Journal of System Simulation

Volume 28 | Issue 2 Article 15

8-17-2020

Facial Vital Sign Based Countermeasure Against 3D Mask Attacks

Xiaojing Gu
Key Laboratory of Advanced Control and Optimization for Chemical Process (Ministry of Education),East China University of Science and Technology, Shanghai 200237, China;

Chuanqing Fu
Key Laboratory of Advanced Control and Optimization for Chemical Process (Ministry of Education),East China University of Science and Technology, Shanghai 200237, China;

Xingsheng Gu
Key Laboratory of Advanced Control and Optimization for Chemical Process (Ministry of Education),East China University of Science and Technology, Shanghai 200237, China;

Facial Vital Sign Based Countermeasure Against 3D Mask Attacks

Abstract

Abstract: Vulnerability to spoofing attacks is the main drawback for current face authentication systems. Traditional spoofing attacks include displaying printed photos and replaying recorded videos. *With the development of 3D printing technology, the 3D mask spoofing attack has been becoming the new threat. A novel anti-spoofing feature was proposed to 3D mask attacks. A liveness feature from the power spectrum of facial color signal was extracted based on a physiological phenomenon that the color of real human face changed periodically due to the blood circulation.* The performance of countermeasure jointly using the liveness feature and facial texture feature was evaluated on a public database named 3D Mask Attack Database (3DMAD) and achieved a higher accuracy comparing to previous methods that only considered texture features.

Keywords

face authentication, spoofing attacks, 3D mask, facial vital signs

第 28 卷第 2 期 系统仿真学报© Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

基于面部生命特征的 3D 假面欺骗攻击检测方法

谷小婧，付传卿，顾幸生
（华东理工大学化工过程先进控制与优化技术教育部重点实验室，上海 200237）

摘要：现有的人脸认证系统大都易于遭受欺骗攻击,传统的攻击方式主要包含影印照片和视频回放。随着 3D 打印技术的不断发展和成熟，使用 3D 面具进行欺骗攻击逐渐成为新的威胁。*针对 3D 面具欺骗攻击提出了一种新的特征用于攻击检测。该特征基于人体心脏搏动会导致真实用户的面部血流量发生周期性变化这一生理现象，提取了面部皮肤颜色信号的频谱。*在公开的 3D 面具欺骗攻击数据库上的试验表明，联合使用该生理特征和面部纹理特征的抗攻击方法相比于以往单独使用纹理特征的方法准确率得到了显著提升，可以更好地抵抗 3D 面具的欺骗攻击。

关键词：人脸认证；欺骗攻击；3D 打印面具；面部生命特征
中图分类号：TP391.4 文献标识码：A 文章编号：1004-731X (2016) 02-0361-08

Facial Vital Sign Based Countermeasure Against 3D Mask Attacks

Gu Xiaojing, Fu Chuanqing, Gu Xingsheng
(Key Laboratory of Advanced Control and Optimization for Chemical Process (Ministry of Education), East China University of Science and Technology, Shanghai 200237, China)

Abstract: Vulnerability to spoofing attacks is the main drawback for current face authentication systems. Traditional spoofing attacks include displaying printed photos and replaying recorded videos. *With the development of 3D printing technology, the 3D mask spoofing attack has been becoming the new threat. A novel anti-spoofing feature was proposed to 3D mask attacks. A liveness feature from the power spectrum of facial color signal was extracted based on a physiological phenomenon that the color of real human face changed periodically due to the blood circulation.* The performance of countermeasure jointly using the liveness feature and facial texture feature was evaluated on a public database named 3D Mask Attack Database (3DMAD) and achieved a higher accuracy comparing to previous methods that only considered texture features.

Keywords: face authentication; spoofing attacks; 3D mask; facial vital signs

引言

人脸认证系统中的欺骗攻击是指通过不正当的方式获取合法用户的生理特征，然后呈现给认证系统，从而获得系统使用权限的一种攻击方式。常见的欺骗攻击方法是向认证系统展现影印照片或回放视频，所以现在的大部分抗攻击算法都是针对这两种攻击方法设计的。这些抗攻击算法大致可以分为 3 类：纹理特征分析、动作特征分析和生理微动特征分析。纹理特征分析方法[1-2]认为影印图像和视频本身存在伪影和模糊现象，于是把噪声作为特征进行分类，另外影印图像及展示视频的 LED 屏幕均存在明显不同于真实人脸的纹理模式，这可以作为判别的重要依据。动作特征分析方法[3]认为

收稿日期：2015-04-13 修回日期：2015-09-11；
基金项目：国家自然科学基金项目(61205017，61502293，61573144)；中央高校基本科研业务费专项资金项目；
作者简介：谷小婧(1983-)，女，山东，博士，讲师，研究方向为机器视觉，模式识别，红外图像处理。

影印图像或播放视频的电子屏幕等都是平面模型，而真实人脸是 3D 模型，它们的动作模式之间存在明显的区别，这些动作模式可以作为有效特征进行判别。生理微动特征分析方法[4-5]通常是指通过分析面部是否存在由于神经调节而产生的非自主动作模式，如眼睛的眨动、嘴唇的运动、头部的晃动等来区分真假人脸。

随着 3D 打印技术的不断发展和成熟，制作出价格低廉、形象逼真的人脸 3D 面具已经可以实现，3D 面具攻击方式已逐渐成为人脸认证系统的新威胁。然而，许多以前提出的攻击检测方法在面对 3D 面具的攻击时基本失去效果[6]。例如，因为 3D 面具不再是平面模型，所以基于动作特征分析的检测方法便不再成立；而将去掉眼睛和嘴巴等部位的面具戴在攻击者的脸上就可以轻易地骗过以往的生理微动特征检测方法；由于 3D 面具极为逼真并且不再需要借助纸张、LED 屏幕等媒介呈现，基于噪声检测和纹理检测的方法的效能也被极大削弱。

1 相关工作

此前针对 3D 面具攻击方式的研究并不多见，这主要是由以下 2 方面原因造成的：（1）没有公开的数据库可供使用，这导致相关研究成果没有可比性；（2）因为之前的 3D 打印技术并不成熟，制作出低成本、形象逼真的人脸面具是一项艰难的任务，所以面具攻击方式不具备明显的威胁性。

文献[7]提出一种基于反射光谱特征检测的判别方法，作者使用 Lambertian 模型对皮肤和多种非皮肤材质的反射光谱分布进行分析，并利用 SVM 分类器进行学习及判别。他们的实验数据库共包含 20 个由 5 种不同材料制作而成的面具，其实验结果准确率为 89.18%。但是他们的检测需要在近红外光照中进行，不适用于只具有普通摄像头的人脸认证系统；并且他们试验数据库中所用的面具并不是针对真实人脸制作而成，也没有对面具的攻击性能进行分析。文献[8]提出一种基于纹理特征的判别方法，作者利用局部二值模式算子(LBP)分别提取出彩色图像和位深图像的纹理特征，然后使用分类器进行判别。他们的实验数据库包含 16 张真实人脸及相应的仿制 3D 面具，针对色彩图像和位深图像，其算法分别获得 88.12%和 86%的准确率。在文献[8]的基础上，作者联合使用从色彩图像和位深图像提取出的 LBP 纹理特征并使用分类器进行判别，实验结果准确率上升为 93.5%[9]。文献[8]第一次提出了针对 3D 面具欺骗攻击方式的检测方法，但文献[8-9]仍然存在以下不足：1) 实验数据库没有公开，这导致其他研究人员很难在他们的基础上进行相关实验；2) 实验中没有测试所用 3D 面具的攻击性能。文献[6]为了弥补上述研究的不足，作者创建并公开了他们的 3D 面具攻击数据库—3DMAD，并且测得了 3D 面具的攻击性能。作者采用 LBP 算子以及另外 3 种改进的 LBP 算子对色彩图像和位深图像分别进行纹理特征提取，并分别采用 χ^2 、线性判别分析(LDA)和支持向量机(SVM)等 3 种不同的分类器进行判别，针对色彩图像和位深图像，得到的最高准确率分别为 99.05%和 98.73%。

本文在文献[6]的研究基础上，引入一种全新的面部生命特征，并且联合使用该生命特征及纹理特征用于攻击检测。本文的贡献在于：

1) 针对 3D 面具欺骗攻击，提出一种全新的面部生命特征。该特征基于人体心脏搏动会引起面部皮肤颜色产生周期性变化这一生理现象，提取出肤色信号的频谱特征，对真实用户及 3D 面具具有很强的鉴别性。

2) 联合使用该生命特征和基于 LBP 的面部纹理特征进行检测。在公开的 3D 面具攻击数据库(3DMAD)进行的测试表明本文方法有效降低了人脸认证系统遭受 3D 面具欺骗攻击的风险。

2 3D 面具数据库

本文使用的 3D 面具攻击数据库是由瑞士 Idiap 研究所建立并公开的。数据库共包含 17 位不同的测试对象以及相应的人脸 3D 面具，其中人脸面具的尺寸大小和真实的人脸一致，它们均交由专门的 3D 打印公司制作，如图 1 所示。制作 3D 面具时，可以仅利用真实用户的人脸照片就可制作出较为逼真的面具，而不需要获得用户的人脸 3D 模型。该制作工艺不需要用户的参与配合，甚至可以在用户不知情的状态下拍摄得到他/她的照片，从而制作出相应的 3D 面具。

图 1 3D 人脸面具

采集视频使用的记录工具是微软公司的 Kinect，采集的每段视频帧频均为 30 fps，视频时长均为 10 s。其中每一帧图像包括：位深图像、相应的色彩图像和手工标记的眼睛位置。视频数据由 3 部分构成，其中前 2 部分是 17 位真人测试对象数据，但采集时间有间隔，第 3 部分是 17 位真人测试对象带着 3D 面具的数据。对各部分数据中的真人测试对象或 3D 面具，分别在 5 个不同时刻进行采集，从而共得到 255 段视频数据。

相关的攻击性能评估实验显示[6]，在只使用 2D 人脸识别算法(ISV)[13]时，3DMAD 数据库中有 65.70%的 3D 面具攻击被当做是合法用户。由此可见，该数据库中的 3D 面具仿真度高，具有很高的攻击性能。

3 欺骗攻击检测

针对 3D 面具欺骗攻击检测的目的是准确判断出呈现在人脸认证系统前的对象是合法用户还是用户的 3D 面具模型。如前所述，面对 3D 面具欺骗攻击时，基于生理微动特征的方法，如依据眼睛的眨动或嘴唇的运动等将失去判别效果，于是文献[6]的作者认为基于生命特征的检测方法注定会失败。然而，基于人脸局部区域运动的检测方法并不代表生命特征检测的全部。其他生命体的内在固有特征，如真实皮肤对光照的吸收变化、血液中的含氧量、血压、脑电波信号以及心电信号等都可以用来区别真实用户和伪装攻击。

本文在此分析的基础上，基于人体心脏搏动会引起面色周期性变化这一生理现象提出了一种新的抗攻击检测特征。实验表明，该特征与基于 LBP 的面部纹理特征联合使用可有效提升检测算法的性能。类似的面色改变特征还被用于脉搏频率检测[10]以及人脸跟踪[11]等。

3.1 面部生命特征提取方法

借助光电容积原理可很好地解释只有真实人脸上才会出现面色周期性变化这一现象。光电容积原理由 Hertzman 在 1938 年首次提出，是基于光电传播和吸收原理，通过观察皮肤表面反射光变化来检测血液容积变化并测量相关生理参数的一种检测方法。其原理为，当一定波长的光束照射到生命体皮肤表面时，皮肤表面反射出的光强度因受到皮肤、组织、肌肉和血液的吸收作用而减弱。其中皮肤、组织、肌肉对特定波长光的吸收强度在血液循环中是保持恒定不变的，只有皮肤内的血液容积因随心脏跳动而周期性充盈进而对光强的吸收呈现出搏动性变化。因此，皮肤表面的反射光会产生与心率一致的强度变化。与真实人脸不同，由于面具的制作材料内不存在可以随心跳而变化的血液容积，3D 面具上不会出现与心率一致的反射光强度变化。

实验中，我们选择彩色视频中的人脸区域作为感兴趣区域(ROI)，分析 ROI 内反射光的强度变化，即分析该面部区域内是否包含血液循环信息，以此

作为真假人脸的鉴别特征。

血液对光线中红、绿、蓝 3 种不同波段的吸收强度是不同的。文献[12]及相关实验数据表明数字图像分解为 R，G，B 三通道后，G 通道包含了较多的血液循环信息，并且受噪声干扰最小。基于此，本文直接使用了 G 通道信息作为有效信号。具体做法是，把视频进行 R，G，B 三通道分离，求取每帧上 ROI 内的 G 通道均值，然后按照帧序列记录得到所需信号。

图 2 所示为数据库中一段真人被试视频的 R，G，B 三通道信号。观察可发现被分离出的 R，G，B 三个通道的信号中，G 通道信号的变化比较有规律，与心率信号最为接近。在后续分析中，我们将对 G 通道信号做傅里叶频谱分析。

做傅里叶变换前，首先要对 G 通道的信号 $x_G(t)$ 进行归一化操作：

$$x'_G(t)=\left(x_G(t)-\mu_G\right)/\sigma_G \tag{1}$$

其中：μ_G 为 $x_G(t)$ 的平均值；σ_G 为 $x_G(t)$ 的标准差，归一化的目的是使得 $x_G(t)$ 具有均值为 0、方差为 1 的分布特性。

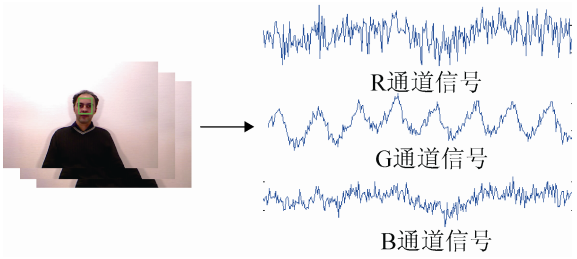
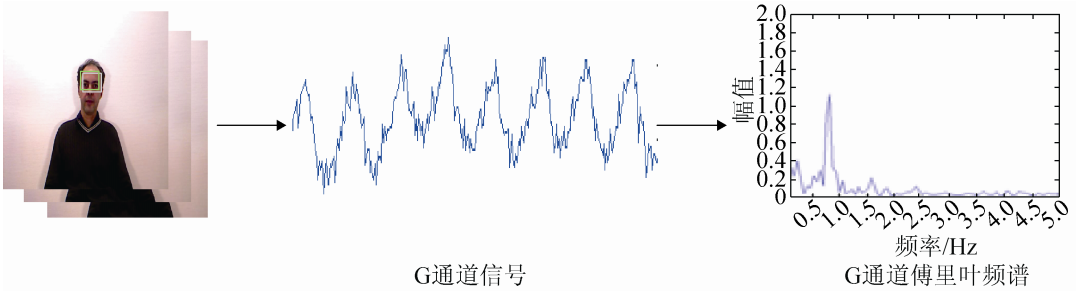
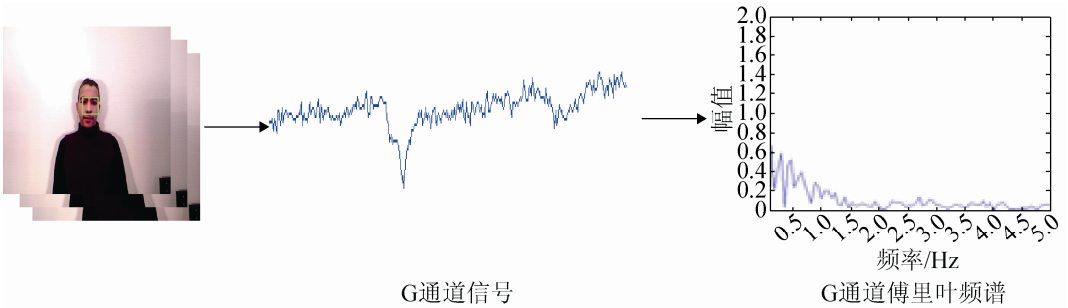


图 2 G 通道信号的提取

图 3 显示了数据库中真人被试和带 3D 面具被试的 ROI 的 G 通道信号傅里叶变换结果。一般人体心率范围是 30~120 次/min，对应的频率范围是 0.5~1.5 Hz。从图上可以看到，真实人脸的 G 通道信号在 0.5~1.5 Hz 范围内出现了一个明显的高峰，对应着被试的心率；而带 3D 面具的被试由于面部被非皮肤材料遮挡，在 0.5~1.5 Hz 范围内没有出现较明显的高峰。



(a) 真实人脸 G 通道信号频谱



(b) 3D 面具 G 通道信号频谱

图 3 真实人脸与 3D 面具频谱图

事实上，由于视频噪声的存在，不论是真实人脸还是 3D 面具，在 0.5~1.5 Hz 范围内都存在若干个峰值。两者的区别在于真实人脸在该范围内出现的最高峰与其他的高峰相比差异明显，而 3D 面具

在该范围内出现的各峰高度差异较小。为描述这一区别，本文设计了一种生命特征，计算公式为：

$$\mathrm{ind}_{\mathrm{live}} = (\max_{Ps} - \mathrm{mean}(\mathrm{sed}_{Ps}, \mathrm{thd}_{Ps})) / \max_{Ps} \quad (2)$$

其中，ind_{live} 为生命特征，$\max_{Ps}$ 为频谱图中 0.5~1.5 Hz 范围内的最大峰值，$\mathrm{mean}(\mathrm{sed}_{Ps}, \mathrm{thd}_{Ps})$ 为该范围内第 2 和第 3 高峰值的平均值。

对于真实人脸，频谱图在 0.5~1.5 Hz 范围内存在明显的峰值，并且在该范围内与其他峰值相比较特别明显，所以对应的 $\mathrm{ind}_{\mathrm{live}}$ 接近于 1；相反地，对于 3D 面具，所取范围内通常不存在明显的峰值，所以对应的 $\mathrm{ind}_{\mathrm{live}}$ 接近于 0。计算得到数据库中每段视频的 $\mathrm{ind}_{\mathrm{live}}$ 值，把该指标作为判别欺骗攻击的面部生命特征。

3.2 纹理特征提取方法

局部二值模式(LBP)是一种有效的纹理描述算子，由 Ojala 等人[14]最早提出。LBP 以及它的改进模式已经被证明在抵抗 2D 和 3D 人脸欺骗攻击时具有很高的有效性[1,8]。本文采用多种 LBP 算子分别提取出色彩图像和位深图像的纹理特征，用于 3D 面具欺骗攻击检测。

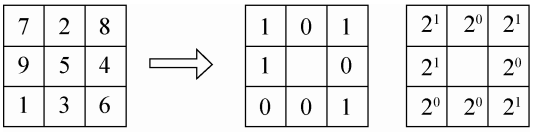
LBP 的基本思想是选定一个像素，与其周围的像素进行对比，将对比结果求和作为该像素的特征值。即选定像素作为中心和阈值，与相邻像素进行比较，如果相邻像素值≥该阈值，标记为 1，否则标记为 0。LBP 算子的计算方式是：

$$\mathrm{LBP}(x_c, y_c) = \sum_{P=0}^{P-1} 2^P s(i_p - i_c) \quad (3)$$

其中：(x_c, y_c) 为中心像素；i_c 为它的亮度；i_p 为其相邻像素的亮度；P 为相邻像素的总数；s 是一个符号函数：

$$s(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{else} \end{cases} \quad (4)$$

一个基本的 LBP 算子如图 4 所示。



LBP 特征值= 169 = (10101001)
十进制 二进制

图 4 基本的 LBP 算子示意图

在本文中，除了基本的 LBP 算子，我们还使用了其他 3 种扩展 LBP 算子[15]：渐变局部二值模式(transitional LBP，tLBP)、方向编码局部二值模式(direction-coded LBP，dLBP)以及修正局部二值模式(modified LBP，mLBP)。其中，tLBP 考虑到 8 邻域像素之间的关系，按照顺时针方向对邻域中相邻的 2 个像素进行比较，其二值比较结果作为 8 位中的一位。dLBP 则考虑到 8 邻域的方向信息，在 8 邻域中有 4 个基本方向，每个方向都用 2 个二进制位编码：第 1 位表示中心像素是否为极值(是极值则该位为 1，否则为 0)；第 2 位表示各个方向的两个像素对于中心像素的差值。mLBP 设定邻域像素并不与中心像素进行比较，而是与该邻域块像素的平均值进行比较。

使用任何一种 LBP 算子都可以在每个像素点处得到一个数值，这称为原始特征值。然而，原始特征值与位置信息是紧密相关的。直接对 2 幅图像提取原始特征值用于匹配会因为位置没对准而产生很大误差。一般有 2 种提取 LBP 最终特征的方式。一种是直接对整幅图像上的 LBP 特征值建立统计直方图，将统计直方图作为最终的特征向量。另一种是先对图像进行分块处理[16]，分别计算出每个图像块中的统计直方图，再将它们依次串联到一起作为最终的特征向量。一般来说，图像的分块操作可能会影响到所提取的纹理特征。进行图像分块，有时会显著提高判别性能，有时却可能破坏判别性能。本文的实验部分将比较 2 种不同提取最终特征的方式对 3D 面具攻击检测的影响。

3.3 判别方法

本文分别采集了测试对象的面部生命特征及纹理特征，并把这两种特征串联成新的特征向量，

即 3.2 节的纹理特征向量加上一维的 3.1 节的面部生命特征 ind_{live}。在后续的攻击检测中，我们共采用了 3 种判别方法，分别为：χ^2 检验、线性判别分析(LDA)和支持向量机(SVM)。

1) χ^2 检验广泛用于独立性或相关性检验，是一种非参数检测方法。当实际观测值与理论推断值的偏差越小时，χ^2 值就越小。相反，χ^2 值越大。本文实验中，χ^2 检验用于对测试图像的特征向量与训练集中真实人脸的均值特征向量进行 χ^2 检验，置信度为 95%。

2) LDA 是一种有监督学习的算法，在高维特征空间中，可以选择出最具判别能力的低维特征。这些特征将同一个类别的所有样本聚集在一起，不同类别的样本尽量地分开，即使得样本类间离散度和样本类内离散度的比值最大。

3) 支持向量机(SVM)是一种基于统计学习理论的机器学习算法，该算法采用结构风险最小化准则，具有较小的样本误差和模型泛化误差，所以具备较高的模型泛化能力。SVM 可以通过核函数进行空间变换，将输入从低维空间变换到高维空间，使得在低维空间线性不可分的情形变为在高维空间线性可分，并在高维空间中求取最优线性分类面。

4 实验结果

实验前数据库中的所有彩色视频及位深视频都经过了预处理：根据眼睛标注的位置信息进行了对齐及裁剪，统一为 64×64 的尺寸。

实验中每段彩色视频都按照 3.1 节所述的面部生命特征提取方法得到 ind_{live}，并转为灰度模式后按照 3.2 节所述的面部纹理特征提取方法得到 LBP 特征。位深视频的 ind_{live} 由其相应的彩色视频计算得到，位深视频的纹理特征与彩色视频的计算相同。

实验使用了 4 种 LBP 算子来提取纹理信息，分别是，基本 LBP，tLBP，dLBP 及 mLBP。使用了 2 种 LBP 特征统计方法，基于整幅图像的统计方法和基于图像分块的统计方法。图像分块时，图像被分为 3×3 的子块。

实验随机地将数据库数据分为训练集、验证集和测试集等 3 类，各类数量分别为 7，5 和 5。分类器首先利用训练集数据进行训练，然后分别在验证集和测试集数据上得到检测效果。3D 面具欺骗攻击检测的本质上是一个二分类问题，即判断呈现在识别系统面前的是真实用户还是 3D 人脸面具。最终的决策通常会出现 2 种不同的错误：一种是错误接受率(FAR)，即把 3D 面具判别为真实人脸；另一种错误拒绝率(FRR)，即把真实人脸判别为 3D 面具。通常比较抗攻击性能的指标为错误率均值(HTER)：

$$\text{HTER} = (\text{FFR} + \text{FAR}) / 2 \tag{5}$$

HTER 的值越小，表明算法的性能越好。考虑到各个 3D 面具的攻击性能不同，实验结果取 1 000 次交叉验证的平均 HTER 作为最终结果。

文献[5]使用 LBP，mLBP，dLBP 和 tLBP 4 种 LBP 算子在色彩图像和位深图像的验证集和测试集上，分别求得基于整张图像和基于图像块的 HTER，结果如图 5 所示。可以看到，除了位深图像 χ^2 分类结果，其余基于图像块的方法的 HTER 较基于整幅图像的均有减小。3 种分类中，LDA 的分类效果普遍较好。另外，对于不同的 LBP 算子，3 种分类方法的效果也不一致：在色彩图像中使用 LDA 和 SVM 分类时，使用基本 LBP 方法的判别性能最好，使用 χ^2 分类时，dLBP 方法的判别性能最好；在位深图像中使用 χ^2 和 LDA 分类时，tLBP 方法的判别性能最好，使用 SVM 分类时，mLBP 方法的判别性能最好。综合所有的判别结果，不论色彩图像还是位深图像，基于图像块的基本 LBP 算子在使用 LDA 分类算法时取得最小的 HTER 值，分别为 0.95%和 1.27%。

本文方法在文献[6]的基础上，增加了新的面部的生命特征，实验使用 LBP，mLBP，dLBP 和 tLBP 4 种 LBP 算子在色彩图像和位深图像的验证集和测试集上，分别求得基于整张图像和基于图像块的 HTER，结果如图 6 所示。

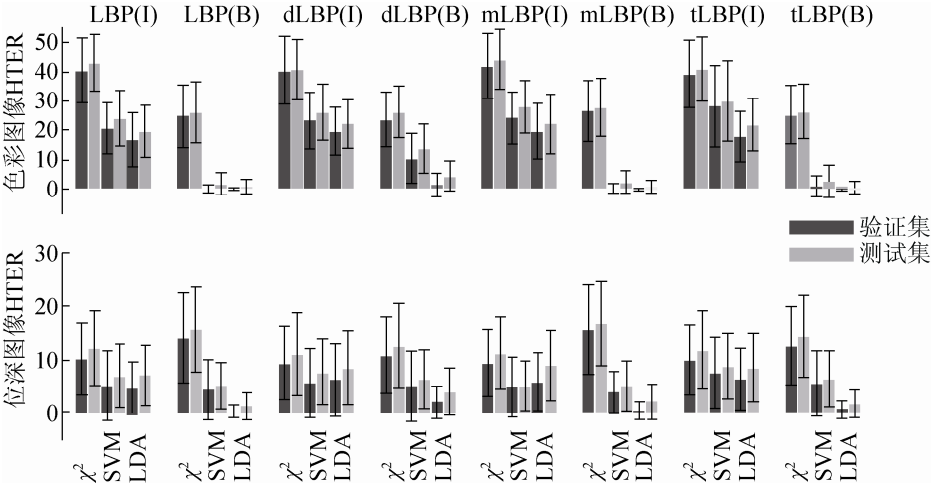


图 5 文献[5]在 3DMAD 上的 HTER 结果

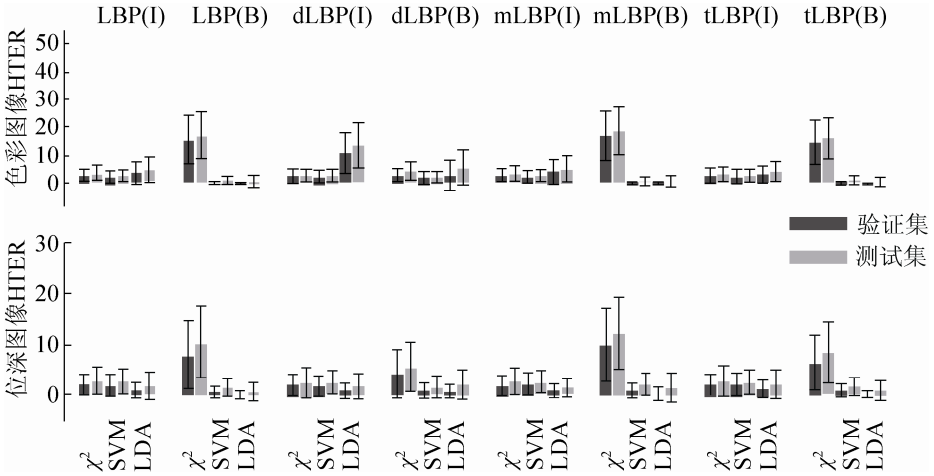


图 6 本文方法在 3DMAD 上的 HTER 结果

与图 5 结果相比，在增加了新的面部的生命特征后，4 种 LBP 算子以及 3 种分类器对应的 HTER 值均有明显减小，除了个别算法的 HTER 值高于 10%，其他大部分算法得到的 HTER 结果均低于 4%。在所有得到的 HTER 结果中：对于色彩图像，基于图像分块的 mLBP 算子在使用 LDA 分类算法时对应的 HTER 值最小，为 0.45%。对于位深图像，基于图像分块的基本 LBP 算子在使用 LDA 分类方法时对应的 HTER 值最小，为 0.74%。相比于仅使用纹理特征进行欺骗攻击检测，本文方法的效果取得了显著的提升。实验结果表明，人脸生命特征可以有效提高各类攻击检测算法的性能。

综合所有实验，本文方法在检测 3D 面具欺骗攻击方面有明显效果，对色彩图像和位深图像，判别准确率分别可以达到 99.55%和 99.26%。

5 结论

针对 3D 面具欺骗攻击，提出一种融合使用面部生命特征和纹理特征的攻击检测算法。本文利用人脸颜色周期性细微变化这一生理现象，提取出面部生命特征，又基于 LBP 算子提取出面部纹理特征。我们使用公共的 3D 面具数据库对所提出方法进行试验。结果表明，本文方法可以有效地提升 3D 面具欺骗攻击检测的效果，在 3DMAD 数据库上最高可以达到 99.55%的准确率。如何实现对多种生命特征的联合提取是本文后续的研究方向。

参考文献:

[1] I Chingovska, A Anjos, S Marcel. On the effectiveness of local binary patterns in face anti-spoofing [C]// IEEE Biometrics Special Interest Group (BIOSIG), 2012. USA: IEEE, 2012.

[2] J Maatta, A Hadid, M Pietika. Face spoofing detection from single images using texture and local shape analysis [J]. IET Biometrics (S2047-4938), 2012, 1(1): 3-10.

[3] M Marsico, M Nappi, M Riccio, et al. Moving face spoofing detection via 3d projective invariants [C]// 5th IAPR International Conference on Biometrics (ICB), 2012. USA: IEEE, 2012.

[4] G Pan, Z Wu, L Sun. Liveness detection for face recognition [Z]// Recent Advances in Face Recognition. Croatia: INTECH Open Access Publisher, 2008: 109-124.

[5] S Bharadwaj, T I Dhamecha, M Vatsa, et al. Computationally Efficient Face Spoofing Detection with Motion Magnification [C]// IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). USA: IEEE, 2013: 105-110.

[6] N Erdogmus, S Marcel. Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect [C]// Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems, 2013. USA: IEEE, 2013.

[7] Z Zhang, D Yi, Z Lei, et al. Face liveness detection by learning multi-spectral reflectance distributions [C]// IEEE International Conference on Automatic Face Gesture Recognition and Workshops, 2011. USA: IEEE, 2011: 436-441.

[8] N Kose, J L Dugelay. Countermeasure for the protection of face recognition systems against mask attacks [C]// IEEE Automatic Face and Gesture Recognition, 2013. USA: IEEE, 2013.

[9] N Kose, J L Dugelay. Shape and Texture Based Countermeasure to Protect Face Recognition Systems Against Mask Attacks [C]// IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2013. USA: IEEE, 2013: 111-116.

[10] M Z Poh, D J McDuff, R W Picard. Non-contact, automated cardiac pulse measurements using video imaging and blind source separation [J]. Optics Express (S1094-4087), 2010, 18(10): 10762-10774.

[11] G Gibert, D D'Alessandro. Face detection method based on photoplethysmography [C]// IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2013. USA: IEEE, 2013: 449-453.

[12] W Verkruysse, L O Svaasand, J S Nelson. Remote plethysmographic imaging using ambient light [J]. Optics Express (S1094-4087), 2008, 16(26): 21434-21445.

[13] R Wallace, M McLaren, C McCool, et al. Inter-session variability modelling and joint factor analysis for face authentication [C]// IEEE International Joint Conference on Biometrics, 2011. USA: IEEE, 2011.

[14] T Ojala, M Pietikainen, T Maenpaa. Multi-resolution gray-scale and rotation invariant texture classification with local binary patterns [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence (S0162-8828), 2002, 24(7): 971-987.

[15] J Trefny, J Matas. Extended set of local binary patterns for rapid object detection [C]// Proceedings of the Computer Vision Winter Workshop, 2010. Czech Republic, 2010.

[16] J Maatta, A Hadid, M Pietikainen. Face spoofing detection from single images using micro-texture analysis [C]// IEEE International Joint Conference on Biometrics, 2011. USA: IEEE, 2011.