

УДК 004.932.2

ОСОБЕННОСТИ ОЦЕНКИ СОДЕРЖИМОГО СЖАТОГО ВИДЕОПОТОКА

П. С. Санкин¹,

аспирант

М. Ю. Литвинов²,

соискатель

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Вводятся понятия первичной и вторичной информации применительно к цифровым изображениям. Рассматриваются особенности проявления вторичной информации в последовательностях сжатых изображений.

Ключевые слова — свойства изображений, маскирование изображений, JPEG.

Введение

В наше время наблюдается постоянный рост объема обрабатываемой информации, в результате чего становится все труднее с ней работать. Кроме того, появляются новые виды информации, эффективных алгоритмов анализа которой еще не существует. К ним можно отнести и цифровой видеопоток. В данной работе рассмотрена уязвимость потоков видеоинформации, передаваемых внутри систем видеоконтроля.

В многофункциональных системах регистрации существует проблема передачи графической информации между элементами системы. Для передачи телевизионного сигнала в системах видеоконтроля могут использоваться как проводные каналы связи, так и беспроводные — радиоканал или ИК-канал. Для передачи сигнала на большие расстояния применяют видеосушители и модемы (передатчики-модуляторы и приемники-демодуляторы). При этом видеосигнал с помощью специальной аппаратуры преобразуется, запоминается и передается в линию связи. Время передачи может составлять от долей секунды до ми-

нуты, в зависимости от требований к качеству «картинки». В настоящее время наиболее широко используются три системы передачи изображений по цифровым линиям [1]:

1) с компрессией изображений по принципу «условного обновления» (CR), предназначенные для передачи только информации об изменении изображения от кадра к кадру;

2) с MPEG-компрессией, где используют специальные алгоритмы компрессии изображений движущихся объектов;

3) с JPEG-компрессией, обеспечивающие независимое сжатие кадра изображения.

Современные системы передачи ориентированы на использование цифровых технологий и уменьшение за счет их загрузки канала. Зачастую данные могут передаваться по сетям общего пользования как проводным, так и беспроводным, что накладывает дополнительные требования к конфиденциальности информации. Как правило, данные передаются в маскируемом виде, при этом метод кодирования значительно не изменяет размера маскируемого файла или битовой скорости его передачи.

Изображения и форматы данных

Различают несколько классов изображений [2], которые обладают своими особенностями. Классификация основывается на размере палитры, а также на внешних характеристиках областей изображения.

1. Деловая графика (большие области одного цвета, плавные и резкие переходы, мало цветов).

¹ Научный руководитель — доктор техн. наук, профессор, заведующий кафедрой безопасности информационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения *Е. А. Крук*.

² Научный руководитель — доктор техн. наук, профессор, заведующий кафедрой вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения *М. Б. Сергеев*.

2. Фотореалистичные изображения (большое количество цветов $\sim 2^{16}$, плавные переходы).

3. Фотореалистичные изображения с наложением деловой графики (например, логотипа, даты, времени и другой служебной информации).

Эти особенности должны учитываться при разработке алгоритмов защищенного кодирования и не должны приводить к снижению качества маскирования видеoinформации. По характеру можно выделить два основных типа изображений — статические (картинки) и динамические (видео).

Формат предполагает структурированное описание изображения в цифровой форме. Это позволяет упростить отображение графики и видео в вычислительной технике. Можно выделить два основных типа форматов, характеризующихся объемом данных, — сжатые и несжатые.

К несжатым относятся форматы, которые хранят в себе структурированные данные, позволяющие упростить отображение графики и видео в вычислительной технике. Информация, как правило, хранится попиксельно, типичным примером является формат BMP.

Изображения и видео обладают большой избыточностью, поэтому для уменьшения объема передаваемой информации применяют сжатие. Изображение может сжиматься целиком (формат РСХ) либо блоками (формат JPEG). Сжатие графических данных возможно без потерь или с потерями. Большинство методов кодирования видео для достижения эффекта сжатия используют два типа избыточности — временную и пространственную. Во временной области имеется значительная корреляция между видеокадрами, зафиксированными в близкие моменты времени. Смежные по времени кадры имеют высокую степень корреляции, особенно при высокой частоте кадров. В пространственной области также наблюдается высокая зависимость величин пикселей, лежащих близко друг к другу.

Наибольшее распространение получили методы компрессии видео и изображений с потерей качества, которые основаны на психовизуальных особенностях зрительной системы человека и позволяют достичь высоких степеней сжатия.

Не всегда применение сжатия дает уменьшение размера файла (по сравнению с несжатым форматом), неоптимальные условия и неправильный выбор алгоритма могут дать увеличение объема.

Типы информации

Первичная информация

Под первичной мы будем понимать информацию, характеризующую саму картинку независимо от формата данных. При рассмотрении ра-

стровых изображений это будут массивы пикселей. По ним можно охарактеризовать фон, контуры и границы объектов, произвести поиск объектов и распознавание их образов.

Первичная информация нашла свое отражение в растровых форматах, не использующих сжатие, например BMP.

Понятие вторичной информации.

Особенности сжатия данных

Под вторичной мы будем понимать информацию, по которой не прямо, а косвенно можно охарактеризовать изображение. Применительно к цифровым данным такой информацией будет размер файла и статистические данные, связанные со структурой файла.

Для защиты от раскрытия информации об изображении по размеру передаваемых данных предлагается перед маскированием дописывать к коротким кадрам случайную информацию, это позволит поддерживать размер передаваемых кадров на постоянном уровне. В то же время потребуются следить за максимальным размером кадра и обрезать лишнее, как правило, эта обязанность возложена на кодер. Основная стратегия сокрытия — поддержание некоего постоянного эффективного размера кадра.

Для форматов, не использующих сжатие данных, по вторичной информации можно определить физические размеры изображения при наличии знаний об объемах данных, необходимых для описания заголовка и одного пикселя.

У сжатых форматов такого недостатка нет, так как степень сжатия заранее не известна.

Однако если рассматривать последовательность из нескольких изображений, полученных из одного источника и имеющих одинаковые размеры, можно выделить следующие особенности:

- 1) применение форматов без сжатия даст нам несколько одинаковых порций данных;
- 2) при сжатии абсолютно одинаковые изображения будут иметь одинаковый размер;
- 3) в зависимости от графической сложности (избыточности) изображения при сжатии размер файла будет изменяться.

Таким образом, в случае применения покадрового сжатия изображений с видеоканеры можно получить файлы кадров разной длины. Это связано с такой особенностью подавляющего большинства сжатых форматов, как отсутствие возможности задавать строго определенную степень сжатия. В них задается верхняя граница степени сжатия, а нижней не придается значение — в результате изображения разных классов будут иметь разный размер.

Применение других стратегий сжатия также дает появление вторичной информации. Основным

параметром для анализа данных при их передаче с камеры будет являться битовая скорость [3], напрямую связанная с частотой кадров. Паузы между порциями данных, возникающие при неполной загрузке канала, дают возможность отделить один кадр от другого. Изменение размера порций данных характеризует работу кодера при удалении определенной избыточности в исходном материале. При этом объем соседних порций данных может незначительно различаться (например, по причине внутренних шумов видеокамеры), поэтому для получения информации о характере изображения необходимо проводить анализ кадров, немного отстоящих друг от друга. Таким образом, можно провести анализ любого сжатого видеопотока на наличие в нем вторичной информации.

Применение маскирования изменяет общий характер и распределение сжатых данных, что позволяет определить сам факт маскирования, однако не мешает провести анализ вторичной информации. В системах видеонаблюдения такая информация даст возможность сделать выводы о наличии или отсутствии движения в наблюдаемой области, о ее освещенности и контрастности, что крайне нежелательно.

Возможные методы анализа вторичной информации

Рассмотрим возможные методы анализа вторичной информации, остающейся после выполнения процедуры маскирования изображения, применяя для этого классические уровни атак.

1. Анализ без использования какой-либо дополнительной информации.

В этом случае, используя доступную, преобразованную в результате процедуры маскирования видеoinформацию, можно оценить насыщенность передаваемого изображения или наоборот однотонность изображения и отсутствие большого числа различных фрагментов. Например, легко определить, имеем ли мы дело с видеofрагментом, представляющим хорошо освещенную сцену со множеством деталей, или это подвергнутый маскированию однотонный темный кадр. В первом случае размер маскированного кадра будет практически совпадать со стандартным размером видеоизображения, а во втором случае будет существенно меньше.

В качестве примера приведем стадии завершения рабочего дня в помещении, снятые IP-камерой видеонаблюдения (Genius IPCam Secure-300R). Для различных ситуаций парами показаны исходный и специально подготовленный кадр, заполненный аналогичным объемом случайных данных (рис. 1, а—г, см. с. 3 обложки). Заполнение шумом является моделированием маскированно-го файла с восстановленной заголовочной частью.

Наблюдается блоковый шум и зависимость числа блоков от размера файла. Настройки камеры во время работы были неизменными: разрешение 640×480 точек, степень сжатия — максимальная. Типичные кадры имеют следующие размеры, Б:

- ярко освещенное помещение — 26 150;
- в основном помещении погашен свет — 11 208;
- в дальнем помещении свет погашен — 8 990;
- освещение отключено — 6 950.

2. Анализ при использовании пар исходного и маскированного изображения.

При возможности получить доступ к большому числу разнообразных обработанных и исходных видеofрагментов можно более точно провести классификацию маскированных изображений по их размеру, соотнеся размер анализируемого кадра формата JPEG и возможное исходное изображение. Так, например, имея набор кадров одного и того же места в различных ситуациях (наличие машин, людей или их полное отсутствие), можно с высокой степенью достоверности соотнести размер доступного маскированного кадра с ситуацией на месте, изображение которого передается. Пары кадров с различной активностью в помещении представлены на рис. 2 (см. с. 3 обложки).

Размер файла кадра в первом случае составил 28 011 Б, а во втором — 26 495 Б и 7,1 и 1,3 % соответственно относительно размера изображения пустого помещения.

3. Анализ по выбранному исходному изображению.

Эффективность и оперативность анализа вторичной информации существенно повышаются, если интересует только наличие или отсутствие конкретной ситуации на месте, маскированное изображение которой удалось получить.

Следует также отметить, что при анализе вторичной информации могут использоваться два подхода. Так как маскированные, т. е. фактически случайные данные стандартным декодером декодируются и отображаются без ошибок, возможен визуальный анализ по непрорисованной части изображения. Второй подход — детальный разбор каждого блока MCU (Minimum Coded Unit), входящего в кадр, без визуального сравнения и анализа бит, требуемых для заполнения кадра.

Вторичная информация в JPEG и MJPEG

Формат JPEG предназначен для описания отдельных изображений, он не предусматривает однозначного предсказания размера файла после сжатия. Таким образом, размер файла будет нести вторичную информацию об общих характеристиках изображения.

Иллюстрации к статье П. С. Санкина, М. Ю. Литвинова «Особенности оценки содержимого сжатого видеопотока», с. 45–48

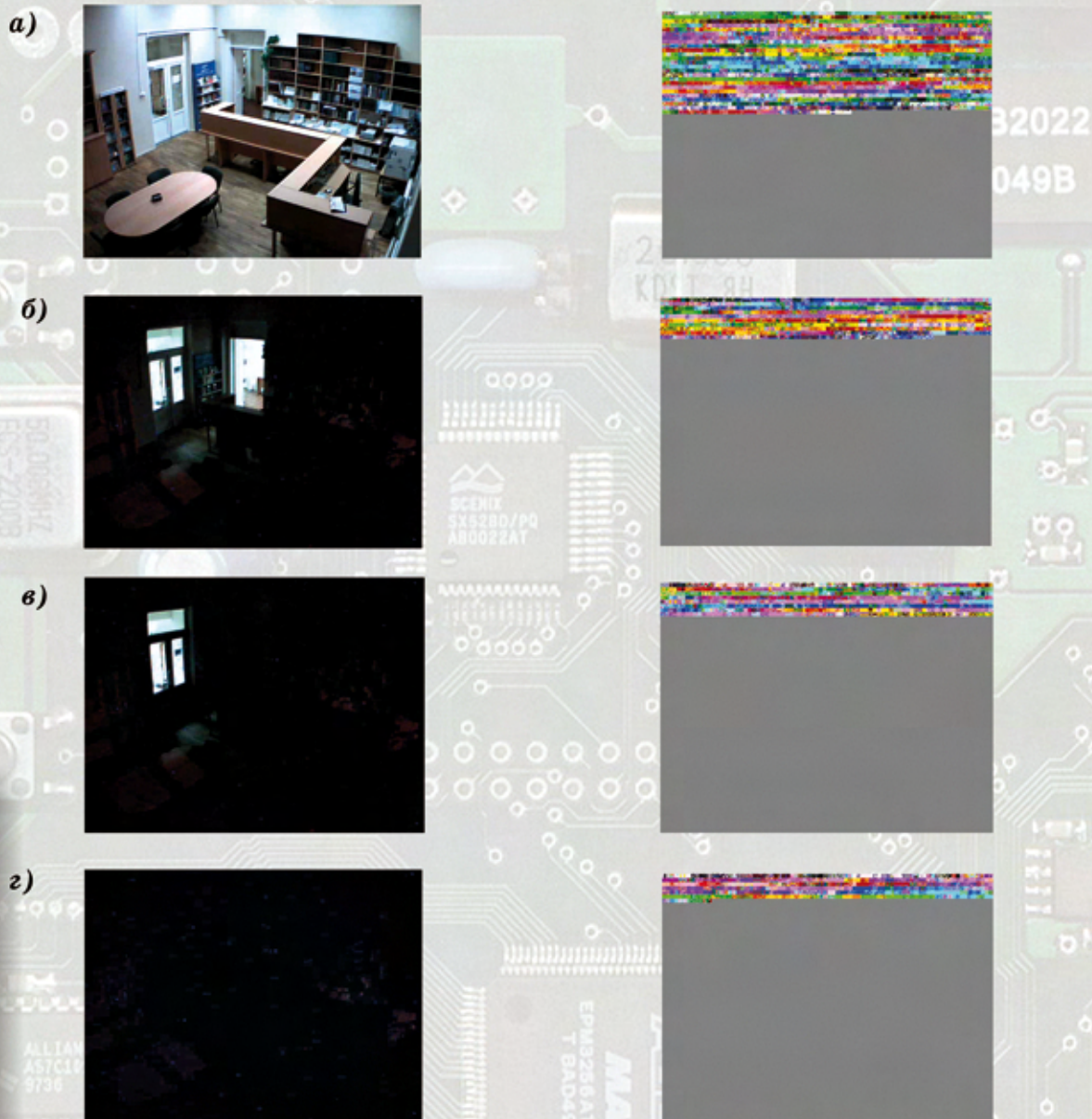


Рис. 1. Освещенность помещения: а – ярко освещенное помещение; б – в основном помещении погашен свет; в – в дальнем помещении свет погашен; г – освещение отключено



Рис. 2. Активность в помещении: а – высокая; б – низкая

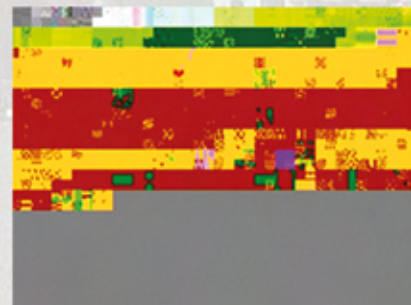


Рис. 3. Маскированный кадр JPEG

Другим распространенным форматом в системах видеонаблюдения является MJPEG, который был разработан для подвижных видеоизображений. В его основе лежит сжатие JPEG. Фактически формат MJPEG рассматривает цифровой видеопоток как последовательность отдельных кадров, сжимаемых независимо друг от друга согласно схеме компрессии JPEG. Данный формат хорошо подходит для систем видеонаблюдения, так как в нем кадры обрабатываются по отдельности, что позволяет осуществлять быстрый покадровый поиск, получать качественные стоп-кадры и отображать покадровое видео с регулируемой скоростью воспроизведения. Таким образом, отдельные кадры в формате MJPEG будут обладать всеми особенностями JPEG-формата. Если пропустить видеопоток за некий фиксированный промежуток времени, зная частоту кадров, можно получить представление о среднем размере кадра в группе. Проведя несколько таких измерений, получим информацию об изменении размера кадров в потоке, следовательно, определим качественные изменения передаваемого видео.

Рассматривая кадр в формате JPEG, со стороны декодера можно представить его размер, измеряемый не только единицами информации (байтами), но и числом блоков данных. Их появление связано с тем, что JPEG является блоковым кодером, и данные в нем обрабатываются поблочко.

Согласно спецификации [4], формат JPEG имеет четкую структуру, определяемую маркерами, при этом блоки, содержащие данные, описывающие само изображение (scan), являются самыми крупными. Из-за использования энтропийного кодирования на последнем этапе сжатия данных итоговый размер этих блоков и степень сжатия изображения нельзя предсказать. Такая особенность позволяет проявиться вторичной информации.

Следует отметить, что маркеры в файле JPEG могут идти в различной последовательности и повторяться (например, для задания двух таблиц квантования). Несмотря на то что кодеры дают на выходе заголовки фиксированного размера, для вычисления его размера, т. е. длин всех маркеров, необходимо просмотреть файл и суммировать длины всех сегментов маркеров.

В изображении, до маскирования, сжатом по стандарту JPEG, при отображении проявляются однотонные полосы, которые периодически довольно резко меняют свой цвет. Кроме того, нередко при заданном разрешении изображения отображается не вся область, а только некоторая часть, пример такого изображения в укрупненном виде показан на рис. 3 (см. с. 3 обложки).

Для объяснения данных эффектов в маскированных (т. е. фактически для случайных) данных

необходимо подробно описать этапы разбора случайных данных кодером. JPEG является блоковым кодером, на выходе мы получаем блоковые искажения. Для рассмотрения интерпретации шума применительно к разбору JPEG-декодером блока MCU нужна математическая модель, описывающая средний размер MCU для случайных значений коэффициентов.

Заключение

В ходе работы были проведены анализ структуры JPEG-файлов, оценка поведения декодера при разборе шума. JPEG-декодер способен осмысленно разбирать шум, при этом искажение картинки будет блоковым. При разборе шума в теле JPEG-файла кодер сможет графически отобразить все данные при условии, что в них нет двухбайтовых блоков, похожих на маркер, т. е. начинающихся с FF и не содержащих 00. Возможно неполное отображение маскированной картинки, вероятно использование этой информации для анализа последовательностей изображений.

Качественные характеристики изображения влияют на размер конечного файла. Таким образом, существует возможность определять общие особенности картинки по изменению битовой скорости видеопотока. Резкое изменение скорости передачи данных с камеры видеонаблюдения может свидетельствовать о серьезном изменении картинки, например таком, как появление новых объектов или движение в наблюдаемой области, даже в том случае, когда сам поток передается в маскированном виде.

Литература

1. Р 78.36.002–99. Выбор и применение телевизионных систем видеоконтроля: Рекомендации / НИЦ «Охрана» ГУВО МВД России. М., 1999. 51 с.
2. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: Диалог—МИФИ, 2003. 384 с.
3. Санкин П. С. Особенности оценки содержимого видеопотока // Научная сессия ГУАП: Сб. докл. Ч. 1. Технические науки. СПб.: ГУАП, 2008. С. 132–134.
4. CCITT Rec. T.81 (1992 E) | ISO/IEC 10918-1 : 1993(E). Information technology — Digital compression and coding of continuous-tone still images: Requirements and guidelines. <http://www.w3.org/Graphics/JPEG/itu-t81.pdf>