A multimodal model makes it possible to assess a multimedia object as a potential carrier of a cyber threat by taking into account a set of heterogeneous features, including pixel-based, frequency-based, structural, metadata-related, and behavioral characteristics. Such representation allows the object to be analyzed not only as an image, video, or graphic file, but also as a complex information container in which hidden modifications may appear at different levels.

To protect web resources, it is advisable to combine statistical, structural, frequency-based, neural network, and behavioral methods within an integrated risk assessment framework. This combination increases the reliability of detecting hidden modifications in multimedia content, since each group of methods covers a specific class of indicators and compensates for the limitations of the others.

This approach reduces the detection system's reliance on a single type of indicator and enables it to respond more effectively to various methods of concealing threats. As a result, the assessment of multimedia content becomes more comprehensive and better adapted to the detection of hidden cyber threats in web environments.

1. Almehmadi L., Basuhail A., Alghazzawi D., Rabie O. Framework for Malware Triggering Using Steganography. Applied Sciences. – 2022. – Vol. 12, No. 16. – Article 8176. DOI: https://doi.org/10.3390/app12168176
2. Koch L., Oesch S., Chaulagain A., Adkisson M., Erwin S., Weber B. Toward the Detection of Polyglot Files. Proceedings of CSET 2022 – 15th Workshop on Cyber Security Experimentation and Test. – 2022. – P. 120–128. DOI: https://doi.org/10.1145/3546096.3546106
3. Denysiuk D., Savenko O., Lysenko S., Savenko B., Kashtalian A. Method for Detecting Steganographic Changes in Images Using Machine Learning. Proceedings of the 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Athens, Greece, 2023. – P. 1–6. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416453

Optimizing uav routes under conditions of restricted access to confidential objects

UDC 623.746.4-519:004

Юлія Ткач[1], Ігор Дюба[2]

Національний університет "Чернігівська політехніка",
[1]tkachym79@gmail.com, [2] idyuba@gmail.com

Introduction. Modern scenarios for the use of Unmanned Aerial Vehicles (UAVs) require solving complex routing problems in dynamic environments. This issue becomes particularly acute when planning flights over territories containing restricted access objects or critical infrastructure. Traditional approaches based on the complete bypass of "No-Fly Zones" lead to significant time and energy expenditures.

Problem Statement. This study considers the applied task of constructing a UAV route from point A to point C through a transit area B. Area B contains objects whose coordinates are confidential. It is necessary to minimize the travel time while ensuring

the non-disclosure of information regarding these objects by maintaining a safe distance D. The primary contradiction lies in the need for route optimization without providing the planning algorithm with the precise coordinates of the critical objects.

Research Methodology. A dual-level data access model was used to solve this problem. Unlike the classic model, which addresses security issues by bypassing the entire perimeter of area B, the proposed approach allows movement directly through area B using adaptive trajectory analysis.

The non-disclosure criterion is defined as preventing the UAV from approaching critical points closer than distance D. Furthermore, the pathfinding algorithm operates under conditions of informational uncertainty regarding the exact location of the objects, which satisfies confidentiality requirements.

To formalize the problem of safe UAV passage through area B, we introduce the following notations:

$P(t) = \big(x(t), y(t)\big)$ state vector (coordinates) of the UAV at a given moment in time t;

$Oi = (x_i, y_i)$ coordinates of the i - th critical object in area B, where $i\epsilon\{x_i, y_i\}$;

D - minimally permissible distance (radius of the non-disclosure zone).

The criterion of non-disclosure of information about objects within the framework of the two-level access model is defined as a system of restrictions on the trajectory of movement:

$$\forall t \in \left[T_{start}, T_{end}\right], \quad \forall i: \sqrt{(x(t) - x_i)^2 + (y(t) - y_i)^2} \geq D$$

At the same time, according to the confidentiality terms, the exact values of O_i are not transmitted to the global planning system. Instead, a 'contact function' is used, which is activated only when approaching the boundary D.

The route construction algorithm is based on iterative approximation to the target point C with dynamic adjustment of the movement vector when entering a restricted access zone.

Stages of algorithm implementation:

1. Global planning: Construction of a straight trajectory A → C. Determination of entry and exit points for region B.

2. Local monitoring: When located in region B, the system continuously analyzes the gradient of the "disclosure threat field."

3. Two-level verification:

- Level 1 (Zone access): Permission to stay in region B to shorten the path.
- Level 2 (Object access): Prohibition on entering radius D.

4. Adaptive correction: If the current trajectory leads to the violation of the condition |P(t) - Oi| < D, the algorithm calculates the tangent to the circle of radius D and changes course H with minimal deviation from the target.

Experimental Part. A series of 10,000 numerical experiments were conducted. Modeling conditions included:

Four objects were generated in area B following a uniform distribution.

Two types of routes were constructed: a guaranteed bypass (maximum) and an optimized route through area B with accuracy H.

Forbidden and restricted access zones were defined for the objects in area B.

Analysis of Results. Statistical data processing demonstrated that as the number of iterations increases, the distribution of results converges to a normal distribution.

The findings indicate that utilizing the dual-level model allows for an average flight time gain of 19% compared to the maximum bypass trajectory. Such an indicator is critically important for the operational planning of UAV missions, particularly in electronic warfare, reconnaissance, and monitoring tasks under time-sensitive conditions.

Conclusions.

1. The application of an adaptive trajectory model instead of rigid "No-Fly Zones" significantly increases the efficiency of UAV utilization.

2. The dual-level access model ensures reliable protection of confidential information regarding critical objects even during the physical transit of the vehicle through their location zone.

3. The results confirm the algorithm's stability under the random distribution of objects, allowing for its recommended integration into the intelligent control systems of autonomous unmanned complexes.

1. Zhou, Y., Ma, L., & Wen, M. (2015). Task-Constrained RBAC Model and Its Privilege Redundancy Analysis. 2nd ISCE, pp. 489–492.
2. Ren, M., et al. (2024). Conception of Foreign Heterogeneous EW UAV Cross Domain Cooperative Operations. ICAUS 2023, vol 1171.
3. Zhang, Y., et al. (2023). Modeling and simulation of UAVs swarm electromagnetic operation. Systems Engineering and Electronics, Vol. 45(7).

Кібербезпека систем розпізнавання мовлення в реальному часі

УДК 004.056

Олег Єгоров[1], Тарас Кравченко[2]

Український державний університет науки і технологій,
[1]egoroffoleg@ukr.net, [2]t.o.kravchenko@ust.edu.ua

Розвиток технологій синтезу мовлення та deepfake-голосу створює нові кіберзагрози для систем розпізнавання мовлення. Синтетичний голос може використовуватися для підміни особи, обходу голосової автентифікації і несанкціонованого доступу до інформаційних ресурсів. За таких умов традиційні підходи до розпізнавання мовлення, орієнтовані переважно на точність і швидкодію, не забезпечують достатнього рівня захисту даних.

Актуальність дослідження зумовлена поширенням голосових сервісів і одночасним зростанням доступності засобів генерації синтетичного мовлення. Для систем реального часу особливо важливим є своєчасне виявлення deepfake-голосу без істотного збільшення затримки обробки, оскільки від цього залежить безпека доступу до даних і надійність роботи мовних сервісів.

Метою роботи є підвищення рівня захисту даних у системах розпізнавання мовлення реального часу шляхом виявлення deepfake-голосу та синтетичного мовлення на основі інтелектуального аналізу аудіопотоку.