E-mail: jig@aircas.ac.cn
Website: www.cjig.cn
Tel: 010-58887035
中国图象图形学报
JOURNAL OF IMAGE AND GRAPHICS

中图法分类号:TP391.4　　**文献标识码**:A　　**文章编号**:1006-8961(2024)09-2780-13

论文引用格式:Yuan C S, Xu Z Y, Xiang L Y, Fu Z J and Xia Z H. 2024. High-generalization spoofing fingerprint detection based on commonality feature learning. Journal of Image and Graphics, 29(09):2780-2792(袁程胜, 徐震宇, 向凌云, 付章杰, 夏志华. 2024. 共性特征学习的高泛化伪造指纹检测. 中国图象图形学报, 29(09):2780-2792)[DOI:10.11834/jig.230638]

共性特征学习的高泛化伪造指纹检测

袁程胜[1,2*],徐震宇[1,2],向凌云[3],付章杰[1,2],夏志华[4]

1. 南京信息工程大学计算机学院、网络空间安全学院,南京　210044; 2. 南京信息工程大学数字取证教育部工程研究中心,南京　210044; 3. 长沙理工大学计算机与通信工程学院,长沙　410114; 4. 暨南大学网络空间安全学院,广州　510632

摘　要:**目的**　指纹识别技术已大规模应用于人们的日常生活中,如身份鉴定、指纹支付与考勤等。然而,最新研究表明这些系统极易遭受伪造指纹的欺骗攻击,因此在使用指纹认证用户身份前,鉴别待测指纹的真伪至关重要。伪造指纹的制作材料具有多样性,现有工作忽视了不同材料伪造指纹之间数据分布的关联性,致使跨材料检测泛化性普遍较低。因此,本文通过分析不同材料伪造指纹数据间的分布关联性,挖掘不同伪造指纹间的材料域不变伪造特征,提出了一种基于共性特征学习的高泛化伪造指纹检测方法。**方法**　首先,为了表征和学习不同材料伪造指纹间的特征,设计了一种多尺度伪造特征提取器(multi-scale spoofing feature extractor, MSFE),包含一个多尺度空间通道(multi-scale spatial-channel, MSC)注意力模块,以学习真假指纹类间的细粒度差异特征。然后,为了进一步分析不同材料伪造指纹数据间的分布关联性,又构造了一种共性伪造特征提取器(common spoofing feature extractor, CSFE),在MSFE先验知识的引导下进行多任务的材料域不变伪造特征学习。最后,设计一个材料鉴别器对学习到的共性伪造特征进行约束,同时构建一个自适应联合优化损失模块来平衡多个模块在训练过程中的损失权重,以进一步提高面对未知材料伪造指纹检测时的泛化性。**结果**　在两个公开的指纹数据集(LivDet(liveness detection competition)2017和LivDet2019)上进行了跨材料测试,实验结果表明所提算法相较对比工作,ACE(average classification error)降低了1.34%,TDR(true detection rate)提高了1.43%,表现出较高的泛化性。**结论**　本文算法在ACE和TDR方面均取得优异性能。此外,当面对未知材料的伪造指纹检测时,同样表现出较强的泛化性。

关键词:伪造指纹检测;材料域不变伪造特征;注意力;共性特征学习;泛化性

High-generalization spoofing fingerprint detection based on commonality feature learning

Yuan Chengsheng[1,2*], Xu Zhenyu[1,2], Xiang Lingyun[3], Fu Zhangjie[1,2], Xia Zhihua[4]

1. School of Computer Science, School of Cyber Science and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China; 2. Engineering Research Center of Digital Forensics of Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, China; 3. College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China; 4. College of Cyber Security, Jinan University, Guangzhou 510632, China

Abstract: **Objective** The realm of our daily lives has witnessed the ubiquitous integration of fingerprint recognition tech-

收稿日期:2023-09-12;**修回日期**:2024-01-04;**预印本日期**:2024-01-11

*通信作者:袁程胜　ycs_nuist@163.com

基金项目:国家自然科学基金项目(62102189,62122032);江苏省自然科学基金项目(BK20200807);国家社会科学基金项目(2022-SKJJ-C-082);国防科技大学科研项目(JS21-4,ZK21-43)

Supported by: National Natural Science Foundation of China (62102189,62122032); Natural Science Foundation of Jiangsu Province, China(BK20200807); National Social Science Fund of China(2022-SKJJ-C-082); National University of Defense Technologyy (NUDT) Scientific Research Program(JS21-4,ZK21-43)

nology in domains, such as authorized identification, fingerprint-based payments, and access control systems. However, recent studies have revealed the vulnerability of these systems to spoofing fingerprint attacks. Attackers can deceive authentication systems by imitating fingerprints using artificial materials. Thus, the authenticity of fingerprint under scrutiny must be ascertained prior to its use to authenticate the user's identity. The development of a spoofing fingerprint detection technology has attracted extensive attention from the academia and industry. The creation of spoofing fingerprints involve the use of diverse materials. The present research disregards the correlation of data distribution among spoofing fingerprints crafted from various materials, which consequently leads to limited generalization in cross-material detection. Hence, a high-generalization spoofing fingerprint detection method based on commonality feature learning is proposed through the analysis of the distribution correlation among counterfeit fingerprint data originating from diverse materials and the exploration of invariant forgery features within the material domain of distinct counterfeit fingerprints. **Method** First, to characterize and learn the features of spoofing fingerprints obtained using various materials, a multiscale spoofing feature extractor (MFSE) is designed, and it includes a multiscale spatial-channel attention module to allow the MFSE to pay more attention to fine-grained differences between live and fake fingerprints and improve the capability of the network to learn spoofing features. Then, a common spoofing feature extractor (CSFE) is constructed for further analysis of the distribution correlation between spoofing fingerprint data of different materials and extraction of common spoofing features between spoofing fingerprints made from various materials. Under the guidance of prior knowledge on MFSE, CSFE calculates the distance of the feature distribution extracted by MFSE and CSFE in the regenerated Hilbert space through the feature distance measurement module and minimizes the maximum mean difference (MMD) of data distributions to reduce the distance between them. The multitask material domain invariant spoofing feature learning is implemented, and a material discriminator is designed to constrain the learned common spoofing features and remove specific material information from the spoofing fingerprint. CSFE involves the calculation of multiple loss functions. Manually setting the weight ratio of these loss functions may prevent the improvement of model performance. Therefore, an adaptive joint-optimization loss function is used to balance the loss values of each module and further expand the generalization capability of the network in the presence of unknown material spoofing fingerprints. The training process involves the use of a fingerprint image containing two kinds of labels, which include the authenticity label of the fingerprint and material label of the forged fingerprint. The true fingerprint lacks material properties and is marked as 0. Forged fingerprints are numbered from 1 based on the material category, and the authenticity of fingerprints and type of forged materials are assessed based on the authenticity and material labels, respectively. The random gradient descent method is used for optimization, and the learning rate setting is from 0.001, which is reduced by 0.1 time per 10 epoch. **Result** The experimental results on two public datasets revealed that the algorithm proposed in this paper achieved the best comprehensive performance in the cross-material detection of forged fingerprints. On the GreenBit sensor of LivDet2017 dataset, average classification error (ACE) reduced the rate by 0.16% compared with the second-ranked spoofing fingerprint detection model and increased true detection rate (TDR) by 2.4%. On the Digital persona sensor of LivDet2017 dataset, ACE reduced the rate by 0.26% compared with the second-ranked forgery fingerprint detection model and increased TDR by 0.7%. On LivDet2019 dataset, ACE reduces the rate by 1.34% on average compared with the second-ranked spoofing fingerprint detection model and increases TDR by 1.43% on average. These findings indicate a an increase in the corresponding generalization. A comparative experiment was performed to verify the superiority of the multi-scale spatial-channel (MSC) attention module to the convolutional block attention module (CBAM) module in spoofing fingerprint detection. To better evaluate our method, we conducted a series of ablation experiments to verify each module involved in common feature extraction training to aid in the cross-material spoofing fingerprint detection task. To reveal the improved generalization performance of CSFE compared with MFSE in cross-material spoofing fingerprint detection, this paper visualized the distribution of the proposed features using the t-distributed stochastic neighbor embedding algorithm. **Conclusion** The method proposed in this paper achieved better detection results than other methods and exhibited a higher generalization performance in the detection of spoofing fingerprints made of unknown materials. Compared with spoofing fingerprint detection using the same material, the extant spoofing fingerprint detection technique harbors substantial scope for the refinement of its generalization capabilities for cross-material detection. Cross-material spoofing fingerprint detection aptly aligns with practical requirements and bears immense importance in the realm of

research pursuits.

Key words: spoofing fingerprint detection; material domain invariant spoofing feature; attention; commonality feature learning; generalization

0 引 言

随着大数据和区块链技术的高速发展,互联网上每天都会产生海量的数据,如何对其中的涉密数据进行保护和安全使用越来越重要,生物特征识别技术作为一种高效的身份认证手段,广泛用于各种身份认证领域,其中,指纹因其稳定性、唯一性、持久性和便捷性的特性,成为当下生物特征识别研究的热点(Valdes-Ramirez等,2019;Yang等,2019;王任颖等,2022)。但是,新近研究显示,指纹识别系统存在严重的安全隐患,极易遭受伪造指纹的欺骗攻击(Karampidis等,2021;孙哲南 等,2021)。为了提高指纹识别系统的安全和可信,精准鉴别待认证指纹的真伪,成为当下工业界和学术界的研究热点。

伪造指纹检测技术的提出,为抵御欺骗攻击提供了一种强有力的防御手段。该技术旨在提高指纹识别系统的安全,即在身份认证前先判断待认证指纹的真伪,只有判定为真指纹的用户才能进行后续的认证与授权,从而更好地保障涉密数据的安全和完整(Shaheed等,2021)。深度学习在众多领域均取得极佳性能,研究人员也将其应用到伪造指纹检测任务中,通过改进和优化模型框架来提高伪造指纹检测任务的性能,是目前研究的热点(Chiroma,2021;Zeng等,2019)。现有的伪造指纹制作方法是使用一些特殊材料,通过手工的方式仿制指纹,难以制作和构建海量的伪造指纹图像库,因此在模型训练中可用的伪造指纹有限,当面对已知材料伪造的假指纹时检测性能较高,但是面对未知材料伪造的假指纹时检测性能会大幅下降,泛化性较差(甘俊英 等,2019)。此外,现有工作大多通过构建特定模块或优化网络来自动学习真假指纹间的样本特征,未考虑不同材料伪造指纹时的数据分布关联性问题,检测未知材料仿制的指纹时精度较低。为此,本文提出了一种基于共性特征学习的高泛化伪造指纹检测方法,通过探索不同材料伪造指纹数据的分布关联性,设计一种自适应联合优化损失模块来提取未知材料伪造指纹数据间的共性特征,以提升检测模型的泛化性。

本文主要贡献如下:1)提出一种多尺度伪造特征提取器(multi-scale spoofing feature extractor,MSFE),以表征和学习不同材料伪造指纹间的脊线不连续程度、汗孔汗渍频率等伪造特征。此外,设计了一个多尺度空间通道(multi-scale spatial-channel,MSC)注意力模块,使MSFE更加聚焦真假指纹类间的细粒度差异,提升模型学习伪造特征的能力。2)提出一种共性伪造特征提取器(common spoofing feature extractor, CSFE),在MSFE先验知识的引导下提取不同材料伪造指纹间共同的伪造特征。同时,构建一个特征距离度量模块,通过计算两个数据分布间的最大均值差异(maximum mean discrepancy,MMD)以学习多任务的材料域不变伪造特征;紧接着又设计一个材料鉴别器对学习到的共性伪造特征进行约束,以剔除伪造指纹中的特定材料信息。3)本文在两个公开的指纹数据集LivDet(liveness detection competation)2017和LivDet2019上进行了测试。实验结果表明,所提方法相较于对比方法取得了更佳的泛化性能。

1 相关工作

现有检测方法主要分为基于硬件式和基于软件式两类。前者需要在特定硬件设备的支持下,通过筛查人体的生理信号实现指纹的真伪鉴别,致使其检测成本较高,且不利于后期维护。为此,基于软件式的方法应运而生。通过对现有工作梳理后发现,基于软件式的方法又可划分成3类:基于启发式的方法、基于纹理特征的方法和基于深度学习的方法。

1)基于启发式。指纹脊线上有序排列着大量的汗孔,假指纹很难仿制,可作为指纹真伪鉴别的依据(Maltoni等,2022)。Nguyen和Jain(2019)提出一种基于端到端的指纹孔提取和匹配模型,通过汗孔定位提取完成真伪鉴别,但任务性能不高。紧接着,Barhoumi等人(2021)提出一种高精度的指纹孔提取和匹配算法,但是该方法只适用于高分辨率的指纹图像,对于分辨率较低的指纹图像性能一般。一方

面，基于启发式的检测方法均需依赖图像质量；另一方面，目前的人工智能（artificial intelligence，AI）合成技术已经能生成带有汗孔的指纹，该类检测方法面临巨大的挑战。

2）基于纹理特征。受制造工艺的制约，在制作伪造指纹过程中会掺杂一些杂质，伪造指纹的图像质量较差（Ametefe 等，2022）。为此，Sharma 和 Dey（2019）通过分析真假指纹图像的质量，从多个角度对指纹的脊线和谷线质量进行评估，鉴于不同材料仿制的假指纹图像质量存在差异性，致使该方法的泛化性一般。Xia 等人（2017）对指纹纹理进行挖掘，通过构建二阶和三阶共生矩阵来计算像素梯度的特征值，显著提升了任务性能。Zhang 等人（2014）将小波处理应用于指纹鉴伪中，提出一种融合小波和局部二值模式优化的方法，通过统计局部二值模式的直方图，更好地挖掘差异性信息。基于纹理特征的方法对指纹图像质量也有一定的要求，不同材料制成假指纹呈现出的图像质量参差不齐，实现强泛化性的检测同样面临挑战。

3）基于深度学习。卷积神经网络作为深度学习的代表性算法之一，能够从给定的样本中自动学习高阶的语义特征，如图像纹理、形状和拓扑结构等（Abrishambaf 等，2008）。Khade 等人（2018）提出一种基于特征融合的伪造指纹检测方法。该方法从多个方向计算指纹脊线频率以构建空间域特征，使用正交变换域在指纹上提取变换域特征，将变换域和空间域特征融合作为最终的样本特征，并进行后续的模型训练和性能测试，该方法可以在一定程度上提高跨材料伪造指纹检测性能，但提升幅度有限。Anusha 等人（2020）提出了一种基于端到端的伪造指纹检测方法。首先将指纹图像切分成无重叠的补丁，然后利用所提网络学习每个局部补丁的特征，以便更好地表征真假指纹的差异。为了解决局部最优的问题，Yuan 等人（2022）通过对经典的残差神经网络进行优化和改进，设计一种自适应学习模块和指纹纹理增强模块。同时提出一种基于自适应残差神经网络的伪造指纹算法，显著提高了模型的泛化能力。Liu 等人（2022）提出了一种逐通道特征去噪和自适应损失方法，通过削弱“噪声”通道的影响来提高模型对差异性特征的学习。此外，还设计了一个自适应损失来约束特征分布，取得了较好的检测效果。

事实上，上述方法在伪造指纹检测上均能表现出良好的泛化性，但是它们都采用数据驱动方法，即直接学习指纹数据的特征，并未挖掘不同材料下伪造指纹的共同特征，使其在面对未知材料执行跨材料检测任务时性能普遍不佳。

2 基础知识

本节首先给出域不变特征的定义，然后详细介绍注意力机制的相关概念。

2.1 域不变特征

一般而言，每个领域的数据都会呈现出不同的风格，包括该领域独有的个性特征和与其他领域通用的共性特征。由于个性特征表现为本领域数据的独有风格，会干扰其他领域数据的聚类，而共性特征兼容不同领域数据的风格，对其他领域数据聚类起到引导作用，因此挖掘不同领域的共性特征，对提高任务的泛化性极其关键。上述共性特征也称为域不变特征（Li 等，2018）。

在伪造指纹检测研究中，基于深度学习的跨材料伪造指纹检测性能普遍不高。究其原因是不同材料仿制的指纹呈现不同的数据分布，即不同类伪造指纹的特征聚类中心不一。然而，现有的研究表明，不同材料仿制的指纹上一般会呈现相似的伪造痕迹，具体表现为脊线的连续性差、脊谷线间隔不均匀、指纹汗孔难以仿制等问题，上述伪造痕迹称为材料域共性特征，即使未知材料仿制的伪造指纹同样具有这些信息，因而提取该伪造特征对于提高模型面对未知材料仿制指纹检测的泛化性至关重要。

不同材料的指纹特征聚类分布图情况如图 1 所示，其中圆圈表示真指纹的特征分布，三角形和正方形分别为两种不同材料伪造指纹的特征分布，六边形为未知材料伪造指纹的特征分布。红圈内为借助深度学习在已知材料数据集上学习的伪造特征分布，但在检测未知材料伪造指纹时部分指纹无法被正确分类。通过学习不同材料伪造指纹之间共性特征，即材料域不变伪造特征，并将其作为真伪鉴别的依据，能够提高伪造指纹检测的泛化性。

2.2 注意力机制

伪造指纹检测是一种典型的二分类任务，即通过学习真假指纹的差异性特征来鉴别指纹真伪。注意力机制通过聚焦图像感兴趣区域，忽略其他次要

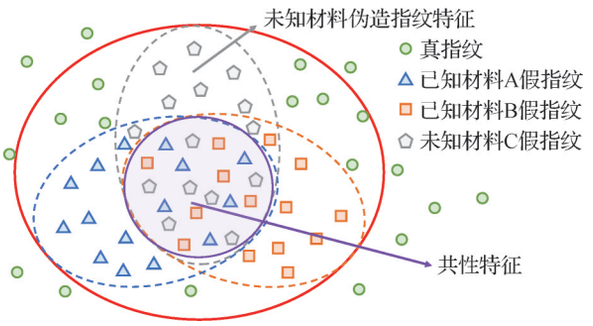

图1　不同指纹特征的聚类分布图

Fig. 1　Distribution map of fingerprint characteristics

区域来提高模型的特征学习能力(Hu等人,2022;Lu等人,2021;Wang等人,2021)。有关卷积注意模块(convolutional block attention module,CBAM)(Woo等,2018)中的通道注意力和空间注意力详细介绍如下。

1)空间注意力机制。主要目标是寻找指纹中与真伪鉴别强相关的区域,计算为

$$M_s(\boldsymbol{x})=\sigma(f^{(7\times7)}([AvgPl(\boldsymbol{x});MaxPl(\boldsymbol{x})])) \tag{1}$$

式中,$\boldsymbol{x}$为输入特征图,$f^{7\times7}$表示卷积核大小为7×7的卷积层,σ表示非线性激活函数ReLU。

2)通道注意力机制。主要用于评估特征图的不同通道对当前任务的重要性,计算为

$$M_c(\boldsymbol{x})=\sigma(MLP(AvgPl(\boldsymbol{x}))+MLP(MaxPl(\boldsymbol{x}))) \tag{2}$$

式中,$\boldsymbol{x}$为输入特征图,MLP为多层感知机,σ表示非线性激活函数ReLU,平均池化层$AvgPl$和最大池化层$MaxPl$共享同一个MLP。

3　本文方法

本文所提检测方法的实现流程如图2所示,主要包含两个步骤:1)提取不同材料伪造指纹各自的伪造特征;2)从多种材料伪造指纹的伪造特征中学习共同特征。

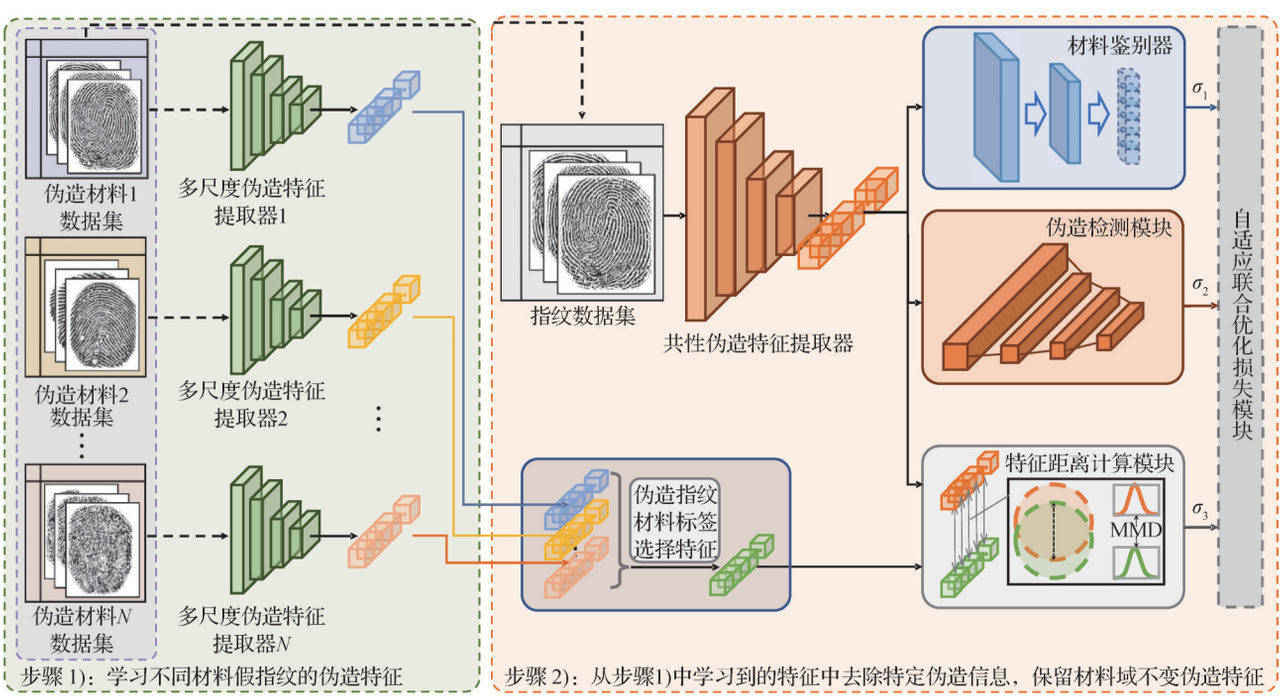

图2　本文算法的具体实现步骤

Fig. 2　The specific implementation steps of the proposed algorithm

3.1　多尺度伪造特征提取模块

为了分析和挖掘真假指纹中的细粒度差异特征,设计了一个多尺度伪造特征提取器(MSFE),如图3所示。与自然图像分类任务相比,真假指纹图像间的相似性更高、类间差异更难表示,是一项极具挑战的细粒度图像分类任务。为了解决因模型层数增加而引发的梯度消失或爆炸问题,本文采用ResNet(residual network)网络作为主干网络。鉴于残差块中的多层卷积操作易使得部分细粒度信息丢失,无法全面表征图像中的细粒度差异,为此,又设计了一个多尺度空间通道(MSC)注意力模块以学习真假指纹的多尺度细粒度信息,即在残差模块的每个卷积层后引入一个空间注意力层M_s,然后再将其与特征图进行融合,确保学习特征的完整性。最后,

为了权衡多特征通道的重要性，添加了一个通道注意力层M_c，通过自适应的权重分配，进一步提升模型学习伪造特征的能力。注意力模块计算为

$$\boldsymbol{F}_{\mathrm{R}}(x)=W_1(\boldsymbol{F})+W_2(\boldsymbol{F}')+W_3(\boldsymbol{F}'')+\boldsymbol{F}_{\mathrm{s}}+M_{\mathrm{c}}(\boldsymbol{F}_{\mathrm{s}})$$
$$\boldsymbol{F}_{\mathrm{s}}=M_{\mathrm{s}}(\boldsymbol{F})+M_{\mathrm{s}}(\boldsymbol{F}')+M_{\mathrm{s}}(\boldsymbol{F}'') \quad (3)$$

式中，$\boldsymbol{F}_{\mathrm{R}}$为残差模块的特征输出，$W_1$，$W_2$，$W_3$分别表示 3 个不同卷积层的权重，$\boldsymbol{F}$，$\boldsymbol{F}'$，$\boldsymbol{F}''$分别为上述 3 个卷积层提取的特征，$\boldsymbol{F}_{\mathrm{s}}$为 3 层空间注意力特征权重图融合得到的特征图，$M_{\mathrm{s}}$是空间注意力层，$M_{\mathrm{c}}$是通道注意力层。已有工作（Abdullahi 等，2022）指出直接对图像进行卷积运算易使部分关键信息丢失，为此在卷积运算前首先对图像进行分块，将指纹图像块输入 MSC 注意力模块获得相应的注意力权重图，然后再与原指纹图像进行加权融合，以提出指纹图像中脊线、汗渍等细微伪造差异，进一步提升 MSFE 对特定伪造特征的学习能力。该模块由 4 个全连接层组成，并采用 dropout 策略进行剪枝，使用二元交叉熵损失函数计算伪造分类损失L_{sfcls}，具体为

$$L_{\mathrm{sfcls}}=-[\boldsymbol{x}\log\hat{\boldsymbol{x}}+(1-\boldsymbol{x})\log(1-\hat{\boldsymbol{x}})] \quad (4)$$

式中，$\boldsymbol{x}$为指纹样本的标签，$\hat{\boldsymbol{x}}$为多尺度伪造特征提取器对指纹样本图像的预测输出。对于同材料伪造指纹，MSFE 能够很好地学习到伪造特征，并使用该特征进行指纹真伪鉴别。

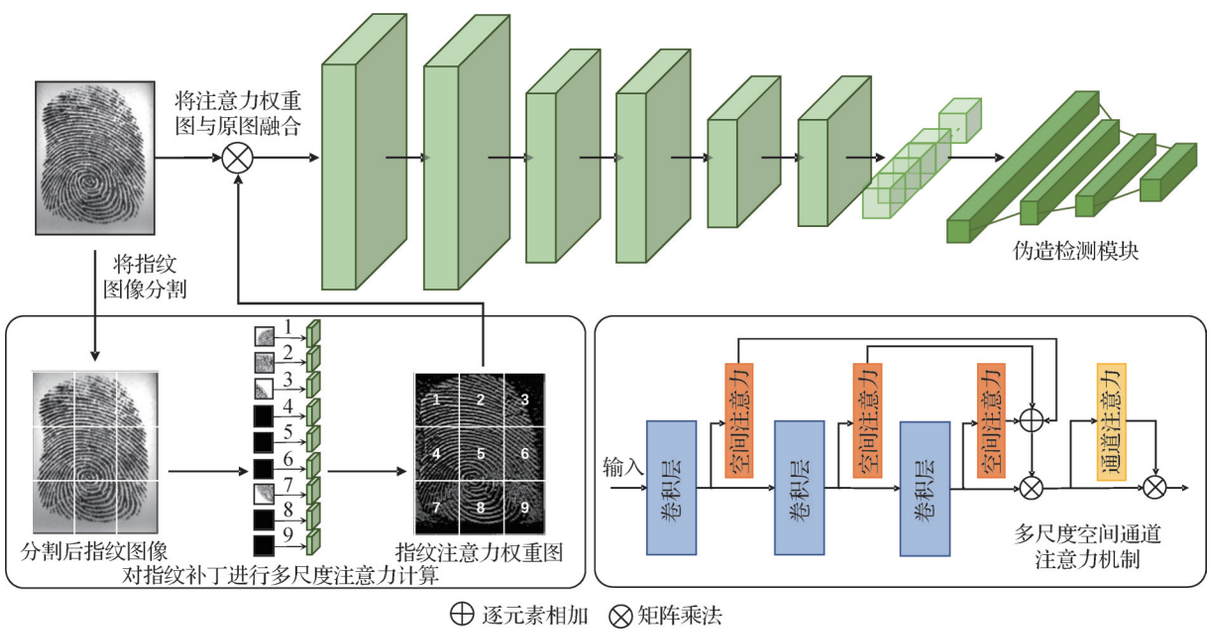

图 3　多尺度伪造特征提取器

Fig. 3　Multi-scale spoofing feature extractor

3.2　共性伪造特征提取

MSFE 是针对特定材料伪造指纹的表征学习而设计的特征提取器，其在检测伪造指纹时虽然能够取得不错的效果，但是当训练数据集有限时，易出现过拟合问题，在面对未知材料检测任务时泛化性一般。本文在研究中发现，模型学习的伪造特征中具有一部分特定的伪造特征，使得 MSFE 在进行跨材料伪造指纹检测时的性能急剧下降。多种材料伪造指纹之间存在一些共同的伪造特征，能够将部分跨材料伪造指纹样本进行正确分类。因此，本文又设计了一个共性伪造特征提取器 CSFE，其骨干网络仍采用 ResNet，CSFE 是指在 MSFE 先验知识的引导下，利用特征距离度量模块进行多任务的材料域不变伪造特征的学习，如图 4 所示，该网络由 5 个部分组成，即共性伪造特征提取器、训练完毕的多尺度伪造特征提取器、特征距离计算模块、材料鉴别器和伪造指纹分类模块，其中，σ_1，σ_2，σ_3分别为 3 个模块的损失值所对应的权重参数。其中材料鉴别器、特征距离计算模块和伪造分类模块主要用于计算相应的损失以协助 CSFE 的训练，训练过程中 MSFE 的网络参数并不会动态更新。

1）特征距离度量模块。伪造指纹检测是一个二元分类任务，涉及两类标签，分别为指纹的真伪标签及材料类别标签。鉴于真指纹无材料属性，将其标注为 0，对于仿制指纹的材料类别则按编号进行标注。在使用 CSFE 提取伪造特征的同时，一并将该伪

造指纹输入到MSFE中进行特征提取。为了使CSFE学习到真假指纹的细粒度差异特征，还引入一个特征距离计算模块，即最大均值差异(MMD)距离(贾修一 等，2021)，利用再生希尔伯特空间($\boldsymbol{H}$)中CSFE和MSFE，对同一假指纹所提取的特征分布进行度量。本文将CSFE提取到的伪造特征作为源域($\boldsymbol{S}$)，将MSFE提取到的特征作为目标域($\boldsymbol{T}$)，通过对抗博弈，最小化两者最大均值差异来拉进两者的距离，源域与目标域之间的最大均值差异为

$$D_{\mathrm{mmd}}(\boldsymbol{S},\boldsymbol{T})=\left\|\frac{1}{n}\sum_{i=1}^{n}\phi(\boldsymbol{S}_i)-\frac{1}{m}\sum_{j=1}^{m}\phi(\boldsymbol{T}_j)\right\|_{\mathrm{H}}^{2} \tag{5}$$

式中，$\boldsymbol{S}$，$\boldsymbol{T}$分别表示两个不同的特征分布，$\phi(x)$为映射函数，对每一样本进行映射投影计算并求和，和差大小即表示两个特征分布的距离。特征距离损失函数L_{mmd}的计算式为

$$L_{\mathrm{mmd}}=\frac{1}{N}\sum_{i=1}^{N}D_{\mathrm{mmd}}(\boldsymbol{F}_S(\boldsymbol{X}_i),\boldsymbol{F}_T(\boldsymbol{X}_i)) \tag{6}$$

式中，$\boldsymbol{F}_S(\boldsymbol{x})$和$\boldsymbol{F}_T(\boldsymbol{x})$分别为CSFE和MSFE提取的特征集，$\boldsymbol{X}$为指纹样本，$N$为样本的数量，利用最大均值差异距离度量函数$D_{\mathrm{mmd}}$来计算两者的距离。

2)伪造材料鉴别器。在特征距离计算模块的约束下，CSFE可以学习不同材料仿制指纹的伪造特征。由于仍可能掺杂部分特定伪造信息，为了剔除特定伪造特征保留共性特征，又设计一个伪造材料鉴别器，通过引入域对抗网络的思想对共性伪造特征进行学习。伪造材料鉴别器是一个训练好的多分类器，将CSFE(G)提取到的伪造特征输入到材料鉴别器(D)中进行对抗博弈，直至材料鉴别器无法依据该特征判断伪造材料类型，表明CSFE提取的特定伪造信息被剔除。伪造材料判别损失L_{mdisc}的计算式为

$$L_{\mathrm{mdisc}}=-\frac{1}{M}\sum_{i=1}^{M}l_i\times\log(1-D(G(\boldsymbol{X}_i))) \tag{7}$$

式中，$\boldsymbol{X}_i$表示伪造指纹样本，l_i为样本的材料类别，M为样本材料类别的种类。通过材料鉴别器的对抗训练可剔除掉CSFE提取的特定伪造信息。

3)伪造检测模块。利用CSFE学习共性特征的同时，还需要兼顾真假指纹鉴别的任务性能，为此又设置一个伪造指纹检测模块，主要由全连接层组成，使用dropout策略进行剪枝，采用二元交叉熵损失函数计算伪造指纹的分类损失L_{cfcls}，计算式为

$$L_{\mathrm{cfcls}}=-[\boldsymbol{y}\log\hat{\boldsymbol{y}}+(1-\boldsymbol{y})\log(1-\hat{\boldsymbol{y}})] \tag{8}$$

式中，$\boldsymbol{y}$为指纹样本的真实标签，$\hat{\boldsymbol{y}}$为指纹样本做出推理的预测值。

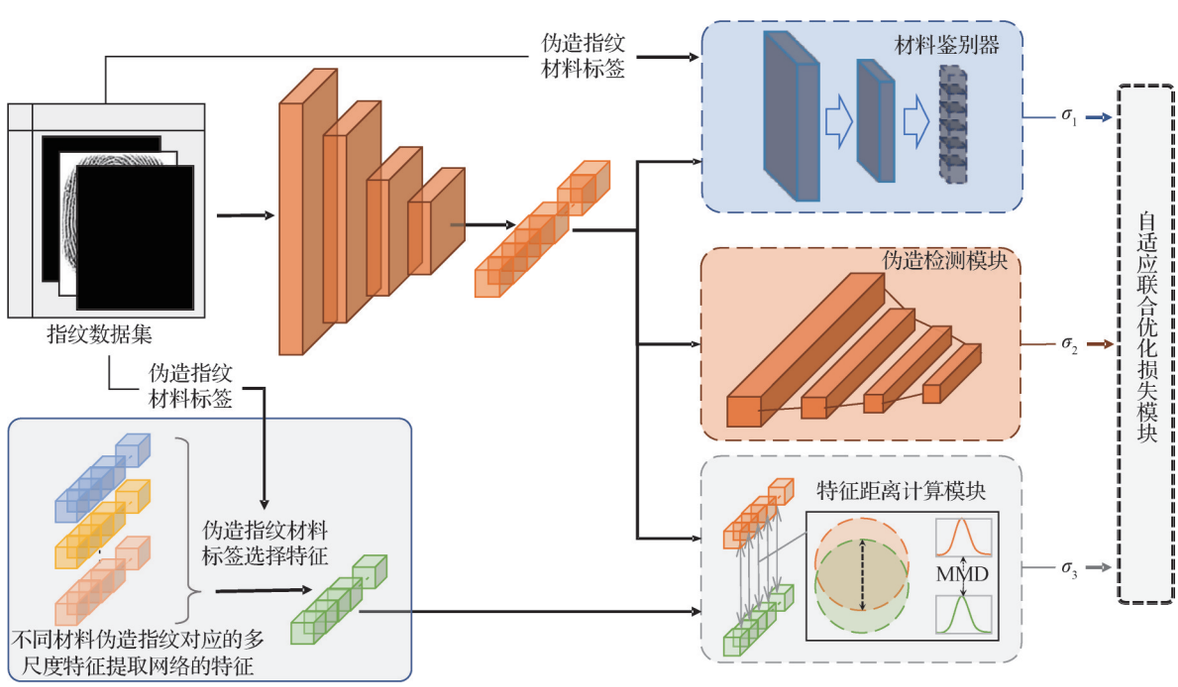

图4　共性伪造特征提取器

Fig. 4　Common spoofing feature extractor

3.3　自适应联合优化损失函数

CSFE包含多个损失函数项，分别为特征距离损失、伪造材料鉴别损失以及伪造检测损失。鉴于手动设置上述损失函数的权重无法权衡子项的最优，

致使模型无法收敛到全局最优。因此采用Kendall提出(Cipolla等,2018)的自适应权重学习方法,自适应损失函数L的计算式为

$$L=\frac{L_{\mathrm{mmd}}}{2\sigma_1^2}+\frac{L_{\mathrm{mdisc}}}{2\sigma_2^2}+\frac{L_{\mathrm{cfcls}}}{2\sigma_3^2}+\log(\sigma_1\sigma_2\sigma_3) \tag{9}$$

式中,σ_1,σ_2,σ_3分别为3个损失对应的权重系数,通过模型参数的训练,实现各个损失函数项权重的动态调整。

4 实验分析

本节首先介绍实验中使用的指纹图像集,然后给出相应的性能评价指标,接着列出对应的实验配置,最后给出实验结果并对其进行讨论分析。

4.1 数据集

为了验证本文所提方案的性能,在两个公开的指纹数据集上进行实验,分别为LivDet2017和LivDet2019(Mura等,2018;Orrù等,2019)。两个数据集均采用3个传感器,通过对不同性别和年龄的志愿者进行采样,详细信息如表1所示。

LivDet2017和LivDet2019两个指纹数据集来自2017年和2019年举行的指纹活性检测竞赛,是为了便于不同算法间的性能对比而发布的两个指纹数据集,分别包含17 000幅指纹图像和12 000幅指纹图像。两个数据集均由GreenBit、Orcathus和DigitalPersona 3个不同的传感器采样得到。其中GreenBit和DigitalPersona采集的是2D图像,Orcathus采集的是2.5D图像。

表1 实验数据集LivDet2017和LivDet2019的详细信息

Table 1 Details of the experimental datasets LivDet2017 and LivDet2019

数据集	传感器(类型)	图像/幅		训练集伪造材料	测试集伪造材料
		训练集(真/假)	测试集(真/假)		
LivDet2017	GreenBit(光学)	1 000/1 200	1 700/2 040	Wood Glue, Exoflex, Body Double	Gelatin, Liquid Ecoflex, Latex
	DigitalPersona(光学)	999/1 199	1 700/2 028		
	Orcanthus(热擦除)	1 000/1 200	1 700/2 018		
LivDet2019	GreenBit(光学)	1 000/1 000	1 020/1 224	Wood Glue, Exoflex, Body Double, Gelatin,	Liquid Ecoflex, Latex, Mix
	DigitalPersona(光学)	1 000/1 200	990/1 088		
	Orcanthus(热擦除)	1 000/1 200	1 019/1 224		

4.2 性能评价指标及基准模型

为了比较不同算法的性能,仍沿用LivDet2017和LivDet2019竞赛官网提供的评价指标。鉴于DeFraudNet(Anusha等,2020)和CFD-PAD(Liu等,2022)两个方法的出色表现,作者还开源了相关源码。本文对其进行复现,并与所提方法进行对比。此外,还采用了多个经典的评估指标进行方法比对,如准确率(accuracy,Acc)、平均分类错误率(average classification error,ACE)、真实检测率(true detection rate,TDR),其中真实检测率表示伪造指纹被正确区分的占比。平均分类错误率的计算依赖于攻击呈现分类错误率(attack presentation classification error rate,APCER)和真实呈现分类错误率(bona fide presentation classification error rate, BPCER),其中APCER为伪造指纹被错误分类为真指纹的比例,BPCER表示真指纹被错误分类成伪造指纹的比例。ACE值越小,则对应的算法性能越好。具体为

$$f_{\mathrm{APCER}}=\frac{FP}{TN+FP} \tag{10}$$

$$f_{\mathrm{BPCER}}=\frac{FN}{TP+FN} \tag{11}$$

$$f_{\mathrm{ACE}}=\frac{f_{\mathrm{APCER}}+f_{\mathrm{BPCER}}}{2} \tag{12}$$

4.3 实验环境和参数设置

在验证过程中,实验设备的操作系统为Win-10,处理器型号为Intel Core i7-10700,显卡型号为Nvidia RTX 2070,计算机运行内存大小为16 GB。在训练过程中,采用随机梯度下降法进行优化,学习率从0.000 1开始,每隔10轮epoch下降为之前的1/10。

4.4 实验结果与分析

本文采用ResNet作为骨干网,为了验证模型层

数是否影响任务性能，在ResNet 18 、ResNet 50和ResNet 101共3个模型上进行了测试。实验结果如表2所示，虽然随着层数的增加，性能会有所提升，大约为0.24%，但是在时间推理和模型参数量方面，ResNet 101是ResNet 18的4倍。因此，从实际应用方面，模型层数的增加不仅无法显著提升检测性能，还会造成计算开销和存储资源的激增，不利于方案的落地和推广。为此，本文后续实验采用ResNet18作为骨干网。

本文所提框架涉及多个模块，为了验证不同模块组合对检测结果的影响，进行了消融实验，实验结果如表3所示。其中伪造鉴别模块是伪造指纹检测任务必不可少的部分，因此主要验证特征距离计算模块和材料鉴别模块对共性伪造特征提取网络跨材料性能的影响。因为特征距离计算模块可使3个传感器的平均结果ACE从5.52%下降到3.76%，TDR从76.98%增加到89.22%，表明在不同材料对应MSFE的监督下，多任务协同训练能够学习到伪造指纹的共性特征。紧接着，引入材料鉴别器后，可使3个传感器的平均ACE从3.76%下降到2.60%，TDR从89.22%增加到93.54%。实验结果表明，材料鉴别器能够剔除不同材料伪造指纹的特定伪造信息并保留共性伪造特征，最终提高跨材料检测任务的泛化性。

表2　不同网络层数下的性能比较

Table 2　Comparison between different network layers

主干网络层数	Acc/%				Flops/GMac	参数/M
	DigitalPersona	GreenBit	Orcathus	平均		
101	95.13	95.71	93.62	**94.82**	8.95	47.30
50	95.02	95.98	93.21	94.73	4.67	26.06
18	94.74	95.41	93.59	94.58	**2.67**	**15.36**

注：加粗字体表示各列最优结果。

表3　共性伪造特征提取器训练过程中各个模块的消融实验

Table 3　The ablation experiments of each module in the training process of common feature extractor

/%

模块设置			GreenBit		DigitalPersona		Orcathus	
伪造鉴别模块	特征距离模块	材料鉴别器	ACE	TDR	ACE	TDR	ACE	TDR
√	–	–	5.86	79.25	5.93	74.32	4.79	77.37
√	√	–	3.66	91.63	3.79	88.76	3.84	87.28
√	√	√	**2.28**	**94.72**	**2.43**	**93.92**	**3.10**	**91.99**

注：加粗字体表示各列最优结果，“√”表示使用该模块，“–”表示未使用。

针对CBAM存在的细微伪造特征丢失问题，提出了一个适用于伪造指纹检测任务的MSC注意力模块。相较于CBAM模块，所提的MSC注意力模块能够保留指纹图像中脊线、汗渍等细粒度伪造差异。如图5所示，3个传感器的平均结果ACC从95.70%增加到99.23%。与DeFrauNet和CFD-PAD两个方法对比后发现，本文算法当面对同材料伪造指纹检测任务时，同样表现出极佳的性能，具体如表4。在LivDet2017数据集上，所提方法在3个传感器的TDR均值为99.45%，明显优于Banerjee和Liu两个方法；在LivDet2019指纹数据集上，所提方法在

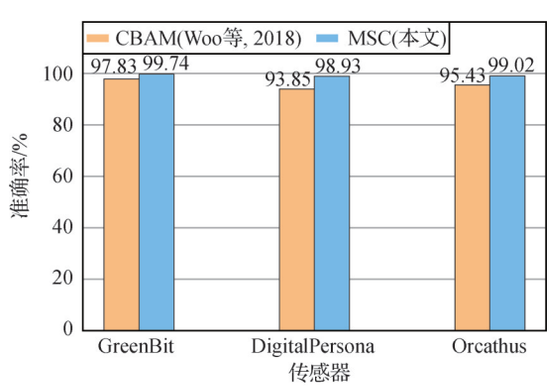

图5　多尺度伪造特征提取器中注意力模块的对比实验

Fig. 5　Comparative experiment of attention module in multi-scale spoofing feature extractor

3个传感器的TDR均值为99.49%，较CFD-PAD增加了0.42%，相较于DeFraudNet有0.08%的提升。

此外，从表4的同传感器同材料实验结果还可观察到，现有工作在进行同传感器（或同材料）的检测任务时，均能够取得无限逼近100%的极佳性能。但是在实际应用中，0.2%的细微误差对实际检测任务基本上可忽略不计，而在面对未知材料伪造指纹的检测方面，泛化性普遍不佳。因此，解决和提高面对未知材料伪造指纹检测的泛化性问题是本文首要解决的难题。

表4　所提方法在LivDet2017和LivDet2019上的检测性能（TDR）比较

Table 4　Comparison of detection performance (TDR) of our method with the same sensor and the same material on LivDet2017 and LivDet2019

/%

数据集	LivDet2017			LivDet2019		
	GreenBit	DigitalPersona	Orcanthus	GreenBit	DigitalPersona	Orcanthus
DeFraudNet（Anusha等，2020）	99.67	99.14	99.04	99.42	99.26	99.56
CFD-PAD（Liu等，2022）	**99.24**	98.85	99.26	99.46	98.43	**99.33**
CSFE（本文）	99.13	**99.73**	**99.48**	**99.52**	**99.66**	99.29

注：加粗字体表示各列最优结果。

本文在LivDet2017和LivDet2019两个公开的指纹数据集上进行了跨材料伪造检测测试，实验结果如表5所示，相较于对比方法，所提方法均取得较好的检测性能，相比于CFD-PAD，ACE降低了0.16%和0.26%，TDR增加了2.4%和0.7%。在Orcathus传感器上的检测结果全面优于DeFraud-Net方法，但是与CFD-PAD方法相比，ACE表现出1.19%的差距，TDR落后了3.94%，原因为Orcathus传感器的成像原理不同，本文方法在2D图像上表现出较好的性能，但在面对Orcathus传感器所采集的2.5D图像时表现不佳，仍有提升空间。在LivDet2019指纹数据集上，所提方法在GreenBit和Digitalpersona传感器上取得的结果均领先于DeFraudNet方法，但是与CFD-PAD相比，在ACE上有0.43%的差距，TDR落后了1.95%。通过对上述实验结果分析可知，利用GreenBit和DigitalPersona两个传感器采集的指纹图像，本文算法在面对跨材料伪造指纹的检测时，较CFD-PAD，分别在ACE上降低了0.1%和3.96%，TDR增加了1.17%和5.06%。在检测Orcathus传感器所采集到的指纹数据时展现出更好的泛化性，但是在面

表5　所提方法在LivDet2017和LivDet2019上的跨材料检测性能比较

Table 5　Comparison of the performance of the proposed method on LivDet2017 and LivDet2019 with the same sensor across materials

/%

方法	LivDet2017						LivDet2019					
	GreenBit		DigitalPersona		Orcanthus		GreenBit		DigitalPersona		Orcanthus	
	ACE	TDR	ACE	TDR	ACE	TDR	ACE	TDR	ACE	TDR	ACE	TDR
FSG（Chugh等，2018）	4.84	91.07	5.35	62.29	5.62	66.59	–	–	–	–	–	–
DeFraudNet（Anusha等，2020）	3.17	90.47	3.52	87.95	5.32	86.61	3.46	89.82	4.68	85.96	5.04	85.09
FUSION（González-Soler等，2021）	4.84	–	5.35	–	5.62	–	–	–	–	–	–	–
CFD-PAD（Liu等，2022）	2.59	93.43	3.33	90.73	**1.68**	**97.32**	2.78	93.55	6.39	88.86	**2.67**	**93.94**
OPG（Rai等，2023）	5.26	–	6.36	–	3.47	–	–	–	18.45	–	2.45	–
CSFE（本文）	**2.43**	**95.83**	**3.07**	**91.43**	2.87	93.38	**2.28**	**94.72**	**2.43**	**93.92**	3.10	91.99

注：加粗字体表示各列最优结果，“–”表示作者并未进行该实验。

对 Orcathus 传感器采集的指纹图像，相较于 CFD-PAD，跨材料检测任务略有差距，究其原因为图像成像原理所致，Orcathus 传感器采集到的指纹图像是 2.5D 图像，而另外两个传感器是 2D 图像。但是从整体上看，所提方法依然取得了较好的检测性能。

最后，本文借助 T-SNE（T-distribute stochastic neighbor embedding）算法（van der Maaten 和 Hinton，2008）对多尺度伪造特征提取器和共性伪造特征提取器所提的特征分布进行了可视化。具体来说，选择 LivDet2019 中 4 种材料伪造指纹数据集各训练一个 MSFE，并将其中一个材料的指纹数据集设为测试集，使用其他 3 类材料伪造指纹对应的 MSFE，在多个 MSFE 先验知识驱动下训练共性伪造特征提取网络。图 6 展示了多尺度伪造特征提取器和共性伪造特征提取器学习到的指纹特征分布图，可清晰发现，在利用 T-SNE 算法进行特征聚类时，本文方法表现出更好的聚类效果，表明不同的多尺度伪造特征提取器在检测同材料伪造指纹时可以很好地鉴别真假指纹，但在检测其他材料伪造指纹时部分指纹无法正确区分。而共性伪造特征提取网络在其他 3 个 MSFE 的协助训练下学习共性伪造特征，在跨材料检测中依然能够很好地鉴别真假指纹，进一步说明本文所提的共性特征学习能够提高跨材料伪造指纹检测任务的性能。

5 结 论

跨材料伪造指纹检测泛化性弱严重制约了伪造指纹检测技术的推广和普及。本文通过探索和研究不同材料仿制指纹中存在的相似伪造痕迹，提出了

图 6 多尺度伪造特征和共性伪造特征的特征分布图

Fig. 6 The multi-scale spoofing feature extractor and the common feature extractor extract the fingerprint feature distribution map

一种基于共性特征学习的高泛化伪造指纹检测方法。通过构造多尺度伪造特征提取模块以表征和学习不同材料伪造指纹间的特征，接着，设计了一个多尺度空间通道模块以挖掘真假指纹类间的细粒度差异。然后，为了统计不同材料伪造指纹数据间的分布关联性，又设计了一个共性伪造特征提取CSFE模块，在MSFE先验知识的引导下进行多任务的材料域不变特征学习，并引入了一个材料鉴别器来约束共性特征，以挖掘不同材料伪造指纹脊线不连续、无汗孔汗渍等共同的伪造特征。最后，在两个公开的指纹数据集上进行了大量实验，实验结果表明，本文算法在跨材料伪造指纹检测任务中取得了较好的泛化性。

伪造指纹检测目前在同材料（传感器）检测、跨材料样本泛化性方面取得了突破性的进展，但仍存在一个亟需解决的难题，即真假指纹样本不平衡问题。指纹涉及到用户隐私，难以构建一个海量的指纹样本集。相较于真指纹，伪造指纹样本数量严重不足。如何扩充和生成高分辨率、高视觉质量的伪造指纹，是当前迫切需要解决的问题，而生成对抗网络、扩散模型等技术有望解决这一难题。

参考文献（References）

Abdullahi S M, Sun S F, Malik A, Khudeyberdiev O and Basheer R. 2022. Spoofed fingerprint image detection using local phase patch segment extraction and a lightweight network//Proceedings of the 18th IFIP WG 11.9 International Conference on Advances in Digital Forensics XVIII. Virtual Event: Springer: 85-105 [DOI: 10.1007/978-3-031-10078-9_5]

Abrishambaf R, Demirel H and Kale I. 2008. A fully CNN based fingerprint recognition system//Proceedings of the 11th International Workshop on Cellular Neural Networks and Their Applications. Santiago de Composteia, Spain: IEEE: 146-149 [DOI: 10.1109/CNNA.2008.4588667]

Ametefe D S, Sarnin S S, Ali D M and Zaheer M Z. 2022. Fingerprint liveness detection schemes: a review on presentation attack. Computer Methods in Biomechanics and Biomedical Engineering: Imaging and Visualization, 10(2): 217-240 [DOI: 10.1080/21681163.2021.2012826]

Anusha B V S, Banerjee S and Chaudhuri S. 2020. DeFraudNet: End2End fingerprint spoof detection using patch level attention//Proceedings of 2020 IEEE Winter Conference on Applications of Computer Vision. Snowmass, USA: IEEE: 2684-2693 [DOI: 10.1109/WACV45572.2020.9093397]

Barhoumi S, Khmila H and Kallel I K. 2021. Efficient fingerprint analysis based on sweat pore map//Derbel N and Kanoun O, eds. Advanced Methods for Human Biometrics. Cham: Springer: 3-20 [DOI: 10.1007/978-3-030-81982-8_1]

Chiroma H. 2021. Deep learning algorithms based fingerprint authentication: systematic literature review. Journal of Artificial Intelligence and Systems, 3(1): 157-197 [DOI: 10.33969/AIS.2021.31010]

Chugh T, Cao K and Jain A K. 2018. Fingerprint spoof buster: use of minutiae-centered patches. IEEE Transactions on Information Forensics and Security, 13(9): 2190-2202 [DOI: 10.1109/TIFS.2018.2812193.]

Cipolla R, Gal Y and Kendall A. 2018. Multi-task learning using uncertainty to weigh losses for scene geometry and semantics//Proceedings of 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Salt Lake City, USA: IEEE: 7482-7491 [DOI: 10.1109/CVPR.2018.00781]

Gan J Y, Qi L, Qin C B and He G H. 2019. Lightweight fingerprint classification model combined with transfer learning. Journal of Image and Graphics, 24(7): 1086-1095 (甘俊英, 戚玲, 秦传波, 何国辉. 2019. 结合迁移学习的轻量级指纹分类模型. 中国图象图形学报, 24(7): 1086-1095) [DOI: 10.11834/jig.180499]

González-Soler L J, Gomez-Barrero M, Chang L, Perez-Suarez A and Busch C. 2021. Fingerprint presentation attack detection based on local features encoding for unknown attacks. IEEE Access, 9: 5806-5820 [DOI: 10.1109/ACCESS.2020.3048756]

Hu C, Zhu L Q, Qiu W B and Wu W J. 2022. Data augmentation vision transformer for fine-grained image classification [EB/OL]. [2023-08-20]. https://arxiv.org/pdf/2211.12879.pdf

Jia X Y, Zhang W Z, Li W W and Huang Z Q. 2021. Feature representation method for heterogeneous defect prediction based on variational autoencoders. Journal of Software, 32(7): 2204-2218 (贾修一, 张文舟, 李伟漳, 黄志球. 2021. 基于变分自编码器的异构缺陷预测特征表示方法. 软件学报, 32(7): 2204-2218) [DOI: 10.13328/j.cnki.jos.006257]

Karampidis K, Rousouliotis M, Linardos E and and Kavallieratou E. 2021. A comprehensive survey of fingerprint presentation attack detection. Journal of Surveillance, Security and Safety, 2(4): 117-161 [DOI: 10.20517/jsss.2021.07]

Khade S, Thepade S D and Ambedkar A. 2018. Fingerprint liveness detection using directional ridge frequency with machine learning classifiers//Proceedings of the 4th International Conference on Computing Communication Control and Automation (ICCUBEA). Pune, India: IEEE: 1-5 [DOI: 10.1109/ICCUBEA. 2018.8697895]

Li Y, Tian X M, Gong M M, Liu Y J, Liu T L, Zhang K and Tao D C. 2018. Deep domain generalization via conditional invariant adversarial networks//Proceedings of the 15th European Conference on Computer Vision. Munich, Germany: Springer: 647-663 [https://doi.org/10.1007/978-3-030-01267-0_38]

Liu F, Kong Z, Liu H Z, Zhang W T and Shen L L. 2022. Fingerprint presentation attack detection by channel-wise feature denoising. IEEE Transactions on Information Forensics and Security, 17: 2963-2976 [DOI: 10.1109/TIFS.2022.3197058]

Lu X W, Ding W Q, Li H Y, Yu P F and Gu J. 2021. Fine-grained image classification algorithm based on attention self-supervision//Proceedings of the 5th IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). Chongqing, China: IEEE: 517-521 [DOI: 10.1109/IAEAC50856.2021.9390994]

Maltoni D, Maio D, Jain A K and Feng J J. 2022. Latent fingerprint recognition//Maltoni D, Maio D, Jain A K and Feng J J, eds. Handbook of Fingerprint Recognition. Cham: Springer: 339-383 [DOI: 10.1007/978-3-030-83624-5_6]

Mura V, Orrù G, Casula R, Sibiriu A, Loi G, Tuveri P, Ghiani L and Marcialis G L. 2018. LivDet 2017 fingerprint liveness detection competition 2017//Proceedings of 2018 International Conference on Biometrics (ICB). Gold Coast, Australia: IEEE: 297-302 [DOI: 10.1109/ICB2018.2018.00052]

Nguyen D L and Jain A K. 2019. End-to-end pore extraction and matching in latent fingerprints: going beyond minutiae [EB/OL]. [2023-08-20]. https://arxiv.org/pdf/1905.11472.pdf

Orrù G, Casula R, Tuveri P, Bazzoni C, Dessalvi G, Micheletto M, Ghiani L and Marcialis G L. 2019. LivDet in action-fingerprint liveness detection competition 2019//Proceedings of 2019 International Conference on Biometrics (ICB). Crete, Greece: IEEE: 1-6 [DOI: 10.1109/ICB45273.2019.8987281]

Rai A, Anshul A, Jha A, Jain P, Sharma R P and Dey S. 2023. An open patch generator based fingerprint presentation attack detection using generative adversarial network. Multimedia Tools and Applications, 83: 27723-27746 [DOI: 10.1007/s11042-023-16503-6]

Shaheed K, Mao A H, Qureshi I, Kumar M, Abbas Q, Ullah I and Zhang X M. 2021. A systematic review on physiological-based biometric recognition systems: current and future trends. Archives of Computational Methods in Engineering, 28(7): 4917-4960 [DOI: 10.1007/s11831-021-09560-3]

Sharma R P and Dey S. 2019. Fingerprint liveness detection using local quality features. The Visual Computer, 35(10): 1393-1410 [DOI: 10.1007/s00371-018-01618-x]

Sun Z N, He R, Wang L, Kan M N, Feng J J, Zheng F, Zheng W S, Zuo W M, Kang W X, Deng W H, Zhang J, Han H, Shan S G, Wang Y L, Ru Y W, Zhu Y H, Liu Y F and He Y. 2021. Overview of Biometrics research. Journal of Image and Graphics, 26(6): 1254-1329 (孙哲南, 赫然, 王亮, 阚美娜, 冯建江, 郑方, 郑伟诗, 左旺孟, 康文雄, 邓伟洪, 张杰, 韩琥, 山世光, 王云龙, 茹一伟, 朱宇豪, 刘云帆, 何勇. 2021. 生物特征识别学科发展报告. 中国图象图形学报, 26(6): 1254-1329) [DOI: 10.11834/jig.210078]

Valdes-Ramirez D, Medina-Pérez M A, Monroy R, Loyola-Gonzalez O, Rodriguez J, Morales A and Herrera F. 2019. A review of fingerprint feature representations and their applications for latent fingerprint identification: trends and evaluation. IEEE Access, 7: 48484-48499 [DOI: 10.1109/ACCESS.2019.2909497]

van der Maaten L and Hinton G. 2008. Visualizing data using t-SNE. Journal of Machine Learning Research, 9(86): 2579-2605

Wang J, Yu X H and Gao Y S. 2021. Mask guided attention for fine-grained patchy image classification//Proceedings of 2021 IEEE International Conference on Image Processing (ICIP). Anchorage, USA: IEEE: 1044-1048 [DOI: 10.1109/ICIP42928.2021.9506424]

Wang R Y, Chu B L, Yang Z and Zhou L N. 2022. An overview of visual DeepFake detection techniques. Journal of Image and Graphics, 27(1): 43-62 (王任颖, 储贝林, 杨震, 周琳娜. 2022. 视觉深度伪造检测技术综述. 中国图象图形学报, 27(1): 43-62) [DOI: 10.11834/jig.210410]

Woo S, Park J, Lee J Y and Kweon I S. 2018. CBAM: convolutional block attention module//Proceedings of the 15th European Conference on Computer Vision (ECCV). Munich, Germany: Springer: 3-19 [DOI: 10.1007/978-3-030-01234-2_1]

Xia Z H, Lv R, Zhu Y F, Ji P, Sun H Y and Shi Y Q. 2017. Fingerprint liveness detection using gradient-based texture features. Signal, Image and Video Processing, 11(2): 381-388 [DOI: 10.1007/s11760-016-0936-z]

Yang W C, Wang S, Hu J K, Zheng G L and Valli C. 2019. Security and accuracy of fingerprint-based biometrics: a review. Symmetry, 11(2): #141 [DOI: 10.3390/sym11020141]

Yuan C S, Yu P P, Xia Z H, Sun X M and Wu Q M J. 2022. FLD-SRC: fingerprint liveness detection for AFIS based on spatial ridges continuity. IEEE Journal of Selected Topics in Signal Processing, 16(4): 817-827 [DOI: 10.1109/JSTSP.2022.3174655]

Zeng F F, Hu S D and Xiao K. 2019. Research on partial fingerprint recognition algorithm based on deep learning. Neural Computing and Applications, 31(9): 4789-4798 [DOI: 10.1007/s00521-018-3609-8]

Zhang Y L, Fang S S, Xie Y and Xu T T. 2014. Fake fingerprint detection based on wavelet analysis and local binary pattern//Proceedings of the 9th Chinese Conference on Biometric Recognition. Shenyang, China: Springer: 191-198 [DOI: 10.1007/978-3-319-12484-1_21]

作者简介

袁程胜,男,副教授,硕士生导师,主要研究方向为信息隐藏、多媒体取证与人工智能安全。E-mail:ycs_nuist@163.com

徐震宇,男,硕士研究生,主要研究方向为生物特征取证。E-mail:xzy1341439190@163.com

向凌云,女,副教授,硕士生导师,主要研究方向为信息隐藏与数字水印。E-mail:sander_2001@163.com

付章杰,男,教授,博士生导师,主要研究方向为区块链安全、隐写与隐写分析。E-mail:wwwfzj@126.com

夏志华,男,教授,博士生导师,主要研究方向为人工智能安全、云计算安全。E-mail:xia_zhihua@163.com