

ГРАФИЧЕСКИЕ СТЕГОКОНТЕЙНЕРЫ

С.С. Кувшинов, Н.Н. Прохожев

Научный руководитель – О.В. Михайличенко

В работе предлагаются подходы к реализации задачи скрытой передачи данных с помощью неподвижных изображений. Эти подходы базируются на использовании особенностей системы человеческого зрения и избыточности визуальной информации. Освещены вопросы встраивания сообщений в графические стегоконтейнеры, а также проблема выбора конкретного контейнера для того или иного объема информации. Также приводится пример одного из алгоритмов встраивания.

Введение

Как известно, цель криптографии состоит в сокрытии содержания секретных сообщений. Стеганография идет принципиально дальше. Ее задача – скрыть от непосвященных сам факт существования сообщений. Такие скрытые сообщения могут включаться в различные внешне безобидные данные, вместе с ними храниться и передаваться без всяких подозрений со стороны. Эти данные – контейнеры стеганографических сообщений – могут иметь разнообразную природу. Для цифровой стеганографии это, прежде всего, файлы различных мультимедийных форматов (форматов изображений, музыкальных форматов, форматов видео и т.д.).

Возможность встраивания информации в изображения основана на факте некоторой избыточности визуальной информации. Цифровые фотографии (как и цифровая музыка, цифровое видео) представляются матрицами чисел, которые кодируют интенсивность сигналов в дискретные моменты в пространстве и/или времени. В нашем случае, контейнер (изображение) – матрица чисел, представляющих интенсивность света в определенный момент времени. Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия изображения человеческим глазом, что и дает возможность скрытия в графическом файле нужной нам информации. С другой стороны, некоторые форматы изображений (JPEG) можно рассматривать как структуры, в которых для уменьшения объема информации для хранения точек используются зависимости, корреляции между близко расположенными друг к другу областями изображения.

Возникает два пути, по каждому из которых можно пойти при решении рассматриваемой задачи. Цель работы – рассмотрев особенности этих принципов, показать обоснованности применимости того или иного решения в конкретной ситуации.

Система человеческого зрения

Свойства системы человеческого зрения (СЧЗ) можно разделить на две группы: низкоуровневые («физиологические») и высокоуровневые («психофизиологические»). Выделяют три наиболее важных низкоуровневых свойства, влияющих на заметность постороннего шума в изображении:

- чувствительность к изменению яркости изображения;
- частотная чувствительность;
- эффект маскирования.

Чувствительность к изменению яркости можно определить следующим образом [1]. Испытуемому показывают некоторую однотонную картинку (рис. 1а). После того, как глаз адаптировался к ее освещенности I , «настроился на нее», постепенно изменяют яркость вокруг центрального пятна. Изменение освещенности ΔI продолжают до тех пор, пока оно не будет обнаружено. На рис. 1б показана зависимость минимального контраста $\Delta I / I$ от яркости I (для удобства изменено привычное расположение осей). Как видно из рисунка, для среднего диапазона яркости контраст примерно постоянен,

тогда как для малых и больших яркостей значение порога неразличимости возрастает. Было установлено, что $\Delta I \approx 0.01 - 0.03I$ для средних значений яркости. Результаты исследований показывают, что при малых значениях яркости СЧЗ порог неразличимости уменьшается, т.е. СЧЗ более чувствительна к шуму в этом диапазоне.

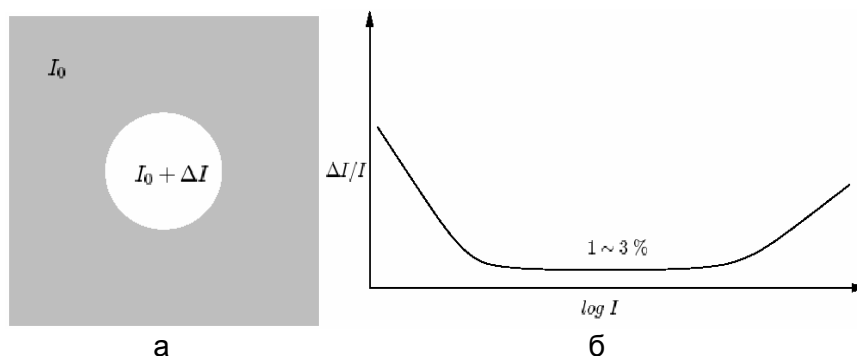


Рис. 1. Чувствительность к контрасту и порог неразличимости ΔI

Частотная чувствительность СЧЗ проявляется в том, что человек гораздо более восприимчив к низкочастотному (НЧ), чем к высокочастотному (ВЧ) шуму. Можно показать, что частотная чувствительность тесно связана с яркостной. Известно также и выражение для определения порога маскирования на основе известной яркостной чувствительности, что позволяет найти метрику искажения изображения, учитывающую свойства СЧЗ. Такого типа математические модели хорошо разработаны для случая квантования коэффициентов дискретного косинусного преобразования изображения, так как именно оно применяется в стандарте JPEG.

Эффект маскирования в пространственной области может быть объяснен путем построения стохастических моделей изображения. При этом изображение представляется в виде марковского случайного поля, распределение вероятностей которого подчиняется, например, обобщенному гауссовскому закону.

Таким образом, можно предложить следующую обобщенную схему внедрения данных в изображение, которую так или иначе используют многие алгоритмы встраивания информации:

- Выполнить фильтрацию изображения при помощи ориентированных полосовых фильтров. При этом получим распределение энергии по частотно-пространственным компонентам.
- Вычислить порог маскирования на основе знания локальной величины энергии.
- Масштабировать значение энергии внедряемого ЦВЗ в каждом компоненте так, чтобы оно было меньше порога маскирования.

Высокоуровневые свойства СЧЗ пока редко учитываются при построении стегоалгоритмов. Основными из этих свойств являются:

- чувствительность к контрасту (высококонтрастные участки изображения, перепады яркости обращают на себя значительное внимание);
- чувствительность к размеру (большие участки изображения «заметнее» меньших размером). Существует порог насыщения, когда дальнейшее увеличение размера не существенно;
- чувствительность к форме (длинные и тонкие объекты вызывают большее внимание, чем круглые и однородные);
- чувствительность к цвету (некоторые цвета, например красный, «заметнее» других) Эффект усиливается, если фон заднего плана отличается от цвета фигур на нем;
- 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);
- чувствительность к внешним раздражителям (движение глаз наблюдателя зависит от конкретной обстановки, от полученных им перед просмотром или во время него инструкций, дополнительной информации).

Встраивание сообщения в незначащие биты контейнера

Цифровые изображения представляют собой матрицу пикселей. Пиксель – это единичный элемент изображения, имеющий фиксированную разрядность двоичного представления. Например, пиксели полутонового изображения кодируются 8 битами (значения яркости изменяются от 0 до 255).

Младший значащий бит (LSB) изображения несет в себе меньше всего информации. Известно, что человек обычно не способен заметить изменение в этом бите. Фактически он является шумом, поэтому его можно использовать для встраивания информации. Таким образом, для полутонового изображения объем встраиваемых данных может составлять 1/8 объема контейнера. Например, в изображение размером 512×512 можно встроить 32 килобайта информации. Если модифицировать два младших бита (что также почти незаметно), то можно скрытно передать вдвое больший объем данных.

Достоинства рассматриваемого метода заключаются в его простоте и сравнительно большом объеме встраиваемых данных. Однако он имеет серьезные недостатки. Во-первых, скрытое сообщение легко разрушить. Во-вторых, не обеспечена секретность встраивания информации. Нарушителю точно известно местоположение всего ЦВЗ. Для преодоления последнего недостатка было предложено встраивать ЦВЗ не во все пиксели изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известным только законному пользователю. Пропускная способность при этом уменьшается. Рассмотрим подробнее вопрос выбора пикселей изображения для встраивания в них скрытого сообщения.

Встраивание

Характер поведения младшего значащего бита изображений чаще всего неслучаен. Скрываемое сообщение не должно изменять статистики изображения. На практике обычно ограничиваются поиском пикселей, модификация которых не вносит заметных искажений в изображение. Затем из этих пикселей в соответствии с ключом выбираются те, которые будут модифицироваться. Скрываемое сообщение шифруется с применением другого ключа. Этот этап может быть дополнен предварительной компрессией для уменьшения объема сообщения.

Рассмотрим пример – обработка изображения в формате BMP [3]. Если взять картинку, лучше всего TrueColor в 24-х битном формате, и изменить по какому-то известному только нам принципу младшие значащие биты цвета, то на глаз разница между исходным и полученным изображениями не будет заметна. 24 бита – очень удобный формат хранения информации об изображении, при таком представлении за один цветовой канал отвечает отдельный байт. Внедрение может осуществляться так.

1. Берем сообщение и предварительно подготавливаем его – шифруем и пакуем. Этим достигаются сразу две цели – повышение КПД и увеличение стойкости системы. В начало для удобства можно записать сигнатуру метода, что не секретно, зато просто.
2. Берем контейнер и внедряем в его младшие биты подготовленное сообщение любым удобным для нас способом, например, раскладываем упакованное сообщение

в битовую последовательность и заменяем избыточные биты (НЗБ) контейнера битами сообщения.

Надежность такого внедрения прямо пропорциональна соответствию характера распределения НЗБ в контейнере и сообщении. А распределения эти в подавляющем большинстве случаев совпадать не будут. В некоторых случаях это будет визуально заметно на картинке, построенной из одних только младших битов контейнера. Например, берем и картинку и внедряем в нее информацию (см. рис. 2).



Рис. 2. Визуальный анализ изображения

При помощи простой утилиты, показывающей картинку побитно (т.е. только интересные нас биты нужных цветовых компонентов) видно внедрение данных, т.е. файл внедрения легко определить. Конечно, для большинства наблюдателей достаточно и того, что «на глаз не видно», но слабые места своей защиты надо знать.

Особенности BMP контейнеров

Все BMP контейнеры можно разделить на два класса: «чистые» и зашумленные [3, 5]. В «чистых» картинках прослеживается связь между младшим битом и остальными 7-ю битами элементов цвета, а также существенная зависимость самих младших битов между собой. Внедрение сообщения в «чистую» картинку разрушает существующие зависимости, что видно из рис. 3. Если же картинка зашумлена (например, получена со сканера или фотокамеры), то определить вложение становится на порядок сложнее. Различить, какой контейнер попал вам под руку, можно тоже побитным просмотром картинки. Например, сканированное изображение, в которое ничего не внедрялось, показано на рис. 3.

Объясняется это шумом матрицы сканера (или цифровой камеры). Следует сказать, что просмотром и анализом распределения НЗБ иногда очень просто определить факт компьютерной обработки (подчистки) картинки (рис. 4 – изображение без внедрения, рис. 5 – то же изображение, но с внедрением). Четко видна граница между «своим» шумом и шумом, возникшим в результате внедрения сообщения. Отсюда вытекает еще одно необходимое правило – всегда нужно распределять биты сообщения по всем младшим битам контейнера (например, внедрять не последовательно, а в каждый 2-й, 3-й и т.д. НЗБ) или же дополнять чем-то (шумом с тем же законом распределения) длину сообщения так, чтобы она стала равна объему НЗБ контейнера. Еще одно интересное решение – подбор картинки под сообщение: из множества имеющихся картинок подобрать такую, которая исказится менее всего при внедрении сообщения.

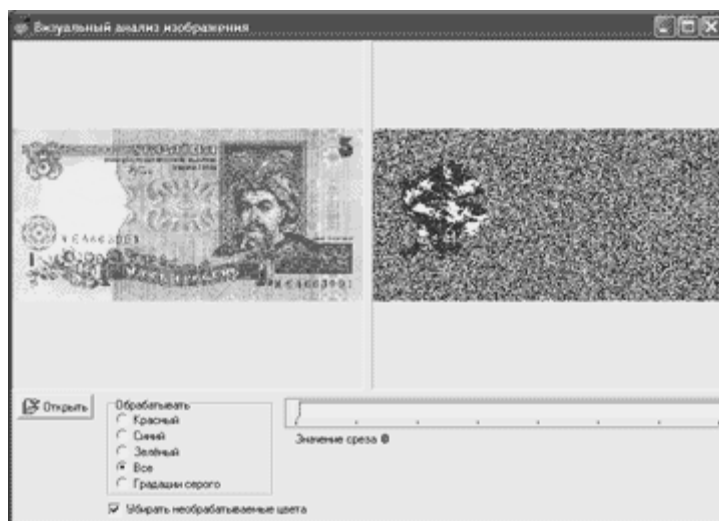


Рис. 3. Отсканированное изображение

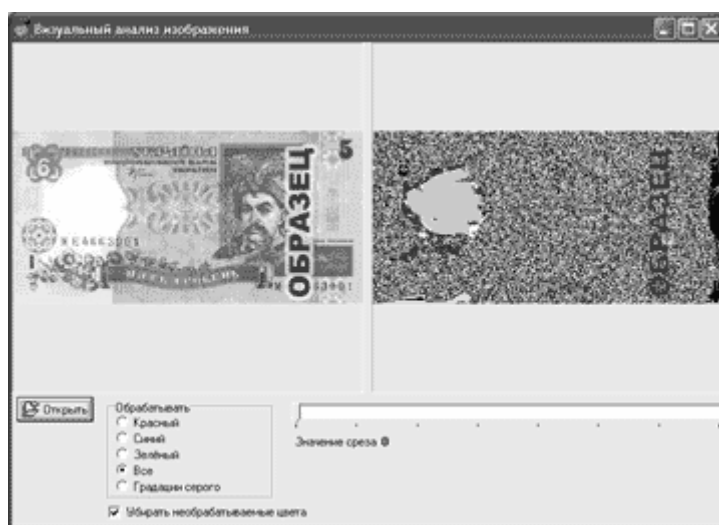


Рис. 4. Изображение без внедрения сообщения

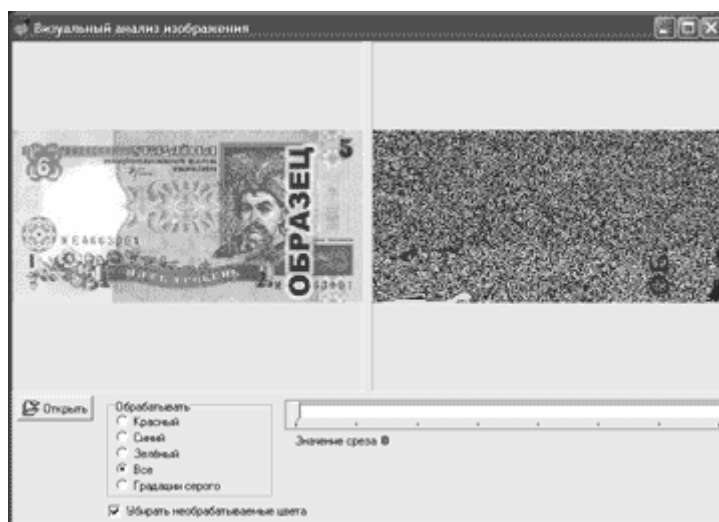


Рис. 5. Изображение с внедренным сообщением

Ситуация с форматом JPEG

Другим популярным методом встраивания сообщений является использование особенностей форматов данных, использующих сжатие с потерей данных (например, JPEG). Этот метод (в отличие от LSB) более стоек к геометрическим преобразованиям и обнаружению канала передачи, так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения.

Если в случае BMP нас интересовали младшие биты градаций серой шкалы или RGB-значений при цветном изображении, то в формате JPEG речь пойдет о другом виде информационной избыточности.

JPEG – формат, в котором для уменьшения объема информации для хранения точек используются зависимости, корреляции между близко расположенными друг к другу областями изображения [2].

Стандарт сжатия JPEG является в настоящее время наиболее распространенным и своеобразным «benchmark`ом» для алгоритмов цифровых водяных знаков (ЦВЗ) (т.е. устойчивость системы ЦВЗ к сжатию JPEG проверяется обычно в первую очередь). В соответствии с этим стандартом изображение разбивается первоначально на блоки 8×8 элементов, к каждому из которых применяется дискретное косинусное преобразование (ДКП). Назначением ДКП является перераспределение энергии: значимые коэффициенты группируются в левом верхнем углу квадрата спектральных коэффициентов, так как соседние пикселы изображения коррелированы. Далее следуют равномерное табличное квантование коэффициентов, кодирование длин серий и кодирование Хаффмана.

Вейвлет-преобразование, также как и ДКП, перераспределяет энергию изображения. Эта компактность энергии ведет к эффективному применению скалярных квантователей. Однако они не учитывают остаточную структуру, сохраняющуюся в вейвлет-коэффициентах, в особенности высокочастотных субполос. Современные алгоритмы сжатия тем или иным образом используют эту структуру для повышения эффективности сжатия.

Алгоритм встраивания “F5”

Данный алгоритм встраивает биты сообщения в произвольным образом выбираемые коэффициенты ДКП [4]. Для его реализации необходимо определить:

1. качество стегопосылки;
2. изображение-контейнер;
3. выходной файл;
4. файл с сообщением;
5. пароль для встраивания.

Процесс встраивания состоит из 6 следующих шагов:

1. получение RGB-представления изображения-контейнера;
2. расчет таблицы квантования исходя из требования качества стегопосылки, сжатие изображения путем сохранения значений ДКП-коэффициентов;
3. преобразование изображения в сигнал с нулевым средним и определенной дисперсией так, чтобы абсолютные значения коэффициентов ДКП находились в диапазоне (200, 250);
4. определение распределения битов сообщения по коэффициентам с использованием указанного пароля;
5. разделение сообщения на сегменты по k бит, которые встраиваются в небольшие по размеру блоки коэффициентов ДКП изображения. Этот процесс имеет то преимущество, что при этом существует возможность адаптации к локальной яркости и

гладкости изображения. Однако при достаточной энергии встраиваемых битов появляется эффект блочности;

6. оценка результата. Если длина сообщения укладывается в оцененную размерность, встраивание прошло успешно. В противном случае возникает ошибка переполнения контейнера.

Заключение

Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к ней будет усиливаться все больше и больше. Сильнейшим катализатором этого процесса является лавинообразное развитие Internet, в том числе такие нерешенные проблемы, как защита авторского права, защита прав на личную тайну, организация электронной торговли, компьютерная преступность и кибертерроризм.

Очевидно, цифровые изображения будут еще очень долгое время применяться в качестве стегоконтейнеров, поскольку цифровые фотографии распространены повсеместно, и обмен файлами такого типа – весьма распространенное действие, чтоб вызывать подозрения факта скрытой передачи информации.

Наиболее перспективными являются алгоритмы, приспособленные для работы с файлами JPEG и JPEG 2000. Эти форматы допускают сжатие за счет избыточности визуальной информации, основанной на корреляции соседних областей изображения. В этом случае изображение рассматривается как сигнал, который может подвергаться преобразованиям Фурье, вейвлет-преобразованиям, дискретному конусному преобразованию.

Литература

1. Воробьев В.И., Грибунин В.Г. Теория и практика вейвлет-преобразования. Учебное пособие. СПб.: ВУС, 1999. 204 с.
2. Грибунин В.Г. Цифровая стеганография. СПб.: Солон-Пресс, 2002. 272 с.
3. Стеганография. Особенности использования программ на основе метода наименьшего значащего бита, URL <http://www.compdoc.ru/secur/crypt/steganografiya/>
4. Fridrich J., Goljan M., Hoge D. Steganalysis of JPEG Images: Breaking the F5 Algorithm <http://www.ws.binghamton.edu/fridrich/Research/f5.pdf>.
5. Основные положения стеганографии, URL <http://www.citforum.ru/security/articles/stegano.shtml>