

Лекции

Лекция 1

Основы стеганографии

Стеганография — то наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Стегосистема - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

Положения и требования стегосистемы:

- аутентичность и целостность файла;
- необходимое сохранение всех свойств открыто передаваемого файла при внесении в него секретного сообщения и ключа;
- сложная вычислительная техника при извлечении сообщения противником.

Основные задачи стеганографии

1. Защита конфиденциальной информации от несанкционированного доступа;
2. Преодоление систем мониторинга и управления сетевыми ресурсами;
3. Камуфлирования программного обеспечения;
4. Защита авторского права на некоторые виды интеллектуальной собственности.

Модель стегосистемы



Определения:

- Сообщение - это термин, используемый для общего названия передаваемой скрытой информации.

- Контейнер - так называется любая информация, используемая для сокрытия тайного сообщения.
- Пустой контейнер - контейнер, не содержащий секретного послания.
- Заполненный контейнер (стегоконтейнер) - контейнер, содержащий секретное послание.
- Стеганографический канал (стегоканал) - канал передачи стегоконтейнера.
- Ключ (стегоключ) - секретный ключ, нужный для сокрытия стегоконтейнера.

Требования для стегосистемы

Свойства контейнера должны быть модифицированы, чтобы изменение невозможно было выявить при визуальном контроле.

Это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стегосообщения по каналу связи не должно привлечь внимание атакующего.

Стегосообщение должно быть устойчиво к искажениям, в том числе и злонамеренным. В процессе передачи изображение (звук или другой контейнер) может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т.д. Кроме того, оно может быть сжато, в том числе и с использованием алгоритмов сжатия с потерей данных.

Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.

Для повышения надежности встраиваемое сообщение должно быть продублировано.

Общая классификация стеганографии

В конце 90-х годов выделилось несколько направлений стеганографии:

- Классическая стеганография.
- Компьютерная стеганография.
- Цифровая стеганография.

Классическая стеганография

Среди классических методов можно выделить следующие:

- манипуляции с носителем информации (контейнером). пример с древними греками и рабами, где брили им головы и писали там сообщения, ждали, когда зарастёт голова и отправляли раба получателю;
- симпатические чернила. Виды воздействия: химические и органические;
- микронадписи и микроточки;
- литературные приемы: пустышный шифр, акrostих, решётка кардана, жаргонный код;
- семаграммы - это секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр;узелки на нитках и т. д..

Компьютерная стеганография

Компьютерная стеганография - направление классической стеганографии, основанное на особенностях компьютерной платформы.

Примеры:

- Метод использования особых свойств полей форматов, которые не отображаются на экране.
Недостатки: маленькая производительность, небольшой объём передаваемой информации.
- Использование особенностей файловых систем. Недостаток данного метода: лёгкость обнаружения.
Пример про fat32, кластеры.

Цифровая стеганография

Цифровая стеганография направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Примеры контейнеров: аудио-, видео- файлы, изображения (любые мультимедийные файлы)

Включает в себя следующее:

- встраивание информации с целью ее скрытой передачи;
- встраивание цифровых водяных знаков (ЦВЗ);
- встраивание идентификационных номеров;
- встраивание заголовков.

Лекция 2

Цифровые водяные знаки (ЦВЗ)

Цифровые водяные знаки (ЦВЗ) - используются для защиты от копирования, сохранения авторских прав.

Невидимые водяные знакичитываются специальным устройством, которое может подтвердить либо опровергнуть корректность.

ЦВЗ могут содержать различные данные: авторские права, идентификационный номер, управляющую информацию.

Наиболее удобными для защиты с помощью ЦВЗ являются неподвижные изображения, аудио и видео файлы.

Основные требования, предъявляемые к водяным знакам:

- Надёжность;
- устойчивость к искажениям;
- Незаметности;
- робастности к обработке сигналов (робастность - способность системы к восстановлению после воздействия на неё внешних/внутренних искажений, в том числе умышленных).

Виды ЦВЗ: Хрупкие, полуяркие и робастные - это типы ЦВЗ, которые отличаются по своим характеристикам и назначению.

1. Хрупкие ЦВЗ - разрушаются при изменении стегоконтейнера и применяются для аутентификации сигнала.
2. Робастные ЦВЗ - устойчивы к различного вида воздействия на контейнер.
3. Полуяркие ЦВЗ - обычно бывают стойкие к одному виду воздействия, но не устойчивы по отношению к другим.

Лекция 3

Методы цифровой стеганографии. Стеганография Краткий обзор стеганографических программ. Дестеганография

Основные задачи стеганографии

1. Защита конфиденциальной информации от несанкционированного доступа.
2. Преодоление систем мониторинга и управления сетевыми ресурсами.
3. Камуфлирования программного обеспечения.
4. Защита авторского права на некоторые виды интеллектуальной собственности.

Обзор стеганографических программ

Операционная среда Windows:

- Steganos for Win95 - является легкой в использовании, но все же мощной программой для шифрования файлов и скрытия их внутри BMP, DIB, VOC, WAV, ASCII, HTML — файлов.
- Contraband - программное обеспечение, позволяющее скрывать любые файлы в 24 битовых графических файлах формата BMP.

Операционная среда DOS

- Jsteg - программа предназначена для скрытия информации в популярном формате
- FFEncode - интересная программа, которая скрывает данные в текстовом файле. Программа запускается с соответствующими параметрами из командной строки.
- StegoDos - пакет программ, позволяющий выбирать изображение, скрывать в нем сообщение, отображать и сохранять изображение в другом графическом формате.
- Wnstorm - пакет программ, который позволяет шифровать сообщение и скрывать его внутри графического файла PCX формата.

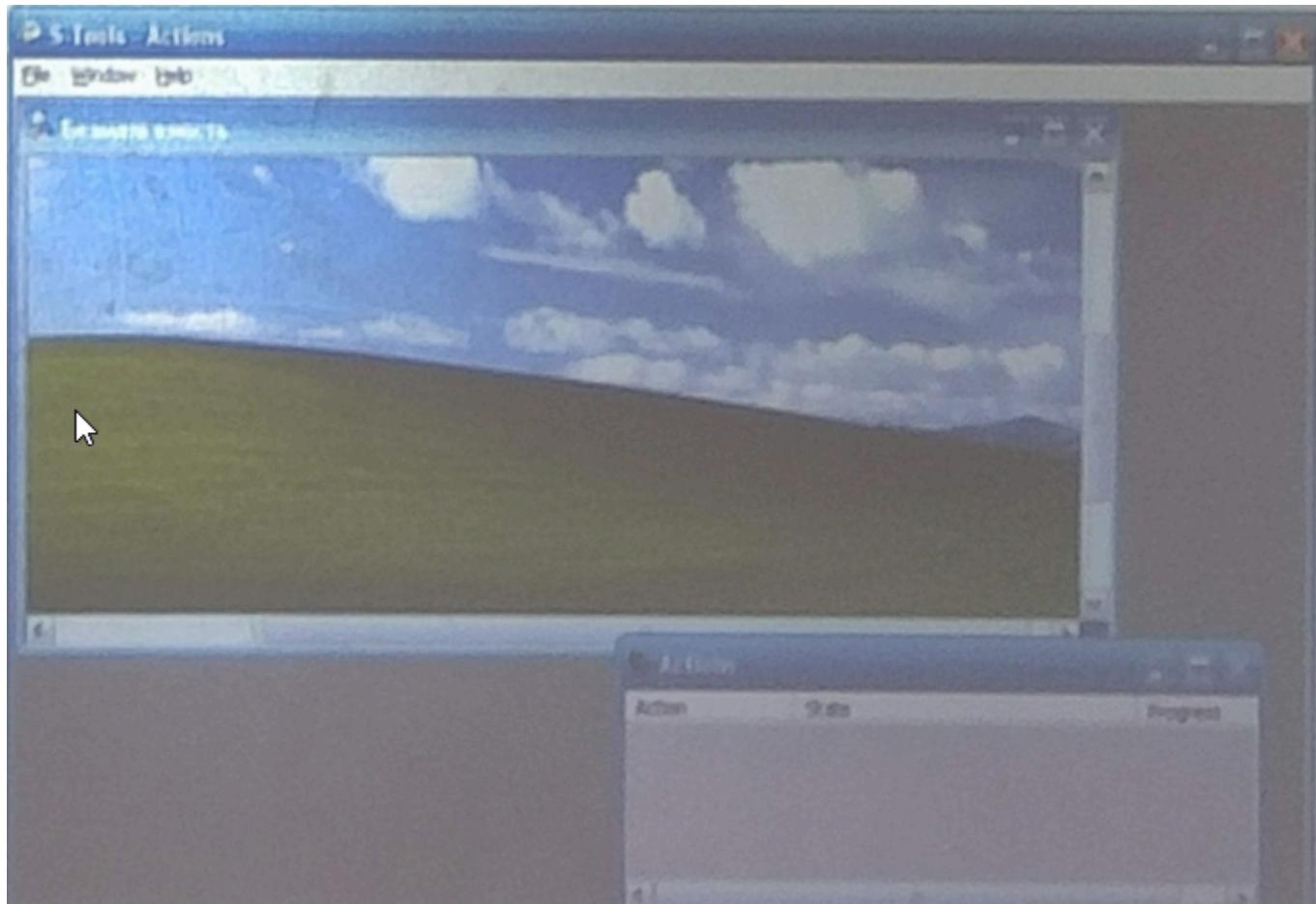
Операционная среда OS/2:

- Hide4PGP v1.1 - программа позволяет прятать информацию в файлах формата BMP, Дей VOC, при этом для скрытия можно использовать любое число самых младших битов.
- Texto - стеганографическая программа, преобразующая данные в английский текст. • Wnstorm — аналогична программе для DOS. Для ПК Macintosh
- Stego - позволяет внедрять данные в файлы формата PICT без изменения внешнего вида и размера PICT -файла.
- Paranoid - эта программа позволяет шифровать данные по алгоритмам IDEA и DES, а затем скрывать файл в файле звукового формата.

Программы для скрытия информации в компьютерных изображениях (эти примеры нужно будет рассказать при сдаче второй практики)

Steganography Tools

Программа S-Tools (Steganography Tools) имеющей статус freeware, можно спрятать информацию в графическом или звуковом файле. Утилита не требует инсталляции, достаточно распаковать архив и запустить файл s-tools.exe. Архив программы занимает всего лишь порядка 280 Кибайт.



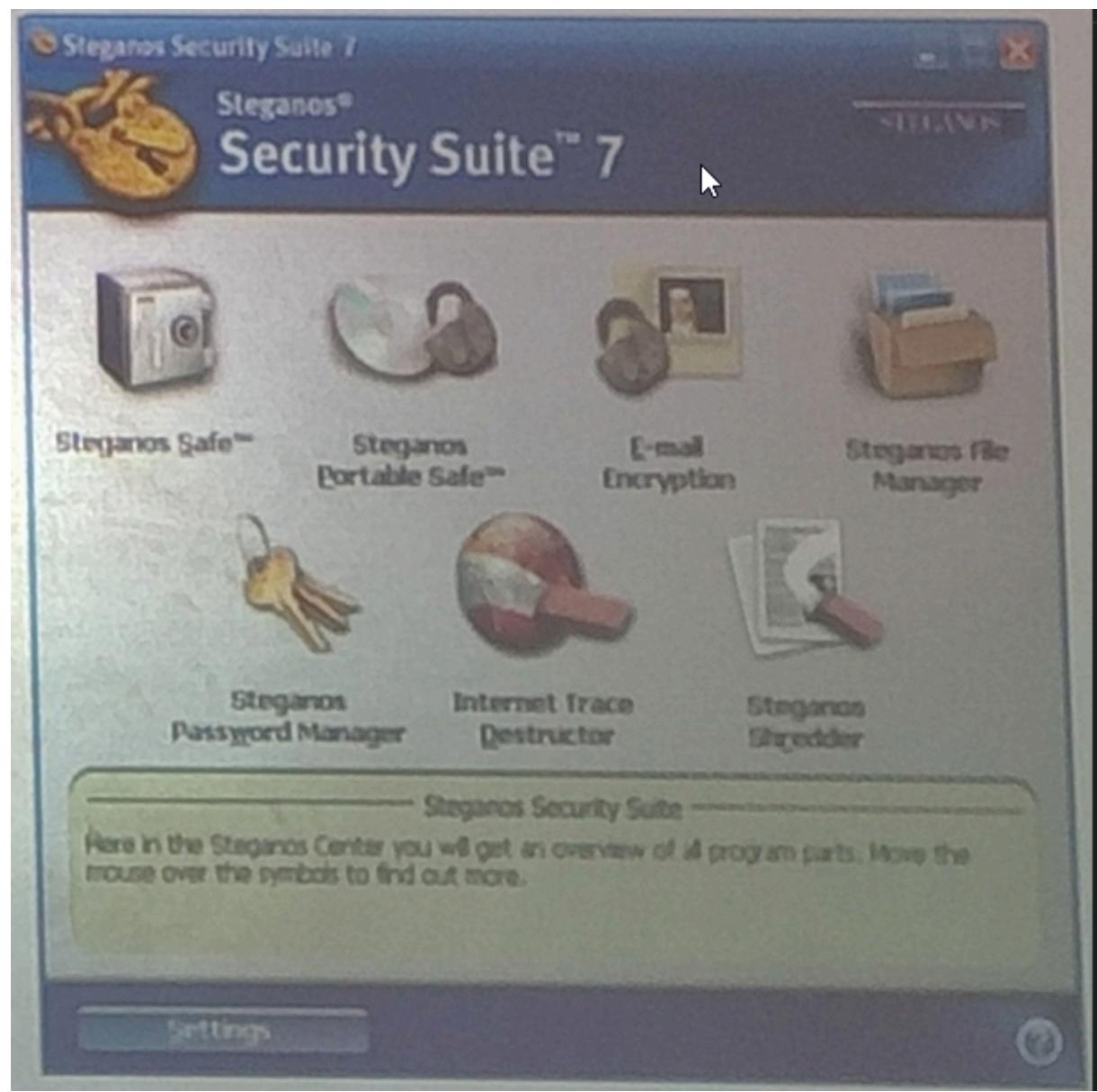
Технология работы программы - шифруемые данные сначала сжимаются, а уже затем непосредственно шифруются. Программа может использовать несколько разных алгоритмов шифрования данных в зависимости от желания пользователя, включая одни из лучших алгоритмов - DES, Triple DES и IDEA. Последние два алгоритма обеспечивают высокий уровень защиты данных от дешифрования (до сих пор не было зарегистрировано ни одного случая дешифрования информации, зашифрованной с использованием данных методов).

Процесс шифрования - достаточно из проводника Windows перетащить графический или звуковой файл в окно программы. В правом нижнем углу программы появится информация о размере файла, который можно спрятать. На следующем этапе нужно перетащить файл с информацией на изображение, ввести пароль, выбрать вариант шифрования и определить метод скрытия. Через некоторое время программа выдаст вторую картинку с условным именем **hidden data**, которая уже содержит скрытую информацию. Затем следует сохранить новую картинку с конкретным именем и расширением gif или bmp, выбрав команду «Save as».

Для расшифровки информации нужно перетащить в окно программы картинку со скрытой информацией, выбрать из контекстного меню, вызываемого нажатием правой кнопки мыши, команду «Reveal», затем ввести пароль - и на экране появится дополнительное окно с именем скрытого файла.

Steganos Security Suite

Программа Steganos Security Suite является довольно популярной программой, по качеству превосходящей S-Tools, однако не являющейся бесплатной. Данный программный продукт представляет собой универсальный набор средств, необходимых для защиты информации.

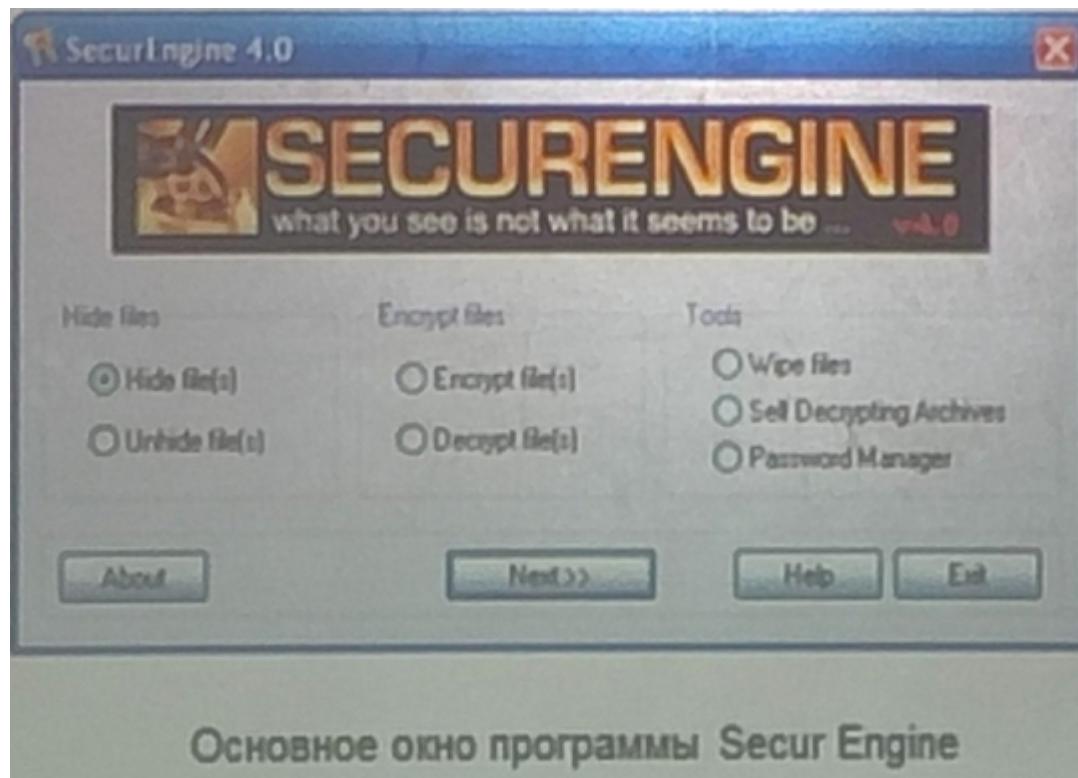


Программа позволяет организовывать виртуальные зашифрованные диски, шифровать сообщения электронной почты, надежно удалять файлы с жесткого диска и многое другое. В большинство из возможностей, предоставляемых Steganos, встроены стеганографические методы. При шифровании какого-либо файла можно дополнительно к этому выбрать контейнер (изображение формата BMP, JPEG или аудиофайл WAV), в который будет встроено предварительно сжатый и зашифрованный файл. Касательно формата BMP программа позволяет использовать изображения только в режиме True Color.

Secur Engine

Программа Secur Engine позволяет как просто шифровать файлы с использованием криптографических методов, так и встраивать их в контейнеры форматов BMP, JPEG, WAV. Имеется возможность выбрать один из 6 алгоритмов шифрования, одним из которых является отечественный алгоритм ГОСТ.

Весь процесс скрытия и шифрования выполнен в форме мастера. Пользователю предлагается последовательно выбрать файлы, которые ему необходимо скрыть, алгоритм шифрования, файл-контейнер, в который будут внедрены данные, и имя получающегося контейнера с внедренным сообщением.



Дестеганография - метод выявления секретной информации

Простые методы дестеганографии заключаются в следующем: для начала нужно найти все места возможных закладок инородной информации, которые допускает формат файла-контейнера. Далее требуется извлечь данные из этих мест и проанализировать их свойства на соответствие стандартным значениям.

Дестеганографические программы

- Stegdetect весьма эффективен против большого числа стеганографических программ: JSTEG, JPHS, Gifshuffle, Hide-and-Seek, Steganos
 - FTK Imager позволяет быстро создать образ жесткого диска для последующего изучения, а также на лету просмотреть файлы MS Office, архивов или изображений.
 - Stego Sulte - автоматический программный сканер, содержащий 9 стеганографических алгоритмов детектирования, рассчитанных на все общие типы файлов цифрового изображения и аудио файлов.
 - File Signature Header позволяет не только определить принадлежность какого-либо файла, но и зачастую идентифицировать программу, его создавшую, или заострить внимание на каких-либо файлах (в рамках конкретного дела).
- А также:

- ProDiscover
- Illok Investigator
- Maresware Forensic Suite
- Paraben E-mail Examiner

Для последней лабы скачать любую из этих программ, чтобы проверить свой контейнер (попытаться извлечь из контейнера информацию)

Лекция 4

Методы ЦВЗ

Методы ЦВЗ направлены на встраивание скрытых маркеров устойчивых к различным преобразованиям контейнера (атакам).

Области применения стеганографии

1. Защита от копирования - Электронная коммерция, контроль за копированием (DVD), распространение мультимедийной информации (видео по запросу).
2. Скрытая аннотация документов - Медицинские снимки, картография, мультимедийные БД.
3. Аутентификация - Системы видеонаблюдения электронной коммерции, голосовой почты, электронное конфиденциальное делопроизводство.
4. Скрытая связь - Военные в разведывательные приложения, а также применение в случаях, когда криптографию использовать нельзя.

Методы стеганографии основываются на двух ключевых принципах:

1. Существуют файлы, которым не нужна полная точность (мультимедийные файлы) и их можно подвергать изменениям без особых потерь функциональности.
2. Органы чувств человека не могут различать незначительные отклонения в изменение вышеуказанных файлов, а также нет специального оборудования для данной задачи.

Классификация методов классической стеганографии:

1) По способу выбора контейнера:

1. суррогатные (эрзац-методы)
2. селективные (методы отбраковки)
3. конструирующие (методы имитации)

2) По способу доступа к информации:

1. потоковые
2. фиксированные

3) По способу организации контейнера:

1. систематические
2. несистематические

4) По способу извлечения сообщения:

1. с оригиналом
2. без оригинала контейнера по фрагменту оригинала контейнера

5) По принципу скрытия:

1. непосредственной замены
2. спектральные

6) По формату контейнера:

1. Текстовые (комп этап)
2. аудио
3. графические
4. видео

7) По назначению:

1. Защита конф. данных
2. защита авторских прав
3. аутентификация данных

8) По свойствам форматов файлов:

1. поля файлов
2. форматирование данных
3. незадействованные участки на носителях
4. файловые заголовки-идентификаторы

Основной подход реализации методов стеганографии основан на выделении в используемой среде малозначительных фрагментов и изменения этих фрагментов на скрываемую информацию

1) Выбор контейнера:

1. Суррогатный (безальтернативный) (эрзац-методы) - нельзя выбрать пустой контейнер, берётся первый попавшийся и данный контейнер является не оптимальным
2. Селективные (методы отбраковки) - скрытое сообщение обязано повторять определённые статистические характеристики шума пустого контейнера. Для использования данного вида контейнера генерируется множество пустых контейнеров и выбирается подходящий для данного сообщения.
3. Конструирующие контейнеры (методы имитации) - стегосистема сама генерирует пустые контейнера (под необходимые характеристики скрываемой информации)

2) По способу доступа к скрываемой информации:

1. Потоковый (бесперерывный вид контейнеров) подразумевает использование, когда биты скрываемой информации заранее не определены и (или) сокрытие информации происходит в режиме реального времени.
2. Фиксированные - ограниченной длины, когда размеры и параметры определены сразу.

3) По способу организации контейнера:

1. Систематические - в контейнерах такого типа можно выбрать биты, в которых находится информация контейнера, и в которых шумовые данные.
2. Несистематические - в контейнерах такого типа извлечение информации происходит при обработке полностью заполненного контейнера

4) По способу извлечения сообщения:

1. с оригиналом - есть возможность сравнивать с оригиналом, для извлечения скрытого сообщение
2. без оригинала контейнера по фрагменту оригинала контейнера - злоумышленник противника анализирует стегоконтейнер пытается другими способа определить есть ли там скрытое сообщение.

5) По используемому принципу скрытия:

1. метод непосредственной замены - представляют собой замену неважных битов пустого контейнера битами, скрываемой информации, основываясь на избытке информационной среды.
2. спектральный метод - использует спектральное представление элементов встраивания для сокрытия сообщения.

6). По формату контейнера:

1. Текстовые (комп этап)
2. аудио
3. графические
4. видео

7). По назначению:

1. Защита конф. данных
2. защита авторских прав
3. аутентификация данных

8). По свойствам форматов файлов:

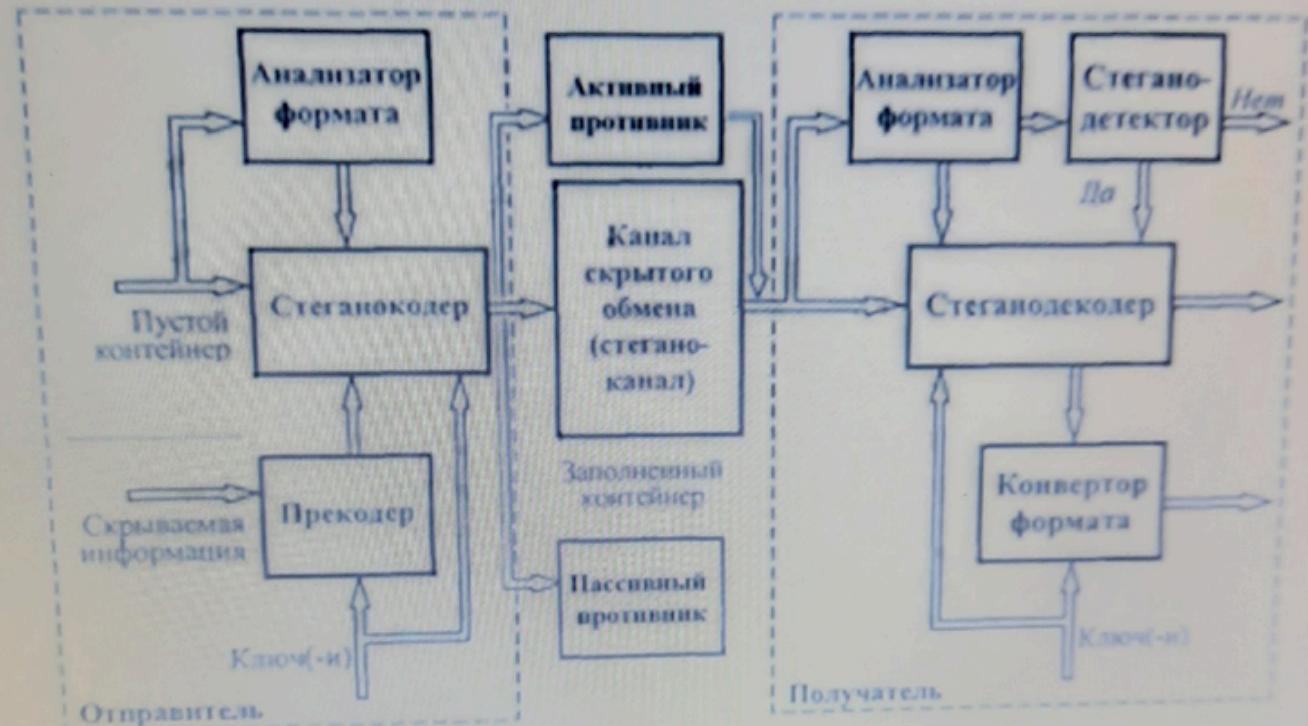
1. поля файлов
2. форматирование данных
3. незадействованные участки на носителях
4. файловые заголовки-идентификаторы

Эту схему надо будет рисовать на 3 лабе

Структурная схема стеганографической системы



Структурная схема стеганографической системы



Сравнительная характеристика стенографических методов.

Методы сокрытия информации в аудиоконтейнерах

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--|--|---|--|
| Метод сокрытия в наименьших значащих битах (НЗБ) | Основан на записи сообщения в наименьшие значащие биты исходного сигнала. В качестве контейнера используется, как правило, несжатый аудиосигнал. | Невысокая скрытность передачи сообщения. Низкая устойчивость к искажениям. Используется только для определенных форматов аудиофайлов. | Достаточно высокая емкость контейнера (до 25 %). |
| Метод сокрытия на основе распределения по спектру | Основан на генерации псевдослучайного шума, являющегося функцией внедряемого сообщения, и подмешивании полученного шума к основному сигналу-контейнеру в качестве аддитивной составляющей. Кодирование потоков информации путем рассеяния кодированных данных по спектру частот. | Низкий коэффициент использования контейнера. Значительные вычислительные затраты. | Сравнительно высокая скрытность сообщения. |
| Метод сокрытия на основе использования эхосигнала | Основан на использовании в качестве шумоподобного сигнала самого аудиосигнала, задержанного на различные периоды времени в зависимости от внедряемого сообщения («дозвоночного эха»). | Низкий коэффициент использования контейнера. Значительные вычислительные затраты. | Сравнительно высокая скрытность сообщения. |
| Метод сокрытия в фазе сигнала | Основан на факте нечувствительности уха человека к абсолютному значению фазы гармоник. Аудиосигнал разбивается на последовательность сегментов, сообщение встраивается путем | Малый коэффициент использования контейнера. | Обладает значительно более высокой скрытностью, чем методы сокрытия в НЗБ. |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--------------------------|------------------------------------|------------|--------------|
| | модификации фазы первого сегмента. | | |

Методы сокрытия информации в текстовых файлах

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--|---|---|---|
| Метод сокрытия на основе пробелов | Основан на вставке пробелов в конце строчек, после знаков препинания, между словами при выравнивании длины строк. | Методы чувствительны к переносу текста из одного формата в другой. Возможна потеря сообщения. Невысокая скрытность. | Достаточно большая пропускная способность (это показатель того, сколько единиц информации может обработать система за определенный временной промежуток). |
| Метод сокрытия на основе синтаксических особенностей текста | Основан на том, что правила пунктуации допускают неоднозначности при расстановке знаков препинания. | Очень низкая пропускная способность. Сложность детектирования сообщения. | Существует потенциальная возможность подобрать такой метод, при котором потребуются весьма сложные процедуры для раскрытия сообщения. |
| Метод сокрытия на основе синонимов | Основан на вставке информации в текст при помощи чередования слов из какой-либо группы синонимов. | Сложен применительно к русскому языку в связи с большим разнообразием оттенков в разных синонимах. | Один из наиболее перспективных методов. Обладает сравнительно высокой скрытностью сообщения. |
| Метод сокрытия на основе использования ошибок | Основан на маскировке информационных битов под естественные ошибки, опечатки, нарушения правил написания сочетаний гласных и согласных, замене кириллицы на | Невысокая пропускная способность. Быстро вскрывается при статистическом анализе (это процесс сбора и анализа данных с целью выявления закономерностей и | Весьма прост в применении. Высокая скрытность при анализе человеком. |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--|---|--|--|
| | аналогичные по внешнему виду латинские буквы и др. | тенденций, устранныя предвзятости и помоши в принятии решений.) | |
| Метод сокрытия на основе генерации квазитекста | Основан на генерации текстового контейнера с использованием набора правил построения предложений. Используется симметричная криптография. | Невысокая пропускная способность. Бессмысленность созданного текста. | Скрытность определяется методами шифрования и, как правило, весьма высока. |
| Метод сокрытия на основе использования особенностей шрифта | Основан на вставке информации за счет изменения типа шрифта и размера букв, а также на возможности встраивания информации в блоки с неизвестными для Браузера идентификаторами. | Легко выявляется при преобразовании масштаба документа, при статистическом стегоанализе. | Высокий коэффициент использования контейнера. |
| Метод сокрытия на основе использования кода документа и файла | Основан на размещении информации в зарезервированных и неиспользуемых полях переменной длины. | Низкая скрытность при известном формате файла. | Прост в применении. |
| Метод сокрытия на основе использования жаргона | Основан на изменении значений слов. | Низкая пропускная способность. Узко специализирован. Низкая скрытность. | Прост в применении. |
| Метод сокрытия на основе использования чередования длины слов | Основан на генерации текста-контейнера с формированием слов определенной длины по известному правилу кодирования. | Сложность формирования контейнера и сообщения. | Достаточно высокая скрытность при анализе человеком. |
| Метод сокрытия на основе | Основан на внедрении сообщения в первые | Сложность составления сообщения. Низкая | Дает большую свободу выбора оператору, |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|---------------------------|------------------------------------|-----------------------|---------------------------|
| использования первых букв | буквы слов текста с подбором слов. | скрытность сообщения. | придумывающему сообщение. |

Методы скрытия информации в графических контейнерах

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--|--|---|--|
| Метод скрытия в наименьших значащих битах (НЗБ) | Основан на записи сообщения в наименьшие значение биты исходного изображения. | Невысокая скрытность передачи сообщения. Низкая устойчивость к искажениям. | Достаточно высокая емкость контейнера (до 25%). Высокая скорость встраивания и извлечения сообщения. Простота реализации. |
| Метод блочного скрытия. | Встраивание 1 бита происходит в 1 блок контейнера. Метод блочного скрытия — это еще один подход к реализации метода замены и заключается в следующем. Изображение - оригинал разбивается на непересекающиеся блоки произвольной конфигурации, для каждого из которых вычисляется бит четности. В каждом блоке выполняется скрытие одного секретного бита | Низкая устойчивость к искажениям. Низкая пропускная способность | Высокая устойчивость к детектированию и извлечению сообщения. Высокое быстродействие. |
| Метод замены палитры | Основан на перестановке цветов в палитре | Низкая скрытность сообщения | Высокая емкость. |
| Метод квантования | В простейшем случае можно вычислить разницу между смежными пикселями и задать ее как параметр функции. Основан на межпиксельной зависимости. | Низкая устойчивость к искажениям. | Высокая пропускная способность. Устойчивость к детектированию. |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|---|--|--|---|
| Метод Куттера-Джордана-Боссена | Основан на модификации яркости синего цвета отдельных пикселей | Достоверность и величина вносимых искажений сильно взаимосвязаны | Высокая пропускная способность. Устойчивость к детектированию |
| Метод псевдослучайного интервала | Заключается в случайном распределении бит скрываемого сообщения в контейнере, при этом расстояния между битами определяются псевдослучайно. | Низкая устойчивость к искажениям | Достаточно высокая емкость контейнера (до 25%). Высокая скорость встраивания и извлечения сообщения. Простота реализации. Устойчивость к детектированию и извлечению сообщения. |
| Метод псевдослучайной перестановки | Основан на генераторе псевдослучайных перестановок. Информационные данные разбиваются на блоки равной длины n . Над каждым блоком выполняется перестановочное преобразование. | Сложность реализации при больших n . Низкая устойчивость к искажениям | Достаточно высокая емкость контейнера (до 25%). Высокая скорость встраивания и извлечения сообщения. Простота реализации. Устойчивость к детектированию, при больших n . |
| Метод Дармстедтера-Делейгла-Квисковтера-Макка | Нетрадиционный блочный метод встраивания в пространственную область контейнера Алгоритм представляет собой один из вариантов модификации яркости, при котором контейнер разбивается на блоки 8×8 пикселей, соразмерных с блоками при JPEG компрессии | Заметное визуальное искажение. Малый объем сообщения, который можно встроить. | Устойчивость к детектированию и извлечению сообщения. |
| Метод сокрытия с использованием нелинейной модуляции | Основан на модуляции псевдослучайного сигнала сигналом, содержащим скрываемую информацию | Низкая точность детектирования и Искажениям | Достаточно высокая скрытность сообщения |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|---|--|--|---|
| встраиваемого сообщения | | | |
| Метод сокрытия с использованием знаковой модуляции встраиваемого сообщения | Основан на модуляции псевдослучайного сигнала биполярным сигналом, содержащим скрываемую информацию | Низкая точность детектирования. Искажения | Достаточно высокая скрытность сообщения |
| Метод сокрытия, основанный на вейвлет-преобразовании графической информации | Основан на особенностях вейвлет-преобразований (интегральное преобразование, которое представляет собой свертку вейвлет-функции с сигналом) | Сложность расчетов | Высокая скрытность |
| Метод сокрытия, основанный на косинусном преобразовании графической информации | Основан на особенностях дискретного косинусного преобразования (является преобразованием массива пикселей в массив значений пространственной частоты. Это преобразование является обратным с точностью до ошибок округления. Оно позволяет переходить от пространственного представления изображения к его спектральному представлению и обратно.) | Сложность расчетов | Высокая скрытность |
| Метод Коха и Хао | Метод заключается в изменении отношения между абсолютными значениями коэффициентов ДКП в среднечастотной области изображения. | Низкая пропускная способность. Некоторые блоки слабо приспособлены к встраиванию данных | Устойчивость к атакам |
| Метод Бенгама-Мемона-Эо-Юнг | Усовершенствованный метод Коха и Хао, за счет дополнительной отбраковки блоков на основе процедур статистического анализа коэффициентов ДКП и используется 3 коэффициента ДКП вместо двух. | Низкая пропускная способность | Устойчивость к атакам |

| Стеганографический метод | Краткая характеристика метода | Недостатки | Преимущества |
|--------------------------|--|-------------------------------------|--|
| Метод Хсу-Ву | Усовершенствованный метод Коха и Хао | Большие искажения | Повышенная пропускная способность |
| Метод Фридрих | Основан на модификации низкочастотных коэффициентов ДКП. При встраивании используется геометрическая прогрессия действительных чисел и специально введенная индексная функция. | Высокая величина вносимых искажений | Высокая пропускная способность. Устойчивость к детектированию и извлечению сообщения |

Лекция 6

Цифровая стеганография.

Основное понятие цифровой стеганографии было сформулировано на первой международной конференции по скрытию данных в 1996 году и описали определение цифровая стеганография - это наука о надёжном и незаметном скрытии одних битовых последовательностей, другими имеющие аналоговую природу. Определили требования : незаметность и надёжность.

1. Незаметность подразумевает обязательное включение человека в систему в стеганографической передачи данных.
2. Надёжность - это устойчивость к искажениям различного рода.

Для построения стегосистемы необходимо учитывать:

1. Наличие приемлемых вычислительных сложностей реализации стегосистемы.
2. Обеспечение необходимой пропускной способности.
3. Обеспечение аутентичности и целостности секретной информации для авторизованного лица.
4. Если факт существования скрытого сообщения становится известным нарушителю, то извлечь его должно быть невозможно пока ключ будет неизвестен.
5. Нарушитель должен не иметь любых преимуществ в распознавании или раскрытии секретных сообщений.

Основными задачами стеганографии можно считать: Разработку новых и совершенствование имеющихся методов и способов информации и создание на их основе высокоэффективных стеганографических систем безопасного хранения и передачи данных.

Практическое применение стеганографии на сегодняшний момент:

1. Защита авторских прав
2. Незаметная передача информации
3. Скрытое хранение информации

4. Защита исключительного права
5. Защита подлинности документов
6. Индивидуальный отпечаток в системе электронного документооборота
7. Скрыта передача управляющего сигнала
8. Защита конф. инфы от НСД
9. Создание скрытых от законного представителя каналов утечки информации и их детектирование
10. Камуфлирование ПО

Состав стегонасистемы

Стегосистема состоит из:

1. (Сообщение) $m \in M$ (множество сообщений) - всевозможные сообщения объединяются в пространство $M=\{m_1, m_2, m_3, \dots, m_n\}$
2. (Контейнер) $c \in C$ (мн-во контейнеров) всевозможные контейнера объединяются в пространство контейнеров $C=\{c_1, c_2, \dots, c_n\}$; c - пустой контейнер, c_m - (c с индексом) - стегоконтейнер.
3. Файл - мультимедийный объект
4. К - ключ, секретная инф, которая известна законному пользователю, а также определяет какой алгоритм сокрытия использовался
5. Преобразования (прямое и обратное)

В стеганографии алгоритмы представлены в виде протоколов:

1. С секретным ключом
2. С открытым ключом
3. Бесключевой
4. Смешанный

Реализация:

Прямое преобразование (E) - $E: M \times C \times K$

Обратное преобразование (D или \bar{D}): $C_m \times K \rightarrow M$

Стеганосистема (S) это совокупность сообщений секретных ключей контейнера и связывающих преобразований: $S = (E, D; M; C; K)$

Структурная схема стеганографической системы



Иногда получатель = отправитель

Ключ в прекодере и стеганокодере могут быть разными

Активный противник может воздействовать на стегоконтейнер

Пассивный противник просто наблюдает за стегоканалом

1. Прекодер выполняет начальную обработку скрываемой информации, преобразовывает её для удобного встраивания в контейнер, используя ключ для повышения секретности или не используя ключ
2. Стеганокодер выполняет упаковку сообщения в контейнер с учётом выбранного протокола встраивания и типа стеганосистемы
3. Стеганоканал - это канал передачи заполненного контейнера (отправитель может выступать получателем, если направляет контейнер для зранения у себя или предотвращения утечки). Стеганоканал может подвергаться умышленным или случайным атакам
4. Стеганодетектор - определяет наличие в контейнере скрытых данных (контейнер может быть изменён в процессе передачи, например, влиянием ошибок в канале связи или же намеренных атак нарушителей). Стеганодетектор восстанавливает скрытое сообщение (при наличии доп. элементов)

Стеганография Математическая модель типичной стегосистемы

В **стеганодетекторе** определяется наличие в контейнере (возможно уже измененном) скрытых данных. Это изменение может быть обусловлено влиянием ошибок в канале связи, операций обработки сигнала, намеренных атак нарушителей.

Различают стеганодетекторы, предназначенные только для обнаружения факта наличия встроенного сообщения, и устройства, предназначенные для выделения этого сообщения из контейнера, - **стеганодекодеры**.

Алгоритм встраивания сообщения в простейшем случае состоит из двух основных этапов:

1. Встраивание в стеганокодере секретного сообщения в контейнер-оригинал.
2. Обнаружение (выделение) в стеганодекторе (декодере) скрытого зашифрованного сообщения из контейнера-результата.

Процесс стеганографического преобразования:

1. $E: C \times M \rightarrow S;$
2. $D: S \rightarrow M.$

где $S = \{(c_1, m_2), (c_1, m_2), \dots, (c_n, m_n), \dots, (c_q, m_q)\} = \{s_1, s_2, \dots, s_3\}$ — множество контейнеров-результатов (стеганограмм).

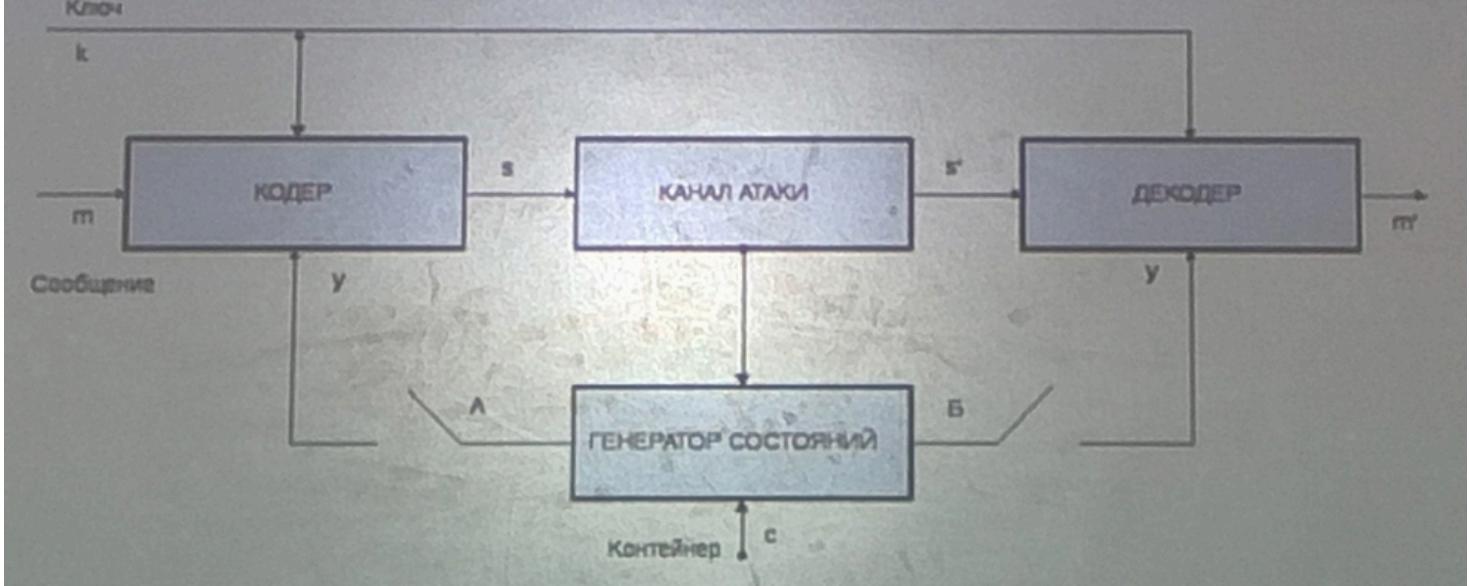
Зависимость (1) описывает процесс скрытия информации, зависимость (2) - извлечение скрытой информации. Необходимым условием при этом является отсутствие «пересечения».

мощность множества $|C| \geq |M|$. При этом оба адресата (отправитель и получатель) должны знать алгоритм прямого (E) и обратного (D) стеганографического преобразования.

Итак, в общем случае стеганосистема — это совокупность $\Sigma = (C, M, S, E, D)$ контейнеров (оригиналов и результатов), сообщений и преобразований, которые их связывают.

Для большинства стеганосистем множество контейнеров C выбирается таким образом, чтобы в результате стеганографического преобразования (2) заполненный контейнер и контейнер-оригинал были подобны.

Представим стеганографическую систему как систему связи с передачей дополнительной информации



Представление стеганосистемы как системы связи с передачей дополнительной информации

В этой модели кодер и декодер имеют доступ, кроме ключа, еще и к информации о канале (то есть о контейнере и о возможных атаках). В зависимости от положения переключателей А и Б выделяют четыре класса стеганосистем (при этом считается, что ключ всегда известен кодеру и декодеру).

- I класс. Дополнительная информация отсутствует (переключатели разомкнуты)— так называемые "классические" стеганосистемы. В ранних работах по стеганографии считалось, что информация о канале является недоступной кодеру. Выявление скрытой информации осуществлялось путем вычисления коэффициента корреляции между принятым контейнером и вычисленным по ключу сообщением.
- II класс. Информация о канале известна только кодеру (ключ А замкнут, Б разомкнут). К недостаткам стеганосистем класса II можно отнести высокую сложность кодера (необходимость построения кодовой книги для каждого контейнера), а также отсутствие адаптации системы к возможным атакам.
- III класс. Дополнительная информация известна только декодеру (переключатель А разомкнут, Б замкнут). Декодер строится с учетом возможных атак. В результате получают устойчивые к геометрическим атакам системы. Сообщение генерируется в декодере на основании ключа.
- IV класс. Дополнительная информация известна как в кодере, так и в декодере (оба переключателя замкнуты). Оптимальность такой схемы достигается путем оптимального согласования кодера с сигналом- контейнером, а также адаптивным управлением декодером в условиях наблюдения канала атак.

Несмотря на сложность выделения и прочтения скрытого сообщения, факт его наличия легко обнаружить и еще проще его уничтожить. По этому при построение стеганосистемы особое внимание нужно уделять защите от атак активных и злонамеренных нарушителей.

Если скрываемое сообщение не может быть заменено без значительной модификации контейнера, при этом он теряет свою функциональность, то такая стеганосистема называется устойчивой к активным атакам.

- стеганографические преобразования сразу же формируются устойчивыми к определенным условиям, предусматривая возможные атаки;

- используются преобразования, которые можно обратить к возможным модификациям для восстановления начального вида заполненного контейнера.

Для оценки и сравнения различных стеганосистем используются количественные методы. В большинстве случаев они применяются для анализа стеганосистем с использованием изображений и аудиофайлов. Наиболее популярным считается показатель искажения, взятый из радиотехники, отношение «сигнал/шум», измеряемое в децибелах.

Протоколы стеганографических систем

И протокол, и алгоритм являются определенной последовательностью действий. Отличие между ними заключается в том, что к протоколу должны быть обязательно привлечены две или более сторон.

При этом допускается, что участники принимают на себя обязательства придерживаться протокола. Так же как и алгоритм, протокол состоит из шагов. На каждом шаге протокола выполняются определенные действия, которые могут заключаться, например, в проведении некоторых вычислений.

В стеганографии различают системы с секретным ключом и системы с открытым ключом. В первых используется один ключ, который должен быть заранее известен авторизованным абонентам до начала скрытого обмена секретными сообщениями.

В системах с открытым ключом для встраивания и извлечения скрытой информации используются разные, не выводимые один из другого ключа — открытый и секретный.

Учитывая большое разнообразие стеганографических систем, целесообразно свести их к следующим четырем типам :

- бесключевые стеганосистемы;
- системы с секретным ключом;
- системы с открытым ключом;
- смешанные стеганосистемы.

Бесключевые стеганосистемы

Для функционирования бесключевых стеганосистем, кроме алгоритма стегано-графического преобразования, отсутствует необходимость в дополнительных данных, наподобие стеганоключа. Совокупность $\Sigma = (C, M, S, E, D)$, где C — множество контейнеров-оригиналов; M — множество секретных сообщений, причем $|M| \leq |C|$; S — множество контейнеров-результатов, причем $sim(C, S) - 1$: $E: C \times M \rightarrow S$ и $D: S \rightarrow M$ — соответственно функции прямого (встраивание) и обратного (извлечение) стеганопреобразований, причем $D[E(c, m)] = m$ для любых $m \in M$ и $c \in C$, называется **бесключевой стеганографической системой**.

Таким образом, безопасность бесключевых стеганосистем базируется только на секретности используемых стеганографически преобразований E и D . Это противоречит определяющему принципу, который установил Керхгофс (A. Kerckhofls) для систем защиты информации,

поскольку стойкость системы зависит только от степени проинформированности нарушителя относительно функций Е и D.

Для повышения безопасности бесключевых систем перед началом процесса стеганографического скрытия предварительно выполняется криптографическое шифрование скрываемой информации. Совершенно очевидно, что такой подход увеличивает защищенность всего процесса связи, поскольку усложняет выявление скрытого сообщения. Однако "сильные" стеганосистемы, как правило, способны выполнять возложенные на них функции без предварительной криптографической защиты встроенного сообщения

Лекция 8

Стеганосистемы с секретным ключом

По принципу Керхгофса, безопасность системы должна базироваться на определенном фрагменте секретной информации — ключе, который (как правило, предварительно) разделяется между авторизованными лицами. Отправитель, встраивая секретное сообщение в выбранный контейнер с, использует стеганоключ k. Если получатель знает данный ключ, то он может извлечь из контейнера скрытое сообщение. Без знания ключа любое постороннее лицо этого сделать не сможет.

Стеганосистемой с секретным ключом называют совокупность $E = (C, M, K, S^K, E, D)$, где C — множество контейнеров-оригиналов; M — множество секретных сообщений, причем $|M| \leq |C|$; S^K — множество контейнеров - результатов, причем $\text{sim}(C, S^K) \rightarrow 1$; K — множество секретных стеганоключей; E: $C \times M \times K \rightarrow S^K$ и D: $S^K \times K \rightarrow M$ — функции прямого и обратного стеганопреобразования со свойством $D[E(c, m, k), k] = m$ для любых $m \in M$, $c \in C$ и $k \in K$.

Данный тип стеганосистем предполагает наличие безопасного (защищенного) канала обмена стеганоключами.

Иногда ключ k вычисляют с помощью секретной хэш-функции, используя некоторые характерные черты контейнера. Если стеганопреобразование E не изменяет в окончательной стеганограмме выбранные особенности контейнера, то получатель также сможет вычислить стеганоключ (хотя и в этом случае защита будет зависеть от секретности хэш-функции, и, таким образом, опять нарушается принцип Керхгофса). Очевидно, что для достижения адекватного уровня защиты такую особенность в контейнере необходимо выбирать достаточно внимательно.

В некоторых алгоритмах во время извлечения скрытой информации дополнительно необходимы сведения о первичном (пустом) контейнере или некоторые другие данные, отсутствующие в стеганограмме. Такие системы представляют ограниченный интерес, поскольку они требуют передачи изначального вида контейнера, что эквивалентно традиционной задаче обмена ключами. Подобные алгоритмы могут быть отмечены как отдельный случай стеганосистем с секретным ключом, у которых $K = C$ или $K = C \times K'$, где K' — множество дополнительных наборов секретных ключей.

Стеганосистемы с открытым ключом

Стеганография с открытым ключом опирается на достижения криптографии последних 30 лет. Стеганографические системы с открытым ключом не имеют потребности в дополнительном канале ключевого обмена. Для их функционирования необходимо иметь два стеганоключа; один секретный, который необходимо хранить в тайне, а другой — открытый, который может храниться в доступном для всех месте. При этом открытый ключ используется для встраивания сообщения, а секретный — для его извлечения.

Стеганосистемой с открытым ключом называют совокупность $Z = (C, M, K, S^K, E, D)$, где C — множество контейнеров-оригиналов; M - множество секретных сообщений, $|M| \leq |C|$; S^K — множество контейнеров- результатов; $\text{sim}(C, S^K) \rightarrow 1$; $K = (k_o, k_c)$ — множество пар стеганоключей (открытый ключ ко используется для скрытия информации, а секретный ключ k_c — для ее извлечения); $E: C \times M \times k_o \rightarrow S^K$ и $D: S^K \times k_c \rightarrow M$ — функции прямого и обратного стеганопреобразования со свойством $D[E(c, m, k_o)] = m$ для любых $m \in M$, $c \in C$ и $k_o, k_c \in K$.

Следует отметить, что стеганоключ не шифрует данные, а скрывает место их встраивания в контейнере. Скрытые данные могут быть дополнительно зашифрованы классическим методом но этот вопрос не касается непосредственно стеганографии.

Стеганосистемы с открытым ключом используют тот факт, что функция извлечения скрытых данных D может быть применена к любому контейнеру, независимо от того, находится в нем скрытое сообщение или нет.

Если скрытое сообщение отсутствует, то на выходе будет получена некоторая случайная последовательность.

Если эта последовательность статистически не отличается от шифртекста крипtosистемы с открытым ключом, тогда в безопасной стеганосистеме можно скрывать полученный таким образом шифртекст, а не открытый текст.

Смешанные стеганосистемы

На практике преимущество отдается бесключевым стеганосистемам, хотя последние могут быть раскрыты в случае, если нарушитель узнает о методе стегано-преобразования, который был при этом использован.

В связи с этим в бесключевых системах часто используют особенности криптографических систем с открытым и/или секретным ключом.

Учитывая большое разнообразие форматов, которые могут иметь скрываемые сообщения и контейнеры (текст, звук или видео, которые, в свою очередь, также делятся на подформаты), представляется целесообразным предварительное преобразование сообщения в удобный для встраивания и оптимальный с точки зрения скрытости в заданном контейнере формат :

Другими словами, необходимо учитывать как особенности встраиваемого сообщения, так и особенности контейнера, в который планируется его ввести.

Произвольность функции U ограничивается требованиями устойчивости к разного рода влияниям на полученный контейнер-результат. Кроме того, функция U является составной: $U = T \circ G$ где $G: M \times K \rightarrow Z$; $T: C \times Z \rightarrow W$.

Функция G может быть реализована, например, с помощью криптографического безопасного генератора ПСП с K в качестве изначального значения. Для повышения устойчивости скрытого сообщения могут использоваться помехоустойчивые коды, например, коды Хемминга, Голея, сверточные коды.

Оператор T модифицирует кодовые слова Z с учетом формата контейнера, в результате чего получается оптимальное для встраивания сообщение. Функция T должна быть выбрана таким образом, чтобы контейнер-оригинал C, контейнер-результат S и модифицированный в предусмотренных границах контейнер-результат Š порождали одно и то же оптимальное для встраивания сообщение: $T: C \times Z = T: S \times Z = T: \tilde{S} \times Z = \rightarrow W$

Процесс встраивания сообщения W в контейнер-оригинал C при этом можно описать как суперпозицию сигналов: $E: C \times V \times W \rightarrow S$; где V — маска встраивания сообщений, которая учитывает, например, характеристики зрительной системы среднестатистического человека и служит для уменьшения заметности этих сообщений

Лекция 9

Использование бесключевых стеганосистем является нецелесообразным, так как базируется только на секретности стеганографических преобразований.

Преимущественно использование протокола с открытым ключом.

Самостоятельна обработка

Анализ стеганографических программ включает изучения из возможностей, принципов работы, преимуществ и недостатков. Программы, которые необходимо проанализировать.

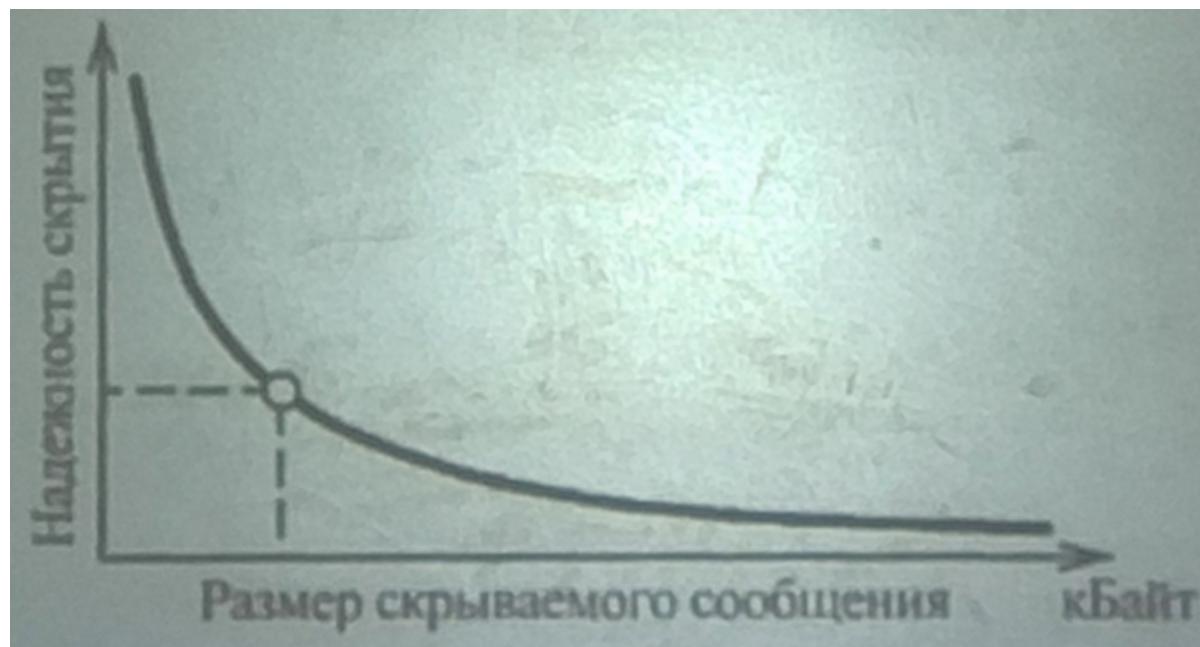
- OutGuess - Сокрытие данных в JPEG-изображение. Возможность контроля вносимых 'Статических искажений', большая стойкость к атакам. Ориентирована на работу в Unix-подобных ОС.
- JSTEG - нестойкость к атакам пассивных противников, возможность автоматического детектирования наличия скрытого сообщения. Ориентирована на ОС MS-DOS.
- JPHS Gifshuffle - Сокрытие данных в графических файлах в формате Gif. Сокрытие инф. посредством изменения порядка цветов в палитре. Возможность предварительного сжатия или шифрования скрываемого сообщения.
- Hide-and-Seek - Сокрытие информации путём замены младших битов цветовых индексов точек изображения. Использует алгоритмы шифрования "Blowfish", осуществляет случайный выбор точек хранения. Ориентирована на ОС MS-DOS.
- Steganos - Сокрытие в граф. файлах BMP, DIP, VOC, WAV, ASCII. Сокрытие информации путем замены младших бит элементов контейнера. Возможность предварительного шифрования скрываемого сообщения. Ориентировано на ОС MS-DOS
- DC-Stegano. Сокрытие данных в графических файлах в формате PCX. Сокрытие посредством замены младших битов ЦВЗ индексов точек изображения. Отсутствие стегоключа, строго заданный размер изображения контейнера

Лекция 10

Анализ угроз и оценка устойчивости стеганографической системы

Анализ угроз и оценка устойчивости системы стеганографической защиты информации

Для каждой из задач цифровой стеганографии необходимо определенное соотношение устойчивости скрытого сообщения к внешним влияниям и размера скрытого сообщения. В большинстве случаев имеет место зависимость надежности системы от объема встраиваемого сообщения



Взаимосвязь между надежностью стеганосистемы и объемом встраиваемого сообщения при неизменном размере контейнера

Таким образом, в зависимости от выбранных целей, можно определить необходимое соотношение надежности и объема встраиваемого сообщения в стеганосистеме, что приводит к использованию разных методов стеганографии

Стегоанализ - оценки перехваченного контейнера на предмет наличия в нем скрытого сообщения. Встраивание скрытого сообщения приводит к изменению свойств контейнера (ухудшение характеристик) - это может указывать на встроенное сообщение и приведёт к тому, что идея стеганографии не будет выполнена.

Основная цель стеганоанализа - моделирование стеганографических систем и их исследование для получения качественных и количественных оценок надежности использования стеганопреобразования, а также построение методов выявления скрываемой в контейнере информации, ее модификации или разрушения.

Стеганосистемы делятся по уровню обеспечения секретности на теоретически устойчивые, практически устойчивые и неустойчивые системы.

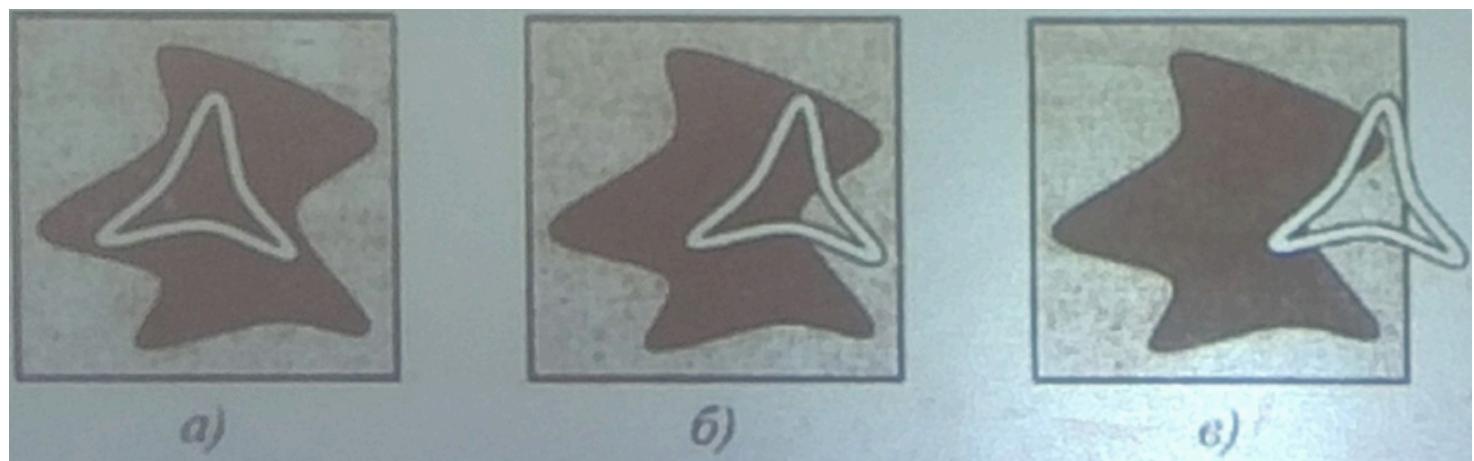
- **Теоретически устойчивая** (абсолютно надежная) стеганосистема скрывает информацию только в тех фрагментах контейнера, значение элементов которых не превышает уровень

шумов или ошибок квантования, и при этом теоретически доказано, что невозможно создать стеганоаналитический метод выявления скрытой информации.

- **Практически устойчивая стеганосистема** так изменяет фрагменты контейнера, что их можно выявить, но при этом известно, что на данный момент необходимые стеганоаналитические методы у нарушителя отсутствуют или пока что не разработаны.

Неустойчивая стеганосистема скрывает информацию таким образом, что существующими стеганоаналитическими средствами ее можно выявить.

Стеганографический анализ обнаруживает уязвимые места стеганографического преобразования и улучшает его так, чтобы все изменения, внесенные в контейнер, оказались бы в области теоретической или, по крайней мере, практической неразличимости.



Соотношение методов стеганозащиты и стеганоанализа:

- а - теоретически устойчивая стегано система;
- б - практически устойчивая стегано система;
- в - неустойчивая стегано система



- область практической неразличимости, в которой изменения контейнера не распознаются существующими у нарушителя аналитическими методами;



- область теоретической неразличимости, в которой скрытые элементы практически не могут быть распознаны, поскольку находятся ниже уровня шумов и ошибок квантования;



- область защиты стеганографической системы.

Нарушитель может быть:

- пассивный - способен только обнаружить факт наличия стеганоканала и узнать о содержании сообщения. Возможность "прочитать" сообщение после его обнаружения, зависит от устойчивости системы.
- активный - способен не только обнаружить стеганоканал и сообщение, но и удалить или разрушить скрытое сообщение.

- злонамеренный - наиболее опасный, способен не только разрушать, но и создавать фальшивые стеганограммы (дезинформацию).

Для осуществления угроз нарушитель применяет атаки.

Чтобы процесс стеганоанализа был успешен необходимо:

- наличие стеганосредства для анализа, используемого для скрытия сообщения;
- наличие возможности восстановления используемых в системе алгоритмов (стеганографических и криптографических); выполнение их экспертного анализа и разработки алгоритмов определения ключей;
- наличие вычислительных ресурсов необходимой мощности для проведения стеганоанализа
- поддержание на высоком уровне необходимых теоретических и практических знаний.

Стеганосистема считается взломанной, если нарушителю удалось, хотя бы, доказать существование скрытого сообщения в перехваченном контейнере.

Нарушитель способен осуществлять любые типы атак и имеет неограниченные вычислительные возможности, если ему не удается подтвердить гипотезу о том, что в контейнере скрыто секретное сообщение, то стеганографическая система считается устойчивой.

Выделяют несколько этапов взлома стеганографической системы:

- Обнаружение факта присутствия скрытой информации.
 - Извлечение скрытого сообщения.
 - Видоизменение (модификация) скрытой информации
 - Запрет на выполнение любой пересылки информации, в том числе скрытой
- Первые два этапа являются пассивными атаками, а последние - активными.

Из криptoанализа можно выделить следующие атаки на шифрованные сообщения :

- атака с использованием только шифртекста;
- атака с использованием открытого текста;
- атака с использованием выбранного открытого текста;
- адаптивная атака с использованием открытого текста;
- атака с использованием выбранного шифртекста.

Аналогично можно выделить следующие типы атак на стеганосистемы:

- **Атака по известному заполненному контейнеру.** У злоумышленника есть один или несколько заполненных контейнеров (одинаковым методом). Его задачей является нахождение стеганоканала, и также извлечение скрытого сообщения или ключа.
- **Атака по известному встроенному сообщению.** В основном используется для систем защиты интеллектуальной собственности, например, когда ЦВЗ - известный логотип. Задана злоумышленнику, в таком случае, - получение ключа. Задача является практически неразрешимой, когда заполненный контейнер, соответствующий скрытому сообщению, неизвестен.

- **Атака на основе выбранного скрытого сообщения.** Злоумышленник может предлагать свои сообщения для передачи и изучать полученные заполненные контейнеры.
- **Адаптивная атака на основе выбранного скрытого сообщения.** Является частным случаем атаки на основе выбранного скрытого сообщения. Злоумышленник может выбирать сообщения для передачи адаптивно, в зависимости от предыдущих результатов анализа заполненных контейнеров.
- **Атака на основе выбранного заполненного контейнера.** Обычно используется для систем ЦВЗ Злоумышленник имеет детектор заполненных контейнеров по типу «черного ящика» и несколько заполненных контейнеров.

Исследуя результаты прохождения заполненных контейнеров через детектор, т.е. скрытые сообщения, можно выявить ключ.

- **Атака на основе известного пустого контейнера.** Если злоумышленник имеет пустой контейнер, то сравнивая его с предположительно заполненным, может выявить факт наличия стеганоканала. Этот случай является довольно простым, но задача усложняется, если пустой контейнер имеет некие деформации (например, добавление шума). Тогда можно рассчитывать на построение стойкой стеганосистемы.
- **Атака на основе выбранного пустого контейнера.** Злоумышленник имеет возможность заставить отправителя использовать, заранее выбранный им, пустой контейнер, в котором будет легко выявить скрытое сообщение.
- **Атака по известной математической модели контейнера.** Злоумышленник ищет различия между подозреваемым заполненным контейнером и его известной моделью. Например, биты в середине определенной части изображения являются коррелированными, тогда отсутствие такой корреляции служит сигналом о наличии скрытого сообщения. В таком случае, задачей отправителя является соблюдение отсутствия нарушений статистики контейнера.

Также вышеперечисленные атаки могут быть скомбинированы. Чем больше злоумышленник знает о стеганосистеме тем более эффективной будет атака.

Безопасность стеганосистем, как и криптографических систем, описывается и оценивается их стойкостью (стеганографической стойкостью или стеганостойкостью).

Стеганостойкость - это способность стеганосистем скрывать факт передачи скрытого сообщения, способность противостоять попыткам злоумышленника разрушить, исказить, удалить скрываемое сообщение, а также способность подтвердить или опровергнуть подлинность скрытого сообщения.

Стеганостойкость можно разделить на:

- стойкость к обнаружению факта передачи (существования) скрываемого сообщения;
- стойкость к извлечению скрываемого сообщения;
- стойкость к навязыванию ложных сообщений по каналу скрытой связи (имитостойкость) - способность стеганосистемы находить и отвергать скомпрометированные злоумышленниками контейнеры;
- стойкость к восстановлению секретного ключа стеганосистемы - способность стеганосистемы противостоять попыткам нарушителей вычислить секретный ключ.

Лекция 11

Метод замена наименее значащего бита Метод Куттера-Джордана-Боссена

Метод наименее значимых битов (LSB - Least Significant Bit): Замена наименее значимых битов пикселей данными сообщения.

Преимущества: Простота реализации.

Недостатки: Относительно низкая устойчивость к сжатию и атакам. Может быть обнаружен с помощью стеганоанализа.

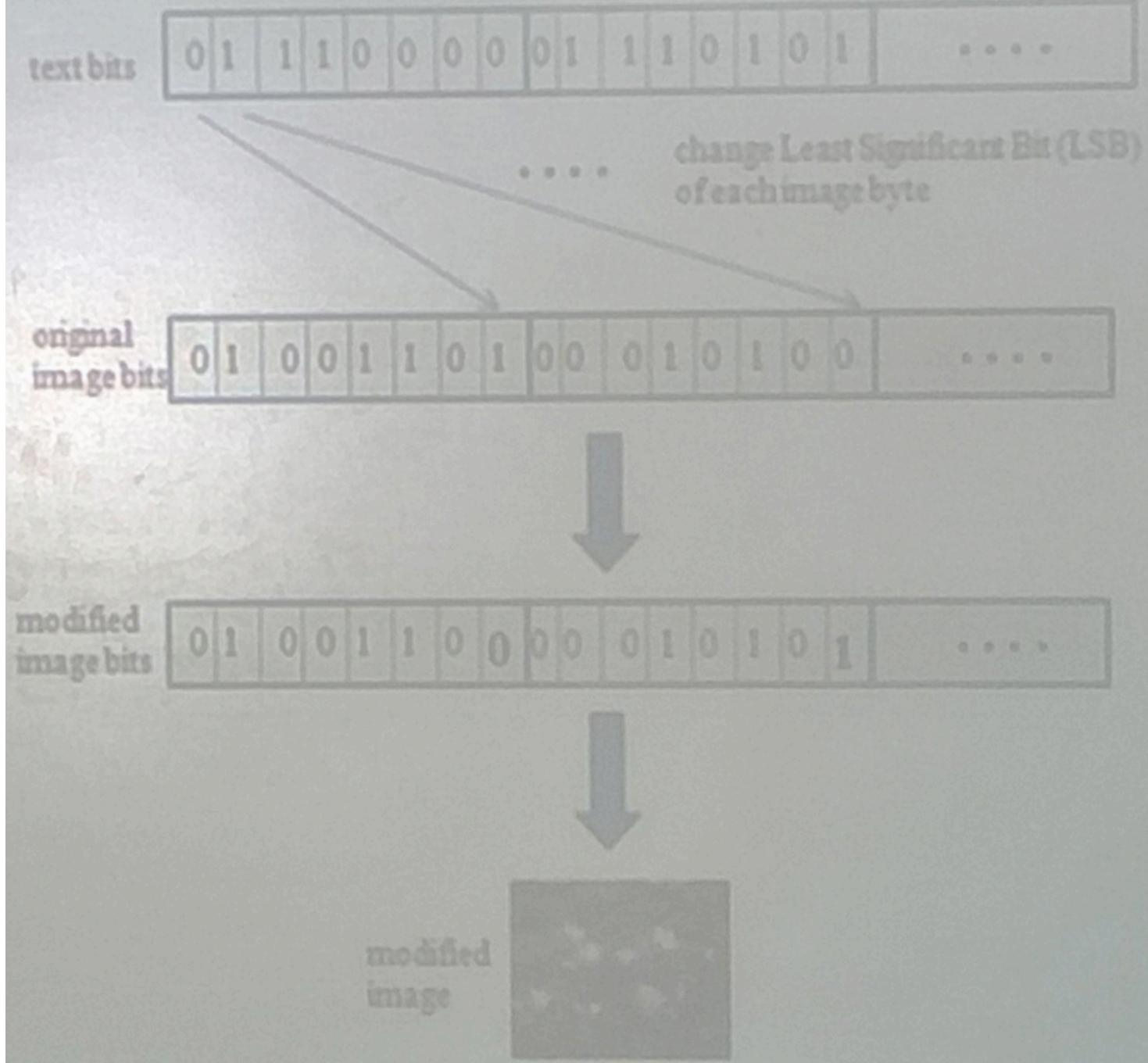
Пример: Если бит сообщения равен 1, а наименее значимый бит пикселя равен 0, бит пикселя заменяется на 1. Аналогично для бита 0.

Суть метода замена наименее значащего бита (Least Significant Bits - LSB) заключается в скрытии информации путем изменения последних битов изображения, кодирующих цвет на биты скрываемого сообщения.

Рассчитаем пропускную способность метода. Если отбросить в расчетах, обычно незначительную относительно размера изображения, служебную информацию в начале файла, то мы имеем возможность скрытно передать сообщение размером в 1/8 размера контейнера ("размазанную" по последним битам в каждом байте матрицы цветов пикселей) или же размером в 1/4 контейнера (соответственно при использовании 2 последних битов в байтах).

Важная информация (лучше запомнить)

В формате `.bmp` изображение хранится, как матрица значений оттенков цвета для каждой точки, если каждая из компонентов пространства RGB (канал цвета) хранится в одном байте, она может принимать значения от 0 до 255, что соответствует 24-битной глубине цвета.



Т.е. метод состоит в простой замене на бит внедряемого сообщения, будь то 0 или 1.

Изменения значения пикселей при последовательном внедрении в них сообщения 1001:

51 80 121 62 заменяет на 51 80 120 63

Пример:

P: (001001111101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11100111)

A: 01000001

P': (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11100111)

Небольшая модификация данной стеганографической техники позволяет исп. для встраивания сообщения два или более младших битов. Это даёт возможность увеличить объём скрытой информации в контейнере, но скрытость сильно снижается , что облегчает обнаружение стеганографии.

Достоинства и недостатки:

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 характеристика распределения значений диапазона младших битов отсчётов цифрового сигнала.

Лекция 12

Метод Куттера-Джордана-Боссена - стеганографический метод, осуществляющий внедрение ЦВЗ в изображение. Метод был представлен Мартином Куттером, Фредериком Джорданом и Фрэнком в апреле 1998 г., как алгоритм встраивания синего цвета изображения, имеющего RGB-кодирование, поскольку к синему цвету зрительная система человека является наименее чувствительной.

Метод Куттера-Джордана-Боссена относится к классу алгоритмов, осуществляющих скрытие данных в пространственной области.

В алгоритмах этого класса внедрение ЦВЗ выполняется за счёт изменения яркостной либо цветовых компонент пикселя.

В этом методе отдельные биты водяного знака многократно внедряются в изображение путём изменения значения синего канала в пикселе. Это изменение пропорционально яркостной

компоненте пикселя и может принимать как положительные, так и отрицательные значения в зависимости от значения встраиваемого бита водяного знака.

Основными свойствами, которыми должен обладать ЦВЗ - это неразличимость для человеческого глаза и устойчивость к различным искажениям и изменениям изображения.

Метод Куттера-Джордана-Боссена удовлетворяет первому требованию за счёт встраивания битов водяного знака именно в синий канал пикселя, так как человеческий глаз наименее чувствителен именно к этому цвету.

Устойчивость к искажениям изображения обеспечивается путём многократного встраивания битов ЦВЗ в различных частях исходного изображения.

Применение этого метода показало высокую эффективность при его использовании для защиты авторских прав изображений и видеоматериалов, а также для проверки целостности изображений и QR-кодов.

ЦВЗ: Основные понятия

ЦВЗ - информация, внедренная в цифровой контент (изображение, аудио, видео и т.д.) для защиты авторских прав, аутентификации, отслеживания копий и других целей.

Встраивание ЦВЗ — процесс добавления ЦВЗ в контент.

Извлечение ЦВЗ — процесс восстановления ЦВЗ из контента.

Стойкость — способность ЦВЗ выдерживать различные виды атак (обработка изображений, сжатие, геометрические преобразования и т.д.) без потери возможности извлечения.

Невидимость (незаметность) — степень, в которой ЦВЗ заметен для человеческого восприятия. Идеальный ЦВЗ должен быть невидимым.

Типы ЦВЗ:

1. Видимые ЦВЗ — накладываются поверх изображения и видны невооружённым глазом (например, логотип телеканала).

2. Невидимые ЦВЗ — встраиваются в изображение таким образом, что они незаметны для человеческого глаза, но могут быть извлечены с помощью специального программного обеспечения.

3. Слепые ЦВЗ — извлекаются из контента без необходимости использования исходного контента.

4. Неслепые ЦВЗ — требуют наличия исходного контента для извлечения ЦВЗ.

Методы встраивания:

1. Пространственные методы — непосредственно изменяют значения пикселей в изображении.

2. Частотные методы — преобразуют изображение в частотную область (например, с помощью дискретного косинусного преобразования — DCT) и встраивают ЦВЗ в коэффициенты преобразования.

Метод Kutter-Jordan-Bossen (KJB)

Общий принцип Метода КJB является пространственным методом встраивания невидимого водяного знака.

Он основан на следующем принципе:

1. Локальная адаптация — вместо того, чтобы встраивать ЦВЗ во все пиксели изображения, метод КJB выбирает только те пиксели, которые имеют достаточную локальную вариацию. Это позволяет минимизировать видимые искажения, вызванные встраиванием ЦВЗ.
2. Анализ локальной статистики — для выбора пикселей, в которые будет встроен ЦВЗ, метод КJB анализирует локальную статистику изображения, в частности, стандартное отклонение значений пикселей в окрестности каждого пикселя.
3. Модификация пикселей — после выбора пикселей, в которые будет встроен ЦВЗ, их значения модифицируются в соответствии с определённым правилом, которое зависит от бита ЦВЗ, который необходимо встроить.

Алгоритм встраивания метода КJB

Алгоритм встраивания метода состоит из следующих шагов:

1. Разбиение изображения на блоки — изображение разбивается на неперекрывающиеся блоки размером $N \times N$ пикселей (например, 3×3 или 5×5). Размер блока определяет локальность, в которой оценивается вариация.
2. Вычисление стандартного отклонения — для каждого блока вычисляется стандартное отклонение значений пикселей (обычно яркости или одного из цветовых каналов).
3. Выбор пикселей для встраивания — блоки, стандартное отклонение которых превышает определённый порог T (заранее определённый), считаются пригодными для встраивания ЦВЗ. В каждом таком блоке выбирается один пиксель для встраивания. Часто выбирают пиксель с максимальной яркостью.
4. Встраивание бита ЦВЗ — значение выбранного пикселя модифицируется в соответствии с битом ЦВЗ, который необходимо встроить. Например, если необходимо встроить бит "1", значение пикселя увеличивается на определённую величину α , а если необходимо встроить бит "0", значение пикселя уменьшается на α .

Формула для встраивания:

$$I'(x, y) = I(x, y) + \alpha * W(i), \text{ где:}$$

- $I'(x, y)$ — значение пикселя после встраивания ЦВЗ
- $I(x, y)$ — значение пикселя до встраивания ЦВЗ
- α — сила ЦВЗ (параметр, определяющий степень воздействия на пиксель)
- $W(i)$ — бит ЦВЗ (либо +1, либо -1, для представления 1 и 0 соответственно).

5. Повторение: Шаги 1-4 повторяются для каждого бита ЦВЗ.

Алгоритм извлечения метода КВ

Состоит из следующих шагов:

1. Разбиение изображения на блоки — изображение разбивается на блоки размером $N \times N$ пикселей, как и при встраивании.
2. Вычисление стандартного отклонения — для каждого блока вычисляется стандартное отклонение значений пикселей.
3. Выбор пикселей для извлечения — блоки, стандартное отклонение которых превышает порог T , считаются пригодными для извлечения ЦВЗ. В каждом таком блоке выбирается пиксель, в который, предположительно, был встроен ЦВЗ (например, пиксель с максимальной яркостью).
4. Извлечение бита ЦВЗ — бит ЦВЗ извлекается путём сравнения значения выбранного пикселя с некоторым порогом или с соседними пикселями. В простейшем случае можно сравнить значение пикселя с его исходным значением (если известен исходный контент) или оценить изменение значения относительно соседних пикселей.

Например, можно использовать следующее правило:

$$W'(i) = \text{sign}(I'(x, y) - I(x, y))$$

где:

- $W'(i)$ — извлечённый бит ЦВЗ.
- $\text{sign}()$ — функция, возвращающая +1, если аргумент положительный, и -1, если аргумент отрицательный.
- $I'(x, y)$ — значение пикселя после встраивания ЦВЗ.
- $I(x, y)$ — значение пикселя до встраивания ЦВЗ (требуется для неслерого извлечения).

Если исходное изображение неизвестно, можно использовать адаптивные методы, основанные на анализе локальных характеристик изображения.

5. Повторение: Шаги 1–4 повторяются для каждого бита ЦВЗ.

Преимущества и недостатки метода КВ

Преимущества:

1. Относительная простота реализации — алгоритм КВ достаточно прост для понимания и реализации.
2. Локальная адаптация — выбор пикселей для встраивания на основе локальной статистики позволяет минимизировать видимые искажения.
3. Неплохая стойкость к некоторым атакам — метод КВ может быть достаточно стойким к некоторым видам атак, таким как добавление шума, фильтрация и сжатие.

Недостатки:

1. Низкая стойкость к геометрическим атакам — метод КВ очень чувствителен к геометрическим преобразованиям (поворот, масштабирование, сдвиг), поскольку он основан на фиксированном местоположении пикселей.

2. Возможность визуального обнаружения — хотя метод KJB пытается минимизировать видимость ЦВЗ, при достаточно высокой силе ЦВЗ (большом значении а) ЦВЗ может быть визуально обнаружен.
3. Требуется оптимизация параметров — для достижения оптимального баланса между стойкостью и невидимостью необходимо тщательно оптимизировать параметры метода, такие как размер блока N, порог T и сила ЦВЗ а.
4. Уязвимость к коллизионным атакам — метод может быть уязвим к коллизионным атакам, когда злоумышленник пытается встроить свой ЦВЗ поверх оригинального, что может привести к неправильному извлечению оригинального ЦВЗ.

Модификация и улучшения метода KJB

Существуют различные модификации и улучшения метода KJB, направленные на повышение его стойкости и невидимости. Некоторые из них включают:

1. Использование адаптивного порога T — вместо фиксированного порога T можно использовать адаптивный порог, который зависит от локальных характеристик изображения.
2. Использование более сложных правил встраивания — вместо простого увеличения или уменьшения значения пикселя можно использовать более сложные правила встраивания, основанные на анализе соседних пикселей.
3. Использование частотных преобразований — можно комбинировать метод KJB с частотными преобразованиями, встраивая ЦВЗ в коэффициенты преобразования, выбранные на основе локальной статистики.
4. Синхронизация — для повышения стойкости к геометрическим атакам можно использовать методы синхронизации, которые позволяют восстановить ориентацию и масштаб изображения после геометрических преобразований.

Метод Куттера-Джордана-Боссена (KJB) является классическим и важным методом в области цифровых водяных знаков.

Представляет собой хороший пример пространственного метода, основанного на анализе локальной статистики изображения.

Хотя метод KJB имеет свои недостатки, он послужил основой для разработки многих других более совершенных методов ЦВЗ.

Понимание принципов работы метода KJB является важным для любого специалиста, работающего в области защиты информации и цифровых прав.

Лекция 13

ОБЗОР СТЕГОАЛГОРИТМОВ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ

По способу встраивания информации стегоалгоритмы делятся 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 «вплывается» (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.

В аддитивных методах внедрения ЦВЗ представляет собой последовательность чисел, длины, которая внедряется в выбранное подмножество отсчетов исходного изображения.

Для увеличения **робастности** внедрения во многих алгоритмах применяются широкополосные сигналы.

При этом информационные биты могут быть многократно повторены, закодированы с применением корректирующего кода, либо к ним может быть применено какое-либо другое преобразование, после чего они модулируются с помощью псевдослучайной гауссовской последовательности.

Такая последовательность является хорошей моделью шума, присущего в реальных изображений.

В то же время синтетические изображения (созданные на компьютере) не содержат шумов, и в них труднее незаметно встроить такую последовательность__.

Обычно легче первоначально сгенерировать равномерно распределенную последовательность.

Известен алгоритм преобразования такой последовательности в гауссовскую (алгоритм Бокса-Мюллера).

Преобразования Бокса-Мюллера, является псевдослучайных чисел выборки способ генерации пар независимого , стандарта, нормально распределены (ноль ожидания , блок дисперсии) случайных чисел, учитывая источник равномерно распределенных случайные числа.

Метод был впервые упомянут в 1934 году.

Выражается в двух формах – основная форма принимает два образца из равномерного распределения на интервале [0, 1], и отображает их на две стандартных, нормально распределенных выборки. Полярная форма принимает два образца из другого интервала, [-1, +1], и отображает их на два нормально распределенных образцы без использования синусоидального или косинуса.

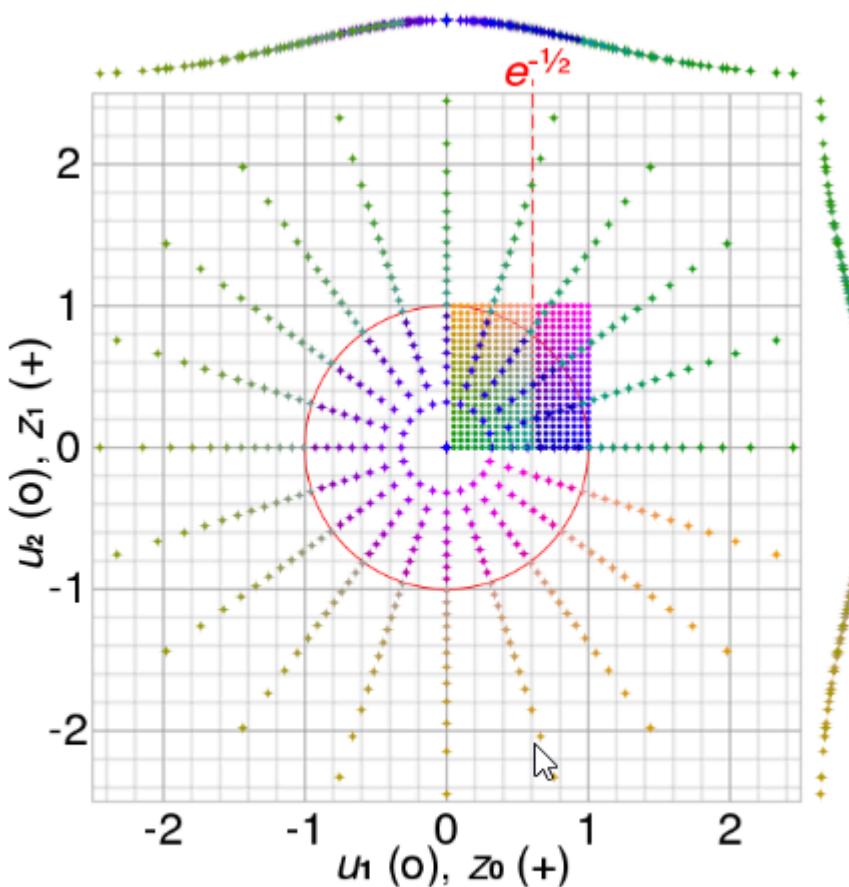


Рис.1 - Визуализация Box-Мюллера преобразования

Рис.1 - Визуализация Box-Мюллера преобразования

Основным недостатком этого метода является то, что само изображение в этом случае рассматривается, как шумовой сигнал.

Существует гибридный подход, когда часть информации об исходном изображении доступно входе извлечения информации, но неизвестно собственно исходное изображение.

Корреляционный метод позволяет только обнаружить наличие или отсутствие ЦВЗ. Для получения же всех информационных битов нужно протестировать все возможные последовательности, что является крайне вычислительно сложной задачей.

Наиболее ярким представителем алгоритмов внедрения ЦВЗ на основе использования широкополосных сигналов является **алгоритм Кокса**.

В данном алгоритме в блок размером 8x8 осуществляется встраивание 1 бита ЦВЗ. Описано две реализации алгоритма: псевдослучайно могут выбираться два или три коэффициента ДКП. Рассмотрим вариацию алгоритма с двумя выбираемыми коэффициентами. Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины:

$$|c_b(j_{i,j}, k_{i,1})| - |c_b(j_{i,2}, k_{i,2})| > \varepsilon, \text{ if } s_i = 0$$

$$|c_b(j_{i,j}, k_{i,1})| - |c_b(j_{i,2}, k_{i,2})| < -\varepsilon, \text{ if } s_i = 1.$$

ЦВЗ представляет собой последовательность псевдослучайных чисел, распределенных по гауссовскому закону, длиной 1000 чисел.

Достоинством алгоритма является то, что благодаря выбору наиболее значимых коэффициентов водяной знак является более робастным при сжатии и других видах обработки сигнала.

Вместе с тем алгоритм уязвим для атак.

Обзор алгоритмов на основе слияния ЦВЗ и контейнера

Если вместо последовательности псевдослучайных чисел в изображение встраивается другое изображение (например, логотип фирмы), то соответствующие алгоритмы внедрения называются алгоритмами слияния.

Размер внедряемого сообщения намного меньше размера исходного изображения.

Перед встраиванием оно может быть зашифровано или преобразовано каким-нибудь иным образом.

У таких алгоритмов есть два преимущества.

Во-первых, можно допустить некоторое искажение скрытого сообщения.

Во-вторых, наличие внедренного логотипа является более убедительным доказательством прав собственности, чем наличие некоторого псевдослучайного числа.

A29 Метод блочного скрытия

Метод блочного скрытия — это еще один подход к реализации метода замены и заключается в следующем. Изображение-оригинал разбивается на непересекающиеся блоки произвольной конфигурации, для каждого из которых вычисляется бит четности. В каждом блоке выполняется скрытие одного секретного бита. Встраивание 1 бита происходит в 1 блок контейнера. Низкая устойчивость к искажениям. Низкая пропускная способность. Высокая устойчивость к детектированию и извлечению сообщения. Высокое быстродействие.

В алгоритме внедряется черно-белое изображение (логотип), размером до 25 % от размеров исходного изображения.

Перед встраиванием выполняется одноуровневая декомпозиция как исходного изображения, так и эмблемы с применением фильтров Хаара (определяется посредством вычитания среднего значения области темных пикселей из среднего значения области светлых пикселей). Вейвлет-коэффициенты исходного изображения - логотип. Модификации подвергаются все коэффициенты преобразования

Исходное изображение
в 24-битном представлении

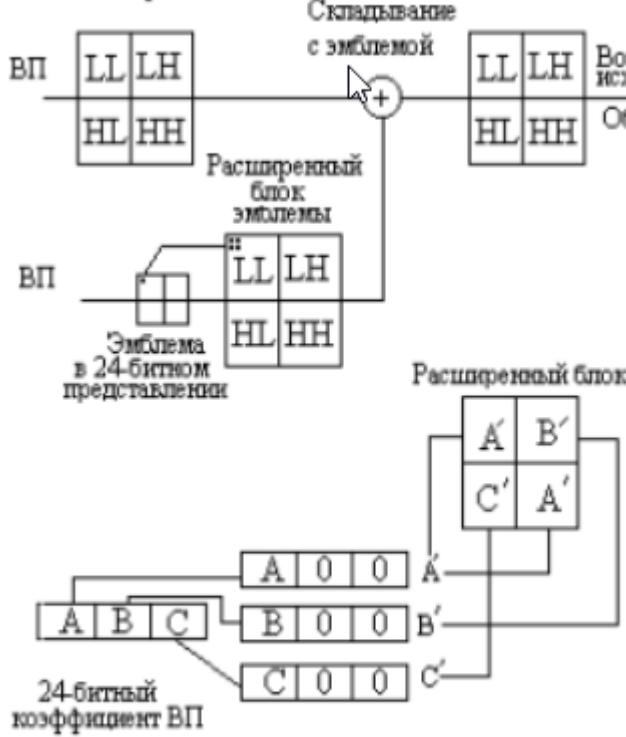


Рис. Схема встраивания ЦВЗ

Рис. Схема встраивания ЦВЗ

Вначале коэффициенты каждого поддиапазона, как исходного изображения, так и логотипа представляются 24 битами (из которых один бит отводится на знак). Так как размер логотипа в 4 раза меньше исходного изображения, то необходимо увеличить количество его коэффициентов.

Для этого выполняются следующие действия.

1. Обозначим, через А, В, и С соответственно, старший, средний и младший байты 24-битного представления логотипа. На рис. показано формирование трех 24-битных чисел А, В и С.
2. Старший байт каждого из этих чисел представляет собой соответственно А, В, или С, два других байта заполняются нулями.
3. Затем формируется расширенный вчетверо блок коэффициентов логотипа.
4. После чего он поэлементно складывается с 24-битной версией исходного Изображения

Данный алгоритм позволяет скрыть довольно большой объем данных в исходном изображении: до четверти от размеров исходного изображения

A30

Исходное и внедряемое изображения подвергаются вейвлет-преобразованию (Вейвлет – преобразование сигналов является обобщением спектрального анализа, типичный представитель которого – классическое преобразование Фурье).

Для встраивания используются все коэффициенты детальных поддиапазонов. Множество этих коэффициентов разбивается на неперекрывающиеся блоки.

Блоки обозначают местоположение коэффициента и уровень разрешения. Водяной знак прибавляется к элементам исходного изображения по формуле:

$$f_{k,l}^*(m,n) = f_{k,l}(m,n) + \alpha_{k,l} \sqrt{S(f_{k,l}(m,n))} w_{k,l}(m,n)$$

где S — коэффициент масштаба, вычисляемый по формуле

$$S(f_{k,l}(m,n)) = \sum_{u,v} C(u,v) |T(f_{k,l}(m,n))|^2$$

C(u,v) — взвешивающая матрица, определяющая частотную чувствительность системы зрения человека, T — оператор ДПФ (Дискретное преобразование Фурье).

Таким образом, алгоритм использует довольно сложную модель человеческого зрения.

Для обнаружения в детекторе может быть использовано как вычисление корреляционной функции, так и визуальное сравнение.

Стеганографические методы на основе квантования

Принципы встраивания информации с использованием квантования. Дизеризованные квантователи.

Под квантованием понимается процесс сопоставления большого (возможно и бесконечного) множества значений с некоторым конечным множеством чисел. При этом происходит уменьшение объема информации за счет ее искажения.

Квантование находит применение в алгоритмах сжатия с потерями. Различают скалярное и векторное квантование. При векторном квантовании, в отличие от скалярного, происходит отображение не отдельно взятого отсчета, а их совокупности (вектора).

Из теории информации известно, что векторное квантование эффективнее скалярного по степени сжатия, обладая большей сложностью.

В кодере квантователя вся область значений исходного множества делится на интервалы, и в каждом интервале выбирается число его представляющее. Это число есть кодовое слово квантователя и обычно бывает центром интервала квантования. Множество кодовых слов называется **книгой квантователя**. Все значения, попавшие в данный интервал, заменяются в кодере на соответствующее кодовое слово.

В декодере принятому числу сопоставляется некоторое значение.

Интервал квантования обычно называют **шагом квантователя**.

Встраивание информации с применением квантования относится к нелинейным методам.

Пропускная способность которой эквивалентна пропускной способности стегосистемы, имеющей на приеме исходный сигнал. При этом делается предположение о гауссовском характере исходного сигнала.

Наиболее предпочтительно внедрение информации в спектральную область изображения.

Если при этом используются линейные методы, то встраивание ЦВЗ производят в средние полосы частот.

Это объясняется тем, что энергия изображения сосредоточена, в основном, в низкочастотной (НЧ) области.

Следовательно, в детекторе ЦВЗ в этой области наблюдается сильный шум самого сигнала.

В высокочастотных (ВЧ) областях большую величину имеет шум обработки, например, сжатия.

В отличие от линейных, нелинейные схемы встраивания информации могут использовать НЧ области, так как мощность внедряемого ЦВЗ не зависит от амплитуды коэффициентов.

Это объясняется тем, что в нелинейных алгоритмах скрытия не используется корреляционный детектор, коэффициенты малой и большой амплитуды обрабатываются одинаково.

Дизеризованный квантователь может применяться и в развитии техники расширения спектра сигнала в стеганографии. Изменение обычного метода встраивания с расширением спектра заключается в простой замене сложения на операцию квантования.

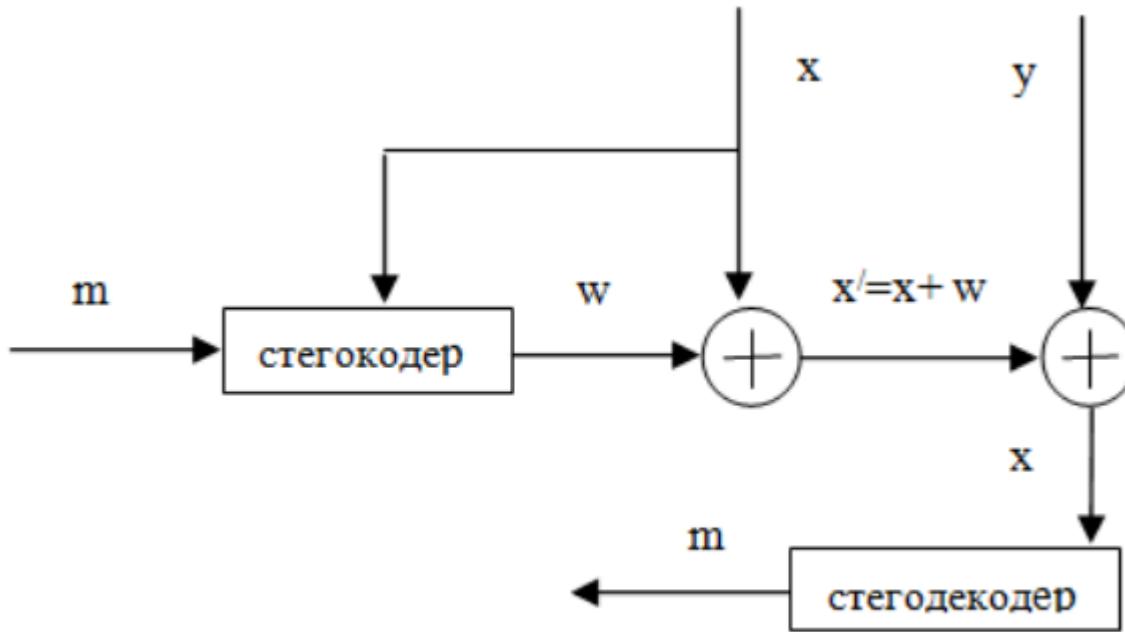


Рис. Модель «слепой» стегосистемы

Рис. Модель «слепой» стегосистемы

На рисунке показано, как может быть построена подобная «слепая» стегосистема, пропускная способность которой эквивалентна пропускной способности стегосистемы, имеющей на приеме исходный сигнал. При этом делается предположение о гауссовском характере исходного сигнала.

СКРЫТИЕ ДАННЫХ В АУДИОСИГНАЛАХ

Требования, которые могут быть предъявлены к стегосистемам, применяемым для встраивания информации в аудиосигналы:

- скрываемая информация должна быть стойкой к наличию различных окрашенных шумов, сжатию с потерями, фильтрованию, аналогово-цифровому и цифро-аналоговому преобразованиям;
- скрываемая информация не должна вносить в сигнал искажения, воспринимаемые системой слуха человека;
- попытка удаления скрываемой информации должна приводить к заметному повреждению контейнера (для ЦВЗ);
- скрываемая информация не должна вносить заметных изменений в статистику контейнера;

Для внедрения скрываемой информации в аудиосигналы можно использовать методы, применимые в других видах стеганографии.

Например, можно внедрять информацию, замещая наименее значимые биты (все или некоторые). Или можно строить стегосистемы, основываясь на особенностях аудиосигналов и системы слуха человека. Систему слуха человека можно представить, как анализатор частотного спектра, который может обнаруживать и распознавать сигналы в диапазоне 10 – 20000 Гц. Систему слуха человека можно смоделировать, как 26 пропускающих фильтров, полоса пропускания которых увеличивается с увеличением частоты. Система слуха человека различает изменения фазы сигнала слабее, нежели изменения амплитуды или частоты.

Аудиосигналы можно разделить на три класса:

- разговор телефонного качества, диапазон 300 – 3400 Гц;
- широкополосная речь 50 – 7000 Гц;
- широкополосные аудиосигналы 20 – 20000 Гц.

Практически все аудиосигналы имеют характерную особенность. Любой из них представляет собой достаточно большой объем данных, для того, чтобы использовать статистические методы внедрения информации

Лекция 14

ОБЗОР МЕТОДОВ ЦИФРОВОЙ АУДИО СТЕГАНОГРАФИИ

Основная цель стеганографии - это безопасный обмен данными совершенно незаметным образом, который отрицает сам факт наличия секретных сообщений. Если метод стеганографии вызывает у кого-то подозрения, то такой метод необходимо признать неудачным.

Основная модель аудио стеганографии состоит из носителя (аудио файл), сообщения и пароля. Под носителем понимается файл, который скрывает или будет скрывать секретную информацию.

Стеганографическая модель изображена на рис.1.

Сообщение - это данные, которые отправитель хочет оставить в тайне. В качестве передаваемого сообщения могут выступать простой текст, изображение, аудио и другие типы файлов.

Пароль символизирует ключ, зная который, получатель сможет гарантированно декодировать

сообщение из файла.

Файл-носитель с конфиденциальной информацией называется стегофайлом.



Рисунок 1 - Стеганографическая модель

Рисунок 1 - Стеганографическая модель

Процесс сокрытия информации состоит из следующих двух шагов:

- Идентификация избыточных битов в файле-носителе. Избыточными битами называются те биты, которые могут быть модифицированы без порчи качества или нарушения целостности файла-носителя.
- Избыточные биты в файле-носителе заменяются битами секретной информации.

БАЗОВЫЕ ПОДХОДЫ В АУДИО СТЕГАНОГРАФИИ

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.2 представлена процедура такого кодирования

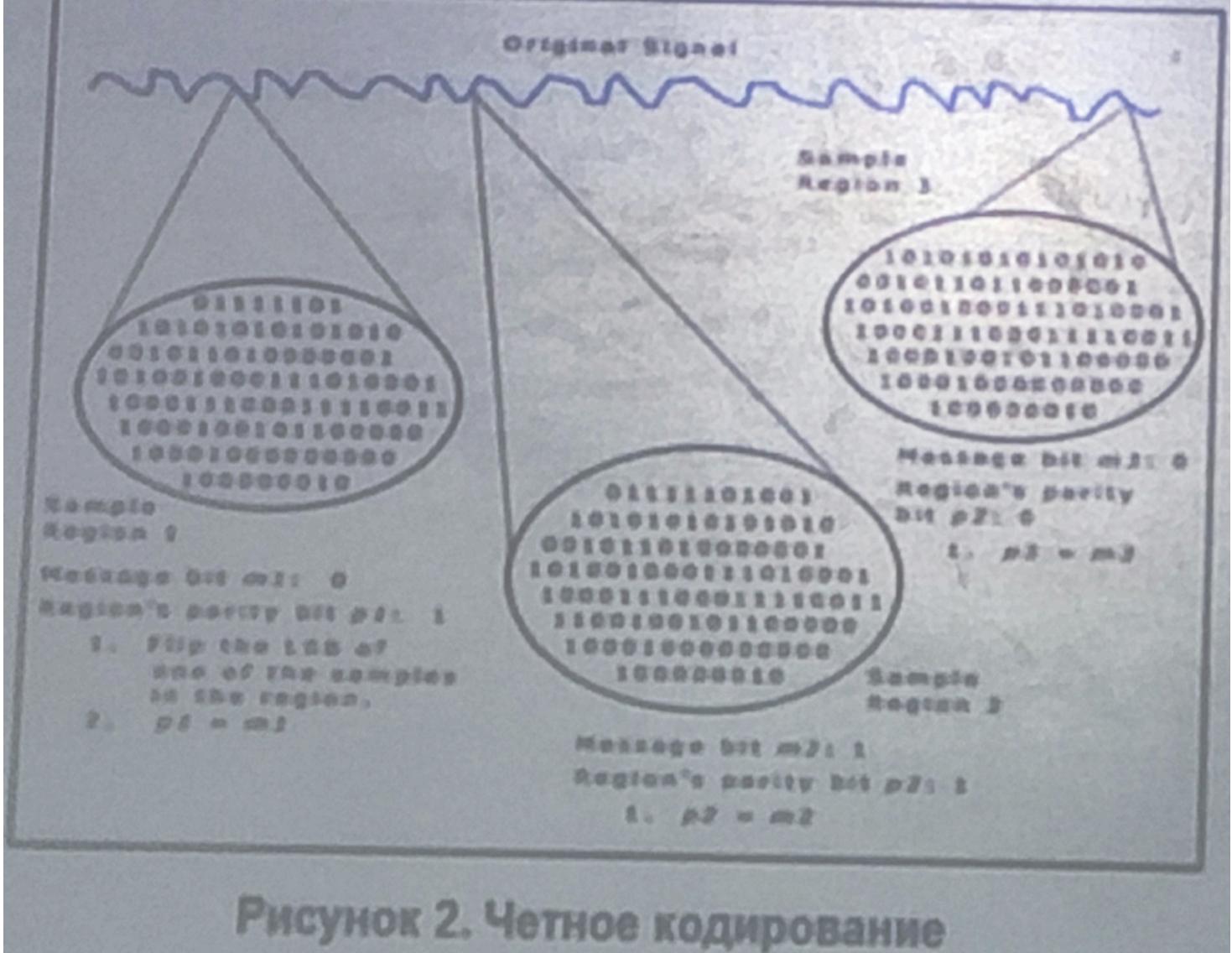


Рисунок 2. Четное кодирование

Рисунок 2. Четное кодирование

ФАЗОВОЕ КОДИРОВАНИЕ

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

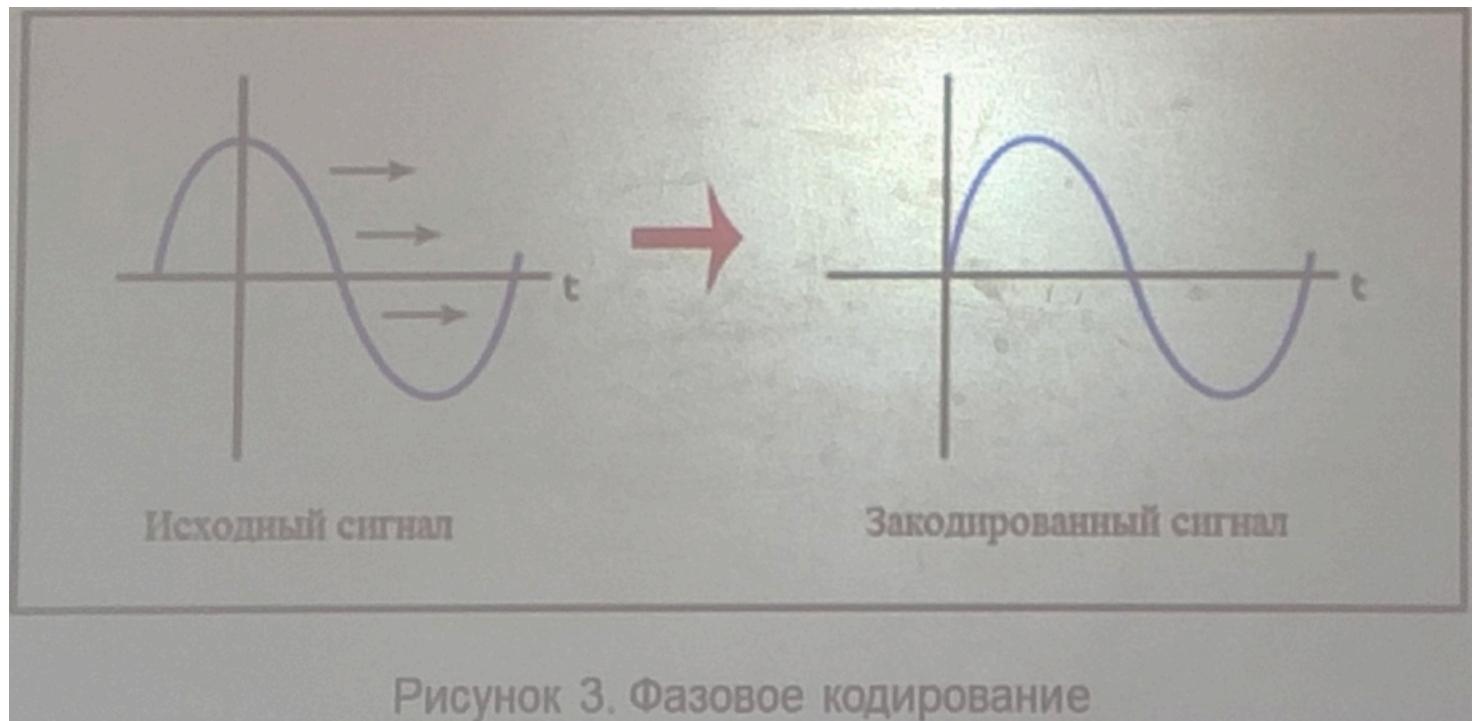


Рисунок 3. Фазовое кодирование

МЕТОД РАСШИРЕННОГО СПЕКТРА

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.4.

(Секретное сообщение -1-> Шифрование -2-> Кодирование сообщения -3-> Модулятор -4-> Чередование носителя сигнала -5-> Квантователь)

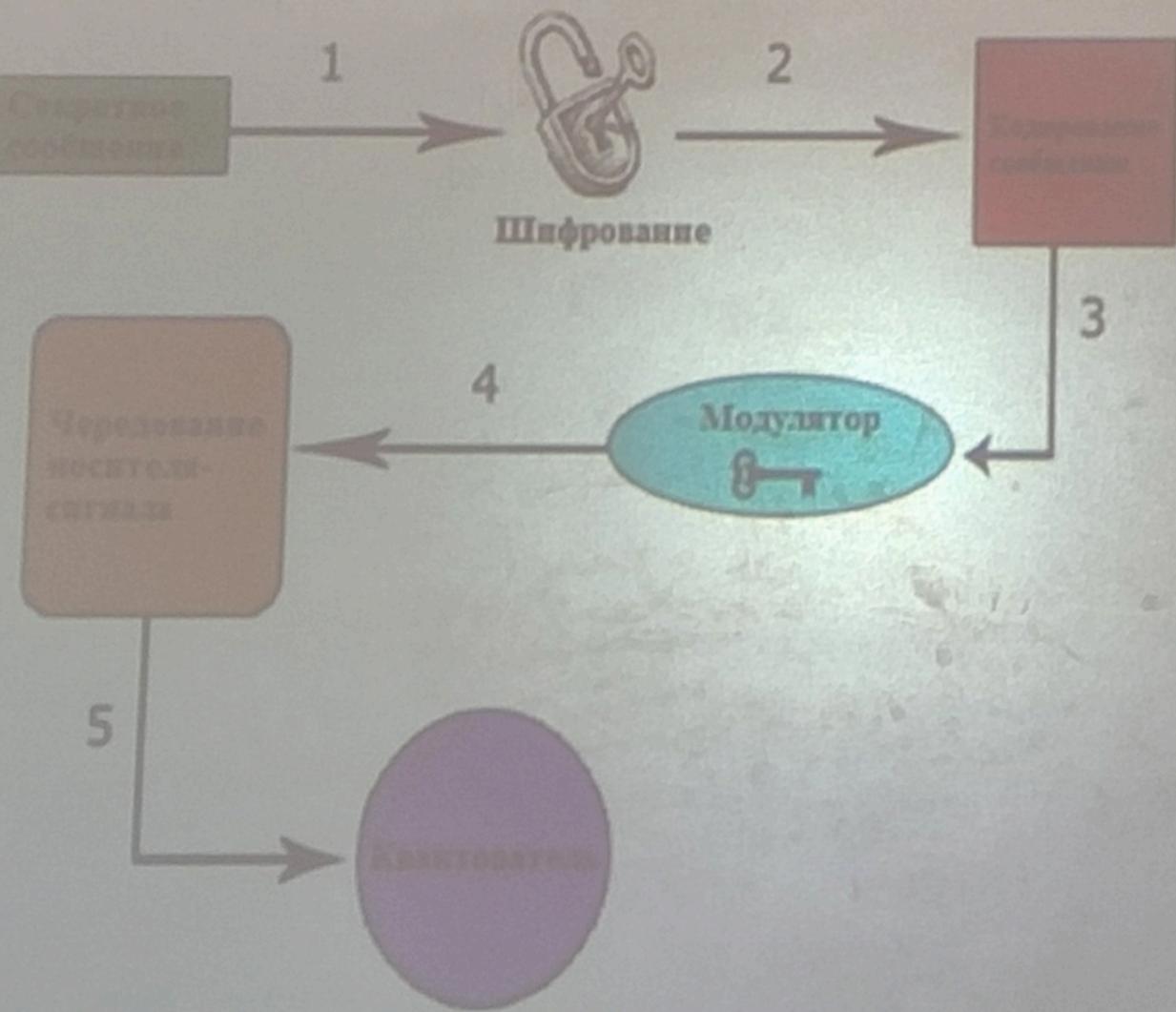


Рисунок 4. Схема работы метода расширенного спектра

Рисунок 4. Схема работы метода расширенного спектра

ЭХО-МЕТОД

Данный метод встраивает секретную информацию в звуковой файл, вводя эхо в дискретный сигнал. Главные преимущества эхо-метода - это высокая скорость передачи данных, а также повышенная устойчивость по сравнению с другими методами. 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.

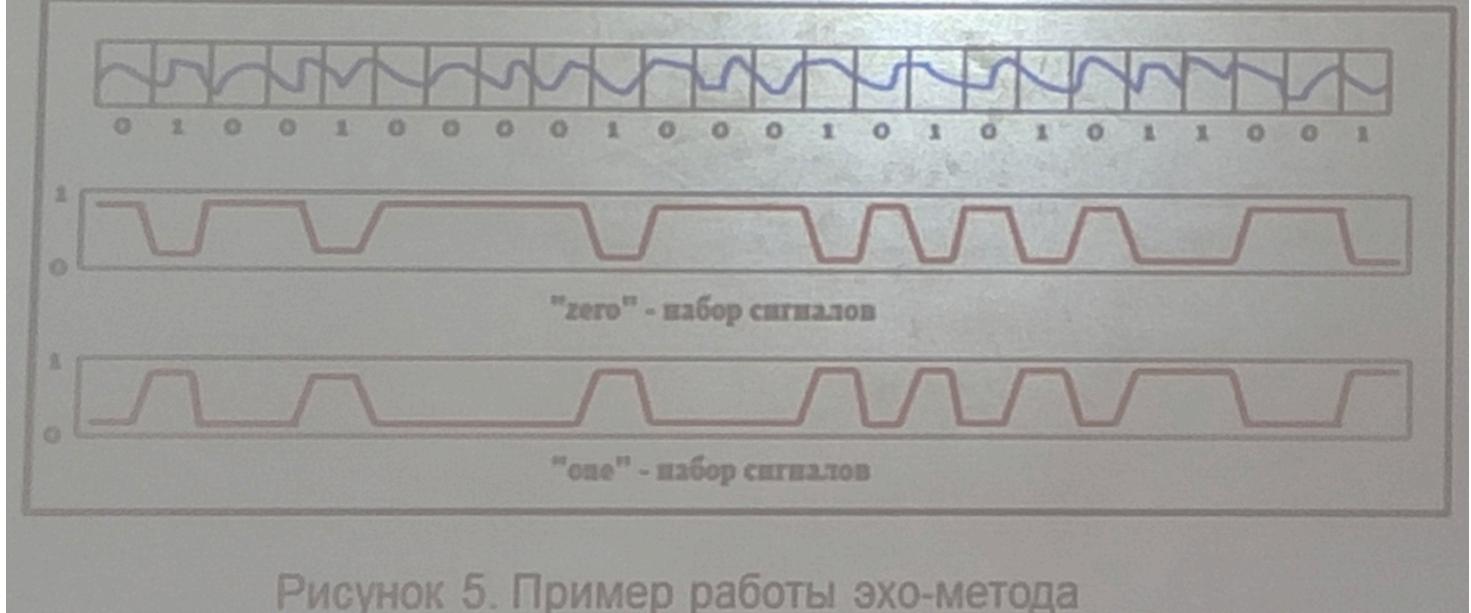


Рисунок 5. Пример работы эхо-метода

Рисунок 5. Пример работы эхо-метода

Основные недостатки использования таких методов как эхо, расширенного спектра и четности кодирования заключаются в том, что они вносят шум в аудиофайл, который может быть довольно различимым для человеческого уха, а также надежность данных методов вызывает вопросы.

Фазовое кодирование имеет основной недостаток, заключающийся в низкой скорости передачи данных из-за того, что секретное сообщение кодируется только на первом сегменте сигнала. Следовательно, этот метод используется только тогда, когда передается небольшое количество данных.

Обзор существующих решений в сфере стеганографического сокрытия информации на мобильных устройствах

В настоящее время существуют разные подходы и решения в области стеганографической защиты информации.

При анализе специального программного обеспечения трех наиболее популярных платформ мобильных устройств (iOS, Android), были получены следующие результаты:

- для мобильных iOS-устройств существуют доступных решений (платные и бесплатны), работающие с графическими стеганографическими контейнерами;
- для устройств, под управление Android, существуют приложения , часть работают с графическими стегоконтейнерами, часть приложений
- с цифровым видео и с аудио- данными. Провести обзор существующих решений для каждой из платформ , описать по 5 приложений с характеристиками для каждой.

iOS: 5 приложений для стеганографического сокрытия информации

| Название приложения | Описание и характеристики |
|---------------------|---|
| iWatermark+ | Позволяет встраивать невидимые стеганографические водяные знаки в фотографии. Поддерживает работу с фото и видео, пакетную обработку, |

| Название приложения | Описание и характеристики |
|----------------------------|--|
| | различные типы водяных знаков (текст, QR, подпись и др.), а также наложение метаданных. Предлагает как видимые, так и невидимые способы защиты. |
| Pictograph - Steganography | Использует метод изменения наименее значимых битов (LSB) в пикселях изображений для сокрытия текста или других изображений. Поддерживает шифрование AES-256 для дополнительной защиты скрытых данных. Позволяет скрывать сообщения и изображения внутри других изображений, без видимых изменений для человеческого глаза. |
| Secret Photo Vault | Приложение для скрытия фотографий и видео в защищённом хранилище. Помимо обычного скрытия, может использовать стеганографические методы для маскировки наличия защищённого контента (информация из общих знаний, так как прямых упоминаний в поиске нет). |
| Steganography+ | Позволяет скрывать текстовые сообщения внутри изображений, поддерживает отправку и извлечение скрытых данных через интерфейс приложения. Часто используется для защиты личной информации при передаче. |
| Hide It Pro | Многофункциональное приложение для скрытия фото, видео, аудио и заметок. Реализует методы стеганографии для маскировки файлов и защищает доступ паролем или биометрией (описание основано на общих сведениях о подобных приложениях). |

Android: 5 приложений для стеганографического сокрытия информации

| Название приложения | Описание и характеристики |
|---|---|
| Steg | Позволяет скрывать текстовые сообщения в изображениях (метод LSB), поддерживает как шифрование, так и декодирование сообщений. Прост в использовании, подходит для быстрой передачи скрытой информации (описание на основе общих сведений). |
| Audio Steganography | Приложение для сокрытия текстовых сообщений в аудиофайлах. Использует изменённые аудиосэмплы для внедрения информации без заметных искажений звука (описание на основе общих сведений). |
| PixelKnot | Разработано The Guardian Project. Позволяет скрывать сообщения в фотографиях, используя LSB-метод, с последующей отправкой через мессенджеры и e-mail. Поддерживает шифрование скрываемого сообщения. |
| Steganography Master | Многофункциональное приложение для сокрытия текста и файлов в изображениях и аудиофайлах. Поддерживает различные алгоритмы стеганографии и шифрования (описание на основе общих сведений). |
| Hide Photos, Video and App Lock - Hide it Pro | Аналогичная версия для Android. Позволяет скрывать фото, видео, заметки и аудио, используя стеганографические методы и защищая доступ паролем или отпечатком пальца (описание на основе общих сведений). |

1. Приложения для iOS

1.1. Steganography Online

- **Описание:** Приложение для скрытия текста в изображениях с использованием LSB-метода (замена младших битов).
- **Формат контейнера:** JPEG, PNG
- **Особенности:** Простота использования, поддержка паролей.
- **Цена:** Бесплатно (с рекламой).

1.2. InSecret

- **Описание:** Позволяет прятать текст и небольшие файлы в изображениях.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** AES-шифрование, возможность отправки через мессенджеры.
- **Цена:** Бесплатно (есть платный функционал).

1.3. PixelKnot

- **Описание:** Разработано организацией **The Guardian Project**, использует стойкие стеганографические методы.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** Поддержка паролей, открытый исходный код.
- **Цена:** Бесплатно.

1.4. Secret Box - Hide Text in Image

- **Описание:** Позволяет скрывать текстовые сообщения в изображениях.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** Простое управление, возможность извлечения на других устройствах.
- **Цена:** Бесплатно.

1.5. Cryptic

- **Описание:** Приложение для шифрования и стеганографии, скрывает данные в изображениях.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** AES-256 шифрование, поддержка iCloud.
- **Цена:** Платное (~\$2.99).

2. Приложения для Android

2.1. StegApp

- **Описание:** Позволяет скрывать текст и файлы в изображениях.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** Поддержка шифрования, простой интерфейс.
- **Цена:** Бесплатно.

2.2. Hide It Pro (Audio Manager)

- **Описание:** Маскирует скрытые файлы (изображения, видео, текст) под приложение для настройки звука.
- **Формат контейнера:** Любые файлы (скрытие в памяти устройства).
- **Особенности:** Скрытый режим, защита паролем.
- **Цена:** Бесплатно.

2.3. Steganography Master

- **Описание:** Позволяет скрывать текст в изображениях и аудиофайлах.
- **Формат контейнера:** JPEG, PNG, WAV, MP3
- **Особенности:** Поддержка нескольких форматов, шифрование.
- **Цена:** Бесплатно.

2.4. Secret Video Recorder

- **Описание:** Приложение для скрытой записи видео, но также поддерживает стеганографию.
- **Формат контейнера:** MP4, AVI
- **Особенности:** Запись видео с возможностью скрытия данных.
- **Цена:** Бесплатно (есть платные функции).

2.5. MobiStego

- **Описание:** Специализированное приложение для стеганографии в изображениях.
- **Формат контейнера:** JPEG, PNG
- **Особенности:** Открытый исходный код, LSB-метод.
- **Цена:** Бесплатно.

Лекция 15

СКРЫТИЕ ДАННЫХ В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЯХ

Стеганография - это наука скрытия сообщений таким образом, что никто, кроме предполагаемого получателя, не знает о существовании сообщения.

Цели: Конфиденциальность, безопасность связи, защита авторских прав.

Основные компоненты:

- Сообщение: Информация, которую нужно скрыть.
- Контейнер: Невинный объект (изображение, аудио, видео), внутри которого скрывается сообщение.
- Ключ (опционально): Информация, необходимая для извлечения сообщения из контейнера.

Стеганографический алгоритм: Метод, используемый для внедрения сообщения в контейнер.

Отличие от криптографии:

- Криптография делает сообщение нечитаемым.
- Стеганография скрывает факт существования сообщения.

Преимущества использования видео в стеганографии:

- **Большой объем:** Видеофайлы обычно имеют большой размер, что позволяет скрывать значительные объемы данных.
- **Подвижность:** Небольшие изменения в видеоряде, вызванные внедрением данных, часто незаметны для человеческого глаза.
- **Широкое распространение:** Видеофайлы широко распространены в Интернете, что делает их идеальным контейнером для скрытия данных.
- **Разнообразие форматов и алгоритмов сжатия:** Существуют различные форматы видео и алгоритмы сжатия, которые можно использовать для скрытия данных.

Основные методы стеганографии в видео

Пространственная область (Spatial domain) - эти методы манипулируют непосредственно пикселями видеокадров.

- **Метод наименее значимых битов (LSB - Least Significant Bit):** Замена наименее значимых битов пикселей данными сообщения.
Преимущества: Простота реализации.
Недостатки: Относительно низкая устойчивость к сжатию и атакам. Может быть обнаружен с помощью стеганоанализа.
Пример: Если бит сообщения равен 1, а наименее значимый бит пикселя равен 0, бит пикселя заменяется на 1. Аналогично для бита 0.
- **Pixel Value Differencing (PVD):** Использование разницы значений соседних пикселей для скрытия данных.
Преимущества: Улучшенная устойчивость к сжатию по сравнению с LSB.
Недостатки: Более сложная реализация

Частотная область (Frequency domain) - эти методы используют преобразования для представления видеокадров в частотной области, где и скрываются данные.

- **DCT (Дискретное косинусное преобразование) Steganography**
Суть: Модификация DCT-коэффициентов (используемых в алгоритмах сжатия видео, таких

как MPEG) для внедрения данных.

Преимущества: Высокая устойчивость к сжатию и другим типам обработки видео.

Недостатки: Более сложная реализация и меньшая емкость по сравнению с методами пространственной области. Пример: Небольшие изменения в DCT-коэффициентах, которые меньше всего влияют на качество видео.

- **DWT (Дискретное вейвлет-преобразование) Steganography**

Суть: Аналогично DCT, но использует вейвлет-преобразования.

Преимущества: Хорошая устойчивость к различным атакам.

Недостатки: Сложность реализации.

- **Методы на основе векторов движения (Motion vector-based)**

Используются в сжатых видеоформатах (например, MPEG). Суть: Модификация векторов движения, используемых для кодирования видео, для внедрения данных.

Преимущества: Высокая емкость и устойчивость к сжатию.

Недостатки: Требует понимания алгоритмов сжатия видео.

- **Методы на основе временной области (Temporal domain)**

Используют временные характеристики видеопоследовательности.

- **Смена кадров (Frame swapping):** Замена некоторых кадров другими (визуально похожими) для внедрения данных.

Например, последовательность замененных кадров может представлять бинарный код.

- **Синхронизация кадров (Frame synchronization):** Небольшие изменения временных интервалов между кадрами.

Критерии оценки стеганографических методов

- **Емкость (Capacity):** объем данных, который можно скрыть в контейнере.
- **Незаметность (Perceptibility):** Насколько трудно обнаружить изменения, внесенные в контейнер. Обычно оценивается субъективно (визуально) или объективно (с использованием метрик качества видео, таких как PSNR - Peak Signal-to-Noise Ratio). Высокий PSNR обычно означает, что изменения незаметны.
- **Устойчивость (Robustness):** Насколько устойчив метод к различным атакам (сжатие, фильтрация, добавление шума, изменение формата).
- **Безопасность (Security):** Насколько трудно извлечь скрытое сообщение без знания ключа.

Атаки на стеганографию в видео (Стеганоанализ)

- **Визуальный анализ:** Поиск необычных артефактов или паттернов в видео.
- Статистический анализ: Анализ статистических характеристик видео (например, гистограмм, DCT-коэффициентов) для выявления аномалий.
- Специализированные методы стеганоанализа: Методы, разработанные специально для обнаружения определенных стеганографических алгоритмов.

Применение стеганографии в видео

- Скрытая передача данных: Передача конфиденциальной информации незаметно.
- Защита авторских прав: Внедрение водяных знаков в видео для защиты от несанкционированного копирования.

- Скрытая коммуникация: Использование видео в качестве канала связи для тайных агентов или других лиц, нуждающихся в конфиденциальной связи.
- Цифровая криминалистика: Обнаружение скрытых данных в видеофайлах, используемых в качестве доказательств в уголовных делах.

MPEG - это название экспертной группы ISO, которая работает над созданием стандартов кодирования и сжатия видео- и аудиоданных.

Стеганографические методы, применяемые для встраивания информации в видео, сжатое по стандарту MPEG-2 (далее - MPEG), должны работать в реальном времени. Способы встраивания ЦВЗ, работающие в реальном времени, должны отвечать некоторым требованиям и, в первую очередь они должны быть слепыми и обладать малой вычислительной сложностью.

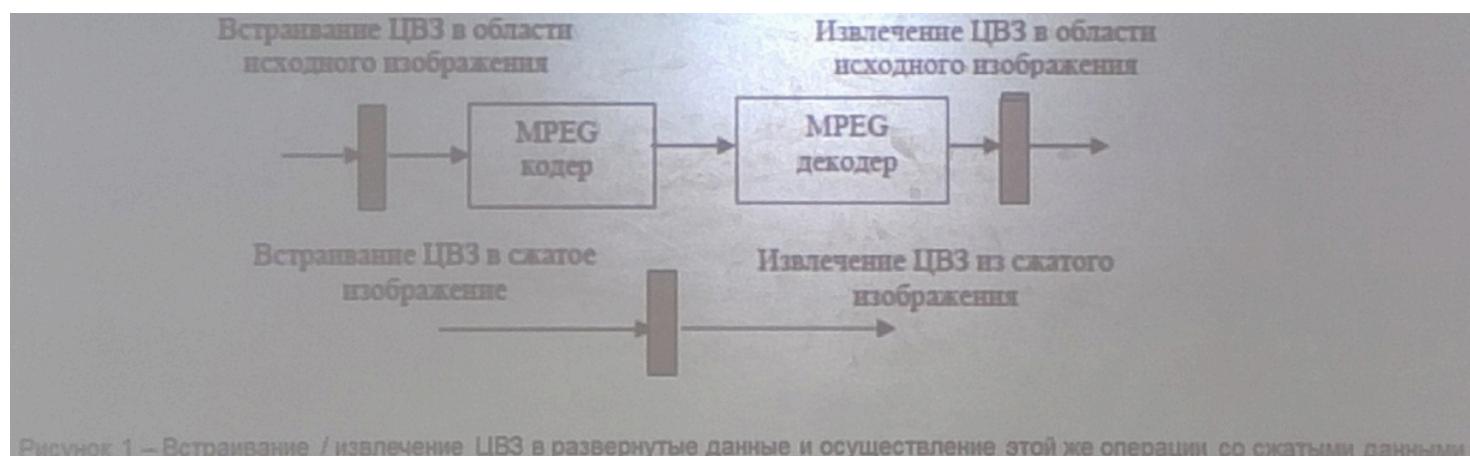


Рисунок 1 – Встраивание / извлечение ЦВЗ в развернутые данные и осуществление этой же операции со сжатыми данными

Рисунок 1 - Встраивание / извлечение ЦВЗ в развернутые данные и осуществление этой же операции со сжатыми данными

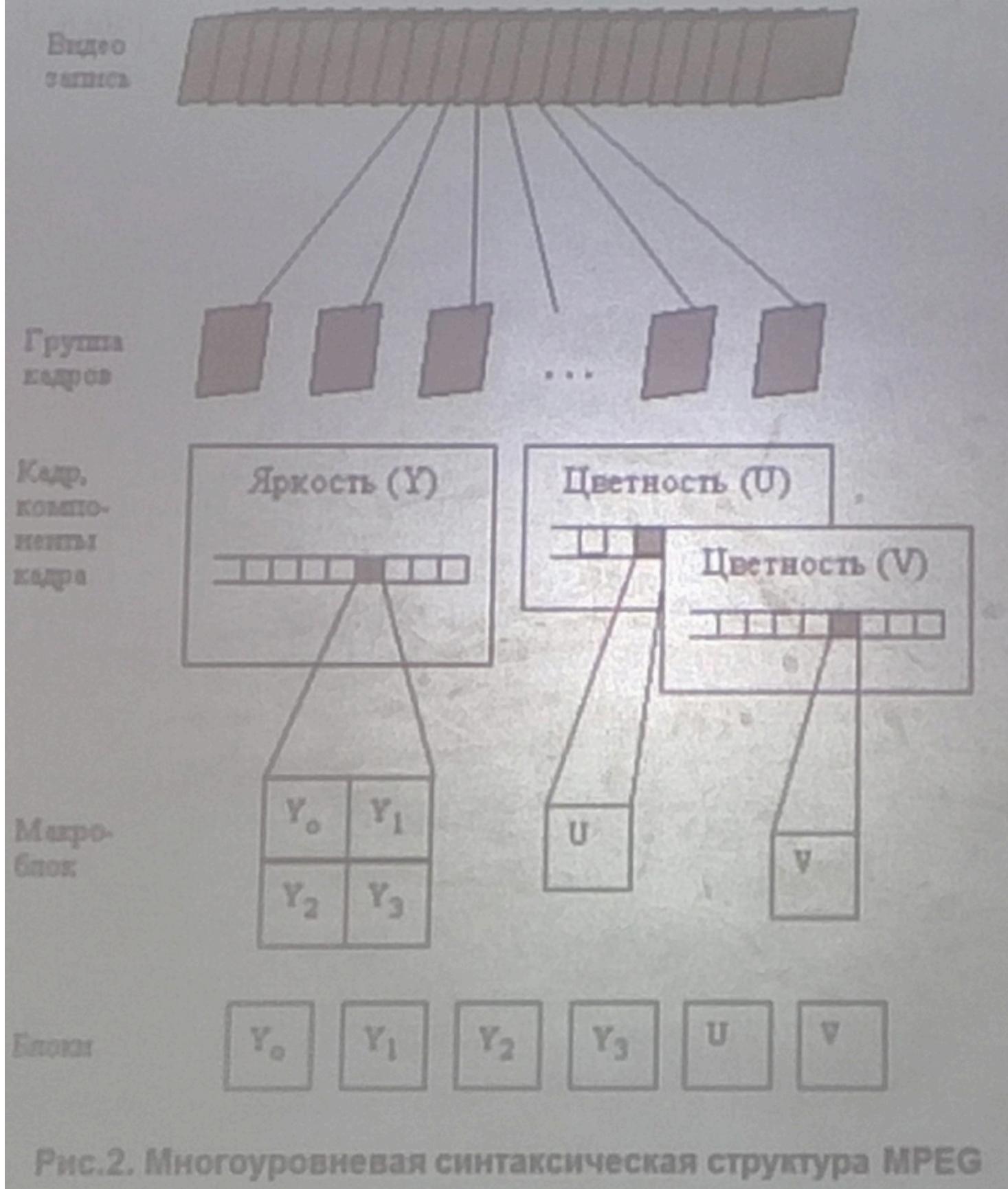


Рис.2. Многоуровневая синтаксическая структура MPEG

Группа кадров видеопотока состоит из компонентов: яркость (Y), цветность (U, V). Кадр представляется формой как YUV, то есть одним каналом яркости и двумя каналами цветности. Изображение в канале яркости - это, по существу, черно-белое изображение. Известно, что зрительная система человека более чувствительна к изменениям в канале яркости, нежели в каналах цветности. Поэтому компоненты U и V могут быть подвергнуты большему сжатию, чем Y.

Вопросы для самостоятельной работы:

1. Какие преимущества и недостатки у разных методов стеганографии в видео?

Пространственная область (Spatial domain) - эти методы манипулируют непосредственно пикселями видеокадров.

- **Метод наименее значимых битов (LSB - Least Significant Bit)**

Преимущества: Простота реализации.

Недостатки: Относительно низкая устойчивость к сжатию и атакам. Может быть обнаружен с помощью стеганоанализа.

- **Pixel Value Differencing (PVD):**

Преимущества: Улучшенная устойчивость к сжатию по сравнению с LSB.

Недостатки: Более сложная реализация

- **DCT (Дискретное косинусное преобразование) Steganography**

Преимущества: Высокая устойчивость к сжатию и другим типам обработки видео.

Недостатки: Более сложная реализация и меньшая емкость по сравнению с методами пространственной области.

- **DWT (Дискретное вейвлет-преобразование) Steganography**

Преимущества: Хорошая устойчивость к различным атакам.

Недостатки: Сложность реализации.

- **Методы на основе векторов движения (Motion vector-based)**

Преимущества: Высокая емкость и устойчивость к сжатию.

Недостатки: Требует понимания алгоритмов сжатия видео.

2. Как можно улучшить устойчивость стеганографических методов к атакам?

- **Использование комбинированных методов:** Например, сочетание пространственной и частотной областей для повышения устойчивости.
- **Применение криптографии:** Шифрование сообщения перед внедрением усложняет его извлечение без ключа.
- **Оптимизация алгоритмов:** Выбор коэффициентов или областей для внедрения, которые меньше всего влияют на качество видео (например, каналы цветности в YUV).
- **Адаптивные методы:** Внедрение данных в области видео, которые менее подвержены изменениям при сжатии или обработке.
- **Использование избыточности:** Добавление контрольных сумм или кодов коррекции ошибок для защиты данных от искажений.
- **Слепые методы:** Разработка алгоритмов, которые не требуют доступа к исходному контейнеру для извлечения данных, что повышает безопасность.

3. Какие этические вопросы связаны с использованием стеганографии?

- **Незаконная деятельность:** Стеганография может использоваться для скрытой передачи конфиденциальной информации, что может быть связано с преступной или шпионской деятельностью.

- **Нарушение авторских прав:** Внедрение водяных знаков может быть использовано как для защиты авторских прав, так и для их незаконного обхода.
- **Конфиденциальность и слежка:** Использование стеганографии для скрытого наблюдения или сбора данных без согласия пользователей нарушает право на приватность.
- **Ответственность разработчиков:** Создатели стеганографических алгоритмов могут нести моральную ответственность за возможное злоупотребление их технологиями.
- **Этические рамки в исследованиях:** Ученые и разработчики должны учитывать потенциальные риски и последствия своих исследований, особенно в военной или разведывательной сферах.

4. Приведите примеры практического применения стеганографии в видео, которые вы знаете.

Технология Cinavia, разработанная Verance, внедряет неслышимые аудио-водяные знаки в лицензионные Blu-ray диски.

При попытке воспроизвести пиратскую копию плеер (например, Sony PlayStation) обнаруживает водяной знак и автоматически отключает звук.

Фильм "Дюна" (2021) от Warner Bros. содержит Cinavia-метку. Если его скопировать и записать на диск, официальные плееры не будут воспроизводить звук.