基于样本生成机制的包装印刷品真伪防御性判别

doi:10.3969/j.issn.1674-7100.2023.05.005

乔俊伟[1] 宛 东[2]

1. 上海出版印刷高等专科学校
智能与绿色柔版印刷重点实验室
上海 200093
2. 上海理工大学
出版印刷与艺术设计学院
上海 200093

摘 要：借助手机实现假包装印刷品的识别，实现主动确权，从而达到更加精确的真假包装印刷品判别。针对造假样品极度缺乏的情况，提出基于记忆增强 DCGAN 样本生成算法来实现假样本扩增，再利用孪生并行注意力卷积神经网络（S-PA-CNN）实现包装印刷品真伪的防御性判别。在 1 种印刷纸张、2 种拍摄光源和 2 种拍摄手机组合的 4 种开放场景中，拍摄多个真包装印刷品和少量的假包装印刷品图像，用基于记忆增强 DCGAN 样本生成算法扩增假包装印刷品样本，建立数据集。实验结果表明：数据扩增后，假样本和真样本数量差不多时，S-PA-CNN 的检测准确率在 97% 以上。本文数据扩增方法能够提升网络模型的真样本特征识别能力、细粒度判别精度和泛化能力。

关键词：包装印刷品；DCGAN；编解码器；卷积神经网络；微小篡改；真伪判别

中图分类号：TB482；TP391 **文献标志码**：A

文章编号：1674-7100(2023)05-0031-37

引文格式：乔俊伟，宛 东 . 基于样本生成机制的包装印刷品真伪防御性判别 [J]. 包装学报，2023，15(5)：31-37.

1 研究背景

假冒伪劣商品会给市场造成严重冲击，扰乱正常的市场经济秩序，也会给消费者带来重大的经济损失，因而如何判别假冒伪劣商品成为一个重要课题。随着搭载高分辨率摄像头的智能手机的普及，人们可以轻松、便捷地拍摄到高质量的包装印刷品图像，使用手机拍摄包装印刷品进行真伪判别成为可能。

在包装印刷品刚推出市场时造假案例还较少的情况下，常规的深度学习方法会因得不到充足的真假匹配样本而导致检测性能无法达到实际要求。样本数据量不足的问题通常采用数据扩增方法来解决。数据扩增方法有非生成式方法和生成式方法。Hu W. J. 等 [1] 基于翻转、旋转等数据扩增方法对训练集进行数据扩增，以提升 MDFC-ResNet 检测模型的效果。高嘉南等 [2] 采用旋转、亮度变换和缩放等数据扩增方法增加实验数据量和数据多样性。3 种数据扩增方法对 YOLOv4 模型的检测性准确率提升分别达到 7.32%，4.84% 和 8.04%。结果表明数据扩增后与数据扩增前相比，YOLOv4 模型的识别精度均值提高了 10.04%。目前，生成式数据扩增方法主要基于生成对抗网络 [3-6]（generative adversarial networks，GAN），利用对抗竞争思想来生成与原始图像数据分布相似的图像数据。A. Radford 等 [4] 提出

收稿日期：2023-06-01

基金项目：上海市东方学者特聘教授基金资助项目（TP2022126）；国家新闻出版署智能与绿色柔版印刷重点实验室开放招标课题（ZBKT202301）

作者简介：乔俊伟（1973-），男，山西左权人，上海出版印刷高等专科学校教授级高工，博士，主要从事印刷智能化、印刷包装智能装备、绿色印刷技术研究，E-mail：113846789@qq.com

的 DCGAN（deep convolutional generative adversarial networks）则是在 GAN 的基础上引入卷积网络，利用卷积网络作特征提取，使模型更加稳定，更适合完成图像生成及检测任务 [7-8]。在 GAN 中，样本特征生成局限于已知的少量假样本，没有提前进行真样本特征与假样本特征之间的交互，从而造成生成的假样本多样性不够。S. Akcay、王齐等 [9-10] 设计了编解码器网络与 GAN 结合的 GANomaly 网络，该网络能使非正常数据生成受到充足正常训练数据集的特征影响。付晓峰等 [11] 为了提高微表情检测准确率，利用自编码器扩充微表情数量，完成了亚洲人表情到欧美人表情的生成，实现了不同表情样本群间的特征交互。Zhao Z. X. 等 [12] 利用 GAN 与编解码器实现了基于真样本训练的缺陷图像生成。研究表明，基于 GAN 模型和编解码器的样本生成方法可以得到与真样本特征更为相似的假样本，但是无法完成细粒度特征生成。为了解决这个问题，Gong D. 等 [13] 在 A. Santoro 等 [14] 提出的记忆增强神经网络（memory augmented neural network，MANN）基础上构建了记忆增强自编码器网络（memory-augmented Autoencoder，MemAE），记忆增强通过硬截断机制舍弃了干扰信息，强化了真样本特征，使识别精度提高。

针对手机拍摄的微小篡改包装印刷品的真伪判别及假样本数量极少的场景，本文提出基于记忆增强 DCGAN 生成机制的包装印刷品真伪防御性判别模型。先提前训练真样本，再在此基础上利用假样本做数据扩增，生成包含更多真样本特征的假样本，最后用王晓红等 [15] 提出的 S-PA-CNN 网络判别包装印刷品真伪。

2 模型设计

2.2 基于记忆增强 DCGAN 样本生成模型框架

基于记忆增强 DCGAN 样本生成模型的网络结构如图 1 所示。训练模块结构与 GAN 网络相似，包含生成器和判别器。生成器包括编码器和解码器 [16]，利用大量真图训练网络，将输入的真图先进行下采样，再进行上采样。判别器则是预测生成图和原始图的真伪，并根据结果优化生成器。使用模块只有从训练模块迁移的生成器，没有对抗学习过程。使用模块能将输入的假样本 F 重构得到假样本 F′，以增加假样本数据数量，解决假样本数据量少时深度学习算法的防御性检测能力差的问题。

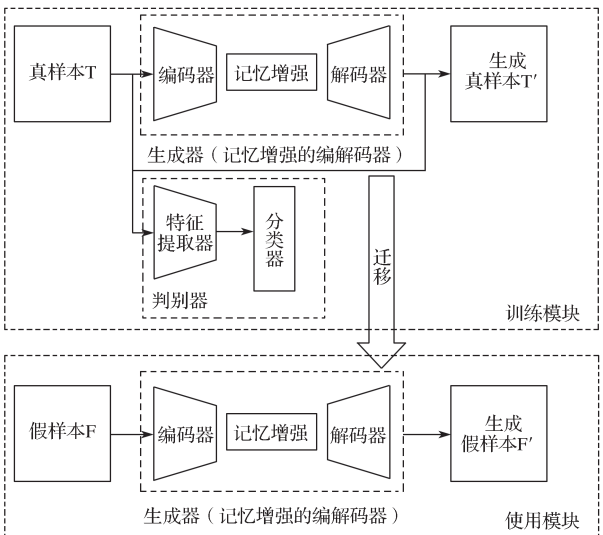


图 1 基于记忆增强 DCGAN 样本生成网络结构图

Fig. 1 Structure diagram of sample generation network based on DCGAN memory enhancement

本模型采用 DCGAN 的编码器、判别器结构，但是常规的 DCGAN 中解码器对多尺度特征信息挖掘不充分，因而需对解码器结构进行改进。

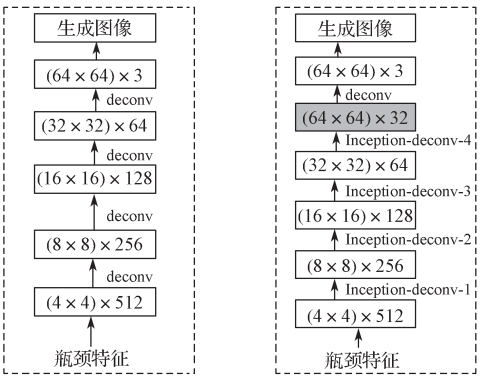
2.2 改进解码器结构

2.2.1 改进思路

本文采用基于 Inception 模块 [17] 的多尺度级联结构代替简单的反卷积级联结构。使用不同大小卷积核的反卷积来恢复得到尺度不同的图像特征，确保特征尺寸不一致时也能提取出同等重要的关键信息，从而提升扩增图像样本数据的生成质量 [18-21]。改进前后的解码器结构如图 2 所示。改进后解码器的详细结构如图 3 所示。

4 个 Inception-deconv 层是对原始 DCGAN 网络中反卷积层（deconv）的改进。卷积（conv）和 deconv 后面的数字代表卷积核的大小和步长，如 deconv1 的 3 × 3/2, 2 代表卷积核大小是 3 × 3、步长是（2, 2）。conv 和 deconv 后面都带有 BN 层和 ReLU 激活函数。ni 层表示最近邻插值操作，用以在扩大特征图的尺寸同时保留恢复得到的图像特征。在 Inception-deconv 模块的各个分支中，反卷积核的大小不同，使模块能学习恢复不同尺度的特征。反卷积后进行 1 × 1 的卷积，其目的是跨通道聚合，避免反卷积的冗余输出。Concatenate 层能合并各个输出的特征向量，使得下一个 Inception-deconv 模块能全面利用已经恢复的特征。并联多种尺度的反卷积可提高网络宽度，使生成器能用于不同尺度的样本，

最终能够达到增加网络的细粒度特征。



a）改进前　　b）改进后

图 2　解码器改进前后的结构示意图

Fig. 2　Structure diagram of decoder before and after improvement

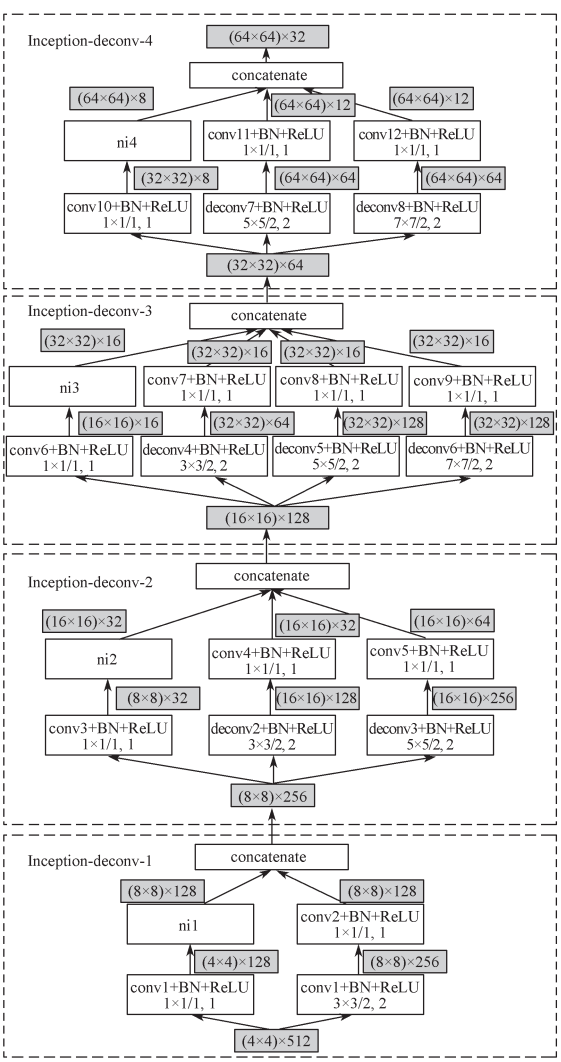


图 3　解码器改进后的详细结构图

Fig. 3　Detailed structure diagram of decoder after improvement

2.2.2　损失函数

损失函数是由单一对抗损失函数（L_0）、重构损失函数（L_1）、对齐损失函数（L_2）和内容感知损失函数（L_3）线性组合而成的多项式。

$$L=L_0+\lambda_1 L_1+\lambda_2 L_2+\lambda_3 L_3+\alpha E(\omega_t'), \tag{1}$$

式中：λ_1、λ_2、λ_3 为权重；

$\alpha E(\omega_t')$ 为记忆模块的正则化项。

重构损失函数主要计算输入图像（x）和重构图像（x'）的欧氏距离，得到生成图与真图在内容上的相似度。

$$L_1 = E_{x\sim p_x}\left\|x-x'\right\|_2, \tag{2}$$

式中 $E_{x\sim p_x}$ 为分布函数的期望值，其中 p_x 为真样本的分布。

对齐损失函数主要计算输入图像（x）和重构图像（x'）的低维度特征欧氏距离。f 函数是判别器提取 x 和 x' 的低维特征。式（4）和（5）得到瓶颈特征 z 和 z'。

$$L_2 = E_{x\sim p_x}\left\|f(x)-f(x')\right\|_2, \tag{3}$$

$$z=f_c(x), \tag{4}$$

$$x'=f_d(z'). \tag{5}$$

内容感知损失函数计算生成网络生成的图像与真图在内容上的相似性。

$$L_3 = E_{x,x'}\left[\left\|\varphi(x)-\varphi(x')\right\|_2\right], \tag{6}$$

式中 φ 为内容感知函数。

3　实验部分

3.1　数据采集

在户外、室内 2 种照明环境下，用 2 种手机（荣耀 V8、苹果 6）对包装印刷品真样本和假样本进行拍照，拍照对焦时要使包装局部的图形、纹理清晰可见，获得真样本 3200 个、假样本 200 个。图 4 所示为部分产品在某一型号纸张上印刷的外包装印刷品示意图。

3.2　实验环境与参数设置

硬件平台配置如下：CPU 为 Intel Xeon Bronze 3106 @ 1.70 GHz 16 核；内存为 128 GB；GPU 为 Nvidia Quadro P4000，显存 8 GB。软件平台配置如下：深度学习框架为 PyTorch，Python 版本为 3.6.0，cuda 和 cudnn 版本为 10.0，操作系统是 Windows 10。

网络的训练参数如下：batch size 设置为 8，学习率设置为 1e−4，网络优化器 optimizer 选择为 Adam。

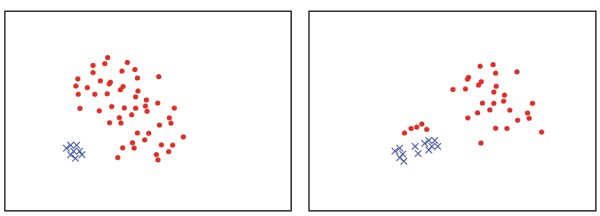
图 4　产品包装真伪示意图

Fig. 4　Schematic diagram of real and fake printing product packaging

3.3　模型特征生产和提取分析

a）编解码器生成样本特征分析

取两组相似的包装印刷品样本局部图，分别用有记忆增强模块和无记忆增强模块的编解码器生成样本特征，再用 t-SNE 可视化方法绘制如图 5 所示的特征分布情况。图中，真样本的特征用十字表示，假样本的特征用圆点表示。由图 5 可知，记忆增强使假样本的部分假特征区域消失，使部分假特征和真特征区域重叠，说明记忆增强能够在假样本上带入部分真特征，增加了样本多样性。



a）无记忆增强模块　　b）有记忆增强模块

图 5　记忆增强特征前后分布情况

Fig. 5　Features changes in the distribution of memory enhancement before and after

b）网络提取样本特征分析

将 S-PA-CNN 网络训练至损失值稳定后，利用网络提取测试样本的特征向量并计算每对测试样本之间的欧氏距离，以此来表征孪生模型的特征提取能力，实验结果如图 6 所示。从图 6 可以看出，“真－假”样本对之间的欧氏距离的主体分布逐渐向右侧聚集，表明本文数据扩增方法能提高篡改特征的提取能力，强化网络对不同特征之间的区分能力。而“真－真”“假－假”样本对之间的欧氏距离的主体分布逐渐向左侧聚集，表明本文数据扩增方法还能提高网络对同种特征的聚合归纳能力。

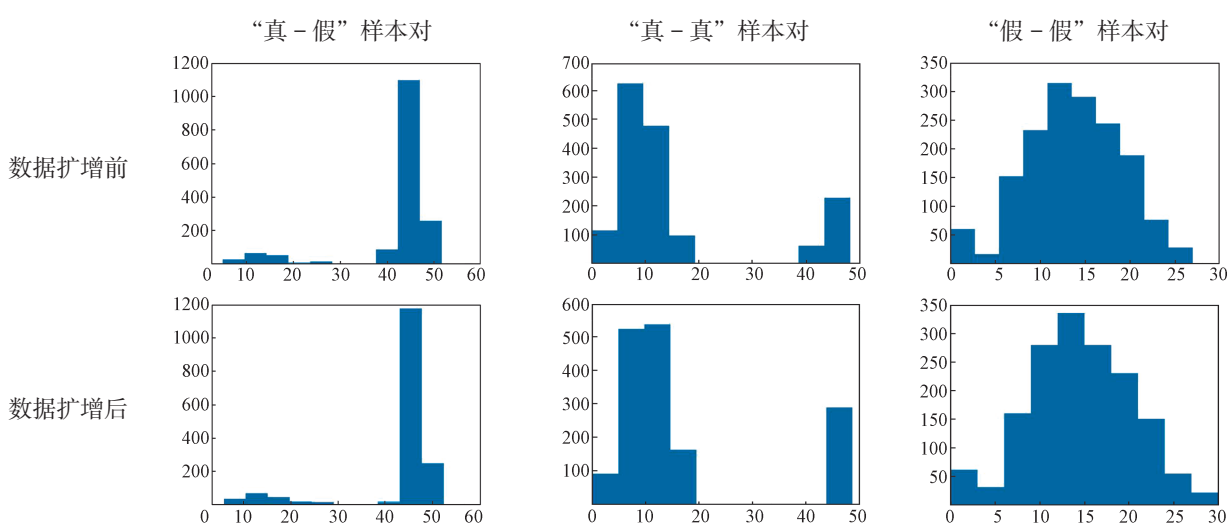


图 6　样本对的特征欧氏距离

Fig. 6　Feature Euclidean distance between sample pairs

3.4 模型检测准确率对比

本实验中，传统数据扩增方法为旋转变换和缩放变换的组合，旋转角度为 90° ，缩放倍数为 0.6, 0.7, 0.8, 0.9, 1.1, 1.2, 1.3, 1.4。当真样本为 3200 个，假样本较少或极少时，无数据扩增方法、传统数据扩增方法与本文数据扩增方法的检测准确率对比如表 1 所示。表 2 为基于 200 个较少假样本的本文数据扩增方法和传统数据扩增方法的准确率对比。表 3 为基于 3 个极少假样本的数据扩增方法在不同扩增程度下得到的烟标综合检测准确率。实验结果表明，在样本数量不充足的情况下 S-PDA-CNN 网络的检测准确率较低；随着数据扩增量的提高，网络检测准确率随之提高，且当假样本的数量扩增到与真样本数量基本持平时，篡改检测效果达到最好，说明数据扩增能帮助 S-PA-CNN 更好地提取篡改图像特征。在同样实验条件下，本文方法的检测准确率高于传统数据扩增方法，说明本文方法能更好地解决假样本不足造成检测准确率不高的问题。

表 1 不同数据扩增方法的检测准确率对比

Table 1 Accuracy of different amplification

假样本数量	检测准确率 /%		
	无数据扩增	传统数据扩增方法	本文方法
较少	87.8	96.1	99.9
极少	50.0	过拟合	97.9

表 2 较少假样本下数据扩增检测准确率对比

Table 2 Accuracy of less fake sample data amplification

样本扩增数量 / 个	检测准确率 /%	
	传统数据扩增方法	本文方法
0	87.8	87.8
600	88.5	89.5
1400	93.2	95.1
2200	95.5	97.1
3000	96.1	99.7
3800	96.1	99.9
4200	96.1	99.9

表 3 极少假样本下数据扩增检测准确率对比

Table 3 Accuracy of minimal fake sample data amplification

样本扩增数量 / 个	检测准确率 /%	
	传统数据扩增方法	本文方法
0	50.0	50.0
1000	过拟合	92.5
2600	过拟合	95.2
4200	过拟合	97.9
4800	过拟合	97.9

4 结语

针对在包装印刷品篡改检测样本少的情形下孪生卷积神经网络判别模型检测准确率较低的问题，本文提出利用 DCGAN 和记忆增强编解码器重建的样本扩增方法，从数据驱动的角度强化网络判别模型的判别能力。本文方法能提前训练和学习真样本特征，提高模型防御性，能用于手机等便携设备对包装印刷品的真伪判别。

参考文献：

[1] HU W J，FAN J，DU Y X，et al. MDFC-ResNet: An Agricultural IoT System to Accurately Recognize Crop Diseases[J]. IEEE Access，2020，8：115287−115298.

[2] 高嘉南，侯凌燕，杨大利，等 . 基于轻量级网络和数据扩增的作物与杂草识别 [J]. 北京信息科技大学学报（自然科学版），2022，37(1)：82−89，95.
GAO Jianan，HOU Lingyan，YANG Dali，et al. Crop and Weed Identification Based on Lightweight Network and Data Amplification[J]. Journal of Beijing Information Science & Technology University，2022，37(1)：82−89，95.

[3] GOODFELLOW I J，POUGET-ABADIE J，MIRZA M，et al. Generative Adversarial Networks[C]//Advances in Neural Information Processing Systems. Ithaca：arXiv e-prints，2014：2672−2680.

[4] RADFORD A，METZ L，CHINTALA S. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks[C]//4th International Conference on Learning Representations(ICLR 2016). Ithaca：arXiv e-prints，2016：1−16.

[5] 杨 宇 . 基于生成对抗网络的图像数据增强方法研究 [D]. 郑州：中国人民解放军战略支援部队信息工程大学，2022.
YANG Yu. Research on Image Data Augmentation Based on Generative Adversarial Network[D]. Zhengzhou：Information Engineering University，2022.

[6] 范 黎 . 基于生成对抗网络的图像数据增强技术研究及应用 [D]. 杭州：浙江大学，2022.
FAN Li. Research and Application of Image Data Augmentation Technology Based on Generative Adversarial Networks[D]. Hangzhou：Zhejiang University，2022.

[7] 谢堂营 . 基于 DCGAN 的图像增强方法研究 [D]. 包头：

内蒙古科技大学，2021.
XIE Tangying. Research on Image Augmentation Method Based on DCGAN[D]. Baotou：Inner Mongolia University of Science & Technology，2021.

[8] 王海涛，高玉栋，侯建新，等 . 基于 DCGAN 的印刷缺陷检测方法 [J]. 哈尔滨理工大学学报，2021，26(6)：24−32.
WANG Haitao，GAO Yudong，HOU Jianxin，et al. A Method of Printing Defect Detection Based on DCGAN[J]. Journal of Harbin University of Science and Technology，2021，26(6)：24−32.

[9] AKCAY S，ATAPOUR-ABARGHOUEI A，BRECKON T P. Ganomaly: Semi-Supervised Anomaly Detection via Adversarial Training[C]//14th Asian Conference on Computer Vision（ACCV 2018）. Perth：Springer，2018：622−637.

[10] 王 齐，陈 功，胡文昕，等 . 使用 GANomaly 网络的面瘫识别应用研究 [J]. 软件工程，2022，25(3)：29−33.
WANG Qi，CHEN Gong，HU Wenxin，et al. Application Research of Facial Paralysis Recognition Based on GANomaly Network[J]. Software Engineering，2022，25(3)：29−33.

[11] 付晓峰，牛 力 . 基于深度卷积和自编码器增强的微表情判别 [J]. 浙江大学学报（工学版），2022，56(10)：1948−1957.
FU Xiaofeng，NIU Li. Micro-Expression Classification Based on Deep Convolution and Auto-Encoder Enhancement[J]. Journal of Zhejiang University (Engineering Science)，2022，56(10)：1948−1957.

[12] ZHAO Z X，LI B，DONG R，et al. A Surface Defect Detection Method Based on Positive Samples[C]//Proceedings of the Pacific Rim International Conference on Artificial Intelligence. Nanjing：Springer，2018：473−481.

[13] Gong D，Liu L Q，Le V，et al. Memorizing Normality to Detect Anomaly: Memory-Augmented Deep Autoencoder for Unsupervised Anomaly Detection[C]//Proceedings of the IEEE International Conference on Computer Vision. Seoul：IEEE，2019：1705−1714.

[14] SANTORO A，BARTUNOV S，BOTVINICK M，et al. Meta-Learning with Memory-Augmented Neural Networks[C]//Proceedings of the 33rd International Conference on International Conference on Machine Learning. New York：ACM，2016：1842−1850.

[15] 王晓红，宛 东 . 基于孪生并行注意力网络的包装印刷品商标真伪鉴别研究 [J]. 包装学报，2023，15(1)：86−94.
WANG Xiaohong，WAN Dong. Research on Discriminating the Authenticity of Packaging Printed Logos Based on Siamese Parallel Attention Network[J]. Packaging Journal，2023，15(1)：86−94.

[16] 蔚 焘，成卫青 . 基于记忆增强的对抗自编码器异常检测算法 [J]. 南京邮电大学学报（自然科学版），2021，41(6)：84−94.
WEI Tao，CHENG Weiqing. Anomaly Detection Algorithm Based on Memory-Augmented Adversarial Autoencoder[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition)，2021，41(6)：84−94.

[17] CHOLLET F. Xception: Deep Learning with Depthwise Separable Convolutions[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Honolulu：IEEE，2017：1800−1807.

[18] 王 波，黄 冕，刘利军，等 . 基于多层聚焦 Inception-V3 卷积网络的细粒度图像分类 [J]. 电子学报，2022，50(1)：72−78.
WANG Bo，HUANG Mian，LIU Lijun，et al. Multi-Layer Focused Inception-V3 Models for Fine-Grained Visual Recognition[J]. Acta Electronica Sinica，2022，50(1)：72−78.

[19] 谢晓燕，杜卓林，胡传瞻，等 . 基于重构设计的 Inception 网络 [J]. 计算机工程与设计，2022，43(4)：1195−1201.
XIE Xiaoyan，DU Zhuolin，HU Chuanzhan，et al. Reconfigurable Design of Inception Network[J]. Computer Engineering and Design，2022，43(4)：1195−1201.

[20] 董跃华，彭辉林 . 改进 Inception 结构的图像分类方法 [J]. 软件导刊，2023，22(2)：41−46.
DONG Yuehua，PENG Huilin. Image Classification Method Based on Improved Inception Structure[J]. Software Guide，2023，22(2)：41−46.

[21] 胡 鹰，郝路通 . 基于改进的 Inception 金属板材表面质量缺陷检测 [J]. 计算机与数字工程，2022，50(7)：1593−1597.
HU Ying，HAO Lutong. Metal Plate Surface Defect Inspection Based on the Improved Inception Neural Network[J]. Computer & Digital Engineering，2022，50(7)：1593−1597.

（责任编辑：邓 彬）

Defensive Identification of Authenticity of Packaging Printed Matter Based on Sample Generation Mechanism

QIAO Junwei[1]，WAN Dong[2]

（1. Key Lab of Intelligent and Green Flexographic Printing，Shanghai Publishing and Printing College，Shanghai 200093，China；2. College of Communication and Art Design，University of Shanghai for Science and Technology，Shanghai 200093，China）

Abstract：With the help of mobile phones, the identification of forged packaging printed matter can be realized, and the active confirmation can be realized, so as to achieve more accurate identification of true and fake packaging printed matter. In the case of extremely lack of fake samples, a sample generation algorithm based on DCGAN memory enhancement was proposed to realize the amplification of fake samples, and the attention convolutional neural network was used to distinguish the authenticity of packaged printed matter defensively. Several groups of authentic packaging printed matter and a very small number of counterfeit packaging printed matter images were shot in four open scenes, which consisted of one kind of printing paper, two kinds of shooting light source and two kinds of shooting mobile phone. The sample of counterfeit packaging printed matter was generated based on DCGAN memory enhancement algorithm, and the algorithm research data set was established. The experimental results show that the discriminant accuracy of S-PA-CNN twin attention convolutional neural network based on amplified data set is more than 97%. The experimental results show that the proposed data amplification method can further improve the authenticity feature recognition ability of the network model, improve the fine-grained discrimination accuracy, and enhance the generalization ability.

Keywords：packaging printed matter；DCGAN；encoder-decoder；CNN；slight tempering；authenticity discrimination