背景

随着数码相机、更加强劲的个人电脑以及更方便的照片剪辑软件的出现，数字图像的修改变得越来越常见和容易。数字图像在杂志的封面上，报纸上，法庭上整个因特网上随处可见。图像可以很轻松地被修改，有时候，我们必须知道我们所看到的究竟是真的还是假的。而用来制作伪造的图像的工具越来越成熟，让每一个人都可以伪造图片。最近几年，伪造的图像已经影响到了科学、法律、政治、媒体以及商业等各个领域。而另一方面伪造检测工具却处于初始阶段，因此开发这些工具迫在眉睫。

心理学研究表明人们记忆的内容可以通过查看篡改的图片而被改变，但是某些图片可能会影响公众对于名人的观点(比如图 1.5)，而在政治方面比如图 1.6，1.7，1.8，在科学和法律方面玷污在公众面前形象的图片可能会引起严重的连带后果。比如在 2007 年密苏里大学的教授 R.Michael Roberts 和其合著者在被发现论文中所使用的图片是伪造的之后取消了他们在科学杂志发表的论文。

有时候在某些场景中知道图片是否真实并了解作为证据图片的来源会更加有效。比如在法律上，美国本土儿童色情预防法案(1996 年 CPPA)中禁止虚拟儿童色情就包括那些利用计算机制作出用于描绘未成年人性行为的图片。2002 年，美国最高法院即宣布 CPPA 为第一修正案(修正 CPPA 中这一条款)。该决定是基于这样一个事实，即虚拟儿童色情图片的制作并没有直接伤害到儿童，所以这些图片是受到言论自由的保护的，并不应该被禁止。修正该法案的一个副作用就是人们开始指责那些原本是人造的儿童色情的图片却辩称是计算机生成的儿童色情图片。因此，

在儿童色情案件中，原告必须证明某个图像确实是从某个特定的摄像头摄取的，而不是计算机生成的图像。这就像在调查射出的子弹的案件中，取证者会将子弹和枪管进行匹配，如果有足够可靠的证据说明子弹和枪管是匹配的，才能够在法庭上证明该子弹是从这把枪射出的。数字图像来源的调查也和这类案件类似，必须找到可靠的证据证明某幅图像的确是从该摄像头摄取的。

设备识别也可以被用在鉴别利用数码摄像机在电影院进行盗版的活动，盗版者获得相对良好的质量的副本之后会将盗版影像卖给黑市或者转码成低码率的非法影像在因特网散发。取证技术能够鉴别来自同一个摄像机的两个片段或者两种转码版本的影片是否拥有同样的来源，这将会极大地帮助取证调查者得到在不同实体和主题之间的联系并将可能成为起诉盗版者的关键证据。

此外，取证分析可以帮助调查者鉴别原始的多媒体内容和非法副本。在各种场景中会有不同类型的图像获取设备包括数码摄像头、扫描仪、手机、PDA、数码摄像机以及利用图像渲染软件生成的摄像机照片般逼真的图像或者视频等等。在所有的这些例子里，图像的真实性和可靠性是一个共同的问题，我们需要一个解决此问题的确切方案。

https://blog.csdn.net/xizero00/article/details/7265717?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-1.channel_param&depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-1.channel_param

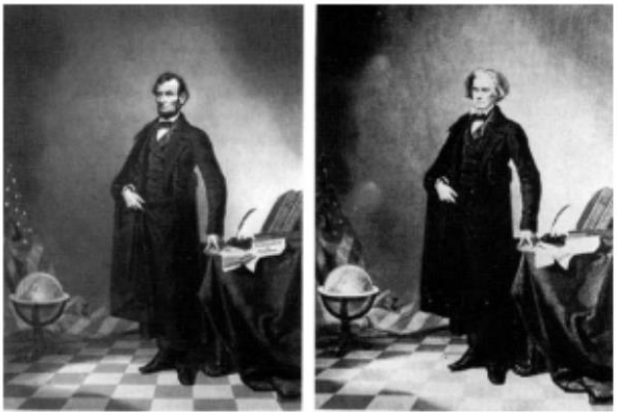

Figure 1.2: *The 1860 portrait of President Abraham Lincoln on the left and the politician John Calhoun on the right.*

Figure 1.3: *The Benito Mussolini portrait (1942) with the original on the right.*

Figure 1.4: *June 2010. This cover of The Economist shows the President Obama on the Louisiana beach inspecting the oil spill. The original photo, shot by Reuters photographer shows other two persons standing next to the President.*

Figure 1.7: *July 2008: Iranian missile test. On the left the tampered image and on the right the orginal.*

Figure 1.8: *April 2009: Prime Minister Benjamin Netanyahu (center left), President Shimon Peres (center right), along with members of the Cabinet in the original image (up) and in the fake image (bottom).*

常见的篡改技术有以下三类：

Image splicing：从一个真实图像复制部分区域然后粘贴它们到其他图片。

Copy-move：复试和粘贴部分区域在相同的图像内。

Remove：从一张图像中删除部分区域，然后修复它。

【综述】

会议：IWDW 是数字图像取证和信息隐藏领域的国际知名会议之一，每年举办一次。

1、对图像取证技术的总结

“谁动了我的图片？” – 图像取证技术

主动的：加水印等

图像取证不添加额外信息，属于被动的检测技术。

2、介绍了一点成像技术（2016 年下半年的，后来又出了一些新的论文）

深度学习在图像取证领域中的进展

取证领域比较常用的网络结构为 AlexNet，选择此网络结构的原因，是因为 AlexNet 网络结构相较于其他网络结构复杂度相对较低并且性能较好，对于解决数据集少的取证问题有更好的尝试性条件。

典型案例为 Luca Baroffio, Luca Bond 等发表的文章“Camera Identification With Deep Convolutional Networks”，文章提出用深度学习解决取证中的相机源辨别问题。

3、IWDW

专业的数字水印国际学术会议: IWDW （International Workshop of Digital Watermarking）

IWDW 是数字图像取证和信息隐藏领域的国际知名会议之一，每年举办一次。

4、面部修饰相关数据集

ND-IIITD

5、图片篡改监测相关论文汇总 GitHub

image_tampering_detection_references

6、Learning Rich Features for Image Manipulation Detection

Adobe 2108 cvpr，利用 Faster R-CNN 和噪声的方法，能够定位篡改区域，但仅针对特定篡改方式和数据库。

[2015-Signal Processing: Image Communication] A bibliography of pixel-based blind image forgery detection techniques **[paper]**

[2014-IAS] Passive Video Forgery Detection Techniques: A Survey**[paper]**

【拼接检测（splicing detection）】

[2017.5-TIFS] On the SPN Estimation in Image Forensics:A Systematic Empirical Evaluation **[paper]**

[2017.4-TIFS] Multi-Scale Analysis Strategies in PRNU-Based Tampering Localization [paper][homepage][code]

[2017.2-TIFS] Optimized 3D Lighting Environment Estimation for Image Forgery Detection [paper][code]

[2017.1-TIFS] JPEG Quantization Step Estimation and Its Applications to Digital Image Forensics [paper]

[2016.12-TIFS] Quaternion-Based Image Hashing for Adaptive Tampering Localization [paper]

[2016.3-TIP] Multi-Scale Fusion for Improved Localization of Malicious Tampering in Digital Images **[paper]**

[2016.4-TIFS] illuminant-Based Transformed Spaces for Image Forensics **[paper]**

[2013-TIFS] Exposing Digital Image Forgeries by Illumination Color Classification[paper][homepage]

【复制-粘贴检测（copy-move detection）】

[2017.5_TIFS] Image Forgery Localization via IntegratingTampering Possibility Maps **[paper]**

[2017.1-TIFS] Effective and Efficient Global Context Verification for Image Copy Detection **[paper]**

[2016.12-TIFS] Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector **[paper]**

[2016.10-TIFS] Behavior Knowledge Space-Based Fusion for Copy-move forgery Detection **[paper][dataset]**

[2015.8-TIFS] Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching**[paper]**

[2015.3-TIFS] Segmentation-Based Image Copy-Move Forgery Detection Scheme **[paper]**

[2012.8-TIFS] An Evaluation of Popular Copy-Move Forgery Detection Approaches **[paper][homepage]**

【Data sets】

【Others】

1.一些代码：https://iapp.dinfo.unifi.it/index.php?page=source-code_en

2.IEEE IFS-TC Image Forensics Challenge [homepage]