2. Чернова Е.В., Доколин А.С. Метод проектов в превенции вовлечения молодежи в киберэкстремистскую деятельность / Психология и педагогика: на рубеже веков. В 2 книгах. К 1.:монография / [авт.кол. : Карпова Н.К., Васильева С.А., Головань М.С. и др.]. – Одесса: КУПРИЕНКО СВ, 2015 – 177 с.

3. Чернова Е.В., Макашова В.Н., Боброва И.И. Современные аспекты распространения киберэкстремистской идеологии в молодежной ИТ-среде // Фундаментальные исследования. – 2014. – № 12. – часть 5. – С. 1294–1297.

4. Хактивизм [Электронный ресурс] – https://ru.wikipedia.org/wiki/Хактивизм

5. Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику [Электронный ресурс] – http://www.crime-research.ru/articles/Tropina0104/5

СЕГМЕНТАЦИЯ ИЗОБРАЖЕНИЯ С ПОМОЩЬЮ ПРОГРАММНОГО СРЕДСТВА MATLAB

Чан Тхюи Зунг
(г. Томск, Томский политехнический университет)
E-mail: bluesky25792@gmail.com

IMAGE SEGMENTATION BY SOFTWARE MATLAB

Tran Thuy Dung
(s. Tomsk, Tomsk Polytechnik University)

Abstract. In computer vision, image segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as superpixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics. The result of image segmentation is a set of segments that collectively cover the entire image, or a set of contours extracted from the image.

Keywords: segmentation, image, matlab, MD5, Certificate**.**

Введение. Сегментация изображений – одна из главных задач распознавания изображений. Сегментация – это процесс разделения цифрового изображения на несколько сегментов, которые отличаются друг от друга элементарными признаками, такими как яркость, цвет, текстура, форма. Цель сегментации заключается в упрощении и изменении представления изображения, чтобы его было проще и легче анализировать. Неправильное выделение сегментов на изображении в конечном счете может отразиться на качестве распознавания и даже сделать его невозможным. Поэтому задача сегментации является чрезвычайно важной. Сегментация широко используется в многих областях. В качестве примера можно перечислить ряд направлений: медицинские изображения (обнаружение опухолей, определение объемов тканей, изучение анатомической структуры, …), выделение объектов на спутниковых снимках, распознавание лиц, распознавание отпечатков пальцев, обнаружение стопсигналов, машинное зрение. В данной работе мы рассмотрим сегментацию с помощью глобального порога.

Принцип работы. Порог – это признак, которое помогает разделить искомый сигнал на классы. Операция порогового разделения заключается в сопоставлении значения яркости каждого пикселя изображения с заданным значением порога. Выбор соответствующего значения пороговой величины дает возможность выделения на изображении областей определенного вида.

Пороговые преобразования занимают центральное место в прикладных задачах сегментации изображений. Операция порогового разделения является одной из наиболее простых и

важных процедур поэлементных преобразований и почти всегда предшествует процессу анализа и распознавания изображений.

Основная проблема операции порогового преобразования заключается в выборе надлежащего значения порога. Определение оптимального порога при преобразовании изображений является важной и трудной задачей, и для её решения разработано много различных методов. В методах глобальной обработки пороговая поверхность является плоскостью с постоянным порогом яркости, т. е. значение порога рассчитывается исходя из анализа гистограммы всего изображения и является одинаковым для всех пикселей исходного изображение.

Простейший из методов пороговой обработки состоит в разделении гистограммы изображения на две части с помощью единого глобального порога. После этого сегментация изображения осуществляется путем поэлементного сканирования изображения, при этом каждый пиксель отмечается как относящийся к объекту или фону, в зависимости от того, превышает ли яркость данного пикселя значение порога t или нет. Успешность этого метода целиком зависит от того, насколько хорошо гистограмма изображения поддается разделению. Определение величины порога с помощью гистограммы яркостей является простым методом, который позволяет достичь «чистой» сегментации, если гистограмма изображения носит четко выраженный бимодальный характер (рис. 1). Такая форма гистограммы означает, что на изображении можно различить два вида сравнительно часто встречающихся пикселей – яркие и темные. При этом 309 гистограмма легко разделяется с помощью одиночного глобального порога *t*, расположенного во впадине между пиками гистограммы.

Рис. 1. Бимодальная гистограмма

Для автоматического выбора значения порога t в случае бимодальной гистограммы может применяться следующий итеративный алгоритм:

- Шаг 1. Выбирается некоторая начальная оценка значения порога *t*.
- Шаг 2. Выполняется сегментация изображения с помощью порога t. В результате образуются две группы пикселей: *G*1, состоящая из пикселей с яркостью больше *t*, и *G*2, состоящая из пикселей с яркостью меньше или равной *t*.
- Шаг 3. Вычисляются средние значение $\mu 1$, $\mu 2$ яркостей пикселей по областям *G1, G2* соответственно.
- Шаг 4. Вычисляется новое значение порога:

$$t = \frac{\mu 1 + \mu 2}{2}$$

- Шаг 5. Повторяются шаги со 2-го по 4-й до те**х** пор, пока разница значений порога t в соседних итерациях не окажется меньше наперед заданного параметра ε.

Отметим, что если объекты и фон на изображении занимают сравнимые площади, то хорошим начальным приближением для порога t является средний уровень яркости изображения. Если же занимаемая объектами площадь мала по сравнению с площадью фона (или наоборот), то одна из групп пикселей будет доминировать в гистограмме, и средняя яркость окажется не слишком хорошим начальным приближением. В подобных случаях более подходящим начальным значением *t* является полусумма минимального и максимального значе-

ний яркости. Параметр ε используется для остановки алгоритма, когда изменения на каждой итерации становятся малы по сравнению с заданным параметром. Такие меры применяются, когда важным соображением является скорость вычислений.

Список литературы

1. http://en.wikipedia.org/wiki/Image_segmentation
2. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB, 2000.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ ФАЙЛОВ PDF

Чан Тхюи Зунг
(г. Томск, Томский политехнический университет)
E-mail: bluesky25792@gmail.com

DIGITAL SIGNATURES FOR PDF DOCUMENT

Tran Thuy Dung
(s. Tomsk, Tomsk Polytechnik University)

Abstract. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Keywords.: Electronic signatures, PDF, RSA, MD5, Certificate.

Постановка задачи. Информация является одним из ценнейших предметов современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. На сегодняшний день основная часть информации, которой обмениваются частные лица и организации, представлена в электронном виде. Поэтому важно обеспечить защиту электронных данных, включая проверку документа на корректность информации о авторе и на целостность. Это позволит гарантировать подлинность документа, то, что документ не был изменен другим лицом. Для решения этой задачи широко применяется электронная подпись. Данная работа посвящена анализу применения технологий электронной подписи для подписания и верификации *PDF*-документов.

Принцип работы. Для подписания и проверки электронной подписи выбраны следующие криптографические алгоритмы: с открытым ключом *RSA* и хеширования *MD5*. Алгоритм *MD5* позволяет получить сокращенную информацию о документе, на основе данной информации можно судить о целостности документа.

Для шифрования и дешифрования подписи применяется алгоритм *RSA*, который требует пары ключей – открытого и закрытого. Для шифрования подписи требуется закрытый ключ, которых представлен в виде *pfx*-файла. Подпись содержит информацию о авторе, времена, месте и рисунке подписи, также хеш-код документа, полученный с помощью алгоритма *MD5*. Этот закрытый ключ использует только автор документа и он не доступен другим лицам. Зашифрованная подпись прикрепится к PDF-документу, и этот документ направляется получателю. Открытый ключ, сохраняющий в файле с расширением *cer*, свободно распространяется и используется для дешифрования и верификации электронной подписи. Пользователь использует открытый ключ для чтения информации о авторе и хеш-коде документа. Документ прошел проверку если информация о авторе верна и документ не был изменен