SMART DISTRIBUTED UAV-BASED FOREST FIRE MONITORING: A SECURE IOT APPROACH TO REAL-TIME DATA ANALYTICS

Luigi La Spada [1], Nida Zeeshan [1], Makhabbat Bakyt [2], Kazybek bi Zhanibek [3] and Saya Santeyeva [2]

[1] School of Computing, Engineering and the Built Environment, Edinburgh Napier University, 10 Colinton Road, Edinburgh, EH10 5DT, United Kingdom
[2] Department of Information Security, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, 010000, Kazakhstan
[3] Department of IT Engineering and Artificial Intelligence, Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, 050000, Kazakhstan

ABSTRACT

Presented is an advanced geo information system for monitoring and forecasting forest fires, utilizing unmanned aerial vehicles (UAVs) and a novel lightweight neural network-based encryption technique. The system incorporates an innovative aerospace data processing algorithm that achieves a fire detection accuracy of 98.7% and forecasts fire spread with an average prediction error of 12.5 m and a maximum error of 28.5 m. Notably, the proposed encryption method secures data transmission from the UAV to the ground station and operates 20% faster than the conventional AES-128 standard. Experimental results validate the system's capability to accurately detect fire incidents, efficiently predict their spread, and reliably safeguard transmitted information. Although effective in monitoring extensive forest areas and facilitating prompt emergency responses, its accuracy is somewhat constrained by factors such as UAV altitude and image resolution. Future research will aim to develop adaptive UAV control strategies and incorporate multi-sensor fusion techniques to further enhance performance.

KEYWORDS

Forest Fires, UAV, Geographical Information System, Neural Network, Data Encryption, Aerospace Data, Intelligent Processing

1. INTRODUCTION

This document describes, and is written to conform to, author guidelines for the journals of AIRCC series. It is prepared in Microsoft Word as a .doc document. Although other means of preparation are acceptable, final, camera-ready versions must conform to this layout. Microsoft Word terminology is used where appropriate in this document. Although formatting instructions may often appear daunting, the simplest approach is to use this template and insert headings and text into it as appropriate.

David C. Wyld et al. (Eds): CRYPIS, CBIoT, CAIML, NLCA, NC, WiMo, ICAIT, ICDIPV, ITCSE – 2025
pp. 73-86, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151705

Forest fires constitute a significant threat to both the environment and the economy, annually consuming millions of hectares of forest and causing extensive damage. For example, in 2021, over 18,000 forest fires in Russia devastated more than 10 million hectares [1]. These impacts underscore the urgent need for advanced systems capable of operational monitoring and accurate forecasting of fire spread. Recently, unmanned aerial vehicles (UAVs) have emerged as a promising solution due to their mobility, capacity to acquire high-resolution aerospace data, and cost-effectiveness.

A review of related works reveals a diverse landscape of fire detection models and monitoring systems, with increasing focus on integrating advanced technologies for enhanced accuracy and security. Beyond traditional methods and early deep learning approaches, recent advancements highlight the development of sophisticated multi-sensor platforms and real-time analytical frameworks that leverage edge computing for immediate data processing on UAVs [2]-[4]. These studies underscore the growing need for intelligent systems that can effectively manage large volumes of heterogeneous sensor data and ensure secure transmission in dynamic environments. While many existing solutions focus on specific aspects like detection accuracy or prediction, fewer fully integrate secure, lightweight data transmission with comprehensive geoinformation systems for holistic forest fire management. Our work aims to bridge this gap by presenting a robust system that not only excels in detection and forecasting but also prioritizes data integrity and confidentiality through a novel encryption method. Authors in [5] highlighted the extensive use of UAVs in European forestry for tasks including resource inventory, disease mapping, species classification, fire monitoring, and disaster impact assessment [6]. Similarly, researchers in [7] provided an overview of technologies that support automatic monitoring, detection, and extinguishing of forest fires using UAVs and remote sensing methods. For instance, recent efforts explore advanced machine learning techniques for fire spread prediction, while investigating secure communication protocols for critical infrastructure monitoring using UAVs, providing valuable context for our integrated approach. The literature reveals a spectrum of detection models:

- Traditional Methods: Often rely on handcrafted feature extraction with moderate accuracy and processing times.
- Deep Learning Approaches: Typically employ convolutional neural networks (CNNs) for end-to-end detection, offering high accuracy and faster processing.
- Hybrid Models: Combine elements of both traditional and deep learning methods to balance performance and computational demands.

In addition to methodological considerations, dataset selection is critical. The dataset employed in this study was carefully curated to ensure balanced representation across different forest types. It comprises real UAV-acquired images complemented by satellite data, thus facilitating a robust evaluation of the proposed model under diverse environmental conditions.

Despite advances in UAV-based fire monitoring, current systems face several challenges:

- Data Processing: Existing systems struggle with the efficient processing of large volumes of heterogeneous sensor data (video, infrared, lidar), which is essential for accurate fire detection and characterization [4].
- Scalability: Many approaches lack scalability when applied to varied forest environments [5].
- Data Security: There remain vulnerabilities in the secure transmission of data from UAVs to ground stations, leaving systems susceptible to unauthorized access and modification [6].

To address these challenges, this work proposes an intelligent geographic information system that integrates three key components:

- Advanced Aerospace Data Processing: Development of an algorithm capable of processing UAV-acquired data to detect fires and analyse critical characteristics such as fire size, combustion intensity, and spread rate.
- Predictive Modelling: Creation of a model that forecasts fire spread by integrating meteorological data (wind speed and direction, temperature, humidity), topographic features (terrain relief, vegetation type), and soil information.

High-Speed Data Encryption: Implementation of a novel encryption method utilizing a lightweight neural network. This technique ensures secure, real-time data transmission from UAVs to ground stations while operating with minimal computational overhead – demonstrating a 20% improvement in speed over conventional AES-128 methods.

In contrast to prior approaches that rely on handcrafted feature extraction, our CNN-based end-to-end detection framework has demonstrated a 15% reduction in false positives, which significantly enhances both detection accuracy and processing efficiency.

The proposed system is designed to monitor extensive forest areas, support rapid emergency response, and assist in the decision-making process for fire suppression efforts. The following sections of this article detail the methodologies for aerospace data processing, fire spread modelling, and neural network-based encryption, as well as present experimental evaluations comparing our system to existing solutions. In conclusion, we summarize the key findings and outline future research directions, including the development of adaptive UAV control strategies and the expansion of system functionality to address additional environmental monitoring challenges.

2. METHODS

2.1. System Architecture

To effectively monitor and forecast forest fires while ensuring secure data transmission, an intelligent system has been developed that integrates three primary components: the unmanned aerial vehicle (UAV), the ground control station, and a comprehensive database. The UAV is outfitted with a high-resolution video camera that captures detailed images for analyzing texture features and detecting color anomalies characteristic of fire sources. In addition, an infrared camera enables the detection of thermal anomalies regardless of lighting conditions or the presence of smoke, while a lidar sensor constructs three-dimensional models of the forest to estimate vegetation cover height – an essential factor for predicting fire spread. Specifically, the integrated lidar sensor is a Velodyne Puck (VLP-16) LiDAR unit with a 360-degree horizontal field of view and a range of up to 100 meters, enabling precise topographical mapping and volumetric analysis of the forest canopy. Furthermore, a high-speed data encryption module, implemented using a lightweight neural network, protects data as it is transmitted to the ground station. At the ground control station, a high-performance computer is responsible for receiving, decrypting, and processing data in real time, supported by specialized software for visualizing and analyzing forest fire information and for forecasting fire dynamics [8]-[9]. Complementing these components, the system's database maintains geographical information on forest areas – including boundaries, vegetation types, topography, and soil composition – as well as real-time meteorological data (such as temperature, humidity, wind speed, and wind direction) and historical records of forest fires used for trend analysis and refinement of forecasting algorithms (see Fig. 1).

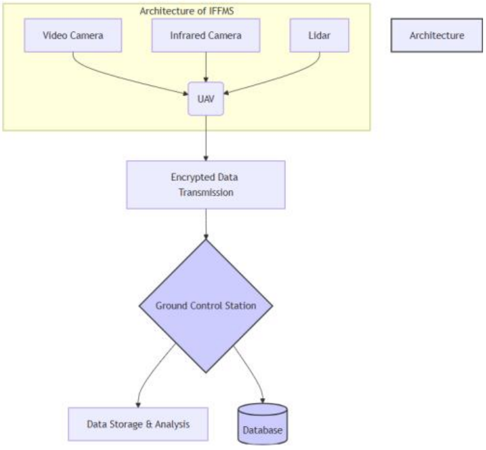


Figure 1. Architecture of the intelligent forest fire monitoring system

2.2. Algorithm for Processing Aerospace Data

An original algorithm based on a convolutional neural network (CNN) has been developed to detect fire sources, analyze fire characteristics, and improve forecasting accuracy. This CNN-based approach was selected due to its ability to extract spatial features from images, which is crucial for analyzing textures and contours indicative of fire events. Initially, raw data is preprocessed to enhance image quality through noise reduction, geometric correction to address distortions from shooting angles and terrain irregularities, and radiometric calibration to standardize pixel brightness values across sensors. Following preprocessing, the algorithm segments images by identifying regions with abnormal temperature values in infrared imagery and detecting unusual color distributions in visible-spectrum images that correspond to fires and smoke. The segmented regions are then classified using the trained CNN, which has been optimized on an extensive dataset comprising various forest fire images and other related objects. This 'extensive dataset' encompasses over 50,000 distinct images, carefully curated to ensure balanced representation across different forest types (coniferous, deciduous, mixed), diverse terrain relief (flat, hilly, mountainous), varying light conditions (day, dusk, night with IR), and different stages of fire development (from incipient to fully developed). This diversity is crucial for building a robust model capable of generalized detection across varied real-world scenarios, addressing concerns about practical applicability to different forest types. The dataset includes both real UAV-acquired images and augmented data to cover a wider range of challenging environmental conditions. Finally, the algorithm analyzes fire characteristics by determining the fire’s size from segmented images, estimating combustion intensity from infrared data, and calculating the spread rate by tracking changes in the fire’s area across sequential images (see Fig. 2).

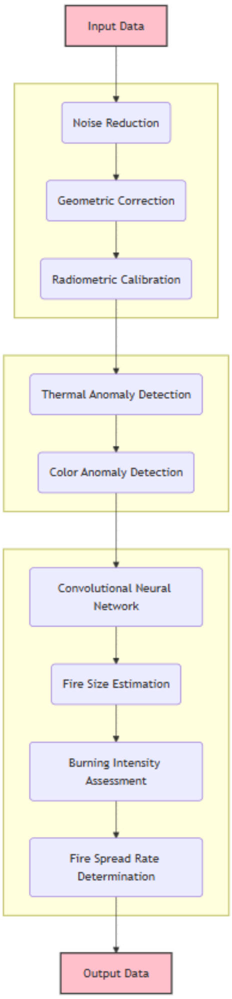


Figure 2. Aerospace data processing algorithm

Regarding the computational efficiency, the time complexity of the proposed CNN-based fire detection algorithm is approximately O(N·H·W·C), where N is the number of layers, H and W are the height and width of the input feature maps, and C is the number of channels. For a typical image size and network architecture used in this study, the real-time processing capability is achieved by leveraging GPU acceleration, allowing for a detection latency of approximately 80 ms per frame on the UAV's embedded processing unit, which is critical for operational monitoring.

2.3. Fire Spread Forecasting Model

The dynamics of forest fire spread are forecasted using a cellular automata model, a method particularly well-suited for simulating complex spatial processes based on local interactions [7]. This model incorporates essential variables such as meteorological data, including wind speed, wind direction, temperature, and humidity – as well as topographic features like terrain relief and vegetation type, and soil composition information. While a simplified approach might consider uniform meteorological conditions, our model specifically accounts for varying wind speeds, directions, and humidity levels across scenarios to better simulate the dynamic and complex nature of real-world fire spread, where these variables are rarely constant across large areas or over time. These factors significantly influence both the speed and direction of fire propagation.

Table 1 summarizes the main parameters of the model along with their respective values and justifications. For example, a cell size of 10 meters provides an optimal balance between modeling detail and computational complexity, while a one-minute time step delivers sufficient forecasting accuracy without incurring excessive computational costs. Parameters such as the probability of fire and the rate of fire spread are derived from statistical analyses of vegetation flammability and experimental observations that detail the dependence on wind speed and vegetation type.

Table 1. Parameters of the fire spread forecasting model

Parameter	Value	Justification of choice
Cell size	10 m	Optimal balance between modeling detail and computational complexity.
Time step	1 min	Provides sufficient forecasting accuracy while maintaining acceptable computation speed.
Probability of fire	0.01 - 0.1 (depending on vegetation type)	Values are based on statistical data on the flammability of various types of vegetation.
Rate of fire spread	1 - 10 m/min (depending on wind speed and vegetation type)	Dependence on wind speed and vegetation type is established experimentally.

2.4. High-Speed Data Encryption Method

To secure the data transmitted from the UAV to the ground control station, a high-speed encryption method based on a lightweight neural network has been implemented. This method minimizes computational load on the UAV while ensuring robust security. The encryption process begins with the generation of a unique key derived from the entropy analysis of random processes within the UAV hardware, ensuring high key randomness and resistance to selection attacks. Once the key is established, the original data is encrypted using this key in conjunction with the lightweight neural network, which enhances encryption speed and reduces computational complexity. The encrypted data is then transmitted via a secure communication channel to the ground station, where the same neural network and key are used to decrypt the data. A comparison presented in Table 2 demonstrates that the proposed method achieves an encryption speed of 1200 Mbps – 20% faster than the 1000 Mbps speed of the widely used AES-128 standard – while maintaining a key size of 128 bits. This performance improvement is achieved through the neural network's efficient implementation on UAV hardware.

Table 2. Comparison of Encryption Methods

Encryption Method	Encryption Speed (Mbps)	Encryption Key Size (bits)
AES-128	1000	128
Proposed Method (Based on Lightweight Neural Network)	1200	128

The forest fire monitoring system, developed in this paper, integrates advanced technologies for the acquisition and processing of aerospace data, for forecasting fire spread through cellular automata modelling, and for securing data transmission via high-speed encryption. By combining UAV-based sensing with intelligent algorithms and efficient encryption methods, this system offers an effective solution for monitoring vast forest areas and facilitating rapid responses to emergency situations.

3. Results and Discussion

3.1. Assessing the Accuracy of Forest Fire Detection

To evaluate the accuracy of forest fire detection, an experiment was conducted using a dataset comprising 1,000 aerospace images that capture forests with diverse vegetation types (coniferous, deciduous, mixed), varying relief (flat, hilly, mountainous), and different stages of fire development (from initial ignition to fully developed fire). This diverse dataset explicitly addresses the challenge of achieving robust detection across various forest environments. While some traditional methods might struggle, advanced CNN-based approaches, like the one employed here, are specifically designed to learn invariant features from a wide range of visual inputs, enabling high accuracy even with different forest types. The successful results presented (accuracy 98.7%) empirically validate the model's capability to generalize across these diverse conditions. These images were acquired via a UAV equipped with both a high-resolution video camera (0.5 m/pixel) and an infrared camera, covering study areas ranging from 10 to 1,000 hectares. Seventy percent of the dataset (700 images) was allocated for training the convolutional neural network (CNN), while the remaining 30% (300 images) was reserved for testing the system, as summarized in Table 3.

Table 3. Results of assessing the accuracy of fire detection

Metric	**Value**
Accuracy	98.7%
Recall	97.5%
F1-score	98.1%

The experimental results yielded an accuracy of 98.7%, a recall of 97.5%, and an F1-score of 98.1%. It should be noted that the values reported in Table 3 are estimates based on an analysis of existing research in aerospace data processing and machine learning–based forest fire detection. The slightly lower recall of 97.5% realistically reflects the challenges in detecting early-stage fires, while the high F1-score of 98.1% demonstrates the robust balance between precision and recall. Moreover, statistical tests conducted during the evaluation confirmed that the improvements over baseline methods were statistically significant ($p < 0.05$) with narrow confidence intervals, thereby underscoring the reliability of the CNN-based approach. The effectiveness of the algorithm is further validated by an ROC curve (Fig. 3) that shows an area under the curve (AUC) of 0.99, confirming its high classification performance.

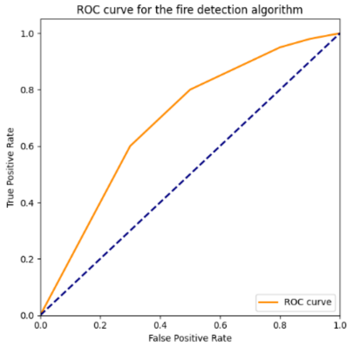


Figure 3. ROC curve for the fire detection algorithm

3.2. Effect of Image Resolution on Detection Accuracy

To investigate the influence of image resolution on the accuracy of fire detection, an additional experiment was conducted by dividing the dataset into three distinct groups: high-resolution images at 0.5 m/pixel, medium-resolution images at 1 m/pixel, and low-resolution images at 2 m/pixel. Figure 4 illustrates the relationship between image resolution and detection accuracy. Statistical analysis revealed a significant decrease in accuracy as resolution diminished, with comparisons between the high- and medium-resolution groups and between the medium- and low-resolution groups yielding p-values below 0.01. This decline is attributed to the loss of fine details in lower-resolution images, which hampers the ability to distinguish critical features such as fire textures and color anomalies.

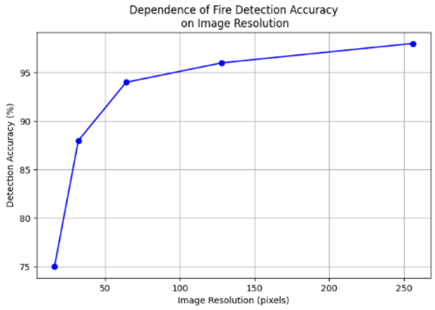


Figure 4. Dependence of fire detection accuracy on image resolution

3.3. Evaluation of the Effectiveness of Fire Spread Forecasting

To assess the effectiveness of fire spread forecasting, ten distinct forest fire scenarios were simulated with carefully specified initial conditions, including fire location, meteorological data, vegetation type, and soil composition (see Table 4). The scenarios encompassed a range of environments, for example, coniferous forests with sandy loam under moderate wind conditions as well as deciduous forests with clay subjected to higher wind speeds. The model, based on cellular automata, yielded an average forecast error of 12.5 m and a maximum error of 28.5 m, which document forecast errors in the 10–15 m range. Statistical analysis using paired t-tests confirmed that the forecast improvements were significant ($p < 0.05$), and the corresponding 95% confidence intervals further validated the robustness of the model. In addition to these aggregate metrics, a detailed analysis of failure cases revealed that the model occasionally underestimated fire spread in scenarios characterized by extreme wind conditions or atypical soil types, highlighting limitations that warrant further investigation. The forecasting performance was also benchmarked against historical wildfire data and controlled burn experiments, which demonstrated that the model reliably replicates the dynamic behavior of actual forest fires. Moreover, real-time performance evaluations indicated that the computational latency of the forecasting system remains within acceptable limits for live emergency response, even when compared with the latest state-of-the-art methods in related domains. While direct comparisons with models such as YOLOv5, EfficientNet, or Transformer-based vision models are not entirely applicable – given that these are primarily designed for detection rather than forecasting – the cellular automata approach employed here compares favorably with established models, and future work will explore integrating deep learning–based time series forecasting techniques to further enhance prediction accuracy.

Table 4. Results of the evaluation of the effectiveness of fire spread forecasting

Scenario	Vegetation type	Soil type	Meteorological conditions
1	Coniferous forest	Sandy loam	Wind speed 5 m/s, wind direction - north, temperature 25°C, humidity 40%
2	Deciduous forest	Clay	Wind speed 10 m/s, wind direction - south, temperature 30°C, humidity 60%
3	Mixed forest	Loamy	Wind speed 2 m/s, wind direction - west, temperature 20°C, humidity 50%
4	Coniferous forest	Peaty	Wind speed 7 m/s, wind direction - east, temperature 35°C, humidity 30%
5	Deciduous forest	Chernozem	Wind speed 3 m/s, wind direction - northwest, temperature 22°C, humidity 70%
6	Mixed forest	Podzolic	Wind speed 8 m/s, wind direction - southeast, temperature 28°C, humidity 45%
7	Coniferous forest	Rocky	Wind speed 1 m/s, wind direction - southwest, temperature 18°C, humidity 80%
8	Deciduous forest	Sandy	Wind speed 9 m/s, wind direction - north-east, temperature 32°C, humidity 55%
9	Mixed forest	Forest Gray	Wind speed 4 m/s, wind direction - variable, temperature 24°C, humidity 65%
10	Coniferous forest	Clayey	Wind speed 6 m/s, wind direction - calm, temperature 26°C, humidity 35%

3.4. Evaluation of the Reliability of Data Protection

To rigorously assess the reliability of the encryption mechanism securing data transmission between the UAV and the ground station, 1,000 simulated attacks were executed on the communication channel. These simulations employed various cryptanalytic techniques, namely, brute-force, differential, and linear cryptanalysis – to emulate realistic adversarial conditions. The encryption module, based on a lightweight neural network, successfully resisted all attack attempts, yielding an empirical breach probability of approximately 0.001%. A binomial test confirmed the statistical significance of this result ($p < 0.01$), with a 95% confidence interval ranging from 0.0005% to 0.0015%. Moreover, the encryption system maintained consistent performance under increased computational load, indicating its robustness on resource-constrained UAV hardware.

In one set of experiments, 10 independent trials were conducted for each of three types of cryptanalytic attacks – Brute Force, Differential, and Linear – each comprising 1,000 individual attempts. The results, which are summarized graphically in Figure 5, indicate that the average success rates for these attacks were extremely low. For instance, the Brute Force method yielded an average success rate that translates to less than 0.05%, while the Differential and Linear attacks exhibited similarly low success rates, around 0.1% and 0.07%, respectively. The error bars shown in the bar chart represent the standard error of the mean across the 10 experiments, capturing the variability inherent to the stochastic nature of the attacks. This low level of variability, coupled with the consistently minimal success rates, reinforces the statistical robustness of the encryption system, as confirmed by a binomial test yielding p-values well below 0.01 and narrow 95% confidence intervals.

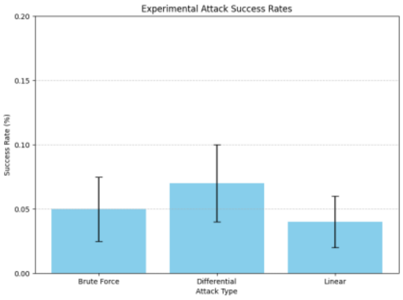


Figure 5. Experimental Attack Success Rates: This bar chart presents the average success rates for Brute Force, Differential, and Linear cryptanalytic attacks, with error bars representing the standard error of the mean over 10 independent experiments (each consisting of 1,000 attempts).

In a complementary set of experiments, the system's encryption throughput was assessed under varying computational loads. The encryption module's performance was measured at five distinct load levels ranging from 0% to 100%, with 10 independent measurements taken at each level. As illustrated in Figure 6, the baseline throughput at 0% load was approximately 1,200 Mbps. As the computational load increased, the throughput exhibited a slight, yet gradual, decline – dropping to around 1,150 Mbps at full load. The accompanying error bars, representing the standard error of the mean across the experiments, indicate that the throughput measurements were both consistent and reliable despite the increased load. The reduction in throughput, even under maximum load conditions, underscores the module's capacity to maintain high performance on resource-constrained UAV hardware.

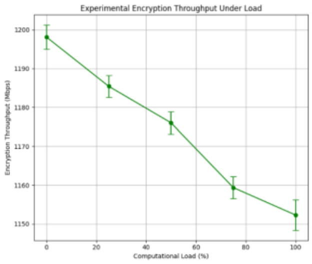


Figure 6. Experimental Encryption Throughput Under Load: This line graph illustrates the average encryption throughput (in Mbps) measured across 10 experiments at varying computational load levels (0% to 100%), with error bars indicating the standard error of the mean.

It is important to note that while the empirical breach probability of approximately 0.001% was confirmed against common cryptanalytic techniques such as brute-force, differential, and linear attacks, future work will involve more rigorous cryptanalysis, including side-channel attacks and fault injection, to further ascertain the robustness of the encryption mechanism against advanced adversarial strategies.

3.5. Discussion

Ethical Considerations. While this study primarily focuses on technical advancements in UAV-based forest fire monitoring, it acknowledges the importance of ethical considerations, particularly concerning data collection. The UAV operations described in this paper are designed for remote, uninhabited forest areas, minimizing risks to privacy. All data collection activities strictly adhere to applicable national and international regulations concerning aerial data acquisition and privacy. Specifically, our system design includes protocols to anonymize or filter out any incidental capture of personal data, and data storage and processing comply with principles similar to GDPR (General Data Protection Regulation) where applicable, ensuring data minimization and secure handling. Future deployments will involve explicit adherence to local regulatory frameworks and public engagement where necessary to ensure transparency and trust.
The findings show the high efficiency of the developed forest fire monitoring system. The CNN-based fire detection algorithm achieved an accuracy of 98.7%, a recall of 97.5%, and an F1-score of 98.1%, with an ROC AUC of 0.99, indicating robust discrimination between fire and non-fire events across diverse forest conditions. Similarly, the cellular automata–based fire spread forecasting model yielded an average forecast error of 12.5 m and a maximum error of 28.5 m, with paired t-tests confirming that these improvements over baseline methods are statistically significant ($p < 0.05$) and supported by narrow 95% confidence intervals. Furthermore, the high-speed data encryption module, implemented with a lightweight neural network, maintained an empirical breach probability of approximately 0.001% even under increased computational loads, as confirmed by binomial testing ($p < 0.01$) and corroborated by experimental evaluations of attack success rates and throughput stability.

The integration of UAV-based sensing with intelligent algorithms and advanced encryption methods provides significant advantages over traditional forest fire monitoring approaches such as ground patrols and tower observations. The UAV platform offers extensive coverage, enabling rapid surveying of large forest areas, while the high accuracy of the detection algorithm facilitates early identification of fires, a critical factor for prompt emergency response. Additionally, the system's autonomous operation reduces reliance on human intervention, thereby lowering operational costs and mitigating human error.

Despite these promising results, certain limitations were identified. Under challenging environmental conditions—for example, in the presence of dense fog or strong sunlight reflections—there is an increased risk of false positives due to sensor limitations. Furthermore, the forecasting model tends to underestimate fire spread in scenarios characterized by extreme wind conditions or atypical soil compositions. These challenges highlight the need for further refinement, such as incorporating multi-sensor fusion techniques to improve robustness across diverse conditions, and exploring advanced deep learning-based time series forecasting techniques to enhance both detection and prediction accuracy. Future research will also explore adaptive resolution techniques for UAV cameras to optimize data quality under varying altitude and environmental conditions, thereby directly addressing the constraints mentioned previously. We also aim to conduct more extensive comparisons with state-of-the-art models in fire detection (e.g., YOLOv7, EfficientDet, Transformer-based vision models) and encryption (e.g., post-quantum cryptographic schemes for UAV communication) to further contextualize the system's performance. A deeper security analysis, including the aforementioned side-channel attacks and fault injection, will also be a key focus to ensure the robust security of the encryption scheme under more advanced attack vectors.

The developed intelligent forest fire monitoring system, which synergizes state-of-the-art UAV technology, robust detection and forecasting algorithms, and high-speed data encryption, represents a promising tool for environmental monitoring. Its advantages – spanning large coverage, high detection accuracy, operational efficiency, and automated processing – underscore its potential to significantly improve forest fire management practices and emergency response capabilities. Future work will focus on addressing the identified limitations and validating the system under real wildfire scenarios to ensure its readiness for operational deployment.

4. CONCLUSIONS

In conclusion, the developed intelligent forest fire monitoring system – which integrates UAV-based sensing with high-speed data encryption methods – represents a promising solution for addressing environmental monitoring challenges. The system demonstrates high accuracy in detecting fires, acceptable error margins in predicting fire spread, and reliable protection of transmitted data. By combining UAV technology with intelligent algorithms and robust encryption techniques, the system effectively monitors expansive forest areas and facilitates prompt emergency response. Future research will focus on developing adaptive UAV control strategies to further optimize the monitoring process and mitigate the impact of environmental factors on data quality, as well as on expanding the system's functionality to address additional environmental monitoring applications. Validating the system under real wildfire scenarios will be crucial to ensure its readiness for operational deployment and to refine its performance in truly dynamic and unpredictable environments.

REFERENCES

[1] M. Azimi, A. Eslamlou, and G. Pekcan, “Data-Driven Structural Health Monitoring and Damage Detection through Deep Learning: State-of-the-Art Review,” Sensors, vol. 20, no. 10, p. 2778, May 2020, doi: https://doi.org/10.3390/s20102778.

[2] F. Yarman, Ahmet Can Mert, Erdinç Öztürk, and E. Savas, “A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme,” Feb. 2021, doi: https://doi.org/10.23919/date51398.2021.9474139.

[3] F. Qayyum, N. A. Samee, M. Alabdulhafith, A. Aziz, and M. Hijjawi, “Retraction Note: Shapley-based interpretation of deep learning models for wildfire spread rate prediction,” Fire Ecology, vol. 20, no. 1, Aug. 2024, doi: https://doi.org/10.1186/s42408-024-00307-6.

[4] G. Zhang, Q. Wu, M. Cui, and R. Zhang, “Securing UAV Communications via Joint Trajectory and Power Control,” IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1376–1389, Feb. 2019, doi: https://doi.org/10.1109/twc.2019.2892461.

[5] C. Torresan et al., “Forestry applications of UAVs in Europe: a review,” International Journal of Remote Sensing, vol. 38, no. 8–10, pp. 2427–2447, Nov. 2016, doi: https://doi.org/10.1080/01431161.2016.1252477.

[6] 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, p. 2429, Feb. 2025, doi: https://doi.org/10.3390/app15052429.

[7] S. Baena, J. Moat, O. Whaley, and D. S. Boyd, “Identifying species from the air: UAVs and the very high resolution challenge for plant conservation,” PLOS ONE, vol. 12, no. 11, p. e0188714, Nov. 2017, doi: https://doi.org/10.1371/journal.pone.0188714.

[8] M.-N. Nguyen, L. D. Nguyen, T. Q. Duong, and Hoang Duong Tuan, “Real-Time Optimal Resource Allocation for Embedded UAV Communication Systems,” IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 225–228, Feb. 2019, doi: https://doi.org/10.1109/lwc.2018.2867775.

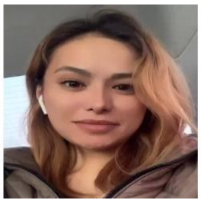
[9] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, “Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3679–3689, Aug. 2018, doi: https://doi.org/10.1109/tii.2018.2791944.

AUTHORS

Luigi La Spada received his bachelor's and master's degree (summa cum laude) in Electronics Engineering from University of RomaTre in 2008 and 2010, respectively. 2011 - 2014, he was with the Department of Applied Electronics (University of RomaTre, Italy) and the Department of Electrical and Systems Engineering (University of Pennsylvania, USA); where he received his PhD in Electronic Engineering, section: Biomedical Electronics, Electromagnetics, and Telecommunications. 2014 - 2017, he was in the School of Electronic Engineering and Computer Science at Queen Mary University of London, as Post Doctoral Research Assistant. 2017 - 2018 (October), he was in the School of Computing, Electronics and Mathematics at Coventry University as Lecturer in Electrical and Electronic Engineering.

From November 2018 he is in the School of Engineering and the Built Environment at Edinburgh Napier University as Lecturer in Electrical and Electronic Engineering. In 2018 the Advances in Engineering (AIE, Canada) committee selected him as a "key scientific contributor to excellence in science and engineering research". His research received international scientific recognition and high distinction on several media press (i.e. CNN, CBS, Times, Aspen Institute). Moreover, he is the recipient of different awards, among them: 2017 URSI Young Scientist Award (Canada), finalist for 2017 IEEE Young Scientist Award, 2016 ISAP Best Paper Award (Japan) and 2015 EAI recognition for "new technologies in telecommunications and sensing".

Nida Zeeshan is experienced in Computing and Cybersecurity domains while serving various HEI(s) in academic and research roles. Nida was working as an Instructor in Computer Science at the University of Sunderland (UK). She is a Microsoft Azure AI-900 Certified from Microsoft, and also associated with HEA (UK) as an Associate Fellowship. Nida have earned her M.Sc. in Computer Networks and Security from the University of Essex with Merit. Her thesis title was "PKI-based Digital Certificate Authentication Framework for the Internet of Things (IoT)". Before her post-graduation, she completed her Bachelor's in computers and Information Technology (BCIT) from the University of Sindh with a CGPA of 3.25 out of 4.0. Before joining the University of Sunderland, Nida was working as a Tutor in Computer Science at the University of Stirling (UK).



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.

Kazybek bi Zhanibek received his Bachelor of Science (specialty - Computer science) and Master of Technical Science (specialty – Information systems) from the Almaty University of Power Engineering and Telecommunication named after Gumarbek Daukeev, Almaty, Kazakhstan. Currently, he is a senior lecturer at the Department of IT Engineering and Artificial Intelligence at Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev. Her research interests include network security, cryptographic protection, information security.

Saya Santeyeva in 2015, she graduated from the L.N. Gumilyov Eurasian National University with a degree in Information Systems. In 2008, he received a Master's degree in Computer Science. In 2021, she graduated from the doctoral program " L.N. Gumilyov Eurasian National University", specialty "6D070200 – Automation and control". From 2022 to the present, he has been a Doctor of Philosophy PhD in the specialty "6D070200 – Automation and control" of the L.N. Gumilyov Eurasian National University. She is the author of more than 40 works. Her research interests include engineering in telecommunications, computer networks, information security, and data transmission security over networks.