МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Компьютерная стеганография

Электронный учебно-методический комплекс
по дисциплине в LMS Moodle

Работа выполнена по мероприятию блока 1 «Совершенствование образовательной деятельности» Программы развития СГАУ на 2009 – 2018 годы по проекту «Разработка контента для системы электронного и дистанционного обучения по основным образовательным программам факультета информатики»
Соглашение № 1/34 от 3.06.2013 г.

САМАРА
2013

УДК 004.93(075), 004.056(075)
К637

Автор-составитель: **Федосеев Виктор Андреевич**

Компьютерная стеганография [Электронный ресурс] : электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle / Мин-во образования и науки РФ, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т); авт.- сост. В. А. Федосеев. - Электрон. текстовые и граф. дан. - Самара, 2013. – 1 эл. опт. диск (CD-ROM).

В состав учебно-методического комплекса входят:

1. Курс лекций.
2. Задания на лабораторные работы.
3. Вопросы для подготовки к экзамену
4. Рабочая программа

УМКД «Компьютерная стеганография» предназначен для студентов факультета информатики, обучающихся по направлению подготовки специалистов 090303.65 «Информационная безопасность автоматизированных систем» в 9 семестре.

УМКД разработан на кафедре геоинформатики и информационной безопасности.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

КУРС ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

«КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ»

Раздел 1: Системы встраивания информации

Самара 2013

Оглавление

1 Системы встраивания информации (СВИ)

1.1 Элементарное введение в предмет дисциплины

Стеганография (steganography) (от греч. стегос — скрытый и графо — пишу, буквально «тайнопись») – это наука о защищённой передаче информации, осуществляющейся путём сокрытия самого факта передачи информации.

В отличие от *криптографии*, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование.

Стеганографическая система (Steganographic system) [внешнее определение] – это совокупность методов и средств, предназначенных для защищённой передачи информации, осуществляющейся путём сокрытия самого факта передачи информации

На рисунке 1.1 схематически представлены основные направления стеганографии, которые будут подробно рассмотрены ниже.

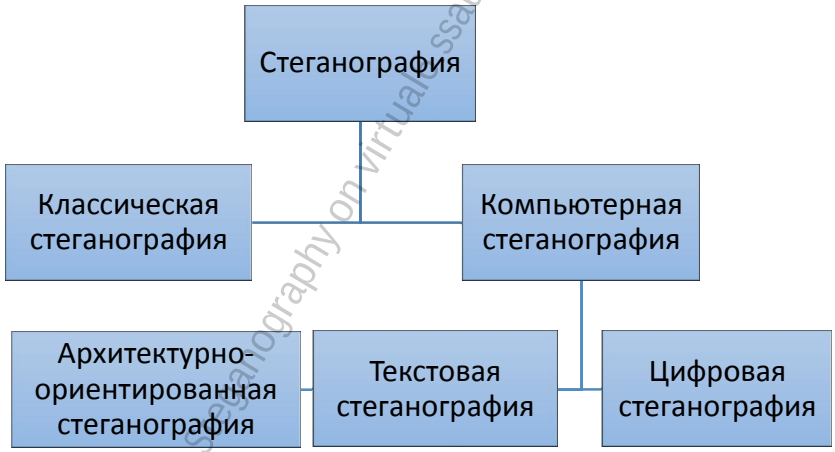


Рисунок 1.1 – Основные направления стеганографии

1.1.1 Классическая стеганография.

Исторические примеры: Древний Мир

- Первое упоминание о стеганографических методах в литературе приписывается Геродоту, который описал случай передачи сообщения Демартом, который соскабливал воск с дощечек, писал письмо прямо на дереве, а потом заново покрывал дощечки воском.
- Другой эпизод, который относят к тем же временам - передача послания с использованием головы раба. Для передачи тайного сообщения голову раба

обривали, наносили на кожу татуировку, и когда волосы отрастали, отправляли с посланием.

- В Китае письма писали на полосках щелка. Поэтому для сокрытия сообщений, полоски с текстом письма, сворачивались в шарики, покрывались воском и затем глотались посыльными.
- Можно также упомянуть акростихи и другие языковые игры.

Исторические примеры: Симпатические чернила

- Чернилами для секретной переписки, то есть симпатическими, пользовались еще в древние времена. В I веке нашей эры Филон Александрийский описал способ изготовления «тайных» чернил из сока чернильных орешков с последующей обработкой написанного раствором железомедной соли
- римский поэт Овидий предлагал использовать для написания текста молоко, проявляющееся после присыпания его порошком из сажи.
- Секрет тайнописи Плиния Старшего заключался в использовании сока растений.
- Члены тайной организации "Черный передел" тоже использовали в переписке невидимые чернила. Но из-за предательства одного из чернопередельцев, знавшего секрет расшифровки писем, почти все были арестованы. Тайные письма были написаны разбавленным водным раствором медного купороса. Проявлялся написанный такими чернилами текст, если бумагу подержать над склянкой с нашатырным спиртом. Буквы окрашиваются в ярко-синий цвет из-за образования аммиачного комплекса меди.
- А вот китайский император Цин Шихуанди (249--206 гг. до н. э.), во время правления которого появилась Великая Китайская стена, использовал для своих тайных писем густой рисовый отвар, который после высыхания написанных иероглифов не оставляет никаких видимых следов. Если такое письмо слегка смочить слабым спиртовым раствором иода, то появляются синие буквы. А император для проявления письма пользовался бурым отваром морских водорослей, видимо, содержащим иод.

В период средневековья рецептами простых симпатических чернил широко пользовались для дипломатической переписки. Со времен Первой мировой войны над составами «тайных» чернил изрядно потрудились химики, существенно

усовершенствовав и разнообразив их. В состав современных симпатических чернил могут входить как в чистом виде, так и в виде составных частей практически любые вещества — кровь, слюна, соки растений, мыльные растворы, кислоты, основания, соли, соль, сахар, крахмал и т.д. Это зависит только от фантазии и профессионализма химика. Хотя не стоят на месте и те специалисты, которые занимаются способами проявления внешне невидимых записей. Для их обнаружения применяют различные методы с использованием механических, термических, химических и оптических методов, что делает такой способ переписки малоперспективным.

Совокупность всех этих методов составляет предмет *классической стеганографии*.

Скрытие информации большинством перечисленных методов возможно лишь благодаря тому, что противнику неизвестен метод скрытия. Между тем, еще в 1883 году был сформулирован принцип Керкхоффса, гласящий:

“Система защиты информации должна обеспечивать свои функции даже при полной информированности противника о её структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемой сведений должна заключаться в ключе, то есть в предварительно (как правило) разделенном между адресатами фрагменте информации.” (Schneir, 1996)

Согласно этому принципу рассмотренные выше примеры классических стегосистем не могут служить надёжными средствами защиты информации. Поэтому на смену им пришли новые.

1.1.2 Компьютерная стеганография. Архитектурно-ориентированная стеганография

Компьютерная стеганография — направление классической стеганографии, при котором в роли контейнера и сообщения могут выступать аппаратное или программное обеспечение компьютера или цифровые данные, которые он хранит и обрабатывает.

Основными положениями современной компьютерной стеганографии являются следующие:

- Методы скрытия должны обеспечивать целостность файла.
- Предполагается, что противнику полностью известны возможные стеганографические методы (согласно принципу Керкхоффса).

– Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа.

На схеме на рисунке 1.1 показаны три основных направления компьютерной стеганографии: «архитектурно-ориентированная», текстовая и цифровая стеганография. Термин *«архитектурно-ориентированная стеганография»* не является общепринятым и характеризует методы, использующие для встраивания информации специфические области памяти, обусловленные использованием определённых физических носителей, операционных систем, форматов файлов и пр. Соотвтественно, для других носителей, операционных систем, форматов представления данных нужны будут другие методы.

Примеры методов архитектурно-ориентированной стеганографии:

1. Использование части зарезервированных полей компьютерных форматов файлов для записи данных. Недостатком этого метода является низкая степень скрытности и малый объем передаваемой информации.
2. Метод скрытия информации в неиспользуемых местах физических носителей. Недостатки: маленькая производительность, передача небольших по объему сообщений.
3. Использование особенностей файловых систем: при хранении на жестком диске файл всегда занимает целое число кластеров (минимальных адресуемых объемов информации). К примеру, в ранее широко используемой файловой системе FAT32 стандартный размер кластера — 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ информации, из которых 1КБ нужен для хранения байта данных, а остальные 3 ни на что не используются — соответственно, их можно использовать для передачи секретной информации. Недостаток данного метода: лёгкость обнаружения.

Выделим основные *общие недостатки* данной группы методов:

1. Физическое (на уровне ячеек памяти) разделение полезной информации и секретного сообщения, приводящее к тому, что последнее может быть легко обнаружено, прочитано, удалено.

2. Неуниверсальность методов, их заточенность на конкретные программно-аппаратные средства. Следствием этого может стать удаление секретной информации при изменении используемых средств, а также необходимость разработки новых методов для новой программно-аппаратной платформы.

1.1.3 Текстовая стеганография

В *текстовой стеганографии* встраивание секретной информации осуществляется в текстовый файл.

Приведём некоторые *примеры* методов текстовой стеганографии.

3. Методы, использующие смещения слов, предложений, абзацев. Основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами.

- Метод 1: один пробел между словами соответствует, например, биту 0, два пробела — биту 1. Однако прямое его применение хотя и возможно, но на практике порождает массу неудобств, в частности, оформление текста становится неряшливым, что позволяет легко заподозрить в нем наличие стеганографического встраивания.
- Метод 2: изменение порядка следования маркеров конца строки CR/LF использует индифферентность подавляющего числа средств отображения текстовой информации к порядку следования символов перевода строки (CR) и возврата каретки (LF), ограничивающих строку текста. Традиционный порядок следования CR/LF соответствует 0, а инвертированный LF/CR означает 1.
- Метод 3 (хвостовых пробелов): дописывание в конце коротких строк (предварительно заданной длины) от 0 до 15 пробелов, кодирующих значение полубайта.

4. Методы выбора определенных позиций букв (нулевой шифр). Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)
5. Методы использования символов другого языка, совпадающих по начертанию.
6. Методы, использующие таблицу синонимов. Синонимы кодируют биграмму (напр.: праздник — 00, торжество — 01... и т.д.). При встраивании информации текст анализируется на наличие слов из таблицы. Их смещения относительно

начала текста сохраняются. Потом секретное сообщение делится на биграммы и далее происходит встраивание – каждое такое слово заменяется на нужный синоним, который кодирует данную биграмму. При тщательном подборе таблицы синонимов текст сохраняет осмысленность. Встраивание информации данным методом обнаружить сложнее всего.

В одной из работ выполнено сравнение некоторых методов текстовой стеганографии по объёму встроенной информации. Результаты исследования отражены в таблице 1.1 и показывают, что наибольший объём данных можно встроить при помощи использования разных символов, имеющих одинковое начертание.

Таблица 1.1. Результаты эксперимента по сравнению объёма встроенной информации для разных методов текстовой стеганографии

Метод	Объём сообщения, бит / символ * 100%
Чередование маркеров конца	0,21
Выравнивание пробелами	0,32
Двоичные нули	0,58
Хвостовые пробелы	0,85
Знаки одинакового начертания	3,21

Общие особенности методов текстовой стеганографии:

– Слабая производительность методов, передача небольших объемов информации.

– Низкая степень скрытности; простота удаления встроенной информации.

+ Простота использования.

1.1.4 Цифровая стеганография и цифровые водяные знаки

В методах *цифровой стеганографии* встраивание секретного сообщения осуществляется в одномерные или многомерные сигналы (мультимедиа), , имеющие физическую природу. К таким сигналам мы будем относить изображения, звуковые и видеофайлы. Важным отличием от архитектурно-ориентированных методов является то, что они не заточены на конкретный формат представления цифрового сигнала, а

встраивание осуществляется за счёт изменения байтов самого сигнала, а не каких-либо специальных полей.

Методы цифровой стеганографии базируются на математической основе, рассматриваемой в дисциплинах «Цифровая обработка сигналов», «Цифровая обработка изображений».

При встраивании информации учитываются особенности человеческого зрения и слуха, за счёт чего может быть достигнута незаметность встроенной информации.

В тесной связи с цифровой стеганографией являются вопросы, связынные с встраиванием цифровых водяных знаков (ЦВЗ).

Встраивание ЦВЗ (Digital Watermarking) – это процесс внедрения в цифровой сигнал (заметного или незаметного!) информации, имеющей некоторое отношение к этому цифровому сигналу.

ЦВЗ – это как раз информация, внедряемая в цифровой сигнал и имеющая некоторое отношение к этому цифровому сигналу.

Система встраивания ЦВЗ (Watermarking system, система ЦВЗ, ЦВЗ-система) [внешнее определение] – это совокупность методов и средств, предназначенных для внедрения в цифровой сигнал информации, имеющей некоторое отношение к этому цифровому сигналу.

1.1.5 Встраивание информации в цифровые сигналы

Цифровая стеганография и цифровые водяные знаки имеют много общего (сам принцип – встраивание одного информационного объекта в другой; методы; свойства). На самом деле они являются составными частями одной области знаний, называемой по-английски “Information Hiding” или “Data Hiding”, т.е. буквально *сокрытие информации.* Предмет и основные понятия её сформировались к середине 90-х годов XX века и описаны в работах Eric Cole (Cole, 2003), Ingemar Cox, Matthew Miller, Jessica Fridrich (Cox, et al., 2008; Miller, et al., 1999), Mauro Barni, Franco Bartolini (Barni, et al., 2004), Fabien Petitcolas (Petitcolas, et al., 1999), Birgit Pfitzmann (Pfitzmann, 1996) и других.

В рамках рассматриваемого курса по-русски мы будём именовать её «встраивание информации». Общепринятое русскоязычное название её в настоящее время отсутствует, а выбор названия «встраивание информации» вместо «сокрытия информации» обусловлен тем, что в ряде методов защиты данных цифровыми водяными знаками

встроенная информация *может* и даже *должна быть* визуально различимой, то есть не *скрытой* от глаз. Отчасти также такое название явным образом уже на уровне названия позволяет отгородиться от предмета и задач криптографии, которая занимается *сокрытием содержания* информации, передаваемой как открытым, так и скрытым способом [Schneier96].

Итак, *встраивание информации (Information Hiding)* – это область знаний, охватывающая широкий круг проблем встраивания информации (называемой секретной информацией, секретным сообщением, водяным знаком) в содержимое другого информационного объекта (называемого открыто передаваемой информацией, контейнером).

Методы встраивания информации разделяются на 4 основных категории (см. таблицу 1.2).

Таблица 1.2. Классификация методов встраивания информации

	Сообщение связано с контейнером	Сообщение не связано с контейнером
Факт наличия сообщения сокрыт	Стеганографическое встраивание ЦВЗ (1)	Скрытая передача информации (стеганографическая) (2)
Факт наличия сообщения известен	Не стеганографическое встраивание ЦВЗ (3)	Открытая опосредованная передача информации (4)

Приведём примеры методов каждого из четырёх типов:

1. В 1981 году фотографические оттиски конфиденциальных документов британского кабинета оказались напечатанными в газетах. Ходят слухи, что для определения источника утечки Маргарет Тэтчер установила порядок распространения однозначно идентифицируемых копий документов для каждого из её министров. Каждая копия имела уникальные интервалы между словами, которые были использованы для кодирования личности получателя. Таким образом, источники утечки могли быть определены. Это пример стеганографического встраивания водяных знаков.
2. Скрытая передача информации, не связанной с контейнером, всегда являлась важной задачей для военных. Примером тому служит книга Симмонса, в которой

он обсуждает технические вопросы, связанные с проверкой ОСВ-II договора между Соединенными Штатами и Советским Союзом. Согласно этому договору, обеим державам допускается иметь много бункеров ракет, но лишь ограниченное число ракет. Для проверки соблюдения договора, каждая страна должна устанавливать датчики в хранилищах ракет в другой стране. Каждый датчик должен был только сообщать о заполненности бункера, в котором он установлен, и ничего больше. Однако внутри законных сообщений удавалось спрятать также и дополнительную информацию, касающуюся, к примеру, местонахождения бункера.

3. Пример нестеганографического водяного знака (т. е. водяного знака, наличие которого является известным) можно увидеть, к примеру, на электронных картах Google. Каждая плитка карты имеет слабозаметный водяной знак, защищающий права Google как владельца изображения, и сообщение в нижней части каждой веб-страницы указывает на это обстоятельство. Знание того, что водяные знаки встроены в каждое изображение, помогает сдерживать пиратство.
4. В качестве примера открытой опосредованной передачи информации можно привести на вставки кода времени в радиоэфире на заданной частоте (800 Гц, например), которые практиковались в конце 1940-х годов. Код внедрялся с периодичностью 15 минут. Его было слышно в эфире, но он не являлся водяным знаком, так как сообщение (текущее время) не было связано с содержанием передачи.

***

Наш курс называется «Компьютерная стеганография», однако мы будем главным образом заниматься вопросами встраивания информации в цифровые сигналы, то есть с одной стороны рассмотрим не только стегосистемы, но и ЦВЗ-системы, а с другой – практически не будем останавливаться (в рамках теоретического курса) на архитектурно-ориентированных и текстовых стеганографических методах, также входящих в предмет компьютерной стеганографии, ввиду их недостатков, отмеченных выше.

1.2 Системы встраивания информации

1.2.1 Система встраивания информации и её основные элементы

Совокупность методов и средств, образующих единое решение для встраивания в цифровой сигнал информации, будем называть *системой встраивания информации* (СВИ). В СВИ относятся и стегосистемы, и ЦВЗ-системы. Любая система встраивания информации состоит из двух основных элементов:

1) подсистемы встраивания информации;
2) подсистемы извлечения информации.

В первой происходит внедрение встраиваемой информации в цифровой сигнал - контейнер в соответствии с *секретным ключом*. Во второй подсистеме происходит либо извлечение встроенной информации, либо проверка наличия в принятом сигнале встроенной информации. Предполагается, что контейнер со встроенной информацией (который будем называть *носителем информации*) передаётся по открытому каналу, в котором он может подвергнуться искажениям и атакам. Обобщённая схема СВИ представлена на рисунке. 1.2.

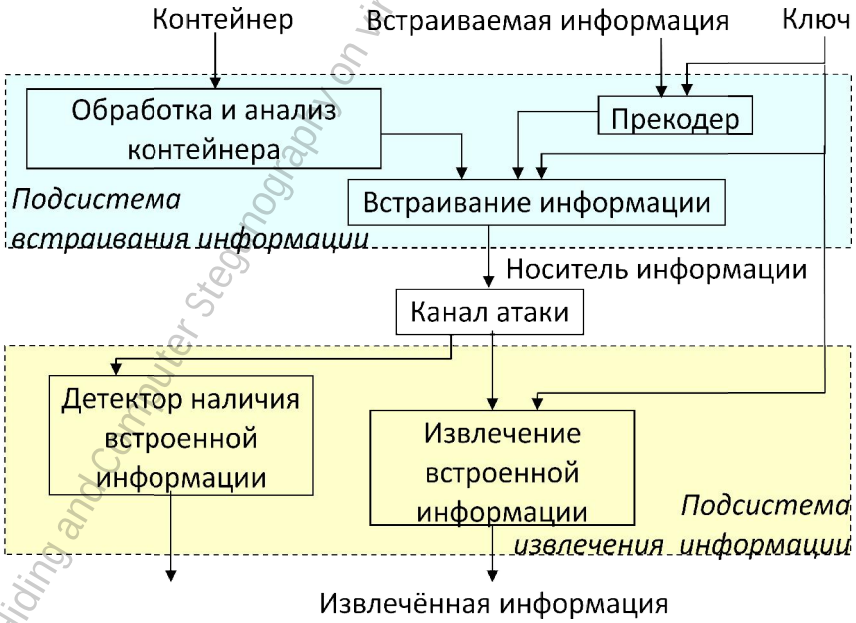


Рисунок 1.2 – Краткая схема системы встраивания информации

Ключевым требованием, возникающим при проектировании *стеганографических систем*, является недопустимость обнаружения наличия скрытой информации несанкционированным получателем. Поэтому основной целью атак на такие системы

является обнаружение факта наличия встроенной информации (извлечение её содержания не является необходимым). Разработка таких атак является задачей стегоанализа, а в случае, если стегосистема является устойчивой к ним, то говорят, что она обладает *стеганографической стойкостью* (Cox, et al., 2008; Аграновский, и др., 2009; Грибунин, и др., 2000). Помимо этого, в задаче скрытой передачи информации, которую решают стеганографические методы, важным является возможность передачи данных большого объёма.

Ключевой характеристикой *ЦВЗ-систем* также является стойкость, но она имеет несколько иной смысл. Под *стойкостью ЦВЗ-систем* понимается возможность извлечения встроенной информации из искажённого носителя информации. При этом круг значимых искажений определяется в зависимости от области применения метода встраивания данных. Более того, в ряде задач (защита от изменений, защита от копирования (Barni, et al., 2004)) требуется, чтобы ЦВЗ не был стоек к определённым преобразованиям. Такие водяные знаки могут называться *полухрупкими* или *хрупкими* (Nakai, 2001; Wu, et al., 2002).

1.2.2 Назначение систем встраивания информации

Существует достаточно широкий круг задач, для решения которых могут использоваться методы встраивания информации. Наиболее значимыми из них являются:

1) защита авторских прав,
2) защиты от несанкционированного распространения,
3) защита от изменений,
4) защита от подделки,
5) скрытая передача информации.

Задача защиты авторских прав может быть решена с использованием сценария «Демонстрация законного права собственности» (Barni, et al., 2004), при котором автор или владелец объекта авторского права встраивает в него *стойкий ЦВЗ*, однозначно определяющий его как владельца.

Задача *защиты от несанкционированного распространения* может быть решена с использованием сценария «Сдерживания копирования» (Barni, et al., 2004), согласно которому владелец распространяемого информационного объекта, представляющего собой определённую ценность, встраивает в каждую копию различные ЦВЗ (которые в

данном случае называются цифровыми отпечатками пальцев), однозначно определяющие получателя документа. Если в дальнейшем где-либо будет обнаружена несанкционированная копия, то ее происхождение может быть восстановлено путем извлечения встроенной информации. Таким образом, данная задача фактически тоже решается при помощи *стойких ЦВЗ-систем*.

Задача *защиты от изменений* может быть решена с использованием *хрупких водяных знаков*, которые разрушаются при какой-либо модификации носителя информации, к примеру, при воспроизведении его на копировальном аппарате. Таким образом, само наличие ЦВЗ является подтверждением подлинности защищаемого сигнала и отсутствия проведённых над ним несанкционированных изменений.

Задача защиты от подделки может быть решена посредством встраивания специальных меток, воспроизведение которых является сложной задачей. Эти метки могут являться *стойкими ЦВЗ*.

Задача *скрытой передачи информации* является ключевой задачей стеганографии, таким образом, и решается она при помощи *стегосистем*.

1.2.3 Свойства систем встраивания информации

При описании систем встраивания информации принято выделять присущие им основные *свойства*. Эти свойства определяют детали подсистем встраивания и извлечения информации, стойкость к различным атакам, а также некоторые численные показатели. Таким образом, они представляют собой важную информацию о системе встраивания информации, и в конечном счёте определяют возможности её использования (см. таблицу 1.3) (Barni, et al., 2004; Cox, et al., 2008). Ниже перечислены наиболее важные из них.

1. *Действие, выполняемое подсистемой извлечения информации:* проверка наличия встроенной информации (детектирование) или извлечение встроенной информации (декодирование).
2. *Знание исходного контейнера подсистемой извлечения информации:* если ни исходный контейнер, ни какие-либо из его параметров не известны на этапе извлечения информации, то такое извлечение называется *слепым*, в противном случае оно называется *неслепым*.

3. *Возможность извлечения встроенной информации:* только санкционированными адресатами или любыми участниками процедуры обмена информацией. В первом случае встроенная информация называется *частной*, во втором – *публичной*.
4. *Тип контейнера*: звук, изображение, видео и пр.
5. Подбор способа встраивания информации к предопределённому методу извлечения информации: если это справедливо, то встраивание называют *информированным*, в противном случае – *слепым*.
6. *Способ модификации сигнала при встраивании информации*.
7. *Визуальная различимость* встроенной информации.
8. *Максимально возможный объем встраиваемой информации*, допускаемый СВИ.
9. *Возможность повторного встраивания* другой информации в тот же сигнал тем же методом.
10. *Стойкость встроенной информации* к искажениям её носителя. По этому признаку принято разделять системы на секретные, стойкие, полухрупкие и хрупкие. В *секретных СВИ* стойкость встроенной информации должна сохраняться как при преднамеренных атаках, так при непреднамеренных искажениях. *Стойкие СВИ* защищены только от произвольных непреднамеренных искажений. *Полухрупкие СВИ* устойчивы к одним преобразованиям и неустойчивы к другим, в то время как в *хрупких* системах встроенная информация разрушается даже при незначительных модификациях заполненного контейнера.

Таблица 1.3 – Требования к свойствам СВИ в зависимости от назначения

Назначение СВИ	Требования по визуальной различимости ВИ	Требования к системам по стойкости	Допустимые способы извлечения
Защита авторских прав	Неразличима или различима	Секретные и стойкие	Декодер или детектор
Защита от несанкционированного распространения	Обязательно неразличима	Секретные и стойкие	Декодер
Защита от изменений	Неразличима или различима	Полухрупкие и хрупкие	Детектор
Передача информации	Обязательно неразличима	Секретные и стойкие	Декодер
Защита от подделки	Неразличима или различима	Секретные и стойкие	Детектор

В таблице 1.3 указаны требования, предъявляемые к основным свойствам СВИ, в зависимости от назначения этих систем.

1.2.4 Атаки на системы встраивания информации

Можно выделить две классификации атак на СВИ: по *целям*, которые они преследуют, и по *знаниям и возможностям*, имеющимся у нарушителей, осуществляющих эти атаки.

В качестве основных целей атак на СВИ выделим следующие:

- обнаружение наличия встроенной информации (такие атаки будем обозначать α_0),
- извлечение встроенной информации без отыскания ключа (α_d),
- удаление встроенной информации (α_r),
- отыскание секретного ключа (α_k),
- подмена встроенной информации (α_c)
- подделка носителя информации (α_f).

В таблице 1.4 представлены требования по стойкости систем ВИ к различным атакам в зависимости от назначения систем: знаком «+» помечены атаки, к которым система обязана быть стойкой, знаком «–» помечены атаки, не являющиеся актуальными для систем данного назначения.

По знаниям и возможностям, которыми обладает нарушитель, можно выделить следующие атаки (Schneir, 1996; Грибунин, и др., 2000):

- только с известным носителем информации,
- с известным контейнером,
- с известной встроенной информацией,
- с выбранным контейнером,
- с выбранной встраиваемой информацией.

Последние два вида атак относятся к так называемой модели «активного нарушителя», а остальные рассмотренные атаки – к модели «пассивного нарушителя» (Аграновский, и др., 2009; Грибунин, и др., 2000).

Наиболее сложным типом атаки и в то же время самым распространенным на практике ввиду минимальности требований для её осуществления является атака с

известным носителем информации. Нарушитель при этом не обладает никакой априорной информацией о контейнере, ключе и встроенной информации.

Таблица 1.4 – Требования по стойкости СВИ к атакам в зависимости от назначения систем

Назначение СВИ	Стойкость к атакам					
	α_0	α_d	α_r	α_k	α_c	α_c
Защита авторских прав	–	–	+ –	+	+	–
Защита от копирования	–	+	+ –	–	+	+
Защита от изменений	–	–	–	+	–	+
Передача информации	+	+	+ –	+	+	–
Защита от подделки	–	–	–	+	–	+

1.3 Структурные компоненты СВИ

1.3.1 Общая структура СВИ

Рассмотрим более подробно структуру СВИ как совокупности данных и процессов (функций) их обработки, представленную на рисунках 1.3–1.6.

Одним из важнейших понятий, которые мы будем использовать при описании математической модели СВИ, является внутренняя информация. Под *внутренней информацией* мы будем понимать встраиваемую (и впоследствии извлекаемую) информацию. Внутренней она является по отношению к контейнеру, поскольку передаётся *внутри* него.

При этом внутренняя информация в зависимости от своего состояния, определяемого процессами ММ СВИ, в рамках которых она рассматривается, может быть встраиваемой, встроенной, извлекаемой, извлечённой, эталонной. Как правило, в этих случаях мы будем для лаконичности опускать слово «внутренняя», то есть использовать термин «встраиваемая информация» вместо термина «встраиваемая внутренняя информация», употребляя его только в том случае, если состояние внутренней информации не определено.

Определение 1.1. Под *цифровым сигналом* при рассмотрении ММ СВИ мы будем понимать величину $X \in \mathbb{X}_{[]}^{m}$, представляющую собой m-мерную матрицу, элементы которой определены на множестве $\mathbb{X} \subseteq \mathbb{R}$. Само множество $\mathbb{X}_{[]}^{m}$ будем называть пространством цифровых сигналов. Цифровые сигналы в разделе 1 будем обозначать большими латинскими буквами.

Определение 1.2. Под *матрицей признаков* $y \in \mathbb{Y}_{[]}^{l}$ будем понимать l-мерную матрицу, элементы которой определены на множестве $\mathbb{Y} \subseteq \mathbb{C}$. Само множество $\mathbb{Y}_{[]}^{l}$ мы будем называть пространством признаков. Матрицы признаков будем обозначать малыми латинскими буквами (за исключением встраиваемой информации в пространстве признаков, обозначаемой Ω).

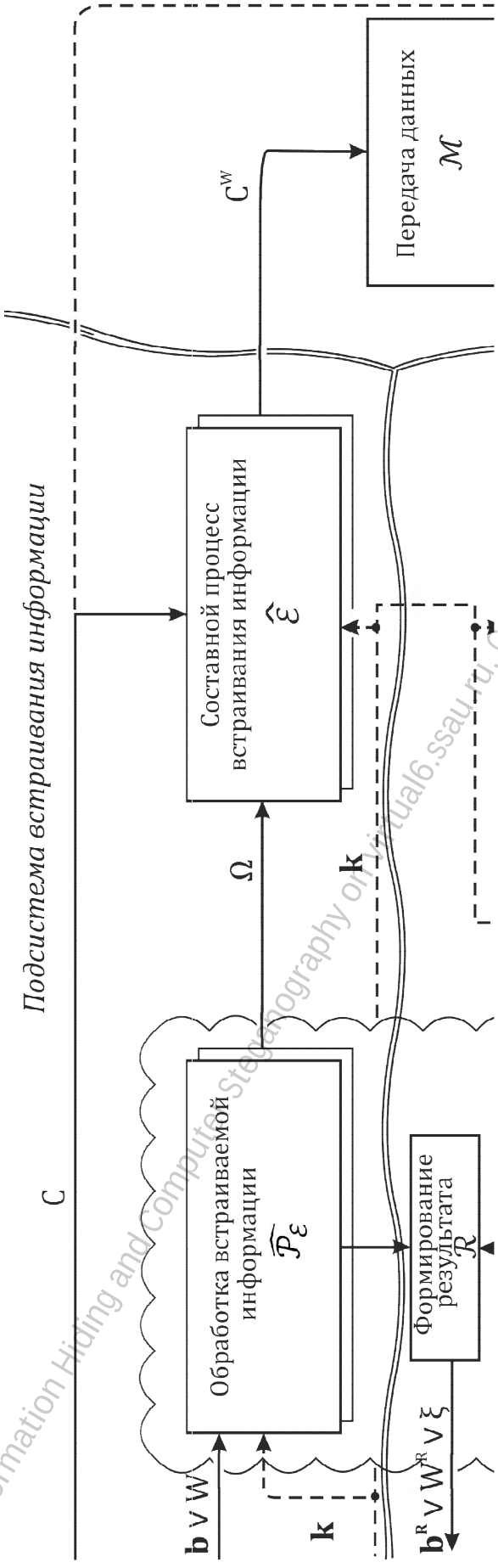


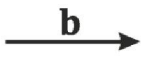
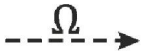
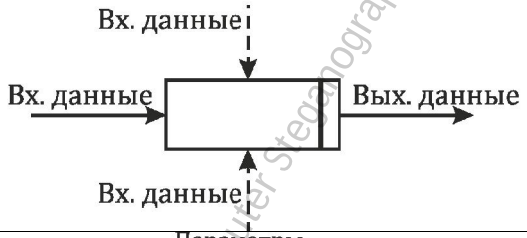
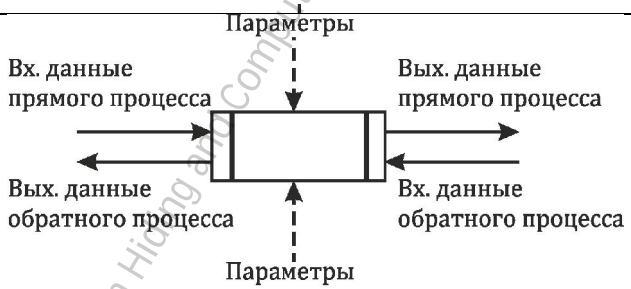
Рисунок 1.3 – Общая схема СВИ

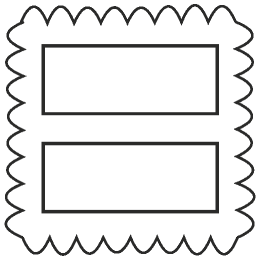
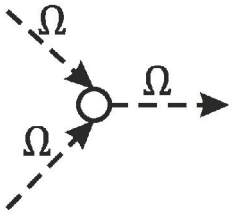
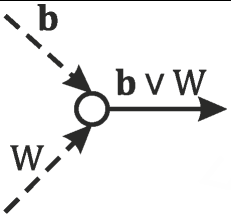
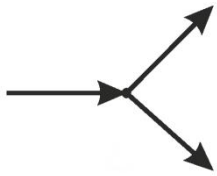
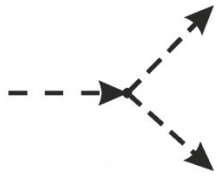
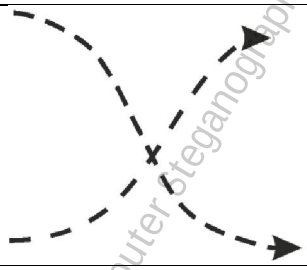
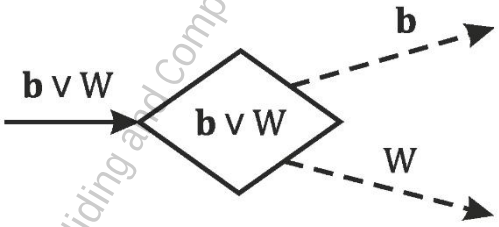
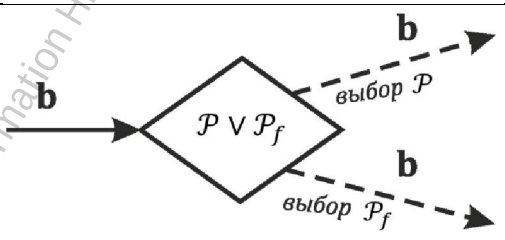
Важной особенностью внутренней информации является возможность её представления в нескольких эквивалентных формах: в виде битовой строки $\mathbf{b} \in \mathbb{B}^{1}_{[N_b]}$, цифрового сигнала $W \in \mathbb{X}^{m}_{[]}$ и матрицы признаков $\Omega \in \mathbb{Y}^{l}_{[]}$. На рисунке 1.3 выделен отдельный блок обработки *внутренней информации*, элементы которого являются составными частями обеих подсистем (встраивания и извлечения информации).

Схематическое описание элементов схем СВИ

В таблице 1.5 представлены описания всех типов элементов, используемых на схемах СВИ. Основу ММ СВИ составляют *данные* и *процессы* (функции) их обработки. Процессы на схемах обозначаются прямоугольниками (строки 3-6 таблицы 1.5), а данные – стрелками, которые мы будем называть *потоками данных* (строки 1-2 таблицы 1.5). Данные, являющиеся содержимым каждого из потоков, отображаются в виде подписей над стрелками или справа от них.

Таблица 1.5. Элементы структурных схем ММ СВИ

	Элемент	Описание
1		Обязательный поток данных, существующий во всех системах *Сами данные обозначаются сверху или справа от стрелки*
2		Опциональный поток данных, который может существовать в одних системах и отсутствовать в других
3		Необратимый или не нуждающийся в обратимости процесс *Аргументы его условно делятся на основные входные данные и параметры, отображаемые в различных частях элемента*
4		Обратимый процесс *Прохождение через неё потока данных слева направо означает выполнение прямой функции, справа налево – обратной*
5		Процесс, содержащий несколько подпроцессов, раскрываемых на схеме более низкого уровня

6		Совокупность однотипных процессов, образующих единый блок и, возможно, взаимодействующих между собой
7		Объединение данных, которые могут быть сформированы одним из двух возможных способов (или прийти из одного из двух доступных источников)
8		Объединение данных, являющихся элементами разных множеств, в одном потоке данных
9		Разветвление обязательного потока данных
10		Разветвление опционального потока данных
11		Графическое пересечение потоков данных, при котором они не оказывают никакого влияния друг на друга
12		Разветвление потока данных в зависимости от передаваемых в нём данных
13		Разветвление потока данных в зависимости от некоторого условия с сохранением состава передаваемых данных

Основные данные СВИ

Определение 1.3. Цифровой сигнал $C \in \mathbb{X}_{[]}^{m}$, в который производится встраивание информации, называется *контейнером*.

Определение 1.4. Вектор $\mathbf{b} \in \mathbb{B}_{[N_b]}^{1}$, являющийся представлением встраиваемой внутренней информации в форме битовой строки длиной N_b и подлежащий встраиванию в контейнер, называется *встраиваемой информацией*.

Будем полагать, что вектор $\mathbf{b} \neq \mathbf{0}$ (где $\mathbf{0}$ – нулевой вектор). Это значение мы зарезервируем для результата извлечения информации $\mathbf{b}^{\boldsymbol{R}}$ (определение будет дано чуть ниже). Такое значение будет свидетельствовать о том, что ничего извлечь не удалось.

Определение 1.5. Представление встраиваемой внутренней информации в виде цифрового сигнала $W \in \mathbb{X}_{[]}^{m}$ называется *встраиваемым сигналом*.

При этом в некоторых системах внутренняя информация изначально представляется в виде вектора $\mathbf{b}$, а в некоторых – сразу в виде сигнала W.

Определение 1.6. Начальной формой внутренней информации будем называть одно из множеств: $\mathbb{B}_{[N_b]}^{1}$ (если внутренняя информация изначально представлена в виде вектора $\mathbf{b} \in \mathbb{B}_{[N_b]}^{1}$) или $\mathbb{X}_{[]}^{m}$ (если она изначально имеет вид $W \in \mathbb{X}_{[]}^{m}$).

Определение 1.7. Представление встраиваемой внутренней информации в виде матрицы признаков $\Omega \in \mathbb{Y}_{[]}^{l}$ называется *матрицей признаков встраиваемой информации*.

Пример. Если начальная форма представления информации – $\mathbb{B}_{[N_b]}^{1}$, а контейнер представляет собой изображение, то сигнал W может представлять собой изображение, на котором напечатана последовательность нулей и единиц, составляющих вектор $\mathbf{b}$, а матрицей признаков может являться дискретное преобразование Фурье (ДПФ) изображения W. В этом случае $\mathbb{X} = \mathbb{B}^{8}, \mathbb{Y} = \mathbb{C}, m = l = 2,$ то есть $W \in (\mathbb{B}^{8})_{[N_1 \times N_2]}^{2}$, а $\Omega \in \mathbb{C}_{[N_1 \times N_2]}^{2}$.

Пример. Если начальная форма представления информации – $\mathbb{B}_{[N_b]}^{1}$, а контейнер представляет собой звуковой сигнал, то сигнал W может являться представлением $\mathbf{b}$ азбукой Морзе. Матрицей признаков также может являться ДПФ сигнала W. В этом случае $\mathbb{X} = \mathbb{B}^{16}, \mathbb{Y} = \mathbb{C}, m = l = 1,$ то есть $W \in (\mathbb{B}^{16})_{[N_1]}^{1}$, а $\Omega \in \mathbb{C}_{[N_1]}^{1}$.

Определение 1.8. Сигнал $C^W \in \mathbb{X}_{[]}^m$, являющийся результатом встраивания информации в контейнер, называется *носителем информации* или *заполненным контейнером*.

Определение 1.9. Сигнал $\widetilde{C^W} \in \mathbb{X}_{[]}^m$, являющийся результатом прохождения C^W через канал передачи данных, называется *принятым носителем информации*.

Определение 1.10. Результат извлечения внутренней информации в форме вектора $\mathbf{b}^{\boldsymbol{R}} \in \mathbb{B}_{[N_b]}^1$ называется *извлечённой информацией*.

Определение 1.11. Результат извлечения внутренней информации в форме цифрового сигнала $W^R \in \mathbb{X}_{[]}^m$ называется *извлечённым сигналом*.

Определение 1.12. Результатом обнаружения внутренней информации называется величина $\xi \in \mathbb{B}$, принимающая значения

$$\xi = \begin{cases} 1, & \text{если } \widetilde{C^W} \text{ содержит } \mathbf{b} \text{ (или } W\text{)}, \\ 0, & \text{если } \widetilde{C^W} \text{ не содержит } \mathbf{b} \text{ (или } W\text{)}. \end{cases}$$

Определение 1.13. Представление извлекаемой внутренней информации в виде $\tilde{\Omega} \in \mathbb{Y}_{[]}^l$ называется *матрицей признаков извлечённой информации*.

Замечание. $\tilde{\Omega}$ существует во всех СВИ вне зависимости от формы начального представления внутренней информации и формы детектирования.

Защищённость информации, передаваемой в СВИ внутри контейнера, от несанкционированного прочтения обеспечивается секретным ключом СВИ.

Определение 1.14. Секретным ключом СВИ называется величина $k^s \in K^s \subseteq \mathbb{B}_{[N_k]}^1$.

Секретный ключ должен быть известен и в подсистеме встраивания информации, и в подсистеме извлечения информации. При этом полагается, что передача его между двумя указанными подсистемами осуществляется заранее, до начала работы СВИ.

Секретный ключ может состоять из двух частей: закрытого ключа, используемого при встраивании, и открытого ключа, используемого при извлечении. Системы ВИ, для которых характерна такая двухключевая модель (Barni, et al., 2004), называются системами ВИ с открытым ключом – по аналогии с криптографическими системами с открытым ключом (Schneir, 1996). Секретный ключ может отсутствовать в некоторых системах, в частности, в системе, описанной в работе (Cox, 1997).

Детали процессов и алгоритмов встраивания и извлечения информации определяются *открытыми параметрами СВИ*. Открытыми они называются потому, что находятся в свободном доступе. Незнание их может создать неудобства при извлечении информации, но не добавляет системе надёжности по отношению к атакам.

Определение 1.15. Открытыми параметрами СВИ будем называть величину $k^p \in K^p$.

Структура множества K^p определяется отдельно для каждой конкретной СВИ.

Определение 1.16. Составной ключ СВИ $\mathbf{k} \in K = K^s \times K^p$ – это совокупность секретного ключа СВИ k^s и открытых параметров СВИ k^p.

Секретный ключ СВИ k^s и *открытые параметры СВИ* k^p – величины, различные как по формату представления, так и по назначению. Объединение их в составной ключ мы производим по той причине, что вместе они образуют полный вектор параметров алгоритмов встраивания и извлечения информации.

В таблице 1.6 представлен полный список обозначений всех элементов данных СВИ.

Отметим, что отсутствие англоязычных эквивалентов для некоторых величин объясняется в частности тем, что зарубежные автоне рассматривали соответствующие структуры в своих построениях.

Таблица 1.6. Список обозначений данных в СВИ

Обозначение	Множество значений	Определение	Название	Употребимые эквиваленты в англоязычной литературе
C	$\mathbb{X}_{[]}^{m}$	1.3	Контейнер	Host asset, container
$\mathbf{b}$	$\mathbb{B}_{[N_b]}^{1}$	1.4	Встраиваемая информация	Information message, secret message, watermarking code
W	$\mathbb{X}_{[]}^{m}$	1.5	Встраиваемый сигнал	Watermarking message, encoded message, watermarking signal
C^W	$\mathbb{X}_{[]}^{m}$	1.8	Носитель информации	Watermarked asset, cover
$\widetilde{C^W}$	$\mathbb{X}_{[]}^{m}$	1.9	Принятый носитель информации	Transformed watermarked asset
k^s	$K^s \subseteq \mathbb{B}_{[N_k]}^{1}$	1.14	Секретный ключ СВИ	Key, watermarking key, steganographic key
k^p	K^p	1.15	Открытые параметры	–

			СВИ	
$\mathbf{k}$	$K = K^s \times K^p$	1.16	Составной ключ СВИ	–
$\mathbf{b}^{\mathbf{R}}$	$\mathbb{B}^1_{[N_b]}$	1.10	Извлечённая информация	Recovered {название $\mathbf{b}$}
W^R	$\mathbb{X}^m_{[]}$	1.11	Извлечённый сигнал	Recovered {название W}
ξ	$\mathbb{B}$	1.12	Результат обнаружения	Detection result
k^C	K^C	1.25	Параметры контейнера	–
$\widetilde{k^C}$	K^C	1.26	Оценённые параметры контейнера	–
Ω	$\mathbb{Y}^l_{[]}$	1.7	Матрица признаков встраиваемой информации	–
$\widetilde{\Omega}$	$\mathbb{Y}^l_{[]}$	1.13	Матрица признаков извлечённой информации	–
f	$\mathbb{Y}^l_{[]}$	1.28	Матрица признаков контейнера	–
f^W	$\mathbb{Y}^l_{[]}$	1.29	Матрица признаков носителя информации	–
$\widetilde{f^W}$	$\mathbb{Y}^l_{[]}$	1.30	Матрица признаков принятого носителя информации	–

Основные процессы ММ СВИ

Элементами общей схемы ММ СВИ (рисунок 1.2) являются следующие процессы:

- обработка встраиваемой информации,
- обобщённое встраивание информации,
- передача носителя информации,
- обобщённое извлечение информации,
- обработка извлечённой информации
- формирование результата.

Ввиду того, что различные СВИ могут иметь отличия в структуре и потоках данных (что находит отражение на схемах 1.3-1.6 в виде опциональных потоков данных), то существуют процессы, для которых различные СВИ могут иметь различный набор входных потоков данных. Это выражается в том, что функции, задающие упомянутые процессы, могут иметь различные наборы аргументов. При описании процессов в ММ СВИ мы будем останавливаться на наиболее общих случаях, зачастую опуская тривиальные варианты.

Определение 1.17. Под *обработкой встраиваемой информации* (обозначается $\widehat{\mathcal{P}_{\mathcal{E}}}$) понимается совокупность процессов по преобразованию внутренней информации из начальной формы (**b** или W) в матрицу признаков Ω. Таким образом, функция $\widehat{\mathcal{P}_{\mathcal{E}}}$ может иметь вид

$$\widehat{\mathcal{P}_{\mathcal{E}}} : \mathbb{B}^1_{[N_b]} \times K \mapsto \mathbb{Y}^l_{[]}, \qquad \Omega = \widehat{\mathcal{P}_{\mathcal{E}}}(\boldsymbol{b}, \boldsymbol{k}) \tag{1.1}$$

или

$$\widehat{\mathcal{P}_{\mathcal{E}}} : \mathbb{X}^m_{[]} \times K \mapsto \mathbb{Y}^l_{[]}, \qquad \Omega = \widehat{\mathcal{P}_{\mathcal{E}}}(W, \boldsymbol{k}). \tag{1.2}$$

Как уже было сказано выше, ключ в некоторых системах может отсутствовать, поэтому, например, функция $\widehat{\mathcal{P}_{\mathcal{E}}}$ в форме (1.1) может иметь вид

$$\widehat{\mathcal{P}_{\mathcal{E}}} : \mathbb{B}^1_{[N_b]} \mapsto \mathbb{Y}^l_{[]}, \qquad \Omega = \widehat{\mathcal{P}_{\mathcal{E}}}(\boldsymbol{b}).$$

Однако в дальнейшем подобные варианты мы будем опускать.

На качественном уровне *встраивание информации* – это добавление в цифровой сигнал некоторой дополнительной информации посредством модификации этого сигнала, при которой он сохраняет свою длину, область значений и информационное наполнение.

В ММ СВИ встраивание информации описывается процессом $\hat{\mathcal{E}}$ обобщённого встраивания информации, а также входящим в его состав процессом $\mathcal{E}$ встраивания информации в пространстве признаков (см. раздел 1.2.2). Под обобщённым встраиванием информации понимается совокупность процессов по встраиванию внутренней информации, представленной в форме матрицы признаков Ω, в цифровой сигнал – контейнер C, результатом чего является носитель информации C^W.

Определение 1.19. Обобщённым встраиванием информации называется функция $\hat{\mathcal{E}}$ вида

$$\hat{\mathcal{E}} : \mathbb{X}^m_{[]} \times \mathbb{Y}^l_{[]} \times K \mapsto \mathbb{X}^m_{[]}, \qquad C^W = \hat{\mathcal{E}}(C, \Omega, \boldsymbol{k}). \tag{1.3}$$

Под процессом передачи носителя информации в СВИ понимается воздействие физических, технических и программных средств на носитель информации C^W в процессе его передачи или использования. Результатом этого воздействия является принятый носитель информации $\widetilde{C^W}$.

Определение 1.20. Передачей носителя информации назовём функцию вида

$$\mathcal{M} : \mathbb{X}^m_{[]} \mapsto \mathbb{X}^m_{[]}, \qquad \widetilde{C^W} = \mathcal{M}(C^W). \tag{1.4}$$

Важной особенностью функции $\mathcal{M}$ является тот факт, что она в отличие от всех остальных функций модели не является строго определённой. Однако о ней можно сказать, что она является элементом некоторого множества функций $\mathbb{M}$, которое задаётся на этапе проектирования системы ВИ. Структура множества $\mathbb{M}$ описана в разделе 1.2.3.

Определение 1.21. *Обобщённым извлечением информации* (обозначается $\widehat{\mathcal{D}}$) будем называть совокупность процессов, предназначенных для отыскания матрицы признаков извлечённой информации $\tilde{\Omega}$ по принятому носителю информации $\widetilde{C^W}$ (возможно, также с использованием исходного контейнера C). Функция $\widehat{\mathcal{D}}$ имеет, таким образом, два возможных представления:

$$\widehat{\mathcal{D}} : \mathbb{X}_{[]}^{m} \times \mathbb{X}_{[]}^{m} \times K \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}, C, \boldsymbol{k}\right), \tag{1.5}$$

$$\widehat{\mathcal{D}} : \mathbb{X}_{[]}^{m} \times K \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}, \boldsymbol{k}\right). \tag{1.6}$$

Определение 1.22. Под *обработкой извлечённой информации* (обозначается $\widehat{\mathcal{P}_{\mathcal{D}}}$) будем понимать совокупность процессов по преобразованию извлечённой информации из формы матрицы признаков $\tilde{\Omega} \in \mathbb{Y}_{[]}^{\mathrm{l}}$ в начальную форму или в форму детектирования (см. раздел 1.2.2).

Результатом обработки извлечённой информации может являться одна из трёх величин: $\boldsymbol{b^R} \in \mathbb{B}_{[\mathrm{N_b}]}^{1}$, $W^R \in \mathbb{X}_{[]}^{m}$ или $\tilde{\Omega} \in \mathbb{Y}_{[]}^{\mathrm{l}}$. Таким образом, в первых двух случаях функция $\widehat{\mathcal{P}_{\mathcal{D}}}$ имеет вид

$$\widehat{\mathcal{P}_{\mathcal{D}}} : \mathbb{Y}_{[]}^{l} \times K \mapsto \mathbb{B}_{[N_b]}^{1}, \qquad \boldsymbol{b^R} = \widehat{\mathcal{P}_{\mathcal{D}}}\left(\tilde{\Omega}, \boldsymbol{k}\right) \tag{1.7}$$

или

$$\widehat{\mathcal{P}_{\mathcal{D}}} : \mathbb{Y}_{[]}^{l} \times K \mapsto \mathbb{X}_{[]}^{m}, \qquad W^R = \widehat{\mathcal{P}_{\mathcal{D}}}\left(\tilde{\Omega}, \boldsymbol{k}\right), \tag{1.8}$$

а в третьем случае в процессе обработки извлечённой информации вовсе не осуществляется никаких действий, а $\widehat{\mathcal{P}_{\mathcal{D}}}$ выражается тождественным оператором, то есть

$$\widehat{\mathcal{P}_{\mathcal{D}}} : \mathbb{Y}_{[]}^{l} \mapsto \mathbb{Y}_{[]}^{l}, \qquad \text{причём } \forall x \in \mathbb{Y}_{[]}^{l}\ \widehat{\mathcal{P}_{\mathcal{D}}}(x) = x, \tag{1.9}$$

Определение 1.23. *Формированием результата* $\hat{\mathcal{R}}$ назовём совокупность процессов по выбору данных, являющихся результатом работы СВИ.

Формирование результата наряду с обработкой встраиваемой и извлечённой информации является внутренним процессом блока обработки внутренней информации.

В таблице 1.5 отмечена справочная информация по всем обобщённым (составным) процессам, рассмотренным в данном разделе. Атомарные (неделимые) процессы, входящие в их состав, будут рассмотрены в следующем разделе.

Таблица 1.5. Составные процессы ММ СВИ

№	Обозн.	Процесс	Формула	Определение
1	$\widehat{\mathcal{P}_{\mathcal{E}}}$	Обработка встраиваемой информации	(1.1)-(1.2)	1.17
2	$\hat{\mathcal{E}}$	Обобщённое встраивание информации	(1.3)	1.19
3	$\widehat{\mathcal{D}}$	Обобщённое извлечение информации	(1.5)-(1.6)	1.21
4	$\widehat{\mathcal{P}_{\mathcal{D}}}$	Обработка извлечённой информации	(1.7)-(1.9)	1.22
5	$\hat{\mathcal{R}}$	Формирование результата	–	1.23

1.3.2 Детализация процессов СВИ

Процессы встраивания информации (строка 2 таблицы 1.5)

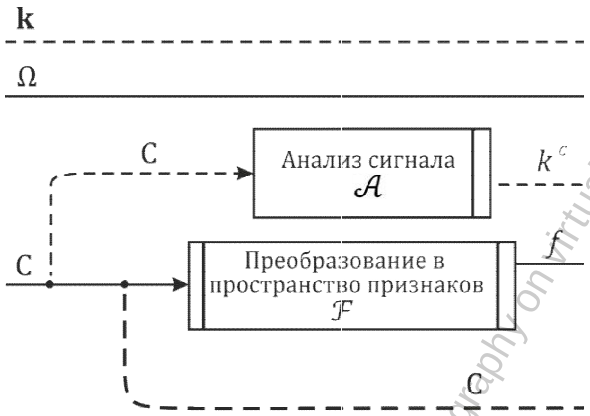


Рисунок 1.3 – ММ СВИ: Подпроцессы обобщённого процесса встраивания информации

Схема подпроцессов и потоков данных, входящих в состав обобщённого процесса встраивания информации, показана на рисунке 1.3.

На схеме представлены следующие процессы, входящие в состав $\hat{\mathcal{E}}$:

- анализ сигнала (контейнера),
- преобразование сигнала в пространство признаков и обратное ему,
- встраивание информации в пространстве признаков.

Определение 1.24. Анализом сигнала (обозначается $\mathcal{A}$) мы назовём процесс оценивания числовых характеристик этого сигнала, которые составляют множество K^C, определяемое индивидуально для каждой СВИ. Функция $\mathcal{A}$ имеет вид

$$\mathcal{A} : \mathbb{X}_{[]}^{m} \longmapsto K^C. \qquad (1.10)$$

Глобальных предположений относительно структуры множества K^C мы делать не будем. Анализ сигнала в СВИ осуществляется применительно к контейнеру C при встраивании внутренней информации (это показано на схеме на рисунке 1.3), а также к принятому носителю информации $\widetilde{C^W}$ при её извлечении (это показано на схеме на рисунке 1.4).

Замечание. Процесс анализа сигнала характерен не для всех систем. Например, он отсутствует в системах, описанных в (Barni, et al., 2004; Meerwald, 2001; Грибунин, и др., 2000).

Определение 1.25. Числовые характеристики $k^C \in K^C$, являющиеся результатом анализа контейнера:

$$k^C = \mathcal{A}(C),$$

называются *параметрами контейнера*.

Определение 1.26. Числовые характеристики $\widetilde{k^C} \in K^C$, являющиеся результатом анализа принятого носителя информации:

$$\widetilde{k^C} = \mathcal{A}\left(\widetilde{C^W}\right),$$

называются *оценёнными параметрами контейнера*.

Анализ сигнала является вспомогательным процессом, результаты которого используются только в последующем процессе встраивания информации в пространстве признаков.

Пример. Анализ контейнера-изображения может состоять в отыскании координат характеристических точек (локальных максимумов функции яркости, точек Харриса (Harris, et al., 1988; Schmid, et al., 2000) и пр.), для последующего встраивания информации за счёт изменения функции яркости в их окрестности.

Встраивание информации согласно ММ СВИ осуществляется в пространстве признаков $\mathbb{Y}_{[]}^{\mathrm{l}}$. В частном случае пространством признаков может являться собственно множество, на котором определены контейнер и встраиваемый сигнал: в этом случае $\mathbb{X} = \mathbb{Y}$, $m = l$ и размеры двух матриц совпадают. Также распространён вариант, при котором множество $\mathbb{Y}_{[]}^{l}$ может являться множеством спектральных компонент множества $\mathbb{X}_{[]}^{m}$, полученных посредством какого-либо дискретного преобразования.

Определение 1.27. Процессом $\mathcal{F}$ *преобразования сигналов в пространство признаков* мы назовём преобразование цифровых сигналов из множества $\mathbb{X}_{[]}^{m}$, на котором они определены, в пространство признаков $\mathbb{Y}_{[]}^{l}$, в котором осуществляется встраивание внутренней информации:

$$\mathcal{F} \ : \ \mathbb{X}_{[]}^{m} \longmapsto \mathbb{Y}_{[]}^{l}. \qquad (1.11)$$

Помимо уже рассмотренных в разделе 1.2.1 матриц признаков встраиваемой и извлечённой информации Ω и $\widetilde{\Omega}$, также на множестве $\mathbb{Y}_{[]}^{\mathrm{l}}$ в рамках ММ СВИ имеют свои представления контейнер, носитель информации, а также принятый носитель информации.

Определение 1.28. Матрицей признаков контейнера называется величина

$$f \in \mathbb{Y}_{[]}^{l}\colon \ f = \mathcal{F}(C).$$

Определение 1.29. Матрицей признаков носителя информации называется величина

$$f^{W} \in \mathbb{Y}_{[]}^{l}\colon \ f^{W} = \mathcal{F}(C^{W}).$$

Определение 1.30. Матрицей признаков принятого носителя информации называется величина

$$\widetilde{f^{W}} \in \mathbb{Y}_{[]}^{l}\colon \ \widetilde{f^{W}} = \mathcal{F}\left(\widetilde{C^{W}}\right).$$

К функции $\mathcal{F}$, осуществляющей преобразование сигнала в пространство признаков, предъявляются два важных требования:

6) она должна быть обратимой

$$\exists\, \mathcal{F}^{-1} \ : \ \mathbb{Y}_{[]}^{l} \longmapsto \mathbb{X}_{[]}^{m} \qquad (1.12)$$

7) преобразования $\mathcal{F}$ и $\mathcal{F}^{-1}$ должны обладать низкой вычислительной сложностью.

Условия 1-2 дают основание использовать в качестве $\mathcal{F}$ дискретные ортогональные преобразования, для которых существуют быстрые алгоритмы расчёта: дискретное преобразование Фурье (ДПФ), дискретное косинусное преобразование (ДКП), дискретное вейвлет-преобразование (ДВП) и другие (Блейхут, 1989; Чернов, 2007; Ярославский, 1979).

Определение 1.31. Встраиванием информации в пространстве признаков $\mathcal{E}$ называется функция вида

$$\mathcal{E} : \mathbb{Y}_{[]}^{l} \times \mathbb{Y}_{[]}^{l} \times K \times K^{C} \mapsto \mathbb{Y}_{[]}^{l}, \qquad f^{W} = \mathcal{E}(f, \Omega, \boldsymbol{k}, k^{C}). \tag{1.14}$$

Наконец, итоговое формирование носителя информации происходит при помощи обратного преобразования $\mathcal{F}^{-1}$:

$$C^{W} = \mathcal{F}^{-1}(f^{W}) \tag{1.15}$$

Процессы извлечения информации (строка 3 таблицы 1.5)

Схема подпроцессов обобщённого процесса извлечения информации показана на рисунке 1.4. Единственным нерассмотренным ранее процессом, представленным на этой схеме, является процесс извлечения информации в пространстве признаков.

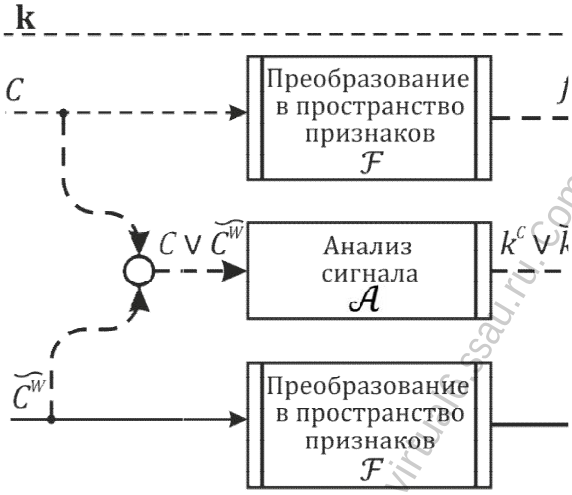


Рисунок 1.4 – ММ СВИ: Подпроцессы обобщённого процесса извлечения информации

Определение 1.32. *Извлечение информации в пространстве признаков* (обозначается $\mathcal{D}$) – это процесс отыскания матрицы признаков извлечённой информации $\widetilde{\Omega}$ по матрице признаков принятого носителя информации $\widetilde{f^W}$ с возможным использованием матрицы признаков исходного контейнера f, его параметров k^C или оценённых параметров $\widetilde{k^C}$, а также полного ключа $\mathbf{k}$.

Можно выделить 4 варианта вида функции $\mathcal{D}$:

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times \mathbb{Y}_{[]}^{l} \times K \times K^{C} \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^W}, f, \boldsymbol{k}, k^{C}\right), \tag{1.17}$$

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times \mathbb{Y}_{[]}^{l} \times K \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^W}, f, \boldsymbol{k}\right), \tag{1.18}$$

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times K \times K^{C} \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^W}, \boldsymbol{k}, \widetilde{k^C}\right). \tag{1.19}$$

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times K \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^W}, \boldsymbol{k}\right). \tag{1.20}$$

Блок обработки внутренней информации (строки 1 и 4 таблицы 1.5)

На рисунке 1.2 было показано, что блок обработки информации образуют процессы обработки встраиваемой и извлечённой информации, а также формирования результата. Расширенная структура описанных процессов представлена на рисунке 1.5.

Как видно из данного рисунка, данный блок главным образом служит для формирования уже упоминавшегося ранее обобщённого представления внутренней информации. В настоящем подразделе оно рассматривается более подробно.

Определение 1.33. *Обобщённым представлением внутренней информации* (сокращённо ОПВИ, обозначается $\mathfrak{I}$ – «готическое И») назовём тройку (двойку) величин: $\Omega \in \mathbb{Y}_{[]}^{l}$, а также $\mathbf{b} \in \mathbb{B}_{[\mathrm{N_b}]}^{1}$ и/или $W \in \mathbb{X}_{[]}^{m}$, – связанных взаимно однозначными отношениями.

Конкретная структура ОПВИ (из трёх возможных вариантов) определяется на основе двух предикатов: *предиката начальной формы внутренней информации* (на схеме он помечен как $\mathbf{b} \vee W$):

$$\pi_{bw} = \begin{cases} true, \text{если начальная форма внутренней информации } \mathbb{B}_{[N_b]}^{1}, \\ false, \text{если начальная форма внутренней информации } \mathbb{X}_{[]}^{m}, \end{cases} \qquad (1.21)$$

и *предиката способа кодирования информации* (на схеме он помечен как $\mathcal{P} \vee \mathcal{P}_f$):

$$\pi_{\mathcal{P}} = \begin{cases} true, \text{если информация кодируется в } \mathbb{X}_{[]}^{m}, \\ false, \text{если информация кодируется в } \mathbb{Y}_{[]}^{l}, \end{cases} \qquad (1.22)$$

следующим образом:

$$\mathfrak{I} = \begin{cases} (\boldsymbol{b}, W, \Omega), & \text{если } (\pi_{bw} = true) \wedge (\pi_{\mathcal{P}} = true), \\ (\boldsymbol{b}, \Omega), & \text{если } (\pi_{bw} = true) \wedge (\pi_{\mathcal{P}} = false), \\ (W, \Omega), & \text{если } (\pi_{bw} = false). \end{cases} \qquad (1.23)$$

В подсистеме встраивания информации при формировании ОПВИ происходит переход от $\mathbf{b}$ или W к матрице признаков Ω. В режиме извлечения информации, напротив, на основе матрицы признаков $\widetilde{\Omega}$ формируются остальные *необходимые* формы внутренней информации. Преобразование информации из одной формы в другую осуществляется при помощи следующих процессов (наличие и отсутствие каждого из них в конкретной системе ВИ определяется предикатами π_{bw} и $\pi_{\mathcal{P}}$): кодирования информации $\mathcal{P}$, кодирования информации в пространстве признаков $\mathcal{P}_f$ и отображения в пространство признаков $\mathcal{F}$.

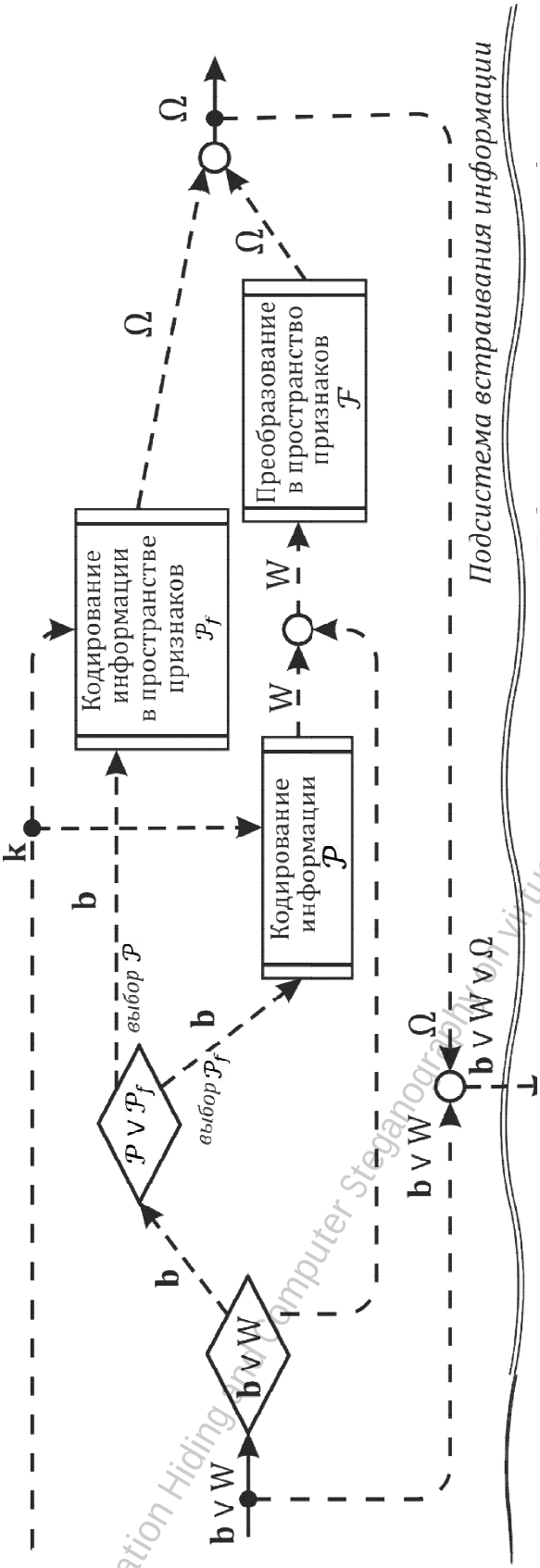


Рисунок 1.5 – ММ СВИ: Блок обработки информации

Определение 1.34. ***Кодированием информации*** (обозначается $\mathcal{P}$) называется преобразование встраиваемой информации $\mathbf{b}$ в цифровой сигнал W:

$$\mathcal{P} \ : \ \mathbb{B}^1_{[N_b]} \times K \longmapsto \mathbb{X}^m_{[]}, \qquad W = \mathcal{P}(\boldsymbol{b}, \boldsymbol{k}). \tag{1.24}$$

<u>Определение 1.35.</u> Кодированием информации в пространстве признаков (обозначается $\mathcal{P}_f$) называется преобразование встраиваемой информации $\mathbf{b}$ в матрицу признаков встраиваемого сигнала минуя цифровой сигнал W:

$$\mathcal{P}_f \ : \ \mathbb{B}^1_{[N_b]} \times K \longmapsto \mathbb{Y}^l_{[]}, \qquad \Omega = \mathcal{P}_f(\boldsymbol{b}, \boldsymbol{k}). \tag{1.25}$$

Поясним более подробно смысл выражений (1.21)-(1.25). В случае, если встраиваемая информация изначально представлена в виде цифрового сигнала $W \in \mathbb{X}^m_{[]}$ (например, изображения, представляющего собой логотип владельца авторских прав на изображение-контейнер), то $\pi_{bw} = false$, а представления внутренней информации в виде $\boldsymbol{b} \in \mathbb{B}^1_{[N_b]}$ попросту не существует. Поэтому $\mathfrak{I} = (W, \Omega)$, а формирование матрицы признаков внутренней информации осуществляется при помощи функции $\mathcal{F}$.

Если встраиваемая информация представлена как вектор $\mathbf{b} \in \mathbb{B}^1_{[N_b]}$ ($\pi_{bw} = true$), то существует два варианта структуры ОПВИ $\mathfrak{I}$ в зависимости от значения $\pi_{\mathcal{P}}$. Случай $\pi_{\mathcal{P}} = true$ означает, что на основе $\mathbf{b}$ формируется W при помощи функции кодирования $\mathcal{P}$. Простейшим способом кодирования в случае, если контейнер представляет собой цифровое изображение, является печать символов нулей и единиц определённого размера на изображении W. Вслед за этим полученный цифровой сигнал W преобразуется в пространство признаков при помощи функции $\mathcal{F}$. Таким образом, ОПВИ имеет вид $\mathfrak{I} = (\boldsymbol{b}, W, \Omega)$.

Наконец, случай $\pi_{\mathcal{P}} = false$ означает, что на основе $\mathbf{b}$ сразу формируется матрица признаков Ω в результате кодирования $\mathcal{P}_f$. Например, если сигнал контейнера является звуковым, а пространство признаков – это множество спектральных компонент некоторого дискретного ортогонального преобразования сигнала, то Ω может формироваться по следующему принципу:

$$\Omega(i) = \begin{cases} 1 & (b_i = 1) \wedge (i < N_b), \\ -1 & (b_i = 0) \wedge (i < N_b), \\ 0 & i \geq N_b, \end{cases}$$

а собственно встраивание в пространстве признаков может осуществляться как поэлементная сумма f и Ω. Извлечение в таком случае возможно лишь с использованием исходного контейнера C. Для рассмотренного варианта ОПВИ содержит два элемента: $\mathfrak{I} = (\boldsymbol{b}, \Omega)$.

Ранее было отмечено, что итоговым результатом работы СВИ могут являться извлечённая информация, представленная в виде двоичного вектора $\mathbf{b}^{\boldsymbol{R}} \in \mathbb{B}^1_{[N_b]}$ или цифрового сигнала $W^R \in \mathbb{X}^m_{[]}$ (в зависимости от начальной формы внутренней информации, то есть значения предиката π_{bw}), или результат обнаружения $\xi \in \mathbb{B}$.

Таким образом, в первом случае используемые в СВИ процессы определяются на основе значений предикатов π_{bw} и $\pi_{\mathcal{P}}$ следующим образом:

11. Если $(\pi_{\mathrm{bw}} = \mathrm{true})$ и $(\pi_{\mathcal{P}} = \mathrm{true})$, то

$$\boldsymbol{b}^{\boldsymbol{R}} = \mathcal{P}^{-1}\left(\mathcal{F}^{-1}\left(\tilde{\Omega}\right), \boldsymbol{k}\right), \tag{1.26}$$

где $\mathcal{P}^{-1}$ – процесс, обратный процессу кодирования информации:

$$\mathcal{P}^{-1} \ : \ \mathbb{X}^m_{[]} \times K \longmapsto \mathbb{B}^1_{[N_b]}. \tag{1.27}$$

12. Если $(\pi_{\mathrm{bw}} = \mathrm{true})$ и $(\pi_{\mathcal{P}} = \mathrm{false})$, то

$$\boldsymbol{b}^{\boldsymbol{R}} = \mathcal{P}_f^{-1}\left(\tilde{\Omega}, \boldsymbol{k}\right), \tag{1.28}$$

где $\mathcal{P}_{\mathrm{f}}^{-1}$ – процесс, обратный процессу кодирования информации в пространстве признаков:

$$\mathcal{P}_f^{-1} \ : \ \mathbb{Y}^l_{[]} \times K \longmapsto \mathbb{B}^1_{[N_b]}, \tag{1.29}$$

13. Если $(\pi_{\mathrm{bw}} = false)$, то

$$W^R = \mathcal{F}^{-1}\left(\tilde{\Omega}\right). \tag{1.30}$$

Итак, если результатом работы СВИ является извлечённая внутренняя информация и $\pi_{\mathrm{bw}} = \mathrm{true}$, то используемый при встраивании процесс кодирования информации $\mathcal{P}$ или $\mathcal{P}_f$ должен быть обратимым в соответствии с выражениями (1.27) или (1.29).

Если же результатом работы подсистемы извлечения информации является *результат обнаружения* $\xi \in \mathbb{B}$, то формируется он в результате работы процесса, называемого детектором встроенной информации.

Определение 1.36. Процессом *обнаружения встроенной информации* (обозначается $\mathcal{R}$) называется процесс сравнения извлечённой внутренней информации и встроенной (эталонной) внутренней информации.

Сравнение осуществляется в одной из форм, входящих в состав ОПВИ.

Определение 1.37. Конкретную форму внутренней информации, подходящую для осуществления процесса обнаружения, будем называть *формой детектирования внутренней информации*.

Форма детектирования определяет один из трёх возможных видов функции $\mathcal{R}$:

$$\mathcal{R} : \mathbb{B}^1_{[N_b]} \times \mathbb{B}^1_{[N_b]} \longmapsto \mathbb{B}, \qquad \xi = \mathcal{R}(\boldsymbol{b}, \boldsymbol{b^R}), \tag{1.31}$$

$$\mathcal{R} : \mathbb{X}^m_{[]} \times \mathbb{X}^m_{[]} \longmapsto \mathbb{B}, \qquad \xi = \mathcal{R}(W, W^R), \tag{1.32}$$

$$\mathcal{R} : \mathbb{Y}^l_{[]} \times \mathbb{Y}^l_{[]} \longmapsto \mathbb{B}, \qquad \xi = \mathcal{R}\left(\Omega, \tilde{\Omega}\right). \tag{1.33}$$

Таким образом, если формой детектирования является множество $\mathbb{Y}^{\mathrm{l}}_{[]}$, то никаких других форм извлечённой информации не требуется, и процесс обработки извлечённой информации $\widehat{\mathcal{P}_{\mathcal{D}}}$ имеет вид (1.9). Если форма детектирования – множество $\mathbb{X}^{\mathrm{m}}_{[]}$, то $\widehat{\mathcal{P}_{\mathcal{D}}}$ состоит лишь из преобразования извлечённой информации из формы матрицы признаков в форму цифрового сигнала при помощи функции $\mathcal{F}^{-1}$ (1.30). Если же множество $\mathbb{B}^1_{[\mathrm{N_b}]}$ является формой детектирования, то процесс обработки извлечённой информации имеет вид (1.26) или (1.28).

Для систем, результатом работы которых является $\mathbf{b^R}$ или W^R, необходимо определить, как отличить сигнал, содержащий некоторую внутреннюю информацию, от сигнала, в который ничего не было встроено. Будем считать, что наличие или отсутствие внутренней информации определяется на этапе декодирования, то есть одним из процессов (1.27) или (1.29). Как было сказано выше, вектор $\mathbf{b^R}$, являющийся результатом одного из этих процессов и состоящий из всех нулей, как раз свидетельствует о том, что ничего извлечь не удалось.

Если начальной формой внутренней информации является $\mathbb{X}^m_{[]}$, то процессы декодирования (1.27) или (1.29), которые мы выделили в качестве определяющих при ответе на вопрос о наличии внутренней информации, отсутствуют. Значит, в таких системах в общем случае нет возможности определения наличия внутренней информации.

В таблице 1.6 отмечена справочная информация по всем атомарным (неделимым) процессам, рассмотренным в разделах 1.2.1-1.2.2.

Таблица 1.6. Атомарные процессы ММ СВИ

Обозн. процесса	Название процесса	Формулы	Опреде-ление	Составные процессы
$\mathcal{P}$	Кодирование информации	(1.24)	1.34	$\widehat{\mathcal{P}_{\mathcal{E}}}$
$\mathcal{P}_f$	Кодирование информации в	(1.25)	1.35	$\widehat{\mathcal{P}_{\mathcal{E}}}$

	пространстве признаков			
$\mathcal{A}$	Анализ сигнала	(1.10)	1.24	$\hat{\mathcal{E}}, \widehat{\mathcal{D}}$
$\mathcal{F}$	Преобразование сигналов в пространство признаков	(1.11)	1.27	$\hat{\mathcal{E}}, \widehat{\mathcal{D}}, \widehat{\mathcal{P}_{\mathcal{E}}}$
$\mathcal{F}^{-1}$	Обратное преобразование из пространства признаков	(1.12)-(1.13)	–	$\hat{\mathcal{E}}, \widehat{\mathcal{P}_{\mathcal{D}}}$
$\mathcal{E}$	Встраивание информации в пространстве признаков	(1.14)	1.31	$\hat{\mathcal{E}}$
$\mathcal{M}$	Передача носителя информации	(1.4)	1.20	–
$\mathcal{D}$	Извлечение информации	(1.17)-(1.20)	1.32	$\widehat{\mathcal{D}}$
$\mathcal{P}^{-1}$	Декодирование информации	(1.27)	–	$\widehat{\mathcal{P}_{\mathcal{D}}}$
$\mathcal{P}_f^{-1}$	Декодирование информации в пространстве признаков	(1.29)	–	$\widehat{\mathcal{P}_{\mathcal{D}}}$
$\mathcal{R}$	Обнаружение встроенной информации	(1.31)-(1.33)	1.37	$\hat{\mathcal{R}}$

1.3.3 Формализация свойств СВИ в рамках рассматриваемой модели

В разделе 1.1.1 были кратко рассмотрены основные свойства СВИ, которые выделяют многие авторы на понятийном уровне (Barni, et al., 2004; Cox, et al., 2008). Предложенная модель СВИ позволяет дать формальные определения многим из них.

Способы извлечения информации

Определение 1.38. Системой ВИ с *детектором* называется СВИ, итоговым результатом работы которой служит величина ξ, определяемая в соответствии с одним из выражений (1.31 – 1.33).

Определение 1.39. Системой ВИ с *декодером* называется СВИ, итоговым результатом работы которой служит одна из величин $\mathbf{b}^{\boldsymbol{R}} \in \mathbb{B}^1_{[N_b]}$ или $W^R \in \mathbb{X}^m_{[]}$, определяемые в соответствии с одним из выражений (1.26), (1.28) или (1.30).

Определение 1.40. Способ извлечения информации в СВИ называется *слепым*, если матрица признаков извлечённой информации $\widetilde{\Omega}$ является результатом функций, имеющих вид (1.19) или (1.20). Также системы ВИ со слепым способом извлечения информации будем называть просто *слепыми СВИ*.

Определение 1.41. Способ извлечения информации в СВИ называется *неслепым*, если матрица признаков извлечённой информации $\widetilde{\Omega}$ является результатом выполнения

функций, имеющих вид (1.17) или (1.18). Также системы ВИ с неслепым способом извлечения информации будем называть просто *неслепыми СВИ*.

Способы встраивания информации

Определение 1.42. Если при проектировании системы встраивания информации заранее определена и фиксирована функция обобщённого извлечения информации (1.5) или (1.6), и функция обобщённого встраивания информации (1.3) должна быть подобрана на основе (1.5) или (1.6) таким образом, чтобы обеспечить работоспособность системы, то такой способ встраивания называется *информированным*.

Определение 1.43. Если при проектировании системы выбирается способ встраивания (1.3), и уже вслед за этим подбирается способ извлечения информации (1.5) или (1.6), то такое встраивание называется *слепым*.

Существуют два распространённых варианта конкретного вида функции слепого встраивания информации в пространстве признаков $\mathcal{E}$.

Определение 1.44. Если функция встраивания информация $\mathcal{E}$ имеет вид

$$\mathrm{f}^{\mathrm{W}} = \mathrm{f} + \alpha \cdot \lambda(\mathrm{f}) \cdot \kappa(\mathbf{k}) \cdot \Omega, \qquad (1.45)$$

где $\lambda(\mathrm{f})$ и $\kappa(\mathbf{k})$ – функции сигнала контейнера и полного ключа соответственно, значения которых определены на $\mathbb{Y}^{\mathrm{l}}_{[]}$; $\alpha \in \mathbb{Y}$ – постоянная величина, характеризующая глобальную степень изменения контейнера (в то время как функция $\lambda(\mathrm{f})$ определяет локальные отклонения данного показателя); символ “$+$” означает поэлементную сумму; символ “$\cdot$” означает поэлементное произведение или умножение на константу, то такое встраивание называется *аддитивным*.

Определение 1.45. Если функция встраивания информация $\mathcal{E}$ имеет вид

$$f^{W} = f \cdot (1 + \alpha \cdot \lambda(\mathrm{f}) \cdot \kappa(\mathbf{k}) \cdot \Omega), \qquad (1.46)$$

то такое встраивание называется *мультипликативным*.

Объём внутренней информации

Понятие допустимого объема встраиваемой информации применимо к системам, в которых начальной формой внутренней информации является множество $\mathbb{B}^{1}_{[N_b]}$. Данное свойство характеризует величину объёма информации, используемого для представления внутренней информации, или отношение данного объёма к объёму контейнера. Если функция $v(\cdot)$ определяет объём информации в битах, то

$$v(\mathbf{b}) = N_b. \qquad (1.47)$$

Если, к примеру, контейнером является полутоновое изображение $C \in (\mathbb{B}^8)^2_{[N_1 \times N_2]}$, то

$$v(C) = 8N_1N_2.$$

Можно выделить три категории систем встраивания информации по допустимому объёму контейнера (определения 1.46-1.48).

Определение 1.46. Системой ВИ *с единичным объёмом внутренней информации* называется система, в которой $v(\mathbf{b}) = 1$, то есть согласно (1.45) $\mathbf{b} \in \mathbb{B}^1_{[1]}$.

Определение 1.47. Системой ВИ *с фиксированным объёмом внутренней информации* называется система, в которой $v(\mathbf{b}) = T_v$, где T_v - константа, не зависящая от объёма контейнера. Значит, согласно (1.47) $\mathbf{b} \in \mathbb{B}^1_{[T_v]}$.

Определение 1.48. Системой ВИ *с фиксированной долей внутренней информации* называется система, в которой

$$\frac{v(\mathbf{b})}{v(C)} = \text{const}.$$

Значит, длина N_b вектора встраиваемой информации определяется на основе размеров контейнера.

Множественное встраивание

Пусть в контейнер C по формуле (1.3) с ключом $\mathbf{k_1}$ встраивается внутренняя информация, имеющая матрицу признаков Ω_1:

$$C_1^W = \hat{\mathcal{E}}(C, \Omega_1, \boldsymbol{k_1}),$$

после чего в принятый носитель информации $\widetilde{C_1^W} = \mathcal{M}(C_1^W)$ с ключом $\mathbf{k_2}$ встраивается другая внутренняя информация, имеющая матрицу признаков Ω_2:

$$\mathrm{C}_{12}^{\mathrm{W}} = \hat{\mathcal{E}}\left(\widetilde{C_1^W}, \Omega_2, \mathbf{k_2}\right).$$

Результаты применения обобщённой функции извлечения информации (1.6) к $\widetilde{C_{12}^W} = \mathcal{M}(C_{12}^W)$ с ключами $\mathbf{k_1}$ и $\mathbf{k_2}$ равны

$$\widetilde{\Omega_1} = \hat{\mathcal{D}}\left(\widetilde{C_{12}^W}, \mathbf{k_1}\right),$$

$$\widetilde{\Omega_2} = \hat{\mathcal{D}}\left(\widetilde{C_{12}^W}, \mathbf{k_2}\right).$$

Пусть для определённости функция обнаружения наличия встроенной информации $\mathcal{R}$ имеет вид (1.33).

Определение 1.49. Будем говорить, что система ВИ допускает *повторное встраивание*, если

$$\xi_1 = \mathcal{R}\left(\Omega_1, \widetilde{\Omega_1}\right) = 1$$

и

$$\xi_2 = \mathcal{R}\left(\Omega_2, \widetilde{\Omega_2}\right) = 1.$$

Можно дать аналогичное определение и для случая функции $\mathcal{R}$ вида (1.31) или (1.32). Также обобщить данное определение на случай множественного (N-кратного) встраивания.

Стойкость к искажениям носителя информации

Определение 1.50. Если множество $\mathbb{M}$ не пусто, то говорят, что система встраивания информации является *стойкой к искажениям из множества* $\mathbb{M}$.

Определение 1.51. Если множество $\mathbb{M}$ не пусто, и включает все возможные искажения $\mathcal{M}_0(A, \boldsymbol{d_0}), \mathcal{M}_1(A, \boldsymbol{d_1}), \dots, \mathcal{M}_{N_{\mathbb{M}}-1}\left(A, \boldsymbol{d}_{N_{\mathbb{M}}-1}\right)$, которые могут происходить при предполагаемых способах передачи и использования носителя информации, то говорят, что система встраивания информации является *стойкой*.

Определение 1.52. Если множество $\mathbb{M}$ помимо указанных в определении 1.46 искажений включает также все известные атаки, применимые для данной системы ВИ, то такая СВИ называется *секретной*.

Определение 1.53. Если множества $\mathbb{M}$ и $\overline{\mathbb{M}}$ не пусты, то говорят, что система встраивания информации является *полухрупкой*.

Определение 1.54. Если множество $\mathbb{M}$ пусто, а $\overline{\mathbb{M}}$ включает все возможные искажения $\overline{\mathcal{M}_0}\left(\mathrm{X}, \overline{\mathbf{d_0}}\right), \overline{\mathcal{M}_1}\left(\mathrm{X}, \overline{\mathbf{d_1}}\right), \dots, \overline{\mathcal{M}_{\overline{\mathrm{N}_{\mathbb{M}}}-1}}\left(\mathrm{X}, \overline{\mathbf{d}_{\overline{\mathrm{N}_{\mathbb{M}}}-1}}\right)$, которые могут происходить при передаче и использовании носителя информации, то говорят, что система встраивания информации является *хрупкой*.

Прочие свойства

Определение 1.55. Информация, передаваемая средствами СВИ, называется *публичной*, если при её извлечении используется функция вида (1.19) или (1.20):

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times K \times K^{C} \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^{W}}, \boldsymbol{k}, \widetilde{k^{C}}\right). \tag{1.19}$$

$$\mathcal{D} : \mathbb{Y}_{[]}^{l} \times K \mapsto \mathbb{Y}_{[]}^{l}, \qquad \tilde{\Omega} = \mathcal{D}\left(\widetilde{f^{W}}, \boldsymbol{k}\right). \tag{1.20}$$

причём $\mathbf{k} = (1, k^{p})$, то есть секретный ключ отсутствует. В противном случае информация называется *частной*.

Свойство *типа контейнера*, для встраивания в который предназначена система ВИ, характеризуется размерностью m и диапазоном значений $\mathbb{X}$ множества $\mathbb{X}_{[]}^{m}$. Ниже перечислим стандартные варианты множества $\mathbb{X}_{[]}^{m}$ для основных типов сигналов:

- для звуковых сигналов $m = 1$ и $\mathbb{X} = \mathbb{B}^{16}$;
- для полутоновых изображений $m = 2$ и $\mathbb{X} = \mathbb{B}^{8}$;
- для видеосигналов и многокомпонентных изображений $m = 3$ и $\mathbb{X} = \mathbb{B}^{8}$.

Свойства визуальной различимости встроенной информации и типа СВИ согласно (см. раздел 1.1.3) формулируются на качественном уровне без использования ММ СВИ.

Список литературы

Barni Mauro and Bartolini Franco Watermarking Systems Engineering [Book]. - New-York : Marcel Dekker, Inc., 2004. - p. 485.

Cole Eric Hiding in Plain Sight: Steganography and the Art of Covert Communication [Book] / ed. Long Carol. - [s.l.] : Wiley Publishing, Inc., 2003. - p. 362.

Cox I.J. [et al.] Digital Watermarking and Steganography [Book]. - [s.l.] : Elsevier, 2008. - 2nd : p. 587.

Cox I.J. Secure Spread Spectrum Watermarking for Multimedia [Article] // IEEE transactions on image processing. - [s.l.] : IEEE, 1997. - 12 : Vol. 6. - pp. 1673-1687.

Harris Chris and Stephens Mike. A combined corner and edge detector [Conference] // Alvey vision conference. - [s.l.] : The Plessey Company plc., 1988. - pp. 147-151.

Meerwald P. Digital Watermatrking in the Wavelet Transform Domain [Report] : Doctoral Dissertation / Department of Computer Science ; University of Salzburg. - Salzburg : [s.n.], 2001. - p. 185.

Miller Matt L. [et al.] A review of watermarking, principles and practices [Book Section] // Digital Signal Processing in Multimedia Systems / book auth. Parhi K.K. and Nishitani T.. - [s.l.] : Marcel Dekker, Inc., 1999.

Nakai Y. Semi Fragile Watermarking Based on Wavelet Transform [Article] // Lecture Notes in Computer Science / ed. Shum H.-Y., Liao M. and Chang S.-F.. - [s.l.] : Springer, 2001. - Vol. 2195. - pp. 796-803.

Petitcolas F.A.P., Anderson R.J. and Kuhn M.G. Information Hiding - A Survey [Journal] // Proceedings of the IEEE. - [s.l.] : IEEE, 1999. - 7 : Vol. 87. - pp. 1062-1078.

Pfitzmann Birgit Information Hiding Terminology: Results of an informal plenary meeting and additional [Conference] // Proc. Information Hiding Workshop, LNCS. - [s.l.] : Springer-Verlag, 1996. - Vol. 1174. - pp. 347-350.

Schmid Cordelia, Mohr Roger and Bauckhage Christian Evaluation of interest point detectors [Article] // International Journal of Computer Vision. - [s.l.] : Springer, 2000. - 2 : Vol. 37. - pp. 151-172.

Schneir B. Applied Cryptography [Book]. - [s.l.] : John Wiley & Sons, Inc., 1996. - 2nd edition : p. 662.

Wu Chung-Ping and Kuo C.-C.J. Fragile Speech Watermarkin for Content Integrity Verification [Conference] // ISCAS 2002. IEEE International Symposium on Circuits and Systems, 2002.. - Phoenix-Scottsdale, AZ : IEEE, 2002. - Vol. 2. - pp. 436-439.

Агрaновский А.В. [и др.] Стеганография, цифровые водные знаки и стеганоанализ [Книга]. - Москва : Вузовская книга, 2009. - стр. 220.

Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов [Книга]. - Москва : Мир, 1989. - стр. 448.

Грибунин В.Г., Оков И.Н. и Туринцев И.В. Цифровая стеганография [Книга]. - Москва : Солон-Пресс, 2000. - стр. 272.

Чернов В.М. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований [Книга]. - Москва : Физматлит, 2007. - стр. 264.

Ярославский Л. П. Введение в цифровую обработку изображений [Книга]. - Москва : Советское радио, 1979. - стр. 312.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

КУРС ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

«КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ»

Раздел 2: Особенности представления мультимедийной информации и восприятия её человеком

Самара 2013

Оглавление

2 Особенности представления мультимедийной информации и восприятия её человеком

2.1 Особенности представления и восприятия изображений

2.1.1 Понятие непрерывного изображения. Спектральная чувствительность

Функция яркости

Рассмотрим объект, освещенный источником света, как показано на рисунке 2.1. На некотором расстоянии от объекта *распределение энергии источника светового излучения*, отраженного объектом, по пространственным координатам x_1, x_2 и по длинам волн λ описывается функцией $C(x_1, x_2, \lambda)$. Эта величина является неотрицательной. Её максимальное значение в изображающих системах ограничено предельной величиной светочувствительности регистрирующих сред:

$$0 \le C(x_1, x_2, \lambda) \le C_{max}, \qquad (2.1)$$

где C_{max}- максимальная яркость изображения.

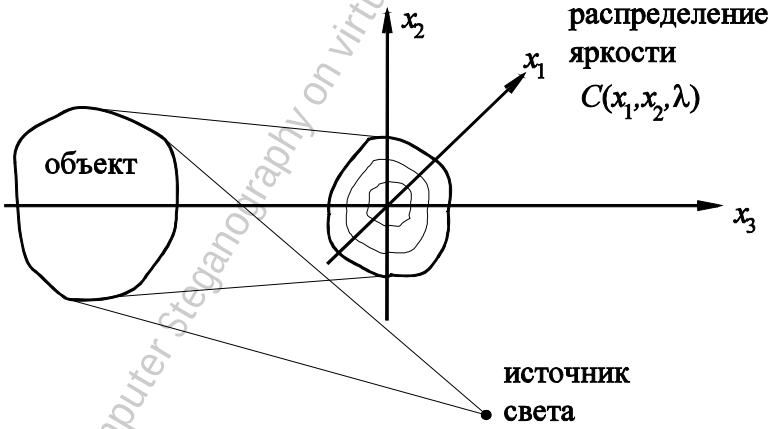


Рисунок 2.1 – Формирование изображения объекта, освещенного источником света

Геометрические размеры ограничены характеристиками формирующей системы и размерами фоторегистрирующей среды. Будем полагать, что все изображения отличны от нуля в прямоугольной области

$$-L_1 \le x_1 \le L_1, \quad -L_2 \le x_2 \le L_2. \qquad (2.2)$$

Понятие непрерывного изображения

Как в случае наблюдения объекта человеком, так и в случае использования видеодатчика, наблюдаемое изображение является результатом усреднения функции $C(x_1, x_2, \lambda)$ по диапазону длин волн с весовой функцией $s(\lambda)$ и описывается выражением

$$f(x_1, x_2) = \int_{\lambda_{min}}^{\lambda_{max}} C(x_1, x_2, \lambda)\, s(\lambda)\, d\lambda. \qquad (2.3)$$

Функцию $f(x_1, x_2)$ в дальнейшем будем называть *изображением*. Таким образом, изображение – это ограниченная функция двух пространственных переменных, заданная на ограниченной прямоугольной области.

Спектральная чувствительность

Человеческое зрение и видеодатчики обладают спектральной чувствительностью, описываемой функцией $s(\lambda)$.

Как известно, человеческий глаз обладает чувствительностью к свету в диапазоне волн от $\lambda_{min} = 0{,}35$ мкм до $\lambda_{max} = 0{,}78$ мкм. В глазу человека содержатся два типа светочувствительных клеток (рецепторов): высоко чувствительные палочки, отвечающие за сумеречное (ночное) зрение, и менее чувствительные колбочки, отвечающие за цветное зрение.

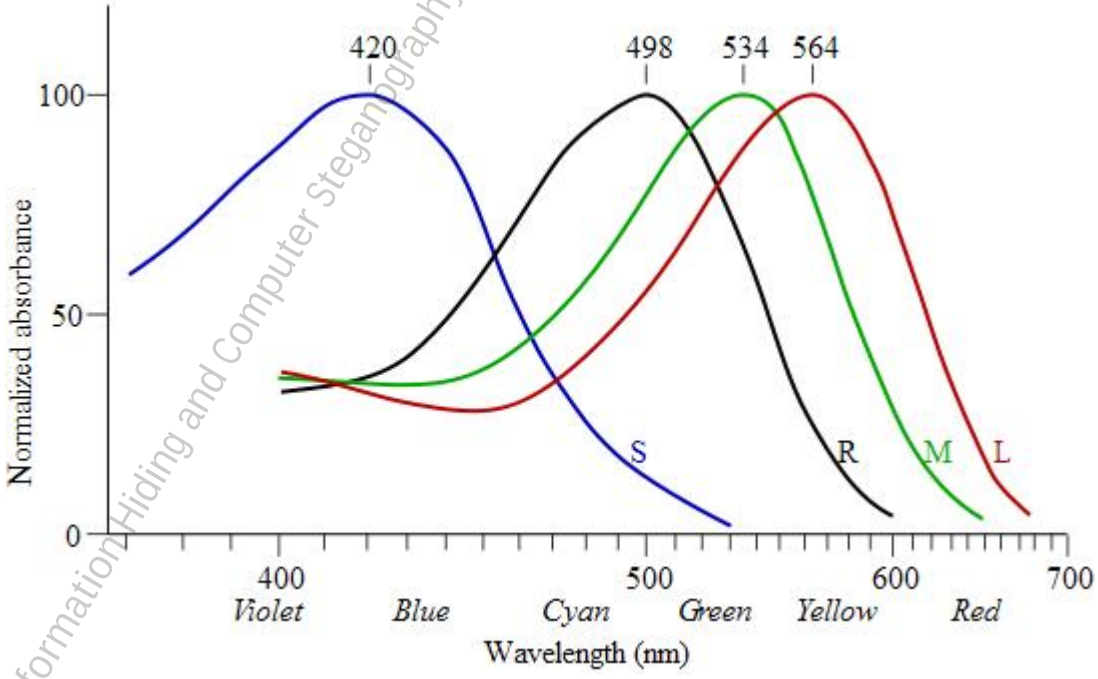


Рисунок 2.2 – Нормализованные графики светочувствительности колбочек S, M, L и палочек R человеческого глаза

В сетчатке глаза человека есть три вида колбочек, максимумы чувствительности которых приходятся на красный, зелёный и синий участки спектра. Соответствие типов колбочек трём «основным» цветам (R, G и B) обеспечивает распознавание человеком тысяч цветов и оттенков. Кривые спектральной чувствительности трёх видов колбочек частично перекрываются. Очень сильный свет возбуждает все 3 типа рецепторов, и потому воспринимается, как излучение слепяще-белого цвета. Равномерное раздражение всех трёх элементов, соответствующее средневзвешенному дневному свету, также вызывает ощущение белого цвета (см. таблицу 2.1). Для справки в таблице 2.2 приведены диапазоны длин волн, соответствующие основным цветам.

Таблица 2.1. Области чувствительности трёх типов колбочек

Тип колбочек	Воспринимаемые длины волн	Максимум чувствительности
S	400—500 нм	420—440 нм
M	450—630 нм	534—545 нм
L	500—700 нм	564—580 нм

Мозг воспринимает комбинированную информацию от разных рецепторов, что обеспечивает различное восприятие света с разной длиной волны.

Каждый видеодатчик также обладает индивидуальной характеристикой спектральной чувствительности, обусловленной физикой прибора. Имеются видеодатчики ультрафиолетового и инфракрасного диапазонов, которые широко используются, например, при проведении спектрозональных съемок Земли из космоса.

Таблица 2.2. Диапазоны длин волн основных цветов видимого диапазона

Название цвета	Границы спектрального диапазона в нм
Красный	620-780
Оранжевый	585-620
Желтый	575-585
Желто-зелёный	550-575
Зелёный	510-550
Голубой	480-510
Синий	450-480

2.1.2 Цветовые пространства

Международным комитетом по освещению CIE (Commission Internationale de l'Eclairage) в первой половине XX века проводились работы по стандартизации традиционно используемых понятий, связанных с восприятием освещения, а также формализации представления цвета.

Так, согласно CIE, цветом называется результат восприятия действия света видимого спектрального диапазона

в 1931 году было доказано, что для правильного отображения цвета достаточно трёх компонент.

Согласно CIE, *цвет* – это результат восприятия действия света видимого спектрального диапазона с длиной волны от 400 нм до 700 нм, попадающего на сетчатку глаза.

Яркость, согласно CIE, – это атрибут визуального восприятия световой области глазом человека. Поскольку яркость, воспринимаемая отдельным человеком, определяется не только характеристиками его зрения, но и особенностями мозговой деятельности, она очень индивидуальна, и объективно количественно определить её невозможно. Тем не менее, на практике существуют методы расчёта примерной яркости, использующие модели системы человеческого зрения.

Рассмотрим основные цветовые пространства, используемые для представления полноцветных изображений.

1. XYZ — линейная трёхкомпонентная цветовая модель, основанная на результатах измерения характеристик человеческого глаза. Построена на основе зрительных возможностей «стандартного наблюдателя», то есть гипотетического зрителя, возможности которого были тщательно изучены и зафиксированы в ходе длительных исследований человеческого зрения, проведённых комитетом CIE (фр. Commission Internationale de l'Eclairage).

Говоря об «эталонных» оттенках, часто говорят только о паре x и y, полагая $z = 1 - x - y$. Говоря о яркости в пространстве XYZ, часто имеют в виду величину Y.

2. RGB (аббревиатура английских слов Red, Green, Blue — красный, зелёный, синий) — аддитивная цветовая модель, описывающая способ синтеза цвета для цветовоспроизведения. В российской традиции иногда обозначается как КЗС.

Аддитивной она называется потому, что цвета получаются путём добавления (англ. “addition”) к черному. Иначе говоря, если цвет экрана, освещённого цветным прожектором, обозначается в RGB как (r_1, g_1, b_1), а цвет того же экрана, освещенного другим прожектором, —(r_2, g_2, b_2), то при освещении двумя прожекторами цвет экрана будет обозначаться как $(r_1 + r_2, g_1 + g_2, b_1 + b_2)$.

Связь компонент RGB и XYZ:

$$r = 0{,}64x + 0{,}33y, \qquad (2.4)$$
$$g = 0{,}29x + 0{,}6y,$$
$$b = 0{,}15x + 0{,}06y.$$

3. CMYK (Cyan, Magenta, Yellow, Key color) — субтрактивная схема формирования цвета, используемая прежде всего в полиграфии для стандартной триадной печати. Схема CMYK, как правило, обладает сравнительно небольшим цветовым охватом. Почему CMYK называют субтрактивной моделью

Так как модель CMYK применяют в основном в полиграфии при цветной печати, а бумага и прочие печатные материалы являются поверхностями, отражающими свет, удобнее считать, какое количество света отразилось от той или иной поверхности, нежели сколько поглотилось. Таким образом, если вычесть из белого три первичных цвета, RGB, мы получим тройку дополнительных цветов CMY. «Субтрактивный» означает «вычитаемый» — из белого вычитаются первичные цвета.

Связь компонент CMY и RGB:

$$c = 1 - r, \qquad (2.5)$$
$$m = 1 - g,$$
$$y = 1 - b.$$

Несмотря на то, что чёрный цвет можно получать смешением в равной пропорции пурпурного, голубого и жёлтого красителей, по ряду причин (чистота цвета, переувлажнение бумаги и др.) такой подход обычно неудовлетворителен. Поэтому используют отдельную компоненту чёрного цвета.

4. HSV (англ. Hue, Saturation, Value — тон, насыщенность, значение) — цветовая модель, в которой координатами цвета являются:

- Hue — цветовой тон, изменяющийся в пределах 0—360°;

- Saturation — насыщенность. Варьируется в пределах 0—100 или 0—1. Чем больше этот параметр, тем «чище» цвет, поэтому этот параметр иногда называют чистотой цвета. А чем ближе этот параметр к нулю, тем ближе цвет к нейтральному серому.
- Value (значение цвета)— яркость. Также задаётся в пределах 0—100 и 0—1.

Связь компонент HSV и RGB осуществляется следующим образом:

$$h = \begin{cases} 0, & c_{min} = c_{max}, \\ 60\dfrac{g-b}{c_{max}-c_{min}}, & c_{max} = r \text{ и } g \geq b, \\ 60\dfrac{g-b}{c_{max}-c_{min}} + 360, & c_{max} = r \text{ и } g < b, \\ 60\dfrac{b-r}{c_{max}-c_{min}} + 120, & c_{max} = g, \\ 60\dfrac{r-g}{c_{max}-c_{min}} + 240, & c_{max} = b, \end{cases} \qquad (2.6)$$

$$s = \begin{cases} 0, & v = 0, \\ 1 - \dfrac{c_{min}}{c_{max}}, & v \neq 0, \end{cases}$$

$$v = c_{max},$$

где

$$c_{min} = min(r, g, b),$$
$$c_{max} = max\,(r, g, b).$$

Также существуют две близкие к HSV цветовые модели HSB и HSI (B – brightness, I – intensity).

5. YCbCr — цветовая модель, в которой координатами цвета являются:

- Y – компонента яркости;
- Cb, Cr – синяя и красная цветоразностные компоненты

Связь компонент YCbCr и RGB осуществляется следующим образом:

$$y = \frac{77}{256}r + \frac{150}{256}g + \frac{29}{256}b, \qquad (2.7)$$
$$Cb = b - y,$$
$$Cy = r - y.$$

Дискретизация изображения

Рассмотрим непрерывное изображение $f(x_1, x_2)$ - функцию двух пространственных переменных x_1 и x_2 на ограниченной прямоугольной области (рис. 2.3).

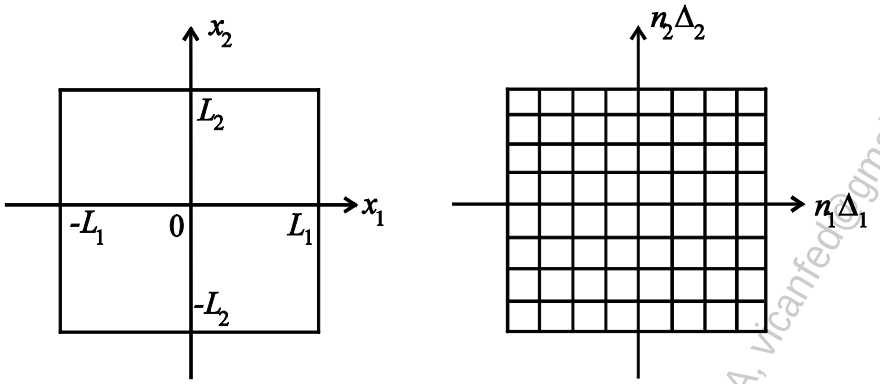


Рисунок 2.3 – Переход от непрерывного изображения к дискретному

Введем понятие шага дискретизации Δ_1 по пространственной переменной x_1 и Δ_2 по переменной x_2. Например, можно представить, что в точках, удаленных друг от друга на расстояние Δ_1 по оси x_1 расположены точечные видеодатчики. Если такие видеодатчики установить по всей прямоугольной области, то изображение окажется заданным на двумерной решетке

$$f(n_1\Delta_1, n_2\Delta_2) = f(x_1, x_2)|_{x_1=n_1\Delta_1, x_2=n_2\Delta_2} \qquad (2.8)$$

Для сокращения записи обозначим

$$f(n_1\Delta_1, n_2\Delta_2) \equiv f(n_1, n_2).$$

Функция $f(n_1, n_2)$ является функцией двух дискретных переменных и называется двумерной последовательностью. То есть дискретизация изображения по пространственным переменным переводит его в таблицу выборочных значений. Размерность таблицы (число строк и столбцов) определяется геометрическими размерами исходной прямоугольной области и выбором шага дискретизации по формуле

$$N_1 = \left[2L_1/\Delta_1\right], \qquad N_2 = \left[2L_2/\Delta_2\right]$$

где [...] обозначает целую часть числа.

Если область определения непрерывного изображения – квадрат с длиной стороны $L_1 = L_2 = L$, и шаг дискретизации выбран одинаковым по осям x_1 и x_2 ($\Delta_1 = \Delta_2 = \Delta$), то

$$N_1 = N_2 = N,$$

и размерность таблицы составляет N^2.

Элемент таблицы, полученной путем дискретизации изображения, называют “*пиксел*” или “*отсчет*”.

Квантование изображений

Память компьютера способна хранить только дискретные числа. Поэтому для записи в памяти непрерывная величина *f* должна быть подвергнута аналогово-цифровому преобразованию с шагом Δf (см. рис. 2.4.). Эту операцию часто называют квантованием. Число уровней квантования, при условии что значения функции яркости лежат в интервале $[f_{min}, f_{min} + A]$, равно

$$Q = \left[A / \Delta f \right].$$

В практических задачах обработки изображений величина *Q* варьируется в широких пределах от *Q*=2 (“бинарные” или “черно-белые” изображения) до $Q=2^{10}$ и более (практически непрерывные значения яркости). Наиболее часто выбираются $Q=2^8$, при этом пиксел изображения кодируется одним байтом информации. Из всего вышеуказанного делаем вывод, что пикселы, хранящиеся в памяти компьютера, представляют собой результат дискретизации исходного непрерывного изображения по аргументам и по уровням. Ясно, что шаги дискретизации Δ_1, Δ_2 должны выбираться достаточно малыми, для того, чтобы погрешность дискретизации была незначительна, и цифровое представление сохраняло основную информацию об изображении.

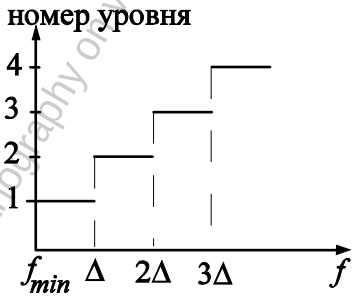


Рисунок 2.4 – Квантование непрерывной величины

2.1.2 Восприятие контраста зрительной системой человека. Закон Вебера. Эксперимент 1 (Вебера)

Яркостная адаптация

Благодаря наличию светочувствительных рецепторов двух видов: палочек и колбочек, человек способен на два разных вида зрительного восприятия окружающего мира:

– скотоскопическое зрение (сумеречное) – осуществляется при слабом свете, при этом возбуждаются только палочки.

– фотоскопическое зрение (при ярком свете) – обеспечивается колбочками.

Особенностью человеческого зрения является его способность адаптироваться к оргромному, порядка 10^{10} диапазону значений яркости – от порога чувствительности скотоскопического зрения до предела ослепляющего блеска. При этом эксперименты показывают, что субъективная яркость (то есть яркость как она воспринимается зрительной системой человека, ЗСЧ) является логарифмической функцией от физической яркости света, попадающего в глаз. На рисунке 2.5 изображён график этой зависимости субъективной яркости от истинной яркости. Длинная сплошная кривая представляет диапазон яркостей в котором способна адаптироваться зрительная система. При использовании одного фотоскопического зрения этот диапазон составляет около 10^6. Постепенный переход от скотоскопического к фотоскопическому зрению показан в виде двух пересекающихся ветвей кривой адаптации.

Рисунок 2.5 – Диапазон субъективно воспринимаемой яркости и конкретный уровень адаптации

Для правильной интерпретации столь впечатляющего динамического диапазона, изображённого на рисунке 2.5, важно понимать, что зрительная система не способна работать на всём диапазоне одновременно. Вместо этого она охватывает такой большой диапазон за счёт изменения общей чувствительности. Это явление известно как яркостная адаптация. Общий диапазон одновременно различаемых уровней яркости относительно

мал по сравнению со всем диапазоном адаптации. Для любого набора внешних условий текущий уровень чувствительности человеческого зрения, называемый уровнем яркостной адаптации, соответстует некоторой яркости, например, точке B_a (рис. 2.5). Короткая кривая B_aB_b, пересекающая основной график, – это диапазон субъективной яркости, которую способен воспринимать глаз при адаптации к заданному уровню B_a. Точка B_b – это граница восприятия яркости, дальше нее по кривой все воспринимается как черное.

Контрастная чувствительность и эксперимент Вебера

Значительный интерес представляет способность зрения различать *изменения* яркости при заданном уровне адаптации. Классический эксперимент для определения способности зрительной системы человека (ЗСЧ) различать разные уровни яркости был выполнен Эрнстом Вебером ещё в XIX в. Ниже приведены основные условия и параметры эксперимента (назовём его экспериментом 1):

- испытуемый смотрит на плоский равномерно освещенный экран, занимающий все поле зрения и имеющий яркость L_0.
- на экран наклонена маленькая добавочная яркость ΔL в границах небольшого объекта.
- испытуемый говорит, при каких ΔL он начинает воспринимать объект яркости $L_0 + \Delta L$.

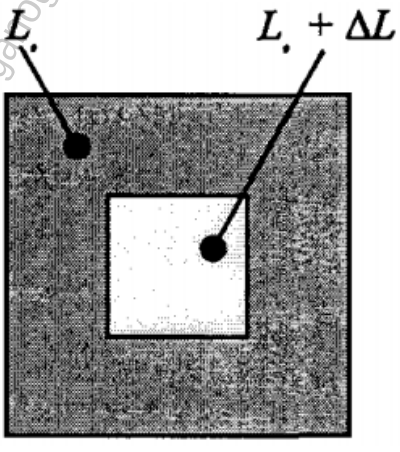


Рисунок 2.6 – Постановка эксперимента Вебера

Величина

$$C_{jn} = \frac{\Delta L_{jn}}{L_0}, \qquad (2.9)$$

где ΔL_{jn} – добавочная яркость, различимая в 50% экспериментов, называется *отношением Вебера*, а ΔL_{jn} *– едва различимой разницей*. Э. Вебер показал, что

$$\frac{\Delta L_{jn}}{L_0} \approx const,$$

то есть практически не зависит от базовой яркости L_0.

Закон Вебера: чем выше яркость фона, тем большей должна быть разница между фоном и сигналом, чтобы последний был воспринят.

Рисунок 2.7 – Пример, показывающий, что воспринимаемая яркость не является просто функцией истинной яркости. Взаимное положение по вертикали двух графиков на рис. б несущественно и выбрано для большей наглядности

Известны два явления, ясно доказывающие, что вопринимаемая яркость не является простой функцией истинной яркости. Первое основывается на том факте, что вблизи границ соседних областей с отличающимися, но постоянными яркостями зрение человека склонно «подчёркивать» яркостные перепады, как бы добавляя

несуществующие выбросы яркости, что убедительно демонстрирует пример на рис. 2.7. Хотя яркость полос постоянна, мы, кроме действительно ступенчатого изменения яркости, видим характерные выбросы вблизи краёв полос. Эти полосы с кажущимися изменениями яркости на краях называются *полосами Маха* в честь Эрнста Маха, впервые описавшего этот феномен в 1865 г. Вообще, фокусируясь на одну точку, типичный наблюдатель способен различать 10-20 различных ступеней яркости. По мере перемещения взгляда средняя яркость фона меняется, поэтому человек фактически может различить большее количество градаций яркости.

Второе явление, называемое *одновременным контрастом*, связано с тем фактом, что воспринимаемая яркость некоторой области не определяется просто её яркостью, как показано на рис. 2.8. Здесь все центральные квадраты имеют в точности одинаковую яркость, однако зрительно воспринимаются тем более тёмными, чем светлее фон.

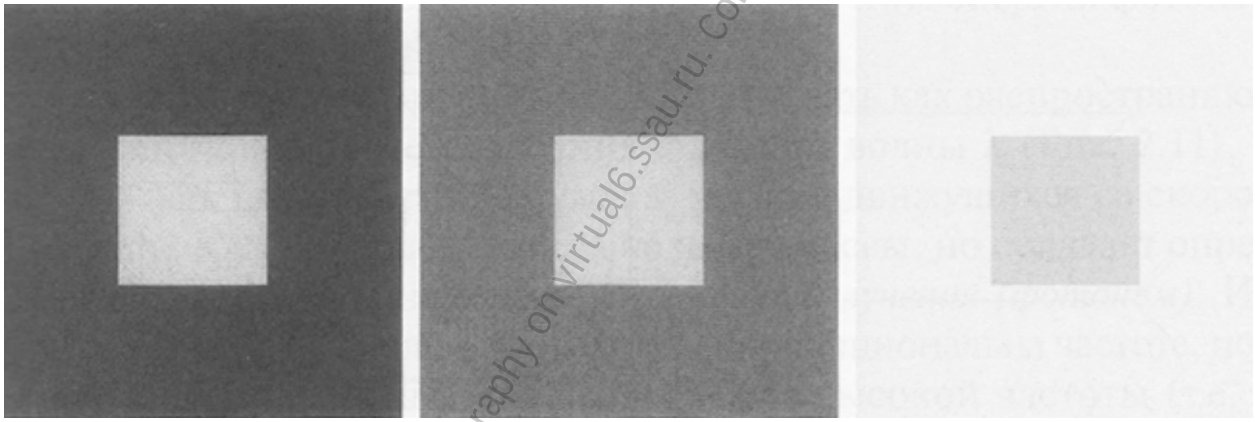


Рисунок 2.8 – Иллюстрация явления одновременного контраста

2.1.3 Функция контрастной чувствительности. Эксперимент 2

Реальные изображения не являются однотонными, а значит эксперимент Вебера не отражает всех особенностей восприятия человеком изображений. Поэтому рассмотрим эксперимент 2, согласно которому наблюдению подвергается изображение, чья яркость меняется в пространстве синусоидально (см. рис. 2.9):

$$L(x,y) = L_0 + \Delta L cos[2\pi\gamma(x\cos\theta + y\sin\theta)], \qquad (2.10)$$

где

θ – угол поворота синусоиды относительно горизонтали,

ΔL – амплитуда синусоиды,

L_0 – постоянная (опорная) яркость,

ν — пространственная частота, измеряется в циклах на метр: $\left[\frac{\text{цикл}}{\text{м}}\right]$.

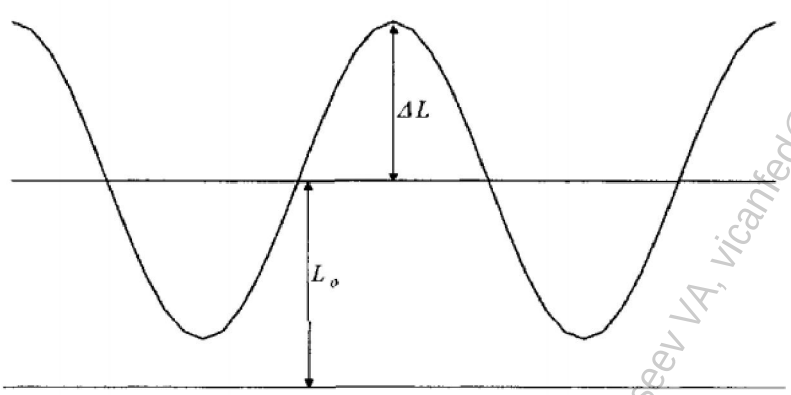


Рисунок 2.9 – Яркостный срез изображения в эксперименте 2

По аналогии с экспериментом 1 (Вебера) величина ΔL, такая, что синусоидальное изменение яркости различимо для 50% наблюдателей – участников эксперимента, называется *едва различимым порогом видимости* и обозначается ΔL_{jn} (индекс *jn* происходит от английского “just noticable” – едва различимый).

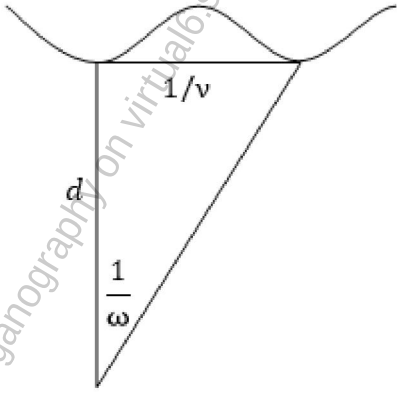


Рисунок 2.10 – Иллюстрация связи различных параметров эксперимента 2

На рис. 2.10 угол $1/\omega$ – угол наблюдения синусоиды, d – расстояние от глаза наблюдателя до изображения, $1/\nu$ – период синусоиды в метрах. Таким образом,

$$tg\frac{1}{\omega} = \frac{1}{\nu d}. \qquad (2.11)$$

При малых углах

$$\frac{1}{\omega} \approx \frac{1}{\nu d} \implies \omega \approx \gamma d. \qquad (2.12)$$

Величина $\omega\left[\frac{\text{цикл}}{\text{рад}}\right]$ – называется угловой частотой синусоиды в радианах, а величина

$$f = \frac{\pi\omega}{180} \approx \frac{\pi\gamma d}{180} \qquad (2.13)$$

– угловой частотой в градусах $\left[\frac{\text{цикл}}{\text{градус}}\right]$.

В эксперименте 2 по аналогии с первым экспериментом рассматривается величина ΔL_{jn}, но она на этот раз является функцией четырёх аргументов:

$$\Delta L_{jn} = \Delta L_{jn}(L_0, \theta, f, W), \qquad (2.14)$$

где W – угол обзора, отношение корня квадратного из площади экрана к расстоянию между экраном и наблюдателем d.

Экспериментально полученная функция $\Delta L_{jn} = \Delta L_{jn}(f)$ показана на рисунке 2.11.

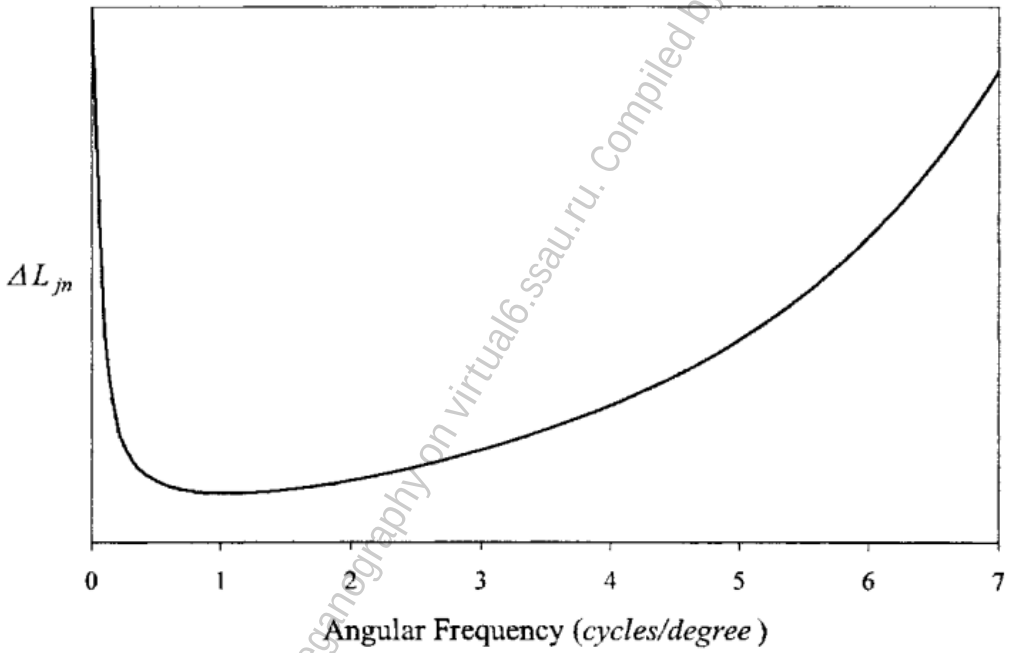


Рисунок 2.11 – График $\Delta L_{jn} = \Delta L_{jn}(f)$ в эксперименте 2

Наряду с величиной ΔL_{jn} рассматривают также величину

$$C_{jn} = \frac{\Delta L_{jn}}{L_0} = C_{jn}(L_0, \theta, W, f), \qquad (2.14)$$

называемую *едва различимым контрастом*.

Обратная величина

$$S_c = \frac{1}{C_{jn}} = \frac{L_0}{\Delta L_{jn}} \qquad (2.15)$$

– это функция контрастной чувствительности (contrast sensitivity function, CSF). CSF имеет эмпирически полученную формулу, но она очень громоздка. На рисунках 2.12 и 2.13 показаны срезы $C_{jn} = C_{jn}(f)$ при разных значениях L_0 и θ.

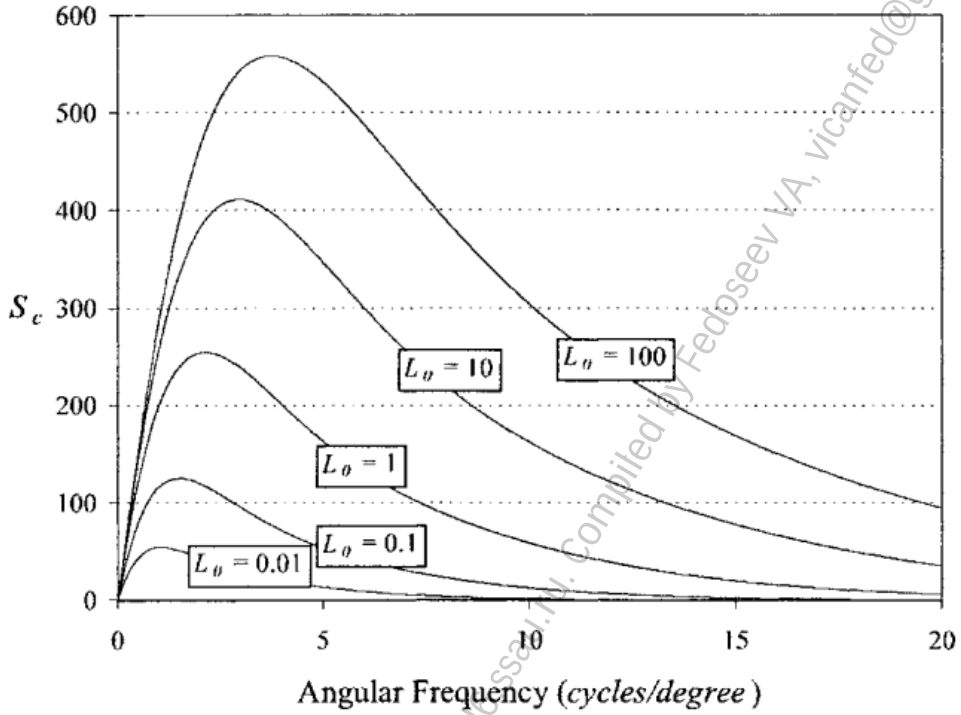


Рисунок 2.12 – График $C_{jn} = C_{jn}(f)$ при различных L_0 в эксперименте 2

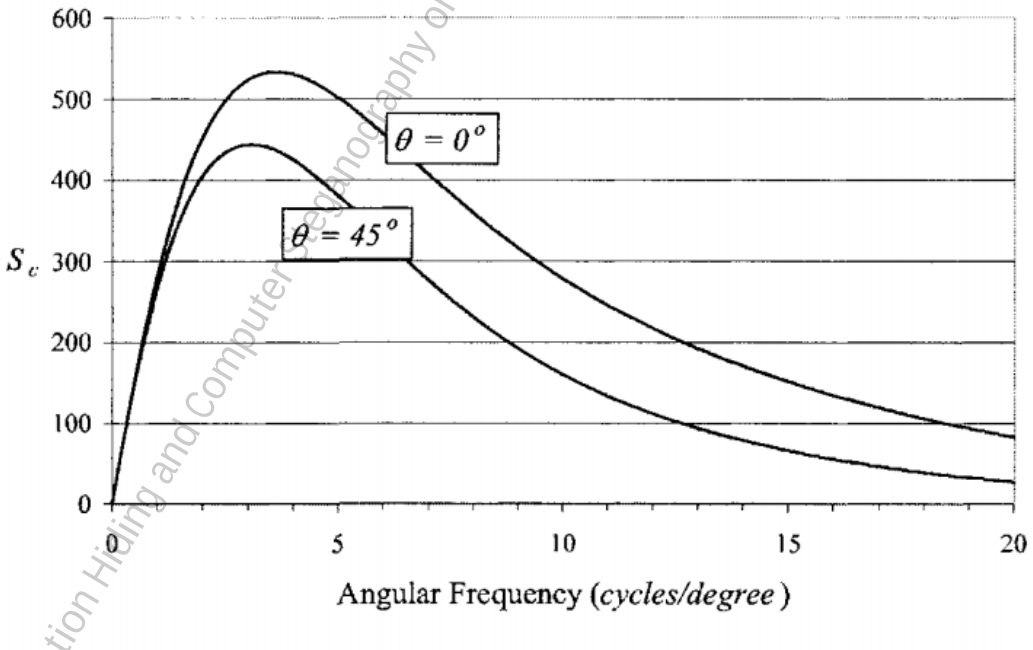


Рисунок 2.13 – График $C_{jn} = C_{jn}(f)$ при различных θ в эксперименте 2

2.1.4 Эффект маскировки в изображениях. Эксперимент 3

Чтобы знать какой сигнал можно замаскировать в изображении, необходимо рассмотреть 3-й эксперимент: контрастная различимость синусоиды на фоне синусоиды. Изображение содержит:

- Постоянный фон – L_0
- Двухмерную синусоиду – модель маскируемого сигнала, параметры $\Delta L, \theta, f$
- Двухмерную синусоиду – модель маскирующего сигнала, параметры $\Delta L_m, \theta_m, f_m$

$$L(x,y) = L_0 + \Delta L_m \cos[2\pi fm(x\cos\theta_m + y\sin\theta_m)] + \Delta L\cos[2\pi f(x\cos\theta + y\sin\theta)]$$

f вместо γ для упрощения

Для начала рассмотрим случай $f_m = f$ и $\theta_m = \theta$. Из психофизических экспериментов было получено, что существование маскирующего сигнала повышает значение едва различимого контраста, то есть большие значения ΔL должны быть, чтобы синусоида была воспринята, нежели на фоне постоянной яркости.

C_{jn}^m – маскированный ЕРК

$$C_{jn}^m = \frac{\Delta L_{jn}^m}{L_0} = C_{jn}(f, L_0, W, \theta) \cdot F\left(\frac{\Delta L_m / L_0}{C_{jn}(f, L_0, W, \theta)}\right)$$

Свойства функции $F(x)$:

- $F(0) = 1$
- $F(x) \le 1, 0 < x \le 1$
- $F(x) > 1, x > 1.$

$w \in [0.5,0.8] - F(x) = max(1, x^w)$

Если $f_m \neq f$ и $\theta_m \neq \theta$, то эффект маскировки ослабевает. Примерно можно сказать, что ухудшение эффекта маскировки зависит от $\frac{f_m}{f}$ и от разницы $|\theta_m - \theta|$. Этот эффект может быть смоделирован путем добавления функции S

$$C_{jn}^m = C_{jn}(f, L_0, W, \theta) \cdot F\left(S\left(\frac{f_m}{f}, |\theta_m - \theta|\right) \cdot \frac{\Delta L_m / L_0}{C_{jn}(f, L_0, W, \theta)}\right)$$

Свойства функции S:

- $S(1,0) = 1$ и это максимум,
- Монотонно убывающая во всех направлениях.

Пример:

$$S\left(\frac{f_m}{f}, |\theta_m - \theta|\right) = exp\left\{-\frac{log^2\left(\frac{f_m}{f}\right)}{\sigma_f^2} + \frac{(\theta_m - \theta)^2}{\sigma_\theta^2}\right\},$$

где $\sigma_f^2, \sigma_\theta^2$ имеют смысл дисперсии.

2.1.5 Эффект маскировки в видео. Эксперимент 4

Как наше зрение чувствительно на движущиеся объекты.

$L(x,t) = L_0 + \Delta L \cdot \cos[2\pi f(x - \vartheta t)]$

$\vartheta\left[\frac{\text{градус}}{\text{с}}\right]$ – скорость движения синусоиды,

$f\left[\frac{\text{цикл}}{\text{градус}}\right]$ – угловая пространственная частота,

$f_t[\text{Гц}]$ – временная частота,

$\gamma = \frac{f_t}{f}$

Экспериментально была получена следующая ФКЧ:

$$S_c = \left(6.1 + 7.3 \cdot \left|\log_{10}\left(\frac{\vartheta}{3}\right)\right|^3\right) \cdot \vartheta \cdot (2\pi f)^2 \cdot \exp\left\{-\frac{4\pi f}{45.9}(\vartheta + 2)\right\}$$

При $f_t \approx 30$ Гц значение $S_c = 2.54$, то есть близко нулю. То есть при такой частоте человеческий глаз перестает замечать движущуюся синусоиду.

Обычно, однако глаз осуществляет слежение, и скорость ϑ снижается:

$$\vartheta_{eye} = \max(g \cdot \vartheta_{object}, \vartheta_{eye}^{max})$$

$0 < g < 1$ – коэффициент, который возникает от того, что глаз вынужден поспевать за объектом, и скорость не может быть такой же. Часто принимают $g = 0.82$.

ϑ_{eye}^{max} – наибольшая скорость перемещения вектора зрения, при котором глаз еще может что-то различать.

Тогда $\vartheta = \vartheta_{object} - \vartheta_{eye} = \vartheta_{object} - \max(g \cdot \vartheta_{object}, \vartheta_{eye}^{max})$. Таким образом f_t, на которой глаз что-то различает, может возрасти до 180 Гц.

2.1.6 Выводы об основных особенностях восприятия изображений человеком

1. *Частотная чувствительность* – человек гораздо более восприимчив к низкочастотному шуму, нежели к высокочастотному шуму.

2. *Яркостная адаптация и контрастная чувствительность* – система человеческого зрения способна адаптироваться к широкому диапазону яркостей, и в каждом диапазоне человек способен различать определенные уровни яркости. Эта разрешающая способность зависит не от разности уровней яркости, а от отношения этой разности к среднему значению яркости, т.е. от контраста.
3. *Спектральная чувствительность (HSV)*: человек гораздо более восприимчив к изменению тона, нежели к изменению насыщенности: CSF(S) <<CSF(H) <<CSF(V)
4. *Спектральная чувствительность (RGB)*: CSF(B) <CSF(R) <CSF(G).

2.1.7 Метрики качества изображений

При обработке и анализе изображений всегда приходится задаваться вопросом об их качестве. Качество столь сложного объекта как изображение является очень важным, но одновременно и довольно нечетким понятием. Оно оценивается разными способами и в связи с различными задачами. В большинстве случаев качество рассматривается как мера близости двух изображений: реального и некоторого идеального, или исходного и преобразованного.

Итак, будем оценивать качество функционалом $Q = Q(X, Y)$, где X – эталонное изображение, и Y – анализируемое изображение.

Рассмотрим наиболее часто используемые показатели качества изображений.

Критерий субъективного визуального восприятия

Человеку представляется идеальное и фактическое изображения и он высказывает мнение: искажения не заметны, малозаметны или не мешают. Этот критерий не численный. Результаты такой оценки очень приблизительны.

Среднеквадратичный критерий

Полагаем, что входное и выходное изображения является фрагментами реализации случайного стационарного поля. Тогда мерой соответствия реального изображения идеальным может служить среднее значение квадрата их разности:

$$\varepsilon_{\text{кв}}^2 = E\{(X - Y)^2\}.$$

Для стационарной модели обычно считается выполненным *условие эргодичности*, при котором усреднение по ансамблю реализаций может быть заменено на усреднение по одной реализации. Тогда для непрерывных изображений, заданных на прямоугольнике $|t_1| < l_1;\ |t_2| < l_2$ имеем:

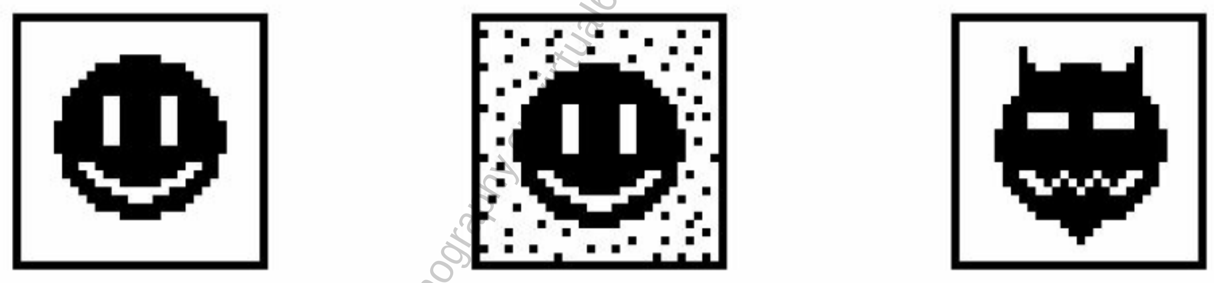
$$\varepsilon_{\text{кв}}^2 \approx \frac{1}{4l_1 l_2} \int_{-l_1}^{l_2} \int_{-l_2}^{l_2} [x(t_1 t_2) - y(t_1 t_2)]^2 dt_1 dt_2. \qquad (2.4)$$

А для дискретных, заданных при $0 \le n_1 \le N_1 - 1$, $0 \le n_2 \le N_2 - 1$:

$$\varepsilon_{\text{кв}}^2 \approx \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} [x(n_1 n_2) - y(n_1 n_2)]^2. \qquad (2.5)$$

Выражения (2.4) и (2.5) позволяют вычислять среднеквадратичную ошибку и для пары произвольных изображений, не обязательно описываемых стационарными полями. Так часто и делается. Однако в этом случае следует иметь в виду, что показатель $\varepsilon_{\text{кв}}^2$ будет характеризовать "среднее" качество изображения в целом, а на различных его фрагментах ошибки, в принципе, могут различаться.

Следует учитывать, что данный критерий плохо согласуется с критерием субъективного восприятия. Так, визуально изображение на рисунке 2.5б кажется более близким к изображению с рис. 2.5а, в то время как по среднеквадратичному критерию более близким может оказаться изображение с рис. 2.5в.



а) б) в)

Рисунок 2.5 – Иллюстрация отличия в восприятии равномерно и локально искажённого изображения: а) эталон, б) равномерно искажённое изображение, в) локально искажённое изображение

<u>Частотно-взвешенный среднеквадратичный критерий</u>

Есть разностный сигнал

$$\varepsilon(t_1, t_2) = x(t_1, t_2) - y(t_1, t_2); \equiv 0, \quad \text{если } |t_1| > l_1, \quad |t_2| > l_2.$$

$$\varepsilon(n_1, n_2) = x(n_1, n_2) - y(n_1, n_2); \ \equiv 0, \quad \text{если вне } [0; N_1 - 1] \times [0; N_2 - 1].$$

Спектры существуют в силу ограниченности поля

$$E(\Omega_1,\Omega_2)=\int_{-l_1}^{l_1}\int_{-l_2}^{l_2}\varepsilon(t_1,t_2)e^{-i[\Omega_1 t_1+\Omega_2 t_2]}dt_1dt_2$$

$$E(e^{i\varpi_1},e^{i\varpi_2})=\sum_{n_1}^{N_1-1}\sum_{n_2}^{N_2-1}\varepsilon(n_1,n_2)\,e^{-i[n_1\varpi_1+n_2\varpi_2]}$$

Теорема Парсеваля: среднее значение по пространству сигнала = среднему значению квадратов спектральных компонент.

$$\int_{-l_1}^{l_1}\int_{-l_2}^{l_2}\varepsilon^2(t_1,t_2)dt_1dt_2=\frac{1}{4\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}|E(\Omega_1,\Omega_2)|^2d\Omega_1d\Omega_2=4l_1l_2\varepsilon_{кв}^2$$

$$\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\varepsilon^2(n_1,n_2)=\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}\left|E(e^{i\varpi_1},e^{i\varpi_2})\right|^2d\varpi_1d\varpi_2=N_1N_2\varepsilon_{кв}^2,$$

Частотно-взвешенный показатель:

$$e_{кв}^2=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}W(\Omega_1,\Omega_2)\cdot|E(\Omega_1,\Omega_2)|^2d\Omega_1d\Omega_2$$

$$e_{кв}^2=\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}W(e^{i\varpi_1},e^{i\varpi_2})\cdot\left|E(e^{i\varpi_1},e^{i\varpi_2})\right|^2d\varpi_1d\varpi_2,$$

W - некоторая неотрицательная вещественная весовая функция; подбирается эмпирически (при дискретизации периодическая). В рамках линейного восстановления рассматривать этот критерий бессмысленно. Пример: $W=\Omega_1^2+\Omega_2^2$.

КРИТЕРИЙ МАКСИМАЛЬНОЙ ОШИБКИ (равномерного приближения).

Это очень строгий критерий. Он используется в тех случаях, когда выдвигается требование высокой точности представления не изображения в целом, а каждой его точки (отсчета). Это необходимо в ответственных случаях, при получении ценных, уникальных изображений.

Однако данный показатель имеет серьезный недостаток – сложность теоретической оценки и, соответственно, использования его в процедурах оптимизации (по крайней мере для общепринятых моделей изображения).

$$\varepsilon_{max}=\max_{(t_1,t_2)}|x-y|\ \text{ или }\ \varepsilon_{max}=\max_{(n_1,n_2)}|x-y|.$$

2.2 Особенности представления и восприятия звука

2.2.1 Звук. Давление звука. Слышимые звуки.

Звук — это упругая волна, продольно распространяющаяся в среде и создающая в ней механические колебания.

Упру́гие во́лны — волны, распространяющиеся в жидких, твёрдых и газообразных средах за счёт действия упругих сил.

Всякое колебание связано с нарушением равновесного состояния системы и выражается в отклонении её характеристик от равновесных значений. Для звуковых колебаний такой характеристикой является давление в точке среды, а её отклонение — звуковым давлением

Если произвести резкое смещение частиц упругой среды в одном месте, например, с помощью поршня, то в этом месте увеличится давление. Благодаря упругим связям частиц давление передаётся на соседние частицы, которые, в свою очередь, воздействуют на следующие, и область повышенного давления как бы перемещается в упругой среде. За областью повышенного давления следует область пониженного давления, и, таким образом, образуется ряд чередующихся областей сжатия и разряжения, распространяющихся в среде в виде волны. Каждая частица упругой среды в этом случае будет совершать колебательные движения.

В жидких и газообразных средах, где отсутствуют значительные колебания плотности, акустические волны имеют продольный характер, то есть направление колебания частиц совпадает с направлением перемещения волны. В твёрдых телах, помимо продольных деформаций, возникают также упругие деформации сдвига, обусловливающие возбуждение поперечных (сдвиговых) волн; в этом случае частицы совершают колебания перпендикулярно направлению распространения волны. Скорость распространения продольных волн значительно больше скорости распространения сдвиговых волн.

Слуховая система человека способна ощущать звуковые волны в виде чистых музыкальных тонов, частоты которых лежат в полосе 20…20000 Гц, а эффективное значение находится в диапазоне от примерно 10 мкПа, что соответствует абсолютному порогу слышимости в центральной части воспринимаемого диапазона частот музыкальных тонов, до 100 Па, что соответствует болевому порогу. Для сравнения

звуковых волн в таком широком диапазоне амплитуд используется логарифмическая мера — уровень звукового давления в децибелах, или умноженный на 20 десятичный логарифм отношения эффективных значений звуковых давлений двух волн: L=20 lg(p1/p2) дБ.

Децибел — безразмерная величина, но ее можно использовать как единицу измерения уровня звука, если уровень звукового давления всегда рассчитывать по отношению к одному и тому же опорному уровню, в качестве принята величина p0 = 20,4 мкПа: L=20 lg(p/p0) дБ.

При использовании этой единицы уровень громовых раскатов оценивается примерно в 120 дБ, шум самолета или музыка на рок-фестивале отвечает уровню 110 дБ, шум проходящего поезда — 100 дБ, звуки шумной улицы — 80 дБ. Разговор в комнате соответствует уровню звука примерно 50…60 дБ, а шепот — 20…30 дБ.

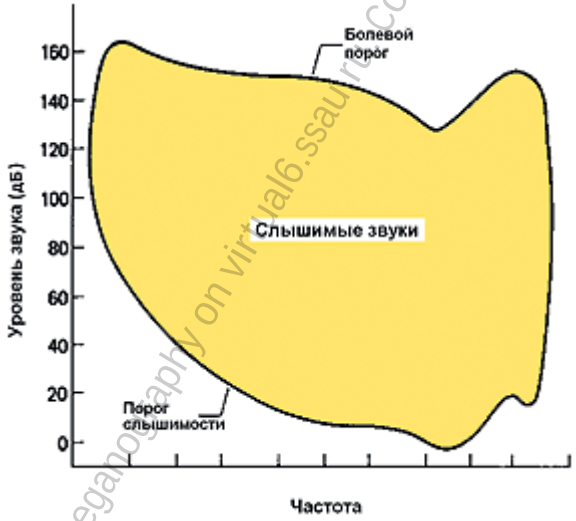


Рис. 2.6. Область слышимых звуков

Общее представление об уровнях звука, которые в среднем слышит человек, дает график на рис.1.5. При уровнях звука, приближающихся к 130 дБ, человек начинает ощущать боль в ухе, которая становится очень сильной при уровнях 145 дБ. При уровнях звукового давления, превышающих 155…160 дБ, разрушается барабанная перепонка. Надо также иметь в виду, что быстродействие системы регулирования усиления среднего уха сравнительно невелико, поэтому скачкообразное усиление интенсивности звуковой волны может привести к повреждениям среднего и внутреннего уха и при уровнях звукового давления, меньших 155…160 дБ.

Аудиосигналы можно разделить на три класса:

разговор телефонного качества, диапазон 300 – 3400 Гц;

широкополосная речь 50 – 7000 Гц;

широкополосные аудиосигналы 20 – 20000 Гц.

Связь частоты с длиной волны

L=U/v, где L - длина волны, U - скорость звука=330 м/с, v - частота=60, 70, 80 Гц.

Стандартный аудио компакт диск (CD - DA) несет информацию в формате ИКМ с параметрами 44100 Гц / 16 бит / стерео (частота дискретизации / разрядность квантования / количество каналов). Несложно подсчитать, что диск CD - DA стандартным объемом 650 Мб хранит около часа музыки: 44100 (Гц) * 16 (бит) * 2 (каналов) * 60 (секунд) * 60 (минут) / 8 (бит в байте) / 1024 (байт в килобайте) / 1024 (килобайт в мегабайте) = ~605 мегабайт.

В соответствии с теоремой Котельникова (Найквиста) частота дискретизации устанавливает верхнюю границу частот, информация о которых сохраняется в оцифрованном сигнале. А именно: максимальная частота спектральных составляющих сигнала равна половине частоты дискретизации. На практике это означает, что аудио компакт-диск, несущий данные, дискретизованные с частотой 44.1 кГц, несет информацию об оригинальной записи в полосе частот от 0 Гц до 22050 Гц. Человеческий слуховой аппарат, кстати, способен улавливать частоты в диапазоне (приблизительно) 0 – 20 кГц.

2.2.2 Частотное и временное маскирование

Частотная маскировка

Частотное разрешение описанного выше спектро-анализатора ограничено шириной полосы пропускания точки мембраны как слухового фильтра, то есть критической полосой. Спектральные компоненты, попадающие в полосу пропускания фильтра, взаимодействуют друг с другом уже в этом слуховом фильтре. При оценке результатов взаимодействия компонентов звука надо иметь в виду, что внутреннее ухо представляет собой нелинейную систему. Как известно из теории систем, теории связи и радиотехники, в нелинейных резонансных системах существуют такие эффекты, как подавление шумов сильным сигналом, подавление сильного сигнала слабым.

Многочисленные психоакустические эксперименты доказали, что подобный эффект, называемый маскировкой, существует и в слуховой системе человека.

Эффект маскировки может быть объяснен следующим образом. Как было отмечено выше, даже чистый тон возбуждает довольно широкую область основной мембраны. Предположим, что появляется второй звук — чистый тон с меньшей амплитудой и частотой, немного отличающейся от частоты первого тона. Второй тон должен возбудить колебания той области мембраны, которая уже колеблется под действием первого тона. Если бы второй тон был один, то он бы возбудил мембрану в соответствующей области и был бы слышен. Но мембрана в этой области уже колеблется, поэтому второй тон может оказаться неслышимым на фоне первого тона.

Может быть предложено следующее объяснение этого эффекта. Если ухо слышит тон с уровнем давления, например, 40 дБ, а затем добавляется тон близкой частоты, попадающей в ту же критическую полосу, что и первый тон, с уровнем 20 дБ, то ухо интегрирует звуковую энергию внутри критической полосы. Добавление второго тона увеличивает уровень результирующего звука только на 0,04 дБ (надо иметь в виду, что складываются интенсивности звуков, а не их эффективные давления). Такая малая добавка оказывается ниже порога различения органа Корти, поэтому второй звук не слышен.

Чтобы второй тон стал слышимым, его уровень должен сравниться или стать больше уровня первого тона. Но тогда уже первый тон может оказаться неслышимым на фоне более интенсивного второго тона. Этот эффект называется спектральной, или частотной, маскировкой. Второй тон может также оказаться слышимым, если при том же малом уровне его частота изменится настолько, что частотный интервал между тонами станет больше критической полосы.

Итак, два звука с близкими частотами, находящимися на расстоянии, меньшем ширины критической полосы, могут маскировать друг друга, поскольку они возбуждают практически одну область основной мембраны и взаимодействуют нелинейным образом. Обнаружению маскируемого тона не может помочь тренировка или стремление услышать. Процессы высшей нервной деятельности не могут исключить маскировку, поскольку информация о маскируемом тоне не образуется во внутреннем ухе и не направляется по слуховому нерву в головной мозг.

Подходя к проблеме временного и частотного разрешения слуха с позиций теории систем, мы придем к выводу, что звуки, имеющие сравнительно небольшой уровень и находящиеся в частотной или во временной близости с более сильным звуком, могут быть маскируемыми (рис.2.7).

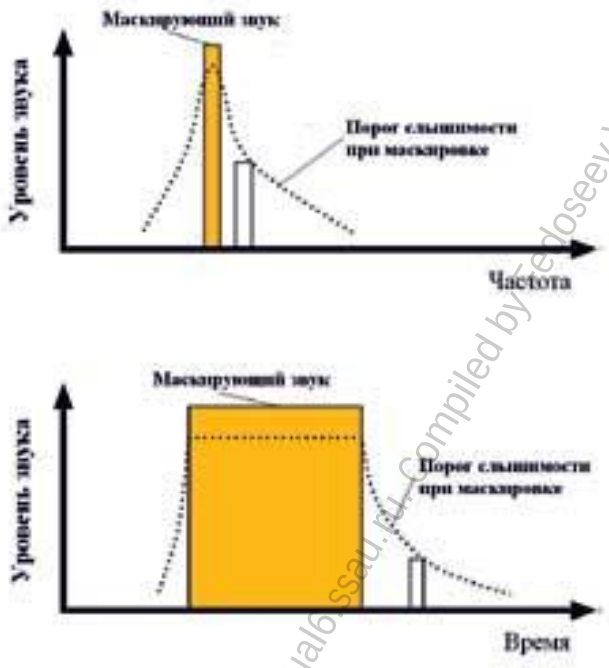


Рис. 2.7. Частотная (вверху) и временная (внизу) маскировка в слуховой системе

Ощущение одного звука может ослабляться или полностью исчезать в присутствии другого звука. В количественном отношении маскировка проявляется в увеличении порога слышимости одного звука в присутствии второго, более сильного. Она характеризуется величиной, на которую увеличивается порог слышимости маскируемого сигнала (по отношению к порогу слышимости в тишине) в присутствии маскирующего. Вследствие конечного частотного и временного разрешения слуховой системы маскировка может быть и в частотной, и во временной области.

Описанные выше свойства слуха позволяют сформулировать общий принцип передачи данных в слуховой системе, оцениваемый с позиций теории систем и техники связи. Широкополосный сигнал с большим динамическим диапазоном, каким является звук, трансформируется в набор узкополосных сигналов, каждый из которых передается в малом динамическом диапазоне и с ограниченным временным разрешением.

Информация, которая теряется в процессе такого преобразования (потери описываются процессом маскировки), не передается в мозг и не может быть слышимой.

Внутреннее ухо действует в некотором смысле как кодер компрессии с потерями. Подавляющая часть информации, которую не слышит ухо человека, теряется в этом кодере — внутреннем ухе. Описанные принципы положены в основу работы эффективных цифровых систем компрессии звуковых данных, таких, например, как MP3.

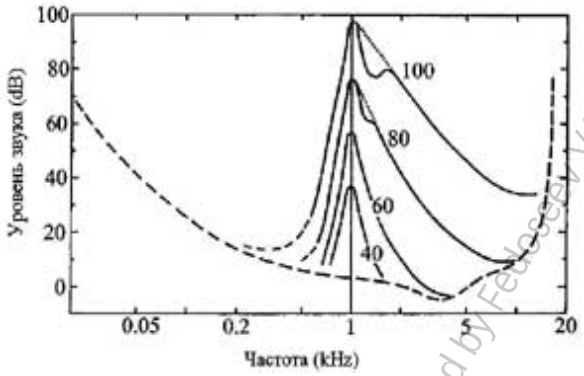


Рис. 2.8. Линии порога слышимости тона при маскировке узкополосным шумом разного уровня

На рис.2/9 показаны результаты измерения порога слышимости чистого тона в присутствии узкополосного шума со средней частотой 1 кГц, шириной полосы 160 Гц и уровнем, равным 40, 60, 80 и 100 дБ. Все кривые имеют максимум на центральной частоте шума, где пороговый уровень на 4 дБ меньше соответствующих уровней шума. В области частот, меньших 1 кГц, линии порога слышимости при маскировке быстро спадают, стремясь к порогу слышимости в тишине.

В области частот, больших 1 кГц, крутизна спада значительно уменьшается с ростом уровня маскирующего шума. Это показывает, что при больших уровнях маскирующего звука эффект маскировки проявляется в нескольких частотных группах (критических полосах), то есть маскирующий и маскируемый звуки могут отличаться по частоте (высоте тона) более, чем на 1 барк. Интерпретацию полученных результатов иллюстрирует рис. 4, на котором показаны слышимые и неслышимые звуки при частотной маскировке узкополосным шумом.

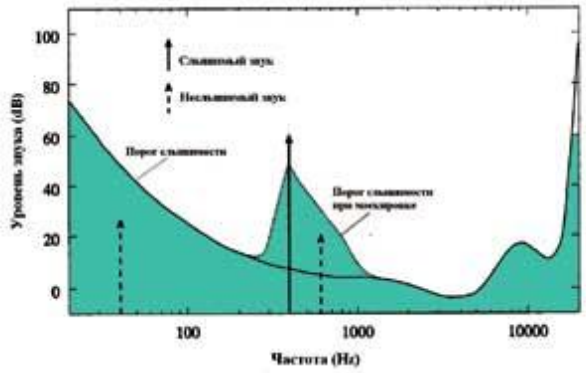


Рис. 2.9. Слышимые и неслышимые звуки при частотной маскировке

График рис. 2.10 показывает результаты измерения порога слышимости чистого тона в присутствии узкополосного шума с уровнем 80 дБ и со средней частотой, равной 200 Гц, 2 и 5 кГц. Надо отметить, что графики рис. 2.10 не отвечают целям оценки частотных характеристик точек основной мембраны, поскольку уровень испытательного (маскируемого) звука при достижении порога в присутствии маскирующего звука велик, и испытательный звук возбуждает большую область основной мембраны, длина которой превышает критическую в данной точке.

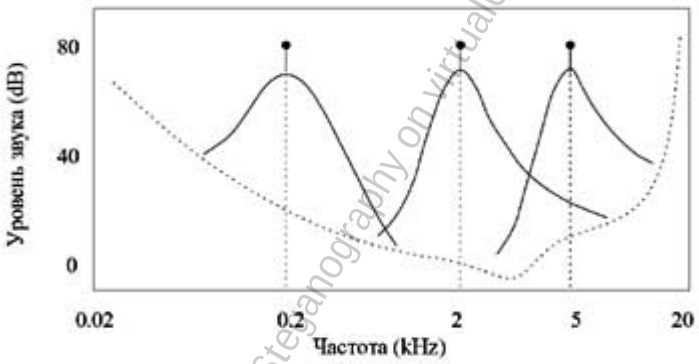


Рис. 2.10. Принцип частотного маскирования

Взгляд инженера уже давно должен был бы остановиться на рис. 2.7. Кажется, что нижний график рис. 2.7 противоречит фундаментальному закону физики — принципу причинности. На нем показано, что маскирующий звук меняет порог слышимости слабого звука перед своим появлением. Однако такая опережающая маскировка, или предмаскировка, действительно существует. На рис. 2.11 показано, что увеличение порога слышимости испытательного импульсного звука, предшествующего маскирующему звуковому импульсу, происходит в сравнительно небольшом интервале, длительность которого составляет 20…50 мс.

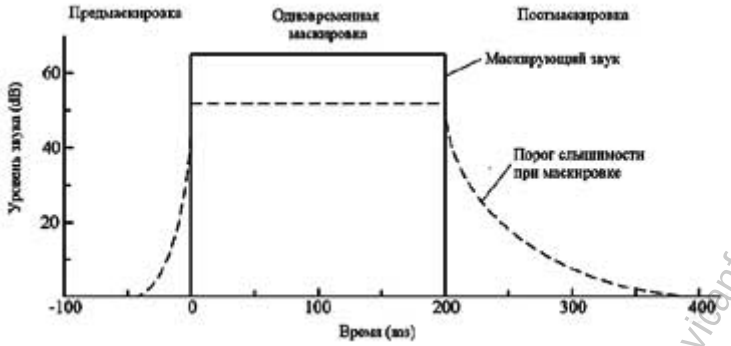


Рис. 2.11. Постмаскировка и предмаскировка

Объяснение заключается в том, что слуховой системе требуется некоторое время для того, чтобы из звука сформировать ощущение. Чем сильнее звук, тем скорее слуховая система реагирует на него. Формирование ощущения слабого сигнала требует большего времени, которое затрачивается на обработку в центральной нервной системе. Сильный маскирующий звук уже слышен к моменту формирования ощущения слабого испытательного звука, что и объясняет эффект предмаскировки.

Временная маскировка, существующая в слуховой системе, — один из важных эффектов, учтенных при создании психоакустической модели слуха и проектировании кодека MP3.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

КУРС ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

«КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ»

Раздел 3: Основные подходы, используемые при встраивании и извлечении информации

Самара 2013

Оглавление

3 Основные подходы, используемые при встраивании и извлечении информации

3.1 Методы преобразования контейнера в пространство признаков

3.1.1 Встраивание информации в пространственной области

$$\overrightarrow{f_{C_W}}(i) = \vec{f}(i) + \alpha \cdot W(i) \qquad (*)$$

$(i) -$ i-ая компонента вектора

В качестве встраиваемой информации может фигурировать встраиваемый сигнал W или встраиваемая информация $\vec{b}$.

$\alpha -$ масштабирующий коэффициент, посредством изменения которого можно регулировать уровень встраиваемого сигнала в составе сигнала-контейнера.

В некоторых схемах встраивания α может варьироваться в зависимости от контейнера.

$$\overrightarrow{f_{C_W}} = \vec{f} + \vec{\alpha} \cdot W, \qquad (**)$$

Где $\vec{\alpha} = \vec{\alpha}(\vec{f})$.

Как правило можно вектор $\vec{\alpha}$ представить в виде $\vec{\alpha} = \alpha \cdot \vec{m}$, тогда $(**)$ переписывается в форме $\overrightarrow{f_{C_W}} = \vec{f} + \alpha \cdot \vec{m} \cdot W$ $(W' = \vec{m} \cdot W)$.

То есть можно эту модель представить и в исходном виде $(*)$, но уже встраиваемый сигнал добавлен к контейнеру.

3.1.2 Схема кодирования с преобразованием

Цели кодирования с преобразованием:

1) Сжатие информации;
2) Встраивание в сигнал дополнительной информации.

Основная идея метода кодирования с преобразованием заключается в использовании "обобщенных представлений" сигнала. Процедура кодирования с преобразованием заключается в следующем. На этапе кодирования:

Каждый блок отсчетов подвергается некоторому преобразованию, в результате которого формируются обобщенные координаты сообщений;

Осуществляется кодирование обобщенных координат с целью сокращения избыточности данных или с целью встраивания сигнала.

На этапе декодирования:

1) Декодируются обобщенные координаты;
2) Вычисляется обратное преобразование, то есть по декодированным значениям обобщенных координат вычисляются отсчеты модифицированного сигнала.

При разработке процедуры кодирования с преобразованием приходится решать две основные задачи:

1. Выбор вида преобразования для получения обобщенных координат.
2. Выбор метода обработки (кодирования) обобщенных координат.
3. Выбор преобразования

В принципе, обобщенными координатами сигнала могут служить любые его характеристики на интервале представления. Но для задачи компрессии данных и встраивания данных (то есть для разделения компонент на хорошо видимые и плохо видимые) нужно, чтобы используемое преобразование отвечало нескольким требованиям:

Преобразование должно быть обратимым, то есть позволять переходить от обобщенных координат обратно к отсчетам.

Обобщенные координаты должны быть менее коррелированными, чтобы основной объем информации о сигнале был сконцентрирован в небольшом числе обобщенных координат (для достижения эффекта сжатия), а также чтобы изменение одних компонент не приводило к изменению других.

Преобразование (прямое и обратное) должно достаточно просто вычисляться.

Практически всегда в качестве обобщенных координат берутся коэффициенты разложения сигнала в ряд по какому-либо дискретному ортогональному базису (иногда называемые трансформантами). Для одномерного сигнала $\mathrm{f(n)}$ на интервале $0 \leq \mathrm{n} \leq \mathrm{N}-1$ такое разложение может быть записано в следующей общей форме:

$$F(m) = \sum_{n=0}^{N-1} f(n)\, A(m,\ n)\ )$$

- прямое преобразование (вычисление трансформант).

$$f(m) = \sum_{m=0}^{N-1} F(m)\, B(m,\ n)$$

- обратное преобразование, где матрицы $\mathrm{A(m,n)}, \mathrm{B(m,n)}$ – ядра прямого и обратного преобразования. Если принять, что строки $\mathrm{B(m,n)}$ ортогональны:

$$\sum_{n=0}^{N-1} B(m,\ n)B^*(k,\ n) = \|B_m\|^2\ \delta(m-k)\ ,$$

то можно получить, что

$$A(m,\ n) = \frac{B^*(m,n)}{\|B_m\|^2}\ .$$

Если при этом все нормы равны:

$$\|B_m\|^2 = \|B\| = const\ ,$$

будут ортогональны и столбцы матрицы $\mathrm{B(m,n)}$, то есть кроме (6.38) будет справедливо и соотношение

$$\sum_{m=0}^{N-1} B(m,\ n)B^*(m,\ k) = \|B_n\|^2\ \delta(n-k)$$

и далее:

$$\sum_{n=0}^{N-1} A(m,\ n)A^*(k,\ n) = \frac{1}{\|B\|^2}\ \delta(m-k)\ ,$$

$$\sum_{m=0}^{N-1} A(m,\ n)A^*(m,\ k) = \frac{1}{\|B\|^2}\ \delta(n-k)\ ).$$

Как видно, в данном случае первое требование (обратимость преобразования) является выполненным.

Ортогональным преобразованием, идеальным с точки зрения второго требования является так называемое преобразование Хотеллинга (дискретное преобразование Карунена-Лоэва). Это преобразование строится из условия получения некоррелированных трансформант. Выведем основное соотношение для нахождения базисных функций Хотеллинга. Пусть искомый базис – вещественный и ортогональный:

$$A(m,n) = B(m,n)\quad (\|B\| = 1\ )$$

АКФ для трансформант (в предположении центрированности сигнала и его трансформант) исходя из требования их некоррелированности должна быть

$$\mathrm{B_F(m,\ k) = E\{F(m)\ \ F(k)\} = E\left\{\sum_{n=0}^{N-1} f(n)\ A(m,n)\ \sum_{l=0}^{N-1} f(l)\ A(k,l)\right\} =}$$
$$\mathrm{= \sum_{n=0}^{N-1}\sum_{l=0}^{N-1} A(m,n)\ A(k,\ l)\ \ B_f(n,\ l) = D_F(m)\delta(m-k)}$$

(при этом необязательно чтобы сигнал был стационарным).

Умножим обе части выражения на последнем шаге (6.39) на $\mathrm{A(k,p)}$ и просуммируем по k:

$$\mathrm{\sum_{k=0}^{N-1} A(k,p)D_F(m)\delta(m-k) = \sum_{k=0}^{N-1}\ \sum_{n=0}^{N-1}\ \sum_{l=0}^{N-1} A(k,p)\ A(m,n)\ A(k,\ l)\ \ B_f(n,}$$
$$\mathrm{l}$$

или

$$D_F(m)\,A(m,p) = \sum_{n=0}^{N-1}\sum_{l=0}^{N-1} A(m,n)\left[\sum_{k=0}^{N-1} A(k,\ p)\ A(k,\ l)\right] B_f(n,\ l) =$$
$$= \sum_{n=0}^{N-1}\sum_{l=0}^{N-1} A(m,n)\delta(p-l)\,B_f(n,l) = \sum_{n=0}^{N-1} A(m,n)B_f(n,\ p)\ .$$

Или окончательно:

$$D_F(m)\,A(m,\ p) = \sum_{n=0}^{N-1} A(m,\ n)\,B_f(n,p)\ .$$

Видно, что строки $A(m,p)$ (и, соответственно, $A(m,n)$) есть собственные функции (векторы) ковариационной функции (матрицы) B_f, а $D_F(m)$ – ее собственные значения. Поэтому преобразование Хотеллинга называют еще разложением по собственным векторам АКФ. Можно показать, что кроме некоррелированности трансформант преобразование Хотеллинга обеспечивает максимально быстрое убывание их дисперсии (собственных значений), то есть обладает именно тем свойством, которое сформулировано выше во втором требовании к преобразованию. Все другие базисы дают более медленное убывание, а значит требуют для той же точности представления данных использования (передачи) большего числа трансформант. Однако несмотря на столь ценное качество преобразования Хотеллинга на практике оно применяется редко, так как, во-первых его базис оказывается жестко привязанным к АКФ сигнала (его пришлось бы все время пересчитывать, а последнее уравнение чаще всего в явном виде не решается), и, во-вторых, для него в общем случае не существует быстрого алгоритма вычисления, то есть оно совершенно не удовлетворяет третьему условию, сформулированному выше. Поэтому преобразование Хотеллинга возникает обычно в теоретических рассмотрениях как идеал, к которому нужно стремиться, а на практике применяются другие преобразования, для которых существуют быстрые алгоритмы.

Сравнительный анализ различных дискретных ортогональных базисов выполнялся большим числом исследователей. Укажем некоторые известные и наиболее важные факты, относящиеся к этому вопросу.

Найдено, что преобразование Хотеллинга хорошо аппроксимируется дискретным преобразованием Фурье (в курсе ЦОС была теорема, согласно которой ДПФ тоже декоррелирует сигнал, правда, не абсолютно, а асимптотически, при $N \to \infty$). Недостатки ДПФ – его комплекснозначность, что затрудняет обработку трансформант. Разработаны и используются вещественные базисы: Фурье в форме Хартли, косинусное, Уолша, семейство вейвлет-преобразований и т.д. Дискретное косинусное преобразование, как выяснилось, чрезвычайно близко подходит по свойствам к преобразованию Хотеллинга

для многих сигналов (например, экспоненциально коррелированных). Преобразование Уолша, Хаара и им подобные применяются тогда, когда предъявляются жесткие требования к сложности аппаратуры и скорости вычислений, однако для компрессии сигналов они менее эффективны.

При обработке изображений все изложенное чаще всего используется в "двумерной" модификации. Матрица отсчетов разбивается на блоки – двумерные интервалы представления и применяются двумерные преобразования. В двумерном случае при кодировании изображений средней детальности чаще всего используют квадратные блоки 8×8, 16×16, 32×32. Дальнейшее увеличение размеров блоков практически не повышает эффективность компрессии, а лишь усложняет процедуру обработки как на кодирующей, так и на декодирующей стороне.

3.1.3 Примеры дискретных спектральных преобразований и их особенности

Одними из наиболее эффективных методов цифровой обработки сигналов являются методы, связанные с использованием дискретных ортогональных преобразований.

$$\mathrm{F(m)} = \sum_{\mathrm{n=0}}^{\mathrm{N-1}} \mathrm{f(n)\,A(m,\quad n)}$$

Определение 5.1. Пусть $\mathrm{f(n)} \in \mathbb{C}$ - периодическая с периодом *N* комплекснозначная последовательность, $\{h_{\mathrm{m}}(\mathrm{n})\}_{\mathrm{m=0}}^{\mathrm{N-1}}$ - семейство *N*-периодических комплекснозначных функций с условием ортогональности

$$\langle h_{\mathrm{m}}, h_{\mathrm{k}} \rangle = \sum_{\mathrm{n=0}}^{\mathrm{N-1}} h_{\mathrm{m}}(\mathrm{n})\overline{h_{\mathrm{k}}(\mathrm{n})} = \delta_{\mathrm{mk}} \qquad (5.1)$$

(δ_{mk} - дельта-символ Кронекера, черта означает комплексное сопряжение). Преобразование

$$\mathrm{f} = \big(\mathrm{f}(0), \ldots, \mathrm{f(N-1)}\big) \mapsto \big(\mathrm{F}(0), \ldots, \mathrm{F(N-1)}\big) = \mathrm{F}, \qquad (5.2)$$

определяемое соотношением,

$$\mathrm{F(m)} = \sum_{\mathrm{n=0}}^{\mathrm{N-1}} \mathrm{f(n)} h_{\mathrm{m}}(\mathrm{n}) \quad (m=0, 1, \ldots, N\text{-}1) \quad (5.3)$$

называется *дискретным ортогональным преобразованием* (ДОП) с базисом $\{h_{\mathrm{m}}(\mathrm{n})\}_{\mathrm{m=0}}^{\mathrm{N-1}}$.

Преобразование (5.3) линейно и может быть записано в матричной форме

$$\mathrm{F}^{\mathrm{T}} = \mathrm{H}\mathrm{f}^{\mathrm{T}}, \qquad (5.4)$$

где f^{T}, F^{T} - транспонированные к векторам (5.2) векторы-столбцы,

$$\mathrm{H} = \begin{pmatrix} h_0(0) & \dots & h_0(\mathrm{N}-1) \\ \dots & \dots & \dots \\ h_{\mathrm{N}-1}(0) & \dots & h_{\mathrm{N}-1}(\mathrm{N}-1) \end{pmatrix}. \qquad (5.5)$$

Определение 5.2. Матрица **H**, определенная равенством (5.5), называется *матрицей дискретного ортогонального преобразования* (5.3).

Пример 5.1. Преобразование (5.3) с базисными функциями

$$h_{\mathrm{m}}(\mathrm{n}) = \frac{1}{\sqrt{\mathrm{N}}} \exp\left\{2\pi \mathrm{i} \frac{\mathrm{mn}}{\mathrm{N}}\right\} \qquad (5.6)$$

называется *дискретным преобразованием Фурье* (ДПФ).

Пример 5.2. Преобразование (5.3) с базисными функциями

$$h_{\mathrm{m}}(\mathrm{n}) = \frac{1}{\sqrt{\mathrm{N}}}\left(\cos\frac{2\pi\mathrm{mn}}{\mathrm{N}} + \sin\frac{2\pi\mathrm{mn}}{\mathrm{N}}\right) \quad (5.7)$$

называется *дискретным преобразованием Хартли*.

Пример 5.3. Преобразование (5.3) с базисными функциями

$$h_{\mathrm{m}}(\mathrm{n}) = \lambda_{\mathrm{m}} \cos\frac{\pi\left(\mathrm{n}+\frac{1}{2}\right)\mathrm{m}}{\mathrm{N}}, \qquad (5.8)$$

где нормирующие коэффициенты λ_{m} определены равенством

$$\lambda_{\mathrm{m}} = \begin{cases} \frac{2}{\sqrt{\mathrm{N}}} & \text{при} \quad \mathrm{m} \neq 0, \\ \frac{1}{\sqrt{\mathrm{N}}} & \text{при} \quad \mathrm{m} = 0 \end{cases} \qquad (5.9)$$

называется *дискретным косинусным преобразованием* (ДКП).

Непосредственное матричное умножение в (5.4) или, что то же самое, вычисление массива *F*(*m*) в (5.3) требует $\sim \mathrm{N}^2$ арифметических операций. Поэтому в практических задачах предпочтение отдается таким ДОП, для которых арифметическая природа базисных функций позволяет синтезировать алгоритмы с существенно более низкой вычислительной сложностью. отличительной особенностью преобразований примеров 5.1-5.3 является возможность синтеза таких высокоскоростных алгоритмов.

3.1.4 Преобразование Хаара. Дискретное вейвлет-преобразование

ДПФ 1908 год.

$\forall\, m(0 \le m < 2^n = N)$ существуют единственные (p, q): $m = 2^p + q - 1$, где $0 \le p \le n - 1$,

$$q\epsilon \begin{cases} \{0 \text{ или } 1\} \text{ при } p = 0 \\ [1, 2^p] \quad \text{при } p > 0 \end{cases}$$

$$h_0(n) = \frac{1}{\sqrt{N}}(n)$$

$$h_m(n) = \begin{cases} 2^{p/2}, & \frac{q-1}{2^p} \le n < \frac{q-\frac{1}{2}}{2^p} \\ -2^{p/2}, & \frac{q-\frac{1}{2}}{2^p} \le n < \frac{q}{2^p} \\ 0, & \text{иначе} \end{cases}$$

Суть, связь с вейвлетами

Пусть имеется строка (1,2,3,4,5,6,7,8)

$$\underbrace{\left(\frac{3}{2}, \frac{7}{2}, \frac{11}{2}, \frac{15}{2}\right)}_{\text{НЧ-L}}, \underbrace{\left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)}_{\text{ВЧ-H}}$$

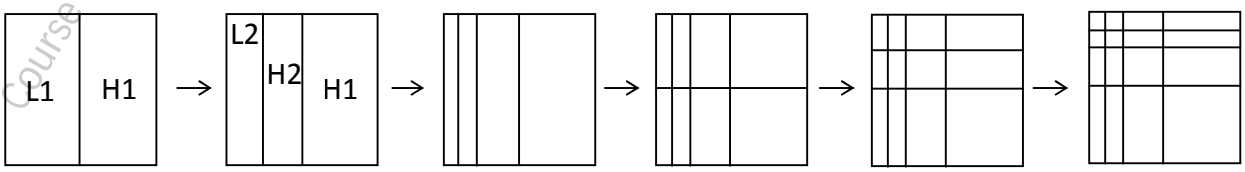
$$\psi(t) = \begin{cases} 1, 0 \le t < 0.5 \\ -1, 0.5 \le t < 1 \end{cases}$$

$$\underbrace{\left(\frac{5}{2}, \frac{13}{2}\right)}_{\text{LL}}, \underbrace{(-1, -1)}_{\text{LH}}, \underbrace{\left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)}_{\text{H}}$$

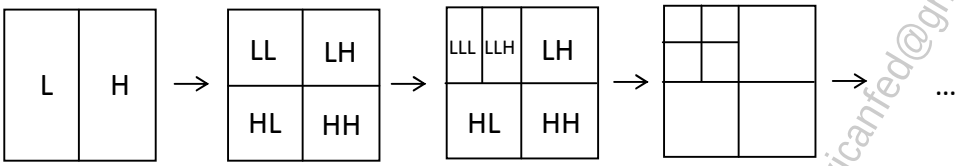
$$\underbrace{\left(\frac{9}{2}\right)}_{\text{LLL}}, \underbrace{(-2)}_{\text{LLH}}, \underbrace{(-1, -1)}_{\text{LH}}, \underbrace{\left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)}_{\text{H}}$$

2D – случай:

1) Стандартное вейвлет-разложение



2) Пирамидальное вейвлет-разложение



3.1.5 Преобразование Фурье-Меллина

Как правило, во вновь проектируемых системах вложения данных стоят требования визуальной неразличимости и (робастности) стойкости к как можно большему количеству преобразований. В этом случае выбирают для встраивания средние частоты.

1) Преобразование
2) Отбор нужных для встраивания частот

Для стойкости к циклическим сдвигам может быть выбран модуль спектра Фурье.

Дискретное Преобразование Фурье-Меллина позволяет осуществлять встраивание, стойкое к:

- К циклическому сдвигу
- Изотропному масштабированию
- К повороту

ДПФ

1) $\mathrm{C}(n_1, n_2) \longrightarrow \mathrm{C}_{\text{ДПФ}}(m_1, m_2)$

2) $\left|\mathrm{C}_{\text{ДПФ}}(m_1, m_2)\right| \quad |-|$

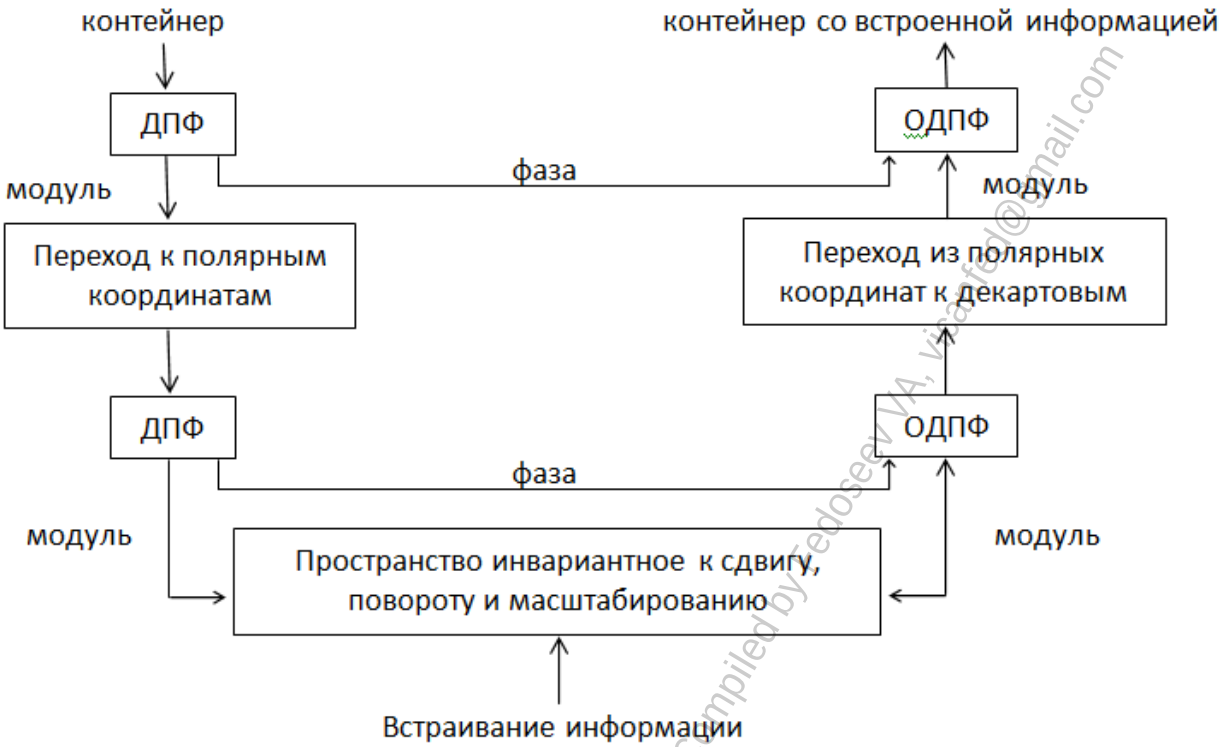
Масштабирование в пространственной области приводит к обратному масштабированию в области спектральной. Поворот в пространственной области приводит к такому же повороту в спектральной области.

Перейдем к полярным координатам в спектральной области:

$$\begin{cases} m_1 = e^{\rho}\cos\theta \\ m_2 = e^{\rho}\sin\theta \end{cases}, \rho \in \mathbb{R}^{+}, \text{угол } \theta \in \mathbb{R} \cap [0, 2\pi].$$

Масштабирование и поворот – это сдвиг в переменных ρ и θ.

ДПФ и оставляем только $|-|$.



3.2 Основные подходы при встраивании и извлечении информации в пространстве признаков

3.2.1 Встраивание информации за счёт переквантования функции яркости. Общая концепция методов QIM. Пример: встраивание информации в наименее значимые биты (НЗБ)

I. Базовый алгоритм QIM

Широко известный метод управляемого переквантования яркости QIM (quantization index modulation, [134, 136, 138]). Метод встраивания QIM может быть кратко описан следующим образом. Пусть даны входное изображение $\mathrm{I}(\mathrm{n},\mathrm{m})$ и бинарное изображение-ЦВЗ $\mathrm{W}(\mathrm{n},\mathrm{m})$, где $\mathrm{n} \in [1,\mathrm{N}]; \mathrm{m} \in [1,\mathrm{M}]$.

Встраивание ЦВЗ производится следующим образом:

$$\mathrm{I}'(\mathrm{n},\mathrm{m}) = \mathrm{Q}(\mathrm{I}(\mathrm{n},\mathrm{m}), \mathrm{W}(\mathrm{n},\mathrm{m}), \mathrm{p}(\mathrm{n},\mathrm{m})), \quad (6.11)$$

где $\mathrm{I}'(\mathrm{n},\mathrm{m})$ - изображение со встроенным ЦВЗ;

$\mathrm{p}(\mathrm{n},\mathrm{m})$ - случайный некоррелированный шумовой сигнал, предназначенный для маскирования (dithering [138]) искажений, возникающих при переквантовании яркости исходного изображения.

Функция $\mathrm{Q}\big(\mathrm{I}(\mathrm{n},\mathrm{m}), \mathrm{W}(\mathrm{n},\mathrm{m}), \mathrm{p}(\mathrm{n},\mathrm{m})\big)$ определяет отображение множества значений яркости пикселей изображения $\mathrm{I}(\mathrm{n},\mathrm{m})$ на множество $\{0, \mathrm{q}, 2\mathrm{q}, 3\mathrm{q}\ldots\}$ при $\mathrm{W}(\mathrm{n},\mathrm{m}) = 0$ и на множество $\left\{\frac{1}{2}\cdot \mathrm{q}, \frac{3}{2}\mathrm{q}, \frac{5}{2}\mathrm{q}, \ldots\right\}$ при $\mathrm{W}(\mathrm{n},\mathrm{m}) = 1$ (где *q* –шаг квантования).

II. Модификация: алгоритм «на основе деления с остатком»

Разработанный алгоритм, будучи основан на схожем методе модификации отсчетов изображения, предполагает встраивание ЦВЗ для целочисленных $\mathrm{I}(\mathrm{n},\mathrm{m})$ и $\mathrm{I}'(\mathrm{n},\mathrm{m})$ по следующему правилу:

$$\mathrm{I}'(\mathrm{n},\mathrm{m}) = \begin{cases} \mathrm{floor}\left(\frac{\mathrm{I}(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right) + \mathrm{mod}\left(\frac{2\cdot\mathrm{I}(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right), & \text{если} \quad \mathrm{W}(\mathrm{m},\mathrm{n}) = 0, \\ \mathrm{floor}\left(\frac{\mathrm{I}(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right) + \frac{\mathrm{q}}{2} + \mathrm{mod}\left(\frac{2\cdot\mathrm{I}(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right), & \text{если} \quad \mathrm{W}(\mathrm{m},\mathrm{n}) = 1, \end{cases} \quad (6.12)$$

где floor – операция округления до меньшего целого;

mod – остаток от деления;

q – шаг квантования, определяющий степень искажения изображения-контейнера.

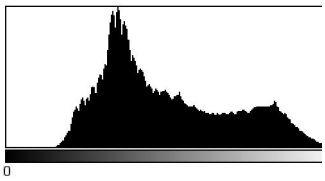
В данном случае для маскирования искажений, возникших при переквантовании, используется компонента исходного сигнала $\mathrm{mod}\left(2 \cdot \mathrm{I}(\mathrm{n},\mathrm{m})/\mathrm{q}\right)$, отбрасываемая при переквантовании. Это позволяет избежать дополнительного зашумления изображения, возникающего при добавлении $\mathrm{p}(\mathrm{n},\mathrm{m})$в методе QIM.

На рисунке 6.20 представлены гистограммы изображения-контейнера до и после встраивания ЦВЗ представленным методом.

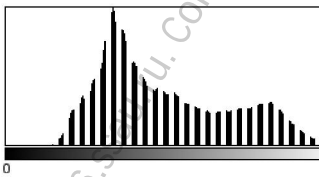
Извлечение ЦВЗ производится следующим образом:

$$\mathrm{W}'(\mathrm{n},\mathrm{m}) = \begin{cases} 0, & \text{если} \quad \mathrm{mod}\left(\frac{\mathrm{I}\prime(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right) < \frac{\mathrm{q}}{2}, \\ 1, & \text{если} \quad \mathrm{mod}\left(\frac{\mathrm{I}\prime(\mathrm{n},\mathrm{m})}{\mathrm{q}}\right) \geq \frac{\mathrm{q}}{2}, \end{cases} \quad (6.13)$$

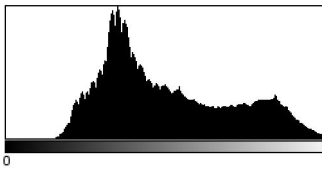
где $\mathrm{W}'(\mathrm{n},\mathrm{m})$ – извлеченный ЦВЗ.



гистограмма до встраивания ЦВЗ



гистограмма после встраивания нулевого ЦВЗ



гист. после встраивания ЦВЗ с равновероятными значениями

III. Поблочная модификация для обеспечения защиты от изменений

Предложенный выше метод встраивания, как и метод QIM, осуществляет встраивание одного пикселя (бита) изображения-ЦВЗ в один пиксель изображения-контейнера, что позволяет максимизировать объем скрытно передаваемой информации (ЦВЗ) но делает метод непригодным для защиты изображений от модификации [131, 132].

Разработанный алгоритм встраивания предполагает встраивание одного бита ЦВЗ в блок пикселей изображения-контейнера и позволяет одновременно со скрытой передачей информации осуществлять защиту изображения-контейнера от модификации.

Пусть *L* – линейный размер блока пикселей изображения-контейнера, в который встраивается пиксель (бит) ЦВЗ $\mathrm{W_b}(\mathrm{u},\mathrm{v})$, где

$u \in \left[1, \text{floor}\left(\frac{N}{L}\right)\right]$, $v \in \left[1, \text{floor}\left(\frac{M}{L}\right)\right]$. Встраивание производится в соответствии с псевдослучайным бинарным изображением-ключом (см. рисунок 6.21) $K(i,j)$, где $i \in [1, L]; j \in [1, L]$.

Пример псевдослучайного ключа K (размер блока $L = 32$)

Тогда

$$I'(n,m) = \begin{cases} \text{floor}\left(\frac{I(n,m)}{q}\right) + \text{mod}\left(\frac{2 \cdot I(n,m)}{q}\right), & \text{если} \quad W'_b(n,m) = 0, \\ \text{floor}\left(\frac{I(n,m)}{q}\right) + \frac{q}{2} + \text{mod}\left(\frac{2 \cdot I(n,m)}{q}\right), & \text{если} \quad W'_b(n,m) = 1, \end{cases}$$

(6.14)

где $W'_b(n,m) = W_b\left(\text{floor}\left(\frac{n}{L}\right), \text{floor}\left(\frac{m}{L}\right)\right) \oplus K\left(\text{mod}\left(\frac{n}{L}\right), \text{mod}\left(\frac{m}{L}\right)\right)$;

$\oplus$ - операция «исключающее ИЛИ».

Кроме того, для уменьшения искажений изображения-контейнера при встраивании (и при извлечении) бита ЦВЗ в блок изображения-контейнера возможна модификация не всех пикселей блока, а только части пикселей, задаваемых ключом. В данном случае псевдослучайный ключ $K(i,j)$ принимает значения из набора $\{-1,0,1\}$, где значение ключа $K(i,j) = -1$ означает, что соответствующий пиксель блока изображения-контейнера не будет модифицирован при встраивании ЦВЗ. Дополнительным параметром при генерации ключа в данном случае является величина $P_{key} \in [0,1)$задающая вероятность появления значения $K(i,j) = -1$ при генерации ключа, и, соответственно, долю неиспользуемых при встраивании пикселей в блоке.

Встраивание ЦВЗ в данном случае производится в соответствии с выражением:

$$I'(n,m) = \begin{cases} \text{floor}\left(\frac{I(n,m)}{q}\right) + \text{mod}\left(\frac{2I(n,m)}{q}\right), & \text{если} \quad W'_b(n,m) = 0 \ \text{и} \ K\left(\text{mod}\left(\frac{n}{L}\right), \text{mod}\left(\frac{m}{L}\right)\right) \geq 0, \\ \text{floor}\left(\frac{I(n,m)}{q}\right) + \frac{q}{2} + \text{mod}\left(\frac{2I(n,m)}{q}\right), & \text{если} \quad W'_b(n,m) = 1 \ \text{и} \ K\left(\text{mod}\left(\frac{n}{L}\right), \text{mod}\left(\frac{m}{L}\right)\right) \geq 0, \\ I(n,m), & \text{если} \quad K\left(\text{mod}\left(\frac{n}{L}\right), \text{mod}\left(\frac{m}{L}\right)\right) < 0. \end{cases}$$

(6.15)

3.2.2 Встраивание информации в наименее значимые биты

Встраивание информации

Встраивание информации в наименее значимые биты (НЗБ) контейнера является одним из первых стеганографических методов. Существует достаточно большое количество его модификаций, однако мы остановимся на простейшем базовом варианте.

Контейнер представляет собой полутоновое изображение $C \in (\mathbb{B}^8)^2_{[N_1 \times N_2]}$, а внутренняя информация, подлежащая встраиванию имеет вид $\mathbf{b} \in \mathbb{B}^1_{[N_b]}$, причём $N_b \leq N_1 \times N_2$. *При встраивании внутренняя информация преобразуется в форму изображения следующим образом:*

$$W(n_1, n_2) = \begin{cases} b_{n_1 N_2 + n_2}, & n_1 N_2 + n_2 \leq N_b, \\ 0, & \text{иначе.} \end{cases} \qquad (1.57)$$

Яркость пикселя контейнера с координатами (n_1, n_2) можно записать в двоичном представлении следующим образом:

$$C(n_1, n_2) = C_0(n_1, n_2) + C_1(n_1, n_2) \cdot 2 + \ldots + C_7(n_1, n_2) \cdot 2^7,$$

где $\forall k = 0..7,\ \forall (n_1, n_2)\ \ C_k(n_1, n_2) \in [0,1]$. Матрицы C_k называют битовыми плоскостями.

Наименее и наиболее значащими битовыми плоскостями являются соответственно C_0 и C_7: если изменить значение бита $C_1(n_1, n_2)$, то яркость изменится на единицу; если же изменить значение бита $C_8(n_1, n_2)$, то яркость изменится на 128. Это означает, что наименее значимую битовую плоскость можно модифицировать с целью встраивания скрытого сообщения или ЦВЗ.

Пространством признаков в данном методе является собственно множество $(\mathbb{B}^8)^2_{[N_1 \times N_2]}$. Битовые плоскости носителя информации C^W формируются в соответствии со следующей формулой:

$$C_k^W(n_1, n_2) = \begin{cases} W(n_1, n_2), & k = 0, \\ C_k(n_1, n_2), & k > 0. \end{cases} \qquad (1.58)$$

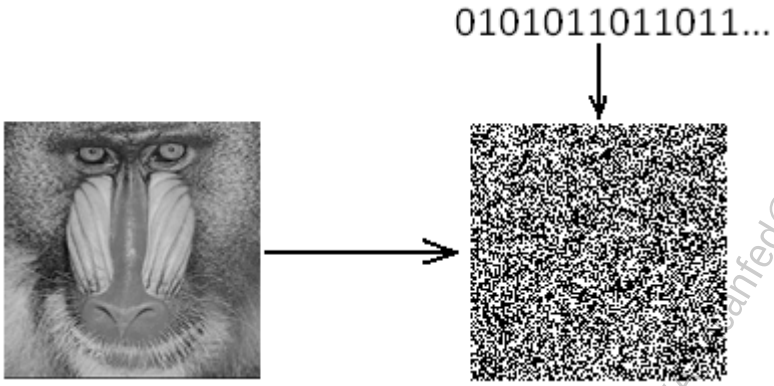


Рисунок 1.6 – Иллюстрация принципа встраивания информации в НЗБ контейнера

На рисунке 1.6 проиллюстрирован принцип встраивания информации в рассматриваемой системе.

Извлечение информации

Извлечение информации происходит путём чтения данных наименее значимой битовой плоскости изображения со встроенной информацией:

$$b_n^R = W^R\left(\left[\frac{n}{N_2}\right],\left\{\frac{n}{N_2}\right\}\right) = \widetilde{C_0^W}\left(\left[\frac{n}{N_2}\right],\left\{\frac{n}{N_2}\right\}\right), \qquad (1.59)$$

где $\left[\frac{n}{N_2}\right]$ и $\left\{\frac{n}{N_2}\right\}$ означают целую и дробную части от деления n на N_2 соответственно. Предполагается, что знание истинной длины вектора внутренней информации N_b не является существенным, и дополнение внутренней информации нулями до длины $N_1 \times N_2$ *является допустимым.*

В качестве функции обнаружения встроенной информации $\mathcal{R}$ для данного метода допустимо использовать функции (1.34) и (1.38).

3.2.3 Аддитивное и мультипликативное встраивание. Алгоритм PatchWork

Случайным образом выбирается подмножество S, даже делится на два равных подмножества S_1 и S_2 согласно ключу k.

$$\begin{cases} C^W(n_1,n_2) = C(n_1,n_2) + d, & C(n_1,n_2) \in S_1 \\ C^W(n_1,n_2) = C(n_1,n_2) \cdot d, & C(n_1,n_2) \in S_2 \end{cases}$$

$$\frac{2}{\|S\|}\left(\sum_{C(n_1,n_2)\in S_1} C^W(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C^W(n_1,n_2)\right)$$

$$= \frac{2}{\|S\|}\left(\|S_1\|\cdot d + \|S_2\|\cdot d + \left[\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2)\right]\right)$$

$$= 2d + \underbrace{\frac{2}{\|S\|}\left[\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2)\right]}$$

Близко к 0 при большом ||S||, при предположении что отсчеты изображения имеют одинаковое распределение.

Поэтому детектор – это сравнение этой величины с порогом.

Выбор порога:

$0 -$ среднее значение$(\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2))$

$2d -$ среднее значение $(\sum_{C(n_1,n_2)\in S_1} C(n_1,n_2) - \sum_{C(n_1,n_2)\in S_2} C(n_1,n_2))$

Порог d

Замечание 1: Существует улучшение алгоритма Patchwork, в котором встраивание происходит блоками. В зависимости от предполагаемого использования блоки могут быть большего или меньшего размера или разной формы.

3.2.4 Концепция встраивания информации с расширением спектра. Алгоритм Cox. Неслепой детектор при аддитивном или мультипликативном встраивании информации

Встраивание информации

Данный алгоритм был предложен И. Коксом в работе [74] для защиты изображений цифровыми водяными знаками, встраиваемыми в области дискретного косинусного преобразования (ДКП) [183, 22, 31]. В ряде источников [45, 151] он упоминается под названием «алгоритм Кокса». Достоинством алгоритма является то, что благодаря выбору наиболее значимых коэффициентов ДКП водяной знак является стойким к сжатию, поэлементным преобразованиям, процедурам обработки скользящим окном, а также многим другим видам обработки изображений. К недостаткам данного

алгоритма стоит отнести трудоёмкость операции вычисления двумерного ДКП всего изображения.

Длина встраиваемой информации N_b строго не задана, но она должна кодироваться матрицей признаков $\Omega \in \mathbb{R}^1_{[1000]}$:

$$\Omega = \mathcal{P}_f(\boldsymbol{b}, \boldsymbol{k}). \quad (1.60)$$

Элементы Ω представляют собой псевдослучайные числа, распределенные по гауссовскому закону.

Для модификации отбираются 1000 самых больших коэффициентов глобального дискретного косинусного преобразования (ДКП) контейнера

$$C_{DCT}(m_1, m_2) = \sum_{n_1=0}^{N_1} \sum_{n_2=0}^{N_2} C(n_1, n_2)\, cos\left(\frac{\pi m_1}{N_1}\left(n_1 + \frac{1}{2}\right)\right) cos\left(\frac{\pi m_2}{N_2}\left(n_2 + \frac{1}{2}\right)\right) \quad (1.61)$$

в змеевидной развёртке, как показано на рисунке 1.7 (при этом DC-отсчёт $C_{DCT}(0,0)$ не включается). Результатом данного отбора является матрица признаков контейнера $f \in \mathbb{R}^1_{[N]}$. Не будем конкретизировать точную формулу расчёта f, поскольку она окажется весьма громоздкой.

Встраивание информации в пространстве признаков осуществляется по формуле по формуле

$$f^W(n) = f(n)\big(1 + \alpha \cdot \Omega(n)\big), \quad (1.62)$$

где $\alpha > 0$ – постоянный множитель, характеризующий глобальную степень изменения контейнера.

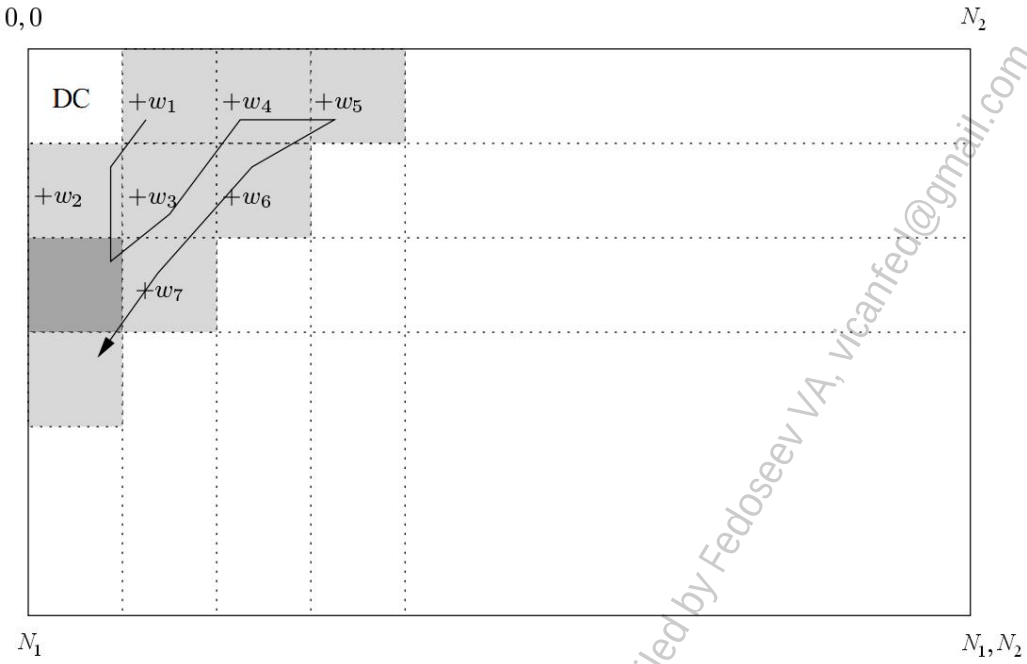


Рисунок 1.7 – Схема встраивания ЦВЗ алгоритмом Кокса

Извлечение информации

Извлечение матрицы признаков встроенной информации осуществляется по формуле

$$\tilde{\Omega}(n) = \frac{\widetilde{f^W}(n) - f(n)}{\alpha \cdot f(n)}. \qquad (1.63)$$

Извлечение информации заключается в обнаружении наличия встроенной матрицы признаков Ω и осуществляется по формуле (1.34) с функцией близости вида

$$\rho(\Omega, \tilde{\Omega}) = \frac{\sum_{n=0}^{N-1} \Omega(n)\tilde{\Omega}(n)}{\sqrt{\sum_{n=0}^{N-1} \Omega^2(n)} \cdot \sqrt{\sum_{n=0}^{N-1} \tilde{\Omega}^2(n)}}. \qquad (1.64)$$

3.2.5 Алгоритм Barni. Слепой детектор при аддитивном или мультипликативном встраивании информации

Проблема: не слепой детектор.

Зачем нужно исходное изображение в методе Кокса:

1) Чтобы отыскать N_w наибольших ДКП-коэффициентов
2) Чтобы вычислить оценку $\widetilde{\Omega}$

Изменения:

1) Вместо наибольших ДКП-коэффициентов встраивание осуществляется всегда в одни и те же компоненты (средне-частотные)
2) Правило встраивания
3) $\overrightarrow{f_{c^w}} = \vec{f}(1 + \alpha W) \Longrightarrow \overrightarrow{f_{c_0^w}} = \vec{f} + \alpha \cdot W \cdot |\vec{f}|$
4) Исходные компоненты не известны детектору и рассматриваются как изменяемые. Незнание их компенсируется большим количеством изменяемых коэффициентов.

Пример: 512x512. Изменяемые ДКП-коэффициенты на диагоналях с 180-й по 250-ю – около 16000. Порядок выбора коэффициентов по зигзагу (не принципиально)

$$C^w(n_1, n_2) = C^w(n_1, n_2) \cdot B(n_1, n_2) + C(n_1, n_2) \cdot \big(1 - B(n_1, n_2)\big)$$

$$B(n_1, n_2) = \frac{MSE_{c,9x9}(n_1, n_2)}{\max\limits_{i.j} MSE_{c,9x9}(i, j)}$$

Таким образом, для текстурированных областей $B \to 1$,

Для однородных $B \to 0$.

$$\delta_1 = \sum_{i=0}^{N_W - 1} \overrightarrow{f_{c_R^w}}(i) \cdot W(i) > Th = 3.3 \cdot \sqrt[2]{\frac{2\sigma_f^2}{N_W}}$$

Рабочие параметры $\alpha = 0.55,\ N_W = 16000$

- JPEG вплоть до 5%
- Размытие
- Медианная фильтрация
- Гаусс-изменения
- Контрастирование
- Эквализация гисторгаммы

$$f^W\big(\varphi(m)\big) = f\big(\varphi(m)\big) + \alpha \cdot W(m) \cdot \big|f\big(\varphi(m)\big)\big|$$

Длина $|\varphi(m)| = |W| = M$.

$$\xi\big(\widetilde{f^W}, W\big) = \frac{1}{p} \sum_{m=0}^{M-1} W(m) \cdot \widetilde{f^W}\big(\varphi(m)\big)$$

Методы статистического анализа для выбора порога корреляции детектора

Гипотеза 0 { Гипотиза А: изображение не содержит ЦВЗ
Гипотиза В: изображение содержит ЦВЗ, отличный от W

Гипотеза 1 {Гипотеза С: изображение содержит ЦВЗ

Метод: вычисление ξ и сравнение с $\mathbb{T}_\xi$

Вопрос: как найти $\mathbb{T}_\xi$

Вероятность ошибки: $p_e = p(1) \cdot p(0|1) + p(0) \cdot p(1|0)$

$p(0|1)$ – вероятность пропуска ЦВЗ (false negative)

$p(1|0)$ – вероятность ложного обнаружения ЦВЗ (false positive)

$p(0), p(1)$ – априорные вероятности Гипотезы 0 и Гипотезы 1.

Если полагать $p(0) = p(1)$

$$p_e = \frac{1}{2}\left[p\left(\xi < \mathbb{T}_\xi|1\right) + p\left(\xi > \mathbb{T}_\xi|0\right)\right]$$

По ЦПТ ξ – нормально распределена. Пусть $\alpha^2 \ll 1$. Можно показать, что

$m_{\xi|0} = 0\ m_{\xi|1} = \alpha - m_{|f|}$

$\sigma^2{}_{\xi|0} = (1+\alpha^2)\frac{\sigma^2{}_f}{M}$ $\sigma^2{}_{\xi|1} = (1+2\alpha^2)\frac{\sigma^2{}_f}{M} + \alpha^2\frac{\sigma^2{}_{|f|}}{M}$

Где $m_{|f|} = \frac{1}{M}\sum_{m=0}^{M-1} E\{|f(\varphi(m))|\}$

среднее значение m_{f_i} по всему множеству изменяемых коэффициентов.

$$\sigma^2{}_f = \frac{1}{M}\sum_{m=0}^{M-1} E\{|f^2(\varphi(m))|\}$$

среднее значение $\sigma^2{}_{f_i}$ по всему множеству изменяемых коэффициентов.

При $\alpha^2 \ll 1$ $\sigma^2{}_{\xi|0} \approx \sigma^2{}_{\xi|1} \approx \frac{\sigma^2{}_f}{M} \triangleq \sigma^2$

Если $p_e \to min$, то $p(1|0) + p(0|1) \to min$.

Если $\alpha \ll 1$, то $p(0|1) = p(1|0)$,

следовательно граница равна середине между $m_{\xi|0}$ и $m_{\xi|1}$: $\mathbb{T}_\xi = \frac{\alpha}{2} m_{|f|}$

Замечания:

1) В практических приложениях полагают, что $m_{|f|} = \frac{1}{M}\sum_{m=0}^{M-1}\left|\widetilde{f^W}(\varphi(m))\right|$ – гипотеза эргодичности
2) Как правило C^W при передаче через канал подвергается воздействиям и преднамеренным атакам. Это влияет на среднее и дисперсию $\xi(\widetilde{f^W}, W)$. Практически было получено, что при этом среднее ${\sigma^2}_{\xi|0}$, $m_{\xi|0}$, $m_{\xi|1}$не меняются, а возрастет ${\sigma^2}_{\xi|1}$. Поэтому порог сдвигать ближе к нулю и используется $\mathbb{T}_\xi = \frac{\alpha}{3} m_{|f|}$.
3) Если существуют атаки, то еще и серьезно возрастет $p(0|1)$ относительно $p(1|0)$. Это происходит оттого, что при этом еще и $m_{\xi|1} < \alpha \cdot m_{|f|} \Longrightarrow \quad p(1|0) = fix = 10^{-6}\ p(0|1) \to min$

$$p\left(\xi > \mathbb{T}_\xi \middle| 0\right) = \frac{1}{2}\Phi\left(\frac{\mathbb{T}_\xi}{\sqrt{2{\sigma^2}_\xi}}\right) = 10^{-6} \Longrightarrow \frac{\mathbb{T}_\xi}{\sqrt{2{\sigma^2}_\xi}} \geq 3.3$$

$$\mathbb{T}_\xi = 3.3\sqrt{2{\sigma^2}_\xi} = 3.3\sqrt{\frac{2\cdot(1+\alpha^2)\cdot{\sigma^2}_f}{M}} \approx 3.3\sqrt{\frac{2\cdot{\sigma^2}_{\widetilde{f^W}}}{M}}$$

3.2.6 Концепция информированного встраивания. Алгоритм Koch. Алгоритм Benham

$C^W(n_1, n_2) = C(n_1, n_2) + \alpha \cdot H(n_1, n_2) \cdot W(n_1, n_2)$, где $H(n_1, n_2)$ – адаптация (величина на которую изменяется исходный контраст).

Свойства информационного встраивания:

1.
2. Сначала определяется детектор и под него подстраивается метод

<u>Алгоритм Zhao & Koch информационного встраивания</u>

Последовательность:

Контейнер разбарается на блоки

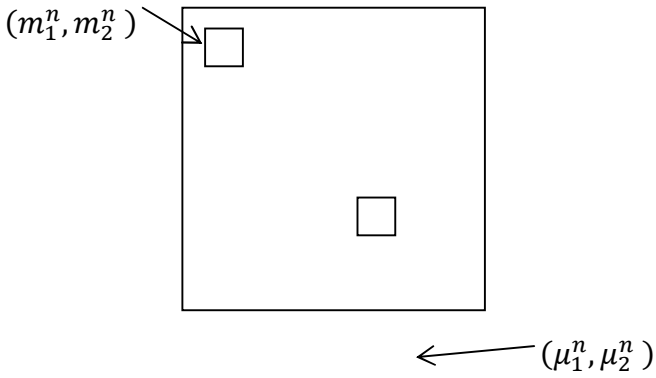
От каждого блока берется косинусное преобразование

$W(n)$ – водяной знак p

k – ключ, для любого $n = 0..p-1$: $k = \left\{(m_1^n, m_2^n)_{n=0}^{p-1}\right\}$ $0 \leq m_1^n, m_2^n \leq 7$

Рассматривается по каждому из блоков, в каждый блок встраивается один бит информации

Блок № n



$f^n(m_1^n, m_2^n)$

$f^n(\mu_1^n, \mu_2^n)$

$$W(n) = \begin{cases} 1 \Longrightarrow |f^n(m_1^n, m_2^n)| - |f^n(\mu_1^n, \mu_2^n)| < -\varepsilon \\ 0 \Longrightarrow |f^n(m_1^n, m_2^n)| - |f^n(\mu_1^n, \mu_2^n)| > \varepsilon \end{cases}$$

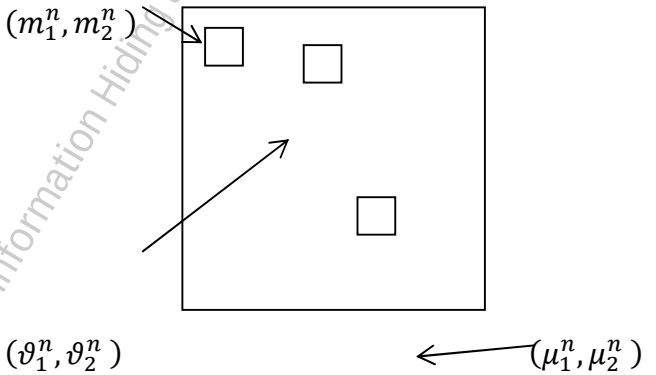
После встраивания:

$$W(n) = \begin{cases} 1, & (\widetilde{F^n})^W(m_1^n, m_2^n) < (\widetilde{f^n})^W(\mu_1^n, \mu_2^n) \\ 0, & \text{иначе} \end{cases}$$

Сначала определяется условие детектора, из этого условия следует условие встраивания водяного знака

Алгоритм Benham

Не везде производится встраивание



Встраивание производится по трем параметрам

$W(n)$	$f^n(m_1^n, m_2^n)$	$f^n(\mu_1^n, \mu_2^n)$	$f^n(\vartheta_1^n, \vartheta_2^n)$
1	H M M	M H M	L L L
0	M L L	L M L	H H H
Нет Ув 3	H L M	L H M	M M M

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

КУРС ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

«КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ»

Раздел 4: Примеры систем встраивания информации в цифровые сигналы

Самара 2013

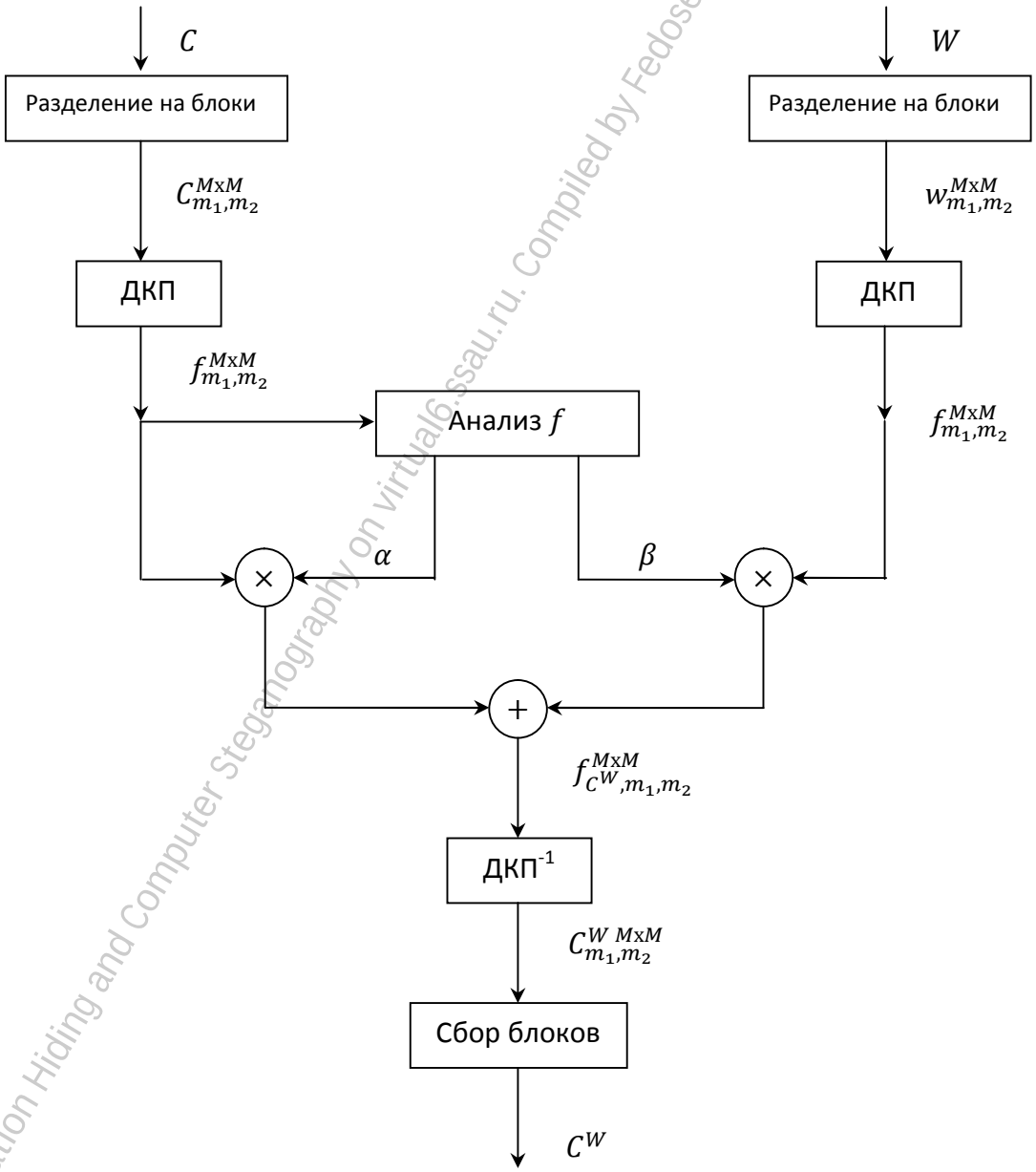
Оглавление

4 Примеры систем встраивания информации в цифровые сигналы

4.1 СВИ в полноцветные изображения

4.1.1 Видимые ЦВЗ

Алгоритм видимого ЦВЗ (Kankanhalli)

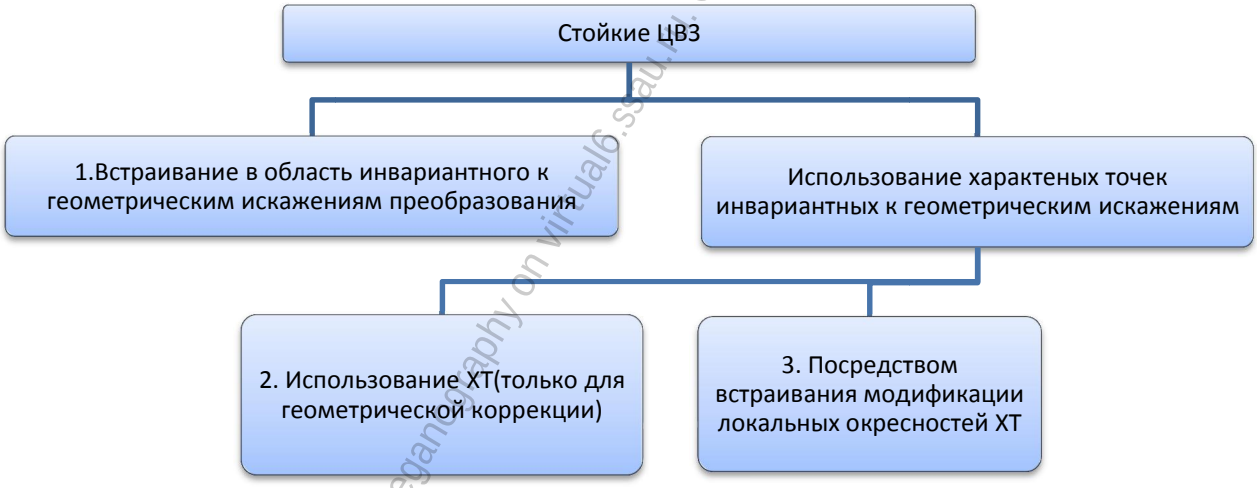


Замечание. Если C – многокомпонентное, то прежде формируется компонента яркости, и встраивание осуществляется в нее.

4.1.2 Стойкие ЦВЗ

Как правило, существенное ухудшение качества извлечения ЦВЗ происходит после гауссовского размытия и геометрических преобразований. Первое сопровождается существенной деградацией изображения, в то время как второе может практически не нарушать основные пропорции изображения, но вызывать потерю встроенного сигнала. Поэтому достижение стойкости к геометрическим преобразованиям – важнейшая задача при проектировании стойких ЦВЗ.

Как правило, ограничиваются обеспечением стойкости к RST, но многие алгоритмы стойки и к аффинным преобразования.



1) Zhend&Zhao (Оттава)

Метод основан на преобразовании в лог-полярные координаты (Преобразование Фурье-Меллина)

$$ДПФ \rightarrow |\cdot| \rightarrow лог-полярные \rightarrow 1ПФ \rightarrow |\cdot|$$

Метод встраивания ЦВЗ – копия алгоритма Сех или Barni.

Пример k – определяет позиции для встраивания,

W – последовательность.

Слепой или неслепой детектор.

$$f^w(\omega_\rho, \omega_\varphi) = f(\omega_\rho, \omega_\varphi) + \alpha(\omega_\rho, \omega_\varphi) \cdot W(\omega_\rho, \omega_\varphi)$$

Неслепой детектор.

$*$) удвоение последовательности для встраивания в амплитудный спектр

$x \geq 0 => (x, 0);\ x < 0 => (0, x)$

$**$) $f^w = \alpha \cdot W$ – но это уж слишком.

2) Подход с использованием ХТ
   - Точки Харриса
   - Точки Харриса-Лапласа

     $XT =$ координаты точки $+$ ее локальный дескритор
   - $SURT$
   - $SIFT$

     $SIFT \rightarrow Lowe -$ Защищены патентом

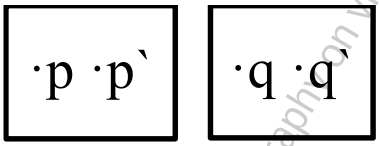
     Gaussian Difference of Gaussian (DoG)

     $SIFT$:

     1) Поиск пиков DoG – последовательности
     2) Отбор пиков
     3) Определить ориентации локального дескритора с использованием локальных градиента изображения

     $SIFT -$ в пространстве $LL2$

     Как установить соответствие между точками?



$q' = C_p$

$p' = C^{-1}{}_q$

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$q' = C_p$

$d(p, p') = d\left(p, C^{-1}{}_q\right) = \left\|p - C^{-1}{}_q\right\|$

$d(q, q') = d\left(q, C_p\right) = \left\|q - C_p\right\|$

$\|\cdot\| -$ Евклидово расстояние

$(i^*, j^*) = drgD = drg\ \min_{i,j} \sum_{i,j} [d^2(p_i, p_i') + d^2(q_i, q_i')]\ \ D <? T -$ порога

МНК

$$\begin{pmatrix} x \\ \bar{y} \\ 1 \end{pmatrix} = \mathrm{C}^{-1}\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{d}{bd-ae} & \frac{a}{ae-bd} & \frac{af-dc}{bd-ae} \\ \frac{e}{ae-bd} & \frac{b}{bd-ae} & \frac{fb-ce}{de-bd} \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix}$$

ВИ(встраивание изображения): $r \in \{0,1,2,3\}$

$$s \in \{LL, LH, HL, HH\}$$

$$(f^{r,s})^W = \begin{cases} f^{r,s}(1+\alpha\cdot\beta\cdot W), r=2, S \neq LL \\ f^{r,s}, \text{в остальных случаях} \end{cases}$$

$\alpha = Const -$ масштабирующий множитель

$\beta -$ функция контраста(из HVS) адаптированная к вейвлет-области

$W -$ изображение

Извлечение: Коррелятор W и $f^{r,s} -$ похоже на Барни

Ищутся Deng

Точки Харриса-Лапласа, их дескрипторы, сопоставляются при этом исключаются точки с накладывающимися друг на друга локальными областями дескрипторов.

Эллиптические регионы нормируются до кругов своего собственного радиуса R.

Определим основное направление эллипса θ и поворот окружности на этот угол.

$W -$ двоичная последовательность с нулевым средним: $W(n) \in \{-1,1\}$

Отображается в окружность, направленную по секторам разного радиуса

$\beta(x,y) = \frac{1}{1+\frac{D\cdot\sigma^2(x,y)}{\sigma^2 max}}$, D –весовой множитель, $\sigma^2 -$ локальная СКО в точку (x,y).

Аддитивное добавление W во все нормированные регионы

$$\alpha_1\big(\beta(x,y)\big)C(x,y) + \alpha_2\big(1-\beta(x,y)\big)W(x,y)$$

Извлечение: те же шаги → Винеровский фильтр → W^* к корреляции (W, W^*).

Порог выбирается аналогичным Барни способом.

4.2 СВИ в бинарные изображения

4.2.1 Полутоновые и бинарные изображения. Методы растрирования изображений. Метод диффузии ошибки. Два подхода к встраиванию информации в бинарные изображения.

Бинарными называются изображения, в которых используется 1 бит для хранения интенсивности каждого пикселя в каждом из каналов. При этом, как правило, под бинарными понимаются одноканальные изображения.

Рис. 1. Пример полутонового изображения

и полученного из него растрированного бинарного изображения

Принято выделять в бинарных изображениях три типа областей: светлая, тёмная и граничная (серая). Светлая область содержит преимущественно белые пиксели, тёмная – преимущественно чёрные, граничная – и те и другие в приблизительно равных пропорциях. Дополнительная информация, внедряемая в изображение за счёт модификации его пикселей, наименее заметна в граничной области. Таким образом, в большинстве методов информация внедряется исключительно в граничные области.

Бинарные изображения чаще всего являются результатом цифрового растрирования полутоновых изображений. В широком смысле *цифровое растрирование* – это технология создания иллюзии непрерывного тона с помощью бинарного устройства вывода. Пользуясь терминологией, используемой в цифровой обработке изображений, можно сказать, что цифровое растрирование – это квантование полутоновых изображений до глубины 1 бит/пиксель. Пример растрированного изображения приведён на рисунке 1.

Метод растрирования изображений с диффузией ошибки

Пусть C – полутоновое изображение размером $N_1 \times N_2$, яркость пикселей которого $C(n_1, n_2)$ принимает целые значения на отрезке $[0{,}255]$. Из него необходимо получить бинарное изображение C^B того же размера. Будем для простоты считать, что яркость пикселей $C^B(n_1, n_2)$ принимает значения 0 или 255 (такие изображения мы будем называть псевдобинарными).

В алгоритме диффузии ошибки (Error Diffusion) используется весовая функция h размерами $M_1 \times M_2$, называемая также *ядром* алгоритма. Как правило, размеры ядра невелики: $1 \le M_1, M_2 \le 5$. Ядро задаёт направления распространения (диффузии) ошибки бинаризации и доли ошибки, передаваемые в каждом из направлений.

Приведём примеры весовых функций, зарекомендовавших себя на практике:

- Ядро 1 (Floyd)

$$\frac{1}{16}\begin{pmatrix} 0 & \odot & 7 \\ 3 & 5 & 1 \end{pmatrix};$$

- Ядро 2 (Jarvis)

$$\frac{1}{48}\begin{pmatrix} 0 & 0 & \odot & 7 & 5 \\ 3 & 5 & 7 & 5 & 3 \\ 1 & 3 & 5 & 3 & 1 \end{pmatrix};$$

- Ядро 3 (Stucki)

$$\frac{1}{42}\begin{pmatrix} 0 & 0 & \odot & 8 & 4 \\ 2 & 4 & 8 & 4 & 2 \\ 1 & 2 & 4 & 2 & 1 \end{pmatrix};$$

- Ядро 4 (Fan)

$$\frac{1}{16}\begin{pmatrix} 0 & 0 & \odot & 7 \\ 1 & 3 & 5 & 0 \end{pmatrix};$$

- Ядро 5 (3-digit)

$$\frac{1}{16}\begin{pmatrix} 0 & \odot & 8 \\ 2 & 6 & 0 \end{pmatrix};$$

Символом $\odot$ отмечен пиксель с координатами $(0,0)$. Значение $h(0,0) = 0$.

На практике используются две математически эквивалентных модели диффузии ошибки: подтягивание ошибок бинаризации из уже пройденных отсчётов (*pull-модель*) и распространение ошибки из текущего отсчёта в последующие (*push-модель*). Обе модели будут рассмотрены ниже.

Алгоритм диффузии ошибки (pull-модель)

Обозначим за D_h множество точек (n_1, n_2), в которых $h(n_1, n_2) \neq 0$. Тогда pull-модель алгоритма растрирования с диффузией ошибки выглядит следующим образом:

$$u(n_1, n_2) = C(n_1, n_2) - \sum_{(m_1, m_2) \in D_h} h\,(m_1, m_2) e(n_1 - m_1, n_2 - m_2),$$

$$C^B(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \ge T \\ 0, & u(n_1, n_2) < T \end{cases}$$

$$e(n_1, n_2) = C^B(n_1, n_2) - u(n_1, n_2)$$

В формулах (6)-(8) $u(n_1, n_2)$ и $e(n_1, n_2)$ – это вспомогательные изображения размерами $N_1 \times N_2$. Первое характеризует корректируемый в зависимости от ошибки бинаризации контейнер, второе – ошибку бинаризации в очередной точке. *T* – пороговое значение, как правило, равное 128. Также алгоритм растрирования (6)-(8) показан в виде схемы на рис. 2.

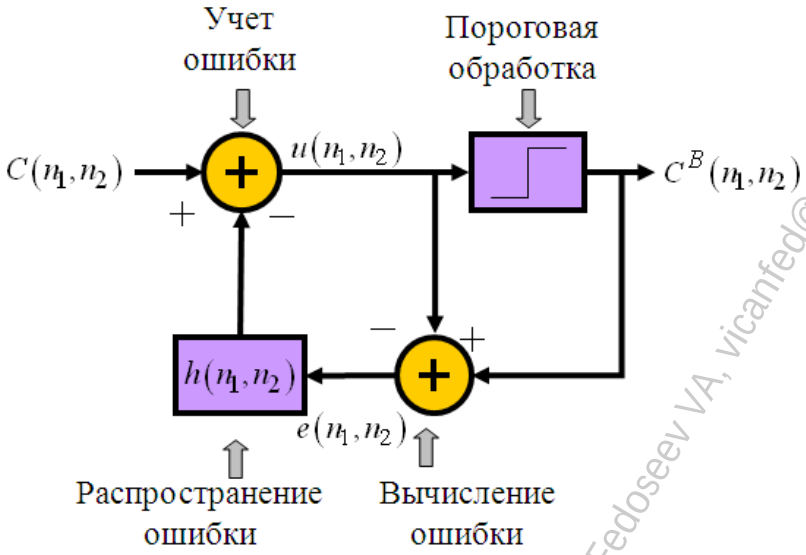


Рис. 2. Схема метода диффузии ошибки

Алгоритм диффузии ошибки (push-модель)

Пусть, аналогично, D_h – множество точек (n_1, n_2), в которых $h(n_1, n_2) \neq 0$. Тогда push-модель алгоритма растрирования с диффузией ошибки выглядит следующим образом:

$$u(n_1, n_2) = C(n_1, n_2) \;\; \forall (n_1, n_2): \; n_1 = \overline{0..N_1 - 1}, \;\; n_2 = \overline{0..N_2 - 1}$$

$$C^B(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \geq T \\ 0, & u(n_1, n_2) < T \end{cases} \quad (1$$

$$e = C^B(n_1, n_2) - u(n_1, n_2) \quad (1$$

$$\forall (m_1, m_2) \in D_h \;\; \rightarrow \;\; u(n_1 + m_1, n_2 + m_2) -= e \cdot h(m_1, m_2) \quad (1$$

Как и в pull-модели, $u(n_1, n_2)$ – вспомогательное изображение размерами $N_1 \times N_2$. Поле ошибок уже хранить не обязательно, поскольку на каждом шаге алгоритма ошибка бинаризации сразу рассеивается по изображению u.

4.2.2 Непосредственное встраивание информации в бинарный контейнер. Группа методов DHST

В данной группе методов в качестве контейнера используется бинарное изображение, полученное из полутонового на предварительном этапе. Также предполагается, что полутоновой источник не известен на этапе встраивания информации и, следовательно, не может оказать влияние на этот процесс.

Алгоритм DHST (Data Hiding Self-Toggling)

В данной схеме встраиваемая информация представляет собой бинарный вектор. Каждый бит секретной информации внедряется в бит контейнера путём непосредственной замены. Ключ, создаваемый при помощи генератора случайных чисел, определяет позицию для внедрения. Один бит информации внедряется в один бит контейнера. Для восстановления информации используется тот же самый ключ. В данном методе высока степень визуальных искажений.

<u>Алгоритм DHSPT (Data Hiding by Smart Pair-Toggling)</u>

В данной схеме встраиваемая информация также представляет собой бинарный вектор, и каждый бит секретной информации внедряется также непосредственно в бит контейнера. Ключ, создаваемый при помощи генератора случайных чисел, определяет позицию для внедрения.

Процедура встраивания происходит следующим образом. Бит информации присваивается биту контейнера, позиция которого выбирается согласно ключу. Если при этом значение бита пикселя контейнера не изменилось, то никакие дополнительные действия не осуществляются. В противном случае из окрестности 3×3 вокруг позиции, выданной генератором,– (m, n) выбирается пиксель со значением яркости, равным яркости измененного пикселя (m, n), и его значение инвертируется для компенсации изменения в пикселе (m, n). Данная процедура называется “pair toggling” и является простейшим способом коррекции искажений, вносимых при встраивании ЦВЗ. Если в окрестности 3×3 отсутствуют пиксели со значением яркости, равной яркости измененного пикселя (m, n), компенсация искажений не производится.

Рассмотрим более подробно процедуру выбора компенсирующего пикселя. Простейшим способом является случайный выбор пикселя с нужным значением яркости в окрестности 3×3. Существует также и более разумный подход. Для каждого пикселя окрестности точки (m, n) рассчитывается его вес, и инвертированию подвергается пиксель с наибольшим весом.

Расчёт веса пикселя (p, q) из окрестности пикселя (m, n) осуществляется также в окне 3×3. Обозначим пиксели окна как $x_1, x_2, \dots x_9$, причем x_5 - центральный пиксель с координатами (p, q). Тогда вес пикселя $V(p, q)$ рассчитывается следующим образом:

$$V(p,q) = \sum_{i=1}^{9} w(i) f(x_5, x_i),$$

$$f(x,y) = \begin{cases} 1 & x \neq y, \\ 0 & x = y; \end{cases}$$

$$w(i) = \begin{cases} 1, & i = 1,3,7,9; \\ 2, & i = 2,4,6,8; \\ 0, & i = 5. \end{cases}$$

Наибольший вес пикселя (p, q) означает, что почти все пиксели его окрестности имеют тот же цвет, что и (m, n). Поэтому если инвертированию подвергается пиксель с наибольшим весом, то это влечёт наименьшие визуальные искажения.

4.2.3 Встраивание информации при растрировании полутоновых изображений. Алгоритм DHCED

В методе, описанном ниже, контейнер представляет собой полутоновое изображение, но передаваться по каналу связи он будет в бинарном виде. Поэтому встраивание информации может происходить до процедуры растрирования или вместе с ней.

В данной схеме встраиваемая информация представляет собой бинарное изображение $W(n_1, n_2)$, размеры которого $N_1 \times N_2$ равны размерам полутонового контейнера $C(n_1, n_2)$. При встраивании ЦВЗ создаются два бинарных изображения C^B и

C^W – результата растрирования $C(n_1, n_2)$ таким образом, чтобы в как можно большем числе точек выполнялось равенство

$$W(n_1, n_2) = C^B(n_1, n_2) \oplus C^W(n_1, n_2), \quad (1$$

Для этого изображение C^B создаётся при помощи алгоритма диффузии ошибки, рассмотренного в разделе 1. Изображение C^W создаётся при помощи модифицированного алгоритма диффузии ошибки, в котором на втором этапе вместо (7) или (10) используется следующее соотношение*:

$$C^W(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \geq T_1 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 255 \\ 0, & u(n_1, n_2) < T_1 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 255 \\ 255, & u(n_1, n_2) \geq T_2 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 0 \\ 0, & u(n_1, n_2) < T_2 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 0 \end{cases}, \quad (1$$

$$T_1 < T < T_2.$$

Как правило, используются значения $T_1 = 64, T_2 = 192$.

Для извлечения информации используется формула (13).

* В формулах (8) и (11), очевидно, вместо C^B также используется C^W.

4.3 СВИ в звуковые сигналы

4.3.1 Встраивание информации в НЗБ звуковых сигналов. Алгоритм Cvejic

Встраивание в НЗБ

Звук представляет собой 16-ю битами на отсчет.

Несжатый звук имеет частоту 44100 Гц.

Имеет место встраивание информации во временной области в наименее значимые биты. Аналогично, НЗБ, допустимые для встраивания (модификации) являются 1,2,3,4 (примерно).

1 бит обеспечивает передачу 44100 бит/с – много. Для некоторых музыкальных стилей возможно увеличение до 4 или 5 бит.

Алгоритм встраивания в НЗБ (Cvejic)

Цель:

- Увеличить пропускную способность с 3 до 4 битовых плоскостей (или отрезков).
- 3-шаговый подход
    1) Стандартное встраивание в 4 НЗБ непосредственной заменой бит, далее выполняются дополнительная обработка сигнала с целью снизить искажения.
    Пусть мы встроили k бит ($k < 16$), тогда $\varepsilon_{max} \leq 2^k - 1$. Существует 2^{16-k} уровней, чьи последние k бит идентичны встроенным. Так вот, тот уровень k, который наиболее похож на исходный, и выбирается.
    Пусть $a(n)$ – исходный уровень
    $s(n)$ – уровень, полученный при прямом встраивании
    $s'(n)$ – уровень, полученный путем замены $(k+1)$-го бита
    $e(n) = |a(n) - s(n)|, e'(n) = |a(n) - s'(n)|$
    Если $e(n) \leq e'(n) \rightarrow s(n)$ выбирается
    $e(n) > e'(n) \rightarrow s'(n)$ выбирается
    2) Замена бита с минимизацией ошибки.
    $\varepsilon_{max} = 2^k - 1, \varepsilon'_{max} = 2^{k-1}$
    3) Error Diffusion

$$a(n+1) \coloneqq a(n+1) + \frac{e(n)}{2}$$

$$a(n+2) \coloneqq a(n+2) + \frac{1}{4}e(n)$$

$$a(n+3) \coloneqq a(n+3) + \frac{1}{8}e(n)$$

$$a(n+4) \coloneqq a(n+4) + \frac{1}{8}e(n)$$

4.3.2 СВИ путём модификациии фазы сигнала. Алгоритм Bender-1

Основная идея метода фазового кодирования состоит в замене фазы исходного сегмента на опорную фазу, характер изменения которой отражает собой данные, которые необходимо скрыть. Для того чтобы сохранить раз-ностную фазу между сегментами, фазы последних соответствующим образом согласовываются.

Фазовое кодирование, когда оно может быть использовано, является одним из наиболее эффективных методов по критерию отношения сиг-нал/воспринимаемый шум. Существенное изменение соотношения фаз меж-ду каждыми частотными составляющими приводит к значительному рассе-иванию фазы. Тем не менее, до тех пор. пока модификация фазы в достаточ-ной мере мала, может быть достигнуто скрытие, неощутимое на слух. Разу-меется, модификация считается малой по отношению к конкретному наблю-дателю, поскольку специалисты по спектральному анализу способны обна-ружить те изменения, которые непрофессионалу могут показаться незначительными.

Процедура фазового кодирования заключается в следующем^

Пусть $c(n), 0 \le n \le N-1$

1) Сигнал разбивается на k коротких сегментов

   $c_k(n), \quad k = 0..K-1$

   $n = 0..N/K-1$

2) К -ому сегменту применяется ДПФ (N/K-точечные)

   Выделяется фаза -$\varphi_k(m)$ и амплитуда $A_k(m), m = 0..N/K-1, k = 0..K-1$

3) Запоминается разность фаз между соседними сегментами

   $k = 0..K-2$

   $\Delta\varphi_k(m) = \varphi_{k+1}(m) - \varphi_k(m).$

1) Бинарный вектор, подлежащий встраиванию, представляется в виде ступенчатой функции в частотной области.

   $\varphi_0' = \varphi_0$

   Ступеньки в $\frac{\pi}{2}$ или $-\frac{\pi}{2}$

   $\varphi_0'(m) = W(m) \quad \forall m = 0..N/K\text{-}1$

2) $\varphi_1'(m) = \varphi_0'(m) + \Delta\varphi_0(m)$

…

$\varphi_k'(m) = \varphi_{k-1}'(m) + \Delta\varphi_k(m)$

…

$\varphi_{K-1}'(m) = \varphi_{K-2}'(m) + \Delta\varphi_{K-1}(m)$

3) Собираем исходную амплитуду и новую фазу и делаем обратное ДПФ

Извлечение. Для него нужны:

- Синхронизация сигнала
- Длина сегмента N/K

- Низкая пропускная способность – 8-32 бит/с.

4.3.3 СВИ с расширением спектра

Метод встраивания с расширением спектра является примером корреляционного метода, где встраиваемая информация представляет собой псевдослучайную последовательность (ПСП), а извлекаемая информация рассчитывается посредством вычисления корреляции между аудиосигналом со встроенным стего и ПСП [6].

Основная идея метода состоит в том, что ПСП распределяется по исходному аудио контейнеру. ПСП, представляющая собой широкополосный шум, может быть внедрена как во временной области, так и в области преобразования не зависимо от вида преобразования. Обычно используют дискретное косинусное преобразование (ДКП), дискретное преобразование Фурье (ДПФ) и дискретное вейвлет преобразование (ДВП). Однако здесь рассмотрим алгоритм во временной области.

Имеется бинарная последовательность $v = \{0,1\}$ или эквивалентная ей биполярная $b = \{-1, 1\}$. Так же имеется ПСП $r(n)$ длины *N*, сгенерированная при помощи секретного ключа. Модулированная последовательность $w(n) = vr(n)$ распределяется по исходному сигналу $s(n)$ в соответствии с масштабным множителем α, который необходим для задания оптимального отношения между устойчивостью заполненного контейнера к искажениям и скрытностью ЦВЗ в этом контейнере. Таким образом, заполненный контейнер имеет вид (1.1):

$$x(n) = s(n) + avr(n). \quad (1.1)$$

Схема обнаружения ЦВЗ использует линейный коррелятор, т.к. ПСП известна получателю по секретному ключу и может быть воспроизведена. Следовательно, наличие ЦВЗ можно определить корреляцией между $x(n)$ и $r(n)$ следующим образом:

$$c = \frac{1}{N}\sum_{i=1}^{N} x(i)r(i). \quad (1.2)$$

Сумму (1.2) можно представить в виде сумм двух компонентов:

$$c = \frac{1}{N}\sum_{i=1}^{N} s(i)r(i) + \frac{1}{N}\sum_{i=1}^{N} avr^2(i). \quad (1.3)$$

Предполагаем, что первый компонент равен нулю, если ПСП и исходный сигнал взаимнонезависимы. Однако часто существует небольшое отличие от нуля. Для того, что бы учесть эту разницу заполненный контейнер подвергают фильтрации. Существуют различные способы реализации этой фильтрации. Наиболее часто встречающимися являются: высокочастотная фильтрация, кодирование с линейным предсказанием и фильтрация белым шумом. На рисунке 1.1 представлена типичная схема предварительной обработки $x(n)$. Посредством фильтрации, второй компонент суммы (1.3) становится определяющим фактором для принятия решения о наличии ЦВЗ.

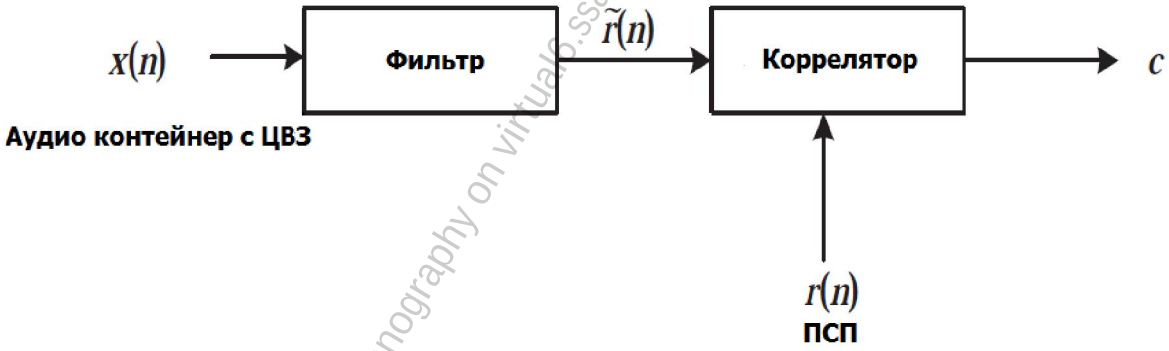


Рисунок 1.1 – Типичная схема предварительной обработки заполненного контейнера

Теоретически был найден порог τ, при помощи которого детектор m указывает на наличие ЦВЗ c, значения которого находятся в интервале от нуля до единицы:

$$m = \begin{cases} 1, \text{если } c > \tau; \\ 0, \text{если } c \leq \tau. \end{cases}$$

Как показывают опыты [3, 6], для того чтобы определить нахождение ЦВЗ в контейнере величина порога τ должна составлять 0,7. В зависимости от того, насколько высока требуемая достоверность определения ЦВЗ, необходимо варьировать значения порога.

Основным достоинством описанного метода является возможность передачи небольших объемов информации при высоком уровне устойчивости к искажениям. По проведенным исследованиям [6], метод позволят сокрыть 4 бита в секунду. Недостатком метода считается добавление некоррелированного белого шума в аудиосигнал в результате встраивания, что может повлиять на восприятие аудио сигнала [7].

РСПП использует двоичную фазовую манипуляцию, поскольку фаза сигнала псевдослучайной последовательности поочередно чередуется с фа-зой модулированной двоичной последовательности сообщения (рисунок 2.4).

На стадии извлечения фазовые значения φ_0 и $\varphi_0 + \pi$ интерпретируются, соответственно, как биты "1" и "0", которыми кодировалась двоичная после-довательность данных. При этом предусматривается следующее:

Псевдослучайный ключ представляет собой М-последовательность (то есть он имеет максимально возможное количество комбинаций, которые равномерно распределены в заданном диапазоне, и максимально долго не повторяются). Следовательно, он имеет относительно плоский частотный спектр.

Принимающей стороне известен поток ключей для шифрования. Выполнена синхронизация сигнала, а также известны точки начала и конца расширенных данных.

Принимающей стороне также известны следующие параметры: час-тота следования элементарных посылок, скорость передачи данных и частота (вид) несущей.

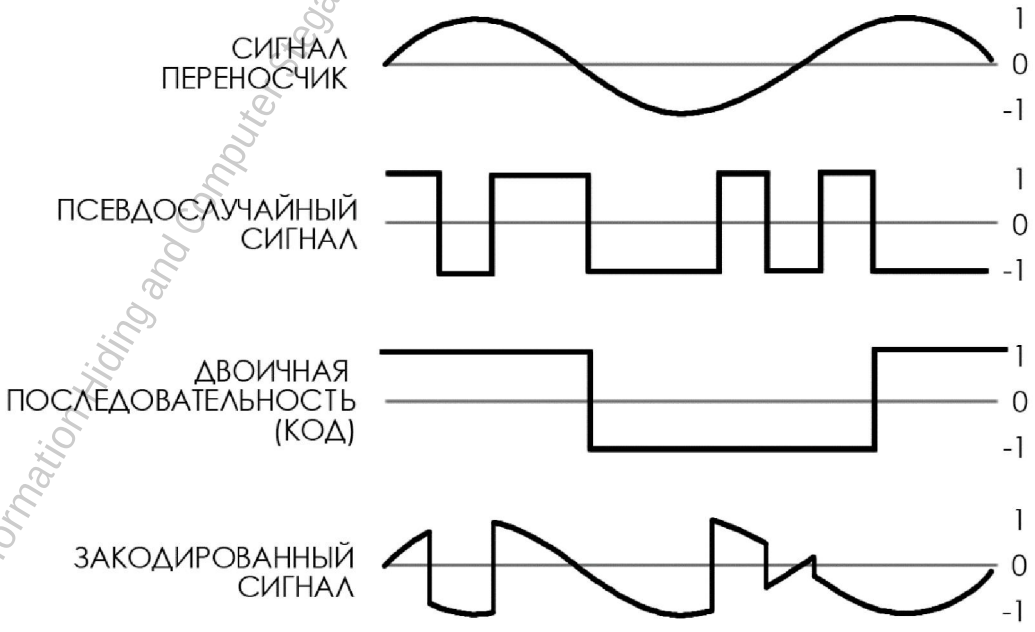


Рисунок 2.4 – Информация, синтезированная расширением спектра и шифрованная методом прямой последовательности

В отличие от рассмотренного выше фазового кодирования, рассмотрен-ный метод РСПП вводит в звук аддитивный случайный шум. Для того чтобы держать уровень шума низким и неощутимым на слух, расширенный код ос-лабляется (без адаптации) приблизительно до уровня 0,5% от динамического диапазона звукового файла-контейнера [8].

Объединение несложной техники повторения и кодирования с исправ-лением ошибок позволяет гарантировать целостность двоичной последова-тельности. Короткие сегменты двоичной кодовой комбинации объединяются и складываются с сигналом аудиоконтейнера таким образом, чтобы умень-шить шумы переходных процессов. Деля этого в процессе декодирования проводится усреднение по всему сегменту. Во время исследований метода РСПП, авторами работы [9] была получена скорость передачи данных около четырех бит в секунду.

4.3.4 СВИ за счёт встраивания эхо-сигнала. Алгоритм Bender-2

Данный метод заключатся во встраивании секретной информации в аудио контейнер путем добавления эхо-сигналов. Идея метода состоит в том, что при малом сдвиге одного сигнала относительно другого, человек воспринимает два сигнала как один, а эхо воспринимается как дополнительный резонанс. Величина сдвига зависит от многих факторов, как, например, от параметров исходного сигнала или чувствительности слуха получателя. Исследования показывают [6], что в общем случае величина сдвига, при которой два сигнала сливаются в один, составляет 0,001 секунды.

Впервые этот метод был описан В. Бендером, Н. Моримото и др. [6]. Коротко рассмотрим основные этапы сокрытия информации. Параметрами кодирования являются две величины: время задержки нуля δ_0 и время задержки единицы δ_1, показанные на рисунке 1.2. Каждое из них не превосходит порога в 0,001 секунды. Вдобавок к этому, необходимо установить коэффициент затухания эхо-сигналов α так, чтобы внедряемое сообщение было невозможно распознать на слух.

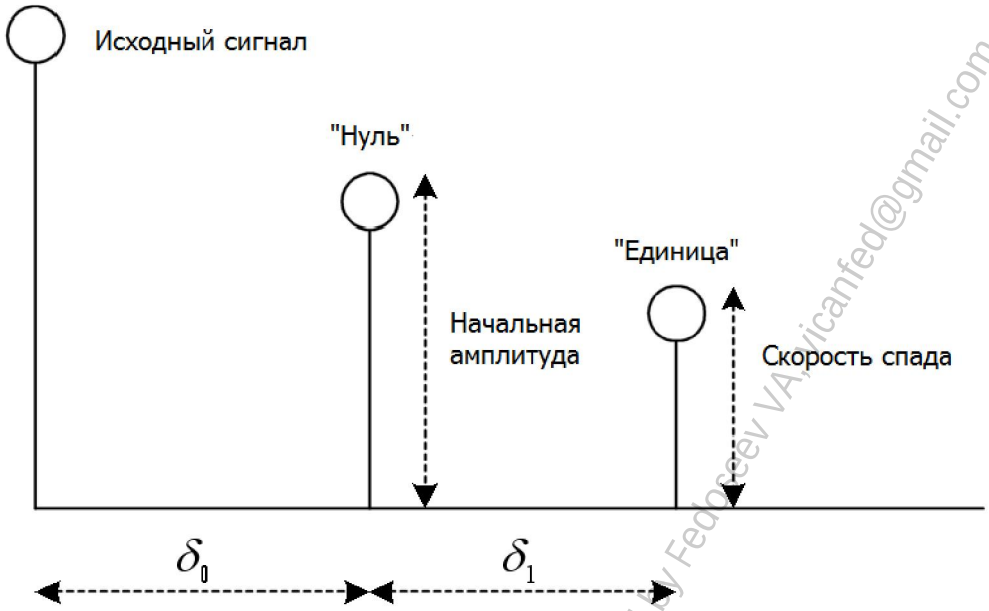


Рисунок 1.2 – Параметры кодирования эхо-сигнала

Для повышения эффективности кодирования исходный сигнал разделяется на сегменты, которые в дальнейшем будут рассматриваться как отдельные сигналы, в каждый из которых можно будет внедрить по одному биту информации. В итоге полученная совокупность будет представлять собой заполненный аудио контейнер. В целях достижения как можно меньшей заметности внедрения информации проводятся некоторые дополнительные вычисления. Для последовательности, разделяемой на сегменты, сначала генерируются два эхо-сигнала: первый содержит только нули, а второй только единицы. На рисунке 1.3 черной кривой представлен исходный сигнал, а цветными кривыми – эхо-сигналы.

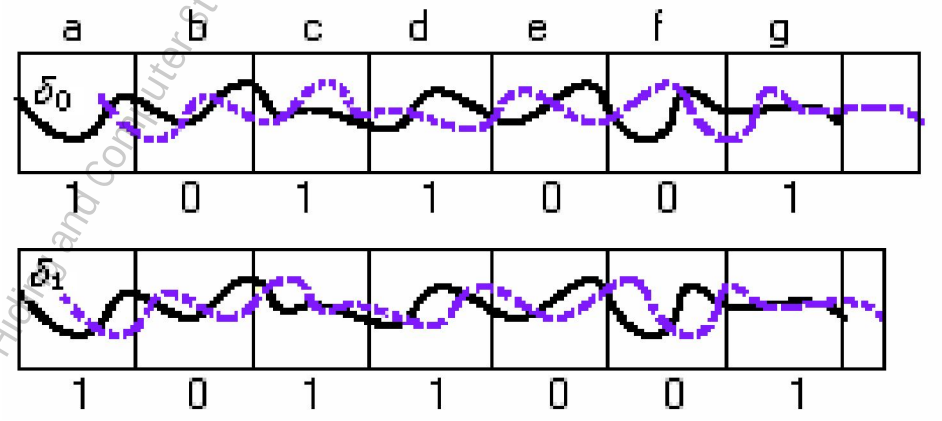


Рисунок 1.3 – Нулевой и единичный эхо-сигналы

Далее создаются еще два дополнительных сигнала, необходимые для внедрения в каждый участок конкретного значения последовательности секретной информации. Эти

сигналы, называемые переключающими или смешивающими сигналами, представлены на рисунке 1.4.

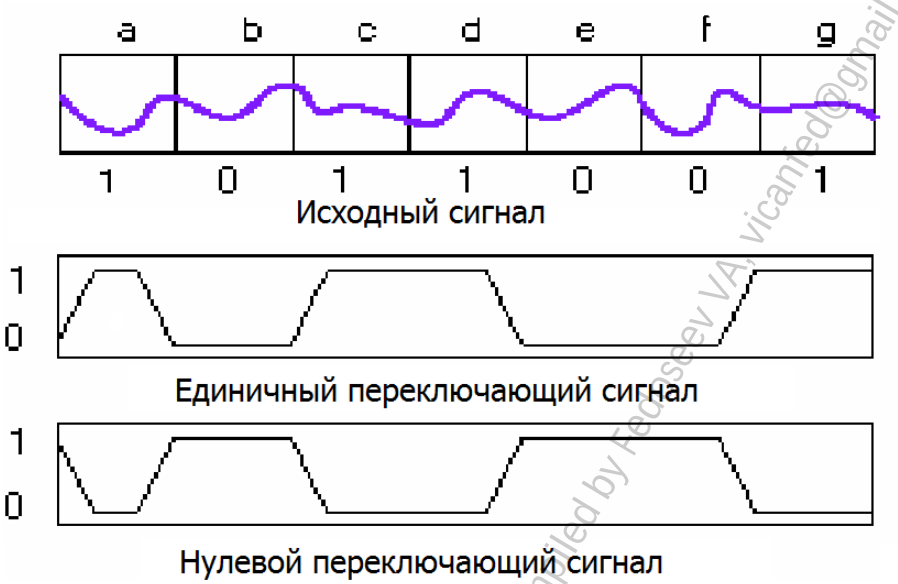


Рисунок 1.4 – Исходный сигнал и переключающие сигналы

Затем идет непосредственно процедура встраивания бинарной последовательности в исходный сигнал. В зависимости от того, какой элемент бинарной последовательности нужно внедрить в каждый сегмент контейнера, эхо-сигнал, советующий встраиваемому нулю, умножается на нулевой переключающий сигнал, а эхо-сигнал, советующий встраиваемой единице – на единичный переключающий сигнал. Благодаря тому, что сумма переключающих сигналов всегда равна единице, осуществляется плавный переход между сегментами, в которых встраиваются различные биты. Для каждого сегмента сумма исходных значений контейнера и преобразованных эхо-сигналов, умноженных на коэффициент затухания, и будет представлять собой заполненный аудио контейнер. На рисунке 1.5 представлен кодер для данного метода.

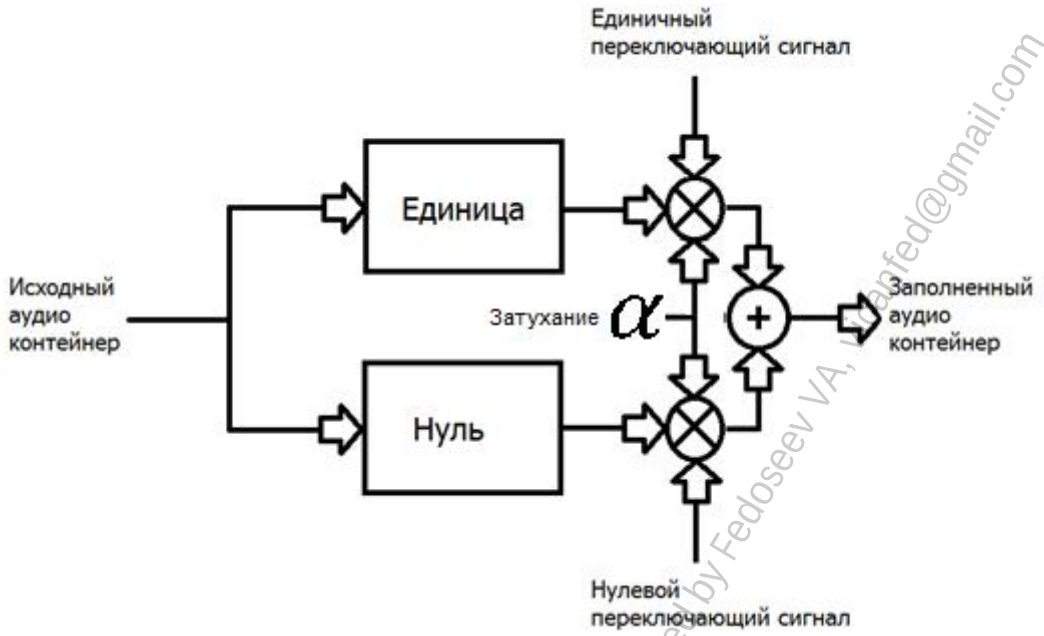


Рисунок 1.5 – Процесс встраивания эхо-сигналов

Процесс расшифровки секретного сообщения строится главным образом на поиске тех параметров сдвига, которые были использованы при кодировании. Рассмотрим алгоритм обратного преобразования, использующий автокорреляционную функцию кепстра сигнала или автокепстр [4].

1. Исходный сигнал $S(t)$ разбивается на непересекающиеся сегменты $S_i(t)$, длительностью d отсчетов каждый, соответственно тому, как это делалось при встраивании.
2. На каждом сегменте вычисляется кепстр сигнала

$$C_i(t) = F^{-1}\{\ln_{complex}(|F(s_i)|^2)\},$$

где F – это дискретное преобразование Фурье (ДПФ);

F^{-1}, соответственно, обратное ДПФ.

3. На каждом сегменте вычисляется функция автокепстра

$$E_i(t) = \sum_{j=0}^{d-t} C_i(j)\, C_i(j+t).$$

В дальнейшем необходимы значения автокепстра соответствующие сдвигу на δ_0 и δ_1. Обозначим их соответственно через $E_{i,0}$ и $E_{i,1}$.

4. Сравниваем эти значения и если $E_{i,0}$ больше $E_{i,1}$, то принимаем решение о том, что был встроен бит соответствующий нулю, иначе – единице.

Если говорить о достоинствах метода кодирования эхо-сигналов, то нельзя не упомянуть то, что алгоритм встраивания скрытной информации является стойким к различным искажениям аудио контейнера, и, при этом, не значительно влияет на содержимое файла, не позволяя распознать факт сокрытия ССЧ. Кроме того, в большинстве случаев дополнительный резонанс в виде эхо-сигнала делает звук слегка более насыщенным [10]. Недостатками этого метода можно считать низкую пропускную способность канала: около 16 бит в секунду, а также достаточно высокую сложность вычисления автокепстра при извлечении секретного сообщения.

4.3.5 Метод маскирования

Еще одним методом, учитывающим особенности системы слуха человека, является метод маскирования сигнала. Известно, что в общем случае, при синхронном воспроизведении двух сигналов, отличающихся по уровню громкости, более громкий сигнал подавляет тихий сигнал. В зависимости от разности в уровнях даже слышимый слабый сигнал может стать неразличимым на фоне более громкого – сигнала маскирования. В этом и состоит основная суть данного метода.

Различают маскирование по частоте и маскирование по времени. Частотное маскирование происходит, когда в ограниченной частотной области одновременно имеется слабый сигнал, к примеру, чистое тональное колебание и более мощный сигнал – узкополосный шум. Возникает так называемый порог маскирования, ниже которого слабый сигнал не слышим. Этот порог зависит от характеристик как маскируемого, так и маскирующего сигналов. Например, порог маскирования для сигнала с уровнем 70 дБ и частотой в 1 кГц может быть достаточно высок. Как показано на рисунке 1.6, он начинается уже от 60 дБ.

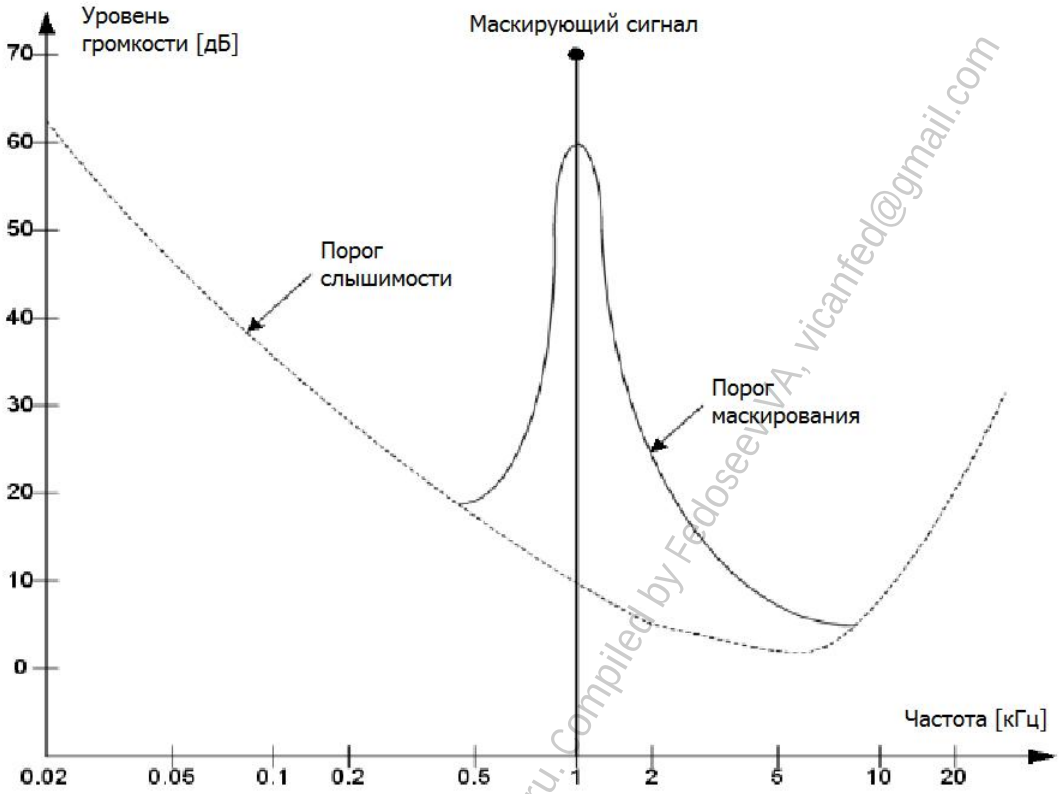


Рисунок 1.6 – Частотное маскирование

Частотное маскирование может быть использовано для сокрытия данных, содержащих информацию об авторских правах. Ниже рассмотрен алгоритм, скрывающий информацию о владельце в аудио контейнере. Алгоритм состоит из 4 этапов [11].

1. Вычисление спектра. Сигнал разделяется на 512 сегментов, каждый из которых взвешивается окном Хэмминга и переводится в частотную область при помощи быстрого преобразования Фурье (БПФ). Компоненты полученного спектра нормализуются по пиковым значениям амплитуды.

2. Определения тональных составляющих. Необходимо различить тональные (синусоидальные) и атональные (шумовые) составляющие, так как они маскируются не одинаково. Тональные составляющие представляют собой локальные максимумы спектра, необходимые для дальнейшей процедуры. Их количество зависит от параметров сигнала и вычисляется в каждом их сегментов. Атональные составляющие – это сумма амплитуд в каждой критической полосе частот, не включая тональных значений.

3. Фильтрация маскируемых компонентов. При помощи прореживающего фильтра отбрасываются компоненты сигнала ниже порога слышимости или те, которые отстоят друг от друга меньше чем на половину критической полосы частот. Этот процесс снижает сложность вычислительную сложность и повышает точность алгоритма.

4. Вычисление порога маскирования. Каждому из компонентов соответствует своя огибающая маскирования. Принимая во внимание показатели всех огибающих, а также порог слышимости, задается общий порог маскирования, ниже которого сигнал не будет распознан системой слуха человека.

Для обнаружения информации используется функция корреляции. При значениях порога равных 0,7 можно утверждать о наличии скрытой информации об авторстве. Для того чтобы извлечь эту информацию необходим секретный ключ автора, который является одним из элементов при создании ПСП, встраиваемой этим методом.

Временное маскирование так же играет важную роль в восприятии звука ССЧ. Считается, что человек не способен различить более слабый сигнал за 5 – 20 мс до включения сигнала маскирования. Этот эффект называется предмаскировкой. Также существует эффект постмаскировки, при котором в течение еще 50 – 200 мс после отключения сигнала маскирования менее слабый сигнал невозможно услышать. Эффекты временного маскирования проиллюстрированы на рисунке 1.7.

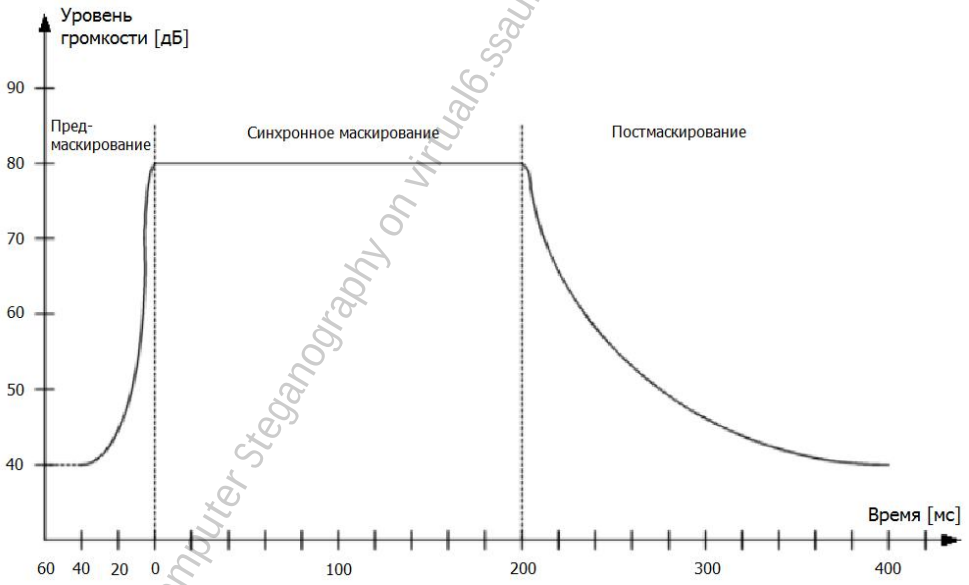


Рисунок 1.7 – Временное маскирование

К достоинствам метода маскирования стоит отнести высокую стойкость к искажениям, таким как добавление аддитивного шума, сжатие с потерями, аналогово-цифровым и цифро-аналоговым преобразованиям, что определяет применение этого метода в защите авторских прав. Для эффективной защиты необходимо относительно небольшое количество внедряемой информации, так что недостатками данного метода являются в основном проблемы вычислительной сложности.

4.4 СВИ в видеосигналы

4.4.1 Алгоритм Hartung для передачи информации в видеосигналах

Встраивание информации

Данная система предложена Ф. Хартунгом и Б. Жиро́ в работе [101] и предназначена для защиты видео цифровыми водяными знаками. Иногда эта система упоминается под названием «алгоритм Хартунга». Внутренняя информация представляется в форме $\mathbf{b} \in \mathbb{B}^1_{[N_b]}$ и встраивается в видеосигнал $C \in \mathbb{Z}^3_{[N_1 \times N_2 \times M]}$ в соответствии с одномерной покадровой построчно-столбцовой развёрткой

$$\varphi(n): n \mapsto (n_1, n_2, m),$$

где $n = \overline{0, N-1}$, $N = N_1 N_2 M$, $n_1 = \overline{0, N_1 - 1}$, $n_1 = \overline{0, N_2 - 1}$, $m = \overline{0, M-1}$, $N_1 \times N_2$ – *размеры кадра, а* M – количество кадров видеопоследовательности. Таким образом, матрицей признаков является $f \in \mathbb{Z}^1_{[N]}$:

$$f(n) = C\big(\varphi(n)\big). \qquad (1.65)$$

Кодирование внутренней информации осуществляется сразу в пространстве признаков: вектор $\Omega \in \mathbb{Z}^1_{[N]}$ формируется из вектора $\mathbf{b}$ следующим образом:

$$\Omega(n) = (-1)^{b_i} \text{ для } i \cdot L \le n < (i+1) \cdot L, \qquad (1.66)$$

где $L \in \mathbb{N}$ – параметр, характеризующий избыточность встраивания, $i = 0..N_b - 1$, а $n = 0..\min(N_b \cdot L, N) - 1$. Если $N_b \cdot L < N$, то в оставшуюся часть сигнала встраивание не производится.

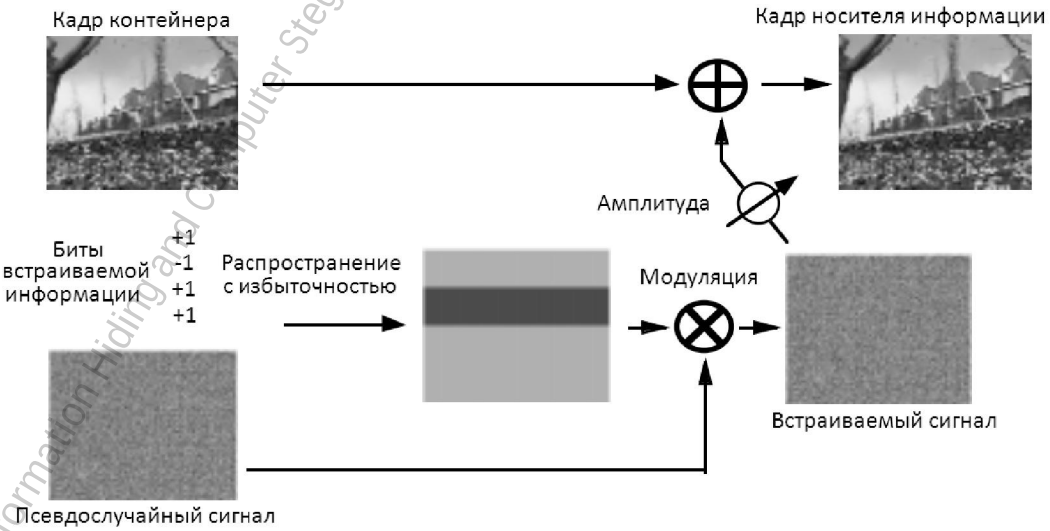


Рисунок 1.8 – Принцип встраивания информации в алгоритме Хартунга

Собственно встраивание информации в контейнер C осуществляется по формуле

$$f^W(n) = f(n) + \alpha \cdot \lambda(n) \cdot \Omega(n) \cdot (-1)^{k_n}, \qquad (1.67)$$

где k_n – n-й бит ключа встраивания $\mathbf{k} \in \mathbb{B}^1_{[N_b]}$, являющегося псевдослучайной двоичной последовательностью* длины N_b, $\alpha > 0$ – постоянный множитель при встраиваемом сигнале, а $\lambda(n) > 0$ – множитель при встраиваемом сигнале, адаптивный к локальным особенностям контейнера и меняющийся слабо, настолько, что можно принять, что

$$\forall i \in [0, N_b - 1] \quad \lambda(n) \approx \lambda(m) \approx \overline{\lambda_i}, \text{если } i \cdot L \le n, m < (i+1) \cdot L,$$

где

$$\overline{\lambda_i} = \frac{1}{L} \sum_{n=i \cdot L}^{(i+1) \cdot L - 1} \lambda(n).$$

На рисунке 1.8 изображена схема, иллюстрирующая принцип встраивания информации в рассматриваемой системе.

Извлечение информации

При извлечении встроенной информации используется слепой метод, не предполагающий знания исходного контейнера. Результатом его является отыскание $\mathbf{b}^{\mathbf{R}} \in \mathbb{B}^1_{[N_b]}$. Оценка матрицы признаков извлечённой информации осуществляется по формуле

$$\widetilde{\Omega}(n) = (-1)^{k_n} \cdot h^W(n), \qquad (1.68)$$

где h^W – вспомогательная величина, которая подбирается таким образом, чтобы было справедливо приближённое равенство

$$h^W(n) \approx f^W(n) - f(n). \qquad (1.69)$$

Поскольку на стадии извлечения информации не известен истинный сигнал-контейнер, то вместо его матрицы признаков $f(n)$ используется оценка $f^W_{mean,s}(n)$ – усреднённая в скользящем окне длиной $s \ge 3$ матрица признаков $f^W(n)$. Таким образом, h^W вычисляется по формуле

$$h^W(n) = f^W(n) - f^W_{mean,s}(n). \qquad (1.70)$$

Значение очередного бита b_i^R определяется на основе анализа величины

* Поскольку ключ должен быть единым для встраивания последовательностей произвольной длины, то предполагается, что истинная длина ключа может быть сколь угодно большой, но используются только его первые N_b бит.

$$\beta_i = \mathcal{P}_f^{-1}(\widetilde{\Omega}) = \sum_{n=i\cdot L}^{(i+1)\cdot L-1} \widetilde{\Omega}(n). \qquad (1.71)$$

Из (1.71), (1.68) и (1.69) получаем, что

$$\beta_i \approx \sum_{n=i\cdot L}^{(i+1)\cdot L-1} \alpha \cdot \lambda(n) \cdot \Omega(n) \cdot (-1)^{2k_n} = \qquad (1.72)$$

$$= \alpha \cdot L\overline{\lambda_\iota} \cdot L \cdot (-1)^{b_i} L = \alpha L^3 \overline{\lambda_\iota} \cdot (-1)^{b_i}.$$

Поскольку $\alpha L^3 \overline{\lambda_\iota}$ – величина положительная, то справедливо простое правило извлечения встроенной информации:

$$b_i^R = \begin{cases} 0, & \beta_i > 0 \\ 1, & \beta_i < 0 \end{cases}. \qquad (1.73)$$

Функция обнаружения встроенной информации $\mathcal{R}$ в оригинальной работе [101] не описана, однако допустимо использовать функцию вида (1.34) и (1.38).

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

КУРС ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

«КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ»

Раздел 5: Атаки на системы встраивания информации

Самара 2013

Оглавление

5 Атаки на системы встраивания информации

5.1.1 Непреднамеренные искажения и преднамеренные атаки. Виды стойкости ЦВЗ. Искажения, по отношению к которым оценивается стойкость ЦВЗ-систем. Влияние ЦАП-АЦП на заполненный контейнер

В данном подразделе описаны виды искажений носителя информации, которые требуется применять в данной лабораторной работе. Эти искажения сопровождаются параметром, характеризующим степень их влияния на сигнал.

1. *Линейное изменение динамического диапазона функции яркости* заключается в линейном поэлементном преобразовании изображения:

$$\widetilde{C^W}(n_1, n_2) = min\{\alpha C^W(n_1, n_2), 255\}, \quad \alpha \in \mathbb{R}, \alpha > 0.$$

   Параметром является коэффициент α при значении функции яркости.

2. При *повороте с последующим восстановлением* происходят два последовательных поворота изображения: на некоторый угол φ и на обратный ему угол $-\varphi$.

   Параметром является угол поворота φ.

3. При *масштабировании с последующим восстановлением* происходит последовательное изменение размера изображения и его возвращение в исходный размер.

   Параметром является коэффициент масштабирования.

4. Под *усреднением* в скользящем окне будем понимать обработку изображения $\mathrm{C^W}$ ЛИС-системой, имеющей конечную импульсную характеристику $g(m_1, m_2)$, имеющую размеры $M \times M$, где $M = 2p + 1, p \in \mathbb{N}$:

$$\widetilde{C^W}(n_1, n_2) = \sum_{m_1=0}^{M-1} \sum_{m_2=0}^{M-1} g(m_1, m_2) \cdot C^W(n_1 - m_1, n_2 - m_2), \tag{1}$$

   причём отсчёты ИХ постоянны и равны $1/M^2$. Например, для $M = 3$

$$g(m_1, m_2) = \frac{1}{9}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

   Параметром является размер окна M.

5. *Гауссовское размытие* заключается в обработке изображения ЛИС-системой с бесконечной импульсной характеристикой $\mathrm{g(m_1, m_2)}$:

$$\widetilde{C^W}(n_1, n_2) = \sum_{m_1=-\infty}^{\infty} \sum_{m_2=-\infty}^{\infty} g(m_1, m_2) \cdot C^W(n_1 - m_1, n_2 - m_2), \tag{1'}$$

   имеющей вид функции Гаусса:

$$g(m_1, m_2) = \frac{1}{2\pi\sigma^2} exp\left\{-\frac{m_1^2 + m_2^2}{2\sigma^2}\right\}, \qquad m_1, m_2 \in (-\infty, \infty).$$

На практике свёртка с БИХ-фильтром (1') заменяется свёрткой с КИХ-фильтром (1), который описывается следующим выражением:

$$g(m_1, m_2) = K \cdot exp\left\{-\frac{(m_1 - м/2)^2 + (m_2 - м/2)^2}{2\sigma^2}\right\},$$

где M – размер окна, определяемый по правилу «трёх сигма»:

$$M = 2 \cdot \left[\frac{3\sigma}{2}\right] + 1, \quad (2)$$

($[x]$ – целая часть числа x), а коэффициент K находится из условия нормировки

$$\sum_{m_1=0}^{M-1} \sum_{m_2=0}^{M-1} g(m_1, m_2) = 1.$$

Параметром преобразования является значение σ.

6. *Повышение резкости* заключается в следующем преобразовании входного изображения

$$\widetilde{\mathrm{C^W}}(\mathrm{n_1}, \mathrm{n_2}) = \mathrm{C^W}(\mathrm{n_1}, \mathrm{n_2}) + q\left(\mathrm{C^W}(\mathrm{n_1}, \mathrm{n_2}) - \mathrm{C^W_{smooth}}(\mathrm{n_1}, \mathrm{n_2})\right),$$

где $\mathrm{C^W_{smooth}}$ – результат усреднения $\mathrm{C^W}$ в окне размерами $M \times M$ (искажение 4 текущего списка), а $q > 0$ – коэффициент усиления разностного изображения.

Параметрами преобразования являются M и q.

7. *Добавление псевдослучайного гауссовского белого шума* $\xi(n_1, n_2)$:

$$\widetilde{C^W}(n_1, n_2) = C^W(n_1, n_2) + \xi(n_1, n_2),$$

значения которого являются реализацией гауссовской случайной величины с плотностью распределения

$$\rho_\xi(x) = \frac{1}{\sqrt{2\pi D_\xi}} exp\left(-\frac{x^2}{2D_\xi}\right). \quad (3)$$

Параметром является дисперсия шума D_ξ.

8. *Медианная фильтрация* – это метод нелинейной обработки сигналов, очень полезный при подавлении аддитивного шума. Метод очень прост, не требует настройки (является непараметрическим) и поэтому получил широкое распространение. Медианный фильтр реализуется как процедура локальной обработки скользящим окном различной формы (в настоящей лабораторной работе предлагается использовать квадратное окно размерами $M \times M$), которое включает нечетное число отсчетов изображения: $M = 2p + 1, p \in \mathbb{N}$.

   Процедура обработки заключается в том, что для каждого положения окна попавшие в него отсчеты упорядочиваются по возрастанию значений. Средний отсчет в этом упорядоченном списке называется *медианой* рассматриваемой группы. Эта медиана заменяет центральный отсчет в окне для обработанного сигнала.

   Параметром является размер окна M.

9. *Сжатие JPEG с последующим восстановлением* заключается в сохранении носителя информации в формате JPEG и последующем восстановлении его в формате без потерь.

   Параметром является показатель качества Q, изменяемый в пределах от 1 до 100.

5.1.2 Методы стегоанализа НЗБ-систем: общая концепция, визуальный анализ, анализ частоты переходов, анализ числа единиц и числа переходов, медианный критерий серий

Основой статистического стегоанализа является изучение статистических характеристик файла. Для текстовой стеганографии эти характеристики – частота встречаемости букв в сообщении, для графических же контейнеров – это [2]:

неоднородность последовательностей отсчетов (байтов информации);

зависимость между битами в отсчетах (корреляция);

зависимость между отсчетами;

неравновероятность условных распределений в последовательности отсчетов;

статистика длин серий (последовательностей из одинаковых бит).

Математическое ожидание единиц

Первый показатель стегоанализа – отношение количества единиц в исследуемом файле к максимально возможному количеству единиц (математическое ожидание появления единицы – *M*) [8]. Поскольку в работе рассматриваются изображения в формате *Bmp*, каждый пиксель формируется записью из трех байтов цвета. Для каждого пикселя считаются все замаскированные (отмеченные) биты, содержащие единицы, и делятся на общее число замаскированных битов. Для изображения, содержащего информацию, *M* должно быть близко к 0,5. Изображение разбивается на блоки размера $m \times n$ и для каждого из них также считается значение M_k (математическое ожидание появления единицы в *k*-ом блоке):

$$\mathrm{M_k} = \frac{\sum_{i,j}^{m,n} \mathrm{P_{i,j}}}{\mathrm{m \times n \times Bits}},$$

где $P_{i,j}$ – количество единиц в выбранных битах одного пикселя,

Bits – число битов, которое анализируется в каждом пикселе.

На основании полученных данных строится график распределения величины *M* по всему изображению.

Число переходов

Другая используемая характеристика *Q* – число переходов между битами соседних пикселей [8]. Так, если в двух соседних пикселях красные составляющие равны (01011001 и 01011001), то число переходов равно 0, а если не равны (например, 00011000 и 00011111), то число переходов равно 3. Между каждыми двумя соседними пикселями в блоке выполняется операция *XOR* (исключающее ИЛИ) и суммируется число единиц по блоку. Результат вычисляется по следующей формуле (для одного блока $m \times n$):

$$Q_k = \frac{\sum_{j=1}^{m}\sum_{i=1}^{n-1} q_{i,j}^{x} + \sum_{j=1}^{n}\sum_{i=1}^{m-1} q_{i,j}^{y}}{([(n-1)\times m+(m-1)\times n]\times Bits)},$$

где $q^x_{i,j}$ и $q^y_{i,j}$ – число переходов соответственно для двух рядом расположенных пикселей по горизонтали и по вертикали соответственно. Полученное значение Q_k будет выражено в долях по отношению к максимально возможному количеству переходов.

На основании полученных данных строится график распределения величины *Q* по всему изображению.

Применение статистического анализа позволяет не учитывать психофизические свойства человеческого зрения и, соответственно, различий между типами изображений нет. В этом случае большое влияние на правильность определения наличия стегоканала оказывает количество встроенной в файл-контейнер информации и то, каким образом производилось встраивание: подряд или равномерно по всему изображению.

Пример статистических характеристик незаполненного контейнера приведен на рисунке 3.

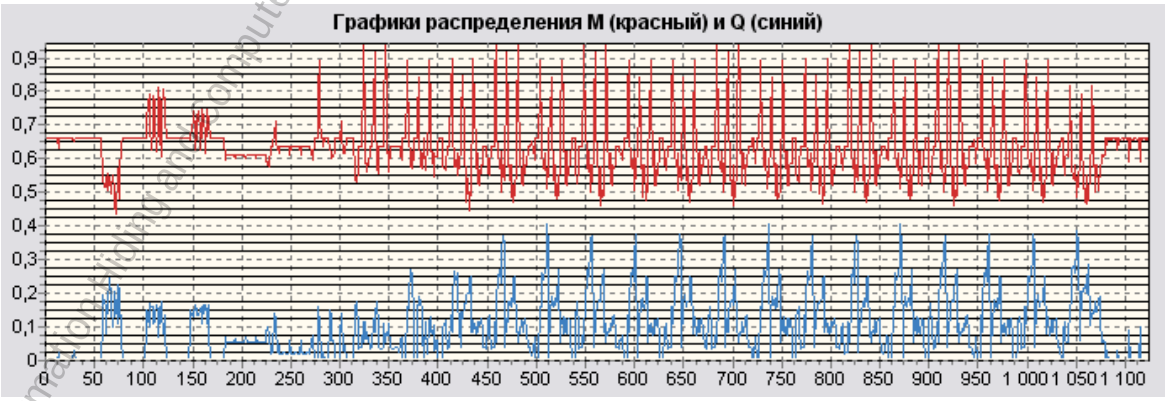


Рисунок 3 - Статистические характеристики незаполненного контейнера

Если информация встраивается подряд, то уже при 5-ти процентном заполнении контейнера происходит локальное нарушение его статистических характеристик (см. рисунок 4).

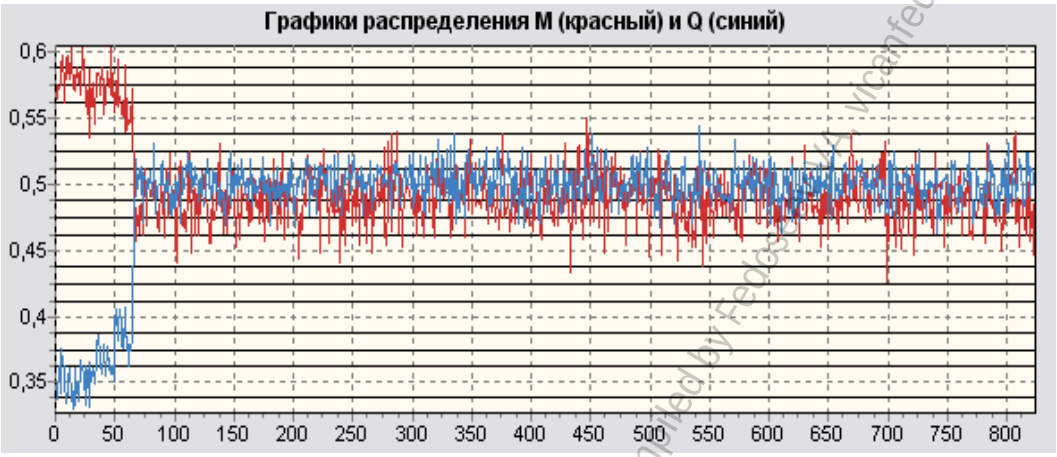


Рисунок 4 – Распределение статистических характеристик контейнера при встраивании информации подряд

Часто этот недостаток устраняют заполнением всего контейнера или использованием для встраивания генератора случайных чисел. В простейшем случае используется схема, когда координата встраивания текущего бита информации X_i зависит от предыдущей (X_{i-1}) и определяется по формуле:

$X_i = (A \cdot X_{i-1} + B) \ mod \ M$,

где A и B – достаточно большие взаимно простые числа, а M – период генератора.

Тогда встроенное сообщение будет распределено по всему контейнеру, однако большое количество скрываемой информации приводит к нарушению общих статистических характеристик (см. рисунок 5).

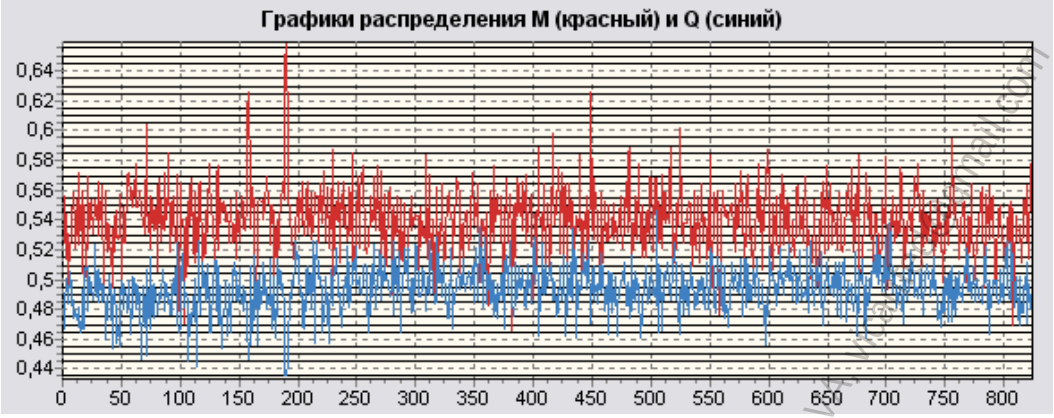


Рисунок 5 – Распределение статистических характеристик контейнера при встраивании информации с помощью генератора случайных чисел

При равномерном встраивании небольших объемов информации достаточно сложно определить факт наличия *стего*. В этом случае можно сравнить статистические характеристики полученного на анализ изображения со статистическими характеристиками изображений того же типа. Две картинки относятся к одному типу, если у них примерно одинаковы следующие характеристики:

непосредственно рисунок (то, что изображено);

цветовая гамма его представления;

частота смены цветов;

размер изображения;

источник изображения.

Так, например, две портретные фотографии двух разных людей должны иметь примерно одинаковые статистические характеристики. Если при сравнении получили сильно различающиеся значения, то можно говорить, что в одно из изображений была встроена информация.

Анализ максимальных отклонений статистических параметров M и Q от их средних значений позволяет определить примерный объем скрытой в контейнере информации. Замечено, что с увеличением процента встраиваемой информации максимальные отклонения пропорционально уменьшаются.

Визуальный анализ

Данный метод позволяет выявлять передачу скрытой информации в том случае, если в изображении присутствуют монотонные области и при встраивании информации подряд. Суть метода заключается в получении битовых срезов, то есть изображения, определяемого замаскированными битами. В те байты цвета пикселя, в замаскированных битах которых стоит хотя бы одна единица, заносят максимальное значение интенсивности цвета (255), а в остальные – минимальное (0). Далее полученное изображение просматривают и визуально сравнивают с исходным.

Если контейнер пуст, монотонные области (контура, тени, текст) будут отображаться единым цветом, поэтому их битовый срез будет относительно «чист». В случае равномерно заполненного контейнера, такие области будут иметь шумы, так как при встраивании информации будут меняться младшие биты цветовых составляющих, что и позволит выявить наличие *стего* (см. рисунок 6). Если информация встраивалась подряд, то искажена будет та область изображения, в которой находится скрытое сообщение.

Рисунок 6 – Результаты визуального анализа контейнера

(слева пустой контейнер, справа – равномерно заполненный)

Медианный критерий серий

Данный метод стеганографического анализа был недавно предложен авторами статьи [5] – В.Н. Кустовым и А.Ю. Параскевопуло. Он применим к полноцветным изображениям с мелкими деталями и практически без монотонных областей, возможно переконвертированным из других графических форматов (*JPEG*, *TIFF* и т.д.). Визуальный анализ таких изображений практически не дает результата, а их математическое ожидание даже для незаполненных контейнеров примерно равно 0,5. Таким образом, стандартными средствами стегоанализа не удается идентифицировать стего данного типа.

Общая идея метода состоит в переходе от выборки (x_1, x_2, ..., x_n) по определенному правилу к совокупности двоичных значений (d_1, d_2, …, d_m), $m \le n$ [5]. Так, последовательность, состоящая из наименее значимых битов байтов цветовой составляющей, уже является последовательностью значений из нулей и единиц:

$$d = \begin{cases} 1 \\ 0 \end{cases}$$

Если такая последовательность получена, то нетрудно понять: при действительно случайной выборке (то есть ее значения независимы) значения 0 и 1 должны чередоваться случайным образом.

Практика показала, что между младшими битами изображений существуют некоторые закономерности, и их поведение вовсе не похоже на случайное [7]. В результате анализа, проведенного А.Т. Алиевым, выяснилось, что в изображениях очень часто встречаются длинные серии из одинаковых бит и практически любое изображение содержит серию минимум из 14 одинаковых бит. В случае внедрения информации в младшие биты изображения, эти закономерности нарушаются. Следовательно, последовательность младших бит *заполненного контейнера*, во-первых, не будет содержать слишком длинных серий и, во-вторых, число серий из подряд идущих одинаковых значений 0 или 1 не будет очень мало.

Функция выборки является двумерной и включает в себя величины $\upsilon(n)$ и $\tau(n)$, где:

n – объем выборки,

$\upsilon(n)$ – число серий, состоящих из подряд идущих одинаковых значений 0 и 1,

$\tau(n)$ – максимальная длина серий.

Задаются пороговые значения $\upsilon_0(n)$ и $\tau_0(n)$, которые определяют собой границы критической области при заданном уровне значимости:

$$\begin{cases} \upsilon(n) > \upsilon_0(n) \\ \tau(n) < \tau_0(n) \end{cases}$$

Если оба неравенства выполняются, то мы находимся в области допустимых значений показателя согласованности и нет оснований отвергать гипотезу о том, что выборочные значения независимы (контейнер заполнен). В противном случае гипотеза отвергается.

Пороговые значения определяются следующим образом:

$\upsilon_0(n) = \mathrm{E}\left[\frac{1}{2}\cdot(\mathrm{n}+1-1{,}96\sqrt{\mathrm{n}-1})\right]$,

$\tau_0(n) = E[3{,}3lg(n+1)]$.

Выполнение неравенств проверяется для всех трех последовательностей битов цветовых составляющих (красной, зеленой и синей), что позволяет повысить точность данного метода. По степени выполнения приведенных выше неравенств можно судить о том, является ли последовательность случайной. Поскольку чаще всего вкладываемая информация архивируется и (или) шифруется, наличие в младших битах статистически случайных значений также говорит об обнаружении *стего*.

По полученным результатам строится график, аналогичный приведенному на рисунке 7. На оси абсцисс откладываются значения максимальной длины серий из числа серий. На оси ординат – значения числа серий. Через пороговые значения $\upsilon_0(n)$ и $\tau_0(n)$ проводятся две линии (AB и CD), параллельные координатным осям, которые разбивают координатную плоскость на четыре области.

Сделать вывод о случайности последовательности можно по точкам на координатной плоскости. Если точки находятся в области I, то значения последовательности независимы (случайны), если точки находятся в области IV, то последовательность не является случайной. В нашем случае определить наличие *закладки* в контейнере можно, если точки находятся в области I. Скорее всего, контейнер будет заполнен и в случаях, когда точки находятся в областях II, III и IV рядом с прямыми AB или CD или с точкой их пересечения. Во всех остальных случаях делается предположение о том, что контейнер пуст.

Рисунок 7 – Результаты медианного критерия серий

(заполненный контейнер)

Недостатком данного метода анализа является его нечувствительность к встраиванию небольшого изображения в контейнер и встраиванию в контейнеры с большими монотонными областями. Кроме того, в незаполненном контейнере младшие биты могут иметь шумовой характер, что может быть ложным основанием обнаружения стего.

Анализ частоты переходов

Этот метод также был предложен авторами статьи [5] и служит дополнением к медианному критерию серий. Его суть заключается в подсчете числа различных переходов среди младших битов для каждой составляющей цвета отдельно. Возможны переходы четырех типов:

из «0» в «0»,

из «0» в «1»,

из «1» в «0»,

из «1» в «1».

В случае пустого контейнера переходов из «0» в «1» и из «1» в «0» будет значительно меньше, чем переходов из «0» в «0» и из «1» в «1». Это, случается из-за

одинакового цвета пикселей, отображающих такие объекты, как фон, тень и т. д. Если же контейнер заполнен, то значения всех переходов будут примерно выровнены. Возможны также варианты, когда значения переходов «0»-«1» и «1»-«0» будут превосходить сразу оба значения переходов «0»-«0» и «1»-«1» или, наоборот, значения переходов «1»-«1» и «0»-«0» будут больше значений переходов «0»-«1» и «1»-«0», но разница между их значениями будет незначительной [5].

Результаты анализа удобно представить в виде диаграмм, изображенных на рисунке 8.

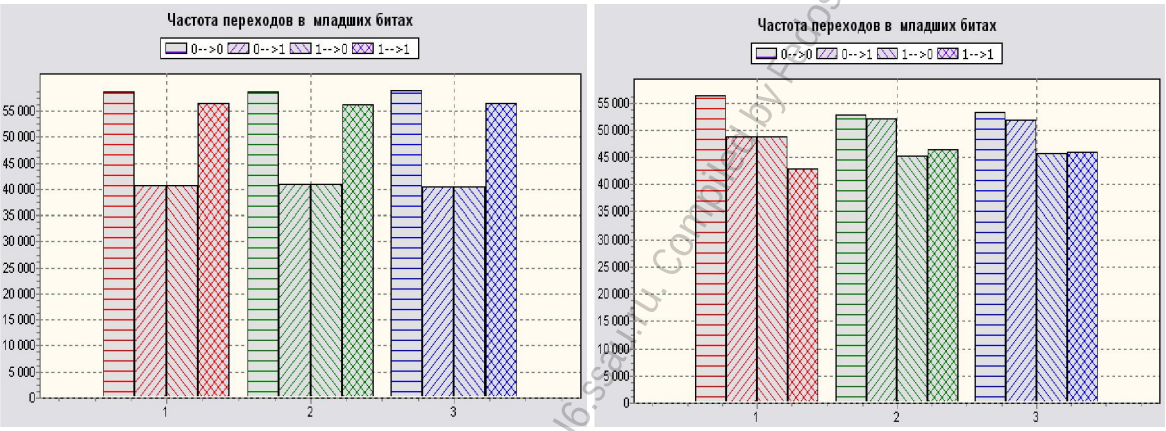


Рисунок 8 – Результаты анализа частоты переходов

(слева пустой контейнер, справа – заполненный)

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

ПРОСТЕЙШИЕ МЕТОДЫ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ПОЛУТОНОВЫЕ ИЗОБРАЖЕНИЯ

Методические указания к лабораторной работе 1
по курсу «Компьютерная стеганография»

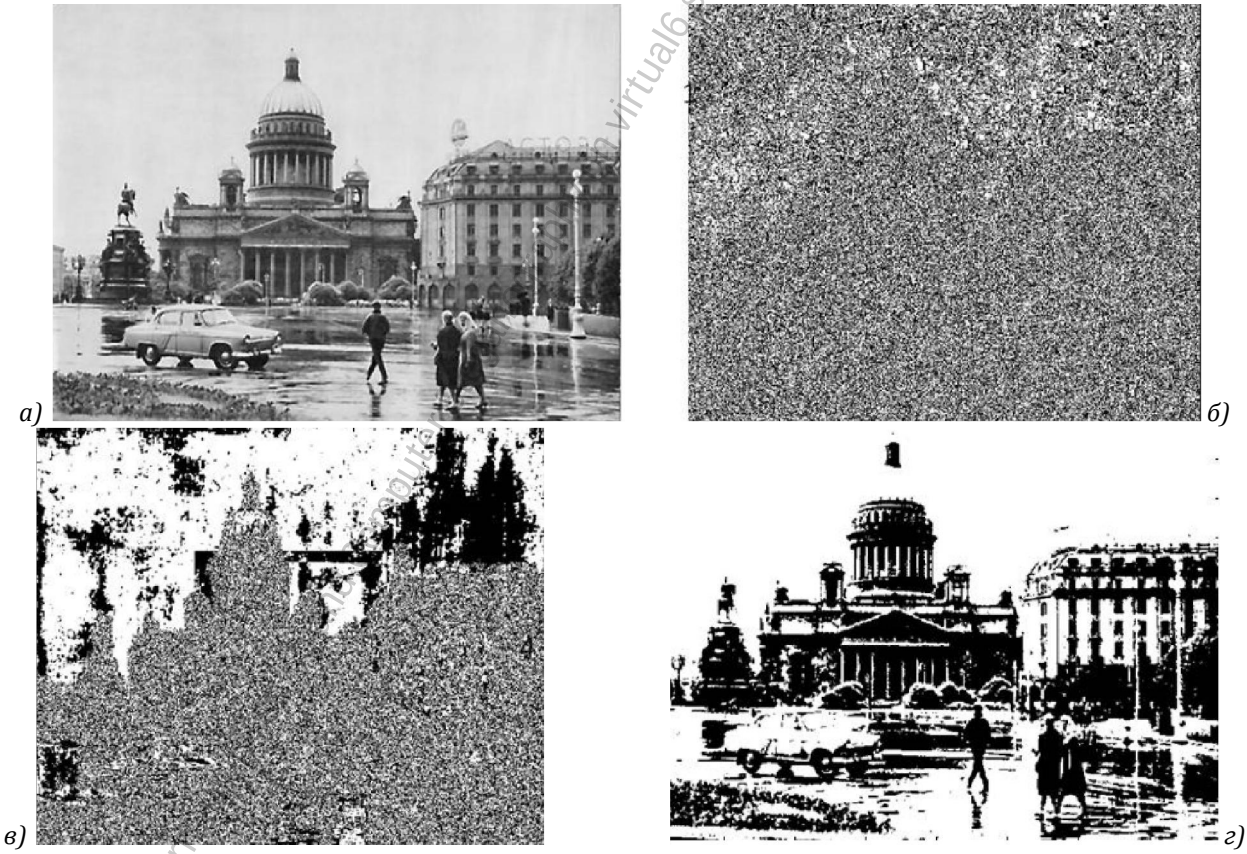
Самара 2012

Содержание

Теоретические основы лабораторной работы

1. Встраивание информации в наименее значимые биты контейнера

Встраивание информации в наименее значимые биты контейнера (НЗБ, least significant bit, LSB) является одним из первых и самых простых методов сокрытия информации. Контейнер для данной группы методов в каноническом случае представляет собой 8-битное полутоновое изображение (однако нетрудно предложить его модификации на случаи большего или меньшего количества бит, а также для многоканальных изображений), а сообщение – бинарное изображение. Для извлечения информации требуется исходное изображение-контейнер.



а) б) в) г)

Рис. 1. Битовые плоскости полутонового изображения: а) исходное изображение; б) первая битовая плоскость; в) 4-я битовая плоскость; г) 8-я битовая плоскость

Яркость пикселя контейнера с координатами (n_1, n_2) можно записать в двоичном представлении следующим образом:

$$C(n_1, n_2) = C_1(n_1, n_2) + C_2(n_1, n_2) \cdot 2 + \ldots + C_K(n_1, n_2) \cdot 2^{K-1},$$

где $\forall k = 1..K,\ \forall(n_1, n_2)\ \ C_k(n_1, n_2) \in [0,1]$, а в случае 8-битного изображения $K = 8$. Матрицы C_k зачастую называют битовыми плоскостями.

Наименее и наиболее значащими битовыми плоскостями являются соответственно C_1 и C_8: если изменить значение бита $C_1(n_1, n_2)$, то яркость изменится на единицу; если же изменить значение бита $C_8(n_1, n_2)$, то яркость изменится на 128. Различие между младшими и старшими битовыми плоскостями хорошо видно визуально на рис.1. Младшие битовые плоскости выглядят как слабокоррелированный шум. Осмысленные детали начинают проступать лишь с четвёртой битовой плоскости. Это означает, что менее значимые битовые плоскости можно модифицировать с целью встраивания скрытого сообщения или ЦВЗ.

Рис. 2. Пример встраивания изображения во вторую битовую плоскость: сверху заполненный контейнер, снизу встраиваемое изображение

Обозначим модифицированный контейнер со встроенной информацией как C^W. В двоичном представлении оно выглядит следующим образом:

$$C^W(n_1, n_2) = C_1^W(n_1, n_2) + C_2^W(n_1, n_2) \cdot 2 + \ldots + C_K^W(n_1, n_2) \cdot 2^{K-1}.$$

На практике применяются два способа встраивания информации за счёт модификации битовой плоскости контейнера:

1. Побитовое сложение бита контейнера с битом скрываемой информации:

$$C_k^W(n_1, n_2) = \begin{cases} C_k(n_1, n_2) \oplus W(n_1, n_2), & k = p, \\ C_k(n_1, n_2), & k \neq p, \end{cases}$$

где p – номер битовой плоскости, в которой осуществляется встраивание. Извлечение информации также происходит путём побитового сложения изображения со встроенной информацией с исходным контейнером.

2. Непосредственная замена бита контейнера битом скрываемой информации.

$$C_k^W(n_1, n_2) = \begin{cases} W(n_1, n_2), & k = p, \\ C_k(n_1, n_2), & k \neq p, \end{cases}$$

где также p – номер битовой плоскости, в которой осуществляется встраивание. Извлечение информации происходит, очевидно, путём чтения соответствующей битовой плоскости изображения со встроенной информацией.

На рис. 2 представлен полутоновой контейнер, во вторую битовую плоскость которого встроено бинарное изображение. Выбор битовой плоскости определяет качество метода и должен удовлетворять двум условиям: визуальная неразличимость и устойчивость при дальнейших преобразованиях заполненного контейнера.

2. Встраивание информации на основе деления с остатком

Данный метод также предназначен для встраивания информации в полутоновые изображения и является обобщением метода встраивания в наименее значимые биты изображения.

Пусть имеются контейнер C - полутоновое изображение и W - скрываемое изображение одного и того же размера. Тогда встраивание в каждом пикселе (n_1, n_2) осуществляется по формуле:

$$C^W(n_1, n_2) = \left[\frac{C(n_1, n_2)}{2q}\right] \cdot 2q + W(n_1, n_2) \cdot q + C(n_1, n_2)\ (mod\ \ q),$$

где $q \in \mathbb{N}$ – параметр встраивания, влияющий на видимость встроенного изображения, $[x]$ означает целую часть рационального числа x, а $x(\mathrm{mod}\ y)$ – остаток от деления x на y.

Формула извлечения информации может быть получена на основе формулы встраивания. Студентам предлагается сделать это самостоятельно.

Преимущество данного метода перед методом встраивания в младшие биты состоит в более широких возможностях вариации качества получаемого заполненного контейнера и устойчивости к искажениям. Это достигается за счёт вариации параметра встраивания q. Помимо этого, при извлечении информации не требуется исходный контейнер.

Задания

Лабораторная работа состоит из двух заданий по вариантам, которые необходимо выполнить при помощи инструментов, предоставляемых системой *ResLook*. По желанию разрешается вместо командного файла с вызовом прикладных модулей *ResLook* написать программу на языке высокого уровня, реализующую требуемое задание. В лабораторных классах имеется среда *Microsoft Visual Studio 2003*, при возможности использования собственного ноутбука допускается использование любой среды программирования.

В обоих заданиях требуется реализовать алгоритмы встраивания информации в изображение, а также процедуры извлечения встроенной информации. В качестве объекта встраивания для любого варианта может применяться изображение или текст.

В качестве базового объекта предлагается использовать изображение. Для реализации встраивания текстовой информации средств *ResLook*'а не достаточно, поэтому необходимо написать программный модуль, записывающий текстовую информацию в изображение. Реализация встраивания текстовой информации не обязательна, но влечёт за собой бонусы тем, кто её сделает.

Задание 1. Встраивание информации в наименее значимые биты контейнера

1. Реализовать встраивание информации в одну из наименее значимых битовых плоскостей контейнера одним из рассмотренных способов встраивания. Номер модифицируемой битовой плоскости и способ модификации определяются вариантом.

2. Реализовать извлечение информации, встроенной в пункте 1.

Задание 2. Встраивание информации на основе деления с остатком

1. Реализовать встраивание информации на основе деления с остатком. Параметр встраивания q определяется вариантом.
2. Реализовать извлечение информации, встроенной в пункте 1.

Таблица вариантов заданий[1]

№ варианта	Модифицируемые битовые плоскости в задании 1	Способ встраивания в задании 1	Значение параметра q в задании 2
1	1-я	Замена	6
2	1-я	⊕	8
3	1-я	Замена	10
4	2-я	⊕	6
5	2-я	Замена	8
6	2-я	⊕	10
7	3-я	Замена	6
8	3-я	⊕	8
9	3-я	Замена	10
10	1-я и 2-я	⊕	6
11	1-я и 2-я	Замена	8
12	1-я и 2-я	⊕	10

Контрольные вопросы

1. Какая битовая плоскость изображения является более значимой: четвёртая или шестая? Почему? Проиллюстрировать ответ средствами *ResLook*.
2. Сравните два метода модификации наименее значимых битов контейнера: побитовое сложение и непосредственная замена.
3. Какие способы встраивания информации в НЗБ контейнера, помимо двух рассмотренных, могут применяться?
4. Как можно изменить схему метода НЗБ, чтобы его можно было применять для проверки подлинности изображения?
5. Какой критерий следует использовать для извлечения информации, встроенной методом деления с остатком?
6. В каком случае метод деления с остатком эквивалентен методу НЗБ?
7. В каких пределах может изменяться параметр q в методе деления с остатком?
8. Что происходит с гистограммой изображения при встраивании в него информации методом деления с остатком?

[1] Зелёным цветом помечены более сложные варианты, голубым более лёгкие, белым – средние. Варианты отсортированы в порядке усложнения задания (впрочем, относительная сложность – понятие субъективное☺).

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

ВСТРАИВАНИЕ ИНФОРМАЦИИ В БИНАРНЫЕ ИЗОБРАЖЕНИЯ

Методические указания к лабораторной работе 2

по курсу «Компьютерная стеганография»

Самара 2012

Содержание

Теоретические основы лабораторной работы

1. Бинарные изображения

Бинарными называются изображения, в которых используется 1 бит для хранения интенсивности каждого пикселя в каждом из каналов. При этом, как правило, под бинарными понимаются одноканальные изображения.

Рис. 1. Пример полутонового изображения
и полученного из него растрированного бинарного изображения

Принято выделять в бинарных изображениях три типа областей: светлая, тёмная и граничная (серая). Светлая область содержит преимущественно белые пиксели, тёмная – преимущественно чёрные, граничная – и те и другие в приблизительно равных пропорциях. Дополнительная информация, внедряемая в изображение за счёт модификации его пикселей, наименее заметна в граничной области. Таким образом, в большинстве методов информация внедряется исключительно в граничные области.

Бинарные изображения чаще всего являются результатом цифрового растрирования полутоновых изображений. В широком смысле *цифровое растрирование* – это технология создания иллюзии непрерывного тона с помощью бинарного устройства вывода. Пользуясь терминологией, используемой в цифровой обработке изображений, можно сказать, что цифровое растрирование – это квантование полутоновых изображений до глубины 1 бит/пиксель. Пример растрированного изображения приведён на рисунке 1.

Метод растрирования изображений с диффузией ошибки

Пусть C – полутоновое изображение размером $N_1 \times N_2$, яркость пикселей которого $C(n_1, n_2)$ принимает целые значения на отрезке $[0{,}255]$. Из него необходимо получить бинарное изображение C^B того же размера. Будем для простоты считать, что яркость пикселей $C^B(n_1, n_2)$ принимает значения 0 или 255 (такие изображения мы будем называть псевдобинарными).

В алгоритме диффузии ошибки (Error Diffusion) используется весовая функция h размерами $M_1 \times M_2$, называемая также *ядром* алгоритма. Как правило, размеры ядра невелики: $1 \le M_1, M_2 \le 5$. Ядро задаёт направления распространения (диффузии) ошибки бинаризации и доли ошибки, передаваемые в каждом из направлений.

Приведём примеры весовых функций, зарекомендовавших себя на практике:

- Ядро 1 (Floyd)

$$\frac{1}{16}\begin{pmatrix} 0 & \odot & 7 \\ 3 & 5 & 1 \end{pmatrix}; \tag{1}$$

- Ядро 2 (Jarvis)

$$\frac{1}{48}\begin{pmatrix} 0 & 0 & \odot & 7 & 5 \\ 3 & 5 & 7 & 5 & 3 \\ 1 & 3 & 5 & 3 & 1 \end{pmatrix}; \tag{2}$$

- Ядро 3 (Stucki)

$$\frac{1}{42}\begin{pmatrix} 0 & 0 & \odot & 8 & 4 \\ 2 & 4 & 8 & 4 & 2 \\ 1 & 2 & 4 & 2 & 1 \end{pmatrix}; \tag{3}$$

- Ядро 4 (Fan)

$$\frac{1}{16}\begin{pmatrix} 0 & 0 & \odot & 7 \\ 1 & 3 & 5 & 0 \end{pmatrix}; \tag{4}$$

- Ядро 5 (3-digit)

$$\frac{1}{16}\begin{pmatrix} 0 & \odot & 8 \\ 2 & 6 & 0 \end{pmatrix}; \tag{5}$$

Символом $\odot$ отмечен пиксель с координатами $(0{,}0)$. Значение $h(0{,}0) = 0$.

На практике используются две математически эквивалентных модели диффузии ошибки: подтягивание ошибок бинаризации из уже пройденных отсчётов (*pull-модель*) и распространение ошибки из текущего отсчёта в последующие (*push-модель*). Обе модели будут рассмотрены ниже.

Алгоритм диффузии ошибки (pull-модель)

Обозначим за D_h множество точек (n_1, n_2), в которых $h(n_1, n_2) \neq 0$. Тогда pull-модель алгоритма растрирования с диффузией ошибки выглядит следующим образом:

$$u(n_1, n_2) = C(n_1, n_2) - \sum_{(m_1,m_2)\in D_h} h\,(m_1, m_2) e(n_1 - m_1, n_2 - m_2), \quad (6)$$

$$C^B(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \geq T \\ 0, & u(n_1, n_2) < T \end{cases} \quad (7)$$

$$e(n_1, n_2) = C^B(n_1, n_2) - u(n_1, n_2) \quad (8)$$

В формулах (6)-(8) $u(n_1, n_2)$ и $e(n_1, n_2)$ – это вспомогательные изображения размерами $N_1 \times N_2$. Первое характеризует корректируемый в зависимости от ошибки бинаризации контейнер, второе – ошибку бинаризации в очередной точке. T – пороговое значение, как правило, равное 128. Также алгоритм растрирования (6)-(8) показан в виде схемы на рис. 2.

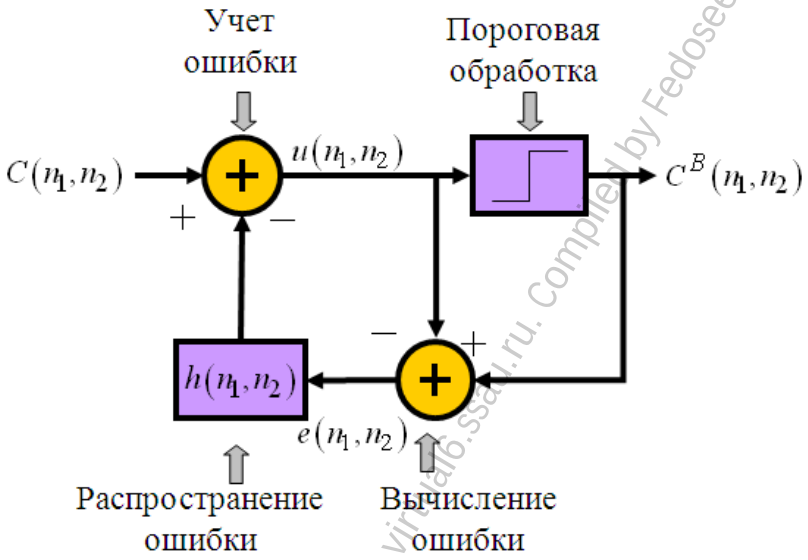


Рис. 2. Схема метода диффузии ошибки

Алгоритм диффузии ошибки (push-модель)

Пусть, аналогично, D_h – множество точек (n_1, n_2), в которых $h(n_1, n_2) \neq 0$. Тогда push-модель алгоритма растрирования с диффузией ошибки выглядит следующим образом:

$$u(n_1, n_2) = C(n_1, n_2) \;\; \forall (n_1, n_2):\; n_1 = \overline{0..N_1 - 1},\; n_2 = \overline{0..N_2 - 1} \quad (9)$$

$$C^B(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \geq T \\ 0, & u(n_1, n_2) < T \end{cases} \quad (10)$$

$$e = C^B(n_1, n_2) - u(n_1, n_2) \quad (11)$$

$$\forall (m_1, m_2) \in D_h \;\; \rightarrow \;\; u(n_1 + m_1, n_2 + m_2) -= e \cdot h(m_1, m_2) \quad (12)$$

Как и в pull-модели, $u(n_1, n_2)$ – вспомогательное изображение размерами $N_1 \times N_2$. Поле ошибок уже хранить не обязательно, поскольку на каждом шаге алгоритма ошибка бинаризации сразу рассеивается по изображению u.

2. Непосредственное встраивание информации в бинарный контейнер

В данной группе методов в качестве контейнера используется бинарное изображение, полученное из полутонового на предварительном этапе. Также предполагается, что полутоновой источник не известен на этапе встраивания информации и, следовательно, не может оказать влияние на этот процесс.

Алгоритм DHST (Data Hiding Self-Toggling)

В данной схеме встраиваемая информация представляет собой бинарный вектор. Каждый бит секретной информации внедряется в бит контейнера путём непосредственной замены. Ключ, создаваемый при помощи генератора случайных чисел, определяет позицию для внедрения. Один бит информации внедряется в один бит контейнера. Для восстановления информации используется тот же самый ключ. В данном методе высока степень визуальных искажений.

Алгоритм DHSPT (Data Hiding by Smart Pair-Toggling)

В данной схеме встраиваемая информация также представляет собой бинарный вектор, и каждый бит секретной информации внедряется также непосредственно в бит контейнера. Ключ, создаваемый при помощи генератора случайных чисел, определяет позицию для внедрения.

Процедура встраивания происходит следующим образом. Бит информации присваивается биту контейнера, позиция которого выбирается согласно ключу. Если при этом значение бита пикселя контейнера не изменилось, то никакие дополнительные действия не осуществляются. В противном случае из окрестности 3×3 вокруг позиции, выданной генератором,– (m,n) выбирается пиксель со значением яркости, равным яркости измененного пикселя (m,n), и его значение инвертируется для компенсации изменения в пикселе (m,n). Данная процедура называется “pair toggling” и является простейшим способом коррекции искажений, вносимых при встраивании ЦВЗ. Если в окрестности 3×3 отсутствуют пиксели со значением яркости, равной яркости измененного пикселя (m,n), компенсация искажений не производится.

Рассмотрим более подробно процедуру выбора компенсирующего пикселя. Простейшим способом является случайный выбор пикселя с нужным значением яркости в окрестности 3×3. Существует также и более разумный подход. Для каждого пикселя окрестности точки (m,n) рассчитывается его вес, и инвертированию подвергается пиксель с наибольшим весом.

Расчёт веса пикселя (p,q) из окрестности пикселя (m,n) осуществляется также в окне 3×3. Обозначим пиксели окна как $x_1, x_2, \ldots x_9$, причем x_5 - центральный пиксель с координатами (p,q). Тогда вес пикселя $V(p,q)$ рассчитывается следующим образом:

$$V(p,q) = \sum_{i=1}^{9} w(i) f(x_5, x_i),$$

$$f(x,y) = \begin{cases} 1 & x \neq y, \\ 0 & x = y; \end{cases}$$

$$w(i) = \begin{cases} 1, & i = 1,3,7,9; \\ 2, & i = 2,4,6,8; \\ 0, & i = 5. \end{cases}$$

Наибольший вес пикселя (p,q) означает, что почти все пиксели его окрестности имеют тот же цвет, что и (m,n). Поэтому если инвертированию подвергается пиксель с наибольшим весом, то это влечёт наименьшие визуальные искажения.

3. Встраивание информации при растрировании полутоновых изображений

В методе, описанном ниже, контейнер представляет собой полутоновое изображение, но передаваться по каналу связи он будет в бинарном виде. Поэтому встраивание информации может происходить до процедуры растрирования или вместе с ней.

Алгоритм DHCED (Data Hiding by Conjugate Error Diffusion)

В данной схеме встраиваемая информация представляет собой бинарное изображение $W(n_1, n_2)$, размеры которого $N_1 \times N_2$ равны размерам полутонового контейнера $C(n_1, n_2)$. При встраивании ЦВЗ создаются два бинарных изображения C^B и C^W – результата растрирования $C(n_1, n_2)$ таким образом, чтобы в как можно большем числе точек выполнялось равенство

$$W(n_1, n_2) = C^B(n_1, n_2) \oplus C^W(n_1, n_2), \tag{13}$$

Для этого изображение C^B создаётся при помощи алгоритма диффузии ошибки, рассмотренного в разделе 1. Изображение C^W создаётся при помощи модифицированного алгоритма диффузии ошибки, в котором на втором этапе вместо (7) или (10) используется следующее соотношение[1]:

$$C^W(n_1, n_2) = \begin{cases} 255, & u(n_1, n_2) \geq T_1 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 255 \\ 0, & u(n_1, n_2) < T_1 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 255 \\ 255, & u(n_1, n_2) \geq T_2 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 0 \\ 0, & u(n_1, n_2) < T_2 \quad and \quad W(n_1, n_2) \oplus C^B(n_1, n_2) = 0 \end{cases}, \tag{14}$$

$$T_1 < T < T_2.$$

Как правило, используются значения $T_1 = 64$, $T_2 = 192$.

Для извлечения информации используется формула (13).

Задания

Лабораторная работа состоит из одного задания по вариантам, для выполнения которых необходимо написать программу в среде *Microsoft Visual Studio*.

Вариант 1. Встраивание текстовой информации в бинарный контейнер

1. Реализовать процедуры генерации битовой последовательности заданной длины K (встраиваемой информации) и сохранения её в текстовый файл.
2. Реализовать процедуры генерации последовательности координат пикселей той же длины K (ключа) и сохранения её в текстовый файл одним из способов по вариантам:
    1) простая генерация пар чисел – координат пикселя по вертикали и горизонтали (“Gen-simple”):

    $$\left(n_1^k, n_2^k\right): \; n_1^k = \overline{0..N_1 - 1}, \qquad n_2^k = \overline{0..N_2 - 1}, \qquad k = \overline{0..K - 1}$$

    2) генерация пар чисел – координат пикселя по вертикали и горизонтали на втрое меньшей сетке (“Gen-div3”):

    $$\left(3n_1^k, 3n_2^k\right): \; n_1^k = \overline{0..\left[\frac{N_1}{3}\right] - 1}, \qquad n_2^k = \overline{0..\left[\frac{N_2}{3}\right] - 1}, \qquad k = \overline{0..K - 1}$$

[1] В формулах (8) и (11), очевидно, вместо C^B также используется C^W.

3) генерация пар чисел на полной сетке с проверкой (“Gen-check”):

$$\left(n_1^k, n_2^k\right):\ n_1^k = \overline{0..N_1-1},\qquad n_2^k = \overline{0..N_2-1},\qquad k = \overline{0..K-1}$$

$$\min_{k\neq m}\left(n_1^k - n_1^m\right) > 1,\qquad \min_{k\neq m}\left(n_2^k - n_2^m\right) > 1,\qquad k,m = \overline{0..K-1}$$

3. Реализовать процедуру встраивания битовой последовательности из текстового файла в заданное псевдобинарное[2] изображение при помощи заданного в текстовом файле ключа одним из алгоритмов по вариантам:
   1) DHST;
   2) DHSPT со случайным выбором компенсирующего пикселя (“DHSPT-random”);
   3) DHSPT с оценкой весов пикселей окрестности для выбора компенсирующего (“DHSPT-weight”).
4. Реализовать процедуру извлечения встроенной битовой последовательности из изображения и сохранения её в текстовый файл.

Вариант 2. Встраивание бинарного изображения при растрировании полутонового изображения

1. Реализовать процедуру растрирования входного полутонового изображения методом диффузии ошибки. Ядро и модель алгоритма определяется вариантом задания.
2. Реализовать процедуру встраивания в растрируемое изображение псевдобинарного изображения алгоритмом DHCED с ядром и моделью, использованными в пункте 1.
3. Реализовать процедуру извлечения информации, встроенной алгоритмом DHCED, и сохранения её в виде псевдобинарного изображения.

Таблица вариантов заданий[3]

№	Основной вариант	Конкретный алгоритм группы DHST	Способ генерации ключа	Ядро в алгоритме DHCED	Модель диффузии ошибки
1	1	DHST	Gen-simple	–	–
2	1	DHSPT-random	Gen-simple	–	–
3	1	DHSPT-random	Gen-div3	–	–
4	1	DHSPT-random	Gen-check	–	–
5	1	DHSPT-weight	Gen-div3	–	–
6	1	DHSPT-weight	Gen-check	–	–
7	2	–	–	Floyd	pull
8	2	–	–	Jarvis	pull
9	2	–	–	Stucki	pull
10	2	–	–	Floyd	push
11	2	–	–	Jarvis	push
12	2	–	–	Stucki	push

[2] Под псевдобинарным изображением понимается двухцветное изображение, для хранения которого используются 8 бит на пиксель: 0 кодирует чёрный цвет, 255 кодирует белый цвет.

[3] Зелёным цветом помечены более сложные варианты, голубым более лёгкие, белым – средние. Варианты отсортированы в порядке усложнения задания (впрочем, относительная сложность – понятие субъективное☺).

Контрольные вопросы

1. Какие способы преобразования из полутонового изображения в бинарное (кроме растрирования) вы знаете? Чем они отличаются друг от друга и от растрирования?
2. Опишите общую концепцию метода диффузии ошибки. Приведите примеры весовых функций, используемых на практике. Какие, по-вашему, весовые функции также могут быть использованы и почему?
3. Опишите pull-модель алгоритма растрирования с диффузией ошибки. Покажите на рисунке, что происходит в окрестности очередного пикселя (n_1, n_2) при работе этого алгоритма.
4. Опишите push-модель алгоритма растрирования с диффузией ошибки. Покажите на рисунке, что происходит в окрестности очередного пикселя (n_1, n_2) при работе этого алгоритма.
5. Опишите в математическом виде алгоритм DHST. Проиллюстрируйте его работу на простом примере (на рисунке).
6. В чём заключаются отличия между различными алгоритмами группы DHST? Проиллюстрируйте различия на простом примере.
7. Зачем производится расчёт весов пикселей в алгоритме DHSPT? Проиллюстрируйте процедуру выбора нужного компенсирующего пикселя по весам.
8. Каким требованиям должны удовлетворять ключи, используемые в алгоритмах группы DHSPT? Расскажите о достоинствах и недостатках каждого из способов генерации ключа, описанных в задании. Можете ли вы предложить какой-либо альтернативный способ?
9. Опишите алгоритм DHCED. Как выбор порогов T_1 и T_2 влияет на результат?
10. Можете ли вы предложить модификацию алгоритма DHCED, которая могла бы улучшить качество извлечения информации?

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Кафедра геоинформатики и информационной безопасности

ИССЛЕДОВАНИЕ СТОЙКОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ К ИСКАЖЕНИЯМ НОСИТЕЛЯ ИНФОРМАЦИИ

Методические указания к лабораторной работе 3

по курсу «Компьютерная стеганография»

Самара 2013

Содержание

Теоретические основы лабораторной работы

1. Стойкость ЦВЗ к искажениям носителя информации

Стойкость систем ЦВЗ

Основным назначением цифровых водяных знаков является защита информации, содержащейся в контейнере. В различных приложениях действуют разные ограничения на способы использования или модификации контейнера, поэтому и средства защиты также должны быть различными. По уровню стойкости системы ЦВЗ можно выделить четыре категории: секретная, стойкая, полухрупкая и хрупкая. Под стойкостью понимается устойчивость ЦВЗ к различного рода воздействиям на носитель информации (контейнер со встроенным ЦВЗ).

В *секретных* системах встраивания информации ЦВЗ должен сохраняться как при преднамеренных атаках, направленных на его удаление, так и при непреднамеренных воздействиях на носитель информации в процессе его передачи или использования. В отличие от секретных систем, в *стойких* системах водяной знак должен сохраняться при произвольных непреднамеренных воздействиях на носитель информации, определяемых особенностями его использования. В *полухрупких* системах ЦВЗ должен быть устойчив по отношению к одним воздействиям и неустойчив по отношению к другим. Например, он может сохраняться в результате сжатия изображения, но должен разрушиться при замене фрагмента носителя информации. В *хрупких* системах ЦВЗ разрушается даже при незначительной модификации заполненного контейнера. Следует также отметить, что, как правило, полухрупкие и хрупкие системы позволяют не только отразить сам факт модификации сигнала, но также указать на способ и местоположение произведённого изменения.

Исследуемые виды искажений

В данном подразделе описаны виды искажений носителя информации, которые требуется применять в данной лабораторной работе. Эти искажения сопровождаются параметром, характеризующим степень их влияния на сигнал.

1. *Линейное изменение динамического диапазона функции яркости* заключается в линейном поэлементном преобразовании изображения:

$$\widetilde{C^W}(n_1, n_2) = min\{\alpha C^W(n_1, n_2), 255\}, \quad \alpha \in \mathbb{R}, \alpha > 0.$$

Параметром является коэффициент α при значении функции яркости.

2. При *повороте с последующим восстановлением* происходят два последовательных поворота изображения: на некоторый угол φ и на обратный ему угол $-\varphi$.

Параметром является угол поворота φ.

3. При *масштабировании с последующим восстановлением* происходит последовательное изменение размера изображения и его возвращение в исходный размер.

Параметром является коэффициент масштабирования.

4. Под *усреднением* в скользящем окне будем понимать обработку изображения C^W ЛИС-системой, имеющей конечную импульсную характеристику $g(m_1, m_2)$, имеющую размеры $M \times M$, где $M = 2p + 1, p \in \mathbb{N}$:

$$\widetilde{C^W}(n_1, n_2) = \sum_{m_1=0}^{M-1} \sum_{m_2=0}^{M-1} g(m_1, m_2) \cdot C^W(n_1 - m_1, n_2 - m_2), \tag{1}$$

причём отсчёты ИХ постоянны и равны $1/M^2$. Например, для $M = 3$

$$g(m_1, m_2) = \frac{1}{9}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Параметром является размер окна M.

5. *Гауссовское размытие* заключается в обработке изображения ЛИС-системой с бесконечной импульсной характеристикой $g(m_1, m_2)$:

$$\widetilde{C^W}(n_1, n_2) = \sum_{m_1=-\infty}^{\infty} \sum_{m_2=-\infty}^{\infty} g(m_1, m_2) \cdot C^W(n_1 - m_1, n_2 - m_2), \tag{1'}$$

имеющей вид функции Гаусса:

$$g(m_1, m_2) = \frac{1}{2\pi\sigma^2} exp\left\{-\frac{m_1^2 + m_2^2}{2\sigma^2}\right\}, \qquad m_1, m_2 \in (-\infty, \infty).$$

На практике свёртка с БИХ-фильтром (1') заменяется свёрткой с КИХ-фильтром (1), который описывается следующим выражением:

$$g(m_1, m_2) = K \cdot exp\left\{-\frac{(m_1 - M/2)^2 + (m_2 - M/2)^2}{2\sigma^2}\right\},$$

где M – размер окна, определяемый по правилу «трёх сигма»:

$$M = 2 \cdot \left[\frac{3\sigma}{2}\right] + 1, \tag{2}$$

($[x]$ – целая часть числа x), а коэффициент K находится из условия нормировки

$$\sum_{m_1=0}^{M-1}\sum_{m_2=0}^{M-1} g(m_1, m_2) = 1.$$

Параметром преобразования является значение σ.

6. *Повышение резкости* заключается в следующем преобразовании входного изображения

$$\widetilde{\mathrm{C^W}}(\mathrm{n_1},\mathrm{n_2}) = \mathrm{C^W}(\mathrm{n_1},\mathrm{n_2}) + q\left(\mathrm{C^W}(\mathrm{n_1},\mathrm{n_2}) - \mathrm{C^W_{smooth}}(\mathrm{n_1},\mathrm{n_2})\right),$$

где $\mathrm{C^W_{smooth}}$ – результат усреднения $\mathrm{C^W}$ в окне размерами $M \times M$ (искажение 4 текущего списка), а $q > 0$ – коэффициент усиления разностного изображения.

Параметрами преобразования являются M и q.

7. *Добавление псевдослучайного гауссовского белого шума* $\xi(n_1, n_2)$:

$$\widetilde{C^W}(n_1, n_2) = C^W(n_1, n_2) + \xi(n_1, n_2),$$

значения которого являются реализацией гауссовской случайной величины с плотностью распределения

$$\rho_\xi(x) = \frac{1}{\sqrt{2\pi D_\xi}} exp\left(-\frac{x^2}{2D_\xi}\right). \quad (3)$$

Параметром является дисперсия шума D_ξ.

8. *Медианная фильтрация* – это метод нелинейной обработки сигналов, очень полезный при подавлении аддитивного шума. Метод очень прост, не требует настройки (является непараметрическим) и поэтому получил широкое распространение. Медианный фильтр реализуется как процедура локальной обработки скользящим окном различной формы (в настоящей лабораторной работе предлагается использовать квадратное окно размерами $M \times M$), которое включает нечетное число отсчетов изображения: $M = 2p + 1$, $p \in \mathbb{N}$.

Процедура обработки заключается в том, что для каждого положения окна попавшие в него отсчеты упорядочиваются по возрастанию значений. Средний отсчет в этом упорядоченном списке называется *медианой* рассматриваемой группы. Эта медиана заменяет центральный отсчет в окне для обработанного сигнала.

Параметром является размер окна M.

9. *Сжатие JPEG с последующим восстановлением* заключается в сохранении носителя информации в формате JPEG и последующем восстановлении его в формате без потерь.

Параметром является показатель качества Q, изменяемый в пределах от 1 до 100.

2. Системы встраивания ЦВЗ

В данном разделе кратко описаны общие сведения о системах встраивания ЦВЗ в изображения, стойкость которых исследуется в настоящей лабораторной работе. Эти сведения приводятся по большей части для справки, носят упрощённый обзорный характер и зачастую не охватывают всех возможностей рассматриваемых систем. Описываемые системы не требуется реализовывать в рамках данной лабораторной работы, поскольку студентам предоставляются готовые исполняемые файлы, реализующие встраивание и излечение ЦВЗ, а также оценку близости встроенного и извлечённого ЦВЗ.

ЦВЗ-система Корви(Corvi)

В данной системе ЦВЗ представляет собой массив псевдослучайных чисел, распределенных по гауссовскому закону (3): $W \in \mathbb{R}^1_{[P\times P]}$, где $P = 32$, то есть 1024 числа.

Исходное изображение

$$C(n_1, n_2), \qquad n_1 = \overline{0..N_1 - 1}, \qquad n_2 = \overline{0..N_2 - 1}$$

подвергается вейвлет-преобразованию на такое число поддиапазонов, которое необходимо для получения низкочастотного изображения (в LL-поддиапазоне) размером $P \times P$:

$$f(m_1, m_2), \qquad m_1 = \overline{0..P - 1}, \qquad m_2 = \overline{0..P - 1}.$$

Для внедрения ЦВЗ отбираются все коэффициенты LL-поддиапазона. Встраивание информации в эти коэффициенты выполняется в соответствии с выражением

$$f^W(m_1, m_2) = f_{mean} + [f(m_1, m_2) - f_{mean}]\big(1 + \alpha W(m_1 \cdot P + m_2)\big),$$

где f_{mean} - среднее значение выборки коэффициентов.

Извлечение информации из принятого носителя информации $\widetilde{f^W}$ выполняется по формуле

$$\widetilde{W}(m_1 \cdot P + m_2) = \frac{\widetilde{f^W}(m_1, m_2) - f(m_1, m_2)}{\alpha(f(m_1, m_2) - f_{mean})}. \tag{4}$$

После извлечения $\widetilde{W}$ сравнивается с подлинным водяным знаком W. В качестве меры идентичности используется значение коэффициента корреляции последовательностей

$$\rho = \frac{\widetilde{W} \cdot W}{\|\widetilde{W}\| \cdot \|W\|} = \frac{\sum_{m=0}^{P-1} \widetilde{W}(m) W(m)}{\sqrt{\sum_{m=0}^{P-1} \widetilde{W}^2(m)} \cdot \sqrt{\sum_{m=0}^{P-1} W^2(m)}}. \tag{5}$$

Если значение $\rho > \tau$, где τ - некий порог, то детектор ЦВЗ срабатывает, в противном случае принимается заключение об отсутствии встроенного водяного знака W на изображении.

ЦВЗ-система Кокса (Cox)

В данной системе ЦВЗ представляет собой последовательность из $P = 1000$ псевдослучайных чисел, распределенных по гауссовскому закону (3). Для модификации отбираются 1000 самых больших коэффициентов глобального дискретного косинусного преобразования (ДКП) контейнера таким образом, как показано на рисунке 1.

DC-отсчёт $\mathrm{f}(0,0)$ остаётся без изменений. Остальные трансформанты разворачиваются в одномерную последовательность по змеевидной развёртке

$$\varphi(m) = \{(m_1, m_2)_m\}_0^{P-1},$$

и к первым 1000 из них производится добавление значений $W(m)$ по формуле

$$f^W\big(\varphi(m)\big) = f\big(\varphi(m)\big)\big(1 + \alpha W(m)\big),$$

а извлечение ЦВЗ – по обратной формуле

$$\widetilde{W}(m) = \frac{\widetilde{f^W}\big(\varphi(m)\big) - f\big(\varphi(m)\big)}{\alpha f\big(\varphi(m)\big)} \tag{6}$$

с последующим вычислением коэффициента корреляции (5).

Достоинством метода является то, что благодаря выбору наиболее значимых коэффициентов водяной знак является более стойким к сжатию и многим другим видам обработки сигнала. Вместе с

тем система уязвима для некоторых видов атак. Кроме того, к недостаткам данной системы стоит также отнести трудоёмкость операции вычисления двумерного ДКП всего изображения.

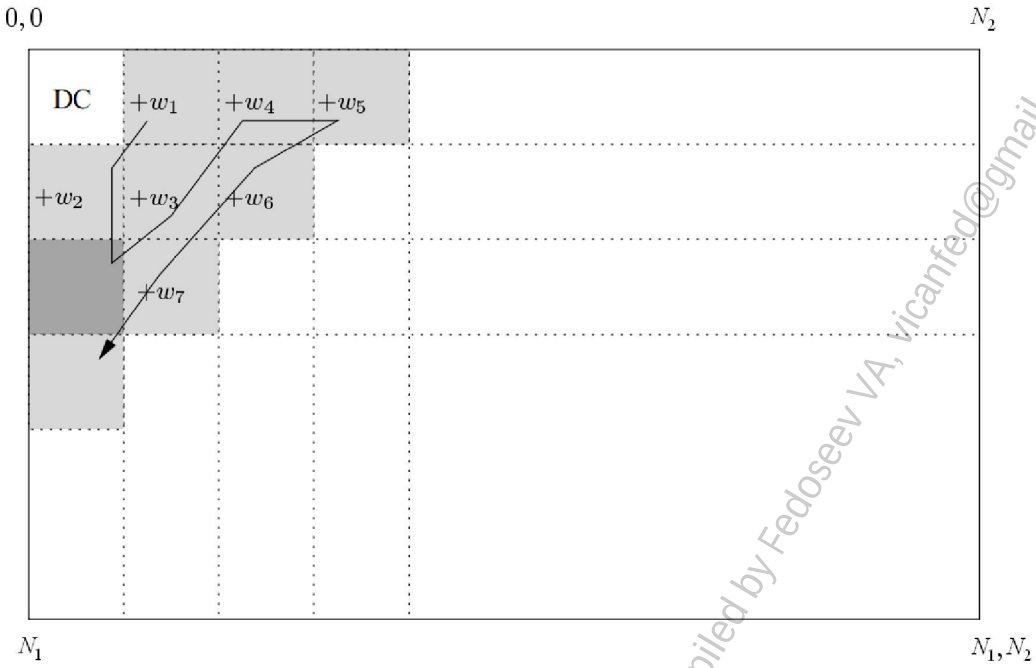


Рис. 1. Схема встраивания ЦВЗ алгоритмом Кокса

ЦВЗ-система Ванга (Wang)

В данной системе в роли ЦВЗ также выступает последовательность псевдослучайных действительных чисел $W(m)$, распределенных по гауссовскому закону (3), длина которой P является параметром системы. Каждое число $W(m)$ аддитивно внедряется в один коэффициент вейвлет-преобразования контейнера. Коэффициенты для встраивания выбираются из всех высокоуровневых поддиапазонов (см. рисунок 2) согласно определяемой при анализе контейнера последовательности

$$\varphi(m) = \{(m_1, m_2)_m\}_0^{P-1}.$$

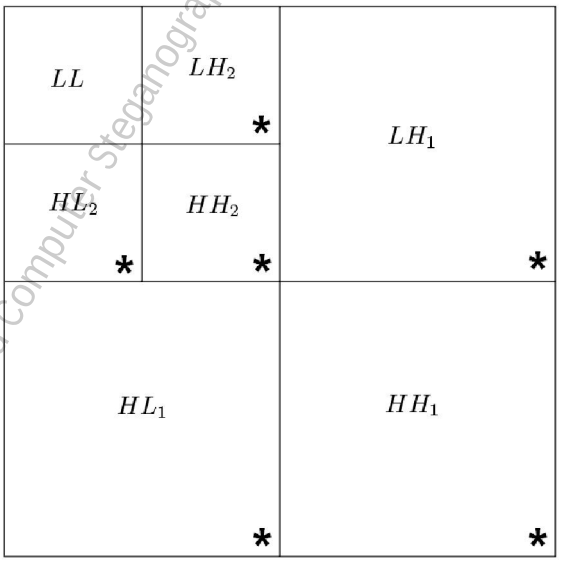


Рис. 2. Используемая в алгоритме Ванга декомпозиция исходных данных.

*Помеченные символом * поддиапазоны используются для встраивания ЦВЗ*

Собственно встраивание ЦВЗ выполняется по формуле

$$f^W\big(\varphi(m)\big) = f\big(\varphi(m)\big) + \alpha_s \cdot T_s \cdot W(m),$$

где s – порядковый номер поддиапазона, к которому относится $(\mathrm{m}_1, \mathrm{m}_2)_\mathrm{m}$, $\alpha_\mathrm{s} \in (0; 1]$ – множитель, управляющий соотношением между сигналом и ЦВЗ в носителе информации, $\mathrm{T_s}$ – пороговое значение для текущего поддиапазона, вычисленное при формировании последовательности $\varphi(\mathrm{m})$.

Извлечение в базовом варианте выполняется по обратной формуле

$$W(m) = \frac{\widetilde{f^W}\big(\varphi(m)\big) - f\big(\varphi(m)\big)}{\alpha_s \cdot T_s}$$

с последующим вычислением коэффициента корреляции (5). Существует также версия метода со слепым детектором, на которой мы не будем останавливаться.

Поиск вейвлет-коэффициентов для встраивания с формированием последовательности $\varphi(m)$ основан на принципах многопорогового вейвлет-кодера (MTWC) и состоит из трёх шагов:

1. На начальном этапе ни один из коэффициентов $\mathrm{f}(\mathrm{m}_1, \mathrm{m}_2)$ не выбран для встраивания. Для всех поддиапазонов, кроме LL, вычисляется первоначальное значение порога $\mathrm{T_s}$:

   $$T_{s,0} = \beta_s \cdot \frac{1}{2} \max_{(m_1,m_2)\in s} f(m_1, m_2),$$

   где β_s - весовой коэффициент поддиапазона, являющийся параметром системы.

2. Просматриваются все поддиапазоны в порядке убывания значений порога $\mathrm{T_s}$ и все пиксели в них в порядке построчной развёртки. Все положения (m_1, m_2) коэффициентов $\mathrm{f}(\mathrm{m}_1, \mathrm{m}_2)$, которые превышают порог, добавляются в последовательность φ, пока ее длина не превысила P.

3. Если текущее количество элементов φ меньше P, то уменьшаем вдвое пороги для всех поддиапазонов:

   $$T_{s,i+1} = \frac{1}{2} T_{s,i}$$

   и повторяем шаг 2.

Для большей защищённости системы встраивание можно выполнять не во все значимые коэффициенты, а в некоторые выбираемые в соответствии с ключом коэффициенты.

Задание

В лабораторной работе необходимо выполнить исследование устойчивости определённой вариантом системы встраивания ЦВЗ к нескольким искажениям, которые также задаются вариантом.

Встраивание, извлечение и сравнение ЦВЗ осуществляется при помощи поставляемой библиотеки исполняемых файлов. При исследовании метода Корви средствами данной библиотеки следует использовать параметр командной строки “-C”.

Искажения предлагается реализовывать средствами библиотек ResLook и/или IrfanView. Результаты сравнения встроенного и извлечённого ЦВЗ для каждого искажения и для каждого значения параметра необходимо привести в отчёте, оформив их в виде графиков.

Таблица параметров искажений

Преобразование	Кодовое имя	Параметр p	p_{min}	p_{max}	Δ_p
Линейное изменение динамического диапазона функции яркости	Contrast	Коэффициент α	0.7	1.3	0.1
Поворот с последующим восстановлением	Rotate	Угол поворота φ (в градусах)	0	40	8
Масштабирование	Scale	Коэффициент масштабирования	0.6	1.5	0.1
Медианная фильтрация	Median	Размер окна M	3	15	2
Усреднение в скользящем окне	Smooth	Размер окна M	3	15	2
Гауссовское размытие	Gauss	Параметр размытия σ	1	4	0.5
Повышение резкости	SharpenWin	Размер окна M; $q = \text{const} = 5$	3	15	2
Повышение резкости	SharpenQ	Коэф-т усиления q; $M = \text{const} = 5$	5	30	5
Добавление гауссовского шума	Noise	Дисперсия шума D_ξ	100	1000	100
JPEG-сжатие с последующим восстановлением	JPEG	Параметр качества Q	50	90	10

Таблица вариантов заданий[1]

№ варианта	Метод встраивания ЦВЗ	Список искажений
1	Corvi	Contrast, Smooth, JPEG
2	Cox	Contrast, Smooth, JPEG
3	Wang	Contrast, Smooth, JPEG
4	Corvi	Scale, Noise, Median
5	Cox	Scale, Noise, Median
6	Wang	Scale, Noise, Median
7	Corvi	Rotate, Gauss, JPEG, SharpenWin
8	Cox	Rotate, Gauss, JPEG, SharpenWin
9	Wang	Rotate, Gauss, JPEG, SharpenWin
10	Corvi	Rotate, Gauss, Noise, Median, SharpenQ
11	Cox	Rotate, Gauss, Noise, Median, SharpenQ
12	Wang	Rotate, Gauss, Noise, Median, SharpenQ

[1] Зелёным цветом помечены более сложные варианты, голубым более лёгкие, белым – средние. Варианты отсортированы в порядке усложнения задания (впрочем, относительная сложность – понятие субъективное☺).

Контрольные вопросы

1. Классификация систем встраивания информации по стойкости.
2. Как на практике могут применяться стойкие системы ЦВЗ?
3. Как на практике могут применяться полухрупкие системы ЦВЗ?
4. Опишите основные этапы при сжатии JPEG. На каких из них возникает потеря информации?
5. Опишите принцип медианной фильтрации изображения. Сравните эффективность её применения с усреднением в скользящем окне для устранения шума типа «соль и перец».
6. Опишите процедуру гауссовского размытия изображения и способ выбора окна фильтра.
7. Опишите смысл и существо процедуры повышения резкости.
8. Перечислите (и при необходимости кратко опишите) основные виды искажений, применяемых к носителю информации для исследования стойкости системы.
9. Охарактеризуйте алгоритм Corvi по типам встраивания и извлечения информации, перечислите его основные особенности.
10. Охарактеризуйте алгоритм Cox по типам встраивания и извлечения информации, перечислите его основные особенности.
11. Охарактеризуйте алгоритм Wang по типам встраивания и извлечения информации, перечислите его основные особенности.

Вопросы к экзамену по курсу «Компьютерная стеганография»

Часть I. Системы встраивания информации (СВИ). Особенности человеческого восприятия сигналов

1. Стеганография, стегосистема. Классическая стеганография. ЦВЗ-системы. Системы встраивания информации (СВИ). Компьютерная стеганография.
2. Текстовая стеганография. Примеры
3. Применение СВИ. Цели атак на СВИ. Требования по защищённости СВИ к различным видам атак в зависимости от назначения
4. Основные компоненты СВИ. Обобщённая схема СВИ
5. Основные компоненты СВИ. Детализированные схемы составных процессов встраивания и извлечения информации в СВИ
6. Свойства систем встраивания информации
7. Непрерывные и дискретные изображения. Цветовые пространства. Восприятие цвета зрительной системой человека
8. Восприятие контраста зрительной системой человека. Эксперименты 1: закон Вебера.
9. Эксперимент 2: восприятие синусоидального сигнала. Функция контрастной чувствительности
10. Эффект маскировки в изображениях. Эксперимент 3
11. Эффект маскировки в видео. Эксперимент 4
12. Метрики качества изображений
13. Особенности представления звуковых сигналов и их восприятие человеком. Частотное и временное маскирование
14. Метрики качества звука
15. Этап преобразования контейнера в пространство признаков при встраивании информации. Встраивание информации в пространственной области
16. Схема кодирования с преобразованием. Дискретное преобразование Карунена-Лоэва
17. Примеры дискретных спектральных преобразований и их особенности
18. Преобразование Фурье-Меллина
19. Преобразование изображения при сжатии его в формате JPEG

Часть II. Системы встраивания информации

20. Встраивание информации за счёт переквантования функции яркости. Общая концепция методов QIM. Встраивание информации в наименее значимые биты (НЗБ) как частный случай QIM
21. Аддитивное и мультипликативное встраивание. Алгоритм PatchWork. Формальное поэтапное описание алгоритма PatchWork. Характеристики алгоритма PatchWork
22. Алгоритм Cox. Неслепой детектор при аддитивном или мультипликативном встраивании информации. Характеристики алгоритма Cox
23. Алгоритм Barni. Слепой детектор при аддитивном или мультипликативном встраивании информации. Характеристики алгоритма Barni
24. Концепция информированного встраивания. Алгоритм Koch. Алгоритм Benham. Их характеристики
25. Видимые ЦВЗ. Простейший алгоритм встраивания видимого ЦВЗ в пространственной области. Видимые ЦВЗ в области преобразования: алгоритм Канканхалли. Характеристики алгоритма Канканхалли
26. Стойкие ЦВЗ. Их назначение. Способы обеспечения стойкости ЦВЗ к геометрическим искажениям. ЦВЗ в области преобразования Фурье-Меллина. Алгоритм Zheng. Его характеристики
27. Стойкие ЦВЗ. Их назначение. Способы обеспечения стойкости ЦВЗ к геометрическим искажениям. Понятие характеристических точек и их использование для стойких ЦВЗ-систем. Алгоритмы Zhao и Deng. Их характеристики
28. Хрупкие ЦВЗ. Их назначение. Базовый алгоритм QIM и его подвиды. Использование методов группы QIM в качестве основы для хрупких СВИ

29. Полутоновые и бинарные изображения. Методы растрирования изображений. Метод диффузии ошибки. Два подхода к встраиванию информации в бинарные изображения
30. Непосредственное встраивание информации в бинарный контейнер. Методы встраивания DHST и DHSPT. Характеристики любого из них
31. Встраивание информации при растрировании полутоновых изображений. Алгоритм DHCED. Его характеристики
32. Встраивание информации в НЗБ звуковых сигналов. Алгоритм Cvejic. Его характеристики
33. Встраивание информации в звук путём модификации фазы сигнала (алгоритм Bender - 1). Его характеристики
34. Встраивание информации в звук за счёт встраивания эхо-сигнала (алгоритм Bender -2). Его характеристики
35. Особенности применения и требования при проектировании СВИ для видеосигналов. Способы защиты DVD-дисков
36. Задача мониторинга видеовещания. Алгоритм JAWS. Его характеристики
37. Алгоритм Hartung & Girod для передачи информации в видеосигналах. Его характеристики
38. Задача стегоанализа. Методы статистического стегоанализа НЗБ-систем

Ассистент кафедры ГИиИБ Федосеев В.А.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»
(СГАУ)

СОГЛАСОВАНО

Управление образовательных программ

_____/ А.В. Дорошин /

"_____"_____ 20___ г.

УТВЕРЖДАЮ

Проректор по учебной работе

_____/ Ф.В. Гречников /

"____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование модуля (дисциплины)

Компьютерная стеганография

Цикл, в рамках которого происходит освоение модуля (дисциплины)	Дисциплины по выбору
Часть цикла	С3.ДВ2.1

Код учебного плана

090303.2.65-2011-О-П-5г00м

Факультет	информатики
Кафедра	геоинформатики и информационной безопасности
Курс	5
Семестр	9
Лекции (СЛ)	36
Семинарские и практические занятия (СП)	0
Лабораторные занятия (СЛР)	36
Контроль самостоятельной работы / Индивидуальные занятия (КСР / ИЗ)	0
Самостоятельная работа (СРС)	36
Всего (Всего с экзаменами)	108

Экзамен -

Зачет 9

Согласовано: ФЛА

Наименование стандарта, на основании которого составлена рабочая программа:

Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090303 «Информационная безопасность автоматизированных систем»

Соответствие содержания рабочей программы, условий ее реализации, материально-технической и учебно-методической обеспеченности учебного процесса по дисциплине всем требованиям государственных стандартов подтверждаем.

Составители:

Федосеев В.А. _____
(подпись)

Заведующий кафедрой:

д.т.н., проф. Сергеев В.В. _____
(подпись)

Рабочая программа обсуждена на заседании кафедры

геоинформатики и информационной безопасности

Протокол №___ от "____" _____ 20___ г.

Наличие основной литературы в фондах научно-технической библиотеки (НТБ) подтверждаем:

Директор НТБ _____ /_____/
(подпись) (расшифровка подписи)

Согласовано:

Декан _____ /_____/
(подпись) (расшифровка подписи)

1 Цели и задачи модуля (дисциплины), требования к уровню освоения содержания

1.1 Перечень развиваемых компетенций

Развиваемые общекультурные компетенции (ОК):
- способность логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-7);
- способность к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания (ОК-9).
Развиваемые профессиональные компетенции (ПК):
общепрофессиональные:
- способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (ПК-1);
- способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (ПК-2);
- способность использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3);
- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);
- способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);в научно - исследовательской деятельности:
- способность применять современные методы исследования с использованием компьютерных технологий (ПК-10);
- способность проводить анализ защищенности автоматизированных систем (ПК-12);
в проектно-конструкторской деятельности:
- способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17);в контрольно-аналитической деятельности:
- способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем (ПК-24);
в организационно-управленческой деятельности:
- способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34).

1.2 Цели и задачи изучения модуля (дисциплины)

Целью дисциплины является наделение студентов знаниями и практическими навыками по разработке математических методов, алгоритмов и программных средств для решения задач скрытой передачи данных, защиты информации с использованием цифровых водяных знаков, а также стеганографического анализа.

В процессе изучения курса студенты должны получить необходимые сведения об основных методах построения систем встраивания информации и атаках на системы этого рода, научиться правильно выбирать стеганографические средства защиты и передачи информации с учётом предъявляемых требований к стойкости систем и их вычислительной сложности.

1.3 Требования к уровню подготовки студента, завершившего изучение данного модуля (дисциплины)

Специалисты, завершившие изучение данной дисциплины, должны знать:
- принципы построения систем встраивания информации;
- особенности человеческого восприятия зрительной и звуковой информации;
- базовые методы защиты цифровых сигналов при помощи цифровых водяных знаков;
- базовые методы и протоколы скрытой передачи информации;
- характеристики систем встраивания информации;
- методы исследования стойкости систем встраивания информации к искажениям в канале передачи данных;
- базовые методы стегоанализа цифровых изображений.

Специалисты, завершившие изучение данной дисциплины, должны уметь:
- изучать новые научные результаты и научную литературу в областях компьютерной стеганографии и цифровых водяных знаков
- применять наукоемкие технологии и пакеты программ для решения задач скрытой передачи информации и защиты информации при помощи цифровых водяных знаков;
- проектировать и применять атаки на системы скрытой передачи данных.

1.4 Связь с предшествующими модулями (дисциплинами)

Курс базируется на знаниях студентов, полученных при изучении следующих дисциплин:
- математический анализ (МА);
- дискретная математика (ДМ);
- теория вероятностей и математическая статистика (ТВиМС);
- теория информации (ТИ);
- физика (Ф);
- языки программирования (ЯП);
- основы информационной безопасности (ОИБ);
- операционные системы (ОИ);
- теория цифровой обработки сигналов и изображений (ТЦОС);
- криптографические методы защиты информации (КМЗИ);
- методы передачи и анализа изображений (МПиАИ).

1.5 Связь с последующими модулями (дисциплинами)

Знания, полученные студентами в рамках настоящего курса, используются при выполнении ими выпускной квалификационной работы (ВКР) специалиста.

2 Содержание рабочей программы (модуля)

Семестр 1		

СЛ 0,3333 36 часов 0,9999 ЗЕТ	Активные 0	
	Интерактивные 0	
	Традиционные 1	Введение в системы встраивания информации: понятие о стеганографии и стеганографических системах, цифровые водяные знаки; компьютерная стеганография; текстовая стеганография; применение систем встраивания информации; основные компоненты систем встраивания
		Особенности восприятия и маскировки изображений: цифровое представление изображений, цветовые пространства, восприятие цвета системой человеческого зрения; восприятие контраста системой человеческого зрения, закон Вебера, эксперимент Вебера, функция контр
		Особенности восприятия и маскировки звука: звук, давление звука, слышимые звуки; цифровое представление звукового сигнала; особенности восприятия звука человеком, частотное маскирование, временное маскирование; метрики качества звука.
		Характеристики систем встраивания информации: слепое и информированное встраивание, детектор и декодер; методы отображения контейнера в пространство признаков; способы модификации контейнера; емкость контейнера.
		Методы встраивания информации в изображения: встраивание информации в пространственной области, встраивание информации в наименее значимые биты; аддитивное и мультипликативное встраивание, алгоритм PatchWork; встраивание информации с расширением спектра,

		Методы встраивания информации в звуковые и видеосигналы: встраивание информации в наименее значимые биты звуковых сигналов, алгоритм Cvejic; встраивание информации в звуковые сигналы путём модификации фазы; встраивание информации в звуковые сигналы за счё
		Стойкость систем встраивания информации к искажениям в канале передачи данных: типы устойчивости систем встраивания информации к искажениям в канале передачи данных, применимость систем каждого из типов; виды возможных искажений в канале передачи данных,
		Стеганографическая стойкость и методы стегоанализа: понятие стеганографической стойкости; виды атак на системы встраивания информации; стегоанализ, статистический стегоанализ, стегоанализ полиграфических изображений.
СП 0 0 часов 0 ЗЕТ	Активные 0	
	Интерактивные 0	
	Традиционные 1	
СЛР 0,3333 36 часов 0,9999 ЗЕТ	Активные 0	
	Интерактивные 1	Встраивание информации в полутоновые изображения в пространственной области
		Встраивание информации в бинарные изображения
		Исследование стойкости систем встраивания информации к искажениям контейнера
		Статистический стегоанализ систем встраивания информации
	Традиционные 0	
КСР 0 0 часов 0 ЗЕТ	Активные 0	
	Интерактивные 0	
	Традиционные 0	

СРС 0,3333 36 часов 0,9999 ЗЕТ	Активные 0	Конечномерные ассоциативные алгебры
		Совмещенные алгоритмы дискретных ортогональных преобразований
		Двумерные БПФ с представлением данных в алгебре (2x2)-матриц
		Кватернионное двумерное ДПФ, совмещенные алгоритмы дискретного косинусного преобразования
		Представление данных в круговых кодах, алгоритмы дискретных ортогональных преобразований, реализуемые в кодах Гамильтона-Эйзенштейна
		Алгоритмы дискретного косинусного преобразования коротких длин
		Унифицированный метрический подход к синтезу быстрых алгоритмов многомерного ДПФ
		Альтернативная интерпретация редукции Кули-Тьюки
		Алгоритмы двумерного ДПФ с покоординатным прореживанием области суммирования
		"Чесс-алгоритмы" двумерного ДПФ
		Интерпретация алгоритмов двумерного ДПФ как алгоритмов с расщеплением основания нецелого порядка (6 час) Алгоритмы двумерного ДПФ с "мультипокрытиями" области суммирования
	Интерактивные 0	
	Традиционные 1	Ознакомление с программно-инструментальной системой ResLook
		Изучение методов встраивания данных в полутоновые изображения в пространственной области
		Изучение методов встраивания данных в бинарные изображения
		Освоение методов исследования устойчивости систем встраивания информации к искажениям в канале передачи данных
		Знакомство с методами стегоанализа

3 Инновационные методы обучения

Лабораторные работы выполняются на ПЭВМ с использованием среды разработки программного обеспечения Microsoft Visual Studio 2008, а также программно-инструментальной системы ResLook.
Использование современных программных и технических средств представления материала (презентации PowerPoint и Beamer, проектор) для изложения материалов лекций.
Предоставление доступа к сети Internet для самостоятельной работы по поиску и изучению дополнительного материала.

4 Технические средства и материальное обеспечение учебного процесса

Компьютерный класс кафедры геоинформатики и информационной безопасности, используемый при проведении лабораторных занятий.
Проектор, предназначенный для демонстрации материалов лекционных занятий.
Лекционные демонстрации: методы встраивания цифровых водяных знаков в бинарные изображения, устойчивость стеганографических систем, стеганографические методы защиты полиграфической продукции и др.
Компьютерные программы для выполнения лабораторных работ: модули программно-инструментальной системы ResLook и средство для просмотра и анализа изображений Visualizer.
Среда разработки программного обеспечения Microsoft Visual Studio 2008 для самостоятельной реализации и исследования стеганографических алгоритмов и методов стегоанализа.

5 Учебно-методическое обеспечение

5.1 Основная литература

Методы компьютерной обработки изображений / под редакцией В.А.Сойфера. – М.: Физматлит, издание второе, 2003. – 784 с. (98 экземпляров)

5.2 Дополнительная литература

Сойфер В.А., Сергеев В.В., Попов С.П., Мясников В.В. Теоретические основы цифровой обработки изображений. Учебное пособие. – Самарский государственный аэрокосмический университет имени академика С.П.Королева. Самара, 2000. – 256 с. (58 экземпляров)
Бабаш, Александр Владимирович. Криптография / А. В. Бабаш, Г. П. Шанкин ; под ред. В. П. Шерстюка, Э. А. Применко. - М. : СОЛОН-Пресс, 2007. - 511 с.
Информационная безопасность систем организационного управления : теорет. основы : в 2 т. / [Н. А. Кузнецов, В. В. Кульба, Е. А. Микрин и др.] ; под ред. Н. А. Кузнецова, В. В. Кульбы ; Рос. акад. наук, Ин-т пробл. передачи информации. - М. : Наука . - 200
Логачев О. А. Булевы функции в теории кодирования и криптологии : к изучению дисциплины / Логачев О. А., Сальников А. А., Ященко В. В. ; Ин-т проблем информ. безопасности МГУ. - М. : МЦНМО, 2004. - 469 с. - (Информационная безопасность: криптография)

5.3 Электронные источники и интернет ресурсы

http://www.des-crypto.ru/stegano/
http://st.ess.ru/publications/articles/steganos/steganos.htm
http://ru.wikipedia.org/wiki/Стеганография

5.4 Методические указания и рекомендации

Текущий контроль знаний студентов в девятом семестре завершается на отчетном занятии, результатом которого является допуск или недопуск студента к экзамену по дисциплине. Основанием для допуска к экзамену является выполнение и отчет студента по всем лабор
Промежуточный контроль знаний студентов проводится в девятом семестре в виде экзамена. Экзамен проводится согласно положению о текущем и промежуточном контроле знаний студентов, утвержденном ректором института. Экзаменационная оценка ставится на основании