

Буква Х стоит на позиции 23 ей соответствует расшифрованная буква, стоящая на позиции $15 \cdot (23 - 21) = 30 \equiv 4 \pmod{26}$. Буква, стоящая в алфавите на позиции 4, — это Е.

Буква К стоит на позиции 10, ей соответствует расшифрованная буква, стоящая на позиции $15 \cdot (10 - 21) = -165 \equiv 17 \pmod{26}$. Буква, стоящая в алфавите на позиции 17, — это R.

Расшифрованное слово – слово WATER.

Одним из существенных достоинств хорошего алгоритма шифрования является способность генерировать большое количество ключей. И шифр Цезаря, и аффинный шифр уязвимы для криптоанализа, поскольку максимальное количество ключей ограничено.

Если мы снимем какие-либо ограничения относительно порядка букв шифроалфавита, то потенциальное количество ключей резко возрастет. Количество ключей для стандартного алфавита из 26 символов (расположенных в произвольном порядке) составляет $26! = 403291461126605635584000000$, то есть более 403 септиллионов ключей.

ЛИТЕРАТУРА

1. Мир математики: в 40 т. Т. 2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. / Пер. с англ. — М.: Де Агостини, 2014. — 144с.
2. Свободная энциклопедия Wikipedia.

УДК004.932

Студ. А. Н. Зайцев
Науч. рук. асс. Т. Г. Шагова
(кафедра высшей математики, БГТУ)

СЖАТИЕ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ MRC-КОМПРЕССИИ

В современном мире человеку приходится работать с огромным количеством информации. И одной из ключевых проблем является сохранение всей информации на различных цифровых носителях. Так как объём данных растёт быстрее, чем вместимость накопителей, то сжатие данных является крайне актуальной темой.

В сфере документооборота это также актуально. Стандартом для сохранения документов в настоящий момент является формат PDF. К сожалению, PDF файлы имеют довольно большой объём. Поэтому и развиваются различные методы сжатия PDF документов.

В данной работе будет рассмотрен метод сжатия документов под названием MRC (Mixed Raster Content).

Технология MRC

MRC (Mixed Raster Content) — технология, которая основана на разделении изображения на различные слои, каждый из которых сжимается особым образом, после чего происходит сборка всех слоев в результирующее изображение и упаковка в PDF-документ.

Выделяют две разновидности MRC-компрессии — трёх- и четырёх- слойная. Трёхслойная MRC-компрессия разделяет входное изображение на три слоя: маска текста, маска цвета текста, фон.

Четырёхслойная MRC-компрессия разделяет входное изображение на четыре слоя: маска текста, маска цвета текста, маска внутренних изображений, фон.

Разделение на слои

Существуют различные подходы для разделения входного изображения на слои. Наиболее простым решением является использование бинаризации для выделения текста на изображении. Бинаризация может использоваться как глобальная (например, метод Отсу), так и адаптивная (локальный метод Отсу). Другой подход заключается в использовании специализированных сегментаторов, которые могут работать как на основе нейронных сетей, так и иметь более сложную реализацию. Качество данного подхода сильно зависит от качества сегментатора, однако оно сильно превосходит в сравнении с использованием бинаризации. Мною в качестве сегментатора была использована COS/CCC сегментация, разработанная университетом Purdue, штат Луизиана, США.

Сжатие слоёв

Как уже отмечалось ранее, сжатие каждого слоя проходит особым образом. К сожалению стандарт PDF поддерживает крайне ограниченное количество алгоритмов сжатия изображений. Поэтому выбор алгоритмов невелик.

Слой маски текста представляет собой бинарную маску, которая показывает, какие пиксели принадлежат тексту. Так как маска бинарная, то на каждый пиксель изображения достаточно 1 бита (для удобства реализации и уменьшения накладных расходов иногда используют 1 байт). Бинарную маску сжимают с помощью алгоритма JBIG2, который наиболее эффективен при сжатии бинарных изображений.

Слой цвета текста и слой фона являются цветными слоями, поэтому здесь мы обязаны использовать алгоритмы для сжатия цветных изображений. Рекомендуется использовать кодировщик Jpeg2000, который использует различные вейвлет-преобразования при

сжатии. Ещё одним методом сжатия данного слоя является уменьшение цветового пространства. В результате мы уменьшим необходимое количество байт для представления одного пикселя (размер цветового пространства выбирается индивидуально). Затем следует устранить на странице пустые области, так как основная часть страницы будет пустая после отделения слоя маски текста. Для устранения пустых областей подходят разные стратегии: заливка средним/медианным цветом, компрессия/декомпрессия при помощи вейвлет-преобразований (могут использоваться разные вейвлет-функции). Для слоя фона при устранении пустых областей могут использоваться алгоритмы для восстановления повреждённых фотографий. К сожалению, данные алгоритмы требуют довольно больших вычислительных мощностей. Также рекомендуется уменьшать размер цветовой маски в несколько раз с последующей записью в PDF-документ оригинального размер, чтобы при показе PDF-страницы слой был увеличен до исходного состояния. Коэффициенты уменьшения подбираются для каждого слоя эмпирическим путём.

Так как для областей, содержащих картинки, важно сохранение качества при сжатии, то слой внутренних картинок рекомендуется сжимать при помощи Jpeg2000 в режиме «без потери качества». Также могут использоваться «регионы интереса» (ROI, Regions of interest), которые позволяют сохранять качество изображения в определённых областях, пренебрегая качеством в других.

Сборка слоёв

После обработки слоёв нам следует создать результирующее изображение, которое будет показываться пользователю. Стандарт PDF позволяет не делать нам этого вручную, а просто в каждую страницу встраивать набор изображений, которые будут при рендеринге страницы автоматически приведены к нужным размерам и отрисованы в нужном порядке. Так что вся сборка состоит из правильной упаковки в PDF-страницу. Данное действие может производиться любой PDF-библиотекой для создания PDF-документов.

Производительность

Производительность – довольно важный аспект системы. В MRC производительность складывается из сегментации, обработки каждого слоя и упаковки в PDF-документ. Скорость работы сегментатора сильно зависит от самого сегментатора. Если в качестве метода сегментации мы будем использовать простую бинаризацию или простые детекторы границ (например, детектор границ Canny), то скорость работы будет достаточно высока. Если же использовать более точные и сложные методы (например, COS/CCC сегментатор), то это может стать «узким горлышком» при работе метода.

Производительность обработки слоёв снова же сильно зависит от того, какие методы обработки были выбраны. Уменьшение размера изображения не занимает много времени (даже при использовании бикубического сглаживания). Вычисление среднего/медианного цвета тоже выполняется быстро. Чуть больше времени занимает метод заливки, основанный на вейвлет-преобразованиях. Но эти методы можно ускорить, используя методы многопоточного программирования или вычисления на основе GPU. Если развить идею дальше, то можно рассмотреть создание устройства на основе PLD (programmablelogicdevice).

Сборка изображений в результирующий PDF-документ занимает крайне мало времени относительно других этапов, поэтому ей можно пренебречь.

Существующие решения

На данный момент существует несколько проприетарных решений от различных компаний. Компания Abbyy использует MRC компрессию в своих продуктах. Одной из особенностей их метода является то, что они для определения слоя текста используют собственное OCR (opticalcharacterrecornition) решение вместо специализированного сегментатора. Качество постобработки слоёв не очень сильное. Лидером на данном рынке является компания Luratech (уже Foxit), которая использует свой собственный сегментатор и имеет довольно качественные (судя по качеству сжатия) методы постобработки слоёв. К сожалению, не существует на данный момент ни одной достаточно качественной открытой реализации MRC-компрессии.

Проблемы

Качество сжатия зависит от многих факторов: качество работы сегментатора, адаптация слоёв для применения алгоритмов сжатия, коэффициенты уменьшения размеров изображения. К сожалению, нет оптимальных параметров, и данные параметры подбираются индивидуально. Для подбора оптимальных параметров могут использоваться методы машинного обучения.

ЛИТЕРАТУРА

1. Wikipedia [Electronic resource]: Mixed raster content. - Mode of access: https://en.wikipedia.org/wiki/Mixed_raster_content. - Date of access: 10.01.2018
2. Wikipedia [Electronic resource]: Wavelet transform - Mode of access: https://en.wikipedia.org/wiki/Wavelet_transform. - Date of access: 10.02.2018

3. ABBYY website [Electronic resource]: PDF MRC - Mode of access: <https://www.abbyy.com/en-us/ocr-sdk-embedded/pdf-mrc/>. - Date of access: 12.01.2018
4. Wikipedia [Electronic resource]: JPEG 2000 - Mode of access: https://en.wikipedia.org/wiki/JPEG_2000. - Date of access: 10.12.2017
5. Wikipedia [Electronic resource]: JBIG2 - Mode of access: <https://en.wikipedia.org/wiki/JBIG2>. - Date of access: 20.01.2018
6. Wikipedia [Electronic resource]: Otsu threshold - Mode of access: https://en.wikipedia.org/wiki/Otsu%27s_method. - Date of access: 18.01.2018
7. Wikipedia [Electronic resource]: PDF - Mode of access: <https://en.wikipedia.org/wiki/PDF>. - Date of access: 07.11.2017
8. IEEE Xplore Digital Library [Electronic resource]: COS/CCC segmentation - Mode of access: <https://ieeexplore.ieee.org/abstract/document/5672783/>. - Date of access: 10.01.2018
9. Wikipedia [Electronic resource]: Group 4 compression - Mode of access: https://en.wikipedia.org/wiki/Group_4_compression. - Date of access: 25.12.2017
10. Luratech website [Electronic resource]: Luratech - Mode of access: <https://www.luratech.com/>. - Date of access: 23.11.2017

УДК 519.683.6

Студ. А. А. Вашинко
Науч. рук. асс. Т. Г. Шагова
(кафедра высшей математики, БГТУ)

БЛИННАЯ СОРТИРОВКА

Сортировка – это последовательное расположение или разбиение на группы чего-либо в зависимости от выбранного критерия. Блинная сортировка (*pancakesort*) – это не конкретный алгоритм сортировки, а класс сортировок, в которых допускается только одна операция – переворот элементов последовательности до какого-либо индекса.

Постановка задачи. Пусть в некотором ресторане работает очень неряшливый повар, который всегда печет блины разных размеров. И официант, работающий с ним, хочет упорядочить блины от самого маленького вверху до самого большого внизу. Он берет любое количество блинов сверху и переворачивает получившуюся стопку, повторяя это действие столько раз, сколько потребуется, для выполнения задачи. Вопрос: какое максимальное число переворотов потре-