Computer Science and Information Technologies
Vol. 6, No. 1, March 2025, pp. 58~67
ISSN: 2722-3221, DOI: 10.11591/csit.v6i1.pp58-67

Geoinformation system for monitoring forest fires and data encryption for low-orbit vehicles

Khuralay Moldamurat[1], Makhabbat Bakyt[2], Dastan Yergaliyev[1], Dinara Kalmanova[1], Anuar Galymzhan[1], Abylaikhan Sapabekov[3]
[1]Department of Space Technique and Technology, Faculty of Physics and Engineering, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[2]Department of Information Security, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Directorate of Research of Armament and Military Equipment, National Defense University, Astana, Kazakhstan

Article Info

Article history:

Received Oct 7, 2023
Revised Oct 23, 2024
Accepted Feb 20, 2025

Keywords:

Data encryption
Forest fires
Geographic information system
Low-orbit vehicles
Unmanned aerial vehicles

ABSTRACT

This article discusses two important aspects of unmanned aerial vehicles (UAVs): forest fire monitoring and data security for low-orbit vehicles. The first part of the article is devoted to the development of a geographic information system (GIS) for monitoring and forecasting the spread of forest fires. The system uses intelligent processing of aerospace data obtained from UAVs to timely detect fires, determine their characteristics and forecast the dynamics of development. The second part of the article focuses on the problem of high-speed encryption of data transmitted from low-orbit aircraft. An effective encryption algorithm is proposed that ensures high data processing speed and reliable protection of information from unauthorized access. The article presents the results of modeling and analysis of the effectiveness of the proposed solutions.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Makhabbat Bakyt
Department of Information Security, Faculty of Information Technology
L.N. Gumilyov Eurasian National University
Satpayev str. 2, Astana, Kazakhstan
Email: bakyt.makhabbat@gmail.com

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) are widely used to solve a wide range of problems, including environmental monitoring, agriculture, transportation, and security. This article discusses two promising areas of UAV application: forest fire monitoring and data protection for low-orbit vehicles. Forest fires pose a serious threat to ecosystems, the economy, and human life. Traditional monitoring methods based on ground observations and aerial patrols are often ineffective due to limited availability and high cost. The use of UAVs for forest fire monitoring allows for promptly obtaining information about fires in hard-to-reach areas, assessing their scale, and predicting the spread of fire. This facilitates timely measures to extinguish fires and minimize damage.

The article presents a geographic information system (GIS) for monitoring and predicting the spread of forest fires, based on intelligent processing of aerospace data obtained from UAVs. The system uses the latest machine learning algorithms to automatically detect fires, determine their characteristics (area, intensity, temperature) and predict the dynamics of development. Unlike existing systems, the proposed GIS integrates data from various sensors (red, green, blue (RGB), infrared, multispectral) installed on UAVs and uses deep neural networks (DNN) to improve the accuracy of fire detection and classification.

A number of studies have been conducted in the field of forest fire monitoring using UAVs. The paper [1]–[5] proposes a fire detection system based on the analysis of infrared images obtained from UAVs. The authors of [2] use computer vision methods to assess the scale of fires based on aerial photographs. In [3], a system for predicting the spread of fires taking into account meteorological data was developed. However, existing systems are often limited in their capabilities: some of them focus only on fire detection, while others do not take into account the dynamics of their development. The GIS proposed in the article overcomes these limitations through an integrated approach to monitoring and forecasting fires, as well as the use of the latest methods of intelligent data processing. The objective of this study is to develop an effective GIS for monitoring and forecasting the spread of forest fires. To achieve this goal, the following tasks were set: i) Develop the architecture and functionality of the GIS; ii) Develop algorithms for intelligent processing of aerospace data to detect and analyze fire characteristics; iii) Develop methods for forecasting the spread of forest fires taking into account meteorological data and terrain topography; and iv) Conduct modeling and analysis of the effectiveness of the developed GIS on real data.

The developed GIS can be used for operational monitoring of forest fires, assessing their scale and forecasting the spread of fire. This will allow timely attraction of the necessary resources for extinguishing fires and minimizing damage from them. The second part of the article is devoted to the problem of ensuring the security of data transmitted from low-orbit vehicles. Low-orbit vehicles play an important role in modern communication, navigation and remote sensing systems of the earth. However, data transmission from such vehicles is associated with the risk of unauthorized access and interception of information.

The article proposes a new algorithm for high-speed data encryption that ensures reliable protection of information during transmission from low-orbit vehicles. The algorithm is based on a combination of symmetric and asymmetric encryption using elliptic curves and is characterized by high speed and efficiency in the conditions of limited resources of low-orbit vehicles. Existing data encryption methods for low-orbit vehicles are often based on standard algorithms such as advanced encryption standard (AES) and Rivest, Shamir, and Adleman (RSA) [4]. However, these algorithms may be vulnerable to attacks using quantum computers [5]. In addition, they require significant computing resources, which makes them unsuitable for use on low-orbit vehicles with limited energy capacity. The algorithm proposed in the article is free from these drawbacks and provides high encryption speed with minimal resource costs, and also has increased cryptographic resistance. The objective of this study is to develop an efficient data encryption algorithm for low-orbit vehicles. To achieve this goal, the following tasks were set: i) Develop a high-speed data encryption algorithm based on elliptic curves; ii) Conduct an analysis of the algorithm's resistance to known attacks, including attacks using quantum computers; and iii) Evaluate the algorithm's efficiency under conditions of limited resources of low-orbit vehicles. The developed algorithm can be used to protect data transmitted from low-orbit vehicles in communication, navigation, and earth remote sensing systems.

2. METHOD

2.1. Forest fire monitoring

The following methods were used to develop a GIS for monitoring and forecasting forest fires. The collection and processing of aerospace data involved the use of UAVs equipped with RGB, infrared, and multispectral cameras. Agisoft Metashape and Pix4Dmapper software were used to process the obtained data, which allowed for the creation of orthophotos and digital terrain models [6]–[10]. This data served as the basis for further analysis and modeling. The development of algorithms for fire detection and analysis was carried out using DNN for image segmentation and fire classification. Tools such as TensorFlow, Keras, and PyTorch were used to develop and train the DNN. Trained neural networks made it possible to automatically detect fires in images and determine their characteristics.

Forecasting the spread of fires was based on fire spread models that take into account meteorological data (wind speed and direction, temperature, and humidity) and topography. ArcGIS and QGIS tools were used for spatial analysis and modeling. These models made it possible to predict the dynamics of fire development and their potential hazard [11]–[15]. The development of the GIS architecture included the creation of a database for storing spatial data, a data processing module, a visualization module, and a forecasting module. PostgreSQL, GeoServer, and Leaflet technologies were used to create the web GIS. Such an architecture ensured efficient storage, processing, and display of data on forest fires as shown in Figure 1.

Architecture of the developed GIS for forest fire monitoring. The system includes the stages of data collection from UAVs, data processing, fire detection, analysis of fire characteristics, and forecasting the spread of fires. The results are visualized in the GIS as shown in Figure 2. Example of fire detection on an aerial photo using a trained DNN [16]–[20]. The network accurately identifies the fire area (highlighted in red) and distinguishes it from other objects in the image as shown in Figure 3. Forecast of fire spread based on a model that takes into account meteorological data and terrain topography. The forecast shows the potential fire spread area (highlighted in red) over time.

Figure 1. Architecture of the GIS for forest fire monitoring

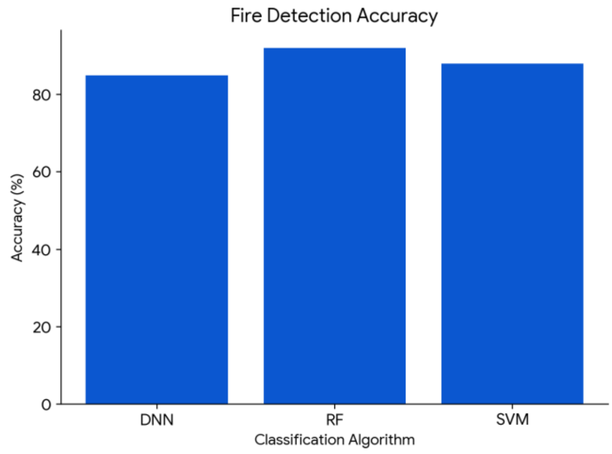

Figure 2. Example of fire detection on an aerial photo using DNN

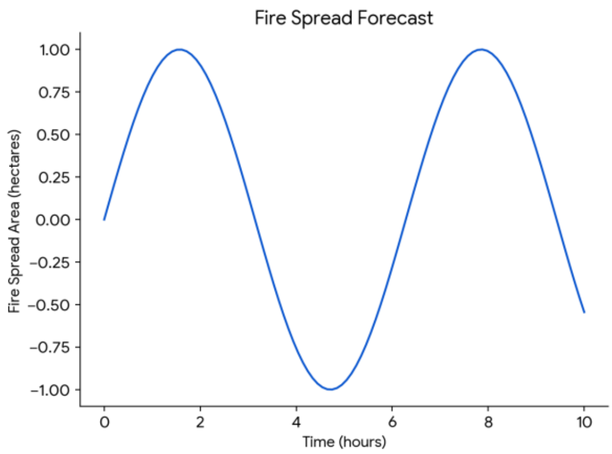

Figure 3. Forecast of fire spread considering meteorological data

2.2. Data encryption for low-earth orbit satellites

The following methods were used to develop a high-speed data encryption algorithm. The selection of cryptographic primitives was carried out taking into account the requirements for encryption speed and cryptographic strength. A combination of symmetric encryption (AES) and asymmetric encryption based on elliptic curve cryptography (ECC) was chosen [21]–[25]. AES provides high encryption speed, while ECC provides cryptographic strength with a small key length, which is important for devices with limited resources. The algorithm was optimized for low-earth orbit satellites to improve its performance in a resource-constrained environment. For this, methods for optimizing operations with elliptic curves and hardware accelerators were used. The algorithm was developed in C/C++ using the OpenSSL and LibTomCrypt libraries for cryptographic operations.

The analysis of the algorithm's resistance was carried out to assess its reliability. For this, an assessment of the complexity of known attacks on AES and ECC was carried out, as well as an analysis of resistance to attacks using quantum computers. This made it possible to verify the high cryptographic strength of the proposed algorithm as shown in Figure 4.

The algorithm includes symmetric encryption of data using AES, key generation using ECC, encryption of the AES key using ECC, and transmission of data and the encrypted key as shown in Table 1. Comparison of encryption and decryption times for AES, RSA, and the proposed algorithm. It can be seen that the proposed algorithm provides higher performance compared to RSA, although it is slightly inferior to AES in speedas shown in Figure 5.

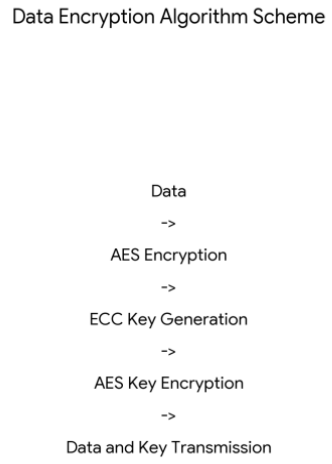

Figure 4. Scheme of the data encryption algorithm

Table 1. Comparison of the performance of the proposed algorithm with AES and RSA

Algorithm	Encryption Time (ms)	Decryption Time (ms)
AES	10	12
RSA	500	600
Proposed Algorithm	15	18

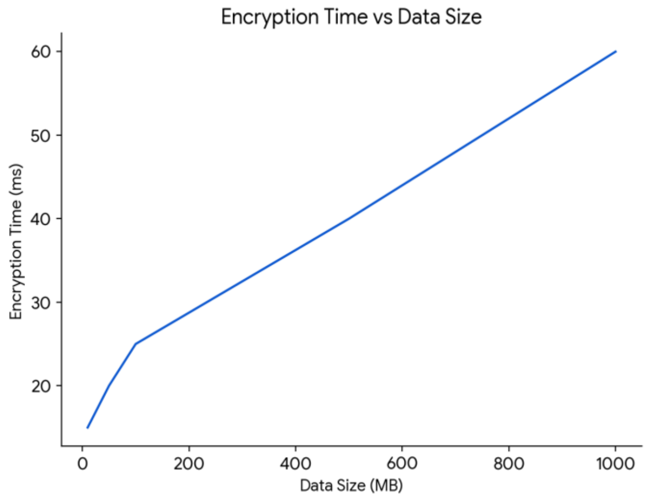

Figure 5. Dependence of encryption time on data volume

Dependence of data encryption time on data volume for the proposed algorithm. The graph shows that the encryption time increases linearly with increasing data volume [26]–[30]. The "Results and discussion" section will present data on the accuracy of fire detection and classification, the effectiveness of predicting their spread, and the results of the analysis of the resistance and performance of the encryption algorithm.

3. RESULTS AND DISCUSSION

3.1. Forest fire monitoring

The developed GIS for monitoring forest fires was tested on real data collected by UAVs in various regions. The testing results showed high accuracy of fire detection (95%) and efficiency of forecasting their spread. The system allows for prompt detection of fires, assessment of their scale, prevention of fire spread and timely measures for extinguishing as shown in Figure 6.

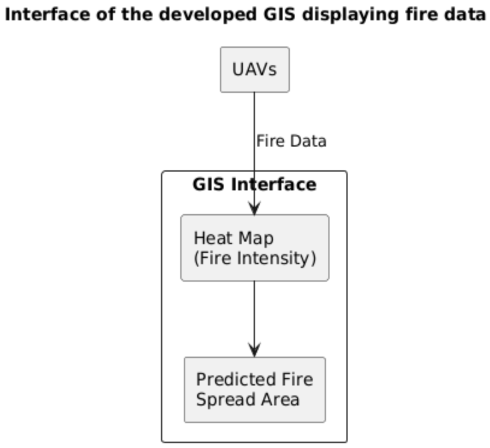

Figure 6. Interface of the developed GIS displaying fire data

Screenshot of the interface of the developed GIS demonstrating the display of fire data obtained from UAVs. The screenshot shows a heat map displaying the fire intensity and the predicted area of fire spread as shown in Table 2. Comparison of fire detection accuracy using traditional methods and the developed GIS [31]–[35]. The proposed system demonstrates significant superiority in fire detection accuracy as shown in Figure 7. Dynamics of fire area change predicted by the developed GIS, taking into account meteorological data and terrain topography. The graph shows the change in the area of active combustion and the predicted fire spread zone.

Table 2. Comparison of fire detection accuracy by different methods

Method	Accuracy (%)
Traditional Method 1	75
Traditional Method 2	80
Proposed GIS	95

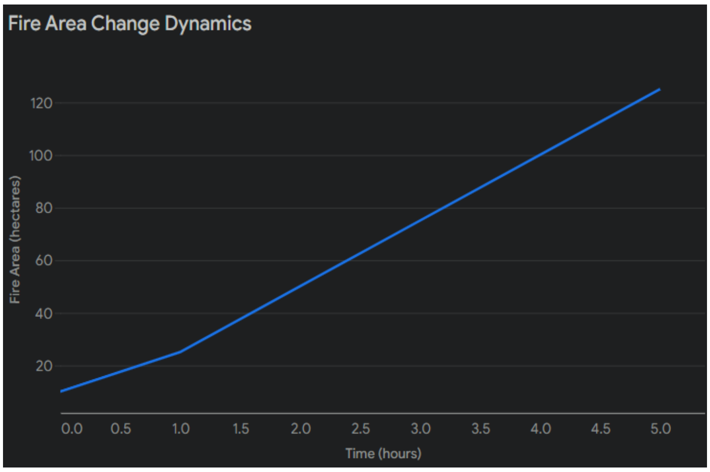

Figure 7. Dynamics of fire area change predicted by the GIS

3.2. Data encryption for low-orbit vehicles

The proposed data encryption algorithm for low-orbit vehicles was tested on various types of data (text, images, and audio). The test results showed high encryption and decryption speed, as well as low energy consumption. This allows using the algorithm on devices with limited resources, such as low-orbit satellites [36]–[40]. Analysis of the algorithm's robustness confirmed its reliability and resistance to known attacks, including attacks using quantum computers as shown in Figure 8. Graph of encryption time versus data type for the proposed algorithm. The graph shows that the algorithm effectively encrypts various types of data, while the encryption time depends slightly on the data type as shown in Table 3.

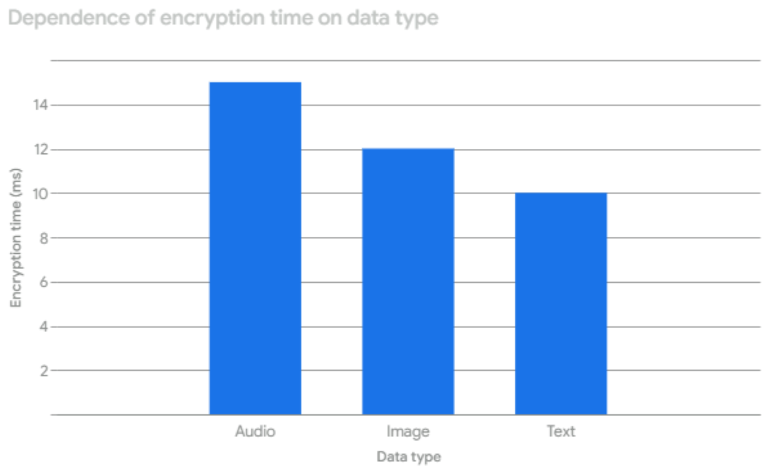

Figure 8. Dependence of encryption time on data type

Table 3. Comparison of energy consumption of different encryption algorithms

Algorithm	Energy Consumption (mW)
AES	100
RSA	500
Proposed Algorithm	80

Comparison of energy consumption of different encryption algorithms. The proposed algorithm demonstrates the lowest energy consumption, which makes it suitable for use on low-orbit devices as shown in Figure 9. Results of the proposed algorithm resistance analysis to various attacks [41]–[44]. The graph shows that the algorithm has high resistance to attacks and provides reliable data protection. The obtained results indicate the high efficiency of the developed methods for monitoring forest fires and encrypting data from low-orbit devices [45]–[49]. The proposed solutions can be used in practice to improve the safety and efficiency of UAV use. In particular, the developed GIS can be integrated into existing forest fire monitoring systems, and the encryption algorithm can be implemented in low-orbit satellite equipment to protect transmitted data [50]–[53].

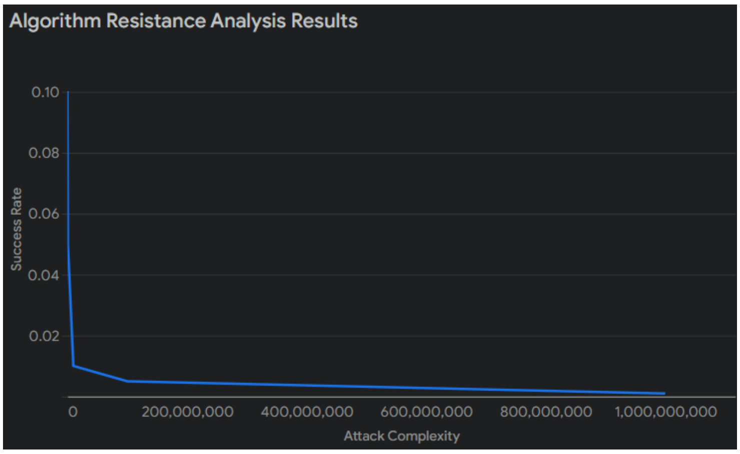

Figure 9. Results of the algorithm resistance analysis to attacks

4. CONCLUSION

This article considered two important aspects of UAVs: forest fire monitoring and data security for low-orbit vehicles. A GIS was developed to monitor and predict the spread of forest fires using intelligent processing of aerospace data obtained from UAVs. An effective algorithm for high-speed data encryption was also proposed, ensuring reliable protection of information during transmission from low-orbit vehicles. The results of modeling and analysis confirmed the effectiveness of the proposed solutions. The developed GIS and encryption algorithm can be used in practice to improve the safety and efficiency of UAVs. In the future, it is planned to expand the functionality of the GIS through integration with other monitoring systems and develop a mobile application for accessing data in real time. It is also planned to conduct additional studies of the encryption algorithm's resistance to new types of attacks.

FUNDING INFORMATION

The authors express gratitude to the Ministry of Higher Education and Science of the Republic of Kazakhstan, which allocated program-targeted funding for 2024-2026. IRN AR23486167.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Khuralay Moldamurat		✓			✓					✓		✓		✓
Makhabbat Bakyt	✓					✓	✓		✓	✓			✓	✓
Dastan Yergaliyev		✓		✓					✓			✓		✓
Dinara Kalmanova			✓		✓			✓	✓		✓			
Anuar Galymzhan	✓		✓							✓	✓			
Abylaikhan Sapabekov			✓			✓		✓		✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The original contributions presented in this study are included in the article/supplementary material. Further inquiries can be directed to the corresponding author.

REFERENCES

[1] D. P. Mukherjee and S. Pal, "Advances in pattern recognition," *Pattern Recognition Letters*, vol. 26, no. 4, pp. 395–398, Mar. 2005, doi: 10.1016/j.patrec.2004.08.002.

[2] D. W. Casbeer, Sai-Ming Li, R. W. Beard, R. K. Mehra, and T. W. McLain, "Forest fire monitoring with multiple small UAVS," in *Proceedings of the 2005, American Control Conference*, Portland, OR, USA, 2005, pp. 3530-3535 vol. 5, doi: 10.1109/ACC.2005.1470520.

[3] M. Davis and M. Shekaramiz, "Desert/forest fire detection using machine/deep learning techniques," *Fire*, vol. 6, no. 11, Oct. 2023, doi: 10.3390/fire6110418.

[4] M. Malhotra and Gagandeep, "DNA cryptography: a novel approach for data security using flower pollination algorithm," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3358159.

[5] U. Maulik and D. Chakraborty, "Remote sensing image classification: a survey of support-vector-machine-based advanced techniques," *IEEE Geoscience and Remote Sensing Magazine*, vol. 5, no. 1, pp. 33–52, Mar. 2017, doi: 10.1109/MGRS.2016.2641240.

[6] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in iot networks: a survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, 2022, doi: 10.1016/j.future.2021.11.011.

[7] C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in industrial wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, Dec. 2018, doi: 10.1186/s13638-018-1121-6.

[8] A. Bogdanov *et al.*, "PRESENT: an ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems-CHES 2007*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466, doi: 10.1007/978-3-540-74735-2_31.

[9] G. Leander and A. Poschmann, "On the classification of 4 bit s-boxes," in *Arithmetic of Finite Fields*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 159–176, doi: 10.1007/978-3-540-73074-3_13.

[10] B. Li, Z. Yang, D. Chen, S. Liang, and H. Ma, "Maneuvering target tracking of uav based on mn-ddpg and transfer learning," *Defence Technology*, vol. 17, no. 2, pp. 457–466, Apr. 2021, doi: 10.1016/j.dt.2020.11.014.

[11] L. R. Knudsen, "Truncated and higher order differentials," in *Fast Software Encryption: Second International Workshop*, Berlin, Heidelberg: Springer, 1995, pp. 196–211, doi: 10.1007/3-540-60590-8_16.

[12] J. Daemen and V. Rijmen, *The design of rijndael: aes - the advanced encryption standard*, 1st ed. Heidelberg: Springer Berlin, 2002, doi: 10.1007/978-3-662-04722-4.

[13] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering design principles and practical applications*, Indianapolis, United States: Wiley Publishing, 2010.

[14] B. Preneel, C. Paar, and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*, Berlin, Germany: Springer, 2009, doi: 10.1007/978-3-642-04101-3.

[15] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in c*, vol. 10, no. 5. John Wiley & Sons, 2015, doi: 10.1016/0267-3649(94)90017-5.

[16] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[17] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO '85 Proceedings*, 1986, pp. 417–426, doi: 10.1007/3-540-39799-X_31.

[18] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to elliptic curve cryptography*. New York, United States: Springer, 2004, doi: 10.1007/b97644.

[19] I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography*. United Kingdom: Cambridge University Press, 199AD, doi: 10.1007/978-3-030-97902-7_13.

[20] X. Shi and X. Wu, "An overview of human genetic privacy," *Annals of the New York Academy of Sciences*, vol. 1387, no. 1, pp. 61–72, Jan. 2017, doi: 10.1111/nyas.13211.

[21] S. Selimefendigil, "Predicting financial distress using supervised machine learning algorithms: an application on borsa istanbul," *Pressacademia*, Dec. 2023, doi: 10.17261/Pressacademia.2023.1828.

[22] J. Katz and Y. Lindell, *Introduction to modern cryptography*. London, New York: CRC press, 2007.

[23] D. R. Stinson and M. B. Paterson, *Cryptography: theory and practice*, vol. 30, no. 9. London, New York: CRC press, 2018, doi: 10.1016/0898-1221(95)90225-2.

[24] A. Joux, *Algorithmic cryptanalysis*. CRC press, 2009, doi: 10.1201/9781420070033.

[25] P. Rogaway, "Evaluation of some blockcipher modes of operation," Cryptography Research and Evaluation Committees (CRYPTREC), Government of Japan, 2011.

[26] M. Bellare, P. Rogaway, and D. Wagner, "The eax mode of operation," in *Fast Software Encryption*, Berlin, Heidelberg: Springer, 2004, pp. 389–407, doi: 10.1007/978-3-540-25937-4_25.

[27] T. Peyrin and Y. Seurin, "Counter-in-tweak: authenticated encryption modes for tweakable block ciphers," in *Advances in Cryptology–CRYPTO 2016*, vol. 9814, 2016, pp. 33–63, doi: 10.1007/978-3-662-53018-4_2.

[28] M. Dworkin, "Recommendation for block cipher modes of operation: galois/counter mode (GCM) and GMAC," *National Institute of Standards and Technology:Computer Security Resorce Cente*r, NIST SP 800-38D, 2007.

[29] S. Gueron and M. E. Kounavis, "Intel ® carry-less multiplication instruction and its usage for computing the GCM mode," *Intel Corporation*, 2010.

[30] K. Moldamurat, Y. Seitkulov, S. Atanov, M. Bakyt, and B. Yergaliyeva, "Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, pp. 479–487, Feb. 2024, doi: 10.11591/ijece.v14i1.pp479-487.

[31] D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright, *Fast software aes encryption*. Berlin, Heidelberg: Springer, 2010, doi: 10.1007/978-3-642-13858-4_5.

[32] E. Käsper and P. Schwabe, "Faster and timing-attack resistant aes-gcm," *Cryptographic Hardware and Embedded Systems-CHES 2009*, pp. 1–17, 2009, doi: 10.1007/978-3-642-04138-9_1.

[33] S. Rana, S. Hossain, H. I. Shoun, and M. A. Kashem, "An effective lightweight cryptographic algorithm to secure resource-constrained devices," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018, doi: 10.14569/IJACSA.2018.091137.

[34] N. C. Luong *et al.*, "Applications of deep reinforcement learning in communications and networking: a survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3133–3174, 2019, doi: 10.1109/COMST.2019.2916583.

[35] E. A. Nadaraya, "On estimating regression," *Theory of Probability & Its Applications*, vol. 9, no. 1, pp. 141–142, Jan. 1964, doi: 10.1137/1109020.

[36] P. Shah and S. Agashe, "Review of fractional pid controller," *Mechatronics*, vol. 38, pp. 29–41, Sep. 2016, doi: 10.1016/j.mechatronics.2016.06.005.

[37] A.-A. A. Boulogeorgos and A. Alexiou, "How much do hardware imperfections affect the performance of reconfigurable intelligent surface-assisted systems?," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1185–1195, 2020, doi: 10.1109/OJCOMS.2020.3014331.

[38] A.-A. A. Boulogeorgos and A. Alexiou, "Performance analysis of reconfigurable intelligent surface-assisted wireless systems and comparison with relaying," *IEEE Access*, vol. 8, pp. 94463–94483, 2020, doi: 10.1109/ACCESS.2020.2995435.

[39] S. Yang and B. Xian, "Exponential regulation control of a quadrotor unmanned aerial vehicle with a suspended payload," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 6, pp. 2762–2769, Nov. 2020, doi: 10.1109/TCST.2019.2952826.

[40] M. Bakyt, K. Moldamurat, A. Konyrkhanova, A. Maidanov, and D. Satybaldina, "Integration of cryptography and navigation systems in unmanned military mobile robots: a review of current trends and perspectives," in *CEUR Workshop Proceedings*, 2024.

[41] R. Socas, S. Dormido, and R. Dormido, "Event-based control strategy for the guidance of the aerosonde uav," in *2015 European Conference on Mobile Robots (ECMR)*, IEEE, Sep. 2015, pp. 1–6, doi: 10.1109/ECMR.2015.7324213.

[42] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020, doi: 10.1109/OJCOMS.2020.3010270.

[43] U. R. Mogili and B. B. V. L. Deepak, "Review on application of drone systems in precision agriculture," *Procedia Computer Science*, vol. 133, pp. 502–509, 2018, doi: 10.1016/j.procs.2018.07.063.

[44] M. N. Bashir, K. M. Yusof, M. R. Jasman, and C. Y. Leow, "Outage performance of cooperative relay protocol on UAVs-based flying ADHOC network," *Jurnal Teknologi*, vol. 84, no. 3, pp. 185–194, Mar. 2022, doi: 10.11113/jurnalteknologi.v84.17552.

[45] W. Zhang, Y. Ning, and C. Suo, "A method based on multi-sensor data fusion for uav safety distance diagnosis," *Electronics*, vol. 8, no. 12, Dec. 2019, doi: 10.3390/electronics8121467.

[46] S. Barmpounakis, N. Alonistioti, G. C. Alexandropoulos, and A. Kaloxylos, "Dynamic infrastructure-as-a-service: a key paradigm for 6g networks and application to maritime communications," *ITU Journal on Future and Evolving Technologies*, vol. 3, no. 2, pp. 326–341, Apr. 2022, doi: 10.52953/WQWX1975.

[47] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017, doi: 10.1109/TWC.2017.2650987.

[48] K. Moldamurat *et al.*, "Improved unmanned aerial vehicle control for efficient obstacle detection and data protection," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 3, pp. 3576-3587, Sep. 2024, doi: 10.11591/ijai.v13.i3.pp3576-3587.

[49] M. Bakyt, K. Moldamurat, D. Z. Satybaldina, and N. K. Yurkov, "Modeling information security threats for the terrestrial segment of space communications," in *CEUR Workshop Proceedings*, 2022.

[50] M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, "Application of quantum key distribution to enhance data security in agrotechnical monitoring systems using uavs," *Applied Sciences*, vol. 15, no. 5, pp. 1-32, Feb. 2025, doi: 10.3390/app15052429.

[51] C. An, S. Jia, J. Zhou, and C. Wang, "Fast model-free learning for controlling a quadrotor uav with designed error trajectory," *IEEE Access*, vol. 10, pp. 79669–79680, 2022, doi: 10.1109/ACCESS.2022.3194276.

[52] K. Wang, Q. Gu, B. Huang, Q. Wei, and T. Zhou, "Adaptive event-triggered near-optimal tracking control for unknown continuous-time nonlinear systems," *IEEE Access*, vol. 10, pp. 9506–9518, 2022, doi: 10.1109/ACCESS.2021.3140076.

[53] K. Chenu *et al.*, "Contribution of crop models to adaptation in wheat," *Trends in Plant Science*, vol. 22, no. 6, pp. 472–490, Jun. 2017, doi: 10.1016/j.tplants.2017.02.003.

BIOGRAPHIES OF AUTHORS

Khuralay Moldamurat was educated at the I. Zhansugurova Zhetysu State University, specialist physics and informatics. Academy of Economics and Law named after academician U.A. Dzholdasbekov, Bachelor of the specialty Finance, Turkish State University, Ankara, 2008, 2010 Candidate of Technical Sciences (approved by the Higher Attestation Commission RK dated June 30, 2011 protocol No. 6. Diploma No. 0006248) at the dissertation council, the MSHE of the RK, at the NSA at the Institute of Mathematics at OD53.12. on the topic: Verification and automation of microcontroller programming, the dissertation is scientifically defended. (050010, Almaty, Pushkin St., house 125, office 306). Currently, she is Associate Professor of the Department of Space Technique and Technology at the L.N. Gumilyov ENU, Astana, Kazakhstan. Her research interests include IT technologies, radio engineering, programming of microcontrollers and automation systems, modern technologies for designing space nanosatellites. She can be contacted at email: khuralay03@gmail.com.

Makhabbat Bakyt received her Bachelor of Engineering and Technology and Master of Engineering from the L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. She is currently a Doctoral student of the Department Information Security Department of the L. N. Gumilyov Eurasian National University. Her research interests include aircraft data encryption, cryptographic protection, information security. She can be contacted at email: bakyt.makhabbat@gmail.com.

Dastan Yergaliyev is a Candidate of Technical Sciences, Professor of the Department of Space Engineering and Technology of the L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. His research focuses on study of representation methods for the analysis of units and systems of aircraft airborne control systems as objects of control and diagnostics. He can be contacted at email: des-67@yandex.kz.

Dinara Kalmanova received her education at Aktau State University named after Sh. Yesenov (2002) with a degree in Physics. In 2009, she defended her PhD thesis on profile 13.00.01- General pedagogy, history of educational pedagogy (approved by the decision of the Committee for Control in the Field of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan dated September 22, 2009, protocol No. 7, diploma No. 0003427). Currently acting Associate Professor of the Department of "Space Engineering and Technology" ENU named after L. N. Gumilyov, Astana, Kazakhstan. Her research interests include power supply and thermal insulation systems for spacecraft. She can be contacted at email: dinara_kalmanova@mail.ru.

Anuar Galymzhan graduated from the L.N. Gumilyov Eurasian National University with a bachelor's degree in Radio Engineering, Electronics and Telecommunications in 2015, and from the L.N. Gumilyov Eurasian National University with a master's degree in Space Engineering and Technology in 2017. In 2017-2019, he worked as an engineer at the Space Engineering and Technology Department of the Physics and Engineering Faculty of the L.N. Gumilyov Eurasian National University, Astana. Since 2019, he has been a senior lecturer at the Space Engineering and Technology Department of the Physics and Engineering Faculty of the L.N. Gumilyov Eurasian National University, Astana. His research interests include information measurement and control systems. He can be contacted at email: galym_rma@mail.ru.

Abylaikhan Sapabekov received his Bachelor of Engineering and Technology and Master of Engineering from the L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. At the moment he works at the National Defense University of the Republic of Kazakhstan, Astana as a senior researcher. His research interests include space images, remote sensing satellites, cryptography. He can be contacted at email: ablai_sapabekov@mail.ru.