Департамент образования города Москвы

Государственное бюджетное общеобразовательное учреждение

города Москвы

«Гимназия № 1505 «Московская городская педагогическая гимназия-лаборатория»»

**ДИПЛОМНОЕ ИССЛЕДОВАНИЕ**

на тему:

**Цифровая стеганография и ее методы. Моделирование сокрытия информации**

Выполнил (а):

Чумаков Антон Сергеевич, 10Б

Руководитель:

Пяткина Галина Александрова

подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензент:

ФИО (указать должность, при наличии – указать ученую степень, ученое звание)

подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва

2017/2018 уч.г.

Оглавление

**Введение…………………………………………………………………...…..3**

**Раздел 1. Основы цифровой стеганографии**

§1. Определение и принципы цифровой стеганографии…………...…….…5

§2. Задачи стеганографии………………….........................................……….6

§3. Классификация алгоритмов цифровой стеганографии………………..10

§4. Метод встраивания ЦВЗ…………………………………………………11

§5. Метод LSB........…..………………………………………………………13

§6. Эхо-методы……………………………………………………………….17

§7. Методы стеганографии для звуковых файлов……...…………………..18

§8. Алгоритмы, связанные с особенностями форматов [файлов](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB)......…..…..22

**Раздел 2.** **Разработка модели сокрытия информации в тексте……….25**

**Заключение…………………………………………………………………..30**

**Список литературы…………………………………………………………31**

**Введение**

Мы живем в мире, в котором одним из важнейших ресурсов является информация. В наше время личные данные, сообщения и интеллектуальная собственность охраняются порой лучше, чем материальные богатства. Но каким образом происходит их защита? Этим занимается такая научная область, как стеганография.

Стеганография (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). Однако, этим дело не ограничивается. С помощью своих методов она решает такие задачи, как: защита авторских прав, встраивание водяных знаков, подтверждение достоверности переданной информации и многое другое.

Защита информации в наш информационный век - это одна из основных проблем. Решение задач совместного обеспечения конфиденциальности, доступности и целостности информации достигается применением криптографических и стеганографических методов ее защиты. Это и есть актуальность моего диплома.

К сожалению, не смотря на огромную пользу стеганографии  многие люди, в том числе и я, практически ничего не знают об этой методике защиты информации и не представляют, как она работает. Это незнание и является проблемой моего исследования.

Целью моего диплома является изучение цифровой стеганографии, её основные принципы и методов, а также построение модели сокрытия информации.

Для достижения данной цели мною поставлены следующие задачи:

* изучить информацию по теме компьютерной стеганографии, в частности цифровых водяных знаков
* систематизировать полученную информацию в соответствии с целью диплома
* написать единый текст
* смоделировать один из способов сокрытия информации

В своем дипломе я хочу рассмотреть:

* основы цифровой стеганографии
* методы цифровой стеганографии
* цифровые водяные знаки

Мой диплом будет состоять из оглавления, введения, теоретической части, практической части, заключения и списка литературы. В теоретической части я рассмотрю основы компьютерной стеганографии, а также цифровые водяные знаки. В практической части я разработаю в Delphi проект, моделирующий один из способов сокрытия информации, а именно сокрытия текста в тексте.

**Раздел 1. Основы цифровой стеганографии**

**§1. Определение и принципы цифровой стеганографии**

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

Каковы принципы цифровой стеганографии? В современной цифровой стеганографии можно выделить четыре основных положения:

* Методы скрытия должны обеспечивать аутентичность и целостность файла.
* Предполагается, что противнику полностью известны возможные стеганографические методы.
* Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации - ключа.
* Даже если факт скрытия сообщения стал известен противнику, извлечение самого секретного сообщения должно представлять сложную вычислительную задачу.

**§2. Задачи стеганографии**

В настоящее время стеганографические системы активно применяются для решения различных задач. Давайте рассмотрим их более подробно.

Во-первых, данные системы используются для незаметной передачи информации. Это классическая задача стеганографии. Она не требует пояснений.

Во-вторых, с помощью стеганографических систем можно не только скрытно передавать информацию, но и хранить её. Данная задача реализуется на носителях информации, а не в каналах связи. Причем многие носители обладают большой избыточностью, которую можно использовать. Похожей задачей является недекларированное хранение информации.

Многие информационные ресурсы позволяют хранить данные только определенного вида. Однако можно использовать стеганографию для хранения данных в других форматах.

Ещё стеганографические системы можно использовать для защиты исключительного и авторского прав. Благодаря данным системам существует возможность определить уникальный идентификатор покупки, дату/время покупки и другую информацию. С их помощью можно защитить каждую копию контента от несанкционированной публикации, продажи или использования.

Технология защиты подлинности документов может быть такая же, как и для защиты авторского права. Только в данном случае стеганография используется не для подтверждения авторства, а для подтверждения подлинности документа. Документ, не содержащий стеганографические водяные знаки считается «ненастоящим», поддельным.  
 В системе электронного документооборота можно использовать индивидуальный отпечаток внутри \*.odt, \*.docx и иных документах при работе с ними пользователем. Для этого должны быть написаны специальные приложения и/или драйверы, которые установлены и работают в системе. Если данная задача выполнена, то с помощью индивидуального отпечатка можно будет опознать, кто работал с документом, а кто нет. В данном случае стеганографию нельзя делать единственным критерием, но как дополнительный фактор идентификации участников работы с документом она может быть полезна.  
 Стеганография может быть применима для предотвращения утечек информации. В отличие от индивидуального отпечатка, в данном применении стеганографии при создании документа, содержащий конфиденциальный характер, вкрапляется определенная метка. При этом метка не изменяется, вне зависимости от количества копий и/или ревизий документа. Для того, чтобы извлечь метку необходим стегоключ. Стегоключ, разумеется, держится в тайне. DLP-система, перед одобрением или отказом выдать документ вовне, проверяет наличие или отсутствие водяного знака. Если знак присутствует, то система не разрешает отправлять документ вовне системы.

Стеганография может быть применима для доставки какого-либо управляющего сигнала системе. Если система может находится в различных состояниях и мы желаем, чтобы противник даже не догадался о том, что система перешла в другое состояние, мы можем воспользоваться стеганографией. Использование только криптографии, без стеганографии, может дать противнику информацию о том, что что-то изменилось и спровоцировать его на нежелательные действия. Данная задача невероятно актуальна в военной сфере. Данная задача может быть актуальной и для преступных организаций. Соответственно, правоохранительные органы должны быть вооружены определенной теорией по данному вопросу и способствовать развитию программ, алгоритмов и систем по противодействию данного применения стеганографии.  
 Стегосообщение может содержать данные, подтверждающие корректность передаваемых данных контейнера. Задача подтверждения достоверности является актуальной, если противник имеет необходимость подделать данные контейнера; по этой причине данное применение не нужно путать с защитой подлинности документов. Данная проблема имеет множество классических решений, в том числе криптографических. Использование стеганографии является ещё одним способом решить данную проблему.  
 Существует ряд документов, для которых важна целостность. Ее можно осуществить резервированием данных. Порой существует необходимость иметь документы в таком виде, чтобы невозможно было одну информацию отделить от другой информации. Это могут быть медицинские снимки, содержащие информацию об имени, фамилии и иных данных пациента, или скриншот игры WoW, в который внедряется имя пользователя, время снятия и адрес сервера. Стеганография также в состоянии справиться с данной задачей.

Стеганографическое отслеживание в некоторой степени похоже на индивидуальный отпечаток, только цель стоит иная — поймать злоумышленника, который «сливает» информацию. В реальном мире можно привести примером «меченые деньги». Они используются правоохранительными органами, для того чтобы преступник, получивший деньги за какую-либо незаконную деятельность, не мог бы потом заявить, что эти деньги были у него до сделки.

Методы стеганографии для каждого типа информации свои. Наиболее популярный тип, используемый стеганографией – изображение.

Стеганографические методы, используемые при работе с изображениями, делятся на две группы.

Методы первой группы предполагают небольшую модификацию изображений. Данные методы обычно используют побитную модификацию, например, изменение наименьшего по значению бита. Эти методы относят к числу простых, они легче поддаются декодированию и допускают потерю информации при тех или иных преобразованиях файла-носителя, скажем, при сжатии. Из трех наиболее популярных алгоритмов сжатия изображений: BMP, GIF и JPEG — чаще используют первые два. Они отличаются меньшими потерями.

Методы второй группы используют трансформацию изображений. В методах этой группы используют тригонометрические преобразования или наложения, незаметные для глаз. Эти методы более устойчивы, вложенная информация не теряется при преобразованиях, поэтому их чаще всего применяют при создании цифровых водяных знаков. Обычно при этом используются файлы формата JPEG.

Метод скрытых гарнитур шрифтов в некоторой степени похож на побитную модификацию изображений. Делаются малозаметные искажения в очертаниях букв, которые будут нести смысловую нагрузку. Так, в документ Microsoft Word можно вставить похожие символы, содержащие скрытое послание.

Сообщения можно передавать и в звуковом формате. Их можно послать, используя шумовое кодирование. Оно будет трудно определимо на фоне аппаратных шумов в телефонной линии или сетевых кабелях.

**§3. Классификация алгоритмов цифровой стеганографии**

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп:

* Работающие с самим цифровым сигналом. Например, метод LSB.
* «Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания цифрового водяного знака (далее ЦВЗ).
* Использование особенностей форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие не используемые зарезервированные поля файла.

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.

**§4. Метод встраивания ЦВЗ**

Цифровой водяной знак – это совокупность невидимых меток, которые носят уникальный цифровой код. В нем и зашифрованы различные данные: авторские права, идентификационный номер, управляющую информацию. Наиболее удобными для защиты с его помощью являются неподвижные изображения, аудио и видео файлы.

Основные требования, предъявляемые к цифровым водяным знакам: надёжность и устойчивость к искажениям, незаметности, робастности к обработке сигналов (робастность — способность системы к восстановлению после воздействия на нее внешних/внутренних искажений, в том числе умышленных). Они имеют небольшой объём, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Перед помещением данного знака в контейнер, водяной знак нужно преобразовать к подходящему виду. Первичную обработку часто производят с использованием ключа — для повышения секретности. Потом водяной знак «укладывается» в контейнер (например, путем изменения младших значащих бит). Здесь используются особенности восприятия изображений человеком, ведь известно, что изображения имеют огромную психовизуальную избыточность. Глаза человека подобны низкочастотному фильтру, который пропускает мелкие элементы изображения. Наименее заметны искажения в высокочастотной области изображений. Внедрение цифрового водяного знака также должно учитывать свойства восприятия человека.

Во многих стегосистемах для записи и считывания ЦВЗ используется ключ. Он может предназначаться для ограниченного круга пользователей или же быть секретным. Не существует таких стегосистем, в которых бы при считывании водяного знака требовалась другая информация, нежели при его записи. В стегодетекторе происходит обнаружение ЦВЗ в защищённом им файле, который, возможно, мог быть изменён. Эти изменения могут быть связаны с воздействиями ошибок в канале связи, либо преднамеренными помехами. При этом задача обнаружения и считывания стегосообщения уже не представляет сложности, но не учитывает двух факторов: неслучайности сигнала контейнера и запросов по сохранению его качества. Учет этих параметров позволит строить более качественные стегосистемы. Для обнаружения факта существования водяного знака и его считывания используются специальные устройства — стегодетекторы. Для вынесения решения о наличии или отсутствии водяного знака используют, к примеру, расстояние по Хэммингу, взаимокорреляцию между полученным сигналом и его оригиналом. В случае отсутствия исходного сигнала в дело вступают более изощренные статистические методы, которые основаны на построении моделей исследуемого класса сигналов.

**§5. Метод LSB**

LSB (Least Significant Bit, наименьший значащий бит) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.  
 Суть метода заключается в следующем: Допустим, имеется 8-битное изображение в градациях серого. 00h (00000000b) обозначает черный цвет, FFh (11111111b) — белый. Всего имеется 256 градаций (28). Также предположим, что сообщение состоит из 1 байта — например, 01101011b. При использовании 2 младших бит в описаниях пикселей, нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого — на 1/255, второго и третьего — на 2/255 и четвертого — на 3/255. Такие градации, мало того что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Для простоты описания можно рассмотреть  принцип работы этого метода на примере 24-битного растрового RGB-изображения. Одна точка изображения в этом формате кодируется тремя байтами, каждый из которых отвечает за интенсивность одного из трех составляющих цветов (в соответствии с рисунком 1).

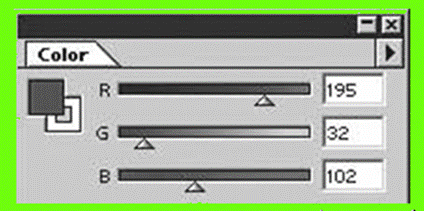
[](http://crypto-blog.ru/wp-content/uploads/2010/09/stego4.png)

Рис. 1. Представление цвета пикселя в 24-битном bmp-изображении

              В результате смешения цветов из красного (R), зеленого (G) и синего (B) каналов пиксель получает нужный оттенок. Чтобы нагляднее увидеть принцип действия метода LSB, распишем каждый из трех байтов в битовом виде. Младшие разряды (на рисунке они расположены справа) в меньшей степени влияют на итоговое изображение, чем старшие. Из этого можно сделать вывод, что замена одного или двух младших, наименее значащих битов, на другие произвольные биты настолько незначительно исказит оттенок пикселя, что зритель просто не заметит изменения.

              Допустим, нам нужно скрыть в данной точке изображения шесть бит: 101100. Для этого разобьем их на три пары и заместим ими по два младших бита в каждом канале (в соответствии с рисунком 2).

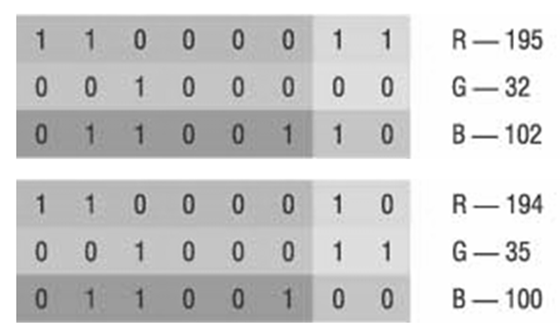
[](http://crypto-blog.ru/wp-content/uploads/2010/09/stego5.png)

Рис. 2. Исходные и измененные компоненты цвета

В результате мы получим новый оттенок, очень похожий на исходный (см. рис. 3). Эти цвета трудно различить даже на большой по площади заливке. Как показывает практика, замена двух младших битов не воспринимается человеческим глазом. В случае необходимости можно занять и три разряда, что весьма незначительно скажется на качестве картинки.

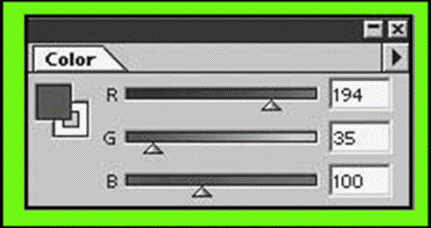
[](http://crypto-blog.ru/wp-content/uploads/2010/09/stego6.png)

Рис. 3. Цвет пикселя с внедренными данными

Теперь можно посчитать полезный объем такого RGB-контейнера. Занимая два бита из восьми на каждый канал, мы будем иметь возможность спрятать три байта полезной информации на каждые четыре пиксела изображения, что соответствует 25 % объема картинки. Таким образом, имея файл изображения размером 200 Кбайт, мы можем скрыть в нем до 50 Кбайт произвольных данных так, что невооруженному глазу эти изменения не будут заметны.

Все BMP контейнеры нужно разделить на два класса: «чистые» и зашумленные. В «чистых» картинках прослеживается связь между младшим битом, который подвергается изменениям, и остальными 7-ю битами элементов цвета, а также видна зависимость самих младших битов между собой. Внедрение сообщения в «чистую» картинку разрушает существующие зависимости, что очень легко выявляется наблюдателем. Если же картинка зашумлена (например, получена со сканера или фотокамеры), то определить вложение становиться намного сложнее.  Таким образом, в качестве файлов-контейнеров для метода LSB рекомендуется использовать файлы, которые не были созданы на компьютере изначально.

Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных.

Обнаружение LSB-кодированного стего осуществляется по аномальным характеристикам распределения значений диапазона младших битов отсчётов цифрового сигнала.  
 Все методы LSB являются, как правило, аддитивными (A17, L18D). Другие методы скрытия информации в графических файлах ориентированы на форматы файлов с потерей, к примеру, JPEG. В отличие от LSB они более устойчивы к геометрическим преобразованиям. Это получается за счёт варьирования в широком диапазоне качества изображения, что приводит к невозможности определения источника изображения.

**§6. Эхо-методы**

Эхо-методы применяются в цифровой аудиостеганографии и используют 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 человеческое ухо не может уже отличить эти два сигнала. Наличие этой точки сложно определить, и она зависит от качества исходной записи, слушателя. Чаще всего используется задержка около 1/1000, что вполне приемлемо для большинства записей и слушателей. Для обозначения логического нуля и единицы используется две различных задержки. Они обе должны быть меньше, чем порог чувствительности уха слушателя к получаемому эху. Если из исходного сигнала можно выделить только одно эхо, то может быть закодирован только один бит секретной информации. Следовательно, перед началом процесса кодирования исходный сигнал разбивается на блоки. После выполнения кодирования блоки объединяются вместе, чтобы образовать окончательный выходной сигнал.

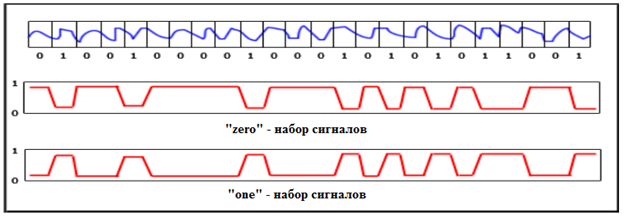


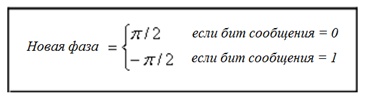
Рисунок 4. Пример работы эхо-метода.

Главные преимущества эхо-метода – это высокая скорость передачи данных по сравнению с другими методами. Также эхо-методы устойчивы к амплитудным и частотным атакам, но неустойчивы к атакам по времени.

**§7. Методы стеганографии для звуковых файлов**

Фазовое кодирование (phase coding, фазовое кодирование) — также применяется в цифровой аудиостеганографии. Метод фазового кодирования работает путем замены фазы исходного звукового сегмента на опорную фазу, которая представляет собой секретную информацию. Остальные сегменты фазы корректируются для сохранения определенной фазы между сегментами. С точки зрения отношения сигнала к шуму, фазовое кодирование является одним из наиболее эффективных методов кодирования. Когда происходит резкое изменение фазового соотношения между каждой частотной составляющей, шумы становятся заметными. Тем не менее, если фазу модифицировать не сильно, то человеческое ухо не распознает каких-либо изменений. Исходя из этого можно сказать, что этот метод основан на том, что изменения, внесенные в аудиофайл, будут незаметны для человеческого слуха.

Фазовое кодирование включает в себя следующие шаги:

1. Разделить оригинальный звуковой сигнал на более мелкие сегменты таким образом, чтобы их общая длина была равна длине сообщения;
2. Создается матрица фаз с помощью дискретного преобразования Фурье;
3. Вычисляется разность фаз между соседними сегментами;
4. В связи с тем, что фазовые сдвиги между двумя соседними сегментами могут быть легко обнаружены, в стегосигнале должны быть сохранены разности фаз. Поэтому секретное сообщение встраивается только в фазу первого сегмента: 
5. Используя новую фазу первого сегмента создается новая матрицы фаз и разницы между ними;
6. Звуковой сигнал восстанавливается путем применения обратного дискретного преобразования Фурье с использованием новой матрицы и исходной матрицы величин, после чего звуковые сегменты сцепляются.

Получатель должен знать длину сегмента, чтобы извлечь секретное сообщение из звукового файла. После чего получатель с помощью дискретного преобразования Фурье может извлечь секретную информацию.

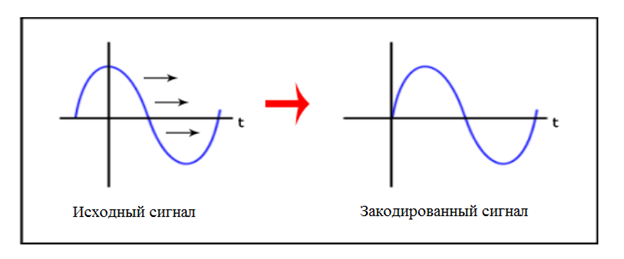


Рисунок 5. Фазовое кодирование.

В аудио стеганографии метод расширенного спектра пытается передать секретные сведения по спектру частот звукового сигнала. Этот метод чем-то схож с методом LSB, который передает биты сообщения случайным образом по всему звуковому файлу. Тем не менее, в отличие от способа LSB, метод расширенного спектра распространяет секретную информацию по спектру частот звукового файла, используя код, который не зависит от фактического сигнала. В результате конечный сигнал занимает полосу пропускания, которая размером больше, чем требуемый размер для передачи.

Метод расширенного спектра может внести вклад в повышение производительности по сравнению с методами LSB, фазового и четного кодирований путем умеренной скорости передачи данных и высоким уровнем устойчивости. Однако, метод расширенного спектра имеет один существенный недостаток – он может вносить шум в аудиофайл. Схема работы метода на рис.6.

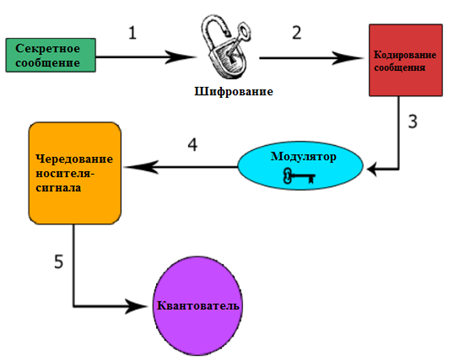


Рисунок 6. Схема работы метода расширенного спектра.

Четное кодирование является одним из самых надежных способов аудио стеганографии. Вместо того, чтобы разбивать сигнал в отдельных выборках, этот метод разбивает сигнал на отдельные части и встраивает каждый бит секретного сообщения в четный бит. Если четный бит в выбранной области не подлежит кодированию в секретный бит, то процесс инвертирует младший бит одной из выборки данной области. На рис.7 представлена процедура такого кодирования.

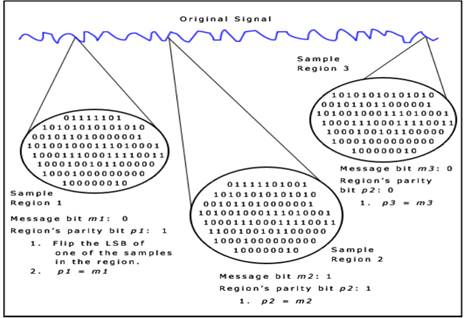


Рисунок 7. Четное кодирование.

**§8. Алгоритмы, связанные с особенностями форматов**[**файлов**](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB)

Этот метод прост в реализации и зачастую не требует специального программного обеспечения. Многие распространённые методы цифровой стеганографии используют графические или звуковые файлы в качестве носителей-контейнеров. Следовательно, будет полезно сделать обзор кодирования графических и звуковых файлов перед обсуждением того, как стеганография и стегоанализ работают с этими контейнерами. Рисунок 8 показывает цветовой куб модели RGB, обычное средство для представления конкретного цвета по относительной интенсивности его трех составляющих цветов – красного, зеленого и синего – каждый со своей собственной осью. Отсутствие всех цветов даёт черный цвет, показанный как пересечение трех цветных осей в нулевой точке. Смесь 100 процентов красного, 100 процентов синего, и отсутствия зеленого цвета образует пурпурный цвет; голубой цвет – это 100 процентов зеленого и 100 процентов синего цвета без красного; а соединение 100 процентов зеленого и 100 процентов красного цвета без синего образуют желтый. Белый цвет – это наличие всех трех цветов.

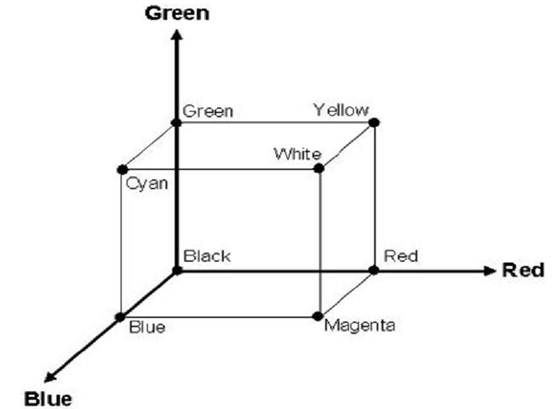


Рис. 8. Цветовой куб модели RGB

Рисунок 9 показывает уровни интенсивности (яркости) модели RGB нескольких различных цветов. Каждый компонент модели RGB задан одним байтом, поэтому значения каждой интенсивности цвета могут меняться от 0 до 255. Данный конкретный оттенок обозначен уровнем красного 191, уровнем зеленого 29 и уровнем синего 152. Затем, один пиксель пурпурного цвета будет закодирован, используя 24 бита. Эта 24- битовая схема кодирования поддерживает 16 777 216 (2^24) уникальных цветов.

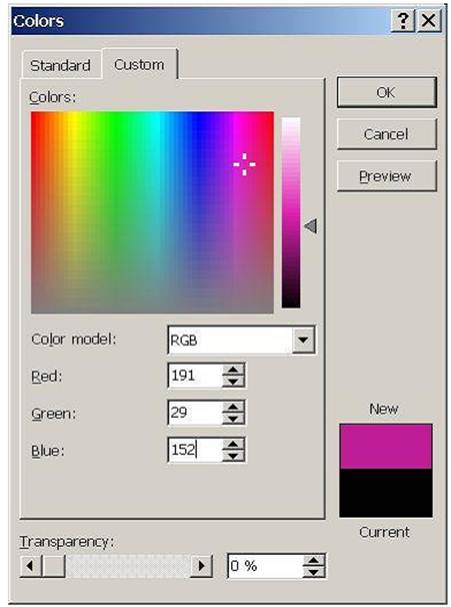


Рис. 9. Это диалоговое окно выбора цвета показывает уровни красного, зеленого и синего (RGB) данного выбранного цвета

Большинство цифровых графических приложений сегодня поддерживает 24-битовую реалистичную цветопередачу, где каждый элемент изображения (пиксел) закодирован в 24 битах, включая три байта модели RGB, как описано выше. Другие приложения кодируют цвет, используя восемь битов/пикселей. Эти схемы также используют 24- битовую реалистичную цветопередачу, но применяют палитру, которая определяет, какие цвета используются в изображении. Каждый пиксел закодирован в восьми битах, где значение указывает на 24-битовую запись цвета в палитре. Этот метод ограничивает уникальное число цветов в данном изображении до 256 (2^8).

**Раздел 2.** **Разработка модели сокрытия информации в текстe**

В первом разделе мною были описаны различные методы стеганографии. В этом разделе я разработаю модель сокрытия текста в тексте. Средой разработки я выбрал Delphi. Она проста в написании кода, а также весьма наглядно представляет результат.

Алгоритм, по которому будет выполняться скрытие, схож по своей идее с методом LSB. В обоих случаях работа ведется с битами сообщения. Только вот в моей модели занесение информации в контейнер производится не заменой младших разрядов, а добавлением (или нет) пробела после конца предложения. Концом предложения модель считает точку, после которой идет пробел. Delphi использует кодировку ASCII, в которой каждый символ представлен восемью битами, поэтому в моей модели каждая восьмерка пробелов и пропусков представляет собой один символ.

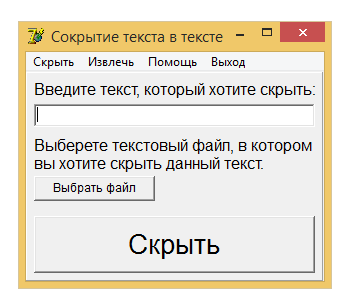
Теперь перейдем к самой программе. Первое окно (рис.10) предназначено для скрытия сообщения в тексте.

Рис. 10. Окно скрытия

В строке для ввода пишем текст, который хотим скрыть, а после этого выбираем текст-контейнер в формате txt (рис. 11 и 12 соответственно).

Рис. 11. Ввод сообщения

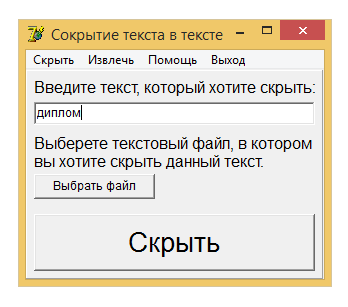
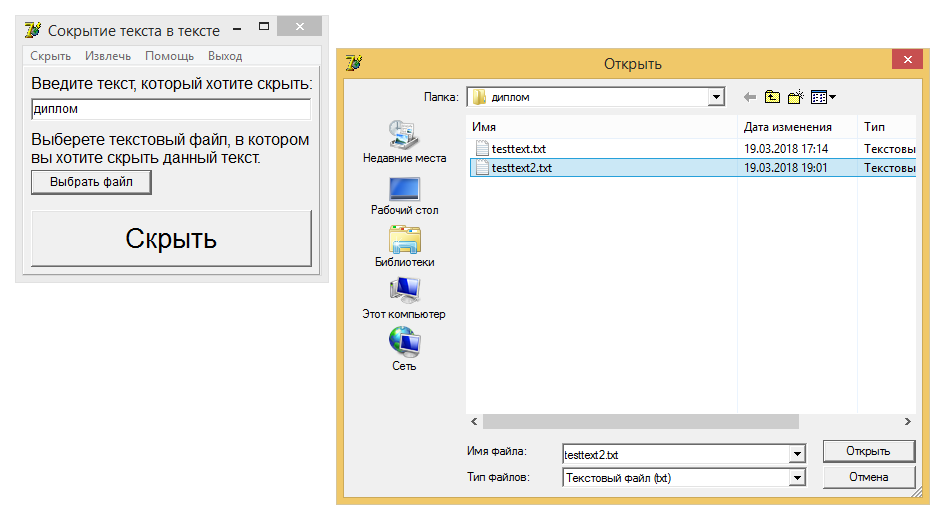


Рис. 12. Выбор текста-контейнера

После этого жмем кнопку “Скрыть” и получаем текст со скрытым в нем сообщении (рис. 13).

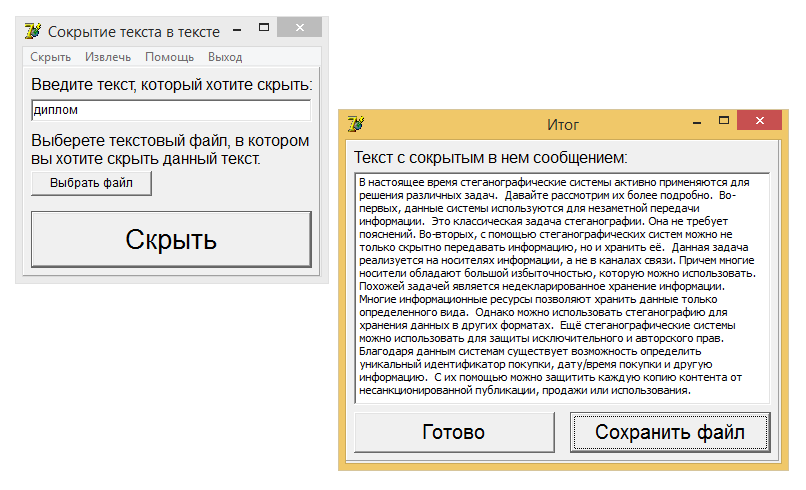


Рис. 13. Текст со скрытым сообщением

Помимо возможности скрыть текст, мы также можем его извлечь. Для этого переходим в раздел “Извлечь” и выбираем текстовый файл с сокрытым сообщением (рис. 14).

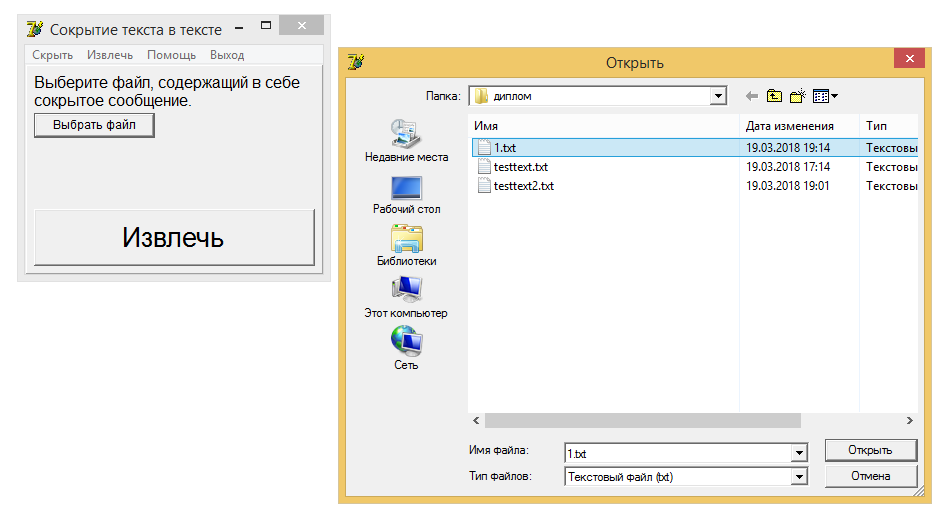


Рис. 14. Выбор файла со скрытым сообщением

После выбора файла остается лишь нажать на кнопку “Извлечь” и увидеть открывшееся окно с извлеченным сообщением (рис. 15).

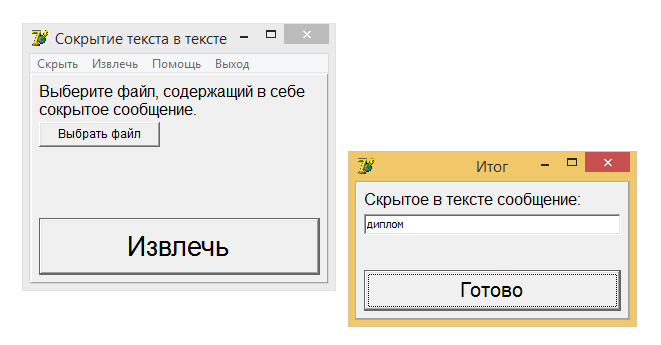


Рис. 15. Окно с извлеченным сообщением

Ниже я приведу блок-схемы для двух основных кнопок: “Скрыть” и “Извлечь”. Для понимания этих схем рассмотрим основные переменные, которые в них используются. Переменные binC и binN работают с двоичным кодом. Переменная k содержит в себе код очередного символа в 10-ой сс. TextC и textF при скрытии представляют собой изначальный и “выходной” текст соответственно (при изъятии они меняются местами).

Первая блок-схема описывает алгоритм работы кнопки “Скрыть”.

textC := Edit1.Text;

Length(textC)<>0

textF:= copy(textC,1,1);

Delete(textC,1,1);

binC := binC + textF;

binC := '';

textF := '';

k := Ord(textF[1]);

Перевод k в 2 систему счисления и ее запись textF.

Нет

Да

Length(binC)<>0

textF := '';

binN := binC[1];

binN = '0'?

binN := '';

binN := ' ';

Поиск конца предложения и запись после него binN.

Form3.Memo1.Text := textF;

Form3.ShowModal;

Delete(binC,1,1);

Вторая блок-схема описывает алгоритм работы кнопки “Извлечь”.

textF := '';

Поиск конца предложения

Есть доп. пробел?

Есть необработанные предложения?

textF := textF + '1';

textF := textF + '0';

textC := textF;

countPlaces := Length(textC) mod 8;

Length(textC) > countPlaces

Form4.Edit1.Text := Form4.Edit1.Text + Chr(k);

Form4.ShowModal;

Перевод первых 8 символов textC в число, а затем запись его в 10 сс. в переменную k.

Delete(textC,1,8);

Да

Нет

Данная модель тестировалась на людях, не знающих алгоритма сокрытия. По итогам обнаружилось, что для обывателя с виду текст-контейнер с сообщением и без него неразличимы.

**Заключение**

Одна из основных проблем в наш информационный век - это защита информации. Решение задач совместного обеспечения конфиденциальности, доступности и целостности информации достигается применением криптографических и стеганографических методов ее защиты. Это и есть актуальность моего диплома.

Проблемой моего исследования являлось незнание многих людей об этой актуальной методике защиты информации и том, как она работает.

В моем дипломе я изучил основы цифровой стеганографии с её основными принципами и методами, а также построил модель сокрытия информации. Для написания диплома я изучил информацию по теме компьютерной стеганографии, в частности цифровых водяных знаков, и систематизировал её в соответствии с поставленной целью.

В теоретической части мной были описаны основы компьютерной стеганографии и рассмотрены различные методы стеганографии, такие как: метод встраивания ЦВЗ, метод LSB, эхо-методы и методы для звуковых файлов.

В практической части я разработал в Delphi программу, моделирующую один из способов сокрытия информации. Для этого был придуман и продуман алгоритм, позволяющий скрывать текст в тексте. Исходя из получаемого в процессе работы модели результата, можно утверждать, что он соответствует особенностям стеганографии (не заметен факт наличия сообщения).

Подводя итог, я считаю, что поставленные мною задачи были выполнены: методы стеганографии рассмотрены, текст написан, модель для сокрытия текста в тексте создана. Из всего этого я делаю вывод, что цель диплома была достигнута.

**Список литературы**

* Нигматуллин Э.В., Ковырзина К.С. ОБЗОР МЕТОДОВ ЦИФРОВОЙ АУДИО СТЕГАНОГРАФИИ // Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. XLII междунар. студ. науч.-практ.конф. №5(41): <https://sibac.info/studconf/tech/xlii/54331>
* Васина Т. С. // Обзор современных алгоритмов стеганографии: <http://technomag.bmstu.ru/doc/370605.html>
* Аграновский А. В., Балакин А. В., Грибунин В. Г. Стеганография, цифровые водяные знаки и стеганоанализ - М.: Издательский дом “Вузовская книга”, 2009.
* Статья о стеганографии: http://shkolnie.ru/informatika/6169/index.html