

## ABSTRACT AND REFERENCES

## INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2024.310521

**IMPROVING PROTECTION OF FALCON ELECTRONIC SIGNATURE SOFTWARE IMPLEMENTATIONS AGAINST ATTACKS BASED ON FLOATING POINT NOISE (p. 6–17)**

**Olena Kachko**Kharkiv National University of Radio Electronics,  
Kharkiv, UkraineInstitute of Information Technologies PrJSC, Kharkiv, Ukraine  
**ORCID:** <https://orcid.org/0000-0001-9249-0497>**Yurii Gorbenko**Institute of Information Technologies PrJSC, Kharkiv, Ukraine  
**ORCID:** <https://orcid.org/0009-0005-0987-4796>**Serhii Kandii**V. N. Karazin Kharkiv National University, Kharkiv, Ukraine  
Institute of Information Technologies PrJSC, Kharkiv, Ukraine  
**ORCID:** <https://orcid.org/0000-0003-0552-8341>**Yevhenii Kaptol**V. N. Karazin Kharkiv National University, Kharkiv, Ukraine  
Institute of Information Technologies PrJSC, Kharkiv, Ukraine  
**ORCID:** <https://orcid.org/0000-0001-8612-2196>

The object of this study is digital signatures. The Falcon digital signature scheme is one of the finalists in the NIST post-quantum cryptography competition. Its distinctive feature is the use of floating-point arithmetic, which leads to the possibility of a key recovery attack with two non-matching signatures formed under special conditions. The work considers the task to improve the Falcon in order to prevent such attacks, as well as the use of fixed-point calculations instead of floating-point calculations in the Falcon scheme. The main results of the work are proposals for methods on improving Falcon's security against attacks based on the use of floating-point calculations. These methods for improving security differ from others in the use of fixed-point calculations with specific experimentally determined orders of magnitude in one case and proposals for modifying procedures during the execution of which the conditions for performing an attack on implementation level arise in the second case. As a result of the analysis, the probability of a successful attack on the recovery of the secret key for the reference implementation of the Falcon was clarified. Specific places in the code that make the attack possible have been localized and code modifications have been suggested that make the attack impossible. In addition, the necessary scale for fixed-point calculations was determined, at which it is possible to completely get rid of floating-point calculations. The results could be used to qualitatively improve the security of existing digital signatures. This will make it possible to design more reliable and secure information systems using digital signatures. In addition, the results could be implemented in existing systems to ensure their resistance to modern threats.

**Keywords:** quantum-resistant transformations, Falcon, floating point, NIST PQC, NTRU.

**References**

- Fouque, P., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T. et al. (2020). Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Available at: <https://falcon-sign.info/falcon.pdf>
- Post-Quantum Cryptography PQC. NIST. Available at: <https://csrc.nist.gov/projects/post-quantum-cryptography>
- Prest, T. (2017). Sharper Bounds in Lattice-Based Cryptography Using the Rényi Divergence. *Advances in Cryptology – ASIACRYPT 2017*, 347–374. [https://doi.org/10.1007/978-3-319-70694-8\\_13](https://doi.org/10.1007/978-3-319-70694-8_13)
- Pornin, T. (2019). New Efficient, Constant-Time Implementations of Falcon. *ePrint IACR*. Available at: <https://eprint.iacr.org/2019/893>
- Karabulut, E., Aysu, A. (2021). FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks. 2021 58th ACM/IEEE Design Automation Conference (DAC). <https://doi.org/10.1109/dac18074.2021.9586131>
- Guerreau, M., Martinelli, A., Ricosset, T., Rossi, M. (2022). The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 141–164. <https://doi.org/10.46586/tches.v2022.i3.141-164>
- Potii, O., Kachko, O., Kandii, S., Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. *Eastern-European Journal of Enterprise Technologies*, 1 (9 (127)), 52–59. <https://doi.org/10.15587/1729-4061.2024.295160>
- Pornin, T. (2023). Improved Key Pair Generation for Falcon, BAT and Hawk. *Cryptology ePrint Archive*. Available at: <https://eprint.iacr.org/2023/290>
- Gentry, C., Peikert, C., Vaikuntanathan, V. (2007). Trapdoors for Hard Lattices and New Cryptographic Constructions. *Cryptology ePrint Archive*. Available at: <https://eprint.iacr.org/2007/432>
- Albrecht, M., Ducas, L. (2021). Lattice Attacks on NTRU and LWE: A History of Refinements. *Cryptology ePrint Archive*. Available at: <https://eprint.iacr.org/2021/799>
- Prest, T. (2015). Gaussian Sampling in Lattice-Based Cryptography. THALES. Available at: <https://tprest.github.io/pdf/pub/thesis-thomas-prest.pdf>
- Ducas, L., Prest, T. (2016). Fast Fourier Orthogonalization. *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*. <https://doi.org/10.1145/2930889.2930923>
- Fisher, R. A. (1922). On the Interpretation of  $\chi^2$  from Contingency Tables, and the Calculation of P. *Journal of the Royal Statistical Society*, 85 (1), 87. <https://doi.org/10.2307/2340521>
- Simard, R., L'Ecuyer, P. (2011). Computing the Two-Sided Kolmogorov-Smirnov Distribution. *Journal of Statistical Software*, 39 (11). <https://doi.org/10.18637/jss.v039.i11>
- Wilk, M. B., Gnanadesikan, R. (1968). Probability plotting methods for the analysis for the analysis of data. *Biometrika*, 55 (1), 1–17. <https://doi.org/10.1093/biomet/55.1.1>
- What Every Computer Scientist Should Know About Floating-Point Arithmetic. Available at: [https://docs.oracle.com/cd/E19957-01/806-3568/ncg\\_goldberg.html](https://docs.oracle.com/cd/E19957-01/806-3568/ncg_goldberg.html)
- IEEE Std 754TM-2008. IEEE Standard for Floating-Point Arithmetic. IEEE Computer Society. Available at: <https://iremi.univ-reunion.fr/IMG/pdf/ieee-754-2008.pdf>
- Pornin, T., Prest, T. (2019). More Efficient Algorithms for the NTRU Key Generation Using the Field Norm. *Public-Key Cryptography – PKC 2019*, 504–533. [https://doi.org/10.1007/978-3-030-17259-6\\_17](https://doi.org/10.1007/978-3-030-17259-6_17)
- [FALCON OFFICIAL] Keygen implementation. Available at: <https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/bjVkrZmI9VM>

**DOI: 10.15587/1729-4061.2024.310547**  
**DEVELOPMENT OF FUNCTIONALITY PRINCIPLES FOR THE AUTOMATED DATA TRANSMISSION SYSTEM THROUGH WIRELESS COMMUNICATION CHANNELS TO ENSURE INFORMATION PROTECTION (p. 18–33)**

**Serhii Yevseiev**

National Technical University “Kharkiv Polytechnic Institute”,  
 Kharkiv, Ukraine

**ORCID:** <https://orcid.org/0000-0003-1647-6444>

**Stanislav Milevskiy**

National Technical University “Kharkiv Polytechnic Institute”,  
 Kharkiv, Ukraine

**ORCID:** <https://orcid.org/0000-0001-5087-7036>

**Vladyslav Sokol**

National Technical University “Kharkiv Polytechnic Institute”,  
 Kharkiv, Ukraine

**ORCID:** <https://orcid.org/0009-0009-9446-2049>

**Vladyslav Yemanov**

National Academy of the National Guard of Ukraine,  
 Kharkiv, Ukraine

**ORCID:** <https://orcid.org/0000-0001-5055-8852>

**Anatolii Volobuiev**

The Central Research Institute of the Armed Forces of Ukraine,  
 Kyiv, Ukraine

**ORCID:** <https://orcid.org/0000-0001-9415-0736>

**Larysa Dakova**

State University of Information and Communication Technologies,  
 Kyiv, Ukraine

**ORCID:** <https://orcid.org/0000-0001-6104-8217>

**Mykola Brailovskiy**

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

**ORCID:** <https://orcid.org/0000-0002-3148-1148>

**Irada Rahimova**

Azerbaijan Technical University, Baku, Azerbaijan

**ORCID:** <https://orcid.org/0000-0003-3278-3225>

**Vladyslav Kravchenko**

State University of Information and Communication Technologies,  
 Kyiv, Ukraine

**ORCID:** <https://orcid.org/0000-0002-4758-7027>

**Oleg Cherniavskiy**

National Technical University “Kharkiv Polytechnic Institute”,  
 Kharkiv, Ukraine

**ORCID:** <https://orcid.org/0000-0002-9388-4604>

The development of data transmission systems based on wireless radio communication channels allowed the construction of fundamentally new networks – mesh networks, which are used not only in smart technologies, but are the basis for the construction of cyber-physical and socio-cyber-physical systems (objects of critical infrastructure). The object is the process of ensuring reliable and secure data transmission based on the use of wireless radio communication channels. A mathematical model of information resources protection system functioning is proposed to ensure the signs of immunity and security of the automated data transmission system. To identify threats, a unified classifier and flow state estimation technique are used, which take into account the hybridity and synergy of targeted (mixed) attacks on communication channels. The critical points of the infrastructure elements, as well as the information that circulates and/or is stored, are determined. The assessment of compliance with

the regulators' requirements, both international and state regulatory acts, and the presence and ability of the security system elements to ensure the required level of infrastructure elements protection is taken into account. The proposed approach allows to determine: coefficients of information and internal availability of a wireless radio communication channel, the vector potential of the lagging magnetic field as a result of data transmission work. When evaluating the coefficient of a wireless radio communication channel internal availability, it is proposed to take into account coherent reception of the signal. At the same time, the immunity factor of the wireless radio communication channel is much higher than 1, which provides sufficient protection of information. A technical solution is proposed that will allow the level of confidentiality, integrity, authenticity and reliability of a wireless radio communication channel to approach 100 %.

**Keywords:** data transmission system, radio signal emitter, magnetic field, radio monitoring, socio-cyberphysical system.

### References

1. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. <https://doi.org/10.15587/978-617-7319-57-2>
2. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. <https://doi.org/10.15587/1729-4061.2021.229221>
3. Sokolov, A. Y. (1999). Algebraic approach on fuzzy control. IFAC Proceedings Volumes, 32 (2), 5386–5391. [https://doi.org/10.1016/s1474-6670\(17\)56917-7](https://doi.org/10.1016/s1474-6670(17)56917-7)
4. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskiy, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. <https://doi.org/10.15587/978-617-7319-31-2>
5. Shao, R., Ding, C., Liu, L., He, Q., Qu, Y., Yang, J. (2024). High-fidelity multi-channel optical information transmission through scattering media. Optics Express, 32 (2), 2846. <https://doi.org/10.1364/oe.514668>
6. Dao, V. A., Thanh Thuy, T. T., Quoc Bao, V. N., Dung, T. C., Quyen, N. X. (2024). Design of A Chaos-based Digital Radio over Fiber Transmission Link using ASK Modulation for Wireless Communication Systems. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 11 (1). <https://doi.org/10.4108/eetinis.v11i1.4530>
7. M, S., Kandasamy, R., Kumar, S. S. (2022). A Novel Approach on Cognitive Radio Sensor Networks for Efficient Data Transmission. <https://doi.org/10.21203/rs.3.rs-1735166/v1>
8. Lacey, K. (2024). Communication in the Radio Century. The Oxford Handbook of Radio and Podcasting, 733–748. <https://doi.org/10.1093/oxfordhb/9780197551127.013.34>
9. Ren, Y., Wu, Y., Tu, Z. (2024). A Multi-Channel Chromatic Dispersion Compensation for 15-km Front-Haul Transmission. Optical Fiber Communication Conference (OFC) 2024. <https://doi.org/10.1364/ofc.2024.w2b.11>
10. Park, J., Choi, D. (2023). Improvement and Utilization of Auxiliary Radio Communication System. Journal of the Korean Society of Hazard Mitigation, 23 (3), 83–93. <https://doi.org/10.9798/kosham.2023.23.3.83>

11. Soliman, N. F., Fadl-Allah, F. E., El-Shafai, W., Aly, M. I., Alabdulhafith, M., El-Samie, F. E. A. (2024). A Hybrid Cybersecurity Algorithm for Digital Image Transmission over Advanced Communication Channel Models. *Computers, Materials & Continua*, 79 (1), 201–241. <https://doi.org/10.32604/cmc.2024.046757>
12. Youvan, D. (2024). Silent Waves: The Role of Ham Radio in a Fictional Communication Blackout Scenario. <https://doi.org/10.13140/RG.2.2.23193.19044>
13. Kolawole, W. (2024). Enhancing Data Security through Chaotic Encryption for Secure Transmission. Available at: [https://www.researchgate.net/publication/380179574\\_Enhancing\\_Data\\_Security\\_through\\_Chaotic\\_Encryption\\_for\\_Secure\\_Transmission](https://www.researchgate.net/publication/380179574_Enhancing_Data_Security_through_Chaotic_Encryption_for_Secure_Transmission)
14. Renteria, L., Jinez, J., Torres, K., Ramos, J. (2023). Data transmission system through FM radio applying Data over Sound techniques. *Novasinerгия*, 6 (2), 129–139. <https://doi.org/10.37135/ns.01.12.08>
15. Soni, V. (2024). ED-SS based Cognitive Radio (CR) over Various Fading Channels for Modern Wireless Communications. *Journal of Electrical Systems*, 20 (7s), 1406–1423. <https://doi.org/10.52783/jes.3713>
16. Mak, B., Arya, S., Wang, Y., Ashdown, J. (2023). Characterization of Low-Latency Next-Generation eVTOL Communications: From Channel Modeling to Performance Evaluation. *Electronics*, 12 (13), 2838. <https://doi.org/10.3390/electronics12132838>
17. Guan, K., Kürner, T., Rupp, M., Nekovee, M. (2024). Guest Editorial: Channel Modeling and Signal Processing for Terahertz Communications. *IEEE Communications Magazine*, 62 (2), 14–15. <https://doi.org/10.1109/mcom.2024.10439199>
18. Yakovlev, M., Volobuev, A., Pribyliev, Yu. (2024). Mathematical modeling of the processes of functioning of automated military radio communication systems in terms of their protection against radio reconnaissance. *The Collection of Scientific Works of the National Academy of the National Guard of Ukraine*, 1 (43), 130–144. <https://doi.org/10.33405/2409-7470/2024/1/43/307934>
19. Makhmudov, F., Privalov, A., Privalov, A., Kazakevich, E., Bekbaev, G., Boldinov, A. et al. (2024). Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems. *Mathematics*, 12 (10), 1452. <https://doi.org/10.3390/math12101452>
20. Luat, P. N., Taparugssanagorn, A., Kaemarungsi, K., Phoojaroenchanachai, C. (2024). Spatial Simultaneous Functioning-Based Joint Design of Communication and Sensing Systems in Wireless Channels. *Applied Sciences*, 14 (12), 5319. <https://doi.org/10.3390/app14125319>
21. Kumar, P., Saxena, V. (2024). Nested Levels of Hybrid Cryptographical Technique for Secure Information Exchange. *Journal of Computer and Communications*, 12 (02), 201–210. <https://doi.org/10.4236/jcc.2024.122012>
22. Mikoni, S. V. (2023). Approach to assessing the level of intelligence of an information system. *Ontology of Designing*, 13 (1), 29–43. <https://doi.org/10.18287/2223-9537-2023-13-1-29-43>
23. Ramsden, J. (2023). The Transmission of Information. *Bioinformatics*, 75–91. [https://doi.org/10.1007/978-3-030-45607-8\\_7](https://doi.org/10.1007/978-3-030-45607-8_7)
24. Laue, F., Jamali, V., Schober, R. (2023). RIS-Assisted Device Activity Detection With Statistical Channel State Information. *IEEE Transactions on Wireless Communications*, 22 (12), 9473–9487. <https://doi.org/10.1109/twc.2023.3271365>
25. Vähä-Savo, L., Veggi, L., Vitucci, E. M., Icheln, C., Degli-Esposti, V., Haneda, K. (2023). Analytical Characterization of a Transmission Loss of an Antenna-Embedded Wall. <https://doi.org/10.36227/techrxiv.170244520.01558910/v1>
26. Elzinga, R., Janssen, M. J., Wesseling, J., Negro, S. O., Hekkert, M. P. (2023). Assessing mission-specific innovation systems: Towards an analytical framework. *Environmental Innovation and Societal Transitions*, 48, 100745. <https://doi.org/10.1016/j.eist.2023.100745>
27. Kramer, G. (2023). Information Rates for Channels with Fading, Side Information and Adaptive Codewords. *Entropy*, 25 (5), 728. <https://doi.org/10.3390/e25050728>
28. dos Santos, A., Barros, M. T. C. de, Correia, P. F. (2015). Transmission line protection systems with aided communication channels – Part II: Comparative performance analysis. *Electric Power Systems Research*, 127, 339–346. <https://doi.org/10.1016/j.epsr.2015.05.010>
29. Enquist, M., Ghirlanda, S., Lind, J. (2023). Acquisition and Transmission of Sequential Information. *The Human Evolutionary Transition*, 167–176. <https://doi.org/10.23943/princeton/9780691240770.003.0012>
30. Menezes, T. S., Barra, P. H. A., Dizioli, F. A. S., Lacerda, V. A., Fernandes, R. A. S., Coury, D. V. (2023). A Survey on the Application of Phasor Measurement Units to the Protection of Transmission and Smart Distribution Systems. *Electric Power Components and Systems*, 52 (8), 1379–1396. <https://doi.org/10.1080/15325008.2023.2240320>
31. Ribeiro, E. P. A., Lopes, F. V., Silva, K. M., Martins-Britto, A. G. (2023). Assessment of communication channel effects on time-domain protection functions tripping times. *Electric Power Systems Research*, 223, 109589. <https://doi.org/10.1016/j.epsr.2023.109589>
32. Shmatko, O., Herasymov, S., Lysetskiy, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. *Eastern-European Journal of Enterprise Technologies*, 6 (9 (126)), 39–49. <https://doi.org/10.15587/1729-4061.2023.293511>
33. Herasymov, S., Tkachov, A., Bazarnyi, S. (2024). Complex method of determining the location of social network agents in the interests of information operations. *Advanced Information Systems*, 8 (1), 31–36. <https://doi.org/10.20998/2522-9052.2024.1.04>
34. Kozhushko, Ya., Karlov, D., Klimishen, O., Bortsova, M., Herasymov, S., Hrichanuk, O., Bykov, V. N. (2018). Comparison of the Efficiency of Some Images Superposition Algorithms Used in Aircraft Map-Matching Navigation Systems. 2018 IEEE 17th International Conference on Mathematical Methods in Electromagnetic Theory (MMET). <https://doi.org/10.1109/mmet.2018.8460319>
35. Fedushko, S., Molodetska, K., Syerov, Y. (2023). Analytical method to improve the decision-making criteria approach in managing digital social channels. *Heliyon*, 9 (6), e16828. <https://doi.org/10.1016/j.heliyon.2023.e16828>
36. Mookerjee, R., Samuel, J. (2023). Managing the security of information systems with partially observable vulnerability. *Production and Operations Management*, 32 (9), 2902–2920. <https://doi.org/10.1111/poms.14015>
37. Marabissi, D., Abrardo, A., Mucchi, L. (2023). A new framework for Physical Layer Security in HetNets based on Radio Resource Allocation and Reinforcement Learning. *Mobile Networks and Applications*, 28 (4), 1473–1481. <https://doi.org/10.1007/s11036-023-02149-z>
38. Yevseiev, S., Khokhlova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskiy, S. et al.; Yevseiev, S., Khokhlova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. <https://doi.org/10.15587/978-617-7319-72-5>
39. Framework for assessing the current state of protection. Available at: <http://skl.khpi.edu.ua/>

40. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. *Eastern-European Journal of Enterprise Technologies*, 3 (9 (105)), 6–19. <https://doi.org/10.15587/1729-4061.2020.205702>
41. Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C. et al. (2020). BIKE: Bit Flipping Key Encapsulation. Available at: [https://bikesuite.org/files/v4.1/BIKE\\_Spec.2020.10.22.1.pdf](https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf)
42. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M. et al. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. 2018 IEEE European Symposium on Security and Privacy (EuroS&P). <https://doi.org/10.1109/eurosp.2018.00032>
43. Supersingular Isogeny Key Encapsulation (2022). Available at: <https://sike.org/files/SIDH-spec.pdf>
44. HQC: Hamming Quasi-Cyclic An IND-CCA2 Code-based Public Key Encryption Scheme. NIST 4 th PQC Standardization Conference. Available at: <https://csrc.nist.gov/csrc/media/Presentations/2022/hqc-update/images-media/session-4-gaborit-hqc-pqc2022.pdf>

**DOI: 10.15587/1729-4061.2024.309387**

**HARDWARE-SOFTWARE IMPLEMENTATION OF A LOCAL WI-FI NETWORK FOR THE TRANSMISSION OF BIOMEDICAL SIGNALS (p. 34–43)**

**Yuliya Gerasimova**

M. Kozybayev North Kazakhstan University, Petropavlovsk, Republic of Kazakhstan

**ORCID:** <https://orcid.org/0000-0003-1877-383X>

**Victor Ivel**

M. Kozybayev North Kazakhstan University, Petropavlovsk, Republic of Kazakhstan

**ORCID:** <https://orcid.org/0000-0003-0854-3846>

**Sayat Moldakhmetov**

M. Kozybayev North Kazakhstan University, Petropavlovsk, Republic of Kazakhstan

**ORCID:** <https://orcid.org/0000-0003-2432-7983>

**Pavel Petrov**

M. Kozybayev North Kazakhstan University, Petropavlovsk, Republic of Kazakhstan

**ORCID:** <https://orcid.org/0000-0001-6669-5149>

The object of this study is a wireless local Wi-Fi network for broadcasting biomedical signals, its structure, and principles of construction. The task of minimizing the power consumption of a Wi-Fi transmitter has been addressed, which provides the possibility of building a wireless system for long-term monitoring of biomedical signals. As a result, a functional diagram of a wireless Holter monitoring system based on an ESP32 microcontroller was constructed, which includes a subsystem for setting up and diagnosing system units using MATLAB software packages, an ECG signal generator, and a multifunctional PCIe board from National Instruments. Evaluation criteria and methods for minimizing power consumption by an autonomous Wi-Fi transmitter have been proposed. Methods for synchronizing the working cycles of the transmitter and receiver of the Holter monitoring system were determined. A procedure for determining the optimal biosignal measurement frequency is presented, at which the distortion of ECG signals would be minimal, which means that the signal could be transmitted without losses. The concept of constructing an algorithm for implementing a program

for a Wi-Fi transmitter has been developed, ensuring parallel execution of ECG signal measurement operations and their transmission over a local network. The data from semi-naturalistic tests with an experimental Holter monitoring system with a pre-setup subsystem and using external measuring devices, a computer, and the MATLAB software environment are presented. A comparative analysis of the experimental data with primary ECG signals and ECG signals at the receiver output showed a fairly stable correspondence between the input and output ECG signals. The proposed algorithms make it possible to reduce the average current consumption of the ESP32 microcontroller to 50.5 mA. The results of the study demonstrate the possibility of constructing an energy-efficient wireless system for long-term monitoring of biomedical signals based on the Wi-Fi interface.

**Keywords:** biomedical signal, Holter monitoring, computer simulation, MATLAB system, Wi-Fi transmission, algorithm, ESP32 module.

**References**

1. Patel, S., Park, H., Bonato, P., Chan, L., Rodgers, M. (2012). A review of wearable sensors and systems with application in rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 9 (1). <https://doi.org/10.1186/1743-0003-9-21>
2. Bekbay, A., Alimbayeva, Z., Alimbayev, C., Bayanbay, N., Ozhikenov, K., Mukazhanov, Y. (2022). Development of an atrioventricular block prediction of method for portable heart monitoring system. *Eastern-European Journal of Enterprise Technologies*, 3 (5 (117)), 15–27. <https://doi.org/10.15587/1729-4061.2022.258791>
3. Subramaniam, S., Akay, M., Anastasio, M. A., Bailey, V., Boas, D., Bonato, P. et al. (2024). Grand Challenges at the Interface of Engineering and Medicine. *IEEE Open Journal of Engineering in Medicine and Biology*, 5, 1–13. <https://doi.org/10.1109/ojemb.2024.3351717>
4. Garudadri, H., Chi, Y., Baker, S., Majumdar, S., Baheti, P. K., Ballard, D. (2011). Diagnostic grade wireless ECG monitoring. 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society. <https://doi.org/10.1109/iembs.2011.6090194>
5. Pinho, F., Correia, J. H., Sousa, N. J., Cerqueira, J. J., Dias, N. S. (2014). Wireless and wearable eeg acquisition platform for ambulatory monitoring. 2014 IEEE 3rd International Conference on Serious Games and Applications for Health (SeGAH). <https://doi.org/10.1109/segah.2014.7067078>
6. Barrett, P. M., Komatireddy, R., Haaser, S., Topol, S., Sheard, J., Encinas, J. et al. (2014). Comparison of 24-hour Holter Monitoring with 14-day Novel Adhesive Patch Electrocardiographic Monitoring. *The American Journal of Medicine*, 127 (1), 95.e11–95.e17. <https://doi.org/10.1016/j.amjmed.2013.10.003>
7. Ivel, V. P., Gerasimova, Y. V., Moldakhmetov, S. S., Petrov, P. A., Gerasimov, I. A., Zainchkovskaya, K. V. (2019). Wireless three-channel Holter monitoring system. *IOP Conference Series: Materials Science and Engineering*, 537 (3), 032090. <https://doi.org/10.1088/1757-899x/537/3/032090>
8. Oresko, J. J., Duschl, H., Cheng, A. C. (2010). A Wearable Smartphone-Based Platform for Real-Time Cardiovascular Disease Detection Via Electrocardiogram Processing. *IEEE Transactions on Information Technology in Biomedicine*, 14 (3), 734–740. <https://doi.org/10.1109/titb.2010.2047865>
9. Frederix, I., Caiani, E. G., Dendale, P., Anker, S., Bax, J., Böhm, A. et al. (2019). ESC e-Cardiology Working Group Position Paper: Overcoming challenges in digital health implementation in car-

- diovascular medicine. *European Journal of Preventive Cardiology*, 26 (11), 1166–1177. <https://doi.org/10.1177/2047487319832394>
10. Mukhopadhyay, S. C. (2015). Wearable Sensors for Human Activity Monitoring: A Review. *IEEE Sensors Journal*, 15 (3), 1321–1330. <https://doi.org/10.1109/jsen.2014.2370945>
  11. Saad, C., Mostafa, B., Ahmadi, E., Abderrahmane, H. (2014). Comparative Performance Analysis of Wireless Communication Protocols for Intelligent Sensors and Their Applications. *International Journal of Advanced Computer Science and Applications*, 5 (4). <https://doi.org/10.14569/ijacsa.2014.050413>
  12. Franceschini, M., Pastrone, C., Spirito, M. A., Borean, C. (2013). On the performance of ZigBee Pro and ZigBee IP in IEEE 802.15.4 networks. 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). <https://doi.org/10.1109/wimob.2013.6673344>
  13. Al Hadidi, M., Al-Azzeh, J. S., Tklich, O., Odarchenko, R., Gnatyuk, S., Khokhlova, Y. (2017). ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing. *International Journal on Communications Antenna and Propagation (IRECAP)*, 7 (1), 48. <https://doi.org/10.15866/irecap.v7i1.10911>
  14. Weyer, S., Menden, T., Leicht, L., Leonhardt, S., Wartzek, T. (2015). Development of a wearable multi-frequency impedance cardiography device. *Journal of Medical Engineering & Technology*, 39 (2), 131–137. <https://doi.org/10.3109/03091902.2014.990161>
  15. Iqbal, S. M. A., Mahgoub, I., Du, E., Leavitt, M. A., Asghar, W. (2022). Development of a wearable belt with integrated sensors for measuring multiple physiological parameters related to heart failure. *Scientific Reports*, 12 (1). <https://doi.org/10.1038/s41598-022-23680-1>
  16. Barylo, H. I., Kuchmii, H. L., Kremer, I. P. (2013). ZigBee wireless communication system for telemedicine. *Eastern-European Journal of Enterprise Technologies*, 6 (12 (66)), 79–82. <https://doi.org/10.15587/1729-4061.2013.19741>
  17. Danbatta, S. J., Varol, A. (2019). Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. 2019 7th International Symposium on Digital Forensics and Security (ISDFS). <https://doi.org/10.1109/isdfs.2019.8757472>
  18. Filho, P., Schulz, F. (2013). Zigbee Network for Biomedical Signal Monitoring: Preliminary Results. *International journal of Engineering Research and Application*, 3 (5), 531–534.
  19. Fernández-López, H., Afonso, J. A., Correia, J. H., Simoes, R. (2012). Towards the design of efficient nonbeacon-enabled ZigBee networks. *Computer Networks*, 56 (11), 2714–2725. <https://doi.org/10.1016/j.comnet.2012.04.013>
  20. Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W. (2016). An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *Journal of Medical Systems*, 40 (12). <https://doi.org/10.1007/s10916-016-0644-9>
  21. Kaliaskarov, N., Ivel, V., Gerasimova, Y., Yugay, V., Moldakhmetov, S. (2020). Development of a distributed wireless Wi-Fi system for monitoring the technical condition of remote objects. *Eastern-European Journal of Enterprise Technologies*, 5(9(107)), 36–48. <https://doi.org/10.15587/1729-4061.2020.212301>
  22. Martínez-Suárez, F., García-Limón, J. A., Baños-Bautista, J. E., Alvarado-Serrano, C., Casas, O. (2023). Low-Power Long-Term Ambulatory Electrocardiography Monitor of Three Leads with Beat-to-Beat Heart Rate Measurement in Real Time. *Sensors*, 23 (19), 8303. <https://doi.org/10.3390/s23198303>
  23. Li, D., Liu, P., Sun, T., Li, L., Xue, Y. (2024). Real-Time PVC Recognition System Design Based on Multi-Parameter SE-ResNet. *IEEE Access*, 12, 70345–70356. <https://doi.org/10.1109/access.2024.3402359>
  24. Ivel, V. P., Gerasimova, Y. V., Moldakhmetov, S. S., Petrov, P. A., Gerasimov, I. A. (2020). Wireless Holter monitoring system with a dual-core processor. *IOP Conference Series: Materials Science and Engineering*, 919 (2), 022040. <https://doi.org/10.1088/1757-899x/919/2/022040>
  25. Data Sheet. AD8232. Available at: <https://www.micro-semiconductor.com/datasheet/29-AD8232ACPZ-R7.pdf>
  26. Sigit, R. (2014). Mini Wireless ECG for Monitoring Athletes' ECG Signal Based on Smartphone. *IOSR Journal of Engineering*, 4 (6), 13–18. <https://doi.org/10.9790/3021-04611318>
  27. Syahmi Md Dzahir, M. A., Seng Chia, K. (2023). Evaluating the Energy Consumption of ESP32 Microcontroller for Real-Time MQTT IoT-Based Monitoring System. 2023 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). <https://doi.org/10.1109/3ict60104.2023.10391358>
  28. Jung, J., Shin, S., Kang, M., Kang, K. H., Kim, Y. T. (2021). Development of Wearable Wireless Electrocardiogram Detection System using Bluetooth Low Energy. *Electronics*, 10 (5), 608. <https://doi.org/10.3390/electronics10050608>
  29. Koshekov, K., Kobenko, V., Koshekov, A., Moldakhmetov, S. (2020). Hand-written character structure recognition technology on the basis of identification measurements. *ARNP Journal of Engineering and Applied Sciences*, 15 (21), 2555–2562. Available at: [https://www.arnpjournals.org/jeas/research\\_papers/rp\\_2020/jeas\\_1120\\_8390.pdf](https://www.arnpjournals.org/jeas/research_papers/rp_2020/jeas_1120_8390.pdf)

DOI: 10.15587/1729-4061.2024.310372

**SEGMENTATION OF IMAGE FROM A FIRST-PERSON-VIEW UNMANNED AERIAL VEHICLE BASED ON A SIMPLE ANT ALGORITHM (p. 44–55)**

**Hennadii Khudov**

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ORCID: <https://orcid.org/0000-0002-3311-2848>

**Illia Hridasov**

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ORCID: <https://orcid.org/0000-0003-4886-4468>

**Irina Khizhnyak**

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ORCID: <https://orcid.org/0000-0003-3431-7631>

**Iryna Yuzova**

Civil Aviation Institute, Kharkiv, Ukraine

ORCID: <https://orcid.org/0000-0002-0013-5808>

**Yuriy Solomonenko**

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ORCID: <https://orcid.org/0000-0002-6503-7475>

The object of this study is the process of image segmentation from the First Person View (FPV) of an unmanned aerial vehicle (UAV). The main hypothesis of the study assumes that the use of a simple ant algorithm could ensure the necessary quality of the segmented image.

The segmentation method, unlike the known ones, takes into account the number of ants in the image, weight, initial amount and evaporation rate of the pheromone, the “greediness” of the algorithm and provides:

– preliminary selection of individual channels of the Red-Green-Blue (RGB) color space;

- preliminary placement of ants according to the uniform law;
- determining the routes of ants;
- taking into account the attractiveness of the route for each ant;
- change (adjustment) in the concentration of ant pheromones;
- calculation of the probability of movement (transition) of the ant on the movement route;
- determination of the objective function at the  $j$ -th iteration and its minimization;
- determining the coordinates of the route of movement (movement) of ants;
- verification of the fulfillment of the stop condition;
- determination of the best routes found by ants;
- calculation of the brightness of the pixels of the segmented image in each channel of the RGB color space;
- further combining the results of channel segmentation.

An experimental study of image segmentation from UAV FPV based on a simple ant algorithm was conducted. The specified object of interest on the segmented image has a certain structure, unevenness of the contours, and can be further used for decoding, categorization, etc. Unlike the object of interest, the background (“garbage” objects) in the segmented image do not have a stable structure and can be further filtered out.

It has been established that the segmented image by the known method based on the gradient module has a low contrast value, there are gaps in the segmented pixels of the object of interest. A segmented image using a method based on a simple ant algorithm is free from that drawback.

**Keywords:** UAV FPV, segmentation, ant movement, pheromone, route attractiveness, objective function.

## References

1. First-person view (FPV) drones. Available at: <https://www.peoplesproject.com/en/first-person-view-drones/>
2. Hashimov, E., Sabziev, E., Huseynov, B., Huseynov, M. (2023). Mathematical aspects of determining the motion parameters of a target by UAV. *Advanced Information Systems*, 7 (1), 18–22. <https://doi.org/10.20998/2522-9052.2023.1.03>
3. Barabash, O., Kyriano, A. (2023). Development of control laws of unmanned aerial vehicles for performing group flight at the straight-line horizontal flight stage. *Advanced Information Systems*, 7 (4), 13–20. <https://doi.org/10.20998/2522-9052.2023.4.02>
4. Kaufmann, E., Bauersfeld, L., Loquercio, A., Müller, M., Koltun, V., Scaramuzza, D. (2023). Champion-level drone racing using deep reinforcement learning. *Nature*, 620 (7976), 982–987. <https://doi.org/10.1038/s41586-023-06419-4>
5. Military Imaging and Surveillance Technology (MIST) (Archived). Available at: <https://www.darpa.mil/program/military-imaging-and-surveillance-technology>
6. LLano, E. G., Roig, D. O., Cabrera, Y. C. (2018). Unsupervised Segmentation of Agricultural Crops in UAV RGB Images. *Revista Cubana de Ciencias Informáticas*, 12 (4), 17–28. Available at: <https://www.redalyc.org/journal/3783/378365912002/html/>
7. Zhu, S., Zhao, J., Guo, L. (2014). Rival Penalized Image Segmentation. *Journal of Multimedia*, 9 (5). <https://doi.org/10.4304/jmm.9.5.736-745>
8. Kinahan, J., Smeaton, A. F. (2021). Image Segmentation to Identify Safe Landing Zones for Unmanned Aerial Vehicles. *Proceedings of the 29th Irish Conference on Artificial Intelligence and Cognitive Science AICS'2021*. <https://doi.org/10.48550/arXiv.2111.14557>
9. Pap, M., Kiraly, S., Moljak, S. (2019). Investigating the usability of UAV obtained multispectral imagery in tree species segmentation. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLII-2/W18, 159–165. <https://doi.org/10.5194/isprs-archives-xlii-2-w18-159-2019>
10. Treboux, J., Genoud, D. (2018). Improved Machine Learning Methodology for High Precision Agriculture. 2018 Global Internet of Things Summit (GIoTS). <https://doi.org/10.1109/giots.2018.8534558>
11. Parsons, M., Bratanov, D., Gaston, K. J., Gonzalez, F. (2018). UAVs, Hyperspectral Remote Sensing, and Machine Learning Revolutionizing Reef Monitoring. *Sensors*, 18 (7), 2026. <https://doi.org/10.3390/s18072026>
12. Lin, Z., Doyog, N. D., Huang, S.-F., Lin, C. (2021). Segmentation and Classification of UAV-based Orthophoto of Watermelon Field Using Support Vector Machine Technique. 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS. <https://doi.org/10.1109/igarss47720.2021.9553715>
13. Miyamoto, H., Momose, A., Iwami, S. (2018). UAV image classification of a riverine landscape by using machine learning techniques. *Geophysical Research Abstracts*, 20, EGU2018-5919. Available at: <https://meetingorganizer.copernicus.org/EGU2018/EGU2018-5919.pdf>
14. Son, J., Jung, I., Park, K., Han, B. (2015). Tracking-by-Segmentation with Online Gradient Boosting Decision Tree. 2015 IEEE International Conference on Computer Vision (ICCV). <https://doi.org/10.1109/iccv.2015.350>
15. Huang, L., Song, J., Yu, X., Fang, L. (2019). Unmanned Aerial Vehicle Remote Sensing Image Segmentation Method by Combining Superpixels with multi-features Distance Measure. *IOP Conference Series: Earth and Environmental Science*, 234, 012022. <https://doi.org/10.1088/1755-1315/234/1/012022>
16. Zimudzi, E., Sanders, I., Rollings, N., Omlin, C. (2018). Segmenting mangrove ecosystems drone images using SLIC superpixels. *Geocarto International*, 34 (14), 1648–1662. <https://doi.org/10.1080/10106049.2018.1497093>
17. Xiang, S., Xu, J., Zhao, J., Li, Y., Zhang, S. (2015). A novel LBP-Mean shift segmentation algorithm for UAV remote sensing images based on LBP textural features and improved Mean shift algorithm. *Proceedings of the 3rd International Conference on Mechatronics, Robotics and Automation*. <https://doi.org/10.2991/icmra-15.2015.79>
18. Wang, H., Shen, Z., Zhang, Z., Xu, Z., Li, S., Jiao, S., Lei, Y. (2021). Improvement of Region-Merging Image Segmentation Accuracy Using Multiple Merging Criteria. *Remote Sensing*, 13 (14), 2782. <https://doi.org/10.3390/rs13142782>
19. Shen, X., Teng, Y., Fu, H., Wan, Z., Zhang, X. (2020). Crop identification using UAV image segmentation. *Second Target Recognition and Artificial Intelligence Summit Forum*. <https://doi.org/10.1117/12.2552195>
20. Bhatnagar, S., Gill, L., Ghosh, B. (2020). Drone Image Segmentation Using Machine and Deep Learning for Mapping Raised Bog Vegetation Communities. *Remote Sensing*, 12 (16), 2602. <https://doi.org/10.3390/rs12162602>
21. Marcu, A., Licaret, V., Costea, D., Leordeanu, M. (2021). Semantics Through Time: Semi-supervised Segmentation of Aerial Videos with Iterative Label Propagation. *Computer Vision – ACCV 2020*, 537–552. [https://doi.org/10.1007/978-3-030-69525-5\\_32](https://doi.org/10.1007/978-3-030-69525-5_32)
22. Khudov, H., Makoveichuk, O., Butko, I., Gyrenko, I., Stryhun, V., Bilous, O. et al. (2022). Devising a method for segmenting camouflaged military equipment on images from space surveillance systems using a genetic algorithm. *Eastern-European Journal of Enterprise Technologies*, 3 (9 (117)), 6–14. <https://doi.org/10.15587/1729-4061.2022.259759>

23. Khudov, H., Makoveichuk, O., Khizhnyak, I., Oleksenko, O., Khazhanets, Y., Solomonenko, Y. et al. (2022). Devising a method for segmenting complex structured images acquired from space observation systems based on the particle swarm algorithm. *Eastern-European Journal of Enterprise Technologies*, 2 (9 (116)), 6–13. <https://doi.org/10.15587/1729-4061.2022.255203>
24. Khudov, H., Ruban, I., Makoveichuk, O., Pevtsov, H., Khudov, V., Khizhnyak, I. et al. (2020). Development of methods for determining the contours of objects for a complex structured color image based on the ant colony optimization algorithm. *EUREKA: Physics and Engineering*, 1, 34–47. <https://doi.org/10.21303/2461-4262.2020.001108>
25. 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. <https://doi.org/10.15587/1729-4061.2019.174576>
26. de O. Bastos, L., Liatsis, P., Conci, A. (2008). Automatic texture segmentation based on k-means clustering and efficient calculation of co-occurrence features. 2008 15th International Conference on Systems, Signals and Image Processing. <https://doi.org/10.1109/iwSSIP.2008.4604387>
27. Hung, C.-C., Song, E., Lan, Y. (2019). Image Texture, Texture Features, and Image Texture Classification and Segmentation. *Image Texture Analysis*, 3–14. [https://doi.org/10.1007/978-3-030-13773-1\\_1](https://doi.org/10.1007/978-3-030-13773-1_1)
28. Tian, Y., Li, Y., Liu, D., Luo, R. (2016). FCM texture image segmentation method based on the local binary pattern. 2016 12th World Congress on Intelligent Control and Automation (WCICA). <https://doi.org/10.1109/wcica.2016.7578571>
29. Gorokhovatskyi, V., Peredrii, O., Tvoroshenko, I., Markov, T. (2023). Distance matrix for a set of structural description components as a tool for image classifier creating. *Advanced Information Systems*, 7 (1), 5–13. <https://doi.org/10.20998/2522-9052.2023.1.01>
30. Hurin, A., Khudov, H., Kostyria, O., Maslenko, O., Siadrystyi, S. (2024). Comparative analysis of spectral anomalies detection methods on images from on-board remote sensing systems. *Advanced Information Systems*, 8 (2), 48–57. <https://doi.org/10.20998/2522-9052.2024.2.06>
31. Khudov, H., Khizhnyak, I., Glukhov, S., Shamrai, N., Pavlii, V. (2024). The method for objects detection on satellite imagery based on the firefly algorithm. *Advanced Information Systems*, 8 (1), 5–11. <https://doi.org/10.20998/2522-9052.2024.1.01>
32. Mohammed Jabbar, A., Ku-Mahamud, K. R., Sagban, R. (2020). An improved ACS algorithm for data clustering. *Indonesian Journal of Electrical Engineering and Computer Science*, 17 (3), 1506. <https://doi.org/10.11591/ijeecs.v17.i3.pp1506-1515>
33. Jablonowski, M. (2020). Beyond drone vision: the embodied telepresence of first-person-view drone flight. *The Senses and Society*, 15 (3), 344–358. <https://doi.org/10.1080/17458927.2020.1814571>
34. Saha, A., Kumar, A., Sahu, A. K. (2017). FPV drone with GPS used for surveillance in remote areas. 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). <https://doi.org/10.1109/icrcicn.2017.8234482>
35. Siddiqui, W. A. (2024). Design and Fabrication of FPV Racing Drone. *Journal of Mechanical and Construction Engineering (JMCE)*, 4 (1), 1–8. <https://doi.org/10.54060/a2zjournals.jmce.38>
36. Salamh, F. E., Karabiyik, U., Rogers, M. K., Matson, E. T. (2021). A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges. *Drones*, 5 (2), 42. <https://doi.org/10.3390/drones5020042>
37. Karp, S. (2023). Introduction to FPV drones. Available at: <https://www.thedroningcompany.com/blog/introduction-to-fpv-drones>
38. Defense industry of Ukraine. Available at: <https://mil.in.ua/en/news/>

**DOI: 10.15587/1729-4061.2024.310521**

**ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПРОГРАМНИХ РЕАЛІЗАЦІЙ ЕЛЕКТРОННОГО ПІДПISУ FALCON ВІД АТАК НА ОСНОВІ ШУМУ ОБЧИСЛЕНЬ З ПЛАВАЮЧОЮ ТОЧКОЮ (с. 6–17)**

**О. Г. Качко, Ю. І. Горбенко, С. О. Кандій, Є. Ю. Каптьол**

Об'єктом дослідження є електронні підписи. Схема електронного підпису Falcon є одним з фіналістів конкурсу NIST з квантово-стійкої криптографії. Однією з її ключових особливостей є використання обчислень з плаваючою крапкою, котре призводить до можливості атаки відновлення ключів при наявності двох неспівпадаючих підписів, сформованих в особливих умовах. Робота присвячена проблемі удосконалення ЕП (електронного підпису) Falcon з метою унеможливлення таких атак, а також використання обчислень з фіксованою точкою замість обчислень з плаваючою точкою в схемі ЕП Falcon. Головним результатом роботи є пропозиції щодо методів покращення безпеки Falcon від атак, заснованих на особливостях використання обчислень з плаваючою точкою. Запропоновані методи покращення безпеки відрізняються від інших використанням обчислень з фіксованою крапкою з конкретним експериментально визначеним масштабом в одному випадку. В іншому випадку – пропозиціями щодо модифікації операцій в ході виконання яких виникають умови для виконання атаки на рівні реалізації. У результаті проведеного аналізу було уточнено ймовірності вдалого проведення атаки на відновлення таємного ключа для еталонної реалізації ЕП Falcon. Було локалізовано конкретні місця в коді, що роблять атаку можливою та запропоновано модифікацію коду, що робить проведення атаки неможливим. Додатково було визначено необхідний масштаб для обчислень з фіксованою точкою, при якому можливо повністю позбутися обчислень з плаваючою точкою. Отримані результати можуть бути використані для якісного покращення безпеки існуючих ЕП. Це дозволить створити надійніші та більш захищені інформаційні системи, що використовують ЕП. Крім того, отримані результати можуть бути впроваджені в існуючі системи для забезпечення їхньої стійкості до сучасних загроз.

**Ключові слова:** квантово-стійкі перетворення, Falcon, плаваюча точка, фіксована точка, NIST, NTRU.

**DOI: 10.15587/1729-4061.2024.310547**

**РОЗРОБКА ПРИНЦИПІВ ФУНКЦІОНУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПЕРЕДАВАННЯ ДАНИХ БЕЗПРОВІДНИМИ КАНАЛАМИ ЗВ'ЯЗКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ (с. 18–33)**

**С. П. Євсєєв, С. В. Мілевський, В. Є. Сокол, А. П. Волобуєв, В. В. Єманов, Л. В. Дакова, М. М. Браїловський, І. Р. Рагімова, В. І. Кравченко, О. Ю. Чернявський**

Розвиток систем передавання даних на основі безпроводних каналів радіозв'язку дозволив будувати принципово нових мереж – mesh-мереж, які використовуються не тільки в смарт-технологіях, а є основою побудови кіберфізичних та соціокіберфізичних систем (об'єктів критичної інфраструктури). Об'єктом є процес забезпечення надійної та безпечної передачі даних на основі використання безпроводних каналів радіозв'язку. Для забезпечення ознак завадостійкості та безпеки автоматизованої системи передачі даних запропонована математична модель функціонування системи захисту інформаційних ресурсів. Для визначення загроз використовується уніфікований класифікатор та методика оцінки потокового стану, які враховують гібридність та синергію цільових (змішаних) атак на канали зв'язку. Визначається критичні точки елементів інфраструктури, а також інформація, яка циркулює та/або зберігається. Враховується оцінка виконання вимог регуляторів, як міжнародних, так й державних нормативних актів, та наявність та спроможність елементів системи безпеки забезпечити необхідний рівень захисту елементів інфраструктури. Запропонований підхід дозволяє визначати: коефіцієнти інформаційної та внутрішньої доступності безпроводного каналу радіозв'язку, векторний потенціал магнітного поля, що запізнюється, як результат роботи на передачу даних. При оцінюванні коефіцієнту внутрішньої доступності безпроводного каналу радіозв'язку запропоновано враховувати когерентне приймання сигналу. При цьому коефіцієнт завадозахищеності безпроводного каналу радіозв'язку набагато більше 1, що забезпечує достатній захист інформації. Запропоновано технічне рішення, яке дозволить наблизити рівні конфіденційності, цілісності, автентичності та достовірності безпроводного каналу радіозв'язку до 100 %.

**Ключові слова:** система передачі даних, випромінювач радіосигналу, магнітне поле, радіомоніторинг, соціокіберфізична система.

**DOI: 10.15587/1729-4061.2024.309387**

**АППАРАТНО-ПРОГРАМНА РЕАЛІЗАЦІЯ ЛОКАЛЬНОЇ WI-FI-СЕТИ ДЛЯ ПЕРЕДАЧІ БІОМЕДИЦИНСКИХ СИГНАЛІВ (с. 34–43)**

**Yuliya Gerassimova, Victor Ivel, Sayat Moldakhmetov, Pavel Petrov**

Об'єктом дослідження є бездротова локальна Wi-Fi мережа для трансляції біомедичних сигналів, її структура та принципи побудови. Вирішується проблема мінімізації енергоспоживання Wi-Fi передавачем, що забезпечує можливість створення бездротової системи тривалого моніторингу біомедичних сигналів. У результаті розроблено функціональну схему бездротової системи Холтерівського моніторингу на базі мікроконтролера ESP32, яка включає в свою структуру підсистему налаштування та діагностики блоків системи з використанням програмних пакетів MatLab, генератора ЕКГ-сигналів та багатофункціональної PCIe плати від компанії National Instruments. Запропоновано критерії оцінки та способи мінімізації енергоспоживання автономним Wi-Fi передавачем. Визначено методи синхронізації робочих циклів передавача та приймача системи Холтерівського моніторингу.



Представлено методику визначення оптимальної частоти вимірювання біосигналу, за якої спотворення ЕКГ-сигналів буде мінімальним, що забезпечує передачу сигналу без втрат. Розроблено концепцію побудови алгоритму реалізації програми для Wi-Fi передавача, яка забезпечує паралельність виконання операцій вимірювання ЕКГ-сигналів та їх передачі по локальній мережі. Представлено дані напівнатурних випробувань з експериментальною системою Холтерівського моніторингу з підсистемою попереднього налаштування та з використанням зовнішніх вимірювальних приладів, комп'ютера і програмного середовища MatLab. Порівняльний аналіз даних експериментів з первинними ЕКГ-сигналами та ЕКГ-сигналами на виході приймача показав досить стійку відповідність вхідних і вихідних ЕКГ-сигналів. Запропоновані алгоритми дозволяють знизити середній струм споживання мікроконтролера ESP32 до 50,5 мА. Результати проведеного дослідження показують можливість побудови енергоефективної бездротової системи тривалого моніторингу біомедичних сигналів на основі Wi-Fi інтерфейсу.

**Ключові слова:** біомедичний сигнал, Холтерівське моніторування, комп'ютерне моделювання, система MatLab, Wi-Fi передача, алгоритм, модуль ESP32.

**DOI: 10.15587/1729-4061.2024.310372**

## **СЕГМЕНТУВАННЯ ЗОБРАЖЕННЯ З FIRST-PERSON-VIEW БЕЗПЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ НА ОСНОВІ ПРОСТОГО МУРАШИНОГО АЛГОРИТМУ (с. 44–55)**

**Г. В. Худов, І. Ю. Грідасов, І. А. Хижняк, І. Ю. Юзова, Ю. С. Соломоненко**

Об'єктом дослідження є процес сегментування зображення з First Person View (FPV) безпілотного літального апарату (БПЛА). Основна гіпотеза дослідження полягала в тому, що використання простого мурашиного алгоритму дозволить забезпечити необхідну якість сегментованого зображення.

Метод сегментування, на відміну від відомих, враховує кількість мурах на зображенні, вагу, початкову кількість та швидкість випаровування феромону, «жадібність» алгоритму та передбачає:

- попереднє виділення окремих каналів кольорового простору Red-Green-Blue (RGB);
- попереднє розміщення мурах по рівномірному закону;
- визначення маршрутів мурах;
- врахуванням привабливості маршруту для кожної мурахи;
- зміну (корегування) концентрації феромонів мурах;
- розрахунок ймовірності руху (переходу) мурахи на маршруті руху;
- визначення цільової функції на  $j$ -ій ітерації та її мінімізація;
- визначення координат маршруту руху (переміщення) мурах;
- перевірка виконання умови зупинки;
- визначення кращих знайдених маршрутів мурах;
- розрахунок яскравостей пікселів сегментованого зображення в кожному каналі кольорового простору RGB;
- подальшим поєднанням результатів поканального сегментування.

Проведено експериментальне дослідження сегментування зображення з FPV БПЛА на основі простого мурашиного алгоритму. Наведений об'єкт інтересу на сегментованому зображенні має певну структуру, нерозривність контурів та може бути в подальшому використаний для проведення дешифрування, класифікації тощо. На відміну від об'єкту інтересу, фонові («сміттєві» об'єкти) на сегментованому зображенні не мають сталої структури та можуть бути в подальшому відсіянні.

Встановлено, що сегментоване зображення відомим методом на основі модуля градієнту має низьке значення контрасту, є пропуски сегментованих пікселів об'єкту інтересу. Сегментоване зображення методом на основі простого мурашиного алгоритму вільне від зазначеного недоліку.

**Ключові слова:** FPV БПЛА, сегментування, рух мурах, феромон, привабливість маршруту, цільова функція.