计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20190319
57(7): 1508-1521, 2020

基于差分量化局部二值模式的人脸反欺诈算法研究

束 鑫[1] 唐 慧[1] 杨习贝[1] 宋晓宁[2] 吴小俊[2]
[1](江苏科技大学计算机学院 江苏镇江 212003)
[2](江南大学物联网工程学院 江苏无锡 214122)
(shuxin@just.edu.cn)

Research on Face Anti-Spoofing Algorithm Based on DQ_LBP

Shu Xin[1], Tang Hui[1], Yang Xibei[1], Song Xiaoning[2], and Wu Xiaojun[2]
[1](*School of Computer Science, Jiangsu University of Science and Technology, Zhenjiang, Jiangsu* 212003)
[2](*School of IOT Engineering, Jiangnan University, Wuxi, Jiangsu* 214122)

Abstract As face recognition technology has been integrated into human daily life, face spoofing detection as a key step before face recognition has attracted more and more attention. For print attack and video attack, we propose a difference quantization local binary pattern (DQ_LBP) algorithm for refining the feature of traditional local binary pattern (LBP) by quantifying the difference between the value of central pixel and its neighborhood pixels. DQ_LBP can extract the difference information between the local pixels without increasing the original dimension of LBP, and thus be able to describe the local texture features of images more accurately. In addition, we use the spatial pyramid (SP) algorithm to calculate the histogram of DQ_LBP features in different color spaces and cascade them into a unified feature vector, so as to obtain more elaborate local color texture information and spatial structure information from the face sample, thus, the fraud face detection performance of the algorithm in this paper has been further improved. Extensive experiments are conducted on three challenging face anti-spoofing databases (CASIA FASD, Replay-Attack, and Replay-Mobile) and show that our algorithm has better performance compared with the state of the art. Moreover, it has great potential in the application of real-time devices.

Key words face anti-spoofing; local binary pattern(LBP); difference quantization local binary pattern (DQ_LBP); space pyramid; color space

摘 要 随着人脸识别技术已经融入到人们日常生活中,人脸欺诈检测作为人脸识别前的一个关键步骤越来越受到重视.针对打印攻击和视频攻击,提出了一种通过量化局部像素之间的差值来细化传统局部二值模式(local binary pattern, LBP)特征的差分量化局部二值模式(difference quantization local binary pattern, DQ_LBP)算法.DQ_LBP能够在不增加LBP维度的基础上提取像素之间的差值信息,以便更精确地描述图像的局部纹理特征.此外,使用空间金字塔算法统计了不同彩色空间中的DQ_LBP特征并将其融合成统一的特征向量,从而更加充分地描述了人脸的局部彩色纹理信息及其空间结构信息,进一步提高了算法的检测性能.实验结果表明:该算法在CASIA FASD,Replay-Attack,Replay-Mobile三个具有挑战性的人脸反欺诈数据库中都取得了较为优异的结果,而且在实时性设备的应用上具有很大的潜能.

收稿日期:2019-05-31;**修回日期**:2020-01-13
基金项目:国家自然科学基金面上项目(61572242,61672265,61876072,61772244)
This work was supported by the General Program of the National Natural Science Foundation of China (61572242, 61672265, 61876072, 61772244).

关键词　人脸反欺诈;局部二值模式;差分量化局部二进制模式;空间金字塔;彩色空间

中图法分类号　TP391

目前人脸识别技术在生活中的应用十分广泛,大到机场车站的安检系统,小到随处可见的移动终端上的身份验证功能.人脸识别技术不仅大大提高了身份信息验证的效率,还给用户带来快捷方便的生活体验.但是,当有人伪造客户人脸并试图通过人脸识别系统的验证时就会出现欺诈攻击.目前,大部分基于脸部识别的反欺诈操作都需要人机交互.比如,客户需要根据系统提示进行组合动作操作完成银行系统的实名验证过程、用户需要眨眼完成支付宝的身份信息验证等,这些交互过程极大降低了客户体验的满意程度.一些公司或者社区使用人脸识别门禁系统时,还需要雇佣一些安保人员参与其中以实现"双保险".因此,在进行人脸识别前增加非人机交互的人脸欺诈检测以解决人脸识别系统中存在的风险与漏洞是一项非常有意义的工作.

人脸欺诈攻击一般可分为3种方式:打印攻击、重放攻击和3D模型攻击.打印攻击也称为照片攻击,是指将合法用户的照片打印出来或呈现在电子设备屏幕上,然后显示在人脸识别系统的镜头前,或是攻击者将用户人脸照片的眼部区域剪裁后放在自己的面部模拟用户眨眼来响应系统指令.重放攻击也指视频攻击,是指在人脸识别系统的镜头前重复播放录制好的用户脸部视频以试图通过系统验证.3D模型攻击是指利用特殊材料构造3D模型来模拟用户头部,当欺诈检测系统提示用户做出相应动作时,攻击者用手左右转动模型来模拟用户的头部运动.打印攻击和重放攻击相对于3D模型攻击所用的欺诈材料易获取,欺诈样本的制作也更为简单,因此前两者欺诈方式在人脸识别系统中存在的风险系数较高,针对打印攻击和视频攻击提出的反欺诈方法也比较广泛.

近年来,特征提取成为人脸反欺诈检测的热点研究内容[1-6].如Boulkenafet等人[1,6]使用局部二值模式(local binary pattern, LBP)提取颜色纹理特征,这种方法简单有效而且在经典的人脸欺诈数据库上都表现出了很强的泛化能力.但是,LBP只反映了图片局部区域中心点与邻近点像素值间的大小关系而忽略了重要的纹理细节信息.针对传统LBP的这一不足,本文提出了差分量化局部二进制模式(difference quantization local binary pattern, DQ_LBP),即利用图像局部中心点与周围点之间的差值来细化局部二值模式的纹理信息.除此之外,本文将DQ_LBP与空间金字塔算法[7](spatial pyramid, SP)结合大大提升了该算法的分类性能.

本文的主要贡献在于4个方面:

1) 提出的DQ_LBP与传统的LBP相比,不仅能够反映中心点与邻近点之间像素值的大小关系,更能将像素之间的差值量化并利用量化结果描述人脸局部纹理的细节特征.DQ_LBP保持了LBP构造简单的优点,且得到的DQ_LBP特征不会因为增加额外的纹理信息而增加特征的维度.

2) 使用空间金字塔算法一方面可以细致地表示人脸的空间结构信息,另一方面可以将不同尺寸的人脸图片转化成统一维度的特征向量.DQ_LBP和空间金字塔算法相结合既提取了图片的纹理和空间结构信息,又反映了图片局部和全局的特征信息.

3) 通过分析该算法在不同颜色空间中的性能说明彩色纹理对欺诈检测的作用,并将不同的颜色空间融合以增强算法的鲁棒性.

4) 仅需提取视频中的一帧图片就可以对该样本进行分类,从而有效节约了算法的运算时间.

1　相关工作

近年来,随着公共人脸欺诈数据库的增加,人脸反欺诈的研究得到了快速的发展.现有的人脸欺诈检测方法主要分为基于局部特征、基于3D深度信息分析和基于人体运动信息分析的方法.除此之外,将以上方法与深度学习相结合在该领域的应用也越来越广泛.

基于局部特征提取的方法[2-3]是利用图片再造过程中产生的纹理差异(包括打印瑕疵、视频伪影、显示设备的噪声信号和云纹效果等)辨别镜头前人脸的真假.文献[8]为了提取更强的边缘纹理特征,提出GS-LBP(guided scale based local binary pattern)淡化图像纹理的冗余度.Pereira等人[4]和Maatta等人[5]分别提出LBP-TOP(local binary pattern from three orthogonal planes)算子和基于不同模式的LBP组合的特征提取方法.前者通过LBP-TOP算子将时间和空间信息组合,大大提高了欺诈识别精度;后者通过实验证明了LBP相比局部相位量化(local phase quantization, LPQ)和Gabor算子在人

脸欺诈识别上具有更好的鉴别能力.Chingovska 等人[9]首次将 LBP 应用到欺诈检测领域,并通过实验证明 LBP 对于不同数据库中不同的攻击类型的检测都有一定的适用性.Wen 等人[10]将镜面反射、模糊、颜色矩和色彩差异信息结合进行图像失真分析,并提出基于颜色质量的特征提取方法并表明重新获得的面部图像不仅颜色退化还缺乏颜色多样性.随后 Boulkenafet 等人[1]提出一种基于颜色纹理分析的人脸反欺诈方法,证明在未知条件下面部颜色纹理的表现比灰度表示的表现更加稳定,该方法简单有效而且在跨数据库间具有很强的泛化能力.文献[11]提出使用彩色共生局部二值模式(chromatic co-occurrence of local binary pattern, CCoLBP),该算法在脸部实时应用设备上具有很大的潜力.

真实人脸是一个 3D 的面部结构,而打印攻击和视频攻击所产生的假脸在形成过程中会丢失部分脸部 3D 结构信息.基于 3D 深度信息分析[12]主要是利用 2D 图像和 3D 物体之间深度信息的差异来辨别真脸和假脸.例如文献[12-13]分别通过使用卷积神经网络输出深度图谱和在深度学习框架下从对齐的人脸图像和所有视频帧中获取深度纹理特征.

基于人体运动信息的欺诈检测主要研究人体的生理反应或运动反应,如眨眼[14-15]、人体运动[14]和头部旋转[16].Frischholz 等人[17]提出使用 3 种不同的特征——脸部、声音和嘴唇动作进行活体检测,这种方法比仅使用单特征提取方法具有更高的识别精度.由于基于人体运动信息的检测方法需要提取多帧信息,因此容易受到重放视频的攻击;Patel 等人[12]提出了一种融合深度纹理特征和面部运动线索(如眨眼)的鲁棒表示方法以应对图片和回放等攻击.

随着设备和技术的逐渐完善,将以上方法与深度学习结合后应用到人脸反欺诈领域取得了显著的效果.如 Feng 等人[18]利用卷积神经网络构造出一种层次性可扩展的框架,该框架能够融合图像的质量和运动等信息,因此在跨数据库之间具有很强的泛化能力;Atoum 等人[13]将图片分为若干小块,利用卷及神经网络(convolutional neural network, CNN)计算每个小块的欺诈分数及其平均值,再根据基于全局深度信息的 CNN 判别脸部是否具有深度,最后将二者结合判别样本真假.实验表明,该方法在高分辨率样本上也取得较好的结果,而且因使用切片代替以往使用全局图片的方法使得该算法具有鲁棒性.以上 2 种方法需要大量的欺诈样本才能通过 CNN 训练出较好的模型,但欺诈样本收集却是个难题.Li 等人[19]在卷积特征图中提取彩色 LBP 特征,并用已有的 VGG-Face 模型对其进行微调来减少过拟合影响,该算法在 CASIA FASD, Replay-Attack 数据库上都取得了稳定的性能.

以上方法在人脸反欺诈领域都表现出显著的分类效果,但也存在不足之处.例如在获取样本运动信息时往往要计算大量的视频帧,在提取样本深度信息时易受到欺诈照片卷曲影响而错误分类.使用卷积神经网络虽为目前较为先进的方法,但是容易受到欺诈样本限制而且模型训练的时间较长.对于局部特征纹理提取的方法,文献[1]虽然详细阐明了颜色通道对于欺诈识别分类的作用,但使用的特征提取方法不能充分反映图片的局部纹理信息.针对该问题,本文提出基于 DQ_LBP 的人脸反欺诈算法.该算法将 DQ_LBP 和空间金字塔算法结合,一方面 DQ_LBP 能够获取更细微的纹理特征,另一方面空间金字塔算法能够将不同尺度的脸部纹理图片转变成统一维度的特征向量,并且能更加准确地反映图片的空间结构信息.此外,为说明彩色空间对辨别真脸和假脸的作用,本文分别在 Gray, RGB, HSV, YCbCr 彩色空间进行了大量实验,并将互补的彩色空间进行融合来提高算法的识别性能.该方法简单高效而且节省大量时间,仅需提取视频中的一帧就可在 CASIA FASD, Replay-Attack, Replay-Mobile 上达到很好的检测效果.

2 基于 DQ_LBP 的人脸反欺诈算法

针对打印攻击和重放攻击,本文提出了一种 DQ_LBP 特征提取算法,并在颜色空间中将其与空间金字塔算法结合进行人脸欺诈检测.该算法的总体框架如图 1 所示,主要包含 5 个步骤:

Step1. 为提高人脸的识别效率,从每一个视频中仅提取一帧作为图片样本,然后进行脸部定位,确定脸部位置之后对原始图片进行剪裁形成新的人脸图片数据库;

Step2. 原始图片的彩色空间为 RGB 形式,为探究本文算法在不同颜色空间表示之间的差异,分别将原始图片转换为 HSV、YCbCr 和灰度图形式;

Step3. 分别在灰度图、RGB、HSV 和 YCbCr 颜色空间内提取人脸图片的 DQ_LBP 特征;

Step4. 利用空间金字塔算法提取颜色空间中各通道的全局和局部纹理特征,然后将各通道特征级联形成表示人脸的特征向量;

Step5. 利用支持向量机(support vector machine, SVM)算法进行真假人脸的检测与分类.

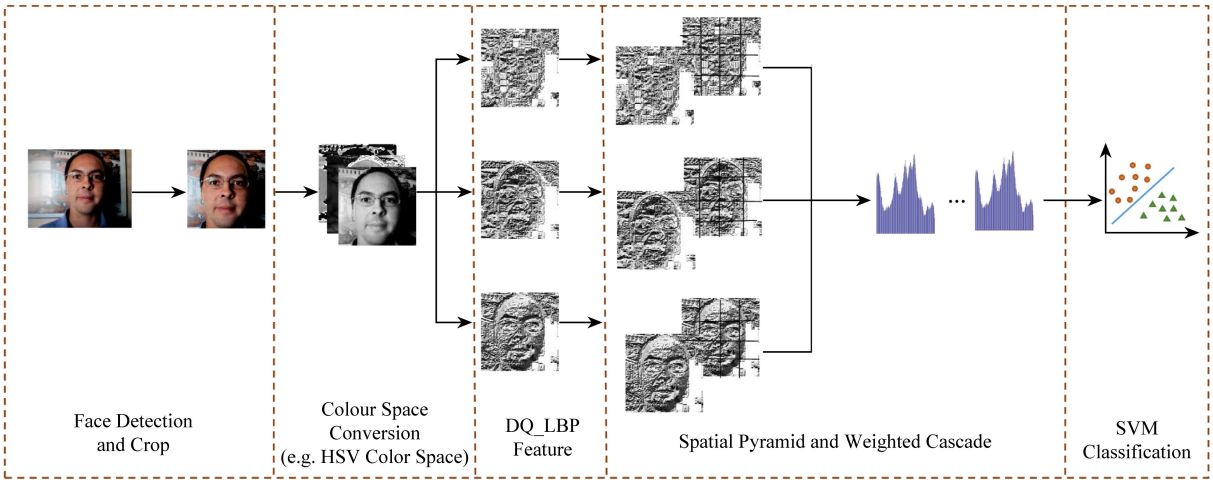


Fig. 1　Framework of proposed face anti-spoofing algorithm based on DQ_LBP

图 1　基于 DQ_LBP 的人脸反欺诈算法的框架图

2.1　脸部提取

首先利用级联目标检测器[20]获取脸部位置信息,在该过程中由于用户头部旋转可能会造成当前帧的脸部位置获取异常,此时将会对下一帧图片进行检测.适当的背景信息能够帮助欺诈检测系统有效地鉴别真脸和假脸,本文把检测到的人脸区域扩充到原来的 1.5 倍后再进行剪裁.不同于文献[1,6]中需要把剪裁后的脸部图片标准化为 64×64 像素,为了避免图片标准化后使得纹理信息丢失,本文不对剪裁后的人脸图片进行任何处理,并用空间金字塔算法解决图片多尺度问题.将 CASIA FASD 数据库中提取的人脸图像进行剪裁和扩充,形成 32×32,64×64,128×128,150×150,200×200 像素的标准人脸图片库和一个未经处理的人脸图片库.图 2 为在 HSV 空间中使用 DQ_LBP 结合空间金字塔算法提取的特征在以上 6 个人脸库中的等错误率(equal error rate, EER)和半总错误率(half total error rate, HTER).可以看出算法在未经标准化处理的人脸库中表现的性能最好.

2.2　颜色空间转换

人脸在重造过程中会产生许多纹理差异,这种差异在彩色通道上的表现更为明显.图 3(a)行 1 和行 2 分别是低分辨率下真脸和假脸在 RGB、灰度图

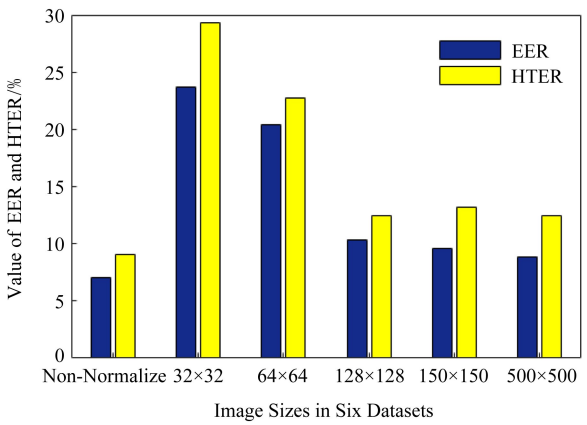


Fig. 2　Comparison of EER and HTER in the six datasets

图 2　EER 和 HTER 在 6 个数据库中比较

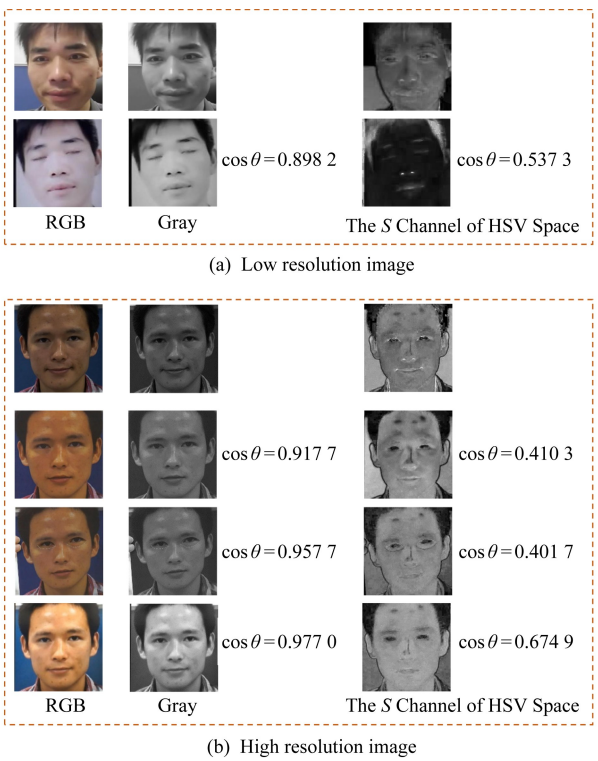


Fig. 3　Representation of real and fake faces at low and high resolution in the CASIA FASD database

图 3　CASIA FASD 中低分辨率和高分辨率下真脸和假脸

和 HSV 空间中的表示.图 3(b)是高分辨率图片示例,从上到下分别表示真脸、卷曲照片、剪切照片和重放攻击图片.cos θ 表示对应假脸图片和真脸图片的余弦相似度:

$$\cos\theta=\frac{\sum_{k=1}^{n}x_{1k}x_{2k}}{\sqrt{\sum_{k=1}^{n}x_{1k}^{2}}\sqrt{\sum_{k=1}^{n}x_{2k}^{2}}},\tag{1}$$

其中,x_{1k},x_{2k}($k=1,2,\cdots,n$)分别表示第 1 幅图片和第 2 幅图片的第 k 个特征点.

如图 3 所示,自然状态下的图片是以 RGB 形式呈现在人眼中.低分辨率真脸和假脸图片在 RGB 和 S 通道中的差异比灰度表示下的差异更为明显.但对于高分辨率的图片,在彩色空间或通道内也很难直观地辨别真脸和假脸.通过比较 S 通道和灰度图的值可知,真脸和假脸在彩色空间中的差异更大.

2.3 DQ_LBP 特征提取

纹理反映了图像灰度的性质及其空间拓扑关系.其中,LBP 因其简单高效和灰度不变性等优点被广泛应用到人脸欺诈识别领域,但是传统 LBP 只考虑中心像素值与其邻近像素值之间大小关系,而没能将它们之间的差值信息进行量化,针对传统 LBP 的这一不足,本文提出一种新颖的 LBP 改进方法.

2.3.1 LBP

局部二进制模式的原理是利用局部区域中心像素点与周围点的大小关系形成二进制编码,该二进制编码的十进制表示则为中心像素点的 LBP 值,具体定义:

$$LBP_{P,R}(x,y)=\sum_{n=1}^{P}\delta(r_n-r_c)2^{n-1},\tag{2}$$

$$\delta(x)=\begin{cases}1, & x\geqslant 0,\\ 0, & \text{otherwise},\end{cases}\tag{3}$$

其中,r_c 和 r_n($n=1,2,\cdots,P$)分别表示中心点(x,y)的像素值和位于半径为 R($R>0$)的圆上的 P 个邻域的像素值.

2.3.2 DQ_LBP

传统 LBP 忽略了局部中心点与相邻点像素之间的差异信息,如图 4①和图 4②这 2 个 3×3 窗口的中心像素点和周边像素点的差值虽然不同,但经过计算之后其 LBP 序列完全相同.针对该问题,DQ_LBP 借鉴了 LBP 的构造过程来量化局部相邻像素之间的差值,即将量化的差值附加在以 2 为底的指数中,使 DQ_LBP 在进行编码时把差值信息融合进去.因此 DQ_LBP 的特征维度与 LBP 一致且包含更丰富的纹理信息.这种增加 LBP 差值信息的纹理提取方法能够有效地表示真脸和假脸之间的差异,在人脸欺诈检测方面具有较好的表现.

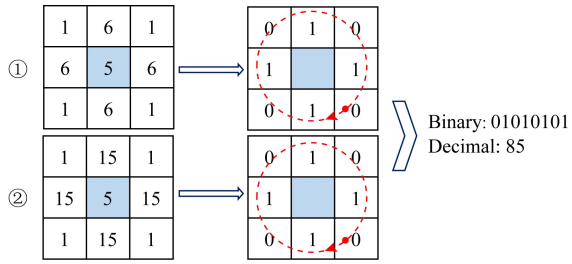


Fig. 4 Examples of LBP evaluation

图 4 LBP 求值示例

如式(2)所示,LBP 的计算过程类似于幂指函数求和运算.由于中心点像素与其相邻像素差值的范围为[0,255],如果本文直接将差值作为指数进行运算,将会使得当前位的二值权重激增,因此在运算前需要将差值进行归一化.本文构造有关差值和中心点像素值归一化为:

$$A=\left|\frac{r_n-r_c}{max-r_c}\right|,\tag{4}$$

其中,r_n 和 r_c 分别表示图像相邻点和中心点的像素值,差值大小为 $r_n>r_c$.从式(4)可以看出,A 值随差值和中心点像素值的变化而变化.max 表示该 $DQ\_LBP_{P,R}$ 所能表示的最大值,其大小取决于周围点选取的个数,与 max 关系可用 $max=2^{P-1}$ 表示,如果 $P=8$,则 $max=255$.在式(2)中,LBP 值随 n 呈指数关系递增.在细化 LBP 纹理时,为了不增加 DQ_LBP 的特征维度,本文借鉴 LBP 构造过程将 A($A\in(0,1]$)作为附加信息添加到指数中,构造的 DQ_LBP:

$$DQ\_LBP_{P,R}=\sum_{n=1}^{P}\theta(r_n-r_c)\,2^{(n-1)+(n-1)A}=\sum_{n=1}^{P}\theta(r_n-r_c)2^{(n-1)(1+A)},\tag{5}$$

$$\theta(x)=\begin{cases}1, & x>0,\\ 0, & \text{otherwise},\end{cases}\tag{6}$$

式(6)与式(3)不同,其中 $x>0$(即 $r_n>r_c$)一方面可避免式(4)的分母,另一方面约束了 $DQ\_LBP_{P,R}$ 的大小.式(5)中,$DQ\_LBP_{P,R}$ 的值会随着 n 的增加以 $2^{(1+A)}$ 的倍数递增,当 $n=P$ 时 A 值对 $DQ\_LBP_{P,R}$ 的影响最大,当 $n=1$ 时 $DQ\_LBP_{P,R}$ 值将不受 A 的限制.假设 $n=(p+1)/2$ 时 A 对 DQ_LBP 值的影响最大,那么 $DQ\_LBP_{P,R}$ 算法不会因为 n 较小而过多改变当前位 LBP 信息,也不会因为 n 太大

使 $DQ\_LBP_{P,R}$ 值远远超出 max 范围.鉴于上述假设,本文构造二次函数:

$$y=(p-n)(n-1), \tag{7}$$

为了约束 $DQ\_LBP_{P,R}$ 的大小,需要对 y 进行归一化.求 y 关于 n 的导数为

$$\frac{\partial y}{\partial n}=p+1-2n. \tag{8}$$

当 $\partial y/\partial n=0$ 时,$n=(p+1)/2$,此时 y 的最大值 $y=((p+1)/2)^2$,得到值域为[0,1]的约束函数 C:

$$C=\frac{(P-n)(n-1)}{\left\lfloor\left(\frac{P-1}{2}\right)^2\right\rfloor}. \tag{9}$$

最终得到的 DQ_LBP:

$$DQ\_LBP_{P,R}=\sum_{n=1}^{P}\theta(r_n-r_c)2^{(n-1)(1+AC)}. \tag{10}$$

当图像分辨率越高时,图片局部像素间的差异越小.图 5 表示高分辨率样本的灰度图,任取其局部纹理可知中心点与周围点像素值的差不超过 5.事实上,通过统计 CASIA FASD 和 Replay-Attack 数据库中每张图片的差值得知,像素之间的差值多数分布在 0～25 之间,差值的最大值不超过 50.由式(10)知,当周围点与邻近点差值越小,$DQ\_LBP_{P,R}$ 值就越小.因此,对于像素值变化较为平缓的中、高分辨率人脸图像,其 $DQ\_LBP_{P,R}$ 值一般不会超过最大值 max,如果 $DQ\_LBP_{P,R}>max$,则设置 $DQ\_LBP_{P,R}=max$.

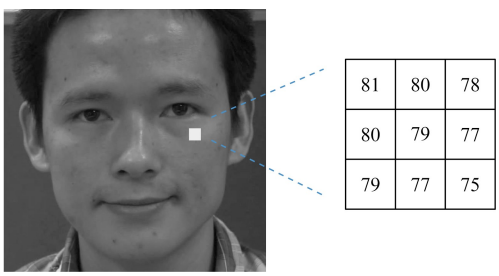
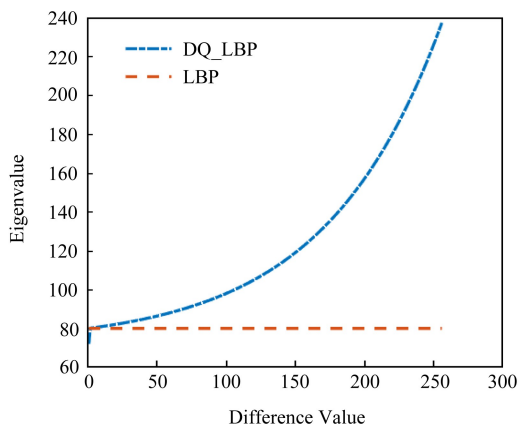


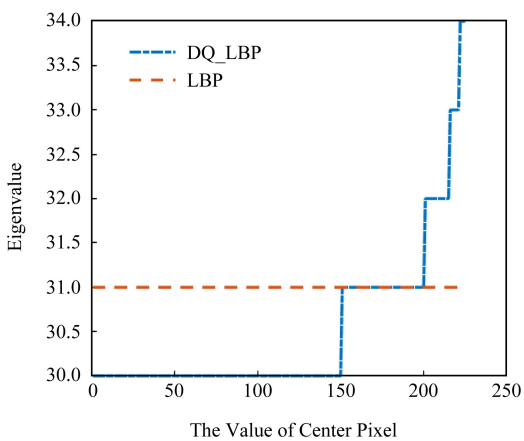
Fig. 5　Local texture of the high resolution sample

图 5　高分辨率样本的局部纹理

本文提出的 DQ_LBP 是综合考虑实际图片的差值分布和传统 LBP 的构造过程而设计的一种特征提取方式.因此 DQ_LBP 在细化原始 LBP 特征时不会增加其特征维度.图 6(a)给出了当中心点像素值不变时 LBP 和 DQ_LBP 随差值变化的曲线.从中可以出,DQ_LBP 会随着差值增大而增大,而 LBP 始终保持不变.图 6(b)是衡量 LBP,DQ_LBP 特征值和中心点像素值关系的曲线图.其中 DQ_LBP 是随中心点像素值的变化而变化的,而且这种变化的差异较小.总之,DQ_LBP 增加了纹理差值信息的同时在一定程度上保留了 LBP 的灰度尺度不变性.值得注意的是,当中心点像素值为 0～150 时,DQ_LBP 值比 LBP 值要小,这是因为式(6)对特征值的增加具有约束作用.3.3.1 节介绍了 DQ_LBP 和其他常用的特征提取方式以及 3 种 LBP 改进方法的实验比较,进一步说明了 DQ_LBP 的优越性.



(a) The graph between eigenvalue and difference



(b) The graph between eigenvalue and center pixel

Fig. 6　LBP and DQ_LBP with difference value and center pixel

图 6　差值和中心点像素值对 LBP 和 DQ_LBP 的影响

2.4　空间金字塔

在计算机视觉应用中,空间金字塔算法经常被用来解决图片多尺度问题[21].文献[22]提出基于序的空间金字塔池化算法,该算法不仅能够处理多尺度的子图像块,还解决了传统池化方法容易损失大量重要信息和易过拟合的问题.基于上述原因,本文将 DQ_LBP 纹理与经典的空间金字塔算法结合,其过程如图 7 所示.首先将一张纹理特征图片分为 L

层,对于第 l($l\in\{0,1,\cdots,L-1\}$)层的图片则会被划分为 $2^l\times 2^l$ 个均匀大小的方块;然后统计每个方块中的特征直方图并将其按照顺序级联;最后将每一层的直方图级联一起形成表示样本图片的一维向量.空间金字塔算法实际上是对图片进行粒度划分,当层数越高就意味对图片的划分越精细,因此更能详细地反映图片的空间结构和局部纹理信息.表示在 S 彩色空间 i 通道内获取的特征向量:

$$\boldsymbol{H}^{S_i}=(\boldsymbol{H}_1^{S_i},\boldsymbol{H}_2^{S_i},\cdots,\boldsymbol{H}_L^{S_i}), \tag{11}$$

将 S 彩色空间内各个通道的特征向量级联形成表示该图片的特征向量:

$$\boldsymbol{H}^{S}=(\boldsymbol{H}^{S_1},\boldsymbol{H}^{S_2},\cdots,\boldsymbol{H}^{S_I}). \tag{12}$$

其中 I 为 S 彩色空间内的通道个数.

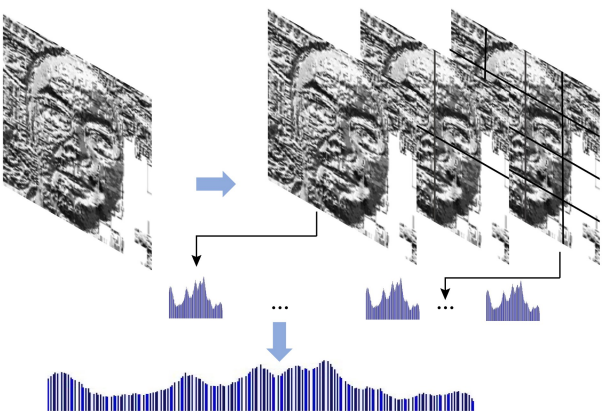


Fig. 7 Spatial pyramid layer number setting and its cascade

图 7 空间金字塔层数设置及其级联方式

空间金字塔算法的使用可以大幅度提高算法的识别精度,但是也会使其数据维度扩增,因此研究人员在使用金字塔算法时通常将其设置为 3 层.考虑到人脸欺诈识别是一种二分类问题,过于细化特征图片的结构信息会存在数据干扰,于是本文使用空间金字塔的第 1 层和第 3 层,其主要优点是将特征维度降低为原来的(1+16)/(1+4+16).

3 实验结果与分析

为了评估本文所提出算法的有效性,本文在 CASIA FASD,Replay-Attack,Replay-Mobile 三个权威的人脸反欺诈数据库进行实验.主要工作:

1) 通过在不同颜色空间中比较 DQ_LBP,DQ_LBP 结合空间金字塔算法(DQ_LBP+SP)和其他常用的 6 种特征提取方法的性能来说明 DQ_LBP 及其 DQ_LBP+SP 算法的优越性;

2) 将不同的颜色空间融合以增强算法的泛化能力;

3) 根据实验数据分析该算法的检测性能;

4) 将本文算法和前沿的人脸反欺诈算法进行比较.

3.1 数据库介绍

3.1.1 CASIA FASD 数据库

在 CASIA FASD 脸部反欺诈数据库[23]中,研究人员对 50 名实验者的真实面部进行了记录并设计了 3 种欺诈攻击:卷曲照片攻击、剪切照片攻击(摄影掩模)和视频攻击.真实的访问和攻击尝试都使用低、正常和高 3 种成像质量来记录.50 名受试者被分成 2 个不相交子集进行训练和测试,其中训练集为 20 个类,测试集为 30 个类.图 8 是来自文献[1]

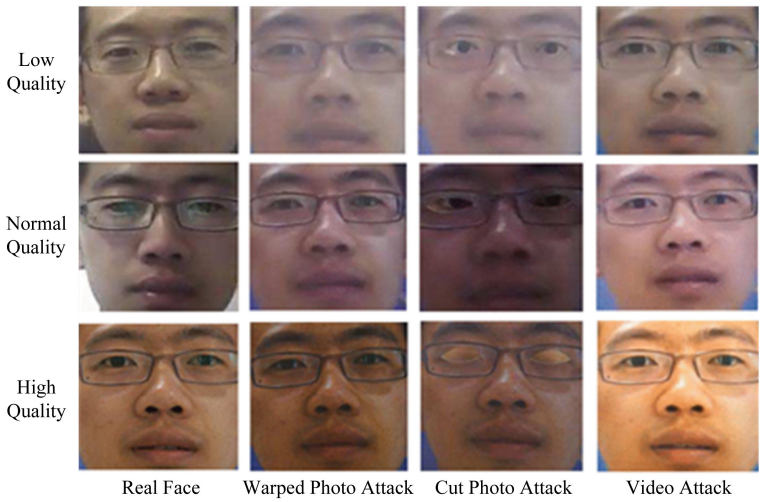


Fig. 8 Cropped and standardized faces in CASIA FASD

图 8 CASIA FASD 中裁剪和标准化的示例人脸

中 CASIA FASD 数据库的示例人脸图像,从上到下为:低质量、正常质量和高质量的人脸图像.从左到右为:真实脸部照片和相应的卷曲照片、剪切照片和视频回放攻击.

3.1.2　Replay-Attack 数据库

Replay-Attack 数据库[9]中设计了打印攻击、手机攻击和高清攻击 3 种攻击类型.根据在摄像机前展示假脸的设备时所使用的支撑物不同定义了手持和固定支持攻击.50 名受试者被分为 3 个独立的小组进行训练、验证和测试.图 9 是来自文献[1]中 Replay-Attack 数据库的示例人脸图像,行 1 显示来自受控场景的图像,而行 2 对应于来自非控制场景的图像.从左到右为:真实人脸图片和相应的高清攻击、手机攻击和打印攻击.

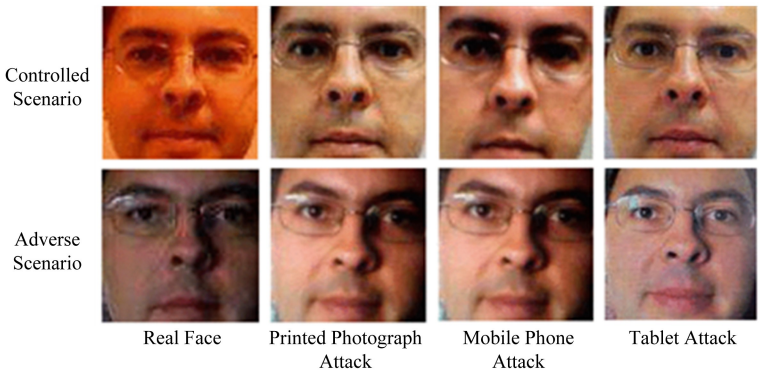


Fig. 9　Cropped and standardized faces in Replay-Attack

图 9　Replay-Attack 中裁剪和标准化的示例人脸图像

3.1.3　Replay-Mobile 数据库

Replay-Mobile 数据库是近年提出的一种新型的人脸欺诈检测数据库,相比于 Replay-Attack,该数据库使用更高分辨率的设备进行样本录制,和 CASIA FASD 相比,前者增加了移动场景的测试.Replay-Mobile 数据库[24]收集了 40 个研究对象的 1 030 个视频.包含了打印照片攻击、平板照片攻击和移动视频攻击;检测环境包括受控场景、非受控场景、直接场景、横向场景和扩散场景;攻击设备类型包括基于手持的设备和固定支持设备.该数据库分为训练集、测试集和验证集 3 个非重叠的子集,分别包含 12,16,12 个类.Replay-Mobile 数据库的人脸示例如图 10 所示:行 1 表示智能手机上捕获的攻击访问样本,行 2 表示平板电脑上采集的样本.从左到

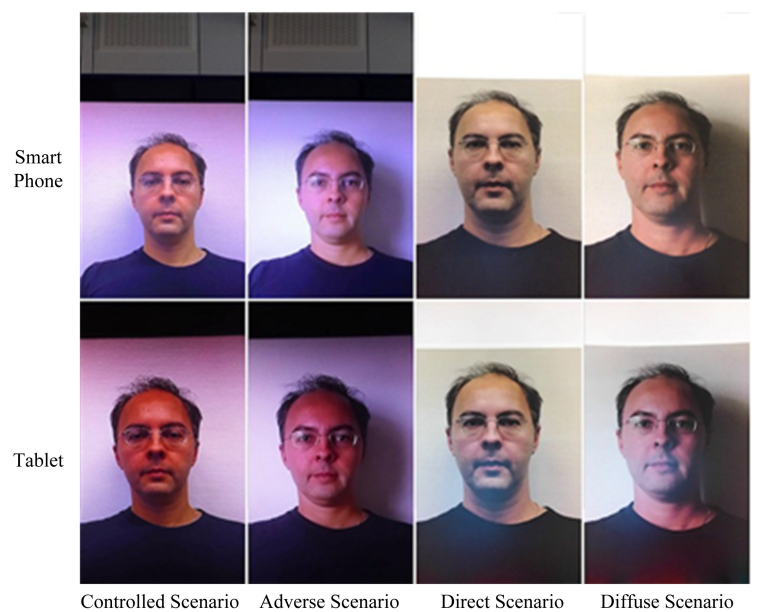


Fig. 10　Face samples in Replay-Mobile

图 10　Replay-Mobile 中的示例人脸

右的列分别显示了光照条件下哑光屏幕、无光照条件下哑光屏幕、光照条件下打印和非光照打印的人脸示例.

3.2 评价指标

本文采用线性核的支持向量机(SVM)分类器进行二值分类.以 *EER* 和 *HTER* 为评价指标.其中 *HTER* 为 *FAR* 与 *FRR* 的均值,*FAR*(false acceptance rate)为错误接受率,*FRR*(false rejection rate)为错误拒绝率.*EER* 为 *FAR*,*FRR* 的 2 条曲线的相交点对应的值.为了将本文算法和其他算法进行公平比较,本文在 Replay-Mobile 中增加了 *APCER*(attack presentation classification error rate),*BPCER*(bona fide presentation classification error rate), *ACER*(average classification error rate)三个指标,其中 *APCER* 和 *BPCER* 类似上述 *FAR* 和 *FRR*,区别在于前 2 个指标为了考虑每种攻击类型的攻击潜力和成功概率,最终的 *APCER*, *BPCER* 用所有攻击类型中性能表现最差的值进行评估,而且 *ACER* 为 *APCER* 与 *BPCER* 的均值.所有指标值越小表示该算法的整体性能越好.

3.3 实验结果与分析

3.3.1 与其他特征提取方法的比较

为了验证 DQ_LBP 特征提取方法及其结合空间金字塔算法在人脸欺诈检测中的有效性,表 1 和表 2 给出 $LBP_{8,1}^{U2}$,CoALBP(co-occurrence of adjacent local binary pattrens),LPQ(local phase quantization), BSIF(binarized statistical image features),SID(scale-invariant descriptor),LTP(local ternary pattern)[25], DQ_LBP,DQ_LBP+SP 这 8 种特征提取方法在各个颜色通道的表现结果,其中前 5 种实验数据来自于文献[1].从表 1 和表 2 可以看出,虽然相比已有的特征提取方法,DQ_LBP 并不是在所有的颜色空间内具有最好的检测性能,但是因为量化了原始 LBP 的差值信息使得其性能有了很大的提高.比如在 Replay-Attack 数据库中,DQ_LBP 在 RGB 空间的 *HTER* 值达到 0.0%.在前 6 种特征提取方法中,LTP,CoALBP 和本文提出的 DQ_LBP 表现的性能较为突出.其中 LTP 也对局部像素间的差值进行量化并在人脸识别领域具有突出的表现,但可能由于 LTP 过多地考虑了光照不变性而在人脸欺诈检测方面的性能并不理想.而 CoALBP 在 CASIA FASD 中的表现和 DQ_LBP 相当,但在 Replay-Attack 中的表现不如 DQ_LBP.而且 CoALBP 因为增加了原始 LBP 的结构信息使得其维度大幅增加.综上所述,

Table 1 *EER* Comparison Between the Proposed Algorithm and Other Feature Extraction Methods in the CASIA FASD Database

表 1 CASIA FASD 数据库中本文算法和其他特征提取方法 *EER* 比较 %

Method	GrayScale	RGB	HSV	YCbCr
$LBP_{8,1}^{U2}$	22.6	21.0	13.6	12.4
CoALBP	14.8	11.0	5.5	10.0
LPQ	23.2	14.4	7.4	16.2
BSIF	26.2	21.0	6.7	17
SID	19.9	15.8	11.2	11.6
LTP	26.2	13.5	7.96	5.93
DQ_LBP	16.3	7.8	8.0	8.9
DQ_LBP+SP	**4.6**	**4.3**	**2.2**	**3.3**

Note: The data in bold in the table represents the best results.

Table 2 *EER* and *HTER* Comparison Between the Proposed Algorithm and Other Feature Extraction Methods in the Replay-Attack Database

表 2 Replay-Attack 数据库中本文算法和其他特征提取方法的 *EER*,*HTER* 比较 %

Method	Gray		RGB		HSV		YCbCr	
	EER	*HTER*	*EER*	*HTER*	*EER*	*HTER*	*EER*	*HTER*
$LBP_{8,1}^{U2}$	17.9	13.7	4.6	6.8	6.9	10.6	2.3	5.6
CoALBP	12.9	16.7	6.2	8.0	3.7	4.3	1.4	4.7
LPQ	25.3	31.1	9.7	10.3	7.9	9.2	6.3	11.5
BSIF	31.5	30.8	13.5	11.3	8.2	10.3	10.9	10.7
SID	22.2	21.8	14.5	12.3	3.0	8.7	4.9	11.2
LTP	12.5	20.4	5.0	13.1	4.2	8.1	5.7	13.8
DQ_LBP	3.3	0.8	1.7	**0.0**	**2.7**	0.5	2.5	0.5
DQ_LBP+SP	**0.0**	**0.3**	**0.0**	**0.0**	**2.7**	**0.3**	**1.2**	**0.0**

Note: The data in bold in the table represents the best results.

DQ_LBP 能够更加准确的描述真脸和假脸的差异信息.为了增加图片纹理的结构信息,本文将 DQ_LBP 和空间金字塔算法结合.实验表明 DQ_LBP+SP 在 CASIA FASD 和 Replay-Attack 上都表现出最好的结果.表 1 中 8 种特征提取方法在 RGB,HSV,YCbCr 中的识别性能要比在灰度图中表现的结果好.虽然表 2 中不是所有的颜色空间中的实验表现都比在灰度图中的优越,但是始终存在某个颜色空间(如 RGB)会表现出最佳的性能.综上所述,彩色纹理能够提高人脸欺诈检测的性能,但对于不同的数据库彩色空间发挥的作用具有不稳定性.针对该问题,本文在 3.3.2 节将不同的彩色空间融合来增加算法的泛化能力.为研究 DQ_LBP 和空间金字塔层数对算法性能的影响,图 11 给出 LBP,DQ_LBP,DQ_LBP 结合 3 层空间金字塔 DQ_LBP_SP(0,1,2)和 DQ_LBP 结合 2 层空间金字塔 DQ_LBP_SP(0,2)在 CASIA FASD,Replay-Attack,Replay-Mobile 数据库中的 ROC 图横坐标为假正例率(false positive rate, *FPR*),纵坐标表示真正例率(true positive rate, *TPR*).可以看出 DQ_LBP 能够有效提高原始 LBP 的分类性能;DQ_LBP 结合空间金字塔算法进一步提高算法的泛化能力;当去除空间金字塔中间一层时并没有对算法性能造成大的影响,而且大大降低了数据的维度.

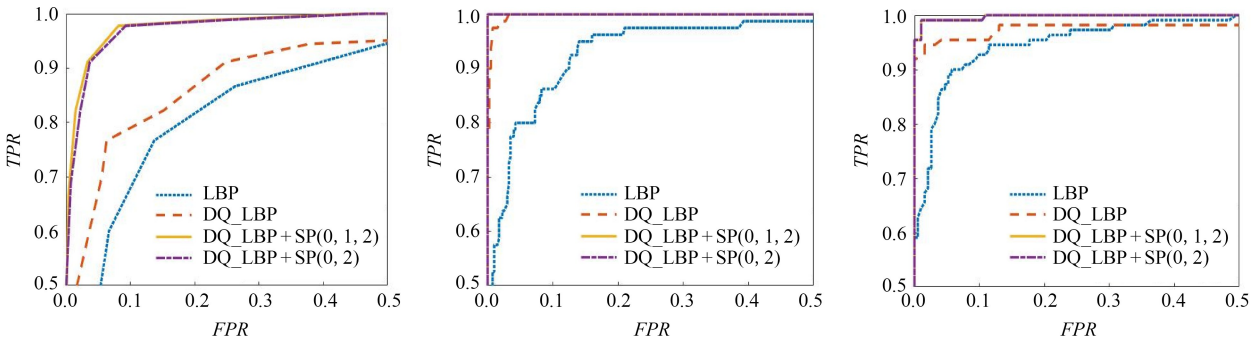


Fig. 11　ROC graphs of LBP,DQ_LBP,DQ_LBP+SP(0,1,2), and DQ_LBP+SP(0,2)

图 11　LBP,DQ_LBP,DQ_LBP+SP(0,1,2)和 DQ_LBP+SP(0,2)的 ROC 曲线

3.3.2　彩色纹理融合

彩色空间相比灰度图可以提高欺诈检测的性能,但由于使用的数据库不同,算法在何种彩色空间中表现的性能最好具有不确定性,为了提高算法整体的泛化能力,本文将不同彩色空间进行融合.表 3 给出了彩色纹理融合方式及其实验结果,其中 HSV 和 YCbCr 空间结合增加了算法在 CASIA FASD 和 Replay-Mobile 数据库中的性能,本文算法的最终结果将统一以在 HSV+YCbCr 中得到的实验数据为准.

Table 3　Fusion Performance of Color Texture in Replay-Attack,CASIA FASD, and Replay-Mobile Databases

表 3　算法在 Replay-Attack,CASIA FASD,Replay-Mobile 数据库中的彩色纹理融合　%

Colour Space	Replay-Attack		CASIA FASD		Replay-Mobile	
	EER	*HTER*	*EER*	*HTER*	*EER*	*HTER*
RGB	**0.00**	**0.00**	4.44	1.85	1.21	0.52
HSV	2.67	0.25	2.04	2.22	0.31	**0.00**
YCbCr	1.17	**0.00**	3.33	3.33	0.70	0.52
RGB+HSV	**0.00**	**0.00**	1.85	2.59	0.51	0.52
RGB+YCbCr	**0.00**	**0.00**	3.15	3.70	0.90	0.26
HSV+YCbCr	0.33	**0.00**	**1.30**	**1.30**	**0.00**	0.52
RGB+HSCV+YCbCr	**0.00**	**0.00**	3.15	2.59	0.70	0.52

Note: The data in bold in the table represents the best results.

3.3.3 检测性能分析

为了解本文算法在不同成像质量和不同欺诈攻击样本中的性能表现，表 4～6 分别给出算法在 Replay-Mobile，CASIA FASD，Replay-Attack 中的实验结果.在上述 3 种数据库中，本文算法分别在视频图片攻击、数码图片攻击和移动设备攻击下具有更高的检测精度.值得注意的是，本文算法能够完美地检测出 Replay-Attack 数据库中的数码图片攻击.

Table 4 Performance of Our Algorithm Under Different Protocols in Replay-Mobile Database

表 4 本文算法在 Replay-Mobile 数据库中不同协议上的性能表现 %

Protocol	Mobile		Tablet		All Devices	
	EER	*HTER*	*EER*	*HTER*	*EER*	*HTER*
Paper Hand	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Paper Fixed	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	1.04
Paper AllSupport	**0.00**	**0.00**	**0.00**	1.04	**0.00**	0.52
Mattescreen Video	**0.00**	**0.00**	**0.00**	**0.00**	0.31	**0.00**
Mattescreen Photo	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	1.04
Mattescreen AllType	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.52
Grandtest	**0.00**	**0.00**	**0.00**	0.52	**0.00**	0.52

Note: The data in bold in the table represents the best results.

Table 5 Performance of Our Algorithm Under Different Protocols in CASIA FASD Database

表 5 算法在 CASIA FASD 中不同协议上的性能表现 %

Scenario	*EER*	*HTER*
Low Quality	0.56	0.56
Middle Quality	2.78	8.33
High Quality	2.22	0.56
Warped Photo	3.33	1.67
Cut Photo	3.33	3.33
Video Photo	**0.00**	**1.11**
Over All	1.30	1.30

Note: The data in bold in the table represents the best results.

Table 6 Performance of Our Algorithm Under Different Protocols in Replay-Attack Database

表 6 算法在 Replay-Attack 数据库中不同协议上的性能表现 %

Scenario	Training Test		Training Devel	
	EER	*HTER*	*EER*	*HTER*
Print	**0.00**	0.63	**0.00**	**0.00**
Mobile	0.52	0.63	**0.00**	**0.00**
Highdef	0.63	1.25	**0.00**	**0.00**
Photo	**0.00**	**0.00**	**0.00**	2.50
Digital Photo	**0.00**	**0.00**	**0.00**	**0.00**
Video	1.25	1.25	**0.00**	**0.00**
Over All	**0.00**	**0.00**	0.33	4.17

Note: The data in bold in the table represents the best results.

3.3.4 与现有算法比较

表 7 给出了本文算法和经典的以及前沿的人脸反欺诈算法比较，其中 DQ_LBP+SP 和前 6 种方法是使用传统的纹理特征提取方法，而文献[13，18-19，28]是将深度信息、运动信息、纹理信息等和卷积神经网络相结合的算法.对比传统方法中 $LBP^{U^2}_{8,1}$，CLBP，LBP+DCT 的实验结果可知，将多种信息融合的算法比提取单一信息的算法更加高效.其中 LBP

Table 7 Comparison Between Our Algorithm and Other Frontier Algorithms in Replay-Attack and CASIA FASD Database

表 7 本文算法和其他前沿算法在 Replay-Attack 和 CASIA FASD 数据库中的比较 %

Method	Replay Attack		CASIA FASD
	EER	HTER	EER
LBP-TOP$^{U^2}_{8,8,8,1,1,1}$[4]	7.8	7.6	10.6
CTMF[26]	4.0	4.4	8.0
$LBP^{U^2}_{8,1}$[6]	0.4	2.9	6.2
CLBP[1]	0.4	2.8	2.1
LBP+DCT[27]	**0.0**	**0.0**	18.1
LBP+CCoLBP[11]		5.4	4.1
Two-Stream CNN[13]	0.8	0.7	2.7
Bottleneck Feature Fusion+ NN[18]	0.8	**0.0**	5.8
Deep LBP[19]	0.5	1.6	2.2
3D CNN[28]	0.3	1.2	1.4
Ours	0.3	**0.0**	**1.3**

Note: The data in bold in the table represents the best results.

结合多层离散余弦变量的算法和本文算法都在Replay-Attack数据库中达到了完美检测,但是本文算法在CASIA FASD中的*EER*值比LBP+DCT降低了97.79%.近年来,卷积神经网络因其强大的分类性能被广泛应用于活体检测领域.从表7可以看出结合CNN的算法在整体上比传统方法表现的性能更佳,比如文献[28]中提出的适合时空输入的3D卷积神经网络在Replay-Attack,CASIA FASD中都具有较为突出的性能.但是欺诈样本获取相对困难从而使网络模型的训练受到限制,而且模型在训练时也耗费较多的时间.综合来看,本文算法的性能明显优于其他传统算法,而且与大部分卷积神经网络算法相比,其泛化能力也更胜一筹.在表8所示的Replay-Mobile数据库中,本文方法的ACER值比IQM(image quality measure),Gabor分别降低了92.38%,89.08%.和LBP+GS-LBP,CCoLBP,LBP+CCoLBP这3种改进的LBP算法相比,本文算法也具有更好的性能表现.

Table 8　The Comparison Between this Algorithm and Other Frontier Algorithms in Replay-Mobile Database

表8　算法和其他前沿算法在Replay-Mobile数据库中的比较　%

Method	Test HTER					Test APCER	Test BPCER	Test ACER
	Mattescreen Photo	Mattescreen Video	Paper Fixed	Paper Hand	Grandtest			
IQM[24]	7.70	13.64	4.22	5.43	7.80	19.87	7.40	13.64
Gabor[24]	8.64	9.53	9.40	8.99	9.13	7.91	11.15	9.53
LBP+GS-LBP[8]	0.51	1.16	0.93	0.46	1.13	2.09	1.38	1.74
CCoLBP[11]	0.63	1.15	**0.00**	0.01	1.07	2.08	1.31	1.70
LBP+CCoLBP[11]	0.07	1.05	0.77	0.11	1.23	2.10	0.50	1.30
Ours	**0.00**	**0.00**	0.98	**0.00**	**0.00**	2.08	**0.00**	**1.04**

Note: The data in bold in the table represents the best results.

4　结　　论

本文针对打印攻击和视频攻击提出一种基于DQ_LBP的人脸反欺诈算法.通过将DQ_LBP纹理与空间金字塔算法结合使得该算法在CASIA FASD,Replay-Attack,Replay-Mobile数据库中都表现了较为优异的性能.DQ_LBP是经过分析数据库差值分布和借鉴LBP构造过程形成的一种纹理特征提取方式,该算子能够将像素之间的差值量化来增加原始LBP的纹理信息.将DQ_LBP结合空间金字塔算法一方面解决图片多尺度问题,另一方面提取样本的结构信息.为了降低数据维度,本文还对空间金字塔层数的设置进行讨论.在实验中发现,对于不同的数据集,性能表现最好的颜色空间无法确定,本文将通过将不同的彩色空间进行结合提升本文算法的泛化能力.

本文算法的优点是结合了彩色纹理信息和空间结构信息,能够更加详细地反映样本的纹理特征.DQ_LBP+SP算法和其他传统的算法相比具有更精确的识别性能,和结合卷积神经网络的算法相比,前者训练时间短而且表现出的性能也具有鲁棒性.本文因为细化了图片纹理信息使得算法的跨数据库检测性能不是很好,在后期工作中,我们将会把本文特征提取方法与卷积神经网络结合来尝试提高算法在跨库实验中的性能.

参　考　文　献

[1] Boulkenafet Z, Komulainen J, Hadid A. Face spoofing detection using colour texture analysis [J]. IEEE Transactions on Information Forensics and Security, 2017, 11(8): 1818-1830

[2] Kose N, Dugelay J. Classification of captured and recaptured images to detect photograph spoofing [C] //Proc of the Int Conf on Informatics, Electronics Vision. Piscataway, NJ: IEEE, 2012: 1027-1032

[3] Agarwal A, Singh R, Vatsa M. Face anti-spoofing using Haralick features [C] //Proc of the 8th Int Conf on Biometrics Theory, Applications and Systems. Piscataway, NJ: IEEE, 2016

[4] Pereira T D F, Anjos A, Martino J M D, et al. LBP-TOP based countermeasure against face spoofing attacks [C] //Proc of the 11th Int Conf on Computer Vision. Berlin: Springer, 2013: 121-132

[5] Maatta J, Hadid A, Pietikainen M. Face spoofing detection from single images using micro-texture analysis [C] //Proc of the 1st Int Joint Conf on Biometrics. Piscataway, NJ: IEEE, 2011

[6] Boulkenafet Z, Komulainen J, Hadid A. Face anti-spoofing based on color texture analysis [C] //Proc of the 22nd Int Conf on Image Processing. Piscataway, NJ: IEEE, 2015: 2636-2640

[7] Lazebnik S, Schmid C, Ponce J. Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories [C] //Proc of the 6th IEEE Computer Society Conf on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2006: 2169-2178

[8] Peng Fei, Qin Le, Long Min. Face presentation attack detection using guided scale texture [J]. Multimedia Tools and Applications, 2017, 77(7): 8883-8909

[9] Chingovska I, Anjos A, Marcel S. On the effectiveness of local binary patterns in face anti-spoofing [C] //Proc of the Int Conf of Biometrics Special Interest Group. Piscataway, NJ: IEEE, 2012

[10] Wen Di, Han Hu, Jain A K. Face spoof detection with image distortion analysis [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4): 746-761

[11] Peng Fei, Qin Le, Long Min. CCoLBP: Chromatic co-occurrence of local binary pattern for face presentation attack detection [C] //Proc of the 27th Int Conf on Computer Communication and Networks. Piscataway, NJ: IEEE, 2018

[12] Patel K, Han Hu, Jain A K. Cross-Database face anti spoofing with robust feature representation [C]//Proc of Biometric Recognition. Berlin: Springer, 2016: 611-619

[13] Atoum Y, Liu Yaojie, Jourabloo A, et al. Face anti-spoofing using patch and depth-based CNNs [C]//Proc of IEEE Int Joint Conf on Biometrics. Piscataway, NJ: IEEE, 2017: 319-328

[14] Yan Junjie, Zhang Zhiwei, Lei Zhen, et al. Face liveness detection by exploring multiple scenic clues [C] //Proc of the 12th Int Conf on Control Automation Robotics and Vision. Piscataway, NJ: IEEE, 2012: 188-193

[15] Pan Gang, Sun Lin, Wu Zhaohui, et al. Monocular camera-based face liveness detection by combining eyeblink and scene context [J]. Telecommunication Systems, 2011, 47(3/4): 215-225

[16] Komulainen J, Hadid A, Pietikainen M, et al. Complementary countermeasures for detecting scenic face spoofing attacks [C] //Proc of Int Conf on Biometrics. Piscataway, NJ: IEEE, 2013

[17] Frischholz R W, Dieckmann U. BiolD: A multimodal biometric identification system [J]. Computer, 2000, 33(2): 64-68

[18] Feng Litong, Po Laiman M, Li Yuming, et al. Integration of image quality and motion cues for face anti-spoofing: A neural network approach [J]. Journal of Visual Communication and Image Representation, 2016, 38(C): 451-460

[19] Li Lei, Feng Xiaoyi, Jiang Xiaoyue, et al. Face anti-spoofing via deep local binary patterns [C] //Proc of IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2017: 101-105

[20] Alionte E, Lazar C. A practical implementation of face detection by using Matlab cascade object detector [C] //Proc of the 19th Int Conf on System Theory, Control and Computing. Piscataway, NJ: IEEE, 2015: 785-790

[21] Lin Tsungyi, Dollár P, Girshick R, et al. Feature pyramid networks for object detection [C] //Proc of IEEE Conf on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2017: 936-944

[22] Shi Zenglin, Ye Yangdong, Wu Yunpeng, et al. Crowd counting using ranking-based spatial pyramid pooling network [J]. Acta Automatica Sinica, 2016, 42(6): 866-874 (in Chinese)
(时增林, 叶阳东, 吴云鹏, 等. 基于序的空间金字塔池化网络的人群计数方法[J]. 自动化学报, 2016, 42(6): 866-874)

[23] Zhang Zhiwei, Yan Junjie, Liu Sifei, et al. A face antispoofing database with diverse attacks [C] //Proc of the 5th IAPR Int Conf on Biometrics. Piscataway, NJ: IEEE, 2012: 26-31

[24] Costa-Pazo A, Bhattacharjee S, Vazquez-Fernandez E, et al. The replay-mobile face presentation-attack database [C] //Proc of the Int Conf on Biometrics Special Interests Group. Piscataway, NJ: IEEE, 2016: 209-216

[25] Tan Xiaoyang, Triggs B. Enhanced local texture feature sets for face recognition under difficult lighting conditions [J]. IEEE Transactions on Image Processing, 2010, 19(6): 1635-1650

[26] Zhang Lebin, Peng Fei, Qin Le, et al. Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination [J]. Journal of Visual Communication and Image Representation, 2018, 51: 112-121

[27] Tian Ye, Xiang Shijun. LBP and multilayer DCT based anti-spoofing countermeasure in face liveness detection [J]. Journal of Computer Research and Development, 2018, 55(3): 643-650 (in Chinese)
(田野, 项世军. 基于 LBP 和多层 DCT 的人脸活体检测算法[J]. 计算机研究与发展, 2018, 55(3): 643-650)

[28] Li Haoling, He Peisong, Wang Shiqi, et al. Learning generalized deep feature representation for face anti-spoofing [J]. IEEE Transactions on Information Forensics & Security, 2018, 13(10): 2639-2652

Shu Xin, born in 1979. PhD, associate professor. His main research interests include pattern recognition, face recognition, and computer vision.

Tang Hui, born in 1994. Master. Her main research interests include face recognition and multimedia information security.

Song Xiaoning, born in 1975. PhD, professor. His main research interests include pattern recognition, face recognition, and computer vision.

Yang Xibei, born in 1980. PhD, professor. His main research interests include rough set, granular computing and data mining.

Wu Xiaojun, born in 1967. PhD, professor and PhD supervisor. Senior member of CCF. His main research interests include pattern recognition, computer vision, fuzzy systems, neural networks, and intelligent systems.

2020 年《计算机研究与发展》专题(正刊)征文通知
——人机混合增强智能的典型应用

当前,以大数据驱动的机器学习为核心的人工智能在不确定性、脆弱性和开放性实际应用环境中面临重大挑战.随着知识引导的兴起,一种新的学习范式——“知识引导+数据驱动”的人机混合增强智能应运而生.其基本思路是将人的高级认知、推理和随机决策能力引入到机器高效的计算过程中,实现人在回路的混合增强智能.人机混合的增强智能还面临一系列难题,例如,如何将人的认知、决策行为与机器的知识表征、因果推理过程有效融合;如何构建面向不同计算应用任务的人机混合智能增强智能方法;如何表征和评估人与机器形成的混合增强智能系统的性能等.

《计算机研究与发展》拟于 2020 年 12 月出版应用技术专题——人机混合增强智能的典型应用.本专题希望围绕上述难题讨论人机混合增强智能的关键技术与发展趋势,报导相关技术在行业中的实践案例,交流思想和成果,进而促进相关技术的研究与发展.

征文内容　本专题包括(但不限于)下列主题:

1) 人机混合的知识表征与融合;
2) 人机混合的知识理解与因果推理;
3) 人机混合增强智能在教育领域的典型应用;
4) 人机混合增强智能在舆情分析领域的典型应用;
5) 人机混合增强智能在智慧税务领域的典型应用;
6) 人机混合增强智能在智慧医疗领域的典型应用.

投稿要求

1) 论文应属于作者的科研成果,数据真实可靠,具有重要的学术价值与推广应用价值,未在国内外公开发行的刊物或会议上发表或宣读过,不存在一稿多投问题.作者在投稿时,需向编辑部提交版权转让与投稿声明.
2) 论文一律用 Word 排版,格式体例请参考《计算机研究与发展》近期文章.
3) 论文请通过期刊网站 (http://crad.ict.ac.cn)进行投稿,并在作者留言中注明“人机混合增强智能 2020 专题”(否则按自由来稿处理).

重要日期

征文截止日期: 2020 年 9 月 15 日
录用通知日期: 2020 年 10 月 15 日
修改稿提交日期: 2020 年 10 月 20 日
出版日期: 2020 年 12 月

特邀编委

郑庆华　教授　西安交通大学　qhzheng@mail.xjtu.edu.cn

联系方式

编 辑 部:crad@ict.ac.cn, 010-62620696, 010-62600350
通信地址: 北京 2704 信箱《计算机研究与发展》编辑部
邮　　编:100190