МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Самарский национальный исследовательский университет имени
академика С.П. Королева» (Самарский университет)

В.А. Федосеев, В.А. Митекин

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СТЕГАНОГРАФИИ И ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Самара
Издательство Самарского университета
2017

УДК 004.056(075)
ББК 32.97я7
Ф338

Рецензенты: доцент кафедры систем связи ПГУТИ, к.т.н., доцент *М.В. Кузнецов*;
проф. каф. технической кибернетики Самарского университета, д.т.н., доцент *А.Г. Храмов*

Федосеев, Виктор Андреевич
Ф338 **Теоретические основы стеганографии и цифровых водяных знаков: учеб. пособие** / В.А. Федосеев, В.А. Митекин. – Самара: Самарский университет, 2017. – 132 с.

ISBN 978-5-7883-1130-2

Учебное пособие посвящено изучению базовых методов защиты информации с помощью цифровых водяных знаков, методов цифровой стеганографии (то есть передачи скрытых сообщений внутри цифровых контейнеров), а также методов противодействия системам, реализующим подобные методы.

Пособие предназначено для студентов направления «Информационная безопасность автоматизированных систем».

УДК 004.056(075)
ББК 32.97я7

ISBN 978-5-7883-1130-2

Оглавление

Указатель рассмотренных систем встраивания информации

Список сокращений

ДВП	–	Дискретное вейвлет-преобразование
ДКП	–	Дискретное косинусное преобразование
ДОП	–	Дискретное ортогональное преобразование
ДПФ	–	Дискретное преобразование Фурье
НЗБ	–	Наименее значимые биты
НЗБ-встраивание	–	Встраивание в наименее значимые биты
НЗБП	–	Наименее значимая битовая плоскость
СВИ	–	Система встраивания информации
ЦВЗ	–	Цифровой водяной знак

Список обозначений

Основные обозначения

$\mathbb{N}$	–	Множество натуральных чисел
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$	–	Множество целых неотрицательных чисел
$\mathbb{B}^n = \mathbb{N}_0 \cap [0, 2^n - 1]$	–	Множество целых неотрицательных чисел, для хранения которых достаточно n бит
$\mathbb{B} = \mathbb{B}^1$	–	Множество, элементы которого равны 0 или 1
$\mathbb{Z}$	–	Множество целых чисел
$\mathbb{R}$	–	Множество действительных чисел
$\mathbb{C}$	–	Множество комплексных чисел
$\mathbb{S}^m_{[N_1 \times N_2 \times \ldots \times N_m]}$	–	m-мерная матрица размерами $N_1 \times N_2 \times \ldots \times N_m$ из элементов некоторого множества $\mathbb{S}$
$\mathbb{S}^m_{[]}$	–	m-мерная матрица некоторого размера из элементов некоторого множества $\mathbb{S}$ (употребляется, когда размеры матрицы не важны в рассматриваемом контексте)
$\mathbb{X}^m_{[]}$, где $\mathbb{X} \subseteq \mathbb{R}$	–	Множество цифровых сигналов
$\mathbb{Y}^l_{[]}$, где $\mathbb{Y} \subseteq \mathbb{C}$	–	Множество матриц признаков цифровых сигналов

Обозначения данных в системах встраивания информации

Обозначение	Множество значений	Название	Употребимые эквиваленты в англоязычной литературе
$\mathbf{b}$	$\mathbb{B}^1_{[N_b]}$	Встраиваемая информация	Secret message, watermarking code
$\mathbf{b}^{\mathbf{R}}$	$\mathbb{B}^1_{[N_b]}$	Извлечённая информация	Recovered {название $\mathbf{b}$}
C	$\mathbb{X}^m_{[]}$	Контейнер	Host asset, container
C^W	$\mathbb{X}^m_{[]}$	Носитель информации	Watermarked asset, cover
$\widetilde{C^W}$	$\mathbb{X}^m_{[]}$	Принятый носитель информации	Transformed watermarked asset
f	$\mathbb{Y}^l_{[]}$	Матрица признаков контейнера	–
f^W	$\mathbb{Y}^l_{[]}$	Матрица признаков носителя информации	–
$\widetilde{f^W}$	$\mathbb{Y}^l_{[]}$	Матрица признаков принятого носителя информации	–
$\mathbf{k}$		Секретный или составной ключ СВИ	–
W	$\mathbb{X}^m_{[]}$	Встраиваемый сигнал	Watermarking message (signal), encoded message
W^R	$\mathbb{X}^m_{[]}$	Извлечённый сигнал	Recovered {название W}
ξ	$\mathbb{B}$	Результат обнаружения	Detection result
Ω	$\mathbb{Y}^l_{[]}$	Матрица признаков встраиваемой информации	–
$\tilde{\Omega}$	$\mathbb{Y}^l_{[]}$	Матрица признаков извлечённой информации	–

Предисловие

Настоящее учебное пособие содержит теоретический материал, посвящённый методам защиты информации с помощью цифровых водяных знаков, методам цифровой стеганографии (то есть передачи скрытых сообщений внутри цифровых контейнеров), а также методам противодействия системам, реализующим подобные методы.

Тематика пособия относится к весьма популярному направлению информатики, именуемому в англоязычной литературе термином “Information Hiding” и методологически находящемуся на стыке цифровой обработки сигналов и изображений и информационной безопасности.

Содержание пособия во многом основано на лекциях, читаемых одним из авторов пособия на протяжении нескольких лет студентам Самарского университета, обучающимся по направлению «Информационная безопасность автоматизированных систем». Помимо преподавательского опыта, авторы при написании пособия использовали свой более чем 10-летний опыт научно-исследовательской работы в описываемой области информатики.

При написании настоящего пособия использовались в основном книги [1, 2] и конспекты авторских лекций. Все материалы, заимствованные из сторонних источников, сопровождаются ссылками на оригинал. Изображения, приведённые в качестве иллюстраций, взяты из стандартного репозитория [3] Университета Ватерлоо.

Пособие подготовлено при поддержке государственного задания вузу №2014/198, код проекта 2298 (главы 2–4), а также грантов Президента Российской Федерации молодым учёным МК-4506.2015.9 (глава 1) и МК-1907.2017.9 (параграф 3.5).

1. Теоретические основы встраивания информации

1.1. Введение в стеганографию и цифровые водяные знаки

Стеганографией (англ. Steganography, от греч. стегос — скрытый и графо — пишу, буквально «тайнопись») мы будем называть науку о защищённой передаче информации, осуществляемой путём сокрытия самого факта передачи информации.

В отличие от *криптографии*, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт существования канала передачи информации.

По аналогии с определением стеганографии можно определить и понятие *стеганографической системы* (или коротко «*стегосистемы*», англ. steganographic system). Под этим термином мы будем понимать совокупность методов и средств, предназначенных для создания канала защищённой передачи информации, осуществляемой путём сокрытия самого факта передачи информации.

На рис. 1.1 выделены основные направления стеганографии, которые будут рассмотрены в последующих подразделах.

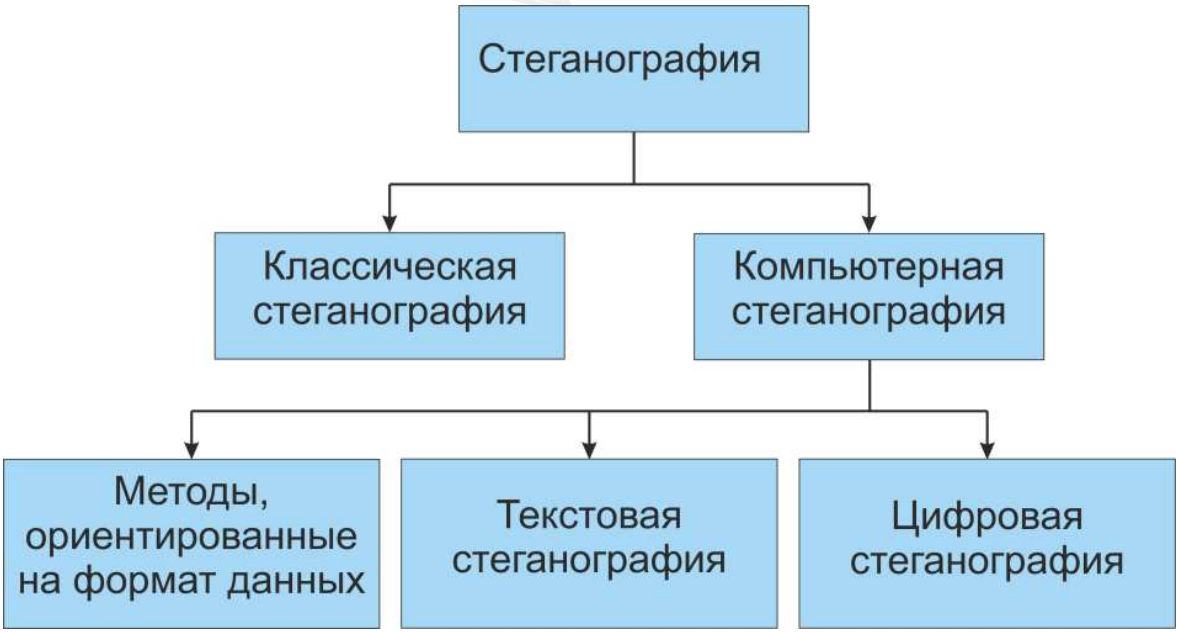


Рис. 1.1 – Основные направления стеганографии

1.1.1. Классическая стеганография

К классической стеганографии принято относить все примеры скрытой передачи информации в докомпьютерную эру, то есть такие, в которых компьютер не требуется ни до, ни после, ни во время передачи информации. В литературе [4, 5] и ряде интернет-источников [6, 7, 8] описано множество исторических примеров использования методов классической стеганографии.

Так, первое упоминание о стеганографических приёмах в литературе приписывается Геродоту, который описал случай передачи сообщений посредством восковых дощечек. В отличие от традиционного использования (нанесения текста на воске) скрытый текст наносился непосредственно на дощечке, после чего покрывался воском, становясь незаметным. 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, раба отправляли с посланием. Очевидно, скорость и пропускная способность подобного «канала передачи данных» были не на высоте. В Китае же люди оказались ещё более изощрёнными: для сокрытия сообщений шёлковые полоски с текстом письма сворачивались в шарики, покрывались воском и затем глотались посыльными. Ещё одним примером классической стеганографии является акростих.

Исторически большое распространение получили симпатические чернила для секретной переписки, которые проявлялись при определённом физическом или химическом воздействии на письмо. Так, ещё 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 скрытого текста молоко, проявляющееся после присыпания его порошком из сажи. В более поздние времена члены тайной организации «Чёрный передел» использовали в переписке чернила из раствора медного купороса. Проявлялся написанный такими чернилами текст под воздействием паров нашатырного спирта.

Со времён Первой мировой войны над составами симпатических чернил, равно как и над методами их проявления, активно трудились химики противоборствующих сторон. Однако, в конечном счёте защищённость подобной системы определялась лишь секретностью химического состава чернил. Как только противник восстанавливал секретную формулу,

дальнейшее проявление оставалось лишь вопросом времени. Иными словами, сокрытие информации методами классической стеганографии являлось возможным лишь благодаря тому, что противнику неизвестен метод сокрытия информации. Между тем, еще в 1883 году голландцем Огюстом Керкгоффсом был сформулирован известный принцип, названный впоследствии его именем, который гласит:

«Система защиты информации должна обеспечивать свои функции даже при полной информированности противника о её структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемых сведений должна заключаться в секретном ключе, то есть в предварительно (как правило) разделенном между адресатами фрагменте информации» [9].

Согласно этому принципу, рассмотренные выше примеры классических стегосистем не могли служить надёжными средствами защиты информации, и на смену им с началом компьютерной эры пришли методы компьютерной стеганографии.

1.1.2. Компьютерная стеганография. Методы, ориентированные на формат данных

Компьютерная стеганография — это раздел стеганографии, изучающий системы скрытой передачи информации, в которых в качестве контейнера и сообщения выступают аппаратное или программное обеспечение компьютера или цифровые данные, которые он хранит и обрабатывает.

Расцвет компьютерной стеганографии пришёлся на период, последовавший за массовым распространением персональных компьютеров и их внедрением во многие сферы жизни, то есть на 90-е годы XX века, однако некоторые авторы отмечают примеры использования компьютерных методов стеганографии ещё во времена холодной войны [10].

В настоящее время выделяют следующие основные положения современной компьютерной стеганографии:

1. Методы скрытия должны обеспечивать целостность файла.
2. Предполагается, что противнику полностью известны возможные стеганографические методы (согласно принципу Керкгоффса).
3. 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 рис. 1.1 показаны три основных направления компьютерной стеганографии: методы текстовой стеганографии, методы цифровой стеганографии и методы, ориентированные на формат данных. Последняя категория включает методы, использующие для встраивания информации специфические области памяти или особенности определённых операционных, файловых систем, форматов файлов, физических носителей и пр.

Соответственно, для других носителей, операционных систем, форматов представления данных нужны будут другие методы.

Приведём несколько примеров этой группы методов [11]:

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. Недостаток: возможность передачи лишь 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 широко используемой в настоящее время файловой системе NTFS стандартный размер кластера составляет 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ информации, из которых 3 КБ ни на что не используются — значит, их можно использовать для передачи секретной информации. Недостаток данного метода – лёгкость обнаружения информации.

Выделим основные общие недостатки данной группы методов:

1. Физическое (на уровне областей памяти) разделение полезной информации и секретного сообщения, приводящее к тому, что последнее может быть легко обнаружено, прочитано или удалено.
2. Эти методы не универсальны, а адаптированы под использование конкретных программно-аппаратных средств. Следствием этого может стать удаление секретной информации при изменении используемых средств, а также необходимость разработки новых методов для новой программно-аппаратной платформы.

Эти недостатки являются причиной того, что подобные методы не получили достаточного распространения на практике. Поэтому, а также

ввиду их специфичности, мы не будем останавливаться на них подробнее в рамках данного издания.

1.1.3. Текстовая стеганография

К *текстовой стеганографии* принято относить все методы, в которых встраивание секретной информации осуществляется в содержимое текстового файла.

Приведём некоторые примеры методов текстовой стеганографии [12].

1. Методы, использующие смещения слов, предложений, абзацев. Они 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. Метод крайне прост, однако его применение на практике порождает массу неудобств. В частности, оформление текста становится неряшливым, что позволяет легко заподозрить в нем наличие стеганографического встраивания. Более того, встроенная информация легко может быть удалена даже средствами простейших текстовых редакторов.
   - Метод 2: изменение порядка следования маркеров конца строки CR/LF. В данном методе используется 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. Этот метод менее заметен, чем предыдущий (хотя программно обнаружить его не составит труда), однако уступает ему по *ёмкости* скрытого канала, то есть соотношению объёма скрытой информации к длине открыто передаваемого текста.
   - Метод 3 (хвостовых пробелов) заключается в дописывании в конце коротких строк (предварительно заданной длины) от 0 до 15 пробелов, кодирующих значение полубайта. Как и в предыдущих методах, информацию, встроенную таким образом, легко обнаружить и удалить.
2. Метод выбора определенных позиций букв (также известен под названием нулевой шифр). Акростих – частный случай этого мето-

да, при котором начальные буквы каждой строки образуют скрытое сообщение. Данный метод сложнее поддаётся обнаружению по сравнению с предыдущими. Однако для эффективного использования даного метода текстовый контейнер должен быть согласован с ключом, определяющим позиции букв. На практике добиться этого достаточно трудно.

3. Метод использования символов другого языка, совпадающих по начертанию. Данный метод позволяет добиться, пожалуй, наибольшей ёмкости среди рассмотренных, однако скрытое сообщение легко может быть обнаружено и удалено при знании используемого алгоритма замены символов.
4. Метод, использующий таблицу синонимов. Наиболее интересный метод рассматриваемого класса, поскольку он достаточно сложно поддаётся обнаружению. На предварительном этапе (до начала использования метода) формируется таблица синонимов. Выбор того или иного варианта слов из данной таблицы означает встраивание бита (или нескольких бит информации). Например, праздник может кодировать бит 0, торжество — 1; бегемот – 0, гиппопотам – 1 и т.д. При встраивании информации в тексте-контейнере производится поиск слов из таблицы синонимов. Далее происходит встраивание – каждое найденное слово заменяется на нужный синоним в соответствии с очередным по счёту битом встраиваемой информации. При тщательном подборе таблицы синонимов текст сохраняет осмысленность. Разумеется, дополнительную сложность в реализации данного метода представляет собой склонение заменяемых слов.

В работе [12] выполнено сравнение некоторых методов текстовой стеганографии по ёмкости. Для исследования использовался ASCII-текст объёмом около 128 Кбайт. Результаты исследования, отражённые в табл. 1.1, показывают, что наибольший объём данных можно встроить при помощи использования разных символов, имеющих одинаковое начертание.

Говоря о достоинствах и недостатках рассмотренных методов текстовой стеганографии в целом, следует отметить их относительную простоту. Однако её обратной стороной являются недостаточная защищённость, а также низкая пропускная способность. И если первый недостаток может быть исправлен за счёт использования более совершенных методов, то второе ограничение является неустранимым. Поэтому в основном в каче-

стве контейнера для скрытой передачи информации используют данные, обладающие большей избыточностью, нежели текстовые. К таковым в первую очередь можно отнести изображения, звуковые и видеосигналы.

Табл. 1.1 – Результаты эксперимента по сравнению объёма встроенной информации для разных методов текстовой стеганографии [12]

Метод	Объём сообщения, бит / символ × 100%
Лишние пробелы	0,32
Чередование маркеров конца строки	0,21
Хвостовые пробелы	0,85
Знаки одинакового начертания	3,21

1.1.4. Цифровая стеганография и цифровые водяные знаки

В методах *цифровой стеганографии* встраивание секретного сообщения осуществляется в одномерные или многомерные цифровые сигналы (мультимедиа), имеющие физическую природу. К таким сигналам мы будем относить цифровые изображения, звуковые файлы и видеофайлы.

Важным отличием от методов, ориентированных на формат данных, является то, что они не используют особенностей конкретного формата представления информации, поскольку встраивание осуществляется за счёт изменения содержимого самого сигнала, а не каких-либо специальных полей. При встраивании информации учитываются особенности человеческого зрения и слуха, за счёт чего может быть достигнута незаметность встроенной информации.

В тесной связи с цифровой стеганографией находятся вопросы, связанные с так называемыми цифровыми водяными знаками (ЦВЗ).

Встраиванием ЦВЗ (Digital Watermarking) называется процесс внедрения в цифровой сигнал (как заметного, так и незаметного) информации, имеющей некоторое отношение к этому цифровому сигналу. *Цифровым водяным знаком* называется собственно внедряемая информация. Примером такой информации может быть идентификатор автора, предназначенный для защиты авторских прав на аудиовизуальное произведение, или электронная цифровая подпись, подтверждающая аутентичность цифровой мультимедийной информации.

Системой встраивания ЦВЗ (Watermarking system, система ЦВЗ, ЦВЗ-система) будем называть совокупность методов и средств, предна-

значенных для внедрения в цифровой сигнал информации, имеющей некоторое отношение к этому цифровому сигналу.

1.1.5. Information Hiding

Цифровая стеганография и цифровые водяные знаки имеют много общего: сам принцип – встраивание одного информационного объекта в другой; методы и алгоритмы встраивания и извлечения информации; свойства и понятия. Это объясняется тем, что они являются составными частями более широкой области знаний, называемой по-английски “Information Hiding” или “Data Hiding”, т.е. буквально *сокрытие информации.* Данное направление информатики сформировалось к середине 90-х годов XX века, а первые крупные монографии появились лишь на рубеже тысячелетий. Наиболее серьёзный вклад в её развитие внесли Ingemar Cox [13, 14], Jessica Fridrich [2, 15], Mauro Barni, Franco Bartolini [1], Fabien Petitcolas [16, 17], Stefan Katzenbeisser [17], Eric Cole [18], Birgit Pfitzmann [19].

В рамках данного пособия мы будем переводить “Information Hiding” как «встраивание информации». Общепринятое русскоязычное название в настоящее время отсутствует, а термин «встраивание информации» кажется авторам более предпочтительным по сравнению с термином «сокрытие информации», поскольку в ряде методов защиты данных цифровыми водяными знаками встроенная информация *может* и даже *должна быть* визуально различимой, то есть *не скрытой* от глаз. Кроме того, такое название позволяет явным образом отгородиться от предмета и задач криптографии, которая занимается *сокрытием содержания* информации [9].

Итак, под *встраиванием информации* (в узком смысле) будем понимать область знаний, охватывающую широкий круг проблем внедрения информации (называемой в различных ситуациях *секретной информацией*, *секретным сообщением* или *цифровым водяным знаком*) в содержимое другого информационного объекта (называемого *открыто передаваемой информацией* или *контейнером*).

Методы встраивания информации могут быть разделены на 4 основные категории, как показано в табл. 1.2.

Вслед за авторами книги [2] приведём исторические примеры использования каждой группы методов:

1. В 1981 году фотографические оттиски конфиденциальных документов британского кабинета оказались напечатанными в газетах. Согласно слухам, для определения источника утечки Маргарет Тэт-

чер 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 могли быть установлены источники утечки информации.

Табл. 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	Нестеганографическое встраивание ЦВЗ (3)	Открытая опосредованная передача информации (4)

2. Скрытая передача информации, не связанной с контейнером, всегда являлась важной задачей для военных. Например, согласно договору ОСВ-II между СССР и США, обеим державам допускалось иметь достаточно много бункеров ракет, но лишь ограниченное число ракет. Для проверки соблюдения договора каждый участник соглашения должен был устанавливать датчики, разработанные в другой стране, в своих хранилищах ракет. Каждый такой датчик должен был только сообщать о наполненности бункера, в котором он установлен, и ничего больше. Однако по свидетельствам некоторых источников [10], внутри законных сообщений удавалось спрятать также и дополнительную информацию, касающуюся, в частности, местонахождения бункера.
3. Пример нестеганографического водяного знака (т. е. водяного знака, наличие которого является известным) можно увидеть, к примеру, на электронных картах Google Maps. Каждая плитка карты имеет слабозаметный водяной знак, защищающий права Google как владельца изображения, и на это обстоятельство указывает сообщение в нижней части каждой веб-страницы. Знание того, что водяные знаки встроены в каждое изображение, помогает сдерживать несанкционированное использование этих материалов.
4. В качестве примера открытой опосредованной передачи информации можно упомянуть вставки кода времени в радиоэфире на заданной частоте, 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.

В рамках настоящего учебного пособия далее будут рассматриваться только цифровые водяные знаки и методы цифровой стеганографии, то есть и методы встраивания информации в цифровые сигналы, имеющие физическую природу. Основная причина этого в их большой практической значимости и универсальности. Наибольшее внимание будет уделено использованию в качестве контейнеров цифровых изображений, однако многие из рассмотренных методов применимы и к контейнерам других типов.

1.2. Краткие сведения о системах встраивания информации

1.2.1. Понятие систем встраивания информации

Совокупность методов и средств, образующих единое решение для встраивания информации в цифровой сигнал, будем называть *системой встраивания информации* (СВИ). К СВИ относятся *стеганографические системы* (*стегосистемы*), предназначенные для скрытой передачи информации, и *системы встраивания цифровых водяных знаков* (ЦВЗ), предназначенные для защиты контейнера. Последние мы будем сокращённо обозначать как *ЦВЗ-системы*. Любая система встраивания информации состоит из двух основных блоков:

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. Упрощённая схема СВИ представлена на рис. 1.2.

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 необхо-

димым). Разработка таких атак является задачей *стегоанализа*. Если стегосистема является устойчивой к ним, то говорят, что она обладает *стеганографической стойкостью* [4, 5, 20]. Очевидно, что методы, используемые для скрытой передачи информации, должны позволять встраивать большой объём данных.

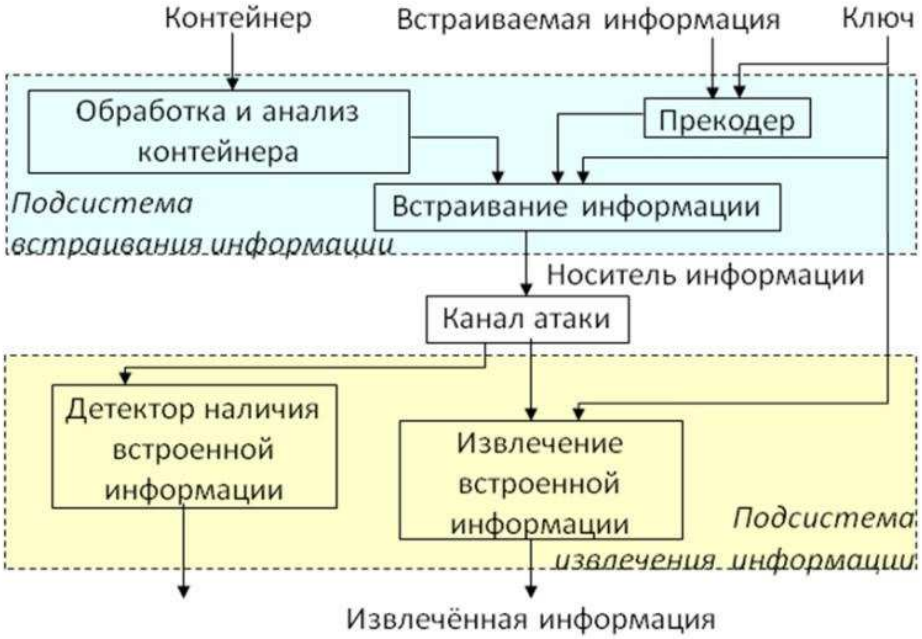


Рис. 1.2 – Упрощённая схема системы встраивания информации

Ключевой характеристикой *ЦВЗ-систем* также является стойкость, но она имеет несколько иной смысл. Под *стойкостью ЦВЗ-систем* понимается возможность извлечения встроенной информации из искажённого (преднамеренно или случайно) контейнера. ЦВЗ-система будет называться стойкой к аддитивному зашумлению и компрессии JPEG, если ЦВЗ будет корректно извлекаться из искаженного (зашумленного и сжатого в формате JPEG) контейнера. При этом круг значимых искажений определяется в зависимости от области применения метода встраивания данных.

Более того, в ряде задач (защита контейнера от изменений, защита от копирования [1]) требуется, чтобы ЦВЗ был гарантированно нестойким к определённым преобразованиям. Такие водяные знаки будут называться *полухрупкими* или *хрупкими*. Более подробно вопросы стойкости СВИ рассматриваются в параграфе 3.3, а системы хрупких и полухрупких ЦВЗ – в параграфе 3.4.

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) защита 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» [1], 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 «Сдерживание копирования» [1], 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 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 быть реализованы в виде стойких ЦВЗ.

Задача *скрытой передачи информации* является ключевой задачей стеганографии. Поэтому для её решения используются стегосистемы.

Помимо пяти рассмотренных задач, системы встраивания информации могут также применяться в задачах мониторинга телевещания, контроля копирования видео, встраивания метаданных и др. Некоторые из этих задач будут рассмотрены в параграфе 3.5.

1.2.3. Свойства систем встраивания информации

При описании систем встраивания информации принято выделять присущие им основные *свойства*. Эти свойства определяют детали под-

систем 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. Ниже перечислены наиболее важные из этих свойств.

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*, который допускает 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 защищённые, стойкие, полухрупкие и хрупкие. В *защищённых СВИ* стойкость встроенной информации должна сохраняться как при преднамеренных атаках, так и 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 встроен-

ная информация разрушается даже при незначительных модификациях заполненного контейнера.

Свойства СВИ находятся в тесной связи с назначением СВИ. Для различных практических задач подходят системы, обладающие разным набором свойств. Для иллюстрации этого принципа в табл. 1.3 показана связь задач СВИ с требованиями, предъявляемыми к основным свойствам систем.

Табл. 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

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* нарушителей, осуществляющих эти атаки.

В качестве основных целей атак на СВИ выделим следующие:

- обнаружение наличия встроенной информации,
- извлечение встроенной информации без отыскания ключа,
- удаление встроенной информации,
- отыскание секретного ключа,
- подмена встроенной информации,
- подделка носителя информации (контейнера).

В табл. 1.4 представлены некоторые требования по стойкости систем встраивания информации к различным атакам в зависимости от назначения систем: знаком «+» помечены атаки, к которым система, как правило,

должна быть стойкой, знаком «–» помечены атаки, не являющиеся актуальными для систем данного назначения, в случае «+ –» возможны различные варианты.

Табл. 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_f
Защита авторских прав	–	–	+ –	+	+	–
Защита от копирования	–	+	+ –	–	+	+
Защита от изменений	–	–	–	+	–	+
Передача информации	+	+	+ –	+	+	–
Защита от подделки	–	–	–	+	–	+

По знаниям и возможностям, которыми обладает нарушитель, можно выделить следующие атаки [9, 4]:

- 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» [5, 4].

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.

1.2.5. Основные обозначения и определения

Одной из важных особенностей функционирования систем встраивания информации является преобразование информационной последовательности из одной формы в другую (с сохранением содержания). Это обусловливает необходимость введения обобщённого термина *внутренней информации* (внутренней она является по отношению к контейнеру, поскольку передаётся внутри него). Мы редко будем пользоваться этим термином, но важно понимать его суть. Существует три формы внутренней информации: двоичный вектор, цифровой сигнал и матрица признаков. Первая форма соответствует, например, содержанию скрываемого сооб-

щения, передаваемому внутри стеганографического контейнера, или цифровому коду защитного ЦВЗ. Вторая форма соответствует традиционной форме контейнера, в который встраивается информация, то есть это может быть цифровой аудиосигнал с заданными характеристиками дискретизации и квантования, изображение, видео и пр. Третья форма индивидуальна для каждой системы и является представлением, в котором непосредственно происходит встраивание информации, то есть модификация данных контейнера.

Говоря более формализовано, под *цифровым сигналом* 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.

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.

Изначально внутренняя информация может быть представлена в виде вектора $\mathbf{b}$ двоичных значений длиной N_b (будем обозначать множество таких векторов $\mathbb{B}_{[N_b]}^{1}$) или цифрового сигнала $W \in \mathbb{X}_{[]}^{m}$. Контейнером является цифровой сигнал $C \in \mathbb{X}_{[]}^{m}$. Далее перед встраиванием отыскиваются матрицы признаков контейнера – $f \in \mathbb{Y}_{[]}^{l}$ и встраиваемой информации – $\Omega \in \mathbb{Y}_{[]}^{l}$.

Следует заметить, что в ряде систем встраивание информации осуществляется непосредственно в отсчёты цифрового сигнала, т.е. в m-мерную матрицу X. Такие методы применительно к цифровым изображениям называются *встраиванием в пространственной области*. В этом случае просто будем полагать отображение сигнала в матрицу признаков тождественным.

Результатом встраивания Ω в f является матрица признаков носителя информации $f^{W} \in \mathbb{Y}_{[]}^{l}$. Вслед за этим на основе f^{W} отыскивается собственно носитель информации в форме цифрового сигнала $C^{W} \in \mathbb{X}_{[]}^{m}$, который передаётся подсистеме извлечения информации. При передаче он может быть подвергнут атакам или искажениям, поэтому важно отличать отправленный носитель информации от принятого, который обозначается как $\widetilde{C^{W}}$.

Результатом работы подсистемы извлечения информации является либо результат обнаружения встроенной информации:

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

(в случае системы с детектором), либо собственно извлечённая информация в начальной форме, то есть $\mathbf{b^R} \in \mathbb{B}^1_{[\mathrm{N_b}]}$ или $W^R \in \mathbb{X}^m_{[]}$ (где символ R является сокращением от “recovered”, то есть характеризует восстановленную информацию).

Величина ξ на практике рассчитывается по формуле вида

$$\xi = \begin{cases} 1, & \rho(x, x^R) \geq T_\rho, \\ 0, & \rho(x, x^R) < T_\rho, \end{cases} \quad (1.1)$$

где под символами x и x^R подразумевается встроенная и извлечённая информации в *форме детектирования* (то есть в одной из форм внутренней информации, определённой на уровне конкретной системы), $T_\rho \in \mathbb{R}$ – порог, а $\rho(x, x^R)$ – некоторая функция близости величин x и x^R, имеющая в зависимости от формы детектирования одну из трёх форм:

$$\rho : \mathbb{B}^1_{[N_b]} \times \mathbb{B}^1_{[N_b]} \longmapsto \mathbb{R}, \quad (1.2)$$

$$\rho : \mathbb{X}^m_{[]} \times \mathbb{X}^m_{[]} \longmapsto \mathbb{R}, \quad (1.3)$$

$$\rho : \mathbb{Y}^l_{[]} \times \mathbb{Y}^l_{[]} \longmapsto \mathbb{R}. \quad (1.4)$$

Аргументами функции ρ в первом случае являются $(\boldsymbol{b}, \boldsymbol{b^R})$, во втором – (W, W^R), в третьем – $\left(\Omega, \tilde{\Omega}\right)$, где $\tilde{\Omega}$ – оценённая матрица признаков внутренней информации. При извлечении информации всегда в первую очередь по принятому носителю информации отыскивается оценка $\tilde{\Omega}$, после чего осуществляется её конвертация в требуемую форму детектирования.

Если формой детектирования является двоичный вектор, то чаще всего используется функция вида

$$\rho(\boldsymbol{b}, \boldsymbol{b^R}) = \frac{1}{N_b} \sum_{i=0}^{N_b - 1} (1 - b_i \oplus b_i^R). \quad (1.5)$$

Для формы детектирования $\mathbb{X}^m_{[]}$ может использоваться либо аналогичная побитовая функция, либо какая-либо функция близости двух сигналов. В случае полутоновых изображений, например, может использоваться мера PSNR [21], рассчитываемая по формуле

$$\rho(W, W^R) = PSNR(W, W^R) = 10lg \frac{255^2}{\varepsilon^2_{\text{кв}}(W, W^R)}, \quad (1.6)$$

где

$$\varepsilon^2_{\text{кв}}(W, W^R) = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \left(W(n_1, n_2) - W^R(n_1, n_2)\right)^2, \qquad (1.7)$$

а N_1, N_2 – размеры изображения по вертикали и горизонтали соответственно.

Защищённость информации, передаваемой в СВИ внутри контейнера, от различных атак, определённых в параграфе 1.2.4, обеспечивается *секретным ключом СВИ*, который мы зачастую для удобства будем объединять с открытыми (общеизвестными) параметрами СВИ в виде *составного ключа* $\mathbf{k}$.

В начале данного пособия приведена таблица обозначений всех основных данных, фигурирующих в СВИ.

2. Особенности представления мультимедийной информации и восприятия её человеком

2.1. Особенности представления и восприятия изображений

2.1.1. Непрерывные изображения. Дискретизация и квантование изображений

Функция яркости

Рассмотрим некоторый объект, освещённый источником света [22]. На некотором расстоянии от него *распределение энергии источника светового излучения*, отражённого объектом, по пространственным координатам x_1, x_2 и по длинам волн λ описывается функцией $L(x_1, x_2, \lambda)$. Эта величина является неотрицательной. Её максимальное значение L_{max}, называемое максимальной яркостью изображения, ограничено предельной величиной светочувствительности регистрирующих сред:

$$0 \le L(x_1, x_2, \lambda) \le L_{max}. \quad (2.1)$$

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

$$-M_1 \le x_1 \le M_1, \quad -M_2 \le x_2 \le M_2. \quad (2.2)$$

Понятие непрерывного изображения

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

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

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

Дискретизация изображения

Рассмотрим непрерывное изображение $L(x_1, x_2)$ – функцию двух пространственных переменных x_1 и x_2 на ограниченной прямоугольной области.

Введём понятие шага дискретизации Δ_1 по пространственной переменной x_1 и Δ_2 по переменной x_2. Например, можно представить, что в точках, удалённых 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

$$L(n_1\Delta_1, n_2\Delta_2) = L(x_1, x_2)|_{x_1=n_1\Delta_1, x_2=n_2\Delta_2}. \quad (2.4)$$

Для сокращения записи обозначим

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

Функция $L(n_1, n_2)$ 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

$$N_1 = \left[\frac{2M_1}{\Delta_1}\right], \quad N_2 = \left[\frac{2M_2}{\Delta_2}\right],$$

где [...] обозначает целую часть числа.

Если область определения непрерывного изображения – квадрат с длиной стороны $M_1 = M_2 = M$, 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 путём дискретизации изображения, называют *«пиксел»* или *«отсчёт»*.

Квантование изображений

Память компьютера способна хранить только дискретные числа. Поэтому для записи в памяти непрерывная величина L должна быть подвергнута аналогово-цифровому преобразованию с шагом ΔL. Эту операцию часто называют квантованием. Число уровней квантования, при условии что значения функции яркости лежат в интервале $[L_{min}, L_{min} + A]$, 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 с точки зрения человеческого восприятия). 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, чтобы погрешность дискретизации была незначительна и цифровое представление сохраняло основную информацию об изображении.

2.1.2. Цветные изображения. Восприятие цвета зрительной системой человека

Цвет. Цветовые пространства

Международным комитетом по освещению CIE (фр. 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.

Согласно CIE, *цвет* – это результат восприятия действия света видимого спектрального диапазона с длиной волны от 400 нм до 700 нм, попадающего на сетчатку глаза. В 1931 году было доказано, что для правильного отображения цвета достаточно трёх компонент [23].

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 (CIE 1931 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 [23].

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 чёрному. Иначе говоря, если цвет экрана, освещённого цветным прожектором, обозначается в RGB как (r_1, g_1, b_1), а цвет того же экрана, освещённого другим прожектором, – (r_2, g_2, b_2), то при освещении двумя прожекторами цвет экрана будет обозначаться как $(r_1 + r_2, g_1 + g_2, b_1 + b_2)$.

В стандарте CIE определена связь цветовых моделей XYZ и RGB:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0{,}49 & 0{,}31 & 0{,}2 \\ 0{,}18 & 0{,}81 & 0{,}01 \\ 0 & 0{,}01 & 0{,}99 \end{pmatrix} \begin{pmatrix} r \\ g \\ b \end{pmatrix}. \quad (2.5)$$

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. Поэтому CMYK называют субтрактивной моделью [24].

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:

$$\begin{aligned} c &= 1 - r, \\ m &= 1 - g, \\ y &= 1 - b. \end{aligned} \quad (2.6)$$

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 [25]:

- 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:

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

$$s = \begin{cases} 0, & v = 0, \\ 1 - \dfrac{c_{min}}{c_{max}}, & v \neq 0, \end{cases} \qquad (2.7)$$

$$v = c_{max},$$

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:

$$y = \frac{77}{256}r + \frac{150}{256}g + \frac{29}{256}b,$$
$$Cb = b - y, \qquad (2.8)$$
$$Cy = r - y.$$

Спектральная чувствительность

Человеческое зрение и видеодатчики обладают спектральной чувствительностью, описываемой функцией $s(\lambda)$ [26].

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

В сетчатке глаза человека есть три вида колбочек, максимумы чувствительности которых приходятся на красный, зелёный и синий участки спектра (см. рис. 2.1). 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 три 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. табл. 2.1).

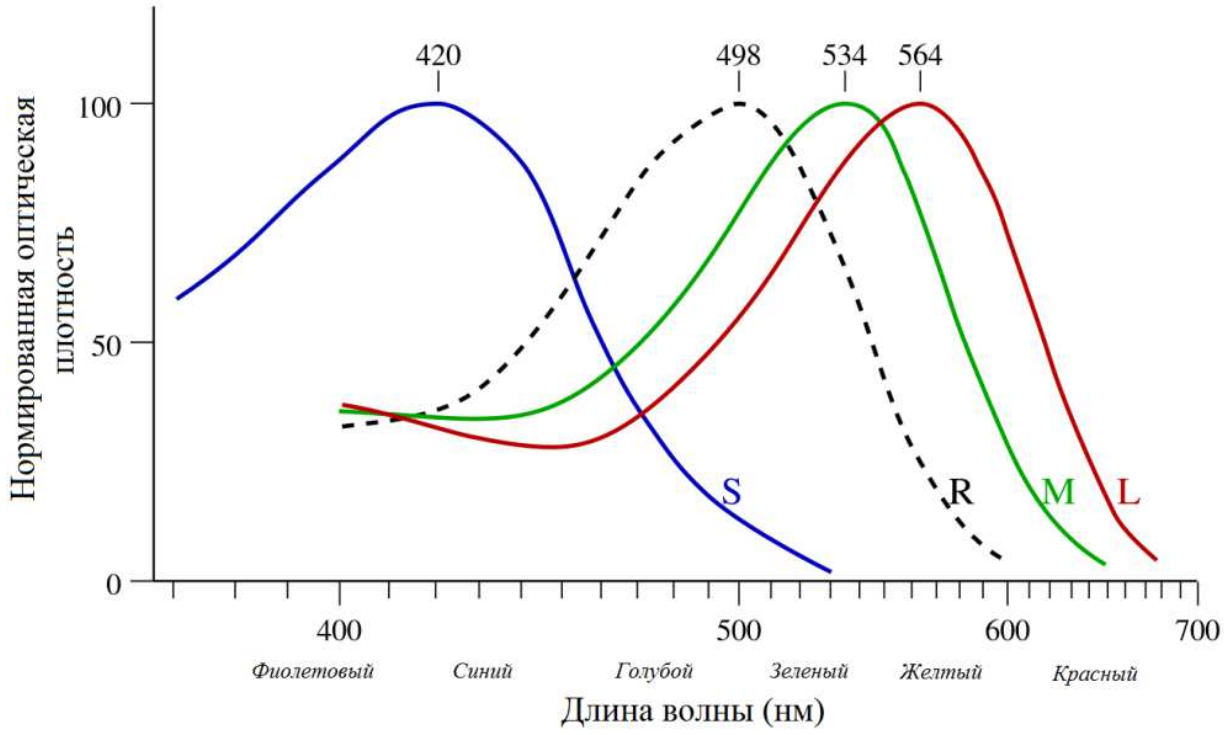


Рис. 2.1 – Нормализованные графики светочувствительности колбочек S, M, L и палочек R человеческого глаза

Табл. 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

Для справки в табл. 2.2 приведены диапазоны длин волн, соответствующие основным цветам. Мозг воспринимает комбинированную информацию от разных рецепторов, что обеспечивает различное восприятие света с разной длиной волны.

Табл. 2.2 – Длины волн основных цветов видимого диапазона

Цвет	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

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

2.1.3. Восприятие контраста зрительной системой человека

Яркостная адаптация

Благодаря наличию светочувствительных рецепторов двух видов: палочек и колбочек, человек способен на два разных вида зрительного восприятия окружающего мира [21]:

- скотопическое зрение (сумеречное) осуществляется при слабом свете, при этом возбуждаются только палочки;
- фотопическое зрение (при ярком свете) обеспечивается колбочками.

Особенностью человеческого зрения является его способность адаптироваться к огромному, порядка 10^{10}, диапазону значений яркости – от

порога чувствительности скотопического зрения до предела ослепляющего блеска. При этом эксперименты показывают, что субъективная яркость (то есть яркость, воспринимаемая зрительной системой человека) является логарифмической функцией от физической яркости света, попадающего в глаз. На рис. 2.2 изображён график зависимости субъективной яркости от истинной яркости. Длинная сплошная кривая представляет диапазон яркостей, в котором способна адаптироваться зрительная система. При использовании одного фотопического зрения этот диапазон составляет около 10^6. Постепенный переход от скотопического к фотопическому зрению показан в виде двух пересекающихся ветвей кривой адаптации.

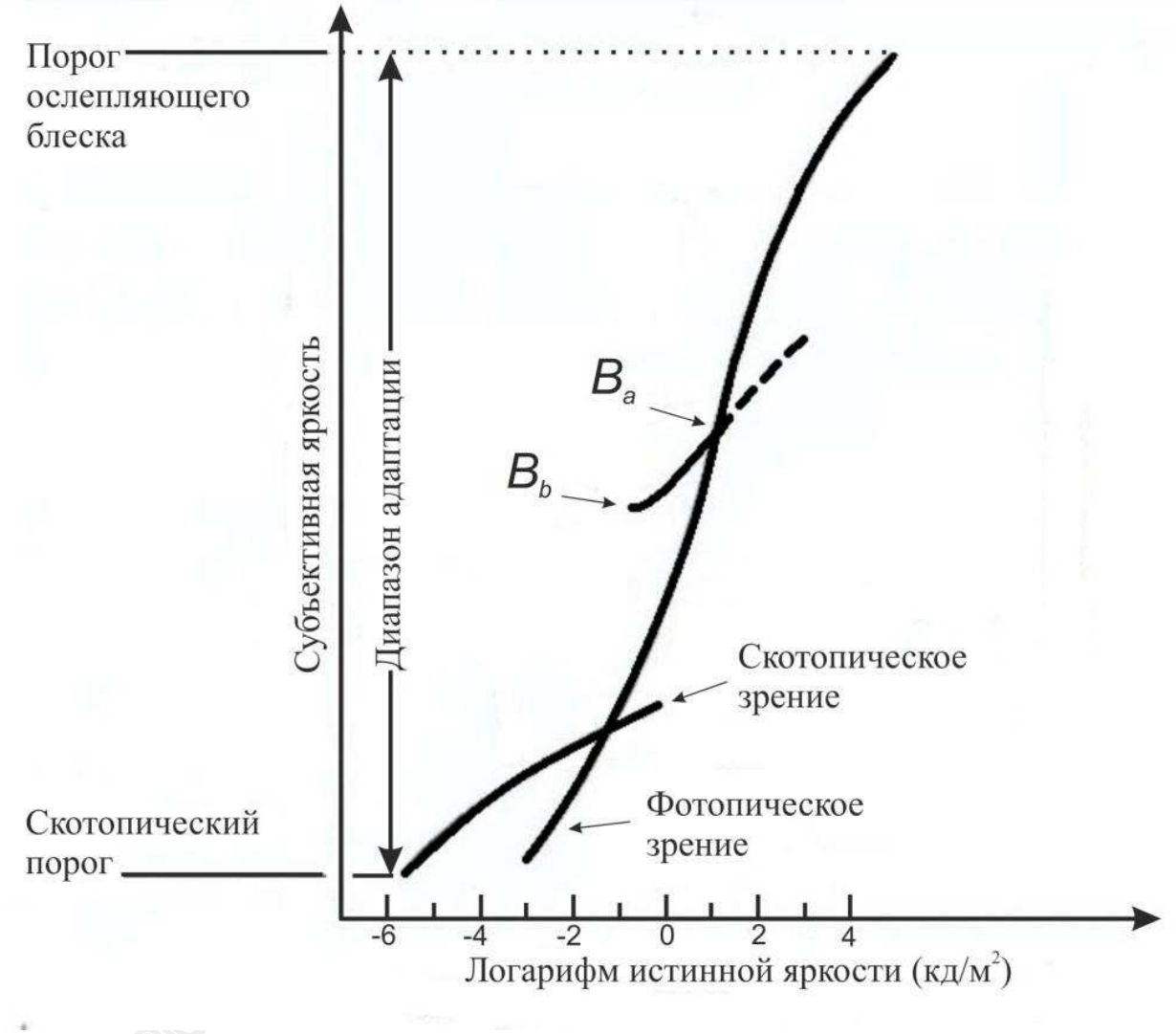


Рис. 2.2 – Диапазон субъективно воспринимаемой яркости и конкретный уровень адаптации

Для правильной интерпретации диапазона, изображённого на рис. 2.2, 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 извест-

но 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, соответствует некоторой яркости, например, точке B_a (рис. 2.2). 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 неё по кривой всё воспринимается как чёрное.

Контрастная чувствительность. Эксперимент 1 (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) [1]:

– Испытуемый смотрит на плоский равномерно освещённый экран, занимающий все поле зрения и имеющий яркость L_0 (см. рис. 2.3).

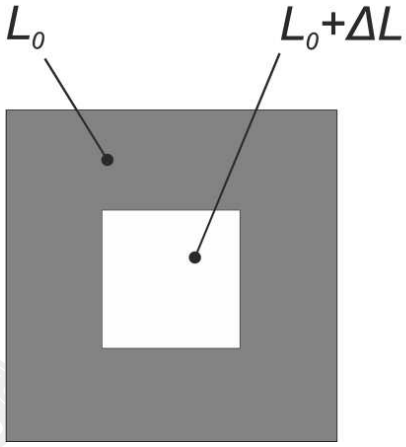


Рис. 2.3 – Постановка эксперимента Вебера

– На экран наложена маленькая добавочная яркость ΔL в границах небольшого объекта.
– Испытуемый говорит, при каких ΔL он начинает воспринимать объект яркости $L_0 + \Delta L$.

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. Вебер показал, что

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

то есть практически не зависит от базовой яркости L_0. Результат этого эксперимента послужил основой для так называемого закона Вебера, который гласит: чем выше яркость фона, тем большей должна быть разница между фоном и сигналом, чтобы последний был воспринят.

Известны два явления, ясно доказывающие, что воспринимаемая яркость не является простой функцией истинной яркости [21]. 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. 2.4.

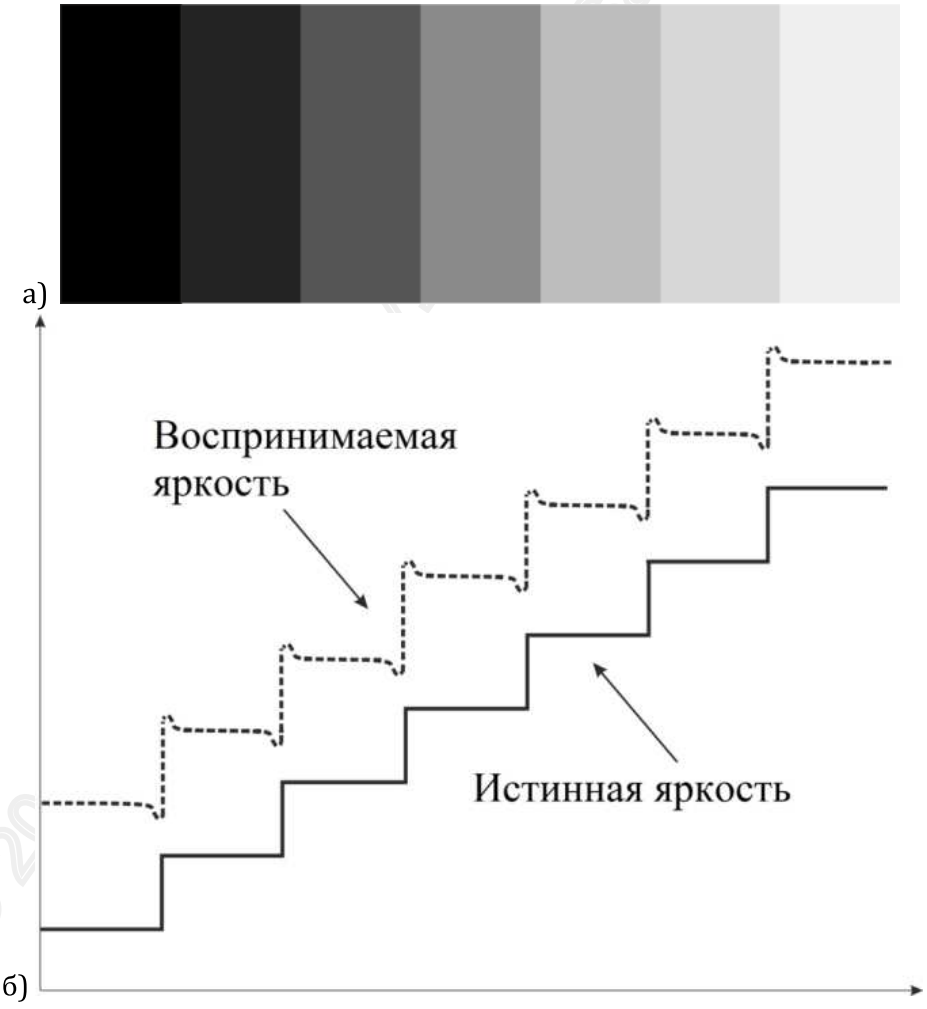


Рис. 2.4 – Пример, показывающий, что воспринимаемая яркость не является просто функцией истинной яркости. Взаимное положение по вертикали двух графиков на (б) несущественно и выбрано для большей наглядности

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. 2.5. Здесь все центральные квадраты имеют в точности одинаковую яркость, однако зрительно воспринимаются тем более тёмными, чем светлее фон.

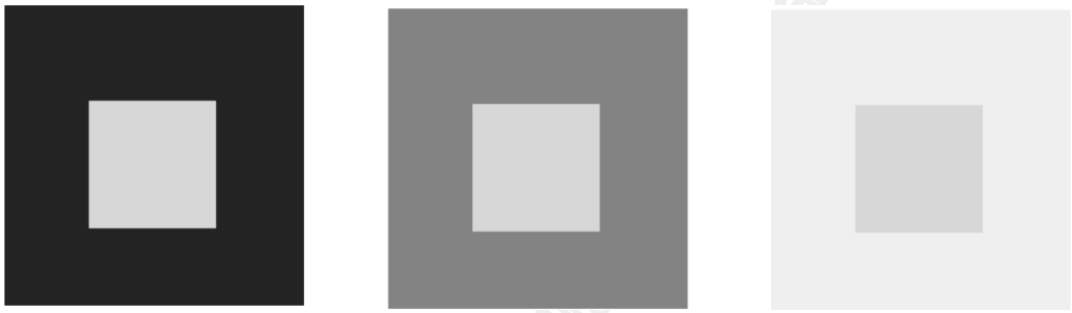


Рис. 2.5 – Иллюстрация явления одновременного контраста

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, в котором наблюдению подвергается изображение, чья яркость меняется в пространстве синусоидально (см. рис. 2.6) [1]:

$$L(x_1, x_2) = L_0 + \Delta L cos[2\pi\nu(x_1 \, cos\,\theta + x_2 \, sin\,\theta)], \qquad (2.10)$$

где

θ – угол поворота синусоиды относительно горизонтали,

ΔL – амплитуда синусоиды,

L_0 – постоянная (опорная) яркость,

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

По аналогии с экспериментом 1 (Вебера) величина ΔL такая, что синусоидальное изменение яркости различимо для 50 % наблюдателей – участников эксперимента, называется едва различимым порогом видимо-

сти и обозначается ΔL_{jn} (индекс *jn* происходит от английского “just noticeable” – едва различимый).

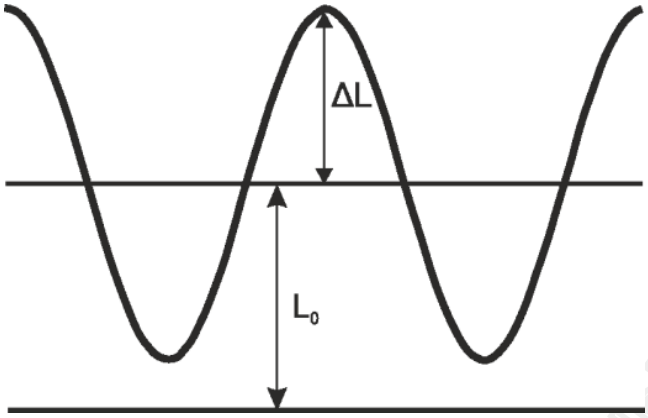


Рис. 2.6 – Яркостный срез изображения в эксперименте 2

На рис. 2.7 угол $^1/_\omega$ – угол наблюдения синусоиды, d – расстояние от глаза наблюдателя до изображения, $^1/_\nu$ – период синусоиды в метрах.

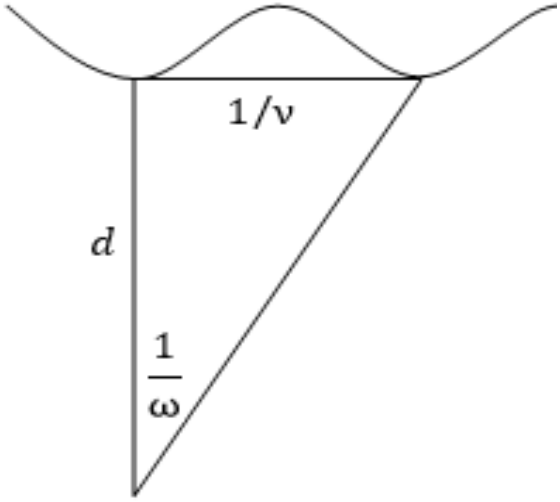


Рис. 2.7 – Иллюстрация связи различных параметров эксперимента 2

Таким образом,

$$tg\frac{1}{\omega} = \frac{1}{\nu d}. \tag{2.11}$$

При малых углах

$$\frac{1}{\omega} \approx \frac{1}{\nu d} \implies \omega \approx \nu d. \tag{2.12}$$

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

$$f = \frac{\pi\omega}{180} \approx \frac{\pi\nu d}{180} - \tag{2.13}$$

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:

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

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 рис. 2.8.

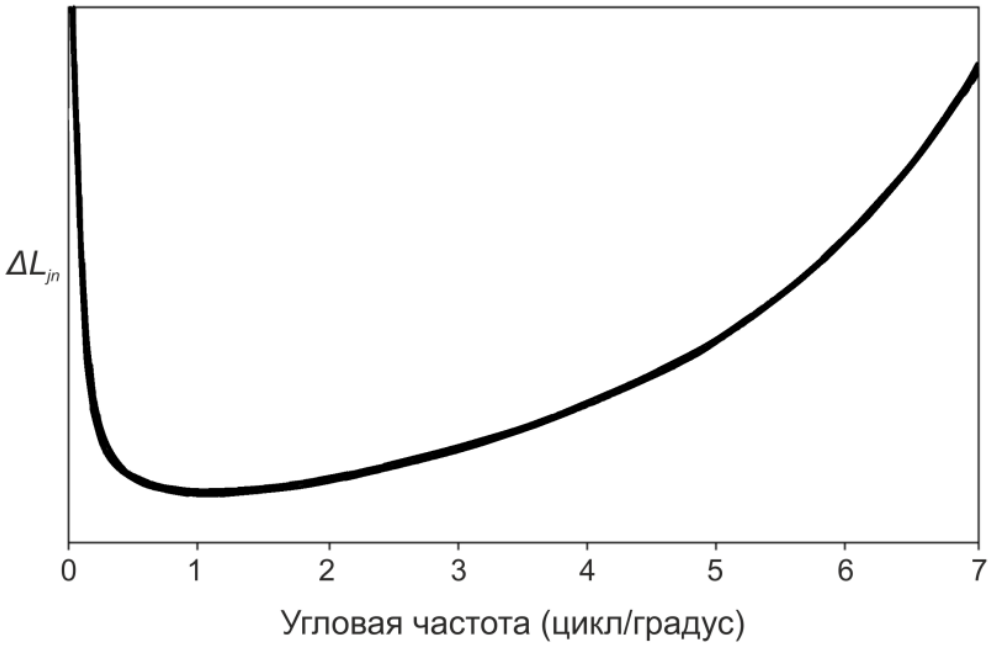


Рис. 2.8 – График $\Delta L_{jn} = \Delta L_{jn}(f)$ в эксперименте 2

Наряду с величиной ΔL_{jn}, рассматривают также величину

$$C_{jn} = \frac{\Delta L_{jn}}{L_0} = C_{jn}(L_0, \theta, W, f), \tag{2.15}$$

называемую едва различимым контрастом.

Обратная величина

$$S_c = \frac{1}{C_{jn}} = \frac{L_0}{\Delta L_{jn}} - \tag{2.16}$$

это функция контрастной чувствительности (contrast sensitivity function, CSF). Известны некоторые приближения функции CSF, но ввиду громоздкости мы не будем их приводить. На рис. 2.9 и рис. 2.10 показаны срезы $C_{jn} = C_{jn}(f)$ при разных значениях L_0 и θ.

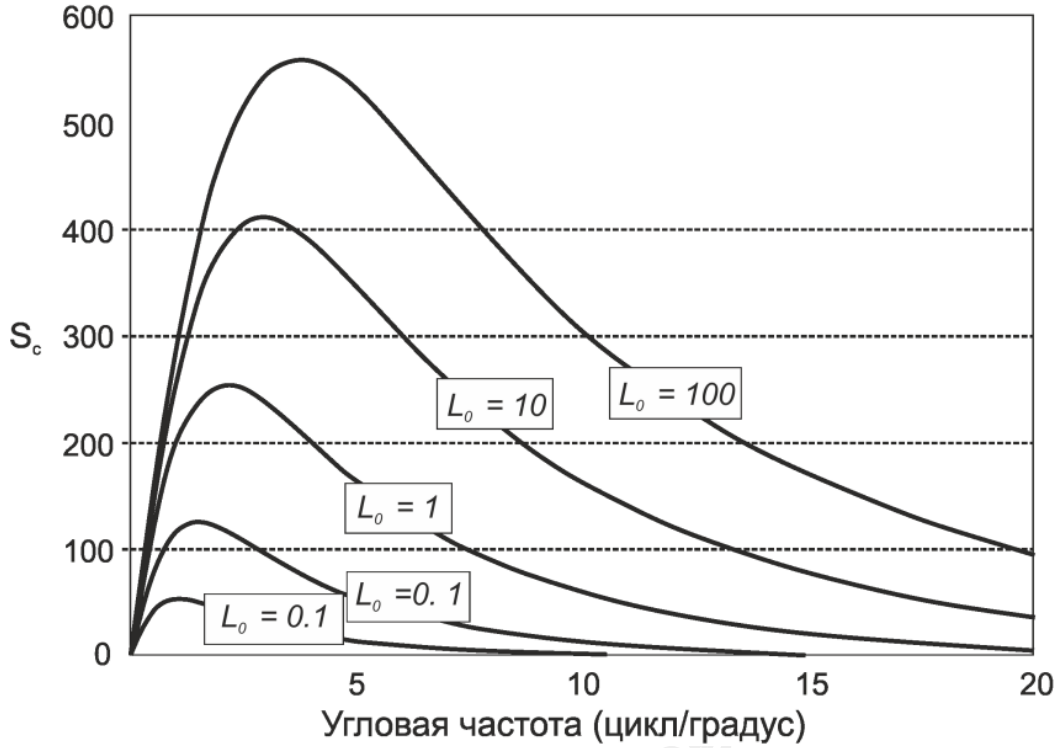


Рис. 2.9 – График $C_{jn} = C_{jn}(f)$ при различных L_0 *в эксперименте 2*

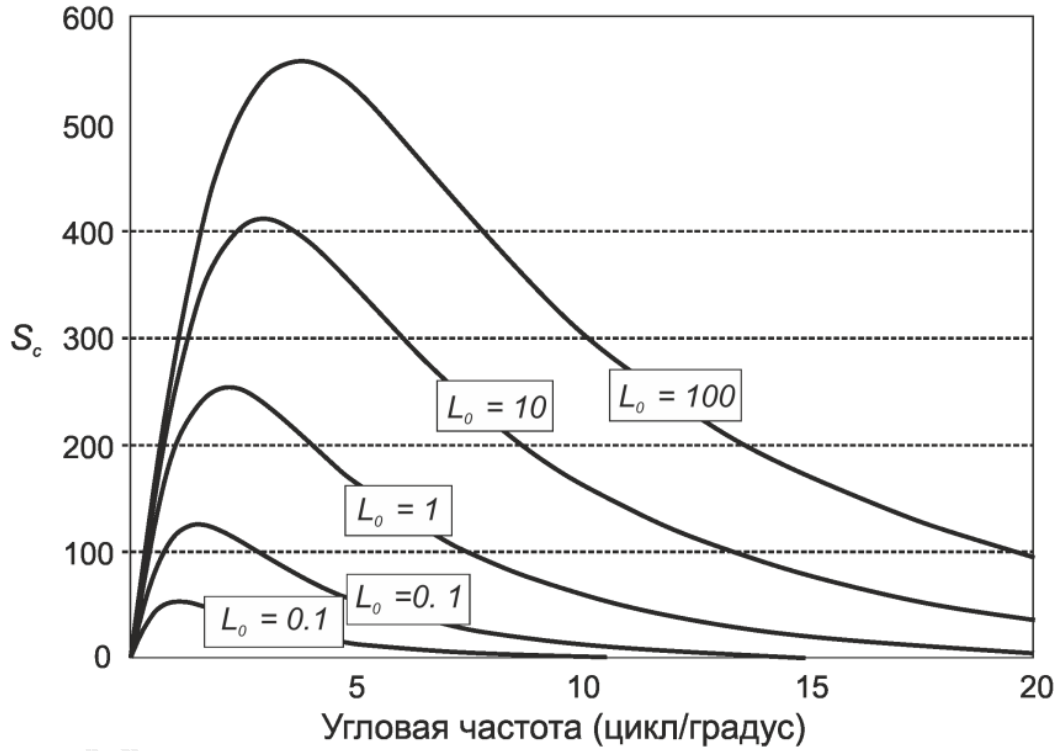


Рис. 2.10 – График $C_{jn} = C_{jn}(f)$ при различных θ в эксперименте 2

Эффект маскировки в изображениях. Эксперимент 3

Чтобы знать, какой сигнал можно замаскировать в изображении, необходимо рассмотреть третий эксперимент, заключающийся в исследовании контрастной различимости синусоиды на фоне синусоиды.

В этом эксперименте анализируемое изображение содержит [1]:

– постоянный фон – L_0;
– двумерную синусоиду – модель маскируемого сигнала, параметры $\Delta L, \theta, f$;
– двумерную синусоиду – модель маскирующего сигнала, параметры $\Delta L_m, \theta_m, f_m$.

$$L(x_1, x_2) = L_0 + \Delta L_m \cos[2\pi f m(x_1 \cos\theta_m + x_2 \sin\theta_m)] + \\ + \Delta L \cos[2\pi f(x_1 \cos\theta + x_2 \sin\theta)]. \quad (2.17)$$

В этой формуле для упрощения выражения использована величина f вместо ν.

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, чтобы синусоида была воспринята, требуются бóльшие значения ΔL, нежели те, которые были достаточны на фоне постоянной яркости.

Обозначим C_{jn}^m едва различимый контраст при условии маскирования. Эксперимент показал, что эта функция может быть оценена по формуле

$$C_{jn}^m(f, L_0, W, \theta) = \frac{\Delta L_{jn}^m(f, L_0, W, \theta)}{L_0} = \\ = C_{jn}(f, L_0, W, \theta) \cdot F\left(\frac{\Delta L_m / L_0}{C_{jn}(f, L_0, W, \theta)}\right), \quad (2.18)$$

где $C_{jn}(f, L_0, W, \theta)$ – едва различимый контраст без маскирования (2.15), а $F(x)$ – функция, обладающая следующими свойствами:
– $F(0) = 1$,
– $F(x) \leq 1$ при $0 < x \leq 1$,
– $F(x) > 1$ при $x > 1$.

На практике зачастую используется следующая аппроксимация функции $F(x)$:

$$F(x) = max(1, x^w), \quad (2.19)$$

где параметр $w \in [0{,}5; 0{,}8]$.

Если $f_m \neq f$ и $\theta_m \neq \theta$, то эффект маскировки ослабевает. Можно сказать, что ухудшение эффекта маскировки зависит от отношения $\frac{f_m}{f}$ и от разницы $|\theta_m - \theta|$. Этот эффект может быть смоделирован путем добавления в (2.18) функции S:

$$C_{jn}^m = C_{jn}(f, L_0, W, \theta) \cdot F\left(S\left(\frac{f_m}{f}, |\theta_m - \theta|\right) \cdot \frac{\Delta L_m / L_0}{C_{jn}(f, L_0, W, \theta)}\right). \quad (2.20)$$

Свойства функции $S(x_1, x_2)$:

– $S(1,0) = 1$, и это её максимальное значение.
– Монотонно убывает при отклонении (x_1, x_2) от $(0,1)$ во всех направлениях.

Подходящей простой аппроксимацией экспериментальных данных является функция вида

$$S\left(\frac{f_m}{f}, |\theta_m - \theta|\right) = exp\left\{-\frac{1}{\sigma_f^2} log^2\left(\frac{f_m}{f}\right) + \frac{1}{\sigma_\theta^2}(\theta_m - \theta)^2\right\}, \quad (2.21)$$

где величины $\sigma_f^2, \sigma_\theta^2$ имеют смысл дисперсии и рассчитываются следующим образом:

$$\begin{aligned} \sigma_f &= 1{,}2 \cdot log_2 B_f, \\ \sigma_\theta &= B_\theta, \end{aligned} \quad (2.22)$$

где

$$\begin{aligned} B_f &= \sqrt{2}, \\ B_\theta &= 27 - 3\, log_2 f. \end{aligned} \quad (2.23)$$

Выводы об основных особенностях восприятия человеком статической визуальной информации

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 определённые 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: $CSF_S \ll CSF_H \ll CSF_V$.
4. *Спектральная чувствительность (RGB)*: $CSF_B < CSF_R < CSF_G$.

Эффект маскировки в видео. Эксперимент 4

До сих пор мы исследовали особенности восприятия человеческим зрением статических изображений. В данном подразделе мы изучим чувствительность зрения к обнаружению движущихся объектов. На практике это поможет нам понять особенности восприятия человеком видеоинформации.

Итак, рассмотрим эксперимент, в ходе которого наблюдатели пытаются обнаружить наличие синусоидального сигнала, распространяющегося не только в пространстве, но и во времени [1]. Для простоты опустим вто-

рую пространственную составляющую, оставив только компоненту $x = x_1$. Итак, освещённость в ходе эксперимента изменяется следующим образом:

$$L(x,t) = L_0 + \Delta L \cdot cos\,[2\pi f(x - vt)], \qquad (2.24)$$

где

– $v = \frac{f_t}{f}\left[\frac{\text{градус}}{\text{с}}\right]$ – скорость движения синусоиды,

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

– f_t [Гц] – временна́я частота.

Для данного эксперимента была получена следующая функция контрастной чувствительности:

$$S_c = \left(6{,}1 + 7{,}3 \cdot \left|log_{10}\left(\frac{v}{3}\right)\right|^3\right) \cdot v \cdot (2\pi f)^2 \cdot exp\left\{-\frac{4\pi f}{45{,}9}(v+2)\right\}. \qquad (2.25)$$

На рис. 2.11 показана поверхность S_c в зависимости от параметров f и f_t.

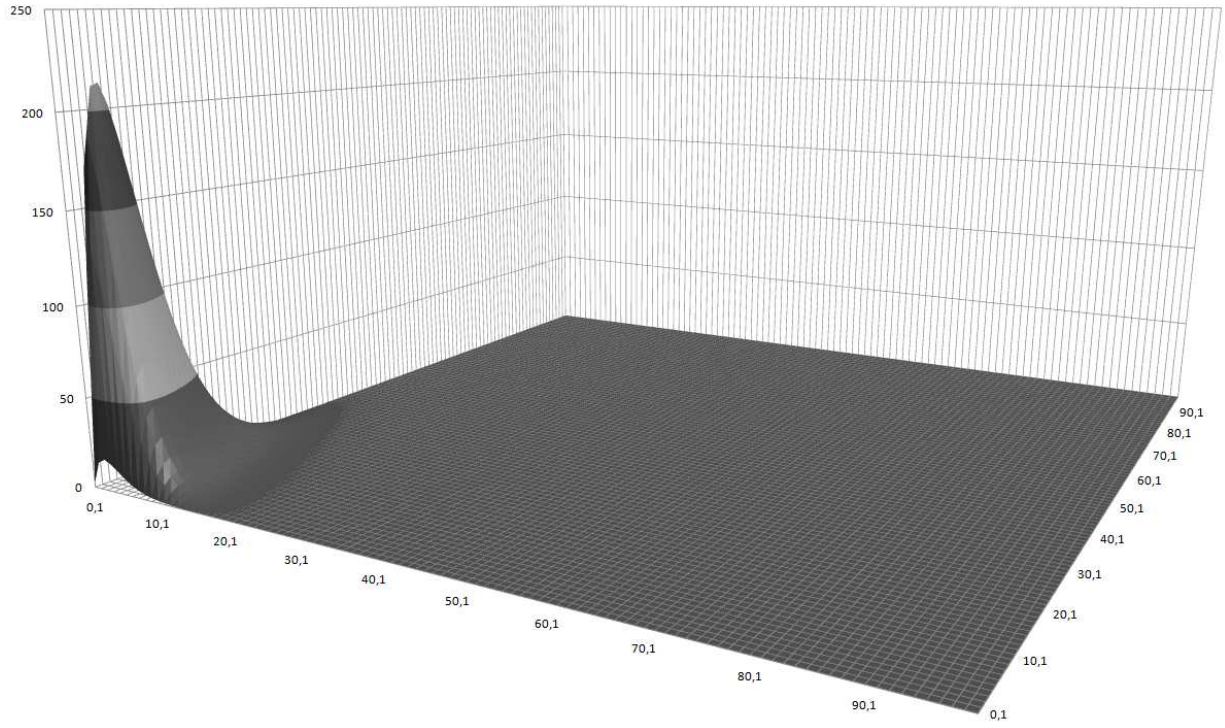


Рис. 2.11 – График $S_c = S_c(f, f_t)$ в эксперименте 4

При $f_t \approx 30$ Гц значение $S_c = 2{,}54$, то есть достаточно близко нулю. При такой частоте человеческий глаз перестаёт замечать движущуюся синусоиду.

Однако человек, как правило, осуществляет слежение за движущимся объектом, перемещая направление взгляда. Ввиду этого эффекта в качестве v в формуле (2.25) следует рассматривать не скорость движения сину-

соиды, а её скорость относительно скорости изменения направления взгляда v_{eye}:

$$v = v_{object} - v_{eye}, \tag{2.26}$$

где v_{object} – абсолютная скорость движения объекта (синусоиды).

v_{eye} оценивается по формуле

$$v_{eye} = max\left(g \cdot v_{object}, v_{eye}^{max}\right), \tag{2.27}$$

где $0 < g < 1$ – коэффициент, который возникает вследствие того, что глаз вынужден поспевать за объектом, и скорость движения направления взгляда не может быть равной скорости движения объекта, за которым осуществляется слежение. Часто используют эмпирически полученное значение $g = 0{,}82$. v_{eye}^{max} – наибольшая скорость перемещения вектора зрения, при котором глаз ещё может что-то различать. При бóльшей скорости человек уже не способен полностью адекватно воспринимать наблюдаемую изобразительную информацию. Экспериментально получено, что $v_{eye}^{max} \approx 80 \left[\frac{\text{градус}}{\text{с}}\right]$.

Таким образом, из (2.26) – (2.27) получаем:

$$v = v_{object} - max\left(g \cdot v_{object}, v_{eye}^{max}\right). \tag{2.28}$$

За счёт слежения за объектом значение f_t возрасти до 180 Гц при пространственной частоте $1 \left[\frac{\text{цикл}}{\text{градус}}\right]$.

2.1.4. Показатели качества цифровых изображений

В тесной связи с изложенными в подпараграфах 2.1.2 – 2.1.3 особенностями восприятия человеком изобразительной информации находятся вопросы оценки качества цифровых изображений. Это обусловлено, в частности, необходимостью сравнения извлечённого ЦВЗ и эталонного (в случае, если детектирование встроенной информации осуществляется в пространственной области). Кроме того, анализ качества изображения – носителя информации может помочь получить ответ на вопрос, насколько изменился контейнер после встраивания в него информации, а значит, позволяет осуществить выбор алгоритмов встраивания информации и их параметров, обеспечивающих приемлемый уровень искажений.

Мы будем рассматривать качество изображения как меру близости искажённого изображения $v(n_1, n_2)$ и соответствующего ему исходного, или эталонного $u(n_1, n_2)$, то есть будем использовать функцию вида

$$Q = Q(u, v). \tag{2.29}$$

Как правило, функции вида Q используют в качестве аргумента разностное изображение

$$\varepsilon(n_1, n_2) = u(n_1, n_2) - v(n_1, n_2), \tag{2.30}$$

то есть

$$Q = Q(\varepsilon).$$

Рассмотрим наиболее часто используемые показатели качества изображений [22].

Показатель субъективного визуального восприятия

Человеку (или чаще нескольким экспертам) предъявляются исходное и искажённое изображения, и он высказывает мнение: искажения не заметны, малозаметны, заметны. Этот критерий не численный. Результаты такой оценки очень приблизительны и субъективны. Поэтому на практике данный критерий практически не используется. Однако важно понимать, что хороший численный показатель качества для заданной пары изображений должен соответствовать показателю субъективного визуального восприятия.

Показатель максимальной ошибки

Показатель максимальной ошибки используется в тех случаях, когда выдвигается требование высокой точности представления не изображения в целом, а каждой его точки (отсчёта). Это необходимо в ответственных случаях, при обработке ценных, уникальных изображений.

Максимальная ошибка оценивается по следующей формуле:

$$\varepsilon_{max} = \max_{(n_1,n_2)} |u(n_1, n_2) - v(n_1, n_2)| = \max_{(n_1,n_2)} |\varepsilon(n_1, n_2)|. \tag{2.31}$$

Очевидно, большие значения $\varepsilon_{\max}$ соответствуют большим искажениям $v(n_1, n_2)$ относительно $u(n_1, n_2)$.

Серьёзным недостатком данного показателя является сложность теоретической оценки и, соответственно, использования его в процедурах оптимизации (по крайней мере для общепринятых моделей изображения). Кроме того, данный показатель плохо согласуется с визуальным восприятием изображения, а также не подходит для оценки качества изображения в целом. Так, если значения u и v совпадают во всех точках, кроме одной – (n_1^*, n_2^*), причём в этой точке

$$u(n_1^*, n_2^*) - v(n_1^*, n_2^*) = 50,$$

то в этом случае $\varepsilon_{\max} = 50$, то есть мера искажений велика, в то время как визуально разница между изображениями может быть практически не заметна.

Показатель среднеквадратичной ошибки

Оценить уровень искажений в среднем позволяет показатель среднеквадратичной ошибки. Полагаем, что входное и выходное изображения являются фрагментами реализации стационарного случайного поля. Тогда мерой соответствия реального изображения идеальному может служить среднее значение квадрата их разности (среднеквадратичная ошибка):

$$\varepsilon_{\text{кв}}^2 = M\{(u-v)^2\} = M\{\varepsilon^2\},$$

где $\mathrm{M}\{\cdot\}$ – математическое ожидание.

Для стационарной модели обычно считается выполненным *условие эргодичности*, при котором усреднение по ансамблю реализаций может быть заменено на усреднение по одной реализации. Тогда для изображений, заданных на области $0 \le n_1 \le N_1 - 1$, $0 \le n_2 \le N_2 - 1$, величина $\varepsilon_{\text{кв}}^2$ оценивается как

$$\varepsilon_{\text{кв}}^2 = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \varepsilon^2(n_1, n_2). \qquad (2.32)$$

Как и для предыдущего показателя, большие значения $\varepsilon_{\text{кв}}^2$ соответствуют большим искажениям.

Наряду с $\varepsilon_{\text{кв}}^2$, на практике зачастую применяется связанная с ней величина *пиковое отношение сигнал/шум* (peak signal to noise ratio, PSNR), рассчитываемая по формуле

$$PSNR(u,v) = 10 \cdot lg \frac{sup^2_{(n_1,n_2)}\, u(n_1,n_2)}{\varepsilon_{\text{кв}}^2(u,v)} = 20 \cdot lg \frac{255}{\varepsilon_{\text{кв}}(u,v)}, \qquad (2.33)$$

где $\sup u(n_1, n_2)$ – точная верхняя грань функции $u(n_1, n_2)$, то есть максимальное значение, которое она может принимать. Большие значения $PSNR$ означают большее сходство u и v. Из-за того, что $PSNR$ – логарифмическая мера, говорят, что он измеряется в децибелах (дБ). Обычно $PSNR$ варьируется в пределах от 20 до 40. Как правило, считается, что увеличение $PSNR$ на 0,5 дБ заметно глазу.

Выражение (2.32) позволяет 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. В этом случае данный критерий иногда не вполне согласуется с критерием субъективного восприятия. Так, визуально изображение на рис. 2.12б кажется более близким к изображению с рис. 2.12а, в

то время как по среднеквадратичному критерию более близким может оказаться изображение с рис. 2.12в.

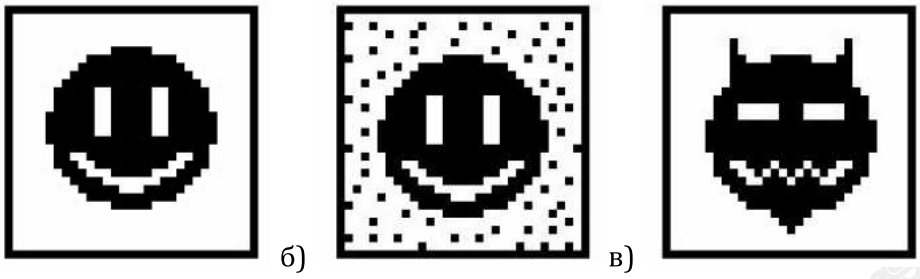


Рис. 2.12 – Иллюстрация отличия в восприятии равномерно и локально искажённого изображения: эталон (а), равномерно искажённое изображение (б) и локально искажённое изображение (в)

Частотно-взвешенный среднеквадратичный показатель

Более близким к визуальному восприятию, нежели $\varepsilon_{\text{кв}}^2$, является его модифицированный вариант – частотно-взвешенный среднеквадратичный показатель.

Рассмотрим разностный сигнал $\varepsilon(n_1, n_2)$ (2.30). Очевидно, что как и оба изображения u и v, он равен нулю вне прямоугольника $[0; \mathrm{N}_1 - 1] \times [0;\mathrm{N}2-1$. Поэтому в силу ограниченности сигнала $en1,n2$ существует его спектр:

$$E(e^{i\omega_1}, e^{i\omega_2}) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \varepsilon(n_1, n_2)\, e^{-i[n_1\omega_1 + n_2\omega_2]}. \qquad (2.34)$$

Согласно равенству Парсеваля, среднее значение квадрата функции в пространстве сигнала равно среднему значению квадратов спектральных компонент, то есть

$$\frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \varepsilon^2(n_1, n_2) = \\ = \frac{1}{N_1 N_2} \cdot \frac{1}{4\pi^2} \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} \left|E(e^{i\omega_1}, e^{i\omega_2})\right|^2 d\omega_1 d\omega_2. \qquad (2.35)$$

Таким образом, среднеквадратичный показатель можно рассчитать по формуле

$$\varepsilon_{\text{кв}}^2 = \frac{1}{N_1 N_2} \cdot \frac{1}{4\pi^2} \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} \left|E(e^{i\omega_1}, e^{i\omega_2})\right|^2 d\omega_1 d\omega_2.$$

Частотно-взвешенный среднеквадратичный показатель рассчитывается по формуле

$$\varepsilon^2_{\text{чв кв}} = \frac{1}{N_1 N_2} \cdot \frac{1}{4\pi^2} \int\limits_{-\pi}^{\pi} \int\limits_{-\pi}^{\pi} W(\omega_1, \omega_2) \cdot \left| E(e^{i\omega_1}, e^{i\omega_2}) \right|^2 d\omega_1 d\omega_2. \qquad (2.36)$$

Здесь W – это некоторая неотрицательная вещественная весовая функция. Подбирается она эмпирически. Фактически эта функция задаёт веса различных частот, которые характеризуют их значимость при оценке близости двух изображений.

Случай $W(\omega_1, \omega_2) \equiv 1$, при котором все частоты являются равноправными, соответствует среднеквадратичному показателю. Между тем, как было показано в подпараграфе 2.1.3, человек более восприимчив к низкочастотным компонентам, нежели к высокочастотным. Поэтому в качестве W, например, может использоваться функция вида

$$W(\omega_1, \omega_2) = \frac{1}{\omega_1^2 + \omega_2^2}.$$

Однако наилучшим вариантом является задание W, равной функции контрастной чувствительности ЗСЧ, введённой в подпараграфе 2.1.3. Согласно (2.15) – (2.16), эта функция зависит от четырёх переменных

$$S_c = S_c(L_0, \theta, W, f).$$

Параметры L_0, θ, W фиксируются на значениях, характерных для цифровых изображений и особенностей их наблюдения с экрана монитора. Таким образом, основным параметром является частота f.

Одним из известных аналитических аппроксимаций функции S_c является приближение Дейли (Daly):

$$S_c(f) = \begin{cases} 2{,}2(0{,}192 + 0{,}114f)\, exp(-(0{,}114f)^{1.1}), \text{если } f > f_{max}, \\ 0, \qquad \text{иначе}, \end{cases} \qquad (2.37)$$

где $f_{max} = 6{,}6$ цикла на градус. В этой точке функция S_c достигает своего максимума.

Для расчёта f на основе ω_1 и ω_2 и последующего использования её для оценки $S_c(f)$ можно использовать предположение об изотропности функции контрастной чувствительности. Тогда

$$f = \frac{\pi}{180} \sqrt{\omega_1^2 + \omega_2^2}. \qquad (2.38)$$

Однако известно [27], что контрастная чувствительность человеческого зрения в горизонтальном и вертикальном направлении выше, нежели во всех остальных (и это иллюстрирует, в частности, рис. 2.11). Поэтому вместо (2.38) используют следующее выражение

$$f = \frac{\frac{\pi}{180} \sqrt{\omega_1^2 + \omega_2^2}}{0{,}15 \cdot cos\, 4\phi + 0{,}85}, \qquad (2.39)$$

где

$$\phi = arctg\frac{\omega_1}{\omega_2}.$$

На рис. 2.13 показан график зависимости аппроксимации Дейли от двух частотных параметров согласно формулам (2.37) и (2.39). Итак, использование этой функции в качестве W в выражении (2.36) позволяет получить объективную меру близости двух изображений, согласующуюся с восприятием их зрительной системой человека.

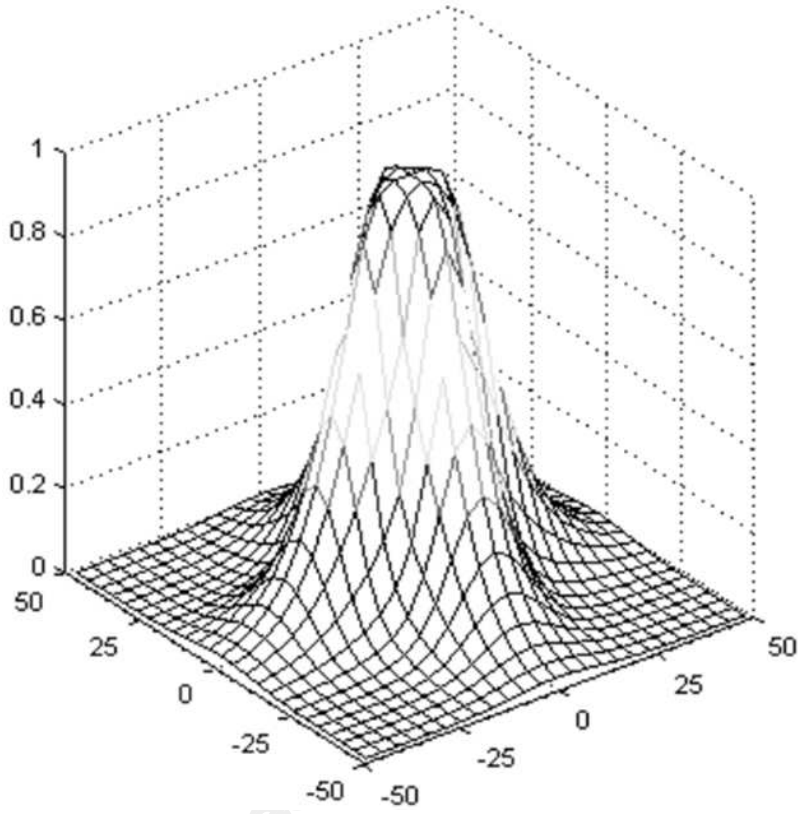


Рис. 2.13 – График зависимости $S_c = S_c(\omega_1, \omega_2)$ согласно приближению Дейли

2.2. Особенности представления и восприятия звука

2.2.1. Звук. Звуковые сигналы. Слышимость звука

Звук. Давление и уровень звука

Звук — это упругая волна, продольно распространяющаяся в среде и создающая в ней механические колебания. Для звуковых колебаний меняющейся (колеблющейся) характеристикой является давление в точке среды.

Если произвести резкое смещение частиц упругой среды в одном месте, например, с помощью поршня, то в этом месте увеличится давление [28]. 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. Таким образом формируется ряд чередующихся областей сжатия и разреженности, 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 [28]. В контексте цифрового представления звука в виде сохранённого в файле компьютера звукового сигнала и воспроизведения его при помощи компьютера нас будет интересовать только распространение звука в воздухе.

Звуковую волну принято характеризовать её частотой ν. При этом, поскольку зависимость длины волны λ от частоты имеет вид

$$\lambda = \frac{u}{\nu},$$

где $u = 330$ м/с – скорость звука в воздухе, при необходимости легко перейти от частот к длинам волн и обратно.

Слуховая система человека способна ощущать звуковые волны в виде чистых музыкальных тонов, частоты которых лежат в полосе (приблизительно) от 20 до 20000 Гц. При этом диапазон воспринимаемых давлений звука 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:

$$l_{1,2} = 20\, lg \frac{p_1}{p_2}. \qquad (2.40)$$

Децибел – безразмерная величина, но её можно использовать как единицу измерения уровня звука, если уровень звукового давления всегда рассчитывать по отношению к одному и тому же опорному уровню. В каче-

стве такого уровня принято использовать величину $p_0 = 20{,}4$ мкПа. Тогда под уровнем звука будем понимать величину

$$l = 20\, lg \frac{p}{p_0}, \qquad (2.41)$$

где p – звуковое давление.

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 55 дБ, а шепот – 20–30 дБ.

Слышимые звуки

Общее представление об уровнях звука, которые в среднем слышит человек, дает график на рис. 2.14 [29]. 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 меньше 155–160 дБ.

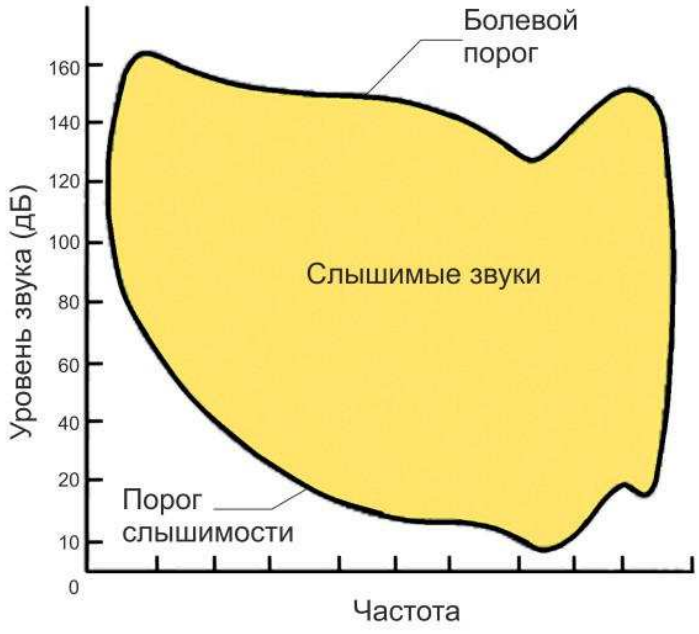


Рис. 2.14 – Область слышимых звуков

Также рис. 2.14 позволяет сделать вывод о том, что в различных частотах слуховая система человека имеет различную восприимчивость к зву-

кам. В целом слуховая система человека настроена на восприятие человеческой речи в диапазоне 50–5000 Гц.

Стоит также отметить, что человек может одинаково слышать звуки, которые сильно отличаются по форме волны. Например, белый шум слышится человеку одинаково вне зависимости от формы его конкретной реализации.

Звуковые сигналы, их дискретизация и квантование

Аудиосигналы можно разделить на три класса:

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

Под непрерывным звуковым сигналом, продолжающимся T секунд, мы будем понимать функцию $s(t) \in \mathbb{R}$, где $t \in \mathbb{R} \cap [0, T)$.

Дискретизация и квантование звуковых сигналов осуществляется так же, как и для изображений (что было рассмотрено в подпараграфе 2.1.1). Поэтому этот материал оставляется на самостоятельное изучение.

При квантовании звукового сигнала, как правило, используется 2^{16} уровней квантования для одного канала. Таким образом, один отсчёт звукового сигнала представляется 16 битами информации. Стандартная частота дискретизации звукового сигнала составляет 44100 Гц. Согласно теореме Котельникова, любая функция, допускающая преобразование Фурье и имеющая непрерывный спектр, ограниченный полосой частот от 0 до ν, полностью определяется дискретным рядом своих значений, отсчитанных через интервалы времени $\Delta t = \frac{1}{2\nu}$. Поэтому дискретного сигнала с частотой дискретизации 44100 Гц достаточно для представления непрерывного сигнала, ограниченного полосой частот 0–22050 Гц, что превышает область слышимых человеком звуков 20–20000 Гц. Исходя из этого, можно оценить продолжительность стереозвука (двухканального), который может быть записан без сжатия на стандартном Audio CD размером 700 МБ (позволяющем записать 846720000 байт в формате аудио):

$$\frac{846\,720\,000 \text{ байт на } CD \cdot 8 \frac{\text{бит}}{\text{байт}}}{44100 \text{ Гц} \cdot 16 \frac{\text{бит}}{\text{отсчёт}} \cdot 2 \text{ канала}} = 4800 \text{ с} = 80 \text{ мин.}$$

2.2.2. Частотное и временное маскирование

Частотная маскировка

Даже чистый тон при восприятии его ухом человека 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 (Рис. 2.15). Этот эффект называется *частотной маскировкой* [29].

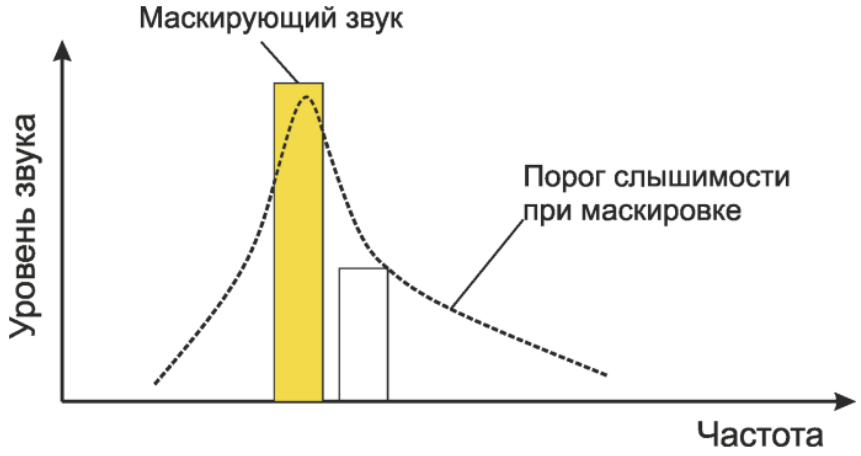


Рис. 2.15 – Частотная маскировка в слуховой системе

В количественном отношении частотная 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.

На рис. 2.16 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.

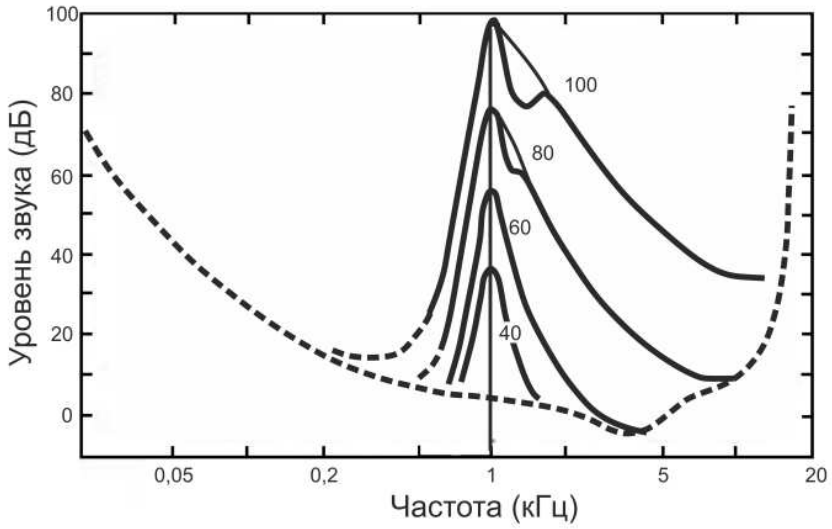


Рис. 2.16 – Влияние уровня маскирующего шума на диапазон маскировки

График на рис. 2.17 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. Данный рисунок показывает, что с увеличением частоты маскирующего тона увеличивается диапазон маскировки в области частот, бóльших частоты шума.

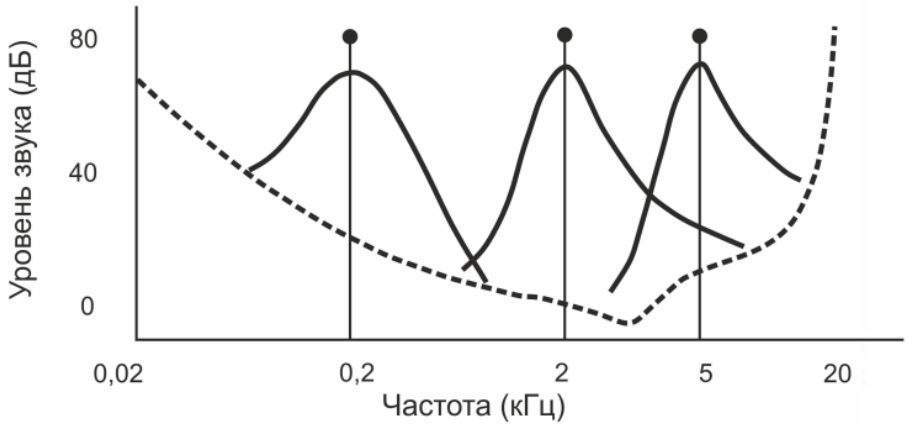


Рис. 2.17 – Влияние частоты маскирующего шума на диапазон маскировки

Временна́я маскировка

Рассмотрим влияние маскирующего шума на слышимость звуков не в частотной, а во временной его окрестности [29]. На рис. 2.18 штриховой линией показаны области маскировки до и после маскирующего сигнала. Казалось бы, маскировка, предшествующая сигналу, противоречит фундаментальному закону физики — принципу причинности. Ведь маскирующий звук меняет порог слышимости слабого звука перед своим появлением. Однако такая опережающая маскировка, называемая также *предмаскировкой*, действительно существует. На рис. 2.18 показано, что увеличение

порога слышимости испытательного импульсного звука, предшествующего маскирующему звуковому импульсу, происходит в сравнительно небольшом интервале, длительность которого составляет 20–50 мс.

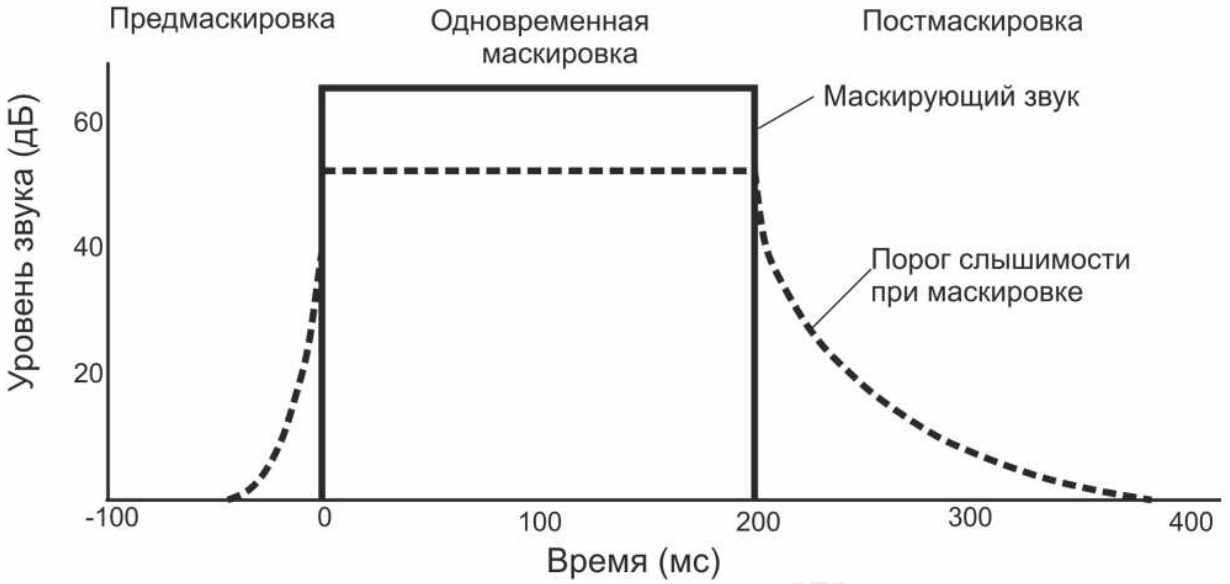


Рис. 2.18 – Временная маскировка

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. Таким образом, сильный маскирующий звук уже воспринят человеком к моменту формирования ощущения слабого испытательного звука, что и объясняет эффект предмаскировки.

Временная маскировка, существующая в слуховой системе, — один из важных эффектов, учтённых при создании психоакустической модели слуха и проектировании многих алгоритмов встраивания информации в аудиосигналы.

2.2.3. Показатели качества звуковых сигналов

Показатели качества звуковых сигналов, как и показатели качества изображений, представляют важность в рамках настоящего курса и используются при сравнении извлечённого ЦВЗ с встроенным, а также при анализе искажений носителя информации. Как и в подпараграфе 2.1.4, будем рассматривать качество звукового сигнала как меру близости искажённого сигнала $v(n)$ и соответствующего ему эталонного $u(n)$

$$Q = Q(u, v). \tag{2.42}$$

Причём, как и для изображений, будем рассматривать исключительно частный (но в то же время наиболее распространённый) случай функций Q, зависящих от разностного сигнала

$$\varepsilon(n) = u(n) - v(n), \tag{2.43}$$

то есть

$$Q = Q(\varepsilon).$$

Показатели, идентичные показателям качества изображений

Ряд показателей, рассмотренных в подпараграфе 2.1.4 для оценки близости двух изображений, применяются и для оценки близости двух звуковых сигналов: это показатель субъективного восприятия (аудиального), показатель максимальной ошибки, а также среднеквадратичный показатель.

Максимальная ошибка оценивается по формуле

$$\varepsilon_{max} = \max_n |u(n) - v(n)| = \max_n |\varepsilon(n)|. \tag{2.44}$$

Среднеквадратичная ошибка для звуковых сигналов имеет вид

$$\varepsilon_{\text{кв}}^2 = \frac{1}{N}\sum_{n=0}^{N-1} \varepsilon^2(n). \tag{2.45}$$

Для расчёта PSNR используется выражение

$$PSNR(u,v) = 10 \cdot lg \frac{sup^2\, u(n)}{\varepsilon_{\text{кв}}^2(u,v)} = 20 \cdot lg \frac{65535}{\varepsilon_{\text{кв}}(u,v)}. \tag{2.46}$$

Частотно-взвешенный среднеквадратичный показатель

По аналогии с изображениями частотно-взвешенный показатель качества звуковых сигналов мог бы согласно (2.36) иметь вид

$$\varepsilon_{\text{чв кв}}^2 = \frac{1}{\text{N}} \cdot \frac{1}{2\pi} \int_{-\pi}^{\pi} W(\omega) \cdot \left|E(e^{i\omega})\right|^2 d\omega.$$

Однако подобный критерий не подходит для анализа звуковых сигналов (в отличие от изображений) по двум причинам. Во-первых, звуковой сигнал на практике, как правило, обладает куда большей длиной N, чем линейные размеры изображения N_1, N_2. Во-вторых, изображение человек может воспринять целиком за мгновения, в то время как для полноценного восприятия звукового сигнала он должен прослушать его целиком, затратив значительно большее время. Таким образом, человеку становится интуитивно трудно сравнивать начало звукового сигнала с его окончанием (поскольку он воспринимал их спустя большой интервал времени), и у него отсутствует возможность глобального анализа всего сигнала.

Эти факторы приводят нас к выводу, что для учёта частотных характеристик при сравнении звуковых сигналов целесообразно анализировать не звуковой сигнал целиком, а делить его на кратковременные фрагменты. Удобным аппаратом для осуществления подобного анализа является *кратковременное преобразование Фурье*, осуществляющее отображение сигнала $\varepsilon(n)$ в величину $E(m, e^{i\omega})$, где ω – частотный аргумент, а m – временной аргумент:

$$E(m, e^{i\omega}) = \sum_{n=-\infty}^{\infty} \varepsilon(n) \cdot \vartheta(n-m) \cdot e^{-i\omega n}, \tag{2.47}$$

где $\vartheta(n)$ – оконная функция, значения которой не равны нулю на ограниченном числе отсчётов N_ϑ. Одной из наиболее часто используемых оконных функций является так называемое *окно Хемминга*, имеющее вид

$$\vartheta(n) = \alpha + (1-\alpha)\, cos\, \frac{2\pi n}{N_\vartheta - 1}, \tag{2.48}$$

где α – параметр. На практике зачастую используется значение $\alpha = 0{,}538$. Отметим также, что частный случай окна Хемминга при $\alpha = 0{,}5$ называется *окном Ханна*.

Итак, частотно-взвешенный показатель близости звуковых сигналов $u(n)$ и $v(n)$ основан на использовании кратковременного спектра $E(m, e^{i\omega})$ их разностного сигнала $\varepsilon(n)$ и имеет вид

$$\varepsilon^2_{\text{чв кв}}(u, v) = \frac{1}{2\pi} \int_{-\pi}^{\pi} W(\omega) d\omega \cdot \frac{1}{N} \sum_{m=0}^{N-1} \left| E(m, e^{i\omega}) \right|^2. \tag{2.49}$$

Здесь $W(\omega)$, как и для изображений, является неотрицательной весовой функцией. Для того, чтобы показатель (2.49) соответствовал субъективному аудиальному восприятию человеком звуковых сигналов, необходимо, чтобы функция $W(\omega)$ характеризовала чувствительность человеческого слуха в различных частотах. Поэтому на практике в качестве $W(\omega)$ используется функция [29]

$$W(\omega) = \frac{C}{T(\omega)}, \tag{2.50}$$

где $T(\omega)$ – аппроксимация функции пороговой слышимости (нижней границы области на рис. 2.14), имеющая вид

$$T(\omega) = 3{,}64 \left(\frac{\omega}{1000}\right)^{-0.8} - 6{,}5\, exp\left\{-0{,}6 \left(\frac{\omega}{1000} - 33\right)^2\right\} + \\ +10^{-3} \left(\frac{\omega}{1000}\right)^4, \tag{2.51}$$

а $C > 0$ – коэффициент.

3. Системы встраивания информации в изображения, видео и звуковые сигналы

3.1. Системы встраивания информации в пространственной области изображений

3.1.1. НЗБ-встраивание

Встраивание информации в наименее значимые биты контейнера (или сокращённо НЗБ-встраивание) – исторически один из первых и, пожалуй, наиболее известный широкой публике подход, который может применяться как для стеганографии, так и для защиты сигналов цифровыми водяными знаками. Он очень прост и позволяет встроить достаточно большое количество информации без сколько-нибудь заметных искажений контейнера, однако методы, использующие данный подход, как правило, обладают низкой стойкостью к искажениям носителя информации и относительно легко могут быть подвергнуты стегоанализу, поэтому имеют весьма ограниченную применимость. Тем не менее, НЗБ-встраивание вполне подходит для задач, в которых отсутствуют жёсткие требования по стойкости к отдельным видам атак.

Основная идея метода заключается в том, что любое полутоновое изображение может быть представлено в виде совокупности битовых плоскостей. Так, контейнер $C(n_1, n_2)$ будет иметь вид:

$$C(n_1, n_2) = C_1(n_1, n_2) + C_2(n_1, n_2) \cdot 2 + \ldots + C_K(n_1, n_2) \cdot 2^{K-1}, \qquad (3.1)$$

где $C_k(n_1, n_2) \in [0,1]$ – битовые плоскости, k – номер битовой плоскости, $K = 8$ – их количество.

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 заметно на рис. 3.1. Младшие битовые плоскости выглядят как слабокоррелированный шум. Осмысленные детали, как правило, начинают проступать лишь с четвёртой битовой плоскости. Это означает, что наименее значимые битовые плоскости можно модифицировать с целью встраивания скрытого сообщения или цифрового водяного знака.

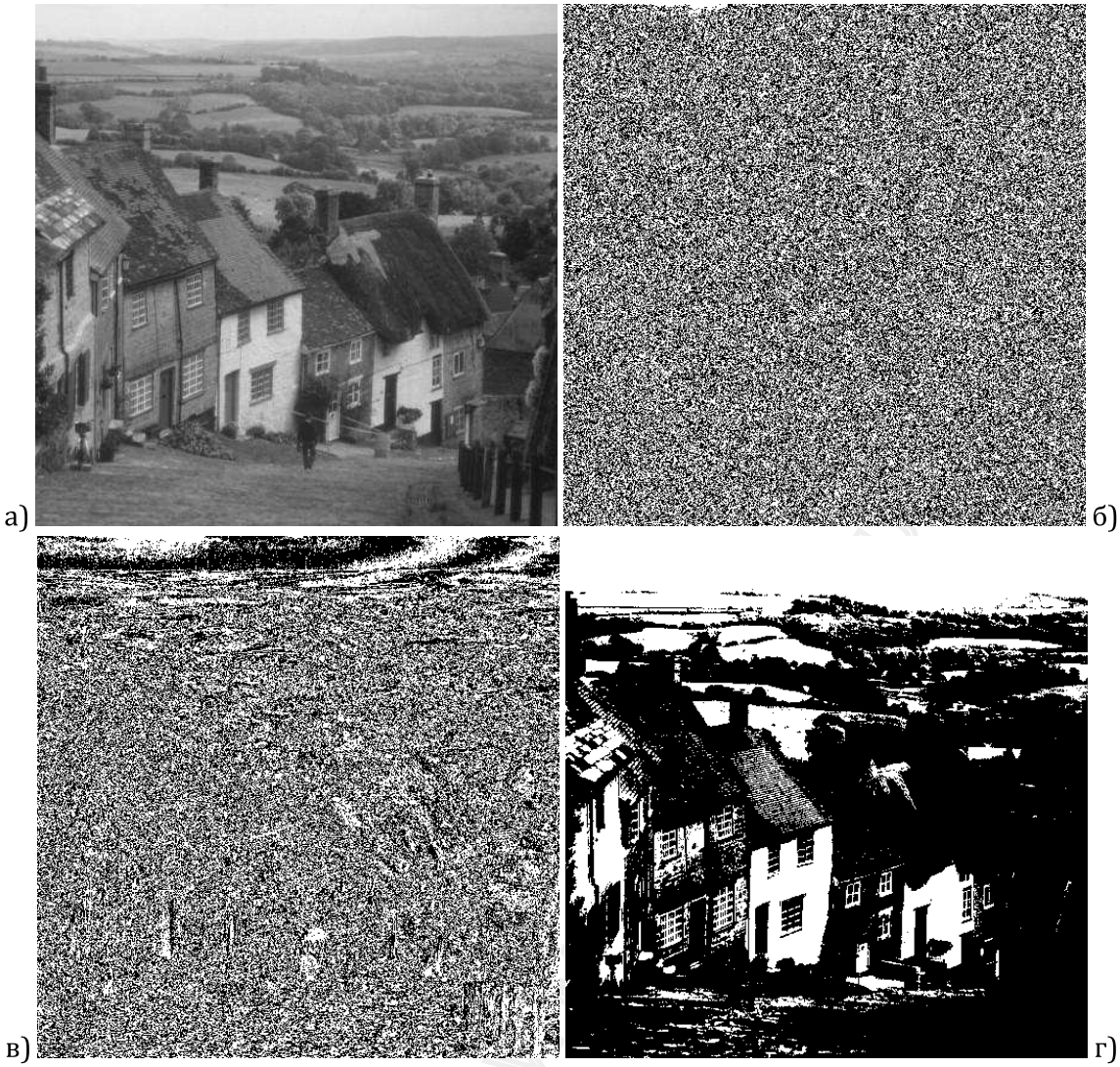


Рис. 3.1 – Битовые плоскости полутонового изображения: а) исходное изображение; б) 1-я битовая плоскость; в) 4-я битовая плоскость; г) 8-я битовая плоскость

Далее будем рассматривать лишь случай встраивания информации в одну p-ю битовую плоскость. Тогда носитель информации будет иметь вид:

$$C^W(n_1, n_2) = C_1^W(n_1, n_2) + \ldots + C_K^W(n_1, n_2) \cdot 2^{K-1}, \qquad (3.2)$$

где $C_k^W(n_1, n_2) = C_k(n_1, n_2)$ для всех $k \neq p$.

Существует достаточно большое количество систем НЗБ-встраивания, которые отличаются способом формирования битовой плоскости $C_p^W(n_1, n_2)$. Ниже мы рассмотрим три такие системы: НЗБ-встраивание ЦВЗ, стеганографическое НЗБ-встраивание и ±-встраивание в полутоновые изображения.

СВИ-1 (НЗБ-встраивание ЦВЗ)

Встраивание цифровых водяных знаков в наименее значимые биты контейнера

Пусть в НЗБ контейнера необходимо встроить изображение (цифровой водяной знак) W того же размера, содержащее бинарные значения. Тогда могут использоваться следующие варианты модификации C_p^W:

1. Непосредственная замена битовой плоскости контейнера битами скрываемой информации:

$$C_p^W(n_1, n_2) = W(n_1, n_2). \quad (3.3)$$

Извлечение информации в этом случае осуществляется, очевидно, путём чтения соответствующей битовой плоскости изображения со встроенной информацией.

2. Побитовое сложение битовой плоскости контейнера с битами скрываемой информации:

$$C_p^W(n_1, n_2) = C_p(n_1, n_2) \oplus W(n_1, n_2). \quad (3.4)$$

Извлечение информации в этом случае происходит путём побитового сложения C_p^W и C_p.

3. Отрицание побитового сложения битовой плоскости контейнера с битами скрываемой информации:

$$C_p^W(n_1, n_2) = \overline{C_p(n_1, n_2) \oplus W(n_1, n_2)}. \quad (3.5)$$

Извлечение информации происходит путём применения той же операции для плоскостей C_p^W и C_p.

На рис. 3.2 представлен пример изображения, во вторую битовую плоскость которого по формулам (3.2), (3.3) встроен бинарный орнамент.

Рис. 3.2 – Пример встраивания изображения во вторую битовую плоскость: слева – заполненный контейнер, справа – встроенное изображение

СВИ-2 (стеганографическое НЗБ-встраивание)

Скрытая передача информации в наименее значимых битах контейнера

При стеганографическом встраивании внутри контейнера $C(n_1, n_2)$ передаётся бинарный вектор $\boldsymbol{b}$ длины $N_b \leq N_1 N_2$. Как правило, встраивание происходит путём замены бит. В простейшем случае информация заносится в НЗБ последовательно:

$$C_p^W(n_1, n_2) = b_{n_1 \cdot N_2 + n_2}, \quad (3.6)$$

где b_i – *i*-й элемент вектора $\boldsymbol{b}$. Однако такое встраивание легко поддаётся стегоанализу, то есть легко обнаруживается на основе анализа статистических характеристик наименее значимой битовой плоскости (НЗБП), использованной для встраивания информации. Методы стегоанализа НЗБ-встраивания будут рассмотрены в параграфе 4.2.

Для противодействия простейшим методам стегоанализа прибегают к следующим мерам:

1) заполняют по возможности небольшую часть наименее значимых бит контейнера, т.е. добиваются того, чтобы величина

$$q = \frac{N_b}{N_1 N_2}, \quad (3.7)$$

называемая заполненностью контейнера, была существенно меньше 1;

2) заполнение контейнера производят в псевдослучайном порядке, который полностью определяется ключом встраивания $\mathbf{k}$.

Ко второму пункту следует добавить, что ключ сам по себе не содержит последовательности координат пикселей, но однозначно определяет её. Например, ключ может представлять собой начальное значение генератора случайных чисел.

Процедура извлечения информации очевидна и представляет собой чтение битов из заданных ключом координат.

При встраивании информации в p-ю битовую плоскость яркость отдельно взятого пикселя либо не меняется, либо меняется ровно на p, причём известно, в какую сторону. Пусть для определённости $p = 2$ и стоит задача встроить в пиксель с яркостью 21 значение 1. Число 21 в двоичной записи имеет вид 10101, то есть во второй битовой плоскости стоит 0. Таким образом, встраивая туда 1, мы прибавляем к текущему значению p и в итоге получаем 23. Однако что произойдёт, если мы не прибавим p, а вычтем? Очевидно, что в этом случае разница между искомым и полученным

значением составит $2p$, то есть изменения произойдут в более старших разрядах двоичной записи, в то время как p-й бит не претерпит изменений. Действительно, в нашем примере получится число 19, то есть 10011 в двоичной записи. Таким образом, мы имеем два способа изменения значения яркости пикселя, приводящих к идентичным изменениям в нужной битовой плоскости и сопровождаемых равными по абсолютной величине искажениями. Это свойство позволяет несколько модифицировать процедуру стеганографического НЗБ-встраивания путём внесения дополнительной неопределённости, способствующей защите от атак, направленных на обнаружение канала скрытой передачи информации.

<u>СВИ-3 (±1-встраивание)</u>

<u>Скрытая передача информации за счёт изменения отсчётов контейнера на ±1 [15]</u>

Рассуждения выше приводились для общего случая p-й битовой плоскости. Однако на практике чаще всего ограничиваются рассмотрением случая $p = 1$. Более того, само название данной модификации НЗБ-метода, укоренившееся в научной литературе – ±1-встраивание – уже косвенно говорит о номере битовой плоскости (в общем случае следовало бы говорить о $\pm$-встраивании). Мы приведём формулу встраивания для этого частного случая, однако её обобщение не составит труда.

Итак, пусть b_i – *i*-й элемент вектора $\boldsymbol{b}$,

$$(n_1, n_2) = \big(n_1(\mathbf{k}, i), n_2(\mathbf{k}, i)\big) \text{ –}$$

координаты *i*-го пикселя, в который необходимо встроить бит b_i, а ξ_i – псевдослучайное число, с равной вероятностью принимающее положительные и отрицательные значения (генерация последовательности $\{\xi_i\}$ также происходит на основе ключа). Тогда встраивание информации осуществляется по формуле

$$C^W(n_1, n_2) = \begin{cases} C(n_1, n_2), & C_1(n_1, n_2) = b_i, \\ C(n_1, n_2) + 1, & \begin{array}{c} (C_1(n_1, n_2) \neq b_i) \wedge \big((\xi_i \geq 0) \wedge \\ \wedge\, (C(n_1, n_2) < 255) \vee (C(n_1, n_2) = 0)\big), \end{array} \\ C(n_1, n_2) - 1, & \begin{array}{c} (C_1(n_1, n_2) \neq b_i) \wedge \big((\xi_i < 0) \wedge \\ \wedge\, (C(n_1, n_2) > 0) \vee (C(n_1, n_2) = 255)\big), \end{array} \end{cases} \qquad (3.8)$$

то есть случайным образом прибавляется или вычитается единица в том случае, если значение бита не совпадает с требуемым.

Извлечение информации происходит так же, как и в СВИ-2.

3.1.2. Встраивание информации за счёт управляемого переквантования яркости

Рассмотрим ещё один метод, широко используемый для встраивания информации (преимущественно ЦВЗ) в изображения. Изначально предложенный в работе [30], он широко известен под аббревиатурой QIM (Quantization Index Modulation). В русскоязычной литературе он чаще всего именуется методом управляемого переквантования яркости. Общий принцип управляемого переквантования заключается в том, что функция встраивания конкретного значения $\mathcal{E}$ представляется в виде семейства функций-квантователей Q_m, где m – индекс функции, причём

$$\forall m \;\; Q_m(x) \approx x. \tag{3.9}$$

Это условие обеспечивает слабое отклонение значений яркости носителя информации от соответствующих значений контейнера. При встраивании информации индекс используемой функции определяется значением отсчёта ЦВЗ:

$$C^W(n_1, n_2) = \mathcal{E}\big(C(n_1, n_2), W(n_1, n_2)\big) = Q_{W(n_1,n_2)}\big(C(n_1, n_2)\big), \tag{3.10}$$

где $W(n_1, n_2) \in \mathbb{N}_0$.

Достоинством этого метода является его теоретически обоснованная стойкость к аддитивному гауссовскому шуму вплоть до уровня дисперсии, определяемого параметрами метода. Это, в частности, делает его удобным инструментом для проектирования систем хрупких и полухрупких ЦВЗ [31]. Подробную информацию о методе QIM и его модификациях можно найти в книге [2], мы остановимся только на частном случае QIM для встраивания двоичной информации.

СВИ-4 (QIM)

Встраивание ЦВЗ за счёт управляемого переквантования [30]

Пусть C – полутоновой контейнер, а W – бинарный ЦВЗ. Тогда встраивание информации в каждом пикселе (n_1, n_2) осуществляется по формуле:

$$C^W(n_1, n_2) = \left[\frac{C(n_1, n_2)}{2q}\right] \cdot 2q + W(n_1, n_2) \cdot q + \vartheta(n_1, n_2), \tag{3.11}$$

где $q > 0$ – параметр алгоритма, $[x]$ означает целую часть рационального числа x, а $\vartheta(n_1, n_2)$ может рассчитываться одним из следующих способов:

$$\vartheta(n_1, n_2) = 0, \tag{3.12}$$

$$\vartheta(n_1, n_2) = \xi(n_1, n_2), \tag{3.13}$$

где $\xi(n_1, n_2)$ – реализация равномерного белого шума с диапазоном значений от 0 до $q - 1$;

$$\vartheta(n_1, n_2) = C(n_1, n_2)\ (mod\ \ q), \tag{3.14}$$

где $x(\mathrm{mod}\ y)$ – остаток от деления x на y.

Очевидно, что первый способ приводит к наибольшим визуальным искажениям ввиду сокращения множества возможных значений яркости, второй и третий способ имеют целью снизить заметность искажений, возникающих при встраивании.

Формулу извлечения информации предлагается вывести самостоятельно. При этом следует заметить, что корректное извлечение информации в данном методе может осуществляться и без использования исходного контейнера.

3.2. Системы встраивания информации для бинарных изображений

Бинарными называются одноканальные изображения, в которых используется ровно 1 бит для хранения интенсивности каждого пикселя. Иными словами, каждый пиксель может быть только чёрным (значение 0) или белым (значение 1). Несмотря на кажущуюся непрактичность подобных изображений, они представляют собой важный случай, поскольку при печати происходит преобразование полутоновых изображений в бинарные с последующей передачей последних на принтер. Таким образом, возможными способами встраивания информации, стойкой к процедуре печати изображения, являются встраивание информации в бинарные изображения или встраивание информации на этапе преобразования изображения в бинарное.

Очевидно, что рассмотренные ранее методы встраивания информации в полутоновые изображения оказываются неприменимыми для бинарных изображений, поскольку последние содержат лишь одну битовую плоскость. Следовательно, для бинарных изображений требуются специфические методы встраивания информации.

Прежде всего, охарактеризуем вкратце, что собой представляют бинарные изображения, полученные из полутоновых. Принцип их формирования использует особенность человеческого зрения, которое усредняет яркость наблюдаемых фрагментов небольшого размера. Пример на рис. 3.3 показывает, что значения пикселей бинарного изображения формируются таким образом, чтобы их среднее в окрестности каждого пикселя было как можно ближе к яркости полутонового оригинала в этой точке. Процесс формирования таких изображений называется *цифровым растриро-*

ванием. Существует довольно большое число методов растрирования: амплитудная и частотная модуляция, диффузия точек, диффузия ошибки (будет рассмотрен ниже), различные методы оптимизации. Подробный обзор этих методов можно найти в книге [32].

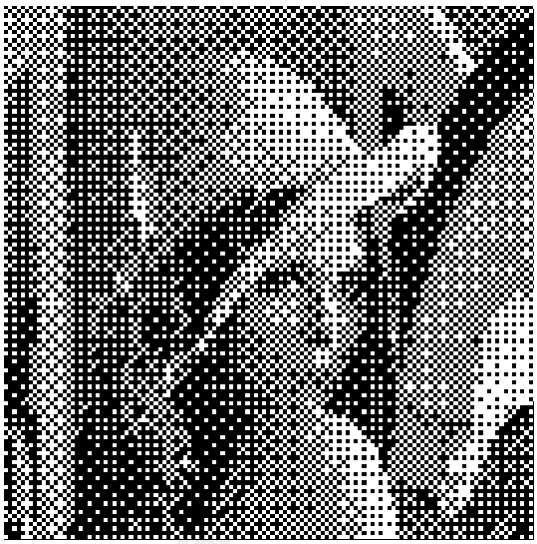
а)   б)

Рис. 3.3 – Изображение Lenna (а) и соответствующее ему бинарное изображение (б), полученное путём растрирования методом частотной модуляции

3.2.1. Непосредственное встраивание информации в бинарные изображения

СВИ-5 (DHST)

Data Hiding Self-Toggling (DHST) – простое стеганографическое встраивание в бинарный контейнер [33]

Пусть контейнер $C(n_1, n_2)$ размерами $N_1 \times N_2$ представляет собой бинарное изображение, внутри которого необходимо передать бинарный вектор $\boldsymbol{b}$ длины $N_b < N_1 N_2$. Ключ $\boldsymbol{k}$ системы представляет собой последовательность координат пикселей изображения длиной $N_k \geq N_b$.

При встраивании информации изначально носитель информации $C^W(n_1, n_2)$ идентичен контейнеру. Затем каждый *i*-й бит вектора $\boldsymbol{b}$ встраивается по простой формуле

$$C^W\big(n_1(\mathbf{k}, i), n_2(\mathbf{k}, i)\big) = b_i, \tag{3.15}$$

где b_i – элементы вектора $\boldsymbol{b}$, а $n_1(\boldsymbol{k}, i), n_2(\boldsymbol{k}, i)$ – координаты *i*-го пикселя, определяемые на основе ключа.

Процедура извлечения информации очевидна. Следует отметить, что при большой длине встраиваемого вектора искажения, являющиеся результатом встраивания информации, становятся весьма существенными.

СВИ-6 (DHSPT)

Data Hiding by Smart Pair-Toggling (DHSPT) – стеганографическое встраивание в бинарный контейнер с компенсацией искажений [33]

Данная система является модификацией системы СВИ-5 (DHST), в которой искажения, внесённые встраиванием по формуле (3.15), компенсируются путём замены значения одного из соседних пикселей на противоположное. В результате средняя яркость в локальной окрестности изменённого пикселя остаётся неизменной, следовательно, визуальное качество носителя информации повышается.

Пусть рассматривается окрестность изменённого пикселя (n_1, n_2) размерами 3×3 или 5×5. Если в этой окрестности отсутствуют пиксели, имеющие то же значение, что и $C^W(n_1, n_2)$, то компенсации искажений не производится. В противном случае необходимо выбрать один пиксель (m_1, m_2) такой, что $C(m_1, m_2) = C^W(n_1, n_2)$, и инвертировать его.

Если таких пикселей несколько, то в простейшем случае выбирается произвольный. Однако авторы системы предложили и более разумный подход. Для каждого из допустимых пикселей рассчитывается его вес, и инвертированию подвергается пиксель с наибольшим весом.

Пусть окно имеет размер 3×3. Пронумеруем пиксели окрестности в построчном порядке: $x_1, x_2, \ldots x_9$, причем x_5 – центральный пиксель с координатами (n_1, n_2). Тогда вес пикселя $V(m_1, m_2)$ рассчитывается следующим образом:

$$V(m_1, m_2) = \sum_{i=1}^{9} w(i) f(x_5, x_i), \tag{3.16}$$

где

$$f(x, y) = \begin{cases} 1, x \neq y, \\ 0, x = y; \end{cases} \tag{3.17}$$

$$w(i) = \begin{cases} 1, & i = 1,3,7,9; \\ 2, & i = 2,4,6,8; \\ 0, & i = 5. \end{cases} \tag{3.18}$$

Веса $w(i)$ в формуле (3.18) соответствуют следующей таблице размерами 3×3:

1	2	1
2	0	2
1	2	1

Наибольший вес пикселя (m_1, m_2) означает, что почти все пиксели его окрестности имеют то же значение, что и $C^W(n_1, n_2)$. Поэтому если ин-

вертированию подвергается пиксель с наибольшим весом, то это влечёт наименьшие визуальные искажения.

В базовом алгоритме DHSPT не описан вид $w(i)$ для случая окрестности 3×3. Однако допустимо, чтобы коэффициенты в этой матрице были обратно пропорциональны расстоянию от центрального отсчёта. В этом случае таблица имеет следующий вид:

$\frac{\sqrt{2}}{4}$	$\frac{1}{\sqrt{5}}$	2	$\frac{1}{\sqrt{5}}$	$\frac{\sqrt{2}}{4}$
$\frac{1}{\sqrt{5}}$	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	$\frac{1}{\sqrt{5}}$
2	1	0	1	2
$\frac{1}{\sqrt{5}}$	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	$\frac{1}{\sqrt{5}}$
$\frac{\sqrt{2}}{4}$	$\frac{1}{\sqrt{5}}$	2	$\frac{1}{\sqrt{5}}$	$\frac{\sqrt{2}}{4}$

В алгоритме DHSPT изменяются не только отсчёты, заданные ключом, но и некоторые отсчёты из их окрестности. Поэтому может сложиться ситуация, при которой значение некоторых пикселей изменится дважды. Это, в свою очередь, может привести к неточному извлечению встроенной информации. Поэтому для алгоритма DHSPT ключ должен генерироваться таким образом, чтобы исключить возможность попадания одного пикселя ключа в окрестность другого пикселя ключа.

Перечислим практические способы генерации ключа для систем DHST и DHSPT:

1) простая генерация координат пикселя по вертикали и горизонтали (только для DHST):

$$\left(n_1^i, n_2^i\right): n_1^i = \overline{0..N_1 - 1}, n_2^i = \overline{0..N_2 - 1}, i = \overline{0..N_k - 1}; \quad (3.19)$$

2) генерация координат пикселя на втрое меньшей сетке:

$$(3n_1^k, 3n_2^k): n_1^k = \overline{0..\left[\frac{N_1}{3}\right] - 1}, n_2^k = \overline{0..\left[\frac{N_2}{3}\right] - 1}, k = \overline{0..N_k - 1}; \quad (3.20)$$

3) генерация пар чисел на полной сетке с проверкой попадания в окрестность 3×3:

$$(n_1^k, n_2^k): n_1^k = \overline{0..N_1-1}, n_2^k = \overline{0..N_2-1}, k = \overline{0..N_k-1},$$
$$\min_{k\neq m}(n_1^k - n_1^m) > 1, \min_{k\neq m}(n_2^k - n_2^m) > 1, k, m = \overline{0..N_k-1}; \quad (3.21)$$

4) генерация координат пикселя на впятеро меньшей сетке:

$$(5n_1^k, 5n_2^k): n_1^k = \overline{0..\left[\frac{N_1}{5}\right]-1}, n_2^k = \overline{0..\left[\frac{N_2}{5}\right]-1}, k = \overline{0..N_k-1}; \quad (3.22)$$

5) генерация пар чисел на полной сетке с проверкой попадания в окрестность 5×5:

$$(n_1^k, n_2^k): n_1^k = \overline{0..N_1-1}, n_2^k = \overline{0..N_2-1}, k = \overline{0..N_k-1},$$
$$\min_{k\neq m}(n_1^k - n_1^m) > 2, \min_{k\neq m}(n_2^k - n_2^m) > 2, k, m = \overline{0..N_k-1}. \quad (3.23)$$

Очевидно, безошибочное извлечение информации при использовании для генерации ключа процедуры (3.19) возможно только для алгоритма DHST. Для безошибочного извлечения информации алгоритмом DHSPT с компенсацией пикселя в окне 3×3 целесообразно использовать один из способов (3.20) или (3.21), а в случае окна 5×5 – (3.22) или (3.23).

3.2.2. Встраивание информации при растрировании изображений

Вторым подходом к встраиванию информации в бинарные изображения (помимо модификации отсчётов подготовленного ранее бинарного контейнера) является внесение дополнительной информации в контейнер на этапе растрирования полутонового изображения. В настоящей главе мы изучим одну систему, реализующую данный подход, однако поскольку она интегрирована с конкретным методом растрирования – диффузией ошибки, то прежде всего необходимо его подробно описать.

Ядро диффузии 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.

В алгоритме диффузии ошибки (Error Diffusion) используется матрица h размерами $M_1 \times M_2$, называемая *ядром* или *весовой функцией*. Как правило, размеры ядра невелики: $1 \leq M_1, M_2 \leq 5$. Ядро задаёт направления распространения (диффузии) ошибки растрирования и определяет доли ошибки, передаваемые в каждом из направлений.

Приведём примеры весовых функций, зарекомендовавших себя на практике:

– ядро размерами 2×2:

$$\frac{1}{4}\begin{pmatrix}\odot & 2\\ 1 & 1\end{pmatrix}; \tag{3.24}$$

– ядро из трёх ненулевых элементов:

$$\frac{1}{16}\begin{pmatrix}0 & \odot & 8\\ 2 & 6 & 0\end{pmatrix}; \tag{3.25}$$

– ядро Floyd & Steinberg [34]

$$\frac{1}{16}\begin{pmatrix}0 & \odot & 7\\ 3 & 5 & 1\end{pmatrix}; \tag{3.26}$$

– ядро Fan [35]

$$\frac{1}{16}\begin{pmatrix}0 & 0 & \odot & 7\\ 1 & 3 & 5 & 0\end{pmatrix}; \tag{3.27}$$

– ядро Jarvis et al. [36]

$$\frac{1}{48}\begin{pmatrix}0 & 0 & \odot & 7 & 5\\ 3 & 5 & 7 & 5 & 3\\ 1 & 3 & 5 & 3 & 1\end{pmatrix}; \tag{3.28}$$

– ядро Stucki [37]

$$\frac{1}{42}\begin{pmatrix}0 & 0 & \odot & 8 & 4\\ 2 & 4 & 8 & 4 & 2\\ 1 & 2 & 4 & 2 & 1\end{pmatrix}. \tag{3.29}$$

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

При практической реализации метода диффузии ошибки может применяться один из двух алгоритмов, которые в конечном счёте приводят к идентичным результатам. Первый из этих алгоритмов реализует подтягивание ошибок растрирования из уже пройденных отсчётов и носит название *pull-модели*. Второй алгоритм, называемый *push-моделью,* осуществляет распространение ошибки из текущего отсчёта в последующие. Рассмотрим подробно оба алгоритма.

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 диффузии ошибки может быть записана в виде следующего набора выражений:

$$u(n_1, n_2) = C(n_1, n_2) - \sum_{(m_1, m_2)\in D_h} h\,(m_1, m_2)e(n_1 - m_1, n_2 - m_2), \tag{3.30}$$

$$C^B(n_1, n_2) = \begin{cases}1, & u(n_1, n_2) \geq T,\\ 0, & u(n_1, n_2) < T,\end{cases} \tag{3.31}$$

$$e(n_1, n_2) = 255 \cdot C^B(n_1, n_2) - u(n_1, n_2). \tag{3.32}$$

В формулах (3.30)–(3.32) $u(n_1, n_2)$ и $e(n_1, n_2)$ – это вспомогательные матрицы размерами $N_1 \times N_2$. Первая характеризует корректируемый в за-

висимости от ошибки растрирования контейнер, вторая – ошибку в очередной точке. T – пороговое значение, как правило, равное 128. Данный алгоритм схематически проиллюстрирован на рис. 3.4.

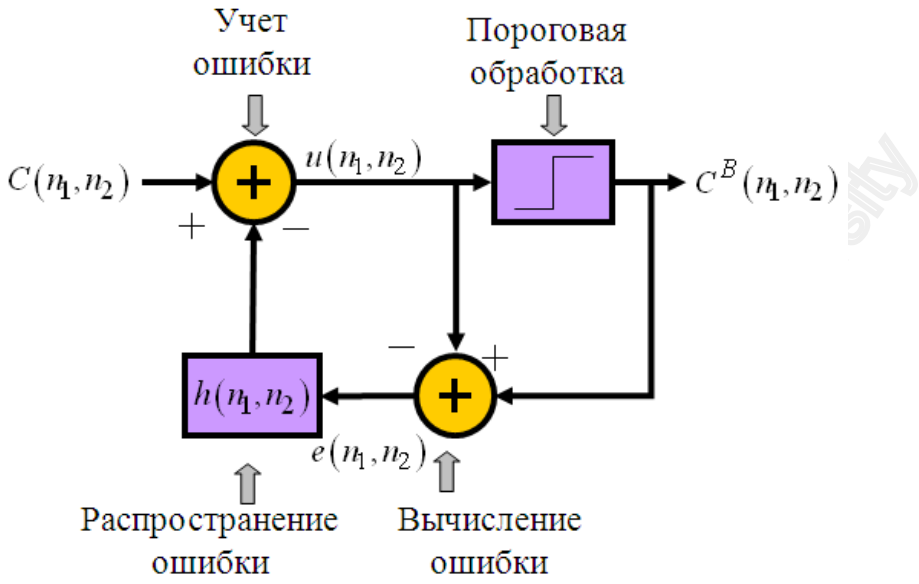


Рис. 3.4 – Схема алгоритма диффузии ошибки (pull-модель)

Алгоритм диффузии ошибки (push-модель)

Пусть D_h, как и ранее, характеризует точки (n_1, n_2), в которых $h(n_1, n_2) \neq 0$. Тогда push-модель алгоритма диффузии ошибки определяется следующими выражениями:

$$u(n_1, n_2) = C(n_1, n_2)\ \forall (n_1, n_2): n_1 = \overline{0..N_1 - 1}, n_2 = \overline{0..N_2 - 1}, \quad (3.33)$$

$$C^B(n_1, n_2) = \begin{cases} 1, & u(n_1, n_2) \geq T, \\ 0, & u(n_1, n_2) < T, \end{cases} \quad (3.34)$$

$$e = 255 \cdot C^B(n_1, n_2) - u(n_1, n_2), \quad (3.35)$$

$$\forall (m_1, m_2) \in D_h \ \rightarrow \ \rightarrow\ u(n_1 + m_1, n_2 + m_2) = u(n_1 + m_1, n_2 + m_2) - e \cdot h(m_1, m_2). \quad (3.36)$$

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 сразу рассеивается по изображению u.

На рис. 3.5 изображён пример работы алгоритма диффузии ошибки. Как видно, качество результирующего изображения является весьма высоким.

Встраивание информации при растрировании методом диффузии ошибки

Теперь перейдём собственно к рассмотрению системы встраивания ЦВЗ, использующей алгоритм диффузии ошибки.

Рис. 3.5 – Пример работы алгоритма диффузии ошибки для растрирования полутонового изображения

СВИ-7 (DHCED)

Data Hiding by Conjugate Error Diffusion (DHCED) – встраивание ЦВЗ за счёт согласованной диффузии ошибки [33]

В данной системе встраиваемая информация представляет собой бинарное изображение $W(n_1, n_2)$, размеры $N_1 \times N_2$ которого равны размерам полутонового контейнера $C(n_1, n_2)$. При встраивании ЦВЗ создаются два бинарных изображения C^B и C^W, являющихся результатом растрирования $C(n_1, n_2)$, таким образом, чтобы в как можно большем числе точек выполнялось равенство

$$W(n_1, n_2) = C^B(n_1, n_2) \oplus C^W(n_1, n_2). \tag{3.37}$$

Для этого изображение C^B создаётся при помощи базового алгоритма диффузии ошибки, рассмотренного выше, а изображение C^W – при помощи модифицированной процедуры диффузии ошибки, в которой на втором этапе вместо формулы (3.31) или (3.34) (в зависимости от используемого алгоритма) используется следующее соотношение:

$$C^W(n_1, n_2) = \begin{cases} 1, & u(n_1, n_2) \geq T_1 \ \wedge \ W(n_1, n_2) \oplus C^B(n_1, n_2) = 1, \\ 0, & u(n_1, n_2) < T_1 \ \wedge \ W(n_1, n_2) \oplus C^B(n_1, n_2) = 1, \\ 1, & u(n_1, n_2) \geq T_2 \ \wedge \ W(n_1, n_2) \oplus C^B(n_1, n_2) = 0, \\ 0, & u(n_1, n_2) < T_2 \ \wedge \ W(n_1, n_2) \oplus C^B(n_1, n_2) = 0, \end{cases} \tag{3.38}$$

где $T_1 < T < T_2$.

Таким образом, в случае pull-модели для всех пикселей изображения в цикле выполняются последовательно шаги (3.30), (3.38), (3.32) (в последней формуле при этом вместо C^B используется C^W). При использовании push-модели после инициализации изображения $u(n_1, n_2)$ по формуле

(3.33) для всех пикселей выполняются последовательно шаги (3.38), (3.35), (3.36) (в формуле (3.35) аналогичным образом используется C^W вместо C^B). Отметим также, что при формировании изображений C^B и C^W возможно использование разных моделей диффузии ошибки.

По умолчанию принято использовать следующие значения параметров системы: $T_1 = 64, T_2 = 192.$

Для извлечения информации используется формула (3.37).

3.3. Стойкие ЦВЗ, основанные на методах расширения спектра

3.3.1. Основные подходы и требования к встраиванию цифровых водяных знаков для защиты авторских прав

Стеганографическое встраивание, кроме задач скрытой передачи встроенной информации, зачастую используется и для решения задачи защиты авторских прав на мультимедиа продукцию (изображения, видеоматериалы, аудиокомпозиции). В этом случае встраиваемая информация выступает в качестве малозаметной, но стойкой «метки», встраиваемой в защищенный мультимедиа контейнер (изображение, видео, аудиозапись). При этом объем встраиваемой информации может быть незначительным – например, для идентификации видеозаписи и установления авторских прав достаточно 20–60-битного идентификатора, встроенного в видеозапись.

Подобные «метки», устойчивые и к **непреднамеренному** искажению (например, зашумлению или компрессии с потерями), и к **преднамеренным** попыткам удаления, в дальнейшем будем называть цифровыми водяными знаками (ЦВЗ, «digital watermark»).

Типичный сценарий использования ЦВЗ для защиты авторских прав может быть описан следующим образом.

Этап 1. На этапе создания цифрового мультимедийного контейнера (изображения, видеозаписи, аудиозаписи) ее автор *A* внедряет в данный носитель визуально малозаметную метку (цифровой водяной знак), содержащую уникальную информационную последовательность (уникальный идентификатор автора).

Этап 2. Далее мультимедийный контейнер с внедренным ЦВЗ распространяется автором A в сети интернет и с использованием других каналов связи.

Этап 3. Автор обнаруживает цифровую копию своего мультимедийного носителя (видео- или аудиозаписи, изображения), распространяемую без его ведома и без указания его авторства, автор A может подтвердить свои права на данную копию, извлекая из нее свой скрытый ЦВЗ.

В данном сценарии присутствует также нарушитель H, задачей которого является удаление из мультимедийного носителя встроенного ЦВЗ. В случае, если нарушитель делает невозможным извлечение ЦВЗ (Этап 3), данный нарушитель может распространять «очищенный от ЦВЗ» мультимедийный контейнер без указания авторства, в том числе присваивать себе авторство.

Разнообразные эвристические (т.е. не основанные на какой-либо математической модели или теории) методы встраивания и извлечения ЦВЗ разрабатывались рядом зарубежных авторов на протяжение 1990-х годов [38]. Математическая модель цифрового водяного знака, а также методы встраивания и извлечения ЦВЗ, основанные на данной модели, были предложены I.J.Cox и соавторами в работах [38, 39, 40].

Так, в работе [39] авторы впервые сформулировали детальный список требований к методам встраивания и извлечения цифрового водяного знака в мультимедийный контейнер. Данный список включал следующие требования:

1. Низкая визуальная заметность ЦВЗ. Данное требование предполагает, что наличие встроенного ЦВЗ не должно быть заметно при просмотре (прослушивании) защищенного мультимедийного носителя. В ряде систем защиты, использующих ЦВЗ, данное требование может быть сформулировано следующим образом – встраивание ЦВЗ не должно приводить к появлению видимых/слышимых искажений мультимедийного носителя (с точки зрения неподготовленного наблюдателя).

2. Стойкость ЦВЗ. Под стойкостью ЦВЗ авторы работ [38, 39, 40] подразумевают возможность извлечения ЦВЗ из мультимедийного носителя даже в случае его (носителя) значительного искажения. В качестве таких искажений могут выступать:

- распространенные процедуры обработки, фильтрации, компрессии мультимедийных сигналов, в том числе цифро-аналоговое и аналого-цифровое преобразование носителя;
- распространенные геометрические искажения носителя (изображения или видеозаписи), в том числе аффинные преобразования

изображения (кадра видеозаписи) и/или кадрирование (удаление части кадра);

– преднамеренные искажения, вносимые с целью удаления ЦВЗ, включая «вычитание» известного ЦВЗ из мультимедийного носителя, «смешивание» (усреднение) двух защищенных носителей с различными ЦВЗ с целью усложнить однозначное извлечение ЦВЗ.

3. Универсальность ЦВЗ. Данное свойство предполагает, что корректное встраивание ЦВЗ должно производиться в любой мультимедийный контейнер заданного формата и объема, вне зависимости от его содержательного наполнения. Например, ЦВЗ должен корректно встраиваться как в цифровую фотографию размером 4000×4000 пикселей, так и в изображение заданного размера, состоящее из пикселей с нулевой яркостью.

4. Уникальность ЦВЗ. Данное свойство предполагает, что информационная последовательность (ЦВЗ) должна однозначно идентифицировать автора/владельца мультимедийного носителя. Например, в системе защиты авторских прав с 10^6 зарегистрированными авторами в качестве ЦВЗ должен выступать 6-значный десятичный идентификатор автора (т.е. каждый автор должен получить уникальный 6-значный ЦВЗ).

Исходя из этих требований, в особенности требования стойкости ЦВЗ, авторами работ [38, 39, 40] было предложено использовать для встраивания ЦВЗ **наиболее визуально значимые** компоненты (области) мультимедийного контейнера. Данный подход противоположен тому, что традиционно используется для скрытой передачи информации путем ее стеганографического встраивания. Так, например, семейство алгоритмов встраивания информации в наименее значимые биты (НЗБ, LSB) построено таким образом, чтобы встраивание информации не затрагивало визуально значимые компоненты изображения (низкочастотные компоненты дискретноого косинусного преобразования или старшие биты значения яркости отдельного пикселя).

Наличие таких диаметрально противоположных подходов к встраиванию информации обосновывается следующим предположением: при встраивании в целью скрытой передачи информации основной угрозой считается **обнаружение** самого факта встраивания информации; в то же время при защите авторских прав с помощью ЦВЗ основной угрозой является **удаление или искажение** встроенной информации [38, 39, 40]. Таким образом, если встраивание ЦВЗ производится в визуально малозначимые компоненты изображения, такие как высокочастотные компоненты Фурье-

спектра или высокочастотные компоненты дискретного косинусного преобразования, младшие биты значения яркости, то ЦВЗ в общем случае будет уязвим к простейшим преднамеренным атакам, направленным на его удаление. Действительно, атакующий, предполагающий наличие ЦВЗ в мультимедийном носителе, может произвольно исказить (например, заполнить нулевыми значениями) все малозначимые компоненты данного носителя, не пытаясь извлечь ЦВЗ или определить его тип. В этом случае ЦВЗ будет гарантированно удален, а искаженный мультимедийный контейнер при этом не будет визуально (аудиально) отличаться от оригинала.

Следовательно, как утверждают авторы работ [38, 39, 40], единственным способом защитить ЦВЗ от подобных «универсальных» атак является встраивание информации исключительно в визуально/аудиально значимые компоненты носителя. Принцип выбора подобных компонент может различаться для различных методов встраивания и, разумеется, зависит от используемой модели человеческого восприятия. Так, предположим, что при встраивании ЦВЗ используется модель Contrast Sensitivity Function (модель зрительной системы, определяющая чувствительность зрительной системы человека к ярким объектам на изображении в зависимости от линейных размеров этих объектов, рис. 2.8).

В данном случае встраивание ЦВЗ должно затрагивать именно тот набор объектов на изображении-контейнере, для которых значение Contrast Sensitivity (2.16) является максимальным, т.е. визуальная система человека будет наиболее чувствительна к изменениям, касающимся именно данных объектов.

Далее авторами [38, 39, 40] формулируется следующая проблема, возникающая при встраивании ЦВЗ в **наиболее значимые** компоненты носителя: как встроить ЦВЗ в контейнер таким образом, чтобы снижение визуального качества носителя было минимальным, а ЦВЗ в то же время оставался стойким? Разумеется, самый очевидный подход – использование малозначимых компонент носителя – является неприемлемым в данном случае по причине существования «универсальной» атаки, рассмотренной выше.

Для ответа на данный вопрос авторами [38, 39, 40] было предложено использовать методы модуляции и кодирования информации, традиционно используемые при проектировании систем связи, устойчивых к случайному зашумлению и средствам радиоэлектронного подавления. Действительно, задачи встраивания и извлечения ЦВЗ могут быть пред-

ставлены как традиционные задачи передачи и приема информации по зашумленному каналу связи. В качестве зашумленного канала связи в данном случае выступает сам мультимедийный контейнер, в качестве передаваемой информации – ЦВЗ, а атака, направленная на удаление ЦВЗ, является частным случаем радиоэлектронного подавления. При этом ключевой для систем связи показатель «сигнал/шум» будет представлять собой соотношение амплитуды шума (т.е. яркости/громкости мультимедийного носителя, в который встраивается ЦВЗ) и амплитуды самого встраиваемого ЦВЗ. При использовании подобной аналогии авторы [38, 39, 40] формулируют задачу встраивания ЦВЗ как задачу надежной передачи информации в зашумленном канале связи с заданным максимальным значением «сигнал/шум». Традиционным подходом к решению данной задачи при проектировании систем связи является использование методов **расширения спектра.** В контексте проектирования систем связи данные методы предполагают такую модуляцию передаваемого сигнала, при которой максимально используется вся доступная передатчику и приемнику полоса пропускания канала связи. В контексте стеганографического встраивания информации использование подобных методов означает, что отдельный бит ЦВЗ встраивается не путем изменения отдельного пикселя или отсчета спектра изображения-носителя, а путем незначительного согласованного изменения большого числа таких отсчетов. Таким образом, искажения контейера, являющиеся результатом встраивания единственного бита ЦВЗ, равномерно распределяются по всем отсчетам/пикселям контейнера. Например, в случае встраивания бита ЦВЗ в видеозаписи можно проиллюстрировать подобный подход рис. 3.6.

На рис. 3.6а заштрихованными областями на серии кадров отмечены те области контейнера, которые были искажены при встраивании отельного бита ЦВЗ. В данном случае искажения, вызванные встраиванием одного бита ЦВЗ, равномерно распределены между кадрами, но при этом в рамках отдельного кадра искажения локализованы в рамках локальной прямоугольной области кадра. Аналогично на рис. 3.6б отдельный бит ЦВЗ встраивается в отдельный кадр видеопоследовательности и локализуется в рамках прямоугольного участка кадра.

Указанные способы встраивания не осуществляют «расширение спектра», как это понимается авторами [38, 39, 40] в контексте задач стеганографического встраивания. Встраивание с расширением спектра, предложенное авторами [38, 39, 40], проиллюстрировано на рис. 3.6в. Отсчеты

видеозаписи-контейнера, искаженные при встраивании отдельного бита ЦВЗ, не локализуются ни в рамках отдельного кадра видеозаписи (как на рис. 3.6б), ни в рамках локальной прямоугольной области всех кадров видеозаписи (как на рис. 3.6а). Фактически, встраиваемый бит ЦВЗ равномерно распределяется по всему трехмерному массиву пикселей в соответствии с некоторой псевдослучайной (т.е. кажущейся случайной для постороннего наблюдателя) «маской областей».

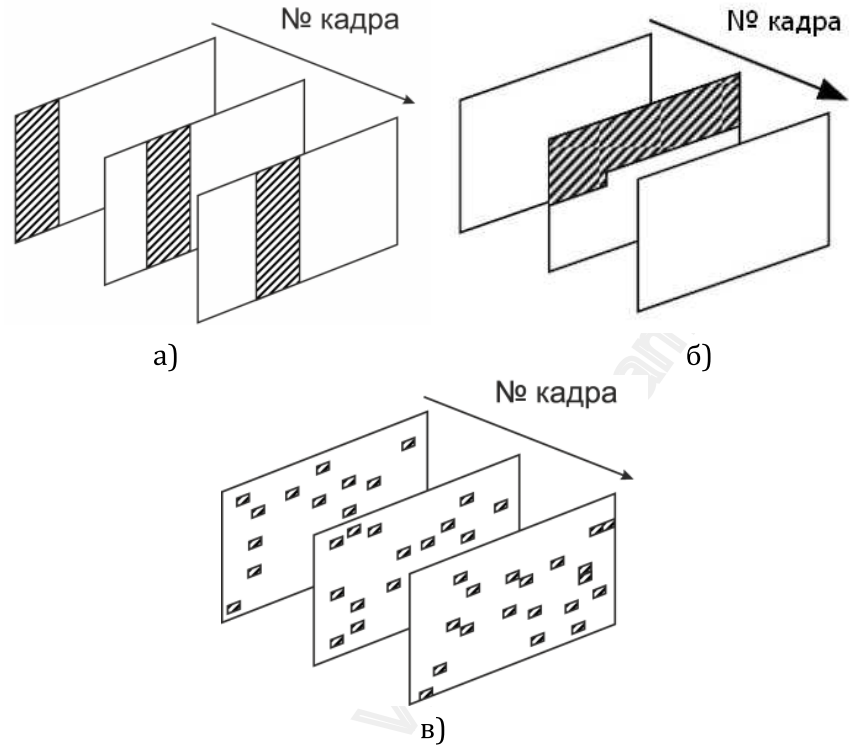


Рис. 3.6 – Распределение бита ЦВЗ по пикселям видеозаписи при встраивании а) без расширения спектра, с дублированием ЦВЗ для всех кадров, б) без расширения спектра и дублирования ЦВЗ, в) с расширением спектра

Ниже представлены наиболее известные методы встраивания ЦВЗ, основанные на методах модуляции с расширением спектра.

СВИ-8 (E_BLIND/D_LC)

Простейшая ЦВЗ-система с расширением спектра [2]

Для примера рассмотрим простейшую систему встраивания ЦВЗ с расширением спектра в пространственной области, а затем уже перейдём к системам, работающим в спектральной области.

Данная система позволяет встроить только один бит информации (то есть $\mathbf{b} \in \{0,1\}$) в полутоновое изображение-контейнер C размерами $N_1 \times N_2$ пикселей. Для встраивания информации формируется псевдослучайный двумерный массив бинарных значений ЦВЗ W_r, размерами совпадающий с исходным контейнером и содержащий нормально распреде-

лённые действительные числа с нулевым средним и единичной дисперсией:

$$W_r(n_1, n_2) \sim N(0,1). \quad (3.39)$$

Массив W_r может генерироваться на основе ключа $\mathbf{k}$ (например, ключ может использоваться в качестве начального значения, seed, генератора псевдослучайных чисел).

Далее производится модуляция с расширением спектра с использованием исходного бита ЦВЗ $\mathbf{b}$.

$$W_{mod}(n_1, n_2) = \begin{cases} W_r(n_1, n_2), \text{если } \boldsymbol{b} = 1, \\ -W_r(n_1, n_2), \text{если } \boldsymbol{b} = 0. \end{cases}$$

Встраивание ЦВЗ осуществляется по аддитивной формуле

$$C^W(n_1, n_2) = C(n_1, n_2) + \alpha \cdot W_{mod}(n_1, n_2), \quad (3.40)$$

где $\alpha > 0$ – коэффициент усиления ЦВЗ.

Для извлечения встроенного бита информации рассчитывается значение линейной корреляции анализируемого изображения-контейнера $\widetilde{C^W}$ с шаблоном W_r, который может быть заново сформирован на основе ключа $\mathbf{k}$:

$$\rho\left(\widetilde{C^W}, W_r\right) = \frac{1}{N_1 N_2} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \widetilde{C^W}(n_1, n_2) \cdot W_r(n_1, n_2), \quad (3.41)$$

после чего полученная величина сравнивается с порогом для принятия решения о наличии ЦВЗ и его значении:

$$\boldsymbol{b^R} = \begin{cases} 1, & \rho\left(\widetilde{C^W}, W_r\right) > \tau_{lc}, \\ 0, & \rho\left(\widetilde{C^W}, W_r\right) < -\tau_{lc}, \\ \text{нет ЦВЗ}, & \text{иначе}. \end{cases} \quad (3.42)$$

Данная система хорошо иллюстрирует характерную особенность метода расширения спектра, указанную ранее: встраивание небольшого объёма информации (в данном случае – одного бита) происходит за счёт малого изменения значительного числа пикселей изображения-контейнера (в данном случае – всех).

Данный подход имеет следующие преимущества.

Во-первых, т.к. вносимые при встраивании бита $\mathbf{b}$ искажения оказываются распределены по большому числу пикселей, то амплитуда искажений, вносимых в отдельный пиксель, может быть мала и при этом ЦВЗ может быть извлечен. Действительно, указанный выше алгоритм извлечения ЦВЗ представляет собой частный случай согласованной фильтрации (т.н. коррелятор). Подобная фильтрация при использовании известного образца

сигнала $W_{mod}(n_1, n_2)$ позволяет устойчиво обнаруживать сигнал на фоне помех (аддитивного белого шума) даже в случае, когда амплитуда помех в каждом отдельном пикселе изображения многократно превосходит амплитуду самого сигнала $W_{mod}(n_1, n_2)$.

Во-вторых, нарушитель H, если он попытается удалить встроенный ЦВЗ путем дополнительного искажения изображения-контейнера, не сможет определить малое подмножество пикселей, искажение которых приведет к гарантированному удалению ЦВЗ. Более того, для гарантированного удаления ЦВЗ нарушитель вынужден будет вносить в изображение искажения с амплитудой, значительно превышающей амплитуду самого ЦВЗ.

Разумеется, если нарушителю известен сигнал $W_{mod}(n_1, n_2)$, то для удаления ЦВЗ ему необходимо будет просто вычесть его из $C^W(n_1, n_2)$. Таким образом, ключ встраивания $\mathbf{k}$ и двумерный массив $W_r(n_1, n_2)$ должны быть сохранены в секрете для обеспечения стойкости ЦВЗ к преднамеренным атакам.

Очевидный недостаток рассмотренной системы – возможность встраивания лишь одного бита информации, однако на её основе легко могут быть построены более интересные и практически значимые СВИ. Например, рассмотрим следующую модификацию системы СВИ-8 (E_BLIND/D_LC).

Пусть необходимо встроить в изображение-контейнер в качестве ЦВЗ битовую строку $\mathbf{b}$, состоящую из отдельных бит $\mathbf{b_k}$, $k \in \{1, K\}$. Пусть кроме массива $W_r(n_1, n_2)$ и полутонового изображения-контейнера C размерами $N_1 \times N_2$ пикселей при встраивании ЦВЗ используется также «карта встраивания»: массив $M(n_1, n_2)$ размером $N_1 \times N_2$ элементов, причем $M(n_1, n_2) \in \{1, K\}$. Кроме того, предполагается, что $M(n_1, n_2)$ также генерируется на основе ключа $\mathbf{k}$, т.е. ключ используется в качестве начального значения генератора псевдослучайных равномерно распределенных целых чисел).

Тогда модуляция с расширением спектра производится следующим образом:

$$W_{mod}(n_1, n_2) = \begin{cases} W_r(n_1, n_2), \text{если } \mathbf{b}_{M(n_1,n_2)} = 1, \\ -W_r(n_1, n_2), \text{если } \mathbf{b}_{M(n_1,n_2)} = 0. \end{cases}$$

Модулированный сигнал содержит в себе информацию о всех битах ЦВЗ; при этом число пикселей изображения-контейнера, по которым будет распределен отдельный бит ЦВЗ, по сравнению с СВИ-8 (E_BLIND/D_LC) снизится в среднем в K раз.

Встраивание ЦВЗ также осуществляется по аддитивной формуле

$$C^W(n_1, n_2) = C(n_1, n_2) + \alpha \cdot W_{mod}(n_1, n_2), \quad (3.43)$$

где $\alpha > 0$ – коэффициент усиления ЦВЗ.

Процедура извлечения ЦВЗ отличается от описанной ранее. Она также основана на использовании коэффициента корреляции, но проходит в несколько этапов, независимо для каждого из K бит ЦВЗ.

Так, для извлечения k-го бита ЦВЗ формируется временный массив

$$W_{temp}(n_1, n_2) = \begin{cases} W_r(n_1, n_2), & \text{если } M(n_1, n_2) = k, \\ 0, & \text{иначе.} \end{cases} \quad (3.44)$$

Фактически, данный массив является копией массива $W_r(n_1, n_2)$, из которого удалены (заменены нулями) все элементы, которые при встраивании не были использованы для модуляции k-го бита ЦВЗ. Далее вычисляется коэффициент корреляции

$$\rho\left(\widetilde{C^W}, W_r\right) = \frac{1}{N_k} \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \widetilde{C^W}(n_1, n_2) \cdot W_{temp}(n_1, n_2), \quad (3.45)$$

где N_k - количество элементов в массиве $M(n_1, n_2)$, равных k.

после чего полученная величина сравнивается с порогом для принятия решения о наличии $\mathrm{k}-$ го бита ЦВЗ и его значении:

$$\boldsymbol{b_k^R} = \begin{cases} 1, & \rho\left(\widetilde{C^W}, W_r\right) > \tau_{lc}, \\ 0, & \rho\left(\widetilde{C^W}, W_r\right) < -\tau_{lc}, \\ \text{нет ЦВЗ}, & \text{иначе.} \end{cases} \quad (3.46)$$

Следует уточнить, что в данном модифицированном алгоритме для извлечения ЦВЗ необходимо точно знать значения следующих параметров, использованных при встраивании ЦВЗ:

1) массив $W_r(n_1, n_2)$,

2) «карту встраивания» $M(n_1, n_2)$.

Как и в предыдущем случае, данные параметры должны сохраняться в секрете для обеспечения стойкости ЦВЗ к преднамеренным атакам (попыткам удаления ЦВЗ).

Недостатком данной модификации алгоритма встраивания ЦВЗ является ее меньшая, по сравнению с исходным алгоритмом, стойкость к зашумлению изображения-контейнера и преднамеренным атакам. Действительно, при увеличении числа K встраиваемых бит ЦВЗ $\mathbf{b_k}$ пропорционально уменьшается и число пикселей изображения-контейнера, по которым оказывается распределен каждый бит ЦВЗ.

Таким образом, концепция встраивания информации в цифровые сигналы с расширением спектра состоит в распределении встраиваемой

информации (ЦВЗ или секретного сообщения) внутри контейнера, имеющего гораздо больший размер, на основе функции, зависящей от секретного ключа.

3.3.2. Системы встраивания информации в области преобразования с расширением спектра

Перейдём к рассмотрению СВИ с расширением спектра в области преобразования. В подобных системах при встраивании ЦВЗ модифицируются не отдельные пиксели изображения-контейнера, а отдельные коэффициенты, полученные в результате применения некоторого интегрального преобразования к исходному изображению-контейнеру (например, дискретного преобразования Фурье, дискретного косинусного преобразования, вейвлет-преобразования и др). Одна из первых и наиболее известных подобных систем была предложена в работе [41] и представляла собой применение концепции встраивания информации с расширением спектра в области дискретного косинусного преобразования.

СВИ-9 (Cox et al.)

Встраивание ЦВЗ в изображения с расширением спектра [41]

Встраивание информации

Особенностью данной системы является использование так называемого «ЦВЗ нулевой длины» (zero-bit watermarking). В этом случае, фактически, ни один бит информации не встраивается и не извлекается из изображения-контейнера – при извлечении ЦВЗ детектор может дать лишь один из двух ответов «ЦВЗ с ключом $\mathbf{k}$ встраивался в данное изображение» или «ЦВЗ с ключом $\mathbf{k}$ не встраивался в данное изображение». В этом случае, очевидно, ни один бит информации не может быть передан в качестве ЦВЗ (как это было в СВИ-8).

Как и в предыдущей рассмотренной системе (СВИ-8), перед встраиванием ЦВЗ производится модуляция с расширением спектра, для чего на основе ключа встраивания $\mathbf{k}$ генерируется вектор Ω длиной $N_\Omega = 1000$ чисел, где $\Omega \in \mathbb{R}^1_{[N_\Omega]}$ и элементы Ω представляют собой псевдослучайные числа, распределенные по гауссовскому закону.

Для модификации отбираются 1000 самых больших коэффициентов глобального дискретного косинусного преобразования контейнера в *змеевидной развёртке*, как показано на рис. 3.7 (при этом нулевой отсчёт $C_{DOT}(0,0)$ не изменяется). Результатом данного отбора является матрица признаков контейнера $f \in \mathbb{R}^1_{[N_\Omega]}$. Не будем конкретизировать точную фор-

мулу расчёта f, поскольку она окажется весьма громоздкой. Встраивание информации в пространстве признаков осуществляется по формуле

$$f^W(m) = f(m)\big(1 + \alpha \cdot \Omega(m)\big). \quad (3.47)$$

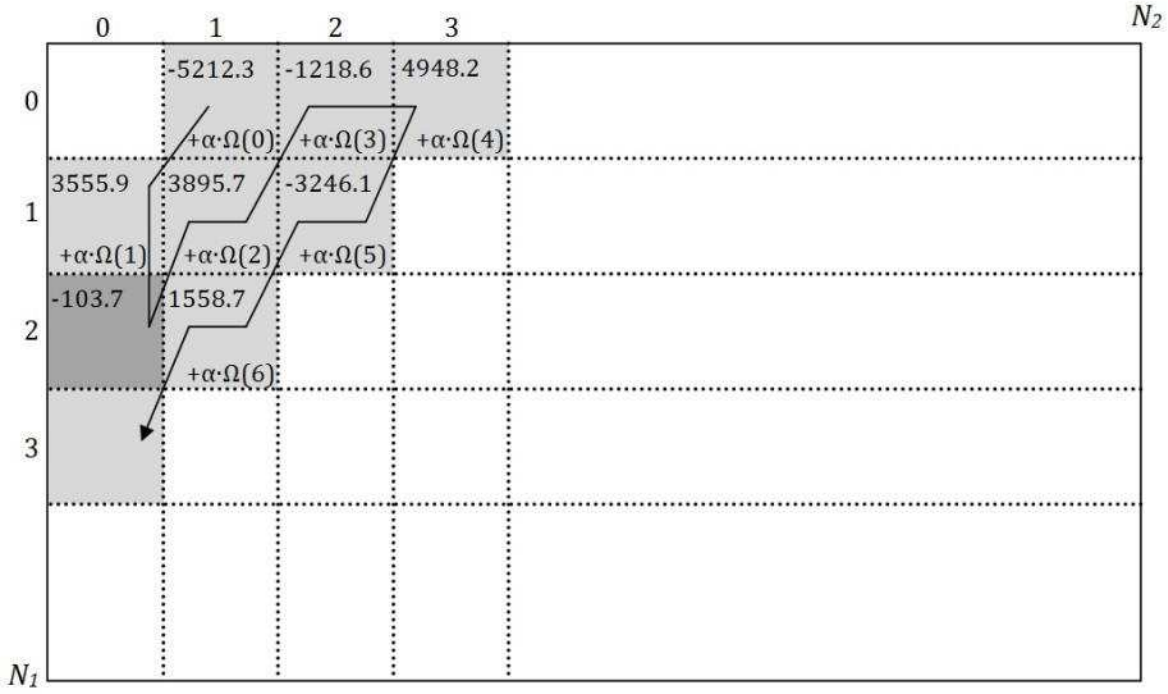


Рис. 3.7 – Схема отбора коэффициентов ДКП для модификации в СВИ-9 (Cox et al.). В каждой ячейке в качестве иллюстрации отображены значения соответствующих компонент ДКП изображения "Lenna" (Рис. 3.3а)

Далее измененные в результате значения коэффициентов $f^W(m)$ объединяются с остальными коэффициентами ДКП изображения-контейнера (при этом модифицированные коэффициенты из $f^W(m)$ замещают исходные коэффициенты $f(m)$ в общей матрице коэффициентов ДКП, рис. 3.7) и используются для вычисления обратного ДКП. Результат обратного ДКП – изображение, совпадающее с оригинальным изображением-контейнером по размеру в пикселях – и является изображением C^W со встроенным ЦВЗ:

$$C^W(n_1, n_2) = \mathcal{F}^{-1}\big(C^W_{DCT}(m_1, m_2)\big). \quad (3.48)$$

Извлечение информации

Для извлечения ЦВЗ требуется исходное изображение-контейнер, по которому рассчитывается вектор f и которому ставится в соответствие вектор признаков принятого носителя информации $\widetilde{f^W}$. При этом вектор f выступает в качестве «карты», определяющей, с каких именно ячеек матрицы коэффициентов ДКП изображения C^W должны быть отобраны коэффициенты для расчета $\widetilde{f^W}$.

Извлечение модулированного сигнала, использованного для встраивания ЦВЗ с расширением спектра, осуществляется по формуле

$$\tilde{\Omega}(m) = \frac{\widetilde{f^W}(m) - f(m)}{\alpha \cdot f(m)}, \tag{3.49}$$

то есть путём прямого выражения Ω из формулы (3.47).

Далее осуществляется детектирование (то есть проверка наличия встроенного) ЦВЗ, которое может осуществляться по формуле (1.1) с функцией близости вида*

$$\rho\left(\Omega, \tilde{\Omega}\right) = \frac{\sum_{n=0}^{\mathrm{N}_\Omega - 1} \Omega(m)\tilde{\Omega}(m)}{\sqrt{\sum_{m=0}^{\mathrm{N}_\Omega - 1} \Omega^2(m)} \cdot \sqrt{\sum_{m=0}^{\mathrm{N}_\Omega - 1} \tilde{\Omega}^2(m)}}. \tag{3.50}$$

Если значение ρ не меньше некоторого порога τ, то детектор ЦВЗ срабатывает, в противном случае принимается решение об отсутствии встроенного водяного знака в рассматриваемом изображении.

Особо стоит отметить, что подобный детектор позволяет обнаружить не наличие ЦВЗ «в целом», а только наличие ЦВЗ, встроенного с использованием конкретного ключа k. Если же ЦВЗ был встроен в изображение с помощью ключа $\mathbf{k}$, а извлекается с использованием ключа $\mathbf{k}'$, отличного от $\mathbf{k}$, то ЦВЗ не будет обнаружен.

Таким образом, для обнаружения ЦВЗ в изображении необходимо точное знание следующих параметров встраивания:

1. Ключа встраивания $\mathbf{k}$ или вектора Ω.

2. Исходного изображения-контейнера C.

Следует отметить, что знание коэффициента α желательно, но не обязательно при обнаружении ЦВЗ. Действительно, формула нормированной взаимной корреляции, используемая при вычислении $\rho\left(\Omega, \tilde{\Omega}\right)$, даст одинаковый результат и для исходного вектора $\tilde{\Omega}(m)$, и для вектора $\alpha \cdot \tilde{\Omega}(m)$. Таким образом, если при обнаружении ЦВЗ исходное значение α неизвестно, то его можно принять равным 1.

Достоинством алгоритма является то, что благодаря выбору наиболее значимых коэффициентов ДКП водяной знак является стойким к сжатию, поэлементным преобразованиям, процедурам обработки скользящим

---

* В оригинальной работе [27] в знаменателе отсутствует длина вектора Ω, однако отмечается, что использование конкретной функции близости не является принципиальным.

окном, а также многим другим видам обработки изображений. К недостаткам данного алгоритма стоит отнести трудоёмкость операции вычисления двумерного ДКП всего изображения, а также необходимость использования исходнго контейнера на этапе извлечения информации.

Для устранения последнего недостатка в работе [42] была предложена модификация СВИ-9 со слепым детектором, т.е. с детектором, не требующим использования исходного изображения-контейнера.

СВИ-10 (Piva et al.)

Слепая модификация системы Cox et al. [42]

Для чего требуется исходное изображение в СВИ-9? Во-первых, чтобы отыскать N_Ω наибольших ДКП-коэффициентов и проранжировать их по порядку, во-вторых, чтобы вычислить оценку $\widetilde{\Omega}$ по формуле (3.49). Для исключения необходимости ранжирования спектральных компонент по убыванию в алгоритм встраивания внесена очевидная корректировка: для встраивания всегда отбираются одни и те же коэффициенты (среднечастотные), отсортированные в порядке змеевидной развёртки. Вместо формулы (3.49) расчёт оценки встроенной последовательности происходит следующим образом:

$$\tilde{\Omega}(m) = \widetilde{f^W}(m), \tag{3.51}$$

то есть сам носитель информации (в форме матрицы признаков) используется в качестве оценки ЦВЗ. Разумеется, такая оценка в случае встраивания по формуле (3.47) далека от истины, поэтому меняется и формула встраивания:

$$f^W(m) = f(m) + \alpha \cdot |f(m)| \cdot \Omega(m). \tag{3.52}$$

Оценка близости рассчитывается как

$$\rho\left(\Omega, \tilde{\Omega}\right) = \sum_{n=0}^{\mathrm{N}_\Omega - 1} \Omega(m)\tilde{\Omega}(m). \tag{3.53}$$

Причину использования (3.52) вместо (3.47) легко понять, подставив (3.51) и (3.52) в (3.53):

$$\rho\left(\Omega, \tilde{\Omega}\right) = \sum_{n=0}^{\mathrm{N}_\Omega - 1} \Omega(m)\widetilde{f^W}(m) \approx \sum_{n=0}^{\mathrm{N}_\Omega - 1} \Omega(m)f(m) + \alpha \sum_{n=0}^{\mathrm{N}_\Omega - 1} \Omega^2(m) \cdot |f(m)|.$$

Второе слагаемое всегда больше нуля, в то время как первое ввиду случайности $\Omega(m)$ и предполагаемой однородности выбранных $f(m)$ по абсолютной величине (поскольку это среднечастотные коэффициенты) может иметь произвольный знак, но небольшое значение по модулю. Та-

ким образом, при детектировании встроенной последовательности $\rho\left(\Omega, \tilde{\Omega}\right)$ будет иметь большое положительное значение.

Для повышения точности детектирования ЦВЗ длина встраиваемой последовательности увеличивается относительно принятого в СВИ-9 значения $N_\Omega = 1000$. В СВИ-10 длина не фиксирована, а может варьироваться в зависимости от размера изображения. В частности, для изображений размером 512×512 для встраивания рекомендуется использовать коэффициенты ДКП со строки 180 до строки 250 (в зигзагообразной развёртке). В этом случае длина последовательности составляет около 15000.

Ещё одно изменение предназначено для снижения визуальных искажений при встраивании ЦВЗ и заключается в том, что C^W формируется по формуле

$$C^W(n_1, n_2) = \mathcal{F}^{-1}\left(C^W_{DOT}(m_1, m_2)\right) \cdot B(n_1, n_2) + \\ + C(n_1, n_2) \cdot \left(1 - B(n_1, n_2)\right), \tag{3.54}$$

где

$$B(n_1, n_2) = \frac{C_{MSE,9\times9}(n_1, n_2)}{\max\limits_{i.j} C_{MSE,9\times9}(i, j)}. \tag{3.55}$$

В последней формуле $C_{MSE,9\times9}(n_1, n_2)$ – результат отыскания локального СКО изображения C в скользящем окне размерами 9×9.

Таким образом, в областях низкой дисперсии (то есть достаточно однородных по яркости) $B(n_1, n_2) \to 0$, значит, $C^W(n_1, n_2)$ практически совпадает с $C(n_1, n_2)$. В областях, характеризуемых высокой дисперсией (то есть на границах областей и в текстурированных регионах), напротив, основную часть в сумме (3.54) составляет $\mathcal{F}^{-1}\left(C^W_{DOT}(m_1, m_2)\right)$. На рис. 3.8 приведён пример поля $B(n_1, n_2)$ для конкретного изображения-контейнера.

В заключение отметим, что авторы данной системы уточнили способ расчёта порога T_ρ:

$$T_\rho = 3{,}3\sqrt{\frac{2\sigma^2_{\tilde{f}}}{N_\Omega}}, \tag{3.56}$$

где $\sigma^2_{\tilde{f}}$ – оценка дисперсии матрицы $\widetilde{f^W}$.

Вывод данной формулы можно найти в статье [43].

СВИ-10, как и его предшественник, обладает высокой стойкостью к ряду преобразований контейнера информации, однако может использо-

ваться в сценариях, которые не предполагают возможности доступа к исходному контейнеру на этапе извлечения информации.

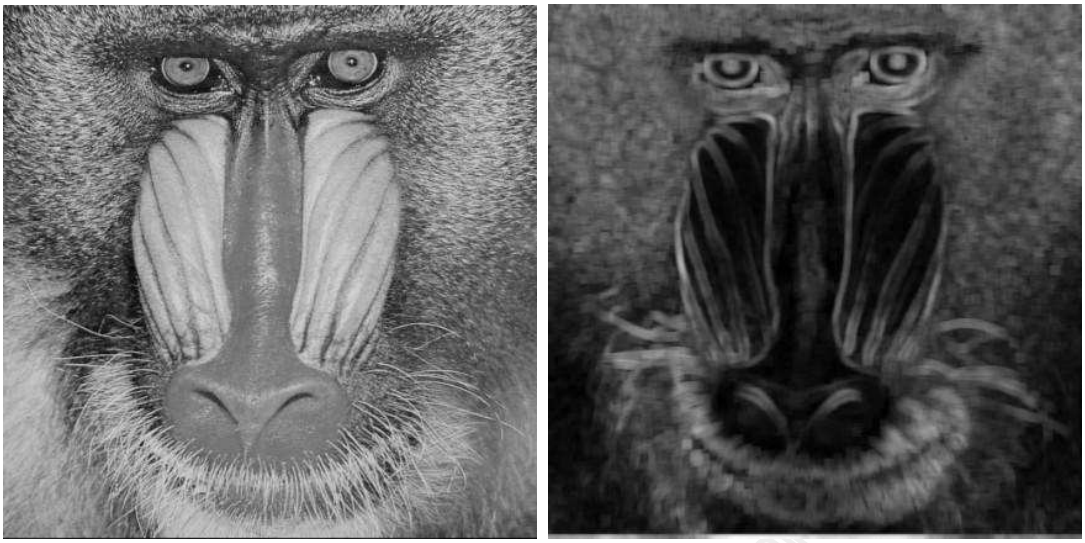


Рис. 3.8 – Полутоновое изображение и его поле локального СКО, соответствующее матрице $B(n_1, n_2)$ в СВИ-10 (Piva et al.)

3.3.3. Методы генерации шумоподобных последовательностей для встраивания ЦВЗ с расширением спектра

Отдельной важной задачей при разработке систем встраивания ЦВЗ является задача генерации псевдослучайных последовательностей, предназначенных для модуляции ЦВЗ с расширением спектра. Генерация таких последовательностей, как уже было отмечено в предыдущем подпараграфе, производится на основе стеганографического ключа.

Самый очевидный и простой способ генерации подобных последовательностей – использование известных генераторов псевдослучайных чисел – зачастую приводит к снижению стойкости встроенного ЦВЗ, и к преднамеренным атакам, и к зашумлению мультимедийного контейнера, в который ЦВЗ был встроен. Кроме того, неочевидной, но важной проблемой является проблема возникновения коллизий при извлечении ЦВЗ – ситуаций, когда ЦВЗ может быть извлечён из контейнера не только с помощью исходного ключа встраивания, но и с помощью нескольких других, «ложных» ключей.

Кроме того, использование общеизвестных генераторов псевдослучайных чисел для синтеза последовательностей может приводить к появлению «сильных» и «слабых» ключей встраивания ЦВЗ, т.е. ключей, при использовании которых в одном и том же алгоритме встраивания стойкость ЦВЗ к атакам и зашумлению будет значительно различаться. Проил-

люстрировать эту проблему можно на тривиальном примере – пусть существует ключ, который при использовании его в качестве начального значения генератора псевдослучайных чисел порождает последовательность $W_r(n_1, n_2)$, состоящую преимущественно из нулей. В данном случае, т.к. модуляция с расширением спектра фактически производиться не будет, нарушитель сможет достаточно легко оценить и статистические характеристики встроенного ЦВЗ, и локализовать пиксели, которые были модифицированы при встраивании конкретного бита ЦВЗ.

Указанные особенности схем встраивания ЦВЗ определяют ряд специфичных требований к генерируемым последовательностям и к алгоритму их формирования на основе стеганографического ключа. К таким требованиям можно отнести (согласно [44, 45, 46, 47]):

1. Возможность установления однозначного соответствия (биекции) между любым допустимым значением ключа пользователя и соответствующей этому ключу последовательностью W_r. Далее будем предполагать, что все возможные последовательности, сгенерированные на основе допустимых ключей k, образуют множество $\widetilde{W}_r$.

2. Возможность генерации последовательности на основе произвольно выбранного ключа за фиксированное время, не зависящее от значения ключа.

3. Возможность генерировать последовательность-метку W_r большой длины (до нескольких тысяч бит), что необходимо для обеспечения устойчивости ЦВЗ к аддитивному шуму при использовании корреляционного детектора ЦВЗ, а также для устойчивости ЦВЗ к ряду специфичных атак, направленных на приближенное вычисление последовательности W_r прямым перебором [48].

4. Фиксированное значение «минимального циклического расстояния» $\lambda = min_{\Delta h} \sum_{h=1}^{L} w'_h \oplus w''_{(h+\Delta h) mod L}$ (минимальное расстояние Хэмминга с учетом циклического сдвига [49, 50, 51]) между любыми двумя последовательностями из множества $\widetilde{W}_r$, где w_h – h-й элемент последовательности W_r. Данное требование позволяет избежать так называемых коллизий при определении авторства ЦВЗ (коллизией в данном случае называется ситуация, когда детектор корректно обнаруживает ЦВЗ даже в том случае, когда вместо последовательности W'_r, использованной для встраивания, использует последовательность W''_r, отличную от W'_r). Кроме того, данное требование позволяет обеспечивать устойчивость ЦВЗ к широкому классу атак, направленных на приближенное вычисление ЦВЗ [48]. Исполь-

зование минимального циклического расстояния λ вместо расстояния Хэмминга в данном случае обусловлено требованием устойчивости ЦВЗ к кадрированию и повороту (при встраивании ЦВЗ в области преобразования Фурье–Меллина [52, 53, 54]).

5. Мощность множества $\widetilde{W}_r$, т.е. число возможных ключей встраивания, должна быть достаточной для защиты от вычисления W_r' методом прямого перебора всех возможных ключей (так называемая brute-force attack). Мы будем предполагать, что мощность $\widetilde{W}_r$, требуемая для защиты от атак методом прямого перебора, должна составлять не менее 2^{40} ключей.

6. Возможность генерировать последовательности с фиксированным весом (соотношением числа единиц и нолей в бинарной последовательности). Данное требование обусловлено необходимостью обеспечивать фиксированное соотношение сигнал/шум при встраивании ЦВЗ в спектральной области [49] вне зависимости от свойств конкретного выбранного пользователем ключа.

7. Малая схожесть (в смысле значения максимума взаимной корреляционной функции) последовательности W_r и изображения-контейнера. Другими словами, сгенерированная последовательность W_r не должна быть схожа с естественными изображениями-контейнерами (цифровыми фотоизображениями, кадрами видеозаписей и т.д.). В противном случае, если W_r «имитирует» некоторое естественное изображение или графический паттерн, возможно возникновение ситуаций ложного обнаружения ЦВЗ, т.е. обнаружения ЦВЗ даже в тех изображениях, куда ЦВЗ не встраивался.

Требования 1 и 4 особенно критичны в случаях, когда ЦВЗ применяется для установления несанкционированного распространения мультимедийных данных и для подтверждения авторства. В данных случаях предполагается, что каждому автору (правообладателю) поставлен в соответствие уникальный ключ встраивания. На этапе встраивания ЦВЗ сформированная на основе ключа последовательность W_r используется для маркировки всех мультимедийных данных данного автора. Коллизия, т.е. неоднозначность в определении детектором последовательности W_r, а следовательно, и неоднозначность в определении авторства, является в данном случае недопустимой.

Как показано в [45, 46, 47], подавляющее большинство существующих алгоритмов встраивания ЦВЗ, предназначенных для подтверждения

авторства и установления фактов несанкционированного распространения данных, при формировании последовательностей-меток не предусматривают защиту от коллизий и атак при формировании ЦВЗ. Наиболее распространенным подходом в данном случае является использование распространенных генераторов бинарных псевдослучайных последовательностей для синтеза W_r. Таким образом, указанные выше требования 4 и 6 не учитываются при использовании данного подхода.

Некоторые из существующих алгоритмов (например, алгоритм [39]) предполагают использование *M*-последовательностей полного периода. Данные последовательности удовлетворяют большинству представленных выше требований, в том числе требованию 4 (максимум циклического расстояния Хэмминга для *M*-последовательностей известен для любых двух последовательностей заданной длины). Это позволяет повысить устойчивость встраиваемого ЦВЗ к шуму и избежать коллизий при формировании последовательностей, но не обеспечивает достаточной мощности множества $\widetilde{W}_r$ для защиты от атак прямого перебора ключа.

В работах [55, 47] предложены алгоритмы генерации последовательностей, схожих с *M*-последовательностями по свойствам, но обеспечивающие гораздо большую (на несколько порядков) мощность $\widetilde{W}_r$при одинаковой длине последовательности.

Далее в рамках данного пособия будут рассмотрены основные свойства *M*-последовательностей при их применении для модуляции ЦВЗ с расширением спектра. Несмотря на их уже упомянутый недостаток (низкая стойкость к перебору ключей), они остаются самыми простыми в программной и аппаратной генерации, и, кроме того, традиционно используются в методах модуляции с расширением спектра. Алгоритмы, описанные в [55, 47], хоть и обеспечивают более полное соответствие рассмотренным выше требованиям, остаются более сложными в реализации и более вычислительно затратными.

Рассмотрим более подробно так называемые бинарные *M*-последовательности полного периода. Традиционно *M*-последовательности используются для модуляции и кодирования цифровых сигналов с расширением спектра и согласно [54] обладают следующими свойствами.

1. Свойство сбалансированности.

Каждая бинарная М-последовательность полного периода, состоящая из $2^{\mathrm{m}}-1$ бинарных разрядов, состоит из $2^{\mathrm{m}-1}-1$ нулей и $2^{\mathrm{m}-1}$ единиц.

2. Свойство сбалансированности серий.

Каждая бинарная М-последовательность полного периода, состоящая из $2^{\mathrm{m}}-1$ бинарных разрядов, содержит равное (или различающееся на единицу) количество всех возможных подпоследовательностей заданной длины (до m включительно). Это свойство, в частности, означает, что в составе М-последовательности полного периода, состоящей из $2^{\mathrm{m}}-1$ бинарных разрядов, содержится равное число двухсимвольных подпоследовательностей (00, 01, 10, 11), равное число трехсимвольных подпоследовательностей (000, 001, 010, 011, 100,101, 110, 111) и т.д.

3. Свойство автокорреляционной функции.

Каждая бинарная М-последовательность полного периода, состоящая из $2^{\mathrm{m}}-1$ бинарных разрядов, имеет периодическую автокорреляционную функцию следующего вида: нулевой отсчет автокорреляционной функции равен 1, все боковые пики (значения автокорреляционной функции для ненулевых смещений) равны $-1/\mathrm{N}$, где $\mathrm{N}=2^{\mathrm{m}}-1$ – длина М-последовательности. Из этого свойства также следует свойство наличия «минимального циклического расстояния», равного для всех М-последовательностей заданной длины: $\lambda \approx N/2$ (т.е. при любом взаимном циклическом сдвиге двух М-последовательностей эти последовательности будут различаться примерно в половине бинарных символов).

Пример автокорреляционной функции *М*-последовательности полного периода приведена на рис. 3.9.

Как можно понять из приведенных свойств *М*-последовательностей, данные последовательности удовлетворяют требованию 4, требованию 6 (вес, т.е. соотношение числа единиц и нулей, *М*-последовательности всегда равен 0,5) и требованию 7. По требованию 7 стоит отдельно отметить следующее: как косвенно указано в свойстве сбалансированности серий, *М*-последовательность достаточной длины (более 1000–2000 бинарных символов) будет статистически неотличима от выхода генератора псевдослучайных бинарных последовательностей, т.е. фактически будет представлять собой «белый шум».

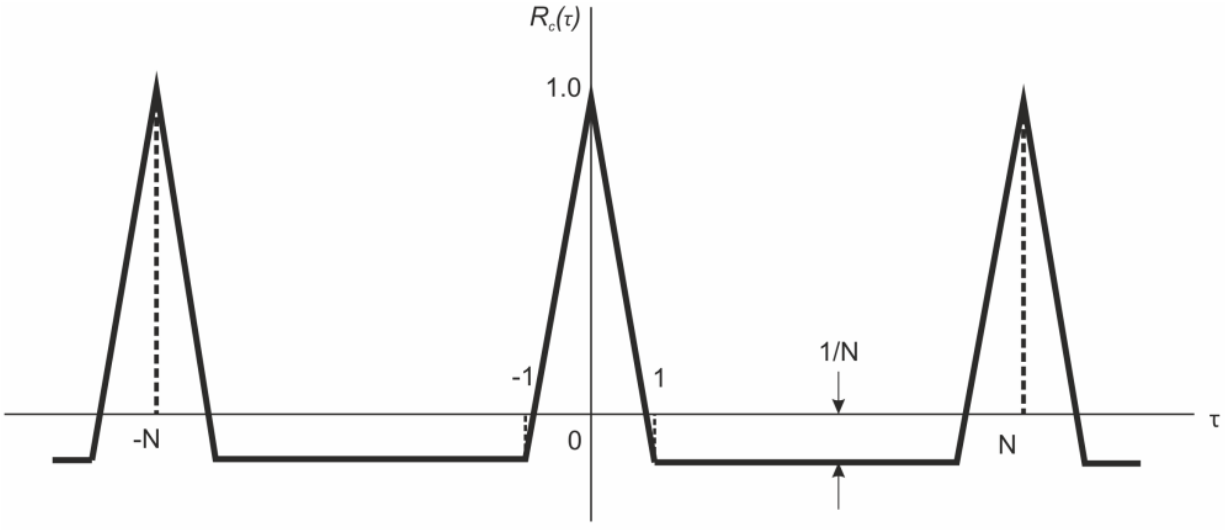


Рис. 3.9 – Вид автокорреляционной функции М-последовательности полного периода (длина последовательности N бит)

Чтобы выяснить, насколько удовлетворяют *M*-последовательности требованиям 1-3 и требованию 6, необходимо подробно рассмотреть алгоритм генерации данных последовательностей.

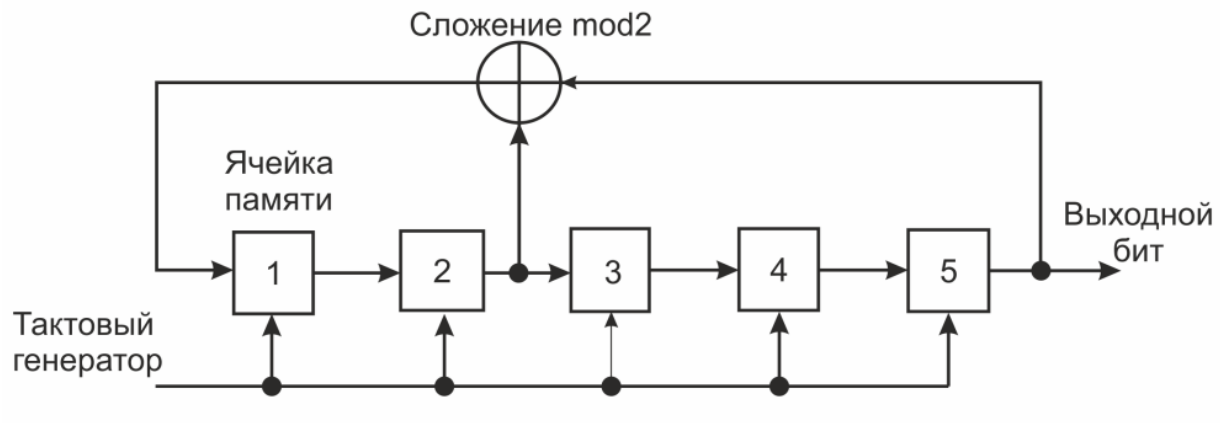
Традиционным способом синтеза *M*-последовательностей является использование **регистров связи с линейной обратной связью** (РСЛОС). Данная схема обладает важным преимуществом – простотой аппаратной реализации (т.к. требует наличия только тактового генератора, сумматора и ячеек памяти, объединенных в схему с обратной связью).

Пример РСЛОС приведен на рис. 3.10. Рассмотрим более подробно его основные функциональные элементы и принцип работы.

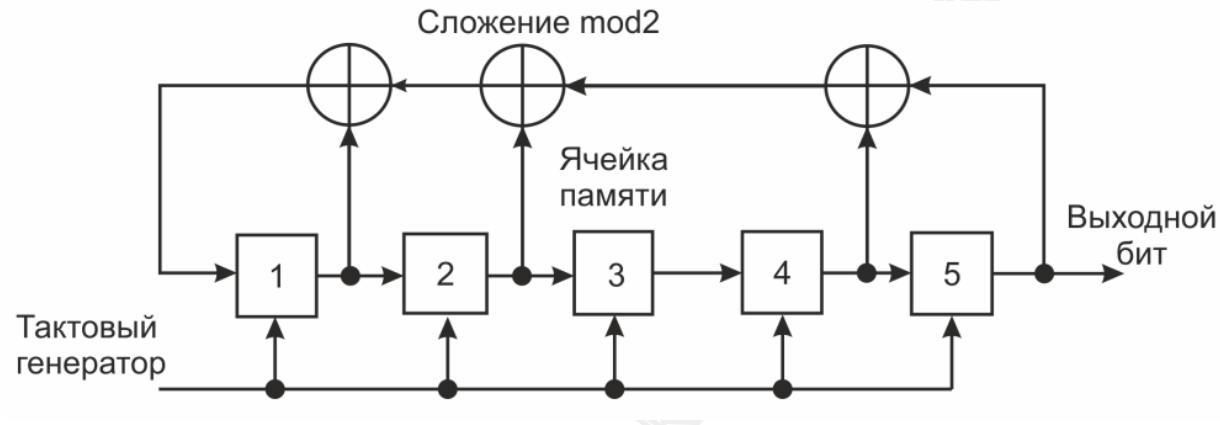
Главным параметром, определяющим работу указанной схемы, является структура обратной связи, подключенной к некоторым из бинарных ячеек памяти. Традиционно принято описывать структуру обратной связи, объединяющей ячейки памяти РСЛОС, с помощью последовательности целых чисел. Так, на рис. 3.10а схема РСЛОС может быть описана последовательностью [5, 2]. Так, если пронумеровать ячейки памяти от 1 до m, как указано на рис. 3.10 (так, что ближайшая к выходному биту ячейка имеет наибольший номер), то последовательность [5, 2] определит номера тех ячеек, справа от которых расположены отводы на **«Сложение mod2»**.

Рассмотрим более подробно принцип работы указанных на рис. 3.10 РСЛОС.

Для запуска РСЛОС необходимо произвести его инициализацию, т.е. заполнение значениями всех ячеек памяти. В качестве начального заполнения ячеек памяти может использоваться любая последовательность бит, кроме последовательности, состоящей исключительно из нулей.



а)



б)

Рис. 3.10 – Пример схемы РСЛОС, генерирующего М-последовательность полного периода: а) для структуры обратной связи по схеме [5, 2]; б) для структуры обратной связи по схеме [5, 4, 2, 1]

Далее работа РСЛОС определяется импульсами тактового генератора. Один импульс генератора одновременно поступает на все ячейки памяти, после чего каждая ячейка пересылает свое содержимое в соседнюю ячейку с большим номером (1-я во 2-ю, 3-я в 4-ю, 5-я – на выход РСЛОС). Кроме того, если справа от ячейки показан отвод на **«Сложение mod2»**, то текущий бит из данной ячейки пересылается не только в соседнюю ячейку, но и дублируется на схему сумматора **«Сложение mod2».** Так, на рис. 3.10а на вход сумматора поступают биты от 2 и 5 ячеек.

Далее результат работы сумматора (результат сложения по модулю 2 или, другими словами, результат последовательного применения битовой операции XOR) поступает в 1-ю ячейку.

В результате выполнения данной последовательности действий один такт работы РСЛОС считается завершенным. Содержимое всех ячеек памяти обновлено; один бит поступает на выход РСЛОС в качестве очередного бита *М*-последовательности.

Следует помнить, что РСЛОС, содержащий m ячеек памяти, способен синтезировать *M*-последовательность длиной $2^m - 1$ за $2^m - 1$ шагов. При этом для синтеза *M*-последовательностей полного периода, обладающих указанными выше свойствами, структура обратной связи должна быть спроектирована в соответствии с рядом ограничений. Данные ограничения и алгоритм выбора структуры обратной связи не рассматривается в рамках данного пособия. Следует лишь отметить, что на данный момент определены корректные, то есть порождающие *M*-последовательности полного периода схемы обратной связи для РСЛОС объемом вплоть до 500 ячеек памяти (соответствующие последовательности имеют длину $2^{500} - 1$ бит!). В табл. 3.1 приведены примеры корректных схем обратной связи для некоторых РСЛОС.

Итак, рассмотрев алгоритм генерации последовательностей, можно утверждать, что *M*-последовательности удовлетворяют и требованиям 1–3. Действительно, схема РСЛОС способна порождать последовательности длиной до $2^m - 1$ бит. Выбор последовательности на основе ключа встраивания может производиться путем выбора структуры обратной связи. Так, для любого m мы можем выбрать все наборы чисел, образующие корректную обратную связь (табл. 3.1), и пронумеровать эти наборы. Далее на основе ключа встраивания будет выбираться конкретный номер набора чисел и, тем самым, определяться структура обратной связи.

Табл. 3.1 – Структура обратной связи для РСЛОС, порождающих M-последовательности полного периода

m	Структура обратной связи
2*	[2, 1]
3*	[3, 1]
4	[4, 1]
5*	[5, 2], [5, 4, 3, 2], [5, 4, 2, 1]
6	[6, 1], [6, 5, 2, 1], [6, 5, 3, 2]
7*	[7, 1], [7, 3], [7, 3, 2, 1], [7, 4, 3, 2], [7, 6, 4, 2], [7, 6, 3, 1], [7, 6, 5, 2], [7, 6, 5, 4, 2, 1], [7, 5, 4, 3, 2, 1]
8	[8, 4, 3, 2], [8, 6, 5, 3], [8, 6, 5, 2], [8, 5, 3, 1], [8, 6, 5, 1], [8, 7, 6, 1], [8, 7, 6, 5, 2, 1], [8, 6, 4, 3, 2, 1]

Нужно заметить, что более простым, но совершенно некорректным способом использования ключа встраивания при генерации последовательности является начальное заполнение ячеек памяти РСЛОС битами ключа. Дело в том, что конкретный РСЛОС с заданной структурой обратной

связи всегда порождает одну и ту же *M*-последовательность. Различное заполнение ячеек памяти РСЛОС определяет лишь циклический сдвиг, с которым эта последовательность будет сгенерирована.

Отдельно рассмотрим требование 6. Как определить число различных *M*-последовательностей заданной длины, которые могут быть сгенерированы с помощью РСЛОС? В книге [56] дается следующая оценка для количества разных *M*-последовательностей длиной N бит: $Q = \varphi(N)/m$, где $\varphi(N)$ – функция Эйлера (количество натуральных чисел, меньших N и при этом взаимно простых с N). Для примера, при длине *M*-последовательности, равной $N = 2^{19} - 1 = 524287$ бит, число разных последовательностей составит всего 27594. Таким образом, схемы модуляции ЦВЗ с расширением спектра могут быть атакованы путем последовательного тестирования каждой из 27594 *M*-последовательностей, при этом число различных ключей встраивания также фактически ограничено этим числом. Следовательно, можно говорить о том, что требование 6 не выполняется для *M*-последовательностей.

Алгоритмы генерации последовательностей, описанные в [55, 47], обеспечивают гораздо большее (на несколько порядков) число возможных последовательностей заданной длины и тем самым позволяют удовлетворить требование 6. Поэтому при проектировании систем встраивания ЦВЗ, устойчивых к атакам прямого перебора ключей, следует использовать данные последовательности вместо *M*-последовательностей. Кроме того, авторами [57] предложено использовать для целей модуляции с расширением спектра последовательностей, схожих с *M*-последовательностями полного периода: последовательностей Касами и Голда. К сожалению, данные последовательности, будучи корректными с точки зрения требований 1–5 и 7, также не могут обеспечить устойчивости к атакам с полным перебором ключей.

Отдельно рассмотрим случай, когда модулирующая последовательность должна представлять собой двумерный массив значений, а не одномерный вектор (см. СВИ-8). В данном случае требование 4, обеспечивающее стойкость ЦВЗ к кадрированию, повороту и другим искажающим преобразованиям, будет формулироваться уже с учетом наличия двумерного циклического сдвига (т.е. циклического сдвига на h строк и v столбцов). В этом случае возникает дополнительная подзадача в задаче генерации последовательностей для модуляции с расширением спектра: как получить из сгенерированной корректной (удовлетворяющей требованиям 1–7) од-

номерной последовательности корректную (с учетом требования 4) двумерную последовательность?

Самый очевидный и простой в реализации способ – построчное «заполнение» двумерного массива элементами из одномерной корректной последовательности – не позволяет гарантировать соответствие требованию 4. Даже если для одномерной последовательности был известен ее минимум циклического расстояния Хэмминга, то подобная «перетасовка» ее элементов не позволяет гарантировать сохранение данного свойства для двумерного случая.

Существует ряд способов, которые позволяют сформировать двумерный массив, удовлетворяющий требованиям 1–7, на основе корректной одномерной последовательности.

Так, наиболее известным алгоритмом преобразования одномерной последовательности в двумерный массив с сохранением минимального циклического расстояния Хэмминга является алгоритм, основанный на китайской теореме об остатках [58].

Пусть дана последовательность $W(m), m \in [1, p \cdot q]$, где p, q – взаимно простые. Тогда двумерный массив $V(n_1, n_2)$, удовлетворяющий требованию

$$V\big(m \cdot p \ (\mathrm{mod}\ \ q), m \cdot q(\mathrm{mod}\, p)\big) = W(m),$$

обладает тем же значением минимума циклического расстояния Хэмминга, что и исходная последовательность $W(m)$.

Алгоритм формирования двумерного массива в данном случае тривиален – перебирая все возможные $m \in [1, p \cdot q]$, вычислять для них соответствующие значения индексов $n_1 = m \cdot p \ (mod\ \ q), n_2 = m \cdot q(mod\, p)$ и заполнять соответствующую ячейку двумерного массива $V(n_1, n_2)$ значением из $W(m)$.

Этот способ применим в тех ситуациях, когда уже сгенерирована одномерная последовательность достаточной длины и необходимо преобразовать ее в двумерный массив.

В случае, когда создание одномерной последовательности достаточной длины является вычислительно затратной задачей, возможно получение двумерного массива $V(n_1, n_2)$ путем многократного дублирования доступной короткой последовательности $W(m)$. Фактически, в этом случае последовательность $W(m)$ используется в качестве первой строки создаваемого двумерного массива, а все последующие строки массива создаются как циклический сдвиг исходной строки на L позиций.

Таким образом, если известна последовательность $W(m), m \in [1, p]$, то двумерный массив $V(n_1, n_2), n_1, n_2 \in [1, p]$ может быть сформирован следующим образом.

1. Первая и вторая строки массива
   $V(1, n_2) = W(n_2), V(2, n_2) = W(n_2)$.
2. Третья и последующие строки:
   $V(n_1, n_2) = W_{n_1}(n_2)$, где $W_{n_1}(n_2)$ – исходная последовательность, циклически сдвинутая на $n_1 \cdot (n_1 - 1)/2$ позиций.

Достоинством данного алгоритма является то, что сконструированный двумерный массив обладает гораздо большим, чем исходная последовательность, минимальным циклическим расстоянием Хэмминга: $\lambda_V \approx (n_1 - 2) \cdot \lambda_W$.

Для генерации двумерных массивов большого объема (более 10–20 млн. элементов), удовлетворяющих требованию 4, возможно также использовать следующий алгоритм.

Как показано в [58, 59, 60], существует простой способ преобразовать одномерную последовательность C_h в два двумерных шумоподобных шаблона M_0 и M_1, предназначенных для встраивания ЦВЗ (M_0 используется для модуляции с расширением спектра для встраивания нуля, M_1 – для встраивания единицы), необходимо выполнить следующие шаги.

На первом шаге необходимо сформировать два временных бинарных массива $R_o(v, h)$ и $R_1(v, h)$ размером $V \times H$ бит, где H равняется длине последовательности C_h,а V выбирается таким образом, чтобы выполнялось равенство $V \cdot H = M \cdot N$. Для этого используется алгоритм формирования ортогональных оптических кодов, представленный в [55]. Так, первая строка массивов $R_o(v, h)$ и $R_1(v, h)$ формируется согласно соотношению $R_0(1, h) = C_h$, $R_1(1, h) = C_h$. Далее, g-я строка массива $R_o(v, h)$ формируется путём циклического сдвига строки $g - 1$ на $g \cdot q_0$ позиций (где q_0 – простое число и величина $g \cdot q_0$ вычисляется по модулю целого числа H). Аналогично формируется массив R_1: строка $g - 1$ массива формируется путём циклического сдвига предыдущей строки на $g \cdot q_1$ позиций ($q_1 \neq q_0$ – простое число, умножение $g \cdot q_0$ производится по модулю H).

В работах [61] и [58] было доказано, что двумерные бинарные массивы $R_o(v, h)$ и $R_1(v, h)$ имеют близкое к максимуму (т.е. к $V \cdot H$) значение циклического расстояния Хэмминга при ненулевых значениях сдвига (для случая циклического сдвига двумерных массивов предполагается, что мас-

сив $R_o(v,h)$ остаётся неизменным, а массив $R_1(v,h)$ циклически сдвигается на Δh строк и Δv столбцов).

На последнем шаге массивы $R_0(v,h)$ и $R_1(v,h)$ преобразуются в шаблоны M_1 и M_0 размером $N \times M$ согласно следующему соотношению:

$$M_0(u\ mod\ N, u\ mod\ M) = R_0(u\ mod\ V, u\ mod\ H),$$
$$M_1(u\ mod\ N, u\ mod\ M) = R_1(u\ mod\ V, u\ mod\ H),$$

где $u \in [1, N \times M]$.

Данный шаг необходим для формирования шумоподобных двумерных массивов, размер которых совпадает с размером изображения-контейнера (см. СВИ-8).

Согласно [61] и [58], предложенная последовательность преобразований исходной последовательности позволяет сохранить минимальное циклическое расстояние Хэмминга равным λ и для полученных двумерных шаблонов. Отличие построенных двумерных шаблонов от исходных ключевых последовательностей будет заключаться лишь в том, что в случае двумерных шаблонов циклический сдвиг шаблонов также является двумерным, т.е. сдвиг шаблонов производится на Δh строк и Δv столбцов.

Таким образом, рассмотренные алгоритмы позволяют генерировать как одномерные, так и двумерные шумоподобные массивы для модуляции ЦВЗ с расширением спектра. Особое внимание при генерации таких последовательностей необходимо уделять ряду специфичных требований (требования 1–7), обусловленных спецификой применения ЦВЗ (наличие зашумления сигнала контейнера и возможность квалифицированных атак, направленных на удаление ЦВЗ). Оценка вычислительной сложности данных алгоритмов в рамках данного пособия не рассматривалась, но оценки вычислительной сложности для большинства упомянутых алгоритмов могут быть найдены в работах-первоисточниках, указанных в библиографическом списке.

3.3.4. Моделирование атак, направленных на удаление, искажение или замену встроенного ЦВЗ

Как отмечалось в главе 1, под стойкостью ЦВЗ-систем понимается возможность корректного извлечения встроенной информации из носителя, который подвергался некоторым искажениям. Иными словами, стойкость ЦВЗ-системы характеризует простоту удаления встроенной информации. Круг возможных искажений, которые могут быть теоретически применены над носителем информации, весьма широк.

Исследование стойкости может осуществляться по одному из двух популярных сценариев. В первом случае проверяется стойкость системы к некоторому множеству преобразований, круг которых главным образом определяется областью применения СВИ, её свойствами и соображениями здравого смысла. То есть это должны быть такие преобразования, которые могут произойти с носителем информации в рамках его использования и которые не нарушают его целостности. Например, если носитель информации представляет собой цветное фотографическое изображение высокого качества, предназначенное для передачи и публикации в цифровом виде, то нет смысла проверять его стойкость к печати-сканированию, поскольку качество результирующего изображения не позволит его полноценно использовать. Также нецелесообразно проверять стойкость системы ЦВЗ для видео к покадровому повороту, поскольку это преобразование нехарактерно для большинства сценариев использования видеофайлов. Рассмотренный сценарий называют *проверкой стойкости к непреднамеренным искажениям носителя информации*. Водяные знаки, сохраняющиеся по результатам данной атаки, принято называть стойкими.

Второй сценарий также предполагает сохранение целостности носителя информации после искажения, но методы преобразования могут быть нестандартными, специально подобранными с целью удаления ЦВЗ. В данном сценарии алгоритм встраивания ЦВЗ предполагается известным, и он определяет способ искажения. Общая процедура в этом случае называется *проверкой стойкости ЦВЗ к преднамеренным атакам*. Алгоритмы, успешно прошедшие проверку определённой атакой данного типа, называются стойкими к данной атаке. ЦВЗ-системы, стойкие ко всем известным атакам данного типа, иногда называются секретными [1].

Круг непреднамеренных искажений, традиционно рассматриваемых для СВИ в изображения, включает:

- поэлементные изменения функции яркости (контрастирование, цветовая коррекция и др.);
- зашумление (аддитивное и импульсное, различные параметры шума и формы АКФ);
- линейную фильтрацию (сглаживание, повышение резкости, нерезкую маску и др.);
- нелинейную фильтрацию (медианную, ранговую фильтрацию и пр.);

- геометрические искажения (поворот, масштабирование, сдвиг, проективное преобразование и пр.);
- потерю части пространственных данных (обрезку, дублирование фрагмента изображения, замену части отсчётов отсчётами другого изображения);
- сжатие с потерями (в форматах JPEG, JPEG-2000 и пр.);
- печать-сканирование;
- повторное встраивание другого ЦВЗ тем же алгоритмом.

Для систем встраивания информации в видео добавляются всевозможные изменения по оси времени: изменение битрейта, вырезание фрагмента по времени, пропуск отдельных кадров; расширяется список форматов сжатия с потерями. В то же время актуальность теряют геометрические искажения, печать-сканирование. Подробную информацию по всем перечисленным преобразованиям можно найти в книгах [22, 21, 62, 63].

3.4. ЦВЗ-системы для аутентификации изображений

Современные инструменты обработки цифровых сигналов позволяют с лёгкостью обрабатывать фотографии, видео- и аудиофайлы, в том числе изменяя содержимое. В ряде случаев такие изменения могут быть преднамеренно вредоносными или могут непреднамеренно повлиять на интерпретацию содержимого. Например, случайное изменение рентгеновского снимка может привести к неправильному диагнозу, а фальсификация фотографических доказательств в уголовном процессе могут привести к неправильному решению суда. Таким образом, в некоторых задачах существует необходимость проверки подлинности или целостности цифровых объектов – изображений, аудио, видео. В частности, важно иметь в своём арсенале методы, позволяющие ответить на следующие вопросы [2]:

- Был ли объект каким-либо образом изменён?
- Если да, то были ли эти изменения значительными?
- Какие фрагменты подверглись изменению?
- Может ли объект быть восстановлен?

Методы, позволяющие ответить на вопросы из данного списка, могут быть разделены на две группы [64]: пассивные и активные методы аутентификации содержимого. Пассивные методы заключаются в расчёте ряда характеристик объекта и сопоставлении их с типичными или априори известными значениями [65]. Например, если объект представляет собой

спутниковый снимок определённой местности, снятый в известное время, то один из способов проверки подлинности заключается в проверке ракурса съёмки и направления теней. Сценарий использования активных методов состоит из двух шагов. На первом нам доступны сырые (неизменённые) данные, что позволяет оценить некоторые их характеристики (например, результат хэширования) или намеренно изменить объект определённым образом. Задача второго шага – проверить подлинность объекта (но уже без доступа к оригиналу). Одним из наиболее эффективных подходов активной защиты является использование цифровых водяных знаков. Далее подробнее остановимся на различных методах встраивания ЦВЗ для решения задач аутентификации изображений и сценариях их использования.

3.4.1. Точная аутентификация

В задаче точной аутентификации требуется выявить любые изменения, произошедшие с изображением, включая в том числе его изменение вследствие встраивания ЦВЗ. Таким образом, ЦВЗ, встроенный в изображение для защиты от изменений, должен быть полностью удалён после проверки. Таким требованиям удовлетворяют так называемые *удаляемые ЦВЗ*. Сценарий использования удаляемых ЦВЗ для точной аутентификации предполагает следующие шаги (изложим его в популярной в криптографии нотации Алисы и Боба):

1. Алиса вычисляет одностороннюю хэш-функцию изображения и встраивает её результат в это изображение в качестве ЦВЗ.
2. Алиса отправляет результирующий носитель ЦВЗ Бобу.
3. Боб извлекает ЦВЗ из полученного изображения.
4. Боб удаляет ЦВЗ из изображения. Теперь оно должно быть эквивалентно исходному в случае отсутствия изменений при его передаче.
5. Боб вычисляет одностороннюю хэш-функцию полученного изображения и сравнивает её результат с ЦВЗ.
6. Изображение признаётся подлинным тогда и только тогда, когда результаты хэширования полностью совпадают.

Таким образом, эффективность решения задачи точной аутентификации сводится к эффективности построения систем удаляемых ЦВЗ. Однако построение таких систем является непростой задачей, поскольку требования, предъявляемые к ним (применимость к любым изображениям, возможность полного восстановления, минимизация числа ложных сраба-

тываний), являются взаимно противоречивыми. Рассмотрим примеры систем встраивания удаляемых ЦВЗ.

СВИ-11 (E_MOD/D_LC)

Система встраивания ЦВЗ на основе модульной арифметики [2]

Данная система является модификацией системы СВИ-8 (E_BLIND/D_LC), рассмотренной в параграфе 3.3 и предназначенной для встраивания одного бита информации. Для системы удаляемого ЦВЗ нет необходимости встраивать один бит (для передачи информации об исходном контейнере этого недостаточно, для системы с детектором – излишне). Поэтому, учитывая, что контейнер представляет собой полутоновое изображение, пиксели которого принимают значения от 0 до 255, формула встраивания информации (3.40) примет вид:

$$C^W(n_1,n_2) = \big(C(n_1,n_2) + \alpha \cdot W_{mod}(n_1,n_2)\big) mod\ 256, \qquad (3.57)$$

где W_r, как и ранее, псевдослучайный шаблон, совпадающий размерами с исходным изображением, но в данном случае он может опосредованно нести информацию о контейнере.

При детектировании ЦВЗ сначала вычисляется значение линейной корреляции $\rho\big(\widetilde{C^W}, W_r\big)$ по формуле (3.41), после чего принимается решение о наличии встроенного ЦВЗ, если $\rho\big(\widetilde{C^W}, W_r\big) > \tau_{lc}$.

Удаление ЦВЗ осуществляется по формуле

$$\tilde{C}(n_1,n_2) = \Big(\widetilde{C^W}(n_1,n_2) - \alpha \cdot W_r(n_1,n_2)\Big)\ mod\ 256. \qquad (3.58)$$

Следует отметить, что модульное встраивание по формуле (3.57) может приводить к шуму «соль-и-перец». Поэтому визуально носитель информации будет выглядеть плохо. Однако здесь следует помнить о том, что эти искажения полностью устраняются при удалении ЦВЗ.

У рассмотренной системы есть следующие недостатки:

1. Шум типа «соль-и-перец», вызванный изменением формулы встраивания, отрицательно сказывается на качестве детектирования и приводит к росту числа ошибок.
2. Корреляционный детектор будет неработоспособен для обнаружения встраивания вида (3.57), если исходный контейнер C содержит значения, равномерно распределённые на отрезке от 0 до 255. Таким образом, метод будет неприменим для защиты изображения, которое было подвергнуто процедуре эквализации гистограммы.

3. Данная система предполагает детектирование ЦВЗ, что не позволяет полноценно использовать её в предложенном выше сценарии точной аутентификации.

Далее рассмотрим другую систему встраивания удаляемых ЦВЗ, обладающую большей практической значимостью.

СВИ-12 (Lossless-LSB)

Удаляемые ЦВЗ за счёт сжатия НЗБ

В литературе описаны по меньшей мере две системы ([66], [67]), использующие сжатие наименее значимых битовых плоскостей для встраивания дополнительной информации. Здесь мы опишем упрощённую систему, реализующую данный подход. Пусть C – полутоновой контейнер размерами $N_1 \times N_2$, C_k – k-я битовая плоскость контейнера. Как было показано в подпараграфе 3.1.1 (см. рис. 3.1), по мере увеличения k битовые плоскости становятся всё менее шумоподобными, и на них начинают проступать очертания крупных объектов. Таким образом, примерно 3-я или 4-я битовая плоскость зачастую являются хорошо сжимаемыми, но в то же время их изменение не слишком существенно сказывается на визуальном качестве.

В рассматриваемой системе осуществляется сжатие без потерь одной из битовых плоскостей $C_k, k = \{3, 4\}$. Далее выбранная битовая плоскость обнуляется, а на её место побитово записывается полученный архив. Далее после метки окончания архива записывается информация об исходном контейнере (например, его хэш). Порядок извлечения и удаления встроенной информации очевиден.

3.4.2. Избирательная аутентификация

Рассмотренные примеры задач защиты медицинских изображений и документальных свидетельств, требующих точной аутентификации, скорее являются исключением из правил. В большинстве же практических приложений допустимы незначительные искажения, вызванные необходимостью внедрить защитный водяной знак. Если ЦВЗ должен разрушаться при малейших изменениях носителя информации, то такие ЦВЗ называются хрупкими. Простейшей система защиты изображений хрупкими ЦВЗ может быть построена на основе СВИ-1 (НЗБ-встраивание ЦВЗ) путём изменения метода извлечения информации с декодера на детектор, проверяющий наличие заданного ЦВЗ в НЗБП. В этом случае если найдётся хотя бы одна точка (n_1, n_2), в которой

$$C_p(n_1, n_2) \neq W(n_1, n_2),$$

где p – номер битовой плоскости, то устанавливается, что изображение изменилось. Для системы хрупких водяных знаков используется $p = 1$.

В то же время весьма распространённой является ситуация, когда незначительные изменения носителя информации считаются допустимыми после встраивания в него защитного ЦВЗ. К таким преобразованиям может относиться слабая фильтрация шума (линейная или медианная), контрастирование, сжатие с потерями (до определённого уровня погрешности), поворот на угол, кратный $\pi/2$, вырезание фрагмента изображения. Водяные знаки, используемые для решения этой задачи, называются полухрупкими.

Для обеспечения стойкости ЦВЗ к незначительным колебаниям яркости может применяться встраивание в битовую плоскость C_p при $p > 1$, а ещё лучше – использование СВИ-4 (QIM) с детектором.

Для каждого из прочих перечисленных искажений применяются специфические модификации базового метода. Например, для достижения стойкости носителя информации C^W размерами $N \times N$ к повороту на угол, кратный $\pi/2$, ЦВЗ, встраиваемый методом QIM, должен удовлетворять следующему ограничению:

$$W(n_1, n_2) = W(N - n_1, n_2) = W(n_1, N - n_2) = W(N - n_1, N - n_2). \quad (3.59)$$

Ниже мы рассмотрим систему, обеспечивающую стойкость к сжатию изображения в формате JPEG с контролируемым уровнем качества. Однако поскольку встраивание информации в этой системе тесно связано с алгоритмом JPEG-сжатия, то прежде всего необходимо остановиться на основных его этапах.

При сжатии изображений в формате JPEG цветное изображение переводится из цветового пространства RGB в YCbCr [21], где компонента Y отвечает за яркость, а Cb и Cr – за цветовую составляющую. Далее нас будет интересовать только яркостная составляющая, поэтому рассмотрим только её. Если изначально изображение является полутоновым, то две других компоненты и вовсе отсутствуют. Пусть $C(n_1, n_2)$ – яркостная компонента. Далее она разбивается на блоки $C_{ij}(n_1, n_2)$ размерами 8×8 (i и j задают положение блока в большой матрице), и на каждом из них осуществляется расчёт ДКП. Результирующие блоки обозначим $f_{ij}(m_1, m_2)$, где $0 \le m_1, m_2 < 8$. Далее все спектральные компоненты поэлементно делятся на отсчёты матрицы η_Q и округляются:

$$p_{ij}(m_1, m_2) = \left[\frac{f_{ij}(m_1, m_2)}{\eta_Q(m_1, m_2)}\right]. \quad (3.60)$$

В матрице η_Q индекс Q определяет параметр качества, представляемый целым числом в диапазоне от 1 до 100. Для любого значения Q матрица η_Q формируется на основе базовой матрицы $\eta = \eta_{50}$ по следующей формуле:

$$\eta_Q(m_1, m_2) = k(Q) \cdot \eta(m_1, m_2), \tag{3.61}$$

где

$$k(Q) = \begin{cases} \left[\frac{5000}{Q}\right], & Q < 50, \\ 200 - 2Q, & Q \geq 50. \end{cases} \tag{3.62}$$

Базовая матрица η задана в табл. 3.2.

Табл. 3.2 – Матрица квантования η в алгоритме JPEG

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Далее осуществляется архивирование полученной квантованной информации, содержащейся в матрицах $p_{ij}(m_1, m_2)$. Более подробно процедура JPEG-сжатия изложена в книге [62]. Теперь перейдём к описанию самой системы встраивания информации.

СВИ-13 (Lin & Chang)

Система полухрупких ЦВЗ, стойких к JPEG-сжатию [68]

Как и в алгоритме сжатия JPEG, контейнер C разбивается на блоки размерами 8×8, которые подвергаются дискретному косинусному преобразованию. В каждый из результирующих блоков $f_{ij}(m_1, m_2)$ встраивается 4 бита информации $b_{ij,k}$, где $k = \overline{0,3}$. Для этого множество из 28 коэффициентов $f_{ij}(m_1, m_2)$, расположенных ниже побочной диагонали, то есть множество

$$D = \{(m_1, m_2): m_1 + m_2 > 7\}, \tag{3.63}$$

разбивается на 4 равных подмножества D_k по 7 коэффициентов в соответствии с ключом встраивания $\mathbf{k}$.

Далее для встраивания каждого бита $b_{ij,k}$ необходимо выполнить следующие шаги:

1. Осуществить деление коэффициентов $f_{ij}(m_1, m_2)$, где $(m_1, m_2) \in D_k$, на элементы матрицы η (табл. 3.2):

$$f'_{ij}(m_1, m_2) = \left[\frac{f_{ij}(m_1, m_2)}{\alpha \cdot \eta(m_1, m_2)}\right], \quad (3.64)$$

где α – параметр, связанный с уровнем качества Q JPEG-сжатия, стойкость к которому требуется обеспечить.

2. Вычислить двоичное значение

$$\beta = \underset{(m_1,m_2)\in D_k}{XOR}\left(f'_{ij}(m_1, m_2)(mod\ 2)\right). \quad (3.65)$$

3. Если $\beta \neq b_{ij,k}$, то инвертировать младший бит $f'_{ij}(m_1, m_2)$ у того коэффициента (m_1, m_2), которому соответствует наибольшее значение $\eta(m_1, m_2)$.

4. Умножить обратно значения $f'_{ij}(m_1, m_2)$ на элементы матрицы η.

$$f^W_{ij}(m_1, m_2) = \alpha \cdot \eta(m_1, m_2) \cdot f'_{ij}(m_1, m_2). \quad (3.66)$$

Носитель информации C^W формируется в результате применения обратного ДКП к каждому из блоков f^W_{ij}.

Извлечение информации происходит по формуле, эквивалентной (3.65):

$$b^R_{ij,k} = \underset{(m_1,m_2)\in D_k}{XOR}\left(\widetilde{f'_{ij}}(m_1, m_2)(mod\ 2)\right), \quad (3.67)$$

где $\widetilde{f'_{ij}}$ получено из носителя информации $\widetilde{f^W}$ аналогично f'_{ij}.

3.4.3. Локализация изменений

В задаче аутентификации с локализацией изменений необходимо иметь возможность не только обнаруживать факт изменений, но и строить маску областей, подвергшихся модификации. Рассмотрим одну из простейших систем, предназначенных для решения этой задачи, предложенную в работе [69].

СВИ-14 (Yeung & Mintzer)

Простейшая система встраивания хрупких ЦВЗ с локализацией изменений [69]

Для встраивания и извлечения информации на основе ключа $\mathbf{k}$ формируется отображение

$$\mu: \mathbb{N}_0 \cap [0,255] \longmapsto \{0,1\}, \quad (3.68)$$

ставящее в соответствие каждому числу от 0 до 255 двоичное значение. Отображение μ обычно формируют псевдослучайным образом, стараясь избегать больших последовательностей подряд идущих чисел, отображае-

мых в одно и то же значение. Например, простейшим подходящим отображением является функция отыскания младшего бита:

$$\mu(x) = x(\mathrm{mod}\ 2).$$

Для встраивания формируется бинарный шаблон ЦВЗ W_r размерами $M_1 \times M_2$. В результате встраивания информации должно быть справедливо следующее условие:

$$\mu(C^W(n_1, n_2)) = W_r\big(n_1(mod\ M_1), n_2(mod\ M_2)\big). \quad (3.69)$$

Если это условие выполняется для некоторого пикселя (n_1, n_2) исходного контейнера C, то значение $C(n_1, n_2)$ не меняется. В противном случае находится такое $v \in \mathbb{N}_0 \cap [0{,}255]$, что

$$\mu(v) = W_r\big(n_1(mod\ M_1), n_2(mod\ M_2)\big) \quad (3.70)$$

и v – ближайшее к $C(n_1, n_2)$ число, удовлетворяющее этому соотношению. То есть

$$v = arg \min_{x:\, \mu(x) = W(n_1(mod\ M_1), n_2(mod\ M_2))} |x - C(n_1, n_2)|. \quad (3.71)$$

Найденное значение v и будет яркостью текущего пикселя носителя информации:

$$C^W(n_1, n_2) = v. \quad (3.72)$$

Такое изменение в пикселе (n_1, n_2) порождает ошибку относительно исходного контейнера, равную $v - C(n_1, n_2)$. Для снижения визуальных последствий эта ошибка компенсируется в последующих отсчётах по методу диффузии ошибки.

Для проверки подлинности принятого носителя информации в каждой его точке проверяется условие (3.69). Очевидно, изображение будет признано неизменённым, если во всех точках условие соблюдается. Если существует ненулевое множество точек, в которых условие не соблюдается, то строится маска изменений

$$E(n_1, n_2) = \begin{cases} 1, & \mu\big(\widetilde{C^W}(n_1, n_2)\big) \neq W_r\big(n_1(mod\ M_1), n_2(mod\ M_2)\big), \\ 0 & \text{иначе.} \end{cases} \quad (3.73)$$

Недостатком алгоритма является тот факт, что по статистике половина изменённых точек будет иметь значение $E(n_1, n_2) = 0$. Отчасти он может быть компенсирован исходя из предположения о кластеризации изменённых пикселей в крупные области. В этом случае для уточнения маски E можно осуществить её постобработку, например, применив морфологическое замыкание [21].

В работе [31] предложена система, позволяющая осуществлять локализацию изменений при помощи полухрупких водяных знаков. В полной версии системы обеспечивается стойкость к линейному контрастированию,

повороту и кадрированию (то есть вырезанию фрагмента изображения без масштабирования), однако мы рассмотрим упрощённый вариант, в котором встраиваемый ЦВЗ является хрупким.

СВИ-15 (Глумов & Митекин)

Хрупкий ЦВЗ с локализацией изменений [31]

Данная система основана на методе QIM, относительно которого произведены две модификации:

1) метод QIM применяется к блокам изображения-контейнера размерами $M \times M$;
2) встраиваемая информация модулируется бинарным шаблоном K, также имеющим размеры $M \times M$ и формируемым на основе секретного ключа системы $\mathbf{k}$.

В данной системе предполагается, что контейнер C имеет квадратный размер $N \times N$, а встраиваемый ЦВЗ W представляется бинарной матрицей, имеющей размеры $[N/M] \times [N/M]$.

Встраивание информации осуществляется по формуле

$$C^W(n_1, n_2) = \left[\frac{C(n_1, n_2)}{2q}\right] \cdot 2q + \widehat{W}(n_1, n_2) \cdot q + C(n_1, n_2)\ (mod\ \ q), \qquad (3.74)$$

где

$$\widehat{W}(n_1, n_2) = \widehat{W}(l_1 \cdot M + m_1, l_2 \cdot M + m_2) = W(l_1, l_2) \oplus K(m_1, m_2), \qquad (3.75)$$

где $0 \le l_1, l_2 < [N/L]$, $0 \le m_1, m_2 < M$.

При извлечении информации используется следующая формула:

$$W^R(l_1, l_2) = \begin{cases} 0, \text{если } \forall m_1, m_2 \\ \widetilde{C^W}(l_1 \cdot M + m_1, l_2 \cdot M + m_2) - qK(m_1, m_2) < q, \\ 0, \text{если } \forall m_1, m_2 \\ \widetilde{C^W}(l_1 \cdot M + m_1, l_2 \cdot M + m_2) - q\overline{K(m_1, m_2)} < q, \\ \text{не определено, иначе.} \end{cases} \qquad (3.76)$$

В случае, если в результате извлечения ЦВЗ некоторые значения $W^R(l_1, l_2)$ не определены, то делается вывод о том, что блок изображения $\widetilde{C^W}$, соответствующий этому биту, был изменён. Таким образом, здесь в отличие от системы СВИ-14 (Yeung & Mintzer) удаётся однозначно определить маску изменений:

$$E(n_1, n_2) = \begin{cases} 1, & W^R\left(\left[\frac{n_1}{M}\right], \left[\frac{n_2}{M}\right]\right) \text{ не определено}, \\ 0, & W^R\left(\left[\frac{n_1}{M}\right], \left[\frac{n_2}{M}\right]\right) \in \{0,1\}. \end{cases} \qquad (3.77)$$

Однако следует помнить, что данная маска изменений дискретизирована на блоки размером $M \times M$.

Пример проверки данной системы приведён на рис. 3.11. Слева изображён носитель информации, в который были внесены следующие модификации:

- блок 1 изображения подвергся аддитивному зашумлению;
- блок 2 был подвергнут гауссовскому размытию;
- блок 3b был замещен блоком 3a.

В центре показана маска изменений (3.77), а справа – результат извлечения (3.76).

Рис. 3.11 – Пример работы СВИ-15: слева носитель информации с локальными искажениями, в центре маска изменений $E(n_1, n_2)$, справа извлечённый ЦВЗ (белым помечены повреждённые блоки) ([31])

3.5. Встраивание информации в видеосигналы

3.5.1. Отличия и особенности СВИ в видео

Предыдущие главы были посвящены изучению различных систем встраивания информации в изображения. В данной главе будут рассмотрены методы, в которых контейнером является видеосигнал.

Области применения методов встраивания информации в видео по большей части те же самые: защита авторских прав, защита от несанкционированного распространения, защита от изменений, скрытая передача информации. Однако появляются и две специфических для видео задачи: контроль копирования и мониторинг телевещания.

Задача контроля копирования заключается в разработке и применении комплексных систем, использующих аппаратные криптографические решения и технологии водяных знаков для воспрепятствования несанкционированному копированию лицензионных дисков с видеоданными, таких как DVD и Blu-ray. Интерес здесь представляют не собственно методы встраивания информации, а сценарии их совместного использования вместе с иными средствами защиты. Эти вопросы рассматриваются в книгах [1, 2], мы же на них останавливаться не будем.

Задача мониторинга вещания актуальна, в частности, для рекламодателей, заказывающих показ их рекламного ролика на телевидении определённое число раз в день и желающих убедиться в точном соблюдении вещателем заключённого контракта. В этом случае рекламодатель будет нуждаться в системе, принимающей видеосигнал в реальном времени и увеличивающий счётчик показов каждый раз, когда обнаружился искомый рекламный ролик. Корреляция видеосигналов в реальном времени является трудоёмкой процедурой. Поэтому вместо этого в рекламный ролик может предварительно внедряться водяной знак, тогда при анализе видеопотока будет постоянно осуществляться попытка извлечения ЦВЗ. Такой подход может оказаться более подходящим для систем реального времени.

В отличие от изображений, которые зачастую могут храниться в формате без потерь, цифровые видео почти всегда подвергаются компрессии (сжатию) с потерями. Поэтому методы встраивания информации в видео должны быть стойкими к стандартным методам сжатия. Помимо этого, методы встраивания должны быть стойкими к кадрированию (обрезке) или прореживанию видео по временной оси. С другой стороны, как правило, нет необходимости добиваться стойкости встроенной информации к сложным геометрическим искажениям кадров. Ещё одно «облегчение», возникающее при использовании видео в качестве контейнера, заключается в допустимости бóльших по амплитуде искажений для каждого кадра ввиду кратковременности их просмотра. Это, в свою очередь, позволяет повысить точность извлечения встроенной информации.

Существует два основных подхода к встраиванию информации в видео. В первом видео рассматривается как набор независимых кадров (изображений), и в каждый кадр встраиваются одни и те же данные. Такой подход позволяет обеспечить стойкость к потере синхронизации (изменениям по временной оси). Однако в этом случае объем данных, который может быть встроен в контейнер, ограничивается не продолжительностью видео, а разрешением кадра. Таким образом, этот подход не позволяет встроить большой объем информации. Кроме того, некоторые методы этой группы подвержены так называемой атаке с «приближённым вычислением ЦВЗ» (“watermark estimation attack”) [70], которая заключается в оценке сигнала ЦВЗ за счёт усреднения большого числа кадров видео с целью его удаления или восстановления встроенной информации.

Во втором подходе видео рассматривается как набор строго упорядоченных кадров, и встраиваемая информация распределяется между

многими кадрами по некоторому правилу. При этом объем встраиваемой информации становится пропорционален продолжительности видео, но встроенная информация становится более уязвимой для атак, связанных с потерей синхронизации.

В данной главе мы рассмотрим две системы, реализующие второй подход и не содержащие в базовом варианте средств защиты от десинхронизирующих атак: это система Hartung & Girod [71], позволяющая встроить очень большой объём данных и, следовательно, подходящая главным образом для задачи стеганографии, а также ЦВЗ-система JAWS, предложенная в работе [72] для мониторинга вещания. А далее мы опишем универсальный подход, позволяющий противостоять атакам потери синхронизации за счёт корректировки встраиваемой информации [73, 74].

3.5.2. Примеры СВИ в видео

СВИ-16 (Hartung & Girod)

Система встраивания информации в видео с расширением спектра [71]

Встраивание информации

Внутренняя информация представляется в форме $\mathbf{b} \in \mathbb{B}^1_{[N_b]}$ и встраивается в видеосигнал $C \in \mathbb{Z}^3_{[N_1 \times N_2 \times T]}$ ($N_1 \times N_2$ – размеры кадра, а T – число кадров видео) в соответствии с одномерной покадровой построчно-столбцовой развёрткой

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

где $n = \overline{0, N-1}$, $N = N_1 N_2 T$, $n_1 = \overline{0, N_1 - 1}$, $n_2 = \overline{0, N_2 - 1}$, $t = \overline{0, T-1}$. Таким образом, признаки контейнера описываются вектором $f \in \mathbb{Z}^1_{[N]}$:

$$f(n) = C\big(\varphi(n)\big). \tag{3.78}$$

Перед встраиванием осуществляется кодирование информации в пространстве признаков по формуле

$$\Omega(n) = (-1)^{b_i} \text{ для } i \cdot L \le n < (i+1) \cdot L, \tag{3.79}$$

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.

Встраивание информации осуществляется по формуле

$$f^W(n) = f(n) + \alpha \cdot \lambda(n) \cdot \Omega(n) \cdot (-1)^{k_n}, \tag{3.80}$$

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 встраи-

ваемом сигнале, адаптивный к локальным особенностям контейнера и меняющийся слабо, настолько, что можно принять, что

$$\forall i \in [0, N_b - 1]\ \forall n \in [i \cdot L, (i+1) \cdot L - 1] \quad \lambda(n) \approx \bar{\lambda}_i, \tag{3.81}$$

где

$$\bar{\lambda}_i = \frac{1}{L} \sum_{n=i \cdot L}^{(i+1) \cdot L - 1} \lambda(n). \tag{3.82}$$

Извлечение информации

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

$$\tilde{\Omega}(n) = (-1)^{k_n} \cdot h^W(n), \tag{3.83}$$

где h^W – вспомогательная величина, которая подбирается таким образом, чтобы было справедливо приближённое равенство

$$h^W(n) \approx f^W(n) - f(n). \tag{3.84}$$

Поскольку на стадии извлечения информации не известен истинный сигнал-контейнер, то вместо его матрицы признаков $f(n)$ используется оценка $f^W_{mean,S}(n)$ – усреднённый в скользящем окне шириной $S \geq 3$ вектор признаков $f^W(n)$. Таким образом, h^W вычисляется по формуле

$$h^W(n) = f^W(n) - f^W_{mean,S}(n). \tag{3.85}$$

Значение очередного бита b_i^R определяется на основе анализа величины

$$\beta_i = \mathcal{P}_f^{-1}\left(\tilde{\Omega}\right) = \sum_{n=i \cdot L}^{(i+1) \cdot L - 1} \tilde{\Omega}(n). \tag{3.86}$$

Из (3.86), (3.83) и (3.84) получаем, что

$$\beta_i \approx \sum_{n=i \cdot L}^{(i+1) \cdot L - 1} \alpha \cdot \lambda(n) \cdot \Omega(n) \cdot (-1)^{2k_n} = \alpha \cdot L\bar{\lambda}_i \cdot (-1)^{b_i}. \tag{3.87}$$

Поскольку $\alpha L\bar{\lambda}_i$ – величина положительная, то справедливо простое правило извлечения встроенной информации:

$$b_i^R = \begin{cases} 0, & \beta_i > 0, \\ 1, & \beta_i < 0. \end{cases} \tag{3.88}$$

СВИ-17 (JAWS)

ЦВЗ-система для мониторинга вещания [72]

JAWS является аббревиатурой от Just Another Watermarking System – такое название дал своей системе автор в работе [72].

Для встраивания цифрового водяного знака используется шаблон P_r размерами $M \times M$, представляющий собой реализацию гауссовского шума, имеющего нормальное распределение. Данный шаблон формируется при помощи ключа $\mathbf{k}$. Далее для каждого кадра t генерируется уникальный шаблон ЦВЗ по формуле вида

$$W_{r,t}(m_1, m_2) = P_r(m_1, m_2) - shift(P_r, \boldsymbol{b_t}), \tag{3.89}$$

где $m_1, m_2 \in [0, M-1]$, $\boldsymbol{b_t}$ – фрагмент встраиваемой последовательности $\boldsymbol{b}$, содержащий биты, встраиваемые в кадр t, а $shift(P_r, \boldsymbol{b_t})$ обозначает операцию циклического сдвига строк и столбцов P_r в соответствии с битами $\boldsymbol{b_t}$.

Встраивание происходит по аддитивной формуле

$$\begin{aligned} C^W(n_1, n_2, t) = {} & C(n_1, n_2, t) + \alpha \cdot \beta(n_1, n_2, t) \cdot \\ & \cdot W_{r,t}\big(n_1(mod\ M), n_2(mod\ M)\big), \end{aligned} \tag{3.90}$$

где α – параметр глобального усиления встраиваемого сигнала, $\beta(n_1, n_2, t)$ – маска адаптивного усиления встраиваемого сигнала, рассчитываемая при помощи оператора Лапласа, то есть свёртки кадра $C(n_1, n_2, t)$ с маской вида

$$g(n_1, n_2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{3.91}$$

с последующим взятием модуля полученного поля. Пример подобного расчёта $\beta(n_1, n_2, t)$ для отдельного изображения показан на рис. 3.12.

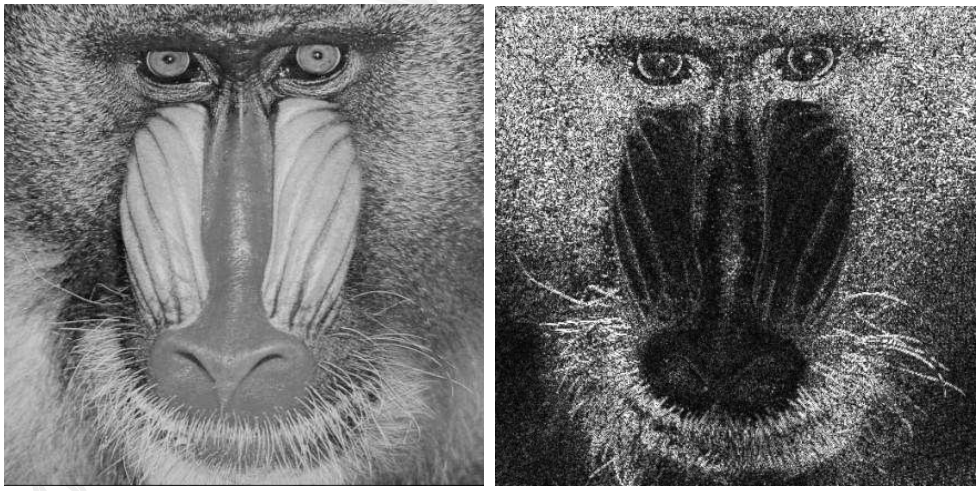


Рис. 3.12 – Полутоновое изображение и его маска адаптивного усиления, рассчитываемая в СВИ-17 (JAWS)

При извлечении информации сначала формируется оценка встроенного шумоподобного сигнала путём усреднения отсчётов в блоках размерами $M \times M$:

$$\widetilde{W_t}(m_1, m_2) = \sum_{i=0}^{[N_1/M]+1} \sum_{j=0}^{[N_2/M]+1} \widetilde{C^W}(i \cdot M + m_1, j \cdot M + m_2, t), \quad (3.92)$$

после чего формируется взаимная корреляционная функция (ВКФ) $\widetilde{W_t}(m_1, m_2)$ и $P_r(m_1, m_2)$, рассчитываемая путём перемножения их спектров [22]

$$B = \mathcal{F}^{-1}\left(\mathcal{F}\left(\widetilde{W_t}\right) \cdot conj\left(\mathcal{F}(P_r)\right)\right), \quad (3.93)$$

где $\mathcal{F}(x)$ означает расчёт двумерного ДПФ для x с использованием алгоритма быстрого преобразования Фурье [22]; $\mathcal{F}^{-1}(x)$ – расчёт обратного ДПФ.

Другой похожий способ, предлагаемый автором данной системы в работе [75], заключается в применении так называемой SPOMF-фильтрации (Symmetrical Phase Only Matched Filtering) вместо расчёта ВКФ, в которой перемножаются нормированные спектры:

$$B^* = \mathcal{F}^{-1}\left(\phi\left(\mathcal{F}\left(\widetilde{W_t}\right)\right) \cdot conj\left(\phi\left(\mathcal{F}(P_r)\right)\right)\right), \quad (3.94)$$

$$\phi(x) = \frac{x}{|x|}. \quad (3.95)$$

Далее на полученном корреляционном поле отыскиваются два пика: один положительный, координаты которого задают сдвиг шаблона P_r, а другой – отрицательный, координаты которого задают сдвиг шаблона $shift(P_r, \boldsymbol{b_t})$ (согласно формуле (3.89)). Таким образом, вектор между двумя этими пиками будет кодировать встроенную информацию $\boldsymbol{b_t}$.

Благодаря избыточному встраиванию и использованию коррелятора при извлечении информации, встроенный ЦВЗ оказывается стойким не только к пережатию видеофайла, но и к обрезке кадра.

3.5.3. Метод противодействия атакам потери синхронизации

Рассмотренные выше системы не являются стойкими к потере временной синхронизации, то есть сдвигу начала видео или изменению числа кадров в секунду. Однако в работах [73, 74] предложен способ предварительного кодирования встраиваемой информации, позволяющий противодействовать подобной атаке.

Пусть $\mathbf{b}$ – последовательность бит встраиваемой информации, состоящая из L непересекающихся фрагментов длиной N_b/L бит каждый. j-й бит i-го фрагмента $\mathbf{b}$ обозначим как $b_{i,j}, i \in [0, L-1], j \in [0, N_b/L - 1]$. В

каждый кадр исходного видео встраивается одна из L битовых последовательностей $\mathbf{s_i}$, каждая из которых состоит из $N_i + N_b/L$ бит, где

$$N_i = \lceil \log_2 L \rceil + 1, \tag{3.96}$$

В (3.96) $\lceil x \rceil$ обозначает операцию округления в бóльшую сторону. Битовые последовательности $\mathbf{s_i}$ формируются по следующему правилу:

$$\boldsymbol{s_i} = \underbrace{i_0 i_1 \dots i_{N_i-1}}_{N_i \text{ бит}} \underbrace{b_{i,0} b_{i,1} \dots b_{i,N_b/L-1}}_{N_b/L \text{ бит}}, \tag{3.97}$$

где $i_0 i_1 \dots i_{N_i-1}$ – бинарное представление индекса i, а $b_{i,0} b_{i,1} \dots b_{i,N_b/L-1}$ – i-й фрагмент встраиваемой последовательности.

Далее при встраивании информации для каждого кадра псевдослучайным образом выбирается одна из последовательностей $\mathbf{s_i}, i \in [0, L-1]$, которая встраивается в кадр видео. Единственным требованием к используемому алгоритму в данном случае является возможность встраивания и слепого извлечения не менее чем $N_i + N_b/L$ бит информации. Такой подход позволяет защититься от возможной потери синхронизации видео без использования дополнительной информации об исходной нумерации кадров.

4. Методы стегоанализа и противодействие им

4.1. Понятие стегоанализа

Под *стегоанализом* обычно понимается атака на стеганографические системы, целью которой является обнаружение канала скрытой передачи информации. Также обычно выделяют *целевой стегоанализ* (target steganalysis), при проведении которого считаются известными используемые стеганографические методы и протоколы, и *слепой стегоанализ*, не ориентированный на какие-либо методы.

Поскольку результатом проведения стегоанализа для какого-либо цифрового носителя информации является бинарный ответ: есть встраивание или нет, – то в сущности задача стегоанализа может быть сведена к задаче классификации объекта на два соответствующих класса. В этом случае её решение будет включать два этапа:

1) выбор информативных признаков;
2) классификация векторов признаков с обучением.

На втором этапе может использоваться любой известный классификатор. Выбор конкретного решения может зависеть от характера векторов признаков, их длины, разделимости, количества имеющихся для обучения данных и прочих факторов. Этот материал выходит за рамки нашего курса, однако может быть изучен самостоятельно по книгам [76, 77, 78], электронному ресурсу [79] или в рамках учебных курсов машинного обучения или распознавания образов. Наиболее часто используемые классификаторы (в том числе и в задачах стегоанализа) – линейный и квадратичный дискриминантный анализ, байесовский классификатор, машины опорных векторов, деревья решений и пр.

4.2. Целевой стегоанализ НЗБ-систем

4.2.1. Простые признаки для НЗБ-стегоанализа

Рассмотрим некоторые популярные методы выбора признаков для решения задачи стегоанализа методов стеганографического встраивания информации в наименее значимые биты полутоновых изображений, а именно собственно НЗБ-встраивания (рис. 3.2) и ±1-встраивания (СВИ-3), рассмотренных в главе 2. Все они используют следующее предположение: стеганографическое встраивание разрушает корреляционные связи между соседними отсчётами цифрового сигнала – контейнера. Таким образом, эти

признаки должны отражать коррелированность сигнала в пространстве сокрытия.

Первый способ расчёта признаков основывается на расчёте среднего значения и среднего числа переходов в битовой плоскости в скользящем окне. Пусть $C_p^W(n_1, n_2)$ – анализируемая битовая плоскость.

Формула свёртки C_p^W с фильтром, имеющем конечную импульсную характеристику $g(m_1, m_2)$, определяемую матрицей $M \times M$, имеет вид:

$$S(n_1, n_2) = C_p^W ** g = \\ = \sum_{m_1=0}^{M-1} \sum_{m_2=0}^{M-1} g(m_1, m_2) \cdot C_p^W(n_1 - m_1, n_2 - m_2). \quad (4.1)$$

Локальное среднее тогда рассчитывается как

$$\mu = C_p^W ** g_\mu, \quad (4.2)$$

где для g_μ $M = 2p + 1, p \in \mathbb{N}$, причём отсчёты ИХ постоянны и равны $1/M^2$.

Среднее число переходов бита (в совокупности по горизонтали и вертикали) рассчитывается в несколько этапов:

$$\tau_{hor} = C_p^W ** g_{hor}, \quad (4.3)$$

$$\tau_{ver} = C_p^W ** g_{ver}, \quad (4.4)$$

$$\tau = \left(\frac{1}{2}(|\tau_{hor}| + |\tau_{\text{ver}}|)\right) ** g_\mu, \quad (4.5)$$

где

$$g_{hor} = (-1 \quad 1), \qquad g_{\text{ver}} = (g_{hor})^{\text{T}}. \quad (4.6)$$

Разумеется, и μ, и τ являются матрицами значений, по которым, в свою очередь, могут рассчитываться скалярные признаки, такие как:

- среднее;
- дисперсия;
- наибольшее значение;
- наименьшее значение;
- разность наибольшего и наименьшего значений.

Любая комбинация полученных чисел может далее использоваться в качестве вектора признаков, построенного путём анализа среднего значения и среднего числа переходов.

Второй способ предполагает развёртку двумерной битовой плоскости в одномерную последовательность нулей и единиц с последующим расчётом некоторых её статистических характеристик.

При одномерной развёртке близкие на плоскости пиксели должны располагаться как можно ближе в результирующей последовательности.

Наиболее часто используются три развёртки: построчная, серпантинная, а также развёртка Пеано (или Гильберта–Пеано) [80]. Все они проиллюстрированы на рис. 4.1. Развёртка Гильберта–Пеано строится по рекуррентной формуле для областей, размеры которых являются целыми степенями двойки, путём склеивания четырёх шаблонов развёртки области предыдущей степени [81]. Таким образом, данная развёртка постоянно меняет своё направление, охватывая близлежащие пиксели в обоих измерениях. Очевидно, что последние две развёртки имеют преимущество по сравнению с построчной, поскольку не имеют разрывов.

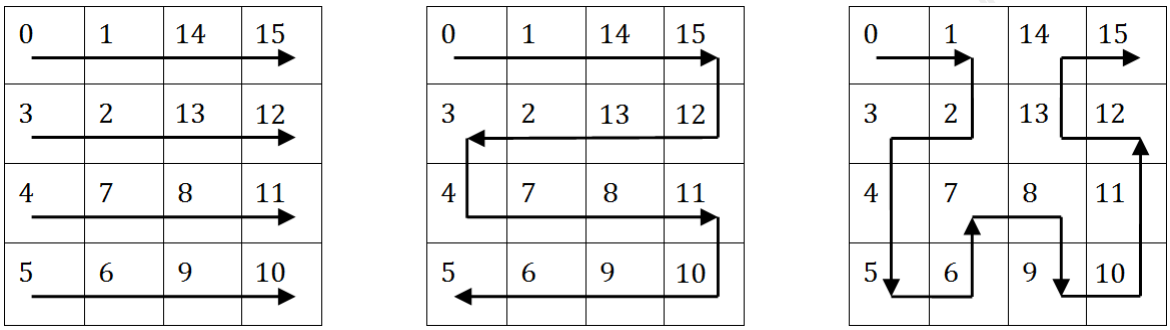


Рис. 4.1 – Развёртки двумерной области 4×4: построчная (слева), серпантинная (в центре), Гильберта–Пеано (справа)

Обозначим полученную последовательность $\{\beta_k\}_{k=0..N-1}$, где $N = N_1 N_2$.

Первый вариант её дальнейшего использования заключается в расчёте относительной частоты переходов между соседними отсчётами последовательности:

$$\pi_{00} = \frac{1}{N-1} \sum_{k=0}^{N-2} \gamma_k^{00}, \tag{4.7}$$

где

$$\gamma_k^{00} = \begin{cases} 1, & (\beta_k = 0) \wedge (\beta_{k+1} = 0), \\ 0, & \text{иначе.} \end{cases} \tag{4.8}$$

По аналогичным формулам находятся также π_{01}, π_{10}, π_{11}, в совокупности образуя вектор из четырёх признаков:

$$(\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}). \tag{4.9}$$

В случае заполненного контейнера частоты переходов должны быть достаточно близкими, в то время как в пустом контейнере частоты переходов из 0 в 0 и из 1 в 1 значительно превышают частоты переходов двух других видов. На рис. 4.2 показан пример диаграммы частот переходов для разных битовых плоскостей пустого контейнера в сравнении с заполненной битовой плоскостью, рассчитанных по последовательности, полученной

при помощи построчной развёртки. Статистика пустого контейнера считалась по изображению “Lenna” (рис. 3.3а).

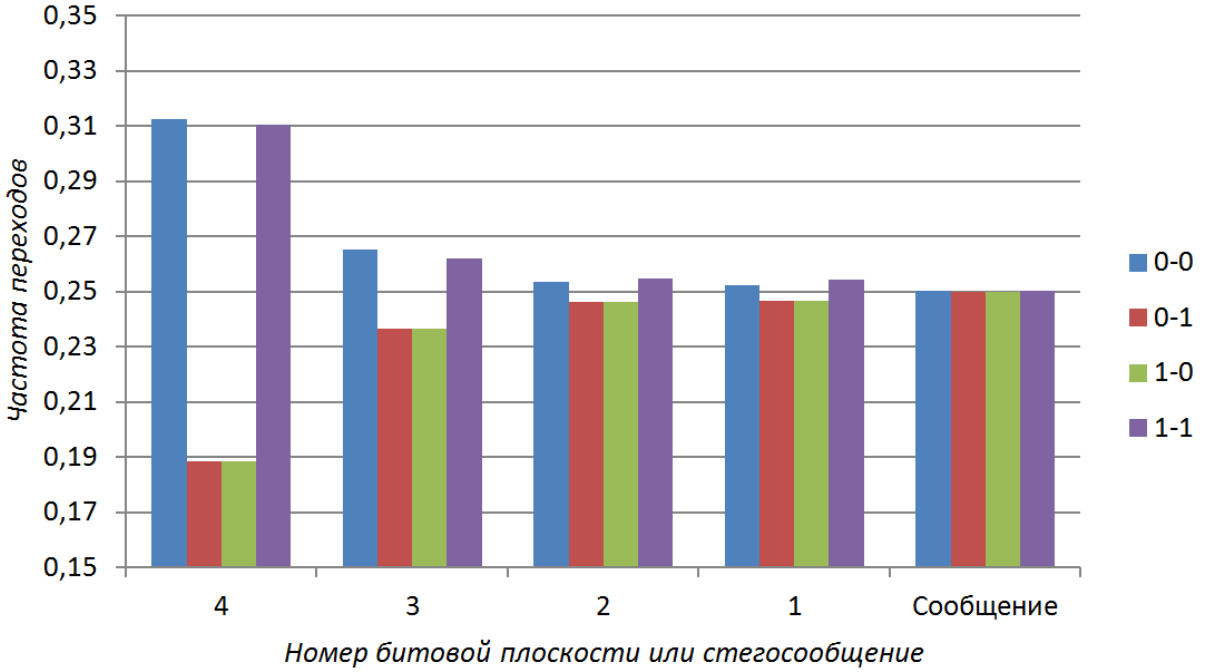


Рис. 4.2 – Диаграмма частоты переходов для пустого и заполненного контейнера

Другой способ формирования признаков по двоичной последовательности – расчёт числа серий разной длины. Серией является фрагмент последовательности, состоящий из одинаковых значений (неважно, единиц или нулей) и ограниченный другими значениями или границей последовательности. Достаточно информативной характеристикой последовательности является статистика, отражающая число серий различной длины. Будем обозначать её $\{s_i\}_i$, где $i > 0$ – длина серии. Иногда эту статистику нормируют на длину последовательности N, чтобы получить значения, не зависящие от объёма контейнера:

$$\{v_i\}_i = \left\{\frac{s_i}{N}\right\}_i. \qquad (4.10)$$

В табл. 4.1 приведён пример статистики числа серий последовательностей, полученных при помощи построчной развертки первой битовой плоскости пустого и заполненного контейнера. Статистика пустого контейнера считалась по изображению “Lenna” (рис. 3.3а).

Как видно из таблицы, число серий малой длины в заполненном контейнере превышает число серий в пустом контейнере, но начиная с некоторого значения i статистика по пустому контейнеру становится выше. Если рассматривать очень большие серии – длиной в несколько десятков отсчётов, то в заполненном контейнере таковые почти всегда отсутствуют, в то время как в пустом время от времени могут появляться.

Табл. 4.1 – Пример статистики числа серий в пустом и заполненном контейнере

i	Число серий s_i		i	Число серий s_i	
	Пустой контейнер	Заполненный контейнер		Пустой контейнер	Заполненный контейнер
1	64097	65363	12	48	37
2	32462	32741	13	14	14
3	16143	16596	14	7	11
4	8124	8131	15	7	1
5	4155	4093	16	6	3
6	2075	2054	17	3	1
7	1076	964	18	1	0
8	584	539	19	1	0
9	320	245	20	1	0
10	169	138	21	0	0
11	94	63	22	0	0

Наиболее простой способ формирования вектора признаков по статистике числа серий – выбор в качестве признаков некоторого количества

$$\{s_i\}_{i\in I}. \tag{4.11}$$

При этом множество I также может формироваться различными способами. Некоторым недостатком такого подхода является существенное различие в абсолютных значениях s_i для разных длин i. Эта проблема может решаться путём корректировки векторов признаков либо априори (то есть путём подбора таких $\{k_i\}_{i\in I}$, что величины $\{s_i k_i\}_{i\in I}$ имеют примерно один порядок), либо на основе обучающей выборки путём нормировки векторов признаков.

Рассмотренные признаки просты для изучения, но не слишком хороши для используемых на практике стеганографических методов. Даже простые модификации системы НЗБ-встраивания позволяют обеспечить стойкость некоторым из рассмотренных признаков. Поэтому учёными были разработаны более эффективные признаки для НЗБ-стегоанализа, такие как HCF [82], ALE [83] и др. Более подробно данный материал рассмотрен в работах [84, 83] и книгах [2, 15].

4.2.2. Метод гистограмм пар значений

Одним из самых простых и наиболее известных методов целенаправленного стегоанализа НЗБ-встраивания является метод гистограмм пар значений.

Данный метод стегоанализа использует расчёт статистики хи-квадрат для проверки гипотезы о виде распределения яркости контейнера. Пусть для простоты проверяется наличие встраивания информации в первую битовую плоскость. Тогда теоретически значения яркости, отличающиеся только младшим битом (0 и 1, 2 и 3, 4 и 5,…), должны быть равновероятны. Таким образом, метод заключается в расчёте эмпирической гистограммы анализируемого изображения $h_i^e, i = 0..255$, а также соответствующей ей теоретической:

$$h_i^t = \frac{h^e_{2\cdot[i/2]} + h^e_{2\cdot[i/2]+1}}{2}. \tag{4.12}$$

На рис. 4.3 показан пример эмпирической и теоретической гистограмм. Соответствие эмпирической гистограммы теоретической проверяется посредством расчёта статистики хи-квадрат для чётных отсчётов гистограммы:

$$\chi^2 = \sum_{i=0}^{127} \frac{(h^t_{2i} - h^e_{2i})^2}{h^t_{2i}} \tag{4.13}$$

Рис. 4.3 – Пример эмпирической гистограммы изображения (жёлтый цвет) и соответствующей ей теоретической гистограммы (красный цвет)

и проверки условия

$$\chi^2 < \chi^2_\alpha(k-1), \qquad (4.14)$$

где α – уровень значимости, а $k-1=127$ – число степеней свободы. Если неравенство (4.14) справедливо, то принимается решение о наличии в контейнере встроенной информации.

Данный метод позволяет обнаружить НЗБ-встраивание в условиях полного заполнения битовой плоскости. При низкой заполненности контейнера (см. формулу (3.7)) метод работает значительно хуже. Кроме того, по понятным причинам он не позволяет обнаружить ±1-встраивание.

В книгах [2, 15] рассматривается метод Sample Pair Analysis, являющийся более эффективным для обнаружения НЗБ-встраивания. Помимо собственно факта встраивания информации, он позволяет с высокой точностью оценить заполненность контейнера.

4.2.3. ±1-встраивание

При встраивании информации в p-ю битовую плоскость яркость отдельно взятого пикселя либо не меняется, либо меняется ровно на p, причём известно, в какую сторону. Пусть для определённости $p=2$ и стоит задача встроить в пиксель с яркостью 21 значение 1. Число 21 в двоичной записи имеет вид 10101, то есть во второй битовой плоскости стоит 0. Таким образом, встраивая туда 1, мы прибавляем к текущему значению p и в итоге получаем 23. Однако что произойдёт, если мы не прибавим p, а вычтем? Очевидно, что в этом случае разница между искомым и полученным значением составит $2p$, то есть изменения произойдут в более старших разрядах двоичной записи, в то время как p-й бит не претерпит изменений. Действительно, в нашем примере получится число 19, то есть 10011 в двоичной записи. Таким образом, мы имеем два способа изменения значения яркости пикселя, приводящих к идентичным изменениям в нужной битовой плоскости и сопровождаемых равными по абсолютной величине искажениями. Это свойство позволяет несколько модифицировать процедуру стеганографического НЗБ-встраивания путём внесения дополнительной неопределённости, способствующей защите от атак, направленных на обнаружение канала скрытой передачи информации.

СВИ-18 (±1-встраивание)

Скрытая передача информации за счёт изменения отсчётов контейнера на ±1 [15]

Рассуждения выше приводились для общего случая p-й битовой плоскости. Однако на практике чаще всего ограничиваются рассмотрением

случая $p = 1$. Более того, само название данной модификации НЗБ-метода, укоренившееся в научной литературе – ±1-встраивание, – уже косвенно говорит о номере битовой плоскости (в общем случае следовало бы говорить о $\pm$-встраивании). Мы приведём формулу встраивания для этого частного случая, однако её обобщение не составит труда.

Итак, пусть b_i – *i*-й элемент вектора $\boldsymbol{b}$,

$$(n_1, n_2) = \big(n_1(\mathbf{k}, i), n_2(\mathbf{k}, i)\big)$$

– координаты *i*-го пикселя, в который необходимо встроить бит b_i, а ξ_i – псевдослучайное число, с равной вероятностью принимающее положительные и отрицательные значения (генерация последовательности $\{\xi_i\}$ также происходит на основе ключа). Тогда встраивание информации осуществляется по формуле

$$C^W(n_1, n_2) = \begin{cases} C(n_1, n_2), & C_1(n_1, n_2) = b_i, \\ C(n_1, n_2) + 1, & (C_1(n_1, n_2) \neq b_i) \wedge \big((\xi_i \geq 0) \wedge \\ & \wedge (C(n_1, n_2) < 255) \vee (C(n_1, n_2) = 0)\big), \\ C(n_1, n_2) - 1, & (C_1(n_1, n_2) \neq b_i) \wedge \big((\xi_i < 0) \wedge \\ & \wedge (C(n_1, n_2) > 0) \vee (C(n_1, n_2) = 255)\big), \end{cases} \quad (4.15)$$

то есть случайным образом прибавляется или вычитается единица в том случае, если значение бита не совпадает с требуемым.

Извлечение информации происходит так же, как и в СВИ-2.

Библиографический список

1. Barni, M. Watermarking Systems Engineering [Text] / M. Barni, F. Bartolini. — New-York: Marcel Dekker, Inc., 2004. — 485 p.
2. Digital Watermarking and Steganography [Text] / I.J. Cox [et al.]. — 2nd ed. — Morgan Kaufmann Publishers, 2008. — 596 p.
3. Mayer, G. Image Repository [Electronic resource] / G. Mayer // University of Waterloo Fractal coding and analysis group, 2009. — Режим доступа: http://links.uwaterloo.ca/Repository.html (23.03.2017).
4. Грибунин, В.Г. Цифровая стеганография [Текст] / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
5. Стеганография, цифровые водяные знаки и стеганоанализ [Текст] / А.В. Аграновский [и др.]. — М.: Вузовская книга, 2009. — 220 с.
6. Генне, О.В. Основные положения стеганографии [Электронный ресурс] / О.В. Генне. — 2000. — Режим доступа: http://citforum.ru/internet/securities/stegano.shtml (дата обращения: 20.12.2016).
7. Секретные чернила [Электронный ресурс]. — Режим доступа: http://www.alhimik.ru/show/show13.html (дата обращения: 20.12.2016).
8. Стеганография [Электронный ресурс] // Википедия: свободная энцикопедия. — Режим доступа: https://ru.wikipedia.org/wiki/Стеганография (дата обращения: 20.12.2016).
9. Schneir, B. Applied Cryptography [Text] / B. Schneir. — John Wiley & Sons, Inc., 1996. — 662 p.
10. Simmons, G.J. The history of subliminal channels [Text] / G.J. Simmons // LNCS. — Vol. 1174. —1996. — P. 237–256.
11. Стеганография [Электронный ресурс] // Академик. — Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/30097 (дата обращения: 20.12.2016).
12. Текин, В. Текстовая стеганография [Электронный ресурс] / В. Текин. — Режим доступа: http://citforum.ru/internet/securities/stegano.shtml (дата обращения: 20.12.2016).
13. A review of watermarking, principles and practices [Text] / M.L. Miller [et al.] // Digital Signal Processing in Multimedia Systems; ed. by K.K. Parhi, T. Nishitani. — Marcel Dekker, Inc., 1999. — P. 461–485.
14. Cox, I.J. Digital Watermarking [Text] / I.J. Cox, M.L. Miller, J.A. Bloom. — San Francisco: Morgan Kaufmann Publishers, 2002. — 568 p.
15. Fridrich, J. Steganography in digital media: principles, algorithms, and applications [Text] / J. Fridrich. — Cambridge University Press, 2010. — 450 p.
16. Petitcolas, F.A.P. Information Hiding - A Survey [Text] / F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn // Proceedings of the IEEE. — 1999. — Vol. 87. — No. 7. — P. 1062–1078.

17. Katzenbeisser, S. Information Hiding Techniques for Steganography and Digital Watermarking [Text] / S. Katzenbeisser, F.A.P. Petitcolas. — Boston, London: Artech House, Inc., 2000. — 237 p.
18. Cole, E. Hiding in Plain Sight: Steganography and the Art of Covert Communication [Text] / E. Cole. — Wiley Publishing, Inc., 2003. — 362 p.
19. Pfitzmann, B. Information Hiding Terminology: Results of an informal plenary meeting and additional [Text] / B. Pfitzmann // Springer LNCS. — Vol. 1174. — 1996. — P. 347–350.
20. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев: МК-Пресс, 2006. — 288 с.
21. Гонсалес, Р. Цифровая обработка изображений [Текст] / Р. Гонсалес, Р. Вудс. — М.: Техносфера, 2005. — 1072 с.
22. Методы компьютерной обработки изображений [Текст] / под ред. В.А. Сойфера. —2-е изд. — М.: Физматлит, 2003. — 784 с.
23. Цветовая модель [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Цветовая_модель (дата обращения: 24.03.2017).
24. CMYK [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/CMYK (дата обращения: 24.03.2017).
25. HSV (цветовая модель) [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/HSV_(цветовая_модель) (дата обращения: 24.03.2017).
26. Зрение человека [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Зрение_человека (дата обращения: 24.03.2017).
27. Axelson, P.E. Quality Measures of Halftoned Images (A Review) [Text] / P.E. Axelson. — Linköping, Linköping University, 2003.
28. Звук [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Звук (дата обращения: 24.03.2017).
29. Вербовой, В. Метрики для сравнения звуковых сигналов с учетом особенностей человеческого слуха [Электронный ресурс] / В. Вербовой. — Режим доступа: http://cgm.computergraphics.ru/content/view/73 (дата обращения: 01.09.2010).
30. Chen, B. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding [Text] / B. Chen, B. Wornell // IEEE Transactions on Information Theory. — 2001. — Vol. 47. — No. 4. — P. 1423–1443.
31. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации [Текст] / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. — 2011. — Т. 35. — С. 262–267.
32. Lau, D.L. Modern digital halftoning [Text] / D.L. Lau, G.R. Arce. — New-York: Marcel Dekker, Inc., 2001.
33. Fu, M.S. Data hiding watermarking for halftone images [Text]: Ph.D. Thesis / M.S. Fu. — The Hong Kong University of Science and Technology, Hong Kong, 2003.

34. Floyd, R.W. An adaptive algorithm for spatial gray-scale [Text] / R.W. Floyd, L. Steinberg // Proceedings Society Information Display. — 1976. — Vol. 17. — No. 2. — P. 75–78.
35. Fan, Z. Error diffusion with a more symmetric error distribution [Text] / Z. Fan // Proceedings of SPIE. — Vol. 2179. — 1994. — P. 150–158.
36. Jarvis, J.F. A survey of techniques for the display of continuous-tone pictures on bilevel displays [Text] / J.F. Jarvis, C.N. Judice, W.H. Ninke // Comp. Graf. Im. Pr. — 1976. — Vol. 5. — No. 2. — P. 13–40.
37. Stucki, P. MECCA – a multiple-error correcting computation algorithm for bilevel image hardcopy reproduction [Text]: Technical Report RZ1060 / P. Stucki. — Zurich, 1981.
38. Cox, I.J. A secure, imperceptible yet perceptually salient, spread spectrum watermark for multimedia [Text] / I.J. Cox, J. Killan, T. Leighton, T. Shamoon // IEEE Southcon'96 Conference Record. — 1996. — P. 192-197.
39. Cox, I.J. A secure, robust watermark for multimedia [Text] / I.J. Cox, J. Killan, T. Leighton, T. Shamoon // International Workshop on Information Hiding. — 1996. — P. 185-206.
40. Cox, I.J. Secure spread spectrum watermarking for images, audio and video [Text] / I.J. Cox, J. Killan, T. Leighton, T. Shamoon // Proceedings of 1996 IEEE International Conference on Image Processing. — 1996. — Vol. 3. — P. 243-246.
41. Cox, I.J. Secure Spread Spectrum Watermarking for Multimedia [Text] / I.J. Cox // IEEE Transactions on Image Processing. — 1997. — Vol. 6. — No. 12. — P. 1673–1687.
42. Barni, M. A DCT-domain system for robust image watermarking [Text] / M. Barni, F. Bartolini, V. Cappellini, A. Piva // Signal Processing. — 1998. — Vol. 66. — No. 3. — P. 357–372.
43. DCT-based watermark recovering without resorting to the uncorrupted original image [Text] / A. Piva [et al.] // Proceedings of 1997 IEEE International Conference on Image Processing. — 1997. — Vol. 1. — P. 520–523.
44. Seo, J.S. On the design of template in the autocorrelation domain [Text] / J.S. Seo, C.D. Yoo // Proc. SPIE. — 2002. — P. 305-312.
45. Das, T.S. Spread spectrum based m-ary modulated robust image watermarking [Text] / T.S. Das, V.H. Mankar, S.K. Sarkar // IJCSNS International Journal of Computer Science and Network Security. — 2007. — Vol. 7. — No. 10. — P. 154-160.
46. Moreno, O. New families of arrays in two dimensions for watermarking applications [Text] / O. Moreno, A.Z. Tirkel, U. Parampalli, R.G. Van Schyndel // Electronics letters. — 2010. — Vol. 46. — No. 22. — P. 1500-1502.
47. Tirkel, A. A two-dimensional digital watermark [Text] / A.Z. Tirkel, R. G. van Schyndel, C. F. Osborne // Dicta. – 1995. – Vol. 95. – P. 5–8.
48. Doërr, G. Danger of low-dimensional watermarking sub-spaces [Text] / G. Doërr, J. L. Dugelay // 29th IEEE International Conference on Acoustics, Speech, and Signal Processing. – 2004. – Vol. 3. – P. 93–96.

49. Gyorfi, L. Constructions of binary constant-weight cyclic codes and cyclically permutable codes [Text] / L. Gyorfi, J. L. Massey // IEEE Transactions on Information Theory. – 1992. – Vol. 38. – P. 940–949.
50. Moreno, O. New constructions of optimal cyclically permutable constant weight codes [Text] / O. Moreno, Z. Zhang, P. V. Kumar, V. A. Zinoviev // IEEE Transactions on Information Theory. – 1995. – Vol. 41. – No. 2. – P. 448–455.
51. Bitan, S. Constructions for optimal constant weight cyclically permutable codes and difference families [Text] / S. Bitan, T. Etzion // IEEE Transactions on Information Theory. – 1995. – Vol. 41. – P. 77–87.
52. Rotation, scale, and translation resilient watermarking for images [Text] / C. Y. Lin, M. Wu, J. A. Bloom [et al.] // IEEE Transactions on Image Processing. – 2001. – Vol. 10. – No. 5. – P. 767–782.
53. Robust digital image watermarking method against geometrical attacks [Text] / B. S. Kim [et al.] // Real-Time Imaging. – 2003. – Vol. 9. – No. 2. – P. 139–149.
54. O'Ruanaidh, J. J. Rotation, scale and translation invariant digital image watermarking [Text] / J. J. O'Ruanaidh, T. Pun // Proceedings of 1997 IEEE International Conference on Image Processing. – 1997. – Vol. 1. – P. 536–539.
55. Mitekin, V. A. A new watermarking sequence generation algorithm for collision-free digital watermarking [Text] / V. A. Mitekin, E. I. Timbay // Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on. – 2012. – P. 256–260.
56. Петрович, Н.Т. Системы связи с шумоподобными сигналами [Текст] / Н.Т. Петрович, М.К. Размахнин – М.: Советское радио, 1969. – 233 с.
57. Moreno, O. New optimal low correlation sequences for wireless communications [Text] / O. Moreno, A. Tirkel // International Conference on Sequences and Their Applications. – 2012. – P. 212–223.
58. Algebraic construction of a new class of quasi-orthogonal arrays for steganography [Text] / R. G. Van Schyndel, A. Z. Tirkel, I. D. Svalbe [et al.] // Electronic Imaging. – 1999. – P. 354–364.
59. Gong, G. New designs for signal sets with low cross correlation, balance property, and large linear span: Gf (p) case [Text] / G. Gong // IEEE Transactions on Information Theory. – 2002. – Vol. 48. – No. 11. – P. 2847–2867.
60. Yu, N. Y. A new binary sequence family with low correlation and large size [Text] / N. Y. Yu, G. Gong // IEEE Transactions on Information Theory. – 2006. – No. 4. – Vol. 52. – P. 1624–1636.
61. Spread-spectrum digital watermarking concepts and higher dimensional array constructions [Text] / R. G. Van Schyndel, A. Z. Tirkel, I. D. Svalbe [et al.] // First International Online Symposium on Electronics Engineering. – 2000. – P. 1–13.
62. Сэломон, Д. Сжатие данных, изображений, звука [Текст] / Д. Сэломон. — М.: Техносфера, 2004. — 339 с.
63. Jähne, B. Digital Image Processing [Text] / B. Jähne. — Springer, 2005. — 631 p.

64. Перспективные информационные технологии дистанционного зондирования земли [Текст] / под ред. В.А. Сойфера. — Самара: Новая техника, 2015. — 255 с.
65. Popescu, A.C. Statistical Tools for Digital Image Forensics [Text]: Ph. D. Thesis / A.C. Popescu. — Dartmouth College, 2004.
66. Celik, M.U. Lossless generalized LSB data embedding [Text] / M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber // IEEE Transactions on Image Processing. — 2005. — Vol. 14. — No. 2. — P. 253–266.
67. Goljan, M. Distortion-Free Data Embedding for Images [Text] / M. Goljan, J. Fridrich, R. Du // Springer LNCS. — Vol. 2137. — 2001. — P. 27–41.
68. Lin, C.-Y. Issues and solutions for authenticating MPEG video [Text] / C.-Y. Lin, S.-F. Chang // Proceedings of SPIE. — Vol. 3657. — 1999.
69. Yeung, M. An invisible watermarking technique for image verification [Text] / M. Yeung, F. Mintzer // International Conference on Image Processing. — 1997. — Vol. 1. — P. 680–683.
70. Doërr, G. Security pitfalls of frame-by-frame approaches to video watermarking [Text] / G. Doërr, J.L. Dugelay // IEEE Transactions on Signal Processing. — 2004. — Vol. 52. — No. 10. — P. 2955–2964.
71. Hartung, F. Watermarking of Uncompressed and Compressed Video [Text] / F. Hartung, B. Girod // Signal Processing. — 1998. — Vol. 66. — No. 3. — P. 283–301.
72. Kalker, T. A Video Watermarking System for Broadcast Monitoring [Text] / T. Kalker // Proceedings of SPIE. — Vol. 3657. — 1999.
73. Митекин, В.А. Метод встраивания информации в видео, стойкий к ошибкам потери синхронизации [Текст] / В.А. Митекин, В.А. Федосеев // Компьютерная оптика. — 2014. — Т. 38, №3. — С. 564–573.
74. Mitekin, V. A new method for high-capacity information hiding in video robust against temporal desynchronization [Text] / V. Mitekin, V. Fedoseev // Proceedings of SPIE. — Vol. 9445. — 2015. — P. 94451A-1—94451A-7.
75. Kalker, T. Analysis of Watermark Detection using SPOMF / T. Kalker, A. Janssen // Proceedings of ICIP. — 1999. — Vol. 1. — P. 316-319.
76. Ту, Д. Принципы распознавания образов [Текст] / Д. Ту, Р. Гонсалес. — М.: Мир, 1978.
77. Вапник, В.Н. Теория распознавания образов. Статистические проблемы обучения [Текст] / В.Н. Вапник, А.Я. Червоненкис. — М.: Наука, 1974.
78. James, G. An introduction to statistical learning [Text] / G. James, D. Witten, T. Hastie, R. Tibshirani. — New York: Springer, 2013.
79. Воронцов, К.В. Машинное обучение (курс лекций) [Электронный ресурс] . — 2015. — Режим доступа: http://www.machinelearning.ru/wiki/index.php?-title=Машинное_обучение_(курс_лекций%2C_К.В.Воронцов) (09.12.2015).
80. Sagan, H. Space-filling curves [Text] / H. Sagan. — New York: Springer, 1994. — 193 p.
81. Сергеев, В.В. Обработка изображений с использованием развертки Гильберта–Пеано [Текст] / В.В. Сергеев // Автометрия. — 1984. — Т. 2. — С. 30–36.

82. Harmsen, J. Higher-order statistical steganalysis of palette images [Text] / J. Harmsen, W. Pearlman // Proceedings of SPIE. — Vol. 5020. — 2003. — P. 131–142.
83. Cancelli, G. New techniques for steganography and steganalysis in the pixel domain [Text]: Ph.D. Thesis / G. Cancelli. — University of Siena, Siena, 2009.
84. A comparative study of ±1 steganalyzers [Text] / G. Cancelli [et al.] // IEEE 10th Workshop on Multimedia Signal Processing. — 2008. — P. 791–796.

Предметный указатель

Учебное издание

Виктор Андреевич Федосеев
Виталий Анатольевич Митекин

Теоретические основы стеганографии
и цифровых водяных знаков
Учебное пособие

Редактор Ю.Н. Литвинова
Вёрстка В.А. Федосеев

Подписано в печать 06.03.2017. Формат 60×90/16.
Печ. л. 8,25. Тираж 30 экз. Заказ
Бумага офсетная. Печать офсетная.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
имени академика С.П. Королева»
443086 Россия, г.Самара, Московское шоссе, 34

Изд-во Самарского ун-та. 443086 Россия, г.Самара, Московское шоссе, 34