Оглавление

[Криптография 2](#_Toc69216804)

[Общие сведения 2](#_Toc69216805)

[Основные алгоритмы шифрования 2](#_Toc69216806)

[Алгоритмы с открытым ключом 4](#_Toc69216807)

[Алгоритмы с симметричным ключом (симметричные шифры) 5](#_Toc69216808)

[Криптографические хэш-функции 6](#_Toc69216809)

[Стеганография 8](#_Toc69216810)

[Основные понятия 8](#_Toc69216811)

[Виды стеганографии 9](#_Toc69216812)

[Практическое применение стеганографии 11](#_Toc69216813)

[Свойства системы человеческого зрения 13](#_Toc69216814)

[Обзор существующих методов встраивания информации в изображение 14](#_Toc69216815)

[Методы замены 15](#_Toc69216816)

[Широкополосные методы 16](#_Toc69216817)

Шифрование данных представляет собой метод сокрытия аутентичной информации, который обеспечивает изменение первоначального вида данных.

# Криптография

http://www.inf.tsu.ru/library/DiplomaWorks/CompScience/2002/Kulenov/diplom.pdf

## Общие сведения

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (strong cryptography) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями – такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

## Основные алгоритмы шифрования

Метод шифровки/дешифровки называют шифром (cipher). Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано, только если известен ключ. Ключ, используемый для дешифровки, может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают. Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы c секретным ключом) и асимметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для 20 шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки. Симметричные алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое. Асимметричные шифры (также именуемые алгоритмами с открытым ключом, или, в более общем плане, криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют открытым ключом, а ключ для дешифрования - закрытым ключом или секретным ключом. Современные алгоритмы шифровки/дешифровки достаточно сложны, и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов. Вообще говоря, симметричные алгоритмы работают быстрее, чем ассиметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения. Многие качественные криптографические алгоритмы доступны широко - в книжном магазине, библиотеке, патентном бюро или в интернете. К широко известным симметричным алгоритмам относятся DES и IDEA. Наверное, самым лучшим асимметричным алгоритмом является RSA.

## Алгоритмы с открытым ключом

Алгоритмы с открытым ключом используют различные ключи для шифрования и дешифрования, при этом ключ дешифрования практически невозможно восстановить по ключу шифрования. Методы с открытым ключом важны, поскольку они могут использоваться для передачи шифровальных ключей или другой информации защищенным способом, даже если стороны не имели возможности договориться частным образом об общем секретном ключе. Все известные методы довольно медленны и обычно 21 используются только для шифровки ключей сессии (которые представляют собой сгенерированные случайным образом "нормальные" ключи), которые затем используются при шифровании тела сообщения с помощью симметричного шифра (о симметричных шифрах см. ниже).

• RSA (Rivest-Shamir-Adelman) является наиболее известным алгоритмом с открытым ключом. Может использоваться как для шифрования, так и для создания подписи. Считается, что алгоритм надежен при использовании достаточно длинных ключей (значение 512 бит считается недостаточным, 768 бит - умеренно надежным, 1024 бит - хорошим). Безопасность RSA основана на проблеме факторизации больших целых чисел. Существенные продвижения в способах факторизации больших чисел могут сделать метод RSA уязвимым. В настоящее время RSA является наиболее важным алгоритмом с открытым ключом. Он запатентован в США (патент оканчивается в 2000 году), и бесплатен в остальной части мира.

• Шифр Диффи-Хеллмана (Diffie-Hellman) является известным алгоритмом с открытым ключом, используемый для обмена ключами. Он считается надежным, если используются достаточно длинные ключи и подходящие генераторы. Безопасность шифра Диффи-Хеллмана основана на сложности решения проблемы дискретного логарифма (ее считают равноценной по сложности задаче факторизации больших чисел). Объявлено, что алгоритм Диффи-Хеллмана запатентован в США, однако патент заканчивается 29 апреля 1997 года. Также ходят упорные слухи, что патент на самом деле недействителен (существует свидетельство, что алгоритм был опубликован за год до того, как был выдан патент).

• DSS (Digital Signature Standard). Метод, используемый только для генерации подписи. Используется правительством США. Детали его реализации пока не опубликованы, но многие уже нашли в нем потенциальные проблемы (например, утечка скрытых в подписи данных; если же вам посчастливится подписать пару разных сообщений с использованием одного и того же случайного числа, это равносильно открытию секретного ключа). Этот алгоритм недавно запатентован американским правительством, и имеется на него еще один патент, который может быть лицензирован в США и Европе за начальный взнос в 25 000 американских долларов плюс отчисления владельцу патента. 22 2.4.4

## Алгоритмы с симметричным ключом (симметричные шифры)

Алгоритмы с секретным ключом используют один и тот же ключ как для шифрования так и для дешифрования (или по одному ключу можно легко вычислить другой).

• DES был разработан в 1970-х. Он был принят как стандарт американским правительством, и, кроме того, принят в некоторых других странах. Он широко используется, и особенно - в финансовой индустрии. DES представляет собой блочный шифр с размером блока в 64 бита. Использует 56-битные ключи. Это делает его легко вскрываемым с помощью современных компьютеров или специализированной аппаратуры. DES еще достаточно силен, чтобы удержать вне игры большинство случайных хакеров и индивидуалов, но легко вскрывается с помощью специализированной аппаратуры правительством, преступными организациями или крупными корпорациями. Стоимость вскрытия ключей DES составляет (при больших объемах) около десятка долларов за ключ. DES становится слишком слабым, и не должен использоваться в современных разработках.

• Blowfish - это алгоритм, разработанный Брюсом Шнейером. Он представляет собой блочный шифр с размером блока в 64 бита и переменной длиной ключа (до 448 бит). Он получил широкое распространение в ряде приложений. Неизвестны успешные атаки на него.

• IDEA (International Data Encryption Algorithm) разработан в ETH, Цюрих, Швейцария. Использует 128-битный ключ и считается очень надежным. В настоящее время этот алгоритм является одним из лучших из известных алгоритмов. Он довольно новый, но уже работает несколько лет, и ни одной успешной атаки на него пока не опубликовано, несмотря на то, что неоднократно предпринимались попытки его анализа.

• RC4 является шифром, разработанным компанией RSA Data Security, Inc. Он был коммерческой тайной до тех пор, пока кто-то не опубликовал в Usenet News исходные тексты алгоритма, который был объявлен эквивалентом RC4. Имеется весьма надежное свидетельство того, что опубликованный алгоритм действительно эквивалентен RC4. Алгоритм очень быстр. Степень его безопасности неизвестна, но вскрытие представляется делом нетривиальным. Благодаря его скорости, он может быть использован в некоторых приложениях. Кроме того, алгоритм работает с ключами произвольной длины. По своей сути RC4 представляет собой генератор псевдослучайных чисел, при этом выходные данные генератора используются для операции xor над потоком данных. Поэтому, чрезвычайно важно, чтобы один и тот же ключ RC4 не использовался для шифровки двух различных сообщений.

## Криптографические хэш-функции

Криптографические хэш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хэш-функции отображают сообщение в имеющее фиксированный размер хэш-значение (hash value) таким образом, что все множество возможных сообщений распределяется равномерно по множеству хэш-значений. При этом криптографическая хэш-функция делает это таким образом, что практически невозможно подогнать документ к заданному хэш-значению. Криптографические хэш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество сообщений, которые когда-либо будут существовать в мире. Много хороших криптографических хэш-функций доступно бесплатно. Широко известные включают MD5 и SHA.

• MD5 (Message Digest Algorithm 5) представляет собой надежный алгоритм хэширования, разработанный компанией RSA Data Security, Inc. Он может использоваться для хэширования строки байт произвольной длины в 128-битное значение. MD5 широко используется и считается достаточно надежным. Однако некоторые исследователи сообщали о потенциальных слабых местах алгоритма, более того, было объявлено о случае вскрытия "MD5 с ключом" (этот метод обычно используют для аутенфикации, когда стороны имеют общий секретный ключ и проверяют аутенфикацию применяя функцию хэширования сначала к секретному ключу, а затем к хэшируемым данным). Также сообщалось о возможности постройки специализированного аппаратного комплекса стоимостью в несколько миллионов долларов, который сможет для заданного хэш-значения подобрать текст за несколько недель.

• MD2, MD4: Эти алгоритмы являются более ранними версиями алгоритма хэширования от RSA Data Security.

• SHA (Secure Hash Algorithm) (также известен как SHS, Secure Hash Standard): хэширующий криптографический алгоритм, опубликованный американским правительством. Он выдает 160-битное хэш-значение по строке произвольной длины. Многие считают его очень хорошим. Он является довольно новым алгоритмом.

• RIPEMD-160 – это наиболее свежий алгоритм хэширования, который создан на смену MD4 и MD5. Он производит дайджест длиной в 20 байт, и, как объявлено, работает со скоростью в 40 Mb/s на 90 MHz Pentium.

# Стеганография

(https://5555455.ru/products/38556642)

## Основные понятия

Стеганография – это наука о способах передачи или хранения информации путем сохранения в тайне самого факта передачи или хранения. Стеганографию, как правило, используют вместе с криптографией, таким образом, расширяя её. Криптография – это наука о методах обеспечения конфиденциальности и целостности информации. Однако, при криптографии наличие шифрованного сообщения само по себе привлекает внимание злоумышленников, при стеганографии же наличие скрытой связи остается незаметным.

Цифровая стеганография, а именно стеганографические программные продукты основываются на двух основных принципах:

Аудио, видео или изображение могут быть в незначительной степени изменены без потери своей функциональности, в отличие от других типов данных, требующих абсолютной точности;

Органы чувств человека неспособны разобрать малозначительные изменения в яркости или контрастности изображения или в качестве видео или звука.

Так как цифровой стеганографией занимаются по всему миру, в  1996 году на конференции Information Hiding: First Information Workshop была принята единая терминология:

Стеганографическая система (стегосистема) — совокупность методов и средств, необходимых для создания скрытого канала передачи данных. При построении такой системы договорились о том, что:

1) Злоумышленник ознакомлен с работой стеганографической системы, но не знает ключ, с помощью которого можно обнаружить скрытое сообщение.

2) Если злоумышленник обнаружит секретное сообщение, он не сможет извлечь из него информацию до тех пор, пока не узнает ключ.

3) Злоумышленник не имеет технических преимуществ.

Ключ (стегоключ) — секретный элемент, который определяет порядок того, как сообщения будут заноситься в контейнер. Различают ключи в стегосистемах двух типов: закрытые (секретные) и открытые. В стегосистеме с секретным ключом используется один ключ. Он создается до начала обмена секретными сообщениями, либо должен быть передан по защищенному каналу. В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи. Особенность ключей состоит в том, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может свободно передаваться по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

## Виды стеганографии

**Цифровые отпечатки (ЦО) (Digital Fingerpring)**

Данный вид стеганографии подразумевает наличие различных стеганографических меток-сообщений для каждой копии контейнера.

Задачи и область применения:

* Корректность использования контента;
* Контроль появления контента в интернете;
* Защита от плагиата;
* Выявление копирования информации, которая является конфиденциальной.

Основные достоинства:

* Устойчивость к таким модификациям, как редактирование, копирование, объединение с другим объектами;
* Скорость работы;
* Сохранение оригинального файла;
* Надежность;
* Неизменность оригинального файла.

В качестве примера применения цифровых отпечатков можно привести продажу электронных книг. При оплате книги и отправки её получателю можно в файл внедрять информацию, которая позволяет идентифицировать отправителя.

Недостаток цифровых отпечатков состоит в том, что если злоумышленник сможет извлечь их из контейнера, то идентифицировать его невозможно, до тех пор, пока он не подделает цифровой отпечаток.

Таким образом, при извлечении цифровых отпечатков третья сторона может преследовать две цели:

* извлечение цифровых отпечатков из контейнера («слабая цель»)
* подмена одного цифрового отпечатка другим цифровым отпечатком («сильная цель»)

**Цифровые водяные знаки (ЦВЗ) (Watermaking)**

Цифровые водяные знаки представляют собой специальные метки, которые внедряются в файл или в изображение с целью контроля их правомерного использования.

В отличие от цифровых отпечатков, цифровые водяные знаки подразумевают наличие одинаковых меток для каждой копии контейнера.

Цифровые водяные знаки можно разделить на два типа — видимые и невидимые. Видимые водяные знаки довольно просто изменить или удалить.  Невидимые – представляют собой вставки, встраиваемые в файл и, которые   не воспринимаются человеческим глазом или ухом. Поэтому цифровые водяные знаки должны отвечать следующим требованиям:

* незаметность для пользователей;
* индивидуальность алгоритма нанесения;
* возможность обнаружения несанкционированного использования файла;
* невозможность удаления посторонними лицами;
* устойчивость к изменениям параметров носителя-контейнера (Например, формата и размеров, сжатию и т.д).

**Скрытая передача данных**

Скрытая передача данных – классический вид стеганографии. Основное отличие скрытой передачи данных от встраивания цифровых водяных знаков состоит в том, что в первом случае злоумышленник должен обнаружить скрытое сообщение, а во втором случае о его существовании знают все. Так же у злоумышленника на законных основаниях может находиться устройство обнаружения цифровых водяных знаков.

## Практическое применение стеганографии

Можно выделить несколько задач, для которых актуальна стеганография.

* Незаметная передача информации

Данное применение является классическим практическим применением стеганографии, поэтому оно стоит на первом месте

* Скрытое хранение информации

Данное применение стеганографии во многом схоже с предыдущим. Однако, в данном случае стеганография используется не для передачи, а для хранения каких-либо данных, обнаружение которых пользователю нежелательно. Данную задачу можно реализовать только на носителях данных.

* Защита авторского права

Для реализации данной задачи необходимо защищать каждую копию контента. В качестве примера можно привести фотографию. В том случае, когда фотографию публикуют без разрешения на то фотографа, опровергнув его авторство, фотограф может доказать, что он является автором, использовав стеганографию. В данном случае в каждую фотографию необходимо внедрить какие-либо данные, которые позволят доказать принадлежность фотографии к фотоаппарату или фотографу.

* Защита подлинности документов

Для защиты подлинности документа можно применить ту же технологию, что и для защиты авторского права. Только в данном случае стеганография будет использоваться не для подтверждения авторства, а для подтверждения подлинности документа. Документ, который не содержит цифровых водяных знаков, будет считаться поддельным.

* Индивидуальный отпечаток в СЭДО

В системах электронного документооборота можно использовать индивидуальный отпечаток, который будет расположен внутри документа и позволит определить, кто работал с документом, а кто нет.

* Водяной знак в DLP системах

Стеганография может быть использована для предотвращения утечек информации (Data Leak Prevention, DLP). В данном случае при создании документа с конфиденциальной информацией в него встраивается определенная метка. При этом метка не изменится, вне зависимости от количества копий и ревизий документа. Для того, чтобы извлечь метку необходимо иметь стегоключ, который содержится в тайне. DLP-система перед отправкой документа проверяет наличие или отсутствие водяного знака. При его наличии система не разрешает отправлять документ за пределы системы.

* Скрытая передача управляющего сигнала

Если имеется система, которая является получателем, а отправителем является оператор, то стеганография может быть применима для доставки управляющего сигнала этой системе. Если система способна находится в различных состояниях, и есть необходимость скрытия факта перехода в другое состояние, то можно также воспользоваться стеганографией.

* Подтверждение достоверности переданной информации

Стегосообщение в данном случае содержит данные, которые подтверждают корректность тех данных, которые передает контейнер. В качестве примера это может быть контрольная сумма или хеш-функция (digest). Например, если речь идет о фотографии, то защитой подлинности является доказательство того, что данная фотография настоящая, не подделанная в графическом редакторе.

* Неотчуждаемость информации

Одним из параметров защиты информации является обеспечение ее целостности. Но что делать, если есть необходимость хранить информацию в таком виде, чтобы невозможно было одни данные отделить от других? В качестве примера можно привести медицинские снимки. Для надежности можно вовнутрь снимков внедрять информацию об имени, фамилии и иных данных пациента.

* Стеганографическое отвлечение

Задача стеганографического отвлечения — отвлечь внимание злоумышленника. Для стеганографического отвлечения необходимо, чтобы генерация стегоконтейнеров была существенно «дешевле» (с точки зрения машинных и временных ресурсов), чем обнаружение стеганографии противником. Грубо говоря, стеганографическое отвлечение чем-то напоминает DoS и DDoS-атаки. Происходит отвлечение внимания противника от контейнеров, которые действительно содержат что-то ценное.

* Стеганографическое отслеживание

Данное применение чем-то похоже на пункт 7, только цель стоит иная — поймать злоумышленника, который передает информацию. Из реального мира можно привести пример отмеченных дензнаков («помеченные купюры»)

## Свойства системы человеческого зрения

Свойства системы человеческого зрения (СЧЗ) можно разделить на два типа: низкоуровневые («физиологические») и высокоуровневые («психофизиологические»).

Выделяют три важнейших низкоуровневых свойства, влияющих на заметность постороннего шума в изображении:

* Чувствительность к изменению яркости (контрастности)
* Частотная чувствительность
* Эффект маскировки

Частотная чувствительность системы человеческого зрения заключается в том, что человек гораздо более восприимчив к низкочастотному (НЧ), чем к высокочастотному (ВЧ) шуму. Это связано с неравномерностью амплитудно-частотной характеристики системы зрения человека. Экспериментально ее можно определить при помощи того же опыта, что и при яркостной чувствительности. Только на этот раз в центральном квадрате изменяются пространственные частоты до тех пор, пока изменения не станут заметными.

Элементы системы человеческого зрения разделяют поступающий видеосигнал на отдельные составляющие. Выделяемые глазом составляющие имеют разные пространственные и частотные характеристики. При одновременном влиянии на глаз двух составляющих с похожими характеристиками возбуждаются одни и те же подканалы. Это приводит к эффекту маскировки, которые заключается в увеличении порога обнаружения зрительного сигнала в присутствии другого сигнала.

Таким образом, можно определить обобщенную схему встраивания информации в изображение:

Выполняется фильтрация изображения с помощью ориентированных полосовых фильтров, распределяющий энергию по частотно-пространственным компонентам.

Рассчитывается порог маскировки.

Значение энергии скрываемых данных корректируется таким образом, чтобы он не превышала порога маскировки.

## Обзор существующих методов встраивания информации в изображение

Развитие мультимедийных средств сопровождается большим потоком информации, представленной в графическом виде. При создании изображения, как правило, используется большое количество элементарных графических примитивов, что представляет особый интерес для стеганографических методов защиты. Зрительная сфера (цифровые изображения и видео) обладает высокой избыточностью различной природы:

* кодовой избыточностью, возникающей при неоптимальном описании изображения;
* межпиксельной избыточностью, которая обусловлена наличием корреляционной зависимости между пикселями реального изображения;
* психовизуальной зависимостью, возникающей из-за того, что орган зрения человека не адаптирован для точного восприятия изображения пиксель за пикселем и воспринимает каждый участок с различной чувствительностью.

В последнее время создано достаточное количество методов скрытия информации в цифровых изображениях, однако анализ предметной области выявил, что основными и наиболее востребованными на практике являются следующие:

* методы замены в пространственной области;
* методы скрытия в частотной области изображения;
* широкополосные методы;
* статистические методы;
* методы искажения;
* структурные методы.

Для дальнейшей разработки алгоритма скрытия информации необходимо раскрыть некоторые особенности, характерные для выделенных групп стеганографических методов.

## Методы замены

Общий принцип для данных методов заключается в том, что происходит замена малозначимой части изображения битами секретного сообщения. Для того, чтобы извлечь это секретное сообщение, необходимо знать алгоритм, по которому в контейнере размещалась скрываемая информация.

Достоинства:

* позволяют скрывать в относительно небольших файлах довольно большие объемы информации;
* простота реализации.

Недостатки:

* сильная чувствительность к малейшим искажениям контейнера.

1.5.2 Методы скрытия в частотной области изображения

Стеганографические методы замены неустойчивы к различным искажениям, а использование сжатия с потерями приводит к абсолютному уничтожению закладки. Более устойчивыми к искажениям, в том числе сжатию, являются методы, которые скрывают данные не в пространственную область, а в спектральную (частотную).

Существуют несколько методов представления изображения в частотной области: с использованием быстрого преобразования Фурье, дискретного косинусного преобразования (ДКП), или вейвлет-преобразования.

Достоинства группы методов скрытия данных в частотной области: устойчивость к искажениям контейнера, различным помехам шумам, а также к JPEG-компрессии с относительно малым коэффициентом сжатия.

Недостатки:

* заметное визуальное искажение стегоконтейнера при большом пороговом значении разницы между коэффициентами ДКП блоков;
* малый объем сообщения, который можно встроить.

## Широкополосные методы

Широкополосные методы скрытия информации широко используются в каналах для обеспечения затруднения процесса перехвата. Идея широкополосных методов заключается в том, что полосы частот сигнала расширяются, более чем это нужно для передачи реальной информации. Увеличение спектра проводится с помощью кода, не зависящего от передаваемых данных. Полезная информация распределяется по всему спектру, следовательно, при потере сигнала в отдельных полосах частот, в других полосах присутствует достаточно информации для ее восстановления.

Таким образом, использование данных методов в стеганографии усложняет обнаружение скрываемой информации и ее уничтожение. Цель широкополосных методов: попытаться “растворить” закладку в стегоконтейнере и сделать обнаружение ее невозможным. Так как сигналы, распределенные по всему диапазону, практически невозможно удалить, стеганографические способы на основе широкополосных методов, являются устойчивыми к преднамеренным и случайным искажениям.

Для скрытия данных используются два основных метода расширения спектра:

* через псевдослучайную последовательность – когда секретный сигнал, различающийся на константу, модулируется псевдослучайным сигналом;
* с помощью прыгающих частот, когда частота несущего сигнала изменяется по некоторому псевдослучайному закону.

Достоинства:

* достаточно высокая устойчивость стегоконтейнера к различным искажениям;
* устойчивость к пассивным и активным атакам.