ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2020.202820

DEVELOPMENT OF BREAST CANCER DIAGNOSIS SYSTEM BASED ON FUZZY LOGIC AND PROBABILISTIC NEURAL NETWORK (p. 6–13)

Taha Mohammed Hasan
University of Diyala, Diyala, Iraq
ORCID: http://orcid.org/0000-0002-4464-4655

Sahab Dheyaa Mohammed
University of Information Technology and Communications, Baghdad, Iraq
ORCID: http://orcid.org/0000-0003-1912-6546

Jumana Waleed
University of Diyala, Diyala, Iraq
ORCID: http://orcid.org/0000-0003-3474-1029

Breast cancer is one of the most common kinds of cancers that infect females in the whole world. It has happened when the cells in breast tissues start to grow in an uncontrollable way. Because it leads to death, early detection and diagnosis is a very important task to save the patient's life. Due to the restriction of human observers, computer plays a significant role in detecting early cancer signs. The proposed system uses a multi-resolution analysis and a top-hat operation for detecting the suspicious regions in a mammogram image. The discrete wavelet transform feature analysis is utilized for extracting features from the region of interest. Fuzzy Logic (FL) and Probabilistic Neural Network (PNN) are utilized for classifying the tumor into normal or abnormal. The differences between the proposed system and other researches are the use of adaptive threshold value depending on each image, by using Discrete Wavelet Transform (DWT) in both segmentation and feature extraction phases, which decrease complexity and time. Additionally, the detection of more than one tumor in the breast mammogram image and the utilization of FL and PNN work on increasing the system efficiency that led to raising the accuracy rate of the system and reducing the time. The obtained results of accuracy, sensitivity, and specificity were equal to 99 %, 98 %, and 47 %, respectively, and these results showed that the proposed system is more accurate than the other previous related works.

Keywords: breast cancer diagnosis, fuzzy logic (FL), probabilistic neural network (PNN).

References

1. Narain Ponraj, M. E. J. D., Poongodi, P., Samuel Manoharan, J. (2011). A Survey on the Preprocessing Techniques of Mammogram For the Detection of Breast Cancer. Journal of Emerging Trends in Computing and Information Sciences (ISSN), 2, 656–664.
2. Kahya, M. A. (2019). Classification enhancement of breast cancer histopathological image using penalized logistic regression. Indonesian Journal of Electrical Engineering and Computer Science, 13 (1), 405. doi: https://doi.org/10.11591/ijeecs.v13.i1.pp405-410
3. Abdullah, A. J., Hasan, T. M., Waleed, J. (2019). An Expanded Vision of Breast Cancer Diagnosis Approaches Based on Machine Learning Techniques. 2019 International Engineering Conference (IEC). doi: https://doi.org/10.1109/iec47844.2019.8950530
4. Bhardwaj, A., Tiwari, A., Chandarana, D., Babel, D. (2014). A genetically optimized neural network for classification of breast cancer disease. 2014 7th International Conference on Biomedical Engineering and Informatics. doi: https://doi.org/10.1109/bmei.2014.7002862
5. Saini, S., Vijay, R. (2015). Mammogram Analysis Using Feed-Forward Back Propagation and Cascade-Forward Back Propagation Artificial Neural Network. 2015 Fifth International Conference on Communication Systems and Network Technologies. doi: https://doi.org/10.1109/csnt.2015.78
6. Naranje, S. (2016). Early Detection of Breast Cancer using ANN. International Journal of Innovative Research in Computer and Communication Engineering, 4 (7), 14008–14013.
7. Tan, Y. J., Sim, K. S., Ting, F. F. (2017). Breast cancer detection using convolutional neural networks for mammogram imaging system. 2017 International Conference on Robotics, Automation and Sciences (ICORAS). doi: https://doi.org/10.1109/icoras.2017.8308076
8. Routray, I., Rath, N. P. (2018). Textural Feature Based Classification of Mammogram Images Using ANN. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). doi: https://doi.org/10.1109/icccnt.2018.8493957
9. Liu, S., Zeng, J., Gong, H., Yang, H., Zhai, J., Cao, Y. et. al. (2018). Quantitative analysis of breast cancer diagnosis using a probabilistic modelling approach. Computers in Biology and Medicine, 92, 168–175. doi: https://doi.org/10.1016/j.compbiomed.2017.11.014
10. Feng, H., Cao, J., Wang, H., Xie, Y., Yang, D., Feng, J., Chen, B. (2020). A knowledge-driven feature learning and integration method for breast cancer diagnosis on multi-sequence MRI. Magnetic Resonance Imaging, 69, 40–48. doi: https://doi.org/10.1016/j.mri.2020.03.001
11. Specht, D. F. (1990). Probabilistic neural networks and the polynomial Adaline as complementary techniques for classification. IEEE Transactions on Neural Networks, 1 (1), 111–121. doi: https://doi.org/10.1109/72.80210
12. Specht, D. F. (1992). Enhancements to probabilistic neural networks. [Proceedings 1992] IJCNN International Joint Conference on Neural Networks, 1, 761–768. doi: https://doi.org/10.1109/ijcnn.1992.287095
13. Kusy, M., Zajdel, R. (2014). Probabilistic neural network training procedure based on Q(0)-learning algorithm in medical data classification. Applied Intelligence, 41 (3), 837–854. doi: https://doi.org/10.1007/s10489-014-0562-9
14. Sawant, S. S., Topannavar, P. S. (2015). Introduction to Probabilistic Neural Network–Used for Image Classifications. International Journal of Advanced Research in Computer Science and Software Engineering, 5 (4), 279–283.

DOI: 10.15587/1729-4061.2020.208554

DEVELOPMENT OF COMPLEX METHODOLOGY OF PROCESSING HETEROGENEOUS DATA IN INTELLIGENT DECISION SUPPORT SYSTEMS (p. 14–23)

Pavlo Zuiev
General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-5446-3671

Ruslan Zhyvotovskyi
Central Scientifically-Research Institute of Arming and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-2717-0603

Oleksii Zvieriev
Central Scientifically-Research Institute of Arming and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-2274-3115

Serhiy Hatsenko
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-0957-6458

Volodymyr Kuprii
Military Unit A 0135, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-3895-1579

Oleksandr Nakonechnyi
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-8854-8983

Mykhailo Adamenko
Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-1345-8833

Andrii Shyshatskyi
Central Scientifically-Research Institute of Arming and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-6731-6390

Yevhenii Neroznak
Military institute of telecommunications and informatization named after Heroes of Kruty, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-5641-5473

Vira Velychko
Military institute of telecommunications and informatization named after Heroes of Kruty, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-9654-4560

The complex methodology for processing heterogeneous data in intelligent decision support systems is developed. This method is made to increase the efficiency of processing heterogeneous data in intelligent decision support systems. The complex methodology consists of the following interrelated procedures: heterogeneous data storing model; heterogeneous data synchronization algorithm; heterogeneous data separation algorithm; heterogeneous data indexing algorithm. The model of storing heterogeneous intelligence data, which is the basis of the methodology, differs in the presence of templates of intelligence objects and parameter templates of intelligence objects. Templates allow storing both unstructured heterogeneous intelligence data and structured intelligence data according to a defined pattern, which reduces the time to access the data. In the heterogeneous intelligence data storage model, a heterogeneous intelligence data synchronization algorithm, heterogeneous intelligence data separation algorithm and heterogeneous intelligence data indexing algorithm are developed. The development of the proposed technique is due to the need to increase the efficiency of processing various information types in intelligent decision support systems with acceptable computational complexity. The proposed method allows increasing the efficiency of intelligent decision support systems through integrated processing of data circulating in them. The proposed method allows increasing the efficiency of information processing in decision support systems from 16 to 20 % depending on the amount of information about the monitoring object.

Keywords: decision support system, monitoring object, different types of data, computational complexity, information processing, type of information.

References

1. Makridenko, L. A., Volkov, S. N., Hodnenko, V. P. (2010). Kontseptual'nye voprosy sozdaniya i primeneniya malyh kosmicheskih apparatov. Voprosy elektromehaniki, 114, 15–26.
2. Bashkirov, O. M., Kostina, O. M., Shishats'kiy, A. V. (2015). Development of integrated communication systems and data transfer for the needs of the Armed Forces. Weapons and military equipment, 5 (1), 35–39.
3. Trotsenko, R. V., Bolotov, M. V. (2014). Data extraction process for heterogeneous sources. Privolzhskiy nauchnyy vestnik, 12-1 (40), 52–54.
4. Bodyanskiy, E., Strukov, V., Uzlov, D. (2017). Generalized metrics in the problem of analysis of multidimensional data with different scales. Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl, 3, 98–101.
5. Noh, B., Son, J., Park, H., Chang, S. (2017). In-Depth Analysis of Energy Efficiency Related Factors in Commercial Buildings Using Data Cube and Association Rule Mining. Sustainability, 9 (11), 2119. doi: https://doi.org/10.3390/su9112119
6. Petras, V., Petrasova, A., Jeziorska, J., Mitasova, H. (2016). Processing UAV and lidar point clouds in Grass GIS. ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLI-B7, 945–952. doi: https://doi.org/10.5194/isprs-archives-xli-b7-945-2016
7. Polovina, S., Radic, B., Ristic, R., Milcanovic, V. (2016). Spatial and temporal analysis of natural resources degradation in the Likodra River watershed. Glasnik Sumarskog Fakulteta, 114, 169–188. doi: https://doi.org/10.2298/gsf1614169p
8. Poryadin, I., Smirnova, E. (2017). Binary Classification Method of Social Network Users. Science and Education of the Bauman MSTU, 17 (02), 121–137. doi: https://doi.org/10.7463/0217.0000915
9. Tymchuk, S. (2017). Methods of Complex Data Processing from Technical Means of Monitoring. Path of Science, 3 (3), 4.1–4.9. doi: https://doi.org/10.22178/pos.20-4
10. Semenov, V. V., Lebedev, I. S. (2019). Processing of signal information in problems of monitoring information security of unmanned autonomous objects. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 19 (3), 492–498. doi: https://doi.org/10.17586/2226-1494-2019-19-3-492-498
11. Zhou, S., Yin, Z., Wu, Z., Chen, Y., Zhao, N., Yang, Z. (2019). A robust modulation classification method using convolutional neural networks. EURASIP Journal on Advances in Signal Processing, 2019 (1). doi: https://doi.org/10.1186/s13634-019-0616-6
12. Zhang, D., Ding, W., Zhang, B., Xie, C., Li, H., Liu, C., Han, J. (2018). Automatic Modulation Classification Based on Deep Learning for Unmanned Aerial Vehicles. Sensors, 18 (3), 924. doi: https://doi.org/10.3390/s18030924
13. Kukulska, A., Salata, T., Cegielska, K., Szylar, M. (2018). Methodology of evaluation and correction of geometric data topology in QGIS software. Acta Scientiarum Polonorum Formatio Circumiectus, 17 (1), 125–138. doi: https://doi.org/10.15576/asp.fc/2018.17.1.125
14. Rulev, A., Yuferev, V. (2015). Theory of geoinformatic mapping of erosion geomorphological systems. Vestnik Volgogradskogo Gosudarstvennogo Universiteta. Serija 11. Estestvennye Nauki, 4, 62–67. doi: https://doi.org/10.15688/jvolsu11.2015.4.7
15. Yousefi, M., Kreuzer, O. P., Nykänen, V., Hronsky, J. M. A. (2019). Exploration information systems – A proposal for the future use of GIS in mineral exploration targeting. Ore Geology Reviews, 111, 103005. doi: https://doi.org/10.1016/j.oregeorev.2019.103005
16. Ashkezari, A. D., Hosseinzadeh, N., Chebli, A., Albadi, M. (2018). Development of an enterprise Geographic Information System (GIS) integrated with smart grid. Sustainable Energy, Grids and Networks, 14, 25–34. doi: https://doi.org/10.1016/j.segan.2018.02.001
17. Wang, S., Zhong, Y., Wang, E. (2019). An integrated GIS platform architecture for spatiotemporal big data. Future Generation Computer Systems, 94, 160–172. doi: https://doi.org/10.1016/j.future.2018.10.034

18. Wan-Mohamad, W. N. S., Abdul-Ghani, A. N. (2011). The Use of Geographic Information System (GIS) for Geotechnical Data Processing and Presentation. Procedia Engineering, 20, 397–406. doi: https://doi.org/10.1016/j.proeng.2011.11.182
19. Pedro, J., Silva, C., Pinheiro, M. D. (2019). Integrating GIS spatial dimension into BREEAM communities sustainability assessment to support urban planning policies, Lisbon case study. Land Use Policy, 83, 424–434. doi: https://doi.org/10.1016/j.landusepol.2019.02.003
20. Mokhtara, C., Negrou, B., Settou, N., Gouareh, A., Settou, B. (2019). Pathways to plus-energy buildings in Algeria: design optimization method based on GIS and multi-criteria decision-making. Energy Procedia, 162, 171–180. doi: https://doi.org/10.1016/j.egypro.2019.04.019
21. Kalantaievska, S., Pievtsov, H., Kuvshynov, O., Shyshatskyi, A., Yarosh, S., Gatsenko, S. et. al. (2018). Method of integral estimation of channel state in the multiantenna radio communication systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (95)), 60–76. doi: https://doi.org/10.15587/1729-4061.2018.144085
22. Karin, S. A. (2012). Integration in the single information space of heterogeneous geospatial data. Informatsionno-upravlyayushchie sistemy, 2, 89–94.
23. Karin, S. A. (2014). Developing a domain-specific ontology in spatial data processing systems. Informatsionno-upravlyayushchie sistemy, 4, 78–84.
24. Belousov, S. M. (2006). Matematicheskaya model' mnogopotochnoy sistemy massovogo obsluzhivaniya, upravlyaemoy planirovshchikom resursov. Vestnik Novosibirskogo gosudarstvennogo universiteta. Ser.: Informatsionnye tehnologii, 4 (1), 14–26.
25. Karin, C. A., Dudin, E. A. (2014). Podhody k sozdaniyu raspredelennoy sistemy sbora, hraneniya i obrabotki geoprostranstvennyh dannyh. Informatsiya i kosmos, 3, 46–51.
26. Koshlan, A., Salnikova, O., Chekhovska, M., Zhyvotovskyi, R., Prokopenko, Y., Hurskyi, T. et. al. (2019). Development of an algorithm for complex processing of geospatial data in the special-purpose geoinformation system in conditions of diversity and uncertainty of data. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 35–45. doi: https://doi.org/10.15587/1729-4061.2019.180197
27. Kuchuk, N., Mohammed, A. S., Shyshatskyi, A., Nalapko, O. (2019). The method of improving the efficiency of routes selection in networks of connection with the possibility of self-organization. International Journal of Advanced Trends in Computer Science and Engineering, 8 (1.2), 1–6. Available at: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01812sl2019.pdf

DOI: 10.15587/1729-4061.2020.209930

DEVELOPMENT OF CAN NETWORK WITH IMPROVED PARAMETERS FOR ADAPTIVE CAR FRONT LIGHTING SYSTEM (p. 24–33)

Konstiantyn Soroka
O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-9091-6861

Victor Kharchenko
O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-1209-609X

Vladyslav Pliuhin
O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-4056-9771

An analysis of implementation principles and algorithms of the adaptive car front-lighting system (AFS) and control methods is carried out. The AFS was adopted by the UNECE in 2007 as the rules for arranging front-lighting systems of vehicles when driving in the dark. Among the known algorithms of AFS operation, a preliminary inspection algorithm is chosen, based on the features of the driver's observation of the road in front of the vehicle, taking into account the characteristics of his vision. The requirements of the algorithm for the control system are analyzed. Control methods using Arduino controllers and computer network are considered. Given the capabilities of network technologies, the CAN network (Controller Area Network) is chosen to ensure the quality of control. It is recommended to use the CAN network option with a length of 40 or 100 m and a speed of 1,000, 500 kbit/s, respectively. Network performance parameters are calculated: speed, error probabilities, performance dependence on load, size of commands and duration of transmission, and compliance with AFS requirements. It is proposed to improve the network arbitration algorithm by increasing the probability of transmission of low-priority commands at high load. The AFS developed on the basis of the CAN network allows creating comfortable conditions for the driver in the dark, preventing accidents, and ensuring traffic safety.

An analysis of the AFS operation shows that it is directly related to the operation of most of the main components of the car, namely: engine, steering, gearbox, brakes, accelerometer, etc. It is operated under the driver's control. Therefore, this system can have extended functions, serve as the basis for the safety system and vehicle control system as a whole.

Keywords: traffic safety, front lighting, adaptive system, Arduino controllers, CAN network, data frame.

References

1. Automotive Adaptive Front-lighting System Reference Design (2013). Texas Instruments, 42. Available at: https://www.ti.com/lit/ug/spruhp3/spruhp3.pdf?ts=1593028730309&ref_url=https%253A%252F%20%252Fwww.google.com%252F
2. Kobayashi, S. (1998). Intelligent Lighting Systems: Their History, Function, & General Direction of Development. SAE Technical Paper Series. doi: https://doi.org/10.4271/981173
3. Regulation No 123 of the Economic Commission for Europe of the United Nations (UN/ECE) – Uniform provisions concerning the approval of adaptive front-lighting systems (AFS) for motor vehicles. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42010X0824%2801%29
4. Gao, Z., Li, Y. (2014). A Study of Bending Mode Algorithm of Adaptive Front-Lighting System Based on Driver Preview Behavior. Mathematical Problems in Engineering, 2014, 1–11. doi: https://doi.org/10.1155/2014/939218
5. Lifu, L., Mingjun, Y., Jinyong, Z. (2015). The bending mode control method of afs system based on preview control. International Journal on Smart Sensing and Intelligent Systems, 8 (1), 637–657. doi: https://doi.org/10.21307/ijssis-2017-776
6. Soroka, K., Kharchenko, V., Shpika, M. (2018). Vehicle lighting equipment and control methods for an adaptive front-lighting system. Lighting Engineering & Power Engineering (LEPE), 2 (52), 63–67. Available at: https://lepe.kname.edu.ua/index.php/lepe/article/view/414/393
7. Dahou, H., El Gouri, R., Alareqi, M., Mateur, K., Mezouari, A., Zemmouri, A., Hlou, L. (2018). Design and Implementation Intelligent Adaptive Front-lighting System of Automobile using Digital Technology on Arduino Board. International Journal of Electrical and Computer Engineering (IJECE), 8 (1), 521. doi: https://doi.org/10.11591/ijece.v8i1.pp521-529
8. Tanenbaum, A. S. (2003). Computer networks. Pearson Education Inc., 674. Available at: https://theswissbay.ch/pdf/Gentoomen%

20Library/Networking/Prentice%20Hall%20-%20Computer%20Networks%20Tanenbaum%204ed.pdf
9. Herrewege, A. V., Singelee, D., Verbauwhede, I. (2011). CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus. Conference: ECRYPT Workshop on Lightweight Cryptography. Available at: https://pdfs.semanticscholar.org/007e/e2559d4a2a8c661f4f5182899f03736682a7.pdf
10. Salunkhe, A. A., Kamble, P. P., Jadhav, R. (2016). Design and implementation of CAN bus protocol for monitoring vehicle parameters. 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). doi: https://doi.org/10.1109/rteict.2016.7807831
11. ISO 11898-1:2015. Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling. Available at: https://www.iso.org/standard/63648.html
12. Feibel, W. (1996). The Encyclopedia of Networking. Sybex Inc, 1315.
13. Schmidt, K., Schmidt, E. G. (2007). Systematic Message Schedule Construction for Time-Triggered CAN. IEEE Transactions on Vehicular Technology, 56 (6), 3431–3441. doi: https://doi.org/10.1109/tvt.2007.906413
14. Kulbashnaya, N., Soroka, K. (2016). Development of a model of a driver's choice of speed considering the road conditions. Eastern-European Journal of Enterprise Technologies, 3 (2 (81)), 32–38. doi: https://doi.org/10.15587/1729-4061.2016.71489
15. Van Derlofske, J. F., McColgan, M. W. (2002). White LED sources for vehicle forward lighting. Solid State Lighting II. doi: https://doi.org/10.1117/12.452569

DOI: 10.15587/1729-4061.2020.210754

METHOD FOR DETERMINING THE RESPONSES FROM A NONLINEAR SYSTEM USING THE VOLTERRA SERIES (p. 34–44)

Mohammed Kassim Ahmed
University of AL-Hamdaniya, Bartela, Hamdaniya, Iraq
ORCID: http://orcid.org/0000-0002-1481-8298

Samah Fakhri Aziz
University of AL-Hamdaniya, Bartela, Hamdaniya, Iraq
ORCID: http://orcid.org/0000-0003-0754-5727

Naors Y. Anad Alsaleem
University of AL-Hamdaniya, Bartela, Hamdaniya, Iraq
ORCID: http://orcid.org/0000-0002-0785-2674

Konstantyn Sielivanov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-1631-9986

Mykola Moskalets
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-1726-1250

A methodology has been proposed for estimating the nonlinear effects in radio tracts of receiving and transmitting devices in radio-electronic means of mobile communication systems, based on using the nonlinear transfer functions of the higher-order Volterra series.

A procedure has been devised for obtaining the output responses from a nonlinear non-inertia circuit under the harmonious input action using a method for determining the transfer functions of higher orders obtained on the basis of the transfer functions of lower orders.

We have derived the analytical expressions for the output responses from a nonlinear system of different orders for three inputs for the case of representing a nonlinear system in the form of a nonlinear non-inertia circuit.

The values of the transfer functions of higher orders for a nonlinear non-inertia circuit were determined by using a state variable method.

This paper demonstrates the derivation of analytical expressions to calculate a harmonic coefficient based on the second and third harmonics using the nonlinear higher-orders transfer functions of a nonlinear non-inertia circuit.

It has been shown that the use of the nonlinear transfer functions to the fifth order inclusive allows a more accurate assessment of nonlinear effects in the form of the harmonious and intermodulation distortions in the radio tracts of radio-electronic means of mobile systems.

The outlined technique for determining the nonlinear transfer functions is invariant to the topology of a nonlinear electrical circuit, as well as to the quantity and type of nonlinear elements. Existing estimation procedures of electromagnetic compatibility related to the problems of calculating intermodulation interference can be improved by the introduction of the determined magnitudes of influence products.

The proposed methodology makes it possible to evaluate the set of nonlinear effects in the problems related to electromagnetic compatibility in the groups of radio-electronic means with the accuracy required by users.

Keywords: nonlinear system, Volterra series, transfer function, nonlinear non-inertia circuit.

References

1. Zaker, N. A., Alsaleem, N., Kashmoola, M. A. (2018). Multi-agent Models Solution to Achieve EMC In Wireless Telecommunication Systems. 2018 1st Annual International Conference on Information and Sciences (AiCIS). doi: https://doi.org/10.1109/aicis.2018.00061
2. Alsaleem, N. Y. A., Moskalets, M., Teplytska, S. (2016). The analysis of methods for determining direction of arrival of signals in problems of space-time access. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 36–44. doi: https://doi.org/10.15587/1729-4061.2016.75716
3. Alsaleem, N. Y. A., Kashmoola, M. A., Moskalets, M. (2018). Analysis of the efficiency of spacetime access in the mobile communication systems based on an antenna array. Eastern-European Journal of Enterprise Technologies, 6 (9 (96)), 38–47. doi: https://doi.org/10.15587/1729-4061.2018.150921
4. Kashmoola, M. A., Alsaleem, M. Y. anad, Alsaleem, N. Y. A., Moskalets, M. (2019). Model of dynamics of the grouping states of radio electronic means in the problems of ensuring electromagnetic compatibility. Eastern-European Journal of Enterprise Technologies, 6 (9 (102)), 12–20. doi: https://doi.org/10.15587/1729-4061.2019.188976
5. Kolyadenko, Yu. Yu., Chursanov, N. A., Bondarenko, O. S. (2019). Model of electromagnetic interactions in LTE network. Radiotekhnika, 196, 46–50. doi: https://doi.org/10.30837/rt.2019.1.196.05
6. Bobreshov, A. M., Mymrikova, N. N. (2013). Problemy analiza sil'no nelineynyh rezhimov elektronnyh ustroystv na osnove ryadov Vol'terry. Voronezhskiy gosudarstvennyy universitet. Vestnik VGU. Seriya: fizika. Matematika, 2, 15–25.
7. Bussgang, D., Erman, L., Greyam, D. (1974). Analiz nelineynyh sistem pri vozdeystvii neskol'kih vhodnyh signalov. TIIER, 62 (8), 56–82.
8. Bedrosyan, E., Rays, S. O. (1971). Svoystva vyhodnogo signala sistem, opisyvaemyh ryadami Vol'terra (nelineynyh sistem s pamyat'yu), pri podache na vhod garmonicheskih kolebaniy i gaussova shuma. TIIER, 59 (12), 58–82.

9. Chong, E. The Volterra series and the direct method of distortion analysis. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.7283&rep=rep1&type=pdf
10. Kolding, T. E., Larsen, T. (1997). High-order volterra series analysis using parallel computing. International Journal of Circuit Theory and Applications, 25 (2), 107–114. doi: https://doi.org/10.1002/(sici)1097-007x(199703/04)25:2<107::aid-cta956>3.0.co;2-y
11. Heiskanen, A., Rahkonen, T. (2002). 5th order multi-tone Volterra simulator with component-level output. 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353). doi: https://doi.org/10.1109/iscas.2002.1010293
12. Schreurs, D., ODroma, M., Goacher, A. A., Gadringer, M. (Eds.) (2008). RF Power Amplifier Behavioral Modeling. Cambrige University Press. doi: https://doi.org/10.1017/cbo9780511619960
13. Dobes, J. (2008). Using Volterra Series for an Estimation of Fundamental Intermodulation Products. Radioengineering, 17 (4), 59–64.
14. Anilionienė, J. (2011). The Volterra series of distortion analysis. Lietuvos Matematikos Rinkinys, 52. doi: https://doi.org/10.15388/lmr.2011.mt01
15. Cooman, A., Bronders, P., Peumans, D., Vandersteen, G., Rolain, Y. (2018). Distortion Contribution Analysis With the Best Linear Approximation. IEEE Transactions on Circuits and Systems I: Regular Papers, 65 (12), 4133–4146. doi: https://doi.org/10.1109/tcsi.2018.2834139
16. Yu, H., El-Sankary, K., El-Masry, E. I. (2015). Distortion Analysis Using Volterra Series and Linearization Technique of Nano-Scale Bulk-Driven CMOS RF Amplifier. IEEE Transactions on Circuits and Systems I: Regular Papers, 62 (1), 19–28. doi: https://doi.org/10.1109/tcsi.2014.2341116
17. Gourary, M. M., Rusakov, S. G., Ulyanov, S. L., Zharov, M. M., Mulvaney, B. J. (2011). Circuit Distortion Analysis Based on the Simplified Newton's Method. Journal of Electrical and Computer Engineering, 2011, 1–11. doi: https://doi.org/10.1155/2011/540305
18. Wei, W., Ye, P., Song, J., Zeng, H., Gao, J., Zhao, Y. (2019). A Behavioral Dynamic Nonlinear Model for Time-Interleaved ADC Based on Volterra Series. IEEE Access, 7, 41860–41873. doi: https://doi.org/10.1109/access.2019.2905365
19. Maas, S. A. (2003). Nonlinear Microwave and RF Circuits. Artech House, 608.
20. Schetzen, M. (2006). The Volterra and Wiener Theories of Nonlinear Systems. Krieger Pub Co, 595.
21. Doroshenko, T. V., Selivanov, K. A. (2006). Opredelenie parametrov vihidnogo signala priemnika signalov s pomoshch'yu ryadov Vol'terra. Radiotekhnika, 144, 182–186.
22. Moskalets, N. V., Selivanov, K. A., Nikitenko, T. V. (2011). Analiz nelineynyh iskazheniy v radiotrakte s primeneniem razlichnyh metodov otsenki nelineynosti. Problemy telekommunikatsiy, 2 (4), 150–161. Available at: https://openarchive.nure.ua/bitstream/document/469/1/112_selivanov_radio.pdf
23. Bogdanovich, B. M. (1980). Nelineynye iskazheniya v priemno-usilitel'nyh ustroystvah. Moscow: Svyaz', 280.
24. Baskakov, S. I. (1988). Radiotehnicheskie tsepi i signaly. Moscow: Vysshaya shkola, 446.

DOI: 10.15587/1729-4061.2020.210683

DEVELOPMENT OF A MODIFIED UMAC ALGORITHM BASED ON CRYPTO-CODE CONSTRUCTIONS (p. 45–63)

Alla Gavrilova
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-2015-8927

Ihor Volkov
Scientific-Research Center of Missile Troops and Artillery, Sumy, Ukraine
ORCID: http://orcid.org/0000-0001-6332-7586

Yuliia Kozhedub
Institute of Special Communication and Information Security of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-6181-5519

Roman Korolev
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-7948-5914

Oleksandr Lezik
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-7186-6683

Volodymyr Medvediev
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-1113-5042

Oleksandr Milov
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-6135-2120

Bogdan Tomashevsky
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: http://orcid.org/0000-0002-1934-4773

Andrii Trystan
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-2137-5712

Oksana Chekunova
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-9613-7244

The development of computer technology has determined the vector for the expansion of services based on the Internet and "G" technologies. The main requirements for modern services in the banking sector are security and reliability. At the same time, security is considered not only as ensuring the confidentiality and integrity of transactions, but also their authenticity. However, in the post-quantum period, US NIST specialists question the durability of modern means of providing basic security services based on symmetric and asymmetric cryptography algorithms. The increase in computing resources allows attackers to use modern threats in combination. Thus, there is a need to search for new and/or modify known algorithms for generating MAC (message authentication codes). In addition, the growth of services increases the amount of information that needs to be authenticated. Among the well-known hash algorithms, the hash functions of universal hashing are distinguished, which allow initially determining the number of collisions and their uniform distribution over the entire set of hash codes. Possibilities of modifying the cascade hashing algorithm UMAC (message authentication code based on universal hashing, universal MAC) based on the use of McEliece crypto-code construction on algebrogeometric (elliptic codes (EC), modified elliptic codes (MEC) and damaged codes (DC). This approach allows preserving the uniqueness property, in contrast to the classical UMAC scheme based on a block symmetric cipher (AES). The presented algorithms for evaluating the proper-

ties of universality and strict universality of hash codes make it possible to evaluate the security of the proposed hashing constructs based on universal hash functions, taking into account the preservation of the universality property.

Keywords: authenticity, hashing algorithm, crypto-code constructions, elliptic codes, modified elliptic codes, damaged codes, UMAC algorithm, MV2 algorithm (universal damage mechanism), post-quantum cryptography.

References

1. Evseev, S., Kotz, H., Korol, O. (2015). Analysis of the legal framework for the information security management system of the NSMEP. Eastern-European Journal of Enterprise Technologies, 5 (3 (77)), 48–59. doi: https://doi.org/10.15587/1729-4061.2015.51468
2. Evseev, S., Abdullayev, V. (2015). (2015). Monitoring algorithm of two-factor authentication method based on passwindow system. Eastern-European Journal of Enterprise Technologies, 2 (2 (74)), 9–16. doi: https://doi.org/10.15587/1729-4061.2015.38779
3. Aktual'nye kiberugrozy – 2017: trendy i prognozy (2018). Positive technologies. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017/
4. Aktual'nye kiberugrozy – 2018. Trendy i prognozy (2019). Positive technologies. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
5. Aktual'nye kiberugrozy: itogi 2019 goda (2020). Positive technologies. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/
6. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multifactor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175
7. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461
8. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903
9. Sidel'nikov, V. M. (2002). Kriptografiya i teoriya kodirovaniya. Materialy konferentsii "Moskovskiy universitet i razvitie kriptografii v Rossii".
10. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K. (2016). Guide for cybersecurity event recovery. NIST. doi: https://doi.org/10.6028/nist.sp.800-184
11. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
12. Cichonski, J., Franklin, J. M., Bartock, M. (2017). Guide to LTE security. NIST. doi: https://doi.org/10.6028/nist.sp.800-187
13. Lohachab, A., Lohachab, A., Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, 9, 100174. doi: https://doi.org/10.1016/j.iot.2020.100174
14. Petrenko, K., Mashatan, A., Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications, 46, 151–163. doi: https://doi.org/10.1016/j.jisa.2019.03.007
15. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o., 284. doi: https://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018
16. Gorbenko, Y., Ganzya, R. (2014). Analysis of the possibility of quantum computers and quantum computings for cryptanalysis of modern cryptosystems. Eastern-European Journal of Enterprise Technologies, 1 (9 (67)), 8–16. doi: https://doi.org/10.15587/1729-4061.2014.19897
17. Korol, O. G., Parhuts, L. T., Evseev, S. P. (2013). Method of forming cascade mac-code using modular transformation. Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika, 15 (158), 147–157.
18. Kuznetsov, A. A., Korol, O. G., Evseev, S. P. (2012). Studying collision characteristics of authentication codes of messages UMAC. Applied Radio Electronics, 11 (2), 171–183.
19. Evseev, S., Yokhov, O., Korol, O. (2013). Data Hashing in Information Systems. Kharkiv: Vyd. KhNEU, 312.
20. Kuznetsov, O. O., Horbenko, Yu. I., Kiyan, A. S., Uvarova, A. O., Kuznetsova, T. Yu. (2018). Porivnialni doslidzhennia ta analiz efektyvnosti hibrydnoi kodovoi kryptosystemy. Radyotekhnyka, 195, 61–69. Available at: http://nbuv.gov.ua/UJRN/rvmnts_2018_195_9
21. Marquez-Corbella, I., Tillich, J.-P. (2016). Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography. 2016 IEEE International Symposium on Information Theory (ISIT). doi: https://doi.org/10.1109/isit.2016.7541435
22. Kapshikar, U., Mahalanobis, A. (2018). A Quantum-Secure Niederreiter Cryptosystem using Quasi-Cyclic Codes. Proceedings of the 15th International Joint Conference on e-Business and Telecommunications. doi: https://doi.org/10.5220/0006843005060513
23. Abidin, A. (2012). On Security of Universal Hash Function Based Multiple Authentication. Lecture Notes in Computer Science, 303–310. doi: https://doi.org/10.1007/978-3-642-34129-8_27
24. Handschuh, H., Preneel, B. (2008). Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. Advances in Cryptology – CRYPTO 2008, 144–161. doi: https://doi.org/10.1007/978-3-540-85174-5_9
25. Abouhogail, R. A. (2011). New multicast authentication protocol for entrusted members using advanced encryption standard. The Egyptian Journal of Remote Sensing and Space Science, 14 (2), 121–128. doi: https://doi.org/10.1016/j.ejrs.2011.11.003
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. Stinson, D. R. (1994). Combinatorial techniques for universal hashing. Journal of Computer and System Sciences, 48 (2), 337–346. doi: https://doi.org/10.1016/s0022-0000(05)80007-8
28. Sarvate, D. G. Seberry, J. (1986) Encryption methods based on combinatorial designs. Available at: https://ro.uow.edu.au/cgi/viewcontent.cgi?article=2034&context=infopapers
29. Khalimov, G. Z. (2013). Strongly universal hashing. Applied Applied Radio Electronics, 12 (2), 220–224.
30. Simmons, G. J. (1988). An Impersonation-Proof Identity Verification Scheme. Lecture Notes in Computer Science, 211–215. doi: https://doi.org/10.1007/3-540-48184-2_17
31. Simmons, G. J. (1985). Authentication Theory/Coding Theory. Lecture Notes in Computer Science, 411–431. doi: https://doi.org/10.1007/3-540-39568-7_32
32. Kuznetsov, A. A., Korol', O. G., Bos'ko, V. V. (2011). Model of forming of codes of authentification of messages with the use of universal hash functions. Systemy obrobky informatsiyi, 3 (93), 117–125.
33. Alekseev, M. O. (2014). Protection against algebraic manipulations based on a scalar product operation. Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy, 2, 47–53.

34. Alekseev, M. O., Mironchikov, E. T. (2011). Ob obnaruzhenii oshibok s pomoshch'yu nelineynyh kodov. Nauchnaya sessiya GUAP, 1, 40–43.
35. Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P. (1999). UMAC: Fast and Secure Message Authentication. Lecture Notes in Computer Science, 216–233. doi: https://doi.org/10.1007/3-540-48405-1_14
36. Ferguson, N., Schneier, B. (2004). Practical Cryptography. Moscow: Izdatel'skiy dom "Vil'yams", 432.
37. Kuznetsov, A. A., Pushkarev, A. I., Svatovskiy, I. I., Shevtsov, A. V. (2016). Nesimmetrichnye kriptosistemy na algebraicheskih kodah dlya postkvantovogo perioda. Radiotehnika, 186, 70–90.
38. Krovetz, T., Rogaway, P. (2001). Fast Universal Hashing with Small Keys and No Preprocessing: The PolyR Construction. Information Security and Cryptology – ICISC 2000, 73–89. doi: https://doi.org/10.1007/3-540-45247-8_7
39. Krovetz, T. (2000). Software-Optimized Universal Hashing and Message Authentication. University of California Davis, 269.
40. Krovetz, T. (Ed.). (2006). UMAC: Message Authentication Code using Universal Hashing. doi: https://doi.org/10.17487/rfc4418
41. Korol, O. G. (2015). Evaluation of the computational complexity of some hash functions. Systemy obrobky informatsiyi, 4, 105–110.
42. Krovetz, T., Black, J., Halevi, S., Hevia, A., Krawczyk, H., Rogaway, P. (2000). UMAC. Primitive submitted to NESSIE, 157–160.
43. Bosselaers, A., Govaerts, R., Vandewalle, J. (1996). Fast Hashing on the Pentium. Lecture Notes in Computer Science, 298–312. doi: https://doi.org/10.1007/3-540-68697-5_23
44. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity and Encryption. Version 0.15 (beta). Springer-Verlag.
45. Evseev, S., Korol, O., Ohurtsov, V. (2014). Advanced algorithm UMAC based modular transformations. Eastern-European Journal of Enterprise Technologies, 1 (9 (67)), 16–23. doi: https://doi.org/10.15587/1729-4061.2014.20130
46. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 19–35. doi: https://doi.org/10.15587/1729-4061.2017.109879
47. Yevseiev, S. (2017). The use of damaged codes in crypto code systems. Systemy obrobky informatsiyi, 5, 109–121. Available at: http://nbuv.gov.ua/UJRN/soi_2017_5_17
48. Havrylova, A., Korol, O., Milevskyi, S. (2019). Mathematical model of authentication of a transmitted message based on a mceliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm. Cybersecurity: Education, Science, Technique, 5, 40–51. doi: https://doi.org/10.28925/2663-4023.2019.5.4051
49. Yevseiev, S., Havrylova, A. (2020). Improved umac algorithm with crypto-code mceliece's scheme. Modern problems of computer science and IT-education. Vienna, 79–92. doi: https://doi.org/10.29013/melnikk.shmatkoo.mpcsie.2020.352
50. 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.
51. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18–26. doi: https://doi.org/10.15587/1729-4061.2016.75250
52. Mishchenko, V. A., Vilanskiy, Yu. V. (2007). Ushcherbnye teksty i mnogokanal'naya kriptografiya. Minsk: Entsiklopediks, 292.
53. Mishchenko, V. A., Vilanskiy, Yu. V., Lepin, V. V. (2007). Kriptograficheskiy algoritm MV 2. Minsk: Entsiklopediks, 176.
54. Korol', O. G. (2010). Issledovanie kollizionnyh svoystv kodov autentifikatsii soobshcheniy UMAC. Systemy obrobky informatsiyi. Problemy i perspektyvy rozvytku IT-industriyi, 7 (88), 221.
55. Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S. et. al. (2000). A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST. doi: https://doi.org/10.6028/nist.sp.800-22

АНОТАЦІЇ
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2020.202820
DEVELOPMENT OF BREAST CANCER DIAGNOSIS SYSTEM BASED ON FUZZY LOGIC AND PROBABILISTIC NEURAL NETWORK (p. 6–13)

Taha Mohammed Hasan, Sahab Dheyaa Mohammed, Jumana Waleed

Рак молочної залози є одним з найбільш поширених видів раку, що вражають жінок у всьому світі. Це відбувається, коли клітини в тканинах молочної залози починають рости неконтрольованим чином. Оскільки рак призводить до смерті, раннє виявлення та діагностика є дуже важливим завданням для порятунку життя пацієнтів. Через обмежену кількість спостерігачів, важливу роль у виявленні ранніх ознак раку грає комп'ютер. Запропонована система використовує багатомасштабний аналіз і перетворення «верх капелюха» для виявлення підозрілих областей на мамограмі. Для виділення ознак в області, що цікавить використовується дискретне вейвлет-перетворення. Для класифікації пухлини на нормальну або аномальну використовуються нечітка логіка (НЛ) і імовірнісна нейронна мережа (ІНМ). Відмінність запропонованої системи від інших досліджень полягає у використанні адаптивного порогового значення в залежності від кожного зображення з використанням дискретного вейвлет-перетворення (ДВП) як на етапі сегментації, так і на етапі виділення ознак, що зменшує складність і час. Крім того, виявлення більше однієї пухлини на мамограмі молочної залози і використання НЛ і ІНМ працює на підвищення ефективності системи, що призводить до підвищення точності системи і скорочення часу. Отримані результати точності, чутливості і специфічності становили 99 %, 98 % і 47 % відповідно. Дані результати показали, що запропонована система є більш точною, ніж інші попередні аналогічні роботи.

Ключові слова: діагностика раку молочної залози, нечітка логіка (НЛ), імовірнісна нейронна мережа (ІНМ).

DOI: 10.15587/1729-4061.2020.208554
DEVELOPMENT OF COMPLEX METHODOLOGY OF PROCESSING HETEROGENEOUS DATA IN INTELLIGENT DECISION SUPPORT SYSTEMS (p. 14–23)

P. Zuiev, R. Zhyvotovskyi, O. Zvieriev, S. Hatsenko, V. Kuprii, O. Nakonechnyi, M. Adamenko, A. Shyshatskyi, Ye. Neroznak, V. Velychko

Розроблену комплексну методику обробки різнотипних даних в інтелектуальних системах підтримки прийняття рішень. Зазначена методика призначена для підвищення оперативності обробки різнотипних даних в інтелектуальних системах підтримки прийняття рішень. Комплексна методика складається з наступних взаємопов'язаних процедур: модель зберігання різнорідних даних; алгоритм синхронізації різнорідних даних; алгоритм розділення різнорідних даних; алгоритм індексування різнорідних даних. Модель зберігання різнорідних розвідувальних даних, яка є основою методики, відрізняється наявністю шаблонів об'єктів розвідки і шаблонів параметрів об'єктів розвідки. Шаблони дозволяють розподіллено зберігати як неструктуровані різнорідні розвідувальні дані, так і структуровані розвідувальні дані відповідно до визначеної схеми, що дозволяє знизити часові витрати на доступ до даних. В моделі зберігання різнорідних розвідувальних даних розроблені алгоритм синхронізації різнорідних розвідувальних даних, алгоритм розділення різнорідних розвідувальних даних та алгоритм індексування різнорідних розвідувальних даних Ефективна структура зберігання різнорідних даних озер даних дозволяє зручно і швидко здійснювати доступ до сховища для пакетної обробки даних. Розробка запропонованої методики обумовлена необхідністю підвищення оперативності обробки різнотипної інформації в інтелектуальних системах підтримки прийняття рішень з прийнятною обчислювальною складністю. Запропонована методика дозволяє підвищити ефективність функціонування інтелектуальних систем підтримки прийняття рішень за рахунок комплексної обробки даних, що в них циркулюють. Запропонована методика дозволяє підвищити оперативність обробки інформації в системах підтримки прийняття рішень від 16 до 20 % в залежності від кількості інформації про об'єкт моніторингу.

Ключові слова: система підтримки прийняття рішень, об'єкт моніторингу, різнотипні дані, обчислювальна складність, обробка інформації, тип інформації.

DOI: 10.15587/1729-4061.2020.209930
DEVELOPMENT OF CAN NETWORK WITH IMPROVED PARAMETERS FOR ADAPTIVE CAR FRONT LIGHTING SYSTEM (p. 24–33)

K. Soroka, V. Kharchenko, V. Pliuhin

Виконано аналіз принципів реалізації та алгоритмів роботи адаптивної системи переднього освітлення (далі – АСПО) автомобіля і методів управління її роботою. АСПО прийнята ЄЕК ООН в 2007 р. в якості правил облаштування систем переднього світла транспортних засобів, при їзді в темний період часу. Серед відомих алгоритмів функціонування АСПО вибрано алгоритм попереднього огляду, оснований на особливостях спостереження водієм за дорогою перед ТЗ, з врахуванням характеристик його зору. Проаналізовано вимоги алгоритму до системи керування. Розглянуто методи керування з використанням контролерів системи Ардуіно і комп'ютерної мережі. Враховуючи можливості, які надають мережеві технології для забезпечення якості керування, вибрано CAN мережу (англ. Controller Area Network – мережа контролерів). Рекомендовано використати варіант CAN мережі довжиною 40 чи 100 м зі швидкодією 1000, 500 кбіт/с відповідно. Розраховані параметри роботи мережі: швидкодія, ймовірності помилок, залежність продуктивності від завантаження, розмір команд і тривалість їх передачі та відповідність вимогам АСПО. Запропоновано удоско-

налити алгоритм арбітражу мережі в напрямку збільшення ймовірності проходження команд із низьким пріоритетом при великій завантаженості. Розроблена на основі CAN мережі АСПО дозволяє створити комфортні умови роботи водія в темний період часу, попереджувати аварійні ситуації, забезпечити безпеку руху.

Аналіз функціонування АСПО показує, що вона безпосередньо пов'язана з роботою більшості основних вузлів автомобіля, а саме: двигуна, рульового керування, коробки передач, гальма, акселерометра та ін. Робота її здійснюється під керуванням водія. Тому ця система може мати розширені функції, може служити основою системи безпеки і основою системи керування роботою автомобіля в цілому.

Ключові слова: безпека руху, переднє освітлення, адаптивна система, контролери Ардуіно, CAN мережа, фрейм даних.

DOI: 10.15587/1729-4061.2020.210754

PROCEDURE FOR DETERMINING THE RESPONSES FROM A NONLINEAR SYSTEM USING THE VOLTERRA SERIES (p. 34–44)

Mohammed Ahmed, Samah Fakhri Aziz, Naors Y. Anad Alsaleem, K. Sielivanov, M. Moskalets

Запропоновано методику оцінки нелінійних ефектів в радіотрактах приймально-передавальних пристроїв радіоелектронних засобів систем мобільного зв'язку заснованої на використанні нелінійних передаточних функцій вищих порядків рядів Вольтера.

Розроблено процедуру отримання вихідних відгуків нелінійного безінерційного кола при гармонійній вхідній дії за допомогою метода визначення передаточних функцій вищих порядків, що отримуються на основі передаточних функцій нижчих порядків.

Отримано аналітичні вирази вихідних відгуків нелінійної системи різних порядків для трьох вхідних вливів у випадку представлення нелінійної системи у вигляді нелінійного безінерційного кола.

Проведено визначення значень передаточних функцій вищих порядків нелінійного безінерційного кола за допомогою метода змінних стану.

Продемонстровано отримання аналітичних виразів щодо розрахунку коефіцієнта гармонік за 2-ю та 3-ю гармоніками з використанням нелінійних передаточних функцій вищих порядків нелінійного безінерційного кола.

Показано, що використання нелінійних передаточних функцій включно до 5-го порядку дає можливість для більш точної оцінки нелінійних ефектів у вигляді гармонійних і інтермодуляційних спотворень у радіотрактах радіоелектронних засобів мобільних систем.

Викладений спосіб визначення нелінійних передаточних функцій є інваріантним до топології нелінійного електричного кола, а також до кількості і виду нелінійних елементів. Існуючі методики оцінки електромагнітної сумісності в задачах розрахунку інтермодуляційних завад можуть бути вдосконалені за рахунок внеску визначених величин продуктів впливу.

Запропонована методика дозволяє провести оцінку комплексу нелінійних ефектів в задачах електромагнітної сумісності в угрупованнях радіоелектронних засобів з необхідною для користувачів точністю.

Ключові слова: нелінійна система, ряди Вольтерра, передаточна функція, нелінійне безінерційне коло.

DOI: 10.15587/1729-4061.2020.210683

DEVELOPMENT OF A MODIFIED UMAC ALGORITHM BASED ON CRYPTOCODE CONSTRUCTIONS (p. 45–63)

A. Gavrilova, I. Volkov, Y. Kozhedub, R. Korolev, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova

Розвиток обчислювальної техніки визначив вектор напрямку розширення послуг на основі Інтернет-технологій та технологій «G». Основними вимогами, визначеними до сучасних послуг в банківському секторі, є безпека і надійність. Однак в умовах постквантового періоду фахівцями НІСТ США ставиться під сумнів стійкість сучасних засобів забезпечення основних послуг безпеки на основі криптоалгоритмів симетричної і несиметричної криптографії. Зростання обчислювальних ресурсів дозволяє зловмисникам використовувати сучасні загрози в комплексі.Таким чином вони отримують властивості синергізму і гібридності, що значно збільшує можливість їх реалізації. Тому виникає необхідність пошуку нових і/або модифікація відомих алгоритмів формування MAC-кодів (message authentication code). Крім того, зростання послуг в кіберпросторі збільшує обсяги інформації, автентичність якої необхідно забезпечити. Серед відомих геш-алгоритмів виділяються геш-функції універсального гешування, що дозволяють спочатку визначити кількість колізій і їх рівномірний розподіл по всій безлічі геш-кодів. Розглянуто можливості модифікації каскадного алгоритму гешування UMAC на основі використання крипто-кодової конструкції Мак-Еліса на алгебро геометричних (еліптичних (EC), модифікованих еліптичних (MEC)) кодах та збиткових кодах (DC). Такий підхід дозволяє зберегти властивість унікальності на відміну від класичної схеми UMAC (message authentication code based on universal hashing, universal MAC) на основі блочного симетричного шифру (AES). Представлені алгоритми оцінки властивостей універсальності і суворої універсальності геш-кодів, які дозволяють оцінити стійкість запропонованих конструкцій гешування на основі універсальних геш-функцій з урахуванням збереження властивості універсальності.

Ключові слова: автентичність, алгоритм гешування, крипто-кодові конструкції, еліптичні коди, модифіковані еліптичні коди,збиткові коди, алгоритм UMAC, алгоритм MV2 (універсальний механізм нанесення збитку), постквантова криптографія.