ГОСУДАРСТВЕННЫЙ КОМИТЕТ

СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра "Информационная безопасность"

Допустить к защите

зав. кафедрой «ИБ»

Юсупов С.Ю._____

" _____ "_____ 2013 г.

Выпускная
квалификационная работа бакалавра

НА ТЕМУ «Анализ стеганографических алгоритмов защиты информации в инфокоммуникационных системах»

Выпускник _____ Алиев И.А.
(подпись) (Ф.И.О)

Руководитель _____ Шарипов З.З.
(подпись) (Ф.И.О)

Консультант по БЖД _____ Кодиров Ф.М.
(подпись) (Ф.И.О)

Рецензент _____ Зарипов О.О.
(подпись) (Ф.И.О)

Ташкент – 2013

СОДЕРЖАНИЕ

Введение

В постановлении Президента Республики Узбекистан "О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий" от 21 марта 2012 год, № ПП-1730 [1] особое внимание уделено вопросам "Совершенствования системы регулирования в сфере информационно-коммуникационных технологий с учетом состояния развития информационных ресурсов технологий и систем...".

Сегодня нередко возникает необходимость передать конфиденциальное сообщение небольшого объёма, при этом использование сложных криптографических систем по ряду причин затруднительно. Одной из таких причин является невозможность использования надёжных продуктов, которые, как правило, являются коммерческими и для рядового пользователя компьютера недоступны.

Стеганография - (от греческого скрытый, буквально «тайнопись») - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Стеганография была изобретена людьми ещё в Древние времена, когда об использовании каких-то технических средств для передачи информации было невозможно, по причине их отсутствия. Сегодня существует огромное количество средств и способов передачи информации, при этом сохранить сам факт передачи информации достаточно сложно.

В этом плане выпускная квалификационная работа Алиев И.А. посвященная вопросам анализа стеганографических алгоритмов защиты информации в инфокоммуникационных системах, не вызывает сомнений в актуальности.

ВКР состоит из введения, трех часть, заключения, списка используемой литературы и приложения.

Во введении обоснована актуальность темы выпускной квалификационной работы.

В первом разделе рассматриваются классификация методов сокрытия информации, анализ существующих методов стегоанализа, стеганографические протоколы, а также описываются методы противодействия атак на стеганографических систем.

Во втором разделе построены математические модели стеганографии, рассмотрено скрытие данных в неподвижных изображениях, проведен анализ аддитивных алгоритмов на основе линейного встраивания данных, а также приведены критерии эффективности и количественная оценка искажений в стеганографии изображений.

Третий раздел включает в себя безопасность жизнедеятельности.

В заключении представлены основные выводы выпускной квалификационной работы и предложения по совершенствованию.

1. ОБЗОРНАЯ ЧАСТЬ. СУЩЕСТВУЮЩИЕ МЕТОДЫ И СПОСОБЫ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

1.1. Классификация методов сокрытия информации

Стеганографическая система (стегосистема) – объединение методов и средств используемых для создания скрытого канала для передачи информации. При построении такой системы условились о том, что:

1) враг представляет работу стеганографической системы. Неизвестным для противника является ключ, с помощью которого можно узнать о факте существования и содержания тайного сообщения.

2) При обнаружении противником наличия скрытого сообщения он не должен смочь извлечь сообщение до тех пор пока он не будет владеть ключом.

3) Противник не имеет технических и прочих преимуществ.

▪ Сообщение – это термин, используемый для общего названия передаваемой скрытой информации, будь то лист с надписями молоком, голова раба или цифровой файл.

▪ Контейнер – так называется любая информация, используемая для сокрытия тайного сообщения. Пустой контейнер – контейнер, не содержащий секретного послания. Заполненный контейнер (стегоконтейнер) – контейнер, содержащий секретное послание [2].

▪ Стеганографический канал (стегоканал) – канал передачи стегоконтейнера.

▪ Ключ (стегоключ) – секретный ключ, нужный для сокрытия стегоконтейнера. Если стегосистема использует секретный ключ, то он должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить из него

закрытый ключ. В этом случае открытый ключ мы можем передавать по незащищённому каналу.

Большинство методов компьютерной стеганографии базируется на двух принципах.

Первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности.

Второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в таких исходных файлах.

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначимых фрагментов среды и замена существующей в них информации на информацию, которую предполагается защитить. Поскольку в компьютерной стеганографии рассматриваются среды, поддерживаемые средствами вычислительной техники и соответствующими сетями, то вся информационная среда, в конечном итоге, может представляться в цифровом виде. Таким образом, незначимые для кадра информационной среды фрагменты в соответствии с тем или иным алгоритмом или методикой заменяются (смешиваются) на фрагменты скрываемой информации. Под кадром информационной среды в данном случае подразумевается некоторая ее часть, выделенная по определенным признакам. Такими признаками часто бывают семантические характеристики выделяемой части информационной среды. Например, в качестве кадра может быть выбран некоторый отдельный рисунок, звуковой файл, Web-страница и др.

Классификация методов компьютерной стеганографии

Для методов компьютерной стеганографии можно ввести определенную классификацию (рис.1.1).

Рис.1.1 Классификация методов сокрытия информации

По способу отбора контейнера, как уже указывалось, различают методы суррогатной стеганографии, селективной стеганографии и конструирующей стеганографии.

В методах суррогатной (безальтернативной) стеганографии отсутствует возможность выбора контейнера и для сокрытия сообщения выбирается первый попавшийся контейнер, зачастую не совсем подходящий к встраиваемому сообщению. В этом случае, биты контейнера заменяются битами скрываемого сообщения таким образом, чтобы это изменение не было заметным. Основным недостатком метода является то, он позволяет скрывать лишь незначительное количество данных.

В методах селективной стеганографии предполагается, что спрятанное сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое число

альтернативных контейнеров, чтобы затем выбрать наиболее подходящий из них для конкретного сообщения. Частным случаем такого подхода является вычисление некоторой хеш-функция для каждого контейнера. При этом для сокрытия сообщения выбирается тот контейнер, хеш-функции которого совпадает со значением хеш-функции сообщения [3].

В методах конструирующей стеганографии контейнер генерируется самой стегосистемой. Здесь может быть несколько вариантов реализации. Так, например, шум контейнера может моделироваться скрываемым сообщением. Это реализуется с помощью процедур, которые не только кодируют скрываемое сообщение под шум, но и сохраняют модель первоначального шума. В предельном случае по модели шума может строиться целое сообщение. По способу доступа к скрываемой информации различают методы для потоковых (непрерывных) контейнеров и методы для контейнеров с произвольным доступом (ограниченной длины).

Методы, использующие потоковые контейнеры, работают с потоками непрерывных данных (например, интернет-телефония). В этом случае скрываемые биты необходимо в режиме реального времени включать в информационный поток. О потоковом контейнере нельзя предварительно сказать, когда он начнется, когда закончится и насколько продолжительным он будет. Более того, объективно нет возможности узнать заранее, какими будут последующие шумовые биты. Существует целый ряд трудностей, которые необходимо преодолеть корреспондентам при использовании потоковых контейнеров. Наибольшую проблему при этом составляет синхронизация начала скрытого сообщения.

Методы, которые используются для контейнеров с произвольным доступом, предназначены для работы с файлами фиксированной длины (текстовая информация, программы, графические или звуковые файлы). В этом случае заранее известны размеры файла и его содержимое. Скрываемые биты могут быть равномерно выбраны с помощью подходящей

псевдослучайной функции. Недостаток таких контейнеров состоит в том, они обладают намного меньшими размерами, чем потоковые, а также то, что расстояния между скрываемыми битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный шум будет иметь экспоненциальное распределение длин интервала. Преимущество подобных контейнеров состоит в том, то они могут быть заранее оценены с точки зрения эффективности выбранного стеганографического преобразования.

По типу организации контейнеры, подобно помехозащищенным кодам, могут быть систематическими и несистематическими. В систематически организованных контейнерах можно указать конкретные места стеганограммы, где находятся информационные биты самого контейнера, а где — шумовые биты, предназначенные для скрываемой информации (как, например, в широко распространенном методе наименьшего значащего бита). При несистематической организации контейнера такого разделения сделать нельзя. В этом случае для выделения скрытой информации необходимо обрабатывать содержимое всей стеганограммы.

По используемым принципам стеганометоды можно разбить на два класса: цифровые методы и структурные методы. Если цифровые методы стеганографии, используя избыточность информационной среды, в основном, манипулируют с цифровым представлением элементов среды, куда внедряются скрываемые данные (например, в пиксели, в различные коэффициенты косинус-косинусных преобразований, преобразований Фурье, Уолша-Радемахера или Лапласа), то структурные методы стеганографии для сокрытия данных используют семантически значимые структурные элементы информационной среды.

Основным направлением компьютерной стеганографии является использование свойств избыточности информационной среды. Следует учесть, что при сокрытии информации происходит искажение некоторых

статистических свойств среды или нарушение ее структуры, которые необходимо учитывать для уменьшения демаскирующих признаков.

В особую группу можно также выделить методы, которые используют специальные свойства форматов представления файлов:

- зарезервированные для расширения поля компьютерных форматов файлов, которые обычно заполняются нулями и не учитываются программой;
- специальное форматирование данных (смещение слов, предложений, абзацев или выбор определенных позиций букв);
- использование незадействованных мест на магнитных носителях;
- удаление идентифицирующих заголовков для файла.

По предназначению различают стеганографические методы собственно для скрытой передачи или скрытого хранения данных и методы для сокрытия данных в цифровых объектах с целью защиты самих цифровых объектов.

По типу информационной среды выделяются стеганографические методы для текстовой среды, для аудио среды, а также для изображений (стоп-кадров) и видео среды.

1.2. Анализ методов стеганографической защиты

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1) Методы, основанные на использовании специальных свойств компьютерных форматов;

2) Методы, основанные на избыточности аудио и визуальной информации.

Сравнительные характеристики стеганографических методов. Таблица 1.1

Стеганографические методы	Краткая характеристика методов	Недостатки	Преимущества
1. Методы использования специальных свойств компьютерных форматов данных			
1.1.Методы использования	Поля расширения имеются во многих	Низкая степень скрытности, передача	Простота использования

зарезервированных для расширения полей компьютерных форматов данных	мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	небольших ограниченных объемов информации	
1.2. Методы специального форматирования текстовых файлов:			
1.2.1. Методы использования известного смещения слов, предложений, абзацев	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	1. Слабая производи-тельность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих - частный случай этого метода (например, начальные буквы каждой строки образуют сообщение)	1. Слабая производи-тельность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.3.Методы использования специальных свойств полей форматов, не отображаемых на экране	Методы основаны на использовании специальных "невидимых", скрытых полей для организации сносок и ссылок (например, использование черного шрифта на черном фоне)		
1.3. Методы скрытия в неиспользуемых местах гибких дисков	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	1.Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.4.Методы использования имитирующих	Метод основан на генерации текстов и является обобщением	1.Слабая производительность метода, передача небольших объемов	Результирующий текст не является подозрительным для систем

функций(mimic-function)	акростиха. Для тайного сообщения генерируется осмысленный текст, скрывающий само сообщение	информации 2. Низкая степень скрытности	мониторинга сети
1.5. Методы удаления идентифицирующего файл заголовка	Скрываемое сообщение шифруется и у результата удаляется идентифицирующий заголовок, оставляя только шифрованные данные. Получатель заранее знает о передаче сообщения и имеет недостающий заголовок	Проблема скрытия решается только частично. Необходимо заранее передать часть информации получателю	Простота реализации. Многие средства (White Noise Storm, S-Tools), обеспечивают реализацию этого метода
2. Методы использования избыточности аудио и визуальной информации			
2.1. Методы использования избыточности цифровых фотографии, цифрового звука и цифрового видео	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и дает возможность скрытия конфиденциальной информации	За счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Для снижения компрометирующих признаков требуется коррекция статистических характеристик	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения товарной марки, регистрационных номеров и т.п.

Как видно из таблицы 1.1, первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения. На основании

анализа материалов таблицы 1.1 можно сделать вывод, что основным направлением компьютерной стеганографии является использование избыточности аудио и визуальной информации.

Цифровые фотографии, цифровая музыка, цифровое видео – представляются матрицами чисел, которые кодируют интенсивность в дискретные моменты в пространстве и/или во времени [4].

Цифровая фотография – это матрица чисел, представляющих интенсивность света в определенный момент времени.

Цифровой звук – это матрица чисел, представляющая интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не точны, т.к. не точны устройства оцифровки аналоговых сигналов, имеются шумы квантования. Младшие разряды цифровых отсчетов содержат очень мало полезной информации о текущих параметрах звука и визуальнного образа. Их заполнение ощутимо не влияет на качество восприятия, что и дает возможность для скрытия дополнительной информации.

Графические цветные файлы со схемой смешения RGB кодируют каждую точку рисунка тремя байтами. Каждая такая точка состоит из аддитивных составляющих: красного, зеленого, синего. Изменение каждого из трех наименее значимых бит приводит к изменению менее 1% интенсивности данной точки. Это позволяет скрывать в стандартной графической картинке объемом 800 Кбайт около 100 Кбайт информации, что не заметно при просмотре изображения.

Другой пример. Только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1%. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

1.3. Стеганографические протоколы в криптографических системах защиты информации

Важное значение для достижения целей стеганографии имеют протоколы. По протоколом понимается «порядок действий, предпринимаемых двумя или более сторонами, предназначенный для решения определенной задачи». Можно разработать исключительно эффективный алгоритм скрытия информации, но из-за его неправильного применения не добиться своей цели. И протокол и алгоритм есть некоторая последовательность действий. Различие заключается в том, что в протокол должны быть обязательно вовлечены двое или более сторон. При этом предполагается, что участники принимают на себя обязательство следовать протоколу. Также как и алгоритм, протокол состоит из шагов. На каждом шаге протокола выполняются некоторые действия, которые могут заключаться, например, в производстве каких-то вычислений, или осуществлении некоторых действий.

Стеганография с открытым ключом

Стеганография с открытым ключом опирается на достижения криптографии последних 25 лет. Понятие «открытый ключ» означает, что для дешифровки сообщения используется другой ключ, чем при его шифровании. При этом один из ключей делается общедоступным, открытым. Криптографическая система с открытым ключом используется, например, при цифровой подписи [5]. При этом сообщение подписывается закрытым ключом, и любой, имеющий соответствующий открытый ключ, может удостовериться в ее подлинности. При шифровании данных используют обратный порядок: сообщение подписывается открытым ключом, а прочитать его может лишь имеющий соответствующий закрытый ключ. Естественно, что из открытого ключа никакими способами нельзя получить закрытый ключ (в вычислительном смысле).

Спрятанные данные могут быть дополнительно зашифрованы обычными методами, но этот вопрос не относится к стеганографии. Для того, чтобы была возможность организации стегоканала, стороны должны, как правило, иметь перед началом сеанса некоторую информацию.

Предположено, что Алиса и Боб еще во время нахождения на свободе обменялись закрытыми или открытыми ключами друг с другом. Тогда их задача заключается во встраивании сообщений в контейнер в соответствии с ключом. Встроенное сообщение не должно заметно изменять контейнер и обнаруживаться посредством статистических тестов [6]. Если Вилли злоумышленный нарушитель, то у него имеется возможность некоторого искажения сигнала, передаваемого от Алисы к Бобу. Это может привести к потере скрытого сообщения, если не использовать специальные методы (например, помехоустойчивое кодирование, или расширение спектра сигналов).

Возможно ли осуществление скрытой связи между Алисой и Бобом, если у них имеются только открытые ключи друг друга? Оказывается, да. В публикации представлен протокол, следуя которому заключенные могут наладить в этом случае скрытую «переписку». При этом надо отметить, что предположение о том, что Алиса и Боб имеют открытые ключи друг друга не является чем-то необычным. Протокол, приведенный в предполагает наличие пассивного нарушителя и заключается в следующем:

1. Алиса встраивает свое сообщение с использованием известного ей открытого ключа Боба в стегоканал, подверженный наблюдению со стороны Вилли.

2. Предполагается, что Бобу известны детали протокола, он ждет сообщение и, приняв его, извлекает из контейнера с использованием своего закрытого ключа.

Очевидным недостатком этого протокола является то что Алиса никаким путем не может предупредить Боба о начале передачи скрытого

сообщения. Поэтому Боб должен подозревать его наличие во всех принятых сообщениях и проверять их. При интенсивном обмене данными, да еще в многопользовательской среде, это может быть невыполнимо.

С другой стороны, то, что Боб проверяет все поступающие данные говорит о том, что он может стать участником стеганографического протокола. При этом у Алисы появляется возможность передать Бобу свой открытый ключ.

Известна также и модификация этого протокола, не требующая предварительного обмена открытыми ключами между Алисой и Бобом:

1. Алиса генерирует на своем компьютере пару открытого и закрытого ключа.

2. Алиса пересылает открытый ключ по каналу Бобу. Эту же информацию получает и Вилли.

3. Боб предполагает, что пересланные данные есть открытый ключ Алисы. С его помощью он шифрует сообщение, состоящее из его открытого ключа для будущей связи и (возможно) краткого «приветствия». Боб пересылает это сообщение Алисе.

4. Алиса знает, что присланные данные содержат открытый ключ Боба, дешифрует их при помощи своего закрытого ключа. У узников есть вся необходимая информация для обеспечения скрытой двусторонней связи. Так как Вилли лишь Наблюдатель, то он не может никоим образом вмешаться и помешать установлению скрытой связи между Алисой и Бобом.

Иное дело, если Вилли является активным или злоумышленным нарушителем. Тогда он не только может вносить помехи в стегоканал, но и даже полностью имитировать, скажем, Алису. Так как у Боба нет никакой априорной информации об Алисе, он не сможет отличить подделку. Поэтому, осуществление скрытой передачи данных с открытым ключом в присутствии активного нарушителя есть намного более трудная проблема, чем при наличии пассивного нарушителя. И так, представлен протокол, позволяющий

решить эту задачу. Он основан на введение в рассмотрение канала с исключительно малой пропускной способностью — надсознательного (supraliminal) канала. Этот канал образуется за счет встраивания скрываемых данных в наиболее важные признаки контейнера, искажение которых приведет к его полной деградации. Дело в том, что Вилли во многих случаях не может вносить значительные помехи в стегоканал, так чтобы передаваемая информация полностью изменялась. Не может по причинам не технического характера, а по юридическим или иным мотивам. Например, если Алиса пересылает Бобу книгу, Вилли не может подменить ее другой. Также недопустимо, например, изменение дипломатических посланий. За счет того, что скрытое сообщение зависит от контейнера, этот тип канала является робастным. По надсознательному каналу передается малый объем внешне незначимых данных. Например, это может быть сеансовый ключ.

Встраивание информации в наиболее важные свойства контейнера — основной принцип применения ЦВЗ (Цифровой водяной знак). Отличие надсознательного канала заключается в том, что для встраивания и извлечения информации в этом случае не требуется секретный ключ. Местоположение скрываемых бит общеизвестно, а вот удалить их невозможно без разрушения контейнера. Кроме того, ЦВЗ может не нести в себе никакой осмысленной информации, например, быть функцией самого изображения. В случае же надсознательного канала, наоборот, контейнер может быть функцией скрываемого короткого сообщения.

В качестве примера надсознательного канала в приведен такой сценарий. Пусть контейнером является озвученный видеоклип — речь Алисы. В целях стеганографии здесь обычно используются младшие значащие биты отсчетов клипа — то есть, фактически, шум. Принцип построения надсознательного канала иной. Предположим, что каждой букве алфавита сопоставлено некоторое числовое значение. Получив аудиоклип, Боб выбирает из него и выписывает все достаточно длинные слова, скажем,

более пяти букв. Далее для каждого слова он находит произведение числовых эквивалентов этих букв по некоторому простому модулю p. Упорядоченные значения получившихся чисел могут рассматриваться как представление некоторого целого числа по модулю p .

Задача Алисы при подготовке клипа заключается в том, чтобы должным образом составить сообщение и сохранить его осмысленность. Эта задача облегчается тем, что для скрытия сообщения используются только длинные слова, а короткими можно манипулировать произвольно. Составив текст, Алиса осуществляет аудиовидеозапись. Получившийся канал является открытым, так как сама запись, числовые значения букв известны всем. Однако канал является и замаскированным, так как любая запись может интерпретироваться, как содержащая скрытое сообщение. Канал является робастным, так как Вилли достаточно трудно заменить отдельные сообщения, имитируя голос Алисы и движения ее губ.

Как видно из приведенного примера, основная трудность заключается в формировании контейнера, тогда как работа Боба может быть легко автоматизирована. Для практического применения надсознательного канала должны быть автоматизированы обе операции. Надсознательный канал не подходит для скрытой передачи сообщений, так как он обладает малой пропускной способностью и читается Вилли [7]. Однако, он может быть использован для тайного обмена открытыми ключами, несмотря на наличие активного нарушителя.

Протокол обмена следующий:

1. Алиса генерирует пару открытого и закрытого ключей.

2. Алиса вычисляет представительное описание контейнера, соответствующее ее открытому ключу, генерирует контейнер и пересылает его Бобу.

3. Боб извлекает из принятого контейнера открытый ключ Алисы. Он генерирует секретный ключ, шифрует его с помощью открытого ключа

Алисы, находит соответствующее получившейся последовательности описание контейнера, генерирует контейнер и пересылает его Алисе.

4. Алиса и Боб теперь могут обмениваться сообщениями, встраиваемыми в контейнер с использованием этого ключа.

Вилли в результате перехвата канала может получить открытый ключ Алисы и зашифрованный этим ключом секретный ключ Боба. Не зная закрытого ключа Алисы он не сможет получить значение секретного ключа.

Обнаружение ЦВЗ с нулевым знанием

Робастные ЦВЗ могут применяться в различных приложениях, соответственно, и требования к ним могут предъявляться различные. Можно выделить следующие категории требований к робастным ЦВЗ:

1. ЦВЗ обнаруживается всеми желающими. В этом случае он служит для уведомления о собственнике защищаемого контента и для предотвращения непреднамеренного нарушения прав собственника.

2. ЦВЗ обнаруживается, по крайней мере, одной стороной. В этом случае его использование связано с поиском нелегально распространяемых копий, например, в сети Интернет.

3. ЦВЗ крайне трудно модифицировать или извлечь из контента. В этом случае ЦВЗ служит для аутентификации.

Одновременное выполнение вышеприведенных требований невозможно, так как они являются противоречивыми. Поэтому, в различных приложениях используются как системы ЦВЗ с секретным, так и с общедоступным ключом. Системы с общедоступным ключом находят гораздо большее применение, так как они могут быть использованы как для обнаружения, так и для предотвращения несанкционированного использования контента. Для того, чтобы поисковая система обнаружила ЦВЗ с секретным ключом, ей необходимо проверить каждое изображение на наличие в нем каждого из возможных ЦВЗ, что является вычислительно трудоемкой задачей. В случае же общедоступного ЦВЗ алгоритм

обнаружения единственный. Однако, общедоступные ЦВЗ обладают серьезным недостатком: так как их местоположение известно, то их можно без труда извлечь из защищаемого изображения.

Создается впечатление, что ЦВЗ с общедоступным ключом не могут быть робастными. Как только ЦВЗ начинает выполнять свои функции по защите контента, у атакующего появляется все больше информации о нем, то есть ЦВЗ становится все более «открытым». Таким образом, сама природа ЦВЗ такова, что их в любом случае можно считать общедоступными, несмотря на наличие секретного ключа. Это делает возможным создание ЦВЗ, который легко обнаруживается, но трудно удаляется. Эта система строится на основе доказательства с нулевым знанием.

Предположено, что Алиса обладает некоторой информацией и хочет доказать этот факт Бобу. При этом доказательство должно быть косвенным, то есть Боб не должен получить каких-либо новых знаний об этой информации. Такое доказательство и называется доказательством с нулевым знанием. Оно принимает форму интерактивного протокола. Боб задает Алисе ряд вопросов. Если Алиса действительно владеет некоторой информацией, то она ответит на все вопросы правильно; если же она мошенничает, то вероятность правильного угадывания мала и уменьшается с увеличением количества вопросов.

В целом базовый протокол с нулевым знанием строится следующим образом:

1. Алисе известна некоторая информация, являющаяся решением некоторой трудной проблемы. Она использует эту информацию и случайное число для превращения этой трудной проблемы в другую, изоморфную первой и получает ее решение.

2. Боб просит Алису либо доказать, что старая и новая проблемы изоморфны, либо открыть решение новой проблемы и доказать, что оно является таковым. Алиса выполняет просьбу Боба.

3. Этапы 1 и 2 повторяются n раз.

В качестве трудной проблемы выбирается обычно вычисление по однонаправленной функции. Одной из наиболее известных однонаправленных функций является дискретный логарифм. При этом общеизвестными являются: большое простое число p и порождающий элемент a. Алиса выбирает некоторое число x и публикует $M=a^2 (\mathrm{mod}\ p)$. Так как определение x на основе знания M есть вычислительно трудная задача, то знание Алисой x подтверждает ее идентичность.

Протокол строится следующим образом.

1. Алиса генерирует другое простое число y, вычисляет число $N=a^2 (\mathrm{mod}\ p)$ и посылает его Бобу. (То есть она передает Бобу изоморфную трудную задачу).

2. Боб может попросить Алису:

а) открыть y, то есть дать решение изоморфной трудной задачи;

б) открыть $y+x (\mathrm{mod}\ p-1)$, то есть логарифм произведения MN.

3. Алиса выполняет просьбу Боба, и шаги протокола повторяются при другом значении N.

Протоколы доказательства с нулевым знанием могут строиться также на основе использования свойств изоморфизма графов и других трудных задач.

Итак, в криптографии известна и решена задача доказательства существования некоторой информации без раскрытия сведений о ней. К сожалению, идея доказательства с нулевым знанием не может быть непосредственно применена для построения системы ЦВЗ, из-за специфики последней. Далее рассмотрена эта специфика и возможные модификации протокола доказательства с нулевым знанием для применения в ЦВЗ.

В рассмотренном выше протоколе Алиса имеет возможность публиковать открытое число M и различные значения N, а также a и p. В случае же системы ЦВЗ вся эта информация должна встраиваться в

изображение. Если ее сделать доступной для Боба, тот может просто удалить ее из изображения, так как это не приведет к существенному ухудшению его качества. Возможным выходом являлось бы использование надсознательного канала, то есть ЦВЗ в виде хэш-функции от наиболее значимых признаков изображения. В этом случае удаление ЦВЗ приведет к значительной деградации изображения. Однако, таким образом невозможно встраивать новую информацию, например, вычисленное значение M. По существу, надсознательный канал доступен для Алисы в режиме «только для чтения».

Рассмотрено возможную реализацию протокола с нулевым знанием в известной схеме построения системы ЦВЗ, носящей имя Питаса. В основе схемы Питаса лежит разделение всего множества пикселов на два подмножества, увеличение значений на некоторое число k в одном подмножестве и уменьшение на то же число k - в другом. Таким образом, средние значения двух подмножеств будут отличаться на $2k$.

Версия схемы Питаса для протокола с нулевым знанием строится следующим образом. После внесения ЦВЗ в контейнер Алиса выполняет перестановку π. Затем она доказывает наличие перестановки ЦВЗ $\pi(W)$ в перестановке контейнера $\pi(I_w)$ без раскрытия значения ЦВЗ W. Для исключения обмана с ее стороны Алиса должна опубликовать множество сигналов Ω таких, что их скремблированные значения дают множество всех возможных ЦВЗ.

Итак,

1.Алиса генерирует перестановку, вычисляет последовательность $\pi(I_w)$ и посылает ее Бобу.

2. Боб теперь знает, как исходный контейнер, так и его перестановку и случайным образом просит Алису:

а) открыть перестановку, чтобы убедиться что нет обмана;

б) показать наличие $\pi(W)$ в $\pi(I_w)$.

3. Алиса выполняет просьбу Боба.

4. Алиса показывает, что она не смошенничала и $\pi(W)$ действительно является перестановкой ЦВЗ. Для этого она предъявляет допустимую процедуру скремблирования σ, такую что $\sigma(\Omega) = \pi(W)$.

5. Использованная перестановка больше в протоколе не применяется.

Данный протокол порождает ряд проблем. Во-первых, даже небольшой сдвиг контейнера приведет к рассогласованию значений $\pi(W)$ и $\pi(I_w)$. В принципе, эта проблема не самого протокола. Она вызвана чувствительностью схемы Питаса к пространственным сдвигам. Другая проблема состоит в некоторой «утечке» информации о выполненной Алисой перестановке [8]. Дело в том, что значения интенсивностей пикселов при перестановке не изменяются, и атакующий будет использовать эту информацию для сужения круга возможных перестановок. Еще одна слабость протокола заключается в том, что Алиса может найти и использовать такие перестановки, что $\pi_2(W)$ будет отыскиваться в $\pi_2(I_w)$, и Боб не сможет обнаружить мошенничество.

Поэтому предложен ряд усовершенствований вышеприведенного стеганографического протокола с нулевым знанием, с использованием криптографических сильных перестановок, основанных на сложных проблемах, например, поиска путей на графах.

1.4. Методы противодействия атак на стеганографических систем

Атаки против используемого протокола

Атаки против используемого протокола показывает, что многие стегосистемы ЦВЗ чувствительны к так называемой инверсной атаке. Эта атака заключается в следующем. Нарушитель заявляет, что в защищенном изображении часть данных есть его водяной знак. После этого он создает ложный оригинал, вычитая эту часть данных. В ложном оригинале присутствует настоящий ЦВЗ. С другой стороны, в защищенном

изображении присутствует провозглашенный нарушителем ложный ЦВЗ. Наступает неразрешимая ситуация. Конечно, если у детектора имеется исходное изображение, то собственник может быть выявлен. Но, как показано в работе, далеко не всегда. Для этого он делается зависимым от изображения при помощи однонаправленной функции.

Пусть V - исходное изображение, W - водяной знак законного собственника. Тогда защищенное изображение $V_w = V + W$. Нарушитель объявляет произвольную последовательность бит W_F своим водяным знаком и вычитает ее из защищенного изображения, в результате чего получает ложный оригинал $V_F = V_w - W$. Теперь если выполняется равенство $V_F = V_F + V_F = V_w$, то цель нарушителя достигнута. ЦВЗ называется в этом случае обратимым. Невозможно определить, что является оригиналом: V или V_F и, следовательно, кто является собственником контента. Далее мы, следуя, дадим определения обратимости и необратимости систем ЦВЗ, а в пункте 2.4 рассмотрим подходы к решению проблемы прав собственника.

В работе дано два определения необратимости: ослабленное и сильное. При этом используются следующие обозначения:

- $E(V, W) = V_w$- процедура встраивания ЦВЗ;
- $D(V, V_w) = W'$ или $D(V_w) = W'$ — процедура извлечения ЦВЗ;
- α - масштабирующий коэффициент;
- C - бинарный признак подобия двух сигналов: равен 1, если коэффициент взаимной корреляции больше некоторого порога δ; в противном случае — равен 0.

Первое определение необратимости следующее.

Стегоалгоритм (E, D, C) является (строго) обратимым, если для любого V_w существует отображение E^{-1} такое, что $E^{-1}(V_w) = (V_F, W_F)$ и $E(V_F W_F) = V_w$. При этом E^{-1} вычислительно осуществимо, W_F принадлежит к классу

допустимых ЦВЗ, истинное и ложное изображения визуально сходны и $C(D(V_w, V_F), W_F, \delta) = 1$. Иначе (E,D,C) (слабо) необратим.

В этом определении требование, чтобы $E(V_F W_F) = V_w$ накладывает слишком сильное ограничение. В самом деле, даже $E(V, W) = V_w$ может не выполняться в силу различного рода искажений V_w. С другой стороны, это требование слишком слабо для определения обратимости. Поэтому, в работе оно заменено на требование, чтобы $E(V_F W_F) = V_w$, где $C(V_w, V_w, \delta) = 1$.

Второе определение необратимости следующее.

Стегоалгоритм (E,D,C) является (слабо) обратимым, если для любого V_w существует отображение E^{-1} такое, что $E^{-1}(V_w) = (V_F, W_F)$ и $E(V_F W_F) = V_w$. При этом E^{-1} вычислительно осуществимо, W_F принадлежит к классу допустимых ЦВЗ, $C(V_w, V_F, \delta) = 1$, $C(V_w, V_w, \delta) = 1$ и $C(D(V_w, V_F), W_F, \delta) = 1$. Иначе (E,D,C) (строго) необратим.

Одним из возможных сценариев, когда ее опасность существует, является следующий. Пусть пользователю разрешено сделать одну копию с оригинала, но не разрешено делать копии с копий. Записывающее устройство должно изменить ЦВЗ с «разрешена копия» на «копирование не разрешено». В этом случае атакующий имеет доступ к сообщению до и после вложения ЦВЗ. Значит, он может вычислить разность между исходным и модифицированным сообщением. Эта разность равна $f(S_0, W)$. Далее исходное изображение предыскажается: из него вычитается $f(S_0, W)$. После осуществления копирования будет записано $S_0 - f(S_0, W) + f(S_0 - f(S_0, W), W$, что очень близко к исходному изображению S_0. Эта близость объясняется тем, что ЦВЗ должны быть робастны к добавлению аддитивного шума. Следовательно, $f(S_0 + \varepsilon, W) \approx f(S_0 W)$. В случае данной атаки в качестве шума выступает стегосообщение и $f(S_0 - f(S_0, W), W \approx f(S_0 W)$.

В ряде случаев гораздо проще не удалять ЦВЗ, а помешать его использованию по назначению. Например, возможно внедрение

дополнительных ЦВЗ так, что становится неясно, какой из них идентифицирует истинного собственника контента.

Другой известной атакой на протокол использования ЦВЗ является атака копирования. Эта атака заключается в оценивании ЦВЗ в защищенном изображении и внедрении оцененного ЦВЗ в другие изображения. Целью может являться, например, противодействие системе имитозащиты или аутентификации.

Одна из слабостей стегосистемы, применяемой для защиты от копирования, является то, что детектор способен обнаружить ЦВЗ только когда видеосигнал визуально приемлем. Однако можно подвергнуть сигнал скремблированию, получить шумоподобный сигнал, затем без помех незаконно скопировать его. В видеоплейер в этом случае встраивается дескремблер, который и восстанавливает незаконно сделанную копию. Аппаратная реализация скремблера и дескремблера весьма проста и иногда используется для защиты, например, программ кабельного телевидения. Возможной защитой против такого подхода является разрешения копирования только определенного формата данных.

Методы противодействия атакам на системы ЦВЗ

В простейших стегосистемах ЦВЗ при встраивании используется псевдослучайная последовательность, являющаяся реализацией белого гауссовского шума и не учитывающая свойства контейнера. Такие системы практически неустойчивы к большинству рассмотренных выше атак. Для повышения робастности стегосистем можно предложить ряд улучшений.

В робастной стегосистеме необходим правильный выбор параметров псевдослучайной последовательности. Известно, что при этом системы с расширением спектра могут быть весьма робастными по отношению к атакам типа добавления шума, сжатия и т. п. Так считается, что ЦВЗ должен обнаруживаться при достаточно сильной низкочастотной фильтрации (7x7 фильтр с прямоугольной характеристикой). Следовательно, база сигнала

должна быть велика, что снижает пропускную способность стегоканала. Кроме того, используемая в качестве ключа ПСП должна быть криптографически безопасной.

Атака «сговора» и возможные методы защиты от нее рассмотрена в работе. Причиной нестойкости систем ЦВЗ с расширением спектра к подобным атакам объясняется тем, что используемая для вложения последовательность обычно имеет нулевое среднее. После усреднения по достаточно большому количеству реализаций ЦВЗ удаляется [9]. Известен специальный метод построения водяного знака, направленный против подобной атаки. При этом коды разрабатываются таким образом, чтобы при любом усреднении всегда оставалась не равная нулю часть последовательности (статическая компонента). Более того, по ней возможно восстановление остальной части последовательности (динамическая компонента). Недостатком предложенных кодов является то, что их длина увеличивается экспоненциально с ростом числа распространяемых защищенных копий. Возможным выходом из этого положения является применение иерархического кодирования, то есть назначения кодов для группы пользователей. Некоторые аналогии здесь имеются с системами сотовой связи с кодовым разделением пользователей (CDMA).

Различные методы противодействия предлагались для решения проблемы прав собственности. Первый способ заключается в построении необратимого алгоритма ЦВЗ. ЦВЗ должен быть адаптивным к сигналу и встраиваться при помощи однонаправленной функции, например, хэш-функции. Хэш-функция преобразует 1000 бит исходного изображения V в битовую последовательность b_i, $i = \overline{1 \dots 100}$. Далее, в зависимости от значения b_i используется две функции встраивания ЦВЗ. Если $b_i = 0$, то используется функция $v_i(1 + \alpha w)$, если $b_i = 1$, то функция $V_i(1 - \alpha w_i)$, где v_i - i-й коэффициент изображения, v_i - i-й бит встраиваемого сообщения. Предполагается, что такой алгоритм формирования ЦВЗ предотвратит

фальсификацию. На примере показано, что для того, чтобы данный алгоритм был необратимым, все элементы w_i должны быть положительными.

Второй способ решения проблемы прав собственности заключается во встраивании в ЦВЗ некоторой временной отметки, предоставляемой третьей, доверенной стороной. В случае возникновения конфликта лицо, имеющее на изображении более раннюю временную отметку, считается настоящим собственником.

Один из принципов построения робастного ЦВЗ заключается в адаптации его спектра. В ряде работ показано, что огибающая спектра идеального ЦВЗ должна повторять огибающую спектра контейнера. Спектральная плотность мощности ЦВЗ, конечно же, намного меньше. При такой огибающей спектра винеровский фильтр дает наихудшую оценку ЦВЗ из возможных: дисперсия значений ошибки достигает дисперсии значений заполненного контейнера. На практике адаптация спектра ЦВЗ возможна путем локального оценивания спектра контейнера. С другой стороны, методы встраивания ЦВЗ в области преобразования достигают этой цели за счет адаптации в области трансформанты.

Для защиты от атак типа аффинного преобразования можно использовать дополнительный (опорный) ЦВЗ. Этот ЦВЗ не несет в себе информации, но используется для «регистрации» выполняемых нарушителем преобразований. В детекторе ЦВЗ имеется схема предыскажения, выполняющая обратное преобразование. Здесь имеется аналогия с используемыми в связи тестовыми последовательностями. Однако, в этом случае атака может быть направлена именно против опорного ЦВЗ. Другой альтернативой является вложение ЦВЗ в визуально значимые области изображения, которые не могут быть удалены из него без существенной его деградации. Наконец, можно разместить стего в инвариантных к преобразованию коэффициентах. Например, амплитуда преобразования Фурье инвариантна к сдвигу изображения (при этом меняется только фаза).

Другим методом защиты от подобных атак является блочный детектор. Модифицированное изображение разбивается на блоки размером 12x12 или 16x16 пикселов, и для каждого блока анализируются все возможные искажения. То есть пикселы в блоке подвергаются поворотам, перестановкам и т.п. Для каждого изменения определяется коэффициент корреляции ЦВЗ. Преобразование, после которого коэффициент корреляции оказался наибольшим, считается реально выполненным нарушителем. Таким образом появляется возможность как бы обратить внесенные нарушителем искажения. Возможность такого подхода основана на предположении о том, что нарушитель не будет значительно искажать контейнер (это не в его интересах).

2. ОСНОВНАЯ ЧАСТЬ. АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ

2.1. Построение математической модели стеганографии в изображениях

Стеганография может быть рассмотрена как система связи. Алгоритм встраивания стеганографических алгоритмов защиты информации состоит из трех основных этапов: 1) генерации ЦВЗ, 2) встраивания ЦВЗ в кодере и 3) обнаружения ЦВЗ в детекторе.

1) Пусть $W*, K*, I*, B*$ есть множества возможных ЦВЗ, ключей, контейнеров и скрываемых сообщений, соответственно. Тогда генерация ЦВЗ может быть представлена в виде

$$F: I* \times K* \times B \rightarrow W*, \; W = F(I, K, B), \quad (2.1)$$

где W, K, I, B - представители соответствующих множеств. Вообще говоря, функция F может быть произвольной, но на практике требования робастности ЦВЗ накладывают на нее определенные ограничения. Так, в большинстве случаев, $F(I, K, B) \approx F(I + \varepsilon, K, B)$, то есть незначительно измененный контейнер не приводит к изменению ЦВЗ. Функция F обычно является составной:

$$F = T \circ G, \text{ где } G: K* \times B* \rightarrow C*, \text{ и } T: C* \times I* \rightarrow W*, \quad (2.2)$$

то есть ЦВЗ зависит от свойств контейнера. Функция G может быть реализована при помощи криптографической безопасного генератора ПСП (псевдослучайная последовательность) с Kв качестве начального значения.

Для повышения робастности ЦВЗ могут применяться помехоустойчивые коды, например, коды БЧХ, сверточные коды. В ряде публикаций отмечены хорошие результаты, достигаемые при встраивании ЦВЗ в области вейвлет-преобразования с использованием турбо-кодов. Отсчеты ЦВЗ принимают обычно значения из множества {-1,1}, при этом для отображения {0,1}→{-1,1} может применяться двоичная относительная фазовая модуляция (BPSK).

Оператор T модифицирует кодовые слова C^*, в результате чего получается ЦВЗ W^*. На эту функцию можно не накладывать ограничения необратимости, так как соответствующий выбор G уже гарантирует необратимость F. Функция T должна быть выбрана так, чтобы незаполненный контейнер I_0, заполненный контейнер I_W и незначительно модифицированный заполненный контейнер F_W порождали бы один и тот же ЦВЗ:

2) Процесс встраивания ЦВЗ $W(i,j)$ в исходное изображение $I(i,j)$ может быть описан как суперпозиция двух сигналов:

$$\varepsilon: I * \times W * \times L * \rightarrow I_W *, \; I_W(i,j) = I_0 \oplus L(i,j)W(i,j)p(i,j), \quad (2.3)$$

где $L(i,j)$ — маска встраивания ЦВЗ, учитывающая характеристики зрительной системы человека, служит для уменьшения заметности ЦВЗ;

$p(i,j)$— проектирующая функция, зависящая от ключа;

знаком $\oplus$ обозначен оператор суперпозиции, включающий в себя, помимо сложения, усечение и квантование [10].

Проектирующая функция осуществляет «распределение» ЦВЗ по области изображения. Ее использование может рассматриваться, как реализация разнесения информации по параллельным каналам. Кроме того, эта функция имеет определенную пространственную структуру и корреляционные свойства, использующиеся для противодействия геометрическим атакам.

Другое возможное описание процесса внедрения получено, представив стегосистему как систему связи с передачей дополнительной информации (рис.2.1). В этой модели кодер и декодер имеют доступ, помимо ключа, к информации о канале (то есть о контейнере и о возможных атаках). В зависимости от положения переключателей А и Б выделяют четыре класса стегосистем (подразумевается, что ключ всегда известен кодеру и декодеру).

I класс: дополнительная информация отсутствует (переключатели разомкнуты) - «классические» стег системы. Обнаружение ЦВЗ

осуществлялось путем вычисления коэффициента корреляции между принятым стега и вычисленным по ключу ЦВЗ. Если коэффициент превышал некоторый порог, выносилось решение о присутствии ЦВЗ. Известно, что корреляционный приемник оптимален лишь в случае аддитивной гауссовой помехи. При других атаках (например, геометрических искажениях) эти стегосистемы показывали удручающие результаты.

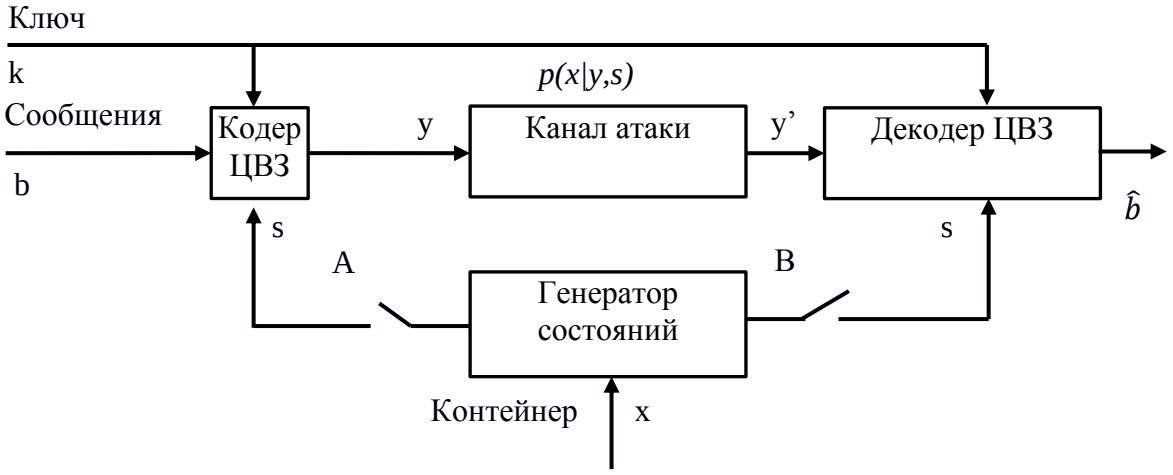


Рис.2.1 Представление стегосистемы, как системы связи с передачей дополнительной информации

II класс: информация о канале известна только кодеру (А замкнут, Б разомкнут). Интересной особенностью схемы является то, что, будучи слепой, она имеет ту же теоретическую пропускную способность, что и схема с наличием исходного контейнера в декодере. К недостаткам стегосистем II класса можно отнести высокую сложность кодера (необходимость построения кодовой книги для каждого изображения), а также отсутствие адаптации схемы к возможным атакам. В последнее время предложен ряд практических подходов, преодолевающих эти недостатки. В частности, для снижения сложности кодера предлагается использовать структурированные кодовые книги, а декодер рассчитывать на случай наихудшей атаки [11].

III класс: дополнительная информация известна только декодеру (А разомкнут, Б замкнут). В этих схемах декодер строится с учетом возможных

атак. В результате получаются робастные к геометрическим атакам системы. Одним из методов достижения этой цели является использование так называемой опорного ЦВЗ (аналог пилот-сигнала в радиосвязи). Опорный ЦВЗ — небольшое число бит, внедряемые в инвариантные к преобразованиям коэффициенты сигнала. Например, можно выполнить встраивание в амплитудные коэффициенты преобразования Фурье, которые инвариатны к аффинным преобразованиям. Тогда опорный ЦВЗ «покажет», какое преобразование выполнил со стего атакующий. Другим назначением пилотного ЦВЗ является борьба с замираниями, по аналогии с радиосвязью. Замираниями в данном случае можно считать изменение значений отсчетов сигнала при встраивании данных, атаках, добавлении негауссовского шума и т. д. В радиосвязи для борьбы с замираниями используется метод разнесенного приема (по частоте, времени, пространству, коду). В стеганографии же используется разнесение ЦВЗ по пространству контейнера. Пилотный ЦВЗ генерируется в декодере на основе ключа.

IV класс: дополнительная информация известна и в кодере и в декодере (оба ключа замкнуты). Как отмечено в, по всей видимости все перспективные стегосистемы должны строиться по этому принципу. Оптимальность этой схемы достигается путем оптимального согласования кодера с сигналом-контейнером, а также адаптивным управлением декодером в условиях наблюдения канала атак.

3) Также как в радиосвязи наиболее важным устройством является приемник, в стегосистеме главным является стегодетектор. В зависимости от типа он может выдавать двоичные либо *M*-ичные решения о наличии/отсутствии ЦВЗ (в случае детектора с мягкими решениями). Обозначим операцию детектирования через *D*. Тогда

$$D: I_W \ast\times K \ast\rightarrow \{0,1\},\ D(I_w, W) = D\big(I_w, F(I_w, K)\big) = \begin{Bmatrix} 1, & \text{если } W \text{ есть} \\ 0, & \text{если } W \text{ есть} \end{Bmatrix}. \quad (2{,}4)$$

В качестве детектора ЦВЗ обычно используют корреляционный приемник, изображенный на рис.2.2.

Пусть у половины пикселов изображения значение яркости увеличено на 1, а у остальных — осталось неизменным, либо уменьшено на 1. Тогда $I_w = I_0 + W$, где $F(I_0 K) = W$. Коррелятор детектора ЦВЗ вычисляет величину $I_w \cdot W = (I_0 + W) \cdot W = I_0 \cdot W + W \cdot W$. Так как W может принимать значения ±1, то $I_0 \cdot W$ будет весьма мало, а $W \cdot W$ будет всегда положительно. Поэтому $I_w \cdot W$ будет очень близко к $W \cdot W$. Тогда можно воспользоваться результатами теории связи и записать вероятность неверного обнаружения стего, как дополнительную (комплементарную) функцию ошибок от корня квадратного из отношения к $W \cdot W$ («энергии сигнала») к дисперсии значений пикселов яркости («энергия шума»).

Для случая мягкого детектора и закрытой стегосистемы имеем две основные меры похожести:

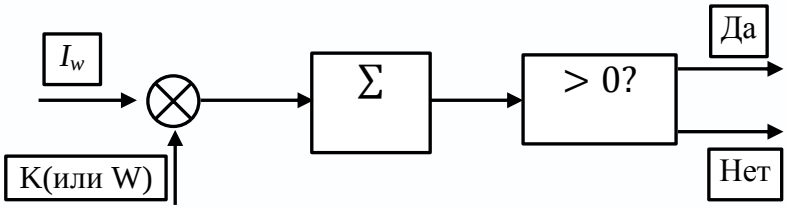


Рис.2.2 Корреляционный детектор ЦВЗ

$$\delta = \frac{I_0 I_w}{\|I_0\| \|I_w\|} \qquad (2.5)$$

нормированный коэффициент взаимной корреляции и

$$\delta = N - \sum_{i=j}^{n} i_0 i_w \quad (2.6)$$

расстояние по Хэммингу.

В детекторе возможно возникновение двух типов ошибок. Существует вероятность того, что детектор не обнаружит имеющийся ЦВЗ и вероятность ложного нахождения ЦВЗ в пустом контейнере (вероятность ложной тревоги). Снижение одной вероятности приводит к увеличению другой. Надежность работы детектора характеризуют вероятностью ложного

обнаружения. Система ЦВЗ должна быть построена таким образом, чтобы минимизировать вероятности возникновения обеих ошибок, так как каждая из них может привести к отказу от обслуживания.

2.2. Скрытие данных в неподвижных изображениях

Большинство исследований посвящено использованию в качестве стеганоконтейнеров именно изображений. Это обусловлено следующими причинами:

- существованием практической необходимости защиты цифровых фотографий, изображений, видео от противозаконного тиражирования и распространения;
- относительно большим объемом цифрового представления изображений, что позволяет встраивать ЦВЗ значительного объема или же повышать устойчивость этого встраивания;
- заранее известным (фиксированным) размером контейнера, отсутствием ограничений, которые накладываются требованиями скрытия в реальном времени;
- наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и наилучшим образом подходящих для встраивания информации;
- слабой чувствительностью человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, содержания в нем шума, искажений вблизи контуров;
- наконец, хорошо разработанными в последнее время методами цифровой обработки изображений.

Однако, как указывается последняя причина вызывает и значительные трудности в обеспечении стойкости ЦВЗ: чем более совершенными

становятся методы компрессии, тем меньше остается возможностей для встраивания посторонней информации [8].

Развитие теории и практики алгоритмов компрессии изображений привело к изменению представлений о технике встраивания ЦВЗ. Если сначала предлагалось встраивать информацию в незначащие биты для уменьшения визуальной заметности, то современный подход, наоборот, заключается во встраивании ЦВЗ в наиболее существенные области изображений, разрушение которых будет приводить к полис деградации самого изображения. Поэтому абсолютно понятна необходимость учета стеганоалгоритмами не только алгоритмов компрессии изображений, но и свойств зрительном системы человека (ЗСЧ).

Основные свойства ЗСЧ, которые необходимо учитывать при построении стеганоалгоритмов

Свойства ЗСЧ можно разделить на две группы: низкоуровневые ("физиологические") и высокоуровневые ("психофизиологические"). Почти до середины 1990-х г.г. исследователи принимали во внимание, главным образом, низкоуровневые свойства зрения. В последние годы обозначилась тенденция построения стеганоалгоритмов с учетом и высокоуровневых характеристик ЗСЧ.

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

- чувствительность к изменению яркости (контрастности) изображения;
- частотная чувствительность;
- эффект маскировки.

На рис.2.3 изображена зависимость минимального контраста $\Delta I/I$от яркости I.

Как видно, для среднего диапазона изменения яркости, контраст приблизительно постоянен, тогда как для малых и больших яркостей

значение порога неразличимости (ΔI) возрастает. Установлено, что $\Delta I \approx (0.01 \div 0.03) \cdot I$ для средних значений яркости.

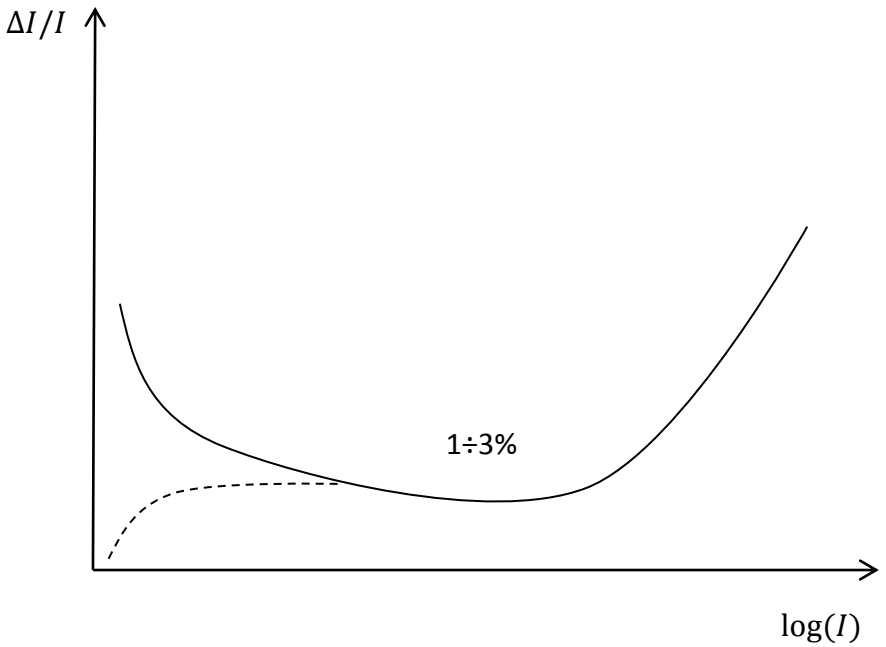


Рис.2.3 Чувствительность к изменению контраста и порог неразличимости ΔI

Кроме того, отмечено, что результаты новейших исследований противоречат “классической” теории и показывают что при малых значениях яркости порог неразличимости уменьшается, то есть ЗСЧ более чувствительна к шуму в этом диапазоне.

Частотная чувствительность ЗСЧ проявляется в том, что человек намного более восприимчив к низкочастотному (НЧ), чем к высокочастотному (ВЧ) шуму. Это связано с неравномерностью амплитудно-частотной характеристики ЗСЧ.

Элементы ЗСЧ разделяют поступающий видеосигнал, на отдельные составляющие, каждая из которых возбуждает нервные окончания глаза через ряд подканалов. Выделяемые глазом составляющие имеют разные пространственные и частотные характеристики, а также различную пространственную ориентацию (горизонтальную, вертикальную, диагональную).

В случае одновременного влияния на глаз двух составляющих с похожими характеристиками возбуждаются одни и те же подканалы. Это приводит к *эффекту маскировки***,** который заключается в увеличении порога обнаружения зрительного сигнала в присутствии другого сигнала, имеющего аналогичные характеристики. Поэтому, аддитивный шум намного заметней на НЧ (однотонных) участках изображения по сравнению с ВЧ участками, то есть, в последнем случае наблюдается маскировка. Наиболее сильно данный эффект проявляется, когда оба сигнала имеют одинаковую ориентацию и место расположения.

Частотная чувствительность тесно связана с яркостью. Известно также и выражение для определения порога маскировки на основе известной яркостной чувствительности, что позволяет найти метрику искажения изображения, которая учитывала бы свойства ЗСЧ. Математические модели такого типа хорошо разработаны для случая квантования коэффициентов дискретного косинусного преобразования, поскольку именно оно применяется в стандарте JPEG.

Эффект маскировки в пространственной области может быть объяснен путем построения стохастических моделей изображения. При этом изображение представляется в виде марковского случайного поля, распределение вероятностей которого описывается, например, обобщенным законом Гаусса.

Перечислим основные из этих свойств:

- чувствительность к контрасту — высококонтрастные участки изображения и перепады яркости обращают на себя больше внимания;
- чувствительность к размеру — большие участки изображения более "заметны" по сравнению с меньшими по размеру, причем существует порог насыщенности, когда дальнейшее увеличение размера не играет роли;
- чувствительность к форме — длинные и тонкие объекты вызывают больше внимания, чем закругленные и однородные;

- чувствительность к цветам — некоторые цвета (например красный) более "заметны", чем другие; этот эффект усиливается, если фон заднего плана отличается от цветов фигур на нем;
- чувствительность к месту размещения — человек склонен в первую очередь рассматривать центр изображения; также внимательней рассматриваются фигуры переднего плана, чем заднего;
- чувствительность *к* внешним раздражителям — движение глаз наблюдателей зависит от конкретной обстановки, от полученных ими перед просмотром или во время его инструкций, дополнительной информации.

В последнее время создано достаточное количество методов скрытия данных в цифровых изображениях, что позволяет провести их классификацию и выделить следующие обобщенные группы:

- методы замены в пространственной области;
- методы скрытия в частотной области изображения;
- широкополосные методы;
- статистические (стохастические) методы;
- метод блочного сокрытия
- метод расширения палитры;
- методы в GIF изображениях;
- методы искажения;
- структурные методы.

2.3. Применение стеганографических методов в изображениях

Скрытие данных в пространственной области

Алгоритмы, описанные в данном подразделе, встраивают скрываемые данные в области первичного изображения. Их преимущество заключается в том, что для встраивания нет необходимости выполнять вычислительно сложные и длительные преобразования изображении.

Цветное изображение C будем представлять через дискретную функцию, которая определяет вектор цвета $c(x,y)$ для каждого пикселя изображения (x,y), где значение цвета задает трехкомпонентный вектор в цветовом пространстве Наиболее распространенный способ передачи цвета — это модель RGB, в которой основные цвета — красный, зеленый и синий, а любой другой цвет может быть представлен в виде взвешенной сумы основных цветов.

Вектор цвета $c(x,y)$ в RGB-пространстве представляет интенсивность основных цветов. Сообщения встраиваются за счет манипуляций цветовыми составляющими $\{R(x,y),\ G(x,y),B(x,y)\}$ или непосредственно яркостью $\lambda(\mathrm{x},\mathrm{y}) \in \{0,1,2,..,\mathrm{L_C}\}$.

Общий принцип этих методов заключается в замене избыточной, малозначимой части изображения битами секретного сообщения. Для извлечения сообщения необходимо знать алгоритм, по которому размещалась по контейнеру скрытая информация.

Метод замены

Популярность метода НЗБ обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах довольно большие объемы информации. Данный метод обычно работает с растровыми изображениями, которые представлены в формате без сжатия (например, GIF и BMP). Основным его недостатком является сильная чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто применяют помехоустойчивое кодирование [12].

Суть метода НЗБ заключается в замене наименее значащих битов пикселей изображения битами секретного сообщения. В простейшем случае проводится замена НЗБ всех последовательно расположенных пикселей изображения. Однако, так как длина секретного сообщения обычно меньше количества пикселей изображения, то после его внедрения в контейнере будут присутствовать две области с различными статистическими

свойствами (область, в которой незначащие биты были изменены, и область, в которой они не менялись). Это может быть легко обнаружено с помощью статистических тестов. Для создания эквивалентного изменения вероятности всего контейнера секретное сообщение обычно дополняют случайными битами так, чтобы его длина в битах была равна количеству пикселей в исходном изображении.

Другой подход, метод случайного интервала, заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Эта методика наиболее эффективна при использовании потоковых контейнеров (видео).

Для контейнеров произвольного доступа (изображений) может использоваться метод псевдослучайной перестановки.

Его суть заключается в том, что генератор псевдослучайных чисел производит последовательность индексов j1, ..., jl(m) и сохраняет k-й бит сообщения в пикселе с индексом jk. Однако в этом случае один индекс может появиться в последовательности более одного раза, т.е. может произойти “пересечение” — искажение уже встроенного бита. Если число битов сообщения намного меньше размера изображения, то вероятность пересечения незначительна, и поврежденные биты могут быть восстановлены с помощью корректирующих кодов. Вероятность, по крайней мере, одного пересечения оценивается как

$$p \sim 1 - \exp\left(-\frac{l(m)[l(m)-1]}{2l(c)}\right),$$ при условии, что $l(m) << l(c)$.

При увеличении l(m) и l(c)=const данная вероятность стремится к единице. Для предотвращения пересечений необходимо сохранять все индексы использованных элементов ji и перед сокрытием нового пикселя проводить проверку его на повторяемость.

Метод блочного сокрытия

Еще один подход в реализации метода замены (метод блочного сокрытия) состоит в следующем. Исходное изображение-контейнер разбивается на l(m) непересекающихся блоков Ii произвольной конфигурации и для каждого из них вычисляется бит четности p(Ii):

$$p(I) = \sum_{j \in I} НЗБ(cj) \bmod 2$$

В каждом блоке проводится сокрытие одного секретного бита mi. Если бит четности p(Ii) блока Ii не совпадает с секретным битом mi, то происходит инвертирование одного из НЗБ блока Ii, в результате чего p(Ii) = mi. Выбор блока может производиться случайно с использованием стегоключа. Хотя этот метод обладает такой же устойчивостью к искажениям, как и все предыдущие, он имеет ряд преимуществ. Прежде всего, имеется возможность изменять значения такого пикселя в блоке, для которого статистика контейнера изменится минимально. Кроме того, влияние последствий встраивания секретных данных в контейнер можно уменьшить за счет увеличения размера блока.

Метод расширения палитры

Для сокрытия данных можно также воспользоваться палитрой цветов, которая присутствует в формате изображения.

Палитра из N цветов определяется как список пар индексов (i, ci), который определяет соответствие между индексом i и его вектором цветности ci. В изображении каждому пикселю присваивается индекс в палитре. Так как цвета в палитре не всегда упорядочены, то скрываемую информацию можно кодировать последовательностью хранения цветов в палитре. Существует N! различных способов перестановки N-цветной палитры, что вполне достаточно для сокрытия небольшого сообщения. Однако методы сокрытия, в основе которых лежит порядок формирования палитры, также неустойчивы: любая атака, связанная с изменениями палитры, уничтожает секретное сообщение.

Зачастую соседние цвета в палитре не обязательно являются схожими, поэтому некоторые стеганометоды перед сокрытием данных проводят упорядочивание палитры так, что смежные цвета становятся подобными. Например, значения цвета может быть упорядочено по расстоянию d в RGB-пространстве, где $d = \sqrt{R2 + G2 + B2}$. Так как орган зрения человека более чувствителен к изменениям яркости цвета, то намного лучше сортировать содержимое палитры по значениям яркости сигнала. После сортировки палитры можно изменять НЗБ индексов цвета без особого искажения изображения.

Некоторые стеганометоды предусматривают уменьшение общего количества значений цветов (до N/2) путем “размывания” изображения. При этом элементы палитры дублируются так, чтобы значения цветов для них различались незначительно. В итоге каждое значение цвета размытого изображения соответствует двум элементам палитры, которые выбираются в соответствии с битом секретного сообщения.

Применение методов в GIF изображениях

Файлы формата GIF имеют блочную структуру. Данные блоки всегда имеют фиксированную длину (либо она зависит от некоторых флагов), так что ошибиться в том, где какой блок находится, практически невозможно. Структура простейшего неанимированного GIF-изображения формата GIF89a (рис.2.4):

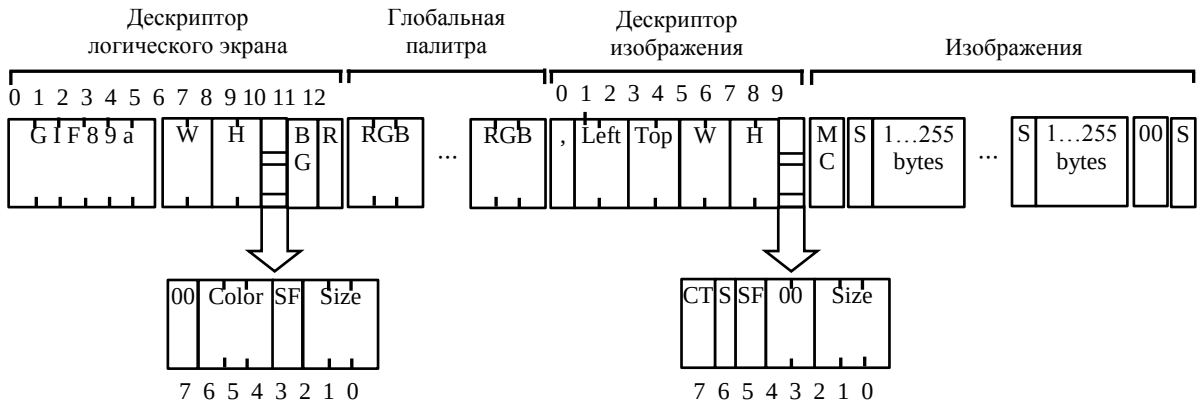


Рис.2.4 Структура простейшего не анимированного GIF-изображения формата GIF89a

Из всех блоков структуры в данном случае нас будут интересовать блок глобальной палитры и параметры, отвечающие за палитру:

CT — наличие глобальной палитры. Если этот флаг установлен, то сразу после дескриптора логического экрана должна начинаться глобальная палитра.

Size — размер палитры и число цветов картинки.

В программе будут использоваться в рамках метода LSB два последних бита в байтах глобальной палитры. Это означает, что для 24-битного изображения, где цвет палитры представляет собой три байта для красного, синего, и зеленого цветов, после внедрения сообщения в него, каждая составляющая цвета изменится максимум на 3/255 градации. Такое изменение, во-первых, будет незаметно или трудно заметно для человеческого глаза, а во-вторых, не будет различимо на низкокачественных устройствах вывода информации.

Количество информации будет напрямую зависеть от размера палитры изображения. Поскольку максимальный размер палитры 256 цветов и, если записывать по два бита сообщения в составляющую каждого цвета, то максимальная длина сообщения (при максимальной палитре в изображении) составляет 192 байта. После внедрения сообщения в изображение, размер файла не изменяется.

Метод расширения палитры, работающий только для структуры GIF. Он будет наиболее эффективен в изображениях с палитрой небольших размеров. Суть его состоит в том, что он увеличивает размер палитры, тем самым дав дополнительное пространство для записи необходимых байт на месте байт цветов. Если учесть что минимальный размер палитры составляет 2 цвета (6 байт), то максимальный размер внедряемого сообщения может быть 256Ч3–6=762 байт. Недостаток — низкая криптозащищенность, прочесть внедренное сообщение можно при помощи любого текстового редактора, если сообщение не подвергалось дополнительному шифрованию.

2.4. Анализ аддитивных алгоритмов на основе линейного встраивания данных и слияния ЦВЗ в изображениях

По способу встраивания информации стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а ее извлечение в декодере производится корреляционными методами. При этом ЦВЗ обычно складывается с изображением-контейнером, либо «вплавляется» (fusion) в него. В нелинейных методах встраивания информации используется скалярное либо векторное квантование. Среди других методов определенный интерес представляют методы, использующие идеи фрактального кодирования изображений.

Аддитивные алгоритмы

В аддитивных методах внедрения ЦВЗ представляет собой последовательность чисел w_i длины N, которая внедряется в выбранное подмножество отсчетов исходного изображения f. Основное и наиболее часто используемое выражение для встраивания информации в этом случае

$$f'(m,n) = f(m,n)(1 + \alpha w_i) \quad (2.1)$$

где α - весовой коэффициент, а f' - модифицированный пиксел изображения.

Другой способ встраивания водяного знака был предложен И.Коксом:

$$f'(m,n) = f(m,n) + \alpha w_i \quad (2.2)$$

или, при использовании логарифмов коэффициентов

$$f'(m,n) = f(m,n)e^{\alpha w_i} \quad (2.3)$$

При встраивании в соответствии с (6.1) ЦВЗ в декодере находится следующим образом:

$$w_i' = \frac{f'(m,n) - f(m,)}{\alpha f(m,n)}. \quad (2.4)$$

Здесь под $f*$ понимаются отсчеты полученного изображения, содержащего или не содержащего ЦВЗ w. После извлечения w_i сравнивается с подлинным ЦВЗ. При чем в качестве меры идентичности водяных знаков используется значение коэффициента корреляции последовательностей

$$\delta = \frac{w \cdot w}{\|w\| \cdot \|w\|}. \qquad (2.5)$$

Эта величина варьируется в интервале. Значения, близкие к единице, свидетельствуют о том, что извлеченная последовательность с большой вероятностью может соответствовать встроенному ЦВЗ. Следовательно, в этом случае делается заключение, что анализируемое изображение содержит водяной знак.

В декодере может быть установлен некоторый порог,

$$r = \frac{\alpha}{SN} \sum |f'|$$

(здесь S — стандартное среднее квадратическое отклонение), который определяет вероятности ошибок первого и второго рода при обнаружении ЦВЗ. При этом коэффициент α может не быть постоянным, а адаптивно изменяться в соответствии с локальными свойствами исходного изображения. Это позволяет сделать водяной знак более робастным (стойким к удалению).

Обычно легче первоначально сгенерировать равномерно распределенную последовательность. Известен алгоритм преобразования такой последовательности в гауссовскую (алгоритм Бокса-Мюллера). Псевдокод этого алгоритма приведен ниже. Здесь ranf() — датчик равномерно распределенных случайных чисел, mean, deviation — среднее значение и СКО последовательности.

Алгоритм 6.1. Полярная форма алгоритма Бокса-Мюллера

```
double x1, x2, w;
do {
 x1 = 2.0 * ranf() — 1.0;
```

```
x2 = 2.0 * ranf() — 1.0;
w = x1 * x1 + x2 * x2;
} while (w >= 1.0);
w = sqrt((-2.0 * log(w)) / w);
double y1 = mean + x1 * w * deviation;
double y2 = mean + x2 * w * deviation;
```

Для извлечения внедренной информации в аддитивной схеме встраивания ЦВЗ обычно необходимо иметь исходное изображение, что достаточно сильно ограничивает область применения подобных методов [5].

Рядом авторов были предложены слепые методы извлечения ЦВЗ, вычисляющие корреляцию последовательности *w* со семи *N* коэффициентами полученного изображения $f*$:

$$\delta = \frac{\sum_n f(m,n)\cdot w_i}{N}. \qquad (2.6)$$

Затем полученное значение коэффициента корреляции δ сравнивается с некоторым порогом обнаружения τ,

$$r = \frac{\alpha}{3N}\sum_N |f(m,n)\cdot|. \qquad (2.7)$$

Основным недостатком этого метода является то, что само изображение в этом случае рассматривается, как шумовой сигнал. Существует гибридный подход (полуслепые схемы), когда часть информации об исходном изображении доступно в ходе извлечения информации, но неизвестно собственно исходное изображение.

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

Наиболее ярким представителем алгоритмов внедрения ЦВЗ на основе использования широкополосных сигналов является алгоритм Кокса, представленный ниже.

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

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

Встраивание информации выполняется в соответствии с выражением (2.2), а извлечение ЦВЗ в соответствии с выражением (2.4).

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

Кроме того, операция вычисления двумерного ДКП трудоемка.

ЦВЗ представляет собой последовательность бинарных псевдослучайных чисел $w_i \in \{-1,1\}$. Длина последовательности определяется размерами исходного изображения M и N, где

$i = 0,\ldots,3 \times {}^{M}/_{2} \times {}^{M}/_{2} - 1.$

При встраивании информации вначале выполняется четырехуровневое ($l = 4$) вейвлет-преобразование с использованием фильтров Добеши-6. Для внедрения водяного знака используются только детальные поддиапазоны первого подуровня разложения. При этом в качестве кандидатов для модификации выбираются все коэффициенты детальных поддиапазонов (LH, HL, HH), которые изменяются с учетом локальной чувствительности к шумам:

$$f'(m,n) = f(m,n) = \alpha\beta(m,n)w_i, \qquad (2.8)$$

где $\beta(m,n) = \theta(l,\sigma) \times A(l,m,n) \times \equiv (l,m,n)$.

Множитель $\theta(l,\sigma)$ в этом выражении определяется поддиапазоном и уровнем разрешения:

$$\theta(l,\sigma) = \left\{ \begin{matrix} \sqrt{2},\ \sigma \in HH \\ 1,\ \sigma \notin HH \end{matrix} \times \left\{ \begin{matrix} 1.00 & l = 1 \\ 0.32 & l = 2 \\ 0.16 & l = 3 \\ 0.10 & l = 4 \end{matrix} \right\} \right\}, \qquad (2.9)$$

второй множитель определяется локальной яркостью:

$$A(l,m,n) = \frac{1}{256} f_4''(\frac{m}{2^{4l}} \times \frac{n}{2^{4l}}), \quad (2.10)$$

и последний множитель $\equiv (l,m,n)$ определяется локальной дисперсией или степенью текстурированности.

В детекторе водяной знак обнаруживается при непосредственном вычислении значения корреляции w_i с коэффициентами вейвлет-преобразования (ВП). Таким образом, возможно обнаружение ЦВЗ вслепую, без знания исходного изображения.

Каждое бинарное значение водяного знака предварительно домножается на весовой коэффициент, полученный на основе модели чувствительности человеческого зрения к шуму. Это позволяет добиться незаметности ЦВЗ

ЦВЗ представляет собой массив псевдослучайных чисел, распределенных по гауссовскому закону, размером 32*32 = 1024 числа.

Исходное изображение подвергается вейвлет-преобразованию для того, чтобы получить низкочастотное изображение размером 32*32.

Для внедрения ЦВЗ отбираются все коэффициенты *LL* поддиапазона.

Встраивание информации в эти коэффициенты выполняется в соотвествии с выражением

$$f^l(m,n) = f_{m\varepsilon an} + (f(m,n) - f_{m\varepsilon an})(1 + \sigma w_i), \quad (2.11)$$

где $f_{m\varepsilon an}$ — среднее значение выборки коэффициентов.

Извлечение информации выполняется по (2.4).

Множество коэффициентов ВП разбивается по секретному ключу на два подмножества. Коэффициенты одного подмножества увеличиваются на некоторую величину *к*, коэффициенты другого подмножества на это же значение уменьшаются. Таким образом, средние значения по каждому из подмножеств в ходе работы алгоритма разносятся. Чтобы определить наличие/отсутствие водяного знака получатель снова поэтому же секретному

ключу разбивает множество коэффициентов на два подмножества и проверяет различаются ли их средние значения приблизительно на два *к*.

ЦВЗ представляет собой последовательность псевдослучайных действительных чисел, распределенных по гауссовскому закону. Длина последовательности соответствует размерам детальных поддиапазонов, несмотря на то, что водяной знак внедряется только в небольшое количество наибольших коэффициентов [10]. Использование водяного знака такой длины помогает избежать зависимости от порядка вычисления корреляции при извлечении ЦВЗ.

Декомпозиция изображения трехуровневая, с использованием фильтров Добеши-8. Для встраивания информации отбираются коэффициенты детальных поддиапазонов, амплитуда которых выше некоторого порога τ.

Выражение для встраивания информации имеет вид

$$f^l(m,n) = f(m,n) = \alpha|f(m,n)|w_i. \quad (2.12)$$

При извлечении информации используется слепой метод обнаружения ЦВЗ, при этом рассматриваются только коэффициенты, амплитуда которых больше некоторого порога обнаружения $\tau_2 \succ \tau_1$.

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

Декомпозиция изображения трехуровневая с использованием биортогональных вейвлет-фильтров.

Для встраивания ЦВЗ отбираются перцептуально значимые коэффициенты (существенное изменение которых приведет к искажениям, воспринимаемым зрительной системой человека). Порог отбора τ_i зависит от абсолютного максимума значений коэффициентов c_i по всем подуровням i-поддиапазона $\tau_i = 2^{log_2 c_i}$. (2.13)

Встраивание информации выполняется в соответствии с (2.2), но при этом коэффициент масштаба α для каждого уровня — свой. Для уровня *LL* коэффициент масштаба равен 0.04, так как значения коэффициентов этого уровня достаточно велики. Для 3, 2 и 1 уровней декомпозиции используются соответственно коэффициенты 0.1, 0.2 и 0.4.

При извлечении ЦВЗ по (2.4) также учитывается адаптивный коэффициент масштаба.

ЦВЗ представляет собой последовательность псевдослучайных действительных чисел, распределенных по гауссовскому закону. Длина последовательности для *LL* поддиапазона 500 чисел, для остающихся поддиапазонов 4500 чисел.

Водяной знак добавляется к наибольшим коэффициентам в каждом из поддиапазонов за исключением поддиапазонов наивысшего уровня разрешения (HL_1, LH_1, HH_1). Количество элементов водяного знака w_i в каждом из поддиапазонов пропорционально энергии этого поддиапазона. Энергия e_s определяется по формуле

$$e_{1=}\frac{1}{M\times N}\sum_{m=0}^{M}\sum_{n=o}^{N}f^2\,(m,n). \qquad (2.14)$$

где *M, N* — размеры поддиапазона.

Перед внедрением коэффициенты сортируются в порядке возрастания их абсолютных значений. Затем последовательность ЦВЗ складывается с последовательностью коэффициентов ВП, взятой в порядке убывания.

$$f^l(m,n) = f(m,n) = \alpha w_i f(m,n) w_i \qquad (2.15)$$

Для *LL* поддиапазона используется сравнительно малый коэффициент α, составляющий приблизительно 1/100 от используемого для других поддиапазонов. Визуальный весовой коэффициент w_s определяется для каждого поддиапазона и вводится в формулу для достижения гарантии незаметности водяного знака.

Извлечение информации выполняется также, как и в предыдущих алгоритмах.

ЦВЗ представляет собой массив биполярных псевдослучайных чисел. В алгоритме используется комплексное вейвлет-пакет преобразование, причем не только изображения, но и ЦВЗ.

Для модификации выбираются 1000 наибольших коэффициентов (рис.2.4).

При встраивании информации элементы водяного знака домножаются на масштабирующий коэффициент и затем добавляются к коэффициентам ВП

$$f^{l}(\mathrm{m},\mathrm{n}) = f(m,n) + \sqrt{a^2 \times U(m,n)^2 + \beta^2 w_i} \qquad (2.16)$$

где α и β -весовые коэффициенты, зависящие от уровня и предназначенные для достижения робастности и незаметности водяного знака, *U(m,n)* -среднее значение по окрестности 3*3 вокруг данного коэффициента.

Извлечение информации выполняется также, как и в предыдущих алгоритмах.

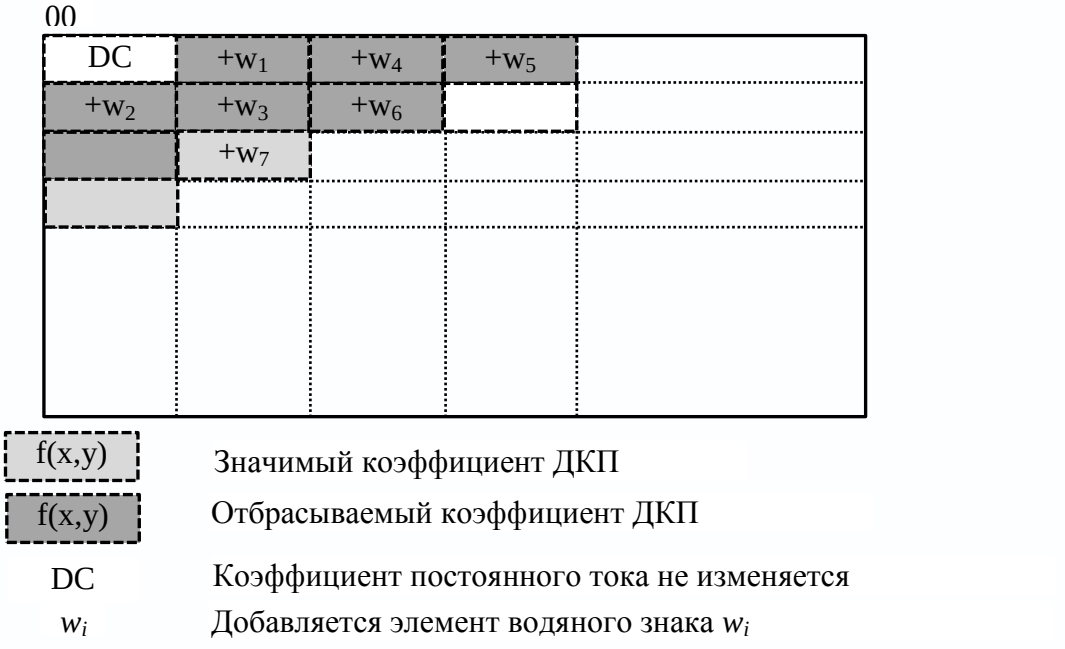


Рис 2.4 Отбор коэффициентов

ЦВЗ представляет собой последовательность псевдослучайных действительных чисел, распределенных по гауссовскому закону $w_i \in \{1, -1\}$, длина последовательности соответствует количеству отобранных коэффициентов.

Для декомпозиции изображения используется трехуровневое ВП.

Для модификации выбираются вейвлет-коэффициенты, амплитуда которых выше некоторого порога [JND — just noticeable difference].

Перед встраиванием информации вейвлет-коэффициенты сортируются в порядке возрастания их амплитуд. Таким же образом переупорядочиваются элементы гауссовской последовательности. На каждой итерации отбираются пара вейвлет-коэффициентов ($f_{положит}$, $f_{отриц}$) из «верха» упорядоченной последовательности вейвлет-коэффициентов исходного изображения и пара элементов последовательности ЦВЗ ($w_{верх}\, w_{нижн}$) из верхней и нижней части последовательности w.

При положительной модуляции правило

$$f^l = \begin{cases} f_{\text{положит}} + Jw_{i\ \text{верх}}\,\alpha & f_{\text{положит}} \succ 0, \\ f_{\text{положит}} + Jw_{i\ \text{нижн}}\,\alpha & f_{\text{положит}} \succ 0, \end{cases} \qquad (2.17)$$

при отрицательной модуляции правило

$$f^l = \begin{cases} f_{\text{отрицат}} + Jw_{i\ \text{верх}}\,\alpha & f_{\text{отрицат}} \succ 0, \\ f_{\text{отрицат}} + Jw_{i\ \text{нижн}}\,\alpha & f_{\text{отрицат}} \succ 0 \end{cases} \qquad (2.18)$$

применяется к отобранным вейвлет-коэффициентам для внедрения водяного знака. J обозначает JND-значение отобранного вейвлет-коэффициента, вычисленное на основе модели человеческого зрения. Весовой коэффициент α определяет максимально возможное изменение и выбирается различным для аппроксимационного и детального поддиапазонов.

Перед извлечением ЦВЗ вейвлет-коэффициенты полученного изображения переупорядочиваются. Затем используется инверсная формула $w^* = \frac{f^* - f}{J - \alpha}$.

Исходное изображение моделируется в ходе процесса извлечения информации с использованием гауссовской модели вейвлет-коэффициентов. Поэтому достаточно конечного количества параметров для описания распределения вероятностей вейвлет-коэффициентов переданного изображения. Но в этом случае только высокочастотные вейвлет-коэффициенты могут быть достаточно точно смоделированы. Следовательно, в этом случае необходимо отбирать коэффициенты только из детальных поддиапазонов.

ЦВЗ представляет собой последовательность псевдослучайных действительных чисел, длина которой зависит от пропускной способности изображения, вычисляемой на основе модели человеческого зрения.

В алгоритме используется четырехуровневая декомпозиция ВП с использованием 7/9 биортогональных фильтров.

Для внедрения ЦВЗ отбираются только вейвлет-коэффициенты *f(m,n),* амплитуда которых выше некоторого порога (JND).

Встраивание информации выполняется в соответствии с (2.2), но с учетом порога JND:

$$f^{l}(m,n) = \begin{cases} f(m,n) + j(m,n)w_i, & f(m,n) > J(m,n), \\ f(m,n), & \text{в ином случае.} \end{cases} \qquad (2.19)$$

Извлечение информации осуществляется при знании исходного изображения, по формуле (2.4). Перед вычислением корреляции все коэффициенты, меньшие по модулю текущего порога отбрасываются. Корреляция вычисляется отдельно для каждого уровня разрешения и рассматриваются пиковые значения корреляции.

Этот алгоритм можно рассматривать как модификацию алгоритма И.Кокса. Модификация заключается в добавлении масштабирующего коэффициента масштаба, зависящего от мощности исходного сигнала. Весовой коэффициент вычисляется, исходя из модели зрения, основанной на парадигме JND. Этот подход применяется для достижения верхней границы

возможной интенсивности ЦВЗ. Поэтому алгоритм позволяет незаметно внедрить достаточно робастный водяной знак. Важно отметить, что построение модели человеческого зрения гораздо проще осуществить при ДВП, чем при ДКП.

Предлагаемая схема может быть применена не только при ДВП, но и при ДКП, что позволяет встраивать информацию в данные сжатые как по стандарту JPEG2000, так и по стандарту JPEG.

Водяной знак представляет собой последовательность псевдослучайных действительных чисел, распределенных по Гауссовскому закону.

Для декомпозиции используется преобразование Хаара.

Для внедрения отбираются наибольшие коэффициенты из высокочастотного и среднечастотного диапазонов (поддиапазоны деталей).

Встраивание выполняется согласно аддитивной формуле

$$f^l(m,n) = f(m,n) - \alpha f(m,n)^\beta w_i, \qquad (2.20)$$

где от значения α зависит энергия ЦВЗ, а от значения -значение больших коэффициентов.

Для извлечения используется инверсная формула, аналогичная (2.4).

Благодаря иерархической декомпозиции, может быть сокращено количество вычислительных операций в процессе обнаружения водяного знака.

Большие вейвлет-коэффициенты соответствуют контурам и текстурам изображения. Именно в таких участках изображения и содержится большая часть энергии водяных знаков, так как человеческий глаз мало чувствителен к небольшим изменениям в таких областях. Внедряется последовательность псевдослучайных действительных чисел, распределенных по гауссовскому закону, длина которой соответствует количеству отобранных коэффициентов. Для встраивания выполняется пятиуровневое вейвлет-преобразование и отбираются значимые коэффициенты всех поддиапазонов.

Поиск таких коэффициентов основан на принципах многопорогового вейвлет-кодера (MTWC). Решение о значимости коэффициентов выносится на основании их сравнения с порогом данной субполосы T_{Si}. После встраивания водяного знака порог делится на два. Начальное значение порога T_{Si} определяется по формуле

$$T_{S,0} = \beta_1 \frac{max|f_s|}{2} \qquad (2.21)$$

где β_1 −весовой коэффициент данного поддиапазона.

Алгоритм начинает работу с наиболее энергетически значимого поддиапазона (наибольшее значение порога) и итерации продолжаются до тех пор, пока все биты ЦВЗ не будут внедрены [3]. Для встраивания используются только детальные поддиапазоны.

Внедрение выполняется в соответствии с формулой

$$f^l(m,n) = j(m,n) - \alpha_s T_s w_i. \qquad (2.22)$$

Для извлечения информации используется инверсная формула, аналогичная (2.4).

Для большей безопасности стегосистемы внедрение можно выполнять не во все значимые коэффициенты подряд, а выбираемые в соответствии с ключом.

Алгоритм A27 может быть изменен так, чтобы извлечение ЦВЗ стало слепым. Декодер должен в этом случае выполнить оценивание значений коэффициентов исходного изображения. Для упрощения его задачи перед встраиванием коэффициенты квантуются для уменьшения числа их возможных значений.

Пусть $f_s(m,n)$ —значимый коэффициент из поддиапазона s. То есть $T_s < f_s(m,n) < 2T_s$. Тогда коэффициент модифицируется согласно формуле

$$f^l(m,n) = sign \times \Delta_\rho(|f(m,n)|) + \alpha_s T_s w_i \qquad (2.23)$$

где sign — знак отобранного коэффициента, а $\Delta_p(\cdot)$ определяется как

$$\Delta_\rho(x) = (1+2)p\alpha_s)T_s \qquad (2.24)$$

Целое число p выбирается таким образом, чтобы расстояние между исходным и квантованным значением коэффициента $\left|\Delta_p(|f_s(m,n)| - |f_s(m,n)|\right|$ было минимальным.

При извлечении ЦВЗ вслепую вместо исходного коэффициента используется его аппроксимация $sign\Delta_p(|\dot{f_s}(m,n)|)$. Таким образом, получим

$$w_i = sign\Delta_p(|\dot{f_s}(m,n) - \dot{f_s}(m.n)|) \qquad (2.25)$$

Анализ алгоритмов на основе слияния ЦВЗ и контейнера

Если вместо последовательности псевдослучайных чисел в изображение встраивается другое изображение (например, логотип фирмы), то соответствующие алгоритмы внедрения называются алгоритмами слияния. Размер внедряемого сообщения намного меньше размера исходного изображения. Перед встраиванием оно может быть зашифровано или преобразовано каким-нибудь иным образом.

У таких алгоритмов есть два преимущества.

Во-первых, можно допустить некоторое искажение скрытого сообщения, так как человек все равно сможет распознать его.

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

Рассмотрено некоторые алгоритмы внедрения изображений в изображения.

В алгоритме внедряется черно-белое изображение (логотип), размером до 25 % от размеров исходного изображения. Перед встраиванием выполняется одноуровневая декомпозиция как исходного изображения, так и эмблемы с применением фильтров Хаара. Вейвлет-коэффициенты исходного изображения обозначаются, как *f(m,n)*, а вейвлет-коэффициенты логотипа - *w(m,n)*.

Модификации подвергаются все коэффициенты преобразования, как это показано на рис.2.5.

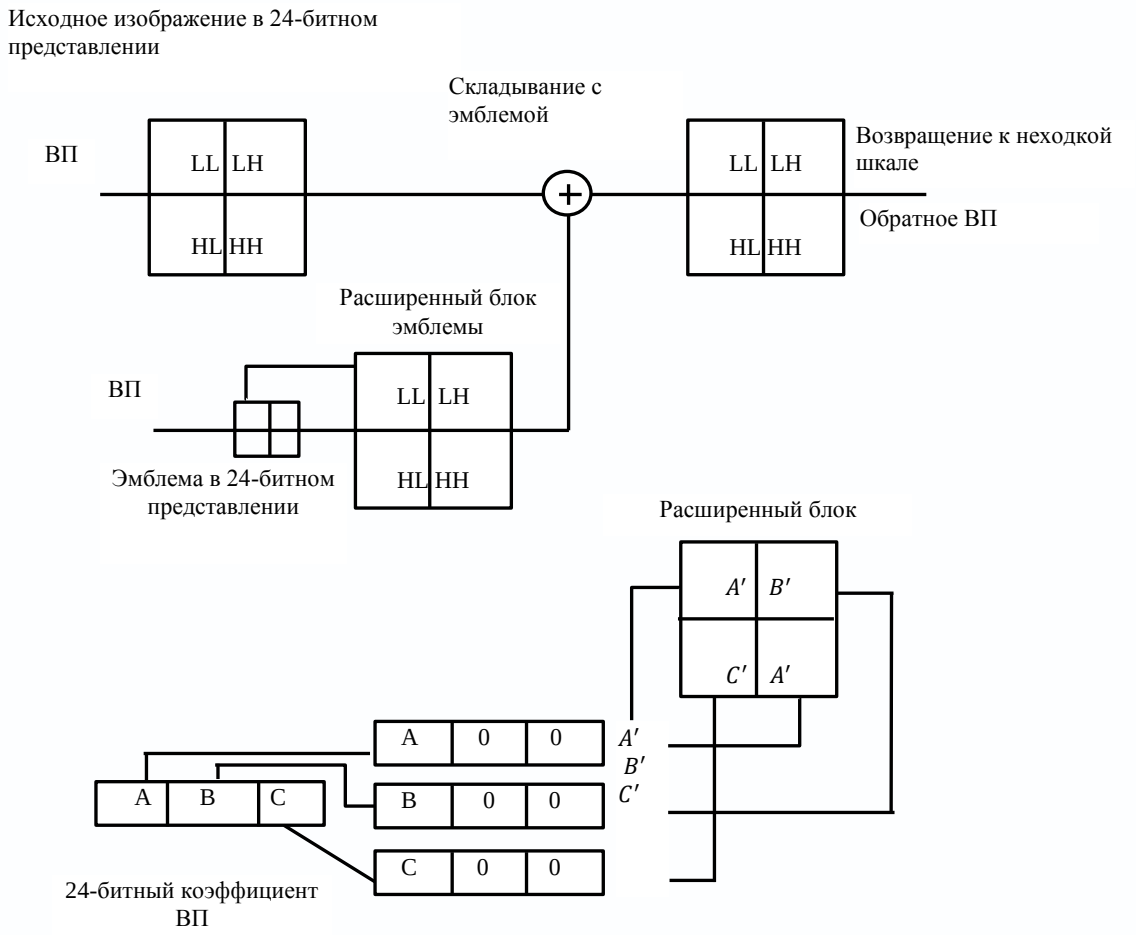


Рис 2.5 Схема встраивания ЦВЗ

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

Обозначим, через A, B, и C соответственно, старший, средний и младший байты 24-битного представления логотипа. На рис. 6.2 показано формирование трех 24-битных чисел A′, B′ и C′. Старший байт каждого из этих чисел представляет собой соответственно A, B, или C, два других байта заполняются нулями.

Затем формируется расширенный вчетверо блок коэффициентов логотипа. После чего он поэлементно складывается с 24-битной версией исходного изображения

$$f^l(m,n) = \alpha f(m,n) + w(m,n). \qquad (2.26)$$

Полученное значение отображается назад к исходной шкале на основе значений минимального и максимального коэффициента поддиапазона. После чего осуществляется обратное дискретное ВП.

Для извлечения ЦВЗ используется инверсная формула, аналогичная (2.4).

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

Также, как и в предыдущем алгоритме, исходное и внедряемое изображения подвергаются вейвлет-преобразованию. Для встраивания используются все коэффициенты детальных поддиапазонов.

Множество этих коэффициентов разбивается на неперекрывающиеся блоки размером $M_w * M_w$. Блоки обозначаются f_{kl}^1, где $i = 1, \ldots, 2^{2(M-l)}$, а k и l, соответственно местоположение коэффициента и уровень разрешения.

Водяной знак прибавляется к элементам исходного изображения по формуле

$$f_{k,j}^1(m,n) = f_{k,j}^1(m,n) + \alpha_{k,j}\sqrt{S\left(f_{k,l}^1(m,n)\right)}\, w_{k,}^1(m,n), \qquad (2.27)$$

где S — коэффициент масштаба, вычисляемый по формуле

$$S\left(f_{k,l}^1(m,n)\right) = \sum_{u,v} C(u,v)\left|T(f_{k,l}^1(m,n)\right|^2, \qquad (2.28)$$

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

Таким образом, алгоритм использует довольно сложную модель человеческого зрения. Для обнаружения в детекторе может быть использовано как вычисление корреляционной функции, так и визуальное сравнение.

2.5. Критерии эффективности и количественная оценка искажений в стеганографии изображений

Под термином «эффективность» в стеганографии понимается возможность решения с помощью цифровых изображений основных задач стеганографии: быстро и скрытно передавать большие объемы информации. Существует очень большое количество факторов, влияющих на эффективность стеганографии цифровых изображений.

Среди этих факторов можно выделить группу технических критериев эффективности, которые поддаются строгому математическому описанию и имеют некоторый набор численных характеристик. В качестве примера такого критерия можно привести отношение максимального размера встраиваемого сообщения, не приводящего к искажению изображения, к размеру самого контейнера.

С другой стороны, существуют критерии эффективности, не поддающиеся техническому описанию, но по-прежнему играющие исключительную роль в формировании понятия «эффективность». Рассматривая несколько графических форматов, можно утверждать, что применять один из них эффективнее, чем другой. Причиной для этого может являться то, что один из форматов имеет гораздо большее распространение (в том числе, в сети Интернет), чем остальные. Более того, использование некоторых форматов для нетипичных для них целей само по себе может быть подозрительным и провоцировать атаки. Например, выложенные на сайт в сети Интернет фотографии друзей в формате BMP (имеющие размер порядка нескольких мегабайт) определенно вызовут подозрение у посетителей (ведь современные алгоритмы сжатия позволяют сжимать фотографии в 20-30 раз с приемлемой потерей качества). К тому же, для некоторых форматов (например, упомянутый выше формат BMP) разработан широчайший спектр методов и инструментов стеганоанализа, и эти форматы являются более уязвимыми, а значит и менее эффективными с точки зрения стеганографии.

Про анализируется наиболее важные критерии эффективности применения цифровых изображений в стеганографии.

1. Скрытность или стеганографическая стойкость. Удовлетворение требованию скрытности является обязательным для абсолютно любой стеганосистемы. В применении к графической стеганосистеме, стойкость связана с изменениями (искажениями), вносимыми в исходное изображение при встраивании сообщения [12]. Требование стойкости считается невыполненным, если изображение поддается атаке посредством простого визуального анализа. Такая стеганосистема обладает крайне низкой эффективностью и не может найти практического применения, так как не соответствует минимальному уровню безопасности (Рис.2.6).

Рис.2.6 Результат работы алгоритма, не отвечающего требованиям стойкости

1 – исходное изображение, 2- изображение со встроенным сообщением

Как правило, при создании стеганографических алгоритмов, наибольший объем исследований связан именно с обеспечением скрытности. Производятся эксперименты, позволяющие установить, как изменение той или иной части файла-контейнера влияет на результирующее изображение. Стойкость стеганоалгоритма в значительной степени определяется размерами встраиваемого сообщения.

2. Размер встраиваемого сообщения. Эффективность использования цифрового изображения для хранения секретной информации в значительной

мере определяется максимальным возможным размером секретного сообщения. Как правило, численно этот критерий характеризуется процентным соотношением между объемом встраиваемого сообщения и исходным объемом контейнера. В отношении изображений, данная величина варьируется в зависимости от используемого графического формата.

Главным «ограничителем» максимального размера сообщения для конкретного графического файла выступает описанное выше требование скрытности. В стеганографии имеется фундаментальная зависимость между стойкостью встраивания и размером встраиваемого сообщения. Эта зависимость имеет обратно пропорциональный характер: чем больше объем встраиваемого в заранее заданный контейнер сообщения, тем ниже надежность сокрытия этой информации в контейнере (Рис.2.7).

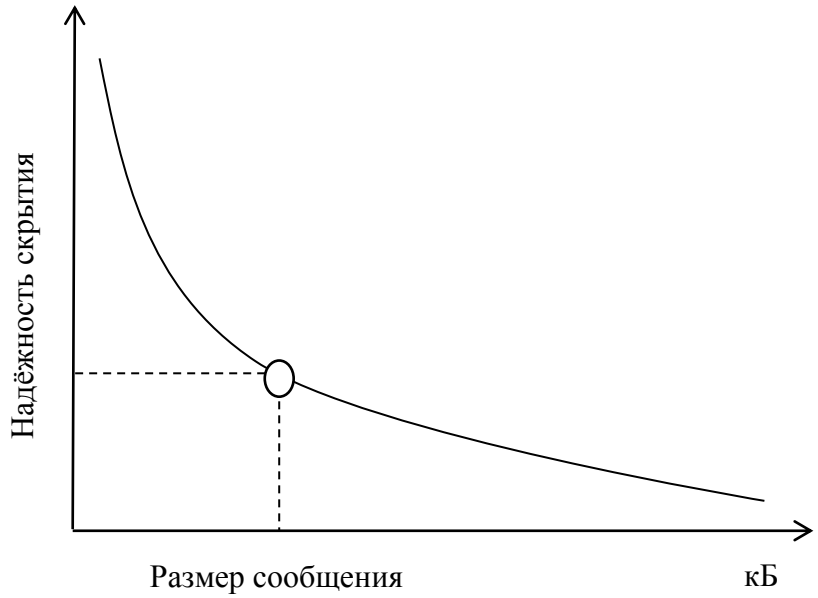


Рис.2.7 Зависимость надежности сокрытия информации от объема сообщения

Казалось бы, приведенная закономерность не позволяет увеличивать эффективность стеганографического встраивания информации путем наращивания размера сообщения. Но это не так. Существует несколько методов повышения размеров сообщения без ущерба стойкости, о которых речь пойдет дальше.

3. Устойчивость к модификации заполненного контейнера (сжатию). Устойчивость к модификации характеризует вероятность восстановления сообщения при условии некоторой модификации заполненного контейнера. Частным случаем модификации является сжатие с потерями. Особое значение этот фактор эффективности имеет для технологий внедрения цифровых водяных знаков [6].

Модификация заполненного контейнера может осуществляться как непреднамеренно (сжатие, ошибки при передаче файла по каналу связи с помехами), так и преднамеренно (попытка нарушить авторские права путем уничтожения ЦВЗ). Повышение устойчивости к сжатию осуществляется путем тщательного исследования алгоритмов компрессии с целью определения областей контейнера, не подвергающихся модификациям. Действенным методом борьбы с преднамеренным разрушением ЦВЗ может считаться встраивание информации в ту область файла-контейнера, изменение которой приводит к деградации изображения. Традиционным и достаточно мощным способом борьбы с «помехами» может служить увеличение избыточности встраиваемого сообщения (Рис.2.8).

4. Объем вычислений, необходимый для встраивания сообщения в цифровое изображение. Несмотря на стремительный рост возможностей современных компьютеров, проблема вычислительной сложности алгоритмов встраивания продолжает играть ключевую роль в некоторых областях применения стеганографии. Это, как правило, информационные системы реального времени, где временные рамки выполнения алгоритма сильно ограничены. В качестве примера, можно привести гипотетический скрытый канал голосовой связи, работающий посредством встраивания аудиоинформации в поток графических файлов, передаваемых по сети. Очевидно, что в данном случае, во избежание потери качества передаваемой информации, пакеты данных (цифровые изображения) должны подготавливаться (заполняться сообщениями) и передаваться без задержек.

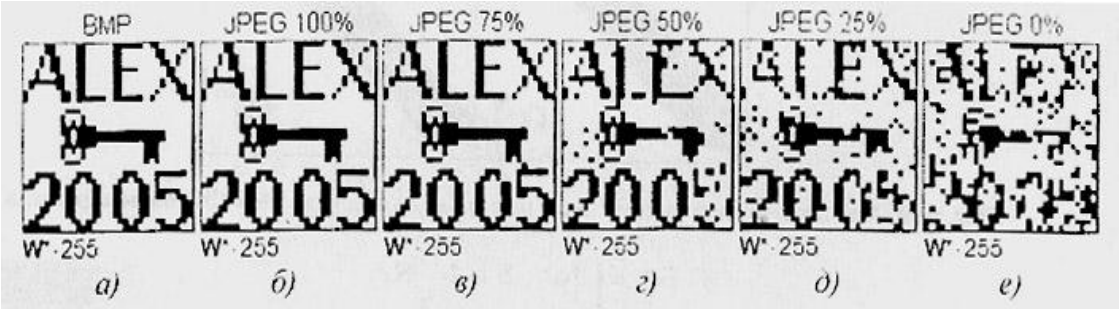


Рис.2.8 Искажение ЦВЗ при сжатии. а) – исходный ЦВЗ; б) - е) – ЦВЗ, извлеченный контейнера, сжатого с различной степенью.

Стоит отметить, что большинство стеганографических алгоритмов не обладают большой вычислительной сложностью. Тем не менее, попытки увеличения некоторых параметров эффективности (скрытность, размер сообщения), могут значительно увеличивать объемы вычислений и ограничивать использование алгоритма в системах реального времени.

5. Используемый графический формат. В значительной степени эффективность применения цифровых изображений в стеганографии зависит от формата их хранения. Поясним это несколькими примерами.

Формат BMP, имевший широкое распространение в прошлом, сегодня утратил свои позиции. Несмотря на обилие алгоритмов и техник встраивания информации в файлы этого формата, его нельзя назвать эффективным с точки зрения современной стеганографии. Во-первых, его применение в настоящее время весьма ограничено. Во-вторых, в отношении контейнеров в формате BMP разработано большое количество методов обнаружения скрытого сообщения, что также снижает эффективность формата.

Одним из наиболее распространенных в сети Интернет форматов является формат GIF, использующий алгоритм сжатия без потерь. Отсутствие потерь при компрессии позволяет использовать для сокрытия информации те же алгоритмы, что и для несжатых изображений. Тем не менее, это не решает проблемы обнаружения встроенного сообщения. К тому же, ограниченность размера цветовой палитры ограничивает возможности

использования его для хранения цифровых фотографий (которые являются наиболее востребованным видом контейнеров).

Наиболее эффективным, выглядит формат JPEG, который используется для хранения подавляющего большинства цифровых фотографий. Преимущества этого формата объясняются ещё и отсутствием эффективных методов обнаружения и изменения сообщений, встроенных в частотную область изображения (коэффициенты дискретного косинусного преобразования, или ДКП).

Количественная оценка искажений изображения

Создание и эксплуатация надежного стеганографического средства предусматривает наличие определенного инструментария для его контроля и оценки. Количественное оценивание стойкости стеганографической системы защиты к внешним воздействиям представляет собой достаточно сложную задачу, которая обычно на практике реализуется методами системного анализа, математического моделирования или экспериментального исследования.

Как правило, профессионально разработанная стеганосистема обеспечивает трехуровневую модель защиты информации, решающую две основные задачи:

- скрытие самого факта наличия защищаемой информации (первый уровень защиты);
- блокирование несанкционированного доступа к информации, осуществляемое путем избрания соответствующего метода скрытия информации (второй уровень защиты).

Наконец, необходимо принимать во внимание и вероятность существования третьего уровня - предварительной криптографической защиты (шифрования) скрываемой информации.

Стеганографический анализ методов встраивания информации в изображения может быть сведен к оценке контроля искажений (контроль

качества) графических изображений, полученных после обработки сравниваемыми методомами. Методы контроля искажений позволяют дать количественную оценку изменениям, произошедшим в результате внедрения конкретного сообщения в конкретный контейнер, т.е. найти компромисс между величиной искажений, характеризующей стойкость стеганографической системы как к атакам активного, так и к атакам пассивного противника, и пропускной способностью канала скрытной передачи.

Критерий оценки качества графических изображений – это метрика между исходным (неискаженным, обозначим его C) и модифицированным (искаженным, обозначим его S) графическим изображением. Понятие качества определяется как мера восприятия человеком вносимых искажений в исходное изображение.

Для оценки качества графического изображения используются показатели:

Максимальная разность, вычисляется по формуле:

$$\mathrm{MD} = \max_{x,y} \left| C_{x,y} - S_{x,y} \right| \qquad (0.1)$$

Средняя абсолютная разность:

$$\mathrm{AD} = \frac{1}{XY} \sum_{x,y} \left| C_{x,y} - S_{x,y} \right| \qquad (0.2)$$

Нормированная средняя абсолютная разность:

$$\mathrm{NAD} = \frac{\sum_{x,y} \left| C_{x,y} - S_{x,y} \right|}{\sum_{x,y} \left| C_{x,y} \right|} \qquad (0.3)$$

Среднеквадратическая ошибка:

$$\mathrm{MSE} = \frac{1}{XY} \sum_{x,y} \left(C_{x,y} - S_{x,y} \right)^2 \qquad (0.4)$$

Нормированная среднеквадратическая ошибка:

$$\mathrm{NMSE} = \frac{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y}\right)^2} \qquad (0.5)$$

Отношение «сигнал/шум»:

$$\mathrm{SNR} = \frac{\sum_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2} \qquad (0.6)$$

Максимальное отношение «сигнал/шум»:

$$\mathrm{PSNR} = \mathrm{XY} \cdot \frac{\max_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2} \qquad (0.7)$$

L_2-норма:

$$\mathrm{L}_2 = \left(\frac{1}{XY} \sum_{x,y} \left| C_{x,y} - S_{x,y} \right|^2 \right)^{1/2} \qquad (0.8)$$

Качество изображения:

$$\mathrm{IF} = 1 - \frac{\sum_{x,y}\left(C_{x,y} - S_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y}\right)^2} \qquad (0.9)$$

Нормированная взаимная корреляция:

$$\mathrm{NC} = \frac{\sum_{x,y}\left(C_{x,y} \cdot S_{x,y}\right)}{\sum_{x,y}\left(C_{x,y}\right)^2} \qquad (0.10)$$

Качество корреляции:

$$CQ = \frac{\sum_{x,y}\left(C_{x,y} \cdot S_{x,y}\right)}{\sum_{x,y}\left(C_{x,y}\right)} \qquad (0.11)$$

Структурное содержание:

$$SC = \frac{\sum_{x,y}\left(C_{x,y}\right)^2}{\sum_{x,y}\left(S_{x,y}\right)^2} \qquad (0.12)$$

В таблице 2.1 представлены значения описанных показателей для методов встраивания информации в пространственную область изображения.

Количественные показатели качества изображения Таблица 2.1

Показатель искажения	Оригинал	Методы скрытия в пространственной области					
		НЗБ	ПС интервала	ПС перестановки	Блочного кодирования	Замены палитры	Квантования
Максимальная разность, *MD*	0	1	1	1	1	3	3
Средняя абсолютная разность, *AD*	0	0,494	$7.690 \cdot 10^{-3}$	$5.920 \cdot 10^{-3}$	$6.165 \cdot 10^{-3}$	$9.827 \cdot 10^{-3}$	$7.141 \cdot 10^{-3}$
Нормированная средняя абсолютная разность, *NAD*	0	$3.823 \cdot 10^{-3}$	$5.956 \cdot 10^{-5}$	$4.585 \cdot 10^{-5}$	$4.774 \cdot 10^{-5}$	$7.611 \cdot 10^{-5}$	$5.535 \cdot 10^{-5}$
Среднеквадратическая ошибка, *MSE*	0	0.494	$7.690 \cdot 10^{-3}$	$5.920 \cdot 10^{-3}$	$6.165 \cdot 10^{-3}$	0.017	$9.460 \cdot 10^{-3}$
Нормированная среднеквадратическая ошибка, *NMSE*	0	$2.010 \cdot 10^{-5}$	$3.132 \cdot 10^{-7}$	$2.411 \cdot 10^{-7}$	$2.510 \cdot 10^{-7}$	$7.084 \cdot 10^{-7}$	$3.853 \cdot 10^{-7}$
Отношение "сигнал/шум", *SNR*	∞	$4.975 \cdot 10^{4}$	$3.193 \cdot 10^{6}$	$4.148 \cdot 10^{6}$	$3.983 \cdot 10^{6}$	$1.412 \cdot 10^{6}$	$2.596 \cdot 10^{6}$
Максимальное отношение "сигнал/ шум", *PSNR*	∞	$1.317 \cdot 10^{5}$	$8.455 \cdot 10^{6}$	$1.044 \cdot 10^{7}$	$1.055 \cdot 10^{7}$	$3.738 \cdot 10^{6}$	$6.873 \cdot 10^{6}$
L2-норма	0	0.703	0.088	0.077	0.079	0.132	0.097

Качество изображения. *IF*	1	0.999980	≈1	≈1	≈1	0.999999	≈1
Нормированная взаимная корреляция, NC	1	0.999439	0.999992	0.999998	0.999988	0.999942	1.000001
Качество корреляции, CO	190.182	190.076	190.181	190.182	190.180	190.172	190.183
Структурное содержание, SC	1	1.001103	1.000016	1 .000004	1 .000025	1.000114	0.999999

Большинство показателей искажения или критериев качества, которые используются при визуальной обработке информации, относятся к группе разностных показателей искажения [8]. Эти показатели базируются на отличии между контейнером-оригиналом (неискаженный сигнал) и контейнером-результатом (искаженный сигнал). Последние три показателя в таблице (WS, CO и SC) относятся к показателям, основанных на корреляции между оригинальным и искаженным сигналами (так называемые корреляционные показатели искажения).

В представленных соотношениях через $C_{x,y}$ обозначается пиксель пустого контейнера с координатами (x,y), а через $S_{x,y}$ - соответствующий пиксель заполненного контейнера.

3. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

3.1. Основные понятия и определения

Жизнедеятельность – сложный биологический процесс, происходящий в организме человека, позволяющий сохранять здоровье и работоспособность. Необходимым и обязательным условием протекания биологического процесса является деятельность. В самом широком смысле слово «деятельность» означает разносторонний процесс создания с общественным субъектом «человеком» условий для своего существования и развития, процесс преобразования природной и социальной реальности в соответствии с индивидуальными потребностями, целями и задачами.

Деятельность – специфически человеческая форма активного отношения к окружающему миру, содержание которой составляет его целесообразное изменение и преобразование. Всякая деятельность включает в себя цель, средство, результат и сам процесс деятельности. Формы деятельности многообразны. Они охватывают практические, интеллектуальные, духовные процессы, протекающие в быту, общественной, культурной, трудовой, научной, учебной и других сферах жизни.

Модель процесса деятельности представляет собой двухцелевую бинарную систему «человек-среда». Одна цель состоит в достижении определенного эффекта, вторая – в исключении нежелательных последствий. Указанные цели являются конкурирующими.

Концепция приемлемого (допустимого) риска

Традиционная техника безопасности базируется на категорическом императиве – обеспечить безопасность, не допустить никаких аварий. Как показывает практика, такая концепция неадекватна законам техносферы. Требование абсолютной безопасности, подкупающее своей гуманностью,

может обернуться трагедией для людей потому, что обеспечить нулевой риск в действующих системах невозможно.

Современный мир отверг концепцию абсолютной безопасности и пришел к концепции приемлемого (допустимого) риска, суть которой в стремлении к такой безопасности, которую приемлет общество в данный период времени.

Восприятие риска и опасностей общественностью субъективно. Люди резко реагируют на события редкие, сопровождающиеся большим числом единовременных жертв. В то же время частые события, в результате которых погибают единицы или небольшие группы людей, не вызывают столь напряженного отношения [13]. Ежедневно на производстве погибает 40-50 человек, а в целом по стране от различных опасностей лишаются жизни более 10000 человек в день. Но эти сведения менее впечатляют, чем гибель 5-10 человек в одной аварии или каком-либо конфликте. Это необходимо иметь в виду при рассмотрении проблемы приемлемого риска. Субъективность в оценке риска подтверждает необходимость поиска приемов и методологий, лишенных этого недостатка. По мнению специалистов, использование риска в качестве оценки опасностей является предпочтительнее, чем использование традиционных показателей.

Приемлемый риск сочетает в себе технические, экономические, социальные и политические аспекты представляющие некоторый компромисс между уровнем безопасности и возможностями ее достижения.

Прежде всего, нужно иметь в виду, что экономические возможности повышения безопасности технических систем не безграничны.

Эргономика

Усложнение производственных процессов и оборудования изменили функции человека в современном производстве: возросла ответственность решаемых задач; увеличился объем информации, воспринимаемой работающим и быстродействие оборудования. Работа человека стала

сложнее, возросла нагрузка на нервную систему и снизилась нагрузка физическая. В ряде случаев человек стал наименее надежным звеном системы «человек-машина». Возникла задача обеспечения надежности и безопасности работы человека на производстве. Эту задачу решает эргономика и инженерная психология.

Эргономика (от греческого ergon - работа и nomos - закон) - научная дисциплина, изучающая человека в условиях его деятельности, связанной с использованием машин. Цель эргономики - оптимизация условий труда в системе "человек-машина" (СЧМ). Эргономика определяет требования человека к технике и условия ее функционирования. Эргономичность техники является наиболее обобщенным показателем свойств и других показателей техники.

Эргономика - наука о том, как люди с их различными физическими данными и способами функционирования взаимодействуют с окружающей рабочей средой (оборудованием и машинами, которыми они пользуются). Цель эргономики состоит в том, чтобы обеспечить комфорт, эффективность и безопасность при пользовании компьютерами уже на этапе разработки клавиатур, компьютерных плат, рабочей мебели и др. для устранения физического дискомфорта и проблем со здоровьем на рабочем месте. В связи с тем, что все больше людей проводят много времени перед компьютерными мониторами, ученые многих областей, включая анатомию, психологию и охрану окружающей среды, вовлекаются в изучение правильных, с точки зрения эргономики, условий работы.

3.2. Связь человека с окружающей средой и параметрами рабочего места

Рабочее место - это зона, в которой совершается трудовая деятельность исполнителя или группы исполнителей. Рабочие места могут быть

индивидуальными и коллективными, универсальными, специализированными и специальными.

Общие требования, которые должны соблюдаться при проектировании рабочих мест, следующие:

- достаточное рабочее пространство для человека;
- оптимальное положение тела работающего;
- достаточные физические, зрительные и слуховые связи между человеком и машиной;
- оптимальное размещение рабочего места в помещении;
- допустимый уровень действия факторов производственных условий; оптимальное размещение информационного и моторного поля;
- наличие средств защиты от производственных опасностей.

Конструирование должно обеспечивать зоны оптимальной и легкой досягаемости моторного поля рабочего места и оптимальную зону информационного поля рабочего места. Угол обзора по отношению к горизонтали должен составлять 30-40°.

Выбор рабочего положения должен учитывать усилия, затрачиваемые человеком, размах движений, необходимость перемещений, темп операций. Выбор рабочей позы должен учитывать физиологию человека, а параметры рабочего места определяются выбором положения тела при работе (сидя, стоя, переменно).

Рабочие места для выполнения работ «сидя» организуются при легкой работе и средней тяжести, а при тяжелой - рабочая поза -"стоя".

Проектирование оборудования должно обеспечить его соответствие антропометрическим и биомеханическим характеристикам человека на основе учета динамики изменения размеров тепла при его перемещении, диапазона движений в суставах.

Для учета в конструкции оборудования антропометрических данных необходимо:

- определить контингент людей, для которых предназначено оборудование;
- выбрать группу антропометрических признаков;
- установить процент работающих, которому должно удовлетворять оборудование;
- определить границы интервала размеров (усилий), которые должны быть реализованы в оборудовании.

Для работы в положении "сидя" используются различные рабочие сиденья. Различают рабочие сиденья для .длительного и кратковременного пользования. Общие требования для сидений длительного пользования следующие: сидение должно обеспечивать позу, уменьшающую статистическую работу мышц; создавать условия для возможности изменения рабочей позы; не затруднять деятельность систем организма; обеспечивать свободное перемещение относительно рабочей поверхности, иметь регулируемые параметры; иметь полумягкую обивку [14].

При организации рабочего места должны быть учтены не только факторы, отражающие опыт, уровень профессиональной подготовки, индивидуально-личностные свойства операторов-связистов, но и факторы, характеризующие соответствие форм, способов представления и ввода информации психофизиологическим возможностям человека.

При оптимизации процедур взаимодействия операторов-связистов с техническими средствами в условиях автоматизации эргономические факторы выступают в качестве основных, обуславливающих вероятностно-временные характеристики и напряженность работы. Эти факторы являются чувствительными к вариациям индивидуально-личностных свойств оператора.

Заключение

Сегодня интерес к компьютерной стеганографии быстро растет. Причин для этого достаточно много. Одной из основных является то, что стеганография предоставляет принципиально новый способ защиты информации и не имеет аналогов. В отличие от криптографии, стеганография скрывает факта передачи информации, который сам по себе может иметь решающее значение. С другой стороны, компьютерная стеганография, как следует из её определения, для сокрытия информации использует файлы, содержащие информацию мультимедиа. Ошеломляющий рост объемов такого рода информации и её повсеместное проникновение делают стеганографию универсальным и ещё более привлекательным инструментом. Одним из значимых факторов является и то, что в отношении стеганография, в отличие от криптографии, на данный момент не разработано соответствующей нормативно-правовой базы, регулирующей её использование. Все вышеперечисленные факторы в большей степени характерны для цифровых изображений, что делает их одним из наиболее эффективных носителей скрываемой информации.

Основные результаты ВКР могут быть сформулированы в следующем виде:

1. Были рассмотрены и изучены методы стеганографической защиты, а также рассмотрены их достоинства и недостатки.
2. Описаны стеганографические протоколы в криптографических системах защиты информации.
3. Рассмотрены виды атак против используемого протокола и методы противодействия атакам на системы ЦВЗ.
4. Построены математические модели стеганографии на основе множества возможных ЦВЗ и скрываемых сообщений.
5. Приведены основные свойства ЗСЧ, которые учитываются при построении стеганоалгоритмов.

6. Описан алгоритм скрываемые данные в области первичного изображения.

7. Исследованы методов стеганографии, позволяющей заменить значащих битов пикселей изображения битами секретного сообщения.

8. Анализированы аддитивных алгоритмов на основе линейного встраивания данных и слияния ЦВЗ в изображениях, которые модификации исходного изображения производится корреляционными методами и внедряется в выбранное подмножество отсчетов исходного изображения.

9. Изучены критерии эффективности и количественная оценка искажений в стеганографии изображений на основе показателей, которые базируются на отличии между контейнером-оригиналом (неискаженный сигнал) и контейнером-результатом (искаженный сигнал).

10. Разработана программа позволяющая скрыть, шифровать и дешифровать информации в изображениях на основе аддитивных алгоритмов.

Использованные литературы

1. Постановление Президента Республики Узбекистан "О дополнительных мерах по дальнейшему развитию информационно-коммуникационных технологий". от 21 марта 2012 года, ПП – 1730.

2. Артёхин Б.В. Стеганография // Журнал "Защита информации. Конфидент", 2008. - №4. - С.47-50.

3. Швидченко И.В. Анализ криптостеганографических алгоритмов // Проблемы управления и информатики, 2011. - № 4. - С. 149-155.

4. Барсуков В.С., Романцов А.П. Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века. Материалы Internet-ресурса «Специальная техника» (http://st.ess.ru/).

5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002. - 272 с.

6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография Теория и практика - К: МК-Пресс, 2007. - 288 с.

7. Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений // Журнал "Защита информации. Конфидент", 2005. - №3. - С.34.

8. Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. Основы компьютерной стеганографии. - М.: Радио и связь, 2003. - 152 с.

9. Барсуков В.С. Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники, 2009. - №2. - С.31 - 40.

10. Перепелицын Е.Г. Нестандартные методы математической статистики и их приложение к технической диагностике и анализу изображений. - Москва: Омега-Л, 2010. - 312 с.

11. Watson A. The cortex transform: rapid computation of simulated neural images // Computer Vision, Graphics, and Image Processing. 1987. Vol. 39. № 3. P. 311-327.

12. Раик Г.А., Садов В.С. Исследование информативности коэффициентов дискретного косинусного преобразования изображений. «Электроника-Инфо» – 2011 – №№4-5, С. 54-61, 52 – 58.

13. Экология и безопасность жизнедеятельности: Учебное пособие для студентов ВУЗов / ред. Л. А. Муравий, 2002.

14. Белов С.В. Безопасность жизнедеятельности М.: Высшая школа. 2003.

ПРИЛОЖЕНИЕ

```
unit uMain;
interface
uses
  Windows, SysUtils, Classes, Controls, Forms, Dialogs, StdCtrls,
ComCtrls, Buttons, XPMan, ExtCtrls, ExtDlgs;
type
  TForm1 = class(TForm)
    xpmnfst1: TXPManifest;
    lbl1: TLabel;
    dlgOpenPic1: TOpenPictureDialog;
    dlgOpen1: TOpenDialog;
    dlgSavePic1: TSavePictureDialog;
    dlgSave1: TSaveDialog;
    pnl1: TPanel;
    lbl2: TLabel;
    bbtnEncrypt: TBitBtn;
    bbtnDecrypt: TBitBtn;
    pb1: TProgressBar;
    bbtnInfo: TBitBtn;
    edtBPC: TEdit;
    udBitsPerChannel: TUpDown;
    lblBPC: TLabel;
    lblNote: TLabel;
    procedure bbtnEncryptClick(Sender: TObject);
    procedure bbtnDecryptClick(Sender: TObject);
    procedure bbtnInfoClick(Sender: TObject);
```

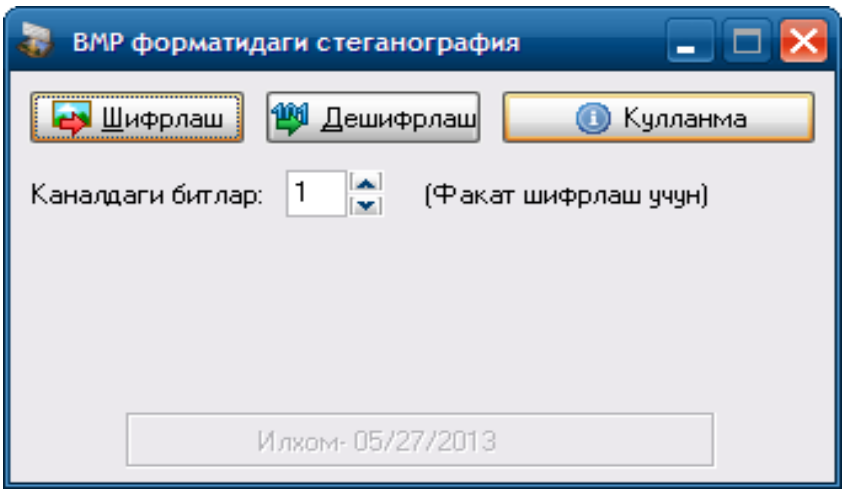
```
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
{$R *.dfm}
uses uProcess, ActiveX;
procedure TForm1.bbtnEncryptClick(Sender: TObject);
begin
  if dlgOpen1.Execute and dlgOpenPic1.Execute and dlgSavePic1.Execute
then
    try
      try
        bbtnEncrypt.Enabled:= False;
        bbtnDecrypt.Enabled:= False;
        bbtnInfo.Enabled:= False;
        lblBPC.Enabled:= False;
        lblNote.Enabled:= False;
        edtBPC.Enabled:= False;
        udBitsPerChannel.Enabled:= False;
        pb1.Show;
        Encrypt(dlgOpen1.FileName, dlgOpenPic1.FileName,
dlgSavePic1.FileName, udBitsPerChannel.Position, pb1);
        MessageBox( Application.Handle, PChar('Done!' + #13#10#13#10 +
'The file ''' +
                dlgSavePic1.FileName + ''' was created.'),
```

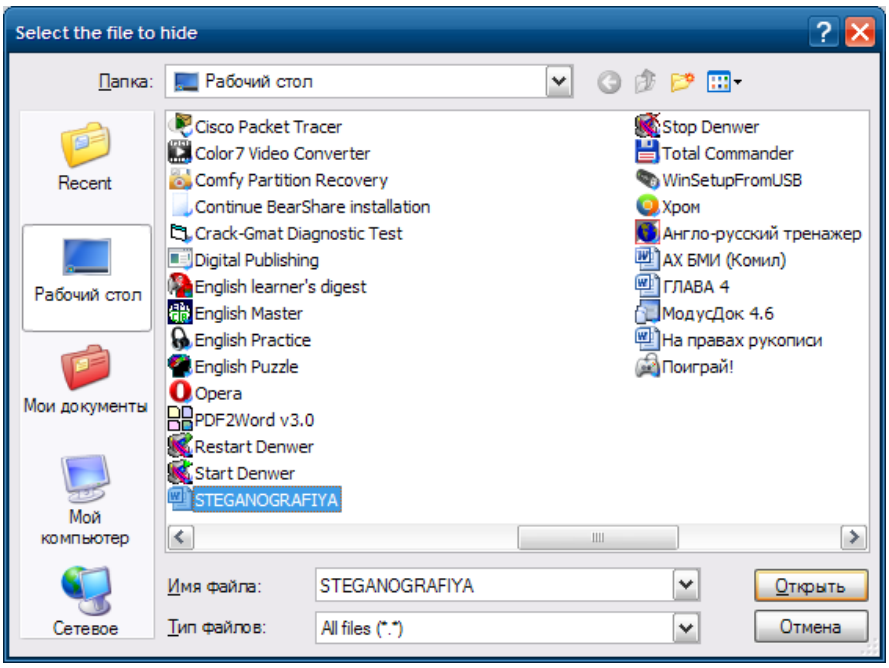
```
                    'StegaImage', MB_OK + MB_ICONINFORMATION);
              finally
                pb1.Hide;
                bbtnEncrypt.Enabled:= True;
                bbtnDecrypt.Enabled:= True;
                bbtnInfo.Enabled:= True;
                lblBPC.Enabled:= True;
                lblNote.Enabled:= True;
                edtBPC.Enabled:= True;
                udBitsPerChannel.Enabled:= True;
              end;
            except
              on e: Exception do
                MessageBox(Handle, PChar('An error has occurred.' + #13#10#13#10
+ e.Message), 'StegaImage', MB_OK + MB_ICONSTOP);
            end;
        end;
        procedure TForm1.bbtnDecryptClick(Sender: TObject);
        begin
          if dlgOpenPic1.Execute and dlgSave1.Execute then
            try
              try
                bbtnEncrypt.Enabled:= False;
                bbtnDecrypt.Enabled:= False;
                bbtnInfo.Enabled:= False;
                lblBPC.Enabled:= False;
                lblNote.Enabled:= False;
                edtBPC.Enabled:= False;
                udBitsPerChannel.Enabled:= False;
```

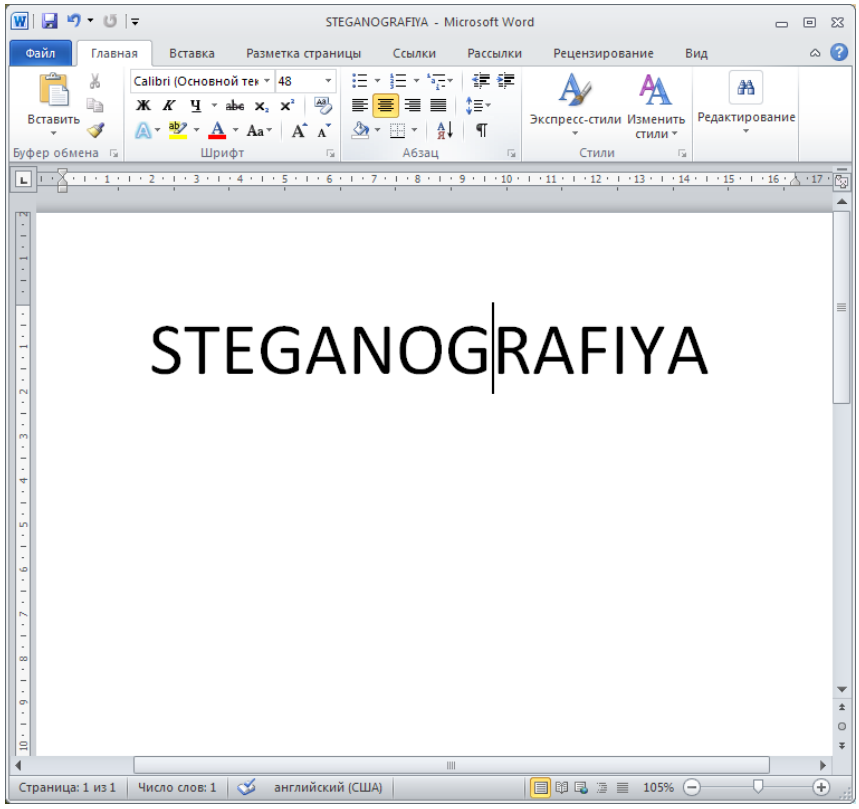
```
            pb1.Show;
            Decrypt(dlgOpenPic1.FileName, dlgSave1.FileName, pb1);
            MessageBox( Application.Handle, PChar('Done!' + #13#10#13#10 +
'The file "' +
                    dlgSave1.FileName + '" was created.'),
                    'StegaImage', MB_OK + MB_ICONINFORMATION);
          finally
            pb1.Hide;
            bbtnEncrypt.Enabled:= True;
            bbtnDecrypt.Enabled:= True;
            bbtnInfo.Enabled:= True;
            lblBPC.Enabled:= True;
            lblNote.Enabled:= True;
            edtBPC.Enabled:= True;
            udBitsPerChannel.Enabled:= True;
          end;
        except
          on e: Exception do
            MessageBox(Handle, PChar('An error has occurred.' + #13#10#13#10
+ e.Message), 'StegaImage',  MB_OK + MB_ICONSTOP);
        end;
      end;
      procedure TForm1.bbtnInfoClick(Sender: TObject);
      begin
        ShowMessage(  'In a 24-bit bitmap, each pixel is made up of (surprise,
surprise) a 24-bit number. Each number is composed of three 8-bit '+
        'numbers (the R, G and B channels). These are the intensity of the Red,
Green and Blue colors that create the final color of the pixel.'+ #13#10#13#10+
```

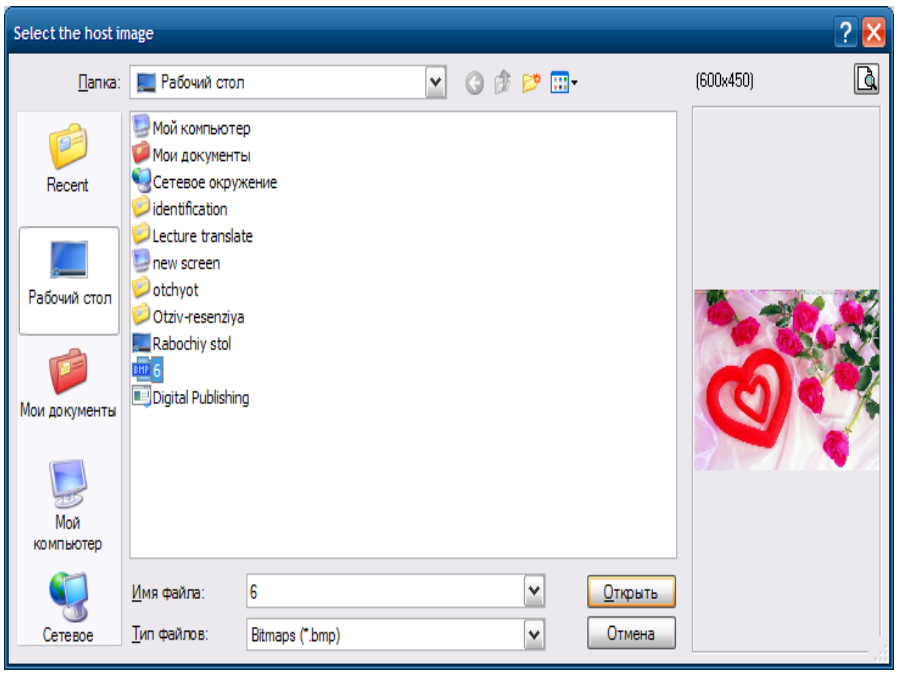
'To hide something inside the image, we will replace the Least Significant Bit (this is, the "rightmost" bit) of each 8-bit channel '+ 'of every pixel, with the bits of the file we want to hide. ' + #13#10#13#10 + 'The image will lose some quality because now the colors of the pixels are not the same, but it will go unnoticed to the human eye.' + #13#10#13#10 + 'Obviously, since we are storing only 3 bits per pixel, the image must have a fenomenal size to accommodate just a tiny little file. '+ 'For example, if we want to hide 1 MB of data, we need an image with 2,796,203 pixels, which would have a size of something like 2,200 x 1,320 pixels. And that is a 8.3 MB file... :O' + #13#10#13#10 + 'We could replace the 2, 3 or 4 rightmost bits of every channel in order to increase the amount of data we can hide, but the quality could decrease considerably.' + #13#10#13#10 + 'Try 8 bits per channel and you''ll see what I''m talking about (amazingly, 7 normally produces intelligible -although very ugly- images).');

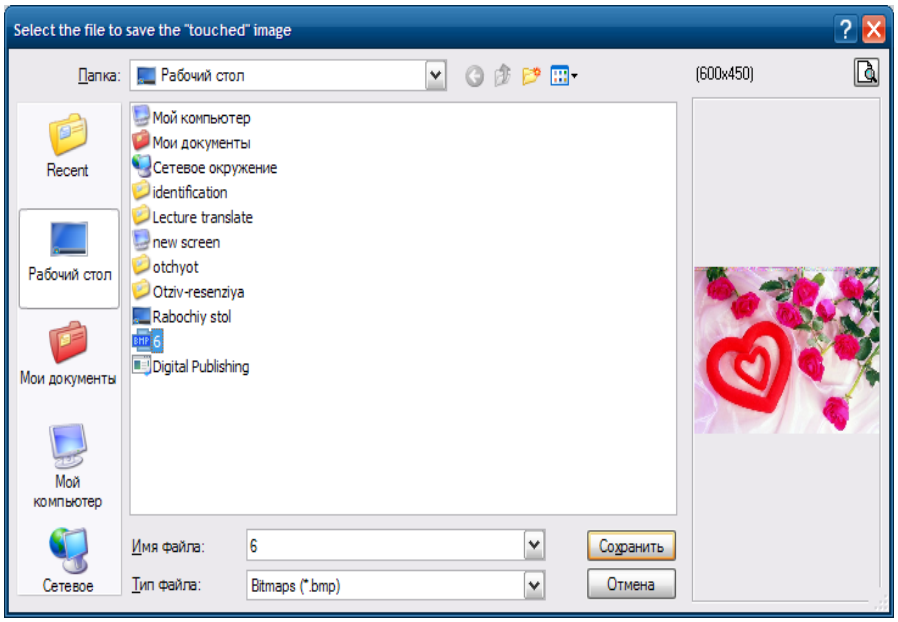
```
end;
// To prevent the nasty open dialog bug that occurs (at least in D7) bwhen the hint for a file is shown.
initialization
  OleInitialize(nil);
finalization
  OleUninitialize;
end.
```

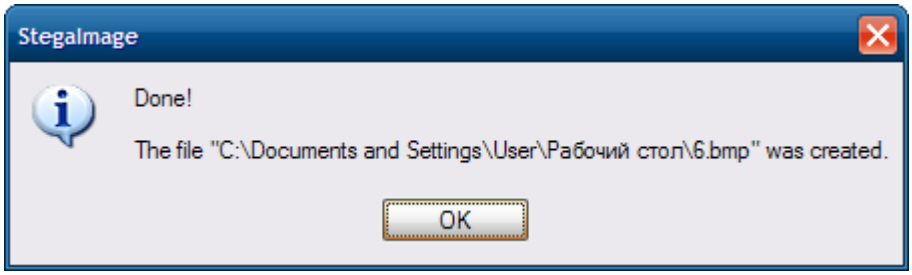



Select the file to hide
Папка:
Рабочий стол
Recent
Рабочий стол
Мои документы
Мой компьютер
Сетевое
Cisco Packet Tracer
Color7 Video Converter
Comfy Partition Recovery
Continue BearShare installation
Crack-Gmat Diagnostic Test
Digital Publishing
English learner's digest
English Master
English Practice
English Puzzle
Opera
PDF2Word v3.0
Restart Denwer
Start Denwer
STEGANOGRAFIYA
Stop Denwer
Total Commander
WinSetupFromUSB
Хром
Англо-русский тренажер
АХ БМИ (Комил)
ГЛАВА 4
МодусДок 4.6
На правах рукописи
Поиграй!
Имя файла:
STEGANOGRAFIYA
Тип файлов:
All files (*.*)
Открыть
Отмена


STEGANOGRAFIYA - Microsoft Word
Файл
Главная
Вставка
Разметка страницы
Ссылки
Рассылки
Рецензирование
Вид
Вставить
Буфер обмена
Шрифт
Абзац
Стили
Редактирование
STEGANOGRAFIYA
Страница: 1 из 1
Число слов: 1
английский (США)
105%


Select the host image
Папка:
Рабочий стол
(600x450)
Recent
Рабочий стол
Мои документы
Мой компьютер
Сетевое
Мой компьютер
Мои документы
Сетевое окружение
identification
Lecture translate
new screen
otchyot
Otziv-resenziya
Rabochiy stol
6
Digital Publishing
Имя файла:
6
Тип файлов:
Bitmaps (*.bmp)
Открыть
Отмена


Select the file to save the "touched" image
Папка:
Рабочий стол
(600x450)
Recent
Рабочий стол
Мои документы
Мой компьютер
Сетевое
Мой компьютер
Мои документы
Сетевое окружение
identification
Lecture translate
new screen
otchyot
Otziv-resenziya
Rabochiy stol
6
Digital Publishing
Имя файла:
6
Тип файла:
Bitmaps (*.bmp)
Сохранить
Отмена


StegaImage
Done!
The file "C:\Documents and Settings\User\Рабочий стол\6.bmp" was created.
OK