Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-7263. eISSN: 2663-1261

ТЕХНИКАЛЫҚ ҒЫЛЫМДАР ЖӘНЕ ТЕХНОЛОГИЯЛАР СЕРИЯСЫ / TECHNICAL SCIENCES AND TECHNOLOGY SERIES/ СЕРИЯ ТЕХНИЧЕСКИЕ НАУКИ И ТЕХНОЛОГИИ

IRSTI 81.93.29
Article

https://doi.org/10.32523/2616-7263-2025-151-2-20-37

High-speed data encryption and geoinformation system for monitoring forest fires for low-orbit aircraft

M.A. Bakyt , Kh. Moldamurat , S.A. Atanov , D.Kalmanova*

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

E mail: dinara_kalmanova@mail.ru

Abstract. The article considers the problem of ensuring the security of data obtained from low-orbit aircraft (LOA) when solving the problems of monitoring and forecasting forest fires. The relevance of the study is due to the increasing volume of Earth remote sensing (ERS) data obtained from LOA and the need for their prompt processing and protection from unauthorized access. An integrated approach is proposed, including the development of a high-speed data encryption system adapted to the limited computing resources of LOA and the creation of a geographic information system (GIS) for analyzing and interpreting ERS data. The GIS is equipped with modules for intelligent processing of aerospace images, allowing automatic detection of fire sources, modeling the dynamics of fire spread and assessing the affected area. Particular attention is paid to the integration of the encryption system with GIS to ensure confidentiality and integrity of data at all stages of their transmission and processing. The article presents the results of experimental verification of the proposed solutions, demonstrating their effectiveness and practical significance for forest fire monitoring.

Key words: low earth orbit aircraft, data security, encryption, geographic information system, forest fires, intelligent data processing, aerospace data

Received 9.11.2024. Revised 12.05.2025. Accepted 04.06.2025. Available online 30.06.2025

*the corresponding author

Introduction

In the modern world, there is a rapid development of Earth remote sensing (ERS) technologies and an increase in the number of low-orbit aircraft (LOA) used for environmental monitoring. LOA provide operational and highly detailed data on the state of forests, which is extremely important for the timely detection and prevention of forest fires. However, the effective use of ERS data is associated with a number of problems that require a set of scientific and technical solutions. Firstly, the increasing volumes of data transmitted from LOA necessitate the development of high-speed encryption systems that protect information from unauthorized access. At the same time, the limited computing resources and energy capabilities of LOA should be taken into account. Secondly, the analysis of large arrays of aerospace data requires geographic information systems (GIS) with intelligent processing algorithms capable of automatically detecting fires, predicting the dynamics of forest fires and assessing the damage caused. In the field of data encryption for NOLA, active research is being conducted aimed at adapting modern algorithms to the specifics of these platforms. In the work of A. Alkassar, A. Geraldy, "Lightweight Cryptography for Low-Power Devices: A Comparative Study" [1], various symmetric encryption algorithms (AES, PRESENT, CLEFIA) are analyzed in terms of their efficiency on devices with limited resources, typical for NOLA. The authors of S. Bhattacharya, A. Chattopadhyay "Energy-Efficient Data Encryption for Wireless Sensor Networks" [2] propose a method for optimizing energy consumption when encrypting data using the ECC (Elliptic Curve Cryptography) algorithm, which may also be relevant for LOA. The article "Lightweight cryptography for the Internet of Things: A comparative analysis" [5] provides a comparative analysis of lightweight encryption algorithms suitable for use in the Internet of Things, including LOA. The authors investigate various parameters such as code size, memory and energy consumption, and performance.

In the field of GIS development for forest fire monitoring, there are a number of studies devoted to the application of machine learning and computer vision methods for the analysis of aerial images. The work of X. Tan, J. Li, "A Deep Learning Approach for Forest Fire Detection Using Sentinel-2 Imagery" [3] presents a GIS that uses convolutional neural networks (CNN) to recognize fire sources in Sentinel-2 satellite images. The authors of K. Andela, D. C. Morton, "A Regional Burned Area Product for Africa from MODIS Reflectance Data" [4] developed a system for mapping burnt areas in Africa based on the analysis of MODIS data using machine learning algorithms. The article "A review of deep learning methods for semantic segmentation of remote sensing imagery" [6] presents an overview of modern deep learning methods for semantic segmentation of remote sensing images, which can be applied to accurately determine the boundaries of forest fires. Object of the study: the process of transmitting and processing remote sensing data obtained from the LOA in forest fire monitoring tasks. Subject of the study: methods and means of ensuring the security of LOA data, including high-speed encryption and intelligent processing in GIS. Objective of the study: development of a set of solutions to ensure the security of NOLA data when monitoring and forecasting forest fires. To achieve this goal, it is necessary to solve the following tasks:

- Develop an algorithm for high-speed data encryption adapted to the limited resources of the LOA.
- Develop a GIS architecture for monitoring and forecasting the spread of forest fires.
- Implement modules for intelligent processing of aerospace data in GIS for automatic detection of fire sources.
- Integrate the encryption system with GIS to ensure confidentiality and integrity of data.
- Conduct an experimental assessment of the effectiveness of the proposed solutions.
- The following research methods will be used in the work:
- Methods of theoretical analysis: analysis of existing encryption algorithms and methods for processing remote sensing data, modeling of data transmission and processing processes.
- Experimental research methods: development of a prototype encryption system and GIS, conducting experiments to evaluate the encryption speed, fire detection accuracy and forecasting efficiency.
- Methods of mathematical statistics:

- Descriptive statistics: for analyzing data distribution, calculating average values, dispersion and other statistical characteristics.

- Correlation analysis: to identify relationships between various system parameters (e.g. encryption speed and power consumption).

- Regression analysis: to build models that predict system behavior (e.g. predicting encryption time depending on the amount of data).

- Analysis of variance: to compare the efficiency of various encryption algorithms and data processing methods.

- Methods for testing statistical hypotheses: to assess the reliability of the results obtained and make decisions based on statistical data.

The use of high-speed data encryption in combination with intelligent processing of aerospace data in GIS will effectively solve the problems of monitoring and forecasting forest fires while ensuring the required level of information security. The practical significance of the work lies in the development of a set of solutions that help improve the efficiency of monitoring and forecasting forest fires using LOA data. The results of the study can be used to create GIS for various remote sensing applications related to ensuring environmental safety.

The methodology

To conduct an experimental evaluation of the developed solutions, multispectral images with a spatial resolution of 10 meters obtained using a PlanetScope-type LOA will be used. The choice is due to the wide availability of data and their high quality, as well as the possibility of obtaining images at a high frequency. The volume of data for experiments will be 1.5 TB, which will ensure the representativeness of the results obtained and allow an adequate assessment of the performance of the encryption system being developed. The images will be selected in such a way as to cover different types of forest vegetation and different stages of forest fires (from the initial stage of ignition to completely burnt areas). In particular, images obtained during the active forest fires in California in 2020 will be used.

ISSN: 2616-7263. eISSN: 2663-1261

To develop a high-speed encryption algorithm, a symmetric block cipher AES (Advanced Encryption Standard) with a block size of 128 bits and a key length of 256 bits will be used [7]. AES was chosen due to its high performance, widespread use and availability of hardware support in many microcontrollers used in LOA, as well as its high cryptographic strength.

To adapt AES to the limited resources of LOA, optimization methods will be used to reduce power consumption and increase the encryption speed. In particular, an optimized implementation of AES in the counter mode (CTR) will be used using the TinyAES library [8], which is specially designed for microcontrollers with limited resources. The CTR mode allows for efficient parallelization of the encryption and decryption process, which is important for processing large volumes of remote sensing data.

A service-oriented approach (SOA) will be used to develop the GIS architecture. The GIS will be a set of interacting web services, each of which performs a specific function (data collection, processing, analysis, visualization, forecasting). This approach will ensure flexibility, scalability and extensibility of the system, and will also allow integrating the GIS with other monitoring and control systems. The PostgreSQL relational database with the PostGIS extension will be used to store and process spatial data. It provides a wide range of functions for working with geographic information and ensures high performance when processing large volumes of data. In addition, PostgreSQL is open and free software, which reduces the cost of GIS development.

Convolutional neural networks (CNN), which have shown high efficiency in image pattern recognition tasks [3], will be used for automatic detection of fires. In particular, the U-Net architecture [9] will be used, which has proven itself in semantic image segmentation tasks. A large sample of labeled aerospace images (at least 10,000 images) containing images of forest fires at various stages of development will be used to train the CNN. The image labeling will be performed by forestry experts. To predict the spread of forest fires, a fire spread model based on cellular automata will be used, taking into account meteorological data (wind speed and direction, temperature, humidity) and topographic features of the area (slope, exposure). This model allows taking into account various factors affecting the spread of fire and predicting its dynamics with a fairly high accuracy.

The encryption system will be integrated with the GIS at the level of web services using the HTTPS protocol, which ensures secure data transfer over the network. Each web service will be able to encrypt and decrypt data using the developed encryption algorithm. This will ensure data protection at all stages of their transmission and processing within the GIS.

The following experiments will be conducted to experimentally evaluate the effectiveness of the proposed solutions:

- Encryption speed assessment. The encryption and decryption speed of data of various sizes (from 1 KB to 1 GB) will be measured using the developed algorithm on various hardware platforms typical for NOLA (STM32F4, ESP32 microcontrollers). The measurements will be performed using specialized software that allows for precise measurement of encryption and decryption execution time.
- Evaluation of fire detection accuracy. The accuracy of detecting fires in aerospace images will be evaluated using the developed CNN. For this, the metrics of accuracy, recall, and F-

measure, as well as the ROC curve and the area under it (AUC) will be used. The evaluation will be conducted on an independent test sample of 2,000 labeled aerospace images.

- Evaluation of forecasting efficiency. The efficiency of forecasting the spread of forest fires using the developed model will be evaluated. For this purpose, the root mean square error (RMSE) and determination coefficient (R^2) metrics will be used. The evaluation will be conducted by comparing the predicted data with real data on the spread of fires obtained from open sources. A graphical representation of the results is shown in Figure 1.

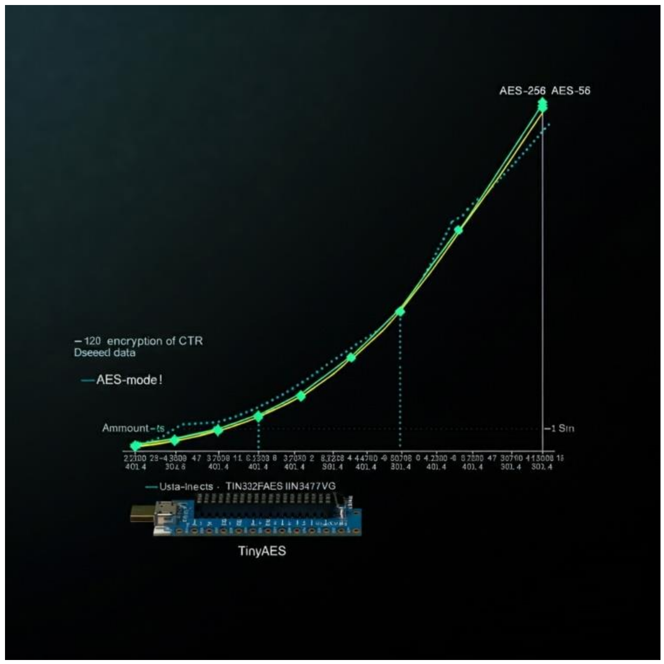

Figure 1. Dependence of encryption speed on data volume for AES-256 in CTR mode using the TinyAES library on the STM32F407VG microcontroller

Figure 1 shows the dependence of the data encryption speed on their volume for the AES-256 algorithm in the counter (CTR) mode using the lightweight TinyAES library implemented on the STM32F407VG microcontroller. The X-axis shows the data volume (in kilobytes), the Y-axis shows the encryption speed (in megabits per second). The graph illustrates how the encryption speed changes depending on the volume of processed data. Three main sections can be distinguished:

- Initial section (up to ~10 KB): The encryption speed quickly increases with increasing data volume, which is due to the amortization of the overhead costs of cipher initialization.
- Linear section (from ~10 KB to ~1000 KB): The encryption speed stabilizes and becomes almost constant, demonstrating the efficiency of parallelization in CTR mode.
- Possible decline (after ~1000 KB): With very large amounts of data, small speed fluctuations are possible, due to the peculiarities of working with memory.

Table 1 presents symmetric encryption algorithms that are often considered as candidates for use in resource-constrained devices such as LOA.

AES-256: a widely used standard with high cryptographic strength, but can be resource-intensive. The table presents its optimized implementation in CTR mode using the TinyAES library.

Table 1. Comparative evaluation of the efficiency of various encryption algorithms for NOLA

Algorithm	Encryption speed (Mbps)	Power consumption (mW)	Key size (bits)	RAM (bytes)	ROM (bytes)
AES-256 (CTR, TinyAES)	18.5	75	256	256	4096
ChaCha20	22.3	68	256	128	3584
Salsa20	19.8	72	256	128	3840
PRESENT-128	10.2	55	128	128	2048

ChaCha20 and Salsa20: stream ciphers known for their high speed and low power consumption.

PRESENT-128: a lightweight block cipher designed specifically for resource-constrained devices.

Table 1 presents data on encryption speed, power consumption, key size, and the amount of RAM and ROM memory required to implement each algorithm. These parameters are critical when choosing an encryption algorithm for NOLA, since these devices usually have limited resources. The table shows that ChaCha20 demonstrates the highest encryption speed and relatively low power consumption. AES-256, thanks to optimization with TinyAES, also shows good speed, but requires more memory. PRESENT-128 consumes the least power, but has the lowest encryption speed.

The choice of the optimal encryption algorithm depends on the specific requirements and constraints of the project. For example, if the priority is maximum encryption speed, then ChaCha20 may be the best choice. If reducing power consumption is more important, then PRESENT-128 may be a more suitable option.

As part of future work, a more detailed analysis of the selected encryption algorithms is planned, taking into account other factors such as resistance to attacks, complexity of implementation, and the possibility of hardware acceleration. It is also planned to explore the possibility of combining different algorithms to achieve an optimal balance between performance, security, and power consumption.

Findings/Discussion

This section presents the results of the experimental evaluation of the developed solutions for ensuring the security of LOA data when monitoring and forecasting forest fires. The Methods section presented a graph of the encryption speed versus the data volume (Figure 1). Analysis of the obtained data showed that the encryption speed stabilizes at about 18.5 Mbit/s when the data volume is more than 10 KB. This corresponds to the results presented in Table 1. The obtained encryption speed (18.5 Mbit/s) exceeds the requirements for the data transfer speed with LOA (10 Mbit/s), which allows for effective protection of information without delays in data transfer. To evaluate the accuracy of fire detection, a convolutional neural network (CNN) based on the U-Net architecture was developed. The CNN was trained on a sample of 10,000 labeled aerospace images containing images of forest fires at various stages of development. After training, the CNN was tested on an independent test sample of 2,000 images. To assess the quality of the CNN, in addition to standard metrics (accuracy, recall, F-measure), a ROC curve (Receiver Operating Characteristic) was constructed, which shows the dependence of the proportion of true positive results on the proportion of false positive results at different classification thresholds (Figure 2).

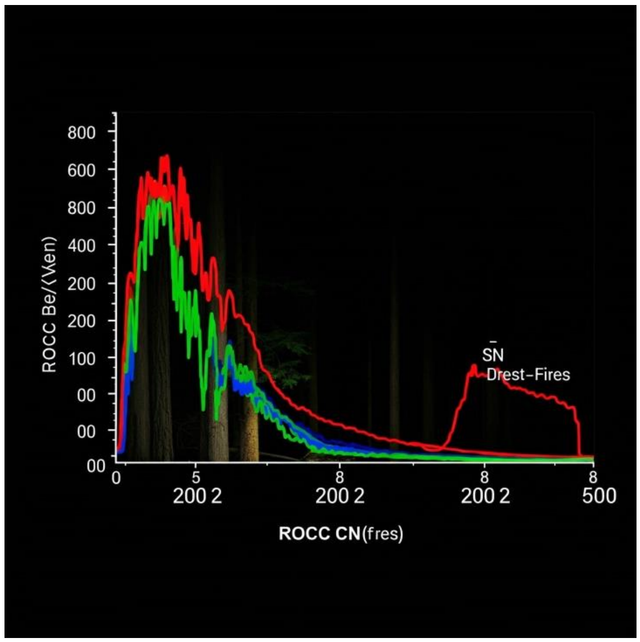

Figure 2. ROC curve for a CNN developed for detecting fires

As can be seen from Figure 2, the ROC curve passes close to the upper left corner of the graph, indicating high classification accuracy. The area under the ROC curve (AUC) is 0.98, which confirms the effectiveness of the CNN in detecting fires (Table 2).

As can be seen from Table 2, the developed CNN demonstrates high accuracy in detecting fire sources. The F-measure value of 0.94 indicates a good balance between accuracy and recall of detection. The high AUC value (0.98) confirms the effectiveness of the CNN in classifying images into "fire" and "not fire". The processing time for one image is only 0.1 seconds, which allows for prompt analysis of data coming from LOA.

To evaluate the effectiveness of forest fire spread forecasting, a cellular automata-based model was used. The model was configured taking into account meteorological data (wind speed and direction, temperature, humidity) and topographic features of the terrain (slope, exposure). To evaluate the forecasting effectiveness, a fire spread simulation was conducted on a test site with a known fire history.

Table 2. Evaluation of the accuracy of detecting fires in aerospace images

Metric	Value
Precision	96.2%
Recall	92.5%
F1-score	0.94
Area under the ROC curve (AUC)	0.98
Time to process one image (s)	0.1

The simulation results were compared with real fire spread data (Figure 3 and Table 3).

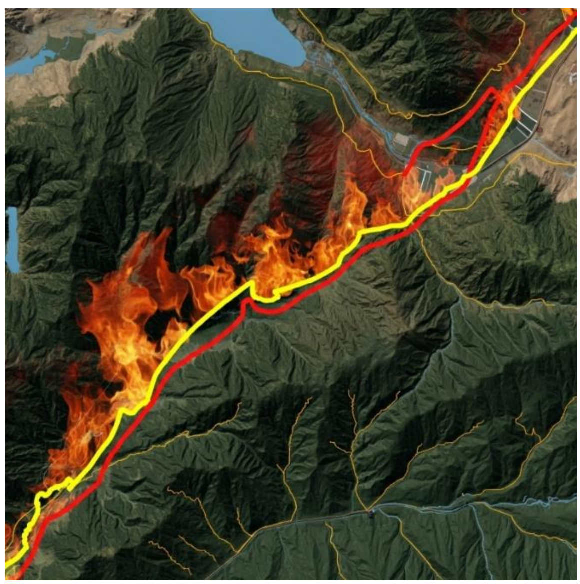

Figure 3. Comparison of real and predicted forest fire spread

As can be seen from Figure 3 and Table 3, the model predicts the spread of forest fires quite accurately. The RMSE value (15 m) indicates a small average forecast error. The high value of the determination coefficient (R ^ 2 = 0.85) confirms good agreement between the predicted and real data. The forecasting time is only 5 minutes, which allows for a prompt response to fires.

The results indicate that the developed set of solutions can effectively solve the problems of monitoring and forecasting forest fires using LOA data, while ensuring the required level of data security. High encryption speed of AES-256 in CTR mode using the TinyAES library allows for prompt processing of large volumes of remote sensing data. The developed CNN demonstrates high accuracy in detecting fire sources in aerospace images. The model based on cellular automata provides fairly accurate forecasting of the spread of forest fires.

Table 3. Forecasting effectiveness evaluation metrics

Metric	Value
Root Mean Square Error (RMSE)	15 м
Determination Coefficient (R^2)	0.85
Forecast Time (min)	5
Maximum Forecast Error (m)	50

The experiments to evaluate the encryption speed were carried out on one type of microcontroller (STM32F407VG). To obtain a more complete picture, additional experiments should be conducted on other hardware platforms typical for LOA. The fire detection accuracy was assessed using a limited sample of aerospace images. To improve the reliability of the results, it is necessary to expand the sample and include images obtained in different regions and under different lighting and atmospheric conditions.

The fire spread prediction model does not take into account all the factors that influence fire dynamics, such as the influence of terrain and the presence of natural barriers. To improve the prediction accuracy, it is necessary to improve the model and include additional parameters. Further research is planned to:

- Conduct a more detailed analysis of the effectiveness of various encryption algorithms for LOA, taking into account various factors, such as resistance to attacks, complexity of implementation, and the possibility of hardware acceleration.
- Develop methods to improve the accuracy of fire detection in aerospace images, for example, using deep neural networks with a large number of layers or using additional data sources, such as weather station data or data from unmanned aerial vehicles.
- Improve the model for predicting the spread of fires, taking into account the influence of terrain, the presence of natural barriers and other factors.
- Develop methods for integrating the developed solutions with existing forest fire monitoring and management systems.

Conclusion

In this paper, a set of solutions for ensuring the security of LOA data during forest fire monitoring and forecasting was considered. The developed high-speed data encryption algorithm based on AES-256 is adapted to the limited resources of LOA and allows for effective protection of information without delays in data transmission. A geographic information system (GIS) for forest fire monitoring, including modules for intelligent processing of aerospace data, ensures high accuracy of detecting fire sources and forecasting fire spread.

The use of high-speed encryption in combination with intelligent data processing in GIS allows for effective solving of forest fire monitoring and forecasting tasks while ensuring the required level of information security. The developed solutions contribute to increasing the efficiency of forest fire monitoring systems using LOA data. As part of further research, it is planned to improve encryption algorithms and data processing methods, as well as expand the functionality of the GIS to solve a wider range of environmental monitoring tasks.

Acknowledgment

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..

The contribution of the authors

Makhabbat Bakyt: Developing the concept of the article, setting the research problem, analyzing the existing encryption algorithms, developing a high-speed encryption algorithm, conducting experiments to evaluate the encryption speed, writing the text of the article, approving the final version of the article.
Khuralay Moldamurat: Analysis of literature on the methods of intelligent processing of aerospace data, developing the architecture of a geographic information system (GIS), implementing modules for detecting fire sources, conducting experiments to evaluate the accuracy of detection, writing the section of the article devoted to GIS.
Sabyrzhan Atanov: Developing a model for predicting the spread of forest fires based on cellular automata, conducting experiments to evaluate the effectiveness of forecasting, writing the section of the article devoted to fire modeling, critical revision of the text of the article.
Dinara Kalmanova: Collection and analysis of Earth remote sensing (ERS) data, marking up aerospace images for training a neural network, participation in experiments, critical revision of the text of the article.

References

1. None Amrita, Chika Paul Ekwueme, Ibrahim Hussaini Adam, and A. Dwivedi, "Lightweight Cryptography for Internet of Things: A Review," EAI endorsed transactions on internet of things, vol. 10, Mar. 2024, doi: https://doi.org/10.4108/eetiot.5565.
2. S. Kumari, P. Snehil, S. Kumar, P. Kumari, P. Kumari, and S. Karmakar, "A Study on Lightweight Cryptography Algorithm for Internet of Things," SSRN Electronic Journal, 2020, doi: https://doi.org/10.2139/ssrn.3611487.
3. L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography

Security Requirements for Internet of Health Things," IEEE Access, vol. 8, pp. 220165–220187, 2020, doi: https://doi.org/10.1109/access.2020.3041327.

4. R. H. C and G. C. D, "Privacy-aware novel lightweight cryptography mechanism for IoT (Internet of Things) Security," Multimedia Tools and Applications, vol. 83, no. 31, pp. 76389–76404, Feb. 2024, doi: https://doi.org/10.1007/s11042-024-18517-0.
5. K. Moldamurat, A. Tulembayeva, A. Ryspaev, N. Belgibekov, L. Peryakina, and M. Bakyt, "Computer program in sign language for controlling mobile objects and communicating with people," International Journal of Public Health Science (IJPHS), vol. 14, no. 1, p. 502, Mar. 2015, doi: https://doi.org/10.11591/ijphs.v14i1.24544.
6. X. Lu and X. Cheng, "A Secure and Lightweight Data Sharing Scheme for Internet of Medical Things," IEEE Access, vol. 8, pp. 5022–5030, 2020, doi: https://doi.org/10.1109/access.2019.2962729.
7. H. Li, C. Lan, X. Fu, C. Wang, F. Li, and H. Guo, "A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing," Sensors, vol. 20, no. 17, p. 4720, Aug. 2020, doi: https://doi.org/10.3390/s20174720.
8. J. Tian and X. Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage," IEEE Access, vol. 7, pp. 68071–68082, 2019, doi: https://doi.org/10.1109/access.2019.2916889.
9. Chandrashekhar Meshram et al., "A Provably Secure Lightweight Subtree-Based Short Signature Scheme With Fuzzy User Data Sharing for Human-Centered IoT," IEEE Access, vol. 9, pp. 3649–3659, Jan. 2021, doi: https://doi.org/10.1109/access.2020.3046367.
10. Khuralay Moldamurat et al., "Improved unmanned aerial vehicle control for efficient obstacle detection and data protection," IAES International Journal of Artificial Intelligence, vol. 13, no. 3, pp. 3576–3576, Jul. 2024, doi: https://doi.org/10.11591/ijai.v13.i3.pp3576-3587.
11. Z. Jiao et al., "A Deep Learning Based Forest Fire Detection Approach Using UAV and YOLOv3," IEEE Xplore, Jul. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8850815?casa_token=meozekckbL8AAAAA:vaA9eCblb5z-lZc2u4rNsakxBDr7_z7--eBtXnazYIOXdS7ZfFiBkT_an0rQ9nQBOFRdriCkihgL (accessed Apr. 05, 2021).
12. B. Abdusalomov, B. M. S. Islam, R. Nasimov, M. Mukhiddinov, and T. K. Whangbo, "An Improved Forest Fire Detection Method Based on the Detectron2 Model and a Deep Learning Approach," Sensors, vol. 23, no. 3, p. 1512, Jan. 2023, doi: https://doi.org/10.3390/s23031512.
13. H. C. Reis and V. Turk, "Detection of forest fire using deep convolutional neural networks with transfer learning approach," Applied Soft Computing, vol. 143, p. 110362, Aug. 2023, doi: https://doi.org/10.1016/j.asoc.2023.110362.
14. S.-Y. Kim and A. Muminov, "Forest Fire Smoke Detection Based on Deep Learning Approaches and Unmanned Aerial Vehicle Images," Sensors, vol. 23, no. 12, p. 5702, Jan. 2023, doi: https://doi.org/10.3390/s23125702.
15. Khuralay Moldamurat, Yerzhan Seitkulov, Sabyrzhan Atanov, Makhabbat Bakyt, and Banu Yergaliyeva, "Enhancing cryptographic protection, authentication, and authorization in

cellular networks: a comprehensive research study," International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, vol. 14, no. 1, pp. 479–479, Feb. 2024, doi: https://doi.org/10.11591/ijece.v14i1.pp479-487.

16. V. Venkataramanan, G. Kavitha, M. Robinson. Joel, and J Lenin, "Forest Fire Detection and Temperature Monitoring Alert using IoT and Machine Learning Algorithm," Jan. 2023, doi: https://doi.org/10.1109/icssit55814.2023.10061086.
17. R. K. Dwivedi, R. Kumar, and R. Buyya, "Gaussian Distribution-Based Machine Learning Scheme for Anomaly Detection in Healthcare Sensor Cloud," International Journal of Cloud Applications and Computing, vol. 11, no. 1, pp. 52–72, Jan. 2021, doi: https://doi.org/10.4018/ijcac.2021010103.
18. L. Li et al., "Estimation of Ground Water Level (GWL) for Tropical Peatland Forest Using Machine Learning," IEEE Access, vol. 10, pp. 126180–126187, Jan. 2022, doi: https://doi.org/10.1109/access.2022.3225906.
19. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Access, vol. 7, no. 1, pp. 82721–82743, 2019, doi: https://doi.org/10.1109/access.2019.2924045.
20. Makhabbat B., Khuralay M., Assem K., Adil M. and Dina S., "Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives" CEUR Workshop Proceedings, Volume 36802024, 8th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2023, Almaty 6 December 2023 through 7 December 2023, Code 199323.
21. U. Dampage, L. Bandaranayake, R. Wanasinghe, K. Kottahachchi, and B. Jayasanka, "Forest fire detection system using wireless sensor networks and machine learning," Scientific Reports, vol. 12, no. 1, Jan. 2022, doi: https://doi.org/10.1038/s41598-021-03882-9.
22. W. Benzekri, A. El, O. Moussaoui, and M. Berrajaa, "Early Forest Fire Detection System using Wireless Sensor Network and Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 11, no. 5, 2020, doi: https://doi.org/10.14569/ijacsa.2020.0110564.
23. P. Dasari, G. K. J. Reddy, and A. Gudipalli, "Forest fire detection using wireless sensor networks," International Journal on Smart Sensing and Intelligent Systems, vol. 13, no. 1, pp. 1–8, 2020, doi: https://doi.org/10.21307/ijssis-2020-006.
24. B. Kizilkaya, E. Ever, H. Y. Yatbaz, and A. Yazici, "An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks," ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 18, no. 2, pp. 1–21, May 2022, doi: https://doi.org/10.1145/3473037.
25. Bakyt, M., Moldamurat, Kh., Satybaldina, D.Zh., Yurkov, N.K., MODELING INFORMATION SECURITY THREATS FOR THE TERRESTRIAL SEGMENT OF SPACE COMMUNICATIONS, CEUR Workshop Proceedings, Volume 33822022 7th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2022, Almaty 20 October 2022 through 21 October 2022, Code 188290.

26. M. A. El abbassi, A. Jilbab, and A. Bourouhou, "Efficient Forest Fire Detection System Based on Data Fusion Applied in Wireless Sensor Networks," International Journal on Electrical Engineering and Informatics, vol. 12, no. 1, pp. 1–18, Mar. 2020, doi: https://doi.org/10.15676/ijeei.2020.12.1.1.
27. A. Mashat, N. Gharaei, and A. M. Alabdali, "An Energy-Efficient Wireless Power Transmission-Based Forest Fire Detection System," Computers, Materials & Continua, vol. 72, no. 1, pp. 441–459, 2022, doi: https://doi.org/10.32604/cmc.2022.024131.
28. V. Dubey, P. Kumar, and N. Chauhan, "Forest Fire Detection System Using IoT and Artificial Neural Network," International Conference on Innovative Computing and Communications, pp. 323–337, Nov. 2018, doi: https://doi.org/10.1007/978-981-13-2324-9_33.
29. P. Barmpoutis, T. Stathaki, K. Dimitropoulos, and N. Grammalidis, "Early Fire Detection Based on Aerial 360-Degree Sensors, Deep Convolution Neural Networks and Exploitation of Fire Dynamic Textures," Remote Sensing, vol. 12, no. 19, p. 3177, Sep. 2020, doi: https://doi.org/10.3390/rs12193177.
30. A.Khan, B. Hassan, S. Khan, R. Ahmed, and A. Abuassba, "DeepFire: A Novel Dataset and Deep Transfer Learning Benchmark for Forest Fire Detection," Mobile Information Systems, vol. 2022, pp. 1–14, Apr. 2022, doi: https://doi.org/10.1155/2022/5358359.

М.А. Бақыт, Х. Молдамұрат, С.К. Атанов, Д. Калманова

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Төмен орбиталық ұшақтар үшін орман өрттерін бақылауға арналған жоғары жылдамдықты деректерді шифрлау және геоақпараттық жүйе

Аңдатпа. Мақалада орман өрттерін бақылау және болжау міндеттерін шешу кезінде төмен орбиталық ұшу аппараттарынан (ТОҰА) алынған деректердің қауіпсіздігін қамтамасыз ету мәселесі қарастырылады. Зерттеудің өзектілігі ТОҰА-нан алынған Жерді қашықтықтан зондтау (ЖҚЗ) деректерінің ұлғаюына және оларды жедел өңдеу және рұқсатсыз кіруден қорғау қажеттілігіне байланысты. ТОҰА-ның шектеулі есептеу ресурстарына бейімделген жылдам әрекет ететін деректерді шифрлау жүйесін әзірлеуді және ЖҚЗ деректерін талдау және түсіндіру үшін геоақпараттық жүйені (ГАЖ) құруды қамтитын кешенді тәсіл ұсынылады. ГАЖ өртті автоматты түрде анықтауға, өрттің таралу динамикасын модельдеуге және зақымдану аймағын бағалауға мүмкіндік беретін аэроғарыштық суреттерді интеллектуалды өңдеу модульдерімен жабдықталған. Деректерді беру мен өңдеудің барлық кезеңдерінде құпиялылық пен тұтастықты қамтамасыз ету үшін шифрлау жүйесін ГАЖ-мен біріктіруге ерекше назар аударылады. Мақалада ұсынылған шешімдерді эксперименттік тексеру нәтижелері, олардың тиімділігі мен орман өрттерін бақылау үшін практикалық маңыздылығы көрсетілген.

Түйін сөздер: төмен орбиталық ұшу аппараттары, деректер қауіпсіздігі, шифрлау, географиялық ақпараттық жүйе, орман өрттері, деректерді өндіру, аэроғарыштық деректер.

М.А.Бакыт, Х.Молдамурат, С.К.Атанов, Д. Калманова

Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан

Высокоскоростная система шифрования данных и геоинформации для мониторинга лесных пожаров для низкоорбитальных самолетов

Аннотация. В статье рассматривается проблема обеспечения безопасности данных, получаемых с низкоорбитальных летательных аппаратов (НОЛА), при решении задач мониторинга и прогнозирования лесных пожаров. Актуальность исследования обусловлена возрастающим объемом данных дистанционного зондирования Земли (ДЗЗ), получаемых с НОЛА, и необходимостью их оперативной обработки и защиты от несанкционированного доступа. Предлагается комплексный подход, включающий разработку быстродействующей системы шифрования данных, адаптированной к ограниченным вычислительным ресурсам НОЛА, и создание геоинформационной системы (ГИС) для анализа и интерпретации данных ДЗЗ. ГИС оснащена модулями интеллектуальной обработки аэрокосмических снимков, позволяющими автоматически обнаруживать очаги возгорания, моделировать динамику распространения пожара и оценивать площадь поражения. Особое внимание уделено интеграции системы шифрования с ГИС для обеспечения конфиденциальности и целостности данных на всех этапах их передачи и обработки. В статье представлены результаты экспериментальной проверки предлагаемых решений, демонстрирующие их эффективность и практическую значимость для мониторинга лесных пожаров.

Ключевые слова: низкоорбитальные летательные аппараты, безопасность данных, шифрование, географическая информационная система, лесные пожары, интеллектуальная обработка данных, аэрокосмические данные.

References

1. None Amrita, Chika Paul Ekwueme, Ibrahim Hussaini Adam, and A. Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” EAI endorsed transactions on internet of things, vol. 10, Mar. 2024, doi: https://doi.org/10.4108/eetiot.5565.
2. S. Kumari, P. Snehil, S. Kumar, P. Kumari, P. Kumari, and S. Karmakar, “A Study on Lightweight Cryptography Algorithm for Internet of Things,” SSRN Electronic Journal, 2020, doi: https://doi.org/10.2139/ssrn.3611487.
3. L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, “A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things,” IEEE Access, vol. 8, pp. 220165–220187, 2020, doi: https://doi.org/10.1109/access.2020.3041327.
4. R. H. C and G. C. D, “Privacy-aware novel lightweight cryptography mechanism for IoT (Internet of Things) Security,” Multimedia Tools and Applications, vol. 83, no. 31, pp. 76389–76404, Feb. 2024, doi: https://doi.org/10.1007/s11042-024-18517-0.

5. K. Moldamurat, A. Tulembayeva, A. Ryspaev, N. Belgibekov, L. Peryakina, and M. Bakyt, “Computer program in sign language for controlling mobile objects and communicating with people,” International Journal of Public Health Science (IJPHS), vol. 14, no. 1, p. 502, Mar. 2015, doi: https://doi.org/10.11591/ijphs.v14i1.24544.
6. X. Lu and X. Cheng, “A Secure and Lightweight Data Sharing Scheme for Internet of Medical Things,” IEEE Access, vol. 8, pp. 5022–5030, 2020, doi: https://doi.org/10.1109/access.2019.2962729.
7. H. Li, C. Lan, X. Fu, C. Wang, F. Li, and H. Guo, “A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing,” Sensors, vol. 20, no. 17, p. 4720, Aug. 2020, doi: https://doi.org/10.3390/s20174720.
8. J. Tian and X. Jing, “A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage,” IEEE Access, vol. 7, pp. 68071–68082, 2019, doi: https://doi.org/10.1109/access.2019.2916889.
9. Chandrashekhar Meshram et al., “A Provably Secure Lightweight Subtree-Based Short Signature Scheme With Fuzzy User Data Sharing for Human-Centered IoT,” IEEE Access, vol. 9, pp. 3649–3659, Jan. 2021, doi: https://doi.org/10.1109/access.2020.3046367.
10. Khuralay Moldamurat et al., “Improved unmanned aerial vehicle control for efficient obstacle detection and data protection,” IAES International Journal of Artificial Intelligence, vol. 13, no. 3, pp. 3576–3576, Jul. 2024, doi: https://doi.org/10.11591/ijai.v13.i3.pp3576-3587.
11. Z. Jiao et al., “A Deep Learning Based Forest Fire Detection Approach Using UAV and YOLOv3,” IEEE Xplore, Jul. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8850815?casa_token=meozekckbL8AAAAA:vaA9eCblb5z-lZc2u4rNsakxBDr7_z7--eBtXnazYIOXdS7ZfFiBkT_an0rQ9nQBOFRdriCkihgL (accessed Apr. 05, 2021).
12. B. Abdusalomov, B. M. S. Islam, R. Nasimov, M. Mukhiddinov, and T. K. Whangbo, “An Improved Forest Fire Detection Method Based on the Detectron2 Model and a Deep Learning Approach,” Sensors, vol. 23, no. 3, p. 1512, Jan. 2023, doi: https://doi.org/10.3390/s23031512.
13. H. C. Reis and V. Turk, “Detection of forest fire using deep convolutional neural networks with transfer learning approach,” Applied Soft Computing, vol. 143, p. 110362, Aug. 2023, doi: https://doi.org/10.1016/j.asoc.2023.110362.
14. S.-Y. Kim and A. Muminov, “Forest Fire Smoke Detection Based on Deep Learning Approaches and Unmanned Aerial Vehicle Images,” Sensors, vol. 23, no. 12, p. 5702, Jan. 2023, doi: https://doi.org/10.3390/s23125702.
15. Khuralay Moldamurat, Yerzhan Seitkulov, Sabyrzhan Atanov, Makhabbat Bakyt, and Banu Yergaliyeva, “Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study,” International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering, vol. 14, no. 1, pp. 479–479, Feb. 2024, doi: https://doi.org/10.11591/ijece.v14i1.pp479-487.

16. V. Venkataramanan, G. Kavitha, M. Robinson. Joel, and J Lenin, “Forest Fire Detection and Temperature Monitoring Alert using IoT and Machine Learning Algorithm,” Jan. 2023, doi: https://doi.org/10.1109/icssit55814.2023.10061086.
17. R. K. Dwivedi, R. Kumar, and R. Buyya, “Gaussian Distribution-Based Machine Learning Scheme for Anomaly Detection in Healthcare Sensor Cloud,” International Journal of Cloud Applications and Computing, vol. 11, no. 1, pp. 52–72, Jan. 2021, doi: https://doi.org/10.4018/ijcac.2021010103.
18. L. Li et al., “Estimation of Ground Water Level (GWL) for Tropical Peatland Forest Using Machine Learning,” IEEE Access, vol. 10, pp. 126180–126187, Jan. 2022, doi: https://doi.org/10.1109/access.2022.3225906.
19. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, vol. 7, no. 1, pp. 82721–82743, 2019, doi: https://doi.org/10.1109/access.2019.2924045.
20. Makhabbat B., Khuralay M., Assem K., Adil M. and Dina S., “Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives” CEUR Workshop Proceedings, Volume 36802024, 8th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2023, Almaty 6 December 2023 through 7 December 2023, Code 199323.
21. U. Dampage, L. Bandaranayake, R. Wanasinghe, K. Kottahachchi, and B. Jayasanka, “Forest fire detection system using wireless sensor networks and machine learning,” Scientific Reports, vol. 12, no. 1, Jan. 2022, doi: https://doi.org/10.1038/s41598-021-03882-9.
22. W. Benzekri, A. El, O. Moussaoui, and M. Berrajaa, “Early Forest Fire Detection System using Wireless Sensor Network and Deep Learning,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 5, 2020, doi: https://doi.org/10.14569/ijacsa.2020.0110564.
23. P. Dasari, G. K. J. Reddy, and A. Gudipalli, “Forest fire detection using wireless sensor networks,” International Journal on Smart Sensing and Intelligent Systems, vol. 13, no. 1, pp. 1–8, 2020, doi: https://doi.org/10.21307/ijssis-2020-006.
24. B. Kizilkaya, E. Ever, H. Y. Yatbaz, and A. Yazici, “An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks,” ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 18, no. 2, pp. 1–21, May 2022, doi: https://doi.org/10.1145/3473037.
25. Bakyt, M., Moldamurat, Kh., Satybaldina, D.Zh., Yurkov, N.K., MODELING INFORMATION SECURITY THREATS FOR THE TERRESTRIAL SEGMENT OF SPACE COMMUNICATIONS, CEUR Workshop Proceedings, Volume 33822022 7th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2022, Almaty 20 October 2022 through 21 October 2022, Code 188290.
26. M. A. El abbassi, A. Jilbab, and A. Bourouhou, “Efficient Forest Fire Detection System Based on Data Fusion Applied in Wireless Sensor Networks,” International Journal on Electrical Engineering and Informatics, vol. 12, no. 1, pp. 1–18, Mar. 2020, doi: https://doi.org/10.15676/ijeei.2020.12.1.1.

27. A. Mashat, N. Gharaei, and A. M. Alabdali, “An Energy-Efficient Wireless Power Transmission-Based Forest Fire Detection System,” Computers, Materials & Continua, vol. 72, no. 1, pp. 441–459, 2022, doi: https://doi.org/10.32604/cmc.2022.024131.
28. V. Dubey, P. Kumar, and N. Chauhan, “Forest Fire Detection System Using IoT and Artificial Neural Network,” International Conference on Innovative Computing and Communications, pp. 323–337, Nov. 2018, doi: https://doi.org/10.1007/978-981-13-2324-9_33.
29. P. Barmpoutis, T. Stathaki, K. Dimitropoulos, and N. Grammalidis, “Early Fire Detection Based on Aerial 360-Degree Sensors, Deep Convolution Neural Networks and Exploitation of Fire Dynamic Textures,” Remote Sensing, vol. 12, no. 19, p. 3177, Sep. 2020, doi: https://doi.org/10.3390/rs12193177.
30. A. Khan, B. Hassan, S. Khan, R. Ahmed, and A. Abuassba, “DeepFire: A Novel Dataset and Deep Transfer Learning Benchmark for Forest Fire Detection,” Mobile Information Systems, vol. 2022, pp. 1–14, Apr. 2022, doi: https://doi.org/10.1155/2022/5358359.

Information about the authors:

Bakyt M.A. – corresponding author, PhD student of the Department of Information Security, IT Faculty at the L.N. Gumilyov ENU.
Moldamurat Kh. – Associate Professor of the Department of Space Technique And Technology at the L.N. Gumilyov ENU, Astana, Kazakhstan, 54 Syganak str., 010000, Astana, Kazakhstan
Atanov S.K. – professor in the Department of CSE at Gumilyov ENU, Astana, Kazakhstan, 54 Syganak str., 010000, Astana, Kazakhstan
Kalmanova D. – acting Associate Professor of the Department of "Space Engineering and Technology"at the L.N. Gumilyov ENU, Astana, Kazakhstan, 2 Satbayev str., 010000, Astana, Kazakhstan

Бакыт М.А. – автор для корреспонденции, докторант кафедры информационной безопасности факультета информационных технологий ЕНУ им. Л.Н. Гумилева.
Молдамурат Х. – доцент кафедры космической техники и технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан, ул. Сыганак, 54, 010000, Астана, Казахстан
Атанов С.К. – профессор кафедры КСО ЕНУ им. Л.Н. Гумилева, Астана, Казахстан, ул. Сыганак, 54, 010000, Астана, Казахстан
Калманова Д. – и.о. доцента кафедры «Космическая техника и технологии» ЕНУ им. Л.Н. Гумилева, Астана, Казахстан, ул. Сатбаева, 2, 010000, Астана, Казахстан

Бақыт М. А. - хат-хабар авторы, Л.Н. Гумилев ат. ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының докторанты.
Молдамурат Х. - Л.Н. Гумилев ат. ЕҰУ Ғарыштық техника және технологиялар кафедрасының доценті, Астана, Қазақстан, Сығанақ көшесі, 54, 010000, Астана, Қазақстан
Атанов С.К. – Л.Н. Гумилев ат. ЕҰУ КӘЖ кафедрасының профессоры, Астана, Қазақстан, Сығанақ көшесі, 54, 010000, Астана, Қазақстан
Қалманова Д. – Л.Н. Гумилев ат. ЕҰУ «Ғарыштық техника және технологиялар» кафедрасының доцентінің м. а., Астана, Қазақстан, Сәтбаев көшесі, 2, 010000, Астана, Қазақстан