Оглавление

[Теоретические основы криптографии 2](#_Toc70623383)

[Основные понятия и определения 2](#_Toc70623384)

[Отправитель и получатель 3](#_Toc70623385)

[Алгоритмы и ключи 3](#_Toc70623386)

[Алгоритмы с открытым ключом 4](#_Toc70623387)

[Алгоритмы с симметричным ключом (симметричные шифры) 5](#_Toc70623388)

[Криптографические хэш-функции 6](#_Toc70623389)

[Основные понятия и определения стеганографии 7](#_Toc70623390)

[Обзор методов стеганографии 9](#_Toc70623391)

[Метод наименьшего бита (LSB) 9](#_Toc70623392)

[Метод встраивания цифрового водяного знака 10](#_Toc70623393)

[Анализ аналогов 13](#_Toc70623394)

# Теоретические основы криптографии

## Основные понятия и определения

Как передать нужную информацию целевому адресату втайне от других? Каждый из читателей в разное время и с разными целями наверняка пытался решить для себя эту практическую задачу (для удобства дальнейших ссылок назовем ее «задача ТП», т. е. задача Тайной Передачи). Выбрав подходящее решение, он, скорее всего, повторил изобретение одного из способов скрытой передачи информации, которым уже не одна тысяча лет.

Размышляя над задачей ТП, нетрудно прийти к выводу, что есть три возможности.

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации практически нереально.

1. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

Разработкой средств и методов скрытия факта передачи сообщения занимается стеганография, речь о которой пойдет далее.

1. Использовать общедоступный канал связи, но передавать по нему нужную информацию в так преобразованном виде, чтобы восстановить ее мог только адресат.

Разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей занимается криптография. Такие методы и способы преобразования информации называются шифрами.

**Шифрование (зашифрование)** — процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

**Дешифрование** — процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в открытый текст с помощью определенных правил, содержащихся в шифре.

**Криптография** — прикладная наука, она использует самые последние достижения фундаментальных наук и, в первую очередь, математики. С другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

### Отправитель и получатель

Основным компонентом криптографии является шифрование. Сообщения шифруются и расшифровываются с помощью сложных алгоритмов, созданных комбинацией информатики и математики.

Коммуникационный процесс в криптографии можно сравнить с этим же процессом в почтовой службе:

* отправитель должен отправить сообщение получателю;
* сообщение направляется получателю в понятном контексте;
* получатель в состоянии прочитать сообщение (расшифровать);
* сообщение передается от отправителя к получателю через «посредника» (например, сервер), который играет роль почтальона.

Информация может передаваться по-разному:

* в виде текста;
* в виде звука и изображения.

Коммуникация считается успешной, когда информация была передана от отправителя к получателю, и получатель смог понять смысл сообщения, то есть дешифрировал сообщение правильно. Это справедливо как в технологическом смысле, так и в психологическом смысле (общение между людьми).

### Алгоритмы и ключи

Шифрование использует алгоритм и ключ для преобразования входных данных в зашифрованные выходные данные. Этот метод защиты позволяет просматривать сообщения исключительно отправителю и получателю, поскольку зашифрованную информацию может прочесть только тот, кто имеет секретный ключ для преобразования сообщения в простой текст. 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).

* Rivest-Shamir-Adelman (RSA) 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 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).
* Digital Signature Standard (DSS). 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).
* Семейство стандартов ГОСТ 34.10. Все стандарты семейства 34.10 основаны на эллиптических кривых. Стойкость этих алгоритмов основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости соответствующей хеш-функции. Первые версии алгоритма разрабатывались Главным управлением безопасности связи ФАПСИ при участии Всероссийского научно-исследовательского института стандартизации, позже разработка перешла в руки Центра защиты информации и специальной связи ФСБ России и АО «ИнфоТеКС». Стандарты используют одинаковую схему формирования электронной цифровой подписи. Новые стандарты с 2012 года отличается наличием дополнительного варианта параметров схем, соответствующего длине секретного ключа порядка 512 бит. После подписания сообщения М к нему дописывается цифровая подпись размером 512 или 1024 бит, и текстовое поле. В текстовом поле могут содержаться, например, дата и время отправки или различные данные об отправителе. Данный алгоритм не описывает механизм генерации параметров, необходимых для формирования подписи, а только определяет, каким образом на основании таких параметров получить цифровую подпись. Механизм генерации параметров определяется на месте в зависимости от разрабатываемой системы.

## 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.

## 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.

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.

## Обзор методов стеганографии

### Метод наименьшего бита (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. 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 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 результате мы получим новый оттенок, очень похожий на исходный. 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.

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 пикселя 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.

Преимущества метода:

1. размер файла-контейнера остается неизменным;
2. при замене одного бита в канале синего цвета внедрение невозможно заметить визуально;
3. возможность варьировать пропускную способность, изменяя количество заменяемых бит.

Недостаток у метода один - он неустойчив к обработке файла-контейнера.

### Метод встраивания цифрового водяного знака

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.