Избыточность и скрытность в элементах стеганографии

Бугаев В.С., Петраков А.В., МТУСИ

Избыточность мультимедийных данных и способы ее сокращения. Медиапродукт, представленный в цифровом виде, обладает значительной избыточностью, от которой стремятся избавиться с целью передачи его по существующим, ограниченным по полосе пропускания, каналам связи.

Различают три основных вида избыточности: пространственную, временную и психофизическую. Устраняя эти избыточности, удается достигать значительных коэффициентов сжатия.

Пространственная избыточность. Большая часть изображения одного кадра обычно приходится на области, имеющие постоянную или мало меняющуюся в пространстве яркость, а резкие световые переходы и детали малых размеров занимают малую долю площади изображения. Коэффициент корреляции соседних элементов изображения, описывающий статистическую связь между яркостями этих элементов, близок к единице. Зная яркость одного элемента, можно с высокой степенью вероятности предсказать яркость соседнего, например, полагая их просто равными. Такого рода избыточность можно назвать пространственной избыточностью изображения

Временная избыточность. Изображения соседних кадров в телевидении обычно очень похожи друг на друга, даже при съемке движущихся объектов. Переходы от сюжета к сюжету встречаются редко [1]. Межкадровая разность на значительной части площади изображения обычно близка к нулю. Зная распределение яркости в одном кадре, можно с высокой степенью уверенности предсказать распределение яркости следующего кадра. Эта предсказуемость указывает на временную избыточность изображения

Психофизическая избыточность. Психофизическая избыточность основана на том, что человеческое зрение более чувствительно к яркости, чем к цветовым составляющим. Можно выделить низкоуровневые (физиологические) и высокоуровневые (психофизиологические) свойства человеческого зрения [2]. К низкоуровневым свойствам относятся:

— частотная чувствительность,

— эффект маскирования

— чувствительность к изменению яркости изображения.

Высокоуровневые свойства проявляются "вторично". Например:

— чувствительность к размеру (большие участки изображения "заметнее" меньших размером, причем существует порог насыщения, когда дальнейшее увеличение размера не существенно);

— чувствительность к контрасту (высококонтрастные участки изображения, перепады яркости обращают на себя значительное внимание);

— чувствительность к форме (длинные и тонкие объекты привлекают большее внимание, чем круглые однородные);

— чувствительность к цвету (некоторые цвета, например, красный, "заметнее" других; этот эффект усиливается, если фон заднего плана отличается от цвета фигур на нем);

— чувствительность к внешним раздражителям (движение глаз наблюдателя зависит от конкретной обстановки, от полученных им перед просмотром или во время него инструкций, дополнительной информации);

— чувствительность к местоположению (человек склонен в первую очередь рассматривать центр изображения, люди обычно внимательнее к изображениям переднего плана, чем заднего).

Если на изображении есть люди, в первую очередь человек обратит свое внимание на них. На фотографии человек обращает первоочередное внимание на лицо, глаза, рот, руки.

1. Устранение пространственной и временной избыточности. Для устранения избыточности в мире было разработано множество стандартов, позволяющих сжимать исходный мультимедийный файл в десятки раз. Широкое распространение получил стандарт JPEG для неподвижных изображений, представляющий собой алгоритм декодирования сжатого мультимедийного файла. Для видеопоследовательностей и телевизионных сигналов широкую популярность получил стандарт MPEG-2, известный также как DVD.

В основе устранения пространственной избыточности в формате MPEG-2 лежит кодирование с преобразованием, в качестве которого используется двумерное четное косинусное преобразование. Этот вид преобразования позволяет осуществить пространственную декорреляцию исходных отсчетов изображения и обеспечить психофизиологически обоснованное частотно-зависимое квантование спектральных отсчетов.

В основе устранения временной избыточности лежит кодирование с предсказанием, обеспечивающее временную декорреляцию, осуществляемое при помощи передачи межкадровой разности с векторами смещения, минимизирующими эту разность, названными векторами движения, а также кодирование с предсказанием вперед и в двух направлениях, и передачи межкадровой разности.

Устранение психофизической избыточности в стандарте MPEG-2 схоже со стандартом JPEG и состоит из нескольких этапов [3]:

Преобразование цветового пространства и дискретизация. На этом этапе осуществляется преобразование изображения из цветового пространства RGB в YCbCr (где Y — яркость, а Cb и Cr — цветоразностные компоненты точки изображения). Применение пространства YCbCr вместо привычного RGB объясняется физиологическими особенностями человеческого зрения, а именно тем, что зрение человека имеет значительно большую чувствительность к яркости (Y), чем к цветоразностным составляющим Cb и Cr. И уменьшение размеров плоскостей Cr и Cb, таким образом уменьшая размер изображения.

Дискретное косинусное преобразование (ДКП) и квантование. На этом этапе применяется прямое ДКП, которое позволяет перейти от пространственного представления изображения к спектральному. Идея квантования состоит в "отбрасывании" некоторого объема информации. Известно, что глаз человека менее восприимчив к высоким частотам. Таким образом, используя таблицы квантования, мы отбрасываем менее значимые высокочастотные коэффициенты. Коэффициенты квантования просто определяют, какое количество данных теряется и, следовательно, определяют диапазон сжатия и качество восстановленного изображения.

2. Стеганографические методы, основанные на избыточности мультимедиа. Стеганография (steganography) — метод скрытой коммуникации между двумя сторонами, само существование которой

неизвестно третьей стороне [4].

Развитие цифровых технологий позволило представлять аналоговый сигнал в цифровом виде. В силу особенностей человеческого зрения и слуха оцифрованные видео- и аудио-файлы обладают психовизуальной избыточностью, что позволяет незаметно для человека вносить незначительные изменения в эти файлы. На этом принципе развилось научное направление известное как цифровая стеганография.

Общую схему стеганографической системы можно представить как систему связи [5] (рис.1).

Цифровые потоки сжимаются в соответствии с каким-либо форматом алгоритмом JPEG, MPEG-2 и др. и поэтому содержательную часть цифрового потока сопровождает управляющая (форматная) часть потока. Стеганографические системы строят таким образом, чтобы формат изображений мог позволить скрывать сообщения в цифровых данных и содержательной (контентной) неформатные системы и управляющей форматные системы частях информационного потока [6].

Форматные методы сокрытия в графических изображениях: в косвенных данных; с использованием маркеров комментариев; с использованием уменьшенного изображения; в палитре; после палитры; в нулевых байтах; дописывание данных в конец файла BMP.

Неформатные методы сокрытия в графических изображениях: в исходных данных изображения; с использованием таблиц квантования; в спектре изображения после квантования (замена наименее значимых бит — НЗБ); в графических изображениях с палитрой цветов (палитра цветов условный набор цветов с интенсивностью цветовых составляющих в каком-либо фиксированном цветовом пространстве, причем каждая точка изображения содержит лишь номер цвета из палитры, а не информацию о ее цвете в цветовом пространстве).

Неформатные стеганографические системы в любом случае вносят дополнительные искажения в контент, это дополнительно к квантованию и различным форматным преобразованиям важны чутье и чувство меры разработчиков (и пользователей) стеганографической системы.

В области стеганографии имеется на сегодня более 100 запатентованных решений.

Стеганография не имеет своего конкретного подкласса, поэтому патенты, связанные со стеганографией, встречаются в разных классах и даже разделах. В основном они сгруппированы по видам носителей (изображение, звук, свет, ДНК) или методам встраивания [7].

Среди авторов наибольшую заинтересованность проявляют крупные корпорации, занятые в сфере мультимедиа (например, Digimarc Corporation), а также правительственные организации.

Широкое применение стеганография получила в области цифровых водяных знаков (ЦВЗ) для защиты авторских прав. Наибольшую популярность получили неформатные методы стеганографии за большое количество подходящих контейнеров, за лучшее их использование и стойкость к возможным атакам.

3. Виды скрытности и стеганография.

Для защиты информации от несанкционированного доступа при ее передаче помимо шифрования рекомендуется использовать дополнительные способы защиты, такие как маскирование сигнала или скрытие самого факта передачи. Скрытием самого факта передачи информации занимается стеганография [2], маскированием сигналов более подробно занимаются в радиосвязи. С целью повышения безопасности передачи информации были исследованы различные виды скрытности [8,9].

Среди скрытностей сигналов различают пять основных видов: энергетическая, структурная, пространственная, временная и информационная скрытности.

Скрытность, зависящую от энергии сигнала, называют энергетической. Ее цель скрыть информационный сигнал среди передаваемых таким образом, чтобы его нельзя было выделить по энергетическому признаку. Так ШПС обладает высокой энергетической скрытностью, поскольку его энергетический уровень меньше шумового, что делает его отделение от шума очень трудоемким.

Энергетическая скрытность определяется неспособностью противника отличить полезный сигнал от шума по уровню и мощности сигнала.

Энергетическая скрытность — это основной показатель скрытности, так как в случае абсолютного значения противник не выявит сам факт передачи сообщения.

Цель стеганографии обеспечить "абсолютную" энергетическую скрытность. Модифицируя контейнер, основные показатели уровня и мощности сигнала кардинально не изменяются, что позволяет говорить о том, что стеганография обеспечивает "абсолютную" энергетическую скрытность

Скрытность, зависящую от структуры передаваемого сигнала, называют структурной или алгоритмической. Она задает правило, по которому из переданного сигнала можно извлечь нужную информацию.

Структурная скрытность определяется сложностью для противника отделения полезного сигнала от шума.

Роль структуры играет расширение или формат файлов. Стеганография использует для скрытия как форматную так и неформатную части файлов и скрытность определяется только методом стеганографического скрытия.

Пространственная скрытность определяется неизвестностью для противника последовательности использования спектра для передачи сигнала.

Стеганографическое скрытие применяется по всему контейнеру (контейнер изначально больше сообщения), тем самым обеспечивается и статистическое выравнивание и пространственная скрытность.

Временная скрытность сигнала определяется неосведомленнос-

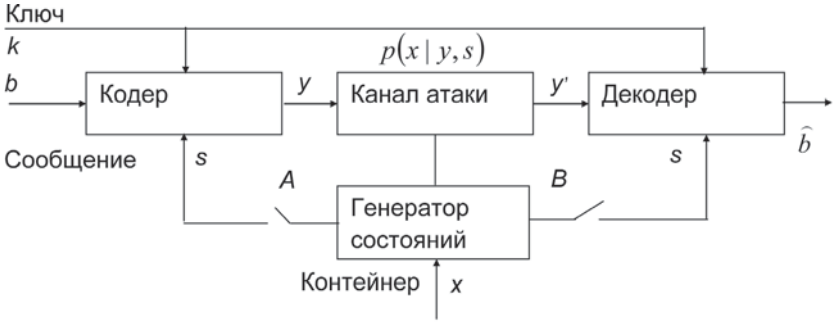

Рис. 1. Представление стеганосистемы как системы связи с пере-дачей дополнительной информации

тью противника о моментах передачи полезного сигнала.

Стеганографическое скрытие информации возможно в различные контейнеры и в разной последовательности это и определяет временную скрытность

Информационная скрытность предназначена для скрытия истинного смысла сообщения от противника

Стеганография не отрицает элементы криптографии поэтому встраиваемое сообщение шифруется для большей надежности. Также "абсолютная" энергетическая скрытность стеганографии вносит дополнительную информационную скрытность.

Методы скрытия информации (в стеганографии)

Разновидности скрытия	Комментарий
Энергетическое	Модификация контейнера не меняет его энергетическую составляющую
Структурное	Определяется методом скрытия
Информационное	Шифрование как дополнительная защита
Пространственное	Встраивание информации по всему контейнеру
Временное	Встраивание информации в определенные контейнеры

О теории скрытности по З.М. Каневскому. В [8] З.М. Каневский затронул такие темы как: разведка, маскировка, оценка скрытности. Он понимал под скрытностью состояние объекта, которое скрыто во множестве себе подобных, и предлагает оценивать скрытность в двоичных измерениях — Дизах. Скрытность характеризует затраты (времени, средств), необходимые для выявления реасобытия с заданной достоверностью. В оценке скрытности объекта используется два подхода. В первом (вероятностном) скрытность определяется как вероятность успешного выявления реасобытия в заданное время. Второй подход предполагает оценивать скрытность объекта через затраты на выявление его состояния с заданной достоверностью. В.И. Тупота в [9] рассматривает скрытность сигналов средств радиосвязи и предлагает использовать конечные поля для решения фундаментальных вопросов помехозащищенности, направленных на обеспечение информационной, структурной и энергетической скрытности. Но он связывает скрытность с кодированием. В частности именно В.И. Тупота предлагает классифицировать скрытность на информационную, структурную и энергетическую.

Скрытность как оценка качества стеганосистемы. Стеганографическая система (стеганосистема) позволяет встраивать секретную информацию в цифровой носитель (контейнер), скрывая сам факт ее наличия. С другой стороны встраивание любой информации вносит дополнительные изменения в контейнер и тем самым сказывается на его качестве. Оценка количества вносимых изменений позволяет говорить об оценке качества стеганосистемы.

В большинстве случаев в качестве контейнера в силу своей избыточности выступает аудиовизуальный материал (изображение, видео, звук), который оценивается человеком, поэтому оценка качества стеганосистемы выходит на первый план. Основная характеристика стеганосистемы — уровень скрытности. Он определяет насколько модифицированный контейнер отличается от исходного. Уровень скрытности можно оценить аналитическими исследованиями или стеганоанализом. Хорошо известны следующие тесты:

— статистические (тесты на запрещенные символы, 2 , на длину цикла и т.д.);

— эмпирические (проверка на монотонность, "покер-тестом", тестом "собирателя купонов"; проверка серий, частот, перестановок, интервалов);

— спектральные тесты.

Для изображений и видео существуют показатели искажения, с помощью которых оценивают искажения, вносимые стеганосистемой. Их можно разделить на две группы: разностные показатели искажения, основывающиеся на отличии пустого и заполненного контейнеров и корреляционные показатели искажения, основанные на корреляции между оригинальным и искаженным сигналами. Одним из наиболее часто применяемых показателей для оценки уровня искажения является соотношение "сигнал/шум", вычисленное в децибелах.

Таким образом, оценка уровня скрытности позволяет оценить качество стеганосистемы [10].

Литература

1. **Бугаев В.С., Петраков А.В.** Новые возможности результатов исследования статистики длительности телекиносюжетов (сжатие и стеганография)//Труды 15-й Всероссийской научно-технической конференции "Современное телевидение" (март 2007 г.). — М.: ФГУП МКБ "Электрон", 2007. — С. 17-20.

2. **Грибунин В.Г., Оков И.Н., Туринцев И. В.** Цифровая стеганография. — М.: СОЛОН-Пресс, 2002. — 272 с.

3. **Романцов А.П., Бугаев В.С., Фролов М.А.** Комплекс лабораторных работ по стеганографии / Под редакцией Заслуженного деятеля науки РФ, д.т.н., профессора А.В. Петракова. — М.: РИО МТУСИ, 2005. — 92 с.

4. **Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В.** Основы компьютерной стеганографии: Учебное пособие для вузов. — М.: Радио и связь, 2003. — 152 с.

5. **Конахович Г.Ф. Пузыренко А.Ю.** Компьютерная стеганография. Теория и практика. — Киев: "МК-Пресс", 2006. — 288 с.

6. **Петраков А.В., Романцов А.П., Бугаев В.С.** Место стеганографии в преобразованиях цифрового телевидения//Труды 14-й всероссийской научно-технической конференции "Современное телевидение" (март 2006 г.). — М.: ФГУП МКБ "Электрон", 2006. — С. 23-26.

7. **Бугаев В.С., Петраков А.В.** О классификации и разнообразии патентов по стеганографии//Технологии информационного общества: Тезисы докладов московской отраслевой научно-технической конференции. — М.: Инсвязьиздат, 2007. — С. 136-137.

8. **Каневский З.М., Литвиненко В.П.** Теория скрытности. — Воронеж: Изд-во ВГУ, 1991. — 144 с.

9. **Тупота В.И.** Адаптивные средства защиты информации в вычислительных сетях. — М.: Радио и связь, 2002. — 176 с.

10. **Бугаев В.С., Петраков А.В.** О взаимозависимости избыточности и скрытности в элементах стеганографии//Труды Международной конференции "Телекоммуникационные и вычислительные системы" (МФИ-2008). — М.: Инсвязьиздат, 2008. — С. 212-217.