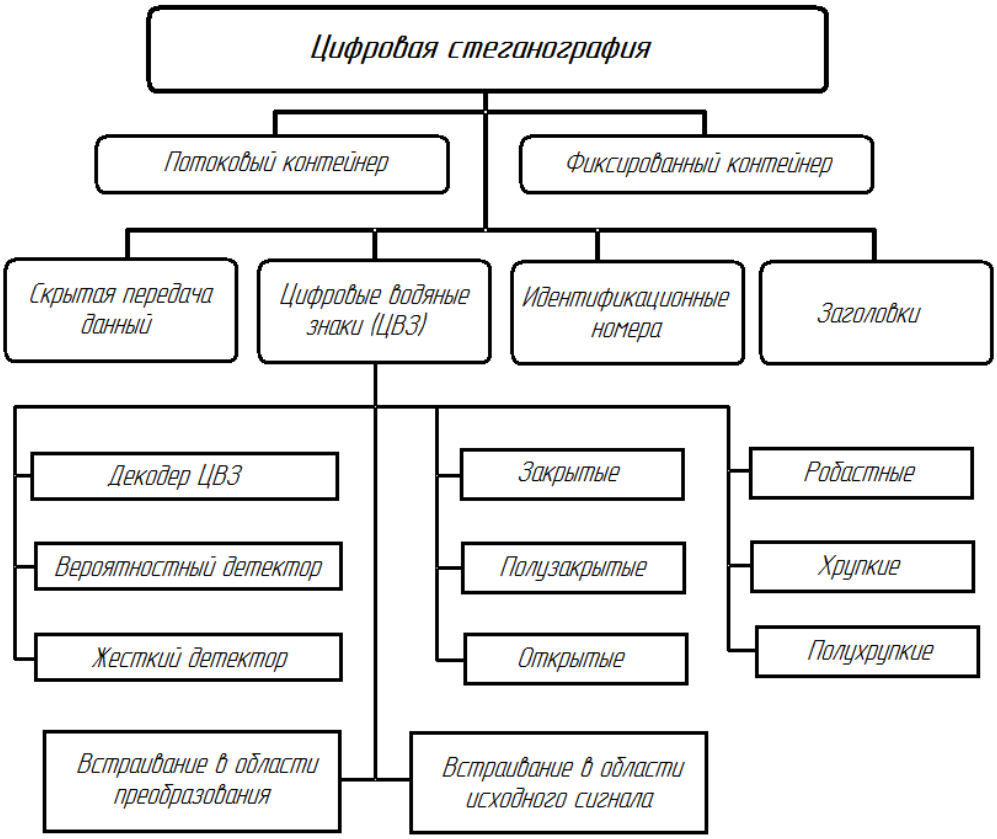

рис.7 Классификация систем цифровой стеганографии

3.2 Алгоритмы встраивания информации в изображения

Все современные алгоритм встраивания информации в контейнеры должны обеспечивать робастность встраиваемых ЦВЗ. В частности, изображения-контейнеры со встроенными ЦВЗ должны предусматривать возможность сжатия контейнера любым из методов. Поэтому стегоалгоритмы учитывают свойства системы человеческого зрения аналогично алгоритмам сжатия изображений, и используют те же преобразования, что и в современных алгоритмах сжатия (дискретное косинусное преобразование в JPEG, вейвлет-преобразование в JPEG2000). Следовательно, вложение информации может производится либо в исходное изображение, либо одновременно с осуществлением сжатия изображения-контейнера, либо в уже сжатое алгоритмом изображение.

Под сжатием понимается уменьшение числа бит, требующихся для цифрового представления изображений. В основе сжатия лежат два фундаментальных явления: уменьшение статистической и психовизуальной избыточности. Статистическая избыточность может быть пространственной, или корреляцией между соседними пикселями, либо спектральной, или корреляцией между соседними частотными полосами.

В алгоритмах сжатия осуществляют обнуление не пикселов изображения, а спектральных коэффициентов. Преимущество такого подхода заключается в том, что близкие к нулю спектральные коэффициенты имеют тенденцию располагаться в заранее предсказуемых областях, что приводит к появлению длинных серий нулей и повышению эффективности кодирования. Большие по величине коэффициенты («значимые») подвергают более или менее точному квантованию и также сжимают кодером длин серий. Последним этапом алгоритма сжатия является применение энтропийного кодера (Хаффмана или арифметического).

Для оценки качества восстановленного изображения используют либо меру среднеквадратического искажения, определяемую как

$$СКО = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2 ,$$

где N - число пикселей в изображении, $x_i, \hat{x}_i$ - значение пикселей исходного и восстановленного изображений.

Либо применяется модификация этой меры - пиковое отношение сигнал/шум, определяемое как

$$ПОСШ = 10\log_2 \frac{N \cdot 255^2}{\sum_{i=1}^{N}(x_i - \hat{x}_i)^2},$$

где 255 - максимальное значение яркости полутонового изображения (т.е. 8 бит/пиксель). Восстановленное изображение считается приемлемым, если $ПОСШ \geq 28 \div 30$ дБ (в среднем).

Часто используется принцип встраивания данных, когда сигнал контейнера представлен последовательностью из n бит. Скрытие информации начинается с определения бит контейнера, которые можно изменять без внесения заметных искажений – стегопути. Далее среди этих бит обычно в соответствии с ключом выбираются биты, заменяемые битами ЦВЗ.

По способу встраивания информации стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения

информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером, либо «вплавляется» (fusion) в него. В нелинейных методах встраивания информации используется скалярное либо векторное квантование. Среди других методов определенный интерес представляют методы, использующие идеи фрактального кодирования изображений.

3.2.1 Алгоритмы встраивания данных в пространственной области

Преимуществом алгоритмов встраивания данных в пространственной области является то, что ЦВЗ внедряется в области исходного изображения и нет необходимости выполнять вычислительно громоздкие линейные преобразования изображений. ЦВЗ внедряется за счет манипуляций яркостью или цветовыми составляющими $l(x,y) \in \{1,...,L\}$ $(r(x,y), g(x,y), b(x,y))$.

Большинство алгоритмов встраивания ЦВЗ в пространственную область изображений основаны на использовании широкополосных сигналов (ШПС). Основной идеей применения ШПС в стеганографии является то, что данные внедряются в шумовой сигнал малой мощности. Так как сигнал малой мощности, то для защиты ЦВЗ применяют помехоустойчивые коды.

3.2.1.1. Алгоритм Катера (Kutter)

Алгоритм Катера предполагает что изображение имеет RGB кодировку. Встраивание выполняется в канал синего цвета, так как к синему цвету система человеческого зрения наименее чувствительна.

S_i - встраиваемый бит, $I = \{R, G, B\}$ - контейнер, $p = (x, y)$ - псевдослучайная позиция, в которой выполняется вложение. Секретный бит встраивается в канал синего цвета путем модификации яркости

$$l(p) = 0.299r(p) + 0.587g(p) + 0.114b(p),$$

$$b'(p) = \begin{Bmatrix} b(p) + ql(p), & если & s_i = 0. \\ b(p) - ql(p), & если & s_i = 1. \end{Bmatrix},$$

где q - константа, определяющая энергию встраиваемого сигнала. Ее величина зависит от предназначения схемы. Чем больше q, тем выше робастность вложения, но тем сильнее его заметность. Извлечение бита получателем осуществляется без наличия у него

исходного изображения, то есть вслепую. Для этого выполняется предсказание значения исходного, немодифицированного пиксела на основании значений его соседей.

Также существует и модификация этого алгоритма, в котором для получения оценки пикселя используют значения нескольких пикселов, расположенных в том же столбце и той же строке. В этом случае оценка $b"(p)$ имеет вид:

$$b"(p) = \frac{1}{4c}\left(-2b"(p)\sum_{i=-c}^{+c} b"(x+i,y) + \sum_{k=-c}^{+c} b"(x,y+k)\right),$$

где c - число пикселов сверху (снизу, слева, справа) от оцениваемого пиксела (c=3). Так как в процессе встраивания ЦВЗ каждый бит был повторен cr раз, то мы получим cr оценок одного бита ЦВЗ. Секретный бит находится после усреднения разности оценки пиксела и его реального значения

$$\delta = \frac{1}{cr}\sum_{i=1}^{cr} \hat{b}_i(p) - b_i(p).$$

Знак этой разности определяет значение встроенного бита.

Данный алгоритм не гарантирует всегда верного определения значения секретного бита, так как функция извлечения бита не является обратной функции встраивания. Алгоритм является робастным ко многим из известных атак: низкочастотной фильтрации изображения, его сжатию в соответствии с алгоритмом JPEG, обрезанию краев.

3.2.1.2. Алгоритм Брундокса (Bruyndonckx)

ЦВЗ представляет собой строку бит. Для повышения помехоустойчивости применяется код Боуза-Чоудхури-Хоквингема (БЧХ). Внедрение осуществляется за счет модификации яркости блока 8x8 пикселов. Процесс встраивания осуществляется в три этапа:

1) Классификация пикселов внутри блока на две группы с примерно однородными яркостями.

2) Разбиение каждой группы на категории, определяемые данной сеткой.

3) Модификация средних значений яркости каждой категории в каждой группе.

При классификации выделяются два типа блоков: блоки с шумовым контрастом и блоки с резко выраженными перепадами яркости. В блоках второго типа зоны с отличающейся яркостью не обязательно должны располагаться вплотную друг к другу, не обязательно должны содержать равное количество пикселов. Более того, некоторые

пиксели вообще могут не принадлежать ни одной зоне. В блоках первого типа классификация особенно затруднена.

Для выполнения классификации значения яркости сортируются по возрастанию. Далее находится точка, в которой наклон касательной к получившейся кривой максимален. Эта точка является границей, разделяющей две зоны в том случае, если наклон больше некоторого порога. В противном случае пиксели делятся между зонами поровну.

Для сортировки пикселов по категориям на блоки накладываются маски, разные для каждой зоны и каждого блока. Назначение масок состоит в обеспечении секретности внедрения.

Множество пикселов оказалось разделенным на пять подмножеств: две зоны, две категории, и пиксели, не принадлежащие какой-либо зоне (для блоков первого типа). $l_{1A}, l_{2A}, l_{1B}, l_{2B}$ - Среднее значение яркости для пикселей двух зон и категорий. $l_{1A} < l_{2A}, \ l_{1B} < l_{2B}$ Встраивание бита ЦВЗ s (модификация) и равенство значений яркостей в каждой зоне обеспечивается:

$$s = \begin{cases} 1, & \begin{cases} l'_{1A} > l'_{1B} \\ l'_{2A} > l'_{2B} \end{cases} \\ 0, & \begin{cases} l'_{1A} < l'_{1B} \\ l'_{2A} < l'_{2B} \end{cases} \end{cases}, \quad \frac{n_{1A} l'_{1A} + n_{1B} l'_{1B}}{n_{1A} + n_{1B}} = l_1 \text{ и } \frac{n_{2A} l'_{2A} + n_{2B} l'_{2B}}{n_{2A} + n_{2B}} = l_2 .$$

Алгоритм извлечения ЦВЗ является обратным алгоритму внедрения. При этом вычисляются средние значения яркостей и находятся разности

$$s'' = \begin{cases} 0, & если \ \ l''_{1A} - l''_{1B} < 0 \ \ и \ \ l''_{2A} - l''_{2B} < 0 \\ 1, & если \ \ l''_{1A} - l''_{1B} > 0 \ \ и \ \ l''_{2A} - l''_{2B} > 0 \end{cases}.$$

3.2.1.3. Алгоритм Ленгелаара (Langelaar)

Данный алгоритм также работает с блоками 8x8. Вначале создается псевдослучайная маска нулей и единиц такого же размера $pat(x, y) \in \{0,1\}$. Далее каждый блок B делится на два субблока B_0 и B_1, в зависимости от значения маски. Для каждого субблока вычисляется среднее значение яркости, l_0 и l_1. Далее выбирается некоторый порог α, и бит ЦВЗ встраивается следующим образом:

$$S = \begin{Bmatrix} 1, & l_0 - l_1 > +\alpha, \\ 0, & l_0 - l_1 < -\alpha. \end{Bmatrix}.$$

Если это условие не выполняется, необходимо изменять значения яркости пикселов субблока B_1. Для извлечения бита ЦВЗ вычисляются средние значения яркости субблоков – l'_0 и l'_1. Разница между ними позволяет определить искомый бит: $S = \begin{Bmatrix} 1, & l_0 - l_1 > 0, \\ 0, & l_0 - l_1 < 0. \end{Bmatrix}$.

3.2.1.4. Алгоритм Питаса (Pitas)

В данном алгоритме ЦВЗ представляет собой двумерный массив бит размером с изображение, причем число единиц в нем равно числу нулей. Существует несколько версий алгоритма, предложенного Питасом. Вначале предлагалось встраивать бит ЦВЗ в каждый пиксель изображения, но позже благоразумно было решено использовать для этой цели блоки размером 2x2 или 3x3 пикселя, что делает алгоритм более робастным к сжатию или фильтрации. ЦВЗ складывается с изображением:

$$l'(x, y) = l(x, y) + \alpha \cdot s(x, y).$$

В случае использования для внедрения блоков детектор ЦВЗ вычисляет среднее значение яркости этого блока. Отсюда появляется возможность неравномерного внедрения ЦВЗ в пиксели, то есть величина $\alpha \neq const$. Таким образом можно получить ЦВЗ, оптимизированный по критерию робастности к процедуре сжатия алгоритмом JPEG. Для этого в блоке 8x8 элементов заранее вычисляют «емкость» каждого пикселя (с учетом ДКП и матрицы квантования JPEG). Затем ЦВЗ внедряют в соответствии с вычисленной емкостью. Эта оптимизация производится раз и навсегда, и найденная маска применяется для любого изображения.

3.2.1.5. Алгоритм Роджена (Rongen)

В этом алгоритме, также, как и в алгоритме Питаса, ЦВЗ представляет собой двумерную матрицу единиц и нулей с примерно равным их количеством. Пикселы, в которые можно внедрять единицы (то есть робастные к искажениям), определяются на основе некоторой характеристической функции (характеристические пиксели). Эта функция вычисляется локально, на основе анализа соседних пикселов. Характеристические пиксели составляют примерно 1/100 от общего числа, так что не все единицы ЦВЗ встраиваются именно в эти позиции. Для повышения количества характеристических пикселов в случае необходимости предлагается осуществлять

небольшое предыскажение изображения. Детектор находит значения характеристических пикселов и сравнивает с имеющимся у него ЦВЗ. Если в изображении ЦВЗ не содержится, то в характеристических пикселях количество единиц и нулей будет примерно поровну

3.2.1.6. Алгоритм PatchWork

В основе алгоритма Patchwork лежит статистический подход. Вначале псевдослучайным образом на основе ключа выбираются два пикселя изображения. Затем значение яркости одного из них увеличивается на некоторое значение (от 1 до 5), значение яркости другого – уменьшается на то же значение. Далее этот процесс повторяется большое число раз (~10000) и находится сумма значений всех разностей. По значению этой суммы судят о наличии или отсутствии ЦВЗ в изображении.

Значения выбираемых на каждом шаге пикселей - a_i и b_i, величина приращения – δ. Сумма разностей значений пикселов

$$S_n = \sum_{i=1}^{n}[(a_i + \delta) - (b_i - \delta)] = 2\delta n + \sum_{i=1}^{n}(a_i - b_i)$$

Матожидание величины $\sum_{i=1}^{n}(a_i - b_i)$ (суммы разности значений пикселов в незаполненном контейнере) близко к нулю при достаточно большом n. Матожидание величины S_n будет больше 2δ. S_n имеет гауссовское распределение. В стегодетекторе в соответствии с ключом проверяется значение и в том случае, если она значительно отличается от нуля, выносится решение о наличии ЦВЗ. Для повышения робастности алгоритма вместо отдельных пикселов можно использовать блоки, или patches (отсюда и название алгоритма). Использование блоков различного размера может рассматриваться как формирование спектра вносимого ЦВЗ шума (шейпинг), аналогично тому, как это применяется в современных модемах.

Алгоритм Patchwork является достаточно стойким к операциям сжатия изображения, его усечения, изменения контрастности. Основным недостатком алгоритма является его неустойчивость к аффинным преобразованиям, то есть поворотам, сдвигу, масштабированию. Другой недостаток заключается в малой пропускной способности. Так, в базовой версии алгоритма для передачи 1 бита скрытого сообщения требуется 20000 пикселов.

3.2.1.7. Алгоритм Бендера (Bender)

Алгоритм Бендера основан на копировании блоков из случайно выбранной текстурной области в другую, имеющую сходные статистические характеристики. Это приводит к появлению в изображении полностью одинаковых блоков. Эти блоки могут быть обнаружены следующим образом:

1) Анализ функции автокорреляции стегоизображения и нахождение ее пиков.
2) Сдвиг изображения в соответствии с этими пиками и вычитание изображения из его сдвинутой копии.
3) Разница в местоположениях копированных блоков должна быть близка к нулю. Выбирается некоторый порог и значения, меньшие этого порога по абсолютной величине, считаются искомыми блоками.

Так как копии блоков идентичны, то они изменяются одинаково при преобразованиях всего изображения. Если сделать размер блоков достаточно большим, то алгоритм будет устойчивым по отношению к большинству из негеометрических искажений. Алгоритм является робастным к фильтрации, сжатию, поворотам изображения. Основным недостатком алгоритма является исключительная сложность нахождения областей, блоки из которых могут быть заменены без заметного ухудшения качества изображения. Кроме того, в данном алгоритме в качестве контейнера могут использоваться только достаточно текстурные изображения.

3.2.2. Алгоритмы встраивания данных в области преобразования

Реальные изображения вовсе не являются случайным процессом с равномерно распределенными значениями величин. Хорошо известно, и это используется в алгоритмах сжатия, что большая часть энергии изображений сосредоточена в низкочастотной части спектра. Отсюда и потребность в осуществлении декомпозиции изображения на субполосы. Стегосообщение добавляется к субполосам изображения. Низкочастотные субполосы содержат подавляющую часть энергии изображения и, следовательно, носят шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ фильтрация. Таким образом, для вложения сообщения наиболее подходящими кандидатами являются среднечастотные субполосы спектра изображения. Типичное распределение шума изображения и обработки по спектру частоты показано на рис.8.

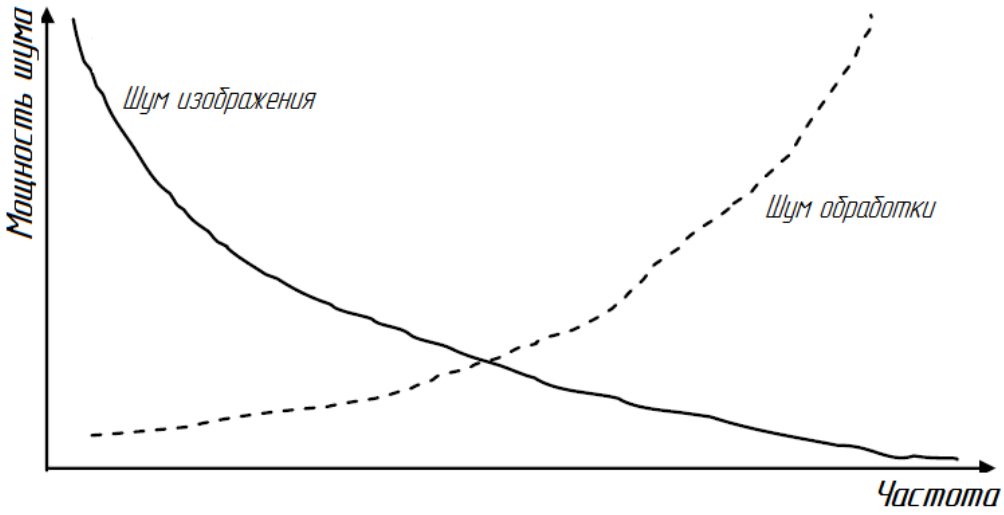

Рис.8. Зависимость шума изображения и шума обработки от частоты

Шум обработки появляется в результате квантования коэффициентов трансформанты. Его можно рассматривать как уменьшение корреляции между коэффициентами трансформанты исходного изображения и квантованными коэффициентами. Например, при высоких степенях сжатия может возникнуть ситуация, когда будут отброшены целые субполосы. То есть дисперсия шума в этих субполосах, вообще говоря, бесконечна. Налицо уменьшение корреляции между коэффициентами субполосы до квантования и после. Для получения приемлемых результатов необходимо усреднить значение шума обработки по многим изображениям.

Преобразования можно упорядочить по достигаемым выигрышам от кодирования: единичное, Адамара, Хаара, ДКП, Вейвлет, Карунена-Лоэва (ПКЛ). Под выигрышем от кодирования понимается степень перераспределения дисперсий коэффициентов преобразования.

Наибольший выигрыш дает преобразование Карунена-Лоэва (ПКЛ), наименьший – разложение по базису единичного импульса (то есть отсутствие преобразования). Преобразования, имеющие высокие значения выигрыша от кодирования, такие как ДКП, вейвлет-преобразование, характеризуются резко неравномерным распределением дисперсий коэффициентов субполос. Высокочастотные субполосы не подходят для вложения из-за большого шума обработки, а низкочастотные – из-за высокого шума изображения. Поэтому приходится ограничиваться среднечастотными полосами, в которых шум изображения примерно равен шуму обработки. Так как таких полос немного, то пропускная способность стегоканала невелика. В случае применения

преобразования с более низким выигрышем от кодирования, например, Адамара или Фурье, имеется больше блоков, в которых шум изображения примерно равен шуму обработки. Следовательно, и пропускная способность выше. Следовательно, для повышения пропускной способности стеганографического канала лучше применять преобразования с меньшими выигрышами от кодирования, плохо подходящие для сжатия сигналов.

Эффективность применения вейвлет-преобразования и ДКП для сжатия изображений объясняется тем, что они хорошо моделируют процесс обработки изображения в СЧЗ, отделяют «значимые» детали от «незначимых». Значит, их более целесообразно применять в случае активного нарушителя, так как модификация значимых коэффициентов может привести к неприемлемому искажению изображения. При применении преобразования с низкими значениями выигрыша от кодирования существует опасность нарушения вложения, так как коэффициенты преобразования менее чувствительны к модификациям.

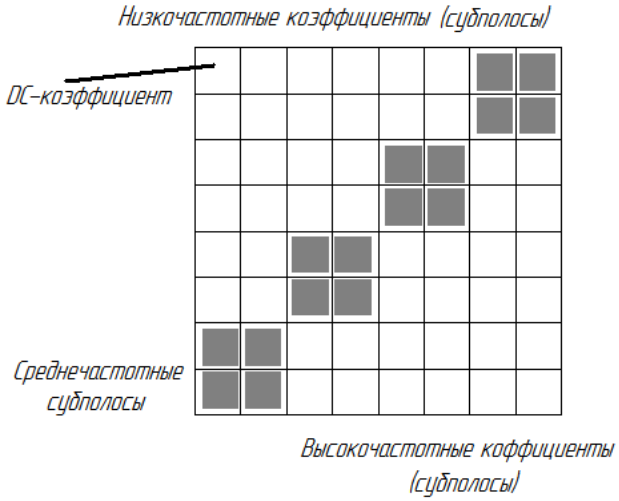

Рис.9. Блок 8x8 пикселей с расположением коэффициентов ДКП

3.2.2.1. Встраивание данных в коэффициенты дискретного косинусного преобразования

При использовании данного метода, контейнер разбивается на блоки размером 8x8 пикселов. ДКП применяется к каждому блоку, в результате чего получаются матрицы коэффициентов ДКП, также размером 8x8. Коэффициенты обозначаются через $c_b(j,k)$, где b – номер блока, (j,k) - позиция коэффициента внутри блока. Если блок сканируется в зигзагообразном порядке (как это имеет место в JPEG), то коэффициенты обозначаются

через $c_{b,j}$. Коэффициент в левом верхнем углу $c_b(0,0)$ обычно называется DC-коэффициентом. Он содержит информацию о яркости всего блока. Остальные коэффициенты называются AC-коэффициентами. Иногда выполняется ДКП всего изображения, а не отдельных блоков. Далее рассмотрим некоторые из алгоритмов внедрения ЦВЗ в области ДКП.

3.2.2.2 Алгоритм Коча (Koch)

В данном алгоритме в блок размером 8x8 осуществляется встраивание 1 бита ЦВЗ. Описано две реализации алгоритма: псевдослучайно могут выбираться два или три коэффициента ДКП. Рассмотрим вариацию алгоритма с двумя выбираемыми коэффициентами.

Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины:

$$\left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| > \varepsilon, \quad если \quad s_i = 0,$$

$$\left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| < -\varepsilon, \quad если \quad s_i = 1.$$

3.2.2.3 Алгоритм Бенхама (Benham)

Этот алгоритм является улучшенной версией предыдущего. Улучшения проведены по двум направлениям: для встраивания используются не все блоки, а лишь «пригодные» для этого, внутри блока для встраивания выбираются не два, а три коэффициента, что уменьшает искажения. Пригодными для встраивания информации считаются блоки изображения, не являющиеся слишком гладкими, а также не содержащие малого числа контуров. Для первого типа блоков характерно равенство нулю высокочастотных коэффициентов, для второго типа – очень большие значения нескольких низкочастотных коэффициентов. Эти особенности и являются критерием отсечения непригодных блоков.

При встраивании бита ЦВЗ псевдослучайно выбираются три коэффициента ДКП блока. Если нужно вложить 1, коэффициенты изменяются так (если требуется), чтобы третий коэффициент стал меньше каждого из первых двух; если нужно встроить 0 он делается больше других. В том случае, если такая модификация приведет к слишком большой деградации изображения, коэффициенты не изменяют, и этот блок просто не используется. Изменение трех коэффициентов вместо двух, а тем более отказ от

изменений в случае неприемлемых искажений уменьшает вносимые ЦВЗ погрешности. Декодер всегда сможет определить блоки, в которые ЦВЗ не встроен, повторив анализ, выполненный в кодере.

3.2.2.4Алгоритм Подилчука (Podilchuk)

При обнаружении ЦВЗ этот алгоритм требует наличия у детектора исходного изображения. Встраиваемые данные моделируются вещественным случайным процессом с нормальным распределением, единичной дисперсией и нулевым средним. Для каждого коэффициента ДКП определяется значение порога, изменение сверх которого может привести к деградации изображения. Этот порог зависит от позиции коэффициента в матрице (то есть частотного диапазона, за который он отвечает). Кроме того, порог обуславливается и свойствами самого изображения: контрастностью и яркостью блока.

Встраивание осуществляется следующим образом: если абсолютное значение коэффициента меньше порога, то он не изменяется. В противном случае к нему прибавляется произведение значения порога и значения ЦВЗ. При обнаружении ЦВЗ вначале коэффициенты исходного изображения вычитаются из соответствующих коэффициентов модифицированного изображения. Затем вычисляется коэффициент корреляции, и устанавливается факт наличия ЦВЗ.

3.2.2.5 Алгоритм Хсю (Hsu)

В данном алгоритме декодеру ЦВЗ также требуется исходное изображение. Однако, декодер определяет не факт наличия ЦВЗ, а выделяет встроенные данные. В качестве ЦВЗ выступает черно-белое изображение размером вдвое меньше контейнера. Перед встраиванием это изображение подвергается случайным перестановкам. ЦВЗ встраивается в среднечастотные коэффициенты ДКП (четвертая часть от общего количества). Эти коэффициенты расположены вдоль второй диагонали матрицы ДКП.

Для внедрения бита ЦВЗ s_i в коэффициент $c_b(j,k)$, находится знак разности коэффициента текущего блока и соответствующего ему коэффициента из предыдущего блока $d_1(i) = sign(c_b(j,k) - c_{b-1}(j,k))$. Если надо встроить 1, коэффициент $c_b(j,k)$ меняют так, чтобы знак разности стал положительным, если 0 – то чтобы знак стал отрицательным.

Имеется и ряд улучшений основного алгоритма. Во-первых, вместо значений коэффициентов можно использовать их абсолютные значения. Во-вторых, вместо

коэффициента из предыдущего блока можно использовать DC-коэффициент текущего блока. Также берется в учет процесс квантования коэффициентов:

$$d_2(i) = sign\left(\left\lfloor \frac{|c_b(j,k)|}{Q(j,k)} \right\rfloor \cdot Q(j,k) - \left\lfloor \frac{|c_b(0,0)|}{Q(0,0)} \right\rfloor \cdot Q(0,0) \right).$$

Еще одним усовершенствованием этого алгоритма является порядок сортировки, при котором блоки ЦВЗ упорядочиваются по убыванию в них числа единиц. Блоки исходного изображения-контейнера также упорядочиваются по убыванию дисперсий. После этого выполняется соответствующее вложение данных. Данный алгоритм не является робастным по отношению к JPEG-компрессии.

3.2.2.6 Алгоритм Кокса (Cox)

Этот алгоритм является робастным ко многим операциям обработки сигнала. Обнаружение встроенного ЦВЗ в нем выполняется с использованием исходного изображения. Внедряемые данные представляют собой последовательность вещественных чисел с нулевым средним и единичной дисперсией. Для вложения информации используются несколько АС-коэффициентов ДКП всего изображения с наибольшей энергией. Автором предложено три способа встраивания ЦВЗ в соответствии со следующими выражениями:

$$c'_i = c_i + \alpha s_i; \quad c'_i = c_i(1+\alpha s_i); \quad c'_i = c_i e^{\alpha s_i}.$$

Первый вариант может использоваться в случае, когда энергия ЦВЗ сравнима с энергией модифицируемого коэффициента. В противном случае либо ЦВЗ будет неробастным, либо искажения слишком большими. Поэтому так встраивать информацию можно лишь при незначительном диапазоне изменения значений энергии коэффициентов.

При обнаружении ЦВЗ выполняются обратные операции: вычисляются ДКП исходного и модифицированного изображений, находятся разности между соответствующими коэффициентами наибольшей величины.

3.2.2.7 Алгоритм Барни (Barni)

Этот алгоритм является улучшением алгоритма Кокса, и в нем также выполняется ДКП всего изображения. В нем детектору уже не требуется исходного изображения, то есть схема слепая. Для встраивания ЦВЗ используются не наибольшие АС-коэффициенты, а средние по величине. В качестве ЦВЗ выступает произвольная строка бит.

Выбранные коэффициенты модифицируются следующим образом: $c'_i = c_i + \alpha s_i |c_i|$. Далее выполняется обратное ДКП, и производится дополнительный шаг обработки: исходное и модифицированное изображения складываются с весовыми коэффициентами:

$$l''(x,y) = \beta(x,y) l'(x,y) + (1-\beta) l(x,y) .$$

Здесь $\beta \approx 1$ для текстурированных областей (в которых человеческий глаз малочувствителен к добавленному шуму) и $\beta \approx 0$ в однородных областях. Значение β находится не для каждого пикселя в отдельности, а для неперекрывающихся блоков фиксированного размера. Например, в качестве β целесообразно использовать нормализованную дисперсию блоков. В детекторе ЦВЗ вычисляется корреляция между модифицированным изображением и ЦВЗ, $\sum_{i=1}^{n} c_i'' s_i''$.

3.3 Аддитивные алгоритмы

Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером, либо «вплавляется» (fusion) в него.

3.3.1 Алгоритмы на основе линейного встраивания данных

В аддитивных методах внедрения ЦВЗ представляет собой последовательность чисел w_i длины N, которая внедряется в выбранное подмножество отсчетов исходного изображения f. Основное и наиболее часто используемое выражение для встраивания информации в этом случае:

$$f'(m,n) = f(m,n)(1+\alpha w_i) ,$$

где α – весовой коэффициент, а f' – модифицированный пиксель изображения. Другой способ встраивания водяного знака был предложен И.Коксом:

$$f'(m,n) = f(m,n) + \alpha w_i$$

или, при использовании логарифмов коэффициентов

$$f'(m,n) = f(m,n) e^{\alpha w_i} .$$

При встраивании в соответствии с первой формулой, ЦВЗ в декодере находится следующим образом:

$$w_i^* = \frac{f^*(m,n) - f(m,n)}{\alpha f(m,n)}.$$

Здесь под f^* понимаются отсчеты полученного изображения, содержащего или не содержащего ЦВЗ w. После извлечения w_i^* сравнивается с подлинным ЦВЗ. Причем в качестве меры идентичности водяных знаков используется значение коэффициента корреляции последовательностей: $\delta = \frac{w^* \cdot w}{\|w^*\| \cdot \|w\|}$.

Эта величина варьируется в интервале [-1; 1]. Значения, близкие к единице, свидетельствуют о том, что извлеченная последовательность с большой вероятностью может соответствовать встроенному ЦВЗ. Следовательно, в этом случае делается заключение, что анализируемое изображение содержит водяной знак.

В декодере может быть установлен некоторый порог, $\tau = \frac{\alpha}{SN} \sum |f'|$ (здесь S – стандартное среднее квадратическое отклонение), который определяет вероятности ошибок первого и второго рода при обнаружении ЦВЗ. При этом коэффициент α может не быть постоянным, а адаптивно изменяться в соответствии с локальными свойствами исходного изображения. Это позволяет сделать водяной знак более робастным (стойким к удалению).

Для увеличения робастности внедрения во многих алгоритмах применяются широкополосные сигналы. При этом информационные биты могут быть многократно повторены, закодированы с применением корректирующего кода, либо к ним может быть применено какое-либо другое преобразование, после чего они модулируются с помощью псевдослучайной гауссовской последовательности. Такая последовательность является хорошей моделью шума, присутствующего в реальных изображений. В то же время синтетические изображения (созданные на компьютере) не содержат шумов, и в них труднее незаметно встроить такую последовательность.

Для извлечения внедренной информации в аддитивной схеме встраивания ЦВЗ обычно необходимо иметь исходное изображение, что достаточно сильно ограничивает область применения подобных методов.

Также существуют слепые методы извлечения ЦВЗ, вычисляющие корреляцию последовательности w со всеми N коэффициентами полученного изображения f^*: $\delta = \frac{\sum_N f^*(m,n) w_i}{N}$.

Затем полученное значение коэффициента корреляции δ сравнивается с некоторым порогом обнаружения $\tau = \frac{\alpha}{3N} \sum_N \left| f^*(m,n) \right|$.

Основным недостатком этого метода является то, что само изображение в этом случае рассматривается, как шумовой сигнал. Существует гибридный подход (полуслепые схемы), когда часть информации об исходном изображении доступно в ходе извлечения информации, но неизвестно собственно исходное изображение.

Корреляционный метод позволяет только обнаружить наличие или отсутствие ЦВЗ. Для получения же всех информационных битов нужно протестировать все возможные последовательности, что является крайне вычислительно сложной задачей.

3.3.2. Алгоритмы на основе слияния ЦВЗ и контейнера

Если вместо последовательности псевдослучайных чисел в изображение встраивается другое изображение (например, логотип фирмы), то соответствующие алгоритмы внедрения называются алгоритмами слияния. Размер внедряемого сообщения намного меньше размера исходного изображения. Перед встраиванием оно может быть зашифровано или преобразовано каким-нибудь иным образом.

У таких алгоритмов есть два преимущества. Во-первых, можно допустить некоторое искажение скрытого сообщения, так как человек все равно сможет распознать его. Во-вторых, наличие внедренного логотипа является более убедительным доказательством прав собственности, чем наличие некоторого псевдослучайного числа.

3.3.2.1. Алгоритм Чайа (Chae)

В алгоритме внедряется черно-белое изображение (логотип), размером до 25 % от размеров исходного изображения. Перед встраиванием выполняется одноуровневая декомпозиция как исходного изображения, так и эмблемы с применением фильтров Хаара. Вейвлет-коэффициенты исходного изображения обозначаются, как $f(m,n)$, а вейвлет-коэффициенты логотипа - $w(m,n)$. Модификации подвергаются все коэффициенты преобразования.

Вначале коэффициенты каждого поддиапазона, как исходного изображения, так и логотипа представляются 24 битами (из которых один бит отводится на знак). Так как размер логотипа в 4 раза меньше исходного изображения, то необходимо увеличить количество его коэффициентов. Для этого выполняются следующие действия.

Обозначим, через A, B, и C соответственно, старший, средний и младший байты 24-битного представления логотипа. Старший байт каждого из этих чисел представляет собой соответственно A, B, или C, два других байта заполняются нулями. Затем формируется расширенный вчетверо блок коэффициентов логотипа. После чего он поэлементно складывается с 24-битной версией исходного изображения

$$f'(m,n) = \alpha f(m,n) + w(m,n).$$

Полученное значение отображается назад к исходной шкале на основе значений минимального и максимального коэффициента поддиапазона. После чего осуществляется обратное дискретное ВП. Для извлечения ЦВЗ используется инверсная формула,

$$w_i^* = \frac{f^*(m,n) - f(m,n)}{\alpha f(m,n)}$$

Данный алгоритм позволяет скрыть довольно большой объем данных в исходном изображении: до четверти от размеров исходного изображения.

3.3.2.2 Алгоритм Кандара (Kundur)

Также, как и в алгоритме Чайа, исходное и внедряемое изображения подвергаются вейвлет-преобразованию. Для встраивания используются все коэффициенты детальных поддиапазонов.

Множество этих коэффициентов разбивается на неперекрывающиеся блоки размером $N_W \cdot M_W$. Блоки обозначаются $f_{k,l}^i$, где $i = 1...2^{2(M-l)}$, а k и l, соответственно местоположение коэффициента и уровень разрешения. Водяной знак прибавляется к элементам исходного изображения по формуле:

$$f_{k,l}^i(m,n) = f_{k,l}^i(m,n) + \alpha\sqrt{S(f_{k,l}^i(m,n))}w_{k,l}^i(m,n),$$

где S – коэффициент масштаба, вычисляемый по формуле:

$$S\left(f_{k,l}^i(m,n)\right) = \sum_{u,v} C(u,v)\left|T\left(f_{k,l}^i(m,n)\right)\right|^2,$$

где C(u,v) – взвешивающая матрица, определяющая частотную чувствительность системы зрения человека, T – оператор ДПФ.

Таким образом, алгоритм использует довольно сложную модель человеческого зрения. Для обнаружения в детекторе может быть использовано как вычисление корреляционной функции, так и визуальное сравнение.

3.3.4 Алгоритмы на основе квантования

Под квантованием понимается процесс сопоставления большого (возможно и бесконечного) множества значений с некоторым конечным множеством чисел. Понятно, что при этом происходит уменьшение объема информации за счет ее искажения. Квантование находит применение в алгоритмах сжатия с потерями. Различают скалярное и векторное квантование. При векторном квантовании, в отличии от скалярного, происходит отображение не отдельно взятого отсчета, а их совокупности (вектора). Из теории информации известно, что векторное квантование эффективнее скалярного по степени сжатия, обладая большей сложностью. В стеганографии находят применение оба вида квантования.

В кодере квантователя вся область значений исходного множества делится на интервалы, и в каждом интервале выбирается число его представляющее. Это число есть кодовое слово квантователя и обычно бывает центроидом интервала квантования. Множество кодовых слов называется книгой квантователя. Все значения, попавшие в данный интервал, заменяются в кодере на соответствующее кодовое слово. В декодере принятому числу сопоставляется некоторое значение. Интервал квантования обычно называют шагом квантователя. Встраивание информации с применением квантования относится к нелинейным методам.

Передаваемое сообщение имеет ограниченную энергию для выполнения требования его незаметности. Помехами являются исходный сигнал и еще одна гауссовская помеха – шум обработки (квантования). Кодеру исходный сигнал известен, декодер должен извлечь ЦВЗ без знания обеих составляющих помех. Существуют многочисленные улучшения метода Костаса (направленных на борьбу с помехами), заключающиеся в применении различных структурированных квантователей (например, решетчатых или древовидных).

Наиболее предпочтительно внедрение информации в спектральную область изображения. Если при этом используются линейные методы, то встраивание ЦВЗ

производят в средние полосы частот. Это объясняется тем, что энергия изображения сосредоточена, в основном, в низкочастотной (НЧ) области. Следовательно, в детекторе ЦВЗ в этой области наблюдается сильный шум самого сигнала. В высокочастотных (ВЧ) областях большую величину имеет шум обработки, например, сжатия. В отличие от линейных, нелинейные схемы встраивания информации могут использовать НЧ области, так как мощность внедряемого ЦВЗ не зависит от амплитуды коэффициентов. Это объясняется тем, что в нелинейных алгоритмах скрытия не используется корреляционный детектор, коэффициенты малой и большой амплитуды обрабатываются одинаково.

Раздел 4. Классификация и сопоставительный анализ методов и средств встраивания данных в различные контейнеры.

Вопросы для самостоятельного изучения и обсуждения на семинарах.

1) Принятая терминология.
2) Теоретические положения стеганографии с учетом принятой терминологии.
3) Сопоставительный анализ средств встраивания данных в различные контейнеры.

Литература для изучения темы.

10. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.
11. Kutter M. Watermarking Resisting to Translation, Rotation, and Scaling. Signal Processing Laboratory, 1998. P. 10.
12. Kutter M. Digital Signature of Color Images using Amplitude Modulation. Signal Processing Laboratory, 1997. P. 9.
13. Herrigel A., Pereira S., Petersen H. Secure Copyright Protection Techniques for Digital Images. International Workshop on Information Hiding, 1998. P. 22.
14. Ramkumar M. Data Hiding in Multimedia – Theory and Applications. New Jersey Institute of Technolog, 1999. P. 70.
15. Bender W. Applications for Data Hiding. IBM Systems Journal, 2000. P. 22.
16. Chae J., Manjunath B. A Robust Data Hiding Technique using Multidimensional Lattices. Proc. IEEE Conference on Advances in Digital Libraries, 1998. P. 8.
17. Chae J., Manjunath B. A Technique for Image Data Hiding and Reconstruction without Host Image. Proceedings of the SPIE - The International Society for Optical Engineering. 1999, P.
18. Cuche E., Marquet P., Spatial filtering for zero-order and twin-image elimination in digital off-axis holography. Applied Optics V.39, 2000. P. 4070–4075

4.1 Встраивание ЦВЗ в контейнер-изображение.

Встраивание ЦВЗ возможно благодаря особенностям системы восприятия человека. Хорошо известно, что изображения обладают большой психовизуальной избыточностью. Глаз человека подобен низкочастотному фильтру, поэтому особенно незаметными оказываются искажения в высокочастотной области спектра изображений.

Для преодоления воздействий фотопечати и сканирования наиболее успешными оказались методы, получившие название методов “модуляции” изображения-контейнера, причем модуляция может осуществляться как в частотной, так и в пространственных областях изображения. Для компенсации геометрических искажений типа смещения, поворота и изменения масштаба изображения используется полярная логарифмическая система координат с углом θ и логарифмическим радиусом по осям координат или применяется инвариантное к повороту и масштабу преобразование Меллинга.

В случае внедрения ЦВЗ в частотной области модуляции подвергаются амплитудные составляющие комплексного спектра изображения-контейнера. Для этого предварительно осуществляется вычисление амплитудной и фазовой составляющих компонентов преобразования Фурье. Для оценки последствий геометрических искажений, связанных со случайным поворотом, смещением или изменением масштаба, в изображение-контейнер, кроме ЦВЗ, встраивается изображение-шаблон. В случае внедрения ЦВЗ в пространственной области сигнал ЦВЗ встраивается путем модуляции исходного изображения-контейнера, а извлечение ЦВЗ (демодуляция) выполняется с помощью линейной фильтрации изображения. Если изображение цветное, сигнал ЦВЗ внедряется путем модификации значений пикселов в Blue канале RGB изображения. Модификация осуществляется либо добавлением, либо вычитанием в зависимости от значения внедряемого бита ЦВЗ яркости изображения-контейнера.

4.2 Методы, использующие в качестве контейнеров аудиофайлы.

Для надежного сокрытия данных в акустическом канале система сокрытия должна отвечать следующим требованиям:

- быть стойкой к повсеместно используемым алгоритмам сжатия с потерями

- не вносить в сигнал воспринимаемые человеческим слухом искажения

- не вносить заметных изменений в статистику контейнера

Де-факто стандартным форматом звуковых файлов в текущий момент является формат **MP3**. Следовательно, работа не вызывающих подозрений стегосистемы в акустическом канале должна быть основана именно на данном формате.

MP3 - полное название MPEG 1 Layer 3 - формат кодирования звуковых файлов, входящий в стандарт кодирования видеоинформации MPEG 1. Принципиальной особенностью формата является сжатие с потерями: после упаковки и распаковки звукового файла с помощью MP3 результат не является побитной копией оригинала. Напротив, при кодировании несущественные компоненты целенаправленно исключаются из упаковываемого сигнала. При сохранении приемлемого качества, MP3 позволяет сжать звуковые данные в десять и более раз.

Это достигается учетом особенностей человеческого слуха, в том числе эффекта маскирования слабого сигнала одного диапазона частот более мощным сигналом соседнего диапазона, когда он имеет место, или мощным сигналом предыдущего фрейма, вызывающего временное понижение чувствительности уха к сигналу текущего фрейма (удаляются второстепенные звуки, которые не слышатся человеческим ухом из-за наличия в данный или предыдущий момент другого, более громкого). Учитывается так же неспособность большинства людей различать сигналы, по мощности лежащие ниже определенного уровня, разного для разных частотных диапазонов.

Данный процесс называется адаптивным кодированием и позволяет экономить на наименее значимых с точки зрения восприятия человеком деталях звучания. Степень сжатия (следовательно и качество), определяется задаваемой при кодировании шириной потока данных - **битрейтом.**

Как и в рассмотренном случае внедрения информации в изображения, алгоритмы внедрения в аудиофайлы размещают скрываемые данные либо в несжатом сигнале до его сжатия, либо непосредственно в сжатый сигнал - как правило, в энтропийно сжатые коэффициенты преобразования. Некоторые методы так же используют для сокрытия не аудиосигнал как таковой, а различные особенности и служебную информацию самих файлов-контейнеров.

Рассмотрим сначала алгоритмы сокрытия данных в несжатом звуковом потоке.

Широкополосное кодирование. В сигнал добавляется модулированный сообщением шум с амплитудой чуть выше предела маскирования. Преимуществом данной схемы

является эффективность работы и высокая пропускная способность, недостатком - вносимые в сигнал слышимые искажения.

При сокрытии одного бита в последовательности коэффициентов выходная последовательность вычисляется следующим образом:

$x_i' = \begin{cases} x_i + \omega_i \mid x_i \mid \alpha_i & s_i = 1 \\ x_i - \omega_i \mid x_i \mid \alpha_i & s_i = 0 \end{cases}$ где $\omega_i \in -1, +1$ - случайная двоичная последовательность, α_i - порог слышимости i - той подполосы, s_i - скрываемый бит.

Для вычисления порога слышимости может быть использована психоакустическая модель, содержащаяся в формате кодирования MP3, или любая другая. Таким образом, метод позволяет управлять психоакустическим характером вносимых в сигнал искажений.

Для извлечения скрытого бита из последовательности коэффициентов используется функция корреляции принятых коэффициентов и исходной случайной последовательности.Следует отметить, что из-за ненадежности извлечения данный метод требует использования кодов коррекции ошибок. Это приводит к уменьшению как быстродействия, так и пропускной способности метода.

Фазовое кодирование. В данном методе используется тот факт, что человеческое ухо воспринимает не значения фазы, а только их разность.

Сигнал разбивается на участки, значения фазы на первом участке используются для кодирования скрываемого сообщения, значения фаз остальных участков таким образом, чтобы разность фаз между участками осталась неизменной.

Для кодирования значений фаз, на множестве фаз выделяется набор равномерно распределенных значений, соответствующих битам 0 и 1. Значение фазы заменяется ближайшим значением, соответствующим требуемому биту. Разность значений в наборе зависит от частоты полосы, и варьируется от $\frac{\pi}{12}$ на чувствительных полосах до $\frac{\pi}{4}$ на высокочастотных полосах.

Для кодирования одного бита скрываемого сообщения используется определенная последовательность изменений фаз, различная для кодирования 0 и для кодирования 1. Для извлечения скрытого сообщения используется следующая функция обнаружения:

$q = \sum r_i (v_i - \phi_i)^2 - r(u_i - \phi_i)^2$, где r_i, ϕ_i - амплитуда и фаза i - го полученного сигнала.

$u = \{\alpha_0, \beta_1, \alpha_2, \beta_2\}$ - ожидаемая последовательность фаз при кодировании бита 1.

$v = \{\beta_0, \alpha_1, \beta_2, \alpha_3\}$ - ожидаемая последовательность фаз при кодировании бита 0.

α_i и β_i - ближайшие к ϕ_i значения фаз, соответствующие 1 и 0.

Если $q > 0$, бит скрытого сообщения принимается равным 1, иначе равным 0.

Метод обеспечивает высокую эффективность кодирования по критерию отношения сигнал-шум, однако его пропускная способность невелика, и составляет от 8 до 32 бит в секунду.

Эхо-кодирование использует неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия. Эхо характеризуется тремя параметрами: начальной амплитудой, степенью затухания, задержкой. При достижении некоего порога между сигналом и эхом они смешиваются. В этой точке человек не может отличить эти два сигнала. Наличие этой точки сложно определить, так как она зависит от качества исходной записи и слушателя. Как правило, используется задержка около одной тысячной секунды, что вполне приемлемо для большинства записей и слушателей. Используются две различные задержки при кодирования нуля и единицы. Обе эти задержки должны быть меньше, чем порог чувствительности уха слушателя к получаемому эху.

Замена шума. В данном методе используется тот факт, что человеческое ухо воспринимает не столько форму, сколько энергию шума. Так как в формате MP3 полностью кодируется форма шумных частотных подполос, данные подполосы могут быть использованы для сокрытия данных. Входной сигнал преобразуется в частотную область с помощью используемого в MP3 **модифицированного дискретного косинусного преобразования**(**МДКП**).

При сокрытии одного бита в последовательности коэффициентов, выходная последовательность вычисляется следующим образом:

$x_i' = \begin{cases} p_i / x_i / & \text{при кодировании 1} \\ -p_i / x_i / & \text{при кодировании 0} \end{cases}$, где p - случайная двоичная последовательность, $p_i \in -1, +1$.

При извлечении скрытого бита, как и в случае широкополосного кодирования, используется функция корреляции принятых коэффициентов и исходной случайной последовательности.

В качестве шумных предлагается использовать полосы с частотами выше 5 кГц.

Следует отметить, что метод устойчив по отношению к MP3 сжатию, так как алгоритм кодирования MP3 не меняет знаки коэффициентов МДКП. Пропускная способность метода составляет от 20 до 60 бит в секунду. Метод так же достаточно прост в реализации, так как базируется на широко реализованном на различных платформах алгоритме МДКП, входящем в состав MP3 кодировщика.

В целом методы сокрытия данных в несжатом звуковом потоке имеют ряд серьезных недостатков:

- возможную заметность при прослушивании;

- ограниченную пропускную способность;

- сложность реализации.

Вносимые в сигнал неестественные искажения в сигнал, такие как белый шум определенной амплитуды, дискретные фазы сигнала и т.д., могут быть с высокой вероятностью обнаружены специфическими методами обнаружения.

Таким образом, более перспективными являются алгоритмы, скрывающие данные **непосредственно в сжатом MP3 потоке.**

В текущее время предлагается ряд алгоритмов, использующих для сокрытия данных служебную информацию MP3, наиболее известным из них является алгоритм **mp3stego.** Данный алгоритм модифицирует процесс MP3 кодирования с тем, чтобы младший бит служебного поля кадра MP3, например, объем основной информации внутри кадра, совпадал с текущим битом скрываемого сообщения.

Особенностями метода являются: практическая незаметность при прослушивании; высокая сложность реализации и медленная работа, так как необходимо выполнить весь процесс MP3 кодирования; пропускная способность порядка 50 бит в секунду.

Следует отметить, что вносимые в служебную информацию изменения приводят к расхождению результата работы таких методов с результатом работы стандартного кодировщика MP3. Такие изменения могут быть с высокой вероятностью обнаружены противником.

В качестве более быстродействующей альтернативы был предложен метод сокрытия данных с использованием особенности формата MP3 - межкадровых промежутков.

Поток данных MP3 состоит из кадров - участков данных, кодирующих 26мс звукового сигнала. Каждый кадр содержит 4х-байтный заголовок, содержащий синхронизирующее слово и служебную информацию. Служебная информация содержит, в частности, версию формата, стерео режим и битрейт. Эти значения однозначно определяют размер кадра.

Количество байт, необходимых для сжатия звука с заданным качеством, зависит от характеристик конкретного звукового сигнала. Таким образом, на сложные для сжатия участки сигнала с большим количеством деталей требуется больше байт чем на простые. Исходя из этого, MP3 предусматривает возможность хранения упакованных данных кадра в оставшихся незанятыми байтах предыдущего кадра. Чтобы правильно позиционироваться, в заголовке кадра указывается смещение на начало данных. Признака конца данных как такового нет, декодирование останавливается при завершении распаковки требуемого числа коэффициентов косинусного преобразования.

Любая информация между концом данных одного кадра и началом данных следующего кадра игнорируется декодером, соответственно, именно там можно разместить скрываемые данные. Для этого увеличивается размер кадра путем увеличения его битрейта на одну ступень, например, с 128кбит/с до 160кбит/с.

Данный метод не вносит искажений в звуковой сигнал-контейнер, прост, быстр обладает значительной пропускной способностью(порядка 20% от объема контейнера). Однако зная алгоритм сокрытия, легко обнаружить наличие скрытой информации, исходя из того что в стандартном MP3 потоке нет "лишних" байт. Таким образом, метод можно использовать только в том случае, когда необходима быстрая передача значительного объема информации и не ожидается серьезного противодействия противника.

Наиболее устойчивым к обнаружению является метод сокрытия в ошибках квантования MP3 коэффициентов. MP3 кодирование построено по классической схеме сжатия с потерями, состоящей из трех шагов:

- преобразования сигнала, с тем чтобы большая часть информации о сигнале была сосредоточена в небольшом количестве коэффициентов. В MP3 использовано модифицированное дискретное косинусное преобразование.

- квантования, то есть деления полученных коэффициентов на определенные значения с последующим округлением результата до целого числа. Именно на этом этапе происходит потеря информации. Значения делителей при квантовании в MP3 вычисляются исходя из заданного битрейта и психоакустической модели, определяющей максимально допустимый уровень шума.

- энтропийного сжатия без потерь. В MP3 используется сжатие с помощью статических кодов Хаффмана.

Полученные на этапе квантования целочисленные коэффициенты могут быть непосредственно использованы для сокрытия данных, например посредством встраивания в наименьший значащий бит. Это, однако, вносит значительный шум в выходной сигнал и с высокой вероятностью может быть обнаружено. Можно использовать для сокрытия лишь часть коэффициентов, выбирая их так чтобы минимизировать вносимые искажения. Так как модифицированный коэффициент отличается от исходного не более чем на 1, минимизация суммарных отклонений от исходного сигнала сводится к отбору коэффициентов с дробной частью близкой к 0,5. Кроме того, для сохранения структуры потока сжатых данных, отбираются коэффициенты, модификация которых не изменяет размера кодирующего их слова, в частности, отбрасываются коэффициенты с нулевым значением. Возникает проблема декодирования данных на стороне получателя - декодер не обладает информацией о том, какие коэффициенты использованы для сокрытия, т.е. сообщение должно быть представлено как известная декодеру функция от вектора бит всех коэффициентов, как использованных, так и нет. Используя в качестве данной функции умножение на общую для отправителя и получателя задаваемую секретным ключем матрицу, получаем систему линейных алгебраических уравнений, которую отправитель решает относительно вектора бит коэффициентов. Не подлежащие модификации коэффициенты задают значения некоторых переменных. Максимально возможный размер передаваемого сообщения, при котором система имеет решение,

стремится к числу модифицируемых коэффициентов при увеличении данного числа, таким образом, метод позволяет без потерь в емкости использовать для сокрытия произвольные элементы контейнера.

Структура энтропийного кодирования в MP3 накладывает дополнительные ограничения на допустимые для модификации коэффициенты. Коэффициенты в рамках одного блока разбиты на 3 группы, каждая из которых упакована с помощью отдельной Хаффман-таблицы. Первые 2 группы упакованы парами следующим образом: в потоке записан код из таблицы, соответствующий паре, после чего записаны знаковые биты каждого отсчета. Числа, больше максимального для таблицы, кодируются как максимально возможный отсчет, плюс определяемое таблицей количество бит, записанных после кода, которые содержат прибавляемое к значению число.

Последний блок коэффициентов закодирован четверками с возможными значениями коэффициентов -1, 0, 1. Длина блоков содержится в служебной информации кадра, что позволяет вычислить количество нулевых значений отсчетов в конце кадра.

Внесение изменений в коэффициенты последнего блока, то есть замена -1 и 0, 0 и 1, приведет к изменению размера сжатого коэффициента(из-за появления или исчезновения знакового бита), что в свою очередь может привести к нарушению структуры MP3 файла - информация окажется больше или меньше отведенного под нее места в кадре.

Из коэффициентов первых двух блоков модификации подлежит не более одного коэффициента в паре, при этом необходимо чтобы размер кода модифицированной пары совпадал с размером исходного кода. Как правило, это условие выполняется для кодов больших чисел. Процент доступных коэффициентов резко падает с уменьшением битрейта, так как большее количество коэффициентов кодируются нулями или близкими к нулю значениями.

Данные ограничения приводят к отсеиванию около 85% подходящих коэффициентов.

Предельно допустимое отклонение дробной части коэффициента от 0,5 задается исходя из размера сообщения, которое надо скрыть в данном контейнере, с тем чтобы количество доступных коэффициентов было максимально близким к размеру сообщения.

Для достижения допустимого уровня быстродействия метода, MP3 поток разбивается на группы кадров одинакового размера. Количество кадров в группах выбирается с тем чтобы количество модифицируемых коэффициентов в них было приблизительно одинаковым. В каждой группе СЛАУ сокрытия решается независимо. Таким образом, несмотря на то что время работы метода Гаусса в каждой группе пропорционально кубу

от числа уравнений, общее время работы растет линейно с увеличением числа используемых коэффициентов. Однако каждая группа должна содержать определенное количество служебных бит, в которых записана длина сообщения в этой группе. Следовательно чем меньше группы, (и быстрее работает метод), тем больше бит расходуется на служебную информацию.

Данный метод при высокой защите от обнаружения предоставляет пропускную способность порядка половины процента от объема контейнера. Он хорошо подходит для ситуаций, когда ожидается противодействие информированного противника.

Раздел 5. Стегоанализ: Основные положения и анализ методов и средств.

УЧЕБНЫЕ ЦЕЛИ РАЗДЕЛА 4.

1) Раскрыть понятие стегоанализа.

2) Определить основную терминологию.

3) Изучить основные теоретические посылки

Тема 5. Стеганоанализ: Принятая терминология, основные теоретические аспекты.

Вопросы для самостоятельного изучения и обсуждения на семинарах.

1) Принятая терминология.
2) Теоретические положения стегоанализа с учетом принятой терминологии.
3) Пример гистограммного стегоанализа.

Литература для изучения темы.

1. Mitchell T. Machine Learning. "— McGraw-Hill, 1997.

2. Farid H., Lyu S. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines // Information Hiding. "— 2002. "— Pp. 340–354.

3. Farid H., Lyu S. Steganalysis using color wavelet statistics and one-class support vector machines // Security, Steganography, and Watermarking of Multimedia Contents. "— 2004. "— Pp. 35–45.

4. Cristianini N., Shawe-Taylor J. An introduction to support vector machines and other kernel-based learning methods. "— Cambridge University Press, 2000. "— March.

5. Schoelkopf B., Sung K., Burges C. et al. Comparing Support Vector Machines with Gaussian Kernels to Radial Basis Function Classifiers: Tech. rep.: Massachusetts Institute of Technology, 1996.

6. Bedi C., Goyal H. Qualitative and Quantitative Evaluation of Image Denoising Techniques // International Journal of Computer Applications. "— 2010. "— October. "— Vol. 8, no. 14. "— Pp. 31–34.

7. Pevný T., Fridrich J. Merging Markov and DCT Features for Multi-Class JPEG Steganalysis // Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX. "— Vol. 6505. "— 2007.

8. Pevný T., Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix // Trans. Info. For. Sec. "— 2010. "— June. "— Vol. 5. "— Pp. 215–224.

5. Стегоанализ

Стегоанализ — раздел стеганографии, посвященный выявлению факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку.

5.1 Общая методика стегоанализа

В качестве первого шага стегоаналитик представляет исследуемое сообщение в виде контейнера, соответствующего известному ему методу стеганографии данного типа сообщений. Для определения контейнера требуется понимание метода занесения скрытой информации и знание места в сообщении, куда могло быть помещено стего. Таким образом, на первом этапе стегоаналитик:

- выбирает метод стеганографии, с помощью которого могла быть занесена скрытая информация в исследуемое сообщение,
- структурирует сообщение в виде соответствующего контейнера и получает представление о возможных способах добавления стего в сообщение выбранным методом.

Место в контейнере (или его объём), куда может быть занесено стего данным методом стеганографии, как правило называют полезной ёмкостью контейнера.

Вторым шагом служит выявление возможных атак исследуемого сообщения — то есть видоизменений контейнера (которым является данное сообщение в рамках выбранного метода

стеганографии) с целью проведения стегоанализа. Как правило, атаки проводятся путём внесения произвольной скрытой информации в контейнер с помощью выбранного для анализа метода стеганографии.

Третьим, и заключительным, шагом является непосредственно стегоанализ: контейнер подвергается атакам, и на основе исследования полученных «атакованных» сообщений, а также исходного сообщения, делается вывод о наличии или отсутствии стего в исследуемом сообщении. Совокупность производимых атак и методов исследования полученных сообщений представляет собой метод стегоанализа. Атака(и), с помощью которой(ых) удалось выявить наличие скрытой информации, называют успешной атакой.

Как правило, стегоанализ даёт вероятностные результаты (то есть возможность наличия стего в сообщении), и реже — точный ответ. В последнем случае, как правило, удаётся восстановить исходное стего.

5.2 Пример стегоанализа с использованием гистограмм

В случае стеганографического встраивания т.е. замены НЗБ на случайную последовательность, количество пикселей в парах выравняется. Гистограмма станет ступеньками (по два соседних значения яркости). На рисунке синим цветом обозначена гистограмма изображения без встраивания, а красным - гистограмма того же изображения после встраивания заархивированных данных вместо последнего слоя. Сравнение двух гистограмм и дает возможность стегоанализа последовательно скрываемых бит.

Стегоанализ - это противодействие стеганографии, как криптоанализ - это противодействие криптографии. Основная цель стеганографии - скрыть факт передачи данных. Следовательно, основная цель стегоанализа - обнаружить факт сокрытия передачи данных. Рассмотрим метод обнаружения последовательного встраивания в LSB на примере изображения формата BMP. Бытует мнение, что Указатели в LSB изображений являются случайными. На самом деле это не так. Хотя человеческий глаз и не заметит изменений изображения при изменении последнего бита, статистические параметры изображения будут изменены. Перед сокрытием данные обычно архивируются (для уменьшения объема) или шифруются (для обеспечения дополнительной стойкости сообщения при попадании в чужие руки). Это делает биты данных очень близкими к случайным.Последовательное встраивание такой информации заменит LSB изображения случайными битами. Это можно обнаружить. Для примера возьмем одну цветовую компоненту полноцветного изображения BMP и на ней

покажем процесс отыскания встраивания. Яркость цветовой компоненты может принимать значения от 0 до 255. В двоичной системе исчисления - от 0000 до1111. Рассмотрим пары:

0000 0000<->0000 0001;

0000 0010<->0000 0011;

...

1111 1100<->1111 1101;

1111 1110<->1111 1111.

Данные числа различаются между собою только в LSB. Таких пар для цветовой компоненты BMP изображения: 256/2=128

В случае стеганографического встраивания т.е. замены LSB на случайную последовательность, количество пикселей в парах выравняется. Гистограмма станет ступеньками (по два соседних значения яркости рис. 10)

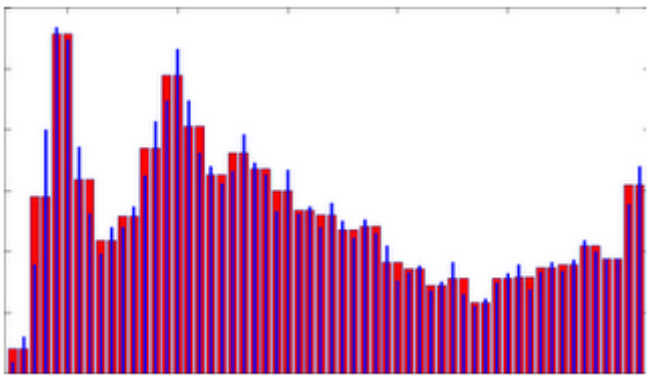

Рис.10. Гистограмма контейнера со встроенным сообщением.

На рисунке 10 синим цветом обозначена гистограмма изображения без встраивания, а красным - гистограмма того же изображения после встраивания заархивированных данных вместо последнего слоя. Сравнение двух гистограмм и дает возможность стегоанализа последовательно скрываемых бит.

5.3 Необнаружимость скрываемых данных

Быстродействие и пропускная способность являются общепринятыми критериями оценки каналов передачи сообщений и не учитывают специфики методов сокрытия данных, хотя и легко поддаются измерению. Методики измерения необнаружимости не являются

общепринятыми. В данной работе предлагается универсальная и объективная методика, основанная на синтезе оптимального алгоритма обнаружения.

Задачей сокрытия данных, по определению, является создание методов, аппаратуры и программного обеспечения, совокупность которых обеспечивала бы минимальную вероятность обнаружения скрытых данных. Данную вероятность можно оценить с помощью прогноза теоретически возможных действий противника при анализе перехваченного сообщения.

Вероятные действия противника рассматривались, исходя из следующих постулатов:

• любые скрытые данные могут быть обнаружены и идентифицированы;

• задача обнаружения формируется относительно контейнера, вызывающего подозрение о присутствии скрытых данных;

• контейнер, в отношении которого решается задача обнаружения, представляет собой реализацию случайного процесса Y, поскольку случай возникновения подозрения не-предсказуем;

• вероятность присутствия скрытых данных в реализации Y равна $P(\alpha/Y)$, где α - скрытые данные;

• вероятность отсутствия скрытых данных в реализации Y равна

$P(0/Y)$.

Перечисленные вероятности являются условными и апостериорными. Они соответствуют условию возникновения скрытых данных в анализируемом сообщении.

По теореме о вероятности совместного появления (произведения) двух событий A и B

$$P(A,B) = P(A) \cdot P(B/A) = P(B) \cdot P(A/B)$$

Таким образом,

$$P(Y,\alpha) = P(Y) \cdot P(\alpha/Y) = P(\alpha) \cdot P(Y/\alpha)$$

Следовательно искомая апостериорная вероятность наличия скрытых данных в реализации Y:

$$P(\alpha/Y) = \frac{P(\alpha)\cdot P(Y/\alpha)}{P(Y)}$$

Аналогично апостериорная вероятность отсутствия скрытых данных:

$$P(0/Y) = \frac{P(0)\cdot P(Y/0)}{P(Y)}$$

По формуле полной вероятности имеем:

$P(Y) = P(\alpha)\cdot P(Y/\alpha) + P(0)\cdot P(Y/0)$, где

$P(\alpha)$ и $P(0)$ определяют априорные вероятности наличия и отсутствия скрытых данных в анализируемого сообщении.

В задаче обнаружения скрытых данных оба из перечисленных выше случаев содержат полную группу событий, поэтому

$$P(\alpha) + P(0) = 1$$

$$P(\alpha/Y) + P(0/Y) = 1$$

При такой постановке задачи можно воспользоваться основными выводами теории обнаружения.

Поэтому, далее вводим в рассмотрение критерий абсолютного отношения правдоподобия

$$L_\alpha = \frac{P(\alpha/Y)}{P(0/Y)} = \frac{P(\alpha/Y)}{1-P(\alpha/Y)} = \frac{P(\alpha)}{P(0)}\cdot\frac{P(Y/\alpha)}{P(Y/0)}$$

На основании изложенного можно записать

$$P(\alpha/Y) = \frac{L_\alpha}{1+L_\alpha}$$

Таким образом, можно считать, что L_α определяет вероятность наличия скрытых данных в анализируемом сообщении. Если в результате анализа подозрительного сообщения было установлено, что $L_\alpha > 1$, то это означало бы, что $P(\alpha/Y) > 0,5$, и, следовательно $P(0/Y) = 1 - P(\alpha/Y) < 0,5$.

Отсюда следует, что $P(\alpha/Y) > P(0/Y)$, то есть вероятность наличия скрытых данных в подозрительном сообщении выше вероятности их отсутствия.

Однако, для определения L_α необходимо не только определить величину $W = \frac{P(Y/\alpha)}{P(Y/0)}$ - отношение правдоподобия, но узнать заранее значения $P(\alpha/Y)$ и $P(0/Y)$.

Таким образом, можно считать, что решения задачи обнаружения всегда сопровождаются ошибками. Программно-аппаратные средства, которыми располагает противник, могут также вырабатывать ошибочные посылки, связанные с естественным несовершенством названных средств, т. е. наличием методических ошибок, носящих случайный характер.

По аналогии с определениями, выработанными в теории обнаружения, далее рассматриваются следующие понятия:

• ошибка «ложной тревоги»;

• ошибка необнаружения скрытых данных в подозрительном сообщении.

Будем обозначать далее событие принятия решения об обнаружении скрытых данных в подозрительном сообщении как «ДА», а событие, связанное с необнаружением скрытых данных - как «НЕТ». Вводим далее следующие обозначения:

Р(ДА/0) - Р(лт) - вероятность ложной тревоги

Р(НЕТ/α) - Р(но) - вероятность необнаружения.

События, связанные с принятием решения о наличии, либо отсутствии скрытых данных в подозрительном сообщении образуют полную группу, так что

Р(НЕТ/α) + Р(ДА/α) = 1,

Р(НЕТ/0) + Р(ДА/0) = 1.

Тогда вероятность обнаружения Р(обн) определяется зависимостью

Р(обн) = Р(ДА/α) = 1 - Р(НЕТ/α)= 1 - Р(но),

Р(пно) = Р(НЕТ/0) = 1 - Р(ДА/0)= 1 - Р(лт).

Величина Р(обн) - вероятность заключения противника о наличии в подозрительном сообщении скрытых данных при условии, что скрытые данные действительно присутствуют.

Величина P(пно) - вероятность заключения противника об отсутствии скрытых данных в подозрительном сообщении, при условии, что их действительно там нет - вероятность правильного необнаружения.

Таким образом, можно считать, что чем больше значение P(но) (или чем меньше P(обн)) при заданном значении P(лт), тем выше качество системы сокрытия данных.

С учетом вышеперечисленного можно записать выражения для безусловных вероятностей:

$$P^{a}(\text{лт}) = P(0) \cdot P(\text{лт})$$

$$P^{a}(\text{но}) = P(\alpha) \cdot P(\text{но})$$

$$P^{a}(\text{обн}) = P(\alpha) \cdot P(\text{обн})$$

$$P^{a}(\text{пно}) = P(0) \cdot P(\text{пно})$$

Вышеперечисленные вероятности в среднем могут быть вычислены опытным путем через частоты принятия противником правильных и ошибочных решений в процессе анализа множества подозрительных контейнеров, содержащих (либо нет) сокрытые одним и тем же методом данные.

Таким образом, оценка необнаружимости основывается в первую очередь на экспериментальных результатах обнаружения скрытых данных методами обнаружения.

5.4 Постановка задачи обнаружения скрытого сообщения

Подавляющее большинство методов обнаружения сокрытых данных основаны на анализе характеристик вероятностного распределения элементов контейнера. Это позволяет прогнозировать действия противника при решении задачи обнаружения скрытых данных. Ниже рассматривается математическая модель основных наиболее вероятных действий противника, основанная на положениях теории обнаружения.

Принятие противником решения о наличии скрытых данных на исследуемом носителе производится не по одному значению какой-то величины, характеризующей содержимое носителя, а по всему объему носителя, т.е. по выборке, состоящей из N значений реализации, что позволяет более полно использовать априорную информацию и получить тем больший положительный эффект, чем значительней объем выборки N.

Таким образом, задача противника по разработке метода обнаружения может интерпретироваться, как задача оптимизации:

$$\max_F P_{\text{обн}} \text{при} P_{\text{лт}} \le P_{\text{лт}}^{max}$$

$$P_{\text{обн}} = \frac{1}{n}\sum_i^n F(S(I_i))$$

$$P_{\text{лт}} = \frac{1}{n}\sum_i^n F(I_i)$$

где I набор пустых контейнеров, $S(I)$ функция сокрытия данных, $F(I)$ - функция обнаружения,

$$F(I) = \begin{cases} 1, & \text{если решение «ДА»} \\ 0, & \text{если решение «НЕТ»} \end{cases}$$

Запишем функцию обнаружения через оценку $E(I)$:

$$F(I) = \begin{cases} 1, & E(I) \ge E_{\text{крит}} \\ 0, & E(I) < E_{\text{крит}} \end{cases}$$

$E_{\text{крит}}$ - пороговая оценка.

Так как в качестве контейнеров используются реальные избыточные источники сигнала, содержимое контейнера можно разделить на сигнал и «шум», где под шумом понимается шум дискретизации, квантовый шум и т.п. искажения, вносимые в «идеальный» сигнал. В случае использования энергонезависимых носителей как контейнеров, под шумом будем понимать неиспользуемые блоки файловой системы.

Представим контейнер I как

$$I = L + G$$

где L - контейнер без шумов, G - присутствующий в контейнере шум.

Тогда

$$E(I) = w_L E_L(L) + w_G E_G(G)$$

где w_L, w_G - веса соответствующих оценок.

Очевидно, что с ростом ресурсов противника, в частности, числа доступных пустых контейнеров n, оценка E_L улучшается:

$$\lim_{n\to\infty} E_L(L) = 0$$

$$\lim_{n\to\infty} E_L(S(L)) = \infty$$

Кроме того внедрение сокрытых данных в сигнал-контейнер может привести к «видимым» стороннему наблюдателю искажениям. Соответственно, исходя из результатов проведенного анализа и модели скрытого канала передачи данных, практически применимые алгоритмы сокрытия данных размещают скрываемые данные в шуме контейнера:

$$S(I) = L + S(G)$$

Таким образом, оптимальный метод обнаружения скрытых данных строится, основываясь на следующем алгоритме обнаружения:

1)выделяютстся параметры шума G из предоставленного для анализа контейнера I с помощью выбранного метода выделения шума N, $G = N(I)$

2)принимается решение «ДА» или «НЕТ» в зависимости от оценки наличия скрытых данных в выделенном шуме $E_G(G)$

Следовательно, задача разработки метода обнаружения может быть представлена как поиск оптимальной функции оценки E_G и оптимальной функции выделения шума N:

$$\max_{E_G,N} P_{\text{обн}} \text{при} P_{\text{лт}} \le P_{\text{лт}}^{max}$$

Задача построения оценки шума E_G является задачей классификации. Согласно ее трактовки в рассматриваем случае требуется построить алгоритм, относящий объект шума, полученный из представленного для анализа контейнера к одному из двух классов - классу шумов, содержащих скрытые данные или классу шумов, не содержащих скрытые данные. Объект шума в данном случае может быть представлен как вектор, состоящий из p отдельных характеристик шума. Для построения алгоритма используется учебная выборка, состоящая из набора пустых и заполненных контейнеров.

Принято считать оптимальным методом решения данной задачи метод опорных векторов.

Метод опорных векторов основан на поиске гиперплоскости в p-мерном пространстве, разделяющую два класса p-мерных векторов, так, что расстояние между гиперплоскостью и ближайшими точками классов максимально.

Гиперплоскость определяется геометрическим местом точек x, таким что

$$w \cdot x - b = 0$$

w - нормаль гиперплоскости, $\frac{b}{||w||}$ - смещение гиперплоскости от начала координат.

В случае линейной разделимости классов w и b выбираются таким образом чтобы максимизировать расстояние между максимально возможно удаленными разделяющими классы гиперплоскостями

$$w \cdot x - b = 1$$

и

$$w \cdot x - b = -1$$

,равное $\frac{2}{||w||}$. Таким образом, требуется решить задачу минимизации $||w||$ для параметров w, b при условии

$$\forall i : c_i(w \cdot x_i - b) \geq 1$$

где $c_i \in \{-1; 1\}$ - класс, к которому принадлежит вектор x_i

Решением задачи является линейная комбинация векторов учебной выборки

$$w = \sum_i^n \alpha_i c_i x_i$$

Векторы x_i, для которых $\alpha_i > 0$, называются опорными. Для них верно

$$c_i(w \cdot x_i - b) = 1$$

Следовательно

$$b = w \cdot x_i - c_i$$

В случае линейной неразделимости классов в методе опорных векторов вводится величина ошибки ξ_i, соответствующая ошибке классификации вектора x_i:

$$\forall i : c_i(w \cdot x_i - b) \geq 1 - \xi_i$$

Задача оптимизации таким образом ставится как

$$\min_{w,\xi} \left\{ \frac{1}{2}\|w\|^2 + C \sum_{i}^{n} \xi_i \right\}$$

при условии

$$\forall i : c_i(w \cdot x_i - b) \geq 1 - \xi_i, \xi_i \geq 0$$

Для нелинейной классификации вместо скалярного произведения векторов используется нелинейная функция ядра. В соответствие со сложившейся практикой оптимальной функцией представляется радиально-базисная функция

$$k(x_i, x_j) = e^{-\gamma \|x_i - x_j\|^2}$$

Таким образом, оценка параметров шума задается следующими параметрами:

• набором используемых характеристик шума

• параметром штрафной функции C

• параметром радиально-базисной функции γ

5.5 Анализ методов выделения параметров шума

Так как предложенная схема наиболее вероятных действий противника основана на разделении сигнала и шума, в частности, на поиске оптимальной функции выделения шума N, рассмотрим возможные методы выделения шума для наиболее часто используемых типах контейнеров.

Видеоканал

Для восстановления зашумленного видеоканала разработано значительное количество различных методов фильтрации. Параметры шума в данном случае вычисляется как

$$G = I - L$$

где I - исходное изображение, L восстановленное изображение.

Фильтр, основанный на вычислении среднего арифметического

Такой фильтр является простейшим. Он сглаживает локальные вариации яркости на изображении, и удаление шума происходит за счет этого сглаживания.

Пусть S_{xy} - некоторая окрестность размерами m*n и с центром в точке (x, y). Необходимо вычислить среднее арифметическое по окрестности S_{xy}. Таким образом, для произвольной точки обрабатываемой окрестности имеем:

$$f(x,y) = \frac{1}{mn} \sum_{s,t \in S_{xy}} g(s,t)$$

Данную операцию можно представить в виде маски, все коэффициенты которой равны $\frac{1}{mn}$.

Фильтр, основанный на вычислении среднего геометрического

Изображение, восстановленое таким фильтром задается выражением

$$f(x,y) = \left[\prod_{s,t \in S_{xy}} g(s,t) \right]^{\frac{1}{mn}}$$

Здесь значение восстановленного изображения в каждой точке является корнем степени mn из произведения значений в точках окрестности S_{xy}. Применение этого фильтра приводит к сглаживанию изображения, но в отличие от среднеарифметического фильтра, теряется намного меньше деталей.

Фильтры, основанные на вычислении среднего гармонического

Результат обработки этим фильтром задается выражением

$$f(x,y) = \frac{mn}{\sum_{s,t \in S_{xy}} \frac{1}{g(s,t)}}$$

Среднегармонический фильтр хорошо справляется с «белым» шумом (т.е. когда зашумление выражается в появлении белых точек на изображении). Этот фильтр так же хорошо применим при работе с Гауссовым шумом.

Медианный фильтр

Действие этого фильтра сводится к замене значения в точке изображения на медиану значений яркости в окрестности этой точки:

$$f(x,y) = med_{s,t \in S_{xy}}\{g(s,t)\}$$

При вычислении медианы, значение в самой точке также учитывается. Широкая популярность этих фильтров обоснована тем, что они прекрасно приспособлены к подавлению случайных шумов, и при этом приводят к наименьшему размыванию по сравнению с другими фильтрами. Медианные фильтры особенно успешно работают в случаях импульсного шума.

Фильтры, основанные на вычислении максимума и минимума

Откликом медианного фильтра на некоторую последовательность данных является среднее значение из упорядоченной последовательности этих данных. Однако можно использовать либо максимальное, либо минимальное значение в упорядоченной последовательности. Если мы выбираем максимальное значение, то это приводит к поиску в изображении точек с максимальным значением яркости. Такой фильтр хорошо использовать в случае «черного» импульсного шума. Если же напротив, использовать минимальное значение, то мы найдем точки с минимальным значением яркости. Это значит, что такой фильтр хорошо применять для исключения «белого» импульсного шума.

Выбор средней точки

Применение фильтра средней точки заключается в вычислении среднего между максимальным и минимальным значениями в соответствующей окрестности точки. Такой фильтр сочетает в себе методы порядковых статистик и усреднения, что делает его хорошо применимым в случае распределенных шумов.

Фильтрация на основе вейвлет-преобразований

Поскольку изображение является дискретным сигналом, то для его обработки можно использовать фильтры, основанные на частотном разделении в дискретной области. В данном случае речь идет о фильтрах, основанных на вейвлет-преобразованиях. Вейвлет-анализ является на сегодняшний день одной из самых перспективных технологий анализа данных.

Модель сигнала можно записать следующим образом:

$$s(t) = f(t) + \sigma e(t)$$

где $f(t)$ полезный сигнал, $e(t)$ шум, σ уровень шума, $s(t)$ исследуемый сигнал.

Для такой модели удаление шума с помощью вейвлет-преобразования выполняется в 4 этапа:

• разложение сигнала по базису вейвлетов;

• выбор порогового значения шума для каждого из уровней разложения;

• пороговая фильтрация коэффициентов детализации;

• реконструкция сигнала.

Со статистической точки зрения такая методика представляет собой непараметрическую оценку модели сигнала с использованием ортогонального базиса. Методика наилучшим образом работает на достаточно гладких сигналах, т.е. на сигналах, в разложении которых лишь небольшое количество коэффициентов детализации значительно отличается от нуля.

Выбор используемого вейвлета и глубины разложения, в общем случае, зависит от свойств конкретного сигнала.

При выборе порога шума используют, как правило, критерии, минимизирующие квадратичную функцию потерь для выбранной модели шума.

Аудиоканал

Для аудиоканала используется набор одномерных фильтров, аналогичных фильтрам, используемым для видеоканала. Наиболее перспективным методом, как и в случае видеоканала, представляется фильтрация на основе вейвлет-преобразований. Аудиосигнал разбивается на сегменты фиксированной длины(порядка 5 секунд), затем для каждого сегмента производится удаление шума согласно вышеизложенной модели вейвлет-фильтрации с использованием мягкой пороговой фильтрации:

$$|X| = \begin{cases} |X| - X_{\text{пор}} & |X| \geq X_{\text{пор}} \\ 0, & |X| < X_{\text{пор}} \end{cases}$$

Файловая система носителя

Методы сокрытия на макроуровне используют как контейнер видимую файловую систему носителя и скрывают данные в неиспользуемых в текущий момент блоках. Таким образом, выделение шума тривиально - шумом считаются все не используемые в текущий момент блоки видимой файловой системы.

5.5.1 Возможные характеристики шума

Для оптимизации задачи необходимо построение оптимальной оценки наличия скрытых данных в шуме E_G. Критерий согласия Пирсона позволяет оценить соответствие распределения шума в представленном для анализа контейнере распределению шума в контейнере, не содержащем скрытых данных.

Все возможные значения шума разбиваются на интервалы. Расчитывается статистика

$$\chi^2 = N \sum \frac{P_i^e - P_i^o}{P_i^e}$$

где $P_i^e = \int_{x_{i-1}}^{x_i} f(x)dx$ - предполагаемая вероятность попадания значения в i-й интервал, $P_i^o = \frac{n_i}{N}$ - соответствующее эмпирическое значение, n_i число элементов выборки из i-го интервала.

Если полученное значение χ^2 больше квантили закона распределения χ^2 заданного уровня значимости α с $(k-1)$ степенями свободы

$$P(x) = \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} x^{\frac{k-1}{2}-1} e^{-\frac{x}{2}}$$

где k - количество интервалов разбиения, то распределение шума считается соответствующим распределению шума пустого контейнера.

5.5.2 Моментные характеристики шума

Как и критерий согласия Пирсона, моменты применяются чтобы охарактеризовать наблюдаемое распределение случайной величины.

Начальный момент p-го порядка шумовой последовательности g:

$$m_p = \frac{1}{n} \sum_i^n g_i^p$$

Центральный момент p-го порядка шумовой последовательности g:

$$\mu_p = \frac{1}{n} \sum_i^n |g_i - \bar{g}|^p$$

где $\bar{g}$ - среднее значение шума.

Моделирование шума с помощью Марковских процессов.

Данные метрики оценивают взаимозависимость элементов шума, которая нарушается при внедрении несвязанного с шумом стегосигнала.

Для каждого элемента шума расчитывается вероятность его появления в зависимости от значения одного (для цепи первого порядка) или более предшествующих элементов.

Вероятность перехода в цепи Маркова первого порядка:

$$M_{u,v} = P(N_{i+1} = u | N_i = v)$$

Следует отметить возможность моделировать с помощью цепи Маркова первого порядка переходы между левым и правым каналом в стерео аудиоконтейнере.

5.5.4 Общие метрики искажений

Оценка шума может быть произведена основываясь на метриках искажений между представленным для анализа контейнере и очищенном от шума контейнере. Рекомендуется использовать следующие метрики:

• отношение сигнал-шум:

$$SNR = 10 \log_{10} \frac{\sum_i^N x_i^2}{\sum_i^N (x_i -)^2}$$

• сегментированное отношение сигнал-шум:

$$SSNR = \frac{10}{M} \sum_{m=0}^{M-1} \log_{10} \sum_{i=Nm}^{Nm+N-1} \left(\frac{x_i^2}{(x_i - y_i)^2} \right)$$

• метрика Ченаковски:

$$CZD = \frac{1}{N} \sum_i^N \left(1 - \frac{2 \min(x_i, y_i)}{x_i + y_i} \right)$$

• метрика Хаусдорфа:

$$H = \max\{h(X, Y), h(Y, X)\}$$

$$h = \max_i \min_j ||x_i - y_j||$$

5.5.5 Пример синтеза оптимального алгоритма обнаружения

Пример основан на использовании генетического алгоритма. Идея генетических алгоритмов заимствована у живой природы и состоит в организации эволюционного процесса, конечной целью которого является получение оптимального решения в сложной комбинаторной задаче.

Генетический алгоритм работает с популяциями, состоящими из хромосом - векторов переменных решаемой задачи оптимизации. Состав хромосомы, задающей параметры E_G и N, выглядит следующим образом:

1) Используемый метод выделения шума, целое число

2) Используемые характеристики шума, набор бит

3) Параметры метода опорных векторов C и γ, два вещественных числа

Общая схема работы генетического алгоритма:

1) Создание начальной популяции

2) Повторять, пока не достигнуто максимальное число итераций:

3) Выбрать наиболее полезных родителей из популяции

4) Построить их потомков с помощью оператора скрещивания

5) Внести изменения в потомков с помощью оператора мутации

6) Добавить потомков в популяцию вместо наименее полезных членов популяции

Могут быть использованы стандартные операторы скрещивания и мутации с учетом границ разнотипных элементов хромосомы.

Функция полезности вычисляется, как

$$F(E_G, N) = P_{\text{обн}}(E_G, N) - 1000 \max(0, P_{\text{лт}}(E_G, N) - P_{\text{лт}}^{max})$$Итак, решая задачу с использованием описанного генетического алгоритма, можно синтезировать оптимальный метод обнаружения скрытых данных для конкретного типа контейнеров и метода сокрытия данных, и получить искомую экспериментальную оценку вероятности необнаружения сокрытых данных.

Приложение 1. Вещественный интеграл Фурье. Сжатие изображений

Непериодическая вещественная функция $s(x)$ не может быть разложена в ряд Фурье. Однако ее всегда можно считать периодической с периодом $T_x \to \infty$. Пусть она удовлетворяет условиям Дирихле, т. е. определена на всей числовой оси, имеет конечное число точек разрыва на каждом конечном промежутке и абсолютно интегрируема $\int_{-\infty}^{\infty} |s(x)|\,dx < \infty$, что всегда выполняется на практике. Тогда посредством предельного перехода $T_x \to \infty$ получается разложение $s(x)$ в так называемый вещественный (тригонометрический) интеграл Фурье

$$s(x) = \int_0^{\infty} d\nu_x \int_{-\infty}^{\infty} s(u)\cos[2\pi\nu_x(x-u)]\,du = 2\int_0^{\infty} [a_{\cos}(\nu_x)\cos(2\pi x\nu_x) + s_{\sin}(\nu_x)\sin(2\pi x\nu_x)]\,d\nu_x \to (1.1)$$

где

$$b_{\cos}(\nu_x) = \int_{-\infty}^{\infty} s(u)\sin[2\pi\nu_x u]\,du = \int_{-\infty}^{\infty} s(x)\cos[2\pi\nu_x]\,dx \to (1.2)$$

$$a_{\sin}(\nu_x) = \int_{-\infty}^{\infty} s(u)\cos[2\pi\nu_x u]\,du = \int_{-\infty}^{\infty} s(x)\sin[2\pi\nu_x]\,dx \to (1.3)$$

ν_x – текущее значение пространственной (временной) частоты.

Интеграл Фурье (1.1) представляет вещественную функцию $s(x)$ в виде суммы бесконечного числа косинусоидальных гармоник с амплитудой $dA = a_{cos}(\nu_x)d\nu_x$ и синусоидальных гармоник с амплитудой $dB = b_{sin}(\nu_x)d\nu_x$ при непрерывно изменяющейся частоте $0 \le \nu_x < \infty$. Функцию $a_{cos}(\nu_x)$ называют **косинус-преобразованием Фурье**, а $b_{sin}(\nu_x)$ – **синус-преобразованием Фурье** сигнала s(x). В зависимости от физического смысла переменной x говорят о **непрерывном вещественном спектре амплитуд** несмещенных по фазе косинусоидальных $a_{cos}(\nu_x)$ и синусоидальных $b_{sin}(\nu_x)$гармоник или о **непрерывном вещественном спектре амплитуд** $a_{cos}(\nu_t), b_{sin}(\nu_t)$которые также называют **вещественной спектральной плотностью амплитуд** соответственно косинусоидальных и синусоидальных гармоник.

Для углубления смысла вещественного интеграла Фурье выражение (1.1) можно преобразовать к виду

$$s(x) = \int_0^{\infty} d_{\cos}(nu_x) \cos\left[2\pi x \nu_x + \phi(nu_x)\right] d\nu_x \rightarrow (1.4)$$

где $d_{\cos}(\nu_x) = \sqrt{a^2_{\cos}(\nu_x) + b^2_{\sin}(\nu_x)}$

$$\phi(\nu_x = \arctan\left[-b_{\sin}(\nu_x)/a_{\cos}(\nu_x)\right]$$
$$\cos\phi(\nu_x = a_{\cos}(\nu_x)/d(\nu_t)$$
$$\sin\phi(\nu_x = -b_{\sin}(\nu_x)/\phi(\nu_t)$$

Тогда говорят о **непрерывных вещественных спектрах амплитуд** $d_{\cos}(\nu_x)$ и **фаз** $\phi(\nu_x)$ или о **непрерывных вещественных ЧВС амплитуд** $d_{\cos}(\nu_t)$ и **фаз** $\phi(\nu_t)$, смещенных по фазе косинусоидальных гармоник. Эти спектры часто называют **вещественной спектральной плотностью амплитуд и фаз**. При этом частоты непрерывно заполняют действительную полуось $0 \le \nu_x, \nu_t < \infty$, а функции $d_{\cos}$ и ϕ задают закон распределения амплитуд и начальных фаз в зависимости от частоты. В результате интеграл Фурье (3.4) представляет вещественную функцию $s(x)$ в виде суммы бесконечного числа смещенных по фазе косинусоидальных гармоник с амплитудой $dD = d_{\cos}(\nu_x)d\nu_x$ при непрерывно изменяющейся частоте.

Тригонометрический интеграл Фурье (1.1) обычно применяют для разложения в вещественный спектр непериодических многомерных и электрических сигналов, описываемых четными или нечетными функциями. Для четной функции (1.1) имеет вид **косинус-интеграла Фурье** из несмещенных по фазе косинусоидальных гармоник:

$$s^{chot}(x) = 2\int_0^{\infty} a^{chot}_{\cos}(\nu_x) \cos(2\pi x \nu_x)\, d\nu_x \rightarrow (1.6)$$

где **косинус-преобразование Фурье** (1.2)

$$a^{chot}_{\cos}(\nu_x) = 2\int_0^{\infty} s^{chot}(x) \cos(2\pi x \nu_x)\, dx \rightarrow (1.7)$$

В случае нечетной функции имеем **синус-интеграл Фурье**, задающий непрерывное разложение по не смещенным по фазе синусоидальным гармоникам:

$$s^{nechot}(x) = 2\int_0^{\infty} b_{\sin}^{chot}(\nu_x)\sin(2\pi x\nu_x)\,d\nu_x \rightarrow (1.8)$$

где **синус-преобразование Фурье** (1.3)

$$b_{\sin}^{nechot}(\nu_x) = 2\int_0^{\infty} s^{nechot}(x)\sin(2\pi x\nu_x)\,dx (1.9)$$

Формулы (1.6) – (4.6) обычно используют вместо (1.1) – (1.3) для временных сигналов $s(t)$, так как последние заданы для $t \geq 0$ и могут быть продолжены на всю действительную ось четным или нечетным образом.

Приложение 2. Математическое определение прямого ДКП [DCT (FDCT)] и обратного ДКП [DCT (IDCT)] применительно к использованию в формате хранения растровых изображений JPEG

Процесс сжатия изображения JPEG из следующих этапов:

1) Преобразование цветового пространства: [R G B] -> [Y Cb Cr] (R,G,B - 8-битовые величины без знака)

$$\begin{vmatrix} Y \\ C_b \\ C_r \end{vmatrix} = \begin{vmatrix} 0.299 & 0.587 & 0.114 \\ -0.1687 & -0.3313 & 0.5 \\ 0.5 & -0.4187 & -0.0813 \end{vmatrix} \cdot \begin{vmatrix} R \\ G \\ B \end{vmatrix} + \begin{vmatrix} 0 \\ 128 \\ 128 \end{vmatrix}$$

Новая величина $Y = 0.299 \cdot R + 0.587 \cdot G + 0.114 \cdot B$ названа яркостью. Это величина, используемая монохромными мониторами, чтобы представить цвет RGB. Физиологически, передает интенсивность цвета RGB воспринятого глазом.

Формула для Y, подобно средневзвешенному значению с разным весом для каждого спектрального компонента: глаз наиболее чувствителен на Зеленый цвет, затем следует Красный компонент и в последнюю очередь - Синий.

Величины $C_b = -0.1687 \cdot R - 0.3313 \cdot G + 0.5 \cdot B + 128$ и $Cr = 0.5 \cdot R - 0.4187 \cdot G - 0.0813 \cdot B + 128$ названы цветовыми величинами и представляют 2 координаты в системе, которая измеряет оттенок и насыщение цвета (эти величины указывают количество синего и красного в этом цвете). Эти 2 координаты кратко названы цветоразностью.

2) Дискретизация и JPEG Стандарт

JPEG Стандарт принимает во внимание то, что глаз более чувствителен к яркости цвета, чем к оттенку этого цвета. (Черно-белые ячейки вида имеют больше влияния, чем ячейки дневного видения).

Так, для большинства JPG, яркость взята для каждого пикселя, тогда как цветоразность – как средняя величина для блока 2x2 пикселей. Имейте в виду, что это не обязательно, но при этом можно достичь хороших результатов сжатия, с незначительным убытком в визуальном восприятии нового обработанного изображения.

Примечание: JPEG стандарт определяет, что для каждого компонента образа (подобно, например Y) должно быть определено 2 коэффициента дискретизации: один для горизонтальной дискретизации и один для вертикальной дискретизации. Эти коэффициенты дискретизации определяются в файле JPG как относительно максимального коэффициента дискретизации (дополнительно об этом позже).

3) Сдвиг Уровня

Все 8-битовые величины без знака (Y,Cb,Cr) в изображении - "смещенные по уровню": они преобразовываются в 8-битовое знаковое представление вычитанием 128 из их величины.

4) 8x8 Дискретное Косинусное Преобразование (DCT)

Изображение делится на блоки 8x8 пикселей, затем для каждого блока 8x8 применяется DCT-трансформация. Заметьте, что если размер X исходного образа не делится на 8, шифратор должен сделать его делимым, дополняя остальные правые столбцы (пока X не станет кратным 8). Аналогично, если размер Y не делимо на 8, шифратор должен дополнить строки.

Блоки 8x8 обрабатываются слева направо и сверху вниз.

Поскольку каждый пиксель в блоке 8x8 имеет 3 компонента (Y,Cb,Cr), DCT приложен отдельно в трех блоках 8x8:

- Первый блок 8x8 является блоком, который содержит яркость пикселей в исходном блоке 8x8;
- Второй блок 8x8 является блоком, который содержит величины Cb;
- И, аналогично, третий блок 8x8 содержит величины Cr.

Цель DCT-трансформации в том, что вместо обработки исходных изображений, Вы работаете с пространством частот изменения яркости и оттенка. Эти частоты очень связаны с уровнем детализации изображения. Высокие частоты соответствуют высокому уровню детализации.

DCT-трансформация очень похожа на 2-мерное преобразование Фурье, которое получает из временного интервала (исходный блок 8x8) частотный интервал (новые коэффициенты 8x8=64, которые представляют амплитуды проанализированного частотного пространства)

Математическое определение прямого DCT (FDCT) и обратного DCT (IDCT).

FDCT:

$$F(u,v) = \frac{c(u,v)}{4} \cdot \sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) \cdot \cos(\frac{2x+1}{16} \cdot u\pi)\cos(\frac{2y+1}{16} \cdot v\pi)$$

где $u,v = 0,...,7; c(u,v) = 1/2$, когда $u = v = 0; c(u,v) = 1$ - в остальных случаях.

IDCT:

$$f(x,y) = \frac{1}{4} \cdot \sum_{x=0}^{7}\sum_{y=0}^{7} c(u,v) \cdot F(u,v) \cdot \cos(\frac{2x+1}{16} \cdot u\pi)\cos(\frac{2y+1}{16} \cdot v\pi)$$

где $x,y = 0,...,7$

Применение этих формул непосредственно в вычислительном отношении дорого, особенно, когда имеются разработанные более быстрые алгоритмы для прямого или обратного DCT. Один, названный AA&N, имеет только 5 операций умножения и 29 операций сложения. Больше информации и реализацию этого можно найти в свободном программном обеспечении для JPEG кодировщиков от Независимой JPEG Группы (IJG), их C-источники могут быть найдены на www.ijg.org.

Зигзагообразная перестановка 64 DCT коэффициентов

Так, после того, как мы выполнили DCT-преобразование над блоком величин 8x8, у нас есть новый блок 8x8. Затем, этот блок 8x8 просматривается по зигзагу подобно этому (числа в блоке 8x8 указывают порядок, в котором мы просматриваем 2-мерную матрицу 8x8). После того, как прошли по зигзагу матрицу 8x8, мы имеем теперь вектор с 64 коэффициентами (0..63) Смысл этого зигзагообразного вектора – в том, что мы просматриваем коэффициенты 8x8 DCT в порядке повышения пространственных частот. Так, мы получаем вектор, отсортированный критериями пространственной частоты: первая величина на векторе (индекс 0) соответствует самой низкой частоте в изображении – она обозначается термином DC. С увеличением индекса на векторе, мы получаем величины соответствующие высшим частотам (величина с индексом 63 соответствует амплитуде гармоники самой высокой частоты в блоке 8x8). Остальная часть коэффициентов DCT обозначается AC.

Приложение 2. Обзор свободно распространяемых стеганографических средств.

Blindside является применением стеганографии, которое позволяет скрыть файл или набор файлов в стандартном образе компьютера. Новое изображение выглядит идентично, но может содержать до 50 Мбайт или около того секретных данных. Скрытые файлы могут также быть зашифрованы паролем, чтобы предотвратить несанкционированный доступ к данным.

DataMark реалиует технологии четырых цифровых продуктов стеганографии - **StegComm** для конфиденциальной мультимедийной связи, **StegMark** для цифровых водяных знаков на цифровом носителе, **StegSafe** для хранения цифровой информации и связи и **StegSign** для электронной коммерции. Каждый программный продукт поставляется в стандартной версии и профессиональной версии. В то время как стандартные версии предназначены удовлетворения общих потребностей, дополнительную безопасность и доступность функций можно найти в профессиональной версии.

Digital Picture Envelope представляет собой программу, позволяющую (по заявлениям разработчиков) сделать секретные данные незаметными для любого человеческого глаза. Таким образом, можно сохранить / отправить его безопасно с помощью компьютера. На самом деле, она может вставлять секретные данные в контейнер не изменяя визуальное качество контейнера. Не меняется отображаемый размер файла.

Hide4PGP - это бесплатная программа, которая распространяется в виде исходного кода вANSIC и в виде скомпилированных исполняемых файлов для DOS (любой версии 1.x, , OS / 2 (Warp и выше), а также Win32 консоль (9x и NT). По заявлениям разработчиков она позволяет скрыть любые данные таким образом, что зритель или слушатель не признает никакой разницы при сравнении с контейнером.

InThePicture осуществляет шифрование файлов и сообщений в избыточные пространства в Windows Bitmap (BMP) файлов изображений.

Invisible Secrets скрывает личные данные в файлы, которые невинно выглядят, как изображения или веб-страницы. Характеризуется:

- сильными алгоритмами шифрования;
- позволяет защитить паролем определенные приложения,
- решениями для управления паролями,
- наличием генератора случайных паролей,
- наличием «измельчителя», который позволяет уничтожить без возможности восстановления файлы, папки и интернет следы,
- возможностью создания саморасшифровывающихся пакетов, обеспеченных передачей пароля.

JPHIDE и JPSEEK - программы, которые позволяют скрыть файл в формате JPEG изображение визуально. Есть много версий подобных программ, доступных в Интернете, но и JPHIDE и JPSEEK являются особыми. Целью разработки было не просто, скрыть файл, а сделать это таким образом, что невозможно доказать, что хост-файл содержит скрытый файл. Учитывая типичный зрительный образ, низкую скорость введения (до 5%) и отсутствие оригинального файла, не представляется возможным заключить с высокой уверенность, что хост-файл содержит вставленные данные. Когда процент вставки увеличивается, статистический характер коэффициентов JPEG отличаются от "нормальных" в такой степени, что возникает подозрение. При достижении 15% эффекты начинают становятся видными невооруженным глазом.

MP3Stego скрывает данные в MP3-файлах в процессе сжатия. Данные сначала сжаты, зашифрованы и скрыты в потоке битов. Хотя MP3Stego была написана для стеганографических приложений , она может быть использована для защиты авторских прав. Система маркировки для файлов MP3 слабая, но все же гораздо лучше, чем флагом авторских прав в MPEG, как определено стандартом. Любой противник может распаковать поток битов и сжать его, чтобы удалить скрытые данные.

NICETEXT представляет собой пакет, который преобразует текст в любой файл на псевдо-естественном языке. Псевдоесте́ственный язы́к — компьютерный язык, конструкции которого намеренно сделаны похожими на конструкции естественного языка (английского, русского и т. д.). Псевдоестестенные языки рассчитаны на неопытного

пользователя. У некоторых псевдоестественных языков (например, SQL) лишь простейшие конструкции похожи на естественный язык, сложные запросы имеют явно «компьютерный» вид.

OutGuess - это универсальный инструмент стеганографии, который обеспечивает вставку скрытых данных в избыточные биты котейнера. По заявлениям разработчиков, характер источника данных не имеет никакого значения. Программа опирается на данные конкретных обработчиков, которые будут извлекать избыточные биты и записать их обратно после модификации. В основной версии поддерживаются изображения формата PNM и JPEG.

ScramDisk - это программа, которая позволяет создавать и использовать виртуальные зашифрованные диски. Создается файл-контейнер на существующем жестком диске, который создается с определенным паролем. Этот контейнер может быть установлен на ScramDisk программным обеспечением, которое создает новую букву диска для представления дисков. Виртуальный диск может быть доступен только с правильным паролем.

Snow. Используется для сокрытия сообщения в ASCII текст, путем добавления пробелов в конце строк. Из-за пробелов и символов табуляции, данные как правило, не видны в тексте , сообщение фактически скрыто от случайного наблюдателя. И если встроенные данные зашифрованы, сообщение невозможно прочитать, даже если оно было обнаружено.

Steganos скрывает секретные данные в звуковые, графические и текстовые файлы. Эти данные не зашифрованы заранее. Таким образом, файлы могут быть отправлены через Интернет, не будучи замеченным со стороны третьих лиц.

StegParty представляет собой систему для сокрытия информации внутри текстовых файлов. В отличие от аналогичных инструментов в настоящее время не используется для кодирования данных - она опирается на небольшие изменения в сообщениях, такие, как изменения в орфографии и пунктуации. Из-за этого вы можете использовать любой текстовый файл в качестве своего оператора, и он будет более-менее понятен после того, как тайное сообщение встроено.

TextHide - программное обеспечение для скрытия данных в тексте не вызывая подозрений того, что хранятся или передаются секреты (текстовая стеганография)

wbStego является инструментом, который скрывает любые типы файлов в растровые изображения, текстовые файлы, HTML файлы или Adobe PDF файлов. Контейнер, в котором скрываются данные оптически не изменяется. Он может быть использован для безопасного обмена конфиденциальными данными или для добавления скрытых данных об авторских правах в файл.

Один из лучших и самых распространенных продуктов для платформы Windows95/NT - это программная система S-Tools, которая имеет статус freeware. Следует отметить, что подобных систем на сегодняшний день достаточно много, все они имеют свои особенности: как в организации своей работы, так и в используемых алгоритмах шифрования.

Программа S-tools позволяет прятать любые файлы как в изображениях формата gif и bmp, так и в аудио файлах формата wav (другие программные системы стеганографии поддерживают ряд других графических, видео и аудио форматов файлов). При этом S-Tools - это стеганография и криптография в одной программной системе потому, что файл, подлежащий сокрытию, еще и шифруется с помощью одного из криптографических алгоритмов, например, с симметричным ключом: DES, тройной DES или IDEA - два последних алгоритма на сегодня вполне заслуживают доверия. Файл-носитель перетаскивается (визуально буксируется при помощи мыши) в окно программы, затем в этот файл перетаскивается файл с данными любого формата, вводится пароль, выбирается алгоритм шифрования. Внешне графический файл остается практически неизменным, меняются лишь кое-где оттенки цвета.

Звуковой файл также не претерпевает заметных изменений. Для большей безопасности используются неизвестные широкой публике изображения, изменения в которых не бросятся в глаза с первого взгляда, а также изображения с большим количеством полутонов и оттенков. Соотношение между размером файла с изображением или звуком и размером текстового файла, который можно спрятать, зависит от конкретного случая. Иногда размер текстового файла даже превышает размер графического. Впрочем, даже если подозрения у кого-то и возникнут, то их придется оставить при себе: не зная пароля, сам факт использования S-Tools установить и доказать нельзя, тем более нельзя извлечь и информацию.

Steganos for Windows 95 - распространенная стеганографическая программа. Она обладает практически теми же возможностями, что и S-Tools, но использует другой криптографический алгоритм (HWY1), и, кроме того, способна скрывать данные не только в файлах формата bmp и wav, но и в обычных текстовых и HTML файлах (стандарт файлов Интернет), причем весьма оригинальным способом - в конце каждой строки добавляется определенное число пробелов.

Кроме того, Steganos добавляет в свое программное меню "Отправить" (то, которое появляется при правом щелчке мышью на файле) опцию отправки в шредер, что позволяет удалить файл с диска без возможности его последующего восстановления.

Приложение 3. Контрольные вопросы.

1. Проведите сопоставление возможностей криптографических и стеганографических методов сокрытия данных при передаче в каналах передачи сообщений.
2. В чем заключаются различия и сходство методов компьютерной и цифровой стеганографии.
3. Проведите анализ уязвимостей стеганографической системы на основе ее структурной схемы.
4. Проведите анализ «возможностей» Евы в попытках выявить переписку Алисы и Боба.
5. Определите ограничения возможностей успешного сокрытия данных в изображениях.
6. Сопоставьте возможности успешного сокрытия данных в файлах, содержащих изображения и в аудиофайлах рассмотренными алгоритмами цифровой стеганографии.
7. Имеются ли принципиальные (теоретичиские) ограничения в развитии, разработке новых методов цифровой стеганографии.
8. Имеются ли принципиальные (теоретичиские) ограничения в развитии, разработке новых методов компьютерной стеганографии.
9. Дайте оценку уязвимостей директорий FAK при применений стегосистемы Steg FS.
10. Определите принципиально оригинальный метод цифровой стеганографии из числа описанных в пособии. Проведите сопоставительный анализ этих методов по критерию «оригинальность».
11. Определите принципиальные отличия в постановке задачи криптоанализа и стегоанализа.

12. Оцените достоинства и недостатки генетических алгоритмов для решения задач стеганоанализа.

Список литературы

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс, 2002. – 272с.
2. Rotation scale and translation invariant spread spectrum digital image watermarking. IEEE Int. Conf. on Image Processing, 1998. P. 4.
3. Pereira S., Joseph J., Deguillaume F. Template Based recovery of Fourier-Based Watermarks Using log-polar and Log-log Maps. IEEE Int. Conf on Multimedia Computing and Systems, 1999. P. 5.
4. Lin Ch-Y., Chang Sh.-F. Distortion Modeling and Invariant Extraction for Digital Image Print-and Scan Process. International Symposium on Multimedia Information Processing, 1999. P. 10.
5. Lin Ch-Y., Chang Sh.-F. Public Watermarking Surviving General Scaling and Cropping: An Application for Print-and-Scan Process. Multimedia and Security Workshop at ACM Multimedia, 1999.
6. Pereira S., Thierry P. Fine Robust Template Matching for Affine Resistant Image Watermarks. IEEE Trans. on Image Processing, 1999. - P. 12.
7. Kutter M. Watermarking Resisting to Translation, Rotation, and Scaling. Signal Processing Laboratory, 1998. P. 10.
8. Kutter M. Digital Signature of Color Images using Amplitude Modulation. Signal Processing Laboratory, 1997. P. 9.
9. Herrigel A., Pereira S., Petersen H. Secure Copyright Protection Techniques for Digital Images. International Workshop on Information Hiding, 1998. P. 22.
10. Ramkumar M. Data Hiding in Multimedia – Theory and Applications. New Jersey Institute of Technolog, 1999. P. 70.
11. Bender W. Applications for Data Hiding. IBM Systems Journal, 2000. P. 22.
12. Chae J., Manjunath B. A Robust Data Hiding Technique using Multidimensional Lattices. Proc. IEEE Conference on Advances in Digital Libraries, 1998. P. 8.
13. Chae J., Manjunath B. A Technique for Image Data Hiding and Reconstruction without Host Image. Proceedings of the SPIE - The International Society for Optical Engineering. 1999, P. 11.

14. Cuche E., Marquet P., Spatial filtering for zero-order and twin-image elimination in digital off-axis holography. Applied Optics V.39, 2000. P. 4070–4075.

15. W.Diffie,M.E.Hellman. New Directions in cryptography// IEEE Trans. Inform. Theory, IT-22, vol 6 (Nov. 1976), pp. 644-654.

16. У.Диффи. Первые десять лет криптографии с открытым ключом. /пер. с англ./ М., Мир, ТИИЭР.–1988.–т.76.–N5.