ABSTRACT AND REFERENCES

INFORMATION TECHNOLOGY. INDUSTRY CONTROL SYSTEMS

DOI: 10.15587/1729-4061.2024.317103

LANDMINE DETECTION WITH A MOBILE APPLICATION (p. 6–13)

Oleksandr Kunichik
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4938-9446

The object of the research is the detection of explosive objects in an image, with a particular focus on the identification of anti-personnel landmines. The objective of this research is to develop effective tools for the recognition of landmines.

A mobile application for the recognition of explosive objects, trained on a deep learning model using landmine replicas, has been developed. The application was tested on images of actual landmines. The model utilized in the application exhibited a recall rate of 89 % (calculated as the ratio of correctly identified landmines to the total number of landmines present in the image). The results indicated that the recall rate for a specific category of landmines was less than that observed for the others. The average time required for offline image recognition was 2.1 seconds.

This paper presents the results of the evaluation of the effectiveness of the mobile application for landmine detection and classification. Furthermore, it describes the ways in which the application allows for the improvement of the model through the collection of data from users. It also describes the architecture and interface of the application, as well as an analysis of its potential applications in landmine recognition.

The efficacy of the mobile application can be attributed to its intuitive interface, the high accuracy of the deep learning model, and the capacity to obtain user feedback promptly. The program enables not only the identification of hazardous objects but also the transmission of data for the enhancement of the model.

The mobile application has the potential to be utilized for a multitude of tasks pertaining to the detection of explosive objects, in addition to enhancing the precision of the model. Furthermore, the app can be utilized in training centers for deminers and in mine-contaminated areas. The mobile application can be employed to identify unknown explosive objects and enhance the efficacy of deep learning models. The resulting models can be leveraged in the future to automate the demining process.

Keywords: landmine detection, explosive ordnance disposal, humanitarian demining, mobile demining application.

References

1. Landmine Monitor 2022. Available at: https://backend.icblcmc.org/assets/reports/Landmine-Monitors/LMM2022/Chapter-Images/Downloads/2022_Landmine_Monitor_web.pdf
2. Landmine Monitor 2023. Available at: https://backend.icblcmc.org/assets/reports/Landmine-Monitors/LMM2023/Downloads/Landmine-Monitor-2023_web.pdf
3. In Ukraine, 128,000 km2 of land and 14,000 km2 of water area are contaminated with explosives. Ministry of Defence of Ukraine. Available at: https://www.mil.gov.ua/news/2024/10/05/128-000-kv-km-suhodolu-ta-14-000-kv-km-akvatorii-ukraini-zabrudneno-vibuhonebezpechnimi-predmetami
4. Dog works faster than person with metal detector. Rescue operations by SES in Mykolaiv. Hromadske. Available at: https://www.youtube.com/watch?v=HDz17-1yeIk
5. Dorn, A. W. (2019). Eliminating Hidden Killers: How Can Technology Help Humanitarian Demining? Stability: International Journal of Security and Development, 8 (1). https://doi.org/10.5334/sta.743
6. Annual Report 2013. United Nations Mine Action Service. Available at: https://www.unmas.org/sites/default/files/unmas_2013_annual_report_digital_presentation_0.pdf
7. Susanto, A. P., Winarto, H., Fahira, A., Abdurrohman, H., Muharram, A. P., Widitha, U. R. et al. (2022). Building an artificial intelligence-powered medical image recognition smartphone application: What medical practitioners need to know. Informatics in Medicine Unlocked, 32, 101017. https://doi.org/10.1016/j.imu.2022.101017
8. Mori, R., Okawa, M., Tokumaru, Y., Niwa, Y., Matsuhashi, N., Futamura, M. (2024). Application of an artificial intelligence-based system in the diagnosis of breast ultrasound images obtained using a smartphone. World Journal of Surgical Oncology, 22 (1). https://doi.org/10.1186/s12957-023-03286-1
9. Hameed, Q. A., Hussein, H. A., Ahmed, M. A., Salih, M. M., Ismael, R. D., Omar, M. B. (2022). UXO-AID: A New UXO Classification Application Based on Augmented Reality to Assist Deminers. Computers, 11 (8), 124. https://doi.org/10.3390/computers11080124
10. Interaktyvna mapa terytoriy, yaki potentsiyno mozhut buty zabrudneni vybukhonebezpechnymy predmetamy. State Emergency Service of Ukraine. Available at: https://mine.dsns.gov.ua/
11. Bezpeka Info. United Nations Children's Fund (UNICEF). Available at: https://courses.bezpeka.info/home
12. Kalifa, I., Youssif, A., Adel, A. (2014). The Use of Mobile Technology for Detecting Landmines. International Journal of Computer Applications, 92 (5), 42–45. https://doi.org/10.5120/16008-5034
13. Mobile Operating System Market Share Worldwide for 2023 year. Statcounter Global Stats. Available at: https://gs.statcounter.com/os-market-share/mobile/worldwide/2023
14. C++ Framework. Qt. Available at: https://www.qt.io
15. Open Neural Network Exchange. Available at: https://onnx.ai
16. ONNX Runtime. Available at: https://onnxruntime.ai
17. Redmon, J., Divvala, S., Girshick, R., Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779–788. https://doi.org/10.1109/cvpr.2016.91
18. Kunichik, O., Tereshchenko, V. (2023). Improving the accuracy of landmine detection using data augmentation: a comprehensive study. Artificial Intelligence, 28 (2), 42–54. https://doi.org/10.15407/jai2023.02.042
19. Kunichik, O., Tereshchenko, V. (2024). Determining the effectiveness of using three-dimensional printing to train computer vision systems for landmine detection. Eastern-European Journal of Enterprise Technologies, 5 (1 (131)), 17–29. https://doi.org/10.15587/1729-4061.2024.311602
20. Secure Sockets Layer (SSL). Available at: https://openssl.org
21. Dwyer, B., Nelson, J., Solawetz, J. et al. (2022). Roboflow (Version 1.0) [Software]. Available at: https://roboflow.com

DOI: 10.15587/1729-4061.2024.317092

ENHANCING SKELETON-BASED ACTION RECOGNITION WITH HYBRID REAL AND GAN-GENERATED DATASETS (p. 14–22)

Talgat Islamgozhayev
Astana IT University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-7891-242X

Beibut Amirgaliyev
Astana IT University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-0355-5856

Zhanibek Kozhirbayev
Nazarbayev University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-4235-9049

This research addresses the critical challenge of recognizing mutual actions involving multiple individuals, an important task for applications such as video surveillance, human-computer interaction, autonomous systems, and behavioral analysis. Identifying these actions from 3D skeleton motion sequences poses significant challenges due to the necessity of accurately capturing intricate spatial and temporal patterns in diverse, dynamic, and often unpredictable environments. To tackle this, a robust neural network framework was developed that combines Convolutional Neural Networks (CNNs) for efficient spatial feature extraction with Long Short-Term Memory (LSTM) networks to model temporal dependencies over extended sequences. A distinguishing feature of this study is the creation of a hybrid dataset that which combines real-world skeleton motion data with synthetically generated samples, produced using Generative Adversarial Networks (GANs). This dataset enriches variability, enhances generalization, and mitigates data scarcity challenges. Experimental findings across three different network architectures demonstrate that our method significantly enhances recognition accuracy, mainly due to the integration of CNNs and LSTMs alongside the broadened dataset. Our approach successfully identifies complex interactions and ensures consistent performance across different perspectives and environmental conditions. The improved reliability in recognition indicates that this framework can be effectively utilized in practical applications such as security systems, crowd monitoring, and other areas where precise detection of mutual actions is critical, particularly in real-time and dynamic environments.

Keywords: action recognition, convolutional neural network, generative adversarial networks, LSTM.

References

1. Pareek, P., Thakkar, A. (2020). A survey on video-based Human Action Recognition: recent updates, datasets, challenges, and applications. Artificial Intelligence Review, 54 (3), 2259–2322. https://doi.org/10.1007/s10462-020-09904-8
2. Cermeño, E., Pérez, A., Sigüenza, J. A. (2018). Intelligent video surveillance beyond robust background modeling. Expert Systems with Applications, 91, 138–149. https://doi.org/10.1016/j.eswa.2017.08.052
3. Fang, M., Chen, Z., Przystupa, K., Li, T., Majka, M., Kochan, O. (2021). Examination of Abnormal Behavior Detection Based on Improved YOLOv3. Electronics, 10 (2), 197. https://doi.org/10.3390/electronics10020197
4. Hejazi, S. M., Abhayaratne, C. (2022). Handcrafted localized phase features for human action recognition. Image and Vision Computing, 123, 104465. https://doi.org/10.1016/j.imavis.2022.104465
5. Yan, S., Xiong, X., Arnab, A., Lu, Z., Zhang, M., Sun, C., Schmid, C. (2022). Multiview Transformers for Video Recognition. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 3323–3333. https://doi.org/10.1109/cvpr52688.2022.00333
6. Tong, Z., Song, Y., Wang, J., Wang, L. (2022). VideoMAE: Masked Autoencoders are Data-Efficient Learners for Self-Supervised Video Pre-Training. arXiv. https://arxiv.org/abs/2203.12602
7. Hochreiter, S., Schmidhuber, J. (1997). Long Short-Term Memory. Neural Computation, 9 (8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
8. Soltau, H., Liao, H., Sak, H. (2017). Neural Speech Recognizer: Acoustic-to-Word LSTM Model for Large Vocabulary Speech Recognition. Interspeech 2017. https://doi.org/10.21437/interspeech.2017-1566
9. Kozhirbayev, Z., Yessenbayev, Z., Karabalayeva, M. (2017). Kazakh and Russian Languages Identification Using Long Short-Term Memory Recurrent Neural Networks. 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), 1–5. https://doi.org/10.1109/icaict.2017.8687095
10. Lu, Y., Lu, C., Tang, C.-K. (2017). Online Video Object Detection Using Association LSTM. 2017 IEEE International Conference on Computer Vision (ICCV). https://doi.org/10.1109/iccv.2017.257
11. Huang, R., Zhang, W., Kundu, A., Pantofaru, C., Ross, D. A., Funkhouser, T., Fathi, A. (2020). An LSTM Approach to Temporal 3D Object Detection in LiDAR Point Clouds. Computer Vision – ECCV 2020, 266–282. https://doi.org/10.1007/978-3-030-58523-5_16
12. Yuan, Y., Liang, X., Wang, X., Yeung, D.-Y., Gupta, A. (2017). Temporal Dynamic Graph LSTM for Action-Driven Video Object Detection. 2017 IEEE International Conference on Computer Vision (ICCV). https://doi.org/10.1109/iccv.2017.200
13. Zhang, B., Yu, J., Fifty, C., Han, W., Dai, A. M., Pang, R., Sha, F. (2021). Co-training Transformer with Videos and Images Improves Action Recognition. arXiv. https://doi.org/10.48550/arxiv.2112.07175
14. Wang, Y., Li, K., Li, Y., He, Y., Huang, B., Zhao, Z. et al. (2022). InternVideo: General Video Foundation Models via Generative and Discriminative Learning. arXiv. https://doi.org/10.48550/arXiv.2212.03191
15. Kay, W., Carreira, J., Simonyan, K., Zhang, B., Hillier, C., Vijayanarasimhan, S. et al. (2017). The Kinetics Human Action Video Dataset. arXiv. https://doi.org/10.48550/arXiv.1705.06950
16. Carreira, J., Noland, E., Banki-Horvath, A., Hillier, C., Zisserman, A. (2018). A short note about kinetics-600. arXiv. https://doi.org/10.48550/arXiv.1808.01340
17. Carreira, J., Noland, E., Hillier, C., Zisserman, A. (2019). A short note on the kinetics-700 human action dataset. arXiv. https://doi.org/10.48550/arXiv.1907.06987
18. Goyal, R., Kahou, S. E., Michalski, V., Materzynska, J., Westphal, S., Kim, H. et al. (2017). The "Something Something" Video Database for Learning and Evaluating Visual Common Sense. 2017 IEEE International Conference on Computer Vision (ICCV). https://doi.org/10.1109/iccv.2017.622
19. Heilbron, F. C., Escorcia, V., Ghanem, B., Niebles, J. C. (2015). ActivityNet: A large-scale video benchmark for human activity understanding. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). https://doi.org/10.1109/cvpr.2015.7298698
20. Zhao, H., Torralba, A., Torresani, L., Yan, Z. (2019). HACS: Human Action Clips and Segments Dataset for Recognition and Temporal Localization. 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 8667–8677. https://doi.org/10.1109/iccv.2019.00876
21. Kuehne, H., Jhuang, H., Garrote, E., Poggio, T., Serre, T. (2011). HMDB: A large video database for human motion recognition. 2011

International Conference on Computer Vision, 2556–2563. https://doi.org/10.1109/iccv.2011.6126543
22. Shahroudy, A., Liu, J., Ng, T.-T., Wang, G. (2016). NTU RGB+D: A Large Scale Dataset for 3D Human Activity Analysis. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). https://doi.org/10.1109/cvpr.2016.115
23. Liu, J., Shahroudy, A., Perez, M., Wang, G., Duan, L.-Y., Kot, A. C. (2020). NTU RGB+D 120: A Large-Scale Benchmark for 3D Human Activity Understanding. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42 (10), 2684–2701. https://doi.org/10.1109/tpami.2019.2916873
24. Degardin, B., Neves, J., Lopes, V., Brito, J., Yaghoubi, E., Proenca, H. (2022). Generative Adversarial Graph Convolutional Networks for Human Action Synthesis. 2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2753–2762. https://doi.org/10.1109/wacv51458.2022.00281
25. Caetano, C., Sena, J., Bremond, F., Dos Santos, J. A., Schwartz, W. R. (2019). SkeleMotion: A New Representation of Skeleton Joint Sequences based on Motion Information for 3D Action Recognition. 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). https://doi.org/10.1109/avss.2019.8909840
26. Groleau, G. A., Tso, E. L., Olshaker, J. S., Barish, R. A., Lyston, D. J. (1993). Baseball bat assault injuries. The Journal of Trauma: Injury, Infection, and Critical Care, 34 (3), 366–372. https://doi.org/10.1097/00005373-199303000-00010
27. DegardinBruno/Kinetic-Gan. Available at: https://github.com/DegardinBruno/Kinetic-GAN
28. Li, C., Zhong, Q., Xie, D., Pu, S. (2017). Skeleton-based action recognition with convolutional neural networks. 2017 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 597–600. https://doi.org/10.1109/icmew.2017.8026285
29. Goodfellow, I. J., Warde-Farley, D., Mirza, M., Courville, A. C., Bengio, Y. (2013). Maxout networks. arXiv. https://doi.org/10.48550/arXiv.1302.4389
30. Zheng, W., Li, L., Zhang, Z., Huang, Y., Wang, L. (2019). Relational Network for Skeleton-Based Action Recognition. 2019 IEEE International Conference on Multimedia and Expo (ICME), 826–831. https://doi.org/10.1109/icme.2019.00147

DOI: 10.15587/1729-4061.2024.318554

OPTIMIZATION OF IMAGE COMPRESSION USING ARTIFICIAL NEURAL NETWORKS (p. 23–35)

Oleksandr Lytvyn
Ivan Franko National University of Lviv, Lviv, Ukraine
ORCID: https://orcid.org/0009-0006-3765-5125

Nadiya Kolos
Ivan Franko National University of Lviv, Lviv, Ukraine
ORCID: https://orcid.org/0000-0001-9710-9667

The object of research is artificial neural networks of adaptive resonance theory (ART). ART neural networks are classified by matching input data to one of the existing classes, provided that the data is sufficiently similar to the Class prototypes. Continuous and discrete adaptive resonance theory networks ART-1 and ART-2 work effectively in recognition systems, especially in conditions of high uncertainty, when it is necessary to identify a large number of different images.

The main problem that was solved in this study was to optimize the process of image compression using artificial neural networks, because image compression is widely used in many scientific and technical fields and becomes especially relevant when transmitting over narrow-band communication channels. A way to overcome these difficulties may be to select basic data for reconstruction from an open data set (Modified National Institute of Standards and Technology) – Fashion-MNIST. There are still unresolved issues related to the fact that lossy compression algorithms with increasing compression ratio usually generate artifacts that are clearly visible to the human eye.

A compression algorithm based on neural networks is described, which establishes a correspondence between the input and output spaces consisting of elements of the codebook and neurons. The proposed method uses a different approach (First Order), rather than a simple difference coding scheme (zero order), where the new code is calculated by subtracting the previous encoded block. The peak signal-to-noise ratio of PSNR and the root-mean-square error (MSE) of these algorithms is 24.7 DB with a compression ratio of 25.22.

The main area of practical use of the results obtained is improved image compression for processing large – volume video and photo materials without significant loss of quality.

Keywords: image compression, image processing, neural network, compression method, compression algorithm.

References

1. Ali, A. N. M., Ahmad, N., Noor, N. M., Aris, S. A. M. (2022). Image Compression Using AMBTC with Artificial Neural Networks. 2022 IEEE Symposium on Future Telecommunication Technologies (SOFTT), 78–82. https://doi.org/10.1109/softt56880.2022.10009930
2. Dashkevich, A. (2016). Study of multilayer neural networks for automatic feature extraction in solving the problem of pattern recognition. Naukovyi visnyk TDATU, 2 (6), 134–139. Available at: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/883b0aec-89a9-48c9-bb07-3c515300dd80/content
3. Lesyk, V. O., Doroshenko, A. Yu. (2023). Image compression module based neural network autoencoders. Problems in Programming, 1, 48–57. https://doi.org/10.15407/pp2023.01.048
4. Bosse, S., Maniry, D., Wiegand, T., Samek, W. (2016). A deep neural network for image quality assessment. 2016 IEEE International Conference on Image Processing (ICIP), 3773–3777. https://doi.org/10.1109/icip.2016.7533065
5. Syzonenko, Yu. I. (2016). Systema stysnennia ta zakhystu zobrazhen za dopomohoiu neitronnoi merezhi. Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky: Materialy Vseukrainskoi naukovo-praktychnoi konferentsiyi. Kropyvnytskyi, 157–158. Available at: https://core.ac.uk/download/pdf/84825428.pdf
6. Atta, R. E., Kasem, H., Attia, M. (2020). A comparison study for image compression based on compressive sensing. Eleventh International Conference on Graphics and Image Processing (ICGIP 2019), 60. https://doi.org/10.1117/12.2557296
7. Netalkar, R. K., Barman, H., Subba, R., Preetam, K. V., Raju, U. S. N. (2021). Distributed compression and decompression for big image data: LZW and Huffman coding. Journal of Electronic Imaging, 30 (05). https://doi.org/10.1117/1.jei.30.5.053015
8. Hrytsyk, V. (2017). Basic image quality estimates methods are used today to solve the problem of automatic image processing. Shtuchnyi intelekt, 1, 38–44. Available at: http://dspace.nbuv.gov.ua/handle/123456789/132099
9. Myasischev, O. A., Lenkov, Ye. S., Bilik, O. M. (2016). Recognition of graphic images using neural networks. Collection of Scientific Works of the Military Institute of Kyiv National Taras Shevchenko University, 54, 143–149. Available at: https://miljournals.knu.ua/index.php/zbirnuk/article/view/174

10. Jalilian, E., Hofbauer, H., Uhl, A. (2022). Iris Image Compression Using Deep Convolutional Neural Networks. Sensors, 22 (7), 2698. https://doi.org/10.3390/s22072698
11. Yelahina, K., Zhukovska, D., Voropaeva, V. (2021). Use of neural network architecture based on adaptive resonance for speech signal recognition. Naukovyi Visnyk Donetskoho Natsionalnoho Tekhnichnoho Universytetu, 1 (6)-2 (7), 55–67. https://doi.org/10.31474/2415-7902-2021-1(6)-2(7)-55-67
12. Hussain, A. J., Al-Fayadh, A., Radi, N. (2018). Image compression techniques: A survey in lossless and lossy algorithms. Neurocomputing, 300, 44–69. https://doi.org/10.1016/j.neucom.2018.02.094
13. Sadeeq, H. T., Hameed, T. H., Abdi, A. S., Abdulfatah, A. N. (2021). Image Compression Using Neural Networks: A Review. International Journal of Online and Biomedical Engineering (IJOE), 17 (14), 135–153. https://doi.org/10.3991/ijoe.v17i14.26059
14. Ding, K., Ma, K., Wang, S., Simoncelli, E. P. (2021). Comparison of Full-Reference Image Quality Models for Optimization of Image Processing Systems. International Journal of Computer Vision, 129 (4), 1258–1281. https://doi.org/10.1007/s11263-020-01419-7
15. Feng, Y., Zhang, Y., Zhou, Z., Huang, P., Liu, L., Liu, X., Kang, J. (2024). Memristor-based storage system with convolutional autoencoder-based image compression network. Nature Communications, 15 (1). https://doi.org/10.1038/s41467-024-45312-0
16. Zhang, S., Zhao, C., Basu, A. (2024). Principal Component Approximation Network for Image Compression. ACM Transactions on Multimedia Computing, Communications, and Applications, 20 (5), 1–20. https://doi.org/10.1145/3637490
17. Yang, F., Herranz, L., Cheng, Y., Mozerov, M. G. (2021). Slimmable Compressive Autoencoders for Practical Neural Image Compression. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 4996–5005. https://doi.org/10.1109/cvpr46437.2021.00496

DOI: 10.15587/1729-4061.2024.317456

DEVISING A METHOD FOR DETECTING INFORMATION THREATS IN THE UKRAINIAN CYBER SPACE BASED ON MACHINE LEARNING (p. 36–48)

Victoria Vysotska
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0001-6417-3689

Mariia Nazarkevych
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-6528-9867

Serhii Vladov
Kremenchuk Flight College of Kharkiv National University of Internal Affairs, Kremenchuk, Ukraine
ORCID: https://orcid.org/0000-0001-8009-5254

Olga Lozynska
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-5079-0544

Oksana Markiv
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-1691-1357

Roman Romanchuk
LLC TIETO UKRAINE SUPPORT SERVICES, Lviv, Ukraine
ORCID: https://orcid.org/0009-0004-4352-1073

Vitalii Danylyk
Genesis Space, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-5928-7235

The object of this study is a disinformation detection process based on search algorithms for identifying fake news. The main task was to define a set of criteria and parameters for detecting the Ukrainian-language disinformation based on machine learning. A methodology has been considered for developing and filling a dataset of fakes for further training of the model and testing it for the purpose of identifying disinformation and propaganda, as well as determining the attributes of primary sources and routes of their distribution. This makes it possible to reasonably approach the definition of a model for forecasting the development of information threats in the cyberspace of Ukraine. In particular, the accuracy of automatic detection of the probability of disinformation in texts can be increased. For the English-language texts using balanced datasets for training when applying classical machine learning classifiers, the accuracy of identification and recognition of fakes is ≥90 %, and for the Ukrainian-language texts – ≥52 % and ≤90 %. That has made it possible to devise requirements for the structure and content of a typical dataset of fakes in the period after the full-scale invasion of Ukraine. The practical result of this work is the designed decision-making support system for monitoring, detecting, recognizing, and forecasting information threats in the cyberspace of Ukraine based on NLP and machine learning. The implementation of preliminary processing of the Ukrainian-language news, taking into account the linguistic features of the language in the text, increases the accuracy of fake identification by ≈1.72 times. Approaches to the construction of models for forecasting the development of information threats in cyberspace have been developed, which is an urgent task when fake news and information manipulation can affect public sentiment, politics, and the economy.

Keywords: information threat, fake news, machine learning, disinformation detection, dataset, cyber security.

References

1. Trofymenko, O. H. (2019). Monitorynh stanu kiberbezpeky v Ukraini. Pravove zhyttia suchasnoi Ukrainy. Mizhnar. nauk.-prakt. konf. Vol. 1. Odesa: VD «Helvetyka», 642–646. Available at: https://dspace.onua.edu.ua/items/3aa8c85a-0013-4a36-9c74-bedbcd915593
2. Trofymenko, O., Prokop, Y., Loginova, N., Zadereyko, O. (2019). Cybersecurity of Ukraine: analysis of the current situation. Ukrainian Information Security Research Journal, 21 (3). https://doi.org/10.18372/2410-7840.21.13951
3. Yashchuk, V. I. (2024). Rol ta mistse stratehiyi kiberbezpeky ukrainy u zabezpechenni informatsiynoi bezpeky derzhavy. Available at: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/13824/1/1%20Yashchuk_monogr_rozdil13.pdf
4. Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podiy u kiberprostori (2023). Postanova Kabinetu Ministriv Ukrainy vid 04.04.23 r. No. 299. Available at: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text
5. Vysotska, V., Chyrun, L., Chyrun, S., Holets, I. (2024). Information technology for identifying disinformation sources and inauthentic chat users' behaviours based on machine learning. CEUR Workshop Proceedings, 3723, 427–465. Available at: https://ceur-ws.org/Vol-3723/paper24.pdf
6. Vysotska, V., Przystupa, K., Chyrun, L., Vladov, S., Ushenko, Y., Uhryn, D., Hu, Z. (2024). Disinformation, Fakes and Propaganda Identifying Methods in Online Messages Based on NLP and Machine Learning Methods. International Journal of Computer Network and Information Security, 16 (5), 57–85. https://doi.org/10.5815/ijcnis.2024.05.06

7. Khairova, N., Galassi, A., Lo, F., Ivasiuk, B., Redozub, I. (2024). Unsupervised approach for misinformation detection in Russia-Ukraine war news. Proceedings of the 8th International Conference on Computational Linguistics and Intelligent Systems. Volume IV: Computational Linguistics Workshop. https://doi.org/10.31110/colins/2024-4/003
8. Wierzbicki, A., Shupta, A., Barmak, O. (2024). Synthesis of model features for fake news detection using large language models. Proceedings of the 8th International Conference on Computational Linguistics and Intelligent Systems. Volume IV: Computational Linguistics Workshop. https://doi.org/10.31110/colins/2024-4/005
9. Oliinyk, V.-A., Vysotska, V., Burov, Ye., Mykich, K., Basto-Fernandes, V. (2020). Propaganda Detection in Text Data Based on NLP and Machine Learning. CEUR workshop proceedings, 2631, 132–144. Available at: https://ceur-ws.org/Vol-2631/paper10.pdf
10. Vysotska, V., Mazepa, S., Chyrun, L., Brodyak, O., Shakleina, I., Schuchmann, V. (2022). NLP Tool for Extracting Relevant Information from Criminal Reports or Fakes/Propaganda Content. 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), 93–98. https://doi.org/10.1109/csit56902.2022.10000563
11. Dar, R. A., Hashmy, Dr. R. (2023). A Survey on COVID-19 related Fake News Detection using Machine Learning Models. CEUR Workshop Proceedings, 3426, 36–46. Available at: https://ceur-ws.org/Vol-3426/paper4.pdf
12. Mykytiuk, A., Vysotska, V., Markiv, O., Chyrun, L., Pelekh, Y. (2023). Technology of Fake News Recognition Based on Machine Learning Methods. CEUR Workshop Proceedings, 3387, 311–330. Available at: https://ceur-ws.org/Vol-3387/paper24.pdf
13. Afanasieva, I., Golian, N., Golian, V., Khovrat, A., Onyshchenko, K. (2023). Application of Neural Networks to Identify of Fake News. CEUR Workshop Proceedings, 3396, 346–358. Available at: https://ceur-ws.org/Vol-3396/paper28.pdf
14. Shupta, A., Barmak, O., Wierzbicki, A., Skrypnyk, T. (2023). An Adaptive Approach to Detecting Fake News Based on Generalized Text Features. CEUR Workshop Proceedings, 3387, 300–310. Available at: https://ceur-ws.org/Vol-3387/paper23.pdf
15. Saquete, E., Tomás, D., Moreda, P., Martínez-Barco, P., Palomar, M. (2020). Fighting post-truth using natural language processing: A review and open challenges. Expert Systems with Applications, 141, 112943. https://doi.org/10.1016/j.eswa.2019.112943
16. Elzayady, H., Mohamed, M. S., Badran, K. M., Salama, G. I. (2022). Detecting Arabic textual threats in social media using artificial intelligence: An overview. Indonesian Journal of Electrical Engineering and Computer Science, 25 (3), 1712–1722. http://doi.org/10.11591/ijeecs.v25.i3.pp1712-1722
17. Shahbazi, Z., Byun, Y.-C. (2021). Fake Media Detection Based on Natural Language Processing and Blockchain Approaches. IEEE Access, 9, 128442–128453. https://doi.org/10.1109/access.2021.3112607
18. Guo, Z., Schlichtkrull, M., Vlachos, A. (2022). A Survey on Automated Fact-Checking. Transactions of the Association for Computational Linguistics, 10, 178–206. https://doi.org/10.1162/tacl_a_00454
19. Liu, X., Qi, L., Wang, L., Metzger, M. J. (2023). Checking the Fact-Checkers: The Role of Source Type, Perceived Credibility, and Individual Differences in Fact-Checking Effectiveness. Communication Research. https://doi.org/10.1177/00936502231206419
20. Martín, A., Huertas-Tato, J., Huertas-García, Á., Villar-Rodríguez, G., Camacho, D. (2022). FacTeR-Check: Semi-automated fact-checking through semantic similarity and natural language inference. Knowledge-Based Systems, 251, 109265. https://doi.org/10.1016/j.knosys.2022.109265
21. Ali, F., El-Sappagh, S., Islam, S. M. R., Ali, A., Attique, M., Imran, M., Kwak, K.-S. (2021). An intelligent healthcare monitoring framework using wearable sensors and social networking data. Future Generation Computer Systems, 114, 23–43. https://doi.org/10.1016/j.future.2020.07.047
22. Camacho, D., Panizo-LLedot, Á., Bello-Orgaz, G., Gonzalez-Pardo, A., Cambria, E. (2020). The four dimensions of social network analysis: An overview of research methods, applications, and software tools. Information Fusion, 63, 88–120. https://doi.org/10.1016/j.inffus.2020.05.009
23. Daud, N. N., Ab Hamid, S. H., Saadoon, M., Sahran, F., Anuar, N. B. (2020). Applications of link prediction in social networks: A review. Journal of Network and Computer Applications, 166, 102716. https://doi.org/10.1016/j.jnca.2020.102716
24. Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M., Ridhawi, I. A. (2020). An incentive-aware blockchain-based solution for internet of fake media things. Information Processing & Management, 57 (6), 102370. https://doi.org/10.1016/j.ipm.2020.102370
25. Avelino, M., Rocha, A. A. de A. (2022). BlockProof: A Framework for Verifying Authenticity and Integrity of Web Content. Sensors, 22 (3), 1165. https://doi.org/10.3390/s22031165
26. Wang, X., Xie, H., Ji, S., Liu, L., Huang, D. (2023). Blockchain-based fake news traceability and verification mechanism. Heliyon, 9 (7), e17084. https://doi.org/10.1016/j.heliyon.2023.e17084
27. Boyen, X., Herath, U., McKague, M., Stebila, D. (2021). Associative Blockchain for Decentralized PKI Transparency. Cryptography, 5 (2), 14. https://doi.org/10.3390/cryptography5020014
28. Xue, J., Wang, Y., Tian, Y., Li, Y., Shi, L., Wei, L. (2021). Detecting fake news by exploring the consistency of multimodal data. Information Processing & Management, 58 (5), 102610. https://doi.org/10.1016/j.ipm.2021.102610
29. Sahoo, S. R., Gupta, B. B. (2021). Multiple features based approach for automatic fake news detection on social networks using deep learning. Applied Soft Computing, 100, 106983. https://doi.org/10.1016/j.asoc.2020.106983
30. Kaliyar, R. K., Goswami, A., Narang, P., Sinha, S. (2020). FNDNet – A deep convolutional neural network for fake news detection. Cognitive Systems Research, 61, 32–44. https://doi.org/10.1016/j.cogsys.2019.12.005

DOI: 10.15587/1729-4061.2024.317000

DESIGN OF AN INTELLIGENT MODULE FOR DETECTING SIGNS OF INFORMATION SECURITY THREATS AND THE EMERGENCE OF UNRELIABLE DATA (p. 49–63)

Irina Cherepanska
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-0741-7194

Artem Sazonov
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7124-5863

Yuriy Kyrychuk
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-8638-6060

Petro Melnychuk
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0002-7071-651X

Dmytro Melnychuk
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0002-9918-0608

Nataliia Nazarenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-6533-7323

Volodymyr Pryadko
Polissia National University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0001-8284-1062

Serhii Bakhman
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0009-0001-9568-0621

Davyd Khraban
Zhytomyr Polytechnic State University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0003-2621-2370

At the stage of production preparation, there is an urgent need for an automated system that would timely detect signs of threats to information security and the emergence of unreliable data. To solve this problem, an intelligent module capable of detecting such threats and unreliable and/or anomalous data has been designed. The proposed intelligent module is the state-of-art, original, and effective toolkit. It can be recommended for practical use as part of the well-known information and computer system for automated modeling of the system of automatic orientation of production objects at the stage of technological preparation of machine and instrument-building production. Its application makes it possible to increase information security and reliability of important production data at the stage of technological preparation of production, in particular, when modeling systems for automatic orientation of production objects. In addition, the use of the proposed intelligent module makes it possible to obtain a number of important social and economic effects. Some of these effects are manifested in the prevention or reduction of material, intellectual and time costs for saving and restoring information, etc.

Automated analysis of important production data regarding their reliability and abnormality is carried out by machine learning methods using a specially designed advanced variational autoencoder based on classification algorithms and using wavelet transformation.

The designed intelligent module for detecting signs of a threat to information security and the emergence of unreliable and/or anomalous data works in real time with a high accuracy of 97.53 %. It meets the requirements of modern production.

Keywords: information-computer system, automated modeling, control, artificial intelligence, flexible production system.

References

1. Cherepanska, I., Sazonov, A., Melnychuk, P., Melnychuk, D., Kalchuk, S., Pryadko, V., Yanovsky, V. (2024). Design of an information-computer system for the automated modeling of systems for automatic orientation of production objects in the machine and instrument industries. Eastern-European Journal of Enterprise Technologies, 3 (2 (129)), 6–19. https://doi.org/10.15587/1729-4061.2024.306516
2. Gao, Y., Yin, X., He, Z., Wang, X. (2023). A deep learning process anomaly detection approach with representative latent features for low discriminative and insufficient abnormal data. Computers & Industrial Engineering, 176, 108936. https://doi.org/10.1016/j.cie.2022.108936
3. Aschepkov, V. (2024). The use of the Isolation Forest model for anomaly detection in measurement data. Innovative technologies and scientific solutions for industries, 1 (27), 236–245. https://doi.org/10.30837/itssi.2024.27.236
4. Vos, K., Peng, Z., Jenkins, C., Shahriar, M. R., Borghesani, P., Wang, W. (2022). Vibration-based anomaly detection using LSTM/SVM approaches. Mechanical Systems and Signal Processing, 169, 108752. https://doi.org/10.1016/j.ymssp.2021.108752
5. Huang, X., Wen, G., Dong, S., Zhou, H., Lei, Z., Zhang, Z., Chen, X. (2021). Memory Residual Regression Autoencoder for Bearing Fault Detection. IEEE Transactions on Instrumentation and Measurement, 70, 1–12. https://doi.org/10.1109/tim.2021.3072131
6. Panza, M. A., Pota, M., Esposito, M. (2023). Anomaly Detection Methods for Industrial Applications: A Comparative Study. Electronics, 12 (18), 3971. https://doi.org/10.3390/electronics12183971
7. Mokhtari, S., Abbaspour, A., Yen, K. K., Sargolzaei, A. (2021). A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data. Electronics, 10 (4), 407. https://doi.org/10.3390/electronics10040407
8. Zipfel, J., Verworner, F., Fischer, M., Wieland, U., Kraus, M., Zschech, P. (2023). Anomaly detection for industrial quality assurance: A comparative evaluation of unsupervised deep learning models. Computers & Industrial Engineering, 177, 109045. https://doi.org/10.1016/j.cie.2023.109045
9. Jaramillo-Alcazar, A., Govea, J., Villegas-Ch, W. (2023). Anomaly Detection in a Smart Industrial Machinery Plant Using IoT and Machine Learning. Sensors, 23 (19), 8286. https://doi.org/10.3390/s23198286
10. Tang, M., Chen, W., Yang, W. (2022). Anomaly detection of industrial state quantity time-Series data based on correlation and long short-term memory. Connection Science, 34 (1), 2048–2065. https://doi.org/10.1080/09540091.2022.2092594
11. Evangelou, M., Adams, N. M. (2020). An anomaly detection framework for cyber-security data. Computers & Security, 97, 101941. https://doi.org/10.1016/j.cose.2020.101941
12. Ameer, S., Gupta, M., Bhatt, S., Sandhu, R. (2022). BlueSky. Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, 235–244. https://doi.org/10.1145/3532105.3535020
13. Szymanski, T. H. (2022). The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). IEEE Access, 10, 45893–45930. https://doi.org/10.1109/access.2022.3169137
14. Liu, R., Shi, J., Chen, X., Lu, C. (2024). Network anomaly detection and security defense technology based on machine learning: A review. Computers and Electrical Engineering, 119, 109581. https://doi.org/10.1016/j.compeleceng.2024.109581
15. Das, T. K., Adepu, S., Zhou, J. (2020). Anomaly detection in Industrial Control Systems using Logical Analysis of Data. Computers & Security, 96, 101935. https://doi.org/10.1016/j.cose.2020.101935
16. Patel, P., Deshpande, V. (2017). Application Of Plan-Do-Check-Act Cycle For Quality And Productivity Improvement-A Review. International Journal for Research in Applied Science & Engineering Technology, 5 (1), 197–201. Available at: https://www.researchgate.net/publication/318743952_Application_Of_Plan-Do-Check-Act_Cycle_For_Quality_And_Productivity_Improvement-A_Review
17. Molodetska-Hrynchuk, K. (2017). The model of decision making support system for detection and assessment of the state information security threat of social networking services. Ukrainian

Scientific Journal of Information Security, 23 (2). https://doi.org/10.18372/2225-5036.23.11803

18. Gong, X., Yu, S., Xu, J., Qiao, A., Han, H. (2023). The effect of PDCA cycle strategy on pupils' tangible programming skills and reflective thinking. Education and Information Technologies, 29 (5), 6383–6405. https://doi.org/10.1007/s10639-023-12037-4
19. Cherepanska, I., Sazonov, A., Melnychuk, D., Melnychuk, P., Khazanovych, Y. (2023). Quaternion Model of Workpieces Orienting Movements in Manufacturing Engineering and Tool Production. Lecture Notes in Mechanical Engineering, 127–135. https://doi.org/10.1007/978-3-031-42778-7_12
20. Voronin, A. N. (2009). Nelineynaya skhema kompromissov v mnogokriterial'nyh zadachah otsenivaniya i optimizatsii. Kibernetika i sistemniy analiz, 45 (4), 106–114. Available at: http://nbuv.gov.ua/UJRN/KSA_2009_45_4_10
21. Nykolyuk, O. M., Martynchuk, V. (2018). A Methodology for Assessing Resource Potential of Innovation-Oriented Agricultural Enterprises. Problemy Ekonomiky, 1 (35), 207–213. Available at: https://www.proquest.com/openview/1716ad4663e51395c99da80118e1204e/1?pq-origsite=gscholar&cbl=2048964

DOI: 10.15587/1729-4061.2024.318336

DESIGN OF AN INTEGRATED DEFENSE-IN-DEPTH SYSTEM WITH AN ARTIFICIAL INTELLIGENCE ASSISTANT TO COUNTER MALWARE (p. 64–73)

Danyil Zhuravchak
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-4989-0203

Maksym Opanovych
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-2748-2965

Anastasiia Tolkachova
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-8196-7963

Valerii Dudykevych
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0001-8827-9920

Andrian Piskozub
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-3582-2835

The object of this study is multi-layered cybersecurity systems for detecting and countering advanced persistent threats through the integration of machine learning technologies, artificial intelligence, and multi-layered security systems. The task relates to the need to design adaptive detection systems capable of effectively responding to new and modified threats while improving accuracy and minimizing delays. An integrated approach was devised in the study, which combines conventional detection methods (signature analysis, correlation rules) with modern technologies such as machine learning and Artificial Intelligence assistants. Each layer of the system showed varying levels of effectiveness: for example, antivirus solutions were most effective at detecting known threats but failed to cope with modified threats, which were detected by correlation rules. Machine learning proved most effective at detecting fileless attacks and anomalous activity that other tools could not detect. It is through the combination of these methods that the detection system proved to be effective, providing a high level of protection. The results are due to the efficiency of combining several layers of defense, in which each subsequent layer compensates for the shortcomings of the previous one. Antivirus solutions detected 100 % of known threats, while correlation rules identified all modified malicious files. Overall, the system was able to detect 98 % of malicious files and 99 % of tactics, techniques, and procedures used in advanced persistent threats attacks. A unique feature of the research is the integration of the Artificial Intelligence assistant, which automates threat analysis processes and speeds up response times by leveraging historical data and the context of past incidents. This reduces the workload on cybersecurity specialists and improves the overall effectiveness of the detection system, allowing for the quick identification of new threats and a reduction in false positives. Practical application of the results is possible in various critical sectors, including financial institutions, government organizations, and energy companies. The system demonstrates high flexibility and scalability, making it possible to easily adapt to different infrastructures and types of threats.

Keywords: advanced persistent threat, intrusion detection systems, machine learning, anomaly detection, large language models.

References

1. The swiss cheese model of security and why its important to have multiple layers of security. Firm Guardian. Available at: https://www.firmguardian.com/blog/swiss-cheese-model
2. McKee, F., Noever, D. (2023). Chatbots in a Botnet World. International Journal on Cybernetics & Informatics, 12 (2), 77–95. https://doi.org/10.5121/ijci.2023.120207
3. Ruby, A. R., Banu, A., Priya, S., Chandran, S. (2023). Taxonomy of AISecOps Threat Modeling for Cloud Based Medical Chatbots. arXiv. https://doi.org/10.48550/arXiv.2305.11189
4. Third-Party Cybersecurity Risk Management: A Short Guide for 2024. Available at: https://flare.io/learn/resources/blog/third-party-cybersecurity-risk-management/
5. Hassannataj Joloudari, J., Haderbadi, M., Mashmool, A., Ghasemigol, M., Band, S. S., Mosavi, A. (2020). Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning. IEEE Access, 8, 186125–186137. https://doi.org/10.1109/access.2020.3029202
6. Li, S., Dong, F., Xiao, X., Wang, H., Shao, F., Chen, J. et al. (2024). NODLINK: An Online System for Fine-Grained APT Attack Detection and Investigation. Proceedings 2024 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2024.23204
7. Wang, N., Wen, X., Zhang, D., Zhao, X., Ma, J., Luo, M. et al. (2023). TBDetector:Transformer-Based Detector for Advanced Persistent Threats with Provenance Graph. arXiv. https://doi.org/10.48550/arXiv.2304.02838
8. Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., Djukic, P. (2022). Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats. ACM Computing Surveys, 55 (5), 1–37. https://doi.org/10.1145/3530812
9. Pham, V.-H., Nghi Hoang, K., Duy, P. T., Ngo Duc Hoang, S., Huynh Thai, T. (2024). Xfedhunter: An Explainable Federated Learning Framework for Advanced Persistent Threat Detection in Sdn. https://doi.org/10.2139/ssrn.4883207
10. Zhang, R., Sun, W., Liu, J.-Y. (2020). Construction of two statistical anomaly features for small-sample APT attack traffic classification. arXiv. http://dx.doi.org/10.48550/arXiv.2010.13978
11. Jia, B., Tian, Y., Zhao, D., Wang, X., Li, C., Niu, W. et al. (2021). Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack. Information Security and Cryptology, 37–52. https://doi.org/10.1007/978-3-030-71852-7_3

12. Getting Started with Windows Security and Windows Defender. Institute for Advanced Study. Available at: https://www.ias.edu/security/getting-started-with-windows-security-windows-defender
13. Downloads. Available at: https://www.snort.org/downloads
14. About data models. Splunk. Available at: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutdatamodels
15. VMware Workstation Pro: Now Available Free for Personal Use. VMware Workstation Zealot. Available at: https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html
16. Redcanaryco/atomic-red-team. Small and highly portable detection tests based on MITRE's ATT&CK. GitHub. Available at: https://github.com/redcanaryco/atomic-red-team
17. Piskozub, A., Zhuravchak, D., Tolkachova, A. (2023). Researching vulnerabilities in chatbots with LLM (large language model). Ukrainian Scientific Journal of Information Security, 29 (3), 111–117. https://doi.org/10.18372/2225-5036.29.18069
18. Sysmon v15.15. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

DOI: 10.15587/1729-4061.2024.317471

EVALUATION AND OPTIMIZATION OF THE NAIVE BAYES ALGORITHM FOR INTRUSION DETECTION SYSTEMS USING THE USB-IDS-1 DATASET (p. 74–82)

Nurbek Konyrbaev
Korkyt Ata Kyzylorda University, Kyzylorda, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-8788-4149

Yevheniy Nikitenko
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-9222-644X

Vadym Shtanko
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0009-0001-4977-1450

Valerii Lakhno
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9695-4543

Zharasbek Baishemirov
Abai Kazakh National Pedagogical University, Almaty, Republic of Kazakhstan
Kazakh-British Technical University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-4812-4104

Sabit Ibadulla
Korkyt Ata Kyzylorda University, Kyzylorda, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-1312-8690

Asem Galymzhankyzy
Korkyt Ata Kyzylorda University, Kyzylorda, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0004-4624-8797

Erkebula Myrzabek
Korkyt Ata Kyzylorda University, Kyzylorda, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0006-6676-8102

This study takes a look into the application of the Naive Bayes machine learning algorithm to enhance the accuracy of Intrusion Detection Systems (IDS). The primary focus is to assess the algorithm's performance in detecting various types of network attacks, particularly Denial of Service (DoS) attacks. This research proposes using Naive Bayes to improve intrusion detection systems that struggle to keep pace with evolving cyber threats. This study evaluated the efficiency scores of the Naive Bayes classifying model for two different dependency scenarios and identified strong and weak properties of this model. The Naive Bayes classifier demonstrated satisfactory results in detecting network intrusions, especially in binary classification scenarios where the goal is to distinguish normative and malicious traffic due to its simplicity and efficiency. However, its performance declined in multi-class classification tasks, where multiple types of attacks need to be differentiated. The study also highlighted the importance of data quality and quantity in training machine learning models because of the impact of those parameters on the model efficiency. The USB-IDS-1 dataset, while useful, has limitations in terms of the variety of attacks. Using datasets with a wider range of attack types could significantly improve the accuracy of IDS. The findings of this research can be applied to such domains as network security, cybersecurity, and data science. The Naive Bayes classifier can be integrated into IDS systems to enhance their ability to detect and respond to cyber threats. However, it is essential to consider the limitations of the algorithm and the specific conditions of its environment. To maximize the effectiveness of the Naive Bayes classifier, it could be promising to optimize and normalize the data to improve the accuracy of the model and combine Naive Bayes with the other machine learning algorithms to address its limitations.

Keywords: intrusion detection systems (IDS), Naive Bayes method, python, machine learning, Denial of Service (DoS) attacks, USB-IDS-1 dataset.

References

1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32 (1). https://doi.org/10.1002/ett.4150
2. Moustafa, N., Slay, J. (2015). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015 Military Communications and Information Systems Conference (MilCIS), 1–6. https://doi.org/10.1109/milcis.2015.7348942
3. Dwibedi, S., Pujari, M., Sun, W. (2020). A Comparative Study on Contemporary Intrusion Detection Datasets for Machine Learning Research. 2020 IEEE International Conference on Intelligence and Security Informatics (ISI). https://doi.org/10.1109/isi49825.2020.9280519
4. Chatzoglou, E., Kambourakis, G., Kolias, C. (2021). Empirical Evaluation of Attacks Against IEEE 802.11 Enterprise Networks: The AWID3 Dataset. IEEE Access, 9, 34188–34205. https://doi.org/10.1109/access.2021.3061609
5. Jose, J., Jose, D. V. (2023). Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset. International Journal of Electrical and Computer Engineering (IJECE), 13 (1), 1134. https://doi.org/10.11591/ijece.v13i1.pp1134-1141
6. Catillo, M., Del Vecchio, A., Ocone, L., Pecchia, A., Villano, U. (2021). USB-IDS-1: a Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation. 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 1–6. https://doi.org/10.1109/dsn-w52860.2021.00012

7. Özsarı, M. V., Özsarı, Ş., Aydın, A., Güzel, M. S. (2024). USB-IDS-1 dataset feature reduction with genetic algorithm. Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, 66 (1), 26–44. https://doi.org/10.33769/aupse.1320795
8. Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer Communications, 199, 113–125. https://doi.org/10.1016/j.comcom.2022.12.010
9. Zou, L., Luo, X., Zhang, Y., Yang, X., Wang, X. (2023). HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering. IEEE Access, 11, 21404–21416. https://doi.org/10.1109/access.2023.3251354
10. Sammut, C., Webb, G. I. (2010). Encyclopedia of Machine Learning. Springer New York, 1031. https://doi.org/10.1007/978-0-387-30164-8
11. Gushin, I., Sych, D. (2018). Analysis of the Impact of Text Preproccessing on the Results of Text Classification. Young Scientist, 10 (62), 264–266. Available at: https://molodyivchenyi.ua/index.php/journal/article/view/3755
12. Shkarupylo, V., Lakhno, V., Konyrbaev, N., Baishemirov, Z., Adranova, A., Derbessal, A. (2024). Hierarchical model for building composite web services. Journal of Mathematics, Mechanics and Computer Science, 122 (2), 124–137. https://doi.org/10.26577/jmmcs2024-122-02-b10
13. USB-IDS Datasets. Universita Degli Studi del Sannio. Available at: https://idsdata.ding.unisannio.it/datasets.html

DOI: 10.15587/1729-4061.2024.318585

OPTIMIZATION OF DATA TRANSMISSION IN SENSOR NETWORKS FOR ENHANCED CONTROL OF OZONATOR EFFICIENCY (p. 83–94)

Askar Abdykadyrov
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1143-4675

Sunggat Marxuly
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-7330-5927

Gulzhaina Tolen
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-6010-1167

Ainur Kuttybayeva
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-7281-3690

Mukhit Abdullayev
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0002-3349-1881

Gulnar Sharipova
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-6703-3013

The main object of the research is the efficiency of real-time ozonator control based on sensor networks. The study addressed the issue of low efficiency in ozonator control systems and the lack of reliability and speed in real-time data transmission. The research revealed that changes in pressure and temperature have a direct impact on ozone concentration. This finding made it possible to increase the ozonator's productivity by 15 %, reduce energy consumption by 10 %, and improve system reliability by 20 %. The key features of the results include the ability to monitor ozone levels in real-time, maintaining the stability of the ozonator, and optimizing its performance. Additionally, sensor networks ensured fast and accurate data delivery, enhancing the energy efficiency and reliability of the system. These results were explained based on experimental data that demonstrated how changes in pressure and temperature affect ozone concentration. The use of sensor networks contributed to increased system stability, reduced energy consumption, and improved control accuracy. The obtained results can be applied to ozonator systems and other fields requiring real-time environmental monitoring and control. The methods proposed in the study provide opportunities for optimizing industrial processes, reducing costs, and achieving sustainable development goals.

Keywords: sensor networks, real-time control, ozonator efficiency, effect of pressure and temperature, ozone concentration, energy efficiency, system reliability.

References

1. Sydykova, G., Umbetova, S., Baimakhanova, Z., Abieva, G., Kurmanbayev, G. (2023). Modern Applications of Ozone Technology. Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 10 (04). https://doi.org/10.5109/7160908
2. Abdykadyrovk, A., Marxulyk, S., Baikenzheyeva, A., Bakyt, G., Abdullayev, S., Kuttybayeva, A. E. (2023). Research of the Process of Ozonation and Sorption Filtration of Natural and Anthropogenicly Pollated Waters. Journal of Environmental Management and Tourism, 14 (3), 811. https://doi.org/10.14505/jemt.v14.3(67).20
3. Abdykadyrov, A., Marxuly, S., Kuttybayeva, A., Almuratova, N., Yermekbayev, M., Ibekeyev, S. et al. (2023). Study of the Process of Destruction of Harmful Microorganisms in Water. Water, 15 (3), 503. https://doi.org/10.3390/w15030503
4. Draginsky, V. L., Alekseeva, L. P., Samoilovich, V. G. (2007). Ozonation in water purification processes. Moscow: Delhi Print, 190.
5. Brodowska, A. J., Nowak, A., Śmigielski, K. (2017). Ozone in the food industry: Principles of ozone treatment, mechanisms of action, and applications: An overview. Critical Reviews in Food Science and Nutrition, 58 (13), 2176–2201. https://doi.org/10.1080/10408398.2017.1308313
6. Chys, M., Audenaert, W. T. M., Stapel, H., Ried, A., Wieland, A., Weemaes, M. et al. (2018). Techno-economic assessment of surrogate-based real-time control and monitoring of secondary effluent ozonation at pilot scale. Chemical Engineering Journal, 352, 431–440. https://doi.org/10.1016/j.cej.2018.07.041
7. Petani, L., Koker, L., Herrmann, J., Hagenmeyer, V., Gengenbach, U., Pylatiuk, C. (2020). Recent Developments in Ozone Sensor Technology for Medical Applications. Micromachines, 11 (6), 624. https://doi.org/10.3390/mi11060624
8. Manfredi, J. (2019). Ozone Applications in Biotech and Pharmaceuticals. Filtration and Purification in the Biopharmaceutical Industry, 609–626. https://doi.org/10.1201/9781315164953-24
9. İbanoğlu, Ş. (2023). Applications of ozonation in the food industry. Non-Thermal Food Processing Operations, 55–91. https://doi.org/10.1016/b978-0-12-818717-3.00003-2
10. Iqbal, M. M., Muhammad, G., Hussain, M. A., Hanif, H., Raza, M. A., Shafiq, Z. (2023). Recent trends in ozone sensing technology. Analytical Methods, 15 (23), 2798–2822. https://doi.org/10.1039/d3ay00334e
11. Petruci, J. F. da S., Barreto, D. N., Dias, M. A., Felix, E. P., Cardoso, A. A. (2022). Analytical methods applied for ozone gas detection: A review. TrAC Trends in Analytical Chemistry, 149, 116552. https://doi.org/10.1016/j.trac.2022.116552

12. Williams, D. E., Henshaw, G. S., Bart, M., Laing, G., Wagner, J., Naisbitt, S., Salmond, J. A. (2013). Validation of low-cost ozone measurement instruments suitable for use in an air-quality monitoring network. Measurement Science and Technology, 24 (6), 065803. https://doi.org/10.1088/0957-0233/24/6/065803
13. Thomas, G. W., Sousan, S., Tatum, M., Liu, X., Zuidema, C., Fitzpatrick, M. et al. (2018). Low-Cost, Distributed Environmental Monitors for Factory Worker Health. Sensors, 18 (5), 1411. https://doi.org/10.3390/s18051411
14. Yi, W., Lo, K., Mak, T., Leung, K., Leung, Y., Meng, M. (2015). A Survey of Wireless Sensor Network Based Air Pollution Monitoring Systems. Sensors, 15 (12), 31392–31427. https://doi.org/10.3390/s151229859
15. Rodríguez-Peña, M., Barrios Pérez, J. A., Lobato, J., Saez, C., Barrera-Díaz, C. E., Rodrigo, M. A. (2022). Influence of pressure and cell design on the production of ozone and organic degradation. Separation and Purification Technology, 297, 121529. https://doi.org/10.1016/j.seppur.2022.121529
16. Homola, T., Pongrác, B., Zemánek, M., Šimek, M. (2019). Efficiency of Ozone Production in Coplanar Dielectric Barrier Discharge. Plasma Chemistry and Plasma Processing, 39 (5), 1227–1242. https://doi.org/10.1007/s11090-019-09993-6
17. Lewis, A., Peltier, W. R., von Schneidemesser, E. (Eds.) (2018). Low-cost sensors for the measurement of atmospheric composition: overview of topic and future applications. World Meteorological Organization. Available at: https://eprints.whiterose.ac.uk/135994/1/WMO_Low_cost_sensors_post_review_final.pdf
18. Chang, M. B., Wu, S.-J. (1997). Experimental Study on Ozone Synthesis via Dielectric Barrier Discharges. Ozone: Science & Engineering, 19 (3), 241–254. https://doi.org/10.1080/01919519708547304
19. Park, Y., Dong, K.-Y., Lee, J., Choi, J., Bae, G.-N., Ju, B.-K. (2009). Development of an ozone gas sensor using single-walled carbon nanotubes. Sensors and Actuators B: Chemical, 140 (2), 407–411. https://doi.org/10.1016/j.snb.2009.04.055
20. Janssen, C., Simone, D., Guinet, M. (2011). Preparation and accurate measurement of pure ozone. Review of Scientific Instruments, 82 (3), 034102. https://doi.org/10.1063/1.3557512
21. Kaiser, H.-P., Köster, O., Gresch, M., Périsset, P. M. J., Jäggi, P., Salhi, E., von Gunten, U. (2013). Process Control For Ozonation Systems: A Novel Real-Time Approach. Ozone: Science & Engineering, 35 (3), 168–185. https://doi.org/10.1080/01919512.2013.772007
22. Kalandarov, P., Murodova, G. (2024). Study on microprocessor control of agricultural greenhouse microclimate. E3S Web of Conferences, 497, 03026. https://doi.org/10.1051/e3sconf/202449703026
23. Jodzis, S., Baran, K. (2022). The influence of gas temperature on ozone generation and decomposition in ozone generator. How is ozone decomposed? Vacuum, 195, 110647. https://doi.org/10.1016/j.vacuum.2021.110647
24. Majewski, J. (2012). Methods for measuring ozone concentration in ozone-treated water. Przegląd Elektrotechniczny (Electrical Review), 88, 253–255. Available at: http://pe.org.pl/articles/2012/9b/61.pdf
25. Nakagawa, H., Okazaki, S., Asakura, S., Shimizu, H., Iwamoto, I. (2001). A new ozone sensor for an ozone generator. Sensors and Actuators B: Chemical, 77 (1-2), 543–547. https://doi.org/10.1016/s0925-4005(01)00696-7
26. Abdykadyrov, A. A., Korovkin, N. V., Tashtai, E. T., Syrgabaev, I., Mamadiyarov, M. M., Sunggat, M. (2021). Research of the process of disinfection and purification of drinking water using ETRO-02 plant based on high-frequency corona discharge. 2021 3rd International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 1–4. https://doi.org/10.1109/reepe51337.2021.9388046
27. Abdykadyrov, A. A., Korovkin, N. V., Mamadiyarov, M. M., Tashtay, Y., Domrachev, V. N. (2020). Practical Research of Efficiency of the Installation Etro-02 Ozonizer Based on the Corona Discharge. 2020 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 1–5. https://doi.org/10.1109/reepe49198.2020.9059150
28. Kozhaspaev, N., Makanov, U., Bokanova, A. A., Abdykadyrov, A. A., Dagarbek, R., Kodzhavergenova, A. K. (2016). Experience in application of ozonic technology for sewage treatment in the Kumkul region of Kazakhstan. Journal of Industrial Pollution Control, 32 (2), 486–489. Available at: https://www.icontrolpollution.com/articles/experience-in-application-of-ozonic-technology-for-sewage-treatment-in-the-kumkul-region-of-kazakhstan.php?aid=79551
29. Ando, M., Biju, V., Shigeri, Y. (2018). Development of Technologies for Sensing Ozone in Ambient Air. Analytical Sciences, 34 (3), 263–267. https://doi.org/10.2116/analsci.34.263
30. Abdykadyrov, A. A., Kozhaspaev, N. K., Dagarbek, R., Rakhimov, D. T., Turdybek, B. (2014). Innovation Pat. No. 28562. Device for obtaining an ozone-air mixture "ETRO-02". Available at: https://kz.patents.su/patents/abdykadyrov-askar-ajjtmyrzaevich
31. Nakagawa, H., Okazaki, S., Asakura, S., Iwamoto, I., Shimizu, H. (2001). Sensing characteristics of a newly developed ozone sensor. Analytical Sciences/Supplements, 17, i253–i256. https://doi.org/10.14891/analscisp.17icas.0.i253.0

АНОТАЦІЇ

INFORMATION TECHNOLOGY. INDUSTRY CONTROL SYSTEMS

DOI: 10.15587/1729-4061.2024.317103

РОЗПІЗНАВАННЯ МІН ЗА ДОПОМОГОЮ МОБІЛЬНОГО ДОДАТКУ (с. 6–13)

О. В. Кунічік

Об'єктом дослідження є розпізнавання вибухонебезпечних предметів на зображенні. Основна увага приділяється ідентифікації протипіхотних мін. Дослідження спрямоване на розробку ефективних інструментів для розпізнавання мін.

Розроблено мобільний додаток для розпізнавання вибухонебезпечних предметів за допомогою моделі глибокого навчання, навченої на репліках мін. Додаток протестований на зображеннях справжніх мін. Модель, що використовується в додатку, продемонструвала повноту 89 % (відношення кількості правильно розпізнаних мін до загальної кількості досліджуваних мін на зображенні). За допомогою програми було виявлено, що для одного з класів мін повнота була нижчою, ніж для інших. Середній час розпізнавання зображення в офлайн режимі склав 2.1 секунди.

Представлено результати оцінки ефективності мобільного додатку для розпізнавання і класифікації мін. Також описано, як додаток дозволяє покращувати модель завдяки збору даних від користувачів. Описано архітектуру та інтерфейс програми, а також проаналізовано перспективи її застосування для розпізнавання мін.

Ефективність мобільного додатку зумовлена його простотою використання, високою точністю моделі глибокого навчання та можливістю легкого отримання зворотного зв'язку від користувачів. Програма дозволяє не тільки розпізнати небезпечні об'єкти, а й за бажанням відправити дані для покращення моделі.

Мобільний додаток може бути використаний для вирішення широкого кола завдань, пов'язаних з виявленням вибухонебезпечних предметів, а також для покращення точності моделі. Додатково, програма може бути використана в навчальних центрах для саперів, а також безпосередньо на місцевості, забрудненій мінами. Мобільний додаток може бути використаний для ідентифікації невідомих вибухонебезпечних об'єктів та покращення роботи моделей глибокого навчання. Отримані моделі можуть бути використані в майбутньому для автоматизації процесу розмінування.

Ключові слова: виявлення мін, розпізнавання мін, пошук вибухонебезпечних предметів, гуманітарне розмінування.

DOI: 10.15587/1729-4061.2024.317092

ПОКРАЩЕННЯ РОЗПІЗНАВАННЯ ДІЙ НА ОСНОВІ СКЕЛЕТА ЗА ДОПОМОГОЮ ГІБРИДНИХ РЕАЛЬНИХ ТА ЗГЕНЕРОВАНИХ НАБОРАМИ ДАНИХ (с. 14–22)

Talgat Islamgozhayev, Beibut Amirgaliyev, Zhanibek Kozhirbayev

Це дослідження стосується критичної проблеми розпізнавання взаємних дій за участю кількох осіб, важливого завдання для таких програм, як відеоспостереження, взаємодія людини з комп'ютером, автономні системи та аналіз поведінки. Ідентифікація цих дій із тривимірних послідовностей рухів скелета створює значні проблеми через необхідність точного захоплення складних просторових і часових моделей у різноманітних, динамічних і часто непередбачуваних середовищах. Щоб вирішити цю проблему, було розроблено надійну структуру нейронної мережі, яка поєднує згорткові нейронні мережі (CNN) для ефективного вилучення просторових ознак із мережами довготривалої короткочасної пам'яті (LSTM) для моделювання часових залежностей у розширених послідовностях. Відмінною рисою цього дослідження є створення гібридного набору даних, який поєднує дані про рух скелета в реальному світі з синтетично згенерованими зразками, створеними за допомогою генеративних змагальних мереж (GAN). Цей набір даних збагачує варіативність, покращує узагальнення та пом'якшує проблеми дефіциту даних. Експериментальні результати в трьох різних мережевих архітектурах демонструють, що запропонований в даному дослідженні метод значно підвищує точність розпізнавання, в основному завдяки інтеграції CNN і LSTM разом із розширеним набором даних. Такий підхід успішно визначає складні взаємодії та забезпечує стабільну продуктивність у різних точках зору та в умовах навколишнього середовища. Підвищена надійність розпізнавання вказує на те, що цю структуру можна ефективно використовувати в практичних програмах, таких як системи безпеки, моніторинг натовпу та інших областях, де точне виявлення взаємних дій є критичним, особливо в реальному часі та динамічних середовищах.

Ключові слова: розпізнавання дій, згорткова нейронна мережа, генеративні змагальні мережі, LSTM.

DOI: 10.15587/1729-4061.2024.318554

ОПТИМІЗАЦІЯ СТИСНЕННЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ (с. 23–35)

О. А. Литвин, Н. М. Колос

Об'єктом дослідження є штучні нейронні мережі адаптивної резонансної теорії (ART). Штучні нейронні мережі ART класифікують, зіставляючи вхідні дані з одним з існуючих класів, за умови, що дані мають достатню схожість з прототипами класів. Безперервні та дискретні адаптивні мережі теорії резонансу ART-1 та ART-2 ефективно працюють в системах розпізнавання, особливо в умовах високої невизначеності, коли потрібно ідентифікувати велику кількість різних зображень.

Основна проблема, що вирішувалася в даному дослідженні, полягала в оптимізації процесу стиснення зображень за допомогою штучних нейронних мереж, адже стиснення зображень широко використовується в багатьох науково-технічних галузях і стає особливо актуальним при передачі по вузькосмугових каналах зв'язку. Варіантом подолання відповідних труднощів може бути підбір основних даних для реконструкції із відкритого набору даних (Modified National Institute of Standards and Technology) – Fashion MNIST. Залишаються невирішеними питання, пов'язані з тим, що алгоритми стиснення з втратами при збільшенні ступеня стиснення як правило породжують добре помітні для людського ока артефакти.

Описано алгоритм стиснення на основі штучних нейронних мереж, який встановлює відповідність між вхідним і вихідним просторами, що складаються з елементів кодової книги і нейронів. Варіантом подолання втрати якості при збільшенні ступеня стиснення може бути об'єднання двох добре відомих алгоритмів: штучної нейронної мережі Кохонена і зірки Гроссберга Запропонований метод використовує інший підхід (першого порядку), а не просту схему різницевого кодування (нульового порядку), де новий код обчислюється шляхом віднімання попереднього закодованого блоку. Пікове співвідношення сигналу до шуму (peak signal-to-noise ratio) PSNR і середньоквадратичної похибки (MSE) цих алгоритмів становить 24,7 дБ при коефіцієнті стиснення 25,22.

Головна сфера практичного використання отриманих результатів полягає у покращеному стисненні зображення для потреб обробки великих за обсягом відео- та фотоматеріалів без значної втрати якості.

Ключові слова: стиснення зображень, обробка зображень, штучна нейронна мережа, метод стиснення, алгоритм стиснення.

DOI: 10.15587/1729-4061.2024.317456

РОЗРОБЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ В КІБЕРПРОСТОРІ УКРАЇНИ НА ОСНОВІ МАШИННОГО НАВЧАННЯ (с. 36–48)

В. А. Висоцька, М. А. Назаркевич, С. І. Владов, О. В. Лозинська, О. О. Марків, Р. В. Романчук, В. М. Данилик

Об'єктом дослідження є процеси виявлення дезінформації на основі пошукових алгоритмів ідентифікації фейкових новин. Основною проблемою є визначення множини критеріїв та параметрів виявлення україномовної дезінформації на основі машинного навчання. Розглянуто методику розроблення та наповнення датасету фейків для подальшого навчання моделі та проведення її тестування з метою ідентифікації дезінформації та пропаганди, визначення ознак першоджерел та маршрутів їх розповсюдження. Це дозволяє обґрунтовано підходити до визначення моделі прогнозування розвитку інформаційних загроз в кіберпросторі України. Зокрема, може бути підвищена точність автоматичного виявлення ймовірності дезінформації у текстах. Для англомовних текстів з використанням збалансованих датасетів для навчання при застосуванні класичних класифікаторів машинного навчання точність ідентифікації та розпізнавання фейку ≥90 %, а для україномовних текстів – ≥52 % та ≤90 %. Це дало можливість розробити вимоги до структури та наповнення типового датасету фейків в період після повномасштабного вторгнення Україну. Практичним результатом роботи є розроблена система підтримки прийняття рішень для моніторингу, виявлення, розпізнаванні та прогнозування інформаційних загрозах в кіберпросторі України на основі NLP та машинного навчання. Реалізація попереднього опрацювання україномовних новин з врахуванням лінгвістичних особливостей мови тексту збільшує точність ідентифікації фейку в ≈1.72 рази. Розроблено підходи до формування моделей прогнозування розвитку інформаційних загроз у кіберпросторі, що є актуальним завданням, коли фейкові новини та інформаційні маніпуляції можуть вплинути на суспільні настрої, політику та економіку.

Ключові слова: інформаційна загроза, фейкова новина, машинне навчання, виявлення дезінформації, датасет, кібербезпека.

DOI: 10.15587/1729-4061.2024.317000

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОГО МОДУЛЯ ВИЯВЛЕННЯ ОЗНАК ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА ПОЯВИ НЕДОСТОВІРНИХ ДАНИХ (с. 49–63)

І. Ю. Черепанська, А. Ю. Сазонов, Ю. В. Киричук, П. П. Мельничук, Д. П. Мельничук, Н. М. Назаренко, В. А. Прядко, С. О. Бахман, Д. В. Храбан

На етапі підготовки виробництва виникає гостра потреба в автоматизованій системі, яка б своєчасно виявляла ознаки загроз інформаційній безпеці та появи недостовірних даних. Для вирішення цієї проблеми розроблено інтелектуальний модуль, здатний виявляти такі загрози та недостовірні та/або аномальні дані. Запропонований інтелектуальний модуль є новітнім, оригінальним та ефективним інструментарієм. Він може бути рекомендований до практичного застосування у складі відомої інформаційно-комп'ютерної системи автоматизованого моделювання системи автоматичного орієнтування об'єктів виробництва на етапі технологічної підготовки машино- та приладобудівного виробництва. Його використання дозволяє підвищити інформаційну безпеку та достовірність важливих виробничих даних на етапі технологічної підготовки виробництва, зокрема при моделюванні систем автоматичного орієнтування об'єктів виробництва. Крім того застосування запропонованого інтелектуального модуля дозволяє отримати низку важливих соціальних та економічних ефектів. Деякі з цих ефектів проявляються у запобіганні або зменшенні матеріальних, інтелектуальних та часових витрат на збереження та відновлення інформації та ін.

Автоматизований аналіз важливих виробничих даних щодо їх достовірності та аномальності здійснюється методами машинного навчання із застосуванням спеціально розробленого розширеного варіаційного автокодувальника за алгоритмами класифікації та з використанням вейвлет-перетворення.

Розроблений інтелектуальний модуль виявлення ознак загрози інформаційній безпеці та появи недостовірних та/або аномальних даних працює в режимі реального часу з високою точністю, яка становить 97,53 %. Це відвідає вимогам сучасного виробництва.

Ключові слова: інформаційно-комп'ютерна система, автоматизоване моделювання, керування, штучний інтелект, гнучка виробнича система.

DOI: 10.15587/1729-4061.2024.318336

РОЗРОБКА ІНТЕГРОВАНОЇ СИСТЕМИ ГЛИБОКОГО ЗАХИСТУ З ПОМІЧНИКОМ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ШКІДЛИВИМ ПРОГРАМАМ (с. 64–73)

Д. Ю. Журавчак, М. Ю. Опанович, А. Ю. Толкачова, В. Б. Дудикевич, А. З. Піскозуб

Об'єктом дослідження є багаторівневі системи кіберзахисту для виявлення та протидії розвиненим сталим загрозам шляхом інтеграції технологій машинного навчання, штучного інтелекту та багаторівневих систем безпеки. Проблема полягає в необхідності розробки адаптивних систем виявлення, здатних ефективно реагувати на нові та модифіковані загрози. В ході дослідження розроблено інтегрований підхід. Він поєднує традиційні методи виявлення з сучасними технологіями, такими як машинне навчання та помічники Штучного інтелекту. Кожен із шарів системи показав різний рівень ефективності, наприклад, антивірусні рішення були найбільш ефективними у виявленні відомих загроз, але не змогли впоратися з модифікованими загрозами, які виявили кореляційні правила. Машинне навчання проявило себе найкраще у виявленні безфайлових атак та аномальної активності, яка не могла бути помічена іншими засобами. Отримані результати зумовлені ефективністю комбінації кількох рівнів захисту, де кожен наступний рівень компенсує недоліки попереднього. Антивірусні рішення виявили 100 % відомих загроз. Кореляційні правила виявили всі зловмисні файли. Загалом, система змогла виявити 98 % шкідливих файлів та 99 % тактик, технік і процедур, що використовуються під час атак типу постійної сталої загрози. Особливістю дослідження є інтеграція помічника Штучного інтелекту, що дозволяє автоматизувати процеси аналізу загроз і пришвидшити реагування завдяки використанню історичних даних та контексту минулих інцидентів. Це сприяє зменшенню навантаження на фахівців із кібербезпеки та покращує загальну ефективність системи виявлення загроз, дозволяючи швидко виявляти нові загрози та знижувати кількість хибних спрацювань. Практичне застосування результатів можливе в різних критичних секторах, зокрема у фінансових установах, урядових організаціях та енергетичних компаніях.

Ключові слова: постійна стала загроза, системи виявлення вторгнень, машинне навчання, виявлення аномалій, великі мовні моделі.

DOI: 10.15587/1729-4061.2024.317471

ОЦІНКА ТА ОПТИМІЗАЦІЯ НАЇВНОГО АЛГОРИТМУ БАЙЄСА ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРЖЕНЬ ЗА ВИКОРИСТАННЯМ НАБОРУ ДАНИХ USB-IDS-1 (с. 74–82)

Nurbek Konyrbaev, Yevheniy Nikitenko, Vadym Shtanko, Valerii Lakhno, Zharasbek Baishemirov, Sabit Ibadulla, Asem Galymzhankyzy, Erkebulan Myrzabek

У цьому дослідженні розглядається застосування наївного алгоритму машинного навчання Байєса для підвищення точності систем виявлення вторгнень (СВВ). Основна увага полягає в оцінці ефективності алгоритму при виявленні різних типів мережевих атак, зокрема атак типу «відмова в обслуговуванні». У цьому дослідженні пропонується використовувати наївний баєсів класифікатор для вдосконалення систем виявлення вторгнень, яким важко йти в ногу з кіберзагрозами, що розвиваються. У цьому дослідженні було оцінено показники ефективності моделі наївного баєсового класифікатора для двох різних сценаріїв залежності та визначено сильні та слабкі властивості цієї моделі. Наївний баєсів класифікатор продемонстрував задовільні результати у виявленні мережевих вторгнень, особливо в сценаріях бінарної класифікації, де метою є розрізнення нормативного та шкідливого трафіку завдяки його простоті та ефективності. Однак його продуктивність знизилася в завданнях багатокласової класифікації, де потрібно розрізняти кілька типів атак. Дослідження також підкреслило важливість якості та кількості даних у навчанні моделей машинного навчання через вплив цих параметрів на ефективність моделі. Набір даних USB-IDS-1, хоч і корисний, але має обмеження щодо різноманітності атак. Використання наборів даних із ширшим діапазоном типів атак може значно підвищити точність СВВ. Результати цього дослідження можна застосувати до таких областей, як мережева безпека, кібербезпека та наука про дані. Наївний баєсів класифікатор можна інтегрувати в системи СВВ, щоб покращити їхню здатність виявляти кіберзагрози та реагувати на них. Однак важливо враховувати обмеження алгоритму та специфічні умови його середовища. Щоб максимізувати ефективність наївного баєсового класифікатора, може бути перспективним оптимізувати та нормалізувати дані, щоб підвищити точність моделі та поєднати наївний баєсів класифікатор з іншими алгоритмами машинного навчання, щоб усунути його обмеження.

Ключові слова: системи виявлення вторгнень, наївний баєсів метод, Python, машинне навчання, атаки на відмову в обслуговуванні, набір даних USB-IDS-1.

DOI: 10.15587/1729-4061.2024.318585

ОПТИМІЗАЦІЯ ПЕРЕДАЧІ ДАНИХ В СЕНСОРНИХ МЕРЕЖАХ ДЛЯ ПОСИЛЕННЯ КОНТРОЛЮ ЕФЕКТИВНОСТІ ОЗОНАТОРА (с. 83–94)

Askar Abdykadyrov, Sunggat Marxuly, Gulzhaina Tolen, Ainur Kuttybayeva, Mukhit Abdullayev, Gulnar Sharipova

Основним об'єктом дослідження є ефективність керування озонатором у режимі реального часу на основі сенсорних мереж. Дослідження стосувалося проблеми низької ефективності систем керування озонаторами та недостатньої надійності та

швидкості передачі даних у реальному часі. Дослідження показало, що зміни тиску і температури безпосередньо впливають на концентрацію озону. Ця знахідка дозволила підвищити продуктивність озонатора на 15 %, зменшити енергоспоживання на 10 % і підвищити надійність системи на 20 %. Ключові характеристики результатів включають можливість моніторингу рівня озону в режимі реального часу, підтримання стабільності озонатора та оптимізацію його продуктивності. Крім того, сенсорні мережі забезпечували швидку та точну передачу даних, підвищуючи енергоефективність і надійність системи. Ці результати були пояснені на основі експериментальних даних, які продемонстрували як зміни тиску та температури впливають на концентрацію озону. Використання сенсорних мереж сприяло підвищенню стабільності системи, зниженню споживання енергії та підвищенню точності керування. Отримані результати можуть бути застосовані до озонаторних систем та інших галузей, що потребують моніторингу та контролю навколишнього середовища в режимі реального часу. Методи, запропоновані в дослідженні, надають можливості для оптимізації промислових процесів, зниження витрат і досягнення цілей сталого розвитку.

Ключові слова: сенсорні мережі, керування в режимі реального часу, ефективність озонатора, вплив тиску та температури, концентрація озону, енергоефективність, надійність системи.