ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEMS

DOI: 10.15587/1729-4061.2018.139997

DETECTION OF HUMAN RESPIRATION PATTERNS USING DEEP CONVOLUTION NEURAL NETWORKS (p. 6-13)

Anatoly Petrenko
Institute of Applied Systems Analysis
National Technical University of Ukraine
"Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-6712-7792

Roman Kyslyi
Institute of Applied Systems Analysis
National Technical University of Ukraine
"Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-8290-9917

Ihor Pysmennyi
Institute of Applied Systems Analysis
National Technical University of Ukraine
"Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-7648-2593

The method for real-time recognition of respiration types (patterns) of a patient to monitor his conditions and threats to his health, which is a special case of the problem of human activities recognition (HAR), was proposed. The method is based on application of deep machine learning using the convolution neural network (CNN) to classify the chest motion speed. It was shown that the decisions, taken in this case, are coordinated with mobile medicine technology (mHealth) of the use of body sensors and smartphones for signals processing, but CNN offer important additional opportunities at improving the quality of processing the accelerometer-sensor signals in the presence of interfering signals (noise) from other sources and instrumental errors of devices. We proposed the method of transformation of one-dimensional (1D) accelerometer signals into two-dimensional (2D) graphic images, processed using CNN with multiple processing layers, due to which the accuracy of determining the respiration pattern in various situations for different physical states of patients increases compared with the case when two-dimensional accelerometer signal conversion is not used. In this case, an increase in accuracy (or quality) of determining different types of respiration occurs while maintaining a sufficient speed of performing procedures of the planned method, which allows classification of respiration types in real time. This technique was tested as a component of the Body Sensor Network (BSN) and high accuracy (88 %) of determining the patient's respiration state was established, which in combination with contextual data, obtained from other BSN nodes, makes it possible to determine the patient's state and a signal of the aggravation of their respiratory diseases.

Keywords: accelerometer, deep learning, respiration patterns, convolution neural networks, machine learning.

References

1. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. Available at: http://www.deeplearningbook.org/
2. Huynh, T., Schiele, B. (2005). Analyzing features for activity recognition. Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence Innovative Context-Aware Services: Usages and Technologies – sOc-EUSAI '05. doi: https://doi.org/10.1145/1107548.1107591
3. Larson, E. C., Goel, M., Boriello, G., Heltshe, S., Rosenfeld, M., Patel, S. N. SpiroSmart: Using a Microphone to Measure Lung Function on a Mobile Phone. Available at: https://homes.cs.washington.edu/~shwetak/papers/SpiroSmart.CR.Final.pdf
4. Shephard, R. J. (1966). The oxygen cost of breathing during vigorous exercise. Quarterly Journal of Experimental Physiology and Cognate Medical Sciences, 51 (4), 336–350. doi: https://doi.org/10.1113/expphysiol.1966.sp001868
5. Rakhimov, A. Abnormal breathing pattern causes asthma and attacks. Available at: https://www.worldwidehealth.com/health-article-Abnormal-breathing-pattern-causes-asthma-and-attacks.html
6. Fekr, A. R., Janidarmian, M., Radecka, K., Zilic, Z. (2005). Movement analysis of the chest compartments and a real-time quality feedback during breathing therapy. In Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence: Innovative Context-aware Services: Usages and Technologies.
7. Bates, A., Ling, M. J., Mann, J., Arvind, D. K. (2010). Respiratory Rate and Flow Waveform Estimation from Tri-axial Accelerometer Data. 2010 International Conference on Body Sensor Networks. doi: https://doi.org/10.1109/bsn.2010.50
8. Que, C.-L., Kolmaga, C., Durand, L.-G., Kelly, S. M., Macklem, P. T. (2002). Phonospirometry for noninvasive measurement of ventilation: methodology and preliminary results. Journal of Applied Physiology, 93 (4), 1515–1526. doi: https://doi.org/10.1152/japplphysiol.00028.2002
9. Liu, G.-Z., Guo, Y.-W., Zhu, Q.-S., Huang, B.-Y., Wang, L. (2011). Estimation of Respiration Rate from Three-Dimensional Acceleration Data Based on Body Sensor Network. Telemedicine and e-Health, 17 (9),705–711. doi: https://doi.org/10.1089/tmj.2011.0022
10. Yoon, J.-W., Noh, Y.-S., Kwon, Y.-S., Kim, W.-K., Yoon, H.-R. (2014). Improvement of Dynamic Respiration Monitoring Through Sensor Fusion of Accelerometer and Gyro-sensor. Journal of Electrical Engineering and Technology, 9 (1), 334–343. doi: https://doi.org/10.5370/jeet.2014.9.1.334
11. Jin, A., Yin, B., Morren, G., Duric, H., Aarts, R. M. (2009). Performance evaluation of a tri-axial accelerometry-based respiration monitoring for ambient assisted living. 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society. doi: https://doi.org/10.1109/iembs.2009.5333116
12. Uddin, J., Van, D. N., Kim, J.-M. (2015). Accelerating 2D Fault Diagnosis of an Induction Motor using a Graphics Processing Unit. International Journal of Multimedia and Ubiquitous Engineering, 10 (1), 341–352. doi: https://doi.org/10.14257/ijmue.2015.10.1.32
13. Ciobotariu, R., Adochiei, F., Rotariu, C., Costin, H. (2011). Wireless breathing system for long term telemonitoring of respiratory activity. Advanced topics in electrical engineering, Proceedings of the 7th international symposium ATEE, 635–638.
14. Bulling, A., Blanke, U., Schiele, B. (2014). A tutorial on human activity recognition using body-worn inertial sensors. ACM Computing Surveys, 46 (3), 1–33. doi: https://doi.org/10.1145/2499621
15. Zhang, J., Mitliagkas, I. YellowFin and the Art of Momentum Tuning. Available at: https://arxiv.org/pdf/1706.03471.pdf

16. Yang, J. B., Nguyen, M. N., San, P. P., Li, X. L., Krishnaswamy, S. (2015). Deep Convolutional Neural Networks On Multichannel Time Series For Human Activity Recognition. Proceeding IJCAI'15 Proceedings of the 24th International Conference on Artificial Intelligence, 3995–4001.
17. Zeng, M., Nguyen, L. T., Yu, B., Mengshoel, O. J., Zhu, J., Wu, P., Zhang, J. (2014). Convolutional Neural Networks for Human Activity Recognition using Mobile Sensors. Proceedings of the 6th International Conference on Mobile Computing, Applications and Services. doi: https://doi.org/10.4108/icst.mobicase.2014.257786
18. Jiang, W., Yin, Z. (2015). Human Activity Recognition Using Wearable Sensors by Deep Convolutional Neural Networks. Proceedings of the 23rd ACM International Conference on Multimedia – MM '15. doi: https://doi.org/10.1145/2733373.2806333
19. Ordóñez, F., Roggen, D. (2016). Deep Convolutional and LSTM Recurrent Neural Networks for Multimodal Wearable Activity Recognition. Sensors, 16 (1), 115. doi: https://doi.org/10.3390/s16010115

DOI: 10.15587/1729-4061.2018.139682

ANALYSIS OF PROBABILITIES OF DIFFERENTIALS FOR BLOCK CIPHER "KALYNA" (DSTU 7624:2014) (p.14-19)

Victor Ruzhentsev
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-1007-6530

Valerii Sokurenko
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-8923-5639

Yuriy Ulyanchenko
Kharkiv Regional Institute of Public Administration of the National Academy of Public Administration attached to the Office of the President of Ukraine, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-2770-8685

The adaptation and application of the method for estimating the upper bound of the probability of two-round differentials for the block symmetric cipher Kalyna is carried out. This cipher was adopted as the Ukrainian standard DSTU 7624: 2014 in 2015. Known methods allow getting only the approximate value of this parameter for this cipher or cannot be applied explicitly through the structural features of this cipher. Using the approximate probability of two-round differentials gives an even greater error in the evaluation of the probabilities of differentials with a large number of rounds, as well as in assessing the resistance of the encryption algorithm to other types of differential attacks.

The main stages of the used method are the following: definition of the minimum number of active S-boxes; definition of the type of differential characteristic having the maximum probability; determination of the number and probabilities of additional differential characteristics.

In the course of research, an adapted method has allowed clarifying the upper bound of the probability of 2-round differentials for the cipher Kalyna significantly. This bound is ≈2–47.3 instead of 2–40 when using the method for nested SPN ciphers.

The elaborated upper bound of the probability of 2-round differentials allowed clarifying also the bound value of the probability of 4-round differentials. For Kalyna-128 (block size 128 bits), the value is specified 214.6 times, for Kalyna-256 – 229.2 times, Kalyna-512 – 258.4 times.

The main advantage of the method adapted for the Kalyna cipher was the possibility of a significant specification of the upper bound of the probability of a 2-round differential. The disadvantage of the adapted method is that assumptions are made, such as, for example, the use of one substitution instead of four in the original algorithm. The result of this assumption is that a real bound of the probability of 2-round differentials could be even smaller.

Keywords: block ciphers, cryptographic security, Rijndael, AES, Rijndael-like cipher, differential probability, differential characteristic, difference table, Kalyna, DSTU 7624: 2014.

References

1. Hong, S., Lee, S., Lim, J., Sung, J., Cheon, D., Cho, I. (2001). Provable Security against Differential and Linear Cryptanalysis for the SPN Structure. Lecture Notes in Computer Science, 273–283. doi: https://doi.org/10.1007/3-540-44706-7_19
2. Keliher, L., Meijer, H., Tavares, S. (2001). Improving the Upper Bound on the Maximum Average Linear Hull Probability for Rijndael. Lecture Notes in Computer Science, 112–128. doi: https://doi.org/10.1007/3-540-45537-x_9
3. Sano, F., Ohkuma, K., Shimizu, H., Kawamura, S. (2003). On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis. IEICE Trans. Fundamentals, 37–46.
4. Daemen, J., Rijmen, V. Two-Round AES Differentials. Available at: https://eprint.iacr.org/2006/039.pdf
5. Daemen, J., Lamberger, M., Pramstaller, N., Rijmen, V., Vercauteren, F. (2009). Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers. Computing, 85 (1-2), 85–104. doi: https://doi.org/10.1007/s00607-009-0034-y
6. Oliynykov, R., Gorbenko, I., Dolgov, V., Ruzhentsev, V. (2010). Results of Ukrainian national public cryptographic competition. Tatra Mountains Mathematical Publications, 47 (1), 99–113. doi: https://doi.org/10.2478/v10127-010-0033-6
7. Granger, R., Kleinjung, T., Zumbrägel, J. On the discrete logarithm problem in finite fields of fixed characteristic. Available at: https://eprint.iacr.org/2015/685.pdf
8. Keliher, L., Sui, J. (2007). Exact maximum expected differential and linear probability for two-round Advanced Encryption Standard. IET Information Security, 1 (2), 53. doi: https://doi.org/10.1049/iet-ifs:20060161
9. Ruzhentsev, V. I. (2011). Two-rounds AES differentials probability estimation. Applied Radio Electronics, 10 (2), 116–121.
10. Lysytska, I. V. (2012). Comparing on effectiveness of superboxes for some modern cipher. Radioelectronics, computer science, management, 1, 37–44.
11. Dolgov, V. I., Kuznetsov, A. A., Isaev, S. A. (2011). Differential properties of block symmetric ciphers submitted to the Ukrainian competition. Electronic simulation, 33 (6), 81–99.
12. Ruzhentsev, V. I. (2014). The probabilities of two-rounds differentials for Rijndael-like ciphers with random substitutions. Applied Radio Electronics, 13 (3), 235–238.
13. Kang, J.-S. K., Hong, S. H., Lee, S. L., Yi, O. Y., Park, C. P., Lim, J. L. (2001). Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks. ETRI Journal, 23 (4), 158–167. doi: https://doi.org/10.4218/etrij.01.0101.0402

DOI: 10.15587/1729-4061.2018.139923
IMPROVING THE EFFECTIVENESS OF TRAINING THE ON-BOARD OBJECT DETECTION SYSTEM FOR A COMPACT UNMANNED AERIAL VEHICLE (p. 19-26)

Vyacheslav Moskalenko
Sumy State University, Sumy, Ukraine
ORCID: http://orcid.org/0000-0001-6275-9803

Anatoly Dovbysh
Sumy State University, Sumy, Ukraine
ORCID: http://orcid.org/0000-0003-1829-3318

Igor Naumenko
Research Center for Missile Troops and Artillery, Sumy, Ukraine
ORCID: http://orcid.org/0000-0003-2845-9246

Alyona Moskalenko
Sumy State University, Sumy, Ukraine
ORCID: http://orcid.org/0000-0003-3443-3990

Artem Korobov
Sumy State University, Sumy, Ukraine
ORCID: http://orcid.org/0000-0003-3239-1977

The model of object detector and the criterion of leaning effectiveness of the model were proposed. The model contains 7 first modules of the convolutional Squeezenet network, two convolutional multiscale layers and the information-extreme classifier. The multiplicative convolution of the particular criteria that takes into account the effectiveness of detection of objects in the image and accuracy of the classification analysis was considered as the criterion of learning effectiveness of the model. In this case, additional use of the orthogonal matching pursuit algorithm in calculating high-level features makes it possible to increase the accuracy of the model by 4 %. The training algorithm of object detector under conditions of a small size of labeled training datasets and limited computing resources available on board of a compact unmanned aerial vehicle was developed. The essence of the algorithm is to adapt the high-level layers of the model to the domain application area, based on the algorithms of growing sparse coding neural gas and simulated annealing. Unsupervised learning of high-level layers makes it possible to use effectively the unlabeled datasets from the domain area and determine the required number of neurons. It is shown that in the absence of fine tuning of convolutional layers, 69 % detection of objects in the images of the test dataset Inria Aerial Image was ensured. In this case, after fine tuning based on the simulated annealing algorithm, 95 % detection of the objects in test images is ensured.

It was shown that the use of unsupervised pretraining makes it possible to increase the generalizing ability of decision rules and to accelerate the iteration process of finding the global maximum during supervised learning on the dataset of limited size. In this case, the overfitting effect is eliminated by optimal selection of the value of hyperparameter, characterizing the measure of coverage of the input data of by network neurons.

Keywords: growing neural gas, objects detector, information criterion, simulated annealing algorithm.

References

1. Patricia, N., Caputo, B. (2014). Learning to Learn, from Transfer Learning to Domain Adaptation: A Unifying Perspective. 2014 IEEE Conference on Computer Vision and Pattern Recognition. doi: https://doi.org/10.1109/cvpr.2014.187
2. Nguyen, A., Yosinski, J., Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). doi: https://doi.org/10.1109/cvpr.2015.7298640
3. Ayumi, V., Rere, L. M. R., Fanany, M. I., Arymurthy, A. M. (2016). Optimization of convolutional neural network using microcanonical annealing algorithm. 2016 International Conference on Advanced Computer Science and Information Systems (ICACSIS). doi: https://doi.org/10.1109/icacsis.2016.7872787
4. Antipov, G., Berrani, S.-A., Ruchaud, N., Dugelay, J.-L. (2015). Learned vs. Hand-Crafted Features for Pedestrian Gender Recognition. Proceedings of the 23rd ACM International Conference on Multimedia – MM '15. doi: https://doi.org/10.1145/2733373.2806332
5. Carrio, A., Sampedro, C., Rodriguez-Ramos, A., Campoy, P. (2017). A Review of Deep Learning Methods and Applications for Unmanned Aerial Vehicles. Journal of Sensors, 2017, 1–13. doi: https://doi.org/10.1155/2017/3296874
6. Xu, X., Ding, Y., Hu, S. X., Niemier, M., Cong, J., Hu, Y., Shi, Y. (2018). Scaling for edge inference of deep neural networks. Nature Electronics, 1 (4), 216–222. doi: https://doi.org/10.1038/s41928-018-0059-3
7. Loquercio, A., Maqueda, A. I., del-Blanco, C. R., Scaramuzza, D. (2018). DroNet: Learning to Fly by Driving. IEEE Robotics and Automation Letters, 3 (2), 1088–1095.doi: https://doi.org/10.1109/lra.2018.2795643
8. Mathew, A., Mathew, J., Govind, M., Mooppan, A. (2017). An Improved Transfer learning Approach for Intrusion Detection. Procedia Computer Science, 115, 251–257. doi: https://doi.org/10.1016/j.procs.2017.09.132
9. Qassim, H., Verma, A., Feinzimer, D. (2018). Compressed residual-VGG16 CNN model for big data places image recognition. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). doi: https://doi.org/10.1109/ccwc.2018.8301729
10. Nakahara, H., Yonekawa, H., Sato, S. (2017). An object detector based on multiscale sliding window search using a fully pipelined binarized CNN on an FPGA. 2017 International Conference on Field Programmable Technology (ICFPT). doi: https://doi.org/10.1109/fpt.2017.8280135
11. Moskalenko, V., Moskalenko, A., Pimonenko, S., Korobov, A. (2017). Development of the method of features learning and training decision rules for the prediction of violation of service level agreement in a cloud-based environment. Eastern-European Journal of Enterprise Technologies, 5 (2 (89)), 26–33. doi: https://doi.org/10.15587/1729-4061.2017.110073
12. Feng, Q., Chen, C. L. P., Chen, L. (2016). Compressed auto-encoder building block for deep learning network. 2016 3rd International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS). doi: https://doi.org/10.1109/iccss.2016.7586437
13. Chen, X., Xiang, S., Liu, C.-L., Pan, C.-H. (2014). Aircraft Detection by Deep Convolutional Neural Networks. IPSJ Transactions on Computer Vision and Applications, 7, 10–17. doi: https://doi.org/10.2197/ipsjtcva.7.10
14. Labusch, K., Barth, E., Martinetz, T. (2009). Sparse Coding Neural Gas: Learning of overcomplete data representations. Neurocomputing, 72 (7-9), 1547–1555. doi: https://doi.org/10.1016/j.neucom.2008.11.027
15. Mrazova, I., Kukacka, M. (2013). Image Classification with Growing Neural Networks. International Journal of Com-

puter Theory and Engineering, 422–427. doi: https://doi.org/10.7763/ijcte.2013.v5.722
16. Palomo, E. J., Lopez-Rubio, E. (2016). The Growing Hierarchical Neural Gas Self-Organizing Neural Network. IEEE Transactions on Neural Networks and Learning Systems, 1–10. doi: https://doi.org/10.1109/tnnls.2016.2570124
17. Rere, L. M. R., Fanany, M. I., Arymurthy, A. M. (2016). Metaheuristic Algorithms for Convolution Neural Network. Computational Intelligence and Neuroscience, 2016, 1–13. doi: https://doi.org/10.1155/2016/1537325
18. Maggiori, E., Tarabalka, Y., Charpiat, G., Alliez, P. (2017). High-Resolution Aerial Image Labeling With Convolutional Neural Networks. IEEE Transactions on Geoscience and Remote Sensing, 55 (12), 7092–7103. doi: https://doi.org/10.1109/tgrs.2017.2740362

DOI: 10.15587/1729-4061.2018.139723

FORMATION OF REFERENCE IMAGES AND DECISION FUNCTION IN RADIOMETRIC CORRELATION-EXTREMAL NAVIGATION SYSTEMS (p. 27-35)

Nataliia Yeromina
Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-0463-2342

Serhii Petrov
Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-8933-9649

Alexander Tantsiura
Ivan Kozhedub Kharkiv National University of Air Force, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-3214-8643

Maksym Iasechko
Ivan Kozhedub Kharkiv National University of Air Force, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-5643-0059

Volodymyr Larin
Ivan Kozhedub Kharkiv National University of Air Force, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-0771-2660

Methods for formation of reference images (RI) and unimodal decision function (DF) have been developed to ensure efficient functioning of radiometric correlation-extreme navigation systems (CENS) of flying machines (FM). The methods were developed for the conditions of CENS position finding on the surfaces of sighting (SS) with a highly developed infrastructure at insignificant altitudes of flight of the flying machine which leads to formation of current images (CI) with a non-stationary structure. Non-stationarity of CI arises when geometric conditions of sighting the three-dimensional objects change. The method of RI formation is based on the use of a set of three-dimensional stationary objects with the highest radio-brightness temperature, their contouring and determination of mean radiobrightness temperature.

A method for forming a unimodal DF of radiometric CENS which takes into account three-dimensional form of SS objects, spatial position and orientation of the FM was developed. The method is based on CI pre-processing which consists in its layering with respect to the mean radiobrightness temperature of background and determination of a set of objects with the highest radiobrightness temperature. The set of objects defined by their contouring is used as a geometric invariant with an informative attribute in the form of average radiobrightness temperature.

It was established by simulating the process of formation of DF that pronounced unimodal DFs are formed at signal-to-noise ratio (q=5...10) at the output of the radiometric channel. At the same time, the possibility of correct localization of the binding object in TI is close to unity and reduction of influence of perspective and scale distortions of images on accuracy of CENS location is ensured.

The simulation results have confirmed effectiveness of the proposed methods of formation of RI and DF for location of radiometric CENS on the sighting surfaces with complex three-dimensional objects leading to formation of a non-stationary CI.

Keywords: correlation-extreme system, reference image, geometric invariants, selective images, decision function.

References

1. Blohinov, A. (2011). Metod kompleksirovaniya dannyh raznorakursnoy s'emki dlya obnaruzheniya slozhnyh ob'ektov v usloviyah sil'noy zashumlennosti. Shtuchnyi intelekt, 3, 220–227.
2. German, E. (2013). Klassifikaciya i issledovanie mer informativnosti izobrazheniy podstilayushchey poverhnosti v korrelyacionno-ekstremal'nyh navigacionnyh sistemah. Vestnik RGRTU, 2 (44), 35–40.
3. Sotnikov, A., Tarshyn, V., Yeromina, N., Petrov, S., Antonenko, N. (2017). A method for localizing a reference object in a current image with several bright objects. Eastern-European Journal of Enterprise Technologies, 3 (9 (87)), 68–74. doi: https://doi.org/10.15587/1729-4061.2017.101920
4. Fursov, V. A., Bibikov, S. A., Yakimov, P. Y. (2013). Localization of objects contours with different scales in images using Hough transform. Computer Optics, 37(4), 496–502. doi: https://doi.org/10.18287/0134-2452-2013-37-4-496-502
5. Potapov, A. A. (2013). Fractal paradigm and fractal-scaling methods in fundamentally new dynamic fractal signal detectors. 2013 International Kharkov Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves. doi: https://doi.org/10.1109/msmw.2013.6622151
6. Tsvetkov, O. V., Tananykina, L. V. (2015). A preprocessing method for correlation-extremal systems. Computer Optics, 39 (5), 738–743. doi: https://doi.org/10.18287/0134-2452-2015-39-5-738-743
7. Vasil'eva, I. (2017). Vydelenie vneshnih konturov ob'ektov raspoznavaniya na mnogokanal'nyh izobrazheniyah. Radioelektronni i kompiuterni systemy, 2 (82), 17–23.
8. Abramov, N., Fralenko, V. P. (2012). Opredelenie rasstoyaniy na osnove sistemy tekhnicheskogo zreniya i metoda invariantnyh momentov. Informacionnye tekhnologii i vychislitel'nye sistemy, 4, 32–39.
9. Gnilitskii, V. V., Insarov, V. V., Chernyavskii, A. S. (2010). Decision making algorithms in the problem of object selection in images of ground scenes. Journal of Computer and Systems Sciences International, 49 (6), 972–980. doi: https://doi.org/10.1134/s1064230710060158
10. Bogush, R., Maltsev, S. (2007). Minimax Criterion of Similarity for Video Information Processing. 2007 Siberian Conference on Control and Communications. doi: https://doi.org/10.1109/sibcon.2007.371310
11. Kharchenko, V., Mukhina, M. (2014). Correlation-extreme visual navigation of unmanned aircraft systems based on speed-up robust features // Aviation, 18 (2), 80–85. doi: https://doi.org/10.3846/16487788.2014.926645
12. Mukhina, M. P., Seden, I. V. (2014). Analysis of modern correlation extreme navigation systems. Electronics and Con-

trol Systems, 1 (39). doi: https://doi.org/10.18372/1990-5548.39.7343
13. Muñoz, X., Freixenet, J., Cufí, X., Martí, J. (2003). Strategies for image segmentation combining region and boundary information. Pattern Recognition Letters, 24 (1-3), 375–392. doi: https://doi.org/10.1016/s0167-8655(02)00262-3
14. Hruska, R., Mitchell, J., Anderson, M., Glenn, N. F. (2012). Radiometric and Geometric Analysis of Hyperspectral Imagery Acquired from an Unmanned Aerial Vehicle. Remote Sensing, 4 (9), 2736–2752. doi: https://doi.org/10.3390/rs4092736
15. Acevo-Herrera, R., Aguasca, A., Bosch-Lluis, X., Camps, A., Martínez-Fernández, J., Sánchez-Martín, N., Pérez-Gutiérrez, C. (2010). Design and First Results of an UAV-Borne L-Band Radiometer for Multiple Monitoring Purposes. Remote Sensing, 2 (7), 1662–1679. doi: https://doi.org/10.3390/rs2071662

DOI: 10.15587/1729-4061.2018.139763

DEVELOPMENT OF SIGNAL CONVERTER OF THERMAL SENSORS BASED ON COMBINATION OF THERMAL AND CAPACITY RESEARCH METHODS (p. 36-42)

Oksana Boyko
Danylo Halytsky Lviv National Medical University, Lviv, Ukraine
ORCID: http://orcid.org/0000-0002-8810-8969

Grygoriy Barylo
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: http://orcid.org/0000-0001-5749-9242

Roman Holyaka
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: http://orcid.org/0000-0002-7720-0372

Zenon Hotra
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: http://orcid.org/0000-0002-6566-6706

Kateryna Ilkanych
Danylo Halytsky Lviv National Medical University, Lviv, Ukraine
ORCID: http://orcid.org/0000-0002-6536-7802

The problem of functional integration of thermal and capacity research methods, which provides the possibility of realizing a new generation of analog front-end of the Internet of Things in the areas of materials science, biophysics and medicine, is solved. Functional integration means the possibility of the use of the same structure for its controlled heating and temperature measurement. For this purpose, instead of discrete resistive heaters and temperature sensors, transistor structures are proposed. This helps to minimize the sizes of measurement transducers, and so the spatial resolution of the transducers-based sensors of thermal analysis.

The concept of constructing the functionally integrated thermal sensors based on the transistor structures and capacitive signal transducers is developed. The novelty of the proposed sensors of thermal analysis, in addition to measurement of temperature and amount of thermo-energy emitted and absorbed in the object of research, is the possibility of measuring the electrical capacity. This possibility could be particularly assured by the measurement of temperature deformation of a research object or a console that is bent under the effect of the object.

The new solution of the control scheme of the transistor transformers that support the pulse managed heating and forming the informative signal of the temperature of transistor is proposed. The high precision Analog Devices AD7747 24-bit converter is taken as the basis of the capacitive signal transducer.

The developed transducer provides the managed heating of research objects and is characterized by the high values of temperature resolution (not worse than 0.01 °C) and electrical capacity (not worse than 10–16 aF) measurement.

Keywords: temperature sensor, transistor structures, capacitive signal transducer, functional integration, converter.

References

1. Baccelli, E., Gundogan, C., Hahm, O., Kietzmann, P., Lenders, M. S., Petersen, H. et. al. (2018). RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT. IEEE Internet of Things Journal, 1. doi: https://doi.org/10.1109/jiot.2018.2815038
2. Kim, J., Yun, J., Choi, S.-C., Seed, D. N., Lu, G., Bauer, M. et. al. (2016). Standard-based IoT platforms interworking: implementation, experiences, and lessons learned. IEEE Communications Magazine, 54 (7), 48–54.doi: https://doi.org/10.1109/mcom.2016.7514163
3. Huang, P.-C., Rabaey, J. M. (2017). A Bio-Inspired Analog Gas Sensing Front End. IEEE Transactions on Circuits and Systems I: Regular Papers, 64 (9), 2611–2623. doi: https://doi.org/10.1109/tcsi.2017.2697945
4. Rahimi, A. A., Hu, H., Gupta, S. (2017). A compressive sensing information aware analog front end for IoT sensors using adaptive clocking techniques. 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). doi: https://doi.org/10.1109/mwscas.2017.8052926
5. Vistak, M. V., Dmytrakh, V. Y., Diskovskyu, I. S., Kobylinska, L. I., Mikityuk, Z. M., Petryshak, V. S. (2017). The optoelectronic sensor creatinine and urea. Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2017. doi: https://doi.org/10.1117/12.2280990
6. Barylo, G., Holyaka, R., Prudyus, I., Fabirovskyy, S. (2017). Parametric analysis of galvanostatic type impedance measuring front-end. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T doi: https://doi.org/10.1109/infocommst.2017.8246407
7. Mohammad, K., Thomson, D. J. (2017). Differential Ring Oscillator Based Capacitance Sensor for Microfluidic Applications. IEEE Transactions on Biomedical Circuits and Systems, 11 (2), 392–399 doi: https://doi.org/10.1109/tbcas.2016.2616346
8. Hotra, Z., Holyaka, R., Marusenkov, T., Potencki, J. (2010). Signal transducers of capacitive microelectronic sensors, 8, 129–132.
9. Scarlett, J. (2014). Using CDCs to Control Motion for Sample. Application Note AN-1301. Analog Devices, 6. Available at: http://www.analog.com/media/en/technical-documentation/application-notes/AN-1301.pdf
10. Holyaka, R., Kostiv, N. (2011). Energy-efficient signal converter of thermocouple, temperature sensors. Informatyka, Automatyka, Pomiary, 4, 26–28.
11. Hotra, O., Boyko, O., Zyska, T. (2014). Improvement of the operation rate of medical temperature measuring devices. 13th International Scientific Conference on Optical Sensors and Electronic Sensors. doi: https://doi.org/10.1117/12.2070167
12. Cassel, B., Packer, R., Shelton, C. T. Modulated Temperature DSC and the DSC 8500: A Step Up in Performance. PerkinElmer, Inc. Available at: http://labsense.fi/uploads/7/1/9/5/71957143/modulated_temperature_dsc_and_dsc_8500__a_step_up_in_performance_009122b_01_tch.pdf

13. Barreneche, C., Solé, A., Miró, L., Martorell, I., Fernández, A. I., Cabeza, L. F. (2012). New methodology developed for the differential scanning calorimetry analysis of polymeric matrixes incorporating phase change materials. Measurement Science and Technology, 23 (8), 085606. doi: https://doi.org/10.1088/0957-0233/23/8/085606
14. Elhissi, A. M. A., O'Neill, M., Ahmed, W., Taylor, K. M. G. (2011). High-sensitivity differential scanning calorimetry for measurement of steroid entrapment in nebulised liposomes generated from proliposomes. Micro & Nano Letters, 6 (8), 694. doi: https://doi.org/10.1049/mnl.2011.0086
15. Jiang, Y., Wang, D., Chen, J., Zhang, Q., Xuan, T. (2018). Electromagnetic-Thermal-Fluidic Analysis of Permanent Magnet Synchronous Machine by Bidirectional Method. IEEE Transactions on Magnetics, 54 (3), 1–5. doi: https://doi.org/10.1109/tmag.2017.2760928
16. Alberti, L., Bianchi, N. (2008). A Coupled Thermal–Electromagnetic Analysis for a Rapid and Accurate Prediction of IM Performance. IEEE Transactions on Industrial Electronics, 55 (10), 3575–3582. doi: https://doi.org/10.1109/tie.2008.2003197
17. Boyko, O., Holyaka, R., Hotra, Z. (2018). Functionally integrated sensors on magnetic and thermal methods combination basis. 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). doi: https://doi.org/10.1109/tcset.2018.8336296
18. Karpaty, D. (2013). Modeling Amplifiers as Analog Filters Increases SPICE Simulation Speed. Analog Dialogue, 47 (1), 18–22.
19. MICRO-CAP. Electronic Circuit Analysis Program. Spectrum Software (2014). Available at: http://www.spectrum-soft.com

DOI: 10.15587/1729-4061.2018.139689

METROLOGICAL TRACEABILITY OF IMPEDANCE PARAMETER MEASUREMENTS IN UKRAINE (p. 43-49)

Oleh Velychko
Scientific and Production Institute of Electromagnetic Measurements
State Enterprise "All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer", (SE "Ukrmetrteststandard"), Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-6564-4144

Sergii Shevkun
Department of state standards of electromagnetic quantity, time and frequency
State Enterprise "All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer", (SE "Ukrmetrteststandard"), Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-1923-6227

Tetyana Gordiyenko
Odessa State Academy of Technical Regulation and Quality
ORCID: http://orcid.org/0000-0003-0324-9672

Maryna Dobroliubova
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-3647-3320

The equivalence rates of the national standard of a unit of electrical capacitance for denominations of 10 pF and 100 pF at frequencies of 1 kHz and 1.592 kHz and expanded uncertainties obtained from the results of international comparisons of national measurement standards for electrical capacitance units were established and their comparative analysis was carried out. The equivalence of the national standard of the inductance unit for the nominal values of 10 mH and 100 mH at a frequency of 1 kHz and the expanded uncertainties obtained from the results of international additional comparisons of the national measurement standards of inductance units were established and their comparative analysis was carried out. The comparisons were conducted by Regional Metrology Organizations with the participation of the National Metrology Institute of Ukraine.

The analysis of the data processing methods applied in the comparison reports was carried out with the aim of adequately evaluating the results obtained by each of the comparison participants. The results of the National Metrology Institute of Ukraine became the basis for establishing the metrological traceability of measurements of impedance parameters in the country and the recognition of the results of these measurements in other countries.

Values of the expanded uncertainty of the measurements of the electrical capacitance in the range of values from 10 pF to 10 nF for high-precision calibration of the measures of electrical capacitance were calculated. Values of the expanded uncertainty of inductance measurements in the range from 1 μH to 10 H with high-precision calibration of inductance measures were calculated.

The best values of the expanded uncertainty of measurements of impedance parameters (electrical capacitance and inductance) in a wide range of values in Ukraine were established. The comparative analysis showed that the published data on the calibration and measurement capabilities of the national metrology institutes of Ukraine for measuring the electrical capacitance and inductance can be significantly improved in wide ranges of values.

Keywords: comparison of standards, metrological traceability, impedance, national metrological institute, regional metrological organization.

References

1. Measurement comparisons in the context of the CIPM MRA. CIPM MRA-D-05:2013. Available at: http://www.bipm.org/en/cipm-mra/cipm-mra-documents/
2. The BIPM key comparison database (KCDB). Available at: http://kcdb.bipm.org/
3. Text of the CIPM MRA. Available at: http://www.bipm.org/en/cipm-mra/cipm-mra-text/
4. International vocabulary of metrology. – Basic and general concepts and associated terms (VIM 3-rd edition). JCGM 200:2012. Available at: https://www.bipm.org/utils/common/documents/jcgm/JCGM_200_2012.pdf
5. Velichko, O. N. (2009). Traceability of measurement results at different levels of metrological work. Measurement Techniques, 52 (11), 1242–1248. doi: https://doi.org/10.1007/ s11018-010-9428-7
6. ILAC Policy on Traceability of Measurement Results. ILAC P10:1/2013. Available at:http://www.enao-eth.org/publication_documents/ILAC_P10_01_2013%20ILAC%20Policy%20on%20Traceability%20of%20Measurement%20Results.pdf
7. Uncertainty of measurement. – Part 3: Guide to the expression of uncertainty in measurement (GUM). JCGM 100:2008. Available at: https://www.bipm.org/en/about-us/
8. Calibration and Measurement Capabilities in the context of the CIPM MRA. CIPM MRA-D-04:2013. Available at: http://www.bipm.org/en/cipm-mra/cipm-mra-documents/

9. Velichko, O. N. (2010). Calibration and measurement capabilities of metrological institutes: features of preparation, examination, and publication. Measurement Techniques, 53 (6), 721–726. doi: https://doi.org/10.1007/s11018-010-9567-x
10. Velychko, O., Gordiyenko, T. (2010). The implementation of general international guides and standards on regional level in the field of metrology. Journal of Physics: Conference Series, 238, 012044. doi: https://doi.org/10.1088/1742-6596/238/1/012044
11. Cox, M. G. (2002). The evaluation of key comparison data. Metrologia, 39 (6), 589–595. doi: https://doi.org/10.1088/0026-1394/39/6/10
12. Cox, M. G. (2007). The evaluation of key comparison data: determining the largest consistent subset. Metrologia, 44 (3), 187–200. doi: https://doi.org/10.1088/0026-1394/44/3/005
13. Mana, G., Massa, E., Predescu, M. (2012). Model selection in the average of inconsistent data: an analysis of the measured Planck-constant values. Metrologia, 49 (4), 492–500. doi: https://doi.org/10.1088/0026-1394/49/4/492
14. Jeffery, A.-M. (2002). Final report on key comparison CCEM-K4 of 10 pF capacitance standards. Metrologia, 39 (1A), 01003–01003. doi: https://doi.org/10.1088/0026-1394/39/1a/3
15. Delahaye, F., Witt, T. J. (2002). Linking the results of key comparison CCEM-K4 with the 10 pF results of EUROMET.EM-K4. Metrologia, 39 (1A), 01005–01005. doi: https://doi.org/10.1088/0026-1394/39/1a/5
16. Johnson, L., Chua, W., Corney, A., Hsu, J., Sardjono, H., Lee, R. D. et. al. (2009). Final report on the APMP comparison of capacitance at 10 pF: APMP.EM-K4.1. Metrologia, 46 (1A), 01003–01003. doi: https://doi.org/10.1088/0026-1394/46/1a/01003
17. Johnson, L., Chua, W., Corney, A., Hsu, J., Sardjono, H., Lee, R. D. et. al. (2008). Final report on the APMP comparison of capacitance at 100 pF (APMP supplementary comparison APMP.EM-S7). Metrologia, 45 (1A), 01003–01003. doi: https://doi.org/10.1088/0026-1394/45/1a/01003
18. Velychko, O., Akhamadov, O. (2017). Final report on COOMET key comparison of capacitance at 10 pF (COOMET.EM-K4). Metrologia, 54 (1A), 01005–01005. doi: https://doi.org/10.1088/0026-1394/54/1a/01005
19. Velychko, O., Akhamadov, O. (2017). Final report on COOMET key comparison of capacitance at 100 pF (COOMET.EM-S4). Metrologia, 54 (1A), 01006–01006. doi: https://doi.org/10.1088/0026-1394/54/1a/01006
20. Velychko, O., Shevkun, S. (2015). Final report: COOMET supplementary comparison of capacitance at 10 pF and 100 pF (COOMET.EM-S13). Metrologia, 52 (1A), 01005–01005. doi: https://doi.org/10.1088/0026-1394/52/1a/01005
21. Eckardt, H. (2001). International Comparison of 10 mH Inductance Standards at 1 kHz. CCEM-K3. Final Report. CCEM WGKC/2001-15. PTB, 35.
22. Kölling, A. (2011). Final report on EUROMET comparison EUROMET.EM-K3: a 10 mH inductance standard at 1 kHz. Metrologia, 48 (1A), 01008–01008. doi: https://doi.org/10.1088/0026-1394/48/1a/01008
23. Callegaro, L. (2007). EUROMET.EM-S20: Intercomparison of a 100 mH inductance standard (Euromet Project 607). Metrologia, 44 (1A), 01002–01002. doi: https://doi.org/10.1088/0026-1394/44/1a/01002
24. Dierikx, E., Nestor, A., Melcher, J., Kölling, A., Callegaro, L. (2011). Final report on the supplementary comparison EURAMET.EM-S26: inductance measurements of 100 mH at 1 kHz (EURAMET project 816). Metrologia, 49 (1A), 01002–01002. doi: https://doi.org/10.1088/0026-1394/49/1a/01002
25. Moreno, J. A., Côté, M., Koffman, A., Castro, B. I., Vasconcellos, R. de B. e, Kyriazis, G. et. al. (2016). SIM.EM-K3 Key comparison of 10 mH inductance standards at 1 kHz. Metrologia, 53 (1A), 01002–01002. doi: https://doi.org/10.1088/0026-1394/53/1a/01002
26. Velychko, O., Shevkun, S. (2016). Final report on COOMET supplementary comparison of inductance at 10 mH and 100 mH at 1 kHz (COOMET.EM-S14). Metrologia, 53 (1A), 01009–01009. doi: https://doi.org/10.1088/0026-1394/53/1a/01009
27. Guidelines on COOMET key comparison evaluation. COOMET R/GM/14:2016. Available at: http://www.coomet.org/DB/isapi/cmt_docs/2016/5/2BMD1O.pdf
28. Guidelines on COOMET supplementary comparison evaluation. COOMET R/GM/19:2016. Available at: http://www.coomet.org/DB/isapi/cmt_docs/2016/5/21XQGO.pdf
29. EA guidelines on the expression of uncertainty in quantitative testing. EA-04/16G:2003. Available at: http://www.european-accreditation.org/publication/ea-4-16-g-rev00-december-2003-rev
30. Velychko, O., Shevkun, S. (2017). Support of metrological traceability of capacitance measurements in Ukraine. Eastern-European Journal of Enterprise Technologies, 3 (9 (87)), 4–10. doi: https://doi.org/10.15587/1729-4061.2017.101897
31. Evaluation of the Uncertainty of Measurement in Calibration. EA-04/02 M:2013. Available at: http://www.european-accreditation.org/publication/ea-4-02-m-rev01--september-2013
32. Velychko, O., Shevkun, S. (2017). A support of metrological traceability of inductance measurements in Ukraine. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 12–18. doi: https://doi.org/10.15587/1729-4061.2017.109750
33. DSTU ISO/IEC 17025:2006. Zahalni vymohy do kompetentnosti vyprobuvalnykh ta kalibruvalnykh laboratoriy (ISO/IEC 17025: 2005, IDT) (2007). Kyiv: Derzhspozhyvstandart Ukrainy, 26.

DOI: 10.15587/1729-4061.2018.139755

ENHANCEMENT OF PRODUCTIVITY OF RANDOM SEQUENCES GENERATION FOR INFORMATION PROTECTION SYSTEMS (p. 50-60)

Serhii Ivanchenko
Institute of Special Communication and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-1850-9596

Serhii Yevseiev
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-1647-6444

Vitalii Bezshtanko
Institute of Special Communication and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-7998-246X

Vasyl Bondarenko
State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-7578-3236

Oleksii Gavrylenko
National Aviation University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-9552-5832

Nadiia Kazakova
Odessa State Academy of Technical Regulation and Quality, Odessa, Ukraine
ORCID: http://orcid.org/0000-0003-3968-4094

Roman Korolev
Ivan Kozhedub Kharkiv University of Air Force, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-7948-5914

Serhii Mazor
Institute of Special Communication and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org//0000-0002-7086-6585

Vadym Romanenko
Institute of Special Communication and Information Protection National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-8668-177X

Oleksii Fraze-Frazenko
Odessa State Academy of Technical Regulation and Quality, Odessa, Ukraine
ORCID: http://orcid.org/0000-0002-2288-8253

The ways of enhancement of productivity of generation of random sequences, derived from physical sources for information protection systems were substantiated. This is necessary because today there is a rapid growth of technological capabilities and of rate indicators of implementation of various information services and applications, required by community. One of the main issues of the safe use of these services is to ensure information security, which requires the use of effective high-rate information protection systems and high-performance generation of random data sequences. In the course of conducting research with the aim of enhancing productivity, the features of conversion of actual noise processes, taking into consideration their non-stationarity and deviations from the probability distribution were analyzed. We proposed the ways to improve the methods of analog-to-digital conversion with the optimization of the scale dynamic range quantization and the pitch of discretization of a noise process over time. With a view to aligning statistical characteristics, the possibility of using the processing methods that enhance its statistical quality with economy of high-rate losses was explored. These are the method of sampling equally probable combinations (von Neumann – Elias –Ryabko – Matchikina) and the method of code processing (Santha – Vazirani) that provide an increased effectiveness due to code extension and involve conversion of the sequence: in the first method, with the use of equally probable combinations with rejection of unnecessary data; in the second method, without their rejection with the possibility of linear conversion. In order to optimize the conversion parameters at both stages of generation and to adapt these parameters to the peculiarities and changeability of characteristics of converted random processes, it was proposed to use feedbacks of converters' outputs with previous conversion elements.

The adjustment of the specified parameters can be made during the generation based on the results of statistical analysis of the outputs of conversion stages. The obtained results are quite important, since their implementation in modern information protection systems will enable guaranteeing information security and safe usage of applications of the modern information service and the introduction of new applications.

Keywords: random data, noise processes, information security, conversion, processing, statistical alignment.

References

1. Ivashchenko, A. V., Sypchenko, R. P. (1988). Osnovy modelirovaniya slozhnyh sistem na EVM. Leningrad: LVVIUS, 272.
2. Moldavyan, N. A. (1998). Problematika i metody kriptografii. Sankt-Peterburg: Izdatel'stvo SPbGU, 212.
3. Muramatsu, J., Miyake, S. (2017). Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices. Mathematics for Industry, 177–198.doi: https://doi.org/10.1007/978-981-10-5065-7_10
4. Wyner, A. D. (1975). The Wire-Tap Channel. Bell System Technical Journal, 54 (8), 1355–1387. doi: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
5. Korzhik, V. I., Yakovlev, V. A. (1981). Neasimptoticheskie ocenki effektivnosti kodovogo zashumleniya odnogo kanala. Mosocw: Problemy peredachi informacii, 11–18.
6. Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., Wustrow, E. (2014). Elliptic Curve Cryptography in Practice. Lecture Notes in Computer Science, 157–175. doi: https://doi.org/10.1007/978-3-662-45472-5_11
7. Zhou, H. (2013). Randomness and Noise in Information Systems. California Institute of Technology Pasadena, California, 436.
8. Erven, C., Ng, N., Gigov, N., Laflamme, R., Wehner, S., Weihs, G. (2014). An experimental implementation of oblivious transfer in the noisy storage model. Nature Communications, 5 (1). doi: https://doi.org/10.1038/ncomms4418
9. Wehner, S., Curty, M., Schaffner, C., Lo, H.-K. (2010). Implementation of two-party protocols in the noisy-storage model. Physical Review A, 81 (5). doi: https://doi.org/10.1103/physreva.81.052336
10. Damgård, I., Fehr, S., Morozov, K., Salvail, L. (2004). Unfair Noisy Channels and Oblivious Transfer. Lecture Notes in Computer Science, 355–373. doi: https://doi.org/10.1007/978-3-540-24638-1_20
11. Bobnev, M. P. (1971). Generirovanie sluchaynyh signalov. Moscow: Energiya, 240.
12. Torba, A. A., Bobkova, A. A., Gorbenko, Yu. I., Bobuh, V. A.; Gorbenko, I. D. (Ed.) (2012). Metody i sredstva generacii sluchaynyh bitovyh posledovatel'nostey. Kharkiv: Izd-vo «Fort», 232.
13. Colbeck, R., Renner, R. (2012). Free randomness can be amplified. Nature Physics, 8 (6), 450–453. doi: https://doi.org/10.1038/nphys2300
14. Gallego, R., Masanes, L., De La Torre, G., Dhara, C., Aolita, L., Acín, A. (2013). Full randomness from arbitrarily deterministic events. Nature Communications, 4 (1). doi: https://doi.org/10.1038/ncomms3654
15. Chung, K.-M., Shi, Y. Wu, X. Physical randomness extractors: generating random numbers with minimal assumptions. Available at: https://arxiv.org/pdf/1402.4797.pdf
16. Mironowicz, P., Gallego, R., Pawłowski, M. (2015). Robust amplification of Santha-Vazirani sources with three devices. Physical Review A, 91 (3). doi: https://doi.org/10.1103/physreva.91.032317
17. Brandao, F. G. S. L., Ramanathan, R., Grudka, A., Horodecki, K., Horodecki, M., Horodecki, P. et. al. Robust device-independent randomness amplification with few devices. Available at: https://arxiv.org/abs/1310.4544
18. Ugajin, K., Terashima, Y., Iwakawa, K., Uchida, A., Harayama, T., Yoshimura, K., Inubushi, M. (2017). Real-time fast physical random number generator with a photonic integrated circuit. Optics Express, 25 (6), 6511. doi: https://doi.org/10.1364/oe.25.006511
19. Gurubilli, P. R., Garg, D. (2010). Random Number Generation and its Better Technique. Computer Science and Engineering Department, Thapar University, Patiala.

20. Elsherbeny, M. N., Rahal, M. (2012). Pseudo – Random Number Generator Using Deterministic Chaotic System. International Journal of Scientific & Technology Research, 1 (9), 95–97.
21. Kozierski, P., Lis, M., Królikowski, A. (2014). Parallel uniform random number generator in FPGA. Poznan University of Technology, Academic Journals: Computer Application in Electrical Engineering, 12, 399–406.
22. Yang, J., Liu, J., Su, Q., Li, Z., Fan, F., Xu, B., Guo, H. (2016). 54 Gbps real time quantum random number generator with simple implementation. Optics Express, 24 (24), 27475. doi: https://doi.org/10.1364/oe.24.027475
23. Wang, A., Wang, L., Li, P., Wang, Y. (2017). Minimal-post-processing 320-Gbps true random bit generation using physical white chaos. Optics Express, 25 (4), 3153. doi: https://doi.org/10.1364/oe.25.003153
24. Shinohara, S., Arai, K., Davis, P., Sunada, S., Harayama, T. (2017). Chaotic laser based physical random bit streaming system with a computer application interface. Optics Express, 25 (6), 6461. doi: https://doi.org/10.1364/oe.25.006461
25. Argyris, A., Pikasis, E., Syvridis, D. (2016). Gb/s One-Time-Pad Data Encryption With Synchronized Chaos-Based True Random Bit Generators. Journal of Lightwave Technology, 34 (22), 5325–5331. doi: https://doi.org/10.1109/jlt.2016.2615870
26. Baskakov, S. I. (1988). Radiotekhnicheskie cepi i signaly. Moscow: Vysshaya shkola,. 448.
27. von Neuman, J. (1951). Various Techniques Used in Connection with Random Digits. Monte Carlo Method, Applied Mathematics, 36–38.
28. Elias, P. (1972). The Efficient Construction of an Unbiased Random Sequence. The Annals of Mathematical Statistics, 43 (3), 865–870. doi: https://doi.org/10.1214/aoms/1177692552
29. Ryabko, B. Ya., Machikina, E. P. (1998). Effektivnoe preobrazovanie sluchaynyh posledovatel'nostey v ravnoveroyatnye i nezavisimye. Problemy peredachi informacii, 35 (2), 23–28.
30. Santha, M., Vazirani, U. V. (1986). Generating quasi-random sequences from semi-random sources. Journal of Computer and System Sciences, 33 (1), 75–87. doi: https://doi.org/10.1109/sfcs.1984.715945
31. Ivanchenko, S. O., Parshukov, S. S. (2007). Obgruntuvannia metodu heneratsiyi vypadkovykh poslidovnostei z kodovoiu obrobkoiu dlia kryptohrafichnykh system zakhystu informatsiyi. Spetsialni telekomunikatsiyni systemy ta zakhyst informatsiyi: Tematychnyi vypusk "Matematychni metody prykladnoi kryptohrafiyi", 1 (13), 152–155.
32. Ivanchenko, S. O., Zaitsev, O. D. (2009). Metod vysokoproduktyvnoho peretvorennia shumovykh syhnaliv u vypadkovu poslidovnist. Spetsialni telekomunikatsiyni systemy ta zakhyst informatsiyi, 2 (16), 140–144.
33. Gallager, R. G. (1974). Teoriya informacii i nadezhnaya svyaz'. Moscow: Sovetskoe radio, 720.
34. Mak-Vil'yams, F. Dzh., Sloen, N. Dzh. A. (1979). Teoriya kodov, ispravlyayushchih oshibki. Moscow: Svyaz', 744.
35. Murry, H. F. (1970). A General Approach for Generating Natural Random Variables. IEEE Transactions on Computers, C-19 (12), 1210–1213. doi: https://doi.org/10.1109/t-c.1970.222860
36. Maurer, U. (1990). Provable Security in Cryptography. Diss. ETH No 9260, 86–93.
37. Bassham, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B. et. al. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology, 131. doi: https://doi.org/10.6028/nist.sp.800-22r1a

DOI: 10.15587/1729-4061.2018.139964

DEVELOPMENT OF A METHOD FOR THE SYNTHESIS OF A THREE-DIMENSIONAL MODEL OF POWER TRANSMISSION LINES FOR VISUALIZATION SYSTEMS OF TRAINING COMPLEXES (p. 61-70)

Petro Kachanov
National Technical University
«Kharkiv Polytechnic Institute», Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-0781-0853

Zuev Andrey
National Technical University
«Kharkiv Polytechnic Institute», Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-8206-4304

Representation of the wire line shape depending on the wire tension and temperature was considered. A method was developed for constructing a geometric three-dimensional line model and synthesis of its images used in the visualization system of the simulator complex. Solution of the problem of synthesis and visualization of extended objects is hard and computationally complex because of the high detail of such objects and strong unevenness of their projection. The method makes it possible to obtain a set of triangles describing the line in real time using known sagging parameters and distance between the suspension points. To do this, one does not need the line scanning in contrast to the used methods of lidar scanning or photogrammetry. Sagging of the line wires can vary in real time depending on external conditions. The resulting set does not contain explicitly visible kinks or artifacts for any position of the observer within the simulated section of the line.

The method minimizes aliasing artifacts on the wire line elements remote from the observer, automatic texturing and calculation of normals to the line surface which enables correct calculation of illumination for any line fragment when synthesizing images in the visualization system. The speed of the method was evaluated, its implementation within the visualization system has shown a functioning speed enough for real-time operation and examples of synthesized line images were given.

The required computational resources for synthesis of the line image were minimized by using a flexible system of detail levels which has enabled use of cheaper hardware for constructing visualization systems and resulted in reduction of the price of the simulator complex in general.

Keywords: UAV, wire lines, simulation complexes, three-dimensional models, rasterization, image synthesis, visualization system, graphics accelerator, aliasing.

References

1. Skarbek, L., Zak, A., Ambroziak, D. (2014). Damage detection strategies in structural health monitoring of overhead power transmission system. 7th European Workshop on Structural Health Monitoring. La Cité, Nantes, 663–670.
2. Li, L. (2015). The UAV intelligent inspection of transmission lines. Proceedings of the 2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics. doi: https://doi.org/10.2991/ameii-15.2015.285
3. Adabo, G. J. (2014). Long Range Unmanned Aircraft System for Power Line Inspection of Brazilian Electrical System. Journal of Power and Energy Engineering, 8 (2), 394–398.
4. Arbuzov, R. S. (2009). Sovremennye metody diagnostiki vozdushnyh liniy elektroperedachi. Novosibirsk: Nauka, 136.

5. Kachanov, P. A., Zuev, A. A., Yacenko, K. N. (2015). Space perception analysis in the panini projection and its using in computer graphics. Eastern-European Journal of Enterprise Technologies, 4 (2 (76)), 36–43. doi: https://doi.org/10.15587/1729-4061.2015.47678
6. Watts, A. C., Ambrosia, V. G., Hinkley, E. A. (2012). Unmanned Aircraft Systems in Remote Sensing and Scientific Research: Classification and Considerations of Use. Remote Sensing, 4 (6), 1671–1692. doi: https://doi.org/10.3390/rs4061671
7. Zhang, C., Elaksher, A. (2011). An Unmanned Aerial Vehicle-Based Imaging System for 3D Measurement of Unpaved Road Surface Distresses1. Computer-Aided Civil and Infrastructure Engineering, 27 (2), 118–129. doi: https://doi.org/10.1111/j.1467-8667.2011.00727.x
8. Hämmerle, M., Lukač, N., Chen, K.-C., Koma, Z., Wang, C.-K., Anders, K., Höfle, B. (2017). Simulating various terrestrial and UAV LIDAR scanning configurations for understory forest structure modelling. ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences, IV-2/W4, 59–65. doi: https://doi.org/10.5194/isprs-annals-iv-2-w4-59-2017
9. Seidel, D., Ehbrecht, M., Puettmann, K. (2016). Assessing different components of three-dimensional forest structure with single-scan terrestrial laser scanning: A case study. Forest Ecology and Management, 381, 196–208. doi: https://doi.org/10.1016/j.foreco.2016.09.036
10. Remondino, F., Barazzetti, L., Nex, F., Scaioni, M., Sarazzi, D. (2012). UAV Photogrammetry for Mapping and 3D Modeling – Current Status and Future Perspectives. ISPRS – International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XXXVIII-1/C22, 25–31. doi: https://doi.org/10.5194/isprsarchives-xxxviii-1-c22-25-2011
11. Martin, R., Rojas, I., Franke, K., Hedengren, J. (2015). Evolutionary View Planning for Optimized UAV Terrain Modeling in a Simulated Environment. Remote Sensing, 8 (1), 26. doi: https://doi.org/10.3390/rs8010026
12. Gatziolis, D., Lienard, J. F., Vogs, A., Strigul, N. S. (2015). 3D Tree Dimensionality Assessment Using Photogrammetry and Small Unmanned Aerial Vehicles. PLOS ONE, 10 (9), e0137765. doi: https://doi.org/10.1371/journal.pone.0137765
13. Brumana, R., Oreni, D., Alba, M., Barazzetti, L., Cuca, B., Scaioni, M. (2012). Panoramic UAV Views for Landscape Heritage Analysis Integrated with Historical Maps Atlases. Geoinformatics FCE CTU, 9, 39–50. doi: https://doi.org/10.14311/gi.9.4
14. Liang, Y., Qu, Y., Cui, T. (2017). A three-dimensional simulation and visualization system for UAV photogrammetry. ISPRS – International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLII-2/W6, 217–222. doi: https://doi.org/10.5194/isprs-archives-xlii-2-w6-217-2017
15. Kryukov, K. P. (1979). Konstrukcii i mekhanicheskiy raschet liniy elektroperedachi. Leningrad: Energiya, 312.
16. Design of Latticed Steel Transmission Structures (1991). American Society of Civil Engineers. ANSI/ASCE, A.N.S.I. New York: A.S.C.E., 64.
17. Hongnan, L., Haifeng, B. (2006). High-voltage transmission tower-line system subjected to disaster loads. Progress in Natural Science, 16 (9), 899–911. doi: https://doi.org/10.1080/10020070612330087
18. Ageev, D. M., Bostynec, I. P., Didyuk, A. Ya. (2010). Noviy sposob mekhanicheskogo rascheta provodov i trosov vozdushnyh liniy elektroperedachi. Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta.
19. Boshnyakovich, A. D. (1962). Mekhanicheskiy raschet provodov i trosov liniy elektroperedachi. Leningrad: Gosenergoizdat, 255.
20. Sotnikova, V. N., Solovey, P. I., Tanasoglo, A. V., Perevaryuha, A. N. (2015). Issledovaniya provesa provodov LEP, vyzvannogo solnechnym nagrevom. Visnyk Donbaskoi natsionalnoi akademiyi budivnytstva i arkhitektury, 3, 108–111.
21. Kachanov, P. A. (2012). Povyshenie tochnosti kodirovaniya normaley dlya sistem vizualizacii, ispol'zuyushchih metod otlozhennogo rascheta osveshcheniya. Informatsiyno-keruiuchi systemy na zaliznychnomu transporti, 6, 26–29.