https://doi.org/10.31891/csit-2025-4-6
UDC 004.056:621.391

KASHTAN Vita, HNATUSHENKO Volodymyr
Dnipro University of Technology

ENTROPY-CRYPTOGRAPHIC APPROACH FOR TRANSMISSION OF SATELLITE DATA IN TELECOMMUNICATION NETWORKS

Amid rapid advances in satellite observations and increasing risks associated with high-resolution multispectral data downloads, stronger satellite image encryption techniques are becoming increasingly important. To address these challenges, the paper proposes a new cryptographic methodology based on entropy and nonlinear methods. This approach offers high resistance against brute-force attacks, generates a high-entropy key, and employs a dynamic non–linear transformation in multi-layered encryption, which is AES-256-bit encrypted. This comprehensive approach is designed to safeguard the security of satellite data in transit from modern cryptanalysis as it traverses communication networks. The approach begins with entropy-based initializations, iteratively expands the key space, and applies adaptive transformations to render the encrypted data highly unpredictable. Experiments with satellite images of various resolutions demonstrate that this approach is resistant to cryptanalysis. The evaluation included measuring entropy, analysing the correlation between neighbouring pixels, and testing resistance to statistical and frequency-based attacks. The encrypted images achieved entropy values close to the theoretical maximum and showed almost no correlation between adjacent pixels, demonstrating the strength and uniformity of the encryption process. Performance tests on systems with multiple threads and processors revealed clear links between execution time, data size, and the level of parallelization. Moderate parallelism provided the best speed improvements, and the method remained scalable for large datasets, making it suitable for high-throughput environments. This approach ensures strong satellite-image robustness in image size, content, or spectral characteristics. The flexible structure and good performance make it a promising candidate for future telecom networks and secure satellite data distribution systems.

Keywords: data transmission channels, adaptive encryption, and cryptographic protection.

КАШТАН Віта, ГНАТУШЕНКО Володимир
Національний технічний університет «Дніпровська політехніка»

ЕНТРОПІЙНО-КРИПТОГРАФІЧНИЙ ПІДХІД ПЕРЕДАЧІ СУПУТНИКОВИХ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

З огляду на швидке зростання систем супутникового моніторингу та підвищення ризиків під час передачі багатоспектральних супутникових даних, питання створення сучасних криптографічних засобів захисту супутникових знімків стає надзвичайно важливим. У статті представлено новий підхід до захисту супутникових даних, який базується на використанні ентропії та нелінійних методів. Запропонований в роботі підхід поєднує генерацію ключів з високою ентропією, складні динамічні перетворення та адаптивне багаторівневе шифрування, доповнене етапом AES-256. Це дозволяє забезпечити надійний захист, конфіденційність і цілісність супутникових зображень під час передачі через телекомунікаційні мережі, а також стійкість до сучасних криптоаналітичних атак. Ефективність методу підтверджена експериментами з різними типами зображень: було проведено оцінку ентропії зашифрованих даних, аналіз кореляції між сусідніми пікселями, перевірку стійкості до статистичних і частотних атак, а також тестування продуктивності на багатопотокових системах. Результати показали, що зашифровані зображення мають ентропію, близьку до максимальної, і майже нульову кореляцію між сусідніми пікселями, що свідчить про високу однорідність і надійність захисту. Дослідження часу виконання операцій шифрування виявило, що оптимальне прискорення досягається при використанні до чотирьох потоків, а для великих обсягів даних продуктивність залишається стабільною. Загалом, запропонований підхід забезпечує надійний захист супутникових знімків незалежно від їх розміру чи спектральних характеристик, що робить його перспективним для впровадження у сучасні телекомунікаційні системи.

Ключові слова: канали передачі даних, адаптивне шифрування, криптографічний захист.

Received / Стаття надійшла до редакції 01.09.2025
Accepted / Прийнята до друку 24.09.2025

Introduction

Satellite systems play a key role in the digital transformation of telecommunication networks. They not only deliver essential civilian services, such as broadcasting, navigation, and internet access to remote areas, but also provide crucial data transmission channels for government and defence. These channels are fundamental for information security and strategic management [1]. Under the conditions of full-scale military operations, when terrestrial communication infrastructure is exposed to destruction or cyberattacks, satellite systems remain the primary reliable channel for exchanging intelligence, navigation, and geospatial information. Leading corporations, such as SpaceX, Amazon, and OneWeb, among others, are actively developing next-generation satellite networks integrated with 6G architectures, underscoring the strategic importance of space-based communications for the secure functioning of future telecommunication systems [2–5]. Alongside the growing volume of transmitted data and the increasing complexity of network structures, the number of threats related to unauthorized access to satellite communication channels is also on the rise. Of particular importance are satellite images, which are crucial for geospatial analytics, emergency monitoring, intelligence operations, and environmental observation. Their loss or distortion may lead to significant consequences for national security and international stability.

Many modern satellite systems still use outdated or limited encryption methods that aren't designed for the unique features of multichannel image streams. It makes them more vulnerable to cyberattacks, as recent research has shown [6, 7]. As a result, developing adaptive encryption models that can protect the confidentiality and integrity of satellite data, even in the face of complex external threats, is a significant challenge for today's cryptography. The most considerable risk for satellite communication remains the potential leakage of geospatial data due to inadequate cryptographic protection.

Related works

Studies by the authors [8], [9] demonstrate that satellite data transmission systems face significant threats to the confidentiality, integrity, and availability of information. Critical threats include spoofing (GNSS spoofing [10]), manipulation of satellite imagery, and availability attacks such as jamming and denial-of-service (DoS/DDoS). Recent research has focused particularly on chaotic pseudorandom number generators, notably the three-dimensional generalized Hénon map [11], which is characterized by aperiodic dynamics and high sensitivity to initial conditions. Lyapunov exponents facilitate the identification of chaotic and hyperchaotic system regimes, while hardware implementations on field-programmable gate arrays (FPGAs) [12] confirm their resistance to hardware attacks and their applicability in secure systems, such as blockchain systems. Existing countermeasures focus on channel and network layers and include standard encryption algorithms, authentication, intrusion detection systems, and the integration of SDN and 5G technologies [13]. However, most current approaches do not account for the specifics of key initialization and spectral channel structure, resulting in the loss of inter-channel correlation and a reduction in cryptographic robustness [11, 14].

Therefore, there is a need to develop a new approach for the cryptographic transmission of satellite data that ensures comprehensive resistance to modern attacks.

Purpose

The study aims to develop an approach for nonlinear cryptographic transmission of satellite data based on entropy-determined key-space initialization and adaptive multilevel encryption. The proposed approach ensures enhanced resistance to attacks while also preserving data integrity and confidentiality during transmission through telecommunication networks. To achieve this aim, the following tasks are defined:

– to develop a mechanism for key-space generation that combines system entropy (noise, timing, delay) with parameters of deterministic nonlinear dynamics for the formation of cryptographic keys;

– to develop an adaptive multilevel encryption algorithm that accounts for inter-channel correlation of satellite images and the distribution of information across pixels depending on the number of spectral bands;

– to apply AES-256 Post Encryption as an additional encryption layer to improve resistance to cryptanalytic attacks and minimize the risk of information leakage;

– to develop a format for the output data packet that includes both the encrypted satellite image and all necessary encryption details, making sure the information can be sent reliably over telecommunication networks.

Proposed technique

The structure of the proposed approach is presented in Figure 1 and consists of input data formation, key-space initialization, adaptive multilevel encryption, and output packet generation. The first stage involves loading the satellite image, which may be single-channel or multi-channel.

The second stage of the approach focuses on forming the entropy-based key space, which serves as the foundation of the model's cryptographic robustness. The generation of key parameters is determined by three main factors: the cryptographic password, the entropy E_s, which includes environmental parameters (such as timing delays, noise, and latency), and the nonlinear dynamic parameters that define the behavior of a deterministic dynamic system with a non-periodic trajectory. The combination of entropy, the cryptographic password, and dynamic parameters forms the initial system state S_0, which is used to initialize the pseudorandom number generator. To provide a dynamic description of the combined initialization process, a system of nonlinear differential equations is proposed, representing the evolution of the system state $S(t)$:

$$\begin{cases} \frac{dS_1}{dt} = \mu S_1(1 - S_1^2) + \lambda_a S_2 + \beta \sin(S_3 + E_s), \\ \frac{dS_2}{dt} = -S_1 + S_2(\chi_a - S_3^2) + P, \\ \frac{dS_3}{dt} = S_1 S_2 - \beta S_3 + E_s, \end{cases} \quad (1)$$

where $S=[S_1,S_2,S_3]^T$ is the vector of dynamic states that reflects the variation of the system's internal parameters; μ is a parameter that controls the intensity of the system's nonlinear dynamic variations; χa is the asymmetry coefficient of the dynamic system, which determines its sensitivity to initial conditions; β is a characteristic describing the rate of dynamic transformations of the system under conditions of its nonlinear behavior.

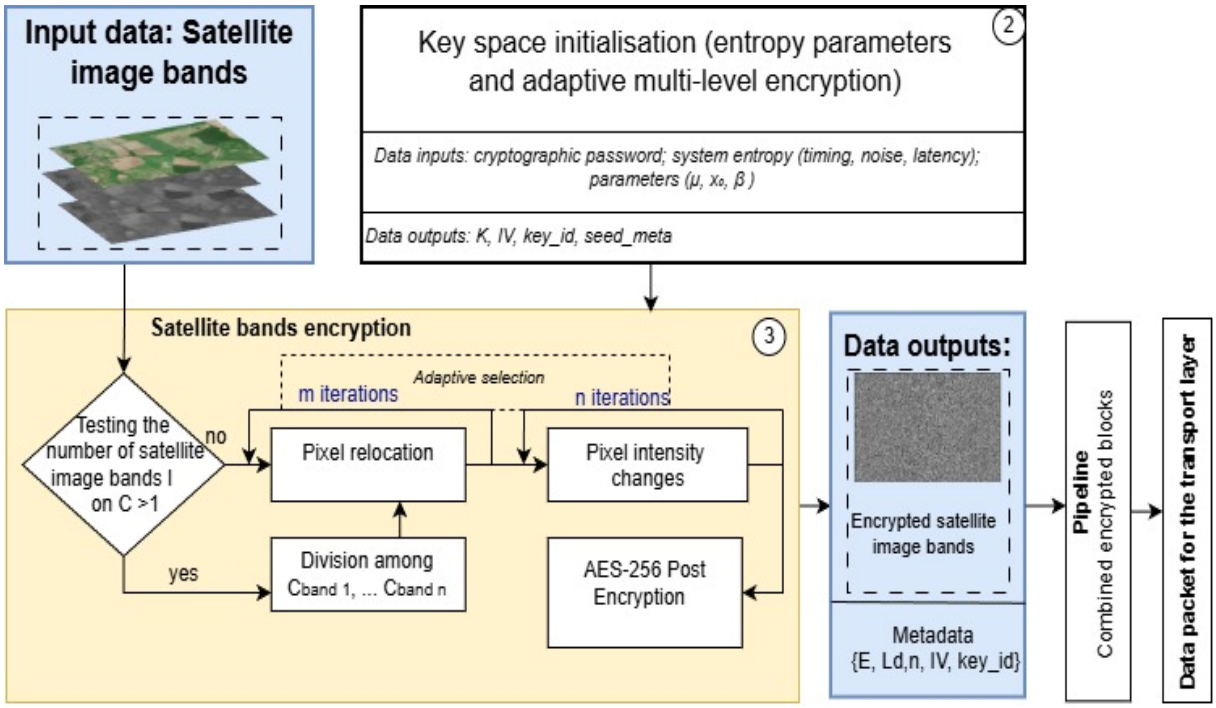


Fig.1. Proposed cryptographic satellite data transmission flowchart

The initial state $S_0=S(t_0)$ is used to form a set of key metadata:

$$\{K,IV,key\_id,seed\_meta\}, \tag{2}$$

where K is the primary cryptographic key, IV is the initialization vector, *key_id* is the key identifier, and *seed_meta* represents the entropy metadata required to reproduce the key-generation process during decryption.

The third stage involves adaptive multilevel encryption of the satellite image, considering its number of channels. Let the input image be defined as I with C bands. For a single-channel image (C=1), encryption is applied directly to the pixel matrix I. For a multi-channel image (C>1), the data are separated into individual spectral bands: $\{C_{band1},\ldots,C_{bandn}\}$. Each channel is subjected to a two-step cryptographic transformation that includes a pixel permutation controlled by the output data of the key generator {*K, IV*, key_id, *seed_meta*}.

The pixel permutation for band I_c is performed as:

$$I_c^{(d)} = \delta(I_c^{(d)}, S_0, n_c), \tag{3}$$

Adaptive selection of m_c and n_c enables the determination of the degree of encryption based on the number of channels and inter-channel correlation.

AES-256 post-encryption is applied to ensure standardized cryptographic robustness [15]:

$$AES-256\left(I_c^{(d)}, K, IV\right), \tag{4}$$

where $I_c^{(enc)}$ is the final encrypted channel.

The output data are formed as a packet:

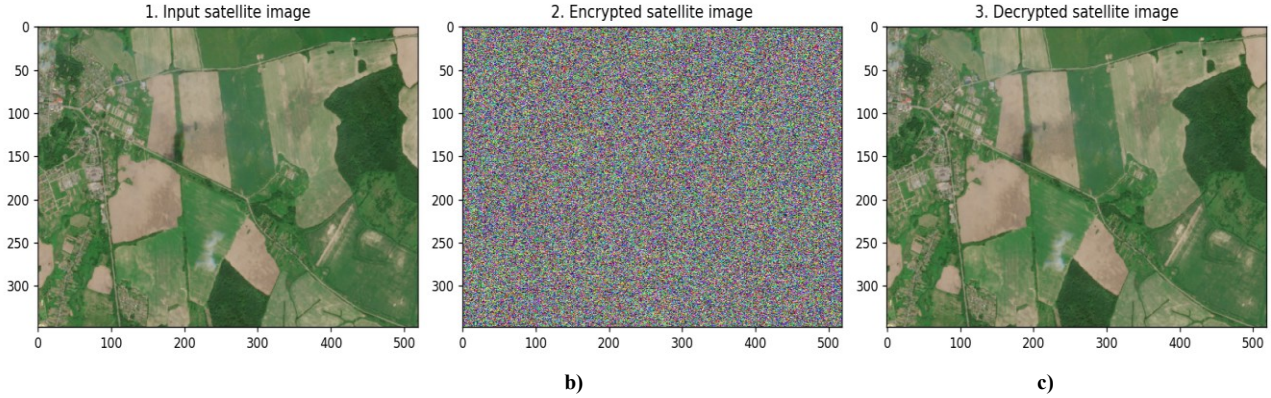
$$\left\{I_1^{(enc)}, \ldots, I_c^{(enc)}, \{E, L_d, n, IV, key_{id}\}\right\}, \tag{5}$$

where E is the encryption type, L_d is the data block size, n is the number of iterations, and IV and *key_id* are responsible for reproducing the key space. The packet P is ready for secure transmission through telecommunication networks, considering transport-layer protocols.

Results

RGB Sentinel-2 images were used (Fig. 2), with sizes of 348 × 519 pixels (180,612 pixels) and 1334 × 2000 pixels (2,668,000 pixels). After encryption, the image completely loses all structural and visual characteristics of the original (Fig. 2b), taking on the appearance of white noise, which indicates the loss of structural order

achieved through adaptive nonlinear transformation and AES-256 post-encryption. Decryption fully restores the original image without visible distortions.



b) c)

Fig. 2. Satellite image from the Sentinel-2 spacecraft with a resolution of 348×519 pixels: a) original multispectral; b) encrypted image; c) decrypted image

Figure 3 shows pixel intensity histograms for evaluating the statistical robustness of the proposed encryption method. For the original image, the histogram demonstrates a non-uniform distribution of intensities with pronounced peaks corresponding to dominant brightness values in the image (green fields in satellite imagery), which is typical for natural images. After encryption, the histograms of all three channels (R, G, and B) achieve an almost perfectly uniform distribution within the range of 0–255. Such a distribution indicates the attainment of maximum Shannon entropy (8.0 bits), corresponding to optimal information dispersion.

The quantitative metric values obtained to assess the cryptographic quality of the proposed method are presented in Table 1. These metrics enable the evaluation of the degree of entropic saturation in encrypted images and the level of absence of correlations between neighbouring pixels. The results in Table 1 demonstrate that the encrypted images exhibit properties of white noise with nearly “ideal” entropy, indicating maximal information dispersion and a high level of “diffusion.” Correlation values are close to zero, confirming the absence of statistical dependencies between neighboring pixels and a high resistance to statistical analysis and cryptanalytic attacks. High entropy values and the lack of correlation are observed regardless of the satellite image size, indicating the universality and effectiveness of the proposed approach.

To evaluate the efficiency of satellite image encryption (for sizes 348 × 519 pixels and 1334 × 2000 pixels), multithreaded data processing was applied (Tables 2 and 3). The reference execution time for single-thread encryption was T_1 (for threads) = 0.0120 s, representing the minimum computational time for this data volume without parallel processing. In parallel, baseline performance was evaluated at the process level, where the encryption time on a single process was T_1 (for processes) = 5.3957 s.

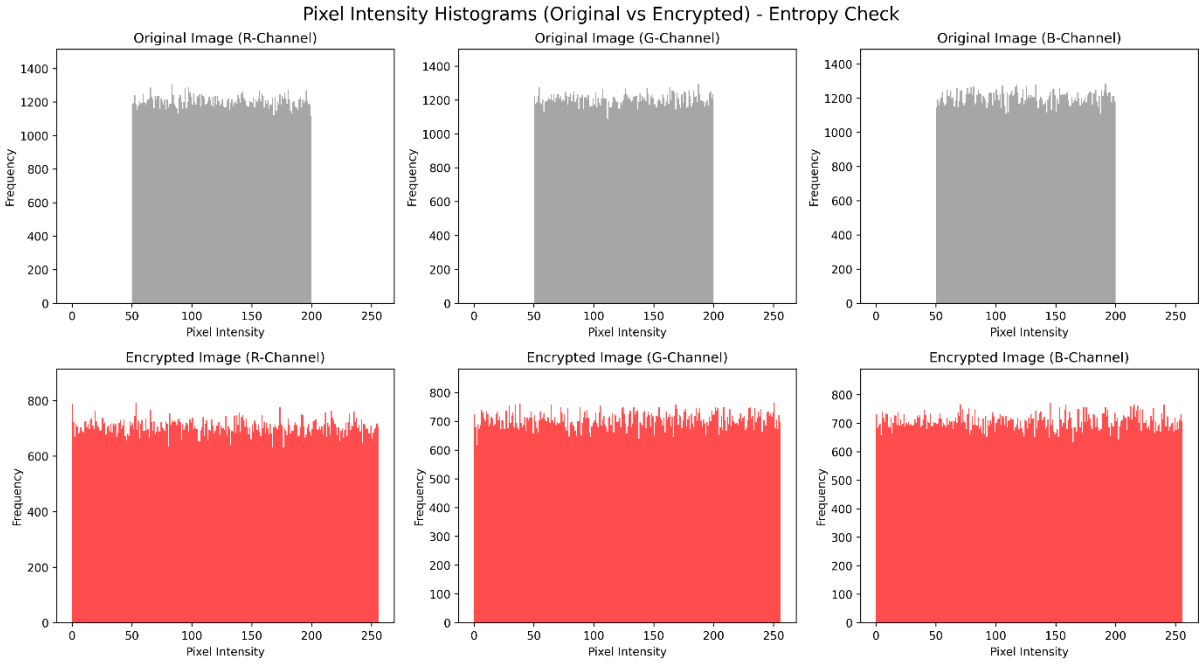


Fig. 3. Pixel intensity histograms

Table 1

Values of metrics for the proposed satellite data encryption approach

Metric	Value (encrypted.)			Best value
Satellite image 348 × 519 pixels				
Entropy	≈7.9990			8.0
Bands entropy	R	G	B	
	7.9989	7.9990	7.9989	
Correlation	≈0.0019			≈0.0
Bands correlation	R	G	B	
	0.0048	0.0026	0.0005	
Satellite image 1334 × 2000 pixels				
Entropy	≈7.9990			8.0
Bands entropy	R	G	B	
	7.9999	7.9999	7.9999	
Correlation	≈0.0004			≈0.0
Bands correlation	R	G	B	
	0.0011	0.0002	0.0003	

Analysis of Table 2 shows a consistent dependence of execution time on the number of threads. Increasing the number of threads up to four reduces the computation time from 0.0120 s to 0.0040 s, corresponding to a threefold speedup and 75% efficiency. It indicates effective utilization of multithreading in the early stages of parallel processing. Further increasing the number of threads (beyond four) gradually decreases efficiency, from 44.5% for six threads to 30.0% for eight threads. The reduced parallel encryption efficiency is due to additional computational overhead associated with thread management, synchronization, and load balancing. Another important factor is the latency caused by transmitting encrypted data blocks through communication channels, which increases the exchange time between threads and slightly reduces the overall system performance. Maximum speedup is achieved with four threads, providing an optimal balance between processing speed, resource efficiency, and result stability. Therefore, the proposed method is effective under moderate parallelism, and scaling to larger data volumes can enhance the overall performance of the encryption system.

Table 2

Performance analysis of the satellite data encryption approach (348 × 519 pixels)

Number of threads	Execution time (s)	Speedup	Efficiency (%)
1	0.0120	1.00	100.0
2	0.0070	1.71	85.5
3	0.0055	2.18	72.7
4	0.0040	3.00	75.0
6	0.0045	2.67	44.5
8	0.0050	2.40	30.0

Table 3

Performance analysis of the satellite data encryption approach (1334 × 2000 pixels)

Number of threads	Execution time (s)	Speedup	Ефективність (%)
1	5.3957	1.00	100.0
2	2.8398	1.90	95.0
3	1.9621	2.75	91.7
4	1.5416	3.50	87.5
6	1.1990	4.50	75.0
8	0.9810	5.50	68.8

The data in Table 3 demonstrate that encryption time decreases from 5.3957 s for single-thread execution to 0.9810 s using eight threads, corresponding to a speedup from 1.0 to 5.5 and an efficiency of 68.8%. It indicates that for large data volumes, the overhead of thread management, synchronization, and load balancing has a minor effect on the overall processing time. Increasing the number of threads significantly reduces execution time, demonstrating the high scalability of the approach. The gradual decrease in efficiency, from 100% to 68.8%, is attributed to coordination overhead and latency arising during the transmission of data blocks between threads via communication channels.

Conclusions

This study proposed an approach for cryptographic transmission of multichannel satellite data in telecommunication networks, combining key-space generation based on system entropy and nonlinear dynamic parameters, adaptive multilevel encryption, and AES-256 post-encryption. The proposed method ensures a high

level of data protection and resistance to attacks by utilizing keys with optimal entropy, thereby providing uniform information distribution and complicating the recovery of the original data. Experimental studies showed that encrypted images exhibit maximum entropy (≈7.9–8.0 bits), indicating optimal information dispersion. Correlation analysis revealed no statistical dependence between neighbouring pixels, confirming high resistance to frequency and statistical attacks. Decryption fully restores original images without visible distortions, confirming the reliability and reproducibility of the method. Performance analysis revealed that parallel processing efficiency is influenced by the data volume and computational overhead associated with thread management, synchronization, and data block transmission. For large datasets, increasing the number of threads significantly reduces encryption time, demonstrating the high scalability of the approach.

Future research directions include optimizing multilevel encryption algorithms for large satellite images, considering hardware and network limitations, developing adaptive transformation strategies based on the spectral structure of images, and integrating the proposed approach into real telecommunication systems to ensure secure transmission of critically important satellite data.

Author Contributions

Conceptualization, V.K. and V.H.; methodology, V.K.; software, V.K.; validation, V.H.; formal analysis, V.K.; investigation, V.K.; resources, V.K and V.H.; data curation, V.K. and V.H.; writing – original draft preparation, V.K. and V.H.; writing – review and editing, V.K. and V.V.; visualization, V.K. and V.V.; supervision, V.K. and V.V.; project administration, V.H.; funding acquisition, V.H. All authors have read and agreed to the published version of the manuscript.

Declaration on the use of generative artificial intelligence tools

The authors used Grammarly to check the grammar and spelling. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

Acknowledgements

The article was prepared within the framework of the project 2025.06/0047 "Information technologies of cryptographic protection and data authentication for mobile and satellite communication systems". This project received funding from the National Research Foundation of Ukraine.

References

1. Maral, G., Bousquet, M., Sun, Z. Satellite communications systems: Systems, techniques and technology. 6th Edition. Wiley, 2020. 3–11. DOI: https://doi.org/10.1002/9781119673811
2. Space.com. Starlink: SpaceX's satellite internet project. 2021. URL: https://www.space.com/starlink-spacex-satellite-internet-project (accessed 10 July 2025).
3. Porter, J. Facebook's satellite internet team joins Amazon. 2021. URL: https://www.theverge.com/2021/7/14/22576788/amazon-acquires-facebook-satellite-team-project-kuiper (accessed 10 July 2025).
4. Fang, X., Feng, W., Wei, T., Chen, Y., Ge, N., Wang, C.-X. 5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks. IEEE Internet of Things Journal, 2021, 8(18), 14399–14417.
5. Rappaport, T. S., Xing, Y., Kanhere, O., Ju, S., Madanayake, A., Mandal, S., Alkhateeb, A., Trichopoulos, G. C. Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond. IEEE Access, 2019, 7, 78729–78757.
6. Jedermann, T., et al. RECORD: A RECeption-Only Region Determination Attack on LEO Satellite Users (USENIX Security 24). 2024. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/jedermann (accessed 15 January 2025).
7. Driessen, B. Eavesdropping on satellite telecommunication systems. 2018. URL: https://eprint.iacr.org/2012/051
8. Yue, P., An, J., Zhang, J., Ye, J., Pan, G., Wang, S., Xiao, P., Hanzo, L. Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. IEEE Communications Surveys & Tutorials, 2023, 25(3), 1604–1652. DOI: https://doi.org/10.1109/COMST.2023.3296160
9. Salim, S., Moustafa, N., Reisslein, M. Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments. IEEE Communications Surveys & Tutorials, 2024, 1–1. DOI: https://doi.org/10.1109/COMST.2024.3408277
10. Tedeschi, P., Sciancalepore, S., Di Pietro, R. Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks, 2022, 216, 109246. DOI: https://doi.org/10.1016/j.comnet.2022.109246
11. Hobincu, R., Datcu, O. A novel chaos-based PRNG targeting secret communication. In: Proceedings of the 12th IEEE International Conference on Communications (COMM), Bucharest, Romania, 2018, 459–462.
12. Hobincu, R., Datcu, O. FPGA implementation of a chaos-based PRNG targetting secret communication. In: Proceedings of the 13th Symposium on Electronics and Telecommunications (ISETC), Timişoara, Romania, 2018.
13. Kodheli, O., Lagunas, E., Maturo, N., Sharma, S. K., Shankar, B., Montoya, J. F. M., Duncan, J. C. M., Spano, D., Chatzinotas, S., Kisseleff, S., Querol, J., Lei, L., Vu, T. X., Goussetis, G. Satellite communications in the new space era: A survey and future challenges. IEEE Communications Surveys & Tutorials, 2021, 23(1), 70–109. DOI: https://doi.org/10.1109/COMST.2020.3028247
14. Pavur, J., Moser, D., Lenders, V., Martinovic, I. Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 2019, 277–284.
15. Xin, L., Xiaohua, T., Zhongwen, H. Improving satellite image fusion via generative adversarial training. IEEE Transactions on Geoscience and Remote Sensing, 2020, 1–14. DOI: https://doi.org/10.1109/TGRS.2020.3025821

Vita Kashtan **Віта Каштан**	PhD., Associate Professor of Information Technology and Computer Engineering Department, Dnipro University of Technology, Dnipro, Ukraine, e-mail: kashtan.v.yu@nmu.one. https://orcid.org/0000-0002-0395-5895 Scopus Author ID: 57201902879	кандидат технічних наук, доц., доцент кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», Дніпро, Україна.
Volodymyr Hnatushenko **Володимир Гнатушенко**	Doctor of Technical Sciences, Professor, Head of Information Technology and Computer Engineering Department, Dnipro University of Technology, Dnipro, Ukraine, e-mail: vvgnat@ukr.net. https://orcid.org/0000-0003-3140-3788 Scopus Author ID: 6505609275	доктор технічних наук, проф., завідувач кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», Дніпро, Україна.