

开放环境下 图像源识别技术

KAIFANG HUANJINGXIA
TUXIANGYUAN SHIBIE JISHU

黄永刚 刘 旭 刘玉莹 著

41

开放环境下 图像源识别技术

黄永刚 刘旭 刘玉莹 著

KAIFANG HUANJINGXIA
TUXIANGYUAN SHIBIE JISHU



电子科技大学出版社

University of Electronic Science and Technology of China Press

· 成都 ·

图书在版编目(CIP)数据

开放环境下图像源识别技术 / 黄永刚, 刘旭, 刘玉莹著. — 成都: 电子科技大学出版社, 2019.3
ISBN 978-7-5647-6893-5

I. ①开… II. ①黄… III. ①图象识别—研究 IV.
①TP391.413

中国版本图书馆CIP数据核字(2019)第071034号

开放环境下图像源识别技术

黄永刚 刘旭 刘玉莹 著

策划编辑 段勇

责任编辑 魏彬

出版发行 电子科技大学出版社

成都市一环路东一段159号电子信息产业大厦九楼 邮编 610051

主 页 www.uestcp.com.cn

服务电话 028-83203399

邮购电话 028-83201495

印 刷 四川煤田地质制图印刷厂

成品尺寸 170mm×240mm

印 张 6

字 数 200千字

版 次 2019年3月第一版

印 次 2019年3月第一次印刷

书 号 ISBN 978-7-5647-6893-5

定 价 29.00元

版权所有, 侵权必究

目 录

第一章 绪 论	1
1.1 研究背景	1
1.2 研究意义	1
1.3 研究内容	2
1.4 本书结构	3
1.5 本章小结	4
第二章 图像源识别研究现状	5
2.1 引 言	5
2.2 图像源识别研究现状	5
2.2.1 基于元数据的方法	5
2.2.2 基于数字水印的方法	6
2.2.3 基于图像特征的方法	7
2.2.4 小 结	7
2.3 基于图像特征的图像源识别研究现状	8
2.3.1 图像特征表示	8
2.3.2 基于统计学习的图像源识别	12
2.4 本章小结	13
第三章 有未知模型的图像源识别技术	14
3.1 引 言	14
3.2 有未知模型的图像源识别系统框架	15
3.2.1 未知图像源数据识别	16
3.2.2 鲁棒训练集的建立	17
3.2.3 算法复杂度分析	18
3.3 实验结果分析	18
3.3.1 实验数据及设置	18
3.3.2 实验结果及分析	19
3.4 本章小结	37

第四章 抗噪的图像源识别方法	39
4.1 引 言	39
4.2 噪声样本影响的理论分析	39
4.3 抗噪的图像源识别系统框架	42
4.4 抗噪的图像源识别系统算法	43
4.4.1 噪声级别评估	43
4.4.2 基于噪声级别的采样	43
4.5 抗噪的图像源识别方法有效性验证	45
4.6 实验结果分析	47
4.6.1 实验数据及特征提取	47
4.6.2 实验评估指标	48
4.6.3 实验结果与分析	48
4.7 本章小结	53
第五章 基于集合约束的图像源识别技术	54
5.1 引 言	54
5.2 基于约束的聚类方法	54
5.3 基于集合约束的图像源聚类方法	57
5.4 实验结果及分析	58
5.4.1 实验数据及设置	59
5.4.2 实验结果及分析	59
5.5 本章小结	61
第六章 探索图像源识别的特征耦合与模型耦合	62
6.1 引 言	62
6.2 特征耦合与模型耦合问题研究	63
6.2.1 特征耦合	63
6.2.2 模型耦合	64
6.3 捕获特征耦合与模型耦合的方法研究	66
6.3.1 耦合特征表示	66
6.3.2 耦合概率表示	69
6.4 实验结果与分析	71
6.4.1 数据集以及实验设置	71
6.4.2 试验评估指标	73
6.4.3 耦合特征表示的评估	74
6.4.4 耦合概率表示的评估	76

6.4.5 单个模型识别性能评估	79
6.4.6 计算成本评估	82
6.4.7 方法比较	82
6.5 本章小结	83
参考文献	84

1.1 研究背景

当今社会信息科技高速发展,数码相机、工业相机、手机相机等图像采集设备广泛普及,数字图像已成为现代社会信息的重要载体,不仅在日常工作、生活中得到广泛应用,也在军事、工业、医学、农业等重要领域。然而,现今由于网络通信的普及和图像处理软件如Photoshop、AI等的不断涌现,使得数字图像篡改变得简单,数字图像篡改的侵权行为如盗窃法国专利等,为数字图像处理应用信息安全问题的出现,数字图像技术在很大程度上被人们所怀疑,给人们的生活带来不便。方便工业生产的同时,也带来了许多安全隐患。例如大多数人对图像进行编辑加工只是出于增强图像的视觉效果,但不少人利用图像进行恶意伪造、篡改和传播,以传递虚假信息、误导社会、影响经济利益等目的。伪造和篡改图像如果被广泛用于科学研究、新闻报道和司法案件,将会对社会公共信任秩序和社会的稳定产生严重影响,甚至造成国际关系的紧张和混乱甚至引起军事冲突。数字图像安全问题,数字图像可能被犯罪分子用于进行各种金融信息的传播,如利用网络支付系统或个人信息造成严重损害。而篡改修改用于工业生产的数据,则会对整个生产过程造成灾难性影响。

因此,国内外各种图像伪造和篡改的事例层出不穷,而且愈演愈烈,面对数字图像篡改带来的一系列严重问题,我们迫切需要一种可靠的技术来对图像进行篡改,进而进行有效分析、鉴别和认证。在诸多技术中,数字图像篡改检测研究的发展最快,该领域研究主要集中于两个方面:数字图像的篡改检测和数字图像的篡改溯源。本书主要研究数字图像的篡改溯源。

1.2 研究意义

数字图像的篡改溯源问题研究主要基于大前提:数字数字图像,其工作

第一章 绪 论

1.1 研究背景

当今社会信息科技高速发展,数码相机、工业相机、双目相机和扫描仪等成像设备迅猛发展并快速普及,数字图像已经成为现代社会信息的重要载体,不仅在人们的日常、娱乐和工作中得到非常广泛的应用,也在工业生产领域占有越来越重要的地位。然而,现今由于越来越多的图像处理和编辑软件如Photoshop、ACDSee等的不断涌现,使得数字图像的篡改变得越来越简单,数字图像较传统的模拟图像更加容易被加工和修改。先进技术的产生和应用总是伴随着新问题的出现,数字图像技术在极大地方便人们的日常工作,愉悦人们的日常生活,方便工业生产的同时,也带来了许多负面的影响。尽管大多数人对图像进行编辑加工只是出于增强图像的视觉效果,但不乏有人对图像进行恶意伪造、篡改和传播,以达到混淆信息、危害社会、骗取经济利益等目的。伪造和篡改图像如果被大量用于科学发现、新闻媒体和司法证物等,将会对社会的公共信任秩序和社会的稳定产生严重影响;军事、政治和外交中的伪造图像甚至会引起军事冲突、政治风波和外交问题;隐写图像可能被恐怖组织用于进行各种危险信息的传播;换头照等伪造图像可能会对个人名誉造成严重损害;而恶意修改用于工业生产的图像,将对整个生产过程造成毁灭性的影响。

当前,国内外各种图像伪造和篡改的事件数不胜数,而且愈演愈烈。面对数字图像所引发的一系列严峻问题,我们迫切需要一种可靠的技术来对图像进行取证,进而进行有效分析、鉴别和认证。在当今学术界,数字图像取证是研究的重要领域,该领域研究主要专注于两个方面:数字图像的来源和数字图像的篡改检测。本书工作专注于数字图像的来源研究。

1.2 研究意义

数字图像的图像源识别研究主要有基于元数据、基于数字水印、基于特

征三大类方法。而与前两类相比,基于特征的图像源识别研究具有诸多优点,并具有重要科学意义,本书研究内容集中于基于特征的研究方法。基于特征的图像源识别方法可靠、廉价且可以被广泛使用。基于特征的图像源识别方法主要通过挖掘数字图像的成像机理和成像过程、分析图像伪造过程中的伪造痕迹来对图像的来源进行分析和判断。开展对数字图像图像源识别的研究工作,对于确保公共信任秩序、打击犯罪活动、维护司法公正和新闻诚信等具有十分重要的意义。同时,数字图像图像源识别涉及数字图像处理、计算机视觉、数据挖掘、模式识别和机器学习等诸多方面。开展将机器学习算法应用于图像源识别领域的研究,对促进各个学科的交叉融合,探索新技术具有广泛而深远的科学意义。

1.3 研究内容

现有的图像源识别方法,在提取的图片特征基础之上,运用统计机器学习的方法进行研究。现在的图像源识别研究一般假设在封闭数据集上。而在互联网环境下,数据集合一般是开放的。现有的研究未考虑在开放环境下的诸多问题,如未知模型问题、噪声数据问题、标注数据少而未标注数据多的问题、特征耦合和模型耦合问题。

针对开放环境下图像源识别面临的问题,本书提出了一些开放环境下的图像源识别方法,主要包括以下几个方面。

(1) 针对无标签数据的类别超过有标记训练集类别,即存在未知模型的问题,研究有未知模型的图像源识别方法。该方法不仅能够识别训练集已知的类别,同时能够识别来自未知模型的数据。现实中训练数据总是少量的,有大量的数据是没有标记的,同时未标记数据的类别往往超过了训练集的类别。把这些超出训练集类别的数据看成一类,即未知图像源模型。结合原始训练集与部分无标记数据,通过聚类方法识别未知图像源数据,在识别出未知图像源模型数据后把这部分无标记数据扩充到原始训练集中。扩充之后的训练集不仅包含已知类别,同时有超出原始训练集类别的数据。

(2) 针对训练集中存在噪声数据这一问题,研究抗噪的图像源识别方法。此方法能够在保留大部分干净数据的基础上,从训练集中去除大部分噪声数据,从而建立干净的训练集,再用干净的训练集训练分类器。已知训练数据集中存在错误标记的噪声数据,但是哪些数据是噪声数据以及噪声数据占有多少比例均未知。通过集成算法与拒绝采样相结合的方法去除噪声数据。首先用含有噪声数据的训练集训练得到多个基分类器,用这些基分类器对每个样本进行判定,根据判定结果计算每个样本的噪声级别。然后根据噪

声级别以拒绝采样的思想从集合中抽取数据。该方法可以在一定程度上去除噪声数据,从而获得干净的训练数据集。最后,再用统计学习方法在干净的训练集上训练分类器。

(3) 针对具有少部分标记数据和大量无标签数据的问题,研究基于集合约束的聚类方法,约束信息可以来自于部分标记数据,通过把标记转化成约束进而获得更加纯净的聚类效果。在非监督学习中,没有任何标记信息,聚类准则完全依赖于图像特征数据。通过计算相似度来分析图片数据之间的联系。现实中训练集是少量的,本书在基于约束的聚类方法基础之上,提出了一种基于集合约束的聚类方法,利用标记信息建立集合,同时考虑了不同集合之间的约束关系。

(4) 传统的图像源识别方法假设特征之间以及模型之间不存在依赖性。然而,由于特征和模型存在普遍的耦合关系,这两个假设通常是有问题的。为解决这个问题,本书提出了一种新颖的图像源识别方案。对于特征耦合,采用耦合特征表示来分析特征之间的耦合交互,利用皮尔逊的相关系数来测量特征之间的耦合关系,并以类似泰勒的扩展方式进行聚合。关于模型耦合,本书提出了一种新的耦合概率表示。模型耦合关系的特征在于由混淆矩阵计算得到的条件概率,然后将其与总概率定律相结合。通过挖掘特征耦合和模型耦合,可以显著提高识别精度。

1.4 本书结构

本书分为六个章节,各个章节内容安排如下。

第一章绪论,介绍图像源识别的研究背景,研究意义,本书的研究内容以及本书的结构。

第二章概述图像原始源识别相关研究,介绍目前常见的三种研究方法,并深入介绍基于特征的图像源模型识别研究现状。

第三章提出了有未知模型的图像源识别,首先介绍系统框架,然后阐述未知图像源识别的算法及实现细节,最后通过实验来验证有未知模型的图像源识别方法的有效性。

第四章提出抗噪的图像源模型识别,首先描述系统框架,进而阐述有噪声图像源识别系统算法,并对噪声数据的影响进行理论分析。随后通过实验验证噪声去除效果,并从理论上证明所提方法的有效性。

第五章提出基于集合约束的图像源模型识别。首先介绍基于约束的图像源模型识别,进而阐述基于集合约束的图像源识别方法。最后通过实验验证方法的有效性。

第六章提出挖掘特征耦合以及模型耦合图像源识别方法,并通过实验证明该方法的有效性。

1.5 本章小结

本章首先介绍了图像源识别研究的背景和意义,图像源识别是图像取证的重要内容,基于特征的图像源识别方法可以被广泛使用,具有重要意义。然后介绍了本书的主要研究内容。本书主要研究开放环境下的图像源识别技术,包括:有未知模型的图像源识别技术、噪声平滑的图像源识别技术、基于集合约束的图像源识别技术以及挖掘特征耦合和模型耦合的图像源识别技术。最后对论文的各个章节进行了编排。

第二章 图像源识别研究现状

2.1 引言

数字图像作为信息的重要载体，在信息传播中起着举足轻重的作用。媒体常常使用图像表情达意，政府、司法、科研等机构常将数字图像作为重要证据。图像源识别是指识别出当前图像是由具体哪一款相机拍摄。图像源识别是数字图像取证的内容之一，对图像源识别的研究具有重要意义。

2.2 图像源识别研究现状

图像源识别的研究方法主要有三种，即：基于元数据的方法、基于数字水印的方法和基于图像特征的方法。

2.2.1 基于元数据的方法

元数据就是描述、解释、定位或让其更易于检索、利用或管理一个信息资源的结构化的信息。元数据经常被称作数据的数据（data about data）或信息的信息（information about information）。这些定义都是非常抽象的，我们可以把元数据简单的理解成：最小的数据单元。元数据可以为数据说明其元素或属性（名称、大小、数据类型等），或其结构（长度、字段、数据列），或其相关数据（位于何处、如何联系、拥有者）。数码相机产生的数码照片都会存在一个Exif（Exchangeable Image File，可交换图像文件）信息，当中就包含了专门为数码相机的照片儿定制的元数据，根据Exif标准，这些元数据包括：Image Description（图像描述、来源，指生成图像的工具）、Artist（作者）、Maker（生成者）、Mode（型号）、Date（拍照日期）、Time（拍照时间）等等。

Exif的作用可总结为以下四点：第一点，可以提高摄影水平，通过查看优秀作品的Exif参数，能够知道作者使用的器材，并了解作者所处的环境以及拍摄时使用的相机设置；第二点，可以提供编辑依据，很多图像编辑器会

自动读取 Exif 数据来对图像进行优化,最常见的便是从 Exif 中读取相机的各种信息,从而自动识别出竖拍或者颠倒拍摄的照片并对其进行旋转校正;第三点,方便管理,Exif 除了记录技术参数之外,还允许用户加入自定义的信息;第四点,便于验证原图,由于照片经过图像处理软件的编辑后会丢失部分或全部的 Exif 元数据,所以 Exif 信息的完整与否还是判断照片是否为相机原始图像的重要依据。

基于元数据的图像源识别方法一方面依赖于查询包含在图像元数据中的相关图像源信息来识别图像源类型,然而图像元数据很容易被修改;另一方面,厂商注释 (Maker Note) 是储存在 Exif 中的厂商专有的注释数据,采用二进制格式,由不同厂商自行制定,因此没有统一的行业标准,加之设备生产商往往不对外公布其厂商注释采用的格式,使得解码和识别厂商注释变得十分困难,这对图像源识别也十分不方便。

2.2.2 基于数字水印的方法

数字水印 (Digital Watermarking) 技术是将一些标识信息 (即数字水印) 直接嵌入数字载体当中 (包括多媒体、文档、软件等) 或是间接标识 (修改特定区域的结构), 且不影响原载体的使用价值, 也不容易被探知和再次修改, 但可以被生产方识别和辨认。通过这些隐藏在载体中的信息, 可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是保护信息安全、实现防伪溯源、版权保护的有效办法, 是信息隐藏技术研究领域的重要分支和研究方向。与水印相近或关系密切的概念有很多, 从目前出现的文献中看, 已经有诸如信息隐藏 (Information Hiding)、信息伪装 (Steganography)、数字指纹 (Digital Fingerprinting) 等概念。

数字水印技术具有以下几个方面的特点。

(1) 安全性: 数字水印的信息应是安全的, 难以篡改或者伪造, 同时, 应当有较低的误检测率, 当原内容发生变化时, 数字水印应当发生变化, 从而可以检测原始数据的变更; 当然数字水印同样对重复添加有很强的抵抗性。

(2) 隐蔽性: 数字水印应是不可知觉的, 而且应不影响被保护数据的正常使用, 不会降低质量。

(3) 鲁棒性: 鲁棒性是指在经历多种无意或者有意的信号处理过程之后, 数字水印仍能保持部分完整性并能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数字信号和模拟信号的相互转化、重采样、剪切、位移、尺度变化以及有损压缩编码等。

(4) 嵌入容量 (Embedding Capacity): 是指载体在不发生形变的前提下

可嵌入的水印信息量。尤其是隐蔽通信领域的特殊性,对水印的容量需求很大。

基于图像水印的图像源识别方法是利用图片中相关图像源信息的水印。对于嵌入数字图像中的水印,有以下几点功能需求:①隐蔽性或透明性(Imperceptible or Transparency),原始图像在嵌入数字水印后的差异必须是人眼所无法察觉到的,也就是不能降低或破坏原始图像品质;②不易移除性(Non-removable),水印要设计得不容易甚至不可能被黑客移除;③鲁棒性(Robustness),经过水印技术处理后的图像经有噪声、压缩处理、图像处理以及各种攻击后,所萃取的数字水印仍然可以清楚的体现,以便于人眼辨别或判断;④明确性(Unambiguous),提取的数字水印,经过各种攻击后,失真不会很严重,可以明确的让拥有者辨别或判断。然而,数字图像水印需要在照片成像过程中植入,这样的话,就使得相机设计复杂化,并且提高了数码相机的制造成本。

2.2.3 基于图像特征的方法

现有的基于特征的图像源识别方法可以分为两种:第一种是设计复杂的特征,尽可能多的捕捉图像采集过程中留下的指纹,主要包括成像设备内在硬件相关的特征、软件相关的指纹特征以及卷积神经网络(CNNs)特征;在已有的这些特征基础上,第二种研究方法的重点是开发新的基于统计学习的图像源识别方法,包括监督学习方法和非监督学习方法。

图像特征的研究旨在设计各种各样的特征,以捕获图像采集过程中成像设备固有的硬件相关和软件相关的指纹。硬件相关的特征主要包括模式噪声、透镜径向畸变、色差、传感器灰尘等。图像相关的特征和由滤色器阵列特征是软件相关特征的两个代表。

在进行图像特征提取之后,图像源识别问题被转化为多类分类问题,可以作为机器学习问题进行处理,并用统计学习工具解决。目前存在许多针对这一方向的研究工作,主要分为两大类:监督学习方法和无监督学习方法。

基于图像特征方法的进一步介绍见2.3节。

2.2.4 小结

综上所述,图像源识别研究主要从三个方面进行,三种方法对比如表2-1所示。



表 2-1 图像源识别研究三种方法对比

图片源识别相关方法	方法	特点
基于元数据的方法	元数据存储于可交换图像文件中	1. 便于管理,易于提取信息 2. 易被修改,行业标准不同不利于推广
基于数字水印的方法	将标识信息直接嵌入图像中	1. 安全性、隐蔽性、鲁棒性均好 2. 水印生成复杂,提高相机成本
基于图像特征的方法	通过统计机器学习算法分析	1. 具有科学意义,普适性强,算法鲁棒性强 2. 模型训练需要大量数据

2.3 基于图像特征的图像源识别研究现状

2.3.1 图像特征表示

1. 传统特征

Kharrazi.M 等人是图像特征领域的先驱者，他们提出相机模型识别问题的一种解决方案是直接指定一组特征，这些特征代表了相机模型的特征，然后使用这些特征对来自特定相机的图像进行分类。虽然彩色图像的构造过程在不同品牌的数码相机中可能存在很大差异，但是，这些相机模型都是通过以下两个组件来提高输出图像的效果：CFA 配置和 Demosaicing 算法、颜色处理转换。经过这两个组件处理得到的图像，无论原始图像内容如何，RGB 的信号内容都会表现出一定的特征和模式。为了捕捉不同相机的基础颜色特征的差异，需要检查这些相机产生的数字图像的第一、第二甚至更高阶的统计数据。Kharrazi 等人提出的 34 个可用于图像源识别的特征，如表 2-2 所示。

表 2-2 Kharrazi 等人提出的图像特征

特征	个数
Average Pixel Value	3
RGB Pairs Correlation	3
Neighbor Distribution Center of Mass	3
RGB Pairs Energy Ratio	3
Wavelet Domain Statistics	9
Pixel Difference Based Measures	4
Correlation Based Measures	3
Spectral Distance Based Measures	6

在 Z.J.Geradts 等人的研究中，他们利用像素阵列中的缺陷来进行图像源识别。相机中的 CDD（电荷耦合器件）是造成像素阵列中存在缺陷的主要原

因。CCD采用半导体架构,其中电荷通过激发区域传输。CCD寄存器由一系列门组成,以顺序方式操纵栅极电压,以传送带方式将电子从一个栅极传递到下一个栅极。制造大型阵列时,它们有时会包含缺陷。缺陷通常在制造商的数据表中给出。这些工件的定义因制造商而异,具有大量缺陷的阵列比具有少量缺陷的阵列便宜。可以根据不同相机具有不同的阵列缺陷来对相机模型进行识别。

A.E.Dirik等人提出了一种基于单反相机传感器灰尘特性的特征表示方法。DSLR相机上的镜头是可互换的,并且当可更换镜头被移除时会出现传感器灰尘问题,从而使传感器区域暴露在灰尘和湿气的危害之下。一旦取下镜头,相机周围的灰尘颗粒就会被静电场吸引到成像传感器上,从而在传感器表面产生灰尘图案。在一定的条件下,特别是在小孔径条件下,这种尘埃模式可以被看作是小斑点,以局部强度衰减的形式遍布在图像上。虽然定位灰尘位置非常困难,但是当对图像中的每个像素应用块状局部直方图均衡化时,可以很容易地看到传感器尘埃伪影。他们提出的传感器灰尘模型依赖于观察到传感器灰尘具有的两个主要特征:①根据孔径大小引起强度表面的突然变化(例如,强度损失);②最常出现圆形的形状。为了模拟由于灰尘引起的强度退化,他们利用具有特定标准偏差和增益的2D逆高斯函数。

K.S.Choi等人提出了一种使用镜头径向畸变的数字图像分类的替代方法。由于所有透镜元件都不可避免地会产生一些像差,所以它们会在被捕获的图像上留下独特的印记。通过直线相机校准算法,可以定量地测量每个图像的径向畸变程度,并以此作为透镜径向畸变参数。径向畸变参数可以用来进行图像源识别。

L.T.Van等人曾经估计了图像色差的失真参数,并使用这些提取的特征训练分类器来识别源手机。他们的动机来自两个方面,首先,在镜头系统由低端塑料材料而不是高端低色散非球面镜片组成的照相手机中,像差更加严重;其次,每个相机模型具有不同的镜头结构,因此他们的色差有些不同,该差异可以用失真参数表示。

2. PRNU特征

有些研究人员使用光响应非均匀性噪声(PRNU)作为相机识别的指纹。J.Luká's等人的工作是迈向这一方向的第一步。他们开发出一种新的方法来解决图像源识别问题。他们的识别方法是将像素非均匀性噪声作为特征,这是所有数字成像传感器(CCD, CMOS, 包括Foveon™X3和JFET)常见的模式噪声的随机组成部分。

模式噪声的两个主要组成部分是固定模式噪声(FPN)和光响应非均匀

噪声 (PRNU)。PRNU 主要由像素不均匀性 (PNU) 引起的, PNU 被定义为由硅晶片的不均匀性和传感器制造过程中的缺陷引起的像素对光的不同灵敏度。PNU 噪声的特征和起源使得来自同一晶片的均匀传感器不太可能表现出相关的 PNU 模式。因此, PNU 噪声不受环境温度或湿度的影响。

在他们的方法中, 首先, 用小波去噪滤波器对原始图像进行去噪以获得 PRNU。然后, 通过对图像的 PRNU 值求平均, 获得参考 PRNU。最后, 使用图像的 PRNU 与参考 PRNU 之间的相关性来进行图像源识别。

C.T.Li 等人认为可以使用滤色器阵列来捕获每个像素的三个颜色分量中的一个, 引入了颜色内插噪声, 而现有的用于提取 PRNU 的方法没有提供解决该问题的有效手段。由于通过颜色插值过程获得的人工色彩不是通过物理硬件直接从场景中获取的, 他们认为从没有插值噪声的物理成分中提取的 PRNU 应该比从携带插值噪声的人工通道中提取的 PRNU 更可靠。基于该假设, 他们提出了解耦 PRNU (CD-PRNU) 提取方法, 其首先将每个颜色通道分解为 4 个子图像, 然后从每个子图像中提取 PRNU 噪声。然后组装子图像的 PRNU 噪声模式以获得 CD-PRNU。

3. CNN 特征

上述方法需要人工提取特征, 然后根据特征选取合适的机器学习算法进行处理。特征工程是将原始数据转化为特征, 更好地表示预测模型所处理的实际问题。在特征工程中, 手工设计特征有两个前提: 一是需要高超的工程技巧; 另一个是需要相关领域的专家知识。

深度学习可以表示复杂的模型, 能够学习数据的多层抽象表示, 可以从大量数据中根据任务自动学习特征。Camera Model Identification With The Use of Deep Convolutional Neural Networks 中提出了基于深度卷积神经网络 (Convolutional Neural Network, CNN) 图像源识别方法。卷积神经网络在图像识别领域应用尤其广泛, 其设计思想接近生物视觉系统。图像识别一直以来就是难题, 深度神经网络在训练过程中面临着参数过多、梯度弥散、训练时间过久等问题。卷积神经网络的提出很好地解决了参数过多、难以训练等问题, 并且能够对大量的图像数据提取鲁棒的特征。卷积神经网络有四个关键点: 局部连接、权值共享、下采样 (Pooling)、多层表示。

(1) 局部连接。

一般认为对图像的认知是从局部到全局的, 而图像的空间联系也就是局部的像素联系较为紧密。而距离较远的像素相关性则较弱。图像数据具有联通性质。因此, 每个神经元没有必要对全局图像进行感知, 只需要对局部进行感知, 全局感知可能会造成更多的冗余信息。然后, 在更高层将局部的信

息综合起来就得到了全局信息。

局部感知通过卷积操作实现,卷积操作有两个凸出优点。第一,因为图像数据局部相关性较高,卷积操作能够检测出图像中特有的局部特性。第二,卷积操作具有位置不变性。相同的事物可以多次出现在图像中,例如:图像中不同位置可以出现相同的椅子,通过卷积操作,可以得到图像的这些特性。

(2) 权值共享。

权值共享同样通过卷积操作完成,而且在一次局部感知过程当中,采用一个相同的卷积核,此卷积核对图像进行卷积操作之后会得到一个特征图(Feature Map)。一个 5×5 大小的图像在一个 3×3 的卷积核中进行卷积操作,最终可得到 3×3 大小的Feature Map。多个卷积核可以得到多个特征图,每个特征图共享有限个权值。

(3) 下采样(Pooling)。

通过卷积操作之后获得了特征图,在特征图中有些信息是冗余的,如果直接利用特征图进行分类,可能会出现过拟合。于是提出了下采样(池化, Pooling)的聚合操作。图像具有一种静态的特征,即在一个图像区域有用的特征有可能在另一个区域同样适用。池化操作把语义上相似的特征组合起来,相关位置特征形成的基本特性可能稍微会改变,通过池化粗粒度的提取特征,可以可靠的检测到这些基本特性。同时,上一层的元素在位置或表现上改变时,池化之后使得当前的特征表示改变非常微小。

(4) 多层表示。

卷积和池化操作对图像抽取了一层特征,但是如果要获得更加复杂的特征就需要多层的卷积网络,也就是深度卷积神经网络。深度卷积神经网络中每层神经元会对特征做非线性变换,主要起到两个作用:第一是选择性,保持对图像细节特征的敏感性;第二是表示不变性,提取的图像特征不受环境(背景、光线、物体姿态等)的影响。通过深度卷积神经网络的非线性转换,能够根据目标任务对图像自动提取特征,当数据量极大时,所提取特征表示能力超强,分类效果优于人工提取的特征。

神经网络的输入为原始的图片,然后通过卷积和池化层对图片进行特征提取,进而通过全连接和Softmax输出层对图片进行分类。

神经网络首先对原始图片进行预处理,使用 5×5 的卷积核对图片进行卷积处理。预处理操作是完成图像源分类的重要操作,通过卷积操作完成对图像每个颜色通道的滤波去噪。然后进行三层卷积操作,卷积操作之后接一层最大化池化操作,最后两层是全连接操作,输出层是Softmax层,完成图像