ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2022.255203

DEVISING A METHOD FOR SEGMENTING COMPLEX STRUCTURED IMAGES ACQUIRED FROM SPACE OBSERVATION SYSTEMS BASED ON THE PARTICLE SWARM ALGORITHM (p. 6–13)

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

Oleksandr Makoveichuk
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-4425-016X

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

Oleksandr Oleksenko
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-6853-9630

Yuriy Khazhanets
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-8926-2474

Yuriy Solomonenko
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-6503-7475

Iryna Yuzova
Civil Aviation Institute, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-0013-5808

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

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

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

This paper considers the improved method for segmenting complex structured images acquired from space observation systems based on the particle swarm algorithm. Unlike known ones, the method for segmenting complex structured images based on the particle swarm algorithm involves the following:

– highlighting brightness channels in the Red-Green-Blue color space;

– using a particle swarm method in the image in each channel of brightness of the RGB color space;

– image segmentation is reduced to calculating the objective function, moving speed, and a new location for each swarm particle in the image in each RGB color space brightness channel.

Experimental studies have been conducted on the segmentation of a complex structured image by a method based on the particle swarm algorithm. It was established that the improved segmentation method based on the particle swarm algorithm makes it possible to segment complex structured images acquired from space surveillance systems.

A comparison of the quality of segmenting a complex structured image was carried out. The comparative visual analysis of well-known and improved segmentation methods indicates the following:

– the improved segmentation method based on the particle swarm algorithm highlights more objects of interest (objects of military equipment);

– the well-known k-means method assigns some objects of interest (especially those partially covered with snow) to the snow cover (marked in blue);

– the improved segmentation method also associates some objects of interest that are almost completely covered with snow with the snow cover (marked in blue).

It has been established that the improved segmentation method based on the particle swarm algorithm reduces segmentation errors of the first kind by an average of 12 % and reduces segmentation errors of the second kind by an average of 8 %.

Keywords: segmentation, complex structured image, space surveillance system, particle swarm, errors of the first and second kind.

References

1. Gaur, P. (2019). Satellite Image Bathymetry and ROV Data Processing for Estimating Shallow Water Depth in Andaman region, India. 81st EAGE Conference and Exhibition 2019. doi: https://doi.org/10.3997/2214-4609.201901067
2. Military Imaging and Surveillance Technology (MIST) (Archived). Available at: https://www.darpa.mil/program/military-imaging-and-surveillance-technolog
3. Kumar, J. M., Nanda, R., Rath, R. K., Rao, G. T. (2020). Image Segmentation using K-means Clustering. International Journal of Advanced Science and Technology, 29 (6s), 3700–3704. Available at: http://sersc.org/journals/index.php/IJAST/article/view/23282
4. Zheng, X., Lei, Q., Yao, R., Gong, Y., Yin, Q. (2018). Image segmentation based on adaptive K-means algorithm. EURASIP Journal on Image and Video Processing, 2018 (1). doi: https://doi.org/10.1186/s13640-018-0309-3
5. Acharjya, P. P., Bera, M. B. (2021). Detection of edges in digital images using edge detection operators. Computer Science & Engineering An International Journal, 9 (1), 107–113. Available at: https://www.researchgate.net/publication/356379177_Detection_of_edges_in_digital_images_using_edge_detection_operators
6. Srujana, P., Priyanka, J., Patnaikuni, V. Y. S. S. S., Vejendla, N. (2021). Edge Detection with different Parameters in Digital Image Processing using GUI. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). doi: https://doi.org/10.1109/iccmc51019.2021.9418327
7. Otsu, N. (1979). A Threshold Selection Method from Gray-Level Histograms. IEEE Transactions on Systems, Man, and Cybernetics, 9 (1), 62–66. doi: https://doi.org/10.1109/tsmc.1979.4310076
8. Chai, R. (2021). Otsu's Image Segmentation Algorithm with Memory-Based Fruit Fly Optimization Algorithm. Complexity, 2021, 1–11. doi: https://doi.org/10.1155/2021/5564690
9. Xing, J., Yang, P., Qingge, L. (2020). Robust 2D Otsu's Algorithm for Uneven Illumination Image Segmentation. Computational Intelligence and Neuroscience, 2020, 1–14. doi: https://doi.org/10.1155/2020/5047976
10. Akbari Sekehravani, E., Babulak, E., Masoodi, M. (2020). Implementing canny edge detection algorithm for noisy image.

Bulletin of Electrical Engineering and Informatics, 9 (4), 1404–1410. doi: https://doi.org/10.11591/eei.v9i4.1837
11. Minaee, S., Boykov, Y. Y., Porikli, F., Plaza, A. J., Kehtarnavaz, N., Terzopoulos, D. (2021). Image Segmentation Using Deep Learning: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1–1. doi: https://doi.org/10.1109/tpami.2021.3059968
12. Malhotra, P., Gupta, S., Koundal, D., Zaguia, A., Enbeyle, W. (2022). Deep Neural Networks for Medical Image Segmentation. Journal of Healthcare Engineering, 2022, 1–15. doi: https://doi.org/10.1155/2022/9580991
13. Hoeser, T., Bachofer, F., Kuenzer, C. (2020). Object Detection and Image Segmentation with Deep Learning on Earth Observation Data: A Review—Part II: Applications. Remote Sensing, 12 (18), 3053. doi: https://doi.org/10.3390/rs12183053
14. Farshi, T. R., Drake, J. H., Özcan, E. (2020). A multimodal particle swarm optimization-based approach for image segmentation. Expert Systems with Applications, 149, 113233. doi: https://doi.org/10.1016/j.eswa.2020.113233
15. Lokhande, N. M., Pujeri, R. V. (2018). Novel Image Segmentation Using Particle Swarm Optimization. Proceedings of the 2018 8th International Conference on Biomedical Engineering and Technology - ICBET '18. doi: https://doi.org/10.1145/3208955.3208962
16. Ruban, I., Khudov, H., Makoveichuk, O., Chomik, M., Khudov, V., Khizhnyak, I. et. al. (2019). Construction of methods for determining the contours of objects on tonal aerospace images based on the ant algorithms. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 25–34. doi: https://doi.org/10.15587/1729-4061.2019.177817
17. Chaudhari, B., Shetiye, P., Gulve, A. (2021). Image Segmentation using Hybrid Ant Colony Optimization: A Review. 2021 Sixth International Conference on Image Information Processing (ICIIP). doi: https://doi.org/10.1109/iciip53038.2021.9702695
18. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V. et. al. (2019). Segmentation of optical-electronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. Eastern-European Journal of Enterprise Technologies, 2 (9 (98)), 37–45. doi: https://doi.org/10.15587/1729-4061.2019.161860
19. Ruban, I., Khudov, V., Makoveichuk, O., Khudov, H., Khizhnyak, I. (2018). A Swarm Method for Segmentation of Images Obtained from On-Board Optoelectronic Surveillance Systems. 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2018.8632045
20. Satellite Imagery. Available at: https://www.maxar.com/products/satellite-imagery
21. Khudov, H., Makoveichuk, O., Misiuk, D., Pievtsov, H., Khizhnyak, I., Solomonenko, Y. et. al. (2022). Devising a method for processing the image of a vehicle's license plate when shooting with a smartphone camera. Eastern-European Journal of Enterprise Technologies, 1 (2 (115)), 6–21. doi: https://doi.org/10.15587/1729-4061.2022.252310
22. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Lukova-Chuiko, N., Pevtsov, H. et. al. (2019). Method for determining elements of urban infrastructure objects based on the results from air monitoring. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 52–61. doi: https://doi.org/10.15587/1729-4061.2019.174576

DOI: 10.15587/1729-4061.2022.255789

IMPROVEMENT OF NOISY IMAGES FILTERED BY BILATERAL PROCESS USING A MULTI-SCALE CONTEXT AGGREGATION NETWORK (p. 14–20)

Zinah R. Hussein
University of Baghdad, Baghdad, Iraq
ORCID: https://orcid.org/0000-0003-3678-5084

Deep learning has recently received a lot of attention as a feasible solution to a variety of artificial intelligence difficulties. Convolutional neural networks (CNNs) outperform other deep learning architectures in the application of object identification and recognition when compared to other machine learning methods. Speech recognition, pattern analysis, and image identification, all benefit from deep neural networks. When performing image operations on noisy images, such as fog removal or low light enhancement, image processing methods such as filtering or image enhancement are required. The study shows the effect of using Multi-scale deep learning Context Aggregation Network CAN on Bilateral Filtering Approximation (BFA) for de-noising noisy CCTV images. Data-store is used tomanage our dataset, which is an object or collection of data that are huge to enter in memory, it allows to read, manage, and process data located in multiple files as a single entity. The CAN architecture provides integral deep learning layers such as input, convolution, back normalization, and Leaky ReLu layers to construct multi-scale. It is also possible to add custom layers like adaptor normalization (μ) and adaptive normalization (Lambda) to the network. The performance of the developed CAN approximation operator on the bilateral filtering noisy image is proven when improving both the noisy reference image and a CCTV foggy image. The three image evaluation metrics (SSIM, NIQE, and PSNR) evaluate the developed CAN approximation visually and quantitatively when comparing the created de-noised image over the reference image.Compared with the input noisy image, these evaluation metrics for the developed CAN de-noised image were (0.92673/0.76253, 6.18105/12.1865, and 26.786/20.3254) respectively.

Keywords: convolutional neural network, residual learning, multi-scale context aggregation, CCTV images.

References

1. Kwon, H. (2021). MedicalGuard: U-Net Model Robust against Adversarially Perturbed Images. Security and Communication Networks. doi: https://doi.org/10.1155/2021/5595026
2. Zhu, G., Fu, J., Dong, J. (2020). Low Dose Mammography via Deep Learning. Journal of Physics: Conference Series. doi: https://doi.org/10.1088/1742-6596/1626/1/012110
3. Liu, H., Wu, J., Lu, W., Onofrey, J. A., Liu, Y.-H., Liu, C. (2020). Noise reduction with cross-tracer and cross-protocol deep transfer learning for low-dose PET. Physics in Medicine & Biology, 65 (18). doi: https://doi.org/10.1088/1361-6560/abae08
4. Chen, Q., Xu, J., Koltun, V. (2017). Fast Image Processing with Fully-Convolutional Networks. 2017 IEEE International Conference on Computer Vision (ICCV). doi: https://doi.org/10.1109/ICCV.2017.273
5. Sharma, S., Tang, B., Ball, J. E., Carruth, D. W., Dabbiru, L. (2020). Recursive multi-scale image deraining with sub-pixel convolution based feature fusion and context aggregation. IEEE Access. doi: https://doi.org/10.1109/ACCESS.2020.3024542
6. Kim, J., Kim, J., Jang G.-J., Lee, M. (2017). Fast learning method for convolutional neural networks using extreme learning machine and its application to lane detection. Neural Networks, 87. doi: https://doi.org/10.1016/j.neunet.2016.12.002
7. Missert, A. D., Yu, L., Leng, S., Fletcher, J. G., McCollough, C. H. (2020). Synthesizing images from multiple kernels using a deep convolutional neural network. Med Phys, 47 (2). doi: https://doi.org/10.1002/mp.13918
8. Klyuzhin, I. S., Cheng, J.-C., Bevington, C., Sossi, V. (2020). Use of a Tracer-Specific Deep Artificial Neural Net to Denoise Dynamic PET Images. IEEE Transactions on Medical Imaging, 39 (2). doi: https://doi.org/10.1109/TMI.2019.2927199
9. Zhang, J., Zhao, Y., Wang, J., Chen, B. (2020). FedMEC: Improving Efficiency of Differentially Private Federated Learning via Mobile Edge Computing. Mobile Networks and Applications, 25, 2421–2433. doi: https://doi.org/10.1007/s11036-020-01586-4

10. Mehranian, A., Wollenweber, S. D., Walker, M. D., Bradley, K. M., Fielding, P. A., Su, K.-H. et. al. (2022). Image enhancement of whole-body oncology [18F]-FDG PET scans using deep neural networks to reduce noise. European Journal of Nuclear Medicine and Molecular Imaging, 49, 539–549. doi: https://doi.org/10.1007/s00259-021-05478-x
11. Lim, H., Chun, I. Y., Dewaraja, Y. K., Fessler, J. A. (2020). Improved Low-Count Quantitative PET Reconstruction With an Iterative Neural Network. IEEE Transactions on Medical Imaging, 39 (11,) 3512–3522. doi: https://doi.org/10.1109/TMI.2020.2998480
12. Deeba, F., Zhou, Y., Dharejo, F. A., Du, Y., Wang, X., Kun, S. (2021). Multi-scale Single Image Super-Resolution with Remote-Sensing Application Using Transferred Wide Residual Network. Wireless Personal Communications, 120, 323–342. doi: https://doi.org/10.1007/s11277-021-08460-w
13. Kromrey, M.-L., Tamada, D., Johno, H., Funayama, S., Nagata, N., Ichikawa, S. et. al. (2020). Reduction of respiratory motion artifacts in gadoxetate-enhanced MR with a deep learning–based filter using convolutional neural network. European Radiology, 30, 5923–5932. doi: https://doi.org/10.1007/s00330-020-07006-1
14. Grabowski, D., Czyżewski, A. (2020). System for monitoring road slippery based on CCTV cameras and convolutional neural networks. Journal of Intelligent Information Systems, 55, 521–534. doi: https://doi.org/10.1007/S10844-020-00618-5

DOI: 10.15587/1729-4061.2022.253976

OPTIMIZATION OF AN INFORMATION SYSTEM MODULE FOR SOLVING A DIRECT GRAVIMETRY PROBLEM USING A GENETIC ALGORITHM (p. 21–34)

Assem Nazirova
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Republic of Kazakhstan
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-3299-5108

Maksat Kalimoldayev
National Academy of Sciences of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-0025-8880

Farida Abdoldina
Almaty Management University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1816-6343

Yurii Dubovenko
National Academy of Sciences of Ukraine, Kiyv, Ukraine
ORCID: https://orcid.org/0000-0002-8128-5989

Optimal approaches to solving many problems are required in many areas. One of these areas is the determination of the occurrence of gravity anomalies in oil and gas fields. In this paper is proposed a new approach for determining the source of gravity anomalies in an oil and gas fields by estimating the gravity parameters associated with simple-shaped bodies such as a homogeneous sphere, a horizontal prism, and a vertical step. The approach was implemented in the computational module of the GeoM information system for optimizing the solution of a series of direct gravimetry problems using a genetic algorithm (GA). Approach is based on solving the direct gravimetry problem to minimize the discrepancy of gravity variations by the genetic algorithm. The method allows to select values simultaneously for several parameters of the studied environment. The task is realized through successive approximations based on a given initial approximation of the medium.

The paper indicates the initial calculation parameters and criteria for finding optimal solutions for models of the geological environment. The calculations were carried out for such models of the environment as a homogeneous sphere, a horizontal prism and a vertical ledge. For calculations, the results of gravimetric monitoring at one of the Kazakh oil and gas fields were used. The paper demonstrates the operation of the algorithm and presents the results of modeling for three available field profiles. The obtained results of the system showed an acceptable accuracy of the algorithm up to 10^{-11}. The genetic algorithm made it possible to significantly increase the reliability of the model and reduce the working time for analyzing the measured gravitational field.

Keywords: direct gravimetry problem, genetic algorithm, gravimetric monitoring, global optimization methods.

References

1. Obornev, E. A., Obornev, I. E., Rodionov, E. A., Shimelevich, M. I. (2020). Application of Neural Networks in Nonlinear Inverse Problems of Geophysics. Computational Mathematics and Mathematical Physics, 60 (6), 1025–1036. doi: https://doi.org/10.1134/s096554252006007x
2. Abdelrahman, E. M., Sharafeldin, S. M. (1995). A least-squares minimization approach to depth determination from numerical horizontal gravity gradients. GEOPHYSICS, 60 (4), 1259–1260. doi: https://doi.org/10.1190/1.1443857
3. Shlyahovskii, V. A. (1984). Izucheniye neftegazoperspektivnyh struktur s pomowiyu dialogovoi sistemy interpretacii gravitacionnyh anomalii. Kyiv.
4. Holland, J. H. (1975). Adaptation in natural and artificial systems: An introductory analysis with applications to biology, control, and artificial intelligence. The University of Michigan Press, 96.
5. Goldberg, D. E. (1989). Genetic algorithms in search, optimization, and machine learning. Reading, MA: Addison-Wesley, 412.
6. Abdoldina, F. N., Nazirova, A. B., Dubovenko, Y. I., Umirova, G. K. (2021). Solution of the gravity exploration direct problem by the simulated annealing method for data interpretation of gravity monitoring of the subsoil conditions. Series of Geology and Technical Sciences, 445 (1), 13–21. doi: https://doi.org/10.32014/2021.2518-170x.2
7. Tabassum, M. (2014). A genetic algorithm analysis towards optimization solutions. International Journal of Digital Information and Wireless Communications, 4 (1), 124–142. doi: https://doi.org/10.17781/p001091
8. Hamdia, K. M., Zhuang, X., Rabczuk, T. (2020). An efficient optimization approach for designing machine learning models based on genetic algorithm. Neural Computing and Applications, 33 (6), 1923–1933. doi: https://doi.org/10.1007/s00521-020-05035-x
9. Abu Taleb, A. (2021). Sink mobility model for wireless sensor networks using genetic algorithm. Journal of Theoretical and Applied Information Technology, 99, 540–551. Available at: http://www.jatit.org/volumes/Vol99No2/24Vol99No2.pdf
10. Girgis, M. R., Mahmoud, T. M., Abdullatif, B. A., Rabie, A. M. (2014). Solving the Wireless Mesh Network Design Problem using Genetic Algorithm and Simulated Annealing Optimization Methods. International Journal of Computer Applications, 96 (11), 1–10. doi: https://doi.org/10.5120/16835-6680
11. Butko, T., Prokhorov, V., Chekhunov, D. (2017). Devising a method for the automated calculation of train formation plan by employing genetic algorithms. Eastern-European Journal of Enterprise Technologies, 1 (3 (85)), 55–61. doi: https://doi.org/10.15587/1729-4061.2017.93276
12. Baghlani, A., Sattari, M., Makiabadi, M. H. (2014). Application of genetic programming in shape optimization of concrete gravity dams by metaheuristics. Cogent Engineering, 1 (1), 982348. doi: https://doi.org/10.1080/23311916.2014.982348
13. Jabri, A., El Barkany, A., El Khalfi, A. (2017). Multipass Turning Operation Process Optimization Using Hybrid Genetic Simulated Annealing Algorithm. Modelling and Simulation in Engineering, 2017, 1–10. doi: https://doi.org/10.1155/2017/1940635
14. Asfahani, J., Tlas, M. (2011). Fair Function Minimization for Direct Interpretation of Residual Gravity Anomaly Profiles Due to Spheres and Cylinders. Pure and Applied Geophysics, 169 (1-2), 157–165. doi: https://doi.org/10.1007/s00024-011-0319-x

15. Blokh, Y. I. (2009). Interpetaciya gravitacionnyh i magnitnykh anomalii. Moscow, 231. Available at: http://sigma3d.com/pdf/books/blokh-interp.pdf
16. Nazirova, A., Abdoldina, F., Dubovenko, Y., Umirova, G. (2019). Development of GIS subsystems for gravity monitoring data analysis of the subsoil conditions for oil and gas fields. 18th International Conference on Geoinformatics - Theoretical and Applied Aspects. doi: https://doi.org/10.3997/2214-4609.201902099
17. Nazirova, A., Abdoldina, F., Aymahanov, M., Umirova, G., Muhamedyev, R. (2016). An Automated System for Gravimetric Monitoring of Oil and Gas Deposits. Digital Transformation and Global Society, 585–595. doi: https://doi.org/10.1007/978-3-319-49700-6_58
18. Hassanat, A., Prasath, V., Abbadi, M., Abu-Qdari, S., Faris, H. (2018). An Improved Genetic Algorithm with a New Initialization Mechanism Based on Regression Techniques. Information, 9 (7), 167. doi: https://doi.org/10.3390/info9070167
19. Yang, M.-D., Yang, Y.-F., Su, T.-C., Huang, K.-S. (2014). An Efficient Fitness Function in Genetic Algorithm Classifier for Landuse Recognition on Satellite Images. The Scientific World Journal, 2014, 1–12. doi: https://doi.org/10.1155/2014/264512
20. D'Angelo, G., Palmieri, F. (2021). GGA: A modified genetic algorithm with gradient-based local search for solving constrained optimization problems. Information Sciences, 547, 136–162. doi: https://doi.org/10.1016/j.ins.2020.08.040
21. Verma, A., Mittal, N. (2014). Congestion Controlled WSN using Genetic Algorithm with different Source and Sink Mobility Scenarios. International Journal of Computer Applications, 101 (13), 8–15. doi: https://doi.org/10.5120/17746-8819
22. Lambora, A., Gupta, K., Chopra, K. (2019). Genetic Algorithm- A Literature Review. 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). doi: https://doi.org/10.1109/comitcon.2019.8862255
23. Abdoldina, F. N., Nazirova, A. B., Dubovenko, Y. I., Umirova, G. K., Jamalov, D. K., Sliamhan, K. D. (2020). Geoinformacionnaya Sistema "GeoM" dlya obrabotki dannyh gravimetricheskogo monitoringa. Svidetel'stvo o vnesenii v gosudarstvennyi reestrprav na ob'ekty, ohranyaemye avtorskim pravom No.13336 ot "19" noyabrya 2020 g.

DOI: 10.15587/1729-4061.2022.255520

CHARACTERISTIC ANALYSIS OF QUEUE THEORY IN WIFI APPLICATIONS USING OPNET 14.5 MODELER (p. 35–43)

Ali Hamzah Najim
Imam Al-Kadhum College (IKC), Al-Diwaniyah, Iraq
ORCID: https://orcid.org/0000-0003-2898-9634

Hassnen Shakir Mansour
Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq
ORCID: https://orcid.org/0000-0003-4406-0390

Ali Hashim Abbas
Imam Ja'afar Al-Sadiq University, Al-Muthanna, Iraq
ORCID: https://orcid.org/0000-0002-7947-7025

Wireless Fidelity (Wi-Fi) broadband network technology has created great influence in the evolution of broadband wireless networks that are anticipated to progress regarding broadband speed and coverage. Several Wi-Fi hotspots are available everywhere, making it a medium of internet access that is easier to use compared to a local area network (LAN). However, the internet being the best effort network doesn't provide the required Quality of Service (QoS) and there is no differentiation of service traffic. The chief aim of the current paper is to study the operation of the three organizing mechanisms: First-In, First-Out (FIFO) method – the standard method of network implementation to process the packets one by one as it arrives, Priority Queuing (PQ) and Weighted Fair Queuing (WFQ) whereas PQ and WFQ classify the types of traffic based on service priority. In addition, WFQ assigns fair weight to each service on multiple traffic classes like video conferencing, Voice over Internet Protocol (VoIP), and File Transfer Protocol (FTP), using Telkom ST3's Wi-Fi network. This study applies four different scenarios: the first scenario applies the methods without any queuing discipline; the second scenario implements the methods with FIFO; the third scenario carries out the methods with PQ and the last scenario applies the methods with WFQ. The studies have shown that "end-to-end packet delay and packet delay variation for VoIP in the WFQ scenario" is good when compared to other queuing mechanisms with values of 171.717 ms and 0.977 ms, respectively. In the case of videotape conferencing also, the performance is better in the case of WFQ with values of 32.495 ms and 7.207 ms, correspondingly, since the WFQ has a "bandwidth allocation" tailored to the requirements.

Keywords: Wi-Fi, QoS, FIFO, PQ, WFQ, VoIP, FTP, Telkom ST3's, end-to-end packet delay.

References

1. Nwabueze, C. A., Akaneme, S. A. (2009). Wireless Fidelity (Wi-Fi) Broadband Network Technology: An Overview with Other Broadband Wireless Networks. Nigerian Journal of Technology, 28 (1), 71–78. Available at: https://www.ajol.info/index.php/njt/article/view/123428
2. Umoren, I. J., Inyang, S. J. (2021). Methodical Performance Modelling of Mobile Broadband Networks with Soft Computing Model. International Journal of Computer Applications, 174 (25), 7–21. doi: https://doi.org/10.5120/ijca2021921157
3. Najjari, N. (2017). Performance modeling and analysis of wireless local area networks with bursty traffic. Available at: https://ore.exeter.ac.uk/repository/handle/10871/27588
4. Hneiti, W., Ajlouni, N. (2006). Performance Enhancement of Wireless Local Area Networks. 2006 2nd International Conference on Information & Communication Technologies. doi: https://doi.org/10.1109/ictta.2006.1684782
5. Wattimena, G. M. (2013). Performance Analysis of Statistical Distributions for VoIP over WiMAX Access Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 2 (4), 372–376. Available at: https://www.academia.edu/3422091/Performance_Analysis_of_Statistical_Distributions_for_VoIP_over_WiMAX_Access_Networks
6. Gabriel, B., Onuodu, F. E. (2021). An Improved Model For Wireless Fidelity Using Header Compression Algorithm (HCA). International Journal of Innovative Information Systems & Technology Research, 9 (3), 131–141. Available at: https://seahipaj.org/journals-ci/sept-2021/IJIISTR/full/IJIISTR-S-13-2021.pdf
7. Wing Ming Wong, E., Chi Hung Chan, S. (2001). Performance modeling of video-on-demand systems in broadband networks. IEEE Transactions on Circuits and Systems for Video Technology, 11 (7), 848–859. doi: https://doi.org/10.1109/76.931111
8. Singh, G. (2012). Comparative Analysis and Security Issues in Broadband Wireless Networks. Global Journal of Research In Engineering, 12 (8-F), 35–39. Available at: https://engineeringresearch.org/index.php/GJRE/article/view/642/584
9. Muntean, G.-M., Perry, P., Murphy, L. (2004). Performance Comparison of Local Area Video Streaming Systems. IEEE Communications Letters, 8 (5), 326–328. doi: https://doi.org/10.1109/lcomm.2004.827451
10. Mondal, D. C., Misra, I. S., Basu, S. (2012). Performance Evaluation of VoIP Codecs over WiMAX/WiFi ntegrated Network. International Journal of Computer Applications, 0975 (8887), 14–17.
11. Abdelrazig, W. S., El Dawo, H. (2013). Performance Evaluation of VOIP Codecs Over Wi-Fi WIMAX. International Journal of Science and Research (IJSR), 5 (8), 1924–1927. Available at: https://www.ijsr.net/archive/v5i8/ART20161337.pdf

12. Singh, J., Kumar, R., Kumar, M. (2012). Performance analysis of WiMAX with different modulation techniques. International Journal of Engineering Research & Technology (IJERT), 1 (4), 1–6.
13. Fong, B., Hong, G. Y. (2010). On Performance of Multicast Delivery with Fixed WiMAX Telemedicine Networks Using Single-Carrier Modulation. Journal of Advances in Information Technology, 1 (1). doi: https://doi.org/10.4304/jait.1.1.59-65
14. Saeed, A. T., Esmailpour, A., Nasser, N. (2016). Performance analysis for the QoS support in LTE and WiFi. 2016 IEEE Wireless Communications and Networking Conference. doi: https://doi.org/10.1109/wcnc.2016.7564685
15. AlAlawi, K., Al-Aqrabi, H. (2015). Quality of service evaluation of VoIP over wireless networks. 2015 IEEE 8th GCC Conference & Exhibition. doi: https://doi.org/10.1109/ieeegcc.2015.7060070
16. Alturki, R., Nwizege, K., Mehmood, R., Faisal, M. (2009). End to End Wireless Multimedia Service Modelling over a Metropolitan Area Network. 2009 11th International Conference on Computer Modelling and Simulation. doi: https://doi.org/10.1109/uksim.2009.90
17. Sarkar, M., Goel, R. (2008). An Algorithm to Enhance QoS for Streaming Video over WLANs. Advances in Electrical and Electronics Engineering - IAENG Special Edition of the World Congress on Engineering and Computer Science 2008. doi: https://doi.org/10.1109/wcecs.2008.18
18. Sadiwala, R., Saxena, M. (2015). Performance Evaluation of Next Generation Networks using OPNET Simulator. Communications on Applied Electronics, 2 (4), 32–37. doi: https://doi.org/10.5120/cae2015651737

DOI: 10.15587/1729-4061.2022.254545

DEVELOPMENT OF CRYPTO-CODE CONSTRUCTS BASED ON LDPC CODES (p. 44–59)

Serhii Pohasii
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-4540-3693

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

Oleksandr Zhuchenko
Ukrainian State University of Railway Transport, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-3275-810X

Oleksandr Milov
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-6135-2120

Volodymyr Lysechko
Ukrainian State University of Railway Transport, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-1520-9515

Oleksandr Kovalenko
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID: https://orcid.org/0000-0001-9297-0650

Maryna Kostiak
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-6667-7693

Andrii Volkov
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1566-9893

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

Vitalii Susukailo
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-4431-9964

The results of developing post-quantum algorithms of McEliece and Niederreiter crypto-code constructs based on LDPC (Low-Density Parity-Check) codes are presented. With the rapid growth of computing capabilities of mobile technologies and the creation of wireless mesh and sensor networks, Internet of Things technologies, and smart technologies on their basis, information security is becoming an urgent problem. At the same time, there is a need to consider security in two circuits, internal (directly within the network infrastructure) and external (cloud technologies). In such conditions, it is necessary to integrate threats to both the internal and external security circuits. This allows you to take into account not only the hybridity and synergy of modern targeted threats, but also the level of significance (degree of secrecy) of information flows and information circulating in both the internal and external security circuits. The concept of building security based on two circuits is proposed. To ensure the security of wireless mobile channels, it is proposed to use McEliece and Niederreiter crypto-code constructs based on LDPC codes, which allows integration into the credibility technology of IEEE 802.15.4, IEEE 802.16 standards. This approach provides the required level of security services (confidentiality, integrity, authenticity) in a full-scale quantum computer. Practical security technologies based on the proposed crypto-code constructs, online IP telephony and the Smart Home system based on the use of an internal server are considered.

Keywords: crypto-code constructs, low-density parity-check codes, security concept.

References

1. Branco, P. de M. (2017). A new LDPC-based McEliece cryptosystem. Tecnico Lisboa, 79. Available at: https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973967111/Thesis.pdf
2. Engelbert, D., Overbeck, R., Schmidt, A. (2007). A Summary of McEliece-Type Cryptosystems and their Security. Journal of Mathematical Cryptology, 1 (2). doi: https://doi.org/10.1515/jmc.2007.009
3. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2012). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. Available at: https://eprint.iacr.org/2012/409.pdf
4. Baldi, M., Bodrato, M., Chiaraluce, F. (2008). A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes. Security and Cryptography for Networks, 246–262. doi: https://doi.org/10.1007/978-3-540-85855-3_17
5. Chang, K. (2012). I.B.M. Researchers Inch Toward Quantum Computer. The New York Times. Available at: http://www.nytimes.com/2012/02/28/technology/ibm-inch-closer-on-quantum-computer.html?_r=1&hpw
6. Eisenbarth, T., Güneysu, T., Heyse, S., Paar, C. (2009). MicroEliece: McEliece for Embedded Devices. Cryptographic Hardware and Embedded Systems - CHES 2009, 49–64. doi: https://doi.org/10.1007/978-3-642-04138-9_4
7. Ghosh, S., Delvaux, J., Uhsadel, L., Verbauwhede, I. (2012). A Speed Area Optimized Embedded Co-processor for McEliece Cryptosystem. 2012 IEEE 23rd International Conference on Application-Specific Systems, Architectures and Processors. doi: https://doi.org/10.1109/asap.2012.16
8. Heyse, S. (2011). Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices. Lecture Notes in

Computer Science, 143–162. doi: https://doi.org/10.1007/978-3-642-25405-5_10
9. Persichetti, E. (2012). Compact McEliece keys based on quasi-dyadic Srivastava codes. Journal of Mathematical Cryptology, 6 (2). doi: https://doi.org/10.1515/jmc-2011-0099
10. Minder, L. (2007). Cryptography Based on Error Correcting Codes. Lausanne. doi: https://doi.org/10.5075/epfl-thesis-3846
11. Overbeck, R., Sendrier, N. (2009). Code-based cryptography. Post-Quantum Cryptography, 95–145. doi: https://doi.org/10.1007/978-3-540-88702-7_4
12. Bernstein, D. J., Lange, T., Peters, C. (2008). Attacking and Defending the McEliece Cryptosystem. Lecture Notes in Computer Science, 31–46. doi: https://doi.org/10.1007/978-3-540-88403-3_3
13. Cayrel, P.-L., Hoffmann, G., Persichetti, E. (2012). Efficient Implementation of a CCA2-Secure Variant of McEliece Using Generalized Srivastava Codes. Lecture Notes in Computer Science, 138–155. doi: https://doi.org/10.1007/978-3-642-30057-8_9
14. Misoczki, R., Barreto, P. S. L. M. (2009). Compact McEliece Keys from Goppa Codes. Lecture Notes in Computer Science, 376–392. doi: https://doi.org/10.1007/978-3-642-05445-7_24
15. Faugère, J.-C., Otmani, A., Perret, L., Tillich, J.-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. Lecture Notes in Computer Science, 279–298. doi: https://doi.org/10.1007/978-3-642-13190-5_14
16. Berger, T. P., Cayrel, P.-L., Gaborit, P., Otmani, A. (2009). Reducing Key Length of the McEliece Cryptosystem. Lecture Notes in Computer Science, 77–97. doi: https://doi.org/10.1007/978-3-642-02384-2_6
17. Baldi, M., Chiaraluce, F. (2007). Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes. 2007 IEEE International Symposium on Information Theory. doi: https://doi.org/10.1109/isit.2007.4557609
18. Baldi, M., Chiaraluce, F., Garello, R. (2006). On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2006 First International Conference on Communications and Electronics. doi: https://doi.org/10.1109/cce.2006.350824
19. Baldi, M., Chiaraluce, F., Garello, R., Mininni, F. (2007). Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2007 IEEE International Conference on Communications. doi: https://doi.org/10.1109/icc.2007.161
20. Monico, C., Rosenthal, J., Shokrollahi, A. (2000). Using low density parity check codes in the McEliece cryptosystem. 2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060). doi: https://doi.org/10.1109/isit.2000.866513
21. Otmani, A., Tillich, J.-P., Dallot, L. (2010). Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 3 (2), 129–140. doi: https://doi.org/10.1007/s11786-009-0015-8
22. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. 2013 IEEE International Symposium on Information Theory. doi: https://doi.org/10.1109/isit.2013.6620590
23. Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.) (2009). Post-Quantum Cryptography. Springer, 246. doi: https://doi.org/10.1007/978-3-540-88702-7
24. Courtois, N. T., Finiasz, M., Sendrier, N. (2001). How to Achieve a McEliece-Based Digital Signature Scheme. Lecture Notes in Computer Science, 157–174. doi: https://doi.org/10.1007/3-540-45682-1_10
25. Faugere, J.-C., Gauthier-Umana, V., Otmani, A., Perret, L., Tillich, J. P. (2011). A distinguisher for high rate McEliece cryptosystems. 2011 IEEE Information Theory Workshop. doi: https://doi.org/10.1109/itw.2011.6089437
26. Gaborit, P. (2005). Shorter keys for code based cryptography. In International Workshop on Coding and Cryptography – WCC'2005, 81–91.
27. Heyse, S., von Maurich, I., Güneysu, T. (2013). Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices. Lecture Notes in Computer Science, 273–292. doi: https://doi.org/10.1007/978-3-642-40349-1_16
28. Baldi, M., Bianchi, M., Chiaraluce, F. (2013). Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Information Security, 7 (3), 212–220. doi: https://doi.org/10.1049/iet-ifs.2012.0127
29. 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
30. 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
31. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2
32. 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
33. Sidel'nikov, V. M. (2002). Kriptografiya i teoriya kodirovaniya. Materialy konferentsii: Moskovskiy universitet i razvitie kriptografii v Rossii. Moscow: MGU.
34. Ranjitha, C. R., Thomas, J., Chithra, K. R. (2016). A brief study on LDPC codes. International Journal of Engineering Research and General Science, 4 (2), 612–618. Available at: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf
35. Broul´ım, J. (2018). LDPC codes - new methodologies. University of West Bohemia, 127. Available at: https://cds.cern.ch/record/2730008/files/CERN-THESIS-2018-479.pdf
36. Zhu, H., Pu, L., Xu, H., Zhang, B. (2018). Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic. Wireless Communications and Mobile Computing, 2018, 1–9. doi: https://doi.org/10.1155/2018/5264724
37. Singh, H. (2020). Code based Cryptography: Classic McEliece. arxiv.org. doi: https://doi.org/10.48550/arXiv.1907.12754
38. Chen, P.-J., Chou, T., Deshpande, S., Lahr, N., Niederhagen, R., Szefer, J., Wang, W. (2022). Complete and Improved FPGA Implementation of Classic McEliece. Cryptology ePrint Archive: Report 2022/412. URL: https://eprint.iacr.org/2022/412
39. Liva, G., Song, S., Lan, L., Zhang, Y., Lin, S., Ryan, W. E. (2017). Design of LDPC Codes: A Survey and New Results. Journal of Communications Software and Systems, 2 (3), 191. doi: https://doi.org/10.24138/jcomss.v2i3.283
40. Richardson, T. J., Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 47 (2), 638–656. doi: https://doi.org/10.1109/18.910579
41. Chandrasetty, V. A., Aziz, S. M. (2011). FPGA Implementation of a LDPC Decoder using a Reduced Complexity Message Passing Algorithm. Journal of Networks, 6 (1). doi: https://doi.org/10.4304/jnw.6.1.36-45
42. Wang, Y. (2008). Generalized constructions, decoding and implementation of LDPC codes. University of Hawaii at Manoa. Available at: https://scholarspace.manoa.hawaii.edu/bitstream/10125/20577/Ph.D._AC1.H3_5085_r.pdf
43. Sarvaghad-Moghaddam, M., Ullah, W., Jayakody, D. N. K., Affes, S. (2020). A New Construction of High Performance LDPC Matrices

for Mobile Networks. Sensors, 20 (8), 2300. doi: https://doi.org/10.3390/s20082300
44. Hübner, C., Merz, H., Hansemann, T. (2009). Gebäudeautomation. Kommunikationssysteme mit EIB/KNX, LON und BACnet. Hanser. doi: https://doi.org/10.3139/9783446422636
45. 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX / Busch-Watchdog Sky KNX (2017). Busch-Jaeger Elektro GmbH, 198. Available at: https://library.e.abb.com/public/ddedcbf7ab704705affb179ca91e0fa2/2CKA001473B8668_Prasenzmelder_6131_03_ABB_EN.pdf
46. Technical documentation on KNX devices (2006). ABB.
47. KNX Handbook Version 1.1 Revision 1 (2004). Konnex Association.
48. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual. Busch-Watchdog Sky KNX (2016). Busch-Jaeger Elektro GmbH, 648.
49. ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products (2016). ABB, 86. Available at: https://library.e.abb.com/public/d26bd890d3ef476fbc3a59a2fdca6116/Webinar%20ABB%20i-bus%20KNX%20-%20KNX%20Basics%20and%20Products.pdf
50. Manual for KNX Planning (2017). Siemens Switzerland Ltd, 100.
51. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation (2010). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 116.
52. Kottapalli, N. (2011). Diameter and LTE Evolved Packet System. Corporate Headquarters, 10. Available at: http://go.radisys.com/rs/radisys/images/paper-lte-diameter-eps.pdf
53. Ventura, H. (2002). Diameter - Next generation's AAA protocol. Institutionen för Systemteknik, 66. Available at: https://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf
54. Vinay Kumar, S. B., Harihar, M. N. (2012). Diameter-Based Protocol in the IP Multimedia Subsystem. International Journal of Soft Computing and Engineering (IJSCE), 1 (6), 266–269. Available at: https://www.ijsce.org/portfolio-item/F0320121611/
55. Qanbari, S., Mahdizadeh, S., Rahimzadeh, R., Behinaein, N., Dustdar, S. (2016). Diameter of Things (DoT): A Protocol for Real-Time Telemetry of IoT Applications. Lecture Notes in Computer Science, 207–222. doi: https://doi.org/10.1007/978-3-319-43177-2_14
56. Tschofenig, H. (2019). Diameter: new generation AAA protocol – design, practice, and applications. John Wiley & Sons, Inc. doi: https://doi.org/10.1002/9781118875889
57. Ugrozy bezopasnosti yadra paketnoy seti 4G (2017). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
58. Uyazvimosti protokola Diameter v setyakh 4G (2018). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
59. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et. al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. doi: https://doi.org/10.15587/1729-4061.2021.233533
60. Yevseiev, S., Pohasii, S., Khvostenko, V. (2021). Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Information Processing Systems, 3 (166), 35–40. doi: https://doi.org/10.30748/soi.2021.166.03

DOI: 10.15587/1729-4061.2022.252060

DEVELOPMENT AND ANALYSIS OF THE NEW HASHING ALGORITHM BASED ON BLOCK CIPHER (p. 60–73)

Kairat Sakan
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-6812-6000

Saule Nyssanbayeva
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-5835-4958

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

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

Ardabek Khompysh
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0702-9346

Dilmukhanbet Dyusenbayev
Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-4835-1075

This paper proposes the new hash algorithm HBC-256 (Hash based on Block Cipher) based on the symmetric block cipher of the CF (Compression Function). The algorithm is based on the wipe-pipe construct, a modified version of the Merkle-Damgard construct. To transform the block cipher CF into a one-way compression function, the Davis-Meyer scheme is used, which, according to the results of research, is recognized as a strong and secure scheme for constructing hash functions based on block ciphers. The symmetric CF block cipher algorithm used consists of three transformations (Stage-1, Stage-2, and Stage-3), which include modulo two addition, circular shift, and substitution box (four-bit S-boxes). The four substitution boxes are selected from the "golden" set of S-boxes, which have ideal cryptographic properties.

The HBC-256 scheme is designed to strike an effective balance between computational speed and protection against a preimage attack. The CF algorithm uses an AES-like primitive as an internal transformation.

The hash image was tested for randomness using the NIST (National Institute of Standards and Technology) statistical test suite, the results were examined for the presence of an avalanche effect in the CF encryption algorithm and the HBC-256 hash algorithm itself. The resistance of HBC-256 to near collisions has been practically tested.

Since the classical block cipher key expansion algorithms slow down the hash function, the proposed algorithm is adapted for hardware and software implementation by applying parallel computing. A hashing algorithm was developed that has a sufficiently large freedom to select the sizes of the input blocks and the output hash digest. This will make it possible to create an almost universal hashing algorithm and use it in any cryptographic protocols and electronic digital signature algorithms.

Keywords: hash function, hash digest, block cipher, hash function security, collision.

References

1. Teeluck, R., Durjan, S., Bassoo, V. (2020). Blockchain Technology and Emerging Communications Applications. Security and Privacy Applications for Smart City Development, 207–256. doi: https://doi.org/10.1007/978-3-030-53149-2_11
2. Chen, J., Gan, W., Hu, M., Chen, C.-M. (2021). On the construction of a post-quantum blockchain for smart city. Journal of Informa-

tion Security and Applications, 58, 102780. doi: https://doi.org/10.1016/j.jisa.2021.102780
3. Dworkin, M. J. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. NIST. doi: https://doi.org/10.6028/nist.fips.202
4. X 5057-2:2003 (ISO/IEC 10118-2:2000). Available at: http://kikaku-rui.com/x5/X5057-2-2003-01.html
5. The SM3 Cryptographic Hash Function. Available at: https://tools.ietf.org/id/draft-oscca-cfrg-sm3-02.html
6. DSTU 7564:2014. Information Technologies. Cryptographic Data Security. Hash function. Available at: http://online.budstandart.com/ru/catalog/doc-page?id_doc=66229
7. Kim, D.-C., Hong, D., Lee, J.-K., Kim, W.-H., Kwon, D. (2015). LSH: A New Fast Secure Hash Function Family. Lecture Notes in Computer Science, 286–313. doi: https://doi.org/10.1007/978-3-319-15943-0_18
8. GOST 34.11-2018. Information technology. Cryptographic data security. Hash-function. Available at: https://docs.cntd.ru/document/1200161707
9. STB 34.101.77-2020. Informatsionnye tekhnologii i bezopasnost'. Kriptograficheskie algoritmy na osnove sponge-funktsii. Vzamen STB 34.101.77-2016. Available at: http://www.apmi.bsu.by/assets/files/std/bash-spec24.pdf
10. Zou, J., Dong, L. (2018). Cryptanalysis of the Round-Reduced Kupyna. Journal of Information Science and Engineering, 34 (3), 733–748. doi: https://do.org/10.6688/JISE.201805_34(3).0010
11. Chowdhury, A. R., Chatterjee, T., DasBit, S. (2014). LOCHA: A Light-weight One-way Cryptographic Hash Algorithm for Wireless Sensor Network. Procedia Computer Science, 32, 497–504. doi: https://doi.org/10.1016/j.procs.2014.05.453
12. Tchórzewski, J., Jakóbik, A., Iacono, M. (2021). An ANN-based scalable hashing algorithm for computational clouds with schedulers. International Journal of Applied Mathematics and Computer Science, 31 (4), 697–712. doi: https://doi.org/10.34768/amcs-2021-0048
13. Mondal, A., Mitra, S. (2016). TDHA: A Timestamp Defined Hash Algorithm for Secure Data Dissemination in VANET. Procedia Computer Science, 85, 190–197. doi: https://doi.org/10.1016/j.procs.2016.05.210
14. Bao, Z., Dinur, I., Guo, J., Leurent, G., Wang, L. (2020). Generic Attacks on Hash Combiners. Journal of Cryptology, 33 (3), 742–823. doi: https://doi.org/10.1007/s00145-019-09328-w
15. Andreeva, E., Mennink, B., Preneel, B. (2015). Open problems in hash function security. Designs, Codes and Cryptography, 77 (2-3), 611–631. doi: https://doi.org/10.1007/s10623-015-0096-0
16. Naito, Y. (2012). Blockcipher-Based Double-Length Hash Functions for Pseudorandom Oracles. Lecture Notes in Computer Science, 338–355. doi: https://doi.org/10.1007/978-3-642-28496-0_20
17. Bao, Z., Ding, L., Guo, J., Wang, H., Zhang, W. (2020). Improved Meet-in-the-Middle Preimage Attacks against AES Hashing Modes. IACR Transactions on Symmetric Cryptology, 318–347. doi: https://doi.org/10.46586/tosc.v2019.i4.318-347
18. Nandi, M., Paul, S. (2010). Speeding Up the Wide-Pipe: Secure and Fast Hashing. Lecture Notes in Computer Science, 144–162. doi: https://doi.org/10.1007/978-3-642-17401-8_12
19. A study on hash functions for cryptography (2002). SANS Institute. Available at: https://www.giac.org/paper/gsec/3294/study-hash-functions-cryptography/105433
20. Al-Kuwari, S., Davenport, J., Bradford, R. (2011). Cryptographic Hash Functions: Recent Design Trends and Security Notions. IACR. Available at: https://eprint.iacr.org/2011/565.pdf
21. Denton, B., Adhami, R. (2012). Modern Hash Function Construction. Available at: https://www.researchgate.net/publication/267298547_Modern_Hash_Function_Construction
22. Hosoyamada, A., Yasuda, K. (2018). Building Quantum-One-Way Functions from Block Ciphers: Davies-Meyer and Merkle-Damgård Constructions. Advances in Cryptology – ASIACRYPT 2018, 275–304. doi: https://doi.org/10.1007/978-3-030-03326-2_10
23. Preneel, B., Govaerts, R., Vandewalle, J. (1993). Hash functions based on block ciphers: a synthetic approach. Lecture Notes in Computer Science, 368–378. doi: https://doi.org/10.1007/3-540-48329-2_31
24. Manuel, S., Sendrier, N. (2007). XOR-Hash: A Hash Function Based on XOR. In WEWRC '07.
25. Vergili, I., Yucel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n×x S-Boxes. Turkish Journal of Electrical Engineering & Computer Sciences, 9 (2), 137–145. Available at: https://journals.tubitak.gov.tr/elektrik/issues/elk-01-9-2/elk-9-2-3-0008-1.pdf
26. Mulyarchik, K. S. (2013). Lavinnyy effekt v algoritmakh shifrovaniya na osnove diskretnykh khaoticheskikh otobrazheniy. Doklady BGUIR, 6 (76), 86–91. Available at: https://libeldoc.bsuir.by/bitstream/123456789/1592/1/Mulyarchik_Lavinniy.PDF
27. Dobrovolsky, Y., Prokhorov, G., Hanzhelo, M., Hanzhelo, D., Trembach, D. (2021). Development of a hash algorithm based on cellular automata and chaos theory. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 48–55. doi: https://doi.org/10.15587/1729-4061.2021.242849
28. Kapalova, N., Khompysh, A., Arici, M., Algazy, K. (2020). A block encryption algorithm based on exponentiation transform. Cogent Engineering, 7 (1), 1788292. doi: https://doi.org/10.1080/23311916.2020.1788292
29. Algazy, K. T., Babenko, L. K., Biyashev, R. G., Ishchukova, E. A., Kapalova, N. A., Nysynbaeva, S. E., Smolarz, A. (2020). Differential Cryptanalysis of New Qamal Encryption Algorithm. International Journal of Electronics and Telecommunications, 4, 647–653. doi: https://doi.org/10.24425/ijet.2020.134023
30. Lamberger, M., Mendel, F., Rijmen, V., Simoens, K. (2011). Memoryless near-collisions via coding theory. Designs, Codes and Cryptography, 62 (1), 1–18. doi: https://doi.org/10.1007/s10623-011-9484-2
31. Maram, B., Gnanasekar, J. M. (2016). Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output. TEM Journal, 5 (1), 67–75. doi: https://dx.doi.org/10.18421/TEM51-11
32. Biyashev, R. G., Kalimoldayev, M. N., Nyssanbayeva, S. E., Kapalova, N. A., Dyusenbayev, D. S., Algazy, K. T. (2018). Development and analysis of the encryption algorithm in nonpositional polynomial notations. Eurasian Journal of Mathematical and Computer Applications, 6 (2), 19–33. doi: https://doi.org/10.32523/2306-6172-2018-6-2-19-33
33. Saarinen, M.-J. O. (2012). Cryptographic Analysis of All 4×4-Bit S-Boxes. Lecture Notes in Computer Science, 118–133. doi: https://doi.org/10.1007/978-3-642-28496-0_7
34. Kosta, B. P., Sanyasi, P. (2021). Design and Implementation of a Strong and Secure Lightweight Cryptographic Hash Algorithm using Elliptic Curve Concept: SSLHA-160. International Journal of Advanced Computer Science and Applications, 12 (2). doi: https://doi.org/10.14569/ijacsa.2021.0120279
35. Kapalova, N. A., Nysanbaeva, S. E. (2008). Analiz statisticheskikh svoystv algoritma generatsii psevdosluchaynykh posledovatel'nostey. Mater. X Mezhdunar. nauch.-prakt. konf. Informatsionnaya bezopasnost'. Ch. 2. Taganrog: Izd-vo TTI YuFU, 169–172.
36. Ivanov, M. A. Khesh-funktsii. Teoriya, primenenie i novye standarty (chast' 1). Available at: https://docplayer.com/28902735-Hesh-funkcii-teoriya-primenenie-i-novye-standarty-chast-1.html
37. Kumar, M., Dey, D., Pal, S. K., Panigrahi, A. (2017). HeW: AHash Function based on Lightweight Block Cipher FeW. Defence Science Journal, 67 (6), 636. doi: https://doi.org/10.14429/dsj.67.10791
38. Bussi, K., Dey, D., Mishra, P. R., Dass, B. K. (2019). MGR Hash Functions. Cryptologia, 43 (5), 372–390. doi: https://doi.org/10.1080/01611194.2019.1596995

АНОТАЦІЇ

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2022.255203

РОЗРОБКА МЕТОДУ СЕГМЕНТУВАННЯ СКЛАДНОСТРУКТУРОВАНИХ ЗОБРАЖЕНЬ З КОСМІЧНИХ СИСТЕМ СПОСТЕРЕЖЕННЯ НА ОСНОВІ АЛГОРИТМУ РОЮ ЧАСТИНОК (с. 6–13)

Г. В. Худов, О. М. Маковейчук, І. А. Хижняк, О. О. Олексенко, Ю. А. Хажанець, Ю. С. Соломоненко, І. Ю. Юзова, Є. Є. Дудар, С. В. Стецiв, В. Г. Худов

Удосконалено метод сегментування складноструктурованих зображень з космічних систем спостереження на основі алгоритму рою частинок. На відміну від відомих, метод сегментування складноструктурованих зображень на основі алгоритму рою частинок передбачає:

– виділення каналів яскравості в кольоровому просторі Red-Green-Blue;

– використання методу рою частинок на зображенні в кожному каналі яскравості кольорового простору RGB;

– сегментування зображення зведено до обчислення цільової функції, швидкості переміщення та нового місцеположення для кожної частинки рою на зображенні в кожному каналі яскравості кольорового простору RGB.

Проведені експериментальні дослідження щодо сегментування складноструктурованого зображення методом на основі алгоритму рою частинок. Встановлено, що удосконалений метод сегментування на основі алгоритму рою частинок дозволяє проводити сегментування складноструктурованих зображень з космічних систем спостереження.

Проведено порівняння якості сегментування складноструктурованого зображення. Порівняльний візуальний аналіз відомого та удосконаленого методів сегментування свідчить про наступне:

– удосконалений метод сегментування на основі алгоритму рою частинок виділяє більше об'єктів інтересу (об'єктів військової техніки);

– відомий метод k-means відносить деякі об'єкти інтересу (особливо ті, які частково покриті снігом) до снігового покрову (відмічені синім кольором);

– удосконалений метод сегментування також відносить деякі об'єкти інтересу, що практично повністю покриті снігом до снігового покрову (відмічені синім кольором).

Встановлено, що удосконалений метод сегментування на основі алгоритму рою частинок забезпечує зниження помилок сегментування I роду в середньому на 12 % та зниження помилок сегментування II роду в середньому на 8 %.

Ключові слова: сегментування, складноструктуроване зображення, космічна система спостереження, рой частинок, помилки першого та другого роду.

DOI: 10.15587/1729-4061.2022.255789

ПОКРАЩЕННЯ ШУМОВИХ ЗОБРАЖЕНЬ, ЩО ФІЛЬТРУЮТЬСЯ ДВОСТОРОННІМ ПРОЦЕСОМ, З ВИКОРИСТАННЯМ БАГАТОМАСШТАБНОЇ МЕРЕЖІ АГРЕГАЦІЇ КОНТЕКСТА (с. 14–20)

Zinah R. Hussein

Останнім часом глибинному навчанню приділяється багато уваги як можливе вирішення безлічі проблем штучного інтелекту. Згорткові нейронні мережі (ЗНМ) перевершують інші архітектури глибинного навчання у застосуванні ідентифікації та розпізнавання об'єктів у порівнянні з іншими методами машинного навчання. Розпізнавання мови, аналіз образів та ідентифікація зображень – усі вони виграють від глибинних нейронних мереж. Під час виконання операцій над зашумленими зображеннями, такими як видалення туману або покращення слабкого освітлення, потрібні методи обробки зображень, такі як фільтрація або покращення зображення. У дослідженні показано вплив використання багатомасштабної мережі агрегування контексту з глибоким навчанням CAN на апроксимацію двосторонньої фільтрації (АДФ) для усунення шумів у зображеннях відеоспостереження. Ми використовуємо Data-store для управління нашим набором даних, який є об'єктом або набором даних, які величезні для введення в пам'ять. Це дозволяє нам читати, керувати та обробляти дані, розташовані в декількох файлах, як єдине ціле. Архітектура CAN забезпечує інтегровані рівні глибинного навчання, такі як вхідні дані, згортка, зворотна нормалізація та рівні Leaky ReLu для побудови багатомасштабних процесів. Також можна додати в мережу шари, такі як нормалізація адаптера (μ) і адаптивна нормалізація (лямбда). Ефективність розробленого оператора апроксимації CAN на зашумленому зображенні з двостороннім фільтруванням доведена при покращенні як зашумленого еталонного зображення, так і туманного зображення CCTV. Три метрики оцінки зображення (SSIM, NIQE і PSNR) оцінюють розроблене наближення CAN візуально і кількісно у порівнянні створеного очищеного від шуму зображення з еталонним зображенням – зашумлене зображення було (0,92673/0,76253, 6,18105/12,1865 та 26,786/20,3254) відповідно.

Ключові слова: згорткова нейронна мережа, залишкове навчання, багатомасштабна агрегація контексту, зображення відеоспостереження.

DOI: 10.15587/1729-4061.2022.253976

ОПТИМІЗАЦІЯ МОДУЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ РІШЕННЯ ПРЯМОГО ЗАВДАННЯ ГРАВІМЕТРІЇ З ВИКОРИСТАННЯМ ГЕНЕТИЧНОГО АЛГОРИТМУ (с. 21–34)

Assem Nazirova, Maksat Kalimoldayev, Farida Abdoldina, Ю. І. Дубовенко

У багатьох областях потрібні оптимальні підходи до вирішення багатьох завдань. Одним із таких напрямків є визначення виникнення аномалій сили тяжіння на родовищах нафти та газу. У цій роботі пропонується новий підхід до визначення джерела аномалій сили тяжіння на нафтогазових родовищах шляхом оцінки параметрів сили тяжіння, пов'язаних з тілами простої форми, такими як

однорідна сфера, горизонтальна призма та вертикальна сходинка. Підхід реалізований у обчислювальному модулі інформаційної системи ГеоМ для оптимізації розв'язання низки прямих задач гравіметрії з використанням генетичного алгоритму (ГА). Підхід заснований на вирішенні прямого завдання гравіметрії для мінімізації розбіжності варіацій сили тяжіння генетичним алгоритмом. Метод дозволяє вибирати значення одночасно для кількох параметрів досліджуваного середовища. Завдання реалізується шляхом послідовних наближень за заданим початковим наближенням середовища.

У роботі вказано вихідні розрахункові параметри та критерії пошуку оптимальних рішень для моделей геологічного середовища. Розрахунки проводилися для таких моделей середовища, як однорідна сфера, горизонтальна призма та вертикальний уступ. Для розрахунків використовувалися результати гравіметричного моніторингу одному з казахстанських нафтогазових родовищ. У роботі продемонстровано роботу алгоритму та представлено результати моделювання для трьох наявних профілів родовища. Отримані результати системи показали прийнятну точність алгоритму до 10^{-11}. Генетичний алгоритм дозволив значно підвищити надійність моделі та скоротити робочий час на аналіз виміряного гравітаційного поля.

Ключові слова: пряме завдання гравіметрії, генетичний алгоритм, гравіметричний моніторинг, методи глобальної оптимізації.

DOI: 10.15587/1729-4061.2022.255520

ХАРАКТЕРИСТИЧНИЙ АНАЛІЗ ТЕОРІЇ ЧЕРГ У WI-FI-ДОДАТКАХ З ВИКОРИСТАННЯМ OPNET 14.5 MODELER (с. 35–43)

Ali Hamzah Najim, Hassnen Shakir Mansour, Ali Hashim Abbas

Технологія бездротового (Wi-Fi) широкосмугового доступу дуже вплинула на розвиток широкосмугових бездротових мереж, які, як очікується, будуть розвиватися по відношенню до швидкості та покриття. Точки доступу Wi-Fi доступні повсюдно, що робить його більш простим у використанні засобом доступу в Інтернет у порівнянні з локальною мережею (LAN). Однак Інтернет, що є мережею з максимальною ефективністю, не забезпечує необхідної якості обслуговування (QoS) і не має будь-якої диференціації службового трафіку. Основною метою даної роботи є вивчення дії трьох організаційних механізмів: методу «першим прийшов – першим пішов» (FIFO) – стандартний метод мережевої реалізації для обробки пакетів один за одним у міру їх надходження, черга з пріоритетом (PQ) та зважена справедлива черга (WFQ), PQ і WFQ класифікують типи трафіку на основі пріоритету обслуговування. Крім того, WFQ присвоює кожному сервісу справедливу вагу для декількох класів трафіку, таких як відеоконференції, IP-телефонія (VoIP) та протокол передачі файлів (FTP) з використанням бездротової мережі Telkom ST3. У дослідженні застосовуються чотири різних сценарії: у першому сценарії застосовуються методи без будь-якої дисципліни організації черг; другий сценарій реалізує методи з FIFO; третій сценарій реалізує методи з PQ, в останньому застосовуються методи з WFQ. Дослідження показали ефективність «наскрізної затримки передачі пакетів та варіації затримки пакетів для VoIP у сценарії WFQ» в порівнянні з іншими механізмами організації черг зі значеннями 171,717 мс та 0,977 мс відповідно. У випадку відеоконференцзв язку продуктивність також вища у випадку WFQ зі значеннями 32,495 мс та 7,207 мс відповідно, оскільки WFQ має відповідний вимогам «розподіл смуги пропускання».

Ключові слова: Wi-Fi, QoS, FIFO, PQ, WFQ, VoIP, FTP, Telkom ST3, наскрізна затримка передачі пакетів.

DOI: 10.15587/1729-4061.2022.254545

РОЗРОБКА КРИПТО-КОДОВИХ КОНСТРУКЦІЙ НА LDPC-КОДАХ (с. 44–59)

С. С. Погасій, С. П. Євсеєв, О. С. Жученко, О. В. Мілов, В. П. Лисечко, О. В. Коваленко, М. Ю. Костяк, А. Ф. Волоков, О. В. Лезік, В. А. Сусукайло

Приведені результати розробки постквантових алгоритмів крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на кодах LDPC (Low-Density Parity-Check) із малою щільністю перевірок на парність. В умовах стрімкого зростання обчислювальних можливостей мобільних технологій та створення на їхній базі бездротових Mesh-, сенсорних мереж, технологій Інтернет речей, smart-технологій актуальною проблемою стає забезпечення безпеки інформації. При цьому виникає необхідність розгляду безпеки у двох контурах, внутрішньому (безпосередньо всередині інфраструктури мережі) та зовнішньому (хмарних технологіях). У таких умовах необхідно комплексувати загрози як на внутрішній контур безпеки, так і на зовнішній. Це дозволяє враховувати не лише гібридність та синергізм сучасних цільових загроз, але й рівень значущості (ступінь секретності) інформаційних потоків та інформації, що циркулює як у внутрішньому, так і зовнішньому контурі безпеки. Пропонується концепція побудови безпеки на основі двох контурів. Для забезпечення безпеки бездротових мобільних каналів пропонується використовувати крипто-кодові конструкції Мак-Еліса та Нідеррайтера на LDPC-кодах, що дозволяє інтегруватися у технології забезпечення вірогідності стандартів IEEE 802.15.4, IEEE 802.16. Такий підхід дозволяє забезпечити необхідний рівень послуг безпеки (конфіденційності, цілісності, автентичності) в умовах повномасштабного квантового комп'ютера. Розглядаються практичні технології забезпечення безпеки, на основі запропонованих крипто-кодових конструкцій, IP-телефонії в онлайн режимі та системи "Розумний дім" на основі використання внутрішнього сервера.

Ключові слова: крипто-кодові конструкції, коди з малою щільністю перевірок на парність, концепція безпеки.

DOI: 10.15587/1729-4061.2022.252060

РОЗРОБКА ТА ДОСЛІДЖЕННЯ НОВОГО АЛГОРИТМУ ХЕШУВАННЯ, ЗАСНОВАНОГО НА БЛОЧНОМУ ШИФРІ (с. 60–73)

Kairat Sakan, Saule Nyssanbayeva, Nursulu Kapalova, Kunbolat Algazy, Ardabek Khompysh, Dilmukhanbet Dyusenbayev

У даній роботі пропонується новий алгоритм хешування HBC-256 (хешування на основі блокового шифру), заснований на симетричному блоковому шифрі CF (функція стиснення). Алгоритм заснований на конструкції wipe-pipe, модифікованій версії кон-

струкції Меркла-Дамгарда. Для перетворення блокового шифру CF у функцію одностороннього стиснення використовується схема Девіса-Мейера, яка, за результатами досліджень, визнана надійною та безпечною схемою побудови хеш-функцій на основі блокових шифрів. Використовуваний алгоритм на основі симетричного блокового шифру CF складається з трьох перетворень (Етап 1, Етап 2 І Етап 3), що включають додавання за модулем два, циклічний зсув і блок підстановки (чотирьохбітові S-блоки). Чотири блоки підстановки обрані із "золотого" набору S-блоків, що мають ідеальні криптографічні властивості.

Розроблено схему HBC-256 для забезпечення ефективного балансу між обчислювальною швидкістю та захистом від атаки знаходження прообразу. В якості внутрішнього перетворення алгоритм CF використовує AES-подібний примітив.

Хеш-образ був перевірений на випадковість з використанням набору статистичних тестів NIST (Національний інститут стандартів і технологій США), результати були досліджені на наявність лавинного ефекту в алгоритмі шифрування CF та самому алгоритмі хешування HBC-256. Практично перевірена стійкість HBC-256 до близьких зіткнень.

Оскільки класичні алгоритми розширення ключа блокового шифру уповільнюють хеш-функцію, запропонований алгоритм адаптований для апаратної та програмної реалізації із застосуванням паралельних обчислень. Розроблено алгоритм хешування, що має досить велику свободу вибору розмірів вхідних блоків і вихідного хеш-дайджесту. Це дозволить створити практично універсальний алгоритм хешування та використовувати його у будь-яких криптографічних протоколах та алгоритмах електронного цифрового підпису.

Ключові слова: хеш-функція, хеш-дайджест, блоковий шифр, безпека хеш-функції, зіткнення.