数字图像来源取证现状与趋势

王 波　　杨福龙
(大连理工大学电子信息与电气工程学部　辽宁大连　116024)
(bowang@dlut.edu.cn)

An Overview and Trends on Digital Image Source Forensics

Wang Bo and Yang Fulong
(*Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian, Liaoning* 116024)

Abstract The characteristic of editing and forging digital media makes the authenticity of multimedia encountering great challenges in digital age. Due to that, the digital image forensics, which focuses on the source identifiability, content authenticity and information integrity of digital images, has become a hot research issue in multimedia information security field. Focusing on the issue of source identification of digital images, the paper first illustrates the existing general research model and framework. Based on the overview of current typical algorithms from the perspective of device-based, model-based and camera-based source identification respectively, the problems and trends of source identification of digital images are introduced and analyzed. Finally, this paper draws the conclusion and shows the prospect of digital image source identification.

Key words digital image forensics; source identification; device-based; model-based; camera-based

摘　要 数字信息易编辑和伪造的特点,使得数字时代多媒体的真实性遭受了极大的挑战.正因为此,关注数字图像来源辨识性、内容真实性和信息完整性的数字图像取证技术成为多媒体信息内容安全研究的热点.针对数字图像的来源取证问题,首先阐述了已有的一般模型和框架,然后从设备类型、设备型号和设备个体取证鉴别3个层次,分别阐述了目前典型的研究思路和方法,进而在此基础上,分析和介绍了当前数字图像来源取证所面临的问题和发展趋势,最终给出了结论和展望.

关键词 数字图像取证;来源鉴别;设备类型;设备型号;设备个体

中图法分类号 TP391

计算机的普及和网络的便捷,使得数字化信息已经成为人们日常工作和生活中不可或缺的重要角色.但凡事必有两面性,人们在享受数字化信息带来的种种便利的同时,也在面临和承担着其

收稿日期:2016-04-18
基金项目:国家自然科学基金创新团队基金项目(71421001);国家自然科学基金项目(61502076);辽宁省教育厅科学研究项目(L2015114)

带来的安全问题. 信息安全问题小至个人信息安全,大至社会、经济、政治、军事和文化安全. 数字信息具有易获取、易编辑、易修改的特性,这是一把双刃剑:一方面给人们获得和处理信息提供了极大的便利;另一方面也为无意或者恶意的篡改伪造信息提供了可能. 由此引发的对于数字信息完整性和真实性的关注,成为信息内容安全的2个重要问题. 而随着数码相机/智能手机的迅速普及、专业图像处理软件的广泛使用、社交网络平台的高速发展,分别解决了过去数字媒体在获取、处理和传播方面的制约瓶颈,从而使得数字媒体无论是使用范围、生成数量还是影响力都大大超过了传统媒体. 这也直接导致了近10年来,在新闻、政治、司法以及科学等领域层出不穷的篡改伪造数字媒体所引发的各类事件,冲击着人们对于新闻、司法乃至社会诚信体系的信心. 正因为数字媒体完整性和真实性分析的急切需求,也催生了数字内容取证技术的迅速发展[1].

与传统的电子取证/计算机取证关注电子设备、计算机和网络设备中数据的追踪、恢复和溯源不同,数字内容取证更多地是关注数字多媒体(图像、音频、视频等)的来源辨识性、内容真实性和信息完整性,进而才可能满足司法体系中对于证据监督链的要求,确保数字多媒体作为可采信数据的完整和合法性.

一些国际著名大学,如美国的马里兰大学、普渡大学、哥伦比亚大学以及达特茅斯大学等,于2002年前后就开始了数字媒体取证相关技术的研究,其重点集中在数字图像、数字音频的来源鉴别和伪造检测[2],也有一些对数字视频的取证研究[3]. 与此同时,数字媒体取证技术的相关文献也开始见于计算机取证的相关国际会议上. 随着数字媒体取证技术研究的深入,ACM,IEEE的一些国际顶级学术会议和期刊也陆续将其纳为一个重要的主题. 2005年《IEEE Transaction on Information Forensics and Security》和2006年《Springer LNCS Transaction on Data Hiding and Multimedia Security》学术期刊的创建,也标志着数字媒体的取证和安全技术已经成为数字内容安全中的热门领域之一. 我国许多高校和研究机构也和国际上的科研机构几乎同步开展了数字媒体取证的相关研究. 北京电子技术应用研究所、北京邮电大学、大连理工大学、湖南大学、武汉大学和中山大学等在数字图像来源鉴别和数字音频取证方面做了大量的研究工作;南京理工大学、深圳大学、上海大学和同济大学等则在数字图像操作取证、篡改伪造检测等方面开展了深入的研究. 相应地,各国政府机构和工业界也对数字媒体取证给予了极高的重视和相当大的支持. Adobe公司2007年开始与美国达特茅斯大学合作开发对篡改伪造图像进行检测的插件工具. 2015年9月DARPA则启动了名为"Media Forensics"(DARPA-BAA-15-58)的项目[4],旨在开发自动评估数字图像和视频完整性的一系列工具. 而我国的自然科学基金委、科技部等单位也都以国家自然科学基金、"八六三"项目的形式给予数字媒体取证技术的发展极大的支持.

本文针对数字图像取证中的来源鉴别问题,总结了目前主要的分析模型和框架;从基于设备类型(device-based)、基于设备型号(model-based)以及基于设备个体(camera-based)3个不同的层次分别分析了当前典型的数字图像来源取证方法,给出了当前数字图像来源取证所面临的问题和挑战.

1 数字图像来源取证的已有框架

美国哥伦比亚大学Chang所领导的团队很早就开展了数字图像来源鉴别和数字图像取证技术的研究. 他们最早给出了一个包含数字图像来源鉴别在内的数字图像取证系统TrustFoto[5],如图1所示. 该系统综合考虑了数字图像取证的用户、输入图像、系统取证、分析输入以及决策报告5个方面的内容. 而在系统取证中,TrustFoto系统的第1步就是利用数字信号处理和统计分析等方法对输入图像的获取设备进行建模.

Kot等人[6]指出,数字图像的来源鉴别问题通常被建模为机器学习中的分类问题. 通过对已知N种不同来源的数字图像进行有监督的训练,构建一个有效的分类模型,进而可以对输入的未知来源的图像进行来源鉴别. 目前大部分数字图像来源鉴别方法均采用了这种框架. 牛少彰等人[7]

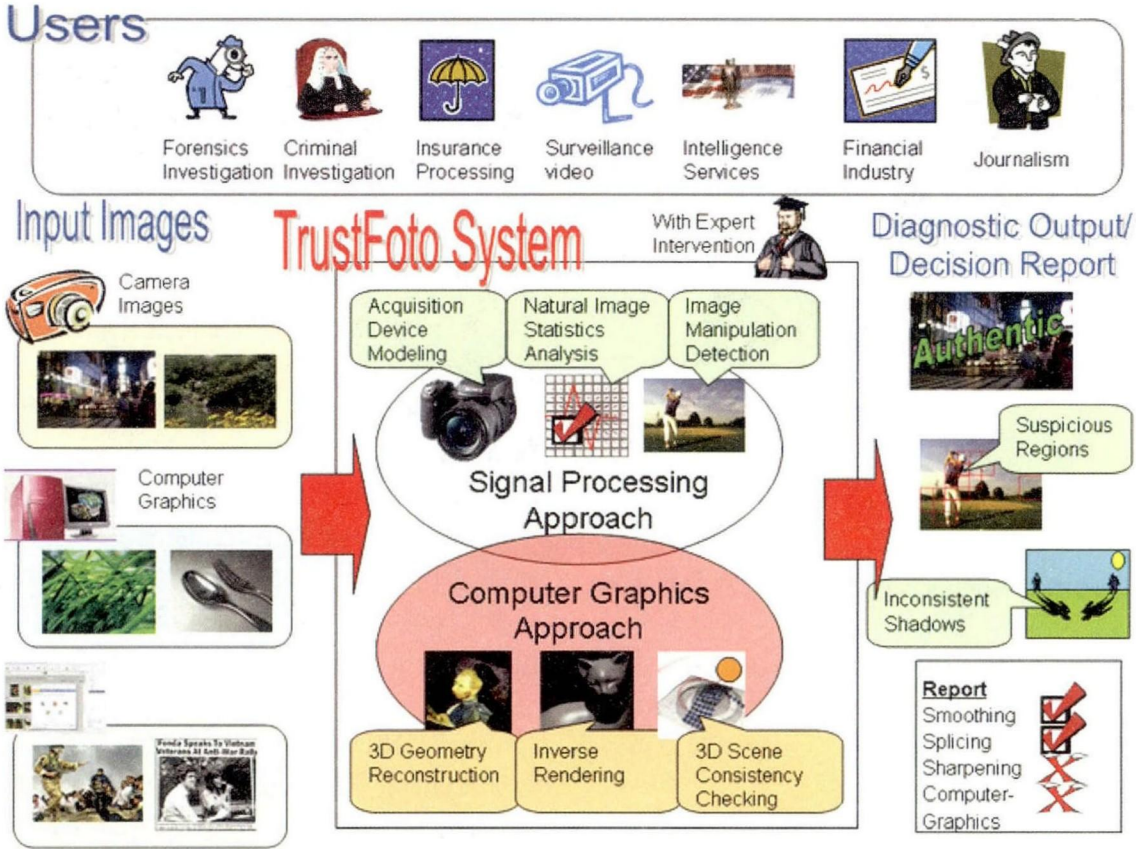

图 1　TrustFoto 系统框图[5]

将其总结为如图 2 所示的模型.

大连理工大学的王波[8]将数字图像的来源取证分为 3 个不同的层次:基于设备类型的数字图像来源鉴别关注数字图像由哪种类型的图像采集设备获取;基于设备型号的数字图像来源鉴别则需要分析数字图像具体是由哪一个厂商哪一个品牌哪一个型号的数码相机/手机/扫描仪等获得的;基于设备个体的来源鉴别技术则需要回答待取证的图像是否由指定的某一个设备个体所拍摄的问题,如图 3 所示.

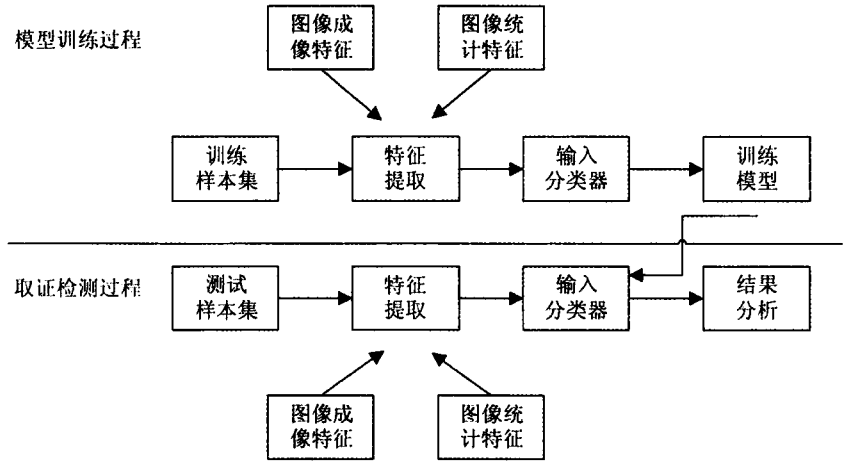

图 2　基于机器学习的数字图像来源取证框架[7]

图3 数字图像来源取证的3个不同层次

2 数字图像来源取证的研究现状

数字图像来源取证的核心目的是判断数字图像的获取设备，只是出于取证目的的不同和先验信息的不同，将其分为设备类型、设备型号和设备个体3个不同层次的技术. 而近年来出于伪造数字图像来源的目的，也出现了一些数字图像来源反取证的技术.

2.1 基于设备类型的数字图像来源取证

最早提出数字图像的设备类型来源取证是面向美国一个现实问题：儿童色情预防法案中允许计算机生成的儿童色情图像合法被制作和传播. 因此，在计算机生成图像(computer graphics, CG)技术日趋成熟、甚至可以以假乱真的时代，如何准确取证数字图像是来源于真实成像设备还是计算机，成为一个现实的司法技术问题.

Lyu等人[9]认为不同的图像采集设备，其成像过程一定会引入不同的设备特征，并可以在频域的不同方向和尺度中反映出来. 因此，他们使用多尺度小波变换提取高维统计特征，来描述数字图像呈现出的这种设备类型之间的差异. Ozparlak等人[10]也提出了类似的方法. Farid等人[11]还对相机拍摄的和计算机获取的人脸图像进行了取证鉴别分析. Chang领导的团队[12]则从景物模型、光线模型和获取方式3个方面分析了数码照片和CG图像的差异，进而从微分几何学的角度提出几何形状和局部碎片特征，在其构建的公开数据库上进行了数字图像的来源取证分析. 他们甚至还开发了一个在线鉴别计算机生成图像和照片图像的系统[13]. 基于亮度和色度的HSV模型由于更为符合人类视觉感知模型(human visual system, HVS)，因此也被用于取证数码照片图像和CG图像[14]. 从CFA插值周期性[15]、视觉特征[16]、纹理特征[17-18]、直方图特性[19]、光照响应不一致性噪声[20]、白平衡[21]、局部二值模式(local binary pattern, LBP)[22]等角度出发，研究者也提出了一些有效的特征对数码照片图像和CG图像进行区分和鉴别.

而针对更多不同的设备类型，Orozco等人[23]利用颜色特征和质量特征等；Khanna等人[24]则使用了噪声特征，分别对相机、扫描仪以及计算机生成图像进行鉴别.

2.2 基于设备型号的数字图像来源取证

对于任意一类数字图像成像设备，例如数码相机、手机、扫描仪等都存在着种类繁多的厂商、品牌以及型号. 对于已经确认设备类型的数字图像，取证分析人员需要进一步对其设备型号进行鉴定和确认.

由于EXIF标准的存在，使得绝大部分成像设备所采集的数字图像都在其EXIF中直接明文声明了采集该图像的设备厂商、型号以及相关的重要参数. 但也正因为EXIF作为公开的标准，并未对这些重要的信息进行任何加密或者其他措施的安全保障，使得这些信息可以很容易地被绝大多数的数字图像编辑和处理软件读取、修改甚至伪造. 可以说，传统的以EXIF作为数字图像来源取证的方法在“有心的”伪造者眼里完全是无用的.

正因为此，面向设备类型的数字图像来源取证技术尝试使用图像数据本身来对其来源进行分析. 由于同一型号的数码相机/手机采用了相同的成像硬件和图像处理算法，因此自然而然地，数码相机和手机的硬件器件特性和图像处理算法特性，就成为基于设备型号数字图像来源取证技术的重要依据.

Choi等人[25]将不同型号数码相机的镜头失真作为来源鉴别的核心特征. 他们提取了数字图像中直线信息的失真来量化描述镜头的失真，进而区分和鉴别不同型号数码相机拍摄的图像.

CFA和对应的插值算法则是被研究得更多的一种成像属性. 不同型号的数码相机往往采用不同的CFA模式和插值算法，研究者相信，通过估计CFA模式和插值系数，可以鉴别和取证数字图

像的设备型号. Farid 等人[26]使用 EM 算法检测数字图像频域中的局部能量峰值点，认为其反映了 CFA 插值向图像局部引入的相关性. 而 Bayram 等人[27]则在此基础上分析确定二维概率图的峰值点，并以此作为特征进行数码相机型号的来源鉴别. Long[28]、Swaminathan[29]、王波等人[30]、Chen 等人[31]则致力于如何准确估计 CFA 的插值系数，并选择合适的分类器达到较高的来源鉴别准确率.

白平衡[32]作为相机成像系统中重要的图像后处理算法，其参数估计也被用于数字图像的型号来源鉴别当中.

与此同时，还有相当一部分研究工作不局限于分析单一成像硬件或者图像处理算法所引入的特征，而是将整个图像采集设备看作为一个整体，认为不同型号成像设备所拍摄的数字图像的特性差异，是成像系统整体差异的综合反映. 因此，他们往往期望从不同的角度构建描述数字图像设备型号差异的整体模型，进而实现来源取证.

Kharrazi 等人[33]认为不同型号数码相机拍摄的图像，其图像整体质量、颜色一定会存在差异，即便这种差异视觉上不可见. 因此他们用图像质量特征、颜色相关性、颜色能量比等特征构建了一个描述相机型号来源的特征集. 类似的还有 Goyal 等人[34]和 Meng 等人[35]的工作. Xu 等人[36]利用一阶和二阶矩特征建立统计模型，并最终提取了 390 维统计特征对数字图像进行来源鉴别. 随后他们又使用 LBP 作为数字图像来源模型的描述特征[37]. Thai 等人[38]则基于异方差噪声模型和 DCT 系数模型提出了数字图像的相机型号来源鉴别方法.

与上述方法将数字图像的设备型号来源取证问题建模为有监督学习的分类问题不同，Amerini[39]和 Luan 等人[40]则将来源取证问题建模为无监督学习中的聚类问题. 但是需要注意的是，由于无监督学习无法获得任何关于设备型号的先验信息，因此这类方法的最终取证结果往往只能是指出数字图像检材中哪些图像属于同一种型号的成像设备所获取，而不能明确究竟是哪一种型号的成像设备.

2.3 基于设备个体的数字图像来源取证

数字图像来源取证的最终目的是判断数字图像由具体的哪一个成像设备获取，或者判断是否由指定的某一个成像设备获取. 显然，要达到这样的目的，需要利用成像设备的个体独有特性，这往往取决于成像设备硬件的差异性. 因此，基于设备个体的数字图像来源取证几乎也默认这样一个假设：取证分析方拥有或者可以获得可能用于获取数字图像检材的成像设备（或者至少拥有该成像设备所获取的一定数量的训练样本）.

传感器的生产制造缺陷最早被用于数字图像的相机个体来源取证. Geradts 等人[41]发现每一个用于数码相机的 CCD 传感器件都存在不同数量和不同位置的感光缺陷点. 因此，可以检测图像中由于感光缺陷所产生的暗电流点来鉴别数字图像的相机个体来源. 另一个有趣的工作则是 Memon 等人[42]所做的利用镜头上的灰尘特征进行相机个体取证. 他们发现数码相机由于其并不出色的密封特性，镜头上不可避免地存在灰尘，而这种灰尘点的分布显然是具有明显的个体特征的. 通过归一化互相关构建灰尘点的局部等高线，他们设计了一种相机个体来源取证算法. 尽管这种方法可能会由于时间的推移或者外界的干扰（例如清理镜头）而失效，但在相对短时期内，镜头的尘埃分布仍不失为一个行之有效的相机个体来源取证方法.

研究更为广泛、认可度更高的则是一种被称为“数字弹道”的传感器模式噪声技术. Fridrich[43]借鉴弹道学的概念，最早在数字图像取证领域提出了“数字弹道”. 他指出，传感器由于其光响应非均匀性和器件特性，不可避免地会存在噪声，而这种噪声正如子弹从不同枪械中射出后留下的独特痕迹，是独一无二的. 进一步地，他将传感器模式噪声分为固有模式噪声和光响应非均匀性噪声，并通过滤波和统计差异的方法获取数码相机的模式噪声，利用相关性检测、假设检验等方法实现数字图像的相机个体来源取证[44].

传感器模式噪声的概念一经提出，受到了广泛地关注和大量深入的研究. 研究者们分别从传感器噪声的准确获取、有效增强和质量改善、参考模式噪声和待测模式噪声的可靠关联 3 个主要方面开展了大量的研究工作.

在传感器噪声的准确获取方面，研究者们发现，亮度高[45]、复杂度低[46-47]以及能量强[48]的图像，其提取的传感器模式噪声更为准确，不易受到数字图像内容的影响. 而 Kang 等人[47]则提出了在

变换域中进行模式噪声提取和分析的方法. 而提取模式噪声的滤波器设计也是研究者关注的重点.

在传感器噪声的增强和质量改善方面,Li 等人[49]认为 CFA 插值可能导致传感器噪声误差,因此他们使用非插值像素点提取 PRNU. Fridrich 等人[50]则进一步总结出 CFA 插值、JPEG 压缩等操作引入的是相机的非独特属性(non-unique artifacts, NUAs),可以通过零均值的方法进行抑制和消除. 光谱均衡[51]、滤波器失真去除[52]、加权平均优化[53]和 PCA[54]等方法也在近年来被用于传感器噪声质量的改善.

在参考模式噪声和待测模式噪声的可靠关联方面,最早使用的方法是相关性检测[44]. 随着研究的深入,相关能量峰值[44]、循环互相关矩阵[55]、假设检验以及三角检测[44]等,也都被用于模式噪声的关联检测.

除此之外,传感器模式噪声技术也被用于手机[56]、便携式数码摄像机[57]、扫描仪[58]的数字图像设备个体来源取证鉴别.

2.4 数字图像来源反取证技术

在取证分析研究者们不断提出新的、行之有效的数字图像来源取证技术的同时,作为其对抗式学科的反取证技术也在不断发展和进步. 数字图像来源鉴别的反取证技术,其目的就是要针对可能的来源取证方法,通过修改、伪造数字图像的数据特性,达到篡改数字图像来源、使来源取证方法失效的目的.

针对数字图像设备型号来源鉴别中使用 CFA 插值系数估计作为核心特征的这类方法,最简单和直接的反取证思想就是再次利用 CFA 插值算法进行数字图像的重建,使其尽可能覆盖原插值算法向图像中引入的相关性特征[59]. 为了最小化重插值过程所引入的数字图像失真,Kirchner 等人[60]利用矩阵变换构建失真模型,并使用最小二乘法计算最小失真.

而针对数字图像设备个体来源鉴别中研究最为广泛的传感器模式噪声,也同样有对应的反取证技术. Li 等人[61]认为,传感器模式噪声实际上是一种加性噪声,据此他们提出了基于传感器模式噪声的指纹移除(signature removal)和指纹替换(signature substitution)反取证技术. 在此基础上,杨弘和 Zeng 等人[62-64]则分别针对指纹移除和替换的强度计算提出了不同的算法,使得数字图像来源鉴别的反取证算法在原始数字图像质量和反取证效果之间达到平衡和优化. 而针对 Fridrich 提出的三角检测,也有一些研究者提出了相应的行之有效的反取证策略[65-67].

为了更好地分析数字图像来源取证技术和反取证技术之间相互影响、相互制约的关系,Barni[68]和 Stamm 等人[69]都使用了博弈论的相关模型和方法来进行理论分析. 在可以预见的未来,有效的数字图像来源鉴别取证技术和反取证技术仍然会相互制约,同时相互提高,提升/抑制来源鉴别分析的准确率必然将会是争夺的关键.

3 面临的问题和发展趋势

数字图像来源取证的根本任务是鉴别和分析获取数字图像的设备类型、型号和个体. 其相关研究发展至今,已经从各个层面取得了一定的研究成果. 在可见的参考文献中,许多数字图像来源鉴别取证的方法都在实验室环境下,针对几个甚至是十几个设备样本,取得了 90% 以上的鉴别准确率. 但很显然,这样的鉴别准确率距离实用的司法技术仍然有一定的距离. 同时,现有算法大多数都对来源鉴别取证的场景和条件进行了一定的假设和约束,以降低实际情况下来源取证的难度. 因此,数字图像来源取证技术目前面临的核心问题,仍然是来源鉴别准确率的问题,尤其是在真实场景和条件下的来源鉴别准确率问题. 更为具体地,可以将目前数字图像来源取证所面临的主要问题和发展趋势总结为如下 3 点.

3.1 开放环境下的数字图像来源取证

如前文所述,现有的数字图像来源鉴别算法,尤其是基于设备类型和设备型号的来源鉴别算法,一般都被建模为机器学习中的多类分类问题,也就是有监督学习分类问题. 因此,其技术方案大多是通过大量已知标签的数字图像样本,提取有效的特征向量并进行有监督的学习,得到用于分类的模型和参数,进而实现来源鉴别和分类的目标. 在这种技术方案中,隐含了一个前提假设条件:训练模型中已知的类别数量代表了该分类任务中未来所有可能面对的类别. 简言之,在这样的模型中,取证分析人员必须假定待取证分析的数

字图像，其来源必然为已知训练样本类别中的其中之一.

显然，这个假设在许多情况下并不合乎常理. 虽然理论上如果建立足够大的样本库（大到包含所有可能的成像设备），这个假设是成立的，但显然这是一个现实中不可能完成的任务.

从有监督机器学习的本质上来说，这是一个封闭环境（已知有限类别）下的分类问题. 而现实中的数字图像来源取证往往是开放环境（无法确认取证检材的类别所属）下的分类问题. 用封闭环境下的分类模型解决开放环境下的分类问题，其结果必然是一旦数字图像检材来源于新的未知型号的图像获取设备，即在分类器的训练过程中未能获得已知类别标签的训练样本，那么该检材将无法避免地被错误鉴别和分类.

针对这个问题，Wang 等人[70]从分类器角度出发，使用一类和多类分类器组合的策略，将设备来源鉴别中的“数字图像是由训练模型中的哪一种相机/手机拍摄”问题，转换为“数字图像是否是被训练模型中的这种相机/手机拍摄”问题. 通过一类分类器引入“其他类”，在一定程度上解决开放环境下的数字图像来源鉴别问题. Costa 等人[71]则从设备连接的角度，使用决策边界切割的方法对数字图像开放集来源鉴别进行了研究. Huang 等人[72]则利用聚类、自训练策略以及 $k+1$ 类分类方法，提出了一种名为 SCIU 的来源鉴别方法，也可以对未知模型的数字图像进行来源取证. 不过可以看出，由于未知模型的数字图像缺乏足够的用于训练的先验信息，上述方法对于未知模型的数字图像来源取证准确率仍然有待进一步提高.

3.2 网络环境下的数字图像来源取证

现有的数字图像来源取证，大多都是直接对成像设备获取的图像进行数据分析，进而达到来源取证的目的. 但是实际情况中，待取证的数字图像检材可能来源于社交媒体等网络平台. 网络环境下数字图像可能会经历尺寸变换、重压缩、润饰等图像处理和增强操作，甚至可能经过 D/A 和 A/D 变换（即打印扫描）. 在这种情况下，网络环境中的数字图像，其数据特性和统计分布与成像设备直接获取的图像存在一定差异. 因此，在实际的取证场景中，对经过图像处理和增强操作的网络环境下的数字图像进行可靠的来源取证是更有实用价值，同时也更具挑战性的.

在设备型号的来源取证研究中，现有的大部分研究工作都将注意力集中在分析成像系统中单一关键部件（如镜头、CFA 插值等）或者整体系统（如质量特征、统计模型）的特性，很少关注图像处理和操作对这些特性的影响，因此这些方法大多对图像处理和增强操作都不具备鲁棒性. 王波等人在文献[73]中简单分析了 JPEG 压缩对数码相机型号来源取证的影响.

而在使用模式噪声进行设备个体的来源取证研究中，Miroslav 等人[74]指出模式噪声对 JPEG 压缩具有一定的鲁棒性，但由于其噪声特性，对于一些加噪和去噪的图像处理操作则相对较为敏感. 同时，由于在模式噪声相关性检测中需要参考模式噪声和图像检材模式噪声进行同步，因此在尺寸变换、图像剪切等操作处理情况下，模式噪声技术也存在一定的局限性. Fridrich 等人针对此问题开展了一些研究工作，他们在模式噪声研究工作的基础上，分别针对缩放和裁剪图像[75]、几何失真图像[76]以及打印图像[77]进行了来源鉴别，并在大规模图像库上进行了测试和验证.

可以预见，未来数字图像来源取证技术走向实用化的过程中，对数字图像处理和增强操作具有较强的鲁棒性，即对网络环境下的数字图像能够保持较高的来源取证鉴别准确率，是必须要跨越的一个技术难关.

3.3 有限样本环境下的数字图像来源取证

在数字图像的设备类型和设备型号来源取证研究中，由于大多数算法均采用了有监督学习的分类技术作为基本的模型和框架，因此不可避免地需要有标签的训练样本进行监督学习，以获得性能优良的分类器实现来源鉴别取证的目的. 而属于统计学习的有监督学习方法，其分类模型的有效性往往依赖于训练样本的代表性、多样性和其统计意义. 也正因为此，现有的数字图像来源算法大多都需要为数不少的有标签样本进行统计学习. 即使不采用有监督学习方法的基于模式噪声匹配的设备个体来源取证算法，也由于提取模式噪声需要尽可能去除数字图像内容对参考模式噪声的影响，使用了多个样本平均的方法来获得参

考模式噪声. 在实验室环境下，获取充足的训练样本并非难事. 但是如果是在实际的取证场景中，有标签训练样本的获取则可能是苛刻的假设条件.

因此，研究少量或者有限的有标签训练样本情况下数字图像的来源鉴别取证技术，对解决实际取证场景中的来源分析问题有着重要的现实意义.

目前针对有限训练样本情况下数字图像来源取证技术的研究并不多. 谭跃等人[79]针对数字图像的设备型号来源取证问题，借鉴传统半监督学习中的自学习和协同训练方法，分别使用 LBP，IQM 和 CFA 插值系数特征，测试和评估了训练样本数量低至 10 情况下的来源鉴别准确率. 其结论表明，对于已有的来源鉴别特征集合，半监督学习能够有效提高在有限训练样本情况下的取证准确率. 进一步地，他们通过构建原型集进行集成映射的半监督学习方法，提出了一种新的有限标签样本情况下的数字图像来源取证方法[80]. 该方法在有标签训练样本数量为 50 时，能够将 LBP 作为特征集合的图像设备型号来源鉴别准确率从 36%提高到 90.2%；甚至在训练样本数量低至 10、LBP 算法鉴别准确率仅有 8.4%时，也能达到 74.5%的来源取证准确率. 这为后续的相关研究提供了一个可借鉴的思路.

4 结论与展望

本文对当前数字图像的来源取证技术进行了分析，从设备类型、设备型号和设备个体 3 个方面总结了已有的典型方法，并讨论了数字图像来源取证的对抗式学科：数字图像来源反取证技术. 在此基础上，本文认为数字图像来源取证的核心问题仍然集中在鉴别准确率的提升，尤其是真实取证场景下的鉴别准确率提高上. 因此，本文总结了目前数字图像来源取证的 3 个主要发展趋势，即开放环境下、网络环境下和有限样本环境下的数字图像来源取证技术研究，指出这 3 个方面来源鉴别技术的深入研究和发展，对于数字图像来源取证从实验室研究走向实际应用，具有重要的现实意义.

参 考 文 献

[1] Piva A. An overview on image forensics [J]. ISRN Signal Processing, 2013, 2013: 1-22

[2] Stamm M C, Wu M, Liu K J R. Information forensics: An overview of the first decade [J]. IEEE Access, 2013, 1: 167-200

[3] Bestagini P, Fontani M, Milani S, et al. An overview of video forensics [J]. APSIPA Trans on Signal and Information Processing, 2012, 1(2): 1229-1233

[4] Media Forensics (MediFor) [EB/OL]. 2015 [2016-04-11]. https://www.fbo.gov/index?s=opportunity&mode=form&id=bfa29e5f04566fbb961cd773a8a8649f&tab=core&_cview=1

[5] Chang S F, Hsu J, Ng T T, et al. TrustFoto [EB/OL]. University of Columbia, 2006 [2016-04-11]. http://www.ee.columbia.edu/ln/dvmm/trustfoto/

[6] Kot A C, Cao Hong. Image and video source class identification [M]. //Digital Image Forensics. Berlin: Springer, 2013: 157-178

[7] 孙晓婷，李叶舟，牛少彰，等. 数字照片相机来源认证方法研究[J]. 中国电子商情通信市场，2013 (6): 100-104

[8] 王波. 利用成像引入特征的数字图像被动盲取证研究[D]. 大连：大连理工大学，2010

[9] Lyu S, Farid H. How realistic is photorealistic? [J]. IEEE Trans on Signal Processing, 2005, 53(2): 845-850

[10] Ozparlak L, Avcibas I. Differentiating between images using wavelet-based transforms: A comparative study [J]. IEEE Trans on Information Forensics and Security, 2011, 6(4): 1418-1431

[11] Farid H, Bravo M J. Perceptual discrimination of computer generated and photographic faces [J]. Digital Investigation, 2012, 8(3/4): 226-235

[12] Ng T T, Chang S F, Hsu J, et al. Physics-motivated features for distinguishing photographic images and computer graphics [C] //Proc of the 13th Annual ACM Int Conf on Multimedia. New York: ACM, 2005: 239-248

[13] Ng T T, Chang S F. An online system for classifying computer graphics images from natural photographs [C] // Proc of the Security, Steganography, and Watermarking of Multimedia Contents VIII. San Francisco, CA: SPIE, 2006: 607211-607211-9

[14] Chen Wen, Shi Y Q, Xuan Guorong. Identifying computer graphics using HSV color model and statistical moments of characteristic functions [C] //Proc of the IEEE Int Conf on Multimedia and Expo. Piscataway, NJ: IEEE, 2007: 1123-1126

[15] Chang T Y, Tai S C, Lin G S. A passive multi-purpose scheme based on periodicity analysis of CFA artifacts for image forensics [J]. Journal of Visual Communication and Image Representation, 2014, 25(6): 1289-1298

[16] Peng Fei, Liu Juan, Long Min. Identification of natural images and computer generated graphics based on hybrid features [J]. International Journal of Digital Crime and Forensics, 2012, 4(1): 1-16

[17] Wang Xiaofeng, Liu Yong, Xu Bingchao, et al. A statistical feature based approach to distinguish PRCG from photographs [J]. Computer Vision and Image Understanding, 2014, 128(11): 84-93

[18] Peng Fei, Li Jiaoting, Long Min. Identification of natural images and computer-generated graphics based on statistical and textural features [J]. Journal of Forensic Sciences, 2015, 60(2): 435-443

[19] 王学良，李生红，金波，等. 一种用于计算机生成图像与自然图像鉴别的改进方法[J]. 光电子·激光，2010，21(5)：783-785

[20] 刘娟. 基于PRNU的自然图像和计算机生成图像来源取证[D]. 长沙：湖南大学，2012

[21] Gao Shang, Zhang Cong, Wu Chanle, et al. A hybrid feature based method for distinguishing computer graphics and photo-graphic image [G] //LNCS 8389: Proc of the Int Workshop on Digital-Forensics and Watermarking 2013. Berlin: Springer, 2013: 303-313

[22] Li Zhaohong, Zhang Zhenzhen, Shi Y Q. Distinguishing computer graphics from photographic images using a multiresolution approach based on local binary patterns [J]. Security and Communication Networks, 2014, 7(11): 2153-2159

[23] Orozco A L S, Corripio J R, Villalba L J G, et al. Image source acquisition identification of mobile devices based on the use of features [J]. Multimedia Tools and Application, 2015: 1-25

[24] Khanna N, Chiu G T C, Allebach J P, et al. Forensic Techniques for classifying scanner, computer generated and digital camera images [C] //Proc of the IEEE Int Conf on Acoustics, Speech and Processing. Piscataway, NJ: IEEE, 2008: 1653-1656

[25] San Choi K, Lam E Y, Wong K K Y. Automatic source camera identification using the intrinsic lens radial distortion [J]. Optics Express, 2006, 14(24): 11551-11565

[26] Popescu A C, Farid H. Exposing digital forgeries in color filter array interpolated images [J]. IEEE Trans on Signal Processing, 2005, 53(10): 3948-3959

[27] Bayram S, Sencarb H T, Memonb N. Classification of digital camera-models based on demosaicing artifacts [J]. Digital Investigation, 2008, 5(1/2): 49-59

[28] Long Yangjing, Huang Yizhen. Image based source camera identification using demosaicking [C] //Proc of the IEEE Workshop on Multimedia Signal Processing. Piscataway, NJ: IEEE, 2006: 419-424

[29] Swaminathan A, Wu Min, Liu K J R. Nonintrusive component forensics of visual sensors using output images [J]. IEEE Trans on Information Forensics and security, 2007, 2(1): 91-106

[30] 王波，孔祥维，尤新刚，等. 利用协方差矩阵检测CFA插值的相机来源鉴别方法[J]. 光电子·激光，2009，20(4)：517-520

[31] Chen Chen, Stamm M C. Camera model identification framework using an ensemble of demosaicing features [C] //Proc of the Int Workshop on Information Forensics and Security. Piscataway, NJ: IEEE, 2015: 1-6

[32] Deng Zhonghai, Gijsenij A, Zhang Jingyuan. Source camera identification using auto-white balance approximation [C] //Proc of the Int Conf on Computer Vision. Piscataway, NJ: IEEE, 2011: 57-64

[33] Kharrazi M, Sencar H T, Memon N. Blind source camera identification [C] //Proc of the Int Conf on Image Processing. Piscataway, NJ: IEEE, 2004: 709-712

[34] Goyal K, Panwar R, Khanna N. Evaluation of IQM's effectiveness for cell phone identification using captured videos and images [C] //Proc of the Int Conf on Power, Control and Embedded Systems. Piscataway, NJ: IEEE, 2014: 1-6

[35] Meng Fanjie, Kong Xiangwei, You Xingang. A new feature-based method for source camera identification [C] //Advances in Digital Forensics IV: Proc of IFIP Int Federation for Information Processing. Berlin: Springer, 2008: 207-218

[36] Xu Guanshuo, Shi Yunqing, Su Wei. Camera brand and model identification using moments of 1-D and 2-D characteristic functions [C] //Proc of the 16th IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2009: 2917-2920

[37] Razzazi F, Seyedadabi. A robust feature for single image camera identification using local binary patterns [C] //Proc of the IEEE Int Symp on Signal Processing and Information Technology. Piscataway, NJ: IEEE, 2014: 462-467

[38] Thai T H, Cogranne R, Retraint F. Camera model identification based on the heteroscedastic noise model [J]. IEEE Trans on Image Processing, 2014, 23(1): 250-263

[39] Amerini İ, Caldelli R, Crescenzi P, et al. Blind image clustering based on the normalized cuts critertion for camera identification [J]. Signal Processing: Image Communication, 2014, 29(8): 831-843

[40] Luan Shuhan, Kong Xiangwei, Wang Bo, et al. Silhouette coefficient based approach on cell-phone classification for unknown source images [C] //Proc of the 2012 IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2012: 6744-6747

[41] Geradts Z J, Bijhold J, Kief M, et al. Methods for identification of images acquired with digital cameras [C] // Proc of the SPIE Conf on Enabling Technologies for Law Enforcement and Security. Boston, MA, USA: SPIE, 2001: 505-512

[42] Dirik A E, Sencar H T, Memon N. Source camera identification based on sensor dust characteristics [C] // Proc of the IEEE Workshop on Signal Processing Applications for Public Security and Forensics. Piscataway, NJ: IEEE, 2007: 1-6

[43] Fridrich J. Sensor Defects in Digital Image Forensic [M]. Berlin: Springer, 2013: 179-218

[44] Fridrich J. Digital image forensics using sensor noise [J]. IEEE Signal Processing Magazine, 2009, 26(2): 26-37

[45] Lawgaly A, Khelifi F, Bouridane. A Weighted averaging-based sensor pattern noise estimation for source camera identification [C] //Proc of the IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2014: 5357-5361

[46] Tan Yue, Wang Bo, Zhao Meijuan, et al. Patch-based sensor pattern noise for camera source identification [C] // Proc of the IEEE China Summit and Int Signal and Information Processing. Piscataway, NJ: IEEE, 2015: 866-870

[47] Kang Xiangui, Chen Jiansheng, Lin Kerui, et al. A context-adaptive SPN predictor for trustworthy source camera identification [J]. EURASIP Journal on Image and Video Processing, 2014, 2014(1): 1-11

[48] Hu Yongjian, Yu Binghua, Jian Chao. Source camera identification using large components of sensor pattern noise [C] //Proc of the 2nd Int Conf on Computer Science and its Applications. Piscataway, NJ: IEEE, 2009: 1-5

[49] Li C T, Li Yue. Digital camera identification using colour-decoupled photo response non-uniformity noise pattern [C] //Proc of IEEE Int Symp on Circuits and Systems. Piscataway, NJ: IEEE, 2010: 3052-3055

[50] Goljan M, Fridrich J, Chen Mo. Defending against fingerprint-copy attack in sensor-based camera identification [J]. IEEE Trans on Information Forensics and Security, 2011, 6(1): 227-236

[51] Lin Xufeng, Li C T. Preprocessing reference sensor pattern noise via spectrum equalization [J]. IEEE Trans on Information Forensics and Security, 2016, 11(1): 126-140

[52] Lin Xufeng, Li C T. Enhancing sensor pattern noise via filtering distortion removal [J]. IEEE Signal Processing Letters, 2016, 23(3): 381-385

[53] Chan L H, Law N F, Siu W C. A confidence map and pixel-based weighted correlation for PRNU-based camera identification [J]. Digital Investigation, 2013, 10(3): 215-225

[54] Li Ruizhe, Yu Guan, Li C T. PCA-based denoising of sensor pattern noise for source camera identification [C] // Proc of the IEEE China Summit and Int Signal and Information Processing. Piscataway, NJ: IEEE, 2014: 436-440

[55] Kang Xiangui, Li Yinxiang, Qu Zhenhua, et al. Enhancing source camera identification performance with a camera reference phase sensor pattern noise [J]. IEEE Trans on Information Forensics and Security, 2012, 7(2): 393-402

[56] Soobhany, Lam K P, Fletcher P, et al. Mobile camera source identification with SVD [G]//LNEE 313: Proc of the Int Joint Conf on Computer Information and Systems Sciences and Engineering. Berlin: Springer, 2015: 123-131

[57] Chen Mo, Fridrich J, Goljan M, et al. Source digital camcorder identification using sensor photo response non-uniformity [C] //Proc of the 9th Conf on Security, Steganography, and Watermarking of Multimedia Contents IX. San Francisco, CA: SPIE, 2007: 65051G-65051G-12

[58] Gou Hongmei, Swaminathan A, Wu Min. Intrinsic sensor noise features for forensic analysis on scanners and scanned images [J]. IEEE Trans on Information Forensics and Security, 2009, 4(3): 476-491

[59] Huang Yizhen. Can digital image forgery detection be unevadable? A case study: Color filter array interpolation statistical feature recovery [C] //Proc of the Visual Communications and Image Processing. San Francisco, CA: SPIE, 2005: 59602W-59602W-12

[60] Kirchner M, Bohme R. Synthesis of color filter array pattern in digital images [C] //Proc of the Media Forensics and Security. San Francisco, CA: SPIE, 2009: 72540K-72540K-14

[61] Li C T, Chang C Y, Li Yue. On the Repudiability of Device Identification and Image Integrity Verification Using Sensor Pattern Noise [G] //LNCS 45: Proc of the Int Conf on Information Security and Digital Forensics. Berlin: Springer, 2010: 15-29

[62] 杨弘,周治平. 数字图像模式噪声篡改反取证[J]. 计算机工程与应用, 2014, 50(18): 156-161

[63] Zeng Hui, Jiang Yunwen, Kang Xiangui, et al. Game theoretic analysis of camera source identification [C] //Proc of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conf. Piscataway, NJ: IEEE, 2013: 1-9

[64] Zeng Hui, Chen Jiansheng, Kang Xiangui, et al. Removing camera fingerprint to disguise photograph source [C] //Proc of the IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2015: 1687-1691

[65] Caldelli R, Amerini I, Novi A. An analysis on attacker actions in fingerprint-copy attack in source camera identification [C] //Proc of the IEEE Int Workshop on Information Forensics and Security. Piscataway, NJ: IEEE, 2011: 1-6

[66] Rao Quanquan, Luo Weiqi, Li Haodong, et al. Anti-forensics of the triangle test by random fingerprint-copy attack [C] //Proc of Computational Visual Media Conf. Piscataway, NJ: IEEE, 2013: 1-6

[67] Marra F, Roli F, Cozzolino D, et al. Attacking the triangle test in sensor-based camera identification [C] // Proc of the IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2014: 5307-5311

[68] Barni M. A game theoretic approach to source identification with known statistics [C] //Proc of the IEEE Int Conf on Acoustics, Speech and Signal Processing. Piscataway, NJ: IEEE, 2012: 1745-1748

[69] Stamm M C, Lin W S, Liu K J R. Forensics vs. anti-forensics: A decision and game theoretic framework [C] // Proc of the IEEE Int Conf on Acoustics, Speech and Signal Processing. Piscataway, NJ: IEEE, 2012: 1749-1752

[70] Wang Bo, Tan Yue, Zhao Meijuan, et al. Classifier combination based source identification for cell phone images [J]. KSII Trans on Internet and Information Systems, 2015, 9(12): 5087-5102

[71] Costa F d O, Silva E, Eckmann M, et al. Open set source camera attribution and device linking [J]. Pattern Recognition Letters, 2014, 39(1): 92-101

[72] Huang Yonggang, Zhang Jun, Huang Heyan. Camera model identification with unknown models [J]. IEEE Trans on Information Forensics and Security, 2015, 10 (12): 2692-2704

[73] 王波, 孔祥维, 尤新刚, 等. 基于协方差矩阵的 CFA 插值盲检测方法[J]. 电子与信息学报, 2009, 31(5): 1175-1179

[74] Miroslav Goljan, Mo Chen, Pedro Comesan □ a, et al. Effect of compression on sensor-fingerprint based camera identification [C] //Proc of the Media Watermarking, Security, and Forensics. San Francisco, CA: SPIE, 2016

[75] Goljan M, Fridrich J. Camera identification from cropped and scaled images [C] //Proc of the Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Francisco, CA: SPIE, 2008: 68190E

[76] Goljan M, Fridrich J. Sensor fingerprint digests for fast camera identification from geometrically distorted images [C] //Proc of the Media Watermarking, Security, and Forensics 2013. San Francisco, CA: SPIE, 2013: 866508

[77] Goljan M, Fridrich J, Lukáš J. Camera identification from printed images [C] //Proc of the Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Francisco, CA: SPIE, 2008: 68190I-68190I-12

[78] Goljan M, Fridrich J, Filler T. Large scale test of sensor fingerprint camera identification [C] //Proc of the Media Forensics and Security XI. San Francisco, CA: SPIE, 2009: 725401-725401-12

[79] 谭跃, 王波, 赵美娟. 有限样本条件下的相机来源鉴别方法[C] //第十二届全国信息隐藏暨多媒体信息安全学术大会论文集, 2015: 448-454

[80] Tan Yue, Wang Bo, Li Ming, et al. Camera source identification with limited labeled training set [G] //LNCS 9569: Proc of the 14th Int Workshop. Berlin: Springer, 2016: 18-27

王 波

博士, 副教授, 主要研究方向为数字图像取证、信息隐藏与信息隐藏分析.

bowang@dlut.edu.cn

杨福龙

硕士研究生, 主要研究方向为数字图像来源鉴别.

153672870@qq.com