Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Cybersecurity—Review

简述图像被动取证技术

林祥 [a], 李建华 [a], 王士林 [a,*], 刘伟聪 [b], 程峰 [a], 黄潇洒 [a]

[a] School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China
[b] School of Information and Communication Technology, Gold Coast Campus, Griffith University, Southport, QLD 4222, Australia

ARTICLE INFO

Article history:
Received 8 December 2017
Revised 20 December 2017
Accepted 15 February 2018
Available online 17 February 2018

关键词
数字图像取证
图像篡改检测
多媒体安全

摘要

随着图像编辑和篡改技术越发成熟，数字图像的真实性通常难以从视觉上直接分辨。为了检测数字图像篡改，在过去十年内，已经出现多种数字图像取证技术。其中，主动取证方法需要嵌入额外信息。相比之下，被动取证方法因为其适用场景更广而更加流行，也吸引了学术界和工业界越来越多的研究兴趣。一般而言，被动取证基于以下依据来检测图像伪造：图像采集或存储过程中会在原始图像中遗留某些固有的模式特征，或者在图像存储或编辑过程中会留下某些特定的模式特征。通过分析上述模式特征，可以验证图像的真实性。被动数字取证方法正处于快速发展之中，本文简要回顾其发展，并全面介绍该研究领域的最新进展。根据所追踪痕迹的不同，这些取证方法被分为 3 类，即采集痕迹法、存储痕迹法和编辑痕迹法。我们将逐一详解这些方法的取证场景、基本原理和研究现状。此外，我们讨论了当前图像取证方法的主要局限，并指出了该领域一些可能的研究方向和关键问题。

1. 引言

过去10年中，数字图像在日常生活中越发流行。和传统文本内容相比，图像更加直观并能传递更多信息。尽管数字图像带来了很多好处，但是它也在一些方面带来了严重的安全问题，即如何检测数字图像的真实性，以及如何发现恶意修改。随着图像处理软件的进步，篡改图片而不留下视觉上可辨的痕迹更加容易，这使得上述问题更具挑战性[1]。

为了精确并鲁棒地鉴定图像内容和发现图像造假，研究者已经提出了多种数字图像取证方法。一般而言，这些方法可分为两大类：主动方法和被动方法[2]。主动取证方法通常通过设计各种水印或指纹，并将它们嵌入数字图像。在鉴定阶段，提取先前嵌入的水印或指纹，并用来检测判断原图是否被篡改。如果被篡改，则确定篡改位置在何处[3]。这种主动方法能够精确探测数字图像的篡改，但是这些方法并未被广泛应用。其主要原因在于不可能事先对所有互联网上的图像进行水印处理。因此，更多的人选择被动取证方法。通过分析图像生成/修改阶段所留下的特定线索或模式，能够发现图像造假[4]。和主动取证方法相比，被动取证方法不依赖先验或预设信息，在图像取证领域中应用范围更广。

在被动数字图像取证中，多种痕迹被用来区别篡改图像和原始图像[5]。本文中，我们将这些痕迹分为3类：

* Corresponding author.
E-mail address: wsl@sjtu.edu.cn (S.-L. Wang)

2095-8099/
英文原文: Engineering 2018, 4(1): 29–39
引用本文: Xiang Lin, Jian-Hua Li, Shi-Lin Wang, Alan-Wee-Chung Liew, Feng Cheng, Xiao-Sa Huang. Recent Advances in Passive Digital Image Security Forensics: A Brief Review. *Engineering*, https://doi.org/10.1016/j.eng.2018.02.008

采集痕迹、存储痕迹和编辑痕迹。对每一种痕迹，我们将简要回顾对应的被动数字取证方法，并着重澄清如下问题：

- 这些痕迹是什么？它们如何形成？
- 图像取证中相关的最新方法是什么？
- 为什么这些方法能够探测特定的痕迹？

本文的组织如下：第2~4节，我们逐一介绍被动数字图像取证方法，包括：采集痕迹法、存储痕迹法和编辑痕迹法。第5节讨论当前技术的主要局限，并提出未来可能的研究方向。

2. 图像采集中的线索

数字图像从被捕获到被存储，中间需要经历多个处理步骤（图1）。在进入成像设备之前，光线首先会通过一系列镜头。之后，成像设备将其传送到彩色滤色阵列（color filter array，CFA）进行特定的彩色像素排列处理，其仅允许光线的特定成分通过。大多数相机的CFA单元只允许每个像素记录一种颜色的值（红、绿、蓝）。在经过CFA滤波后，光线到达图像传感器——数码相机的关键部分。目前，有两种广泛使用的传感器：电荷耦合器（charged coupled device，CCD）和互补金属氧化物半导体（complementary metal-oxide semiconductor，CMOS）。图像传感器中包含大量光敏二极管，每个光敏二极管与图像的像素一一对应。在每个光敏二极管中，经CFA滤色后的光强被转换为电信号。得到的图像数据的每个像素点表示红、绿、蓝中的一种颜色。因此，为了重建全彩图像，需要进行解镶嵌/去马赛克（demosaic）处理，即通过在所有颜色通道上进行插值，重建缺失的色彩分量。

上述每个阶段都会在最终图像中引入特定痕迹。这些可以作为图像源识别和篡改检测的线索。以下几个小节简要介绍了镜头阶段、传感器阶段和CFA插值阶段所留下的痕迹，以及利用这些痕迹进行图像取证的典型方法和目前最先进的方法。

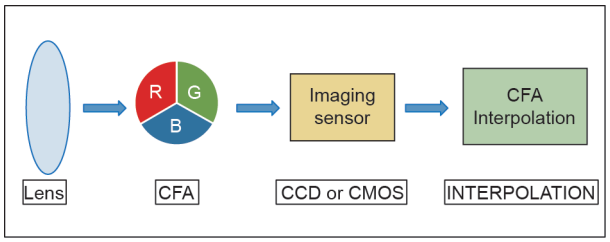

图1. 图像采集流程图。

2.1. 图像采集阶段的痕迹

在采集图像时，镜头的设计和制作工艺使得其无可避免地引入失真/像差。数码相机有两种常见的失真：色差（chromatic aberration，CA）和球面差（spherical aberration，SA）。不同波长的光线通过透镜时的折射率也各不相同，这种现象称为色差现象；轴上物点发出的光束，经球面折射后不再交于一点，这种现象称为球面像差。

传感器模式噪声是图像采集阶段另一种重要特性。在各种传感器噪声中，由光响应不均匀性（photo response non uniformity，PRNU）引起的噪声尤为重要。目前学术界已经提出了多种基于PRNU噪声的数字图像取证方法，涵盖源识别、历史恢复、图像伪造检测等多个领域。PRNU是与成像传感器紧密相关的特性，通过分析图像PRNU可以获得关于成像设备的线索。

CFA过程中的解镶嵌/去马赛克操作同样会留下特定痕迹。在色彩重建时，为了获取图像中每个像素的对应值，需要对3个颜色通道进行插值操作。插值过程不可避免地会在像素之间引入一定的关联性，这种相关性可以被看作是成像设备的固有“指纹”。通过分析解镶嵌/去马赛克痕迹，可以获得成像设备的线索。

2.2. 利用图像采集痕迹的图像取证

2.2.1. 基于传感器噪声的图像取证

利用相机镜头产生的像差，可以将图像与特定设备相关联，或检测图像是否经过篡改。例如，图像中经常出现的径向畸变现象会导致所成图像发生形变。为解决径向失真问题，数码相机制造商通常会采用各种方法来补偿失真，这些方法相应地会产生不同的痕迹。因此，通过分析这些痕迹可以识别相机制造商甚至相机型号。

传感器模式噪声通常会被用于图像取证。对于图像I，其对应的传感器噪声可以通过以下公式表述：

$$R = I - F(I) = I \times P + \varphi \qquad (1)$$

式中，R是总体残差，即原始图像减去经过去噪滤波器F滤波后的图像；P是PRNU因子；φ是图像中其他所有噪声的总和。

假设我们有同一摄像头捕获的N幅图像$I_1, \ldots, I_N$，对应的残差R_k可以通过公式（1）得到。PRNU因子P可以通过最大似然估计，按照以下公式进行计算：

$$P = \frac{\sum_{k=1}^{N} R_k I_k}{\sum_{k=1}^{N} (I_k)^2} \qquad (2)$$

在相机识别中，假设存在M个设备，则需要计算M次PRNU因子，并且针对每个设备（$i = 1,2,\ldots, M$）记录特定的P_i值。在检测阶段，对于待测图像I_t，首先通过公式（1）即$R_t = I_t - F(I_t)$计算残余项。然后，PRNU因子与该残差R_t之间的相关性通过以下公式计算：

$$\tilde{n}_i = I_t P_i \otimes R_t \quad (3)$$

式中，⊗代表归一化互相关；$\tilde{n}_i$最大值对应的设备即为目标设备。

2.2.2. 基于 CFA 痕迹的图像取证

基于CFA痕迹的取证方法的基本原理是，原始图像非篡改区域和篡改区域具有不同的CFA模式。因此，对被检测图像的每个分块进行CFA模式计算，如果存在不同的CFA模式，则为篡改图像，并可以得到篡改区域。另外，由于不同的解镶嵌/去马赛克算法会使得同一颜色通道中相邻像素之间的关联性不同，因此基于CFA模式的图像取证可以分为两个方向：①预测插值参数并识别成像设备的类型；②检查解镶嵌/去马赛克痕迹以找出可能被篡改的区域。

2.3. 最先进的基于采集的图像取证方法

2.3.1. 基于镜头像差的成像设备源识别

如2.1小节所述，不同的相机具有不同的镜头像差，因此镜头像差可以作为源识别中设备的固有“指纹”。Choi等[6]在这方面进行了开创性的工作：鉴于径向畸变会使得直线变弯曲，他们基于像素灰度和畸变程度提出两类特征，从而将成像设备源识别问题转变为二分类问题。与仅使用图像灰度的方法相比，Choi等[6]的方法实现了4%的检测精度提升。

2.3.2. 基于镜头痕迹的篡改检测

使用镜头痕迹进行图像伪造检测的基本思想是：原始图像和插入的图像块很可能来源于不同的拍摄设备。通过检测不同图像块是否具有同一镜头痕迹，可以鉴别图像是否经过伪造。Yerushalmy和Hel-Or [7]提出了一种镜头痕迹——“紫边失真”（purple fringing aberration，PFA）及相应的提取方法。PFA的方向特性被用作唯一的“指纹”来确定被测图像是否具有镜头痕迹不一致性。该算法在图像伪造检测和篡改检测中都取得了很好的效果。

2.3.3. 基于传感器模式噪声的成像设备源识别

由于传感器制造工艺的缺陷，不同像素具有不同的光敏性。因此，传感器噪声（特别是PRNU）可以用来区分各种传感器和相机类型。Lukas等[8]提出了基于PRNU的源识别方法，可以识别9种相机模型。Kulkarni和Mane等[9]注意到在边缘区域对传感器噪声的估计不够准确。基于这一发现，他们在特征提取操作之前进行了特定的预处理操作，利用Canny和Laplace算子进行边缘区域检测，并将检测出的边缘区域移除以做进一步处理。经阈值处理计算得到传感器噪声之后，通过灰度共生矩阵（gray-level co-occurrence matrix，GLCM）从离散小波变换（discrete wavelet transform，DWT）域提取多个统计特征。最后，采用k-近邻（k-NN）作为分类器对特征进行分类。考虑到手机摄像头识别这一应用场景，Sandoval Orozco等[10]提出了一种基于摄像头传感器缺陷的方法。同样从小波域提取特征在手机相机识别中取得了很好的效果。

2.3.4. 基于传感器指纹不一致的篡改检测

与镜头痕迹类似，传感器噪声可用于检测图像是否经过伪造。其基本想法是，篡改区域中的传感器噪声/指纹会与原始图像不一致，这一线索可以用来定位可疑的篡改区域。Fridrich [11]提出了一种基于PRNU信息的图像篡改检测方法。该方法通过建立统计模型来描述PRNU因子，提取出的PRNU因子同样可以用于成像设备识别。实验结果表明，这种方法在100种不同类型的相机检测中实现了近乎100%的准确性。

2.3.5. 基于 CFA 痕迹的成像设备源识别

如前所述，不同相机的CFA模式和解镶嵌/去马赛克操作会有所差异。Gao等[12]提出了一个基于这些信息的成像设备源识别方法。他们提取出69维的特征来描述上述痕迹。在Dresden图像数据库上的实验结果表明，在7类相机模型的识别中，该方法达到99.88%的准确率。

2.3.6. 基于 CFA 痕迹的篡改检测

在篡改检测中使用CFA痕迹的基本思想很简单：篡改区域与原始图像会呈现不同的CFA以及解镶嵌/去马赛克痕迹。Prasad [13]提出了一种描述图像解镶嵌/去马赛克痕迹的特征。如果存在异常区域（即没有原始图像CFA痕迹或具有与原始图像CFA不同的痕迹），则将其

视为篡改区域。Katre和Chandel [14]提出了一种既能检测图像伪造又能定位篡改区域的方法。通过对解镶嵌/去马赛克造成的痕迹进行建模，实现图像伪造检测。该方法对未压缩图像有很好的检测性能。然而，如何处理JPEG压缩图像仍然是一个具有挑战性的问题。

3. 存储过程中的线索

JPEG（joint photographic experts group）是图像传输和存储应用中最广泛使用的图像格式。由于JPEG是一种有损的压缩标准，因此，在图像存储过程中，JPEG将不可避免地引入某些特殊的压缩痕迹。通过分析这些痕迹，研究者可以推导出一些重要的取证线索，例如，①该图像被压缩了多少次；②图像中的所有区域是否被压缩过相同的次数。在之后的几个小节中，笔者将简要介绍JPEG压缩所留下的特定痕迹、JPEG图像取证的典型场景以及该领域最新的取证方法。

3.1. JPEG 压缩遗留的痕迹

针对灰度图像的标准JPEG压缩流程如下（通过在YCbCr色彩空间中的每个通道执行类似的流程，可以将JPEG压缩扩展到彩色图像）：首先，对原始图像上进行不重叠的8×8像素块分割；其次，针对每个块，对其灰度值进行2D-DCT变换，从而将该块从空间域变化至频率域；再次，对各频率分量的幅度通过预设的量化表来量化（其中，图2显示了品质因子为50的典型量化表，其中较大的质量因子表示较高的图像质量和较低的压缩比）；最后，采用熵编码技术（霍夫曼编码）将量化后的频率幅度转换为二进制序列进行存储。

JPEG压缩将对原始图像引入3种误差：量化误差、截断误差和取整误差。量化误差是由频域中的量化过程造成的。量化之后，特定DCT分量的原始值将由最接近的相应量化步长整数倍表示。例如，如果原始DC值为86，量化步长为16（图2），则量化后DC值将变为80，并将差值表示为量化误差（即86 − 80 = 6）。截断误差和取整误差在逆DCT变换中引入。由于图像每个像素点的灰度值应该是一个从0到255的整数，所以任何大于255或小于0的值都会被截断为255或0，这相应地会导致截断错误。另一方面，逆DCT变换后的大多数值不是整数，并且必须执行取整过程，从而造成取整误差。一般来说，量化误差远大于其他两个误差，特别是当品质因子为中或低（小于75）时。通过分析量化误差，可以推断出关于JPEG压缩的一些线索。

3.2. 基于 JPEG 压缩痕迹的图像篡改检测

考虑一个简单的图像篡改场景。我们从图像B中裁剪出一个小块I，并将其插入到图像A中生成一幅合成图像C（图3）。如果使用JPEG压缩存储所有图像A、B和C，则可以观察到以下现象。

3.2.1. 对齐的双 JPEG 压缩

在图像C中，除I之外的所有区域被压缩两次（一次是在存储图像A时，另一次在存储图像C时），并且区域I被压缩了一次。值得一提的是，虽然图像B也被JPEG压缩，但B的8×8像素点的块分割结构很可能（概率为63/64）与包含区域I的图像A的不同。在这种情况下，基于最终合成图像C的8×8块分割结构（与图像A的相同），图像C中的区域I仅被压缩一次（在存储图像C时）。因此，可以通过检查所有区域中是否包含对齐的双JPEG压缩区域来定位插入的区域I。在此处，术语“对齐”是指在前后两次压缩中采用相同的8×8块分割结构。

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

图2. 品质因子为50的量化表。

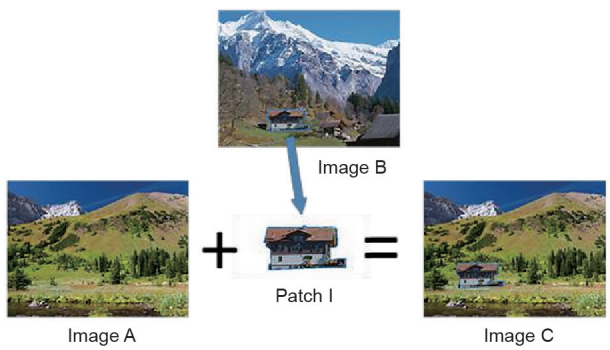

图3. 剪切–粘贴图像篡改示例。

3.2.2. 移位（非对齐）双 JPEG（SDJPEG）压缩

该种情况主要分析插入区域I，该区域的压缩分块结构本身和插入源图像B完全相同，即先进行了一次对齐JPEG压缩。之后，在合成图像C中，该区域有很大概率（63/64）进行了一次分块结构不一致的JPEG压缩。用于前后压缩的分块结构不一致，因此这种针对插入区域I的压缩痕迹被称为SDJPEG压缩。通过在最终图像C中检测是否包含有移位JPEG痕迹的区域，可以有效地检测图像拼接并定位插入区域I。

3.3. 最先进的双 JPEG 压缩检测技术

对于大多数篡改图像来说，最终图像至少进行了两次JPEG压缩。因此，双JPEG压缩检测是数字图像取证中的关键一环。具有代表性的双JPEG压缩检测方法可参考文献[15–21]，其中，最早的检测方法之一是由Lukas和Fridrich[15]提出的，他们发现双JPEG压缩会在DCT直方图中产生两个峰值，并将其作为检测双重JPEG压缩区域的线索。Fu等[16]提出了一个基于广义Benford定律的双JPEG压缩检测方法，并假定JPEG压缩后的DCT系数的第一个数字服从广义Benford定律的分布。进而，违反该假设的任何图像区域被确定为双JPEG压缩区域。Pevny和Fridrich [17]提取了一些低频DCT系数直方图作为检测特征，并使用支持向量机（SVM）作为分类器。Farid [18]指出，如果图像经过了双重JPEG压缩，那么具有相同品质因数的再次压缩会产生最小的重建误差。他将这种最低重建误差的现象称为“JPEG鬼影”，并试图通过搜索JPEG鬼影来检测双重压缩。Lin等[19]提出了一种基于双JPEG压缩检测的篡改区域定位算法，通过假设单JPEG压缩后的DCT系数遵循拉普拉斯分布来推导双JPEG压缩后的系数分布。随后采用期望最大化（EM）优化算法，预测图像中每个区域被双重压缩的概率。最后通过图切割的算法来避免误报。该算法通常适用于具有不同质量因素的双重压缩。但是，当前后两次压缩使用相同的量化表时，大多数现有方法不能实现高精度检测。鉴于此，Huang等[20]设计了一种算法，针对性地检测具有相同质量因子的双JPEG压缩。他们观察到第一次与第二次JPEG压缩之间的差异往往远小于第二次和第三次JPEG压缩之间的差异，通过引入随机扰动策略进行相应的检测。Yang等[21]扩展了这个想法，并全面分析了品质因子相同的两次JPEG压缩中存在的错误块。着重分析了取整误差和截断误差，并相应提取了描述单次和双重JPEG压缩之间差异的一组特征。通过使用SVM分类器，他们的算法[21]能够在质量因子相对较高的情况下准确检测具有相同品质因子的双重JPEG压缩。

当原始图像（即在图3中的图像A）是未压缩图像时，在合成图像中（即在图3中的图像C中）不会存在对齐的双JPEG压缩痕迹。为了在这种情况下检测合成图像，研究人员试图研究SDJPEG压缩效应[22–27]。Luo等[22]通过提出了块伪影特征矩阵（blocking artifact characteristics matrix，BACM）的特定特征来检测SDJPEG压缩效应。对于单次JPEG压缩图像，相应的BACM是具有对称性的；而对于SDJPEG压缩图像，BACM不再是对称的，进而达到检测SDJPEG压缩的目的。然而，BACM特征在一定程度上与图像内容有关。因此，不同的图像内容可能导致不同类型的BACM特征，这可能会混淆分类器，降低对双重JPEG压缩检测的性能。为了解决与内容相关性的问题，Chen和Hsu[23]提出了一个扩展的BACM特征，并考虑了块间的相关性。Qu等[24]提出了一个适用于SDJPEG压缩的卷积混合模型，并采用盲信号分离技术来将双压缩痕迹与图像内容分离。他们提出了一种被称为独立值图（independent value map，IVM）的特征，用于检查整个图像是否经过了SDJPEG压缩（鉴于SDJPEG压缩将打破IVM的对称性）。Bianchi和Piva [25]试图从DCT系数直方图中分析移位JPEG压缩痕迹。为了检测图像中的SDJPEG压缩痕迹，他们对整个图像进行了特定大小区域的全面搜索。当搜索的图像区域与第一次JPEG压缩的块分割结构匹配时，相应的DCT系数直方图中可以观察到整数周期的特定模式。Bianchi和Piva [26]还尝试了一种新的方法解决同样的问题，并提出了由SDJPEG压缩引起的DCT系数分布统计模型。该模型通过向每个DCT系数添加零均值高斯噪声来模拟SDJPEG压缩，并提供了噪声方差的估计方法。Wang等[27]扩展了这个想法，并对SDJPEG压缩如何影响DCT系数分布进行了完整的理论证明。

目前，双JPEG压缩检测算法的主要局限性有以下3点：

（1）大多数检测算法往往基于统计特征或模型。当篡改区域足够小（即小于64×64）时，由于用于构建统计特征（模型）的数据非常有限，大多数检测技术不能提供准确的检测结果。

（2）当第一次JPEG压缩的量化表已知或可以准确估计时，大多数算法的检测准确度较高。但是，这种假设在现实应用中并不易获得。由于错误传播，在穷举搜

索第一次JPEG压缩量化表的过程中，整体检测精度会一定程度的降低。

（3）对于SDJPEG压缩的检测，当第二次JPEG压缩的质量因子远小于第一次压缩的品质因子时，大多数现有检测方法所得到的检测结果与随机猜测无异。

4. 编辑过程中的线索

4.1. 光照不一致性

复制粘贴篡改是一个伪造图像最常用的方法。这些伪造图像通常是无法通过人眼进行分辨的，然而，它们可能在光照、阴影、视角等方面存在不一致性，进而可以通过适当方法来进行检测。图4 [28] 显示了一个著名的光照不一致的场景。在图像成像过程中，场景中的物体被来自某一个方向的光源照射（图5 [28] ）。如果两个对象来自不同的图像，它们的光源不太可能在方向和距离上相似，进而造成光照的不一致性。下面几个小节简要介绍了通过分析光照一致性来进行图像篡改检测。

4.1.1. 光照痕迹

在拍摄照片的过程中，场景中的物体会被某种光源照亮，而该种光源会在物体上留下某些特定痕迹，如物体表面的灰度差异和阴影。因此，可以从这些痕迹来推断出光照的方向。如果图像中的物体被不同的光源照亮，则很有可能这些物体来源于不同场景，即说明该图像有可能为拼接图像。

图4. 图中人物反射光照方向不一致，可被认定为篡改图像。

4.1.2. 基于光照痕迹的图片篡改检测

现实世界中的光照环境是复杂的：光源是三维（3D）立体的，且有时照片中存在多个光源。因此，该领域的研究者一般作出以下假设（对物体表面的朗伯假设）：对象的反射率不变且光源位于无限远。根据上述假设，Johnson和 Faird [28]描述了图像的亮度模型，如下式所示：

$$I_s(x,y) = R_f(\boldsymbol{N}(x,y)\cdot\boldsymbol{L}) + C \tag{4}$$

式中，R_f是对象的反射率；$\boldsymbol{L}$是光源的方向；$\boldsymbol{N}(x,y)$是物体表面坐标点(x,y)的法线方向；常量C是环境光强度。另外，当仅仅需要估计光照方向时，R_f可以视作单位值。给定相同反射率表面上至少p个不同的点（$p \geqslant 4$），可以采用最小二乘估计法计算光的方向，其公式如下所示：

$$E(\boldsymbol{L},C) = \left\| M\begin{pmatrix} L_x \\ L_y \\ L_z \\ C \end{pmatrix} - \begin{pmatrix} I_s(x_1,y_1) \\ I_s(x_2,y_2) \\ \vdots \\ I_s(x_p,y_p) \end{pmatrix} \right\|^2 = \|M\boldsymbol{v} - \boldsymbol{b}\|^2 \tag{5}$$

式中，|| ||表示向量范式；向量$\boldsymbol{L}$是光照方向，它包含(L_x, L_y, L_z)3个分量；M由式（6）给出：

$$M = \begin{pmatrix} N_x(x_1,y_1) & N_y(x_1,y_1) & N_z(x_1,y_1) & 1 \\ N_x(x_2,y_2) & N_y(x_2,y_2) & N_z(x_2,y_2) & 1 \\ \vdots & \vdots & \vdots & \vdots \\ N_x(x_p,y_p) & N_y(x_p,y_p) & N_z(x_p,y_p) & 1 \end{pmatrix} \tag{6}$$

式中，N_x、N_y和N_z是物体表面法线方向的3个分量。将

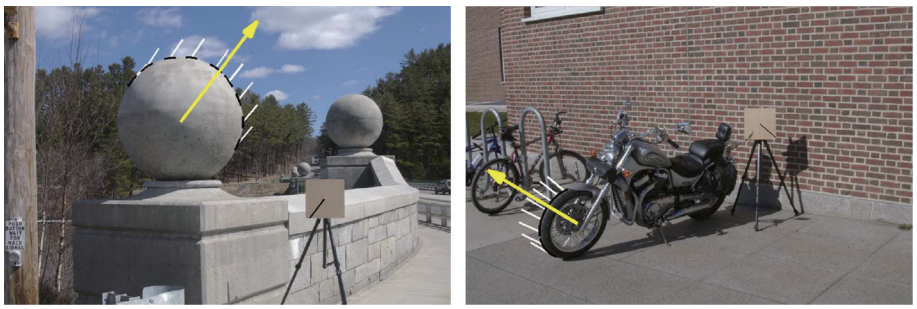

图5. 不同图像具有不同的光照方向。

偏导数设为0，最小平方估计值可由如下公式计算：

$$\boldsymbol{\upsilon} = (M^{\mathrm{T}}M)^{-1}M^{\mathrm{T}}\boldsymbol{b} \tag{7}$$

然而，这种方法的核心问题是：如果只有一张单一的图像而不知道场景中物体的几何形状，则无法获得物体表面法线$\boldsymbol{N}(x, y)$。一个可行的解决办法是将3D场景简化为2D，这意味着我们只需要从数字图像中估计光照方向的（L_x, L_y）两个分量。

在一些场景中，过于严格的简化假设会造成无法检测篡改图像。在这种情况下，我们可以放宽一些简化假设。例如，我们可以放宽反射率恒定的假设，然后判断每个表面上不同的光源方向。此外，对于局部光源而言，光源无穷远的假设就是无效的。在这种情况下，还必须加上一个假设，即光源方向对于局部小块是恒定的。

4.1.3. 最先进的基于光照一致性的图像篡改检测方法

光照痕迹在现实世界中相当复杂。对于室内场景，可能有多个局部光源。对于室外场景，很可能是无限远的点光源。在某些场景中，由于物体的几何形状未知，无法计算光线方向的3D分量。目前大部分此类的图像篡改检测方法都是基于特定的场景或者是有某种局限的。Johnson和Farid [28]最早尝试使用光照不一致进行图像篡改检测。虽然这种方法在计算物体表面的时候存在一些困难，但在许多情况下是可行的，如对于包含人脸的图像，图像中的人眼亮点来用来估计场景中的光源。Johnson和Farid [29]提出了基于人眼亮点的光照3D模型，从人眼中的亮点来估计照射光的方向，并进一步改进并提出了一个低维模型来处理复杂的光照环境[30]。Kee和Farid [31]建立了一个3D头部模型进一步提高复杂光照环境下的光照方向预测性能。Nillius和Eklundh [32]提出了一种从单一图像中自动估计光源方向的算法。该算法需要至少给定一个反射表面各向同性的遮挡物体轮廓（有很多自然图像都满足这个要求）。在该算法中，首先根据颜色和边缘信息提取遮挡轮廓，然后采用阴影模型估计每个轮廓点的光源方向，并采用贝叶斯网络来融合所有估计结果并输出最可能的估计值。值得注意的是，物体的阴影也可以用来检测图像篡改[32]。Koenderink等[33]将光照过程建模为从任意方向投影到随机高斯平面的平行光束，并根据这个模型提出了一种光照方向估计的方法。Zhang等[34]采用平面同源性和阴影亚光来描述图像中阴影的颜色分布、特点和相互关系，提出了一种基于摄影测量与图像阴影几何形状的框架来检测图像篡改。Fan等[35]设计了一个直接对抗现有基于2D光照一致性篡改检测方法的攻击策略，这一策略也揭示了现有检测方法的不足，为今后的研究提出了新的挑战。一般而言，该类方法在检测室外场景中效果更佳，其原因在于，相比室内场景，户外的光照情况更为简单。

4.2. 局部滤波痕迹

4.2.1. 中值滤波检测

中值滤波（median filtering，MF）是一种常见的滤除图像噪声的图像后处理方法。从本质上来说，MF是一种非线性滤波，故而其经常被用于在图像篡改之后去除特定的修改痕迹。一般而言，MF的结果为以特定像素为中心、一定窗口大小（一般为奇数，如3×3或5×5）的邻域中所有像素点的中间值。因为MF取所有像素的中间值作为滤波结果，经过滤波的图像通常会生成很多恒定或是几乎不变的图像块。基于这些特殊的图像块，我们可以检测MF对图像带来的痕迹。

2D MF的基本形式由以下公式计算得出：

$$y_i = \mathrm{median}(x_{i+r,j+c}),\ \ r, c \in [-z/2, z/2] \tag{8}$$

式中，y_i是中值滤波器在像素点(i, j)上以$[z, z]$大小的窗口滤波后得到的输出。

鉴于MF的非线性属性，其无法用线性表达式来表征滤波前后的输入和输出关系。然而，Bovik等[36]发现MF有很好的边缘保持特性。不仅如此，MF后的图像通常会包含很多恒定或几乎恒定的图像块，这种现象被称为streaking特性（streaking artifact）[37]。图6展示了Kirchner和Fridrich所提到的MF图像的streaking特性。基于此，Bovik [37]提出了通过分析一阶差分图像的直方

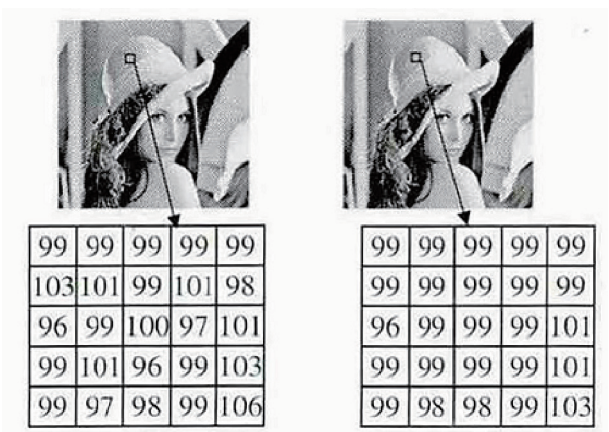

图6. 中值滤波前后图像像素点亮度分布。

图来检测streaking效应的中值滤波检测方法，在未压缩图像上表现良好。而针对JPEG压缩图像，Bovik借鉴了在隐写分析领域表现良好的减法像素邻接矩阵（subtractive pixel adjacency matrix，SPAM）特征来检测MF。然而，由于SPAM的统计模型非常复杂，当图像区域的像素数量过少（如64或128）时，检测效果会变差。Cao等[39]提出了一个基于streaking特性的MF检测算法。在计算了纹理区域横向和纵向的差分图像后，记录零值出现的概率。不仅如此，他们设计的算法还可以把MF操作和诸如图像缩放、高斯低通过滤和平均过滤等局部图像处理过程进行区分[39]。Yuan [40]观察到MF结果有局部依赖特性，因为相邻像素点的局部滤波窗口在MF过程中互相重叠，相邻的局部窗口使用了同样的一些像素点。基于这种观察，他提出了44组特征来表征MF中相邻像素点的内在属性，这44组特征被称为中值滤波特征（MFF）。MFF特征可以在未压缩图像上精确的检测出MF，并在JPEG压缩图像的MF检测中取得和SPAM特征相似的结果。对于质量因子较低的JPEG压缩图像，MFF特征通常比SPAM特征效果更好。

使用streaking特性来检测MF的主要缺陷在于这些方法对于诸如JPEG压缩等图像后处理方法表现不佳。因此，需要引入其他MF痕迹。Chen和Ni [41]观察发现MF后的图像与原始图像在边缘区域展现出不同的图像特征。这些特征体现在相邻像素点的特定相关性以及图像噪声和边缘的关系中。基于上述特征，他们提出了基于边缘的预测矩阵（edge based prediction matrix，EBPM）特征用于检测MF。该方法在图像中的不同边缘区域提取特征，并采用SVM进行分类。相比于先前的方法，EBPM特征在区分MF和其他滤波方法，如高斯低通滤波和均值滤波时表现更好。Kang等[42]提出采用中值滤波残差（MFR）来检测MF。残差是原图像和它的MF输出的差值。他们指出当一张图像再次经过MF后，MFR会减少，同时基于这一原理提出了相应的MF检测方法。该方法采用自回归模型（auto-regressive，AR）来构建基于MFR的MF检测特征集。相比SPAM特征和MFF特征，MFR特征的维数较低（10维）并且检测结果较好。此外，即使对于低JPEG品质因子（如30）的压缩图像来说，该方法依然有一定效果。Chen等[43]利用全局信息（差值图像的累积分布）和局部信息（不同相邻像素对的相关性）来进行MF检测。最终构成的56维特征连接了全局特征和局部特征，在检测低分辨率和低质量因子的JPEG压缩图像MF上表现优异。

最近，一些诸如局部纹理描述和深度学习的方法被用于进行MF检测。Zhang等[44]提出了局部纹理信息描述的特征，即二阶局部三元模式（local ternary pattern，LTP），用于MF检测。这种特征结合了LTP特征的优势和局部纹理描述子的优势，可以更好地描述MF产生的局部特征。除此之外，他们采用基于核函数的主成分分析（KPCA）来降低特征维度和提高特征的鉴别力。他们提出的方法可以快速而有效地检测经过MF的图像。Chen等[45]试图解决图像块较小情况下的MF检测这一挑战性问题。他们设计了一种卷积神经网络（convolutional neural network，CNN）来提取特征并进行分类。该网络的输入是图像块，而输出是检测结果。在文献[45]中，特征可以自动从训练样本中学习，不需要任何人工提取特征步骤。这种方法在图像块较小的情况下显著地提升了性能。

4.2.2. 锐化检测

反锐化掩模（unsharp masking，USM）锐化是一种被广泛应用的锐化技术。它通过增强边缘的对比度来提高图像质量。然而，在许多图像伪造过程中，USM锐化也可以在一定程度上掩盖篡改的痕迹。因此，USM锐化检测已成为数字图像取证领域的一个研究点。USM锐化过程通常包括以下两个步骤。

步骤1　高斯高通滤波：

$$H(x,y) = I_{\mathrm{i}}(x,y) - I_{\mathrm{i}}(x,y) \otimes G_{\sigma} \tag{9}$$

式中，H是高通滤波函数；I_{i}是原始图像；(x, y)表示水平坐标和垂直坐标；G_{σ}代表高斯高通滤波器；σ是G的标准差，它控制锐化范围。

步骤2　将反锐化掩码添加到原始图像：

$$O(x,y) = I_{\mathrm{i}}(x,y) + \lambda H(x,y) \tag{10}$$

式中，O是锐化后的图像；λ是控制锐化强度尺度系数。

图7[46]展示了在USM锐化过程后图像灰度值的变化。相比而言，原始边缘比较平滑。从图7中可以观察到在边缘区域有两个明显的阶跃扩大了边缘效应，该现象被称为超调效应（overshooting artifact），是USM锐化过程的重要线索，由高频信号叠加引起，可被用来检测USM锐化。

近年来，许多研究者提出了多种USM锐化的检测方法[46–49]。其中，使用最广泛的两类方法是基于边缘模型方法和基于局部纹理方法。Cao等[47]首次提出

USM锐化检测。他们研究发现锐化会导致直方图的突变，并建立边缘模型来衡量这些突变。然而，他们之后的研究[47]发现所提出的方法仅在图像像素值分布很广的情况下才有效，于是这些研究者[48]改进并提出了一种新的USM锐化检测，其大致步骤如下：首先，检测原始图像的边缘位置。在此基础上，测量边缘附近的过冲强度，并计算整个图像的过冲强度的平均值。最后，为超调效应设定阈值进而判断一张图片是否经过了USM锐化。虽然文献[48]中所述方法克服了文献[47]中的一些缺点，但它对图像噪声依旧非常敏感。

基于局部纹理的方法在边缘区域尝试提取不同的局部模式特征。局部二值模式（local binary pattern, LBP）与边缘垂直二进制编码（edge perpendicular binary coding，EPBC）[46]是目前使用最多的两种局部纹理特征。Ding等[49]采用LBP纹理：首先利用Canny算子确定边缘区域；然后对边缘像素点计算LBP值；最后统计整张图的LBP直方图，并使用SVM分类器来区分原始图像和锐化图像。实验结果表明，基于LBP的方法优于边缘建模方法。之后，Ding等[46]发现超调效应主要出现在垂直方向的边缘上。因此，他们提出了一种新的纹理——EPBC来进行USM锐化检测。与LBP纹理相比，EPBC纹理特征聚焦在边缘像素和沿边缘法线的矩形窗口，并对其进行了一种特殊的二进制编码。相比其他的方法，EPBC方法具有更好的检测准确性与效率。这种方法在一定程度上也对JPEG压缩和其他图像噪声有一定的鲁棒性。

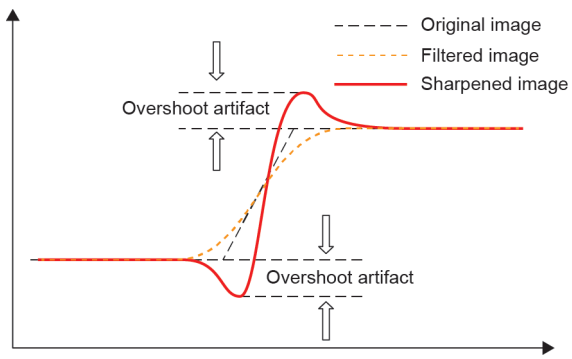

图7. 超调效应示意图。

4.3. 复制粘贴攻击检测

复制移动攻击的目的是故意伪造或删除源图像中的一个或多个对象。如图8所示，右图中所添加的新对象是通过复制源对象并将其移动到同一图像中的另一个位置来生成的。对于对象移除，被删除的对象区域被相同图像中的一些背景区域所替代。为了更具有视觉欺骗性，复制粘贴操作之前通常需要先进行缩放、旋转等仿射变换。

考虑到复制粘贴攻击的机制，可以得出以下结论：在被篡改的图像中的目标或背景区域中至少存在一对具有非常相似的颜色、形状和纹理图像区域。通过分析这些相似的图像区域对，可以检测复制粘贴攻击。准确性和效率是复制粘贴检测的两个关键问题。Fridrich等[50]和Popescu等[51]提出了进行复制粘贴检测的典型方法。Fridrich等[50]讨论了在复制粘贴检测算法中的几个主要要求：①小图像区域的近似匹配；②具有较低的虚警率和可接受的时间复杂度。基于上述要求，他们[50]提出了一种基于块匹配的检测算法。被检测的图像首先被划分成一系列重叠的小块，并从每个小块中提取特定的特征。类似小块通过特征比较进行检测：当测试图片在空间域聚集到超过预设数量的匹配块对时，图像则被认为是伪造图像。Popescu 和Farid [51]采用主成分分析（PCA）进行特征提取，以小块的PCA特征值作为其相应的特征。文献[51,52]中的算法的主要计算复杂度是由词典排序决定的，即$O(F\times N\times \log N)$[51]，其中$F$是特征维度，$N$为图像中的像素的数量。然而，当复制区域被较大程度地缩放或旋转时，上述方法不能取

图8. 复制粘贴伪造图像的经典实例。

得可靠的结果。

为了解决因缩放和旋转引起的问题，Bayram等[52]引入了傅里叶梅林变换。傅里叶梅林变换对平移、旋转和缩放具有很强的鲁棒性。此外，他们采用计数型布隆过滤器（counting bloom filter）来减少计算复杂度。实验结果表明，所提特征可以抵抗10%的旋转和10%的缩放。Li和Yu[53]拓展了文献[52]的方法，提出了用向量腐蚀滤波器来解决向量计数问题。他们的算法能够检测具有较大旋转角度的区域重复。Zandi 等[54]提出了一种自适应复制粘贴篡改检测（copy move forgery detection，CMFD）的方法，采用不同的阈值对应不同的图像内容。通过特定块的灰度方差来计算它的自适应阈值，因此，对应的CMFD在光滑和纹理区域均可以检测到复制粘贴篡改的存在。Chiristlein等[55]对不同的CMFD方法进行了综合评价，建立了一个包含48个基图像的图像数据库，数据集中的其余图片是在基图像上精心制作的不会留下明显视觉痕迹的复制粘贴篡改图片。Chiristlein等[55]研究的结果表明，尽管基于关键点的方法非常有效，但是检测结果会受低对比度区域和重复对象的影响。另一方面，基于块的方法以较高的计算复杂度为代价提供高的检测精度。在所有的特征中，Zernike的特征是推荐的选择。

4.4. 重采样检测

在大多数图像拼接场景中，拼接区域通常会进行大小调整和（或）旋转操作以掩盖伪造痕迹并使最终的伪造图像显得更真实。在大小调整和旋转过程中，拼接图像块中的像素必须进行重采样操作以适应新的样本点阵。因此，重采样检测可以帮助检测可能的伪造图像并定位可疑的拼接区域。

2005年，Popescu和Farid [56]进行了重采样检测的先驱工作。他们观察到，对于重采样信号，相邻样本之间存在很强的相关性。在该方法中，EM算法被用来估计相关重采样参数。利用上述参数，可以生成概率图来描述特定像素与其相邻像素之间是否相关的概率。对于未压缩图像，该方法可以获得较高的检测准确率。然而，对于JPEG压缩图像的来说，由于JPEG压缩中的分块离散余弦变换（BDCT）会引起特定重采样模式，从而对检测器造成混淆，降低检测性能。

Gallagher [57]提出了一种简便算法用来检测两种广泛使用的插值算子：线性插值和三次插值。他观察到在线性/三次插值之后，图像的二阶导数信号将具有周期性，并且这种周期性可以用来推测插值因子。实验表明，该方法可以检测1.1~3.0（以0.1为增量）的缩放因子。Mahdian和Saic [58]扩展了该方法，并验证了插值操作将会使信号导数的协方差产生特定的周期性模式。然而，当检测图像经中/高强度的JPEG压缩时，该方法的检测性能也会降低。

为了解决JPEG压缩所带来的问题，Kirchner和Gloe [59]改进了文献[56]的算法，在一定程度上去除了由JPEG压缩引入的混淆。实验结果表明，当后一次压缩程度比前一次压缩程度更高时，检测性能会大大降低。并且在通常情况下，上采样（放大）比下采样（缩小）更容易检测。

Vázquez-Padín等[60]最近提出了一种检测上采样图像/图像块的简便方法。为了区分上采样图像和真实图像之间的差异，他们采用奇异值分解（singular value decomposition，SVD）的方法来表征重采样图像的线性相关性，然后对饱和像素进行度量。这种方法在检测重采样的小图像块中表现良好。

4.5. 拼接图像盲检测

这类方法试图检测各种图像拼接和篡改过程，其出发点是认为任何形式的人为修改将不可避免地对自然图像引入原先并不存在的特殊痕迹。同时，该类方法将篡改检测视为一种二分类过程，即判断测试图像是自然的还是拼接以后的。然而，即便测试图像被认为不是自然的，该类方法仍然无法确定图像经过了何种形式的篡改或者定位篡改区域。尽管如此，盲图篡改检测算法仍可以用作许多图像取证系统的预处理步骤，在不知道编辑/篡改工具的情况下检测可疑图像。

Avcibas等[61]率先提出了一种盲图篡改检测方法，其目标是检测由仿射变换（缩放和旋转）、亮度和对比度调整等引起的图像修改。该方法采用各种图像质量因素作为图像特征，并且采用线性回归作为分类器。并将篡改检测问题归类为二分类问题，为之后大多数盲检测方法提供了参考依据。最后，该方法对图像篡改盲检测的准确率大约为70%。Shi等[62]提出了一种基于DCT系数模型的图像拼接盲检测方法。他们观察到，相邻块DCT系数之间的分布和相关性可用于区分自然图像和拼接图像。该方法采用2D BDCT阵列提取的马尔可夫特征作为判别依据，以支持向量机（SVM）作为分类器进行盲检测。从实验结果来看，该方法在哥伦比亚图像数据库上可以达到90%以上的检测精度[63]。Wang等[64]

提出与灰度信息相比，色度信息更具有区别性。此外，他们采用彩色通道中边缘图的灰度共生矩阵（GLCM）作为判别特征，同样以SVM作为分类器。与文献[62]中的马尔科夫特征类似，GLCM特征也代表数据的二阶统计量，并且它们的鉴别力往往比较接近。He等[65]扩展了文献[62]的思想，在离散小波变换（DWT）域中提取马尔科夫特征。随后，采用递归特征消元支持向量机（SVM-RFE）提取高鉴别力特征，提高检测精度。他们的方法也可以在哥伦比亚图像数据集中获得较高的检测精度[63]。Zhao等[66]提出了一种新的盲图像拼接检测方法。与传统的因果马尔科夫特征[62,64,65]不同，他们采用2D非因果马尔科夫模型来描述DCT和DWT域中自然和拼接图像的基本特征。所提出的非因果模型可以提供更多信息并更好地对2D图像进行建模。随后，Zhao等[66]将模型参数作为判别依据，以支持向量机作为分类器进行篡改检测。除了哥伦比亚数据集之外，作者还通过第一届IEEE信息取证和安全技术委员会（IFS-TC）图像取证挑战赛中所使用的数据集对所提方法进行了综合评估[67]。从实验结果来看，该方法的检测精度在两个数据集中均高于90%，验证了盲检测方法在图像拼接检测中的可行性。

5. 结论和未来工作

根据图像采集、存储和编辑阶段产生的各种痕迹，我们能够在不需要先验信息或知识的情况下检测数字图像篡改。在各种被动图像取证方法中，基于机器学习的技术扮演了重要角色。对于这类技术来说，图像篡改检测被归纳为一个二分类（即原始图像或合成图像）问题，并且各种能够揭示特定篡改痕迹的特征被学术界广泛研究。

数字图像取证中最关键和最具挑战性的问题源于这些被提取特征的区分能力和泛化能力。一方面，提取的特征应该对特定的篡改操作敏感，并且对不同图像内容引起的差异能够保持鲁棒。在大多数情况下，这两个要求互相冲突，如何设计一个具有高鉴别能力，并具有内容适应性的图像取证方法依旧是一个未解难题。另一方面，大多数当前特征都是基于某些假设，或基于篡改程序的特定简化模型而人为设计的。然而，由于图像内容、图像篡改技术和其他方面的差异，现实图像具有复杂性，人工设定的特征难以有效和全面处理各种伪造情况。

随着人工智能技术的发展，深度学习或可为数字图像取证带来有效的解决方案。在许多深度学习结构中，如卷积神经网络和深度残差网络，特征可以从训练样本中自动习得，而不是手工设置。在训练样本充足的前提下，基于深度学习的方法可以为特定篡改操作提供更加全面的描述。新近的基于深度学习的技术在数字图像取证应用中已经展现出巨大的潜力，如对于MF检测。然而，迄今为止，基于深度学习的方法在数字图像取证中并未展现出像在图像识别和理解中的性能。这主要由于目前采用的网络结构大多是从图像识别的网络结构转化而来的，这些结构或多或少都和图像的内容相关，从而导致在许多数字图像取证应用中的性能退化。因此，尽管基于深度学习的取证方法前景广阔，但是还没有成熟，许多工作尚待深入研究[67–71]。

致谢

文中研究工作受国家重点研发计划（编号：2016QY01W0104）和国家自然科学基金面上项目（编号：61771310）资助。

Compliance with ethics guidelines

Xiang Lin, Jian-Hua Li, Shi-Lin Wang, Alan-Wee-Chung Liew, Feng Cheng, and Xiao-Sa Huang declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Peraica A. Image science: Iconology, visual culture, and media aesthetics. Leonardo 2016;49(3):285.
[2] Farid H. A survey of image forgery detection. IEEE Signal Proc Mag 2009; 26(2):16–25.
[3] Zhou G, Lv D. An overview of digital watermarking in image forensics. In: Proceedings of 2011 Fourth International Joint Conference on Computational Sciences and Optimization; 2011 Apr 15–19; Yunnan, China. Washington, DC: IEEE Computer Society; 2011. p. 332–5.
[4] Farid H. How to detect faked photos. Am Sci 2017;105(2):77–81.
[5] Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques: A survey. Digital Invest 2013;10(3):226–45.
[6] Choi KS, Lam EY, Wong KKY. Source camera identification using footprints from lens aberration. In: Sampat N, DiCarlo JM, Martin RA, editors. Proceedings of SPIE—Electronic Imaging 2006: Digital Photography II; 2006 Jan 16–19; San Jose, CA, USA. Bellingham: International Society for Optics and Photonics; 2006. p. 172–9.
[7] Yerushalmy I, Hel-Or H. Digital image forgery detection based on lens and sensor aberration. Int J Comput Vis 2011;92(1):71–91.
[8] Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Trans Inf Foren Sec 2006;1(2):205–14.
[9] Kulkarni N, Mane V. Improvements on sensor noise based on source camera identification using GLCM. In: Proceedings of International Conference on Advances in Science and Technology; 2014 Oct 29–31; Ota, Nigeria. New York:

International Journal of Computer Applications; 2015. p. 1–4.
[10] Sandoval Orozco AL, Arenas González DM, Rosales Corripio J, García Villalba LJ, Hernandez-Castro JC. Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections. Computing 2014;96(9):829–41.
[11] Fridrich J. Digital image forensics using sensor noise. IEEE Signal Proc Mag 2009;26(2):26–37.
[12] Gao S, Xu G, Hu RM. Camera model identification based on the characteristic of CFA and interpolation. In: IWDW'11 Proceedings of the 10th International Conference on Digital-Forensics and Watermarking; 2011 Oct 23–26; Atlantic City, NJ, USA. Berlin: Springer-Verlag; 2012. p. 268–80.
[13] Prasad P. Image forgery localization via CFA based feature extraction and Poisson matting. Int J Sci Res 2014;3(10):1273–8.
[14] Katre Y, Chandel GS. Image forgery detection using analysis of CFA artifacts. Int J Adv Technol Eng Sci 2014;2(1):381–9.
[15] Lukas J, Fridrich J. Estimation of primary quantization matrix in double compressed JPEG images. In: Proceedings of Digital Forensic Research Workshop; 2003 Aug 5–8; Cleveland, OH, USA. p. 5–8.
[16] Fu D, Shi YQ, Su W. A generalized Benford's law for JPEG coefficients and its applications in image forensics. In: Delp EJ, Wong PW, editors. Proceedings of SPIE—Electronic Imaging 2007: Security, Steganography, and Watermarking of Multimedia Contents IX; 2007 Jan 28–Feb 1; San Jose, CA, USA. Bellingham: International Society for Optics and Photonics; 2007. 65051L1–11.
[17] Pevny T, Fridrich J. Detection of double-compression in JPEG images for applications in steganography. IEEE Trans Inf Foren Sec 2008;3(2):247–58.
[18] Farid H. Exposing digital forgeries from JPEG ghosts. IEEE Trans Inf Foren Sec 2009;4(1):154–60.
[19] Lin Z, He J, Tang X, Tang CK. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognit 2009;42 (11):2492–501.
[20] Huang F, Huang J, Shi YQ. Detecting double JPEG compression with the same quantization matrix. IEEE Trans Inf Foren Sec 2010;5(4):848–56.
[21] Yang J, Xie J, Zhu G, Kwong S, Shi YQ. An effective method for detecting double JPEG compression with the same quantization matrix. IEEE Trans Inf Foren Sec 2014;9(11):1933–42.
[22] Luo W, Qu Z, Huang J, Qiu G. A novel method for detecting cropped and recompressed image block. In: Proceedings of IEEE International Conference on Acoustic, Speech and Signal Processing; 2007 Apr 15–20; Honolulu, HI, USA. Piscataway: IEEE; 2007. p. 217–20.
[23] Chen YL, Hsu CT. Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. IEEE Trans Inf Foren Sec 2011;6(2):396–406.
[24] Qu Z, Luo W, Huang J. A convolutive mixing model for shifted double JPEG compression with application to passive image authentication. In: Proceedings of IEEE International Conference on Acoustic, Speech and Signal Processing; 2008 Mar 30–Apr 4; Las Vegas, NV, USA. Piscataway: IEEE; 2008. p. 1661–4.
[25] Bianchi T, Piva A. Detection of nonaligned double JPEG compression based on integer periodicity maps. IEEE Trans Inf Foren Sec 2012;7(2):842–8.
[26] Bianchi T, Piva A. Image forgery localization via block-grained analysis of JPEG artifacts. IEEE Trans Inf Foren Sec 2012;7(3):1003–17.
[27] Wang SL, Liew AWC, Li SH, Zhang YJ, Li JH. Detection of shifted double JPEG compression by an adaptive DCT coefficient model. EURASIP J Adv Signal Process 2014;2014:101.
[28] Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: Proceedings of the 7th Workshop on Multimedia and Security; 2005 Aug 1–2; New York, NY, USA. New York: ACM Press; 2005. p. 1–10.
[29] Johnson MK, Farid H. Exposing digital forgeries through specular highlights on the eye. In: Proceedings of the 9th International Conference on Information Hiding; 2007 Jun 11–13; Saint Malo, France. Berlin: Springer-Verlag; 2007. p. 311–25.
[30] Johnson MK, Farid H. Exposing digital forgeries in complex lighting environments. IEEE Trans Inf Foren Sec 2007;2(3):450–61.
[31] Kee E, Farid H. Exposing digital forgeries from 3-D lighting environments. In: Proceedings of 2010 IEEE International Workshop on Information Forensics and Security; 2010 Dec 12–15; Seattle, WA, USA. Piscataway: IEEE; 2010. p. 1–6.
[32] Nillius P, Eklundh JO. Automatic estimation of the projected light source direction. In: Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition; 2001 Dec 8–14; Kauai, HI, USA. Piscataway: IEEE; 2001. p. 1076–83.
[33] Koenderink JJ, van Doorn AJ, Pont SC. Light direction from shad(ow)ed random Gaussian surfaces. Perception 2004;33(12):1405–20.
[34] Zhang W, Cao X, Zhang J, Zhu J, Wang P. Detecting photographic composites using shadows. In: Proceedings of 2009 IEEE International Conference on Multimedia and Expo; 2009 Jun 28–Jul 3; New York, NY, USA. Piscataway: IEEE; 2009. p. 1042–5.
[35] Fan W, Wang K, Cayre F, Xiong Z. 3D lighting-based image forgery detection using shape-from-shading. In: Proceedings of the 20th European Signal Processing Conference; 2012 Aug 27–31; Bucharest, Romania. Piscataway: IEEE; 2012. p. 1777–81.
[36] Bovik AC, Huang TS, Munson DC. The effect of median filtering on edge estimation and detection. IEEE Trans Pattern Anal Mach Intell 1987;9 (2):181–94.
[37] Bovik AC. Streaking in median filtered images. IEEE Trans Acoust Speech Signal Process 1987;35(4):493–503.
[38] Kirchner M, Fridrich J. On detection of median filtering in digital images. In: Proceedings of SPIE—Electronic Imaging 2010: Media Forensics and Security II; 2010 Jan 17–21; San Jose, CA, USA. Bellingham: International Society for Optics and Photonics; 2010. p. 7541101–12.
[39] Cao G, Zhao Y, Ni R, Yu L, Tian H. Forensic detection of median filtering in digital images. In: Proceedings of 2010 IEEE International Conference on Multimedia and Expo; 2010 Jul 19–23; Singapore, Singapore. Piscataway: IEEE; 2010. p. 89–94.
[40] Yuan HD. Blind forensics of median filtering in digital images. IEEE Trans Inf Foren Sec 2011;6(4):1335–45.
[41] Chen C, Ni J. Median filtering detection using edge based prediction matrix. In: Shi YQ, Kim HJ, Pérez-González F, editors Proceeding of 10th International Workshop on Digital Forensics and Watermarking; 2011 Oct 23–26; Atlantic City, NJ, USA. Berlin: Springer-Verlag; 2012. p. 361–75.
[42] Kang X, Stamm MC, Peng A, Ray Liu KJ. Robust median filtering forensics using an autoregressive model. IEEE Trans Inf Foren Sec 2013;8(9):1456–68.
[43] Chen C, Ni J, Huang J. Blind detection of median filtering in digital images: A difference domain based approach. IEEE Trans Image Process 2013;22 (12):4699–710.
[44] Zhang Y, Li S, Wang S, Shi YQ. Revealing the traces of median filtering using high-order local ternary patterns. IEEE Signal Proc Lett 2014;21(3):275–9.
[45] Chen J, Kang X, Liu Y, Jane Wang Z. Median filtering forensics based on convolutional neural networks. IEEE Signal Proc Lett 2015;22(11):1849–53.
[46] Ding F, Zhu G, Yang J, Xie J, Shi YQ. Edge perpendicular binary coding for USM sharpening detection. IEEE Signal Proc Lett 2015;22(3):327–31.
[47] Cao G, Zhao Y, Ni R. Detection of image sharpening based on histogram aberration and ringing artifacts. In: Proceedings of the 2009 IEEE International Conference on Multimedia and Expo; 2009 Jun 28–Jul 3; New York, NY, USA. Piscataway: IEEE; 2009. p. 1026–9.
[48] Cao G, Zhao Y, Ni R, Kot AC. Unsharp masking sharpening detection via overshoot artifacts analysis. IEEE Signal Proc Lett 2011;18(10):603–6.
[49] Ding F, Zhu G, Shi YQ. A novel method for detecting image sharpening based on local binary pattern. In: Shi Y, Kim HJ, Pérez-González F, editors. Proceedings of 12th International Workshop on Digital Forensics and Watermarking; 2013 Oct 1–4; Auckland, New Zealand. Berlin: Springer-Verlag; 2013. p. 180–91.
[50] Fridrich AJ, Soukal BD, Lukas AJ. Detection of copy-move forgery in digital images. Int J 2003;3(2):652–63.
[51] Popescu AC, Farid H. Exposing digital forgeries by detecting duplicated image regions. Technical report. Hanover: Department of Computer Science, Dartmouth College; 2004. Report No.: TR2004-515.
[52] Bayram S, Sencar HT, Memon N. An efficient and robust method for detecting copy-move forgery. In: Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing; 2009 Apr 19–24; Taipei, Taiwan, China. Washington, DC: IEEE Computer Society; 2009. p. 1053–6.
[53] Li W, Yu N. Rotation robust detection of copy-move forgery. In: Proceedings of 2010 IEEE International Conference on Image Processing; 2010 Sep 26–29; Hong Kong, China. Piscataway: IEEE; 2010. p. 2113–6.
[54] Zandi M, Mahmoudi-Aznaveh A, Mansouri A. Adaptive matching for copy-move Forgery detection. In: Proceedings of 2014 IEEE International Workshop on Information Forensics and Security; 2014 Dec 3–5; Atlanta, GA, USA. Piscataway: IEEE; 2014. p. 119–24.
[55] Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Foren Sec 2012;7(6):1841–54.
[56] Popescu AC, Farid H. Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process 2005;53(2):758–67.
[57] Gallagher AC. Detection of linear and cubic interpolation in JPEG compressed images. In: Proceedings of the 2nd Canadian Conference on Computer and Robot Vision; 2005 May 9–11; Victoria, BC, Canada. Washington, DC: IEEE Computer Society; 2005. p. 65–72.
[58] Mahdian B, Saic S. Blind authentication using periodic properties of interpolation. IEEE Trans Inf Foren Sec 2008;3(3):529–38.
[59] Kirchner M, Gloe T. On resampling detection in re-compressed images. In: Proceedings of the 1st IEEE International Workshop on Information Forensics and Security; 2009 Dec 6–9; London, UK. Piscataway: IEEE; 2009. p. 21–5.
[60] Vázquez-Padín D, Comesana P, Pérez-González F. An SVD approach to forensic image resampling detection. In: Proceedings of the 23rd European Signal Processing Conference; 2015 Aug 31–Sep 4; Nice, France. Piscataway: IEEE; 2015. p. 2112–6.
[61] Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In: Proceedings of the International Conference on Image Processing; 2004 Oct 24–27; Singapore, Singapore. Piscataway: IEEE; 2004. p. 2645–8.
[62] Shi YQ, Chen C, Chen W. A natural image model approach to splicing detection. In: Proceedings of the 9th Workshop on Multimedia and Security; 2007 Sep 20–21; Dallas, TX, USA. New York: ACM Press; 2007. p. 51–62.
[63] Ng TT, Hsu J, Chang SF. Columbia image splicing detection evaluation dataset [Internet]. Available from: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/dlform.html.
[64] Wang W, Dong J, Tan T. Effective image splicing detection based on image chroma. In: Proceedings of the 16th IEEE International Conference on Image Processing; 2009 Nov 7–10; Cairo, Egypt. Piscataway: IEEE; 2009. p. 1257–60.

[65] He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognit 2012;45(12):4292–9.
[66] Zhao X, Wang S, Li S, Li J. Passive image-splicing detection by a 2-D noncausal Markov model. IEEE Trans Circuits Syst Video Techn 2015;25(2):185–99.
[67] Bayar B, Stamm MC. A deep learning approach to universal image manipulation detection using a new convolutional layer. In: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security; 2016 Jun 20–22; Vigo, Spain. New York: ACM Press; 2016. p. 5–10.
[68] Bondi L, Güera D, Baroffio L, Bestagini P, Delp EJ, Tubaro S. A preliminary study on convolutional neural networks for camera model identification. In: Proceedings of IS&T International Symposium on Electronic Imaging: Media Watermarking, Security, and Forensics; 2017 Jan 29–Feb 2; San Francisco, CA, USA. Washington, DC: Society for Imaging Science and Technology; 2017. p. 67–76.
[69] Bayar B, Stamm MC. On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection. In: Proceedings of 2017 IEEE International Conference on Acoustics, Speech and Signal Processing; 2017 Mar 5–9; New Orleans, LA, USA. Piscataway: IEEE; 2017. p. 2152–6.
[70] Chen J, Kang X, Liu Y, Wang ZJ. Median filtering forensics based on convolutional neural networks. IEEE Signal Proc Lett 2015;22(11):1849–53.
[71] Liu Y, Guan Q, Zhao X, Cao Y. Image forgery localization based on multi-scale convolutional neural networks. 2017. arXiv: 1706.07842v3.