**КОНТРОЛЬНАЯ РАБОТА**

***«Стеганография. Использование программ скрытого шифрования»***

**Введение**

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Слово «стеганография» имеет греческие корни и буквально означает «тайнопись». Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. Тайнопись осуществляется самыми различными способами. Общей чертой этих способов является то, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимание объект. Затем этот объект открыто транспортируется адресату. При криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, при стеганографии же наличие скрытой связи остается незаметным.

Какие только стеганографические методы не использовали люди для защиты своих секретов. Известные примеры включают в себя использование покрытых воском дощечек, вареных яиц, спичечных коробков и даже головы раба (сообщение читалось после сбривания волос гонца). В прошлом веке широко использовались так называемые симпатические чернила, невидимые при обычных условиях. Скрытое сообщение размещали в определенные буквы невинных словосочетаний, передавали при помощи внесения в текст незначительных стилистических, орфографических или пунктуационных погрешностей. С изобретением фотографии появилась технология микрофотоснимков, успешно применяемая Германией во время мировых войн. Крапление карт шулерами – это тоже пример стеганографии.

Во время Второй мировой войны правительством США придавалось большое значение борьбе против тайных методов передачи информации. Были введены определенные ограничения на почтовые отправления. Так, не принимались письма и телеграммы, содержащие кроссворды, ходы шахматных партий, поручения о вручении цветов с указанием времени и их вида; у пересылаемых часов переводились стрелки. Был привлечен многочисленный отряд цензоров, которые занимались даже перефразированием телеграмм без изменения их смысла.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео. Известны также предложения по встраивании информации в текстовые файлы и в исполняемые файлы программ.

Существуют два основных направления в компьютерной стеганографии: связанные с цифровой обработкой сигналов и не связанные. В последнем случае сообщения могут быть встроены в заголовки файлов, заголовки пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и / или уничтожения скрытой информации. Большинство текущих исследований в области стеганографии, так или иначе, связаны с цифровой обработкой сигналов. Это позволяет говорить о цифровой стеганографии.

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом защищать информацию от несанкционированного копирования, отслеживать распространение информации по сетям связи, обеспечивать поиск информации в мультимедийных базах данных.

Международные симпозиумы по скрытию данных проводятся с 1996 года, по стеганографии первый симпозиум состоялся в июле 2002 года. Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации.

**1. Общие сведения о стеганографии**

**1.1 Основные понятия и определения стеганографии**

Несмотря на то, что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография – молодое и развивающееся направление.

Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии.

До недавнего времени для описания модели стеганографической системы использовалась предложенная 1983 году Симмонсом так называемая «проблема заключенных». Она состоит в том, что два индивидуума (Алиса и Боб) хотят обмениваться секретными сообщениями без вмешательства охранника (Вилли), контролирующего коммуникационный канал. При этом имеется ряд допущений, которые делают эту проблему более или менее решаемой. Первое допущение облегчает решение проблемы и состоит в том, что участники информационного обмена могут разделять секретное сообщение (например, используя кодовую клавишу) перед заключением. Другое допущение, наоборот, затрудняет решение проблемы, так как охранник имеет право не только читать сообщения, но и модифицировать (изменять) их.

Позднее, на конференции Information Hiding: First Information Workshop в 1996 году было предложено использовать единую терминологию и обговорены основные термины.

**Стеганографическая система или стегосистема** – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

При построении стегосистемы должны учитываться следующие положения:

* противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
* если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;
* потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Обобщенная модель стегосистемы представлена на рис. 1.

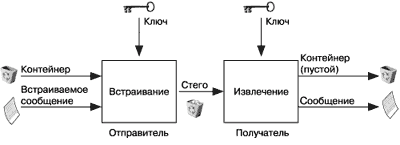


Рисунок 1 – Обобщенная модель стегосистемы

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т.п.

В общем же случае целесообразно использовать слово «**сообщение**», так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

**Контейнер** – любая информация, предназначенная для сокрытия тайных сообщений.

**Пустой контейнер** – контейнер без встроенного сообщения; **заполненный контейнер** или **стего – контейнер**, содержащий встроенную информацию.

**Встроенное (скрытое) сообщение** – сообщение, встраиваемое в контейнер.

**Стеганографический канал** или просто **стегоканал** – канал передачи стего.

**Стегоключ** или **просто ключ** – секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

* с секретным ключом;
* с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

* 1. **Сокрытие данных (сообщений)**

Под цифровой стеганографией понимается скрытие одной информации в другой. Причем сокрытие это должно реализоваться таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, неизбежная модификация информационного носителя, не только не уничтожила смысловые функции, но и на определенном уровне абстракции даже не меняла их. Тем самым факт передачи одного сообщения внутри другого не выявляется традиционными методами.

В качестве носителя скрытой информации должен выступать объект (файл), допускающий искажения собственной информации, не нарушающие его функциональность. Внесенные искажения должны быть ниже уровня чувствительности средств распознавания.

В качестве носителя обычно используются файлы изображений или звуковые файлы. Такие файлы обладают большой избыточностью и, кроме того, обычно велики по размеру, обеспечивая достаточно места для сокрытия простого или форматированного текста. Скрываемое сообщение может быть простым набором чисел, изображением, простым или зашифрованным текстом. Многие мультимедийные форматы имеют поля расширения, которые могут заполняться пользовательской информацией, а могут быть забиты нулями – в последнем случае их также можно использовать для хранения и передачи информации. Однако этот наивный способ не только не обеспечивает требуемого уровня секретности, но и не может прятать значительные объемы данных. Решение этих проблем нашлось в следующем подходе.

В графических файлах, аудио и видео файлах обычно содержится множество избыточной информации, которая совершенно не воспринимается органами чувств человека (следует, правда, заметить, что даже эта избыточная информация очень и очень далека от оригинала, поскольку, во-первых данные всегда разбиваются на конечное число элементов, каждый из которых описывается конечным двоичным числом. Аналоговый же сигнал содержит потенциально бесконечное число сведений, которые обрубаются при оцифровке.) Поэтому при умеренной декрементации цифровых данных обычный человек, в силу своего анатомического строения не может заметить разницы между исходной и модифицированной информацией.

Предположим, что в качестве носителя используется 24-битовое изображение размером 800х600 (графика среднего разрешения). Оно занимает около полутора мегабайта памяти (800х600х3 = 1440000 байт). Каждая цветовая комбинация тона (пикселя – точки) – это комбинация трех основных цветов – красного, зеленого и синего, которые занимают каждый по 1 байту (итого по 3 на пиксел). Если для хранения секретной информации использовать наименьший значащий бит (Least Significant Bits – LSB) каждого байта, то получим по 3 бита на каждый пиксел. Емкость изображения носителя составит – 800х600х3/8=180000 байт. При этом биты в каких-то точках будут совпадать с битами реального изображения, в других – нет, но, главное, что на глаз определить такие искажения практически невозможно.

Цифровая стеганография реализуется следующим образом: имеется какой-то цифровой файл – контейнер (фото) (1) и сам файл-сообщение (2). Для обеспечения разрозненности и случайности значений зашифруем (A), так как шифровка обеспечивает большую степень защиты данных. Затем производится вставка сообщения в файл-контейнер. Затем можно свободно передавать файл, но пароль для расшифровки должен быть заранее передан по независимому каналу получателю информации.

Самой главной задачей является обеспечить наибольшее сходство файла контейнера с уже вложенным сообщением.

В младших битах изображений и других мультимедиа файлов имеются шумы – они распределены по всему файлу произвольным образом, и как правило представляют собой случайные числовые значения.

Для обеспечения псевдослучайности при вставке файла в контейнер используют алгоритмы шифрования. Для большей надежности и схожести оригинала следует использовать изображения с шумами в младших разрядах – это изображения, полученные при помощи цифровой фотокамеры или со сканера. Такие изображения уже содержат внутри себя случайный шум, который дополнительно маскирует факт внедрения посторонней информации внутрь файла.

Кроме скрытой передачи сообщений, стеганография является одним из самых перспективных направлений, применяемых для аутентификации и маркировки авторской продукции. При этом часто в качестве внедряемой информации используются дата и место создания продукта, данные об авторе, номер лицензии, серийный номер, дата истечения срока работы (удобно для распространения shareware-программ) и др. Эта информация обычно внедряется как в графические и аудио – произведения так и в защищаемые программные продукты. Все внесенные сведения могут рассматриваться как веские доказательства при рассмотрении вопросов об авторстве или для доказательства факта нелегального копирования, и часто имеют решающее значение.

Цифровая стеганография широкое распространение получила в последние 2 года. Стеганография в сочетании с криптографией практически достигает 100% защищенности информации.

**1.3 Цифровые водяные знаки**

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки (ЦВЗ) и заголовки. Остановимся подробнее на втором приложении.

Цифровые водяные знаки могут применяться, в основном, для защиты от копирования и несанкционированного использования. В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Примерами могут являться фотографии, аудио и видеозаписи и т.д. Преимущества, которые дают представление и передача сообщений в цифровом виде, могут оказаться перечеркнутыми легкостью, с которой возможно их воровство или модификация. Поэтому разрабатываются различные меры защиты информации, организационного и технического характера. Один из наиболее эффективных технических средств защиты мультимедийной информации и заключается во встраивании в защищаемый объект невидимых меток – водяных знаков. Разработки в этой области ведут крупнейшие фирмы во всем мире. Так как методы цифровых водяных знаков начали разрабатываться совершенно недавно, то здесь имеется много неясных проблем, требующих своего разрешения.

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

Технология встраивания идентификационных номеров производителей имеет много общего с технологией водяных знаков. Отличие заключается в том, что в первом случае каждая защищенная копия имеет свой уникальный встраиваемый номер (отсюда и название – дословно «отпечатки пальцев»). Этот идентификационный номер позволяет производителю отслеживать дальнейшую судьбу своего детища: не занялся ли кто-нибудь из покупателей незаконным тиражированием. Если да, то «отпечатки пальцев» быстро укажут на виновного. Встраивание заголовков (невидимое) может применяться, например, для подписи медицинских снимков, нанесения легенды на карту и т.д. Целью является хранение разнородно представленной информации в едином целом. Это, пожалуй, единственное приложение стеганографии, где в явном виде отсутствует потенциальный нарушитель.

Наиболее существенное отличие постановки задачи скрытой передачи данных от постановки задачи встраивания ЦВЗ состоит в том, что в первом случае нарушитель должен обнаружить скрытое сообщение, тогда как во втором случае о его существовании все знают. Более того, у нарушителя на законных основаниях может иметься устройство обнаружения ЦВЗ (например, в составе DVD-проигрывателя).

Основными требованиями, которые предъявляются к водяным знакам, являются надежность и устойчивость к искажениям, они должны удовлетворять противоречивым требованиям визуальной (аудио) незаметности и робастности к основным операциям обработки сигналов.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков. Задачу встраивания и выделения цифровых водяных знаков из другой информации выполняет специальная стегосистема.

Прежде, чем осуществить вложение цифрового водяного знака в контейнер, водяной знак должен быть преобразован к некоторому подходящему виду. Например, если в качестве контейнера выступает изображение, то и последовательность ЦВЗ зачастую представляется как двумерный массив бит. Для того, чтобы повысить устойчивость к искажениям нередко выполняют его помехоустойчивое кодирование, либо применяют широкополосные сигналы. Первоначальную обработку скрытого сообщения выполняет показанный на рис. 2 прекодер. В качестве важнейшей предварительной обработки цифрового водяного знака (а также и контейнера) назовем вычисление его обобщенного преобразования Фурье. Это позволяет осуществить встраивание ЦВЗ в спектральной области, что значительно повышает его устойчивость к искажениям. Предварительная обработка часто выполняется с использованием ключа для повышения секретности встраивания. Далее водяной знак «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. Эти особенности человеческого зрения используются, например, при разработке алгоритмов сжатия изображений и видео.

Процесс внедрения цифровых водяных знаков также должен учитывать свойства системы восприятия человека. Стеганография использует имеющуюся в сигналах психовизуальную избыточность, но другим, чем при сжатии данных образом. Приведем простой пример. Рассмотрим полутоновое изображение с 256 градациями серого, то есть с удельной скоростью кодирования 8 бит/пиксел. Хорошо известно, что глаз человека не способен заметить изменение младшего значащего бита. Еще в 1989 году был получен патент на способ скрытого вложения информации в изображение путем модификации младшего значащего бита. В данном случае детектор стего анализирует только значение этого бита для каждого пиксела, а глаз человека, напротив, воспринимает только старшие 7 бит. Данный метод прост в реализации и эффективен, но не удовлетворяет некоторым важным требованиям к ЦВЗ.

В большинстве стегосистем для внедрения и выделения цифровых водяных знаков используется ключ. Ключ может быть предназначен для узкого круга лиц или же быть общедоступным. Например, ключ должен содержаться во всех DVD-плейерах, чтобы они могли прочесть содержащиеся на дисках ЦВЗ. Не существует, насколько известно, стегосистемы, в которой бы при выделении водяного знака требовалась другая информация, чем при его вложении.

В стегодетекторе происходит обнаружение цифрового водяного знака в (возможно измененном) защищенном ЦВЗ изображении. Это изменение может быть обусловлено влиянием ошибок в канале связи, операций обработки сигнала, преднамеренных атак нарушителей. Во многих моделях стегосистем сигнал-контейнер рассматривается как аддитивный шум. Тогда задача обнаружения и выделения стегосообщения является классической для теории связи. Однако такой подход не учитывает двух факторов: неслучайного характера сигнала контейнера и требований по сохранению его качества. Эти моменты не встречаются в известной теории обнаружения и выделения сигналов на фоне аддитивного шума. Их учет позволит построить более эффективные стегосистемы.

Различают стегодетекторы, предназначенные для обнаружения факта наличия водяного знака и устройства, предназначенные для его выделения (стегодекодеры). В первом случае возможны детекторы с жесткими (да/нет) или мягкими решениями. Для вынесения решения о наличии / отсутствии цифрового водяного знака удобно использовать такие меры, как расстояние по Хэммингу, либо взаимную корреляцию между имеющимся сигналом и оригиналом (при наличии последнего, разумеется). А что делать, если у нас нет исходного сигнала? Тогда в дело вступают более тонкие статистические методы, основанные на построении моделей исследуемого класса сигналов.

**1.4 Атаки на стегосистемы**

Для осуществления той или иной угрозы нарушитель применяет атаки.

Наиболее простая атака – **субъективная**. Злоумышленник внимательно рассматривает изображение (слушает аудиозапись), пытаясь определить «на глаз», имеется ли в нем скрытое сообщение. Ясно, что подобная атака может быть проведена лишь против совершенно незащищенных стегосистем. Тем не менее, она, наверное, наиболее распространена на практике, по крайней мере, на начальном этапе вскрытия стегосистемы. Первичный анализ также может включать в себя следующие мероприятия:

1. Первичная сортировка стего по внешним признакам.
2. Выделение стего с известным алгоритмом встраивания.
3. Определение использованных стегоалгоритмов.
4. Проверка достаточности объема материала для стегоанализа.
5. Проверка возможности проведения анализа по частным случаям.
6. Аналитическая разработка стегоматериалов. Разработка методов вскрытия стегосистемы.
7. Выделение стего с известными алгоритмами встраивания, но неизвестными ключами и т.д.

Из криптоанализа известны следующие разновидности атак на шифрованные сообщения:

– атака с использованием только шифртекста;

– атака с использованием открытого текста;

– атака с использованием выбранного открытого текста;

– адаптивная атака с использованием открытого текста;

– атака с использованием выбранного шифртекста.

По аналогии с криптоанализом в стегоанализе можно выделить следующие типы атак.

– **Атака на основе известного заполненного контейнера**. В этом случае у нарушителя есть одно или несколько стего. В последнем случае предполагается, что встраивание скрытой информации осуществлялось отправителем одним и тем же способом. Задача злоумышленника может состоять в обнаружении факта наличия стегоканала (основная), а также в его извлечении или определения ключа. Зная ключ, нарушитель получит возможность анализа других стегосообщений.

– **Атака на основе известного встроенного сообщения**. Этот тип атаки в большей степени характерен для систем защиты интеллектуальной собственности, когда в качестве водяного знака используется известный логотип фирмы. Задачей анализа является получение ключа. Если соответствующий скрытому сообщению заполненный контейнер неизвестен, то задача крайне трудно решаема.

– **Атака на основе выбранного скрытого сообщения**. В этом случае злоумышленние имеет возможность предлагать отправителю для передачи свои сообщения и анализировать получающиеся стего.

– **Адаптивная атака на основе выбранного скрытого сообщения**. Эта атака является частным случаем предыдущей. В данном случае злоумышленник имеет возможность выбирать сообщения для навязывания отправителю адаптивно, в зависимости от результатов анализа предыдущих стего.

– **Атака на основе выбранного заполненного контейнера**. Этот тип атаки больше характерен для систем ЦВЗ. Стегоаналитик имеет детектор стего в виде «черного ящика» и несколько стего. Анализируя детектируемые скрытые сообщения, нарушитель пытается вскрыть ключ.

У злоумышленника может иметься возможность применить еще три атаки, не имеющие прямых аналогий в криптоанализе.

– **Атака на основе известного пустого контейнера**. Если он известен злоумышленнику, то путем сравнения его с предполагаемым стего он всегда может установить факт наличия стегоканала. Несмотря на тривиальность этого случая, в ряде работ приводится его информационно-теоретическое обоснование. Гораздо интереснее сценарий, когда контейнер известен приблизительно, с некоторой погрешностью (как это может иметь место при добавлении к нему шума).

– **Атака на основе выбранного пустого контейнера**. В этом случае злоумышленник способен заставить отправителя пользоваться предложенным ей контейнером. Например, предложенный контейнер может иметь большие однородные области (однотонные изображения), и тогда будет трудно обеспечить секретность внедрения.

– **Атака на основе известной математической модели контейнера или его части**. При этом атакующий пытается определить отличие подозрительного сообщения от известной ему модели. Например допустим, что биты внутри отсчета изображения коррелированы. Тогда отсутствие такой корреляции может служить сигналом об имеющемся скрытом сообщении. Задача внедряющего сообщение заключается в том, чтобы не нарушить статистики контейнера. Внедряющий и атакующий могут располагать различными моделями сигналов, тогда в информационно-скрывающем противоборстве победит имеющий лучшую модель.

**2. Методы, технологии, алгоритмы**

Большинство методов компьютерной стеганографии базируется на двух принципах.

Первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности.

Второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в таких исходных файлах.

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначимых фрагментов среды и замена существующей в них информации на информацию, которую предполагается защитить. Поскольку в компьютерной стеганографии рассматриваются среды, поддерживаемые средствами вычислительной техники и соответствующими сетями, то вся информационная среда, в конечном итоге, может представляться в цифровом виде. Таким образом, незначимые для кадра информационной среды фрагменты в соответствии с тем или иным алгоритмом или методикой заменяются (смешиваются) на фрагменты скрываемой информации. Под кадром информационной среды в данном случае подразумевается некоторая ее часть, выделенная по определенным признакам. Такими признаками часто бывают семантические характеристики выделяемой части информационной среды. Например, в качестве кадра может быть выбран некоторый отдельный рисунок, звуковой файл, Web-страница и др.

Для методов компьютерной стеганографии можно ввести определенную классификацию (рис. 20.2).



Рис**.** Классификация методов сокрытия информации

По способу отбора контейнера, как уже указывалось, различают методы суррогатной стеганографии, селективной стеганографии и конструирующей стеганографии.

В методах суррогатной (безальтернативной) стеганографии отсутствует возможность выбора контейнера и для сокрытия сообщения выбирается первый попавшийся контейнер, зачастую не совсем подходящий к встраиваемому сообщению. В этом случае, биты контейнера заменяются битами скрываемого сообщения таким образом, чтобы это изменение не было заметным. Основным недостатком метода является то, что он позволяет скрывать лишь незначительное количество данных.

В методах селективной стеганографии предполагается, что спрятанное сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящий из них для конкретного сообщения. Частным случаем такого подхода является вычисление некоторой хеш-функция для каждого контейнера. При этом для сокрытия сообщения выбирается тот контейнер, хеш-функции которого совпадает со значением хеш-функции сообщения (т.е. стеганограммой является выбранный контейнер).

В методах конструирующей стеганографии контейнер генерируется самой стегосистемой. Здесь может быть несколько вариантов реализации. Так, например, шум контейнера может моделироваться скрываемым сообщением. Это реализуется с помощью процедур, которые не только кодируют скрываемое сообщение под шум, но и сохраняют модель первоначального шума. В предельном случае по модели шума может строиться целое сообщение. Примерами могут служить метод, который реализован в программе MandelSteg, где в качестве контейнера для встраивания сообщения генерируется фрактал Мандельброта, или же аппарат функций имитации (mumic function).

По способу доступа к скрываемой информации различают методы для потоковых (непрерывных) контейнеров и методы для контейнеров с произвольным доступом (ограниченной длины).

Методы, использующие потоковые контейнеры, работают с потоками непрерывных данных (например, интернет-телефония). В этом случае скрываемые биты необходимо в режиме реального времени включать в информационный поток. О потоковом контейнере нельзя предварительно сказать, когда он начнется, когда закончится и насколько продолжительным он будет. Более того, объективно нет возможности узнать заранее, какими будут последующие шумовые биты. Существует целый ряд трудностей, которые необходимо преодолеть корреспондентам при использовании потоковых контейнеров. Наибольшую проблему при этом составляет синхронизация начала скрытого сообщения.

Методы, которые используются для контейнеров с произвольным доступом, предназначены для работы с файлами фиксированной длины (текстовая информация, программы, графические или звуковые файлы). В этом случае заранее известны размеры файла и его содержимое. Скрываемые биты могут быть равномерно выбраны с помощью подходящей псевдослучайной функции. Недостаток таких контейнеров состоит в том, они обладают намного меньшими размерами, чем потоковые, а также то, что расстояния между скрываемыми битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный шум будет иметь экспоненциальное распределение длин интервала. Преимущество подобных контейнеров состоит в том, то они могут быть заранее оценены с точки зрения эффективности выбранного стеганографического преобразования.

По типу организации контейнеры, подобно помехозащищенным кодам, могут быть систематическими и несистематическими. В систематически организованных контейнерах можно указать конкретные места стеганограммы, где находятся информационные биты самого контейнера, а где – шумовые биты, предназначенные для скрываемой информации (как, например, в широко распространенном методе наименьшего значащего бита). При несистематической организации контейнера такого разделения сделать нельзя. В этом случае для выделения скрытой информации необходимо обрабатывать содержимое всей стеганограммы.

По используемым принципам стеганометоды можно разбить на два класса: цифровые методы и структурные методы. Если цифровые методы стеганографии, используя избыточность информационной среды, в основном, манипулируют с цифровым представлением элементов среды, куда внедряются скрываемые данные (например, в пиксели, в различные коэффициенты косинус-синусных преобразований, преобразований Фурье, Уолша-Радемахера или Лапласа), то структурные методы стеганографии для сокрытия данных используют семантически значимые структурные элементы информационной среды.

Основным направлением компьютерной стеганографии является использование свойств избыточности информационной среды. Следует учесть, что при сокрытии информации происходит искажение некоторых статистических свойств среды или нарушение ее структуры, которые необходимо учитывать для уменьшения демаскирующих признаков.

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

* зарезервированные для расширения поля компьютерных форматов файлов, которые обычно заполняются нулями и не учитываются программой;
* специальное форматирование данных (смещение слов, предложений, абзацев или выбор определенных позиций букв);
* использование незадействованных мест на магнитных носителях;
* удаление идентифицирующих заголовков для файла.

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

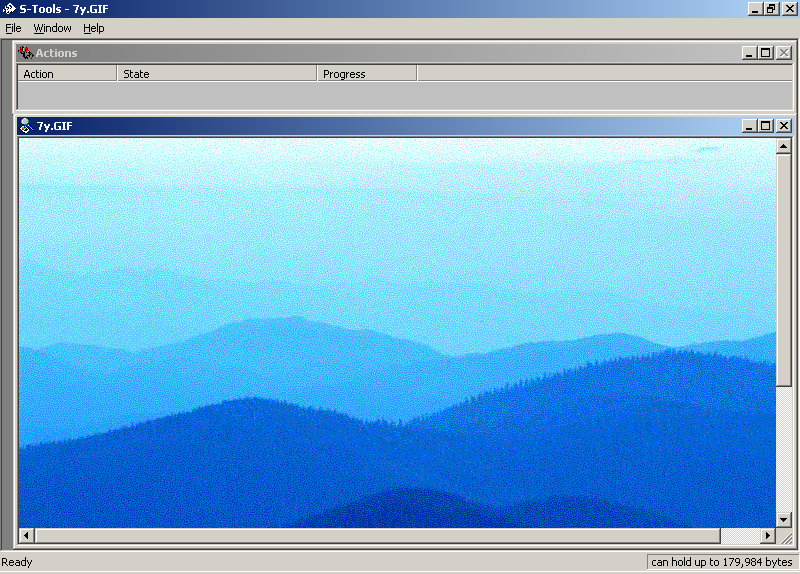
По предназначению различают стеганографические методы собственно для скрытой передачи или скрытого хранения данных и методы для сокрытия данных в цифровых объектах с целью защиты самих цифровых объектов.

По типу информационной среды выделяются стеганографические методы для текстовой среды, для аудио среды, а также для изображений (стоп-кадров) и видео среды.

**3. Практическая реализация**

**3.1 Работа с S-Tools**

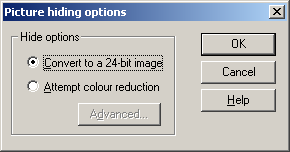
Выбираем файл-контейнер



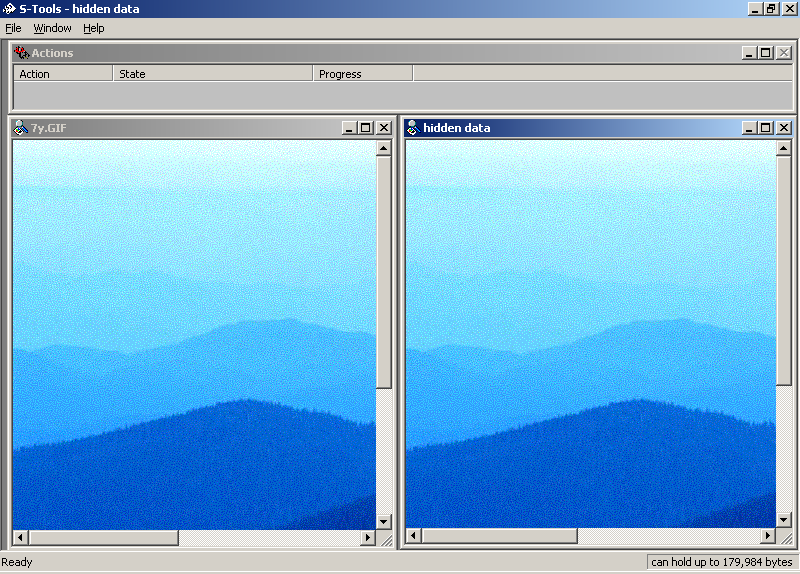
Перетаскиваем файл предназначенный для скрытия на окно. Вводим пароль и выбираем алгоритм шифрования



Выбираем опции преобразования цвета

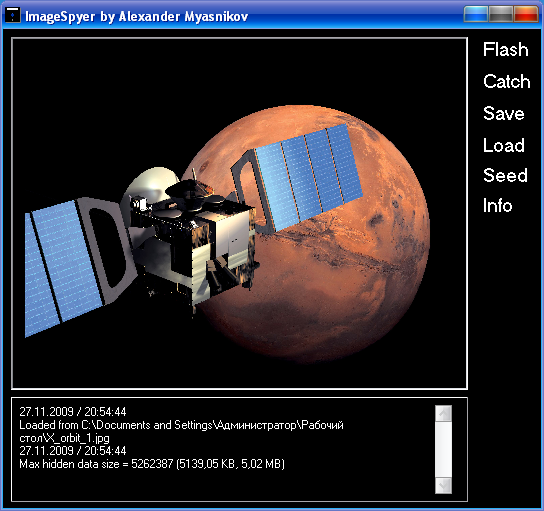


Сохраняем файл со скрытой в нем информацией

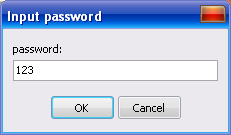


**3.2 Программа ImageSpyer**

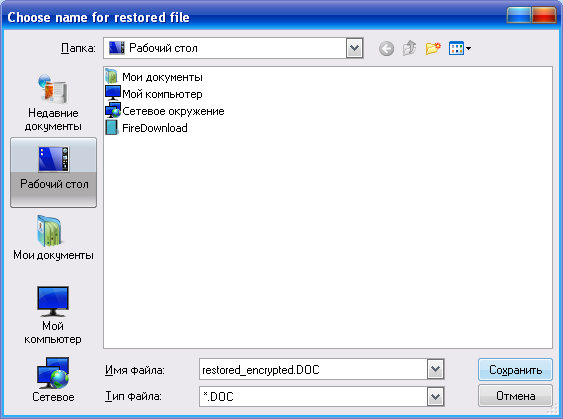
Загружаем файл-контейнер. Нажимая на кнопку Load:



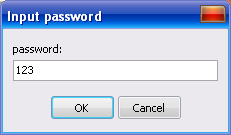
Кнопка Flash поможет выбрать информацию для шифрования, вводим пароль.



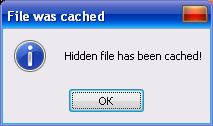
Теперь загружаем файл с зашифрованной информацией, используя ту же самую Load и нажимаем кнопку Catch.



Таким образом получилось выделить скрытую в картинке информацию, предварительно введя тот же пароль:



Об этом и говорит следующее окно:



**Выводы**

1. Рассмотрены методы стеганографии – прием преобразования информации путем внедрения в информацию иного вида для скрытой передачи, цифровые водяные знаки.
2. Проанализированы приемы и алгоритмы внедрения текстовой информации в графические файлы за счет использования битов с минимальной значимостью.
3. Показано, что стеганография может успешно применяться в случае контейнеров с графической, аудио- и видеоинформацией.
4. Применение стеганографии иллюстрируется программами S-Tools и ImageSpyer, а также авторскими графическими материалами.