杭州電子科技大學
HANGZHOU DIANZI UNIVERSITY

计算机学院创新实践课程
课题策划书

学生姓名：算法达摩院

课题名称：翻拍检测

联系邮箱：tzmzy@vip.qq.com

指导教师：张建海

申报日期：2019.1.1

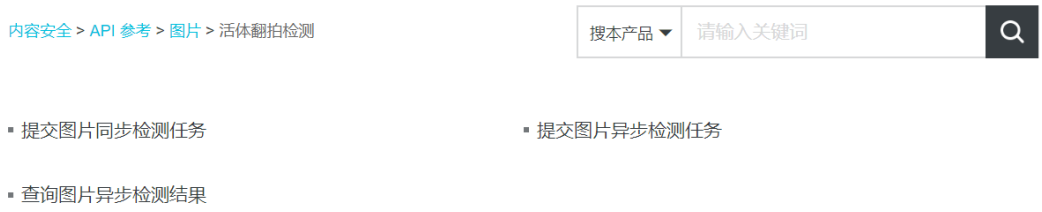
一、 课题背景和意义

随着图像显示技术的不断提升，人们可通过许多方法获取高质量的翻拍图像，越来越多的不法分子开始将这类图像用于非法途径，而目前的图像取证系统往往难以检测出图像是否属于翻拍。鉴于翻拍图像对于社会秩序及公共安全可能带来的潜在危害，这就使得实际应用中，针对视频攻击的防翻拍活体检测服务成为了更强烈的需求。

目前图像翻拍检测可分为三类：从显示媒介特性角度出发，从色彩还原与翻拍场景角度出发以及从噪声分析的角度出发。从显示媒介特性角度出发，考虑到对图像进行翻拍的过程中，显示媒介自身的特性会影响到翻拍图像的性质，如：纹理特性等，利用纹理特征等方面的差异对图像进行翻拍检测。从色彩还原与翻拍场景角度出发，考虑到翻拍图像的光度特性以及翻拍过程中可能携带的背景信息，对翻拍图像进行检测。从噪声分析的角度出发，考虑到了自然图像和原始图像在噪声特征上的不同，对翻拍图像进行检测。

二、 国内外现状

（1）阿里云上线了活体翻拍检测应用



可以根据客户要求进行图片的同步、异步检测任务。同时提供了 API 接口：

活体翻拍检测

接口	描述
/green/image/scan	提交图片同步检测任务，进行活体翻拍检测。
/green/image/asyncscan	提交图片异步检测任务，进行活体翻拍检测。
/green/image/results	提交图片异步活体翻拍检测任务后，调用本接口查询检测结果。

（2）腾讯优图也于 2017 年，发布了人脸核身技术的增强，强防翻拍活体检测技术。

目前，优图已与中国联通展开合作，为联通腾讯王卡提供人脸核身技术，对激活用户进行“实名绑定+活体验证+人脸验证”的三重安全方案来与每一个新开用户进行身份认证。此外，FaceIn 人脸核身也已在微众银行、中国联通、滴滴出行、EMS、钱生钱、通联商务等合作伙伴中广泛使用，该服务应用范围也已经拓展至公安政务、安全监管、金融、社保、直播等领域。

（3）北京交通大学教授提出了基于图像表面梯度的翻拍检测

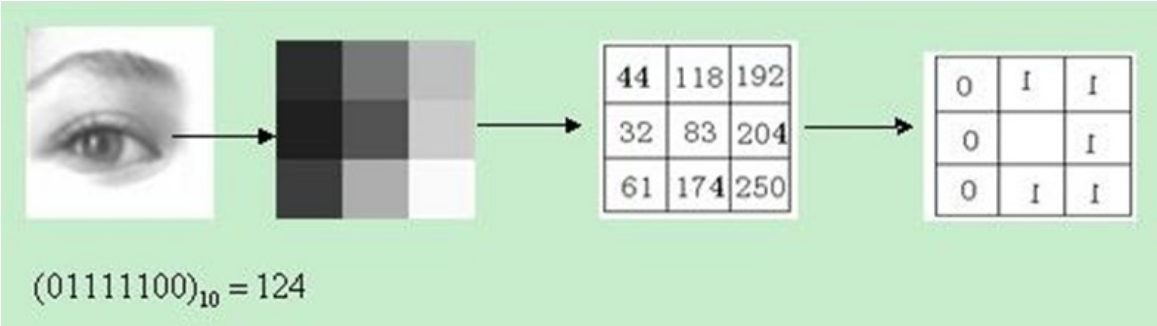
北京交通大学教授提出，经过翻拍后的篡改图像能够轻易绕过现有的图像篡改检测系统，这对图像真实性的检测构成严重的安全威胁. 本文基于翻拍过程中两次使用相机进行拍摄而引入的非线性响应，使用 Lib-SVM 设计图像分类器判别翻拍图像和真实图像. 翻拍后图像表面梯度值与真实图像相比会产生非线性变化，这使翻拍图像表面梯度值产生异常. 本文基于图像表面梯度特性提取相关特征值，使用支持向量机分类器进行翻拍图像和真实图像的判别. 实验结果表明，本文提出的特征分类效果良好，可以正确检测翻拍图像。

三、 课题目标

随着图像拍摄以及显示技术的发展，图像翻拍质量越来越高，这类图像可能会用做非法途径。翻拍检测实验的目的是为了分辨出图片的翻拍与否，从而避免翻拍照片冒充顶替真实照片事情的发生。希望将翻拍检测准确率提升到 85%或以上。

四、 课题内容和方案

（1）通过在网上翻阅论文，查找实验方法，查询特征提取方法得到了两类方法：传统的特征提取分类方法和基于深度学习的分类方法。由于深度学习需要的数据量较大，所以我们在初期先选择了传统的特征提取分类方法。为此我们找了一些常用的特征比如：LBP（Local Binary Patterns）特征， DOG（Difference of Guassian）特征等。首先我们选择了 LBP 特征（暂时我们的所有数据都是基于 LBP 特征提取得来的，其他特征数据正在分析处理，方法类似），我们选择 LBP 特征是因为在进行 LBP 特征提取后，图像表面的某些微纹理差会被扩大，如液晶屏幕的网状条状的纹路。其中原始 LBP 原理如下图：



也就是在灰度图像中的一点，以它为中心的 3*3 像素为一个单位，将中心店的灰度值与周围 8 个像素块的灰度值进行比较，大于中心为 1，小于或等于为 0，最后得到 8 个 0 或者 1 的数，从左上角第一个数开始顺时针取出他们得到一个 8 位二进制数，将其转化成十进制就是该图像的 LBP 值，将所有点的 LBP 值统计重新生成一幅由 LBP 值组成的图像，也就是该图像的 LBP 特征图像。最后将 LBP 特征图像分块求其直方图并重新将其连接得到一个一维向量，也就是改图的一维 LBP 特征向量，至此我们就得到了一张图的待分类数据。

（2）数据采集：根据公司要求，我们的数据采集主要是通过日常大家手中（多种品牌）的手机、平板、相机等对人像、身份证、银行卡在不同灯光不同角度不同背景进行拍摄，由此得到一手照片，下文称为真像。在初期我们只对人像进行了处理和分析。对于翻拍照片，下文称为假像，我们也是通过各种拍摄设备在不同灯光不同角度在不同的投射设备上进行翻拍，主要的投射设备是笔记本电脑屏幕，手机屏幕，平板屏幕，激光相片等。在试验初期，得到完整人像 1550 张，其中真像 539 张，假像 1011 张。

（3）数据处理和得出结论：在对人像处理时，考虑到脸部特征的影响和减少外界多余特征的影响，我们将图片做了脸部截取并将所有图片进行归一化，最后

截取归一化后图片大小为 200*200 像素，截得人头像 1209 张，其中真像 429 张，假像 780 张。原图和截取情况如下：


接着用上述 LBP 特征提取的方法进行处理，处理后的特征图（左真右假）如下：


处理前的真假图（左真右假）如下：


将所有图片的特征向量堆叠成.mat 文件，并通过降维处理到可接受范围，在初期我们使用了 PCA 降维。

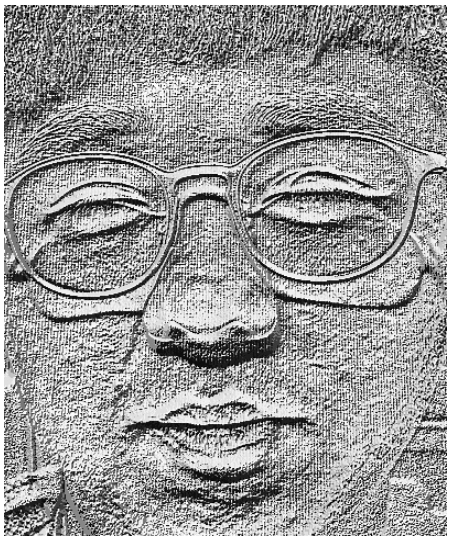
在实验初期（数据量在真假共 338 张时），本人用自己的手机（iphone）和投射设备（挑战者笔记本）拍摄了大量的真假像，所以在初期本人数据占大部分，用各种分类器（包括 svm、knn、逻辑回归、线性判别分析四个）进行分类后发现，翻拍照片能被很好的区分，在按照 3:7 的测试训练比随机抽样 1000 次后 knn 分类器的平均正确率达到了 83.2%。具体平均正确率如下表：

	SVM	KNeighborsClassifier	LogisticRegression	LinearDiscriminantAnalysis
1000 次平均正确率	80.08%	83.2%	81.53%	80.39%

因为考虑到有些照片的多次压缩导致的变形，正确率还能进一步提升。由此得出，在对于处理屏幕上的照片翻拍，LBP 特征提取能够较好的区分真假照片。

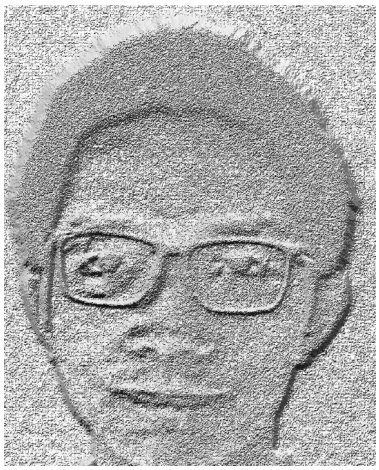
但随着大量其他数据的加入，尤其是其他投影的假照片的加入，正确率有所下降，在最新的总数据量为 1011 时最好的结果也只是 71%。尤其是在对激光照片的翻拍加入训练和测试后，因为激光照片刚打印出来，表面没有明显的纹理印迹，在无明显灯光影响下，正常像素的手机拍摄和真实的照片的 LBP 特征图片区别就并没有之前屏幕的那么明显，如下就是真假（对激光打印的图片翻拍）图片的 LBP 特征图像（左真右假）：

那就得反思是不是因为压缩以后太微小的特征不能保留了呢，这种情况在翻拍 mac 屏幕时很明显，对于 mac 这种屏幕高级的，纹理就更加不明显了，所以我做了直接跑原图的实验，结果如下(左真右假)：

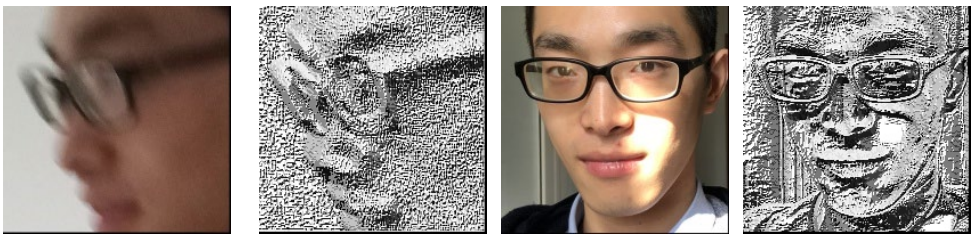
不难发现条纹依旧很明显，所以对于后续的照片我将不进行压缩归一，而是通过切割来处理。

随着新的问题的发现，我又想到那照片的翻拍呢，是不是也可以进行分块来提高正确率，我也试了一部分，结果如下（左真右假）：

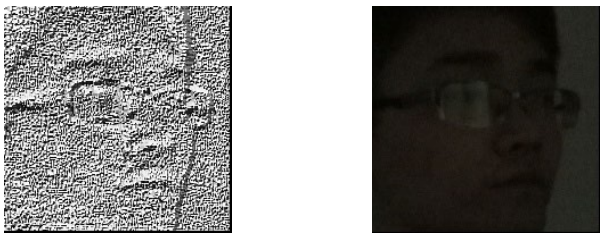



可以发现，并没了那么多的条纹状的微纹理，唯一区分点就是人物轮廓边缘（比如发梢）的真的条理清晰，假的模糊不清，原因可能是在照片打印时会有数据损耗，细小边缘被压缩处理导致 LBP 特征图像模糊化，接下来对照片的翻拍传统方法突破口可能就在这，或者可以用其他特征值比如 HOG 特征，提取目标轮廓等。

对于一些模糊的照片（比如拍摄过程略有移动等），其 LBP 特征图像虽然是真实的，但也会和其他真实照片有明显区别，而更接近与一些翻拍照片，如下图：



虽然 LBP 特征对光照不足并不是很敏感，但是在光照不足时其特征图片还是会有所区别与正常照片：



五、 课题创新性

1、将归一化压缩改为分块不叠加分割或是划窗分割原始图片

有些投射设备（比如 mac 屏幕），以为归一化压缩后图像的特征能保留（屏幕较差的特征可以被保留），换句话说，好的屏幕特征相当不明显，然而结果上看还是得需要修改过程，修改代码，而将归一化压缩改为分块不叠加分割或是划窗分割原始图片就可以解决这个问题；

2、对于训练测试数据的选择上，先是从清晰人脸开始，然后再针对模糊或者光照不足的人脸图像进一步探究；

3、随着数据量的增加，深度学习也会尝试使用。

4、针对图片的不同拍摄装置与呈现装置，分类型分开测试研究，以

追求识别准确率的最大化。

六、初步可行性分析

暂时我们还是使用了一些比较常见的特征：LBP（Local Binary Patterns）特征。

这一块儿还在探索当中，会尽快补充完整。