ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2023.280055

DEVELOPMENT OF A NEW LIGHTWEIGHT ENCRYPTION ALGORITHM (p. 6–19)

Nursulu Kapalova
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-9743-9981

Kunbolat Algazy
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-3670-2170

Armanbek Haumen
Institute of Information and Computational Technologie, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-1670-2520

Lightweight encryption algorithms are considered a relatively new direction in the development of private key cryptography. This need arose as a result of the emergence of a large number of devices with little computing power and memory. Therefore, it became necessary to develop algorithms that can provide a sufficient level of security, with minimal use of resources. The paper presents a new lightweight LBC encryption algorithm. LBC is a 64–bit symmetric block algorithm. It supports 80 bit secret key. The number of rounds is 20. The algorithm has a Feistel network structure. The developed lightweight algorithm has a simple implementation scheme, and the transformations used in this algorithm have good cryptographic properties. This was verified by studying the cryptographic properties of the algorithm using the "avalanche effect" and statistical tests. The avalanche property was checked for each round when each bit of the source text was changed. Based on the work carried out, it was found that the proposed encryption algorithm is effective to ensure a good avalanche effect and the binary sequence obtained after encryption is close to random. Its security against linear and differential cryptanalysis is also evaluated. The results of the research revealed good cryptographic properties of this algorithm. The algorithm will be used for devices with small hardware resources, in information and communication systems where confidential information circulates, and it is also extremely necessary to exchange information in a protected form in an operationally acceptable time.

Keywords: encryption algorithm, lightweight algorithm, cryptographic transformations, avalanche effect, cryptographic stability.

References

1. Usman, M., Ahmed, I., Imran, M., Khan, S., Ali, U. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. International Journal of Advanced Computer Science and Applications, 8 (1). doi: https://doi.org/10.14569/ijacsa.2017.080151
2. Yun, J., Kim, M. (2020). JLVEA: Lightweight Real-Time Video Stream Encryption Algorithm for Internet of Things. Sensors, 20 (13), 3627. doi: https://doi.org/10.3390/s20133627
3. Taresh, H. (2018). LT10 a lightweight proposed encryption algorithm for IOT. Iraqi Journal for Computers and Informatics, 44 (1), 1–5. doi: https://doi.org/10.25195/ijci.v44i1.64
4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L. (2013). Paper 2013/404. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2013/404
5. Gu, D., Li, J., Li, S., Ma, Z., Guo, Z., Liu, J. (2012). Differential Fault Analysis on Lightweight Blockciphers with Statistical Cryptanalysis Techniques. 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography. doi: https://doi.org/10.1109/fdtc.2012.16
6. Kumar V G, K., Rai C, S. (2021). Design and Implementation of Novel BRISI Lightweight Cipher for Resource Constrained Devices. Microprocessors and Microsystems, 84, 104267. doi: https://doi.org/10.1016/j.micpro.2021.104267
7. Yang, W., Wang, R., Guan, Z., Wu, L., Du, X., Guizani, M. (2020). A Lightweight Attribute Based Encryption Scheme with Constant Size Ciphertext for Internet of Things. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). doi: https://doi.org/10.1109/icc40277.2020.9149294
8. Kazlauskas, K., Kazlauskas, J. (2009). Key-Dependent S-Box Generation in AES Block Cipher System. Informatica, 20 (1), 23–34. doi: https://doi.org/10.15388/informatica.2009.235
9. Preneel, B. (2010). Perspectives on Lightweight Cryptography. Shanghai. Available at: https://homes.esat.kuleuven.be/~preneel/preneel_lightweight_shanghaiv1.pdf
10. Ivanov, G., Nikolov, N., Nikova, S. (2016). Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. Lecture Notes in Computer Science, 31–42. doi: https://doi.org/10.1007/978-3-319-29172-7_3
11. Horbenko, I. D., Horbenko, Yu. I. (2012). Prykladna kryptolohiya. Teoriya. Praktyka. Zastosuvannia. Kharkiv: Vydavnytstvo «Fort», 870.
12. Dey, S., Ghosh, R. (2018). A Review of Existing 4-Bit Crypto S-Box Cryptanalysis Techniques and Two New Techniques with 4-Bit Boolean Functions for Cryptanalysis of 4-Bit Crypto S-Boxes*. Advances in Pure Mathematics, 08 (03), 272–306. doi: https://doi.org/10.4236/apm.2018.83015
13. Khompysh, A., Kapalova, N., Algazy, K., Dyusenbayev, D., Sakan, K. (2022). Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. Cogent Engineering, 9 (1). doi: https://doi.org/10.1080/23311916.2022.2080623
14. Kapalova, N. A., Khaumen, A., Sақan, K. (2020). Rasseivayuschie svoystva lineynykh preobrazovaniy. Mater. nauch. konf. IIVT MON RK «Sovremennye problemy informatiki i vychislitel'nykh tekhnologiy». Almaty, 191–196. Available at: https://conf.iict.kz/wp-content/uploads/2020/10/mpcsct-collection-08.07.2020-final.pdf
15. Lisitskaya, I. V., Nastenko, A. A. (2011). Great ciphers - casual substitution. Radiotekhnika, 166, 50–55. Available at: https://openarchive.nure.ua/bitstream/document/15255/1/Radiotehnika_V166_2011_rus.pdf
16. Teh, J. S., Tham, L. J., Jamil, N., Yap, W.-S. (2022). New differential cryptanalysis results for the lightweight block cipher BORON.

Journal of Information Security and Applications, 66, 103129. doi: https://doi.org/10.1016/j.jisa.2022.103129
17. Biham, E., Shamir, A. (1991). Differential Cryptanalysis of DES-like Cryptosystems. Lecture Notes in Computer Science, 2–21. doi: https://doi.org/10.1007/3-540-38424-3_1
18. Carlet, C. (2010). Vectorial Boolean Functions for Cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 398–470. doi: https://doi.org/10.1017/cbo9780511780448.012
19. Kim, J., Hong, S., Lim, J. (2010). Impossible differential cryptanalysis using matrix method. Discrete Mathematics, 310 (5), 988–1002. doi: https://doi.org/10.1016/j.disc.2009.10.019
20. Liu, Y., Liang, H., Wang, W., Wang, M. (2017). New Linear Cryptanalysis of Chinese Commercial Block Cipher Standard SM4. Security and Communication Networks, 2017, 1–10. doi: https://doi.org/10.1155/2017/1461520
21. Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. Lecture Notes in Computer Science, 386–397. doi: https://doi.org/10.1007/3-540-48285-7_33
22. Liu, Z. (2021). Differential-linear cryptanalysis of PRINCE cipher. Chinese Journal of Network and Information Security, 7 (4), 131–140. doi: https://doi.org/10.11959/j.issn.2096-109x.2021072
23. Biryukov, A., De Cannière, C. (2011). Linear Cryptanalysis for Block Ciphers. Encyclopedia of Cryptography and Security, 722–725. doi: https://doi.org/10.1007/978-1-4419-5906-5_589
24. Borghoff, J. (2011). 4.6 Linear Cryptanalysis. Cryptanalysis of Lightweight Ciphers. Technical University of Denmark, 60–65. Available at: https://backend.orbit.dtu.dk/ws/portalfiles/portal/5456432/phd-thesis_Julia_Borghoff.pdf
25. Vergili, I., Yücel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Cho-sen S-Boxes. Turkish Journal of Electrical Engineering and Computer Sciences, 9 (2), 137–146. Available at: https://journals.tubitak.gov.tr/elektrik/vol9/iss2/3
26. Shnayer, B. (2002). Prikladnaya kriptografiya. Moscow:Triumf, 816.
27. Babenko, L. K., Ischukova, E. A. (2006). Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza. Moscow: «Gelios ARV», 376.
28. Algazy, K. T., Babenko, L. K., Biyashev, R. G., Ishchukova, E. A., Kapalova, N. A., Nysynbaeva, S. E., Smolarz, A. (2020). Differential Cryptanalysis of New Qamal Encryption Algorithm. International journal of electronics and telecommunications, 66 (4), 647–653. doi: https://doi.org/10.24425/ijet.2020.134023
29. O'Connor, L. (1995). Properties of linear approximation tables. Lecture Notes in Computer Science, 131–136. doi: https://doi.org/10.1007/3-540-60590-8_10
30. Kuznetsov, A. A., Lisitskaya, I. V., Isaev, S. A. (2011). Lineynye svoystva blochnykh simmetrichnykh shifrov, predstavlennykh na ukrainskiy konkurs. Prikladnaya radioelektronika, 10 (2), 135–140.
31. Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. Cryptologia, 26 (3), 189–221. doi: https://doi.org/10.1080/0161-110291890885
32. Kapalova, N., Sakan, K., Algazy, K., Dyusenbayev, D. (2022). Development and Study of an Encryption Algorithm. Computation, 10 (11), 198. doi: https://doi.org/10.3390/computation10110198
33. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B. et al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. Lecture Notes in Computer Science, 450–466. doi: https://doi.org/10.1007/978-3-540-74735-2_31

DOI: 10.15587/1729-4061.2023.282131

DEVISING A METHOD FOR DETECTING "EVIL TWIN" ATTACKS ON IEEE 802.11 NETWORKS (WI-FI) WITH KNN CLASSIFICATION MODEL (p. 20–32)

Roman Banakh
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0001-6897-8206

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

Ivan Opirskyy
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-8461-8996

The object of research is IEEE 802.11 (Wi-Fi) networks, which are often the targets of a group of attacks called "evil twin". Research into this area is extremely important because Wi-Fi technology is a very common method of connecting to a network and is usually the first target of cybercriminals when they attack businesses. With the help of a systematic analysis of the literature focused on countering attacks of the "evil twin" type, this work identifies the main advantages of using artificial intelligence systems in the analysis of network data and identification of intrusions in Wi-Fi networks. To evaluate the effectiveness of intrusion detection and cybercrime analysis, a number of experiments as close as possible to real attacks on Wi-Fi networks were conducted.

As part of the research reported in this paper, a method is proposed for detecting cybercrimes in IEEE 802.11 (Wi-Fi) wireless networks using artificial intelligence, namely a model built on the basis of the k-nearest neighbors method. This method is based on the classification of previously collected data, namely the signal strength from the access point, and then continuous comparison of the newly collected data with the trained model.

A compact and energy-efficient prototype of a hardware and software system has been designed for the implementation of monitoring, analysis of ethernet network packets and data storage based on time series. In order to reduce the load on the computer network and taking into account the limited computing power of the system, a method of data aggregation was proposed, which ensures fast transfer of information.

The results, namely 100 % of test cases (more than 7 thousand), were classified correctly, which indicates that the chosen method of data analysis will significantly increase the security of information and communication systems at the state and private levels.

Keywords: IEEE 802.11, Wi-Fi, evil twin, machine learning, classification, triangulation, cyber security.

References

1. Nagpal, J., Patil, R., Jain, V., Pokhriyal, R., Rajawat, R. (2018). Evil Twin Attack and Its Detection. International Journal of Emerging Technologies and Innovative Research, 5 (12), 169–171. doi: https://www.jetir.org/view?paper=JETIR1812326
2. Bednarczyk, M., Piotrowski, Z. (2019). Will WPA3 really provide Wi-Fi security at a higher level? XII Conference on Reconnaissance and Electronic Warfare Systems. doi: https://doi.org/10.1117/12.2525020
3. Vanhoef, M., Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. 2020 IEEE Sympo-

sium on Security and Privacy (SP). doi: https://doi.org/10.1109/sp40000.2020.00031
4. Value of Wi-Fi. Wi-Fi Alliance. Available at: https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi
5. Forbes, G., Massie, S., Craw, S. (2020). WiFi-based Human Activity Recognition using Raspberry Pi. 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI). doi: https://doi.org/10.1109/ictai50040.2020.00115
6. Banakh, R., Piskozub, A. (2018). Attackers' Wi-Fi Devices Metadata Interception for their Location Identification. 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). doi: https://doi.org/10.1109/idaacs-sws.2018.8525538
7. Lu, Q., Qu, H., Zhuang, Y., Lin, X.-J., Ouyang, Y. (2018). Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames. IEICE Transactions on Information and Systems, E101.D (10), 2465–2473. doi: https://doi.org/10.1587/transinf.2018edp7030
8. Modi, V., Parekh, C. (2017). Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network. International Journal of Engineering Research And, V6 (04). doi: https://doi.org/10.17577/ijertv6is040102
9. Kuo, E.-C., Chang, M.-S., Kao, D.-Y. (2018). User-side evil twin attack detection using time-delay statistics of TCP connection termination. 2018 20th International Conference on Advanced Communication Technology (ICACT). doi: https://doi.org/10.23919/icact.2018.8323699
10. Agarwal, M., Biswas, S., Nandi, S. (2018). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. International Journal of Wireless Information Networks, 25 (2), 130–145. doi: https://doi.org/10.1007/s10776-018-0396-1
11. Banakh, R., Piskozub, A., Opirskyy, I. (2018). Detection of MAC Spoofing Attacks in IEEE 802.11 Networks Using Signal Strength from Attackers' Devices. Advances in Computer Science for Engineering and Education, 468–477. doi: https://doi.org/10.1007/978-3-319-91008-6_47
12. Harsha, S. et al. (2019). Improving Wi-Fi security against evil twin attack using light weight machine learning application. COMPUSOFT, 8 (3). Available at: https://www.researchgate.net/publication/332344245_Improving_Wi-Fi_security_against_evil_twin_attack_using_light_weight_machine_learning_application
13. Dong, Y., Zampella, F., Alsehly, F. (2023). Beyond KNN: Deep Neighborhood Learning for WiFi-based Indoor Positioning Systems. 2023 IEEE Wireless Communications and Networking Conference (WCNC). doi: https://doi.org/10.1109/wcnc55385.2023.10118752
14. Yang, C., Song, Y., Gu, G. (2012). Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. IEEE Transactions on Information Forensics and Security, 7 (5), 1638–1651. doi: https://doi.org/10.1109/tifs.2012.2207383
15. Scapy. Available at: https://scapy.net/
16. InfluxDB. Available at: https://www.influxdata.com/
17. NumPy. Available at: https://numpy.org/
18. Pandas. Available at: https://pandas.pydata.org/
19. Matplotlib. Available at: https://matplotlib.org/
20. Seaborn. Available at: https://seaborn.pydata.org/
21. Salkind, N. J., Frey, B. B. (2019). Statistics for people who (think they) hate statistics. SAGE Publications, 76–102.
22. Scikit-Learn. Available at: https://scikit-learn.org/stable/
23. Mladenova, T., Valova, I. (2021). Analysis of the KNN Classifier Distance Metrics for Bulgarian Fake News Detection. 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). doi: https://doi.org/10.1109/hora52670.2021.9461333
24. Taunk, K., De, S., Verma, S., Swetapadma, A. (2019). A Brief Review of Nearest Neighbor Algorithm for Learning and Classification. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). doi: https://doi.org/10.1109/iccs45141.2019.9065747
25. sklearn.metrics.classification_report. Available at: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.classification_report.html

DOI: 10.15587/1729-4061.2023.281795

DEVELOPMENT OF AN IMPROVED SSL/TLS PROTOCOL USING POST-QUANTUM ALGORITHMS (p. 33–48)

Serhii Yevseiev
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1647-6444

Alla Havrylova
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2015-8927

Stanislav Milevskyi
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5087-7036

Igor Sinitsyn
Institute of Software Systems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4120-0784

Volodymyr Chalapko
Military Institute for Tank Troops, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-9833-9851

Hennady Dukin
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-7245-7673

Vitalii Hrebeniuk
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5169-8694

Mykhailo Diedov
Scientific-Research Institute of Military Intelligence, Kyiv, Ukraine
ORCID: https://orcid.org/0009-0001-4003-8316

Lala Bekirova
Azerbaijan State Oil and Industry University, Baku, Azerbaijan
ORCID: https://orcid.org/0000-0003-0584-7916

Oleksandr Shpak
Uzhhorod National University, Uzhhorod, Ukraine
ORCID: https://orcid.org/0000-0002-1179-7196

The development of Internet technologies together with mobile and computer technologies have formed smart technologies that allow the formation of both cyber-physical and socio-cyber-physical

systems. The basis of smart technologies is the integration of wireless channel standards with mobile and computer protocols. 4G/5G technologies are integrated with various web platforms, taking into account the digitalization of services in cyberspace. But the SSL/TLS protocol, based on the hybridization of symmetric encryption algorithms with hashing algorithms (AEAD mode), which is supposed to provide security services, is vulnerable to "Meet in the middle", POODLE, BEAST, CRIME, BREACH attacks. In addition, with the advent of a full-scale quantum computer, symmetric and asymmetric cryptography algorithms that provide security services can also be hacked. To increase the level of security, an improved protocol based on post-quantum algorithms – crypto-code constructions is proposed, which will ensure not only resistance to current attacks, but also stability in the post-quantum period. To ensure the "hybridity" of services, it is proposed to use the McEliece and Niederreiter crypto-code constructions (confidentiality and integrity are ensured) and the improved UMAC algorithm on the McEliece crypto-code construction. Taking into account the level of "secrecy" of information, it is suggested to use various combinations of crypto-code constructions on different algebraic geometric and/or flawed codes. The use of crypto-code constructions not only prоł vides resistance to attacks, but also simplifies the formation of a connection – the parameters of elliptic curves are used to transmit a common key. This approach significantly reduces the connection time of mobile gadgets and simplifies the procedure of agreement before data transfer.

Keywords: improved SSL/TLS protocol, post-quantum encryption algorithms, improved UMAC algorithm, algebraic geometric codes, flawed codes.

References

1. Arora, J. et al. (2023). Securing web documents by using piggy-backed framework based on Newton's forward interpolation method. Journal of Information Security and Applications, 75, 103498. doi: https://doi.org/10.1016/j.jisa.2023.103498
2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: https://doi.org/10.15587/978-617-7319-57-2
3. Saribas, S., Tonyali, S. (2022). Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures. 2022 7th International Conference on Computer Science and Engineering (UBMK). doi: https://doi.org/10.1109/ubmk55850.2022.9919545
4. Khan, N. A., Khan, A. S., Kar, H. A., Ahmad, Z., Tarmizi, S., Julaihi, A. A. (2022). Employing Public Key Infrastructure to Encapsulate Messages During Transport Layer Security Handshake Procedure. 2022 Applied Informatics International Conference (AiIC). doi: https://doi.org/10.1109/aiic54368.2022.9914605
5. Ramraj, S., Usha, G. (2023). Signature identification and user activity analysis on WhatsApp Web through network data. Microprocessors and Microsystems, 97, 104756. doi: https://doi.org/10.1016/j.micpro.2023.104756
6. Nie, P., Wan, C., Zhu, J., Lin, Z., Chen, Y., Su, Z. (2023). Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementations. ACM Transactions on Software Engineering and Methodology, 32 (1), 1–32. doi: https://doi.org/10.1145/3510416
7. Berbecaru, D. G., Petraglia, G. (2023). TLS-Monitor: A Monitor for TLS Attacks. 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC). https://doi.org/10.1109/ccnc51644.2023.10059989
8. Wang, K., Zheng, Y., Zhang, Q., Bai, G., Qin, M., Zhang, D., Dong, J. S. (2022). Assessing certificate validation user interfaces of WPA supplicants. Proceedings of the 28th Annual International Conference on Mobile Computing And Networking. doi: https://doi.org/10.1145/3495243.3517026
9. Kottur, S. Z., Kadiyala, K., Tammana, P., Shah, R. (2022). Implementing ChaCha based crypto primitives on programmable SmartNICs. Proceedings of the ACM SIGCOMM Workshop on Formal Foundations and Security of Programmable Network Infrastructures. doi: https://doi.org/10.1145/3528082.3544833
10. Chen, L., Li, X., Yang, Z., Qian, S. (2022). Blockchain-based high transparent PKI authentication protocol. Chinese Journal of Network and Information Security, 8 (4), 1–11. doi: https://doi.org/10.11959/j.issn.2096-109x.2022052
11. Zhang, Z., Zhang, H., Wang, J., Hu, X., Li, J., Yu, W. et al. (2023). QKPT: Securing Your Private Keys in Cloud With Performance, Scalability and Transparency. IEEE Transactions on Dependable and Secure Computing, 20 (1), 478–491. doi: https://doi.org/10.1109/tdsc.2021.3137403
12. Zhou, Z., Bin, H., Li, J., Yin, Y., Chen, X., Ma, J., Yao, L. (2022). Malicious encrypted traffic features extraction model based on unsupervised feature adaptive learning. Journal of Computer Virology and Hacking Techniques, 18 (4), 453–463. doi: https://doi.org/10.1007/s11416-022-00429-y
13. Bertok, C., Huszti, A., Kovacs, S., Olah, N. (2022). Provably secure identity-based remote password registration. Publicationes Mathematicae Debrecen, 100, 533–565. doi: https://doi.org/10.5486/pmd.2022.suppl.1
14. Aayush, A., Aryan, Y., Muniyal, B. (2022). Understanding SSL Protocol and Its Cryptographic Weaknesses. 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). doi: https://doi.org/10.1109/iciem54221.2022.9853153
15. Guo, S., Zhang, F., Song, Z., Zhao, Z., Zhao, X., Wang, X., Luo, X. (2022). Detection of SSL/TLS protocol attacks based on flow spectrum theory. Chinese Journal of Network and Information Security, 8 (1), 30–40. doi: https://doi.org/10.11959/j.issn.2096-109x.2022004
16. Arunkumar, B., Kousalya, G. (2022). Secure and Light Weight Elliptic Curve Cipher Suites in SSL/TLS. Computer Systems Science and Engineering, 40 (1), 179–190. doi: https://doi.org/10.32604/csse.2022.018166
17. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2
18. Gavrilova, A., Volkov, I., Kozhedub, Y., Korolev, R., Lezik, O., Medvediev, V. et al. (2020). Development of a modified UMAC algorithm based on cryptocode constructions. Eastern-European Journal of Enterprise Technologies, 4 (9 (106)), 45–63. doi: https://doi.org/10.15587/1729-4061.2020.210683
19. Guide for Cybersecurity Event Recovery. NIST. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf

20. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
21. Guide to LTE Security. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-187/draft/documents/sp800_187_draft.pdf
22. Report on Post-Quantum Cryptography. Available at: https://csrc.nist.gov/publications/detail/nistir/8105/final
23. Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer. doi: https://doi.org/10.1007/978-3-540-88702-7
24. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. doi: https://doi.org/10.15587/1729-4061.2022.254545
25. Korol, O., Havrylova, A., Yevseiev, S. (2019). Practical UMAC algorithms based on crypto code designs. Przetwarzanie, transmisja i bezpieczenstwo informacji. Vol. 2. Bielsko-Biala: Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 221–232.
26. Carter, J. L., Wegman, M. N. (1979). Universal classes of hash functions. Journal of Computer and System Sciences, 18 (2), 143–154. doi: https://doi.org/10.1016/0022-0000(79)90044-8
27. Bierbrauer, J., Johansson, T., Kabatianskii, G., Smeets, B. (2001). On Families of Hash Functions via Geometric Codes and Concatenation. Lecture Notes in Computer Science, 331–342. doi: https://doi.org/10.1007/3-540-48329-2_28
28. Bettaieb, S., Bidoux, L., Blazy, O., Cottier, B., Pointcheval, D. (2023). Post-quantum and UC-Secure Oblivious Transfer from SPHF with Grey Zone. Lecture Notes in Computer Science, 54–70. doi: https://doi.org/10.1007/978-3-031-30122-3_4
29. Mishhenko, V. A., Vilanskij, Ju. V., (2007). Ushherbnye teksty i mnogokanal'naja kriptografija [Damaged texts and multichannel cryptography]. Minsk: Jenciklopediks, 292.
30. Mishhenko, V. A., Vilanskij, Ju. V., Lepin, V. V. (2006) "Kriptograficheskij algoritm MV 2 [Cryptographic algorithm MV 2]. Minsk: Jenciklopediks, 176.

DOI: 10.15587/1729-4061.2023.281287

EFFECIENCY ASSESSMENT OF IOT DEVICES CONTROL WITH TELETRAFFIC THEORY (p. 49–59)

Madina Konyrova
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-6577-9965

Saule Kumyzbayeva
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-3175-2435

Teodor Iliev
"Angel Kanchev" University of Ruse, Ruse, Bulgaria
ORCID: https://orcid.org/0000-0003-2214-8092

Katipa Chezhimbayeva
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-1661-2226

In connection with the global decarbonization program until 2050, the transition to clean green energy, the growth of the Internet of Things (IoT) number, and energy distribution and control across the load are being raised. The relevance of the work is confirmed that there has been significant growth of the industrial IoT for years, significantly changing the mechanism of industrial enterprise management programs. The object of the research is the IoT device control system for efficient energy distribution using a Queuing Theory, namely the Teletraffic Theory. The novelty of the work is that the Teletraffic Theory, which deals with the mathematical modeling and analysis of traffic patterns in communication networks, can be explicitly applied to IoT device control. The authors developed a mathematical model of IoT control using the Teletraffic Theory and, based on it, created a simulation model of a network router and a transition schedule in the "GPSS World" software. The obtained results of the work were 16 states and a balance equation in which all probabilities were found. Probabilities were used to calculate nodes and network characteristics. 100,000 requests from IoT devices coming to two routers were simulated. The study results showed that the first node's load is 63.2 % with an average processing time per transaction of M=1.436 sec., and the load of the second node is 32 % with M=0.914 sec. The created network router model worked with minimal losses during transactions. Accordingly, the IoT control system developed in this study has shown its effectiveness and is applicable for practical use in controlling IoT devices in Smart Grid. It is planned to research the possibility of using Teletraffic Theory in energy distribution control systems in Smart Grids.

Keywords: teletraffic theory, queuing theory, IoT devices, nett work router simulation model, GPSS world.

References

1. Zaman, A., Hassan, Z., Odarchenko, R., Hassan, S., Ahmed, S., Bilal, M. et al. (2020). Wireless Underground Sensor Networks: Packet Size Optimization Survey. Proceedings of the 2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN 2020). Available at: https://ceur-ws.org/Vol-2616/paper30.pdf
2. Sahraoui, Y., Korichi, A., Kerrache, C. A., Bilal, M., Amadeo, M. (2020). Remote sensing to control respiratory viral diseases outbreaks using Internet of Vehicles. Transactions on Emerging Telecommunications Technologies, 33 (10). doi: https://doi.org/10.1002/ett.4118
3. Vaghani, A., Sood, K., Yu, S. (2022). Security and QoS issues in blockchain enabled next-generation smart logistic networks: A tutorial. Blockchain: Research and Applications, 3 (3), 100082. doi: https://doi.org/10.1016/j.bcra.2022.100082
4. Taherdoost, H. (2023). Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics, 12 (8), 1901. doi: https://doi.org/10.3390/electronics12081901
5. Ashraf, U., Ahmed, A., Al-Naeem, M., Masood, U. (2021). Reliable and QoS aware routing metrics for wireless Neighborhood Area Networking in smart grids. Computer Networks, 192, 108051. doi: https://doi.org/10.1016/j.comnet.2021.108051
6. Ortiz-Garcés, I., Andrade, R. O., Sanchez-Viteri, S., Villegas-Ch., W. (2023). Prototype of an Emergency Response System Using IoT in a Fog Computing Environment. Computers, 12 (4), 81. doi: https://doi.org/10.3390/computers12040081
7. Shreenidhi, H. S., Ramaiah, N. S. (2022). A two-stage deep convolutional model for demand response energy management system in

IoT-enabled smart grid. Sustainable Energy, Grids and Networks, 30, 100630. doi: https://doi.org/10.1016/j.segan.2022.100630

8. Alavikia, Z., Shabro, M. (2022). A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey. Digital Communications and Networks, 8 (3), 388–410. doi: https://doi.org/10.1016/j.dcan.2022.01.002
9. Bhavani, N. G., Kumar, R., Panigrahi, B. S., Balasubramanian, K., Arunsundar, B., Abdul-Samad, Z., Singh, A. (2022). Design and implementation of iot integrated monitoring and control system of renewable energy in smart grid for sustainable computing network. Sustainable Computing: Informatics and Systems, 35, 100769. doi: https://doi.org/10.1016/j.suscom.2022.100769
10. Bogachev, M. I., Kuzmenko, A. V., Markelov, O. A., Pyko, N. S., Pyko, S. A. (2023). Approximate waiting times for queuing systems with variable long-term correlated arrival rates. Physica A: Statistical Mechanics and Its Applications, 614, 128513. doi: https://doi.org/10.1016/j.physa.2023.128513
11. Alghamdi, N. S., Khan, M. A., Karamti, H., Nawaz, N. A. (2022). Internet of Things (IoT) enabled smart queuing model to support massive safe crowd at Ka'aba. Alexandria Engineering Journal, 61 (12), 12713–12723. doi: https://doi.org/10.1016/j.aej.2022.06.053
12. Ibrahim, A. S., Al-Mahdi, H., Nassar, H. (2022). Characterization of task response time in a fog-enabled IoT network using queueing models with general service times. Journal of King Saud University - Computer and Information Sciences, 34 (9), 7089–7100. doi: https://doi.org/10.1016/j.jksuci.2021.09.008
13. Gelenbe, E., Nakıp, M., Czachórski, T. (2022). Improving Massive Access to IoT Gateways. Performance Evaluation, 157–158, 102308. doi: https://doi.org/10.1016/j.peva.2022.102308
14. Gelenbe, E., Sigman, K. (2022). IoT Traffic Shaping and the Massive Access Problem. ICC 2022 - IEEE International Conference on Communications. doi: https://doi.org/10.1109/icc45855.2022.9839054
15. IoT Traffic Generation Patterns Dataset. Available at: https://www.kaggle.com/datasets/tubitak1001118e277/iot-traffic-generation-patterns
16. He, Z., Ning, L., Jiang, B., Li, J., Wang, X. (2023). Vehicle Intersections Prediction Based on Markov Model with Variable Weight Optimization. Sustainability, 15 (8), 6943. doi: https://doi.org/10.3390/su15086943
17. Huang, J., Gao, H., Wan, S., Chen, Y. (2023). AoI-aware energy control and computation offloading for industrial IoT. Future Generation Computer Systems, 139, 29–37. doi: https://doi.org/10.1016/j.future.2022.09.007
18. Chezhimbayeva, K., Konyrova, M., Kumyzbayeva, S., Kadylbekkyzy, E. (2021). Quality assessment of the contact center while implementation the IP IVR system by using teletraffic theory. Eastern-European Journal of Enterprise Technologies, 6 (3 (114)), 64–71. doi: https://doi.org/10.15587/1729-4061.2021.244976
19. Konyrova, M., Kumyzbayeva, S., Kadylbekkyzy, E., Stoyak, V. (2021). Analysis of Direct Load Control in Smart Grids by using Teletraffic Theory. The 7th International Conference on Engineering & MIS 2021. doi: https://doi.org/10.1145/3492547.3492571
20. Kingman, J. F. C. (1961). The single server queue in heavy traffic. Mathematical Proceedings of the Cambridge Philosophical Society, 57 (4), 902–904. doi: https://doi.org/10.1017/s0305004100036094
21. Kendall, D. G. (1953). Stochastic Processes Occurring in the Theory of Queues and their Analysis by the Method of the Imbedded Markov Chain. The Annals of Mathematical Statistics, 24 (3), 338–354. doi: https://doi.org/10.1214/aoms/1177728975
22. Erlang, A. K. (1917). Solution of Some Problems in the Theory of Probabilities of Significance in Automatic Telephone Exchanges. Post Office Electrical Engineer's Journal 10, 189–197. Available at: https://www.scirp.org/(S(vtj3fa45qm1ean45wffcz5%205))/reference/referencespapers.aspx?referenceid=2834641
23. Wentzel, E. S. (2001). Operations Research: Tasks, Principles, Methodology. Moscow: Vysshaya shola, 210.
24. Aliyev, T. I. (2009). Fundamentals of modeling discrete systems. Saint Petersburg.
25. Konyrova, M., Kumyzbayeva, S., Iliev, T. B., Kadylbekkyzy, E. (2022). Smart Grid Network Control Model Based on Blockchain. 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES). doi: https://doi.org/10.1109/ciees55704.2022.9990792

DOI: 10.15587/1729-4061.2023.282374

DETERMINATION OF THE NUMBER OF CLUSTERS ON IMAGES FROM SPACE OPTIC-ELECTRONIC OBSERVATION SYSTEMS USING THE K-MEANS ALGORITHM (p. 60–69)

Hennadii Khudov
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-3311-2848

Oleksandr Makoveichuk
Academician Yuriy Bugay International Scientific and Technical University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-4425-016X

Volodymyr Komarov
Scientific-Research Institute of Military Intelligence, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-2873-8261

Vladyslav Khudov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-9863-4743

Irina Khizhnyak
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-3431-7631

Volodymyr Bashynskyi
The Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-0966-5714

Stanislav Stetsiv
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-1835-9874

Yevhen Dudar
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-3103-8672

Andrii Rudiy
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-2239-2925

Mykhailo Buhera
Central Scientifically-Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-0339-6085

The object of research is the process of clustering images from space optical-electronic surveillance systems. The main hypothesis of the study assumed that experimental studies would make it possible to determine the number of clusters on images from space optical-electronic surveillance systems when using the k-means algorithm.

The method of clustering images from space optical-electronic surveillance systems using the k-means algorithm, unlike the known ones, implies:

– splitting the source image into Red-Green-Blue brightness channels;

– determination of the Euclidean distance between pixels;

– distribution of the entire set of image pixels into clusters;

– recalculation of "centers" of each subset;

– reassignment of new "centers" of each cluster;

– minimization of the total intracluster variance.

Experimental studies were conducted on the clustering of the original image using the k-means method at different values of k. It was established that with an increase in the value of k, the visual quality of clustering improves, and it is possible to visually determine a larger number of clusters in the images.

To determine the number of clusters, the sum of clustering errors of type 1 and 2 at different values of k was evaluated. It was established that when the value of k increases, the sum of errors of the 1st and 2nd kind initially decreases exponentially. A further increase in the value of k does not lead to a significant decrease in errors of the 1st and 2nd kind. It was established that for a typical image from the space optical-electronic observation system, the value of k in the clustering method based on the k-means algorithm should be equal to 4. At the same time, the sum of errors of the 1st and 2nd kind is 31.3 %.

Further research is directed to the development of clustering methods that reduce the sum of errors of the 1st and 2nd kind.

Keywords: image clustering, space observation system, k-means, errors of the 1st and 2nd kind, number of clusters.

References

1. Green, M. (2020). K-Means Clustering for Surface Segmentation of Satellite Images. Available at: https://medium.com/@maxfieldeland/k-means-clustering-for-surface-segmentation-of-satellite-images-ad1902791ebf
2. Lafabregue, B., Gancarski, P., Weber, J., Forestier, G. (2022). Incremental constrained clustering with application to remote sensing images time series. 2022 IEEE International Conference on Data Mining Workshops (ICDMW). doi: https://doi.org/10.1109/icdmw58026.2022.00110
3. Lampert, T., Lafabregue, B., Dao, T.-B.-H., Serrette, N., Vrain, C., Gancarski, P. (2019). Constrained Distance-Based Clustering for Satellite Image Time-Series. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 12 (11), 4606–4621. doi: https://doi.org/10.1109/jstars.2019.2950406
4. Space, the unseen frontier in the war in Ukraine (2022). BBC News. Available at: https://www.bbc.com/news/technology-63109532
5. Khudov, H., Makoveichuk, O., Khizhnyak, I., Shamrai, B., Glukhov, S., Lunov, O. et al. (2022). The Method for Determining Informative Zones on Images from On-Board Surveillance Systems. International Journal of Emerging Technology and Advanced Engineering, 12 (8), 61–69. doi: https://doi.org/10.46338/ijetae0822_08
6. Samanta, S., Chatterjee, S. (2018). A Survey On Data Clustering Approaches. 1st International Business Research Conference (IBRC 2018), 34–42. Available at: https://www.researchgate.net/publication/341134327_A_Survey_On_Data_Clustering_Approaches
7. Pandey, S., Khanna, P. (2014). A hierarchical clustering approach for image datasets. 2014 9th International Conference on Industrial and Information Systems (ICIIS). doi: https://doi.org/10.1109/iciinfs.2014.7036504
8. Aktas, Y. C. (2021). Image Segmentation with Clustering. The Fundamentals of K-Means and Fuzzy-C Means Clustering and their usage for Image Segmentation. Towards Data Science. – 2021. Available at: https://towardsdatascience.com/image-segmentation-with-clustering-b4bbc98f2ee6
9. Dhanachandra, N., Manglem, K., Chanu, Y. J. (2015). Image Segmentation Using K -means Clustering Algorithm and Subtractive Clustering Algorithm. Procedia Computer Science, 54, 764–771. doi: https://doi.org/10.1016/j.procs.2015.06.090
10. Funmilola, A. A., Oke, O. A., Adedeji, T. O., Alade, O. M., Adewusi, E. A. (2012). Fuzzy k-c-means Clustering Algorithm for Medical Image Segmentation. Journal of Information Engineering and Applications, 2 (6), 21–33. Available at: https://core.ac.uk/download/pdf/234676965.pdf
11. Kishor Duggirala, R. (2020). Segmenting Images Using Hybridization of K-Means and Fuzzy C-Means Algorithms. Introduction to Data Science and Machine Learning. doi: https://doi.org/10.5772/intechopen.86374
12. NamAnh, D. (2015). Segmentation by Incremental Clustering. International Journal of Computer Applications, 111 (12), 23–30. doi: https://doi.org/10.5120/19591-1360
13. Niharika, E., Adeeba, H., Krishna, A. S. R., Yugander, P. (2017). K-means based noisy SAR image segmentation using median filtering and otsu method. 2017 International Conference on IoT and Application (ICIOT). doi: https://doi.org/10.1109/iciota.2017.8073630
14. Zheng, X., Lei, Q., Yao, R., Gong, Y., Yin, Q. (2018). Image segmentation based on adaptive K-means algorithm. EURASIP Journal on Image and Video Processing, 2018 (1). doi: https://doi.org/10.1186/s13640-018-0309-3
15. Hess, T., Sabato, S. (2020). Sequential no-Substitution k-Median-Clustering. 23rd International Conference on Artificial Intelligence and Statistics (AISTATS), 108, 962–972. Available at: https://proceedings.mlr.press/v108/hess20a.html
16. Shah, N., Patel, D., Fränti, P. (2021). k-Means image segmentation using Mumford–Shah model. Journal of Electronic Imaging, 30 (06). doi: https://doi.org/10.1117/1.jei.30.6.063029
17. Wang, C., Pedrycz, W., Li, Z., Zhou, M., Ge, S. S. (2021). G-Image Segmentation: Similarity-Preserving Fuzzy C-Means With Spatial Information Constraint in Wavelet Space. IEEE Transactions on Fuzzy Systems, 29 (12), 3887–3898. doi: https://doi.org/10.1109/tfuzz.2020.3029285
18. Khosla, R. (2020). An Approach towards Neural Network based Image Clustering. Analytics Vidhya. Available at: https://www.analyticsvidhya.com/blog/2020/12/an-approach-towards-neural-network-based-image-clustering/

19. Li, H., Li, J., Zhu, M. (2023). End-to-end unsupervised clustering neural networks for image clustering. doi: https://doi.org/10.36227/techrxiv.22147559.v2
20. Guérin, J., Boots, B. (2018). Improving Image Clustering With Multiple Pretrained CNN Feature Extractors. Available at: https://homes.cs.washington.edu/~bboots/files/GuerinBMVC18.pdf
21. Benito-Picazo, J., Palomo, E. J., Dominguez, E., Ramos, A. D. (2020). Image Clustering Using a Growing Neural Gas with Forbidden Regions. 2020 International Joint Conference on Neural Networks (IJCNN). doi: https://doi.org/10.1109/ijcnn48605.2020.9207700
22. Zhang, L.-F., Li, C.-F., Wang, H.-R., Shi, M.-Y. (2018). Research On Face Image Clustering Based On Integrating Som And Spectral Clustering Algorithm. 2018 International Conference on Machine Learning and Cybernetics (ICMLC). doi: https://doi.org/10.1109/icmlc.2018.8526946
23. Ke, S., Zhao, Y., Li, B., Wu, Z., Liu, X. (2016). Fast image clustering based on convolutional neural network and binary K-means. Eighth International Conference on Digital Image Processing (ICDIP 2016). doi: https://doi.org/10.1117/12.2244263
24. Al-Qaisi, L., Hassonah, M. A., Al-Zoubi, M. M., Al-Zoubi, A. M. (2021). A Review of Evolutionary Data Clustering Algorithms for Image Segmentation. Algorithms for Intelligent Systems, 201–214. doi: https://doi.org/10.1007/978-981-33-4191-3_9
25. Abeysinghe, W., Wong, M., Hung, C.-C., Bechikh, S. (2019). Multi-Objective Evolutionary Algorithm for Image Segmentation. 2019 SoutheastCon. doi: https://doi.org/10.1109/southeastcon42311.2019.9020457
26. Khudov, H., Makoveichuk, O., Butko, I., Gyrenko, I., Stryhun, V., Bilous, O. et al. (2022). Devising a method for segmenting camouflaged military equipment on images from space surveillance systems using a genetic algorithm. Eastern-European Journal of Enterprise Technologies, 3 (9 (117)), 6–14. doi: https://doi.org/10.15587/1729-4061.2022.259759
27. Ruban, I., Khudov, H., Makoveichuk, O., Khudov, V., Kalimulin, T., Glukhov, S. et al. (2022). Methods of UAVs images segmentation based on k-means and a genetic algorithm. Eastern-European Journal of Enterprise Technologies, 4 (9 (118)), 30–40. doi: https://doi.org/10.15587/1729-4061.2022.263387
28. Ruban, I., Khudov, H., Makoveichuk, O., Butko, I., Glukhov, S., Khizhnyak, I. et al. (2022). Application of the Particle Swarm Algorithm to the Task of Image Segmentation for Remote Sensing of the Earth. Lecture Notes in Networks and Systems, 573–585. doi: https://doi.org/10.1007/978-981-19-5845-8_40
29. Khudov, H., Makoveichuk, O., Khizhnyak, I., Oleksenko, O., Khazhanets, Y., Solomonenko, Y. et al. (2022). Devising a method for segmenting complex structured images acquired from space observation systems based on the particle swarm algorithm. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 6–13. doi: https://doi.org/10.15587/1729-4061.2022.255203
30. Khudov, H., Makoveichuk, O., Khudov, V., Maliuha, V., Andriienko, A., Tertyshnik, Y. et al. (2022). Devising a method for segmenting images acquired from space optical and electronic observation systems based on the Sine-Cosine algorithm. Eastern-European Journal of Enterprise Technologies, 5 (9 (119)), 17–24. doi: https://doi.org/10.15587/1729-4061.2022.265775
31. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V. et al. (2019). Segmentation of optical-electronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. Eastern-European Journal of Enterprise Technologies, 2 (9 (98)), 37–45. doi: https://doi.org/10.15587/1729-4061.2019.161860
32. Satellite Imagery. Available at: https://www.maxar.com/products/satellite-imagery
33. Khudov, G. V. (2003). Features of optimization of two-alternative decisions by joint search and detection of objects. Problemy Upravleniya I Informatiki (Avtomatika), 5, 51–59. Available at: https://www.researchgate.net/publication/291431400_Features_of_optimization_of_two-alternative_decisions_by_joint_search_and_detection_of_objects
34. Khudov, H., Makoveichuk, O., Misiuk, D., Pievtsov, H., Khizhnyak, I., Solomonenko, Y. et al. (2022). Devising a method for processing the image of a vehicle's license plate when shooting with a smartphone camera. Eastern-European Journal of Enterprise Technologies, 1 (2 (115)), 6–21. doi: https://doi.org/10.15587/1729-4061.2022.252310
35. Khudov, H., Makoveichuk, O., Khizhnyak, I., Glukhov, S., Shamrai, N., Rudnichenko, S. et al. (2022). The Choice of Quality Indicator for the Image Segmentation Evaluation. International Journal of Emerging Technology and Advanced Engineering, 12 (10), 95–103. doi: https://doi.org/10.46338/ijetae1022_11

DOI: 10.15587/1729-4061.2023.279372

IMPROVING THE QUALITY OF OBJECT CLASSIFICATION IN IMAGES BY ENSEMBLE CLASSIFIERS WITH STACKING (p. 70–77)

Oleg Galchonkov
Odessa Polytechnic National University, Odessa, Ukraine
ORCID: https://orcid.org/0000-0001-5468-7299

Oleksii Baranov
Oracle World Headquarters, Austin, USA
ORCID: https://orcid.org/0009-0002-5951-2636

Mykola Babych
Digitally Inspired LTD, Leapale Lane, Guildford, United Kingdom
ORCID: https://orcid.org/0000-0002-3946-9880

Varvara Kuvaieva
Odessa Polytechnic National University, Odessa, Ukraine
ORCID: https://orcid.org/0000-0002-9350-1108

Yuliia Babych
Odessa Polytechnic National University, Odessa, Ukraine
ORCID: https://orcid.org/0000-0001-9966-2810

The object of research is the process of classifying objects in images. The quality of classification refers to the ratio of correctly recognized objects to the number of images. One of the options for improving the quality of classification is to increase the depth of neural networks used. The main difficulties along the way are the difficulty of training such neural networks and a large amount of computing that makes it difficult to use them on conventional computers in real time. An alternative way to improve the quality of classification is to increase the width of the neural networks used, by constructing ensemble classifiers with staking. However, they require the use of classifiers at the first stage with different structured processing of input images, characterized by high quality classification and relatively low volume of calculations. The number of known such architectures is limited. Therefore, the problem arises of increasing the number of classifiers at the first stage of the ensemble classifier by modifying known architectures. It is proposed to use blocks of

rotation of images at different angles relative to the center of the image. It is shown that as a result of structured image processing by the starting classifier, processing of rotated image leads to redistribution of errors on image set. This effect makes it possible to increase the number of classifiers in the first stage of the ensemble classifier. Numerical experiments have shown that adding two analogs of the MLP-Mixer algorithm to known configurations of ensemble classifiers reduced the error from 1 to 11 % when working with the CIFAR-10 dataset. Similarly, for CCT, the error reduction was between 2.1 and 10 %. In addition, it has been shown that increasing the MLP-Mixer configuration in width gives better results than increasing in depth. A prerequisite for the success of using the proposed approach in practice is the structured image processing by the starting classifier.

Keywords: multilayer perceptron, neural network, ensemble classifier, weighting coefficients, classification of objects in images.

References

1. Mary Shanthi Rani, M., Chitra, P., Lakshmanan, S., Kalpana Devi, M., Sangeetha, R., Nithya, S. (2022). DeepCompNet: A Novel Neural Net Model Compression Architecture. Computational Intelligence and Neuroscience, 2022, 1–13. doi: https://doi.org/10.1155/2022/2213273
2. Han, S., Mao, H., Dally, W. J. (2015). Deep compression: compressing deep neural networks with pruning, trained quantization and huffman coding. arXiv. doi: https://doi.org/10.48550/arXiv.1510.00149
3. Galchonkov, O., Nevrev, A., Glava, M., Babych, M. (2020). Exploring the efficiency of the combined application of connection pruning and source data preprocessing when training a multilayer perceptron. Eastern-European Journal of Enterprise Technologies, 2 (9 (104)), 6–13. doi: https://doi.org/10.15587/1729-4061.2020.200819
4. Iandola, F. N., Han, S., Moskewicz, M. W., Ashraf, K., Dally, W. J., Keutzer, K. (2016). SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size. arXiv. doi: https://doi.org/10.48550/arXiv.1602.07360
5. Wu, K., Guo, Y., Zhang, C. (2020). Compressing Deep Neural Networks With Sparse Matrix Factorization. IEEE Transactions on Neural Networks and Learning Systems, 31 (10), 3828–3838. doi: https://doi.org/10.1109/tnnls.2019.2946636
6. Cheng, X., Rao, Z., Chen, Y., Zhang, Q. (2020). Explaining Knowledge Distillation by Quantifying the Knowledge. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). doi: https://doi.org/10.1109/cvpr42600.2020.01294
7. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T. et al. (2021). An image is worth 16x16 words: transformers for image recognition at scale. arXiv. doi: https://doi.org/10.48550/arXiv.2010.11929
8. Yuan, L., Chen, Y., Wang, T., Yu, W., Shi, Y., Jiang, Z. et al. (2021). Tokens-to-Token ViT: Training Vision Transformers from Scratch on ImageNet. 2021 IEEE/CVF International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv48922.2021.00060
9. d'Ascoli, S., Touvron, H., Leavitt, M. L., Morcos, A. S., Biroli, G., Sagun, L. (2022). ConViT: improving vision transformers with soft convolutional inductive biases. Journal of Statistical Mechanics: Theory and Experiment, 2022 (11), 114005. doi: https://doi.org/10.1088/1742-5468/ac9830
10. Yuan, K., Guo, S., Liu, Z., Zhou, A., Yu, F., Wu, W. (2021). Incorporating Convolution Designs into Visual Transformers. 2021 IEEE/CVF International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv48922.2021.00062
11. Wu, H., Xiao, B., Codella, N., Liu, M., Dai, X., Yuan, L., Zhang, L. (2021). CvT: Introducing Convolutions to Vision Transformers. 2021 IEEE/CVF International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv48922.2021.00009
12. Galchonkov, O., Babych, M., Zasidko, A., Poberezhnyi, S. (2022). Using a neural network in the second stage of the ensemble classifier to improve the quality of classification of objects in images. Eastern-European Journal of Enterprise Technologies, 3 (9 (117)), 15–21. doi: https://doi.org/10.15587/1729-4061.2022.258187
13. Rokach, L. (2019). Ensemble Learning. Pattern Classification Using Ensemble Methods. World Scientific Publishing Co. doi: https://doi.org/10.1142/11325
14. Hassani, A., Walton, S., Shah, N., Abuduweili, A., Li, J., Shi, H. (2021). Escaping the Big Data Paradigm with Compact Transformers. arXiv. doi: https://doi.org/10.48550/arXiv.2104.05704
15. Guo, M.-H., Liu, Z.-N., Mu, T.-J., Hu, S.-M. (2022). Beyond Self-Attention: External Attention Using Two Linear Layers for Visual Tasks. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1–13. doi: https://doi.org/10.1109/tpami.2022.3211006
16. Lee-Thorp, J., Ainslie, J., Eckstein, I., Ontanon, S. (2022). FNet: Mixing Tokens with Fourier Transforms. Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. doi: https://doi.org/10.18653/v1/2022.naacl-main.319
17. Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z. et al. (2021). Swin Transformer: Hierarchical Vision Transformer using Shifted Windows. 2021 IEEE/CVF International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/iccv48922.2021.00986
18. Tolstikhin, I., Houlsby, N., Kolesnikov, A., Beyer, L., Zhai, X., Unterthiner, T. et al. (2021). MLP-Mixer: An all-MLP Architecture for Vision. arXiv. doi: https://doi.org/10.48550/arXiv.2105.01601
19. Liu, H., Dai, Z., So, D. R., Le, Q. V. (2021). Pay Attention to MLPs. arXiv. doi: https://doi.org/10.48550/arXiv.2105.08050
20. Brownlee, J. (2019). Deep Learning for Computer Vision. Image Classification, Object Detection, and Face Recognition in Python. Available at: https://machinelearningmastery.com/deep-learning-for-computer-vision/
21. Brownlee, J. (2019). Better Deep Learning. Train Faster, Reduce Overfitting, and Make Better Predictions. Available at: https://machinelearningmastery.com/better-deep-learning/
22. Krizhevsky A. The CIFAR-10 dataset. Available at: https://www.cs.toronto.edu/~kriz/cifar.html
23. Code examples / Computer vision. Keras. Available at: https://keras.io/examples/vision/
24. Brownlee, J. (2021). Weight Initialization for Deep Learning Neural Networks. Available at: https://machinelearningmastery.com/weight-initialization-for-deep-learning-neural-networks/
25. Colab. Available at: https://colab.research.google.com/notebooks/welcome.ipynb

DOI: 10.15587/1729-4061.2023.279891

DEVELOPMENT OF A HYBRID NEURAL NETWORK MODEL FOR MINE DETECTION BY USING ULTRAWIDEBAND RADAR DATA (p. 78–85)

Vasyl Lytvyn
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-9676-0180

Ivan Peleshchak
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-7481-8628

Roman Peleshchak
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-0536-3252

Oleksandr Mediakov
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-2580-3155

Petro Pukach
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-0359-5025

The object of the study is the architecture of a hybrid neural network for mine recognition using ultra-wideband radar data. The work solves the problem of filtering reflected signals with interference and recognizing mines detected by ultra-wideband (UWB) radar. A hybrid neural network model in combination with the Adam learning algorithm is proposed. Filtering of reflected signals from mines is carried out using an MLP (multilayer perceptron) filter, which selects low-amplitude parts of signals that carry information about a hidden mine from the entire reflected signal. Mine recognition is carried out by a Hilbert block and an oscillatory neural network, which are included in the structure of a hybrid neural network. The peculiarity of the obtained results, which allowed to solve the investigated problem, is the transformation of the signal frequency by the Hilbert block and the recognition of mines by the oscillatory neural network in the resonant mode. The three-layer MLP filter effectively filters out the unwanted component in the total signal reflected from the subsurface object, as the MSE (Mean Squared Error) of the MLP filter is $1 \cdot 10^{-5}$. If the frequency of the Hilbert signal is equal to the natural frequency of oscillations of neurons $\Omega_i^H = \omega_{ij}$, then the recognition of signals with a small amplitude from subsurface objects is carried out by an oscillatory neural network based on the resonant amplitude, which is indicated by a small value of cross-entropy. The proposed model of a hybrid neural network provides amplification of useful signals due to resonance and has higher performance compared to existing models of artificial neural networks. The practical significance of the obtained results lies in their application in the field of automated neural network technologies for detection and recognition of subsurface objects of various nature based on reflected radar signals with an amplitude at the noise level.

Keywords: multilayer perceptron-filter, Hilbert block, oscillatory neural network, resonance.

References

1. Daniels, D. J. (2004). Ground penetrating radar. London: IEEE. doi: https://doi.org/10.1049/pbra015e
2. Harmuth, H. (1981). Nonsinusoidal waves for radar and radiocommunications. New York: Academic Press, 404.
3. Taylor, J. D. (2012). Ultrawideband Radar: applications and design. Boca Raton: CRC Press. doi: https://doi.org/10.1201/b12356
4. Ristic, A., Govedarica, M., Vrtunski, M., Pctrovacki, D. (2014). Application of GPR for creating underground structure model of specific areas of interest. Proceedings of the 15th International Conference on Ground Penetrating Radar. Brussels, 450–455. doi: https://doi.org/10.1109/icgpr.2014.6970464
5. Liu, H., Huang, X., Xing, B., Cui, J., Spencer, B. F., uo Liu, Q. H. (2018). Estimating Azimuth of Subsurface Linear Targets By Polarimetric GPR. Proceedings of the IEEE International Geoscience and Remote Sensing Symposium. Valencia, 6784–6787. doi: https://doi.org/10.1109/igarss.2018.8517637
6. Zhao, S., Al-Qadi, I. L. (2019). Super-Resolution of 3-D GPR Signals to Estimate Thin Asphalt Overlay Thickness Using the XCMP Method. IEEE Transactions on Geoscience and Remote Sensing, 57 (2), 893–901. doi: https://doi.org/10.1109/tgrs.2018.2862627
7. Taflove, A., Hagness, S. (2005). Computational Electrodynamics: The Finite-Difference Time-Domain Method. London, Boston: Artech House, 629–670. doi: https://doi.org/10.1016/b978-012170960-0/50046-3
8. Liu, Y., Guo, L. X. (2016). FDTD investigation on GPR detecting of underground subsurface layers and buried objects. Proceedings of the IEEE MTT-S International Conference on Numerical Electromagnetic and Multiphysics Modeling and Optimization. Beijing. doi: https://doi.org/10.1109/nemo.2016.7561622
9. Giannakis, I., Giannopoulos, A., Warren, C. (2019). A Machine Learning-Based Fast-Forward Solver for Ground Penetrating Radar With Application to Full-Waveform Inversion. IEEE Transactions on Geoscience and Remote Sensing, 57 (7), 4417–4426. doi: https://doi.org/10.1109/tgrs.2019.2891206
10. Earp, S. L., Hughes, E. S., Elkins, T. J., Vickers, R. (1996). Ultra-wideband ground-penetrating radar for the detection of buried metallic mines. Proceedings of the 1996 IEEE National Radar Conference. Ann Arbor, 7–12. doi: https://doi.org/10.1109/nrc.1996.510648
11. Millot, P., Castanet, L., Casadebaig, L., Maaref, N., Gaugue, A., Menard, M. et al. (2015). An UWB Through-The-Wall radar with 3D imaging, detection and tracking capabilities. Proceedings of the European Radar Conference (EuRAD). Paris, 237–240. doi: https://doi.org/10.1109/eurad.2015.7346281
12. Hai-zhong, Y., Yu-feng, O., Hong, C. (2012). Application of ground penetrating radar to inspect the metro tunnel. Proceedings of the 14th International Conference on Ground Penetrating Radar (GPR). Shanghai, 759–763. doi: https://doi.org/10.1109/icgpr.2012.6254963
13. Holbling, Z., Mihaldinec, H., Ambrus, D., Dzapo, H., Bilas, V., Vasic, D. (2017). UWB localization for discrimination-enabled metal detectors in humanitarian demining. In Proceedings of the IEEE Sensors Applications Symposium (SAS). Glassboro, 1–4. doi: https://doi.org/10.1109/sas.2017.7894073
14. Morgenthaler, A., Rappaport, C. (2013). Fast GPR underground shape anomaly detection using the Semi-Analytic Mode Matching (SAMM) algorithm. Proceedings of the IEEE International Geoscience and Remote Sensing Symposium (IGARSS). Melbourne, 1422–1425. doi: https://doi.org/10.1109/igarss.2013.6723051
15. Li, W., Zhou, H., Wan, X. (2012). Generalized Hough Transform and ANN for subsurface cylindrical object location and parameters inversion from GPR data. Proceedings of the 14th International Conference on Ground Penetrating Radar (GPR). Shanghai, 281–285. doi: https://doi.org/10.1109/icgpr.2012.6254874
16. Dumin, O., Plakhtii, V., Pryshchenko, O., Pochanin, G. (2020). Comparison of ANN and Cross-Correlation Approaches for Ultra Short Pulse Subsurface Survey. Proceedings of the 15th International Conference on Advanced Trends in Radioelectronics, Tel-ecommunications and Computer Engineering (TCSET – 2020). Lviv-Slavske, 1–6. doi: https://doi.org/10.1109/tcset49122.2020.235459

17. Sharma, P., Kumar, B., Singh, D., Gaba, S. P. (2016). Metallic Pipe Detection using SF GPR: A New Approach using Neural Network. Proceedings of the 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS). Beijing, 6609–6612. doi: https://doi.org/10.1109/igarss.2016.7730726
18. Dumin, O. M., Pryshchenko, O. A., Plakhtii, V. A., Pochanin, G. P. (2020). Detection and classification of landmines using UWB antenna system and ANN analysis. Visnyk of V.N. Karazin Kharkiv National University, Series "Radio Physics and Electronics", 33, 7–19. doi: https://doi.org/10.26565/2311-0872-2020-33-01
19. Bralich, J., Reichman, D., Collins, L. M., Malof, J. M. (2017). Improving convolutional neural networks for buried target detection in ground penetrating radar using transfer learning via pretraining. Detection and Sensing of Mines, Explosive Objects, and Obscured Targets XXII, Vol. 10182. International Society for Optics and Photonics. SPIE, 198–208. doi: https://doi.org/10.1117/12.2263112
20. Lameri, S., Lombardi, F., Bestagini, P., Lualdi, M., Tubaro, S. (2017). Landmine detection from GPR data using convolutional neural networks. Proceedings of the 2017 25th European Signal Processing Conference (EUSIPCO). Kos, 508–512. doi: https://doi.org/10.23919/eusipco.2017.8081259
21. Pochanin, G. P., Capineri, L., Bechtel, T. D., Falorni, P., Borgioli, G., Ruban, V. P. et al. (2020). Measurement of Coordinates for a Cylindrical Target Using Times of Flight from a 1-Transmitter and 4-Receiver UWB Antenna System. IEEE Transactions on Geoscience and Remote Sensing, 58 (2), 1363–1372. doi: https://doi.org/10.1109/tgrs.2019.2946064
22. Dumin, O. M., Plakhtii, V. A., Prishchenko, O. A., Shyrokorad, D. V., Volvach, I. S. (2019). Influence of denoising of input signal on classification of object location by artificial neural network in ultrawideband radiointroscopy. Visnyk of V.N. Karazin Kharkiv National University, Series "Radio Physics and Electronics", 31, 27–35. doi: https://doi.org/10.26565/2311-0872-2019-31-03
23. Peleshchak, R., Lytvyn, V., Bihun, O., Peleshchak, I. (2019). Structural Transformations of Incoming Signal by a Single Nonlinear Oscillatory Neuron or by an Artificial Nonlinear Neural Network. International Journal of Intelligent Systems and Applications, 11 (8), 1–10. doi: https://doi.org/10.5815/ijisa.2019.08.01
24. Lytvyn, V., Vysotska, V., Peleshchak, I., Rishnyak, I., Peleshchak, R. (2018). Time Dependence of the Output Signal Morphology for Nonlinear Oscillator Neuron Based on Van der Pol Model. International Journal of Intelligent Systems and Applications, 10 (4), 8–17. doi: https://doi.org/10.5815/ijisa.2018.04.02
25. Janson, N. B., Pavlov, A. N., Neiman, A. B., Anishchenko, V. S. (1998). Reconstruction of dynamical and geometrical properties of chaotic attractors from threshold-crossing interspike intervals. Physical Review E, 58 (1), R4–R7. doi: https://doi.org/10.1103/physreve.58.r4
26. Kingma, D. P., Ba, J. (2015). Adam: a method for stochastic optimization. Proceedings of the 3rd International Conference on Learning Representations (ICLR 2015). San Diego, 1–15. doi: https://doi.org/10.48550/arXiv.1412.6980
27. Abbasi, A., Javed, A. R., Iqbal, F., Kryvinska, N., Jalil, Z. (2022). Deep learning for religious and continent-based toxic content detection and classification. Scientific Reports, 12 (1). doi: https://doi.org/10.1038/s41598-022-22523-3
28. Bashir, M. F., Arshad, H., Javed, A. R., Kryvinska, N., Band, S. S. (2021). Subjective Answers Evaluation Using Machine Learning and Natural Language Processing. IEEE Access, 9, 158972–158983. doi: https://doi.org/10.1109/access.2021.3130902

DOI: 10.15587/1729-4061.2023.281227

DEVELOPING A CONVOLUTIONAL NEURAL NETWORK FOR CLASSIFYING TUMOR IMAGES USING INCEPTION V3 (p. 86–93)

Ali A. Mahmood
University of Information Technology and Communications, Baghdad, Iraq
ORCID: https://orcid.org/0000-0001-5705-2619

Sadeer Sadeq
University of Information Technology and Communications, Baghdad, Iraq
ORCID: https://orcid.org/0009-0000-8415-8056

Yaser Issam Aljanabi
Middle Technical University, Baghdad, Iraq
ORCID: https://orcid.org/0000-0003-0135-1665

Ahmad H. Sabry
Al-Nahrain University, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-2736-5582

Deep learning algorithms rely on digital pathology to classify tissue tumors, where the whole tissue slides are digitized and imaged. The produced multi-resolution whole slide images (MWSIs) are with high resolution that may range from about 100,000 to 200,000 pixels. MWSIs are often stored in a multi-resolution configuration to simplify the processing of images, navigation, and efficient exposition. This work develops a network for classifying MWSIs that require high memory employing a deep neural Inception-v3 architecture. This work employs the MWSIs from Camelyon16, which is around 451 GB in size of Challenge dataset from two independent sources including 400 MWSIs as a total of lymph nodes. The training dataset contains 111 MWSIs of tumor tissue and lymph nodes and 159 WSIs of normal lymph nodes. The developed model uses sample-based processing to train extensive MWSIs employing the MATLAB platform. The model introduces transfer learning techniques with an Inception-v3-based architecture to categorize separate samples as a tumor or normal. Therefore, the main aim here is to achieve two-classes binary segmentation containing normal and tumor. This includes creating a new fully connected layer for the Inception-v3 architecture with two classes and compensating new layers instead of the original final fully-connected layers. The results obtained demonstrated that the heatmap visualization can recognize the boundary coordinates of ground truth as sketchy Region Of Interest (ROI), where the green boundary represents the normal regions and the tumor area with red boundaries. The proposed Inception v3 Convolutional Neural Network (CNN) architecture can achieve more than 92.8 % accuracy for such MWSIs dataset to categorize brain tumors into normal and tumor tissue.

Keywords: convolutional neural network, deep learning, classification, Inception architecture, brain tumor.

References

1. Abdelaziz Ismael, S. A., Mohammed, A., Hefny, H. (2020). An enhanced deep learning approach for brain cancer MRI images classification using residual networks. Artificial Intelligence in Medicine, 102, 101779. doi: https://doi.org/10.1016/j.artmed.2019.101779

2. Sfayyih, A. H., Sabry, A. H., Jameel, S. M., Sulaiman, N., Raafat, S. M., Humaidi, A. J., Kubaiaisi, Y. M. A. (2023). Acoustic-Based Deep Learning Architectures for Lung Disease Diagnosis: A Comprehensive Overview. Diagnostics, 13 (10), 1748. doi: https://doi.org/10.3390/diagnostics13101748
3. Abd-Ellah, M. K., Awad, A. I., Khalaf, A. A. M., Hamed, H. F. A. (2018). Two-phase multi-model automatic brain tumour diagnosis system from magnetic resonance images using convolutional neural networks. EURASIP Journal on Image and Video Processing, 2018 (1). doi: https://doi.org/10.1186/s13640-018-0332-4
4. Abd El Kader, I., Xu, G., Shuai, Z., Saminu, S., Javaid, I., Salim Ahmad, I. (2021). Differential Deep Convolutional Neural Network Model for Brain Tumor Classification. Brain Sciences, 11 (3), 352. doi: https://doi.org/10.3390/brainsci11030352
5. Houssein, E. H., Emam, M. M., Ali, A. A., Suganthan, P. N. (2021). Deep and machine learning techniques for medical imaging-based breast cancer: A comprehensive review. Expert Systems with Applications, 167, 114161. doi: https://doi.org/10.1016/j.eswa.2020.114161
6. Zhen, S., Cheng, M., Tao, Y., Wang, Y., Juengpanich, S., Jiang, Z. et al. (2020). Deep Learning for Accurate Diagnosis of Liver Tumor Based on Magnetic Resonance Imaging and Clinical Data. Frontiers in Oncology, 10. doi: https://doi.org/10.3389/fonc.2020.00680
7. Alqudah, A. M. (2019). Brain Tumor Classification Using Deep Learning Technique - A Comparison between Cropped, Uncropped, and Segmented Lesion Images with Different Sizes. International Journal of Advanced Trends in Computer Science and Engineering, 8 (6), 3684–3691. doi: https://doi.org/10.30534/ijatcse/2019/155862019
8. Wang, H., Zhou, Z., Li, Y., Chen, Z., Lu, P., Wang, W. et al. (2017). Comparison of machine learning methods for classifying mediastinal lymph node metastasis of non-small cell lung cancer from 18F-FDG PET/CT images. EJNMMI Research, 7 (1). doi: https://doi.org/10.1186/s13550-017-0260-9
9. Hoseini, F., Shahbahrami, A., Bayat, P. (2018). An Efficient Implementation of Deep Convolutional Neural Networks for MRI Segmentation. Journal of Digital Imaging, 31 (5), 738–747. doi: https://doi.org/10.1007/s10278-018-0062-2
10. Wei, J. W., Tafe, L. J., Linnik, Y. A., Vaickus, L. J., Tomita, N., Hassanpour, S. (2019). Pathologist-level classification of histologic patterns on resected lung adenocarcinoma slides with deep neural networks. Scientific Reports, 9 (1). doi: https://doi.org/10.1038/s41598-019-40041-7
11. Mehrotra, R., Ansari, M. A., Agrawal, R., Anand, R. S. (2020). A Transfer Learning approach for AI-based classification of brain tumors. Machine Learning with Applications, 2, 100003. doi: https://doi.org/10.1016/j.mlwa.2020.100003
12. Advanced Guide to Inception v3. Cloud TPU. Google Cloud. Available at: https://cloud.google.com/tpu/docs/inception-v3-advanced
13. Litjens, G., Bandi, P., Ehteshami Bejnordi, B., Geessink, O., Balkenhol, M., Bult, P. et al. (2018). 1399 H&E-stained sentinel lymph node sections of breast cancer patients: the CAMELYON dataset. GigaScience, 7 (6). doi: https://doi.org/10.1093/gigascience/giy065
14. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., Wojna, Z. (2016). Rethinking the Inception Architecture for Computer Vision. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). doi: https://doi.org/10.1109/cvpr.2016.308
15. ImageNet. Available at:https://www.image-net.org/
16. Raharjo, B., Farida, N., Subekti, P., Herlina, S., Doddy, H., Rahim, R. (2021). Optimization forecasting using back-propagation algorithm. Journal of Applied Engineering Science, 19 (4), 1083–1089. doi: https://doi.org/10.5937/jaes0-30175
17. Negassi, M., Suarez-Ibarrola, R., Hein, S., Miernik, A., Reiterer, A. (2020). Application of artificial neural networks for automated analysis of cystoscopic images: a review of the current status and future prospects. World Journal of Urology, 38 (10), 2349–2358. doi: https://doi.org/10.1007/s00345-019-03059-0
18. Zhuang, Z., Ding, W., Zhuang, S., Joseph Raj, A. N., Wang, J., Zhou, W., Wei, C. (2021). Tumor classification in automated breast ultrasound (ABUS) based on a modified extracting feature network. Computerized Medical Imaging and Graphics, 90, 101925. doi: https://doi.org/10.1016/j.compmedimag.2021.101925
19. Alanazi, M. F., Ali, M. U., Hussain, S. J., Zafar, A., Mohatram, M., Irfan, M., AlRuwaili, R. et al. (2022). Brain Tumor/Mass Classification Framework Using Magnetic-Resonance-Imaging-Based Isolated and Developed Transfer Deep-Learning Model. Sensors, 22 (1), 372. doi: https://doi.org/10.3390/s22010372
20. Mahmood, T., Li, J., Pei, Y., Akhtar, F., Rehman, M. U., Wasti, S. H. (2022). Breast lesions classifications of mammographic images using a deep convolutional neural network-based approach. PLOS ONE, 17(1), e0263126. doi: https://doi.org/10.1371/journal.pone.0263126
21. Asif, S., Yi, W., Ain, Q. U., Hou, J., Yi, T., Si, J. (2022). Improving Effectiveness of Different Deep Transfer Learning-Based Models for Detecting Brain Tumors From MR Images. IEEE Access, 10, 34716–34730. doi: https://doi.org/10.1109/access.2022.3153306
22. Jwaid, W. M., Al-Husseini, Z. S. M., Sabry, A. H. (2021). Development of brain tumor segmentation of magnetic resonance imaging (MRI) using U-Net deep learning. Eastern-European Journal of Enterprise Technologies, 4 (9 (112)), 23–31. doi: https://doi.org/10.15587/1729-4061.2021.238957

DOI: 10.15587/1729-4061.2023.282759

DISCRETE ELECTROCARDIOGRAM T AMPLITUDE DETECTION BASED ON CYCLE DURATION (p. 94–105)

Sabar Setiawidayat
Widyagama University of Malang, Malang, Indonesia
ORCID: https://orcid.org/0000-0003-0007-0327

In each cycle of the electrocardiogram wave there are P, Q, R, S and T amplitudes. Many studies have been conducted to obtain amplitude and QRS waves because they are related to ventricular depolarization, but to obtain T amplitude values related to ventricular repolarization are still rarely done, not even for the clinical standard (12 leads). This study aims to obtain the amplitude T value in each cycle and each electrocardiogram lead. Obtaining the amplitude T position on the reference lead will also find the amplitude T value on the other lead. Each cycle duration obtained from the duration RN to R_{N+1} is used to obtain the position of the endpoint of each cycle. The maximum value between the amplitude S position and the end point of the cycle is the amplitude T value. The results of research on 10 Physionet sinus rhythm samples and 10 Saiful Anwar Hospital Malang samples show that the duration of the cycle was successful in obtaining the amplitude T value for each lead. All samples can display a value. The amplitude in each cycle, where the values obtained in each cycle are still in normal conditions. The amplitude T value obtained is certainly accurate because there is only one positive value between the amplitude S position and the end of the cycle position. The position of the amplitude integer T found in

a cycle in one lead will be the same as the position of the amplitude integer T in the cycle for the other lead. This occurs because of the simultaneous transmission of impulses that affect the atrial and ventricular muscle cells. The position of the amplitude T for each cycle can be found by filtering the maximum amplitude value between the amplitude position S and the final position of the cycle. Practically, this method can be programmed to be added to a digital electrocardiograph.

Keywords: detect the amplitude T, cycle duration base, ecg discrete, electrocardiogram.

References

1. Serhani, M. A., T. El Kassabi, H., Ismail, H., Nujum Navaz, A. (2020). ECG Monitoring Systems: Review, Architecture, Processes, and Key Challenges. Sensors, 20 (6), 1796. doi: https://doi.org/10.3390/s20061796
2. He, R., Wang, K., Li, Q., Yuan, Y., Zhao, N., Liu, Y., Zhang, H. (2017). A novel method for the detection of R-peaks in ECG based on K-Nearest Neighbors and Particle Swarm Optimization. EURASIP Journal on Advances in Signal Processing, 2017 (1). doi: https://doi.org/10.1186/s13634-017-0519-3
3. Hamdi, S., Ben Abdallah, A., Bedoui, M. H. (2017). Real time QRS complex detection using DFA and regular grammar. BioMedical Engineering OnLine, 16 (1). doi: https://doi.org/10.1186/s12938-017-0322-2
4. Yochum, M., Renaud, C., Jacquir, S. (2016). Automatic detection of P, QRS and T patterns in 12 leads ECG signal based on CWT. Biomedical Signal Processing and Control, 25, 46–52. doi: https://doi.org/10.1016/j.bspc.2015.10.011
5. Rosenthal, T. M., Masvidal, D., Abi Samra, F. M., Bernard, M. L., Khatib, S., Polin, G. M. et al. (2017). Optimal method of measuring the T-peak to T-end interval for risk stratification in primary prevention. EP Europace, 20 (4), 698–705. doi: https://doi.org/10.1093/europace/euw430
6. Andršová, I., Hnatkova, K., Šišáková, M., Toman, O., Smetana, P., Huster, K. M. et al. (2020). Heart Rate Dependency and Inter-Lead Variability of the T Peak – T End Intervals. Frontiers in Physiology, 11. doi: https://doi.org/10.3389/fphys.2020.595815
7. Costa, R., Winkert, T., Manhães, A., Teixeira, J. P. (2021). QRS Peaks, P and T Waves Identification in ECG. Procedia Computer Science, 181, 957–964. doi: https://doi.org/10.1016/j.procs.2021.01.252
8. Kaur, A., Agarwal, A., Agarwal, R., Kumar, S. (2018). A Novel Approach to ECG R-Peak Detection. Arabian Journal for Science and Engineering, 44 (8), 6679–6691. doi: https://doi.org/10.1007/s13369-018-3557-8
9. Gliner, V., Behar, J., Yaniv, Y. (2018). Novel Method to Efficiently Create an mHealth App: Implementation of a Real-Time Electrocardiogram R Peak Detector. JMIR MHealth and UHealth, 6 (5), e118. doi: https://doi.org/10.2196/mhealth.8429
10. Chen, H., Maharatna, K. (2020). An Automatic R and T Peak Detection Method Based on the Combination of Hierarchical Clustering and Discrete Wavelet Transform. IEEE Journal of Biomedical and Health Informatics, 24 (10), 2825–2832. doi: https://doi.org/10.1109/jbhi.2020.2973982
11. Shang, H., Wei, S., Liu, F., Wei, D., Chen, L., Liu, C. (2019). An Improved Sliding Window Area Method for T Wave Detection. Computational and Mathematical Methods in Medicine, 2019, 1–11. doi: https://doi.org/10.1155/2019/3130527
12. Wani, I. A., Afroz, Ahmad, R. (2022). Detection of R- Peaks in Electrocardiogram based on Wavelet Transform and Wavelet Approximation. Punjab University Journal of Mathematics, 54 (7), 441–453. doi: https://doi.org/10.52280/pujm.2022.540702
13. Wijaya, C., Andrian, Harahap, M., Christnatalis, Turnip, M., Turnip, A. (2019). Abnormalities State Detection from P-Wave, QRS Complex, and T-Wave in Noisy ECG. Journal of Physics: Conference Series, 1230 (1), 012015. doi: https://doi.org/10.1088/1742-6596/1230/1/012015
14. Yu, Q., Liu, A., Liu, T., Mao, Y., Chen, W., Liu, H. (2019). ECG R-wave peaks marking with simultaneously recorded continuous blood pressure. PLOS ONE, 14 (3), e0214443. doi: https://doi.org/10.1371/journal.pone.0214443
15. Lata, S., Kumar, R. (2019). Disease Classification Using ECG Signals Based on R-Peak Analysis With ABC and ANN. International Journal of Electronics, Communications, and Measurement Engineering, 8 (2), 67–86. doi: https://doi.org/10.4018/ijecme.2019070105
16. Abdullah Al, Z. Md., Thapa, K., Yang, S.-H. (2021). Improving R Peak Detection in ECG Signal Using Dynamic Mode Selected Energy and Adaptive Window Sizing Algorithm with Decision Tree Algorithm. Sensors, 21 (19), 6682. doi: https://doi.org/10.3390/s21196682
17. Fahira Adriati, S., Setiawidayat, S., Rofii, F. (2021). Identification Of ECG Signal By Using Backpropagation Neural Network. Journal of Physics: Conference Series, 1908 (1), 012014. doi: https://doi.org/10.1088/1742-6596/1908/1/012014
18. Physionet. Available at: https://archive.physionet.org/cgi-bin/atm/ATM
19. Khelil, B., Kachouri, A., Messaoud, M. B., Ghariani, H. (2007). P Wave Analysis in ECG Signals using Correlation for Arrhythmias Detection. Fourth International Multi-Conference on Systems, Signals & Devices. Available at: https://www.academia.edu/12240318/P_Wave_Analysis_in_ECG_Signals_using_Correlation_for_Arrhythmias_Detection
20. Setiawidayat, S., Putri, S. I. (2016). Filtering Data Diskrit Elektrokardiogram Untuk Penentuan Pqrst Dalam Satu Siklus. SENTIA.
21. Setiawidayat, S., Rahman, A. Y. (2022). Method for Obtain Peak Amplitude Value on Discrete Electrocardiogram. Lecture Notes in Electrical Engineering, 97–108. doi: https://doi.org/10.1007/978-981-19-1804-9_8
22. Webster, J. G. (Ed.) (2010). Medical Instrumentation: Application and Design. John Wiley & Sons, 696. Available at: http://fa.bme.sut.ac.ir/Downloads/AcademicStaff/3/Courses/4/Medical%20instrumentation%20application%20and%20design%204th.pdf

АНОТАЦІЇ
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2023.280055
РОЗРОБКА НОВОГО ЛЕГКОВАГОВОГО АЛГОРИТМУ ШИФРУВАННЯ (с. 6–19)

Nursulu Kapalova, Kunbolat Algazy, Armanbek Haumen

Алгоритми легковагового шифрування вважаються відносно новим напрямом у розвитку криптографії із закритим ключем. Така потреба виникла внаслідок появи великої кількості пристроїв з невеликою обчислювальною потужністю та пам яттю. Тому з'явилась необхідність розробки алгоритмів, здатних забезпечити достатній рівень безпеки, при мінімальному використанні ресурсів. У роботі представлено новий легковаговий алгоритм шифрування LBC. LBC – це 64-бітовий симетричний блоковий алгоритм. Він підтримує 80 битий секретний ключ. Кількість раундів – 20. Алгоритм має структуру мережі Фейстеля. Розроблений легковаговий алгоритм має просту схему реалізації, а перетворення, що використовуються в даному алгоритмі, мають добрі криптографічні властивості. Це перевірено при дослідженні криптографічних властивостей алгоритму за допомогою «лавинного ефекту» та статистичних тестів. Перевірка лавинної властивості виконувалася кожного раунду при зміні кожного біта вихідного тексту. На підставі проведених робіт встановлено, що запропонований алгоритм шифрування ефективний для забезпечення гарного лавинного ефекту та бінарна послідовність, отримана після зашифрування, близька до випадкової. Також оцінено його захищеність від лінійного та диференціального криптоаналізу. Результати досліджень виявили добрі криптографічні властивості даного алгоритму. Алгоритм буде застосовуватися для пристроїв, що володіють малими апаратними ресурсами, в інформаційно-комунікаційних системах, де циркулюють відомості конфіденційного характеру, а також при необхідності в оперативно прийнятні терміни обмінюватися інформацією в захищеному вигляді.

Ключові слова: алгоритм шифрування, легковаговий алгоритм, криптографічні перетворення, лавинний ефект, криптостійкість.

DOI: 10.15587/1729-4061.2023.282131
РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ АТАК «ЗЛИЙ ДВІЙНИК» НА МЕРЕЖІ СТАНДАРТУ IEEE 802.11 (WI-FI) ЗА ДОПОМОГОЮ МОДЕЛІ КЛАСИФІКАЦІЇ KNN (с. 20–32)

Р. І. Банах, А. З. Піскозуб, І. Р. Опірський

Об'єктом дослідження виступають IEEE 802.11 (Wi-Fi) мережі, які часто є цілями групи атак під назвою «злий двійник». Дослідження даної теми є надзвичайно важливим, оскільки технологія Wi-Fi є дуже розповсюдженим методом підключення до мережі і зазвичай є першою ціллю кіберзлочинців в атаках на підприємства. За допомогою систематичного аналізу літератури зосередженої на протидію атакам типу «злий двійник», дана робота визначає основні переваги застосування систем штучного інтелекту, у аналізі мережевих даних та ідентифікації вторгнення в мережі Wi-Fi. Для оцінки ефективності виявлення вторгнень та аналізу кіберзлочинів проведено ряд експериментів максимально наближених до реальних атак на мережі Wi-Fi.

В рамках дослідження, що описано в даній статті, запропоновано метод виявлення кіберзлочинів у бездротових мережах стандарту IEEE 802.11 (Wi-Fi) за допомогою штучного інтелекту, а саме моделі побудованої на базі методу k-найближчих сусідів. Даний метод заснований на класифікації попередньо зібраних даних, а саме потужності сигналу від точки доступу, а потім безперервному порівнянню новозібраних даних із натренованою моделлю.

Розроблено компактний та енергоефективний прототип апаратно-програмного комплексу для реалізації моніторингу, аналізу мережевих пакетів ефірі та збереження даних на основі часових рядів. Задля зменшення навантаження на комп'ютерну мережу, і, зважаючи на обмежену обчислювальну здатність комплексу, було запропоновано метод агрегації даних, який забезпечує швидку передачу інформації.

Отримані результати, а саме 100 % тестових випадків (більше 7 тисяч), було класифіковано правильно, що вказує на те, що обраний метод аналізу даних дозволить значно підвищити безпеку інформаційно-комунікаційних системах державного та приватного рівнів.

Ключові слова: IEEE 802.11, Wi-Fi, evil twin, машинне навчання, класифікація, тріангуляція, кібербезпека.

DOI: 10.15587/1729-4061.2023.281795
РОЗРОБКА УДОСКОНАЛЕНОГО ПРОТОКОЛУ SSL/TLS НА ПОСТКВАНТОВИХ АЛГОРИТМАХ (с. 33–48)

С. П. Євсеєв, А. А. Гаврилова, С. В. Мілевський, І. П. Сініцин, В. В. Чалапко, Г. Ю. Дукін, В. М. Гребенюк, М. А. Дєдов, Lala Bekirova, О. І. Шпак

Розвиток інтернет-технологій разом із мобільними, комп'ютерними технологіями сформували смарт-технології, які дозволяють формувати як кіберфізичні, так і соціокіберфізичні системи. Основою смарт-технологій є комплексування стандартів бездротових

каналів із мобільними та комп'ютерними протоколами. Технології 4G/5G комплексують із різними веб-платформами з урахуванням цифровізації послуг у кіберпросторі. Але протокол SSL/TLS, заснований на гібридизації симетричних алгоритмів шифрування з алгоритмами гешування (режим AEAD), який повинен забезпечити послуги безпеки піддається атакам «Зустріч на середині», POODLE, BEAST, CRIME, BREACH. Крім цього, з появою повномасштабного квантового комп'ютера можуть бути зламані також алгоритми симетричної та несиметричної криптографії, які забезпечують послуги безпеки. Для підвищення рівня безпеки пропонується вдосконалений протокол на основі постквантових алгоритмів – крипто-кодових конструкцій, що дозволить забезпечити не лише протидію чинним атакам, а й стійкість у постквантовий період. Для забезпечення «гібридності» послуг пропонується використовувати крипто-кодові конструкції Мак-Еліса та Нідеррайтера (забезпечується конфіденційність та цілісність) та вдосконалений алгоритм UMAC на крипто-кодовій конструкції Мак-Еліса. З урахуванням рівня «секретності» інформації пропонується використовувати різні комбінації крипто-кодових конструкцій на різних кодах алгеброгеометричних, та/або збиткових кодах. Використання крипто-кодових конструкцій не лише забезпечує стійкість до атак, а й спрощує формування з'єднання – для передачі загального ключа використовуються параметри еліптичних кривих. Такий підхід суттєво знижує час з'єднання мобільних гаджетів та спрощує процедуру узгодження перед передачею даних.

Ключові слова: вдосконалений протокол SSL/TLS, постквантові алгоритми шифрування, вдосконалений алгоритм UMAC, алгеброгеометричні коди, збиткові коди.

DOI: 10.15587/1729-4061.2023.281287

ОЦІНКА ЕФЕКТИВНОСТІ КЕРУВАННЯ ПРИСТРОЯМИ ІНТЕРНЕТУ РЕЧЕЙ ЗА ТЕОРІЄЮ ТЕЛЕТРАФІКУ (с. 49–59)

Madina Konyrova, Saule Kumyzbayeva, Teodor Iliev, Katipa Chezhimbayeva

У зв'язку з глобальною програмою декарбонізації до 2050 року піднімаються наступні питання: перехід до чистої зеленої енергії, зростання кількості Інтернету речей (IP), а також розподіл енергії та контроль за навантаженням. Актуальність роботи підтверджується тим, що протягом багатьох років спостерігається значне зростання промислового IP, що істотно змінює механізм програм управління промисловими підприємствами. Об'єктом дослідження є система керування пристроєм IP для ефективного розподілу енергії з використанням теорії масового обслуговування, а саме теорії телетрафіку. Особливість роботи полягає в тому, що теорія телетрафіку, яка займається математичним моделюванням та аналізом шаблонів трафіку в мережах зв'язку, може бути явно застосована до керування пристроями IP. Автори розробили математичну модель управління IP з використанням теорії телетрафіку та на її основі створили імітаційну модель мережевого маршрутизатора та графік переходів у програмному забезпеченні «GPSS World». Отриманими результатами роботи були 16 станів і рівняння балансу, в якому були знайдені всі ймовірності. Імовірності використовувалися для розрахунку вузлів і характеристик мережі. Було змодельовано 100 000 запитів від пристроїв IP, що надходять до двох маршрутизаторів. Результати дослідження показали, що завантаження першого вузла становить 63,2 % із середнім часом обробки транзакції M=1,436 с, а завантаження другого вузла становить 32 % з M=0,914 с. Створена модель мережевого маршрутизатора працювала з мінімальними втратами під час транзакцій. Відповідно, розроблена в цьому дослідженні система управління IP показала свою ефективність і придатна для практичного використання в управлінні пристроями IP в Smart Grid. Планується дослідження можливості використання теорії телетрафіку в системах управління розподілом енергії в Smart Grids.

Ключові слова: теорія телетрафіку, теорія масового обслуговування, пристрої IoT, імітаційна модель мережевого маршрутизатора, світ GPSS.

DOI: 10.15587/1729-4061.2023.282374

ВИЗНАЧЕННЯ КІЛЬКОСТІ КЛАСТЕРІВ НА ЗОБРАЖЕННЯХ З КОСМІЧНИХ ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМ СПОСТЕРЕЖЕННЯ ПРИ ВИКОРИСТАННІ АЛГОРИТМУ K-MEANS (с. 60–69)

Г. В. Худов, О. М. Маковейчук, В. С. Комаров, В. Г. Худов, І. А. Хижняк, В. Г. Башинський, С. В. Стецiв, Є. Є. Дудар, А. В. Рудий, М. Г. Бугера

Об'єктом дослідження є процес кластерізації зображень з космічних оптико-електронних систем спостереження. Основна гіпотеза дослідження полягала в тому, що експериментальні дослідження дозволять визначити кількість кластерів на зображеннях з космічних оптико-електронних систем спостереження при використанні алгоритму k-means.

Метод кластерізації зображень з космічних оптико-електронних систем спостереження при використанні алгоритму k-means, на відміну від відомих, передбачає:

– розбиття вихідного зображення на Red-Green-Blue канали яскравості;
– визначення евклідової відстані між пікселями;
– розподіл усієї множини пікселів зображення на кластери;
– перерахунок «центрів» кожної підмножини;
– перепризначення нових «центрів» кожного кластеру;
– мінімізація повної внутрішньокластерної дисперсії.

Проведено експериментальні дослідження щодо кластерізації вихідного зображення методом на основі k-means при різних значеннях k. Встановлено, що зі збільшенням величини k візуальна якість кластерізації покращується та візуально можна визначити більшу кількість кластерів на зображеннях.

Для визначення кількості кластерів проведена оцінка суми помилок кластерізації 1 та 2 роду при різних значеннях k. Встановлено, що при збільшенні значення k сума помилок 1 та 2 роду спочатку зменшується за експоненціальною залежністю. Подальше збільшення величини k не приводить до суттєвого зменшення помилок 1 та 2 роду. Встановлено, що для типового зображення з космічної оптико-електронної системи спостереження значення k в методі кластерізації на основі алгоритму k-means повинно дорівнювати 4. При цьому сума помилок 1 та 2 роду складає 31,3 %.

Подальші дослідження направлені та розробку методів кластерізації, що знижують суму помилок 1 та 2 роду.

Ключові слова: кластерізація зображення, космічна система спостереження, k-means, помилки 1 та 2 роду, кількість кластерів.

DOI: 10.15587/1729-4061.2023.279372

ПІДВИЩЕННЯ ЯКОСТІ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ АНСАМБЛЕВИМИ КЛАСИФІКАТОРАМИ ЗІ СТЕКІНГОМ (с. 70–77)

О. М. Галчонков, Oleksii Baranov, Mykola Babych, В. І. Куваєва, Ю. І. Бабич

Об'єктом дослідження є процес класифікації об'єктів на зображеннях. Під якістю класифікації розуміється відношення правильно розпізнаних об'єктів до кількості зображень. Одним з варіантів підвищення якості класифікації є підвищення глибини нейронних мереж, що використовуються. Основними труднощами на цьому шляху є складність навчання таких нейронних мереж і великий обсяг обчислень, що утруднюють їх використання на звичайних комп'ютерах у реальному часі. Альтернативним варіантом підвищення якості класифікації є збільшення ширини нейронних мереж, що використовуються, за рахунок спорудження ансамблевих класифікаторів зі стекінгом. Однак вони вимагають використання на першому ступені класифікаторів з різною структурованою обробкою вхідних зображень, що відрізняються високою якістю класифікації та відносно низьким обсягом обчислень. Кількість відомих таких архітектур обмежена. Тому виникає завдання збільшення кількості класифікаторів на першому ступені ансамблевого класифікатора за рахунок модифікації відомих архітектур. Запропоновано використовувати блоки повороту зображень на різні кути щодо центру зображення. Показано, що в результаті структурованості обробки зображень ісходним класифікатором обробка повернутого зображення призводить до перерозподілу помилок на наборі зображень. Цей ефект дозволяє збільшувати кількість класифікаторів у першому ступені ансамблевого класифікатора. Числові експерименти показали, що додавання двох аналогів алгоритму MLP-Mixer до відомих конфігурацій ансамблевих класифікаторів забезпечило зменшення помилки від 1 до 11 % під час роботи з набором даних CIFAR-10. Аналогічно для CCT зменшення помилки становило від 2,1 до 10 %. Крім цього показано, що збільшення конфігурації MLP-Mixer в ширину дає кращі результати, ніж збільшення в глибину. Обов'язковою умовою успішності використання запропонованого підходу на практиці є структурованість обробки зображень ісходним класифікатором.

Ключові слова: багатошаровий персептрон, нейронна мережа, ансамблевий класифікатор, вагові коефіцієнти, класифікація об'єктів на зображеннях.

DOI: 10.15587/1729-4061.2023.279891

РОЗРОБКА МОДЕЛІ ГІБРИДНОЇ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ МІН З ВИКОРИСТАННЯМ ДАНИХ НАДШИРОКОСМУГОВОГО РАДАРУ (с. 78–85)

В. В. Литвин, І. Р. Пелещак, Р. М. Пелещак, О. О. Медяков, П. Я. Пукач

Об'єктом дослідження є архітектура гібридної нейронної мережі для розпізнавання мін з використанням даних надширокосмугового радару. У роботі вирішено проблему фільтрації відбитих сигналів із завадами та розпізнавання мін, виявлених надширокосмуговим (UWB (Ultra-Wide-Band)) радаром. Запропоновано модель гібридної нейронної мережі у поєднанні з алгоритмом навчання Адам. Фільтрація відбитих сигналів від мін здійснюється за допомогою MLP (multilayer perceptron) фільтру, який зі всього відбитого сигналу виділяє малоамплітудні частини сигналів, що несуть інформацію про приховану міну. Розпізнавання мін здійснюється блоком Гільберта та осциляторною нейронною мережею, що входять у структуру гібридної нейронної мережі. Особливістю отриманих результатів, що дозволили вирішити досліджувану проблему, є трансформація частоти сигналів блоком Гільберта і розпізнавання мін осциляторною нейронною мережею в резонансному режимі. Тришаровий MLP фільтр ефективно відфільтровує некорисну складову у повному сигналі, відбитому від підповерхневого об'єкта, оскільки MSE (Mean Squared Error) MLP фільтра становить $1{\cdot}10^{-5}$. Якщо частота гільбертового сигналу рівна власній частоті коливань нейронів $\Omega_i^H = \omega_{ij}$, то розпізнавання сигналів з малою амплітудою від підповерхневих об'єктів здійснюється осциляторною нейронною мережею на основі резонансної амплітуди, на що вказує мале значення крос-ентропії. Запропонована модель гібридної нейронної мережі забезпечує підсилення корисних сигналів за рахунок резонансу і має вищу продуктивність порівняно з існуючими моделями штучних нейронних мереж. Практичне значення отриманих результатів полягає у їх застосуванні у сфері автоматизованих нейромережевих технологій для виявлення та розпізнавання підповерхневих об'єктів різної природи на основі відбитих радіолокаційних сигналів з амплітудою на рівні шуму.

Ключові слова: багатошаровий перцетрон-фільтр, блок Гільберта, осциляторна нейронна мережа, резонанс.

DOI: 10.15587/1729-4061.2023.281227

РОЗРОБКА ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ КЛАСИФІКАЦІЇ ЗОБРАЖЕНЬ ПУХЛИН ЗА ДОПОМОГОЮ INCEPTION V3 (с. 86–93)

Ali A. Mahmood, Sadeer Sadeq, Yaser Issam Hamodi Aljanabi, Ahmad H. Sabry

Алгоритми глибокого навчання спираються на цифрову патологію для класифікації пухлин тканин, коли цілі слайди тканин оцифровуються та візуалізуються. Отримані повнослайдові зображення зі змінною роздільною здатністю (MWSI) мають високу роздільну здатність, яка може коливатися приблизно від 100 000 до 200 000 пікселів. Для спрощення обробки зображень, навігації та ефективної експозиції MWSI часто зберігаються в конфігурації зі змінною роздільною здатністю. У даній роботі з використанням глибокої нейронної архітектури Inception-v3 розроблена мережа для класифікації MWSI, що потребують великого обсягу пам'яті. У роботі використовуються MWSI з Camelyon16, розмір якого становить близько 451 ГБ набору даних Challenge з двох незалежних джерел, включаючи 400 MWSI для лімфатичних вузлів. Навчальний набір даних містить 111 MWSI пухлинної тканини і лімфатичних вузлів та 159 WSI нормальних лімфатичних вузлів. У розробленій моделі використовується обробка на основі зразків для навчання великих MWSI за допомогою платформи MATLAB. У моделі представлені методи трансферного навчання з архітектурою на основі Inception-v3 для класифікації окремих зразків як пухлини або норми. Таким чином, основною метою є досягнення бінарної сегментації за двома класами, включаючи норму та пухлину. Це передбачає створення нового повнозв'язаного шару для архітектури Inception-v3 з двома класами та компенсацію нових шарів замість вихідних кінцевих повнозв'язних шарів. Отримані результати показали, що візуалізація теплової карти дозволяє розпізнавати граничні координати основної істини як схематичну область інтересу (ROI), де зелена межа представляє нормальні області, а червоні межі – область пухлини. Запропонована архітектура згорткової нейронної мережі (ЗНМ) Inception v3 дозволяє досягти точності понад 92,8 % для такого набору даних MWSI для класифікації пухлин головного мозку на нормальну та пухлинну тканини.

Ключові слова: згорткова нейронна мережа, глибоке навчання, класифікація, архітектура Inception, пухлина головного мозку.

DOI: 10.15587/1729-4061.2023.282759

ВИЗНАЧЕННЯ АМПЛІТУДИ ДИСКРЕТНОЇ ЕЛЕКТРОКАРДІОГРАМИ НА ОСНОВІ ТРИВАЛОСТІ ЦИКЛУ (с. 94–105)

Sabar Setiawidayat

У кожному циклі хвилі електрокардіограми є амплітуди P, Q, R, S і T. Було проведено багато досліджень для отримання амплітуди та хвилі QRS, оскільки вони пов'язані з деполяризацією шлуночків, але для отримання значень амплітуди T, пов'язаних із реполяризацією шлуночків, все ще рідко проводяться навіть для клінічного стандарту (12 відведень). Це дослідження має на меті отримати значення амплітуди T у кожному циклі та кожному відведенні електрокардіограми. Отримання положення амплітуди T на контрольному відведенні також знайде значення амплітуди T на іншому відведенні. Кожна тривалість циклу, отримана від тривалості RN до RN+1, використовується для отримання положення кінцевої точки кожного циклу. Максимальне значення між положенням амплітуди S і кінцевою точкою циклу є значенням амплітуди T. Результати дослідження 10 зразків синусового ритму Physionet і 10 зразків Saiful Anwar Hospital Malang показують, що тривалість циклу була успішною для отримання значення амплітуди T для кожного відведення. Усі зразки можуть відображати значення. Амплітуда в кожному циклі, де значення, отримані в кожному циклі, все ще знаходяться в нормальних умовах. Отримане значення амплітуди T, безумовно, є точним, оскільки між положенням амплітуди S і положенням кінця циклу є лише одне додатне значення. Положення цілого числа амплітуди T, знайденого в циклі в одному відведенні, буде таким самим, як і положення цілого числа амплітуди T у циклі для іншого відведення. Це відбувається через одночасну передачу імпульсів, які впливають на м'язові клітини передсердь і шлуночків. Положення амплітуди T для кожного циклу можна знайти шляхом фільтрації максимального значення амплітуди між положенням амплітуди S і кінцевим положенням циклу. Практично цей метод можна запрограмувати для додавання до цифрового електрокардіографа.

Ключові слова: детектування амплітуди T, база тривалості циклу, дискретна ЕКГ, електрокардіограма.