基于频域解离特征的OCT指纹表征攻击检测

刘 凤[1),2),3)] 曾文锋[1),2),3)] 张文天[1),2),3)] 孔 哲[1),2),3)]
王 磊[4)] 沈琳琳[1),2),3)]

[1)](深圳大学计算机与软件学院 广东 深圳 518060)
[2)](广东省智能信息处理重点实验室 广东 深圳 518060)
[3)](深圳市人工智能与机器人研究院 广东 深圳 518060)
[4)](中国科学院深圳先进技术研究院 广东 深圳 518055)

摘 要 在自动指纹识别系统中,指纹防伪能力的发展至关重要.传统指纹一般由表面成像得到,而这种表面的纹理特征极容易被盗取.基于这种传统指纹的识别系统,检测指纹表征攻击的能力十分有限.因此,现有研究普遍针对具有防伪特征的指纹模态,如具有汗腺特征的高精度指纹和具有指静脉特征的指纹开发表征攻击检测算法.在本篇工作中,为了进一步提高指纹系统的表征攻击检测能力,我们提出一种基于光学相干断层扫描技术(Optical Coherence Tomography, OCT)的频域指纹表征攻击检测方法.与以往方法不同,我们首先利用卷积神经网络和残差结构设计了一个频域特征解离模型,通过该模型可以分别解离出时域中叠加在原始OCT指纹图像上的信息(如区分性特征、无效特征和冗余特征).然后,我们让它学习不同的频域编码,并结合OCT指纹在时域中的重构编码形成相应的潜层编码.利用潜层编码,我们设计了一种用于区分表征攻击指纹和真实指纹的预测模型,用于表征攻击检测.在目前常用的OCT指纹数据集上的实验结果表明,我们的方法可以通过在频域中分离出一些叠加在时域中的无用干扰信息,从而有效地消除干扰.在实例方面,该方法的最小误差(Err.)为0.67%,与已有的基于时域的最优方法相比,最小误差降低了3.03%,性能提高了81.89%.

关键词 表征攻击检测;光学相干断层扫描技术;离散小波变换;频域解离;自动编码器
中图法分类号 TP18 **DOI号** 10.11897/SP.J.1016.2024.00323

OCT Fingerprint Presentation Attack Detection Using Frequency Disentangling Features

LIU Feng[1),2),3)] ZENG Wen-Feng[1),2),3)] ZHANG Wen-Tian[1),2),3)] KONG Zhe[1),2),3)]
WANG Lei[4)] SHEN Lin-Lin[1),2),3)]

[1)](*College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, Guangdong* 518060)
[2)](*The Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen, Guangdong* 518060)
[3)](*Shenzhen Institute of Artificial Intelligence and Robotics for Society, Shenzhen, Guangdong* 518060)
[4)](*Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, Guangdong* 518055)

Abstract In automated fingerprint recognition systems (AFRSs), the development of fingerprint anti-spoofing ability is very crucial. Traditional fingerprints are usually obtained by surface fingerprint imaging, and such texture features are easy to be stolen. Fake fingerprints made of low-cost materials, such as artificial fingerprints made of 2D printing, silicone and other materials

收稿日期:2023-03-03;在线发布日期:2023-11-28.本课题得到国家自然科学基金(62076163,82261138629)、广东省自然科学基金(2023A1515010688)、深圳市基础研究项目基金(No.JCYJ20220531101412030)资助.**刘 凤**(通信作者),博士,副教授,主要研究领域为生物特征识别、图像处理和模式识别.E-mail:feng.liu@szu.edu.cn.**曾文锋**,硕士研究生,主要研究领域为计算机视觉、模式识别和生物特征识别.**张文天**,硕士研究生,主要研究领域为图像处理、模式识别和生物特征识别.**孔 哲**,硕士研究生,主要研究领域为图像处理、模式识别和生物特征识别.**王 磊**,博士,副研究员,主要研究领域为图像处理、计算机视觉和机器学习.**沈琳琳**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为深度学习、人脸识别分析和医疗图像处理.

can easily attack these AFRSs. Therefore, using these traditional fingerprints for recognition will be difficult to detect presentation attacks. Existing research generally focuses on fingerprint modes with anti-counterfeiting features, such as high-resolution fingerprints with sweat gland characteristics and fingerprints with finger vein characteristics to develop presentation attack detection algorithms. This paper proposes a novel Optical Coherence Technology (OCT)-based fingerprint Presentation Attack Detection (PAD) method from the frequency domain to further improve the capability of fingerprint attack detection. OCT fingerprint imaging is a three-dimensional imaging technique that can capture subsurface fingerprint information beneath the fingertip's epidermis. An OCT fingerprint data is presented in the form of multiple cross-sectional images (i. e. B-scan), which can reflect multiple layers of biometric structure. It is very different from the surface image of a fingerprint. However, the existing PAD methods based on OCT fingerprint are traditional manual feature extraction methods and time-domain learning-based methods. Handcrafted extraction of fixed features in OCT fingerprint images is easily affected by noise, and these methods are not robust enough. Learning-based methods can learn the distribution of genuine and fake fingerprints and obtain more robust information representation in PAD. However, the information distribution in the image is superimposed, which may be ignored in the time-domain methods. Different from previous approaches, we first design a Frequency Feature Disentangling (FFD) model using convolutional neural networks and residual structures to decompose OCT-based fingerprint B-scans into four different frequency subbands like Discrete Wavelet Transform (DWT). Through such disentangling, information superimposed in the original image in the spatial domain (e. g., discriminative PAD feature, invalid and redundant feature) can be separated respectively. We then let it learn different frequency codes to form their corresponding latent codes. Finally, the spoofness score which is used to distinguish PAs from bonafides is designed based on the latent codes. The experimental results on the commonly used OCT fingerprint dataset, evaluated on the dataset with 93 200 bonafide B-scans from 137 fingers and 48 400 B-scans from 121 PAs, show that our method can effectively preserve the most significant discriminative features and remove some useless interference information superimposed in the spatial domain by disentangling into the frequency domain for eliminating interference and effective PAD. In the performance comparison experiment with existing PAD methods, the proposed method achieves a minimum error (Err.) of 0.67%, which reduces the minimum error by 3.03% and improves the performance by 81.89% compared with the existing time-domain based state-of-the-art (SOTA) method, and there is a difference of only 0.4s in computing consumption. Additionally, we also compare the performance of the proposed method with the SOTA method in different attack materials. The proposed method achieves superior performance in both 2D and 3D attack materials, with a 3.72% reduction in Err. compared to the SOTA method specifically for 2D attack materials.

Keywords presentation attack detection; optical coherence technology; discrete wavelet transform; frequency disentangle; auto-encoder

1 引 言

生物特征作为一种可靠的身份认证特征,在智能设备和个人终端中得到了广泛的应用.在这些生物特征中,各种基于指纹特征的自动指纹识别系统(Automated Fingerprint Recognition Systems, AFRSs)已经在取证和安全领域应用了几个世纪[1-2].然而,由于传统指纹是由表面指纹成像得到的,这种表面的指纹纹理特征很容易获取并被盗用.因此,这些传统的AFRSs在实际的应用场景中存在被表征

攻击(Presentation Attacks，PAs)的风险[3]，即使用某种外部材料对人的指纹进行复制，并将这种复制的指纹置于识别系统的采集端进行攻击的行为. 即使是用低成本的材料制成的伪造指纹，例如由2D打印、硅胶等制成的人工指纹[4-5]就可以轻松攻击这些AFRSs[6]，这种严重的安全问题引起了人们对此类系统可靠性的担忧[7-10]. 图1展示了使用多种类型和多种模态用于伪造指纹的样例. 它们所制作出的PAs是很难被预测的. 因此建立一个具有鲁棒性的表征攻击检测(Presentation Attack Detection，PAD)功能的AFRS是至关重要的.

为了解决上述问题，现有研究提出使用某些特殊指纹采集传感器获取具有活体特征的指纹图像用于PAD，包括高分辨率指纹[11-12]、多视图3D指纹[13-14]和基于光学相干断层成像(Optical Coherence Tomography，OCT)的传感器[5,15-16]. 汗孔特征作为一种指纹上的活体特征，无法被表征攻击材料提取. Zhao等人[11]应用高分辨率传感器获取指尖上的汗孔信息，防止表征攻击. Liu等人[14]提出从双目立体视觉传感器捕获3D指纹，并利用获取到的3D曲率特征，进行指纹识别和PAD. 然而，上述方法仍是基于指纹表面成像传感器的研究，即它们只能对指纹表面较少的活体特征进行研究，其性能仍然受到限制.

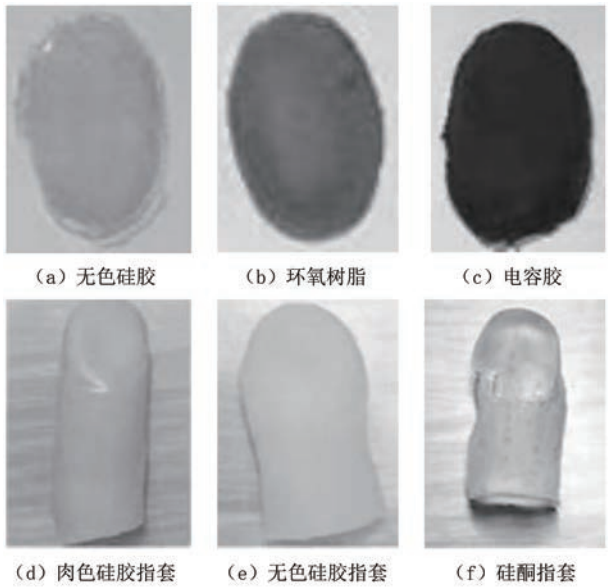
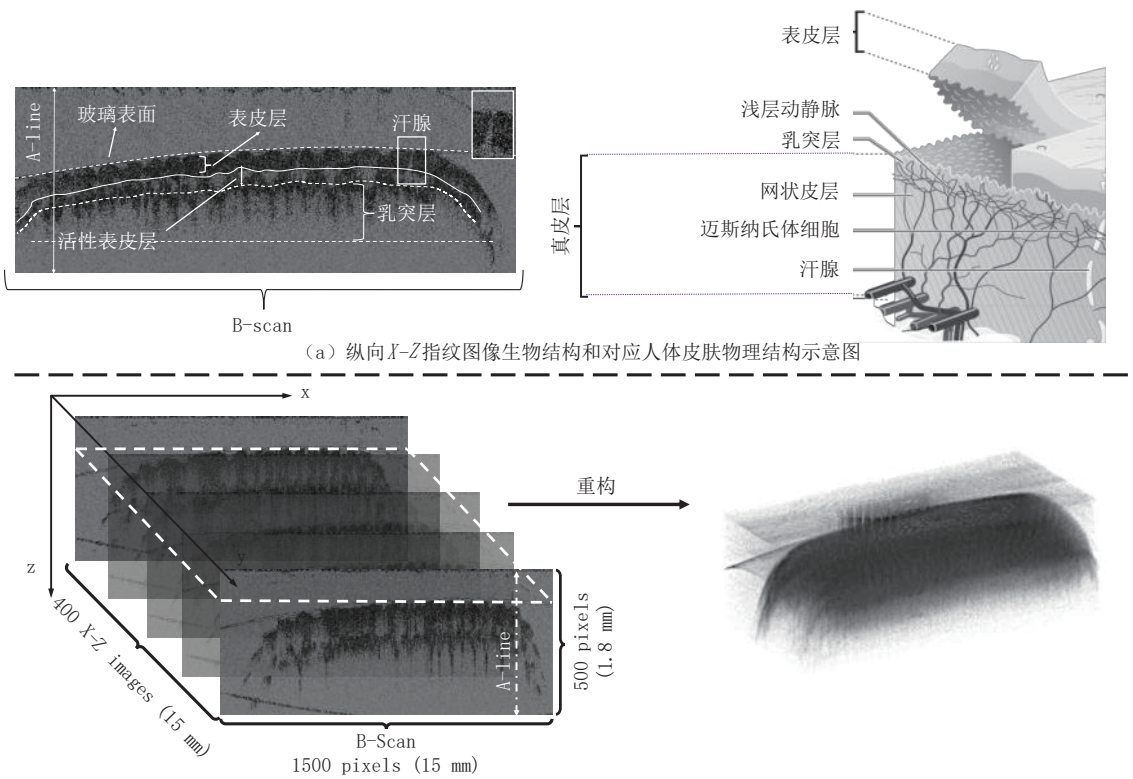


图1　伪造指纹使用材料样例

OCT成像技术的引入为上述表面成像所引起的问题提出一种解决思路[15,17]. 如图2(a)所示，皮肤组织结构与OCT指纹图像相对应，基于OCT成像的指纹可以采集到指尖表皮皮肤以下的指纹亚表面



(a) 纵向*X-Z*指纹图像生物结构和对应人体皮肤物理结构示意图

(b) 一个完整指尖所构成的OCT指纹示意图及对应3D重构结果

图2　OCT指纹图像示例[18]

信息.OCT指纹以多张手指横截面图像(B-scan)的方式对一个指尖的亚表面信息进行表征.每张B-scan图像由多条皮下深度信息(A-line)构成,具有多层次的生物特征结构.如图2(b)所示,OCT传感器沿着水平方向($X-Y$平面)进行扫描,即可得到一个完整指尖的OCT指纹.在图2(a)中,我们展示了在B-scan图像中真实指纹的亚表面结构,可以发现其具有多层的生物特征结构,包括表皮层、活性表皮层、乳突层以及汗腺特征.而对比图3中的表征攻击指纹,即假指纹,无论是2D攻击材料还是3D攻击材料,在它们所表示的B-scan图像中,在亚表面层几乎不存在上述深度信息.已有研究表明,这种深度信息,即多层的生物特征结构包含活体特征.因此,OCT指纹可以用于指纹的表征攻击检测.而如何利用这种多层的深度信息实现高精度的PAD算法,成为OCT指纹研究的关键问题.

一般地,基于OCT指纹的表征攻击检测方法分为两种,即基于特征的方法[5,19-20]和基于学习的方法[16,21-22].基于特征的方法通常指使用特征提取算子或直方图来手动提取OCT指纹图像中固定特征来区分指纹的真伪.Darlow等人[20]通过对A-line不同深度的表示含义提出了两种防伪特征,即双亮特征(Double-bright-feature)和伪造识别特征(Spoof-identification-feature),以区分真实指纹和PAs.这种方法可以达到100%的准确度.但是该方法在论文中仅对少数PAs进行评估,并只在基于OCT的非接触指纹上进行应用.当使用基于接触式的OCT设备采集的样本时,这种方法将无法进行表征攻击检测.为了解决这两个问题,Liu等人[5]基于A-line的深度信息提出了另外两种防伪特征,即深度-双峰特征(Depth-double-peak Feature)和亚单峰特征(Sub-single-peak Feature),可以实现接触式OCT指纹图像的表征检测.通过统计分析这两个特征的比率,可以对指纹的真假进行判别.实验中作者使用四种表征攻击材料对方法进行评估,最终可以达到100%的准确性.然而,这种基于特征的表征攻击检测方法对图像噪声非常敏感,如果测试样本超出确定方法关键参数所需数据集的先验分布,则上述方法有可能会失效.进而研究人员提出了基于学习的表征检测方法,以解决上述问题.

与基于特征的方法相比,基于学习的方法通常使用深度学习模型对真假指纹的分布进行学习,可以在表征检测中获得更加鲁棒的信息表征.Chugh等人[22]提出使用深度卷积神经网络(Convolutional Neural Networks, CNN)进行表征攻击检测,在训练过程中,输入真实指纹和表征攻击的B-scan图像,先提取B-scan的局部块作为检测候选,然后依次输入CNN模型进行分类学习.作者在3413张真实指纹B-scan和357张表征攻击B-scan的数据库上进行评估,在假阳率(False Positive Rate, FPR)为0.2%时,达到了99.73%的真阳率(True Positive Rate, TPR).然而,这种基于有监督的学习模型严重依赖于训练集中极其有限的表征攻击材料样本.在实际情况中,相比容易采集到的真实指纹,表征攻击材料类型虽然十分丰富(如图3),但这种负样本很难在实际场景中进行数据获取.上述方法对未知的表征攻击材料缺乏推广能力.因此,Liu等人[16]设计了一种自监督的表征攻击检测方法来解决这个问题,该方法仅使用真实指纹对模型进行训练.他们提出通过使用自动编码器(Auto-encoder)来表示真

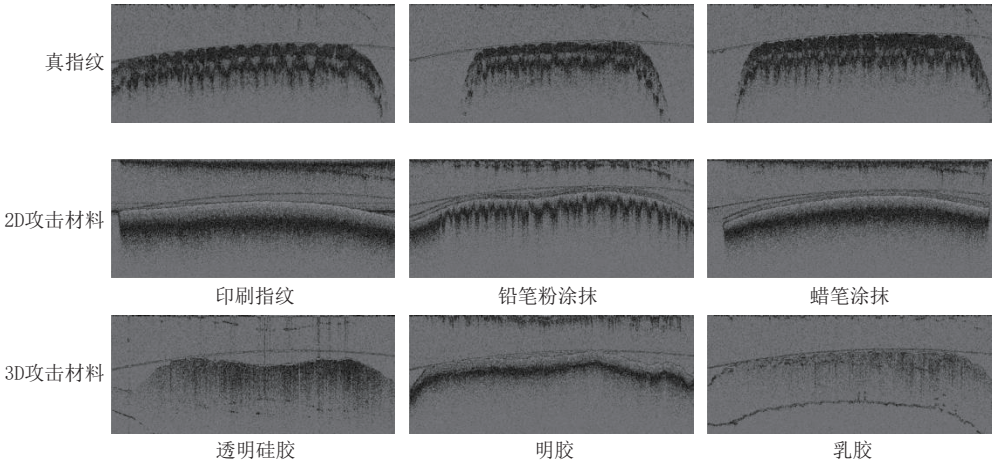


图3 OCT指纹设备采集到的真实指纹和表征攻击指纹B-scan图像示例(第一行表示真实的OCT指纹图像,第二行表示由不同2D攻击材料所制作的伪造指纹图像,第三行表示3D攻击材料形成的表征攻击指纹)

实指纹的分布，并提取重建误差和潜层编码来计算表征攻击检测的分数. 该方法在包含93 200张真实指纹B-scan和48 400张表征攻击B-scan图像上进行验证，当假阳率FPR等于5%时，真阳率TPR达到了96.59%.

我们发现以上的学习型方法都是在时域中直接设计学习模型对攻击材料进行表征检测. 而正如我们所知，图像在时域中的表示虽然更加直观和生动，但图像中信息分布是叠加在一起的. 有研究指出，在频域下可以实现较好的细节信息分离. Nikam等人[23]提出使用Gabor滤波器以提取指纹中细微的纹理细节，基于Gabor能量和共现纹理特征的纹理度量用于表征指纹纹理，通过主成分分析降低特征维度以实现分类. 而Nikam等人[24]提出基于小波能量特征和灰度共生矩阵(GLCM)特征的纹理度量用于表征指纹纹理并用于指纹的表征攻击检测. 我们基于上述频域变换的设计思想，结合学习型方法的优点，设计了一种频域特征的解离方法，把B-scan图像中的信息解离到不同的频域子带，以便于模型对真实指纹的内在表征进行学习和分析. 同时，为了得到推广能力更强的学习模型，我们只使用真实指纹进行训练. 因此，本文提出了一种基于频域特征解离的OCT指纹表征检测方法. 通过将原始的真实指纹图像分解为不同的频域子带，可以有效地在表征攻击检测模型中对无效特征、冗余特征去除并将具有判别性的防伪特征进行学习区分. 我们进一步利用自动编码器将解离的B-scan图像嵌入到不同的潜层编码(例如频域编码和重构编码)中，并设计了一种表征攻击检测的分数计算方法实现更准确的真实指纹聚类和更好的表征攻击检测. 为了验证方法的有效性，我们在自己建立的OCT指纹数据集上进行测试，这个数据集包含来自137名自愿者的93 200张真实指纹B-scan图像和121种攻击材料的48 400张B-scan图像. 实验结果表明，本文所提出的方法可以实现0.67%的检测误差，比目前的最好方法降低了3.03%误差.

论文安排如下：第2节介绍了本文所提出的频域特征解离模型；第3节中描述了本文提出的表征检测分数计算方法；第4节对实验结果进行展示和分析；第5节为本文结论和未来工作的概述.

2　频域特征解离模型

本文提出一种频域特征解离(Frequency Feature Disentangling)模型，在训练中仅输入真实指纹x，以学习不同的频域子带特征. 如图4所示，我们所提出的模型由三部分组成，即频域解离编码器(Enc_{FD})、频域解离解码器(Dec_{IFD})和重构解码器(Dec_R). 其中，Enc_{FD}可以从输入图像中提取不同级别的频域特征，并将其解离到四个不同的频域编码中. 我们使用Dec_{IFD}对不同的频域编码分别进行解码，并生成与输入对应的不同频域子带的B-scan图像. 而Dec_R则定义为从重构编码中学习并生成输入图像. 重构编码则是由不同的频域编码经过特征融合得到，经过Dec_R可以使网络在频域特征解离的过程中保持B-scan的生物结构不变. 最终，利用四个不同的频域编码和重构编码即可进行表征攻击检测. 在训练时，模型使用四个Enc_{FD}针对不同级别的频域特征和四个对应的Dec_{IFD}用于解码.

具体地，在频域解离编码器Enc_{FD}中，我们使用

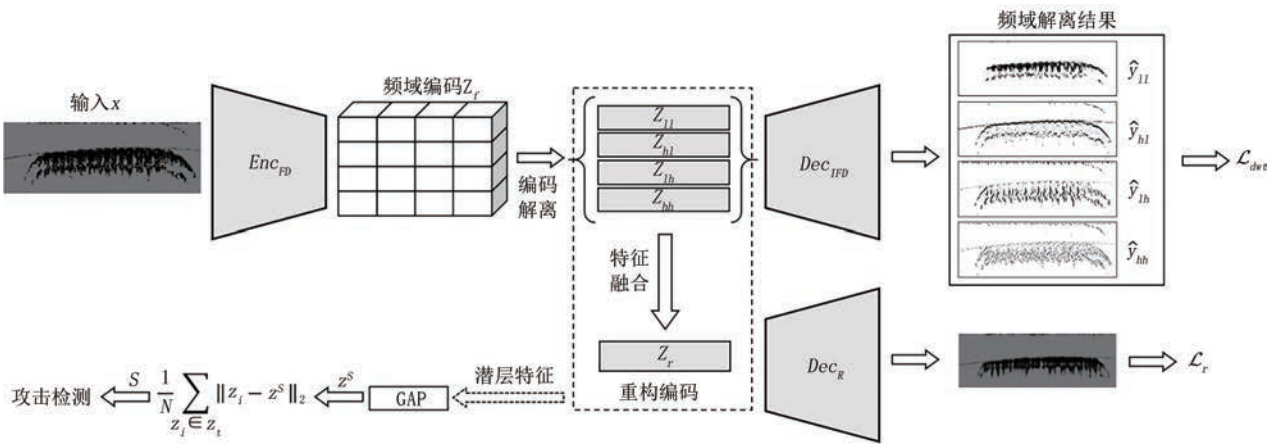


图4　本文所提出的频域特征解离模型(输入图像经过频域解离编码器Enc_{FD}和解码器Dec_{IFD}学习得到不同维度的频域解离结果和输入图像重构结果. 将频域特征解离模型中的潜层特征用于进一步的表征攻击检测)

多个卷积层对输入图像的频域特征f进行解离. 由于Enc_{FD}从垂直和水平两个方向的特征进行提取，并从原始的B-scan图像中每个方向上分别得到低频特征l和高频特征h. 因此频域特征f可以进一步解离得到包含四个子带的特征，定义为$f=\{ll, hl, lh, hh\}$. 在Enc_{FD}中，输入B-scan图像x可以被嵌入到频域编码z_f中，表示为

$$z_f = Enc_{FD}(x) \tag{1}$$

其中z_f包含一个低频特征编码z_{ll}和三个包含高频特征的编码$\{z_{hl}, z_{lh}, z_{hh}\}$. Enc_{FD}的网络结构如表1所示. 执行操作为卷积序列块的类型，步长为特征图缩放的倍数. Enc_{FD}由16个ResNet下采样块[25]构成，每块由两个卷积层(卷积核大小k为(3,3)，步长s为1)和一个卷积层(卷积核大小k为(3,3)，步长s为表1所示)构成，如图5(a)所示.

表1 频域特征解离模型结构说明

	输入	执行操作块	输出通道	操作块数量	步长
Enc_{FD}	65×190×1	block down1	8	2	1
	65×190×16	block down2	16	2	1
	33×95×32	block down3	32	2	2
	35×97×64	block down4	64	2	1
	18×49×128	block down5	128	3	2
	9×25×256	block down6	256	3	2
	13×5×512	block down7	512	2	2
Dec_{IFD} and Dec_R	9×25×256	block up1	256	1	2
	18×49×128	block up2	128	1	2
	35×97×64	block up3	64	1	2
	35×97×32	block up4	32	1	2
	65×190×1	block up5	1	1	2

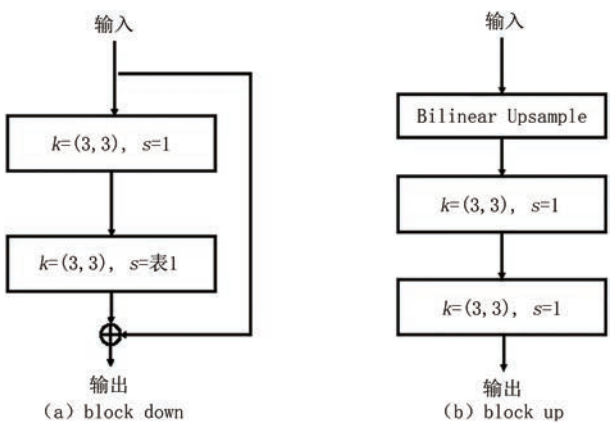


图5 网络结构模块图，(a)编码器中的下采样块，(b)解码器中的双线性上采样块

为了进一步得到图像级别的频域特征解离生成结果，在所提出的模型中我们使用Dec_{IFD}对不同的频域编码z_f进行解码，分别得到相应的4张不同的频域解离图像$\hat{Y}=\{\hat{y}_f | f=ll, hl, lh, hh\}$. 频域编码解码过程表示为

$$\hat{y}_f = Dec_{IFD}(z_f) \tag{2}$$

其中频域解离解码器Dec_{IFD}由5个上采样块构成，如表1所示. 每块包含一个双线性上采样层(步长为2)和两个卷积层(卷积核大小k为(3,3)，步长s为1)，如图5(b)所示.

为了使模型在频域特征解离过程中仍然保持B-scan原有结构特征不变，减少时域信息的损失，我们对频域特征解离模型添加一个重构解码器，增强网络对B-scan图像结构的注意力和学习. 首先我们将频域编码进行特征融合得到重构编码z_r. 具体地，为了使每个频域编码都能关注到B-scan图像在时域的结构特征，我们将每个频域编码在通道维度相连，通过一个卷积层即可得到与每个频域编码大小相同的重构编码z_r. 使用与Dec_{IFD}结构相同的解码器Dec_R，即可从重构编码生成与输入x相对应的重构图像$\hat{y}_r$.

为了让网络模型进行精确的表征学习，我们设计了两个损失函数用于网络训练. 为了实现图像的频域解离，我们使用$\mathcal{L}_{dwt}$损失函数，引导网络对频域特征的表征，并对频域编码和生成的解离结果进行监督. 为了让频域特征解离时仍包含B-scan图像在时域下的生物特征结构，我们使用$\mathcal{L}_r$损失函数完成重构编码的表示和重构图像的监督学习. 本文使用欧氏距离衡量每个损失函数在训练过程中的差异. 最终损失函数表示为

$$\mathcal{L}=\mathcal{L}_{dwt}\left(\hat{Y},Y\right)+\lambda\mathcal{L}_r\left(\hat{y}_r,x\right)=\sum_f\left\|\hat{y}_f-y_f\right\|_2+\lambda\left\|\hat{y}_r-x\right\|_2 \tag{3}$$

其中 $Y=\{y_f|f=ll,hl,lh,hh\}$ 表示 $\hat{Y}$ 的真实标签. 输入 x 为重构图像 $\hat{y}_r$ 的训练标签. Y 由离散小波变换(Discrete Wavelet Transformation, DWT)得到. 为了使模型解离得到最有效的结果,我们在实验中对不同DWT变换的结果进行讨论分析,确定最终 Y 的生成方式. λ 为常数,在训练中作为超参数进行调整. 在网络训练完成时,我们提取不同的频域编码和重构编码作为潜层编码进行表征攻击检测.

3　基于真实指纹潜层编码的表征攻击检测器

由于频域解离模型只在真实指纹中进行特征学习,为了实现表征攻击检测,我们需要手动计算防伪分数,用于区分一个样本是真实指纹或是表征攻击. 本文基于所得到的潜层编码设计了一种防伪分数计算方法. 具体地,我们将每张B-scan所对应的潜层编码在通道维度进行全局平均池化(Global Average Pooling, GAP),得到大小为1×1×512的特征图 z_i 用于表征输入 x 的表征攻击检测编码.

之后为了增加真实指纹与表征攻击所得到编码的差异,我们定义了一个参考分数 z^s. 与文献[16]相似,我们从不同于训练集的真实指纹中定义一个参考集合 S_{score} 来衡量真实指纹在所提频域解离模型中的分布. 在输入数据为 S_{score} 时,参考分数 z^s 由编码 z_i 的平均值计算得到.

计算防伪分数时,我们在测试集合中定义分数计算方式为 $\mathcal{S}$. 测试集中的一个完整指尖的编码被定义为 $Z_t=\{z_1,\cdots,z_i,\cdots,z_N\}$. 防伪分数 $\mathcal{S}$ 计算公示表示为

$$S=\frac{1}{N}\sum_{z_i\in Z_t}\left\|z_i-z^s\right\|_2 \tag{4}$$

其中 $\mathcal{S}$ 是由一个完整指尖的 N 张连续B-scan图像作为输入,使用 N 个 z_i 和 z^s 的欧氏距离的平均值作为分数进行表征攻击检测. 在实际表征攻击检测器中,我们会根据假阳率(FPR)和对应的真阳率(TPR)指标预定义一个阈值 t,当防伪分数超过该阈值时,则输入样本会被检测为表征攻击($Flag=1$),相反,防伪分数小于该阈值时,则表示输入样本越接近真实的指纹($Flag=0$). 基于频域解离模型的表征攻击检测算法总结为算法1.

算法1.　基于频域解离模型的表征攻击检测算法

输入:

训练数据 $x\in$Training set; 测试样本 $x_t\in$ Test Set

频域解离标签: $Y=\{y_f|f=ll,hl,lh,hh\}$

频域解离编码器: Enc_{FD}

频域解离解码器: Dec_{IFD}; 重构解码器: Dec_R

输出:

表征攻击检测分数: $\mathcal{S}$

1. FOR 模型训练迭代次数 DO
2. $z_f\leftarrow$ 公式(1); $z_r\leftarrow$ 融合 z_f
3. $\hat{y}_f\leftarrow$ 公式(2); $\hat{y}_r\leftarrow Dec_R(z_r)$
4. $\mathcal{L}\leftarrow$ 公式(3)
5. 更新 $Enc_{FD}, Dec_{IFD}\leftarrow\partial(\mathcal{L})/\partial\hat{y}_f$
6. 更新 $Enc_{FD}, Dec_R\leftarrow\partial(\mathcal{L})/\partial\hat{y}_r$
7. END FOR
8. $z_i\leftarrow GAP\{z_{ll},z_{hl},z_{lh},z_{hh},z_r\}$
9. $\mathcal{S}\leftarrow$ 公式(4)
10. IF $\mathcal{S}>t$ THEN $Flag=1$
11. ELSE $Flag=0$
12. END IF
13. 返回 $Flag$

4　实验结果与分析

为证明所提出的基于频域特征解离模型进行指纹表征攻击检测方法的合理性和有效性,本节从以下五个小节实验进行论述和分析. 小节4.1介绍训练频域特征解离模型和表征攻击检测效果验证所使用的数据集. 小节4.2介绍模型训练数据划分及详细参数设置. 小节4.3将对本文所提出的频域特征解离模型和具有不同编码器,解码器组合的模型进行实验讨论和对比分析. 小节4.4将对频域特征解离模型学习不同类型离散小波变换的表征攻击检测进行实验,并讨论分析不同频域编码下表征攻击检测效果. 小节4.5将对不同攻击材料的实验结果进行对比分析. 小节4.6将对比本文方法和现有指纹表征攻击检测方法在误差等指标的实验结果.

4.1　数据集介绍

本文采用文献[15]中OCT设备进行指纹扫描和采集,使用的基于OCT指纹的数据集由真实指纹和伪造指纹两部分组成. 其中,真实指纹采集于137位志愿者,共计233×400(手指数量×每手指的B-scan数量)张图像. 伪造指纹采集于121种不同的伪造样本,共计121×400张图像. 伪造样本由专业人员收集的不同三维和二维形式的材料组成,收集时间

超过4个月，具体包含透明硅胶、塑料、乳胶等材料. 同时对于三维伪造材料，由于在采集样本时是否进行手指按压会导致非常不同的数据表征，因此我们也在这两种不同的按压方式下收集三维伪造样本. 具体地，伪造样本包含20个三维未按压样本、20个三维按压样本和81个二维伪造样本. 如图2(b)所示，一个指纹样本的扫描包含400幅B-scan图像，每张B-scan由1500条A-line构成. 每条A-line长度为500像素(pixels). 因此对于每个真实指纹和伪造样本，其图像尺寸为500×1500×400 pixels，对应图像大小为15 mm×15 mm×1.8 mm. 由于B-scan图像经过频域解离得到的标签图像尺寸为190×65，小于1500×500，因此我们在训练频域解离模型前，先将输入图像使用双线性插值调整大小至190×65，再进行频域特征的学习和解离.

4.2 数据划分和参数设置

具体地，我们将上述数据集划分成训练数据和测试数据. 训练数据由训练集和参考集(S_{score})组成，我们从数据集中随机选取来自于41位志愿者的41个真实指纹(16 400张B-scan图像)作为训练集输入到网络进行训练. 而参考集S_{score}包含16个真实指纹(6400张B-scan图像)用于防伪分数的计算，它们采集于8位志愿者(每个手指间隔两周共采集两次). 测试数据由数据集中其他指纹图像和防伪样本构成，包含从88位志愿者手指采集(每个手指间隔两周共采集两次)的176个真实指纹(70 400张B-scan图像)和121个伪造样本(48 400张B-scan图像)对表征攻击检测性能进行验证.

我们的模型基于公共平台PyTorch[26]进行编写和训练. 具体地，频域解离模型由4个独立的频域编码器，对应的4个频域解码器，以及一个重构解码器构成. 在参数初始化阶段，使用标准偏差为0.02的零均值高斯分布初始化模型每层结构中的参数权重. 选取Adam优化器[27]用于频域解离模型的训练，其学习率设置为0.0001，β_1和β_2分别设置为0.9和0.999. 频域解离标签由基于反向双正交小波(rbio)的三阶离散小波变换得到. 模型训练迭代次数为100代. 所使用工作站的CPU为2.2 GHz，内存为32 GB，显卡为NVIDIA Tesla V100.

为了评估表征攻击检测方法的性能，本文采用了三种常用指标，即误差(Err.)、假阳率为10%和5%(FPR=10%和FPR=5%)时的真阳率(TPR)的值. 误差Err.是指在预测中分类错误样本数占总样本数的比例，其中分类错误样本数是错误接受和错误拒绝的样本数量之和. Err.反映了模型的分类性能，Err.越小，所评估方法的检测效果越好. 真阳率TPR(FPR=10%)和TPR(FPR=5%)表示当伪造样本的假阳率为10%和5%时真实指纹判断为真的百分比，其数值越大则表示评估方法的性能越好.

4.3 频域解离模型的有效性验证

本小节为验证所提方法的有效性，在训练完成的频域解离模型上，对基于不同频域编码z_f和重构编码z_r的表征攻击检测性能进行分析. 首先，对频域解离模型中的重构编码进行消融实验，使用生成的不同潜层编码计算防伪分数$\mathcal{S}$. 如表2所示，在频域解离模型中不使用重构编码时，代表图像垂直和水平两个方向只保留低频特征的z_{ll}编码可以取得最好的PAD效果，具有0.67%的误差Err.，以及在FPR为5%时达到了100.00%的TPR. 垂直方向为高频特征，水平方向为低频特征的z_{hl}编码也可以达到有效表征攻击检测效果，具体为3.31%的误差Err.，并且当FPR为5%时TPR才达到97.43%. 而其他两个在水平方向为高频特征的编码均无法达到有效的PAD结果. 在使用重构编码时，可以看到三个具有低频信息的编码都可以取得有效的PAD结果. 相比不使用重构编码，z_{hl}和z_{lh}的PAD指标都取得大幅提升，只有z_{hh}编码无法用于表征攻击检测. 这表明在频域解离模型中加入图像的重构学习可以进一步提升模型频域解离的精度和生成编码在PAD中的性能，并且拉大无效特征编码在PAD中表现的差距. 另外，由表2可知，重构编码z_r的PAD误差指标为3.36%，而z_{ll}和z_{hl}取得的结果远远好于z_r. 这证明学习指纹图像的频域解离特征比在时域下学习指纹图像的重构可以更好地用于指纹表征攻击检测. 在频域空间下，低频信息包含更多的判别信息(活体特征)可用于表征攻击检测，而高频信息包含更多的冗余和无效信息阻碍表征攻击检测性能的提升，进一步证明本文方法有效性.

由于本文频域解离模型使用四个频域解离编码器(Enc_{FD})和四个相应的频域解离解码器(Dec_{IFD})完成频域特征学习和网络的训练. 为验证本文频域解离模型结构的有效性，我们使用多种频域解离编码器和频域解离解码器组合方式进行频域编码的生成学习并用于表征攻击检测. 具体分别为，使用四个对应的Enc_{FD}和一个参数共享的Dec_{IFD}进行训练，使用一个参数共享的Enc_{FD}和四个对应的Dec_{IFD}进行

表2　频域解离模型在是否使用重构编码时的性能对比

评价指标	重构编码(z_r)	频域解离模型编码				
		z_{ll}	z_{hl}	z_{lh}	z_{hh}	z_r
Err.(%)	×	**0.67**	3.31	20.94	38.12	-
TPR(FPR=10%)(%)	×	**100.00**	99.16	64.39	13.44	-
TPR(FPR=5%)(%)	×	**100.00**	97.43	56.70	8.57	-
Err.(%)	√	**0.67**	1.34	5.37	40.94	3.36
TPR(FPR=10%)(%)	√	**100.00**	100.00	96.02	12.50	98.30
TPR(FPR=5%)(%)	√	**100.00**	100.00	92.05	7.96	96.59

训练，以及使用一个参数共享的Enc_{FD}和一个参数共享的Dec_{IFD}进行训练. 如表3所示，我们对四种不同的频域解离模型结构所生成的编码进行表征攻击检测验证，可以发现这四种结构的模型都可以生成有效的频域编码和重构编码用于PAD. 其中，只用一个共享参数的Enc_{FD}和Dec_{IFD}时，其PAD结果相比其他网络结构的结果最差. 这种网络结构下，基于重构编码的误差Err. 为3.69%可以达到更好的PAD结果. 而频域编码中PAD最好的结果(z_{ll}编码)只能达到4.36%的误差Err.. 这是由于编码器和解码器的数量均小于需要进行(四个方向)频域解离特征的数量，网络不能够很好地重构出和频域解离标签更相近的结果，所得到的潜层编码无法更好地与四个方向的频域特征分离，其中混淆的冗余信息导致基于这种编码的PAD结果更差. 同理，当只使用一个共享参数的Enc_{FD}或Dec_{IFD}时，尽管有四个Dec_{IFD}和Enc_{FD}与之相对应，频域编码仍不能够更好地按照四个方向的高低频特征进行分离，在表征攻击检测时它们的结果仍远远低于使用四个Enc_{FD}和四个相应的Dec_{IFD}时的结果. 因此，上述实验表示在本文所提的频域解离模型结构中，所设计和使用的四个频域解离编码器(Enc_{FD})和四个相应的频域解离解码器(Dec_{IFD})结构更好，也证明了本文所提出的模型的有效性和优越性.

表3　不同频域解离模型生成编码的PAD性能对比

Enc_{FD}数量	Dec_{IFD}数量	评价指标	频域解离模型编码				
			z_{ll}	z_{hl}	z_{lh}	z_{hh}	z_r
1	1	Err.(%)	**4.36**	4.63	15.82	37.57	3.69
		TPR(FPR=10%)(%)	**98.30**	97.36	81.95	23.64	98.77
		TPR(FPR=5%)(%)	**96.02**	95.52	75.47	17.29	96.93
4	1	Err.(%)	3.36	**2.35**	11.73	40.94	6.04
		TPR(FPR=10%)(%)	97.16	**100.00**	84.09	21.59	96.02
		TPR(FPR=5%)(%)	96.59	**98.86**	78.98	14.77	90.91
1	4	Err.(%)	**2.69**	3.17	9.74	39.55	3.36
		TPR(FPR=10%)(%)	**98.86**	98.13	88.49	18.85	98.86
		TPR(FPR=5%)(%)	**97.16**	97.66	84.31	10.46	96.59
4	4	Err.(%)	**0.67**	1.34	5.37	40.94	3.36
		TPR(FPR=10%)(%)	**100.00**	100.00	96.02	12.50	98.30
		TPR(FPR=5%)(%)	**100.00**	100.00	92.05	7.96	96.59

同时，我们也探讨了模型损失函数(3)中的超参数λ的具体取值对模型性能的影响分析. 如表4所示，在不使用λ或λ小于等于1时，本文方法使用z_{ll}编码进行表征攻击检测都可以取得相同的结果. 这说明在水平和竖直两个方向都为低通时，目标函数对于指纹重构编码z_r不敏感. 而当λ=1.5时，表征攻击检测的误差升高，这说明，当指纹重构在目标函数中的权重大于频域解码时，指纹重构将干扰z_{ll}编码的正常学习.

表4　本文方法不同λ的Err. 性能表现

λ	0	0.5	1.0	1.5
Err.(%)	0.67	0.67	0.67	0.87
TPR(FPR=10%)(%)	100.00	100.00	100.00	100.00
TPR(FPR=5%)(%)	100.00	100.00	100.00	100.00

4.4　使用不同离散小波变换的PAD对比分析

为了进一步探究不同频域特征对解离模型学习

的影响，本小节使用多种离散小波对指纹图像进行小波变换，并提取频域特征作为标签图像用于解离模型的训练．之后基于上述模型生成的频域编码进行防伪分数计算和表征攻击检测．本文除了使用三阶反向双正交小波(rbio)[28]进行实验，也对比了双正交小波(bior)[29]，离散迈耶小波(dmey)[30]，哈尔小波(haar)[31]，Symlets小波(sym)[32]，多贝西小波(db)[33]以及Coiflets小波(coif)[34]在表征攻击检测任务上的具体效果．表5展示了使用不同离散小波训练的模型用于PAD的性能对比．具体地，使用所有离散小波类型得到的低频编码z_{ll}，都可以在表征攻击检测中取得优秀的实验效果，其中使用反向双正交小波(rbio)可以达到最好结果，具体指标为0.67%的误差Err.．在生成z_{hl}编码时，由表5可以发现，所有离散小波变换基本可以实现有效的PAD，使用离散迈耶小波dmey训练模型，可以达到最好的PAD结果，指标为1.01%的误差Err.．而在生成的z_{lh}编码中，哈尔小波haar和Coiflets小波训练得到的模型无法用于PAD，而其余离散小波变化均可取得有效的结果，最好结果由Symlets小波取得，可达到1.01%的误差Err.．最后在生成的高频编码z_{hh}中，可以发现所有离散小波变换类型得到的指标都具有很高的误差和很低的真阳率，不能用于表征攻击检测．上述实验结果证明，通过频域解离模型得到的两个方向的不同高低频特征中，低频信息包含更多的可以用于表征攻击检测的特征，而高频信息中包含更多的是对于PAD任务无效或冗余的特征．在图像垂直和水平方向都只包含低频信息时，其对应的频域编码可以在PAD任务中有最稳定的表现．对反向双正交小波(rbio)变换得到的频域特征进行训练和特征解离，可以在其PAD任务中有最出色表现．

表5 不同离散小波变换训练模型生成频域编码的PAD性能对比

离散小波类型	z_{ll}			z_{hl}			z_{lh}			z_{hh}		
	Err.(%)	TPR(FPR=10%)(%)	TPR(FPR=5%)(%)	Err.(%)	TPR(FPR=10%)(%)	TPR(FPR=5%)(%)	Err.(%)	TPR(FPR=10%)(%)	TPR(FPR=5%)(%)	Err.(%)	TPR(FPR=10%)(%)	TPR(FPR=5%)(%)
Bior	2.01	99.43	98.86	6.04	94.89	92.05	5.37	96.59	93.75	26.85	55.11	43.18
dmey	5.03	98.30	61.93	**1.01**	**100.00**	**100.00**	3.02	100.00	97.73	40.94	3.41	1.71
haar	3.02	99.43	96.59	2.35	98.86	97.73	37.58	32.39	26.14	20.47	71.59	63.07
sym	2.35	99.43	98.30	16.11	49.43	36.36	**1.01**	**100.00**	**100.00**	39.26	13.07	3.41
db	2.35	100.00	98.30	4.70	97.73	90.34	2.69	99.43	98.3	**17.11**	**63.07**	**54.55**
coif	3.02	100.00	97.73	10.40	7.96	0.57	40.94	1.71	1.14	40.94	14.77	11.36
rbio	**0.67**	**100.00**	**100.00**	1.34	100.00	100.00	5.37	96.02	92.05	40.94	12.50	7.96

另外，我们给出了不同离散小波变换训练频域解离模型时，使用对应的重构编码进行PAD时的结果对比．如表6所示，所有类型生成得到的重构编码都可以取得有效的PAD指标，其中Symlets小波(sym)，多贝西小波(db)和反向双正交小波(rbio)都可以取得最低的检测误差Err.为3.36%．这也表明本文所提出的频域解离模型生成的重构编码几乎都可以有效适用于基于OCT的指纹图像的PAD任务，证明了所提方法的优越性．

表6 不同离散小波变换训练模型生成重构编码的PAD性能对比

离散小波类型	频域解离模型重构编码z_r		
	Err.(%)	TPR(FPR=10%)(%)	TPR(FPR=5%)(%)
bior	3.69	97.73	96.02
dmey	18.46	65.34	54.55
haar	5.71	96.59	92.61
sym	**3.36**	97.73	96.59
db	**3.36**	**99.43**	**97.16**
coif	7.05	94.32	81.25
rbio	**3.36**	98.30	96.59

4.5 不同攻击材料的结果对比分析

本节分别对二维攻击样本和三维攻击样本进行分析，并使用所提频域解离模型进行实验验证．如图3所示，二维攻击样本在采集时只保留了指纹的平面信息，只包括脊线和谷线的分布走向和用于指纹识别的细节点特征．而三维攻击样本不同于上述二维攻击样本，在采集时不仅可以获取已有的平面指纹信息，还可以获得脊线和谷线的深浅信息，即指纹的3D特征．因此在B-scan中，三维攻击样本相比于二维攻击样本，在指纹的活性表皮层和乳突层中普遍也包含指纹特征．因此三维攻击样本在实际的指纹表征攻击检测中难度更高．表7显示了本文方

法使用rbio小波和z_{ll}编码时，在两种不同攻击材料中的实验结果.

表7　本文方法和对比方法在不同攻击材料中的性能表现

攻击材料	方法	Err.(%)	TPR (FPR=10%)(%)	TPR (FPR=5%)(%)
二维攻击样本	本文方法	0.53	100.00	100.00
	OCPAD	4.25	97.16	95.45
三维攻击样本	本文方法	0.58	100.00	100.00
	OCPAD	3.93	87.79	75.88

可以发现，本文方法对两种攻击材料都可以实现有效的检测结果. 其中对二维攻击样本可以达到更低的0.53%的误差Err.，对三维攻击样本的检测结果也可以达到0.58%的误差Err.. 同时我们也对比了目前已经提出的PAD最好方法——基于单类别自动编码表征攻击检测方法(OCPAD)[16]，相比于OCPAD，我们的方法无论是在二维攻击样本还是在三维攻击样本上，都取得了更好的表征攻击检测效果，尤其是在二维攻击样本上，我们方法的误差Err. 相比于OCAPD降低了3.72%.

4.6　现有 PAD 方法结果对比分析

为了进一步验证本文方法的有效性，我们对比了目前已经提出的PAD最好方法，包括基于深度的双峰特征检测方法(Depth-double-peak)[5]、对指纹频域特征主成分分析的方法(PCA)[35]、基于单类别监督的生成对抗方法(One-class GAN)[36]和基于单类别自动编码表征攻击检测方法(OCPAD)[16]. 其中，Depth-double-peak方法和PCA方法是使用手动标注的一种基于特征提取的PAD方法. 而One-class GAN和OCPAD方法都是只使用真实指纹进行的基于模型训练的学习方法. 如表8所示，One-class GAN的误差Err. 高达5.7%，在FPR为10%时TPR虽然可以达到92.05%，但是在FPR为5%时TPR只有20.45%，该值在所有方法中表现最差. 现有最好方法为OCPAD，其指标只能达到3.70%的误差Err.，以及在FPR为10%时TPR达到了99.46%和在FPR为5%时TPR才96.59%. 而本文所提出的方法可以在误差Err. 上达到0.67%，并且在FPR等于5%和10%时，TPR都达到了100.00%，相比OCPAD可以取得大幅的提升，性能提升了81.89%((3.70%-0.67%)/3.70%). 另外，我们对比了现有方法的检测效率，如表8所示，本文方法在计算耗费上与耗时最小的OCPAD方法仅相差0.4 s，但可以获得更高的表征检测性能的提升. 同时本文绘制ROC曲线图，以更加直观的方式展示本文方法的优越性. 如图6所示，相比于其他四种方法，本文方法可以在FPR等于5%之前就取得100%的TPR结果. 而其他对比方法只能在FPR等于10%之后才能达到相同结果，这也表明本文所提出的频域特征解离方法可以有效地将时域中混淆的OCT表征特征进行分离，并将其中最显著的判别特征保留，进一步提升表征攻击检测的效果.

表8　本文方法与现有PAD方法的性能对比

方法	Err.(%)	TPR (FPR=10%)(%)	TPR (FPR=5%)(%)	Time (s)
Depth-double-peak[5]	12.79	84.66	53.98	-
PCA[35]	7.38	93.75	76.14	2.27
One-class GAN[36]	5.70	92.05	20.45	-
OCPAD[16]	3.70	99.43	96.59	2.11
本文方法	0.67	100.00	100.00	2.44

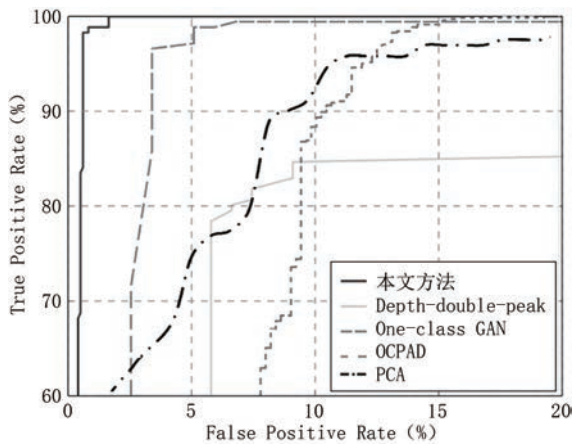


图6　与现有PAD方法结果对比的ROC曲线图

5　结　论

本文提出了一种基于频域特征学习的解离模型，以在频域空间下找到对真实指纹和伪造样本具有判别性的编码，用于提升指纹表征攻击检测的性能. 传统的指纹表征攻击检测方法往往只在时域下对图像中的特征进行提取和分析，但是由于其中的有效特征分布往往是混乱和复杂的，难以找到一种合适的特征表征方式，因此这种表征攻击检测方法的性能提升十分受限. 与传统方法不同，我们首先设计了一种频域特征解离模型，通过让网络学习图

像的离散小波变换过程，掌握指纹图像的高低频信息分离过程，得到高维的包含区分性特征和冗余特征的潜层编码．基于潜层编码，我们进一步设计了一种防伪分数计算方法，用防伪分数进行指纹的表征攻击检测．本文使用基于OCT的指纹防伪数据集（包含70 400个真实指纹数据和12 100个伪造样本）对所提出的方法进行实验验证，并讨论不同高低频特征对表征攻击检测的影响以及不同离散小波变换对于本文模型的影响．实验结果表明在指纹图像仅包含低频特征时，可以得到更好的表征攻击检测性能．同时，在使用反向双正交小波进行变换时，模型可以取得最好的表征攻击检测结果．具体地，本文方法可以实现0.67%的误差，与最佳方法相比降低3.03%的误差．

本文提出的方法在PAD取得不错效果的同时，我们也分析了所提模型存在的瓶颈以及下一步的研究思路：(1)我们的算法对于不同小波变换的结果缺乏一定的自适应调整，如在4.4节中使用不同离散小波变换的PAD对比分析的描述，我们验证了使用不同离散小波变换时PAD效果存在有一定的差异，无法自适应地对不同离散小波进行调整．(2)网络模型泛化性能还不够，我们仅使用自动编码器结构对图像的特征进行提取，后续可以增加对抗训练来提高模型的泛化性．

基于OCT的指纹数据开辟了指纹识别的新领域，同时也带来一些新的问题．OCT指纹构成形式不同于传统指纹表面成像，它由不同的横截面图像(B-scan)构成，需要通过指纹重构方法转换为二维指纹才能进行识别，与现有指纹识别技术衔接存在一定的挑战．团队将在未来的工作中进一步讨论B-scan级别的指纹识别方法，并将防伪方法和识别方法结合，形成一套高度安全的OCT指纹识别系统．

致 谢 感谢国家自然科学基金(62076163，82261138629)、广东省自然科学基金(2023A1515010688)、深圳市基础研究项目基金(No. JCYJ20220531101412030)对本研究的资助．

参 考 文 献

[1] Lin C，Kumar A. Matching contactless and contact-based conventional fingerprint images for biometrics identification. IEEE Transactions on Image Processing，2018，27(4)：2008-2021

[2] Das A，Galdi C，Han H，et al. Recent advances in biometric technology for mobile devices//Proceedings of the IEEE 9th International Conference on Biometrics Theory，Applications and Systems (BTAS). Vancouver，Canada，2018：1-11

[3] Marcel S，Nixon M S，Li S Z. Handbook of Biometric Anti-spoofing：Volume 1. Berilin，Germany：Springer，2014

[4] Sousedik C，Busch C. Presentation attack detection methods for fingerprint recognition systems：a survey. Iet Biometrics，2014，3(4)：219-233

[5] Liu F，Liu G，Wang X. High-accurate and robust fingerprint anti-spoofing system using optical coherence tomography. Expert Systems with Applications，2019，130：31-44

[6] Goicoechea-Telleria I，Fernandez-Saavedra B，Sanchez-Reillo R. An evaluation of presentation attack detection of fingerprint biometric systems applying ISO/IEC 30107-3//Proceedings of the International Biometric Performance Testing Conference. Maryland，USA，2016

[7] Jia J，Cai L，Zhang K，et al. A new approach to fake finger detection based on skin elasticity analysis//Proceedings of the Advances in Biometrics：International Conference (ICB). Seoul，Korea，2007：309-318

[8] Antonelli A，Cappelli R，Maio D，et al. Fake finger detection by skin distortion analysis. IEEE Transactions on Information Forensics and Security，2006，1(3)：360-373

[9] Lee H，Maeng H，Bae Y. Fake finger detection using the fractional Fourier transform//Proceedings of the Biometric ID Management and Multimodal Communication：Joint COST 2101 and 2102 International Conference，BioID_MultiComm 2009. Madrid，Spain，2009：318-324

[10] Nikam S B，Agarwal S. Fingerprint liveness detection using curvelet energy and co-occurrence signatures//Proceedings of the IEEE Fifth International Conference on Computer Graphics，Imaging and Visualisation. Penang，Malaysia，2008：217-222

[11] Zhao Q，Zhang L，Zhang D，et al. Direct pore matching for fingerprint recognition//Proceedings of the Advances in Biometrics：Third International Conference. Alghero，Italy，2009：597-606

[12] Liu F，Zhao Q，Zhang D. A novel hierarchical fingerprint matching approach. Pattern Recognition，2011，44(8)：1604-1613

[13] Liu F，Zhang D. 3D fingerprint reconstruction system using feature correspondences and prior estimated finger model. Pattern Recognition，2014，47(1)：178-193

[14] Liu F，Zhang D，Shen L. Study on novel curvature features for 3D fingerprint recognition. Neurocomputing，2015，168：599-608

[15] Liu F，Shen C，Liu H，et al. A flexible touch-based fingerprint acquisition device and a benchmark database using optical coherence tomography. IEEE Transactions on Instrumentation and Measurement，2020，69(9)：6518-6529

[16] Liu F，Liu H，Zhang W，et al. One-class fingerprint presentation attack detection using auto-encoder network. IEEE Transactions on Image Processing，2021，30(3)：2394-2407

[17] Liu F, Zhang W T, Liu H Z, et al. Subsurface fingerprint reconstruction based on deep learning. Chinese Journal of Computers, 2021, 44(10): 2033-2046
刘凤，张文天，刘浩哲，等. 基于深度学习的亚表面指纹重构. 计算机学报，2021，44(10)：2033-2046
[18] MADHERO88. Layers of the skin. https://en.wikipedia.org/wiki/File:Skin_layers.png
[19] Cheng Y, Larin K V. Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis. Applied Optics, 2006, 45(36): 9238-9245
[20] Darlow L N, Webb L, Botha N. Automated spoof-detection for fingerprints using optical coherence tomography. Applied Optics, 2016, 55(13): 3387-3396
[21] Nogueira R F, de Alencar Lotufo R, Machado R C. Fingerprint liveness detection using convolutional neural networks. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1206-1213
[22] Chugh T, Jain A K. OCT fingerprints: Resilience to presentation attacks. arXiv preprint arXiv: 1908.00102, 2019
[23] Nikam S B, Agarwal S. Gabor filter-based fingerprint anti-spoofing//Proceedings of the International Conference on Advanced Concepts for Intelligent Vision Systems (ACIVS). Juan-les-Pins, France, 2008: 1103-1114
[24] Nikam S B, Agarwal S. Wavelet energy signature and GLCM features-based fingerprint anti-spoofing//Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR). Hong Kong, China, 2008, 2: 717-723
[25] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, USA, 2016: 770-778
[26] Paszke A, Gross S, Chintala S, et al. Automatic differentiation in pytorch//Proceedings of the 31st Conference on Neural Information Processing Systems (NIPS 2017). LongBeach, USA, 2017: 1-4
[27] Kingma D P, Ba J. Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014
[28] Abbasi H, Bennet L, Gunn A J, et al. Latent phase detection of hypoxic-ischemic spike transients in the eeg of preterm fetal sheep using reverse biorthogonal wavelets & fuzzy classifier. International Journal of Neural Systems, 2019, 29(10): 1950013
[29] Dong H, Wang F. Image-denoising based on bior wavelet transform and median filter//Proceedings of the Symposium on Photonics and Optoelectronics. Shanghai, China, 2012: 1-3
[30] Morade S S, Patnaik S. Lip reading by using 3-d discrete wavelet transform with dmey wavelet. International Journal of Image Processing, 2014, 8(5): 384
[31] Stankovic R S, Falkowski B J. The haar wavelet transform: itsstatus and achievements. Computers & Electrical Engineering, 2003, 29(1): 25-44
[32] Wang X, Gong G, Li N. Automated recognition of epileptic eeg states using a combination of symlet wavelet processing, gradient boosting machine, and grid search optimizer. Sensors, 2019, 19(2): 219
[33] Liu Y, Cen Z. Daubechies wavelet meshless method for 2-d elastic problems. Tsinghua science and Technology, 2008, 13(5): 605-608
[34] Elgendi M, Jonkman M, De Boer F. R wave detection using Coiflets wavelets//Proceedings of the IEEE 35th Annual Northeast Bioengineering Conference. Boston, USA, 2009: 1-2
[35] Yuan C, Sun X, Lv R. Fingerprint liveness detection based on multi-scale LPQ and PCA. China Communications, 2016, 13(7): 60-65
[36] Engelsma J J, Jain A K. Generalizing fingerprint spoof detector: Learning a one-class classifier//Proceedings of the International Conference on Biometrics. Crete, Greece, 2019: 1-8

LIU Feng, Ph. D., associate professor. Her research interests include biometrics, image processing and pattern recognition.

ZENG Wen-Feng, M.S. candidate. His research interests include computer vision, pattern recognition and biometrics.

ZHANG Wen-Tian, M. S. candidate. His research interests include image processing, pattern recognition and biometrics.

KONG Zhe, M. S. candidate. His research interests include artificial intelligence, computer vision and biometrics.

WANG Lei, Ph. D., associate researcher. His research interests include image processing, computer vision and machine learning.

SHEN Lin-Lin, Ph. D., professor. His research interests include deep learning, face recognition analysis and medical image processing.

Background

Fingerprint, as one of the reliable biometric features, is widely applied to personal identification systems, i.e., automated fingerprint recognition systems. However, these

systems are in risk of presentation attacks (PAs) like artificial fingerprints made by 2D prints, silica gel or other materials with low cost. Researchers have been seeking effective presentation attack detection (PAD) methods for security reasons. Due to the nature of internal representation of the fingertip skin can be provided by Optical Coherence Technology (OCT) and such internal fingerprints have excellent capability for PAD, fingerprint PAD based on OCT becomes more and more attractive.

In general, PAD methods propose to extract hand-crafted features or learned features from fingerprints to detect PAs. However, methods using hand-crafted features are lack of robustness to image noise and sample dataset beyond prior distribution. Traditional learning-based PAD methods using both bonafides and PAs for training heavily rely on the training data and lack generalization. To facilitate generalization against unpredictable PAs one-class PAD models are proposed, which are only trained by bonafides. They not only have better generalization ability but also alleviate the data dependent problem caused by the unexpected differences among diverse PAs. However, existing one-class methods ignore the distribution of invalid or interference information among bonafides.

As we know, the representation in the spatial domain is more vivid and intuitive, however, its information is superimposed together. Motivated by the design idea of frequency transform, which can separate information into different frequency subbands for concise and convenient analysis, this paper proposed a frequency feature disentangling based method adopting a one-class model for OCT-based fingerprint PAD. Through decomposing original bonafide images into different frequency subbands, invalid, redundant and discriminative features for PAD can be well separated and embedded into different latent codes (e.g., frequency codes and reconstruction code), resulting in more accurate bonafide clustering and better detection of PAs using the designed spoofed scores. The effectiveness of our method is proved by comprehensive experiments carried out on OCT-based fingerprint dataset.