e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2021. № 3
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2021. № 3

UDC 004.056

AN INTELLIGENT MODEL BASED ON DEEP TRANSFER LEARNING FOR DETECTING ANOMALIES IN CYBER-PHYSICAL SYSTEMS

Sukhostat L. V. – PhD, Associate Professor, Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan.

ABSTRACT

Context. The problem of detecting anomalies from signals of cyber-physical systems based on spectrogram and scalogram images is considered. The object of the research is complex industrial equipment with heterogeneous sensory systems of different nature.

Objective. The goal of the work is the development of a method for signal anomalies detection based on transfer learning with the extreme gradient boosting algorithm.

Method. An approach based on transfer learning and the extreme gradient boosting algorithm, developed for detecting anomalies in acoustic signals of cyber-physical systems, is proposed. Little research has been done in this area, and therefore various pre-trained deep neural model architectures have been studied to improve anomaly detection. Transfer learning uses weights from a deep neural model, pre-trained on a large dataset, and can be applied to a small dataset to provide convergence without overfitting. The classic approach to this problem usually involves signal processing techniques that extract valuable information from sensor data. This paper performs an anomaly detection task using a deep learning architecture to work with acoustic signals that are preprocessed to produce a spectrogram and scalogram. The SPOCU activation function was considered to improve the accuracy of the proposed approach. The extreme gradient boosting algorithm was used because it has high performance and requires little computational resources during the training phase. This algorithm can significantly improve the detection of anomalies in industrial equipment signals.

Results. The developed approach is implemented in software and evaluated for the anomaly detection task in acoustic signals of cyber-physical systems on the MIMII dataset.

Conclusions. The conducted experiments have confirmed the efficiency of the proposed approach and allow recommending it for practical use in diagnosing the state of industrial equipment. Prospects for further research may lie in the application of ensemble approaches based on transfer learning to various real datasets to improve the performance and fault-tolerance of cyber-physical systems.

KEYWORDS: anomaly detection, acoustic signal, transfer learning, spectrogram, scalogram, cyber-physical system.

ABBREVIATIONS

XGBoost is an extreme gradient boosting;

AUC is the area under the receiver operating characteristic curve;

CPS is a cyber-physical system;

SPOCU is a scaled polynomial constant unit;

PCA is a principal component analysis;

MIMII is a malfunctioning industrial machine investigation and inspection;

LOF is a local factor outlier;

GMM is a Gaussian mixture model;

OC-SVM is a one-class support vector machine;

STFT is a short-time Fourier transform;

CNN is a convolutional neural network.

NOMENCLATURE

γ is the minimum loss reduction needed for splitting;

λ is a regularization term;

X is a time-frequency signal representation;

F is the number of frequency bins;

T is the time dimension;

x_i is a signal block;

l is the length of the feature vector;

σ is a window function;

$\Theta(\omega, \tau)$ is the Fourier transform;

υ is the loss value of the XGBoost algorithm;

$G(x)$ is an activation function;

$\widetilde{y}_i$ is an objective optimization function;

K is the number of decision trees;

ϕ_k is an independent tree with leaf scores,

Φ is the space of the regression tree;

Ω is a regularization term.

INTRODUCTION

An abnormal state of a cyber-physical system (CPS) can be caused by faulty components, temporary failures, misconfiguration, cyberattacks, or their combination [1, 2]. An adversary intervenes in CPS to manipulate the readings of sensors or actuators, leading to abnormal system operation.

Anomaly detection in an industrial scenario is essential because undetected failures can lead to critical damage. Early detection of anomalies can improve the reliability of fault-prone industrial equipment and reduce operating and maintenance costs.

The development of Industry 4.0 has led to new technologies for efficient and reliable monitoring of such systems. Thus, modern CPSs include devices that form a multi-sensor configuration. These systems simplify the data collection process, resulting in the availability of large datasets. Consequently, there has been an increase in the development of data mining methods for detecting anomalies [3].

DOI 10.15588/1607-3274-2021-3-11

The classical approach to such problems usually involves signal processing techniques that extract useful information from sensor data.

The object of study is complex industrial equipment with heterogeneous sensory systems of various nature. For this purpose, preliminary data processing is required to extract the most informative features [4]. It is usually a very time-consuming task that requires expert knowledge.

The subject of study is methods for detecting anomalies in industrial equipment signals based on transfer learning. Images of signal spectrogram and scalogram are reviewed for a more accurate classification of equipment failures. The SPOCU (scaled polynomial constant unit) activation function [5] is considered to improve the accuracy of the proposed approach. The XGBoost algorithm is applied because it has high performance and requires little computational resources at the training stage.

The purpose of the work is to use transfer learning in combination with the XGBoost algorithm to improve the accuracy of detecting an abnormal state from acoustic signals of CPS.

1 PROBLEM STATEMENT

Suppose we are given an acoustic signal that has a time-frequency representation $X \in R^{F \times T}$, where T is the time dimension, and F is the number of frequency bins. For a given signal dataset, it is necessary to find the function $F : X \to R$ such that $F(X)$ is higher for abnormal samples than for normal operation recordings. The acoustic signal is split into fragments using a sliding window $x_i \in R^{\tau \times T}$ ($\tau < T$). Here it is proposed to extract the l-dimensional feature vector using a feature extractor for each x_i. A pre-trained deep neural network is considered a feature extractor. Then some anomaly detection algorithm F is trained on all features from the fragments of the dataset $\Lambda = \{X_j \in R^{F \times T}\}_{j=1}^{N}$.

2 REVIEW OF THE LITERATURE

The detection of anomalies in industrial equipment is becoming an important area of research. The difficulty here is to obtain information from several sensors that differ in their specific acoustic properties [6]. Researchers propose new methods and expand existing algorithms for detecting industrial equipment faults [6–13].

Morita et al. [7] proposed principal component analysis (PCA) with local factor outlier (LOF) and Gaussian mixture model (GMM) to detect abnormal sounds in the presence of limited computing resources and a small dataset.

Paper [8] described an approach that combines pre-trained OpenL3 embeddings with the reconstruction error of an interpolation autoencoder using GMM as the final predictor. The parameters were set individually for each machine using the results from the development set.

Michau and Fink [9] developed an architecture for learning a meaningful and sparse representation of high-frequency signals. They combined both the wavelets theory and deep learning for classification and anomaly detection tasks.

The application of autoencoder deep learning architectures for unsupervised acoustic anomaly detection based on Dense and convolutional neural networks (CNN) was considered in [10]. The energy features of the mel-spectrogram were extracted from the raw sounds. Several preliminary experiments were conducted to tune the autoencoder hyperparameters.

Tiwari et al. [11] proposed an ensemble of two systems capable of recording anomalous system behavior. In the first system, an outlier detection method based on the nearest neighbor search was proposed. In the second system, *i*-vectors and GMM are applied for anomaly detection. The negative log-likelihood is used as its anomaly scores.

OutlierNets, a family of very compact deep convolutional autoencoder architectures adapted for real-time acoustic anomaly detection, were proposed [12]. It has extremely low complexity and matches or exceeds large convolutional autoencoder architecture by AUC (area under the receiver operating characteristic curve) exhibiting microsecond scale latency on embedded hardware.

The efficiency of acoustic anomaly detection based on image transfer learning was studied [13]. The authors considered various deep neural models. Results showed that features extracted with ResNet18 and ResNet34 with GMM and OC-SVM (one-class support vector machine) achieved the best average AUC. It confirmed that the image-based features with transfer learning models might achieve competitive results in acoustic anomaly detection.

The following conclusions can be drawn summarising the analysis of the current research state in detecting anomalies from industrial facilities acoustic signals:

1) A small amount of work was focused on transfer learning for feature extraction and failure detection in industrial machines.

2) All the functionality of deep neural networks is not taken into account.

All this confirms the relevance of this study.

This paper proposes a new method for the automatic detection of acoustic signal anomalies based on transfer learning. The signal spectral information is considered as input data for the proposed model. The addition of the XGBoost algorithm improves the accuracy of CPS fault detection. Experiments on a real MIMII (malfunctioning industrial machine investigation and inspection) dataset have shown the effectiveness of the proposed approach and can help experts diagnose equipment malfunctions.

3 MATERIALS AND METHODS

The paper proposes an approach to detecting machine signal anomalies using transfer learning. Transfer learning uses weights from a deep neural model, pre-trained on a large dataset. It can be applied to a small dataset, providing convergence without overfitting.

The proposed approach to detecting machine signal anomalies from images using transfer learning consists of the following steps: pre-processing, feature extraction

DOI 10.15588/1607-3274-2021-3-11

using a deep neural network, feature fusion, and classification based on the XGBoost algorithm (Fig. 1).

The considered signals are pre-divided into cells of 128 samples with 64 samples overlap. A scalogram based on a wavelet transform and a spectrogram based on a short-term Fourier transform are extracted from the signals (STFT). STFT splits the signal into several overlapping blocks, multiplying them by the Hanning window function:

$$\Theta(\omega,\tau)=\int_{-\infty}^{+\infty}\theta(t)\sigma(t-\tau)e^{-i2\pi\omega t}dt\,, \qquad (1)$$

where σ is a window function.

And the Morlet wavelet is considered in the wavelet transformation to obtain more informative images [14]:

$$\psi(t)=e^{-\beta^2t^2/2}\cos(\pi t)\,, \qquad (2)$$

where β is a parameter that controls the shape of the mother wavelet.

Acquisition of the scalogram and spectrogram images is performed in parallel. Visual representations (RGB) of 128x128x3 size are then sent to a deep neural network.

Since deep learning models are trained on large datasets of various images, they can be applied to anomalies detection in signals from industrial facilities. Each of the model layers is responsible for different image features.

In this paper, in order to extract features from spectrogram and scalogram images, the following pre-trained deep neural networks are considered: Xception [15], MobileNet [16], DenseNet-121 [17] and InceptionV3 [18].

The MobileNet model is a small network that contains depth-separable convolutions and improves recognition performance [16]. The InceptionV3 network includes parallel convolutional layers that are then combined to produce a result [18, 19]. The Xception network is a linear set of residual convolutional layers [15, 20]. The summation operation speeds up the transition from one model layer to another [21]. The considered DenseNet model is used to collect information from all levels of the network and transfer it to subsequent levels when there is not enough data for training [17].

The fully connected layer was treated as a feature vector using a pre-trained model. The results are combined to extract information about various characteristics and reduce recognition errors. Thus, the total size of the feature vector is 1x1024.

In this work, SPOCU [5] is considered in the proposed model as an activation function in hidden layers to improve the accuracy of anomaly detection in image-based signals and is calculated as follows:

$$G(x)=\rho H\left(\frac{x}{\zeta}+\xi\right)-\rho H(\xi)\,, \qquad (3)$$

where $\xi\in(0,1)$, $\rho,\zeta>0$ and

$$H(x)=\begin{cases}r(c), & x\ge c\\ r(x), & x\in[0,c)\\ 0, & x<0\end{cases}\,, \qquad (4)$$

with $r(x)=x^3(x^5-2x^4+2)$ and $1\le c<\infty$. According to (3), here $c=\infty$, $\rho=3.0937$, $\xi=0.6653$ and $\zeta=4.437$.

Then the resulting feature vector is fed to the XGBoost classifier, which was proposed by Chen et al. in 2016 [22]. XGBoost is a regression tree that supports the classification task. The basis of the algorithm is to optimize the value of the objective function. In this case, the objective optimization function is defined as follows:

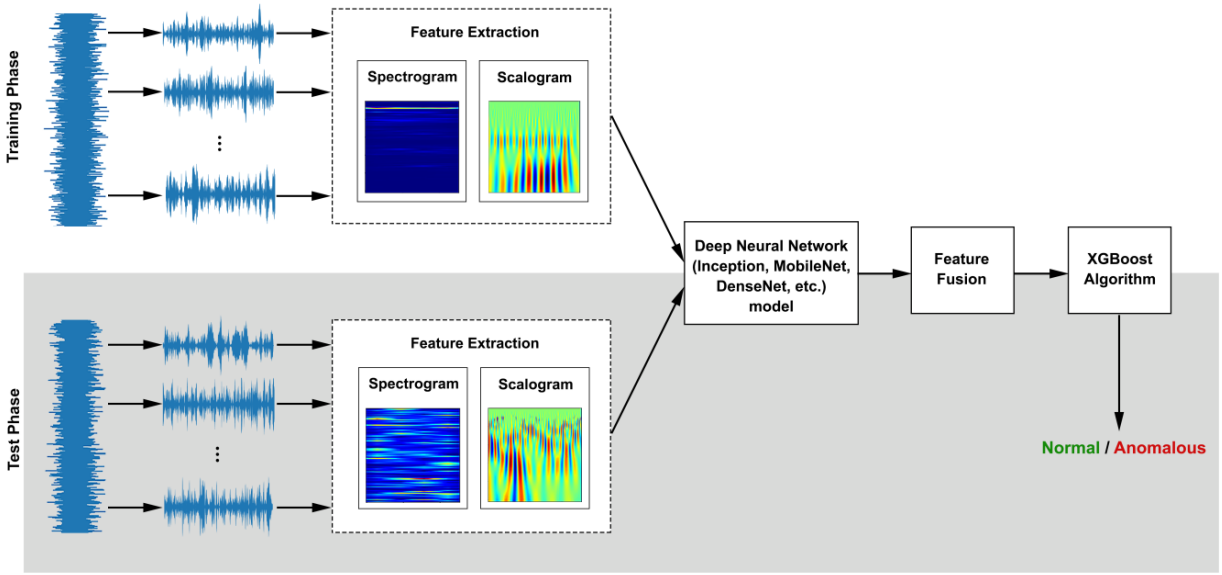

Figure 1 – Flowchart of the proposed approach

DOI 10.15588/1607-3274-2021-3-11

$$\widetilde{y}_i = \sum_{k=1}^{K} \phi_k(x_i), \quad \phi_k \in \Phi, \tag{5}$$

where K is the number of decision trees, ϕ_k is an independent tree with leaf scores, Φ is the space of the regression tree. In this case, the loss function is given by the following equation:

$$L(\phi_t) = \sum \upsilon(\widetilde{y}_i, y_i) + \sum \Omega(\phi_t), \tag{6}$$

where υ is the loss value of the XGBoost algorithm, $\widetilde{y}_i$ is the predicted output, Ω is a regularization term that prevents overfitting (7).

$$\Omega(\phi) = \gamma K + \frac{1}{2}\lambda \|w\|^2, \tag{7}$$

where K is the number of leaf nodes, w is the score on each leaf, γ and λ are constants to control the degree of regularization.

Thus, we get the following:

$$L(\phi_t) \approx \sum_{j=1}^{T} \left[\left(\sum_{i \in I_j} g_i \right) w_j + \frac{1}{2} \left(\sum_{i \in I_j} h_i + \lambda \right) w_j^2 \right] + \gamma K. \tag{8}$$

where g_i is the first derivative, and h_i is the second derivative of loss function, respectively.

For the XGBoost method, the learning rate is 0.001, number of trees to fit 100, maximum tree depth 6, $\gamma = 0$ and $\lambda = 1$.

4 EXPERIMENTS

This section provides the experimental dataset description, the evaluation metrics, and the experimental results to evaluate the proposed approach based on transfer learning.

The dataset of CPS under normal and abnormal operating conditions is considered to evaluate the proposed approach [23]. The audio dataset was collected using a circular microphone array consisting of eight separate microphones as 16-bit audio signals with a sampling rate of 16 kHz [23]. It contains eight separate channels for each segment. The MIMII dataset contains the sound of four different machine types: valves, pumps, fans, and sliders. For each type of machine, different real anomalous scenarios were considered: pollution, leakage, rotating imbalance, rail damage, etc. MIMII also contains data for four machine IDs (00, 02, 04, and 06). Different signal-to-noise ratio levels (6 dB, 0 dB, and −6 dB) were considered in the dataset. It consists of 26.092 "normal" sound segments and 6,065 abnormal sound segments.

The "normal" and abnormal signatures for all machine types in the time domain of the MIMII dataset are shown in Fig. 2 ((a) – (d)) and Fig. 2 ((e) – (h)), respectively.

STFT spectrogram and scalogram based on wavelet transform for fans, pumps, sliders, and valves are shown in Fig. 3 and 4, respectively.

Performance evaluation of the proposed model is based on the following metrics: precision, recall, and F-measure.

The precision measure determines as the number of objects classified as positive that are truly positive:

$$Precision = \frac{TP}{TP + FP}. \tag{9}$$

where TP defines true positive values, TN are true negative values, FP are false positive values, and FN are false negative values.

The recall measure is used to determine the part of the positive samples selected by the classifier:

$$Recall = \frac{TP}{TP + FN}. \tag{10}$$

F-measure combines the recall and precision metrics:

$$F - measure = \frac{2 \times Recall \times Precision}{Recall + Precision}. \tag{11}$$

All considered metrics are widely used performance indicators in machine learning [24].

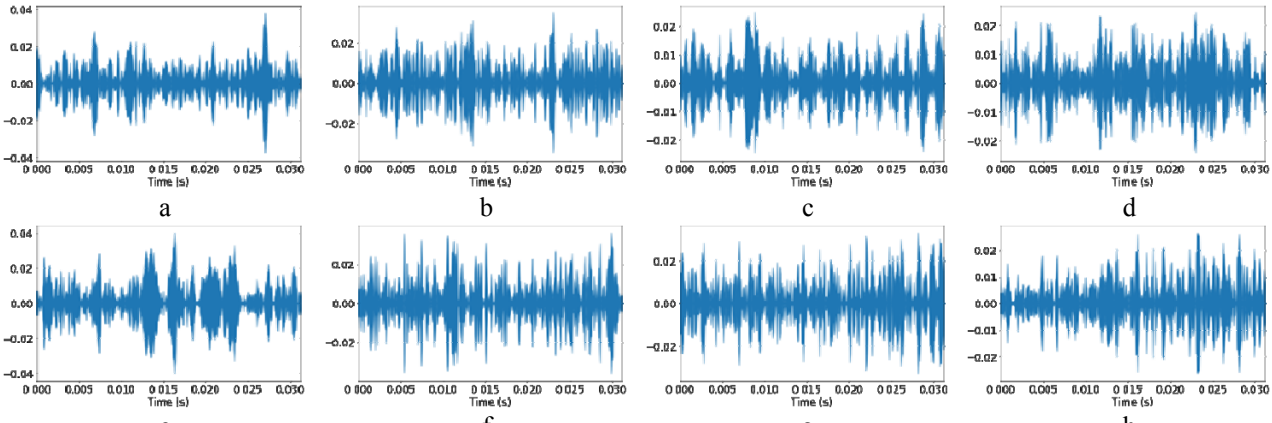

Figure 2 – Waveforms of normal ((a)–(d)) and abnormal operation ((e)–(h)) for four considered machines:
a, e – Fan; b, f – Pump; c, g – Slider; d, h – Valve

DOI 10.15588/1607-3274-2021-3-11

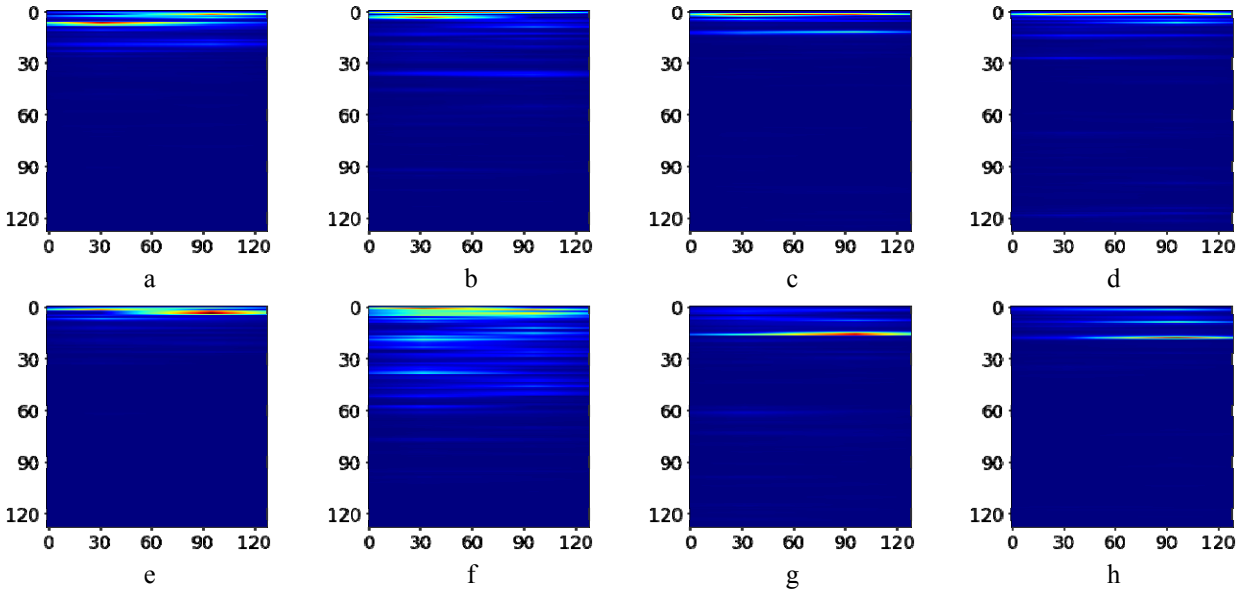

Figure 3 – Short-time Fourier transform spectrogram of the four considered machines (ID: 00) under normal ((a)–(d)) and anomalous ((e)–(h)) conditions at –6dB SNR:
a, e – Fan; b, f – Pump; c, g – Slider; d, h – Valve

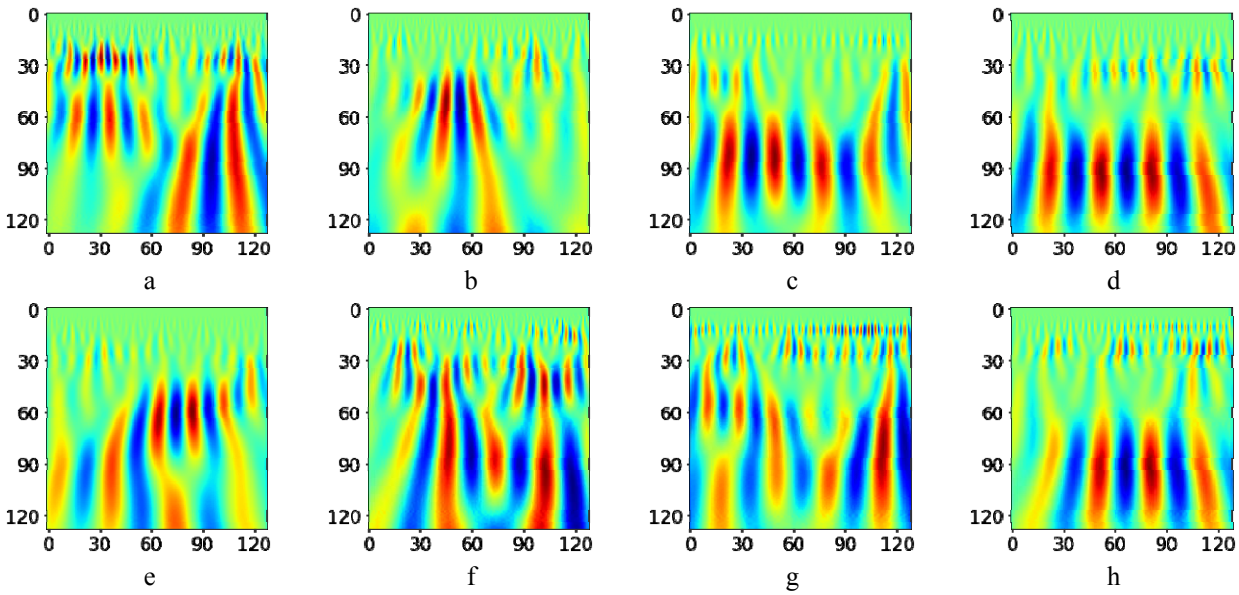

Figure 4 – Continuous wavelet transform scalogram of the four considered machines (ID: 00) under normal ((a)–(d)) and anomalous ((e)–(h)) conditions at –6dB SNR:
a, e – Fan; b, f – Pump; c, g – Slider; d, h – Valve

5 RESULTS

In this paper, the experiments are conducted in Python 2.7.13 using various libraries, including Tensorflow, Librosa, and Keras. Intel Xeon (R) CPU X5670 @ 2.93GHz * 24 with 24 GB of RAM machine was used.

This study analyses and compares various deep learning models (such as Xception, Inception, DenseNet, and MobileNet). They are trained on the MIMII dataset and applied to feature extraction from spectrogram and scalogram. Recall, Precision, and F-measure were considered as evaluation metrics.

Table 1 – Performance evaluation of the proposed approach

Model	Metric	Machine			
		Fan	Pump	Slider	Valve
Inception+ XGBoost	Recall	87.0	95.0	98.0	100
	Precision	89.1	87.9	100	94.3
	F-measure	92.3	90.6	98.1	96.3
Xception+ XGBoost	Recall	100	88.0	98.0	100
	Precision	84.2	100	100	92.6
	F-measure	96.8	92.8	98.1	95.3
Mobilenet+ XGBoost	Recall	96.0	88.0	94.0	100
	Precision	78.7	95.7	100	96.2
	F-measure	92.0	90.9	96.1	97.2
Densenet+ XGBoost	Recall	99.9	96.0	98.0	100
	Precision	87.0	100	100	97.1
	F-measure	98.2	97.1	98.1	97.7

DOI 10.15588/1607-3274-2021-3-11

Hyperparameters optimization was performed using cross-validation. The combination of parameters was chosen based on the lowest training loss and the highest accuracy. The best performance of the model was observed with a batch size equal to 32. Also, the evaluation of the learning rate was performed on different values. The accuracy of the model decreased with the increasing learning rate. It is important to note that all four considered models achieved high accuracy by decreasing the learning rate to 0.001.

The results of the experiments are shown in Table 1. Comparison of various deep neural models showed that Densenet+XGBoost outperformed the other considered models in detecting anomalies from machine signals according to the F-measure metric. Models Inception+XGBoost, Xception+XGBoost, and Densenet performed well for a Slider machine using recall and precision metrics. Even though all models showed the best results in terms of recall for a Valve-type machine, they were inferior to Densenet+XGBoost according to precision and F-measure.

Thus, the Densenet+XGBoost model turned out to be the best. In order to evaluate its performance, it was compared with such models as Alexnet [13], ResNet18 [13], ResNet34 [13], SqueezeNet [13], IAEO3_opt [8] and PCA+LOF+GMM [7] for all types machines and machine IDs (00, 02, 04 and 06) according to the AUC metric (Table 2). Densenet+XGBoost showed the best performance of all machine types, resulting in average AUCs of 93.1%, 97.3%, 98.4%, and 93% for fan, pump, slider, and valve, respectively.

Table 2 – Comparison of mean AUC of different transfer learning models on the MIMII dataset

Machine / Model	Fan				Pump				Slider				Valve			
	00	02	04	06	00	02	04	06	00	02	04	06	00	02	04	06
AlexNet+GMM [13]	57.7	61.7	53.9	94.5	84.1	70.8	81.6	66.0	98.3	80.9	61.4	57.5	60.2	69.2	59.9	53.5
AlexNet+OC-SVM [13]	51.0	73.1	59.7	93.2	77.5	56.4	81.1	60.1	96.2	81.4	53.6	56.5	61.6	73.6	48.3	48.9
ResNet18+GMM [13]	62.6	64.1	59.3	94.4	84.5	71.3	84.0	68.3	99.1	85.8	68.8	65.6	58.3	73.3	60.2	56.9
ResNet34+GMM [13]	58.7	65.6	57.0	90.9	78.4	66.8	87.9	63.2	99.6	90.4	82.5	69.1	73.0	79.1	60.1	61.9
ResNet34+OC-SVM [13]	50.1	67.4	57.5	83.0	64.9	51.5	81.2	60.2	96.8	85.0	71.4	64.3	75.6	77.8	64.3	53.1
SqueezeNet+OC-SVM [13]	55.6	64.8	46.2	78.8	86.7	49.4	88.4	62.3	99.2	81.5	59.4	71.6	69.0	71.3	53.1	58.2
Morita et al. (2020) [7]	67.4	87.1	79.3	96.2	72.5	70.4	94.2	87.1	97.7	75.9	96.9	94.2	99.4	91.8	94.2	80.7
IAEO3_opt [8]	65.5	83.3	71.4	98.1	84.4	77.8	98.0	78.9	95.9	84.0	97.9	85.9	100	99.7	99.8	98.8
Densenet+XGBoost	93.6	95.1	87.9	95.9	97.7	96.9	97.8	97.1	99.6	99.5	97.2	97.3	93.8	95.7	93.9	88.6

6 DISCUSSION

The proposed model made it possible to achieve a significant improvement in anomaly detection according to the data of machine sensors according to AUC 95.45%, compared to the previously proposed models [7, 8, 10, 13]. Densenet+XGBoost improved by about 8% over the PCA model [7] applied to the log spectrogram of the audio signal combined with LOF and GMM on the MIMII dataset. Grollmisch et al. [8] proposed a method combining OPENL3 embeddings and interpolation autoencoder (IAEO3_opt) for acoustic signals anomaly detection. Compared to the IAEO3_opt model, the Densenet+XGBoost model has improved by approximately 7% [8]. Densenet+XGBoost gave comparable results (AUC 95.5%) on the reviewed MIMII dataset. Coelho et al. [10] used CNN and Dense network in combination with an autoencoder for the task of unsupervised acoustic anomaly detection, where the results averaged 72.0%, 73.1%, 91.8%, and 78.9% for the fan, pump, slider, and valve, respectively. The accuracy of the proposed method is 93.1% for the fan, 97.3% for the pump, 98.4% for the slider, and 93.0% for the valve, which is significantly higher than the above result. The results on the MIMII dataset showed that the Densenet + XGBoost model outperformed other approaches. The 10-fold-cv results demonstrated the reliability and robustness of the proposed model.

CONCLUSIONS

The urgent problem of detecting anomalies is solved based on acoustic signals from industrial equipment.

The scientific novelty of obtained results is that a transfer learning approach with the XGBoost classifier is proposed. There has been little research done in this area, and therefore studies are underway on various pre-trained deep neural model architectures to detect anomalies. The spectrogram and scalogram of the acoustic signal were considered as input data for the proposed architecture. The SPOCU activation function [5] was used to improve the accuracy of the proposed approach.

The practical significance of the obtained results is that experiments on a real MIMII dataset showed the effectiveness of the proposed approach and can help experts in diagnosing equipment malfunctions. Comparison with other known methods proves the superiority of Densenet+XGBoost in terms of anomaly detection accuracy.

Prospects for further research are in the development of ensemble approaches based on transfer learning using other real datasets to improve the performance and fault-tolerance of CPS.

DOI 10.15588/1607-3274-2021-3-11

REFERENCES

1. Langner R. Stuxnet: dissecting a cyberwarfare weapon, *IEEE Security & Privacy*, 2011, Vol. 9, No. 3, pp. 49–51. DOI: 10.1109/MSP.2011.67
2. Ahmed C. M., Zhou J. Challenges and opportunities in CPS security: a physics-based perspective, *IEEE Security & Privacy*, 2020, Vol. 18, No. 6, pp. 14–22. DOI: 10.1109/MSEC.2020.3002851
3. Ahmed C. M., Murguia C., Ruths J. Model-based attack detection scheme for smart water distribution networks, *Computer and Communications Security: 17th ACM ASIA Conference, Abu Dhabi, 2–6 April 2017, proceedings.* 2017, pp. 101–113. DOI: 10.1145/3052973.3053011
4. Canizo M., Triguero I., Conde A., Onieva E. Multi-head CNN–RNN for multi-time series anomaly detection: an industrial case study, *Neurocomputing*, 2019, Vol. 363, pp. 246–260. DOI: 10.1016/j.neucom.2019.07.034
5. Kiseľák J., Lu Y., Švihra J., Szépe P., Stehlík M. "SPOCU": scaled polynomial constant unit activation function, *Neural Computing and Applications*, 2021, No. 33, pp. 3385–3401. DOI: 10.1007/s00521-020-05182-1
6. M. R. G. R., Ahmed C. M., Mathur A. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation, *Cybersecurity*, 2021, Vol. 4, No. 27, pp. 1–12. DOI: 10.1186/s42400-021-00095-5
7. Morita K., Yano T., Tran K. Q. Anomalous sound detection by using local outlier factor and Gaussian mixture model, 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Morita_51_t2.pdf
8. Grollmisch S., Johnson D., Abeßer J., Lukashevich H. IAEO3 – combining OpenL3 embeddings and interpolation autoencoder for anomalous sound detection, 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Grollmisch_15_t2.pdf
9. Michau G., Fink O. Fully learnable deep wavelet transform for unsupervised monitoring of high-frequency time series, 2021 [Electronic resource]. Access mode: https://arxiv.org/pdf/2105.00899.pdf
10. Coelho G., Pereira P., Matos L., Ribeiro A., Nunes E., Ferreira A., Cortez P., Pilastri A. Deep dense and convolutional autoencoders for machine acoustic anomaly detection, *Artificial Intelligence Applications and Innovations: 17th IFIP International Conference, Hersonissos, 25–27 June 2021: proceedings*. Cham, Springer, 2021, pp. 337–348. DOI: 10.1007/978-3-030-79150-6_27
11. Tiwari P., Jain Y., Avila A., Monteiro J., Kshirsagar S., Gaballah A., Falk T. H. Modulation spectral signal representation and i-vectors for anomalous sound detection, 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Tiwari_84_t2.pdf
12. Abbasi S., Famouri M., Shafiee M. J., Wong A. OutlierNets: highly compact deep autoencoder network architectures for on-device acoustic anomaly detection, *Sensors*, 2021, Vol. 21, No. 14, pp. 1–12. DOI: 10.3390/s21144805
13. Müller R., Ritz F., Illium S., Linnhoff-Popien C. Acoustic anomaly detection for machine sounds based on image transfer learning, *Agents and Artificial Intelligence, 13th International Conference, 4–6 February 2021, proceedings*. pp. 49–56. DOI: 10.5220/0010185800490056
14. Lin J., Qu L. Feature Extraction based on Morlet wavelet and its application for mechanical fault diagnosis, *Journal of Sound and Vibration*, 2000, Vol. 234, No. 1, pp. 48–135. DOI: 10.1006/jsvi.2000.2864
15. Chollet F. Xception: deep learning with depthwise separable convolutions, *Computer Vision and Pattern Recognition: 30th IEEE Conference. Honolulu, 21–26 July 2017, proceedings*, pp. 1800–1807. DOI: 10.1109/CVPR.2017.195
16. Sandler M., Howard A., Zhu M., Zhmoginov A., Chen L. C. MobileNetV2: inverted residuals and linear bottlenecks, *Computer Vision and Pattern Recognition: IEEE/CVF Conference, Salt Lake City, 18–23 June 2018: proceedings*. pp. 4510–4520. DOI: 10.1109/CVPR.2018.00474
17. Huang G., Liu Z., van der Maaten L., Weinberger K. Q., Densely connected convolutional networks, *Computer Vision and Pattern Recognition, 30th IEEE Conference. Honolulu, 21–26 July 2017, proceedings*, pp. 2261–2269. DOI: 10.1109/CVPR.2017.243
18. Szegedy C., Vanhoucke V., Ioffe S., Shlens J., Wojna Z. Rethinking the inception architecture for computer vision, *Computer Vision and Pattern Recognition, IEEE Conference. Las Vegas, 27–30 June 2016, proceedings*. pp. 2818–2826. DOI: 10.1109/CVPR.2016.308
19. Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A. Going deeper with convolutions, *Computer Vision and Pattern Recognition, IEEE Conference. Boston, 7–12 June 2015, proceedings*, pp. 1–9. DOI: 10.1109/CVPR.2015.7298594
20. Kassani S. H., Kassani P. H., Khazaeinezhad R., Wesolowski M. J., Schneider K. A., Deters R. Diabetic retinopathy classification using a modified Xception architecture, *Signal Processing and Information Technology, IEEE International Symposium, Ajman, 10–12 December 2019, proceedings*, pp. 1–6. DOI: 10.1109/ISSPIT47144.2019.9001846
21. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition, *Computer Vision and Pattern Recognition: IEEE Conference, Las Vegas, 27–30 June 2016: proceedings*. pp. 770–778. DOI: 10.1109/CVPR.2016.90
22. Chen T., Guestrin C. XGBoost: a scalable tree boosting system, *Knowledge Discovery and Data Mining, 22nd ACM SIGKDD International Conference. San Francisco, 13–16 August 2016, proceedings*, pp. 785–794. DOI: 10.1145/2939672.2939785
23. Purohit H., Tanabe R., Ichige K., Endo T., Nikaido Y., Suefusa K., Kawaguchi Y. MIMII dataset: sound dataset for malfunctioning industrial machine investigation and inspection, *Detection and Classification of Acoustic Scenes and Events, 4th Workshop. New York, 25–26 October 2019, proceedings*, pp. 209–213. DOI: 10.33682/m76f-d618
24. Ferri C., Hernández-Orallo J., Modroiu R. An experimental comparison of performance measures for classification, *Pattern Recognition Letters*, 2009, Vol. 30, No. 1, pp. 27–38. DOI: 10.1016/j.patrec.2008.08.010

Received 30.06.2021.
Accepted 13.08.2021.

DOI 10.15588/1607-3274-2021-3-11

УДК 004.056

ІНТЕЛЕКТУАЛЬНА МОДЕЛЬ ВИЯВЛЕННЯ АНОМАЛІЙ У КІБЕРФІЗІЧНИХ СИСТЕМАХ НА ОСНОВІ ГЛИБОКОГО ТРАНСФЕРНОГО НАВЧАННЯ

Сухостат Л. В. – канд. техн. наук, доцент, Інститут інформаційних технологій, Національна академія наук Азербайджану, Баку, Азербайджан.

АНОТАЦІЯ

Актуальність. Розглянуто задачу виявлення аномалій сигналів кіберфізичних систем на основі зображень спектрограм і скалограм. Об'єктом дослідження є складне промислове устаткування, яке має неоднорідні сенсорні системи різної природи.

Мета роботи. Розробка методу виявлення аномалій сигналів на основі трансферного навчання у поєднанні з алгоритмом екстремального градієнтного бустінгу.

Метод. Запропоновано підхід на основі трансферного навчання і екстремального градієентного бустінгу, розроблений для виявлення аномалій в акустичних сигналах кіберфізичних систем. У цій області було проведено мало досліджень, і тому вивчалися різні архітектури заздалегідь навчених глибоких нейронних моделей, щоб поліпшити виявлення аномалій. Трансферне навчання використовує ваги з глибокої нейронної моделі, попередньо навченої на великому наборі даних, і може бути застосоване до невеликого набору навчальних даних, що забезпечує збіжність без перенавчання. Класичний підхід до такого роду проблем зазвичай включає в себе методи обробки сигналів, які дозволяють отримувати корисну інформацію з даних сенсорів. У цій статті виконується завдання виявлення аномалій з використанням архітектури глибокого навчання для роботи з акустичними сигналами, з яких попередньо витягуються спектрограми і скалограми. Функція активації SPOCU була розглянута для поліпшення точності запропонованого підходу. Алгоритм екстремального градієнтного бустінгу був використаний, оскільки він має високу продуктивність і вимагає мало обчислювальних ресурсів на етапі навчання. Застосування даного алгоритму дозволяє домогтися значного поліпшення виявлення аномалій в сигналах промислового обладнання.

Результати. Розроблений підхід реалізований програмно і досліджений під час вирішення завдання виявлення аномалій в акустичних сигналах кіберфізичних систем на наборі даних MIMII.

Висновки. Проведені експерименти підтвердили працездатність запропонованого підходу і дозволяють рекомендувати його для використання на практиці при вирішенні завдань діагностування стану промислового устаткування. Перспективи подальших досліджень можуть полягати в застосуванні ансамблевих підходів на основі трансферного навчання до різних реальних наборів даних для підвищення продуктивності та відмовостійкості кіберфізичних систем.

КЛЮЧОВІ СЛОВА: виявлення аномалій, акустичний сигнал, трансферне навчання, спектрограма, скалограма, кіберфізична система.

УДК 004.056

ИНТЕЛЛЕКТУАЛЬНАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ ГЛУБОКОГО ТРАНСФЕРНОГО ОБУЧЕНИЯ

Сухостат Л. В. – канд. техн. наук, доцент, Институт Информационных Технологий, Национальная Академия Наук Азербайджана, Баку, Азербайджан.

АННОТАЦИЯ

Актуальность. Рассмотрена задача обнаружения аномалий сигналов киберфизических систем на основе изображений спектрограмм и скалограмм. Объектом исследования является сложное промышленное оборудование, которое имеет неоднородные сенсорные системы различной природы.

Цель работы. Разработка метода обнаружения аномалий сигналов на основе трансферного обучения в сочетании с алгоритмом экстремального градиентного бустинга.

Метод. Предложен подход на основе трансферного обучения и экстремального градиентного бустинга, разработанный для обнаружения аномалий в акустических сигналах киберфизических систем. В этой области было проведено мало исследований, и поэтому изучались различные архитектуры заранее обученных глубоких нейронных моделей, чтобы улучшить обнаружение аномалий. Трансферное обучение использует веса из глубокой нейронной модели, предварительно обученной на большом наборе данных, и может быть применено к небольшому набору обучающих данных, что обеспечивает сходимость без переобучения. Классический подход к такого рода проблемам обычно включает в себя методы обработки сигналов, которые позволяют извлекать полезную информацию из данных сенсоров. В этой статье выполняется задача обнаружения аномалий с использованием архитектуры глубокого обучения для работы с акустическими сигналами, из которых предварительно извлекаются спектрограммы и скалограммы. Функция активации SPOCU была рассмотрена для улучшения точности предложенного подхода. Алгоритм экстремального градиентного бустинга был использован, потому что он обладает высокой производительностью и требует мало вычислительных ресурсов на этапе обучения. Применение данного алгоритма позволяет добиться значительного улучшения обнаружения аномалий в сигналах промышленного оборудования.

Результаты. Разработанный подход реализован программно и исследован при решении задачи обнаружения аномалий в акустических сигналах киберфизических систем на наборе данных MIMII.

Выводы. Проведенные эксперименты подтвердили работоспособность предложенного подхода и позволяют рекомендовать его для использования на практике при решении задач диагностирования состояния промышленного оборудования. Перспективы дальнейших исследований могут заключаться в применении ансамблевых подходов на основе трансферного обучения к различным реальным наборам данных для повышения производительности и отказоустойчивости киберфизических систем.

КЛЮЧЕВЫЕ СЛОВА: обнаружение аномалий, акустический сигнал, трансферное обучение, спектрограмма, скалограмма, киберфизическая система.

DOI 10.15588/1607-3274-2021-3-11

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Langner R. Stuxnet: dissecting a cyberwarfare weapon / R. Langner // IEEE Security & Privacy. – 2011. – Vol. 9, № 3. – P. 49–51. DOI: 10.1109/MSP.2011.67
2. Ahmed C. M. Challenges and opportunities in CPS security: a physics-based perspective / C. M. Ahmed, J. Zhou // IEEE Security & Privacy. – 2020. – Vol. 18, № 6. – P. 14–22. DOI: 10.1109/MSEC.2020.3002851
3. Ahmed C. M. Model-based attack detection scheme for smart water distribution networks / C. M. Ahmed, C. Murguia, J. Ruths // Computer and Communications Security: 17th ACM ASIA Conference, Abu Dhabi, 2–6 April 2017: proceedings. – P. 101–113. DOI: 10.1145/3052973.3053011
4. Multi-head CNN–RNN for multi-time series anomaly detection: an industrial case study / [M. Canizo, I. Triguero, A. Conde, E. Onieva] // Neurocomputing. – 2019. – Vol. 363. – P. 246–260. DOI: 10.1016/j.neucom.2019.07.034
5. Kiseľák J. "SPOCU": scaled polynomial constant unit activation function / [J. Kiseľák, Y. Lu, J. Švihra et al.] // Neural Computing and Applications. – 2021. – № 33. – P. 3385–3401. DOI: 10.1007/s00521-020-05182-1
6. M. R. G. R. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation / G. R. M. R., C. M. Ahmed, A. Mathur // Cybersecurity. – 2021. – Vol. 4, № 27. – P. 1–12. DOI: 10.1186/s42400-021-00095-5
7. Morita K. Anomalous sound detection by using local outlier factor and Gaussian mixture model / K. Morita, T. Yano, K. Q. Tran. – 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Morita_51_t2.pdf
8. IAEO3 – combining OpenL3 embeddings and interpolation autoencoder for anomalous sound detection /[S. Grollmisch, D. Johnson, J. Abeßer, H. Lukashevich]. – 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Grollmisch_15_t2.pdf
9. Michau G. Fully learnable deep wavelet transform for unsupervised monitoring of high-frequency time series / G. Michau, O. Fink. – 2021 [Electronic resource]. Access mode: https://arxiv.org/pdf/2105.00899.pdf
10. Deep dense and convolutional autoencoders for machine acoustic anomaly detection / G. Coelho, P. Pereira, L. Matos et al.] // Artificial Intelligence Applications and Innovations: 17th IFIP International Conference, Hersonissos, 25–27 June 2021: proceedings. – Cham : Springer, 2021. – P. 337–348. DOI: 10.1007/978-3-030-79150-6_27
11. Modulation spectral signal representation and i-vectors for anomalous sound detection / [P. Tiwari, Y. Jain, A. Avila et al.] – 2020 [Electronic resource]. Access mode: http://dcase.community/documents/challenge2020/technical_reports/DCASE2020_Tiwari_84_t2.pdf
12. OutlierNets: highly compact deep autoencoder network architectures for on-device acoustic anomaly detection / [S. Abbasi, M. Famouri, M. J. Shafiee, A. Wong] // Sensors. – 2021. – Vol. 21, № 14. – P. 1–12. DOI: 10.3390/s21144805
13. Acoustic anomaly detection for machine sounds based on image transfer learning / [R. Müller, F. Ritz, S. Illium, C. Linnhoff-Popien] // Agents and Artificial Intelligence: 13th International Conference, 4–6 February 2021 : proceedings. – P. 49–56. DOI: 10.5220/0010185800490056
14. Lin J. Feature Extraction based on Morlet wavelet and its application for mechanical fault diagnosis / J. Lin, L. Qu // Journal of Sound and Vibration. – 2000. – Vol. 234, № 1. – P. 48–135. DOI: 10.1006/jsvi.2000.2864
15. Chollet F. Xception: deep learning with depthwise separable convolutions / F. Chollet // Computer Vision and Pattern Recognition: 30th IEEE Conference, Honolulu, 21–26 July 2017: proceedings. – P. 1800–1807. DOI: 10.1109/CVPR.2017.195
16. Sandler M. MobileNetV2: inverted residuals and linear bottlenecks / [M. Sandler, A. Howard, M. Zhu et al.] // Computer Vision and Pattern Recognition: IEEE/CVF Conference, Salt Lake City, 18–23 June 2018: proceedings. – P. 4510–4520. DOI: 10.1109/CVPR.2018.00474
17. Densely connected convolutional networks / [G. Huang, Z. Liu, L. van der Maaten, K. Q. Weinberger] // Computer Vision and Pattern Recognition: 30th IEEE Conference, Honolulu, 21–26 July 2017: proceedings. – P. 2261–2269. DOI: 10.1109/CVPR.2017.243
18. Rethinking the inception architecture for computer vision / [C. Szegedy, V. Vanhoucke, S. Ioffe et al.] // Computer Vision and Pattern Recognition: IEEE Conference, Las Vegas, 27–30 June 2016: proceedings. – P. 2818–2826. DOI: 10.1109/CVPR.2016.308
19. Going deeper with convolutions / [C. Szegedy, W. Liu, Y. Jia et al.] // Computer Vision and Pattern Recognition: IEEE Conference, Boston, 7–12 June 2015: proceedings. – P. 1–9. DOI: 10.1109/CVPR.2015.7298594
20. Kassani S. H. Diabetic retinopathy classification using a modified Xception architecture / [S. H. Kassani, P. H. Kassani, R. Khazaeinezhad et al.] // Signal Processing and Information Technology: IEEE International Symposium, Ajman, 10–12 December 2019: proceedings. – P. 1–6. DOI: 10.1109/ISSPIT47144.2019.9001846
21. Deep residual learning for image recognition / [K. He, X. Zhang, S. Ren, J. Sun] // Computer Vision and Pattern Recognition: IEEE Conference, Las Vegas, 27–30 June 2016: proceedings. – P. 770–778. DOI: 10.1109/CVPR.2016.90
22. Chen T. XGBoost: a scalable tree boosting system / T. Chen, C. Guestrin // Knowledge Discovery and Data Mining: 22nd ACM SIGKDD International Conference, San Francisco, 13–16 August 2016: proceedings. – P. 785–794. DOI: 10.1145/2939672.2939785
23. MIMII dataset: sound dataset for malfunctioning industrial machine investigation and inspection / [H. Purohit, R. Tanabe, K. Ichige et al.] // Detection and Classification of Acoustic Scenes and Events: 4th Workshop, New York, 25–26 October 2019: proceedings. – P. 209–213. DOI: 10.33682/m76f-d618
24. Ferri C. An experimental comparison of performance measures for classification / C. Ferri, J. Hernández-Orallo, R. Modroiu // Pattern Recognition Letters. – 2009. – Vol. 30, № 1. – P. 27–38. DOI: 10.1016/j.patrec.2008.08.010

DOI 10.15588/1607-3274-2021-3-11