# Integral Robustness Indicator as a Basis for Selecting a Steganographic System Under Specific Operational Conditions

**[1]Bobok I.I., [2]Kobozieva A.A.**
[1]Odesa Polytechnic National University, Odesa, Ukraine
[2]Odesa National Maritime University, Odesa, Ukraine

***Abstract.*** Modern energy facilities are undergoing a fundamental transformation driven by the ubiquitous integration of digital technologies, the most complete embodiment of which is the Smart Grid concept. The digital transformation of energy facilities opens up new possibilities for organizing secure control data transmission channels based on steganographic principles. One of the primary requirements for a steganographic system is its robustness; however, at present, this concept in steganography is multi-criterial. For real-time systems, this complicates – or even renders impossible – the process of simultaneously accounting for or ensuring all criteria under the specific operational conditions of the steganographic system. *The aim* of this study is to enable the selection of a steganographic system and the a priori evaluation of its properties by developing an integral quantitative indicator of its robustness. *This goal was achieved* by fulfilling the following objectives: analyzing the interrelationships among existing steganographic system robustness criteria, transforming the set of robustness criteria based on these established relationships, and selecting a method for the quantitative evaluation of their priorities. *The most important result* of this work is the substantiation of the fundamental impossibility of creating a universal, unequivocally defined integral robustness indicator for a steganographic system, as well as substantiating the necessity of its parameterization according to operational conditions. *The significance of the obtained results* is illustrated using the example of organizing a secure steganographic channel for the transmission of control information within a Smart Grid infrastructure.
***Keywords*:** information security, Smart Grid, covert channel, steganographic system, integral metric for steganographic system robustness.

**DOI: https://doi.org/10.52254/1857-0070.2026.3-71.09**
**UDC: 004.056: 621.311.1**

**Integral Robustness Indicator as a Basis for Selecting a Steganographic System Under Specific Operational Conditions**

**[1]Bobok I.I., [2]Kobozieva A.A.**
[1]Odesa Polytechnic National University, Odesa, Ukraine
[2]Odesa National Maritime University, Odesa, Ukraine

***Rezumat.*** Instalațiile energetice moderne trec printr-o transformare fundamentală, determinată de integrarea omniprezentă a tehnologiilor digitale, a cărei expresie cea mai avansată este conceptul Smart Grid. Transformarea digitală a instalațiilor energetice deschide noi posibilități pentru organizarea unor canale securizate de transmitere a datelor de control, bazate pe principii steganografice. Una dintre cerințele esențiale ale unui sistem steganografic este robustețea acestuia. Cu toate acestea, în prezent, conceptul de robustețe în steganografie are un caracter multicriterial. În cazul sistemelor în timp real, acest aspect complică sau chiar face imposibilă luarea în considerare simultană ori asigurarea tuturor criteriilor relevante în condițiile specifice de funcționare ale sistemului steganografic. Scopul acestui studiu este de a facilita selectarea unui sistem steganografic și evaluarea a priori a proprietăților sale prin dezvoltarea unui indicator cantitativ integrat al robusteții. Acest scop a fost atins prin realizarea următoarelor obiective: analiza interrelațiilor dintre criteriile existente de robustețe ale sistemelor steganografice, transformarea setului de criterii pe baza relațiilor identificate și selectarea unei metode de evaluare cantitativă a priorității acestora. Cel mai important rezultat al acestei lucrări îl constituie demonstrarea imposibilității fundamentale de a defini un indicator universal, univoc și integrat al robusteții unui sistem steganografic, precum și argumentarea necesității parametrizării acestuia în funcție de condițiile de operare. Relevanța rezultatelor obținute este ilustrată prin exemplul organizării unui canal steganografic securizat pentru transmiterea informațiilor de control în cadrul unei infrastructuri Smart Grid.
***Cuvinte-cheie***: information security, Smart Grid, covert channel, steganographic system, integral metric for steganographic system robustness.

**Интегральный показатель устойчивости как основа для выбора стеганосистемы в конкретных условиях ее использования**

**[1]Бобок И.И., [2]Кобозева А.А.**

[1]Национальный университет «Одесская политехника», Одесса, Украина

[2]Одесский национальный морской университет, Одесса, Украина

***Аннотация.*** Современные объекты энергетики переживают фундаментальную трансформацию, обусловленную повсеместным внедрением цифровых технологий в процессы управления, мониторинга и диспетчеризации, наиболее полным воплощением которой является концепция Smart Grid. Эта трансформация несет вместе с колоссальными преимуществами принципиально новый класс угроз – кибератаки, способные порождать физические последствия, вплоть до нарушения электроснабжения, повреждения оборудования и каскадных отказов в энергосистеме. Цифровая трансформация объектов энергетики открывает новые возможности для организации защищенных каналов передачи управляющей информации на основе принципов стеганографии. Одним из основных требований к стеганосистеме является ее устойчивость, и это понятие в стеганографии является многокритериальным, что для систем, работающих в режиме реального времени, осложняет/делает невозможным процесс учета/обеспечения всех критериев одновременно в конкретных условиях функционирования стеганосистемы. Наличие множества базовых критериев устойчивости затрудняет объективное сравнение различных стеганосистем, поскольку улучшение одних параметров часто приводит к ухудшению других. Формирование единого интегрального показателя является фундаментальной методологической основой, позволяющей свести многомерный вектор оценок к скалярной величине. Это необходимо для математически обоснованного выбора оптимальной/приемлемой архитектуры защиты информации и формирования целевой функции при автоматизированном проектировании таких систем. *Целью* работы является обеспечение возможности выбора стеганосистемы, априорной оценки ее свойств путем разработки интегрального количественного показателя ее устойчивости. *Поставленная цель была достигнута* путем решения следующих задач: анализа взаимосвязи между существующими критериями устойчивости стеганосистемы, трансформации множества критериев устойчивости стеганосистемы с учетом установленных связей, выбора способа количественной оценки их приоритетов. *Наиболее важным результатом работы* является обоснование принципиальной невозможности создания универсального однозначно определяемого интегрального показателя устойчивости стеганосистемы и обоснование необходимости его параметризации условиями применения. *Значимость полученных результатов* проиллюстрирована на примере организации защищённого стеганографического канала передачи управляющей информации в инфраструктуре Smart Grid.

***Ключевые слова***: информационная безопасность, Smart Grid, скрытый канал, стеганосистема, интегральный показатель устойчивости стеганосистемы.

## INTRODUCTION

Modern energy facilities are undergoing a fundamental transformation driven by the widespread implementation of digital technologies in management, monitoring, and dispatching processes. Traditional analog control systems are being consistently replaced by digital counterparts integrated into the facility's unified communication infrastructure.

This transformation brings tremendous advantages – namely, increased management efficiency, reduced operational costs, and the capability for real-time monitoring and control. However, it also gives rise to a fundamentally new class of threats that was absent in the era of analog systems: whereas disrupting the normal operation of an energy facility previously required physical intervention with the equipment, today a successful attack on the digital channel transmitting control information is sufficient. A cyberattack is capable of producing physical consequences, up to power supply disruptions, equipment damage, and cascading failures across the power grid.

The most comprehensive and consistent embodiment of digital transformation in the electric power industry is the Smart Grid concept – an intelligent power grid that integrates digital communication technologies into the processes of electricity generation, transmission, and distribution. Smart Grids are cyber-physical systems that combine traditional control systems with advanced computing and communication technologies [1]: the smart grid adds a “digital layer” to the existing network of wires, transformers, and substations. Smart meters, sensors, and automated switches transmit real-time data to control centers, where existing software utilizes this data to identify problems, reroute electricity during failures, and plan upgrades based on actual consumption [2]. Modern power grids are gradually transforming into smart grids. These changes are observed in three main aspects [1]. First, off-the-shelf

computing technologies are transforming traditional legacy metering devices into embedded computer systems. Second, off-the-shelf network communication technologies connect physical devices across vast geographical areas to collect increasingly large volumes of data at a high frequency. This capability for large-scale monitoring allows for the detection of anomalies in the power grid with greater accuracy and timeliness. Third, the utilization of distributed energy resources blurs the line between electricity generation and consumption [3].

In certain countries, Smart Grid implementation has already reached a significant scale (e.g., the USA, China, Germany, France, etc.) [4], whereas in others, the Smart Grid serves as the technological foundation for the future of energy. In this regard, a crucial role is played by the awareness that the active digitalization of power systems does not only have a positive aspect. It introduces cyber threats capable of compromising critical power grid functions, thereby opening avenues for data theft, sabotage, or system failure [5]. The Smart Grid fundamentally differs from traditional power grids precisely because the physical processes of electricity management are now mediated by digital communication channels. This creates a fundamentally new attack surface that was absent in analog systems [6]: remote control of substations and equipment, data collection and transmission via communication networks, and automated decision-making systems based on telemetry. Each of these components represents a potential vector for unauthorized adversary access, data tampering, or system interference. In recent years, various cyberattacks have targeted smart grid systems, resulting in severe and disruptive consequences [7]. Gaining a comprehensive understanding of the security and resilience of dynamic cyber-physical Smart Grid infrastructures, as well as developing effective analytical tools to ensure long-term grid stability under various external influences, remains a complex and hitherto unresolved task [1]. Pervasive digital connectivity, while serving as the foundation for the functional advantages of the Smart Grid, simultaneously renders it the most vulnerable environment from an information security standpoint among all types of energy facilities.

Compromised cybersecurity of smart grids affects not only the safety of existing energy systems but also directly impacts national security [8]. The growing number of cyberattacks on smart grids demands more reliable protection technologies to maintain power system security and operation. Most modern infrastructure systems can function effectively precisely due to the intelligent power supply provided within smart grid frameworks [9].

In [8], the authors evaluate the impact of existing cyberattacks on the entire smart grid ecosystem, dividing the total set of threats into two main areas: internal system vulnerabilities and external cyberattacks. An analysis of the vulnerabilities across all smart grid components (hardware, software, data transmission), as well as data management, services and applications, and the operating environment, enables the authors to identify attack strategies, forecast their consequences, and propose technical directions for countering cyberattacks on smart grids.

Attacks on the Smart Grid are highly diverse [10]. An attacker launches spoofing, sniffing, and message replay attacks to obtain sensitive data from a smart meter. Countermeasures against cyberattacks here generally involve non-linear approaches [11]. To ensure Smart Grid security, various frameworks are proposed, such as a zero-sum stochastic game model, which allows for the exploration and evaluation of defense strategies against coordinated cyber-physical attacks.

In the context of Smart Grid cybersecurity, the concept of utilizing covert channels has been gaining increasing traction [12–15]. The rapid rise in the relevance of this issue and the shift in focus toward researching hidden data transmission within the smart power grid infrastructure are driven by a complex of interconnected factors, which can be consolidated into the following key points:

— the Smart Grid architecture integrates a large number of specific protocols developed without considering modern security requirements. The presence of a significant number of reserved, unstructured, or non-essential fields in the headers of operational packets creates a resource base for embedding additional information without disrupting the network's operational logic;
— the simultaneous circulation of a large volume of packets from smart meters and telemetry sensors generates a massive traffic load with a high level of natural statistical noise. In such an environment, covert channels “dissolve”, rendering them virtually imperceptible to conventional monitoring tools;
— concealing the very fact of service information exchange within the Smart Grid

deprives an adversary of the opportunity to identify the most critical and protected power grid nodes through passive scanning;
— the capability to ensure the authentication of control information without increasing the packet size, which is critically important for real-time systems;
— the covert channel acts as a backup for transmitting emergency commands.

Thus, the integration of covert channels into the Smart Grid allows for the implementation of the "asymmetric defense" principle, where the defensive system remains invisible to the adversary, radically enhancing the overall survivability of the cyber-physical system.

In [13], the authors examine the process of establishing a covert channel for smart grids utilizing the channel access procedure in Wi-Fi networks. Wi-Fi networks within smart grids play a vital role in ensuring communication between smart meters and data collection devices. They are also frequently employed in the automation, metering, management, monitoring, and protection of distribution networks. However, a significant challenge here is posed by the uncertainty regarding the authenticity of the data recipient's identity. The article proposes an efficient method for establishing a covert channel to transmit data that requires a high level of security. The effectiveness of this method remains stable even under conditions of network congestion involving additional background traffic generated by other stations.

The same problem related to ensuring the authenticity of data recipients is addressed in [14]. To resolve this issue, the authors propose the establishment of a covert channel for the transmission of data requiring special protection, positioning it as a novel approach to ensuring data integrity and confidentiality within smart grid communications.

To create a covert channel, the principles of steganography are among the most fundamental [15], and the properties of the covert channel will naturally be determined by the properties of the corresponding steganographic system.

One of the primary properties of a steganographic system is its robustness. The concept of steganographic system robustness is significantly more complex and multifaceted than the robustness of a cryptographic system, encompassing [16–18]:
— robustness against the detection of the existence of hidden information, or in other words, robustness against the primary task of steganalysis (criterion $K_1$);
— robustness against the extraction of hidden information (criterion $K_2$);
— robustness against the injection of false messages via the steganographic channel (spoofing resistance) (criterion $K_3$);
— robustness against the recovery of the steganographic system's secret key (criterion $K_4$);
— robustness against attacks targeting the embedded message (criterion $K_5$).

The existence of multiple fundamental criteria, $K_1,\ldots,K_5$, brings to the forefront a core methodological problem for steganography as a whole: the development of an integral metric for steganographic system robustness. This problem is equally and directly relevant to the Smart Grid.

Unlike many other application domains of steganography, the compromise of a covert channel in the Smart Grid entails direct physical consequences – such as power supply disruptions, equipment damage, and cascading failures across the power grid – making the cost of an incorrect system robustness assessment exceptionally high. Furthermore, the Smart Grid operates in real time; consequently, the (a priori) process of evaluating its properties (and, by extension, all its components) must be as computationally inexpensive as possible. This goal is hindered by the large number of different steganographic system robustness criteria that require mandatory consideration.

*The aim* of this work is to enable the selection of a steganographic system and the a priori evaluation of its properties through the development of an integral quantitative robustness metric.

## INTERCONNECTION OF STEGANOGRAPHIC SYSTEM ROBUSTNESS CRITERIA

To date, in pursuing the goal of creating a robust steganographic system, developers invariably prioritize among $K_1,\ldots,K_5$, reasonably dedicating the greatest attention to one or more of them while frequently neglecting the evaluation of the others.

The importance/necessity of ensuring these criteria depends on the conditions of the intended use of the steganographic system. Considering the primary task of a steganographic system in its classical application – namely, concealing the

very fact of hidden communication – $K_1$ is typically given the highest priority. However, if the steganographic system utilizes, for instance, high-speed streaming traffic as a container in real time (Smart Grid), conventional passive steganalysis on the adversary's side becomes critically complicated under such conditions due to strict time constraints on the computational processing of data arrays. Consequently, even with a minimal a priori suspicion regarding the existence of a covert channel, the adversary shifts from a passive strategy to an active one. If one of their objectives is to delay/disrupt potential communication, they are highly likely to deploy low-amplitude and computationally "inexpensive" attacks against the embedded message (e.g., compression attacks, noise injection, etc.), which ultimately results in $K_5$ having the highest priority under these conditions.

Thus, it becomes evident that the integral robustness metric of a steganographic system, hereinafter denoted as $K$, regardless of its immediate functional form, cannot be universal, static, or uniquely determined even for a specific steganographic system (without considering the specific conditions of its use). In the general case, the sought integral criterion fundamentally cannot provide rigid boundaries for its values that would allow for a threshold-based separation of an integrally robust steganographic system from a non-robust one, independently of its conditions of use. It is precisely the operational conditions of the steganographic system that determine the prioritization of its robustness criteria.

Thus, the search for a universal, uniquely determined quantitative robustness criterion for a steganographic system is a fundamentally intractable problem, and any proposed integral metric will inevitably be parameterized by the system's application conditions.

The necessity of identifying and formalizing the internal dependencies among the robustness criteria is driven, first and foremost, by the complex systemic nature of the steganographic process. Attempts at the isolated optimization of an individual criterion can destructively or constructively impact other system parameters. Without understanding the precise topology of these interrelationships, it is impossible to predict the behavior of a steganographic system under dynamic threats, as the compromise of a single security layer can act as a catalyst for the cascading destruction of the entire defense architecture. Furthermore, although multi-criteria problems in classical decision theory are often analyzed under the assumption of mutual parameter independence, in information security tasks – particularly when establishing a steganographic communication channel – such an assumption does not reflect reality.

Determining the structure of the relationships among the criteria is necessary to enable or rule out their classification based on the cause-and-effect principle. This will allow for the separation of fundamental robustness factors from derivative ones, which is critically important for the accurate modeling of an active adversary's actions. Finally, identifying internal dependencies among the criteria is a prerequisite for designing adaptive steganographic systems capable of modifying their parameters directly during a communication session, since under real-world conditions, the prioritization of requirements for a steganographic system can shift within a short period – a factor that is particularly relevant for the Smart Grid.

To formally define the interrelationships among the criteria $K_1,\ldots,K_5$, let us define a binary relation $\rho$ on the set $K=\{K_1,K_2,K_3,K_4,K_5\}$:

$$K_i \rho K_j, \textit{ if ensuring } K_i \textit{ implies ensuring } K_j. \quad (1)$$

Let us first consider the relationship between $K_1$ and each of the remaining criteria. At first glance, it may seem that if steganalysis yields a negative answer regarding the presence of additional information within the information content, the attacker will make no effort whatsoever to extract the hidden information, inject false messages, recover the steganographic system's secret key, or distort the secret information, since the steganographic system is seemingly absent. A formal consequence of this, at first glance, would be the fulfillment of criteria $K_2,K_3,K_4,K_5$. However, firstly, the result of steganalysis is by no means always reliable and is probabilistic in nature. Secondly, given recent advances in adaptive and selective steganography [19-21], as well as the fundamental possibility of selecting an original container such that it already contains the information embedded within it in accordance with the secret key used, we conclude that in this case, a steganographic system that perfectly satisfies criterion $K_1$ is not one where it is futile for an adversary to attempt key recovery, etc. Thus, the adversary may still test other criteria "for robustness", independently of whether $K_1$ is ensured.

In modern steganography, digital images (DIs), video, and audio are most commonly utilized as containers. For the sake of definiteness, and without loss of generality, a DI is hereinafter referred to as the container.

*Definition 1.* We define the robustness criteria $K_i$, $K_j$ of a steganographic system to be independent if neither ensuring $K_i$ is a sufficient condition for ensuring $K_j$, nor ensuring $K_j$ is a sufficient condition for ensuring $K_i$, i.e.: $\overline{K_i \to K_j}\ \&\ \overline{K_j \to K_i}$.

According to the laws of mathematical logic, criteria $K_i$, $K_j$ are independent if and only if:

— there exists a steganographic system in which $K_i$ is ensured and $K_j$ is not ensured;

— there exists a steganographic system in which $K_j$ is ensured and $K_i$ is not ensured.

The fulfillment of criterion $K_1$ does not ensure the fulfillment of $K_2$; that is, the robustness of a steganographic system against steganalysis does not imply its robustness against the extraction of secret information. For instance, imagine a steganographic system where the steganographic embedding is performed via the LSB method with an extremely low covert channel capacity (CCC) – less than 0.01 bpp – which is virtually undetectable by modern steganalytic methods (thus, criterion $K_1$ is ensured). However, knowledge of the secret key, for example, would enable the extraction of the secret information, indicating that $K_2$ is not ensured.The converse is also true; specifically, robustness against information extraction does not guarantee the robustness of a steganographic system against steganalysis. To illustrate, consider a steganographic system that embeds a DI obtained from a precoder using a strong cipher, utilizing the LSB method across all pixels of the container image (CCC = 1 bpp). In this case, criterion $K_2$ is ensured. However, the utilization of the LSB method with such a high capacity is easily detected by existing steganalytic methods, indicating that $K_1$ is not ensured.

Thus, for the ordered pairs $< K_1, K_2 >$ and $< K_2, K_1 >$, the following relations hold: $< K_2, K_1 > \notin \rho$, $< K_1, K_2 > \notin \rho$, respectively. Analogous conclusions can be drawn regarding the ordered pairs $< K_1, K_3 >$ and $< K_3, K_1 >$.

From the foregoing, and taking Definition 1 into account, the validity of the following proposition follows.

*Proposition 1*. Criteria $K_1$ and $K_2$, as well as $K_1$ and $K_3$, are independent.

Let us examine criterion $K_4$ – robustness to key recovery, i.e., to the complete compromise of the steganographic system – in greater detail. The container is a finite set (although possessing a high cardinality for modern images) of constituent elements: pixels whose intensity values belong to the finite set $\{0,1,...,255\}$. Consequently, the container is a discrete object composed of a finite number of components. A brute-force search (of combinations) of these components for an arbitrary purpose (for instance, to recover the steganographic key), while potentially computationally highly complex, will fundamentally and theoretically yield the desired result due to the finiteness of possible variants, provided that this result exists. The implementation of this idea, which is rooted in the finiteness of options, is observed, for example, in the execution of brute-force attacks in cryptography. Thus, even in the case where "container = stego-message", it is theoretically possible to find the key used by the steganographic system, assuming that it is generated in advance (prior to the communication session) and transmitted to the recipient via a secure communication channel. This implies that the use of a one-time pad analogue is excluded – a scenario where any key extracts a meaningful message, preventing the adversary from determining the true key even after searching through all possibilities. Let us denote this as *Condition A.*

Condition A corresponds to a practically meaningful utilization of a steganographic system. Indeed, information regarding the secret key is transmitted in advance to enable the establishment of a covert communication channel at any required moment. Transmitting a secret key – the size of which for a one-time pad must be at least equal to that of the transmitted message – in parallel with the secret message itself (which is essentially required when implementing a one-time pad) renders the establishment of a steganographic communication channel pointless. After all, the secret message itself could simply be transmitted over the existing secure channel, since its size is no larger than the key size, and in the case of a steganographic key, strictly smaller. In fact, a steganographic key essentially consists of several components, including: a cryptographic component used in the steganographic system's precoder (this is particularly relevant today for

crypto-steganographic systems [22]); a key component that determines the steganographic path (the specific pixels, blocks, or frequency coefficients, etc., directly used for embedding the AddInf, as well as their sequence during the steganographic transformation); and the key component used during AddInf decoding, among others. The container itself may also form part of the aggregate steganographic key. The stopping condition for the key recovery process can be the secret information recovered as a result of decoding, provided it possesses a logical meaning and corresponds to the expected context. This issue is examined in detail by the authors in a study whose materials are currently being prepared for publication and are omitted here due to article length constraints.

To mathematically formalize the stopping point of the key brute-force process, the apparatus of information theory and stochastic linguistics is applied. The concepts of “expected context” and “logical meaning” are transformed into cutoff criteria based on the analysis of information entropy and the likelihood function. Granted, to enhance the security of the transmitted secret information, the sender may embed masking information alongside the “target” information within the container, which carries no actual secret data. However, enabling the separation of real information from misinformation when multiple decoded messages are present (potentially even decoded using different keys) does not fall within the direct scope of a steganographic system; therefore, this problem is outside the scope of the present study. The main conclusion drawn from these arguments is the fundamental possibility of recovering the secret key, even when criterion $K_1$ is ensured.

From the foregoing, the validity of the following proposition follows:

*Proposition 2.* Ensuring the robustness criterion $K_4$ of a steganographic system without constraints on the adversary's computational resources is unattainable under Condition A.

Remark 1. Unbounded computational resources for an adversary are impossible in practice.

Thus, the following proposition holds:

*Proposition 3.* Criteria $K_1$ and $K_4$ are independent.

Given that the extraction of secret information and the injection of false messages in a steganographic system cannot be executed without the secret key [23,24], ensuring criterion $K_4$ implies ensuring criteria $K_2$ and $K_3$. Feedback loops (reverse implications) are absent in the general case. This follows from reasoning analogous to that used when establishing the relationship between $K_1$ and $K_4$ (Proposition 2). Indeed, in accordance with Kerckhoffs's principle, a steganographic system fulfills its functions even when the adversary is fully aware of its structure and operational algorithms, with the sole exception of the key. That is, if the adversary cannot extract the secret message, it implies they do not possess the secret key, since everything else about the system is known to them. However, the fact that the adversary does not currently possess the key does not mean that they fundamentally cannot recover it via a brute-force search (Proposition 2). Nevertheless, the computational complexity of this process renders such recovery impossible in practice under mandatory constraints on the adversary's computational and temporal resources (Remark 1). Thus, the following holds:

*Proposition 4.* Ensuring criterion $K_4$ is a sufficient, but not a necessary, condition for ensuring criteria $K_2$ and $K_3$.

Let us consider the relationship between $K_1$ and $K_5$. The following holds:

*Proposition 5.* Criteria $K_1$ and $K_5$ are independent.

Indeed, imagine a steganographic system where the stego-message is formed via the LSB method with a CCC < 0.02 bpp, for which, as noted above, $K_1$ will be ensured; however, due to the inherent properties of the LSB method, $K_5$ will not be ensured even under minor perturbations acting on the stego-message. Now let us consider a steganographic system where the steganographic transformation is performed using the Koch and Zhao method, the parameters of which ensure the robustness of the stego-message against attacks aimed at the embedded message ($K_5$). Moreover, due to the utilization of selective steganography, the perceptual reliability of the resulting stego-message is also ensured; however, the latter may not be achieved without block selection, indicating that criterion $K_1$ is not systematically ensured.

Although there is no dependence between criteria $K_1$ and $K_5$ in the sense of (1), a connection between them nevertheless exists: typically, the better one is ensured, the worse the other becomes. Indeed, if the steganographic transformation

process is represented in accordance with the general approach to the analysis of information systems (previous publications by the authors in this journal (2024, 2025)) as $\overline{F} = F + \Delta F$, where $F$ is the container matrix, $\overline{F}$ is the stego-message matrix, and $\Delta F$ is the formal representation of the steganographic transformation result, then to ensure $K_1$, the value of $\|\Delta F\|$, where $\|\cdot\|$ denotes a matrix norm, must be minimized, whereas to ensure $K_5$, it must be maximized. This specific relationship – the antagonism between $K_1$ and $K_5$ – is discussed in detail below.

*Definition 2.* We define a robustness criterion of a steganographic system to be *fundamental* if it is not a logical consequence of any other robustness criterion from the considered set $K$.

*Definition 3.* We define a robustness criterion of a steganographic system to be *derivative* if it is a logical consequence of some other robustness criterion from the considered set $K$.

Thus, within the set $K$, criteria $K_1$, $K_4$, and $K_5$ are fundamental, whereas criteria $K_2$ and $K_3$ are derivative.

Remark 2. The classification of criteria into fundamental and derivative is exceedingly important for constructing the integral criterion: since the derivative criteria $K_2$ and $K_3$ are logical consequences of the fundamental criterion $K_4$, they do not conceptually contribute new information regarding the system's robustness beyond what is already expressed in $K_4$. This serves as a basis for a potential simplification of the set of criteria $K$, which is utilized below.

Taking into account all of the foregoing – specifically Propositions 1 and 3–5 – we arrive at the graph $G$ of the binary relation (1), as illustrated in Fig. 1.

The binary relation (1) is reflexive, antisymmetric, and can be considered transitive, since pairs of edges of the form $< K_i, K_j >$, $< K_j, K_m >$, where $i \neq j, j \neq m$, are simply absent in the constructed graph. Consequently, (1) can be regarded as a non-strict order relation, thereby defining a partial ordering on the set $K$. However, such a binary relation lacks a maximum element, which precludes the possibility, at this stage of the research, of establishing a hierarchy of criteria with the subsequent ability to evaluate its levels. If such a hierarchy existed, it would make it possible to rank the criteria and obtain quantitative estimates for each, which could be treated as parameters determined by the system's application conditions, as previously discussed. But even the artificial introduction into the set *K* of a maximum element $K_{\max}$: $K_{\max} \rho K_i, i = \overline{1,5}$, conceptually representing the sought integral robustness criterion of a steganographic system – the fulfillment of which would ensure all the others – is fundamentally impossible even in a formal sense due to the existing conflict between $K_1$ and $K_5$: there is no steganographic system that simultaneously maximizes both of these criteria. Consequently, $K_{\max}$, as a maximum element in the strict mathematical sense for the binary relation (1), does not exist. This leads to yet another strictly formal confirmation of the general conclusion derived earlier: the problem of constructing a single, uniquely determined integral robustness criterion for a steganographic system in an absolute sense has no solution. The sought criterion must be the result of a certain compromise in satisfying criteria $K_1, \ldots, K_5$, achieved through the introduction of parameters that depend on the operational conditions of the steganographic system.

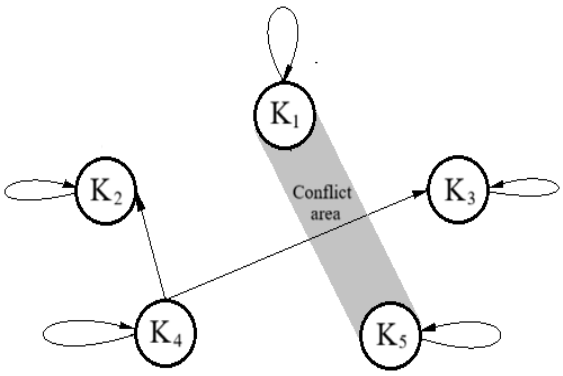


**Fig. 1. Graph *G* of the binary relation (1).**

Criteria $K_1, \ldots, K_5$ differ significantly from one another and are incomparable in the conventional sense:

— all five criteria measure different aspects of the interaction between the same steganographic system and fundamentally different adversaries employing distinct methods of attack: $K_1$, $K_2$, and $K_4$ counter a passive adversary, $K_5$ counters an active adversary, and $K_3$ counters a malicious adversary;

— failure to ensure the criteria for a steganographic system results in qualitatively different types of damage, considering the CIA (Confidentiality, Integrity, Availability) triad: $K_1$ – confidentiality of the channel; $K_2$ – confidentiality of the transmitted

information; $K_3$ – integrity and availability of the transmitted information; $K_4$ – confidentiality, integrity, and availability (complete compromise of the steganographic system); $K_5$ – integrity and availability of the information. Comparing these impacts, even when accounting for the operational conditions of the steganographic system, is exceedingly difficult, as it necessitates a direct comparison of the fundamental information security criteria (CIA);

— fundamentally different outcomes resulting from the failure to ensure the criteria:

- $K_1$ – a detected instance of covert communication;
- $K_2$ – extracted secret information;
- $K_3$ – a newly generated stego-message;
- $K_4$ – complete information regarding the steganographic system;
- $K_5$ – an altered stego-message / destroyed secret information.

Given the "incomparability" of criteria $K_1$ ,…, $K_5$, one might attempt to employ the Analytic Hierarchy Process (AHP) [25] to construct an integral robustness criterion for a steganographic system in order to introduce parameters reflecting its operational conditions. The priority values obtained in this manner for $K_1,\ldots,K_5$ can be treated as parameters. However, a key prerequisite for the AHP is the independence of criteria in the sense of Definition 1, which does not hold in our case. Furthermore, while the graph loops (Fig. 1) can conceptually be ignored without losing information on robustness essential to the functioning of the steganographic system, the possibility of ignoring the ordered pairs $< K_4, K_2 >$ and $< K_4, K_3 >$ is not obvious.

Let us consider the relationship between criteria $K_2$, $K_3$, and $K_4$ in greater detail. In accordance with Proposition 4 and Remark 2, ensuring the fundamental criterion $K_4$ automatically ensures the fulfillment of the derivative criteria $K_2$ and $K_3$. This allows for the logical aggregation of $K_2$, $K_3$, and $K_4$ into a single aggregated criterion $K_{2,3,4}{}^*$ without losing the conceptual completeness of the evaluation, thereby making $K_{2,3,4}{}^*$ a new fundamental criterion. In this regard, it is proposed to use the result of a simple homomorphic contraction of graph $G$ – denoted as graph $G_H$ – as the graph corresponding to the interrelations among the robustness criteria of a steganographic system. This is achieved through a sequence of simple elementary homomorphisms, initially merging $K_2$ and $K_4$ into a macro-vertex (resulting in vertex $K_{2,4}{}^*$) and subsequently forming the macro-vertex $K_{2,3,4}{}^*$ by merging $K_{2,4}{}^*$ and $K_3$ (Fig. 2).


**Fig. 2. Graph $G_H$ of the binary relation (1).**

The logical aggregation of $K_2$, $K_3$, and $K_4$ into a single criterion $K_{2,3,4}{}^*$ makes it possible to reduce the problem of constructing an integral criterion to the aggregation of just three independent components: $K_1$, $K_{2,3,4}{}^*$, $K_5$. It should be noted that the priorities of these criteria, denoted as $w(K_1), w(K_{2,3,4}{}^*), w(K_5)$, can be obtained using the AHP, where, for example, a 1–3 scale is used to construct the pairwise comparison matrix. Obviously, the specific values of the matrix elements here will depend on the intended operational conditions of the steganographic system. In accordance with the AHP, the following relation holds:

$$w(K_1) + w(K_{2,3,4}{}^*) + w(K_5) = 1 \qquad (2)$$

Having the means to obtain quantitative expressions for the priorities of $K_1$, $K_{2,3,4}{}^*$, and $K_5$, let us proceed to construct a formal expression for the integral robustness parameter of a steganographic system. The obtained priorities serve as weighting coefficients when incorporating all the robustness criteria $K_1$, $K_{2,3,4}{}^*$, $K_5$ – into the integral criterion. It is evident that the determination of the criterion weights will be tailored to a specific threat model; this reiterates the fact that the integral robustness criterion of a steganographic system cannot be uniquely defined even for a specific steganographic system, as it will depend on the threat model.

## FORMAL REPRESENTATION OF THE INTEGRAL ROBUSTNESS INDICATOR OF A STEGANOGRAPHIC SYSTEM

Thus, the intended operational conditions of a steganographic system (threat models) are reflected in the pairwise comparison matrix and the determined priorities. This represents the

*desired behavior* of the system. However, the system itself has a specific implementation and specific properties, including the degree to which each of the criteria $K_1$, $K_{2,3,4}{}^*$, $K_5$ is ensured, which must also be quantitatively evaluated. This represents the *actual capabilities of the system*. The sought indicator must integrate both the desired and actual quantitative characteristics of all criteria.

It must be noted here that the previously proposed method for determining the weights (priorities) of $K_1$, $K_{2,3,4}{}^*$, $K_5$ in no way reflects the identified antagonism between $K_1$ and $K_5$, which absolutely must be taken into account when constructing the integral robustness indicator. Indeed, the antagonism between $K_1$ and $K_5$ fundamentally cannot be accounted for during the formulation of the pairwise comparison matrix, into which the expert essentially enters judgments and preferences based on the threat model for the considered steganographic system. The pairwise comparison matrix is a subjective evaluation of the desired state, whereas the antagonism between $K_1$ and $K_5$ is an objective physical limitation of a specific steganographic system; it exists independently of the pairwise comparison matrix and the weights for $K_1$ and $K_5$ derived from it.

Since the antagonism between $K_1$ and $K_5$ is an objective property of any steganographic system, the sought integral robustness indicator should not "penalize" the system for its presence: a system with a pronounced antagonism can be completely acceptable under specific operational conditions, and the integral indicator must reflect this rather than suppress it by a priori giving quantitative preference to a steganographic system where this antagonism is less prominent. Concurrently, the correlation between the quantitative characteristics of $K_1$ and $K_5$ must be clearly evident. We shall refer to this as *Condition B* for the sought robustness indicator.

Let us define a method for the quantitative evaluation of the degree to which each of the criteria $K_1$, $K_{2,3,4}{}^*$, $K_5$ is ensured. Since we are dealing with the robustness of a steganographic system, it is proposed to use the probability of failure of an attack directed against the corresponding criterion as the quantitative characteristic: $q_1$, $q_{2,3,4}{}^*$, $q_5$. With this approach, the antagonism between $K_1$ and $K_5$ will be "embedded" within the actual values of $q_1$ and $q_5$. Thus, for example, a steganographic system with a pronounced antagonism will correspond to: $q_1 >> q_5$ or $q_5 >> q_1$.

For $K$, let us consider several of the primary formal representations commonly used in practice to obtain an integral indicator [26-30]:

1. Linear convolution:

$$K = w(K_1)\cdot q_1 + w\left(K_{2,3,4}{}^*\right)\cdot q_{2,3,4}{}^* + w(K_5)\cdot q_5 . \quad (3)$$

2. Multiplicative convolution:

$$K = (q_1)^{w(K_1)}\cdot\left(q_{2,3,4}{}^*\right)^{w\left(K_{2,3,4}{}^*\right)}\cdot(q_5)^{w(K_5)} \quad (4)$$

3. Minimum of weighted criteria:

$$K = \min\left(w(K_1)\cdot q_1, w\left(K_{2,3,4}{}^*\right)\cdot q_{2,3,4}{}^*, w(K_5)\cdot q_5\right) \quad (5)$$

4. Weighted power mean:

$$K = \left(\frac{1}{w(K_1)+w\left(K_{2,3,4}{}^*\right)+w(K_5)}\right)^{\frac{1}{p}}\times \times\left(\begin{array}{c} w(K_1)\cdot(q_1)^p + w\left(K_{2,3,4}{}^*\right)\cdot\left(q_{2,3,4}{}^*\right)^p + \\ + w(K_5)\cdot(q_5)^p \end{array}\right)^{\frac{1}{p}} \quad (6)$$

Taking (2) into account, equation (6) takes the form:

$$K = \left(\begin{array}{c} w(K_1)\cdot(q_1)^p + w\left(K_{2,3,4}{}^*\right)\cdot\left(q_{2,3,4}{}^*\right)^p + \\ + w(K_5)\cdot(q_5)^p \end{array}\right)^{\frac{1}{p}} \quad (7)$$

Let us consider equations (3)–(7) in view of their scope of application: steganographic system robustness assessment.

*Linear convolution*. One of the primary characteristics of the parameter corresponding to (3) is the capacity for compensation: a high weighted value $w(K_i)\cdot q_i$ of one criterion can compensate for a low value of another. For a steganographic system, this can serve as both an advantage and a disadvantage. For instance, if a steganographic system has the lowest weight for $K_5$ while being vulnerable to attacks against the embedded message (a small value of $q_5$), the value of $w(K_5)\cdot q_5$ may be close to zero. However, the values of $w(K_i)\cdot q_i$ for the other two criteria can compensate for this deficiency, ensuring an acceptable value of $K$, which can be entirely justified in practice. Conversely, if we assume, for example, that $q_{2,3,4}{}^* \approx 0$ or $q_{2,3,4}{}^* = 0$, indicating a complete compromise of the steganographic system, no practical compensation can be

justified; nevertheless, formally, linear convolution (3) fails to reflect this limitation.

*Multiplicative convolution* is more "categorical" than linear convolution, strictly accounting for each criterion. It reduces $K$ to zero if the quantitative indicator for any criterion is zero, even if its weight is low: if at least one of the indicators $q_1, q_{2,3,4}^*, q_5$ is equal (or close) to zero, the value of the integral parameter $K$ (4) will yield a zero (or near-zero) result. This causes such a steganographic system to be excluded from the scope of practical applicability; however, as the examples provided above demonstrate, this is not always justified given the intended operational conditions of the steganographic system. The capacity for compensation remains here, but it is only partial: the deficiency of one criterion can be offset by an increase in another. Nevertheless, as the weaker indicator deteriorates, the "cost" of its remediation rises sharply, and if a criterion indicator drops to zero, compensation becomes mathematically impossible, reducing the overall system evaluation to zero.

Let us examine in greater detail how well the existing antagonism between $K_1$ and $K_5$ is accounted for in cases (3) and (4). Obviously, it is fundamentally impossible to establish an exact functional relationship between $q_1$ and $q_5$ in the form of:

$$q_1 = f(q_5), \tag{8}$$

since the correlation between them depends on numerous factors. These include, among others, the digital watermark embedding algorithm, container properties, whether selective steganography methods are utilized (and, if so, their efficiency), the container domain used for embedding (spatial domain or transform domain), and so forth.

Thus, the function in (8) will be determined by the specific implementation of the steganographic system. However, even without knowing the general form of the function *f*, a comparison of formulas (3) and (4) reveals that linear convolution additively separates the contributions of $q_1$ and $q_5$, preserving them as independent terms with their own weights, thereby making the antagonism explicitly observable within the structural framework of the formula.

In contrast, multiplicative convolution couples $q_1$ and $q_5$ through a product. Given that the arithmetic mean of numbers exceeds their geometric mean, this product "penalizes" any deviation from the balance between them, regardless of whether this deviation stems from the inherent antagonism or represents a deliberate choice by the designer tailored to a specific threat model. Consequently, it can be argued that multiplicative convolution "enforces" balanced systems, whereas linear convolution leaves the antagonism between $K_1$ and $K_5$ in its original form. To illustrate this point, let us consider a highly simplified variant of (8):

$$q_1 + q_5 = c = const \tag{9}$$

(an increase or decrease in $q_1$ leads to a corresponding decrease or increase in $q_5$). Further, for the sake of simplicity, let us assume that $w(K_1) = w(K_5) = w$. Then, the part of expression (3) corresponding to $K_1$ and $K_5$ will be defined as: $w \cdot q_1 + w \cdot q_5 = w \cdot (q_1 + q_5) = w \cdot c$. Thus, a change in the specific values of $q_1$ and $q_5$ within the limits of (9) will not even affect the final value of $K$ (3). In other words, the antagonism apparent in the values of $q_1$ and $q_5$ will not be reflected in the value of the integral indicator, although it is explicitly present within it quantitatively.

The part of expression (4) corresponding to $K_1$ and $K_5$ will be defined as: $(q_1)^w \cdot (q_5)^w = (q_1 q_5)^w$. Since, by applying Cauchy's inequality, we have:

$$q_1 q_5 \le \left( \frac{q_1 + q_5}{2} \right)^2 = \frac{c^2}{4},$$

and the equality maximizing the value of $K$ (4) is achieved when $q_1 = q_5 = \frac{c}{2}$, it becomes evident that multiplicative convolution automatically favors balanced steganographic systems. This occurs regardless of whether such a balance is desirable under the specific operational conditions, which indicates a violation of Condition B for multiplicative convolution.

*Minimum of weighted criteria.* Equation (5) focuses on the "weakest link" within the set of robustness criteria, regardless of the state of fulfillment of the other criteria, sharing a certain conceptual similarity with multiplicative convolution. Equation (5) does not allow for any possibility of compensation, and the result completely ignores the existing antagonism between $K_1$ and $K_5$. The minimum of weighted criteria most strictly reflects the catastrophic nature of the compromise of $K_{2,3,4}^*$ – if the key is recovered by an adversary, the integral indicator

assumes its minimum value regardless of the state of the other criteria, which is conceptually accurate for a steganographic system. However, the complete absence of compensation is an excessively rigid requirement for a steganographic system. As discussed above, for instance, a low value of $q_5$ is acceptable in the absence of active attacks; nevertheless, (5) will determine the integral indicator $K$ precisely based on $q_5$, ignoring the potentially high values of $q_1, q_{2,3,4}^*$. Furthermore, the criteria weights here essentially have no effect on the outcome: only the minimal weighted criterion is decisive, which prevents the full integration of all available information regarding the criteria.

*The weighted power mean* (7) represents an infinite family of various aggregation functions, each determined by the parameter p. This is the most general form of aggregation, encompassing all the cases considered above: $p=1$ defines linear convolution, $p \to 0$ corresponds to multiplicative convolution, and $p \to 0$ yields the minimum of the criteria (without accounting for their weights).

Let us consider the power function $y = x^p$ for $p > 0$ over the domain $x \in [0,1]$, which corresponds to the domain of possible values for $q_1, q_{2,3,4}^*, q_5$. The rate of change of the function is determined by its derivative: $y' = px^{p-1}$, the behavior of which will differ in the cases where $p \in [0,1)$ and $p \in (1,+\infty)$ ($p=1$ is excluded from consideration since this case, corresponding to linear convolution, requires no further investigation). This is because the direction of convexity of $y = x^p$, determined by the second-order derivative $y'' = p(p-1)x^{p-2}$, will be different: under $p \in [0,1)$, the function $y(x)$ will be concave (convex upward), since $y'' < 0$, whereas under $p \in (1,+\infty)$, it will be convex (convex downward). This results in $y'(x)$ being a monotonically increasing function under $p \in (1,+\infty)$, indicating that the rate of change of $y(x)$ will increase as the argument grows. In other words, if the initial values are $q_1 < q_5$, then after being raised to the power of $p \in (1,+\infty)$, the difference between them will increase (which fails to reflect the true relationship, thereby exacerbating the antagonism between $K_1, K_5$). Under $p \in [0,1)$, the function $y'(x)$ is a monotonically decreasing function, causing the rate of change of $y(x)$ to decrease as the argument grows; i.e., for $q_1 < q_5$, after being raised to the power of $p \in [0,1)$, the difference between them will decrease (potentially down to the point of comparability), which may negate Condition B. Although the calculation of (7) involves computing the *p*-th root, this operation in itself cannot ensure that $q_1, q_5$ are accounted for within the integral indicator in accordance with their initial correlation. Thus, for $p > 0$, equation (7) is inferior to linear convolution for solving the specific task of constructing an integral robustness indicator for a steganographic system.

The domain $p < 0$ is formally interesting, as the convolution amplifies the influence of weak criteria. However, in the present case, it is practically inapplicable due to the problem of indeterminacy when evaluating (7) given the potential zero values of the criteria.

Thus, linear convolution (3) is proposed as the final choice for the formal definition of the integral robustness indicator of a steganographic system. It must be noted that none of the considered types of aggregation functions, including linear convolution, is flawless; rather, equation (3) is adopted as a practically justified compromise within the domain under consideration, as its limitations are such that the alternatives perform worse.

The quantitative integral robustness indicator of a steganographic system proposed in this study will enable the selection of a steganographic system from an available set and facilitate the a priori evaluation of its properties under specific operational conditions. The higher the value of $K$, the higher the priority of the corresponding steganographic system.

## AN EXAMPLE OF UTILIZING THE DERIVED INTEGRAL ROBUSTNESS INDICATOR OF A STEGANOGRAPHIC SYSTEM

Let us consider an example of utilizing the derived integral robustness indicator of a steganographic system. The scenario involves the transmission of control information within a Smart Grid infrastructure via a Wi-Fi channel (IEEE 802.11 standard) between an onshore control center and an AMI data concentrator in a distribution network. A video stream from surveillance cameras installed at the substation –

representing standard infrastructure elements – is used as the container. It is necessary to select between two steganographic systems: System A, which performs steganographic transformation in the spatial domain of the video stream frames using the LSB method; and System B, which embeds additional information in the frequency domain of the frames (for example, utilizing the Koch-Zhao method).

For both systems, the organization of a covert communication channel with low capacity is assumed in order to reduce the probability of detecting the covert communication. The comparison of the steganographic systems is conducted at a fixed and identical level of key protection for both systems. For definiteness, $q_{2,3,4}^{*} = 0.7$ is assumed to be at a level typical for a steganographic system with a key of "sufficient" length under the conditions of a computationally bounded adversary.

Conceptually, the degree of fulfillment for criteria $K_1$ and $K_5$ is determined as follows:

— for System A: High (given the low capacity, the probability of detecting the covert channel is small) and low (the LSB method is not robust against any attacks on the embedded message), respectively.
— for System B: Medium (the modification of frequency coefficients is detected via steganalysis with a higher probability than the modification of pixel brightness with an amplitude of 1) and high (embedding in the frequency domain, owing to the parameters of the corresponding steganographic methods, is capable of ensuring robustness against attacks directed at the embedded message), respectively.

*Scenario 1*. The steganographic system operates under the conditions of a passive adversary monitoring the Wi-Fi traffic in the vicinity of the substation. Active attacks are unlikely. Taking the aforementioned into account, the AHP pairwise comparison matrix (on a 1–3 scale) will take the following form:

| | $K_1$ | $K_{2,3,4}^{*}$ | $K_5$ |
|---|---|---|---|
| $K_1$ | 1 | 2 | 3 |
| $K_{2,3,4}^{*}$ | $\frac{1}{2}$ | 1 | 2 |
| $K_5$ | $\frac{1}{3}$ | $\frac{1}{2}$ | 1 |

and $w(K_1) = 0.5396$, $w(K_{2,3,4}^{*}) = 0.2969$, $w(K_5) = 0.1634$. Considering the conceptual fulfillment of the criteria, we assume the following values: $q_1 = 0.9, q_5 = 0.35$ for System A, and $q_1 = 0.65, q_5 = 0.8$ for System B. The values of $q_i$ here and below in the example are of an illustrative nature and have been assigned expertly based on the known properties of the considered steganographic methods. The development of a methodology for their practical measurement is a direction for the authors' future research. Thus, for System A:

$$K = 0.5396 \cdot 0.9 + 0.2969 \cdot 0.7 + 0.1634 \cdot 0.35 = 0.751,$$

and for System B:

$$K = 0.5396 \cdot 0.65 + 0.2969 \cdot 0.7 + 0.1634 \cdot 0.8 = 0.689,$$

which quantitatively indicates that under the conditions of a passive adversary, System A is preferable: the high value of $q_1$, combined with the highest weight $w(K_1)$, determines its advantage despite the weak fulfillment of $K_5$.

*Scenario 2*. The steganographic system operates under the conditions of an active adversary who, despite lacking the (steganalytic) capability to accurately establish the presence of a covert channel, presumes its existence and executes active attacks. Within the Smart Grid environment, an active adversary with access to the transmission channel of the video stream from the substation's surveillance cameras may apply video stream transcoding, noise addition, or lossy recompression – actions that do not disrupt the standard operation of the video surveillance system and are therefore difficult to detect, yet (possibly) effectively distort or destroy the embedded message. The priority shifts to $K_5$. The AHP pairwise comparison matrix is as follows:

| | $K_1$ | $K_{2,3,4}^{*}$ | $K_5$ |
|---|---|---|---|
| $K_1$ | 1 | 1 | $\frac{1}{3}$ |
| $K_{2,3,4}^{*}$ | 1 | 1 | $\frac{1}{3}$ |
| $K_5$ | 3 | 3 | 1 |

and $w(K_1) = 0.2$, $w(K_{2,3,4}^{*}) = 0.2$, $w(K_5) = 0.6$. The values of $q_i$ for the steganographic systems remain the same. Thus, under the conditions of this threat model, we obtain the following for System A:

$$K = 0.2 \cdot 0.9 + 0.2 \cdot 0.7 + 0.6 \cdot 0.35 = 0.53,$$

and for System B:

$$K = 0.2 \cdot 0.65 + 0.2 \cdot 0.7 + 0.6 \cdot 0.8 = 0.75 .$$

Upon switching the threat model (from a passive to an active adversary), System B becomes the preferable choice.

The provided example clearly demonstrates two key properties of the proposed integral indicator: its parameterization according to operational conditions (the exact same steganographic system can exhibit a (relatively) high indicator under certain conditions and a (relatively) low one under others) and its ability to provide a quantitative basis for selecting a steganographic system tailored to a specific threat model. It is noteworthy that the obtained quantitative results fully align with the conceptual expectations of an information security specialist: under a passive adversary model, System A is preferred, whereas under an active adversary model, System B proves to be the better option. This testifies to the conceptual adequacy of the proposed integral steganographic system robustness indicator.

## CONCLUSION

This study proposes a theoretically justified, parameterized integral robustness indicator for a steganographic system, enabling the selection of a steganographic system from an available set and facilitating the a priori evaluation of its properties under specific operational conditions.

During its development, the following were substantiated:

— the fundamental impossibility of creating a universal, unequivocally defined integral robustness indicator for a steganographic system, as well as the necessity of its parameterization according to the operational conditions of the system: the exact same system may exhibit a high indicator under certain conditions and a critically low one under others. A consequence of this is the conclusion that it is fundamentally impossible to establish uniform quantitative boundaries for the integral robustness indicator of a steganographic system (regardless of its formal expression), or to dictate the “suitability/unsuitability” of a steganographic system for deployment irrespective of the application context. The boundary of suitability will always be parameterized by the threat model and the operational conditions of the system;

— the interrelationship among the various robustness criteria $K_1$ and $K_5$ of a steganographic system, the necessity of which is dictated by the complex systemic nature of the steganographic process itself. Establishing the topology of the criteria interrelationships:

- enables the separation of fundamental robustness factors $K_1$, $K_4$ and $K_5$) from derived ones ($K_2$ and $K_3$), which is crucial for modeling the actions of an active adversary;
- served as a basis for simplifying the system of criteria $K$ during the construction of the integral robustness criterion;
- is a prerequisite for designing adaptive steganographic systems.

The separation of robustness criteria into fundamental and derived ones simplifies the monitoring of the steganographic system's state under conditions of dynamic threats. Upon a change in the threat model, it is sufficient to monitor the state of three criteria: $K_1, K_{2,3,4}{}^*, K_5$, where $K_{2,3,4}{}^*$ integrates $K_2, K_4, K_3$ by virtue of the established relationships among them. This approach reduces the dimensionality of the monitoring task without compromising the conceptual completeness of the system's robustness evaluation.

This study substantiates the feasibility of utilizing equation (3) as the formal representation of the integral robustness criterion for a steganographic system. In this equation, the parameters acting as weighting coefficients are the priorities of the fundamental criteria established using the Analytic Hierarchy Process, while the quantitative evaluation of the degree of fulfillment for each of the criteria $K_1$, $K_{2,3,4}{}^*$, $K_5$ is represented by the probability of failure of an attack directed against the corresponding criterion.

The practical applicability of the proposed steganographic system robustness indicator was demonstrated through the example of selecting a steganographic system for organizing a secure steganographic channel for transmitting control information within a Smart Grid infrastructure – an environment where the compromise of a communication channel entails not only information leakage but also direct physical consequences for the operation of the energy facility. The developed integral robustness indicator enabled the justified selection of a steganographic system tailored to the specific

operational conditions of Smart Grid segments and specific threat models.

The direction for the authors' future research involves developing a methodology for the practical estimation of the aforementioned probabilities.

## References


[1] Lin H. *Cyber-Physical Security and Resilience for Smart Grids and Renewable Energy*. Wiley-IEEE Press, 2025.

[2] TechCity. *Smart Grids 2026: The Infrastructure Story Behind Earth Week's Biggest Promise*. Available at: https://www.techcityng.com/smart-grids-2026-earth-week-renewable-energy/amp/ (accessed 15.06.2026).

[3] Kamwa I. Offshore Wind Energy Transmission: Challenges and Innovations in Collecting and Transmitting Electricity from Sea to Cities [Editor's Voice]. *IEEE Power and Energy Magazine*, 2024, 22(5), 4–19.

[4] Tracxn. *Smart Grid Sector*. Available at: https://tracxn.com/d/sectors/smart-grid/__9LT3dKtJ2ppqRT8ZbEZuPFVpgYign-nUl3cDmTydX1UU (accessed 15.06.2026).

[5] Lin H., Alemzadeh H., Kalbarczyk Z., Iyer R. Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks. *Computer*, 2020, 53(3), 26–37.

[6] Formby D. et al. *Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.* Available at: https://www.ndss-symposium.org/wp-content/uploads/2017/09/who-control-your-control-system-device-fingerprinting-cyber-physical-systems.pdf (accessed 15.06.2026).

[7] Le T.D. et al. GridAttackAnalyzer: A Cyber Attack Analysis Framework for Smart Grids. *Sensors*, 2022, 22(13), 4795.

[8] Ding J. et al. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies*, 2022, 15(18), 6799.

[9] Nguyen T.N., Liu B.-H., Nguyen N.P., Chou J.-T. Cyber Security of Smart Grid: Attacks and Defenses. *Proceedings of the 2020 IEEE International Conference on Communications* (ICC-2020), Dublin, Ireland, 2020. P. 1–6.

[10] Kim Y., Hakak S., Ghorbani A. Smart grid security: attacks and defence techniques. *IET Smart Grid*, 2023, 6(2), 103–123.

[11] Liberati F., Garone E., Di Giorgio A. (2021). Review of Cyber-Physical Attacks in Smart Grids: A System-Theoretic Perspective. *Electronics*, 2021, 10(10), 1153.

[12] Cao P. et al. A Novel Wireless Covert Channel for MIMO System. In X. Sun, J. Wang, E. Bertino (Eds.), *Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science*, vol. 1254. Springer, 2020.

[13] Natkaniec M., Dyrcz J. StegoDCF: A New Covert Channel for Smart Grids Utilizing the Channel Access Procedure in Wi-Fi Networks. *Energies*, 2024, 17(9), 2021.

[14] Teca G., Natkaniec M. StegoBackoff: Creating a Covert Channel in Smart Grids Using the Backoff Procedure of IEEE 802.11 Networks. *Energies*, 2024, 17(3), 716.

[15] Grzesiak K., Piotrowski Z., Kelner J.M. A Wireless Covert Channel Based on Dirty Constellation with Phase Drift. *Electronics*, 2021, 10(6), 647.

[16] Chunaryova A.V., Potapenko Ye.O. Metody pidvyschennya stiykosti steganosystem do nesanktsionovanogo dostupu [Methods to increase stability steganosystem from unauthorized access]. *Science-Based Technologies*, 2014, 22(2), 196–199 (in Ukrainian).

[17] Konakhovich G., Progonov D., Puzyrenko O. *Steganographic Processing and Analysis of Multimedia Data*. Center for Educational Literature, 2018.

[18] Nassar M.O. StyleStego: a novel paradigm for high-capacity steganography using per layer noise maps in StyleGAN for cross-domain robustness. *Multimedia Tools and Applications*, 2026, 85, 561.

[19] Azam M.H.N. et al. A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements. *Computer Science Review*, 2025, vol. 56, 100726.

[20] M.S. Subhedar, "Cover selection technique for secure transform domain image steganography," *Iran J Comput Sci*, vol. 4, pp. 241–252, 2021, doi: 10.1007/s42044-020-00077-9v

[21] Shah P.D., Bichkar R.S. Genetic algorithm based approach to select suitable cover image for image steganography. *Proceedings of the 2020 International Conference for Emerging Technology* (*INCET*), Belgaum, India, 2020. P. 1–5.

[22] Kukharska N., Lagun A., Yashchyk O. Crypto-Steganographic System based on the Solver of the Square Root of a Prime Number. *Proceedings of the 2024 14th International Conference on Advanced Computer Information Technologies* (ACIT), Ceske Budejovice, Czech Republic, 2024. P. 535–538.

[23] Zaidoon Kh. AL-Ani, Zaidan A.A., Zaidan B.B., Alanazi H.O. Overview: Main Fundamentals for Steganography. *Journal of Computing*, 2010, 2(3), 158–165.

[24] ScienceDirect. *Steganographic Technique*. Available at: https://www.sciencedirect.com/topics/computer-science/steganographic-technique (accessed 15.06.2026).

[25] Saaty T.L., Vargas L.G. *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process* (2nd Ed.). Springer, 2022.

[26] Wang Z., Rangaiah G.P. *Multi-Criteria Decision-Making: Principles, Methods and Programs*. CRC Press, 2026.

[27] Mateen M.H., Al-Dayel I., Alsuraiheed T. Fermatean Fuzzy Fairly Aggregation Operators with Multi-Criteria Decision-Making. *Axioms*, 2023, 12(9), 865.
[28] Sbert M., Poch J., Chen S., Elvira V. Stochastic Order and Generalized Weighted Mean Invariance. *Entropy*, 2021, 23(6), 662.
[29] Mohd W.R.W., Abdullah L. Aggregation Methods in Group Decision Making: A Decade Survey. *Informatica*, 2017, 41(1), 71–86.
[30] Sun L., Dong H., Liu A.X. Aggregation Functions Considering Criteria Interrelationships in Fuzzy Multi-Criteria Decision Making: State-of-the-Art. *IEEE Access*, 2018, 6, 68104–68136.

**Information about authors.**

**Ivan Igorovych Bobok**
Doctor of Technical Science, Professor. Odesa Polytechnic National University.
Research interests: Steganography, Information security
ORCID: 0000-0003-4548-0709
Email: onu_metal@ukr.net

**Alla Anatoliivna Kobozieva**
Doctor of Technical Science, Professor. Odesa National Maritime University.
Research interests: Steganography, Mathematics in information security
ORCID:0000-0001-7888-0499
Email: alla_kobozeva@ukr.net