Департамент образования города Москвы

Государственное бюджетное общеобразовательное учреждение города Москвы «Гимназия №1505

«Московская городская педагогическая гимназия-лаборатория»»

**РЕФЕРАТ**

**на тему**

**Стеганография**

Выполнил:

Чумаков Антон Сергеевич

Руководитель:

Пяткина Галина Александровна

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись руководителя)

Рецензент:

ФИО рецензента

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись рецензента)

 Москва

 2016/2017 уч.г.

Оглавление

|  |  |  |
| --- | --- | --- |
| 1 | Введение…………………………………………………………… | 3 |
| 2 | Основная часть……………………………………………………. | 4 |
|  | 2.1 Глава I. Основы стеганографии……………………………… | 4 |
|  | 2.2 Глава II. Компьютерная стеганография……………………… | 9 |
|  | 2.3 Глава III. Водяные знаки. Что это такое и зачем они………. | 13 |
| 3 | Заключение………………………………………………………… | 19 |
| 4 | Список литературы……………………………………………….. | 20 |

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.

 Таким образом, сейчас, когда наблюдается быстрое развитие науки и технологий, требуется ознакомление с основами современной компьютерной стеганографии целого круга специалистов. К сожалению, имеющиеся публикации, посвященные стеганографии, не в состоянии в полной мере обеспечить указанные потребности. Это и есть актуальность моего реферата.

 Итак, проблемой моего реферата является отсутствие большого количества специалистов в области стеганографии, вследствие неполноценных источников.

 Цель реферата – изучить методы стеганографии (как до изобретения компьютеров, так и после), её основные принципы и области применения.

 Для достижения поставленной цели определены следующие задачи:

1. Изучить информацию по данной теме
2. Систематизировать полученную информацию в соответствии с целью работы
3. Описать методы, принципы и области применения стеганографии
4. Написать единый текст

Глава I.

Основы стеганографии

 Стеганография – это искусство и наука о способах передачи (хранения) скрытой информации, при которых скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации (Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. М., 2009. С.26). Для этой цели используются различные приёмы. Это может быть:

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

 В стеганографии можно выделить несколько основных понятий. Это контейнер, сообщение и ключ.

 Контейнер – это несекретные данные, уже в которых сокрыта определенная информация (там же, с.27). Имеет место замена этого термина на название “стего”. Контейнер может быть пустым или заполненным. Пустой контейнер – контейнер, в котором пока отсутствует скрытые данные. Заполненным называют контейнер, который содержит скрытые данные. Пространством сокрытия называются участки контейнера, в которых стеганосистема может скрыть информацию. Это могут биты, поля и так далее. Используемое пространство сокрытия представляет собой совокупность областей пространства сокрытия, в которых действительно произошло сокрытие в процессе работы стеганосистемы.

 Сообщение – как раз та информацию, которую нам необходимо скрыть (там же). Всевозможные сообщения объединяются в пространство сообщений. Сообщения содержатся в контейнерах. С сообщениями возможны две операции: внедрение и извлечение. Внедрение (сокрытие) – использование прямого преобразования к определенным сообщению, контейнеру и ключу (смотри ниже). Под извлечением понимают действие, обратное тому, что производилось при внедрении.
 И последнее определение – ключ. Он известен только законному пользователю, и определяет конкретный вид алгоритма сокрытия.

 Стеганографическая система – это совокупность контейнеров, сообщений, ключей и связывающих их преобразований (там же, с.28).

 Сторону стеганографии, пытающуюся раскрыть стеганографическую систему называют стеганоаналитиком. Задача стеганоаналитика состоит в раскрытии стеганографической системы и определения самого сообщения. Под раскрытием (взломом принято понимать нахождения её уязвимости, с помощью которой можно определить факт сокрытия информации в контейнере, и возможность доказать это с высокой степенью достоверности.

 Процесс стеганоанализа можно разделить на два действия:

1. Определение наличия сообщения в контейнере
2. Извлечение содержания скрытого сообщения

 Попытка определить наличие сообщения и его смысла называют атакой на стеганографическую систему. Данные атаки делятся на несколько классов (там же, с.29):

* Атаки со знанием модифицированного контейнера, в данном случае стеганоаналитик обладает только модифицированным контейнером. С его помощью он пытается определить наличие скрытого сообщения. Этот вид атак – базовый из всех, по которым оцениваются стеганосистемы.
* Атаки со знанием немодифицированнного 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 скрытия сообщения в дальнейшем в зависимости от наличия однажды перехваченного контейнера и раскрытого сообщения.
* Атаки с выбором сообщения, в этом случае стеганоаналитик имеет возможность указывать, какие именно сообщения будут сокрыты, но при этом не имеет возможности указать контейнер, который будет для этого использоваться. Устойчивость к этому классу атак характеризует устойчивость самой системы к перехвату и отслеживанию сообщений, посланных с использованием одного и того же контейнера. Данный вид атак иногда также позволяет определить тип применённой стеганографической системы.
* Атаки с выбором контейнера, так же как и предыдущие 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 используют для модификации скрытой информации, либо имитации такой передачи.
* Атаки по противодействию передаче информации используют для уничтожения скрытой информации и снижения пропускной способности каналов скрытой передачи данных.

 Стеганоаналитик, не модифицирующий доступные ему для анализа данные, носит название пассивного нарушителя(там же, с.30). Стеганоаналитик, который может вносить изменения в передаваемые по каналу данные, называется активный нарушитель(там же). Атаки по подмене, имитации и противодействию характерны только для активного нарушителя. Остальные виды атак присущи только пассивным нарушителям.

 Человечеству были известны способы скрывать информацию, и до изобретения компьютеров.

 Уже в V веке до н.э. люди умели оправлять скрытые сообщения. Так как в то время было распространено рабовладение, то для пересылки использовались рабы. Им брили голову, писали на ней послание, ждали когда волосы отрастут обратно, а затем отправляли его к адресату.

 В Китае военные сообщения писались на кусках тончайшего шелка и закатывались в маленький шар, который глотал посыльный. В Риме и Греции сообщения вырезались на кусочках древесины, которые потом опускались в воск, чтобы закрыть запись.

 За свою историю человечество изобрело множество различных способов скрывать сообщения. Наиболее известный и давно использующийся – симпатические чернила. Их особенность в том, что после написания они исчезают. Сделать их обратно видимыми можно только путем специальной обработки. Данный метод применялся в Древнем Риме, на Древнем Востоке, России и так далее.

 Широкое распространение и применение в стеганографии получил метод микроточки. Под микроточкой понимают уменьшенное более чем в сто раз фотоизображение обычного документа. Существует две разновидности микроточки: обычная (0,8 мм в диаметре) и ультра-микроточка (менее 0,2 мм в диаметре).

 Но не будем путать стеганографию и криптографию. Хоть между ними существует только одно отличие, но оно весьма важное.

 Перед тем, как обозначать его, разберемся, что такое криптография. Это наука о математических методах обеспечения конфиденциальности и аутентичности информации[[1]](#footnote-1). Чаще всего результатом данных методов является зашифрованное послание.

 В это и состоит отличие криптографии от стеганографии. Информацию, которую скрывают первой наукой, может увидеть любой человек в виде шифра, однако лишь тот, кто знает ключ, сможет извлечь её. Стеганография, в отличие от криптографии, скрывает сам факт передачи данных как таковой. Ведь чаще всего их переносчиками являются самые обыкновенные и ничем не примечательные изображения, документы и так далее.

Глава II.

Компьютерная стеганография

 В предыдущей главе мы дали определения всем основным понятиям в стеганографии, рассмотрели её методы до изобретения компьютеров и выявили её отличия от криптографии. Но каковы принципы нынешней, компьютерной, стеганографии?

 В современной компьютерной 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.

 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. Подробнее о водяных знаках написано в третьей главе.
 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.

 В этой главе я упомянул водяные знаки. Это один из наиболее распространенных примеров стеганографии. Рассмотрим их подробнее в 3 главе.

Глава III.

 Водяные знаки. Что это такое и зачем они[[2]](#footnote-2)

 Каждодневно человек на протяжении всей своей жизни сталкивается с водяными знаками. Наиболее распространенный вариант – те, что наносят на бумагу при производстве денег, во избежание подделок. Водяной знак – невидимое изображение, нанесенное специальной технологией на бумагу, из которой планируется печать денег, марок или прочей продукции. Данное изображение становиться хорошо заметным только при просмотре на просвет или же через ультрафиолет.

 Авторство водяных знаков приписывают итальянцам, Поскольку именно они были первыми масштабными производителями бумаги были итальянцы, которой снабжали своей продукцией весь континент.

 Бумага в XIII столетии производилась из тряпок, которые обрабатывали предварительно известью с целью выведения грязи или жира. Их тщательно вымачивали, в результате чего образовывалась густая масса похожая на кисель. Следующим этапом производства бумаги заключался в том, что опытные профессионалы данную массу разливали в специально подготовленные формы. Эти лотки мастерили из медной проволоки. Чем больше заливали жидкой консистенции, тем толще получалась бумага в результате. Лишняя вода стекала, а заготовку просушивали и обрабатывали клеем для придания бумаге прочности. Со временем мастера начали подставлять на дно формы проволочные фигурки. Таким образом, бумага в месте, где находилась фигурка, была немного тоньше, чем в иных местах, а после просушки рисунок отменно просвечивался на просвет. Так был изобретен водяной знак. Данный способ получил название ”филигрань”, в переводе с итальянского языка - тонкая работа, украшенная канителью. Вскоре вся бумага, производимая в Италии, помечалась водяными знаками.

 Со временем, когда металлические деньги стали отходить на второй план, данный способ оказался полезен для производства бумажных купюр. Даже до сегодняшнего дня водяные знаки становятся большим камнем преткновения для фальшивомонетчиков. Согласно статистике только до 15% фальшивых купюр, что выявляются, имеют водяные знаки с различной степенью достоверности.

 В России бумага с водяным знаком появилась намного позже – только в конце XVII века, а к середине XVIII данную технологию начинают применять в качестве главной защиты напечатанной бумаги от подделки. Ведь воспроизвести с точностью водяной знак на то время практически было невозможно. Как правило, для таких целей применялся знак с изображением герба, поэтому бумага и получила название гербовая. Впервые русская филигрань – двуглавый орел, как герб Российской Империи появилась на Дудергофской фабрике, что находилась неподалеку Петербурга в 1720 году.

 С середины XIX века все ценные бумаги, документы, деньги, облигации и акции предприятий печатаются только на бумаге с определенными водяными знаками.

 Водяные знаки, которые получают непосредственно при процессе производства бумаги принято называть натуральными или истинными. Существует четыре классических способа:

* ручной метод, в основу лег принцип описанный чуть выше. Водяной знак получается благодаря форме, дно которой устилали сеткой с узором знака;
* машинный способ – используются черпально-листовые машины, которые формируют лист аналогично к ручному черпанию.
* Водяные знаки, производимые с помощью круглосеточных бумагоделательных машин. Сетка цилиндра такого агрегата имеет нанесенной штамповкой или зафиксированный филигранный узор, который и отвечает за нанесения водяного знака. При этом знак производиться одновременно с формированием бумажного листа.
* Водяные знаки, производимые с помощью столовых бумагоделательных машин. При данном способе производства водяной знак предается на еще сырую бумажную прослойку посредством сеточного валика, который носит название дендироль. На его поверхность наносят узор способом штамповки сетки либо с помощью элементов филиграни.

 Все прочие методы получения различных видов водяных знаков лишь их имитируют, поэтому их выделяют отдельно от истинных водяных знаков. Формирование таких водяных знаков происходит за счет различных действий, в результате которых изменяется оптическая плотность уже готовой бумаги. Количество визуально наблюдаемых градаций (оттенков и плотностей), которые выделяются от основного фона как раз легли в основу классификации водяных знаков:

* Однотонные водяные знаки – это видимые на просвет либо темные, либо светлые изображения по сравнению с фоном бумаги;
* Двутоновые водяные знаки содержат в себе как темные, так и светлые части изображения по отношению к основному фону бумаги;
* Многотоновые водяные знаки – это изображения с постепенным переходом от темного оттенка к более светлому (иногда встречается их второе название – полутоновыми);
* Комбинированные водяные знаки – сочетают в себе элементы из предыдущих видов.

 Помимо описанной классификации водяные знаки различают также по размещению:

* водяные знаки на поле; их рисунок либо узор повторяется по фиксированному полю;
* локальные водяные знаки, находятся в определенном месте на купюре банкноты или страницы документа. В большинстве случаев они относятся к многотоновым изображениям и содержат постепенные изменения плотности. Чаще всего их называют полутоновыми, либо портретными, ведь их используют для отображения портретов персоналий, то есть лиц, изображенных на банкнотах;
* разновидностью локальных водяных знаков считают повторяющийся или полосовой знак. Это повторяющееся по вертикали или горизонтали одинаковое изображение. Также встречается чаще всего в виде портретов на банкнотах. Наглядным примером может послужить кроны Швеции или Норвегии.

 Несмотря на давнюю историю своего существования, водяной знак до сих пор является достаточно актуальным. Хотя банкноты имеют несколько уровней защиты, водяной знак играет решающую роль от подделок банкнот в разных стран мира. Бумагу с водяными знаками также широко применяют при печати дипломов, ценных бумаг, документов и даже железнодорожных билетов. Все, что сегодня необходимо защитить от подделки, производят с использованием водяных знаков.

 Но нельзя и не сказать о последнем слове науки – цифровые водяные знаки. Их предназначение – защитить кино и фото-продукцию от незаконного распространения. Правда, название ”водяной знак” такой код получил только традиционно, поскольку он не имеют наималейшего отношения к воде.

 Цифровой водяной знак (далее ЦВЗ) – 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.

Заключение

 В наши дни, информация – весьма ценный ресурс. Как любая стоящая вещь, она требует защиты от злоумышленников. Это задачу выполняет стеганография.

 Стеганография  — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). Она обеспечивает сохранность информации, защиту авторского права и так далее.

Наиболее популярной задачей стеганографии является водяной знак.

 Основными понятиями в стеганографии являются ключ, контейнер и сообщение. Их совокупность образует стеганографическую систему. Существуют различные виды атак на нее: от атак со знанием модифицированного контейнера до атак по имитации и подмене.

 Методы стеганографии различаются в зависимости от задачи и формата исходного файла.

 Итак, я считаю, что все поставленные мною задачи были выполнены. А раз так, значит цель реферата достигнута.

Список литературы

* Аграновский А. В., Балакин А. В., Грибунин В. Г. Стеганография, цифровые водяные знаки и стеганоанализ - М.: Издательский дом “Вузовская книга”, 2009.
* Поляков К.Ю., Еремин Е.А. Информатика (учебник для 10 класса) – М.: Издательский дом “БИНОМ. Лаборатория знаний“, 2013
* Статья “Стеганография” интернет ресурса Википедии. [https://ru.wikipedia.org/wiki/Стеганография](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) Ссылка действительна на 13.02.17
* Статья "Стеганография в XXI веке. Цели. Практическое применение. Актуальность" интернет ресурса для IT-специалистов «Хабрахабр». <https://habrahabr.ru/post/253045/> Ссылка действительна на 13.02.2017.
* Статья "Математика криптографии и теория шифрования" интернет ресурса ИНТУИТ. <http://www.intuit.ru/studies/courses/552/408/lecture/9350?page=3> Ссылка действительна на 13.02.17
* Учебная тема "Стеганография. Методы стеганографии" интернет ресурса учебно – методического комплекса "Электронный учебник" <http://main.tpkelbook.com/pre020.php?grupid=&stid=&spn=Стеганография.%20Методы%20стеганографии&pc=2&apl=293&sid=11&qsid=11&lc=0&lst=0> Ссылка действительна на 13.02.17.
* Статья "Криптография" интернет ресурса научного вики сообщества. [http://ru.science.wikia.com/wiki/Криптография](http://ru.science.wikia.com/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) Ссылка действительна на 13.02.17
* Статья "Цифровой водяной знак" интернет ресурса Википедии. [https://ru.wikipedia.org/wiki/Цифровой\_водяной\_знак](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D0%B2%D0%BE%D0%B4%D1%8F%D0%BD%D0%BE%D0%B9_%D0%B7%D0%BD%D0%B0%D0%BA) Ссылка действительна на 13.02.17
* Статья "Водяные знаки" интернет ресурса портала трейдеров UTMAG. <https://utmagazine.ru/posts/7644-vodyanye-znaki> Ссылка действительна на 13.02.17
* Статья "Использование цифровых водяных знаков для борьбы с инсайдерами" интернет ресурса Бюро Научно-Технической Информации. <http://www.bnti.ru/showart.asp?aid=964&lvl=05.08.01>. Ссылка действительна на 13.02.17
1. Научное вики сообщество [Электронный ресурс] /Криптография: http://ru.science.wikia.com/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F [↑](#footnote-ref-1)
2. Финансовый словарь трейдера [Электронный ресурс]/В/Водяные знаки: <https://utmagazine.ru/posts/7644-vodyanye-znaki> [↑](#footnote-ref-2)