文章编号:1671-4598(2022)10-0240-06 DOI:10.16526/j.cnki.11—4762/tp.2022.10.037 中图分类号:TP391 文献标识码:A

基于生成对抗网络和 DenseNet 的数据信息安全识别方法

夏利玲，顾建华
（盐城工业职业技术学院 信息与安全学院，江苏 盐城 224005）

摘要：针对传统电力巡检过程中必须依靠有经验的人工来完成对电力设备相关数据信息安全进行识别的方法，设计了一种基于生成对抗网络和密集连接网络的数据信息安全识别方法，采用生成对抗网络模型，利用其强大的表征能力，通过针对网络模型的训练完成对训练样本数据库的扩充，实现提升模型生成能力的目的；结合密集连接网络对电力巡检数据信息的安全性进行识别，实现解决电力巡检安全隐患的同时还可以推动人工智能技术的落地应用；通过在电力巡检数据信息集上的验证实验，比较不同方法在不同类型数据集上的识别精度，验证了基于生成对抗网络和密集连接网络的数据信息安全识别方法的有效性与可靠性，为传统识别电力巡检数据信息安全性的方法提供了全新思路。

关键词：生成对抗网络；DenseNet；电力巡检；电力设备；数据信息；安全识别

Data Information Security Identification Method Based on Generation Adversarial Networks and Densenet

XIA Liling, GU Jianhua
(School of Information and Security, Yancheng Polytechnic College, Yancheng 224005, China)

Abstract: In view of the method that the traditional power inspection process must rely on the experienced manual work to complete the identification of data and information security related to power equipment, a data and information security identification method based on Generative Adversarial Networks (GAN) and DenseNet is designed. The GAN model is adopted, and its powerful representation ability is used to complete the expansion of the training sample database through the training for the network model, which realizes the purpose of improving the model generation ability. Combined with the DenseNet, the security of power inspection data information can be identified, which can solve the hidden dangers of power inspection and promote the application of artificial intelligence technology. By the verification experiment on the data information set of electric power inspection, combined with the recognition accuracy of different methods on different types data sets, the validity and reliability of the data information security identification method based on the GAN and DenseNet are verified, which provides a new idea for the traditional identification method of the data information security of electric power inspection.

Keywords: GAN (generative adversarial networks); DenseNet; power inspection; power equipment; data information; information security

0 引言

伴随着我国电力设备的不断建设以及输电线路的不断延伸，传统电力巡检工作模式一方面因为严重依赖人力方式解决，人工成本较高，另一方面由于受限于如地形、天气、人员经验等多种因素影响，想要在全天候条件下完成对电力巡检数据信息安全性的排查工作，存在一定安全风险，这导致传统电力巡检方式已无法满足我国电力发展现状。因此数据信息采集设备被广泛应用于电力巡检任务中。日常电力巡检工作的主要内容包括：对电力线路进行异物检测[1]，避免出现因为异物遮挡而造成安全隐患事件。对重要电力设备的潜在安全风险进行评估，必要时为电力设备进行维护与抢修提供依据。对电力设备缺陷进行日常排查，做到早发现早解决。虽然通过智能采集设备可以获取到相关电力设备的数据信息，例如利用无人机[2]进行电力巡视，利用电子监控设备对电力设施的安全状况进行实时监控等，且这类方式具有全天候工作、跨越地形限制、节约人力成本等优点，但依旧需要经验丰富的人力对采集到的数据信息的安全性进行主观分析，存在漏检和错检的风险。针对上述问题，如何对数据信息的安全性进行有效识别[3]并提高识别效率，是目前研究人员要重点解决的问题。

收稿日期:2022-06-13； **修回日期**:2022-07-19。
基金项目:国家自然科学基金(61502411)；盐城工业职业技术学院横向课题(2021HX-85)。
作者简介:夏利玲(1983-)，女，江苏盐城人，硕士，讲师，主要从事计算机软件、网络安全等方向的研究。
顾建华(1972-)，女，江苏盐城人，硕士，副教授，主要从事计算机网络应用、智能控制等方向的研究。
引用格式:夏利玲，顾建华. 基于生成对抗网络和 DenseNet 的数据信息安全识别方法[J]. 计算机测量与控制，2022，30(10)：240-245.

图像数据具有蕴含信息量丰富、可跨距离、传输速率快等优点，因此图像数据成为人类获取数据信息的主要载体[4]。目前关于电力巡检数据安全性识别检查方法主要针对三种电力巡检数据类型：可见光照条件下采集到的数据类型、红外[5]和紫外光照条件下[6]采集到的数据数据类型，并对这三种数据类型开展智能信息安全性检测。本文主要针对在自然可见光条件下采集到的电力巡检图像数据，同时结合深度学习技术训练网络模型，实现对数据信息的安全性进行有效识别，具有识别效率高、高准确率和可靠性强等优点。

当前图像数据信息识别方法可以分为两类，第一类是传统基于目标物识别的方法，此类方法多数是基于待选区域特征提取的目标安全性识别方法，如文献［7］采用滑动窗口在待识别图像上对区域特征进行滑动提取。文献［8］是较早将红外图像数据应用于电力线路相关信息安全性检查的方法，主要思想是使用自适应方法，利用自然可见光照条件下原始电力设备图像与其红外光照条件下的图像进行背景校对，以增强红外图像数据信息质量，实现对电力线路相关信息的安全检测。针对文献［8］方法存在对高噪声抑制效果不佳，容易产生电力线路相关信息安全识别度低的问题，文献［9］将彩色图像融合技术应用于红外图像高噪声抑制问题，有助于提升输出图的视觉效果，经实验验证增强后的输出图可有效提升电力线路数据信息安全性识别准确度。传统图像数据信息安全性识别方法虽然一定程度上可以实现对电力巡检数据信息的安全性识别，但受制于计算机硬件性能上限，以及数据量有限等问题，识别结果存在鲁棒性差，抗噪声能力弱等缺点。第二类是基于深度学习技术特征提取的数据信息安全性识别方法，如 SIFT（scale invarint frature transform）因为其在目标识别过程中可对目标进行滤波，并且在关键节点的提取和创建上具有独特优势，被众多识别模型应用，文献［10］首次将 SIFT 应用于电力塔侧倾检测问题上，并取得不错的效果，其主要思想是通过 SIFT 计算电力塔的关键节点，最后经过计算匹配度完成对电力塔侧倾问题的检测。文献［11］是较早利用 R-CNN（region-convolutional neural networks）进行目标识别的方法，主要思路是对待识别图像通过分类，组成多个待判别区域构成的层次组，最后进行分类识别。随着卷积神经网络模型（CNN，convolutional neural network）结构的不断改进，诞生了许多改进方法，文献［12］创新性的将数据信息安全性的识别过程分两个阶段，第一阶段主要对数据信息中含有待识别目标的区域进行识别，第二阶段对区域内的目标通过类别标签匹配完成对数据信息安全性的识别。虽然基于深度学习技术特征提取的数据信息安全性识别方法在精准度方面取得较大进步，但因为电力巡检相关图像数据存在特殊性，用于识别网络训练的数据集缺少多元性，导致多数情况下只能对有限的数据类型特征进行提取，无法做到对整体数据类型的特征进行表达。

针对目前电力巡检采集到的图像数据缺乏统一性的问题，本文提出一种基于生成对抗网络[13]和密集连接网络的数据信息安全识别方法，解决电力巡检任务采集数据困难，以及传统 CNN 识别方法存在梯度爆炸等问题。

1　数据信息处理和安全性识别方法

1.1　生成对抗网络

生成对抗网络（GAN，generative adversarial nets）[14]是由生成器 G（generator）网络和判别器 D（discriminator）网络二者相互竞争组成，GAN 组成结构如图 1 所示。以生成图像为例，首先，随机噪声 z 输入 G 网络，输出伪造图像 $G(z)$；其次，从预先准备好的数据集中抽取真实图像 x，同时与 $G(z)$ 作为输入一起传入 D 网络，由 D 网络负责鉴定输入图像是真实图像还是伪造图像，在此期间，G 网络一直在不断提高生成能力，D 网络一直在不断提高判别能力，G 网络与 D 网络二者间不断相互竞争；最终，当 D 网络无法对伪造图像 $G(z)$ 的真伪做出正确判断时，说明此时的 G 网络与 D 网络相互之间保持在一种动态平衡的状态，此时 G 网络的生成效果最佳。

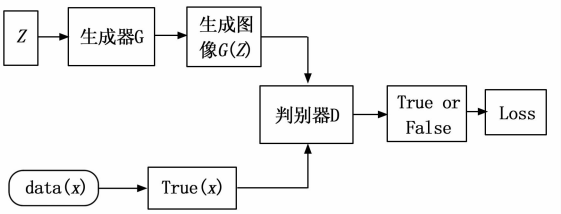

图 1　生成对抗网络原理图

最后给出 GAN 的目标函数：

$$\min_G \max_D V(G,D) = E_{x\sim P_{data}}[\log D(x)] + E_{x\sim P_G}[\log(1-D(x))] \tag{1}$$

其中：V 为 D 网络和 G 网络的最终优化目标；E 为数学期望；$x\sim P_{data}$ 表示数据来源于真实数据；$G(z)$ 为生成的伪造数据；$D(x)$ 和 $D(G(z))$ 为 D 网络分别对真实数据和生成数据进行判别的结果。

1.2　条件生成对抗网络

由于传统 GAN 中生成器网络过于自由导致无法有效控制生成内容，造成生成效果欠佳。条件生成对抗网络（CGAN，condition generative adversarial nets）[15]对传统 GAN 加入了约束条件，起到了监督作用，一定程度上控制了生成器的输出，CGAN 的网络结构如图 2 所示。

CGAN 的目标函数表达式如下：

$$\min_G \max_D V(D,G) = E_{x\sim P_{data(x)}}[\log D(x,y)] + E_{z\sim P_{(z)}}[\log(1-D(G(z,y)))] \tag{2}$$

其中：x 代表真实的图像数据；y 代表约束条件；z 代表随机噪声，目标函数的作用是要最小化生成器 D 网络的生成结果与真实结果之间的分布距离。

1.3　密集连接网络

基于 CNN 的深度学习模型虽然在图像处理方面取得

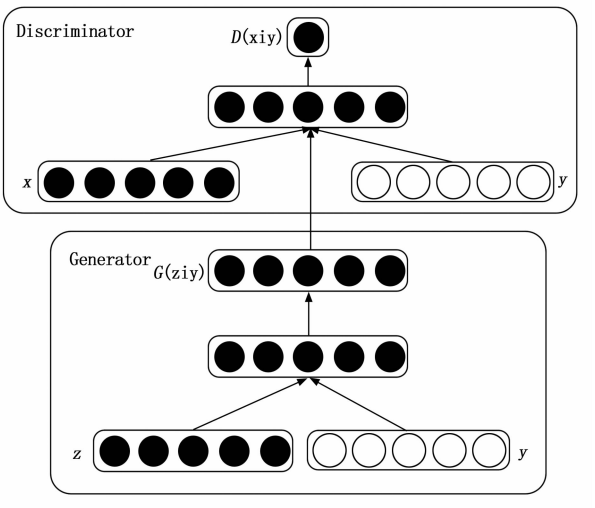

图 2 CGAN 的网络结构图

不错的成果，但也存在发展瓶颈，最突出的问题就是在训练过程中，深度学习模型的准确率会随着网络层数的复杂化而降低，这类现象被称之为“梯度弥散”现象，随着对生成对抗网络研究的不断加深，梯度弥散现象是一个急需解决的问题，虽然出现了 WGAN（wasserstein GAN），其优势是采用 Wasserstein 距离替代原始的 JS 散度衡量办法，实现对生成数据分布与真实数据分布之间距离差异更加平滑的刻画，可有效解决梯度弥散现象，但由于 WGAN 的先决条件是要满足 Lipschitz 约束条件，并对参数取值范围使用 Weight Clipping 截断操作，导致网络对分布在边界处的权值处理效果不佳，造成 WGAN 网络梯度学习速度较慢，影响网络收敛速度。针对 WGAN 中存在的不足，而后出现了（WGAN-GP），使用梯度惩罚项代替原始 WGAN 中的 Weight Clipping 截断操作，实现解决梯度弥散现象的同时有助于网络平稳训练，但因为缺乏对梯度惩罚项的泛化，导致 WGAN-GP 对数据分布之间距离差异刻画的多样性欠佳。针对上述问题，残差网络（ResNet，residual neural network）[16]因此诞生，其特点在于建立前一层与后一层间的快速连接，实现提升训练过程中梯度反向传播的速度。密集连接网络（DenseNet，dense connection net）[17]的构建思想类似于 ResNet，它们二者的结构区别如图 3 所示。

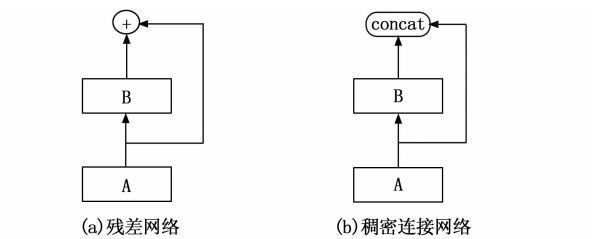

图 3 残差网络与稠密连接网络

DenseNet 与 ResNet 的区别在于，A 层输出和 B 层输出并不是作加法，知识对层与层之间做通道维度上的连接，如图 3（b）所示，A 层的输出直接和 B 层后面所有层进行连接，其优势在于特征重用以及方便梯度传递，可以有效缓解梯度消失。DenseNet 由多个稠密连接模块（Densely Connected Block）[18]组成，由于采用这种密集连接不需要进行卷积操作，如图 4 所示，所以产生的参数较少，可以让 DenseNet 在参数、样本和计算成本更少的任务中获得比 ResNet 更具有优势的性能。

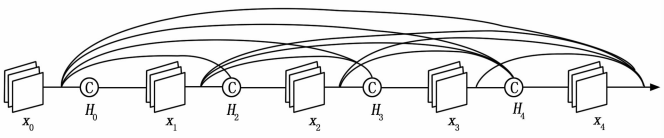

图 4 DenseNet 连接示意图

假设传统 CNN 中一共有 N 层，那么一共会产生 N 个连接，而在 DenseNet 中，N 层网络结构一共会产生 $N(N+1)/2$ 个连接，以图 4 为例，是一个四层结构的 DenseNet Block，其中 x_1，x_2，x_3，x_4 表示每一层输出的特征图；H_1，H_2，H_3，H_4 表示每一层的非线性变换。具体过程从 x_0 输入卷积层开始，依次通过 H_1 卷积层后得到输出 x_1，接着合并 x_0，x_1，结果作为输入传入第二层，输入 H_2 卷积层得到 x_2，再将 x_2 与 x_0，x_1 通道维度合并作为第三层的输入，如此循环反复，直到最后第四层输出的特征结果包含前面所有层的特征输出。由于 DenseNet 采用稠密连接方式，每一层都直接与输入的特征信息和损失函数连接，使特征信息和梯度值在网络训练过程中可以更加高效地传递。

2 本文方法模型

本文方法模型一共包含两部分功能模块：

1）基于条件生成对抗网络的数据扩充模块，该功能模块负责在有限规模的数据集条件下通过对网络的不断训练，得到具有较好生成效果的生成器网络模型，实现生成拥有较高图像质量的电力巡检数据，完成对现有电力巡检图像数据集的扩充。有效改善实际情况下电力巡检数据存在采集困难的缺点，同时扩充后的数据集为下一步提升深度学习网络对电力巡检数据信息安全性识别精准度提供了可靠的数据基础。具体实现步骤为：首先，将随机噪声 z 作为输入传入条件生成对抗网络，其中生成器 G 网络在约束条件即预先准备好的电力巡检图像数据的引导下生成逼真的电力巡检图像数据；然后，将生成图像作为输入传入判别器 D 网络，并在约束条件的辅助下进行真伪判别，利用损失函数反向优化生成器 D 网络与判别器 G 网络的权重参数；最后，当损失值更新停滞不前时，得到具有较好生成效果的生成器 G 网络，并利用其生成能力，生成逼真的电力巡检图像数据来弥补现有数据集规模有限与类型单一的缺点。

2）基于 DenseNet 的电力巡检数据信息安全识别模块，该功能模块负责对电力巡检数据集中的目标物进行特征提取，引导网络训练不断收敛，完成对数据信息中目标物的

检测，实现对电力巡检数据信息安全性的识别。具体实现步骤为：首先，将扩充后的数据集作为输入，并划分为待识别集与目标集，其中目标集中的标签已被预先处理好，待识别集中的标签是需要被分类识别的；然后，利用 DenseNet 的稠密连接方式对待识别图像数据特征进行提取学习，快速定位出待识别数据信息中包含待识别物所在的区域，紧接着计算其与目标集中提取到的特征信息之间距离分布差异，并利用池化层分类器对目标进行分类识别，对待识别物的位置和类别进行精细化判别；最后，根据类别情况给出识别标志，辅助工作人员对数据信息的安全性进行识别[19]。其中 DenseNet 映射公式为式（3），DenseNet 特征提取公式为式（4）。本文对电力巡检数据信息安全性的识别方法流程如图 5 所示。

$$X_L = H_L([X_0, X_1, \ldots, X_{L-1}]) \tag{3}$$

$$F = f + t \times L \tag{4}$$

其中：X_L 表示第 L 层特征通道数的输出；[ ] 表示对第 0 层到第 $L-1$ 层的所有特征输出进行通道维度的合并；H_L（ ）表示对第 L 层使用卷积操作＋批归一化＋Relu 的非线性变化。F 表示经过一层密集连接后的的通道数；f 表示经过一层密集连接前的的通道数；t 表示通道增长率；N 表示层数。

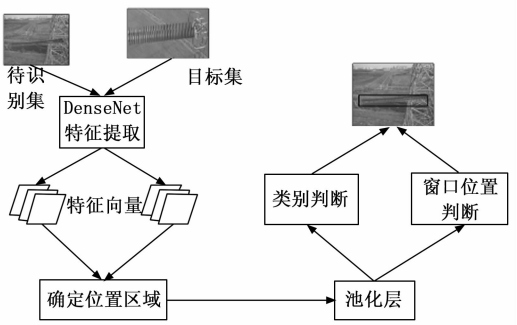

图 5　本文识别方法流程图

3　实验分析

3.1　实验数据集

由于电力巡检图像数据涉及国家安全相关信息，一般很难对外公开，因此本文利用现有公开的电力巡检图像数据通过输入本文提出的 CGAN 来生成样本数据，实现对数据集规模的扩充，同时增加样本数据集的多样性。

3.2　实验环境及设备

本次仿真实验的条件生成对抗网络在训练期间学习率为固定参数 0.000 2，迭代次数为 600 次，batch-size 为 64，Adam 参数设置为：一阶矩估计的动量参数的指数衰减率 b_1 ＝0.5，二阶矩估计的动量参数的指数衰减率 b_2 ＝0.999，另外依据深度学习衰减策略，当网络训练过程中遇到损失值无法更新迭代时，需将模型网络学习率下调至原学习率的一半，同时结合普归一化和梯度惩罚对判别器进行收敛控制，确保网络模型的稳定训练，本次仿真实验在训练到第 56 轮和第 112 轮时，对网络模型学习率进行下调，调整到原始学习率的十分之一，实验环境参数如表 1 所示。

表 1　本章实验环境配置

配置构成	配置参数
编译环境	Tensorflow_GPU－1.9.0
操作系统	Windows 10
编程语言	Python3
CPU	Intel Core i5－10300H
GPU	NVIDIA GeForce GTX 1660ti
内存	16 G

3.3　评价指标

图像数据信息识别评价标准通常使用平均检测精度（mAP）[20]，mAP 的计算包括两项：精准度（Precision）计算和召回率（Recall）计算，二者的数学表达式为式（5）、式（6），Precision 和 Recall 的调和平均数使用 F_1-Score，其数学表达式为式（7）：

$$Precision = \frac{TP}{TP + FN} \tag{5}$$

$$Recall = \frac{TP}{TP + FP} \tag{6}$$

$$F_1 = \frac{2TP}{2TP + FN + FP} \tag{7}$$

其中：TP 表示图像数据信息被识别网络正确识别出非安全性异物的样本数量，FP 表示图像数据信息被识别网络错误识别出非安全性异物的样本数量，FN 表示图像数据信息中存在的异物未被识别网络正确识别出的样本数量。

3.4　实验结果与分析

仿真实验最后采用准备好的验证数据集对方法模型的精准度进行检验，验证本文方法对图像数据信息中存在的异物具有较高的识别正确度。识别结果展示如图 6 所示，需要说明的是测试集中共有样本 180 张，其中将非安全性异物类别进一步划分为重视类和警惕类，重视类主要包含一些非生命的环境障碍物，如树叶、绝缘子、车辆等。警惕类主要包含一些需要及时处置的障碍物，包括人物、塑料袋、鸟类等。当数据信息中包含警惕类非安全性异物时，需要方法模型能够快速进行识别并给出警惕报警，利于巡检人员第一时间进行确认和排查。

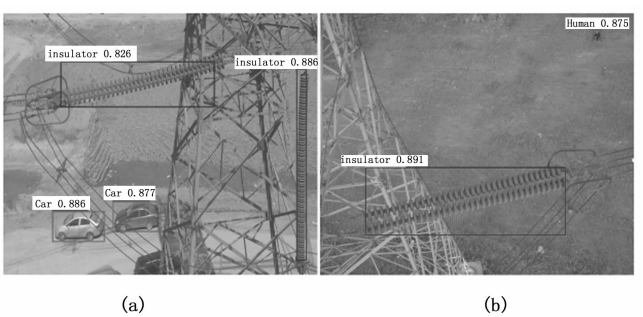

图 6　数据信息安全性识别检测结果

如图 6（a）所示，本文方法准确识别出图像数据信息

中包含警惕类异物，并且给出了所属类别为人物的概率值为 0.875，说明该图像数据信息的安全性需要得到警惕。图 6（b）是本文法规范准确识别出图像数据信息中的绝缘子，并给出所属类的概率值为 0.891，方便电力巡检人员快速对图像数据信息安全性进行判断，并对其安全工作运行状态进行评估。

本文经过多次仿真实验测试，最终得出在学习率固定为 0.000 2，并且识别方法模型训练到第 23000 轮时，本文方法的识别精准度最佳，对重视类和警惕类非安全性异物的识别结果如表 2 所示。从表 2 可以看出本文方法对大部分异物的识别正确度较高。尤其是对警惕类别中的车辆、人物、鸟类、塑料袋具有较高的识别正确度，特别是针对人物和车辆的识别指标 Recall 值得分表现优秀，可以证明本文方法对数据信息的安全性识别覆盖率较高，不易产生漏检和错检的现象。警惕性异物中鸟类事件因为具有很强的随机性和不确定性，对其及时进行安全性检测一直是电力巡检过程中的难点和重点，从表 2 结果中可以看出本文方法对鸟类的正确识别率处于次优位置，说明本文方法可以对警惕类别中的鸟类做到有效检测。但是对塑料袋异物和树叶的识别度表现欠佳，这一定程度上是因为塑料袋形状的过于多变且形状不规则，对其正确识别结果造成一定影响，而树叶作为异物识别目标，由于目标体积较小导致不易识别。本文针对塑料袋与树叶这两类异物存在不易识别且识别正确度不高的问题，采取高斯滤波法对图像进行预处理，高斯滤波法主要是对图像边缘区域的高频噪声进行过滤，可以对内容信息进行增强处理，有助于增强方法模型的泛化能力，仿真实验结果表明本文方法对先经过高斯滤波法处理后得到结果图，再对其进行数据信息安全性识别，最终结果的 AP 得分与 Recall 得分相比较无高斯滤波法处理的结果均有较明显的提升，对比结果如表 2 所示。

表 2 数据信息安全识别结果

项目		车辆	人物	绝缘子	树叶	塑料袋	鸟类
无高斯滤波处理	AP 值	0.882	0.878	0.871	0.602	0.652	0.831
	Recall 值	0.935	0.911	0.894	0.623	0.673	0.885
经过高斯滤波处理	AP 值	0.915	0.946	0.926	0.738	0.706	0.911
	Recall 值	0.933	0.971	0.941	0.742	0.739	0.946

为进一步验证本文方法采用 CGAN 生成图像数据以扩充现有数据集，实现提高数据信息安全识别目标正确率的有效性，本次实验分别使用数据扩充前和数据扩充后的数据集，同时进行 15000 轮训练后得到的测试结果对比如表 3 所示。其中原始数据集扩充前，共包含 180 张真实图像数据，经扩充后新增 360 张由 CGAN 生成的电力巡检图像数据用以扩充原始数据集规模，实验使用 40 张图像数据分别对模型进行测试，从表 3 中结果可明显看出，使用 CGAN 生成数据得到扩充后的数据集，对方法模型进行训练后，其评价指标的 Precision 值，Recall 值，F_1-score 值得分情况均有明显幅度的提升，提升率分别为 22.1%，13.8%，21.8%。证明本文使用 CGAN 对有限数据集进行扩充，从而提高方法模型对数据信息安全识别准确度的方法具有较好的实施效果。

表 3 数据集扩充识别结果

数据集	TP	FN	FP	Precision	Recall	F1
原始数据集	23	10	7	0.692	0.737	0.773
扩充后的数据集	35	3	2	0.846	0.839	0.942

电力巡检数据信息安全性检测方法之所以因其为我国电力设施承担相关安全事故检测与预警工作，所以电力巡检数据信息安全性检测方法模型需具有高可靠性与稳定性。目前在深度学习领域借助统计学思想提出，在极端情况下模型对边界值也能保持平滑、可靠的性质，被称之为鲁棒性。进一步如果一个网络模型的鲁棒性越好，意味着该模型具有三大优点：具有高精准度和多数有效性；在模型遇到较小偏差值时，模型整体性能只受到较小影响；在模型遇到较大偏差值时，模型整体性能并不会出现“灾难性”的结果；图 7 是本文方法模型在测试集上关于 Recall，Precision 的得分分布情况，从中可以看出本文法模型对于大部电力巡检图像数据信息的安全性识别得分较高，且得分分布情况趋近于正态分布，表明本文方法模型具有较强的鲁棒性，证明本文方法模型具有较高的可靠性与稳定性。

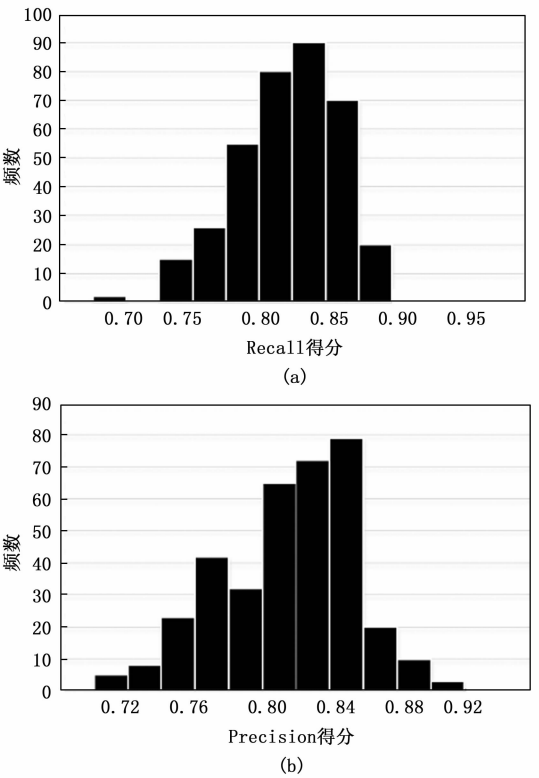

图 7 本文方法在扩充数据集上的 Recall 和 Precision 得分分布情况

4 结束语

针对电力巡检任务采集到的数据，需要进行信息安全

识别的问题，本文提出一种基于 CGAN 和 DenseNet 的数据信息安全识别方法。首先，本文使用 CGAN，在现有数据的规模基础上生成逼真的数据集，解决电力巡检任务采集数据较为困难的缺点；然后，利用 DenseNet 搭建识别网络，对数据信息的安全性进行识别，判断出异物类别，相比传统人工巡检方式，不仅可以提升工作效率，还可以节约资源；最后，通过对仿真实验，证明本文方法对数据信息的安全性具有较好的识别效果。

参考文献：

[1] 李　睿. 基于物联网的输电线路巡检机器人控制策略研究 [J]. 计算机测量与控制，2019，27 (11)：70－73，78.

[2] 赵一粟. 基于图像分割的无人机遥感影像目标提取技术 [J]. 计算机测量与控制，2021，29 (1)：179－183，205.

[3] 刘广振，张黎明，吴　东，等. 基于头戴式双目相机的智能变电站巡检巡视系统设计 [J]. 计算机测量与控制，2020，28 (2)：235－239.

[4] 周静波，郝坤坤，刘荣海，等. 基于域泛化的非均衡电力设备分/合闸 X 射线图像识别 [J]. 计算机应用，2021，41 (S2)：286－293.

[5] 陈莉波，周小华，杨　晒，等. 基于红外成像的电力施工视频监控图像目标识别算法 [J]. 激光杂志，2021，42 (9)：129－133.

[6] 张晓博. 面向电力设备与环境监控的故障多源图像识别软件开发 [D]. 南京：东南大学，2021.

[7] MIKOLAJCZYK K，SCHMID C. A performance evaluation of local descriptors [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2005，27 (10)：1615－1630.

[8] YAMAMOTO K，YAMADA K. Analysis of the infrared images to detect power lines [C] //Proceedings/TENCON. U. S. A：IEEE Press，1997，68：343－346.

[9] YAMAMOTO K，YAMADA K. Development of infrared communication controller device [J]. Shapu Giho/Sharp Technical Journal，1997，68：32－35.

[10] YU P，DONG B G，XUE Y J. Electric power tower inclination angle detection method based on SIFT feature matching [J]. Applied Mechanics&Materials，2012：236－237.

[11] CHENG F，YIN B，CHU M. Research on target recognition algorithm based on improved faster-RCNN [J]. Journal of System Simulation，2022.

[12] YI F W，XIAO C，WENYI Z，et al. Weak and small face target recognition based on MTCNN network in dynamic platform [C] //The International Conference on Cyber Security Intelligence and Analytics，Springer，Cham，2022.

[13] 何子庆，聂红玉，刘　月，等. 基于条件梯度 Wasserstein 生成对抗网络的图像识别 [J]. 计算机测量与控制，2019，27 (6)：157－162.

[14] GOODFELLOW I J，POUGET-ABADIE J，MIRZA M，et al. Generative adversarial networks [EB/OL]. (2014-9-10) [2022-3-1]. https://arxiv.org/abs/1406.2661.

[15] MIRZA M，OSINDERO S. Conditional generative adversarial nets [EB/OL]. (2014-11-6) [2022-3-8]. https://arxiv.org/abs/1411.1784.

[16] 冯　宇，席志红. 基于深度残差网络的人体行为识别算法研究 [J]. 计算机测量与控制，2022，30 (3)：251－258.

[17] HUANG G，LIU Z，WEINBERGER K Q，et al. Densely connected convolutional networks [EB/OL]. (2018-1-28) [2022-3-16]. https://arxiv.org/abs/1608.06993v5.

[18] ZHONG Z，ZHENG M，MAI H，et al. Cancer image classification based on DenseNet model [EB/OL]. (2020-11-23) [2021-4-9]. https://arxiv.org/abs/2011.11186.

[19] ZHAO L，ZHI L，ZHAO C，et al. Fire-YOLO：a small target object detection method for fire inspection [J]. Sustainability，2022，14 (5)：22－29.

[20] 赵　亮，胡　杰，刘　汉，等. 基于语义分割的深度学习激光点云三维目标检测 [J]. 中国激光，2021，48 (17)：177－189.

(上接第 239 页)

[11] 石志勋. 电子对抗干扰效果评估技术现状解析 [J]. 电子技术与软件工程，2020 (11)：108－109.

[12] 亓　亮，李圳峰，李　鹏. 电子干扰机干扰效果评估 [J]. 舰船电子对抗，2020，43 (1)：4－11.

[13] 陈　瀚，王　森. 美军电子对抗装备干扰技术及其效果研究 [J]. 数字技术与应用，2020，38 (5)：221－222.

[14] GRECOM，GINI F，FARINA A. Radar detection and classification of jamming signals belonging to a cone class [J]. IEEE Transactions on Signal Processing，2008，56 (5)：1984－1993.

[15] 陈　旭. 雷达电子对抗技术的应用 [J]. 电子技术 (上海)，2021，50 (3)：26－27.

[16] 刘　振，隋金坪，魏玺章，等. 雷达有源干扰识别技术研究现状与发展趋势 [J]. 信号处理，2017，33 (12)：1593－1601.

[17] 张　杰，陈　栋. 针对跳频电台的弹载通信干扰机干扰种类的选取与论证 [J]. 计算机与数字工程，2020，48 (5)：1091－1094.

[18] 刘　喆，王　萌. 移动通信干扰器技术发展方向初探 [J]. 保密科学技术，2017 (4)：21－24.

[19] 卫　麟. 针对 OFDM 通信系统电子对抗干扰方式的研究 [D]. 南京：东南大学，2016：16－17.

[20] 潘中彬，李　利. 超短波跳频通信仿真与抗干扰性能分析 [J]. 科技创新与应用，2022，12 (17)：15－18.

[21] 张　超. 信息化条件下短波通信抗干扰技术与应用分析 [J]. 中国信通信，2020，22 (4)：29.

[22] 赵云玲. 水声通信 OFDM 信号侦察与干扰技术研究 [D]. 哈尔滨：哈尔滨工程大学，2021.

[23] 韦　卓，黄建忠，姚德龙，等. 防空武器系统复杂干扰环境下的试验评估技术 [J]. 指挥控制与仿真，2017，39 (1)：135－138.

[24] 张学文. 差分跳频通信对抗研究 [D]. 西安：西安电子科技大学，2009.