Computer Science and Application 计算机科学与应用, 2022, 12(12), 2736-2743
Published Online December 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.1212277

Hans汉斯

施工工程现场入侵监测系统设计

金国栋，杨　钦，杨大健

中国建筑第八工程局有限公司，上海

收稿日期：2022年11月5日；录用日期：2022年12月5日；发布日期：2022年12月13日

摘　要

随着社会的快速发展，隐私性和保密性问题日渐受到人们的关注，在施工领域也不例外。工程项目的图纸资料、施工现场的进程与技术本身就带有一定的保密性，而一些特殊的工程项目如机场等则更具有防泄密和防入侵的需求。针对这种问题，提出一种针对施工人员泄密行为和施工现场防入侵的监测系统设计思路。在设计中，分别从网络入侵和场地入侵两方面来进行系统设计，并采用一种融合卷积神经网络和长短时记忆网络的混合深度学习模型，用于自动处理施工现场环境中的可能泄密行为，通过模型识别训练证明了算法的可行性。

关键词

施工现场，入侵监测，行为识别

Design of Intrusion Monitoring System for Construction Site

Guodong Jin, Qin Yang, Dajian Yang

China Construction Eighth Engineering Bureau Co., Ltd., Shanghai

Received: Nov. 5th, 2022; accepted: Dec. 5th, 2022; published: Dec. 13th, 2022

Abstract

With the rapid development of society, privacy and confidentiality issues are increasingly concerned by people, and the construction field is no exception. The drawing data of the engineering project, the process of the construction site and the technology itself have a certain degree of confidentiality, and some special engineering projects such as the airport are more anti-leak and anti-intrusion needs. In order to solve this problem, this paper puts forward a design idea of monitoring system aiming at the leakage behavior of construction personnel and the intrusion prevention of construction site. In the design, two aspects of network intrusion and site intrusion were respectively used

文章引用: 金国栋, 杨钦, 杨大健. 施工工程现场入侵监测系统设计[J]. 计算机科学与应用, 2022, 12(12): 2736-2743.
DOI: 10.12677/csa.2022.1212277

to design the system, and a hybrid deep learning model integrating convolutional neural network and short and long time memory network was used to automate the possible leakage behavior in the construction site environment. The feasibility of the algorithm was proved through model recognition training.

Keywords

Construction Site, Intrusion Detection, Behavior Recognition

1. 引言

施工现场保密性的要求主要来自三个方面：一是施工现场外围非法进入现场内；二是储存工程资料的计算机受到来自网络的入侵；三是施工场地内人员的可能泄密行为，如手机拍照，手持遥控器遥控设备拍摄，打电话等等。而目前行为识别与入侵监测两方面的研究大多是分开进行的，没有统一应用在工程施工中。因此，本文从漏缆周界入侵监测系统设计、网络防入侵系统设计以及基于融合卷积神经网络(CNN, Convolutional Neural Network)和长短时记忆网络(LSTM, Long and Short Term Memory Network)的混合深度学习模型的泄密行为识别算法等方面进行阐述。

2. 漏缆周界入侵监测系统设计

智能周界入侵监测系统的主要作用是在设防地区有非法入侵行为发生时，可以智能准确地识别入侵，并及时报警。目前市面上常用的周界入侵监测方法主要有主动红外、振动电缆、光纤入侵、漏缆入侵等。其中，铺设在防护区域地表浅层的泄露电缆周界入侵监测系统由于其系统的稳定性、强隐蔽性、多地形适应性、全天候工作等优点，受到社会广泛好评[1] [2]。

本文结合军用机场的特殊性，经过调研分析，决定采用漏缆周界入侵监测算法。漏缆周界入侵监测系统主要由发射机、接收机、一对泄露电缆、终端负载以及上位机组成，系统示意图见图 1。

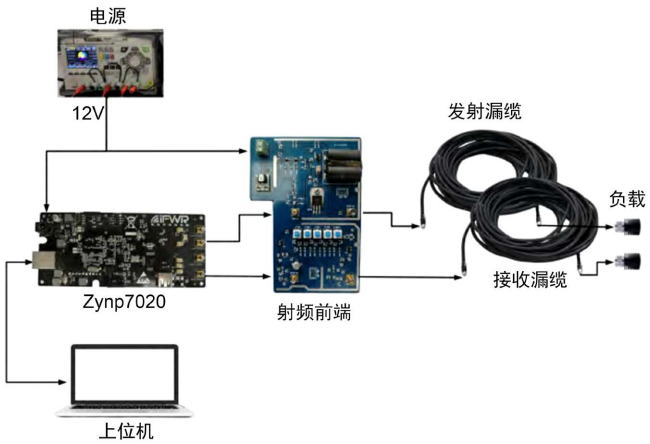

Figure 1. Leaky cable perimeter intrusion system
图 1. 漏缆周界入侵系统

本文采用一种新型报警泄露电缆作为发射、接收天线。电缆外导体采用铜塑复合带沿绝缘体纵包而成，沿电缆轴向开有连续缝隙口，特性阻抗采用 50 Ω，结构如图 2 所示。

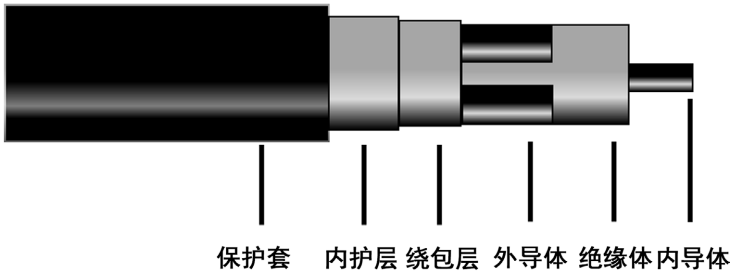

Figure 2. New alarm leak cable
图 2. 新型报警漏缆

将两根等长的新型漏缆以约 1.5 m 的间距平行铺设在浅层地表。同时，需要在漏缆末端用 50 Ω 的终端负载吸收多余信号，用以减小反射。探测信号沿着发射漏缆纵向传播，并通过泄露孔隙向外辐射，辐射信号被接收漏缆耦合接收。此时，二者之间会形成一个稳定的电磁监测场域。发射机中，由现场可编程门阵列(FPGA, Field Programmable Gate Array)产生伪随机序列，再经过二进制相移键控(BPSK, Binary Phase-Shift Keying)调制后的 BPSK 信号作为漏缆发射信号。漏缆发射信号经过转换、滤波、功率放大等操作后，最后通过导入缆注入到发射漏缆。接收机中，由接收漏缆传回来的耦合信号经过滤波、低噪声放大、相关采样等操作后，送入控制处理模块，进行相关算法计算结果，最终的探测结果在上位机中显示。

本设计采用了二相编码脉冲延时测距与人工智能模式识别相结合的方法，对入侵行为进行精准监测定位，脉冲延时测距是雷达监测系统中常用的测距方法[3]。为了在获得较大探测距离的同时，有效提高分辨率，本文使用了基于格雷码的脉冲压缩技术[4]。通过对具有良好自相关性的巴克码进行拓展，获得性能更高的格雷码。

当有人入侵电磁监测防区时，对应距离位置的电磁信号会被散射和衰减。将耦合到的回波信号和延时格雷码信号进行相关计算，即可获得一组可判断有无入侵的自相关数据，根据码元宽度将监测场域划分成不同的距离单位区域段。无入侵行为时，各个距离单元的相关幅值较低；有入侵行为时，入侵位置范围内的相关幅值会相应地变大，可以判断入侵位置的发生地点。同时，通过最高相关峰出现的距离区域段，可以对入侵位置做定位。

3. 网络入侵监测系统设计

随着计算机技术的日益发展，计算机网络在实际运行过程中面临各种安全风险问题[5]。特别是在信息技术快速发展背景下，局域网环境的计算机网络技术及安全防护问题易受到忽视，有些问题发生后甚至导致局域网环境下整体计算机设备瘫痪[6]。当今时代，建筑工程储存在计算机内的相关资料也具有保密的必要，因此有必要对局域网网络入侵监测系统进行设计。

3.1. 网络入侵监测系统硬件设计

根据入侵监测需求[7]预先拟定了 2 种硬件设计方案，一种是网络数据监测，一种是异常行为监测。综合考虑系统资源的消耗程度，以及网络负载情况，决定引用安全加速芯片[8]，借助芯片的特性提高系统的网络处理性能。将数据加密技术、身份认证技术和网络入侵监测技术集成在安全加速芯片中，其内部结构如图 3 所示。该芯片内部由密码处理模块和入侵监测处理模块组成[9] [10]。

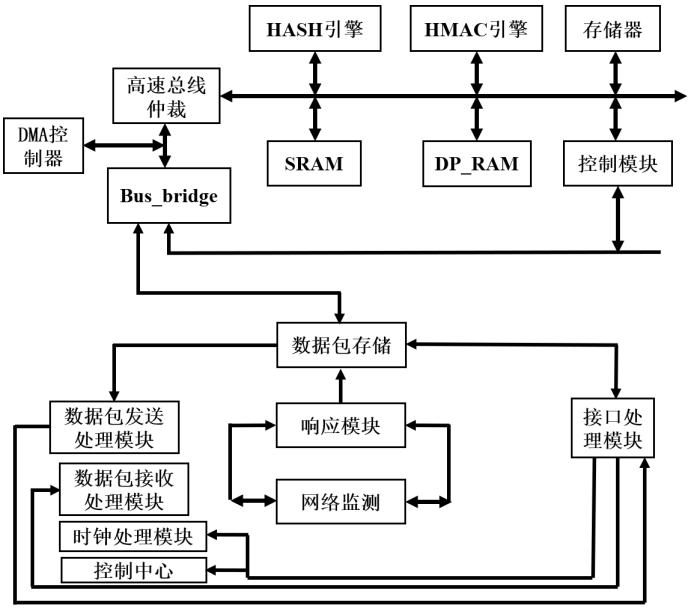

Figure 3. Internal structure diagram of safety accelerator chip
图 3. 安全加速芯片内部结构图

安全加速芯片与 CPU 之间的连接通过 DMA 实现，使用延迟低、带宽高的互联总线和通信总线连接，将加速芯片安置在 CPU 的内部高速总线 QPI 总线上，保证硬件始终保持缓存一致性的同时，使系统在监测过程中始终处于安全高速的状态[11]。通过此芯片，可以达到提高系统工作效率，克服常规网络入侵监测系统中的一些不足之处的需求。

3.2. 统计分析模块设计

统计分析模块是网络入侵监测系统的主要模块，统计分析算法流程如图 4 所示。本文统计分析的原理为，把一天分为 24 个时段，记录各时段对应的流量数据；每一时段结束后根据该时间段收集的正常流量数据对历史流量数据进行更新，如果在此过程中出现数据流量异常，则将该异常值作为历史平均流量值使用之后的数据；在对数据流量进行计算之后，如果当前流量高于历史流量，监测系统就会自动报警；通过解析模块对流量是否异常进行判断，可有效排除因其他因素导致的流量异常。

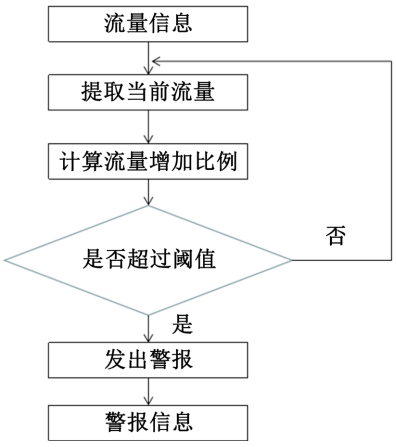

Figure 4. Basic flow of statistical algorithm
图 4. 统计算法的基本流程

4. 基于融合 CNN 和 LSTM 的混合深度学习模型的泄密行为识别算法

目前确定行为异常的传统方法主要基于观察方法，这种方法费时费力且偏于主观，由于这些限制，计算机视觉技术被广泛开发并应用于物体识别领域以及动作识别领域[12] [13] [14]。人类行为识别通常基于深度传感器的使用，以及来自视频的运动数据的收集，这些数据被重建以构建三维(3D)骨骼模型[15]。这种方法为获得准确的运动数据提供了一种有效的途径。更具体来说，它提供了记录、建模和分析执行不安全操作的人体运动的能力。然而，在 3D 环境中监测工人的定位一般需要很长的计算周期，而且深度传感器的运动线也可能受到照明灵敏度的影响。

在此背景下，采用一种融合 CNN 和 LSTM 的混合深度学习模型，用于自动识别施工现场工作环境中的可能泄密行为。混合模型利用 CNN 模型从视频中提取细化视觉特征并通过 LSTM 对学习到的特征基于时间序列进行排序，通过大型的动作视频数据库的训练，最终达到识别可能泄密行为的效果。

4.1. 技术路线

图 5 给出了所提出的动作识别方法的算法框架。深度学习模型经过训练后可以挖掘动作视频中的特征表示，这些动作视频特征是使用 CNN 和 LSTM 模型组合构建的。首先由 CNN 提取每一帧视频中的画面细部特征；然后，连续帧的图像特征输入 LSTM 进一步提取时间序列特征；最终采用 Softmax 分类器对具有空间特征和时间特征的向量进行分类，判断是否为可能的泄密行为。

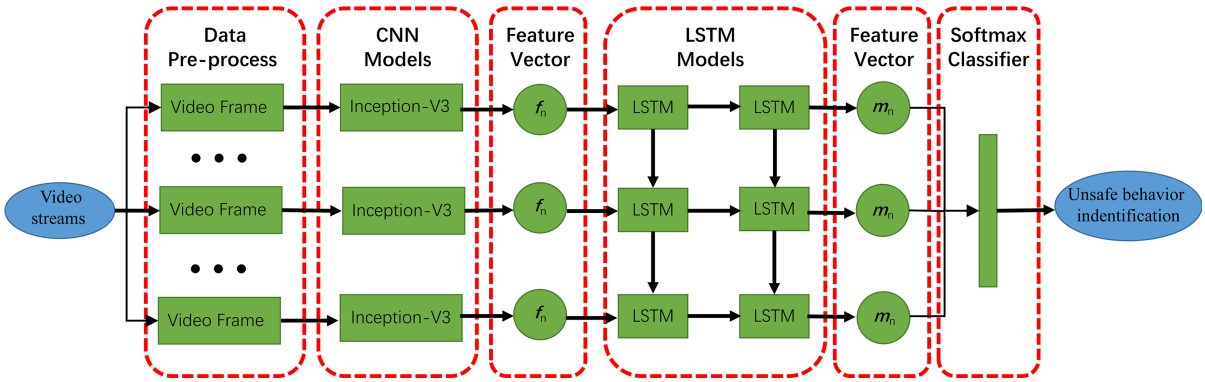

Figure 5. Network architecture diagram
图 5. 网络框架图

该模型的流程如下：

步骤 1：将每个视频流随机分割成 25 个片段作为时间切片的代表，提高训练精度。

步骤 2：将切片的视频帧作为 CNN 的原始输入，视频帧将保留图像的原始像素值。

步骤 3：根据步骤 2 获取每一帧的空间特征，一段视频可获得 25 个特征向量。将这些特征向量输入 LSTM 模型，然后训练得到整个视频的时间序列特征。

步骤 4：将步骤 3 中得到的时域特征向量输入到 Softmax 分类器中，即可得到视频分类概率，用以判断图像中是否存在可能泄密行为。

4.2. 深度卷积网络

CNN 具有多层架构，能够自动生成特征提取，方便了分类器将提取的特征向量映射到最终的预测。CNN 的基本单元及其权重可以共享，从而降低了网络复杂度，因此，网络比多层感知器(MLP)等其他类型深度网络更容易训练[16]。

本文选取了 Inception-v3 深度卷积网络经典框架，该网络曾获得 ImageNet 竞赛的冠军。在 Inception-v3 网络中，模块由 5 个均匀形状的过滤器的复合层组成，包括 1 × 1，3 × 3，5 × 5 卷积核大小和 3 × 3 平均池化操作的输出。在本文的研究中，基于 ImageNet (ImageNet 是一个设计用于视觉识别软件的大型视觉数据库)的具有预训练参数的 Inception-v3 网络直接应用于原始动作视频帧。选择最后一个池化层的 1 × 1 × 2048 输出作为空间特征。也就是说，使用预训练模型的正向传递中最后一个池化层生成的 2048 维特征。因此，模型不会通过反向传播重新训练和重复初始网络，不需要对模型进行再训练，即可以显著减少训练时间。

4.3. 长短期记忆网络

LSTM 用于处理长度为 N 的输入序列$\{x_1, x_2, \cdots, x_n\}$。LSTM 是基于循环神经网络(RNN, Recurrent Neural Network)的改进网络。LSTM 在 RNN 的基础上增加了 3 个门的逻辑控制单元：输入门、遗忘门和输出门。通过门单元的逻辑控制决定数据是否更新或是选择丢弃，克服了 RNN 权重影响过大、容易产生梯度消失和爆炸的缺点，使网络可以更好、更快地收敛，能够有效提高预测精度[17]。

在图 6 所示的混合模型中，构建了一个两层 LSTM 网络，以了解由 Inception-v3 网络的最后一个池化层生成的视频特征的时间动态。在图 7 中，$\{f_1, f_2, \cdots, f_n\}$是 Inception-v3 网络从每个视频的 n 帧中计算出的 n 个特征。因此，从一个输入序列$\{f_1, f_2, \cdots, f_n\}$，两个 LSTM 层中的存储单元将产生一个表示序列$\{m_1, m_2, \cdots, m_n\}$。然后系统通过对这个序列在整个时间段内求平均值的计算方法，得到了特征向量 F。之后将 F 输入到 Softmax 层，这样就可以识别出视频中每个输入的可能泄密行为。W 为最后一层 Softmax 的参数向量。值得注意的是，$\{f_1, f_2, \cdots, f_n\}$是由 Inception-v3 网络从每个视频的 n 帧中计算出的 n 个特征。F 表示从两个 LSTM 层学习到的加权特征$\{m_1, m_2, \cdots, m_n\}$的平均池化特征向量，W 为最后一个逻辑回归层的参数向量。

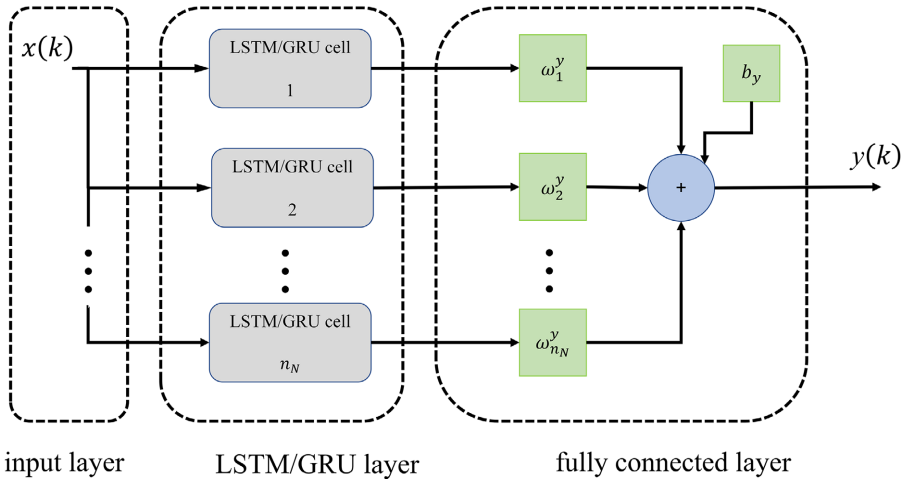

Figure 6. LSTM network architecture diagram
图 6. LSTM 网络框架细节

4.4. 模型有效性验证

手机照相是常见的可能泄密行为之一，针对此类行为，设计了一个实验来检查开发的混合深度学习模型检测此类行为的有效性。在实验中，使用摄像机收集了人员举起手机或相机照相的视频。每个视频的平均长度为 8 秒，分辨率为 1920 × 1080。部分视频素材如图 7 所示。

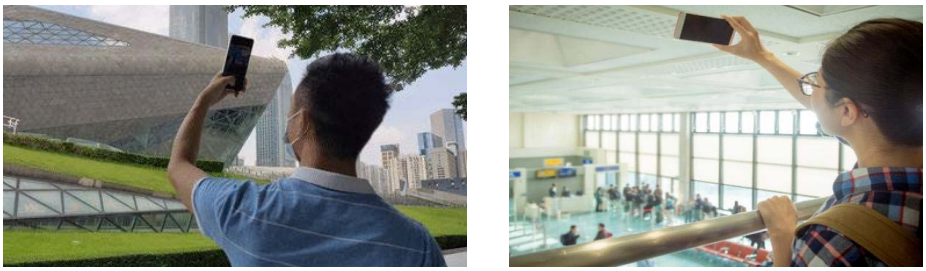

Figure 7. Video footage
图 7. 视频素材

视频素材采集处理完成后，使用 Theano 框架对深度学习模型进行训练。用配有 GeForce RTX 3060ti 显卡的台式电脑中运行。采用数据增强的方法来保证模型的拟合性，以检测和分类不安全动作。利用视频的时间连续性，在每个视频片段中随机选择不同的帧，从而生成新的训练示例。由于 CNN 模型的要求，所有原始视频帧的大小都被调整为 384 × 384。

对于每一个视频，使用 CNN 并行处理 25 个随机抽取的帧，得到它们的向量，并按时间顺序重新排列，以表示空间特征。接着，这些空间特征被用作 LTSM 网络下两层的输入，每层都有 2048 个隐藏单元，以提取 k = 2048 的空间特征。然后在 LSTM 层的输出之后进行均值池化，使用 Softmax 层来获得概率得分。

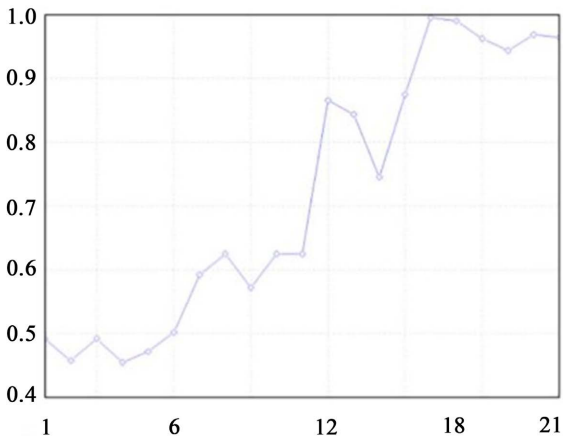

Figure 8. Mixed model accuracy changes
图 8. 混合模型准确率变化

Figure 9. Video recognition status
图 9. 视频识别情况

图 8 表示混合模型在训练中，随着训练次数的增加，分类准确率逐步上升，图 9 展示了对采集到的视频进行分类识别的效果，明显看出，混合模型能很好地识别出手机录像的动作并做出警报。对于其他具有迷惑性质的非泄密动作，例如，抬手但未拿拍摄设备、拿着其他维修工具而非拍摄设备等，也能很好地鉴别而不误检查。

5. 结论与展望

本文将施工现场防入侵作为研究目标，从漏缆周界入侵监测系统设计、网络入侵监测系统设计、泄密行为识别三方面入手进行监测系统设计。采用新型报警漏缆、二相编码脉冲延时测距与人工智能模式识别相结合的方法，提高了漏缆监测的精准性；利用了基于格雷码的脉冲压缩技术，获得性能更高的格雷码，提升了分辨率。以网络数据流量是否异常作为基本判据，建立网络入侵监测系统，对硬件芯片进行了集成改良。利用基于融合 CNN 和 LSTM 的混合深度学习模型建立泄密行为识别算法，提高了识别准确性和运行效率，并通过视频识别试验验证了其可行性。总体上实现了搭建防入侵系统的基本要求。

但行为识别的准确性与样本数据量的多少息息相关，本文只进行了部分泄密行为的识别，加上样本数量相对匮乏，故仍有问题需要进行解决，这里仅提供系统搭建的设计思路，希望为后来同类型系统提供借鉴和思考。

参考文献

[1] 王明吉, 张勇, 李玉爽, 曹文. 单主机高精度周界入侵探测报警系统[J]. 仪器仪表学报, 2006, 27(12): 1718-1720.

[2] 乔宏章, 张军. 泄漏电缆周界监视技术研究[J]. 无线电工程, 2013, 43(3): 43-46.

[3] 刘春, 文化锋, 刘太君, 等. 辐射型泄漏电缆入侵扰动检测系统仿真与实验验证[J]. 数据通信, 2017(2): 19-22.

[4] Harman, K. (2012) Outdoor Perimeter Security Sensors a Forty Year Perspective. 2012 *IEEE International Carnahan Conference on Security Technology* (*ICCST*), Newton, 15-18 October 2012, 1-9. https://doi.org/10.1109/CCST.2012.6393530

[5] 杨怀宇. 局域网环境下计算机网络安全防护技术应用研究[J]. 网络安全技术与应用, 2018(2): 28-29.

[6] 王丽琴. 局域网环境下计算机网络安全防护技术应用探讨[J]. 计算机产品与流通, 2020(4): 57.

[7] 陈志忠. 船舶监控网络入侵检测系统设计[J]. 舰船科学技术, 2018, 40(4): 178-180.

[8] 徐慧, 方策, 刘翔, 等. 改进的飞蛾扑火优化算法在网络入侵检测系统中的应用[J]. 计算机应用, 2018, 38(11): 3231-3235+3240.

[9] 李红军. 大规模网络入侵时联合云计算技术的协同预警技术研究[J]. 自动化与仪器仪表, 2017(3): 16-18.

[10] 李威, 顾海林, 黄兴. 网络被入侵后的信号检测系统设计与优化[J]. 现代电子技术, 2017, 40(3): 58-61.

[11] 程俊, 龚俭, 杨望, 等. 基于 SDN 技术的网络入侵追踪与响应系统的研究[J]. 通信学报, 2018, 39(S1): 244-250.

[12] Dang, Q., Yin, J., Wang, B., *et al*. (2019) Deep Learning Based 2d Human Pose Estimation: A Survey. *Tsinghua Science and Technology*, **24**, 663-676. https://doi.org/10.26599/TST.2018.9010100

[13] Cao, Z., Simon, T., Wei, S.-E., *et al*. (2017) Realtime Multi-Person 2d Pose Estimation Using Part Affinity Fields. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Honolulu, 21-26 July 2017, 7291-7299. https://doi.org/10.1109/CVPR.2017.143

[14] 徐晋卿, 陈唐龙, 占栋, 于龙, 冯超. 基于机器视觉的钢轨轮廓测量方法研究[J]. 传感器与微系统, 2014, 33(4): 27-30.

[15] 朱超平, 杨艺. 机器视觉中的激光智能识别技术[J]. 激光杂志, 2018, 39(8): 122-126.

[16] Noori, F.M., Wallace, B., Uddin, M.Z., *et al*. (2019) A Robust Human Activity Recognition Approach Using Openpose, Motion Features, and Deep Recurrent Neural Network. *Scandinavian Conference on Image Analysis*, Norrköping, 11-13 June 2019, 299-310. https://doi.org/10.1007/978-3-030-20205-7_25

[17] Suzuki, S., Amemiya, Y. and Sato, M. (2019) Enhancement of Gross-Motor Action Recognition for Children by CNN with OpenPose. *IECON* 2019-45*th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, 14-17 October 2019, 5382-5387. https://doi.org/10.1109/IECON.2019.8927828