Journal of Image and Signal Processing 图像与信号处理, 2014, 3, 9-14
http://dx.doi.org/10.12677/jisp.2014.31002 Published Online January 2014 (http://www.hanspub.org/journal/jisp.html)

The Summaries of Blind Digital Image Forensics Based on the Traces of Tamper

Huanwen Wang[1], Xiaogang Xu[2], Guanlei Xu[3], Xiaotong Wang[2]

[1]Department of Communication, Dalian Naval Academy, Dalian
[2]Department of Navigation, Dalian Naval Academy, Dalian
[3]Department of Military Oceanography, Dalian Naval Academy, Dalian
Email: wanghw133@163.com

Received: Dec. 4th, 2013; revised: Dec. 18th, 2013; accepted: Dec. 20th, 2013

Abstract: Blind digital image forensics is a new kind of technique to protect the security of image information. It can detect image authenticity and source without any pre-extraction or pre-embedded information. With great practical value, it has been a new research focus of the current field of security. Taking Blind digital image forensics which is based on the traces of tamper for an example, this paper makes a summary from five aspects: copy-paste forgery, blurring detection, JEPG detection, inconsistence detection in the light source direction and resampling. The typical algorithms are introduced selectively and the future research and development tendency are pointed out.

Keywords: Blind Forensics; Copy-Paste Forgery; Blurring Detection; JPEG Image

基于遗留痕迹的数字图像盲取证综述

王焕文[1]，徐晓刚[2]，徐冠雷[3]，王孝通[2]

[1]海军大连舰艇学院通信系，大连
[2]海军大连舰艇学院航海系，大连
[3]海军大连舰艇学院军事海洋系，大连
Email: wanghw133@163.com

收稿日期：2013 年 12 月 4 日；修回日期：2013 年 12 月 18 日；录用日期：2013 年 12 月 20 日

摘　要：数字图像盲取证是一种新颖的图像信息安全技术，它能够在没有前期预签名或嵌入信息等先验条件下，完成对图像真伪和来源的认证，具有更广的实用价值，成为目前安全领域新的研究热点。本文以基于遗留痕迹的数字图像盲取证为代表，从复制－粘贴检测、模糊篡改检测、JPEG 相关检测、照明不一致检测和重采样检测五个方面进行综述，对与之相应的典型算法进行了重点介绍，并对未来的发展进行展望。

关键词：盲取证；复制－粘贴检测；模糊篡改检测；JPEG 图像

1. 引言

随着科技的发展和进步，人们不仅可以随时抓拍生活瞬间，还可以通过诸如 Photoshop、美图秀秀、光影魔术手等含有图像编辑功能的软件将图像美化，增强图像效果，图像处理软件的出现，使普通大众享受高科技带来的愉悦，同时，也给一些不法分子篡改事实真相的可乘之机。“华南虎事件”就是一个很好的例子，犯罪分子用被篡改过的图像，成功吸引了大

众的眼球。据此，我们还能否简单的以图像作为证据？答案显然是否定的，我们必须首先对图像的真实性进行检测分析，然后才能决定是否以其为依据展开行动。

传统的数字签名和数字水印鉴别技术[1]都需要对原始图像进行信息嵌入处理[2]，有很大的局限性。而图像盲取证技术[3]是一种无需对图像预处理就能鉴别图像真伪和来源的技术，因此有着广阔的应用前景，吸引了国内众多学者、院校和科研机构投入到该领域中来。其中，北京邮电大学、大连理工大学信息安全研究中心、北京交通大学、湖南大学等都在进行相关方面的研究，并取得了一定的成果。

本文针对图像篡改遗留痕迹盲取证技术进行了分类和总结，并对该技术中的复制－粘贴检测[4]、模糊估计检测[5]、JPEG 相关检测[6]、光照不一致性检测[7]和重采样检测[8]的点进行了归纳，列举了其中与之相应的典型方法，并在最后分析了在该领域还存在的问题。

2. 基于遗留痕迹的数字图像盲取证

目前，数字图像取证技术可分为基于图像内容认证和基于图像来源的认证两大类[9]。前者研究内容广泛，包括图像复制－粘贴检测、重采样检测、模糊估计检测、光照不一致性检测、JPEG 相关检测、统计特性检测等方面；后者研究的主要热点在相机镜头检测、扫描仪识别、电脑制图和相机图像的识别等。

2.1. 复制－粘贴检测

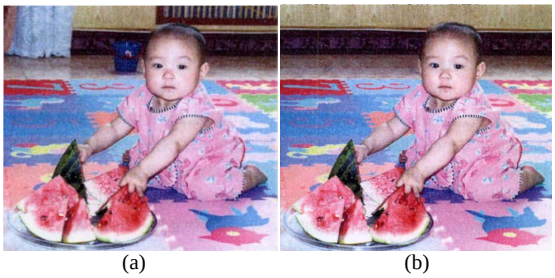
在图像篡改方式中，复制－粘贴篡改是最简单也是最常用的图像修改手段。这种伪造操作分为同一幅图像中的篡改和不同图像之间的篡改。

2.1.1. 同幅图像复制－粘贴篡改检测

同幅图像复制－粘贴篡改就是复制区域和粘贴区域均出自一幅图片，正如图 1 中所示，通过复制一块地板和墙壁的区域，覆盖原有的窗帘、水桶和暖气片。这种操作由于变化不明显，通过肉眼极难被察觉。但是它还是存在较大的破绽，而且当前对这种篡改检测的算法比较多，这些算法大致可以分为以下几类：

1) 遍历搜索法。

这种方法是将图像分块后，选取某一图像块为模版，遍历剩余图像块，检测有无和模版完全一样的图



(a) (b)

Figure 1. **Copy-paste tampering in one picture; (a) Original image; (b) Tampered image**

图 1. **同一幅图像中进行复制－粘贴操作；(a) 原图；(b) 窜改图**

像块。对于图像块匹配检测来讲，穷举搜索无疑是一种最简单的办法。但穷举搜索有两个最大的缺点，一是计算量大，二是对于模糊匹配的搜索结果判定阈值不好设定[10]。

2) 图像块自相关矩阵法

这种方法是根据两个复制－粘贴的图像块完全相同而具有很强的自相关性的原理进行搜索的。该方法首先设定自相关判别阈值，再遍历搜寻所有图像块，如果搜寻到超过设定阈值的两个图像块，则认为这两个图像块中的一块是另一块的复制－粘贴块。这种方法的优点是运算量相对遍历搜寻法小，缺点是只能检测出较大复制－粘贴图像块。

3) 图像块匹配法。

图像块匹配法是在分块的基础上，用一个矩阵去表示每一个图像块，然后通过比较所有的图像块矩阵找到相同的图像块。Fridich 提出了利用 DCT 量化系数来进行字典排序的方法[11]，将点操作改进成了块操作，提高了运算速度。Popescu 和 Hany Farid 利用了 PCA 对提取的特征进行了适当的降维处理[12]，提高了后续处理的时间性能。方君丽提出了基于主转移向量的数字图像复制－粘贴盲取证检测方法[13]，该方法主要思想是将图像分成一定大小的重叠的图像块，然后提取每个图像块的七个特征作为图像块的特征向量，这种操作能够减少错误的匹配图像块。吴琼等人提出了一种基于 SVD (Singular Value Decomposition)同幅图像复制－粘贴篡改取证算法。该算法利用图像小波变换的降维特性大大降低了算法的时间冗余度，但是由于 SVD 是图像特征近似的特征量提取，而且阈值的设定没有理论可依，所以该取证算法的虚警概率不稳定。

2.1.2. 不同幅图像间复制－粘贴篡改检测

不同幅图像间复制－粘贴篡改如图 2 所示，是将

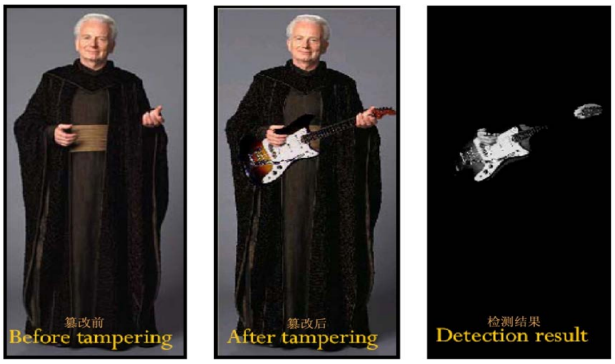


Figure 2. Copy-paste tampering in different pictures
图 2. 不同图复制粘贴篡改检测

两张或多张图像中的不同部分拼接在一起，进而达到掩盖原图信息，制造假象的目的。相比于同一幅图像，多幅图像间复制－粘贴操作后的亮度、色彩区别较大，拼接边缘比较明显，篡改者为了抹去篡改边缘的痕迹，通常会选择边缘模糊等润饰操作。由于不同幅图像间的复制－粘贴并非简单的单一操作，还涉及了其它篡改手段，因此，对不同幅图像间的复制－粘贴检测的方法，本文不再详细介绍，将在介绍其它方法时予以提及。

2.2. 模糊估计篡改检测

在一些实际情况中，为了更好地消除拼接伪造边缘，造假者往往会利用润饰操作对伪造图像进行进一步地润色和修饰，以达到更好的伪造效果。典型的润饰操作有模糊、锐化、涂抹和羽化等。其中，模糊操作的重要作用就是将明显的边缘淡化甚至消除，因此，模糊操作成为篡改伪造图像最为常见也是最为重要的操作之一，而模糊篡改检测，则成为检测图像是否被篡改的重要手段之一。

近年来，国内外的研究人员针对模糊篡改检测开展了一系列的研究，其主要方法包括：

2.2.1. 边缘检测法

卢燕飞等人提出一种针对图像高斯模糊处理痕迹的检测算法[14]，根据图像处理中高斯模糊的基本特性，首先对被检测原始图像采用不同的高斯半径进行二次模糊处理，然后用提出的算法来比较二次模糊后图像边缘的变化情况，发现原始图像的高斯模糊特性，从而发现原始图像中异常模糊处理的痕迹。实验表明这种方法对于实现图像篡改的被动盲检测具有较好的应用价值。

李杭等人提出了一种基于边缘宽度的伪造图像检测方法[15]，该方法通过确定图像的边缘像素，计算边缘的宽度，去除较细边缘保留宽边缘等手段确定伪造数字图像的篡改区域。经实验验证，文中方法能有效地检测出伪造图像中经过模糊操作的边缘，从而确定伪造区域。

王俊文等人提出了一种利用图像正常边缘点和模糊边缘点在 NSCT 后的差异性进行人工模糊检测的方法[16]，根据每个边缘点 NSCT 后的高频信息将其分为强边缘点、次强边缘点和弱边缘点三类，算法指出模糊操作对这三类边缘点会产生一定的影响，导致异常边缘点出现，此种区分两类模糊的方法效果并不是非常明显，不过该算法的确有效地检测出了人工模糊边界，并且具有像素级别的定位能力。

2.2.2. 滤波法

周琳娜等人提出了一种基于数字图像边缘特性的形态学滤波取证技术[17]。通过分析模糊对图像边缘特性的影响，采用同态滤波方法增强人工模糊边缘，可有效检测出图像伪造中的拼接模糊边缘。

何超等人提出了一种基于公共因子提取的模糊篡改检测算法[18]。将图像的线性空间滤波转换成按照行和列方向的一维卷积，通过判断提取出公共因子系数之间的方差来进行篡改检测。该方法特别适用于轻微模糊的情况并且可以同时检测图像的 copy_move 型篡改。实验说明了该方法对数字图像被动认证的有效性。

2.2.3. 统计特性

潘生军等人提出一种人工模糊痕迹检测方法[19]。将经过模糊操作后图像像素之间存在的高度相关性进行模型化表示；采用 EM 算法估算出图像中每个像素属于上述模型的后验概率；根据所得后验概率的大小进行模糊操作检测。实验结果表明，该算法能够有效地检测出篡改图像中的人工模糊痕迹，并对不同模糊类型、有损 JPEG 压缩以及全局缩放操作均具有较好的鲁棒性。

王波等人通过分析由成像系统形成的局部色彩相关性，利用成像系统和模糊操作在数字图像局部色彩属性的差异，定义数字图像异常色调集合和异常色调率的概念，提出了一种基于异常色调率的数字图像取证技术[20]。实验表明，该方法能够有效地检测出对

数码相机拍摄图像进行模糊操作的痕迹，并能够对经过模糊操作的图像局部进行准确判断。

2.3. JPEG 相关检测

由于 JPEG 图像具有可以用较少的磁盘空间获得较好的图像质量的优点，因此其应用非常广泛，大部分额的网络，光盘读物，数码设备都可以见到 JPEG 格式图像的身影。也正因如此，一些不法分子以此类图像作为攻击目标，对其进行过剪切、旋转、采样、压缩，或者复制－粘贴等操作，进而达到掩盖真相的目的。而这个过程之后，必须将图像重新保存为质量因数不同的 JPEG 图像，这就会出现 JPEG 重压缩现象，即检测篡改的突破口。其算法主要包括：

2.3.1. 量化特征检测

J. Fridrich 用直方图特征，通过神经网络对一系列量化阶梯模式组合进行重压缩检测。Lukas 在双重压缩检测的基础上，进一步研究了从 JPEG 双重压缩图像中估计出原始量化表的方法。Hany Farid 教授利用 JPEG 重压缩会使图像 DCT 变换系数的直方图产生的周期性模式来检测和质疑图像的真实性[21]。

扈文斌等人利用篡改后 JPEG 图像量化表不一致的特性，提出一种针对 JPEG 图像的篡改盲检测新方法[22]。通过智能选取若干图像块，迭代估计出待测图像的原始量化表，大致定位出篡改区域。然后用估计出的原始量化表对篡改区域再进行一次 JPEG 压缩，由压缩前后图像像素值的差值最终确定篡改位置。该算法有算法复杂度小，精度高的特点，能有效地检测出多种篡改类型的 JPEG 图像，且对篡改区域和未篡改区域压缩因子相差较小的 JPEG 合成类篡改，检测正确率更高。

吴首阳等人通过研究 JPEG 压缩过程中的量化相关性特征，提出一种基于量化相关性测度的真伪图像盲检测方法[23]，可以对不同压缩参数的图像进行检测，辨别 JPEG 图像的真伪，并标定修改区域。实验结果表明，即使待检测图像经历过多次不同质量因子的 JPEG 压缩，该方法有较高的灵敏度同样具有有效性和鲁棒性。

2.3.2. 块效应检测

魏为民等人提出了一种盲检测 JPEG 合成图像的方法[24]。将图像与 Laplacian 模板卷积得到二阶差分图像，沿水平(垂直)方向平均后进行离散 Fourier 变换得到归一化的频谱，基于频谱幅值构造 JPEG 块效应测度；然后将待检测图像重叠分块并计算其相应块效应测度。该方法利用块效应不一致性，能够快速有效检测篡改区域。

孟宪哲等人根据图像篡改引起的双重 JPEG 压缩特征，提出了分块检测的图像篡改鉴定方法[25]。通过检测每个分块的 DCT 系数，来确定分块经历的 JPEG 压缩情况，并指出篡改类型和篡改位置。当篡改者对篡改过的图像使用原始图像的质量因子保存时，分块的方法无法进行检测，作者提出了滑窗检测的思想，通过滑窗寻找篡改的位置，补充了分块方法的不足。该方法能够检测 JPEG 图像之间的拼接篡改以及双重 JPEG 压缩篡改，拓广了双重 JPEG 压缩取证的检测范围。

赵峰等人对 JPEG 图像整体块效应的分析，定义了新的针对图像局部区域的块效应评价，并由此提出了一种有效的 JPEG 伪造图像盲取证方法[26]。通过获取待测图像在水平方向和垂直方向的差分图像，并对其进行特定大小的分块处理，计算每个分块区域的局部块效应评价，根据待测图像在不同区域局部块效应评价的明显差异分别从水平方向和垂直方向检测出图像被篡改区域的具体位置。该方法可以有效的检测出经过 JPEG 双压缩的伪造图像，进一步使用不同大小的滑块和不同的评价公式对伪造图像进行检测，并从抗干扰性和算法效率上比较不同算法的利弊。

2.4. 光照方向不一致检测

在正常情况下，图像篡改很难将光照效果和定向的光源相匹配，因此可将图像拍摄场景中光照方向的不一致性作为图像篡改的证据。在计算机视觉领域中，光照方向的估计问题已得到了广泛研究。

美国麻省理工大学博士后 Micah K. Johnson 和 Dartouth 大学教授 Hany Farid 最早将光源方向的估计问题引入到数字图像篡改取证的研究领域，提出了从单一的数字图像中估计该图像拍摄场景中的光源方向的理论和方法，对图像盲取证技术的研究具有开拓性意义。

对图像光源方向的计算，以漫反射的理论作为基础。而 Lambert 模型，是最简单的漫反射模型，可以作为计算光源方向的光照模型，如图 3 所示。陈海鹏

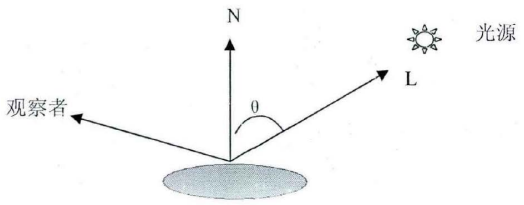


Figure 3. Lighting model of Lampert
图 3. Lampert 光照模型

等提出了基于 Lambert 光照模型的图像真伪盲鉴别算法[27]。针对无限光源图像和局部光源图像，根据其实际的光强度与计算出的光强度之间的误差函数以及光源对光线的约束函数，用相应的算法计算图像中不同区域的光源方向，并根据这些不同区域的光源方向是否一致判定图像是否被篡改，从而对图像真伪进行盲鉴别。

2.5. 重采样检测

检测图像重采样技术是数字取证中发现图像是否被篡改的有效途径之一。篡改者在拼接操作的时通常会将某一图像放大、缩小或者旋转等操作，这样的步骤通常需要运用插值技术对图像进行重采样使其位于一个新的采样网格中。对于重采样的检测，目前主要是基于重采样过程中的插值操作导致的图像某些统计特性发生的特殊变化来实现的。现有的检测方法包括两类[28]，一类是基于分析插值步骤所引起的像素之间的相关性的变化，如图 4 所示，而另一类是通过检测插值信号的二阶导数存在一定周期性来进行重采样的检测。

popeseu 采用期望最大化 EM(Expectation Maximization)算法来检测图像是否经历过重采样操作[29]。利用 EM 算法得到了每个像素点是其周围像素线性组合的概率，那么就可以通过判断这些概率是否存在周期性来检测图像的重采样。Popescu 提出的基于 EM 算法的图像重采样检测方法可以有效的检测出未压缩图像的尺度变换和旋转。

Gallagher 发现重采样图像中，二阶导数的方差信号存在周期性，并以此作为鉴别特征来对重采样进行检测[30]。对周期性的检测同样也是变换到频域，重采样的信号的幅度谱中有明显的峰值，非重采样的信号一般没有。Gallagher 的算法有一个重要的功能，可以部分确定重采样因子。

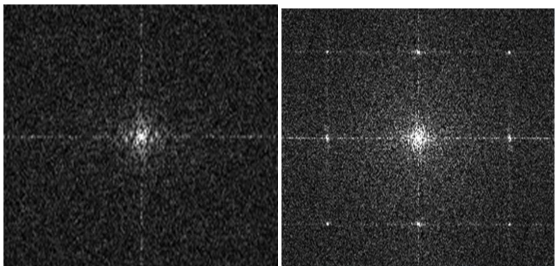


Figure 4. The probability matrix spectrum of resampling image in contrast with original image; (a) The probability matrix spectrum in original image; (b) The probability matrix spectrum in resampling image
图 4. 原始图像和重采样以后的概率矩阵频谱对比；(a) 原始图像概率矩阵频谱；(b) 重采样以后图像的概率矩阵频谱

3. 结束语

基于图像篡改遗留痕迹的盲取证，是在没有任何先验信息的情况下为鉴别图像真伪提供有力证据，其关键是找出充分、可靠、有说服力的证据来证明图像是否发生篡改。本文从复制－粘贴检测、模糊篡改检测、JPEG 相关检测、照明不一致检测和重采样检测五个方面，总结了国内外图像篡改遗留痕迹的盲取证技术，针对不同的篡改方法，列举了现有的一部分经典检测算法。从总体来看，目前数字图像篡改检测理论还不够全面，单个检测方法的局限性太大，自动鉴别能力不高，如果能够解决这些问题，数字图像盲取证技术将迎来它的巅峰，盲取证技术也会具有更大的实用价值。

项目基金

船载航行数据记录仪(VDR)图象篡改鉴别技术研究(61250006)；基于调制解调的图象多分辨率分解理论与方法(61273262)；广义测不准原理及其应用研究(61002052)。

参考文献 (References)

[1] Farid, H. (2009) Image forgery detection. *IEEE Signal Processing Magazine*, **26**, 16-25.
[2] Fridrich, J. (2009) Digital image forensics. *IEEE Signal Processing Magazine*, **26**, 26-37.
[3] 吴琼, 李国辉, 孙韶杰 (2008) 基于小波和奇异值分解的图像复制伪造区域检测. *小型微型计算机系统*, **29**, 730-733.
[4] 蔡明伟 (2012) JPEG 图像复制－粘贴篡改的盲取证技术研究. 杭州电子科技大学, 杭州.
[5] 杜加玉 (2010) 数字图像取证中的模糊与重采样检测研究. 大连理工大学, 大连.

[6] Farid, H. (2009) Exposing Digital Forgeries from JPG Ghosts. *IEEE Transactions on Information Forensics and Security*, **1**, 154-160.
[7] Johnson, M.K. and Farid, H. (2007) Exposing Digital Forgeries in Complex lighting Environments. *IEEE Transactions on Information Forensics and Security*, **2**, 450-461.
[8] Popescu, A and Farid, H. (2005) Exposing digital forgeries by detecting traces of re-sampling. *IEEE Transactions on Signal Processing*, **53**, 758-767.
[9] 魏为民 (2010) JPEG 图像篡改的盲检测技术. *计算机工程与应用*, **46**, 164-166.
[10] 周琳娜 (2007) 数字图像盲取证技术研究. 北京邮电大学, 北京.
[11] Fridrich, J. Soukal, D and Lukas, J. (2003) Detection of copy—move forgery in digital images. *Proceedings of Digital Forensic Research Workshop*, 55-61.
[12] Popescu, A. and Farid, H. (2004) Exposing digital forgeries by detecting duplicated image regions, TR2004-515. Dartmouth College, Hanover, 1-11.
[13] 方君丽 (2009) 自然图像复制粘贴和模糊操作篡改盲取证. 硕士论文, 北京交通大学, 北京.
[14] 卢燕飞, 荆涛 (2011) 利用图像边缘变化特性寻找模糊处理痕迹. *信号处理*, **27**, 732-736.
[15] 李杭, 郑江滨 (2012) 一种人工模糊的伪造图像盲检测方法. *西北工业大学学报*, **30**, 612-616.
[16] 王俊文, 刘光杰, 戴跃伟, 等 (2009) 基于非抽样 Contourlet 变换的图像模糊取证. *计算机研究与发展*, **46**, 1549-1555.
[17] 周琳娜, 王东明, 郭云彪, 杨义先(2008) 基于数字图像边缘特性的形态学滤波取证技术. *电子学报*, **36**, 1047-1051.
[18] 何超, 方勇 (2011) 基于公共因子提取的数字图像篡改检测. *系统仿真技术*, **7**, 6-10.
[19] 潘生军, 杨本娟, 刘本永 (2012) 基于后验概率的图像模糊检测方法. *计算机工程与应用*, **48**, 181-186.
[20] 王波, 孙璐璐, 孔祥维, 尤新刚 (2006) 图像伪造中模糊操作的异常色调率取证技术. *电子学报*, **34**, 2451-2454.
[21] Fridrich, J. and Lukas, J. (2003) Estimation of primary quantization matrix in double compressed JPEG images. Digital Forensics Research Workshop, Ohio.
[22] 扈文斌, 刘凯 (2011) 基于量化表不一致性的 JPEG 图像篡改盲检测. *中国图象图形学报*, **16**, 316-323.
[23] 吴首阳, 刘铭 (2010) 基于量化相关性的 JPEG 图像盲取证. *计算机仿真*, **27**, 258-266.
[24] 魏为民, 唐振军 (2009) 利用 JPEG 块效应不一致性的合成图像盲检测. *中国图象图形学报*, **14**, 2387-2390.
[25] 孟宪哲, 牛少彰, 李叶舟, 朱艳玲, 胡静 (2010) 基于双重 JPEG 压缩特征的数字图像篡改取证技术. 第九届全国信息隐藏暨多媒体信息安全学术大会会议论文集, 342-349.
[26] 赵峰, 刘晓腾, 荆涛, 李兴华, 霍炎 (2010) 基于局部块效应的 JPEG 伪造图像的盲取证. *信号处理*, **26**, 1805-1811.
[27] 陈海鹏, 申铉京, 吕颖达, 金玉善 (2011) 基于 Lambert 光照模型的图像真伪盲鉴别算法. *计算机研究与发展*, **48**, 1237-1245.
[28] 郝丽 (2009) 数字图像重采样检测研究. 大连理工大学, 大连.
[29] Popescu, A. and Farid, H. (2005) Exposing digital forgeries by detecting traees of re-sampling. *IEEE Transactions on Signal Processing*, **53**, 758-767.
[30] Gallagher, A.C. (2005) Detection of linear and cubic interpolation in JPEG compressed images. The 2nd Canadian Conference on Computer and Robot Vision, 65-72.