Secure data exchange in the control system of unmanned aerial vehicles (UAVs) is an important aspect for preventing unauthorized access and safety of aerial vehicles. Given the problems of automatic dependent surveillance-broadcast (ADS-B) data protection, the safety level of UAV flight tasks and air traffic in general is significantly reduced. Therefore, the protection of ADS-B data is an urgent task. The object of the study is the process of steganographic protection of ADS-B format data. A relevant problem of estimating the probabilistic time characteristics of the steganographic protection process is solved, taking into account the features of data embedding in the ADS-B format container. To solve it, a mathematical formalization of the methods of finding probabilistic-temporal characteristics of steganographic systems was carried out. A model of steganographic data transformation operations based on the Chinese remainder theorem has been built. The main difference of the model is taking into account the features of the ADS-B format data. This made it possible to formalize and evaluate the time functions of steganographic encoding and decoding of UAV identifiers with an integrated ADS-B system. A model of steganographic data transformation operations based on the finite integral ring theorem has been constructed. A list of operations performed in the developed algorithm has been compiled. This made it possible to carry out mathematical formalization of operations for complex use in the model of steganographic protection of UAV identifiers with a built-in ADS-B system. The mathematical model was studied and the estimation of the random value of the time of steganographic transformation of data, as well as the confidence interval, was performed. With the help of the reported set of models, it is possible to estimate the probability of the algorithm's execution time falling within the given interval. The results of the calculation of probabilistic-time characteristics could be used in models of a higher level of the hierarchy

Keywords: unmanned aerial vehicles, ADS-B system, information security, steganographic data protection, GERT network

UDC 004.942:004.75
DOI: 10.15587/1729-4061.2023.288178

CONSTRUCTION OF A MODEL OF STEGANOGRAPHIC EMBEDDING OF THE UAV IDENTIFIER INTO ADS-B DATA

Serhii Semenov
Doctor of Technical Sciences, Professor
Institute of Computer Science
University of the National Education Commission, Krakow
Podchorazych str., 2, Krakow, Poland, 30-084
Minjian Zhang
Postgraduate Student
Zhejiang Nova Intelligent Technology Co., Ltd
Zhejiang, China
Oleksandr Mozhaiev
Corresponding author
Doctor of Technical Sciences, Professor*
E-mail: mozhaev1957@gmail.com
Nina Kuchuk
Doctor of Technical Sciences, Professor**
Serhii Tiulieniev
PhD
Director
National Scientific Center
«Hon. Prof. M. S. Bokarius Forensic Science Institute»
Zaliutynska str., 8, Kharkiv, Ukraine, 61177
Yurii Gnusov
PhD, Associate Professor*
Mykhailo Mozhaiev
Doctor of Technical Sciences
Director
Scientific Research Center for Forensic Science of Information Technologies and Intellectual Property
Lesi Ukrainky blvd., 26, Kyiv, Ukraine, 01133
Volodymyr Strukov
PhD, Associate Professor*
Yurii Onishchenko
PhD, Associate Professor*
Heorhii Kuchuk
Doctor of Technical Sciences, Professor**
*Department of Cyber Security and DATA Technologies
Kharkiv National University of Internal Affairs
L. Landau ave., 27, Kharkiv, Ukraine, 61080
**Department of Computer Engineering and Programming
National Technical University «Kharkiv Polytechnic Institute»
Kyrpychova str., 2, Kharkiv, Ukraine, 61002

Received date 07.07.2023
Accepted date 22.09.2023
Published date 30.10.2023

How to Cite: *Semenov, S., Zhang, M., Mozhaiev, O., Kuchuk, N., Tiulieniev, S., Gnusov, Y., Mozhaiev, M., Strukov, V., Onishchenko, Y., Kuchuk, H. (2023). Construction of a model of steganographic embedding of the UAV identifier into ADS-B data. Eastern-European Journal of Enterprise Technologies, 5 (4 (125)), 6–16. doi: https://doi.org/10.15587/1729-4061.2023.288178*

1. Introduction

Features of steganographic protection make it possible to hide the fact of data processing and transmission from intruders and, thereby, to meet the requirements for confidentiality and integrity of information. However, the constant increase in the intensity of malicious actions requires a reasoned choice of methods, techniques, and

means of data protection, as well as an increase in their effectiveness.

One of the possible ways to assess the quality of the applied methods and increase their effectiveness can be the process of mathematical formalization of steganographic protection. Mathematical modeling describes the process of steganographic protection and makes it possible to study and analyze it in order to improve the main characteristics and security indicators. Modeling helps explore various attack scenarios, evaluate the stability of steganographic methods, and calculate the most important probabilistic-time characteristics. In particular, detection probability, detection time, encoding and conversion time, etc. can be analyzed. In addition, mathematical modeling can help in determining the optimal parameters for using steganography in specific situations in practice. This may include choosing effective steganography algorithms, choosing optimal hidden data sizes and formats, and determining the required degree of nesting.

Such a task is especially relevant in practical applications of real-time systems, where the estimation of time parameters comes to the fore. One of such practical examples of the use of steganographic protection methods is the secure information exchange in the UAV flight control system with ADS-B (Automatic Dependent Surveillance-Broadcast) format signal data.

The UAV flight control system uses methods and technologies for data transmission between UAVs and ground stations through ADS-B signal data [1, 2]. ADS-B signal data is used in the aviation industry to share information about the status and other parameters of aircraft. Secure data exchange is an important aspect to prevent unauthorized access and ensure the safety of the air traffic management system.

Secure ADS-B data exchange is a multi-factorial process. The components of the process can be data encryption, authentication, and authorization, steganographic processing, and data hiding. Elements such as data integrity control, physical security, etc. can also be components.

The evaluation of probabilistic-temporal characteristics will make it possible to determine the influence of the main parameters of UAV steganographic data processing on the level of information protection. This, in turn, will allow optimizing process parameters taking into account safety requirements.

Therefore, the issue of adequate assessment of probabilistic-temporal characteristics of the process of protected information exchange in the UAV flight control system with ADS-B signal data is relevant. Solving this issue will improve the level of data protection of the ADS-B format.

2. Literature review and problem statement

There are several approaches to protecting ADS-B data. For example, work [3] presents an analytical report, the purpose of which is to represent innovative ideas in the field of security of ADS-B technology. The work indicates possible ways to increase security and ensure confidentiality using symmetric and asymmetric encryption mechanisms. However, the review nature of the article makes it possible to present a general picture of the problem but does not make it possible to evaluate the characteristics and safety indicators in practice.

In [4], a cryptographic method of data protection in the ADS-B format is considered. A characteristic feature of the protection method proposed in the paper is the blockchain encryption key management scheme. As the authors have shown, this could increase the level of data protection. However, the time costs of performing cryptographic protection operations in the proposed method were not analyzed. Therefore, there are reasonable concerns about the possibility of using the proposed method in real time.

Article [5] presents the classification of UAV cyber threats with a built-in ADS-B system. A generalized assessment of cryptographic protection methods adapted to solving the problems of improving the security of UAVs with an integrated ADS-B system is also given. The authors of that article indicated the possibility of using steganographic data protection in the ADS-B format. However, specific ways of implementing this task, the possibilities of assessing probabilistic-time characteristics, as well as the use of these methods in real time, were not presented.

In a number of works, steganographic methods of real-time data protection have been developed and implemented. So, for example, work [6] reports a hardware solution for discrete cosine transformation of steganographic hiding of secret communication data, which was named Crypto-Stego-Real-Time (CSRT) System. However, the authors of the article did not provide the format of the processed data and the requirements for them. This reduces the practical value and leaves questions about the possibility of using this development for the protection of ADS-B format data.

Work [7] proposed a hidden communication technology taking into account real-time requirements based on audio steganography methods. The article discusses the possibilities of estimating probabilistic characteristics, for example, SNR or BER values. However, temporal characteristics are not investigated in the article. Also, the audio data format differs from the ADS-B format. And this factor must also be taken into account in further development.

Article [8] reports the research results of direct spectrum expansion technology for hiding data in an audio container. The work highlights the advantages of using this technology to ensure data security. The result of the work is a conclusion about the expediency of using the technology of direct spectrum expansion when hiding data to the ADS-B format container. This will increase the level of security under time constraints. However, in order to substantiate this fact and expand the capabilities of existing steganographic protection methods, it is advisable to conduct mathematical modeling. This will make it possible to estimate the probabilistic time characteristics of the steganographic protection process using this technology.

Article [9] describes a model approach to the evaluation and selection of probabilistic UAV flight characteristics for use as a key service in smart cities. A comprehensive approach to assessing and ensuring the reliability of UAV fleets is proposed, including a methodological framework, modeling based on queuing theory, and practical recommendations. At the same time, the article does not pay attention to the estimation of input parameters. This fact is a limitation for the use of this modeling approach in describing the protection of ADS-B steganographic data.

Paper [10] presents a model of the ADS-B data transmission process of an unmanned aerial vehicle in a steganographic system using direct spectrum expansion technology. Its purpose is to improve the safety of unmanned aerial vehicles with a built-in ADS-B system. In the article, a scheme for ADS-B data transmission of an unmanned aerial vehicle in a steganographic system using the technology of direct spectrum expansion is developed. The main security properties, indicators and security characteristics of the ADS-B format

information signal are also formulated. A generalized model of ADS-B data transmission of an unmanned aerial vehicle has been built. At the same time, the work requires further mathematical formalization, which will allow the following:

– to explore various attack scenarios;

– to evaluate the stability of steganographic methods;

– to calculate the most important probabilistic-time characteristics.

Thus, generalized models are used to assess the main characteristics and indicators of the steganographic data protection process. But generalized models do not take into account the peculiarities of the operation of ADS-B technology for unmanned aerial vehicles. This leads to unacceptable errors when evaluating the characteristics and indicators of the data protection process. Therefore, when modeling, it is necessary to focus on the features of the functioning of ADS-B technology for unmanned aerial vehicles. But today there is no such model. Therefore, the unsolved problem is the lack of a mathematical model of steganographic embedding of the UAV identifier in the ADS-B format data.

3. The aim and objectives of the study

The purpose of this study is to build a mathematical model of steganographic embedding of the UAV identifier in ADS-B format data. This model will allow adequate assessment of the main characteristics and indicators of the process of steganographic data protection.

To achieve the goal, the following tasks were set:

– to formalize the methods of finding probabilistic-time characteristics of steganographic systems;

– to build a model of steganographic data transformation operations based on the Chinese remainder theorem;

– to construct a model of steganographic data transformation operations based on the finite integral ring theorem;

– to investigate the mathematical model and estimate the random value of the time of steganographic transformation of data and the confidence interval.

4. The study materials and methods

The object of our study is the process of steganographic protection of ADS-B format data. The work considers only those UAVs that have equipment that allows the use of ADS-B technology. Such UAVs can independently periodically emit radio messages containing current flight parameters. This allows them to broadcast their exact position in space using digital communication channels along with other data such as speed, altitude, etc. Quite cheap and small radio receivers are used to receive ADS-B data from UAVs. Unlike conventional radars, this technology makes it possible to work at low altitudes and on the ground. Therefore, it can be used to monitor air and ground traffic. This technology makes it possible to receive information in real time, both for pilots and for controllers.

The tuple $Z=\langle X, G, R, Y, C, Q\rangle$ was considered as a system of steganographic transformation of ADS-B format data, where X and Q are sets of original and transformed identifiers, respectively; Y and C are sets of inverse transformations; G and R are the set of raw data (containers and data about pseudorandom sequences, respectively) for steganographic transformation of messages. Multifunctional data transformation takes place within the algebra with the following operations:

1. Weighted summing operation. If in systems C_i, $i=1..q$, the sets X and Q are equal, then a weighted sum is formed:

$$S = p_1C_1 + \ldots + p_qC_q,\ \sum_{i=1}^{q} p_i = 1, \quad (1)$$

where p_i are the probabilities of pre-selection of C_i systems during data transformation.

2. Multiplication operation. The product is formed:

$$H = \prod_{i=1}^{q} Y_i, \quad (2)$$

for which a necessary condition is the equality of the set of values of the system Y_i and the set of definitions of the system Y_{i+1}.

Research and assessment of probabilistic-time characteristics were carried out using the computer algebra system MathCad.

5. Results of the construction and research of a mathematical model of the process of steganographic embedding of the identifier of an unmanned aerial vehicle

5. 1. Mathematical formalization of methods for finding probabilistic-temporal steganographic characteristics of systems

In the study, the methods of finding probabilistic-time characteristics of conversion systems C_i, $i=1,2$ were considered. Non-linear theoretical and numerical methods were taken as a basis [11, 12]:

– Chinese remainder theorem (system C_1);

– theorem on a finite integral ring (system C_2).

It is known from works [13, 14] that the Chinese remainder theorem allows solving systems of linear equations modulo. If:

$$x \equiv a_1(\text{mod}\cdot m_1)\ x \equiv a_2(\text{mod}\cdot m_2)\ \ldots\ x \equiv a_n(\text{mod}\cdot m_n),$$

where m_1, m_2, ..., m_n are pairwise mutually prime numbers, then there is a solution to this system:

$$x \equiv (a_1M_1y_1+a_2M_2y_2+\ldots+a_nM_ny_n)\ (\text{mod}\ M),$$

where $M=m_1m_2...m_n$, $M_1=M/m_1$, $M_2=M/m_2$, ..., $M_n=M/m_n$, a y_1, y_2, ..., y_n are solutions of the corresponding equations modulo $M_iy_i \equiv (\text{mod}\ m_i)$.

A steganographic transformation model based on the Chinese remainder theorem can be used to embed a message in an image.

At the same time, the algorithm of such transformation can be described as follows:

– the initial message is divided into blocks of a fixed size;

– a random number is selected for each message block, which is a small public key of asymmetric transformation;

– using asymmetric transformation, each message block is encoded using a public key;

– the received coded texts of each message block are transformed into numerical residues by modules that form a set of numbers $\{a_1, a_2, ..., a_n\}$;

– the carrier image is also divided into blocks of the size of the corresponding message block;

– a random number is selected for each block of the image, which is a small private key of asymmetric transformation;

– using asymmetric transformation, each block of the image is encoded using the corresponding private key;

– the received coded texts of each block of the image are also transformed into residuals by modules that form the set $\{b_1, b_2, ..., b_n\}$;

– for each residue a_i and its corresponding residue b_i, the number x_i is calculated, which is the solution of the equation modulo: $x_i \equiv a_i \pmod{p_i}$, where p_i is the selected prime number;

– the received numbers x_i replace the corresponding numbers b_i in the image blocks.

It should be noted that the received image is a steganographic container since the rest of the message is encoded in it.

For steganographic extraction of a message from an image, the procedure is performed in the reverse order:

– numerical residues from image blocks are extracted;

– the system of comparisons is solved;

– the received numerical remainders are transformed into coded message texts, which are decoded using the appropriate private keys of asymmetric transformation.

This method of steganography based on the Chinese remainder theorem is quite complex and requires a lot of calculations. Nevertheless, it has some advantages compared to other steganography methods:

– the hidden text can be encoded using asymmetric cryptography methods, which provides a high level of information protection;

– the set of simple numbers used to calculate numerical remainders can be chosen randomly, this increases the complexity of the steganographic image;

– unlike other methods of steganography, this method does not lead to a significant deterioration of image quality;

– this method also has the property of robustness, that is, even if part of the information in the image has been damaged, the rest of the information can be successfully extracted.

The model of steganographic transformation based on exponentiation in the ring of integers [15] uses the mathematical properties of the ring of integers for covert information transmission. This model uses integer ring exponentiation to hide the message in the image. Let p and q be two large prime numbers such that $p \cdot q \gg m$, where m is the message length in bits. Then one can choose some random number r from the ring of integers Z_{pq}. Each bit of the message can then be encoded as a power of r in the Z_{pq} ring.

If the i-th bit of the message is equal to 0, then the power r^i corresponding to it will be equal to 1 in the ring Z_{pq}. If the i-th bit of the message is equal to 1, then the power r^i corresponding to it will be equal to r in the ring Z_{pq}. The obtained powers r^i can be used to calculate image coefficients. To do this, you can choose some subset of image coefficients and replace them with values corresponding to powers r^i.

To get the hidden message, it is necessary to find these coefficients and calculate their powers r^i in the ring Z_{pq}. The resulting exponents can then be used to reconstruct the original message.

Thus, the decoding of the message requires knowledge of large prime numbers p and q. Therefore, the method of steganography based on exponentiation in the ring of integers provides a high degree of information protection.

5. 2. A model of steganographic data transformation operations based on the Chinese remainder theorem

It should be noted that when modeling the processes of transmission and steganographic protection of UAV ADS-B format data, the internal structure of the container differs from the structure of the image.

Among the many structural features of the ADS-B format, we can highlight those that must be taken into account in the further modeling of the steganographic system:

– an ADS-B message consists of two parts: a message header and a payload. The message header contains the service information necessary for the correct processing of the message. The payload contains information about aeronautical data such as location, altitude, speed, etc.;

– the ADS-B message format is defined by the latest specification of the DO-260B standard and consists of two types of messages: type 0 and type 1. The type 0 message contains information about the position and altitude of the aircraft, and the type 1 message contains information about the speed and direction of flight;

– ADS-B message format uses information coding in binary form;

– the ADS-B format uses integrity check codes (CRCs) to detect errors in transmitted data.

Taking into account the structural features of the UAV ADS-B format, a model of steganographic data conversion operations was built based on the Chinese remainder theorem.

Data transformation is carried out on the basis of coding by modules of mutually prime numbers $m_1, m_2, ..., m_k$:

$$Z_1 = \langle X_1, G_1, R_1, Y_1, C_1, Q_1 \rangle, \tag{3}$$

where

$$C_1^{(f_1)} = \begin{Bmatrix} f_1 : \ell \equiv c_1 \pmod{m_1}, \ell \equiv c_2 \pmod{m_2}, ..., \\ \ell \equiv c_k \pmod{m_k} \end{Bmatrix},$$

$$K = \{m_1, ..., m_k\}.$$

The procedure for determining the vector of the studied characteristics $f_1^{(-1)}$ is carried out using the Chinese remainder theorem [13, 14].

Let the numbers A_s and A'_s can be calculated from the conditions:

$$m_1, m_2, ..., m_k = A_Q m_Q,\ A_Q A'_Q \equiv 1 \pmod{m_Q}. \tag{4}$$

Also, let $l_0 = A_1 A'_1 c_1 + A_2 A'_2 c_2 + ... + A_k A'_k c_k$. Then the set of l values satisfying the tuple (3) is determined by the comparison $l \equiv l_0 \pmod{m_1, m_2, ..., m_k}$. Result (4) is found by the formula:

$$A_Q \equiv (-1)^{\xi - 1} P_{\xi - 1} \pmod{m_Q}, \tag{5}$$

where $P_{\xi-1}$ is the numerator of the penultimate corresponding fraction in the Euclid algorithm; ξ is the number of incomplete particles.

The part of the algorithm, which includes the procedure for encoding the vector of the studied characteristics f_1, is performed in a time equal to the time of performing k integer division operations. The more time-consuming part is the decoding of the vector $f_1^{(-1)}$. The main factor that determines the spread of execution time is the random number of integer

division operations when calculating the $P_{\xi-1}$ value of the Euclid algorithm [16].

A simulation model was implemented to determine the nature of the change of the investigated vector and random variable. In the model, with the help of generators of integer random numbers, the values of the division corresponding to the 32-bit binary representation were set. The following numbers were used as divisors:

1) the set of random integer divisors from 1 to 3990;

2) constant value of the divisor equal to 3989.

The number of conducted experiments is $N=1000$.

The random and randomize functions were used. The random function was used twice – for the formation of high and low levels of a random divisor.

The results of simulation modeling are affected by the number of experiments N; the number of digits allocated to represent the dividend and the divisor. The option of choosing a divider – constant or random, is selected from a given range.

Under the constancy of the chosen conditions and the growth of N, the random number of integer divisions in the Euclid algorithm is described with increasing accuracy by some distribution law.

In the general case, one can use the «random number of random terms» scheme. This scheme is a method of generating pseudo-random numbers using the addition of several independent random numbers. The process of generating pseudorandom numbers in this scheme looks like this:

– Step 1. A random number n is generated – this number determines the number of terms that will be used when generating pseudo-random numbers;

– Step 2. A random number is generated for each term using a cryptographically reliable random number generator;

– Step 3. All these random numbers are added together, forming a pseudo-random number;

– Step 4. If it is necessary to generate another pseudorandom number, the process of step 2 is repeated.

Our studies have shown that this pseudorandom number generation scheme is quite reliable and safe. It uses cryptographically secure random number generators and independent random numbers for each term. The current paper proposes to use the «random number of random terms» scheme with the characteristic function $\varpi(\varsigma)=A(\varphi(\varsigma))$. Here, φ is the characteristic function of the execution time of integer division, and A is the generating function of the number of divisions. From the value of $\varpi(\varsigma)$, it is possible to determine W – the function of the execution time of the Euclid algorithm.

According to the results of the experiments, it can be noted that in most cases the hypothesis about the validity of the normal distribution of the random value of the execution time of the integer division algorithm was confirmed. Taking into account the hypothesis about the validity of the normal law of the distribution of the execution time of the Euclid algorithm, the model (empirical) values of the mathematical expectation α and variance α were determined. Partially, the results of the study for two variants of the implementation of the simulation model: with random dividers or with a constant divider of 3989 are given in Table 1. With fixed values of mathematical expectation and dispersion, the execution time of the integer division algorithm was fixed for each run, which was compared with the corresponding theoretical value.

The reliability of the hypothesis was tested by the well-known method according to the χ^2-Pearson test. In the research process, the number of degrees of freedom was chosen equal to seventeen. The simulation results confirmed the hypothesis about the plausibility of the estimate with a significance level of $\alpha=0.95$.

Table 1

Comparison of the theoretical and experimental execution time of the integer division algorithm

Random divisors from 1 to 3990, the value of mathematical expectation $\alpha=7.15$ and variance $\sigma^2=4,4$		Constant divisor 3989, the value of mathematical expectation $\alpha=8.5$ and variance $\sigma^2=4$	
Experimental values	Theoretical values	Experimental values	Theoretical values
0.07	0.029	0.084	0.01
0.031	0.045	0.099	0.095
0.088	0.065	0.075	0.101
0.025	0.071	0.094	0.082
0.028	0.089	0.1	0.08
0.047	0.076	0.049	0.1
0.069	0.09	0.1	0.079
0.051	0.045	0.1	0.1
0.09	0.048	0.013	0.098
0.086	0.058	0.05	0.091
0.09	0.091	0.098	0.051
0.08	0.077	0.048	0.101
0.047	0.078	0.064	0.047
0.054	0.083	0.079	0.1
0.047	0.061	0.078	0.079
0.089	0.018	0.028	0.079
0.053	0.088	0.069	0.086
0.019	0.091	0.1	0.1
2.584e-3	0.086	0.045	0.081
0.012	0.084	0.093	0.082
$\chi^2=3.4$		$\chi^2=4.5$	

The value of $P_{\xi-1}$ is found by performing the iterations $P_s=q_sP_{s-1}+P_{s-2}$ in the Euclid algorithm. The execution time of one step $t^{(1)}$ can be represented as a set of times:

$$t^{(1)}=t_1+t_2+t_3+t_4, \quad (6)$$

where t_1 is the time of performing a complete division operation; t_2 is the time of the multiplication operation; t_3 is the time of the addition operation; t_4 is the time of performing the analysis and sign change operation.

The value $t^{(1)}$is taken as the unit of measurement in our paper. At the same time, the distribution of the random value of the calculation time $P_{\xi-1}$ is described by a normal law with the parameters of mathematical expectation α and variance σ^2. The increase in the accuracy of the simulation results can also be attributed to the consideration of the solution time of the comparison of the first degree of finding A_Q. That is, the time t mod of performing the operation of calculating mod m_Q was taken into account, where $t \bmod=t_1/t^{(1)}$.

For the mathematical formalization and estimation of the equivalent W-function of the decoding time, we shall use the two-way Laplace transform from the density distribution of the random value of the execution time of elementary operations [17]. This transformation is the basis of the Chinese remainder theorem. The results of these studies are given in Table 2.

Table 2

Results of studies of the function of moments of distribution of a random variable of the time of execution of elementary operations

No.	Elementary operations	Functioning of moments
1	Calculation A_Q (k times)	$e^{k\left(\alpha+\frac{t_1}{\tau}\right)s+0.5k\sigma^2s^2}$
2	Calculation A'_Q (k times)	$W_E^{(C_1)}(s)=e^{k(k-2)\frac{t_2}{\tau}s}$
3	Calculation $A_QA'_QA_Q$ (k times)	$W_E^{(C_1)}(s)=e^{ks\frac{2t_2}{\tau}}$
4	Calculation $m_1, m_2, ..., m_k$	$W_E^{(C_1)}(s)=e^{\frac{t_2}{\tau}s}$
5	Calculation l_0	$W_E^{(C_1)}(s)=e^{\frac{(k-1)t_3}{\tau}s}$
6	Calculation l_0	$W_E^{(C_1)}(s)=e^{\frac{t_1}{\tau}s}$

Since the execution time of operations is described by independent random variables, the equivalent W-function of the decoding time based on the Chinese remainder theorem $W_E^{(C_1)}(s)$ is defined by the expression:

$$W_E^{(C_1)}(s)=e^{\left(k\alpha+\frac{(k+1)t_1+\left(k^2+1\right)t_2+(k-1)t_3}{\tau}\right)s+0.5k\sigma^2s^2}. \quad (7)$$

Formula (7) makes it possible to evaluate the equivalent W-function of the decoding time using the two-way Laplace transform.

Therefore, a model of steganographic data conversion operations was built based on the Chinese remainder theorem, which takes into account the structural features of the ADS-B format for UAVs.

5. 3. A model of steganographic data transformation operations based on the finite integral ring theorem

Taking into account the structural features of the UAV ADS-B format [5, 10] made it possible to put forward a hypothesis: steganographic coding and decoding of ADS-B data can be performed on the basis of transformations:

$$Z_2=\langle X_2,G_2,R_2,Y_2,C_2,Q_2\rangle,$$

where

$$C_2^{(f_2)}=\left\{\begin{matrix} f_2: A\equiv \ell^{\varepsilon}\pmod M, \\ f_2^{-\ell}: \ell\equiv c^{\gamma}\pmod M, \gamma*\varepsilon\equiv\ell\left(\mathrm{mod}\ {}_{\varphi}(M)\right)\end{matrix}\right\};$$

$(\varepsilon,\varphi(M))=1;\varphi(M)$ is the value of the Euler function from the module M.

The key data of the steganographic transformation can be defined by expressions:

$$K_2^{(1)}=\{\varepsilon,M\}, K_2^{(2)}=\{\gamma,M\}, K_2=K_2^{(1)}\cup K_2^{(2)}. \quad (8)$$

The steganographic transformation (7) is based on the well-known propositions of Euler's and Fermat's theorems. This transformation can be described as follows. When calculating the exponent for encoding the UAV ADS-B format message, the exponent ε is set. A steganographic coded message is described by the expression $c\equiv l^{\varepsilon}(\mathrm{mod}\ M)$. Message recovery is performed according to the expression $c^{\gamma}(\mathrm{mod}\ M)$. At the same time, it can be seen that in the functional (10), the multiplicative inverse element γ is used. This element is determined according to the formula: $\gamma*\varepsilon\equiv l(\mathrm{mod}\ {}_{\varphi}(M))$. The given equation modulo has a solution if $(\varepsilon,\varphi(M))=1$.

The following procedure is used to calculate the equation modulo $\varsigma\equiv x^n(\mathrm{mod}\ M)$ [18, 19]. Let n be represented in binary notation of the form:

$$n=d_02^w+d_12^{w-1}+d_22^{w-2}+\ldots+d_w,$$

where $d_0=1$, $d_j=0$ ($j\geq1$).

Then, if $S_0=d_0=1$ and $S_{j+1}=2S_j+d_{j+1}$, then $S_w=n$. By hypothesizing that $\varsigma_j\equiv x^{S_j}\pmod M$, we obtain the following:

$$\varsigma_0=x;\varsigma_{j+1}\equiv\varsigma_j^2x^{d_{j+1}}\pmod M \text{ and } \varsigma\equiv\varsigma_w\pmod M.$$

Let's apply the finite integral ring theorem. Then, to find ζ, it is sufficient to make one reduction to the square and no more than one multiplication by x at each of the $\log_2n$ steps of its execution. Since $\log_2n<<n$, it can be claimed that the presented algorithm meets the requirements for the speed of the steganographic data encoding process.

The list of operations performed in this algorithm is given in Table 3.

Table 3

List of algorithm operations

Name of the operation	Probability	Functioning of moments
Multiplication by ζ	1	$e^{(t_2/\tau)s}$
Multiplication by x	0.5	$e^{(t_2/\tau)s}$
Determining mod M	1	$e^{(t_1/\tau)s}$

It should be noted that the moment function in Table 3 is represented on the assumption that a uniform distribution is selected for all elementary operations of Table 3.

The operations «multiply by ς» and «multiply by x» are performed w times, and the operation «determining mod M» is performed once. Therefore, the equivalent W-function for the algorithm of power remainders $W_E^{(R_2)}(s)$ is equal to:

$$W_E^{(R_2)}(s)=0.5e^{\frac{(wt_2+t_1)s}{\tau}}+0.5e^{\frac{(2wt_2+t_1)s}{\tau}} \quad (9)$$

Thus, a mathematical model of the process of steganographic embedding of the UAV identifier into ADS-B format data has been built. The model is based on the Chinese remainder theorem and the finite complete ring theorem. The modeling process took into account the features of the UAV ADS-B message format.

It should be noted that the considered model could be the basis for the implementation of various steganographic protection systems.

5. 4. Investigating the mathematical steganographic model of the protection of the identifiers of the unmanned aerial vehicle

The method of graphical evaluation and analysis (GERT, Graphical Evaluation and Review Technique) was used to study the mathematical model of the steganographic conversion process. In particular, the study of the mathematical model based on the C_1 and C_2 systems was carried out using the GERT scheme shown in Fig. 1.

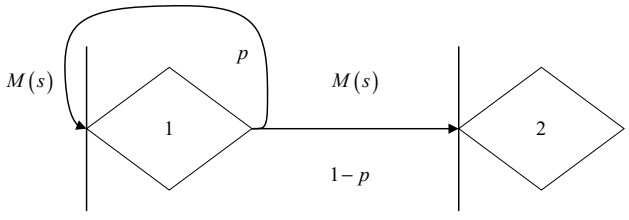

Fig. 1. GERT data conversion scheme of ADS-B format based on C_1 and C_2 systems

Fig. 1 shows that the number of passes of the arc (1,1) may vary depending on safety requirements. That is, a probable choice from some limited space of numbers is considered. Therefore, the studied model is acyclic.

The functioning of the moments $M(s)$ connects the moments of the random value of the steganographic coding time $f(D_1, D_2)$, which depends on the options for using the output systems C_1 and C_2. The presence of the arc (1, 2) means that the steganographic transformation must be performed at least once.

The task of the research is:

– to determine the permissible number h of passing the arc (1, 1) with a limited execution time of the GERT scheme;

– to find the average time of the process of steganographic conversion of ADS-B format data;

– to find the value of the probability of deviation from the average execution time of the GERT scheme.

To consider the probability-time characteristics of the GERT network (Fig. 1), we use the properties of equivalent W-functions.

The equivalent W-function of the GERT network maps one probability distribution to another distribution with the same distribution law as the equivalent distribution function [20]. But a different approach to calculation is used [21]. This function is commonly used to approximate the distribution of random variables that do not have known analytical formulas for the distribution function or probability density. It is defined as the inverse of the Cumulative Probability Density Function (CDF) to the nearest sign. In the general case, the equivalent W-function is defined as follows:

$$W_e\left(X(p)\right)=F(Y),$$

where $X(p)$ – a random variable with an unknown distribution;

$$Y=X^{\frac{(-1)(p)-(1-p)}{f\left(F\left(X^{(-1)(p)}\right)\right)}};$$

$F(X(p))$ – distribution function; $F\left(X^{(-1)(p)}\right)$ – inverse random variable distribution function X; $f(x)$ – probability density of a random variable X; p is the value of the probability in the interval [0, 1].

Let us present the equivalent W-function of the GERT network (Fig. 1):

$$W_e(s)=\frac{(1-p)\left[1-p^{h+1}M^{h+1}(s)\right]}{1-M(s)}. \quad (10)$$

It is known that when solving tasks of steganographic data hiding, an increase in the number of transformation cycles leads to an increase in the execution time of algorithms. This random variable can be estimated by the rule of three sigma. It is very important that the execution time of the algorithm is greater than the permissible value of t_{sup}. The average value t_{aver} and the variance $\tilde{\sigma}^2$ of the random value of the execution time of the steganographic transformation were found:

$$t_{aver}=\left.\frac{\partial W_e(s)}{\partial s}\right|_{s=0}=$$
$$=\left.\frac{\partial M(s)}{\partial s}\right|_{s=0}\times\frac{1-(2+h)p^{h+1}+(1+h)p^{h+2}}{1-p}. \quad (11)$$

We changed $\frac{1-(2+h)p^{h+1}+(1+h)p^{h+2}}{1-p}$ for the coefficient $\tilde{\psi}_1(h)$:

$$t_{aver}=\left.\frac{\partial M(s)}{\partial s}\right|_{s=0}\times\tilde{\psi}_1(h). \quad (12)$$

We calculated the second derivative $W_e(s)$:

$$\left.\frac{\partial^2 W_e(s)}{\partial s^2}\right|_{s=0}=\left.\frac{\partial^2 M(s)}{\partial s^2}\right|_{s=0}\times\tilde{\psi}_1(h)+\left[\left.\frac{\partial M(s)}{\partial s}\right|_{s=0}\right]^2\times\tilde{\psi}_2(h), \quad (13)$$

where $\tilde{\psi}_2(h)=p\left[2\tilde{\psi}_1(h)+p(1-p)\sum_{i=2}^{h}i(i-1)p^{i-2}\right]$.

Then the variance of the random variable of the steganographic transformation time is:

$$\tilde{\sigma}^2=\left.\frac{\partial^2 M(s)}{\partial s^2}\right|_{s=0}\times\tilde{\psi}_1(h)+$$
$$+\left[\left.\frac{\partial M(s)}{\partial s}\right|_{s=0}\right]^2\times\left[\tilde{\psi}_2(h)-\tilde{\psi}_1^2(h)\right]. \quad (14)$$

It can be seen from relations (11) to (13) that the values of coefficients $\tilde{\psi}_1(h)$ and $\tilde{\psi}_2(h)$ depend on the permissible number of cycles h. In turn, the value of h can be determined from the known t_{sup} and $\tilde{\sigma}^2$. The value of derivatives M(s) depends on the type of transformations C_1 and C_2. The GERT scheme of the weighted composition of steganographic transformation operations is shown in Fig. 2.

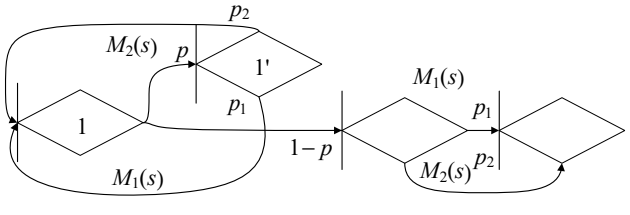

Fig. 2. GERT scheme of weighted C_1 and C_2 systems summing procedures

Next, the function of moments of the random variable of the time of execution of the weighted addition procedure was calculated:

$$M_{wa}(s)=p_1e^{\left(zs+0.5k\sigma^2s^2\right)}+0.5p_2\left(e^{z_1s}+0.5e^{z_2s}\right),$$

where

$$z=k\alpha+\frac{(k+1)t_1+\left(k^2+1\right)t_2+(k-1)t_3}{\tau},$$

$$z_1 = \frac{wt_2+t_1}{\tau};\ z_2 = \frac{2wt_2+t_1}{\tau}.$$

Then:

$$\left.\frac{\partial M_{wa}(s)}{\partial s}\right|_{s=0} = 0.5p_1p_2\left(2z+\frac{(3wt_2+2t_1)}{\tau}\right),$$

$$\left.\frac{\partial^2 M_{wa}(s)}{\partial s^2}\right|_{s=0} = 0.5p_1p_2\left((z+z_1)^2+(z+z_2)^2+2h\sigma^2\right).$$

This has made it possible to calculate the average value of t_{aver} and the variance $\tilde{\sigma}^2$ of the random variable of the transformation execution time:

$$t_{aver} = 0.5\tilde{\psi}_1(h)p_1p_2\times\left(2z+\frac{(3wt_2+2t_1)}{\tau}\right), \quad (15)$$

$$\tilde{\sigma}^2 = 0.5\tilde{\psi}_1(h)p_1p_2\left((z+z_1)^2+(z+z_2)^2+2h\sigma^2\right)+$$
$$+\left(0.25\left(\tilde{\psi}_2(h)-\tilde{\psi}_1^2(h)\right)\cdot p_1^2p_2^2(2z+z_2)\right). \quad (16)$$

The GERT multiplication scheme in steganographic transformation operations is shown in Fig. 3.

The generating function of the moments of the random value of the time of the execution of the multiplication procedure during the steganographic transformation of the ADS-B format data is as follows:

$$M_2(s) = 0.5e^{\left(zs+0.5k\sigma^2s^2\right)}\times\left(e^{z_1s}+e^{z_2s}\right).$$

The first and second moments of its origin can be defined as:

$$\left.\frac{\partial M_2(s)}{\partial s}\right|_{s=0} = 0.5\left(2z+\frac{(3wt_2+2t_1)}{\tau}\right),$$

$$\left.\frac{\partial^2 M_2(s)}{\partial s^2}\right|_{s=0} = 0.5\cdot\left((z+z_1)^2+(z+z_2)^2+2h\sigma^2\right).$$

Then:

$$t_{aver} = 0.5\tilde{\psi}_1(h)\times\left(2z+\frac{(3wt_2+2t_1)}{\tau}\right), \quad (17)$$

$$\tilde{\sigma}^2 = 0.5\tilde{\psi}_1(h)\left((z+z_1)^2+(z+z_2)^2+2h\sigma^2\right)+$$
$$+\left(0.25\left(\tilde{\psi}_2(h)-\tilde{\psi}_1^2(h)\right)\times\left(2z+\frac{(3wt_2+2t_1)}{\tau}\right)\right). \quad (18)$$

As can be seen, expressions (15) to (18) can be used to calculate probabilistic-time characteristics of theoretical-numerical procedures for steganographic conversion of ADS-B format data. At the same time, the considered transformations can be reflected in the form of fragments of the GERT network.

For example, the execution time of an addition operation for systems C_i, $i=\overline{1,q}$ with a weighted sum $S = p_1C_1+\ldots p_qC_q$, $\sum_{i=1}^{q} p_i = 1$ can be represented by a fragment of the GERT model with q parallel branches. In turn, the time of the multiplication operation $H = \prod_{i=1}^{q} Y_i$ can be displayed by q consecutive branches.

It can be noted that the GERT network can be an effective tool for displaying the transformations of the steganographic system. At the same time, the branches of the GERT network formalize the probability-time characteristic of the execution of one of the transformation systems C_i, $i=\overline{1,q}$, and the probability of branching is interpreted as the theoretical probability of choosing the next transformation. The stochastic model, developed on the basis of the GERT network, makes it possible to analyze the probabilistic behavior of the steganographic data protection system.

The most important characteristics of the analyzed system include the average value and variance of the number of transformations performed, as well as the average time and variance of performing a steganographic transformation based on models of the stochastic structure of the GERT network. Methods of finding these characteristics were considered using the example of the ADS-B format steganographic data conversion system shown in Fig. 4.

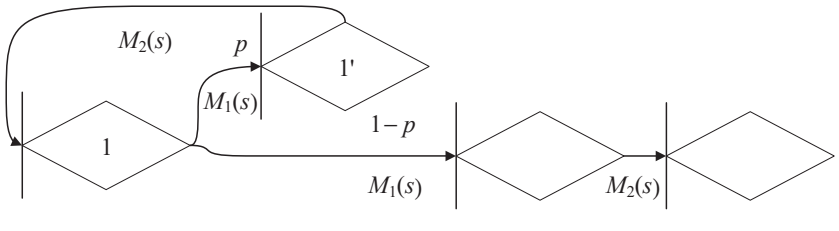

Fig. 3. GERT multiplication scheme in C_1 and C_2 systems conversion operations

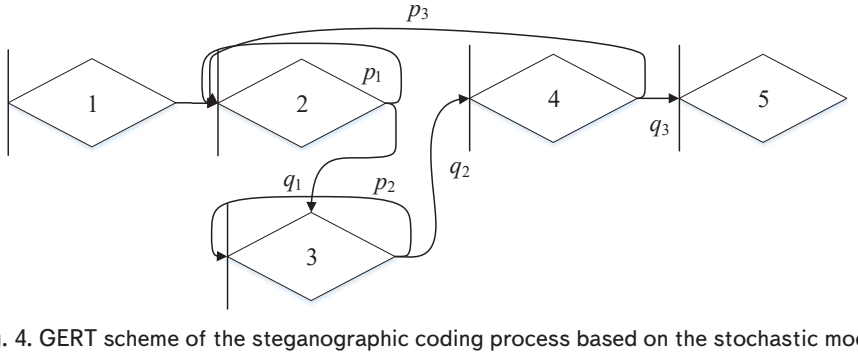

Fig. 4. GERT scheme of the steganographic coding process based on the stochastic model

A hypothesis was proposed that the moment functions of all branches have the value e^s. Then the equivalent W-function of the GERT network will be equal to:

$$W_E(s)=\frac{q_1q_2q_3e^{4\lambda}}{1-(p_1+p_2)e^{\lambda}+p_1p_2e^{2\lambda}-q_1q_2p_3e^{3\lambda}},$$

where $q_i=1-p_i$, $i=1, ..., 3$ is the possibility of choosing branches of the GERT network.

In the system, the average execution time of the steganographic transformation depends on the average value of the number of elementary transformations N_{aver} [22, 23]. Therefore, it was necessary to calculate and analyze N_{aver} and its variance σ_N^2:

$$N_{aver}=\frac{3q_1q_2q_3+2q_1q_2p_3-p_1p_2+1}{q_1q_2q_3}, \quad (22)$$

$$\tilde{\sigma}^2=$$

$$=\frac{(2q_1q_2p_3-p_1p_2+1)^2-q_1q_2q_3\left(1-4(q_1q_2p_3)^2+p_1p_2\right)}{(q_1q_2q_3)^2}. \quad (23)$$

An example of the results of our experiment with different variants of probabilities and the corresponding values of N_{aver} and its variance σ_N^2 is given in Table 4. From Table 4, it can be seen that even for a simple combination of steganographic transformation, the assignment of different values of probabilities $q_i=1-p_i$, $i=1, ..., 3$ forms a variety of possible paths from the source of the GERT network to the drain. Each variant of the task of key information corresponds to the value of the average number of executions of transformations N_{aver} and its variance σ_N^2.

Table 4

Combinations of probabilities and values of the average number of executions of transformations Naver and its variance σ_N^2

No.	q_1	q_2	q_3	N_{aver}	σ_N^2
1	0.2	0.2	0.2	135	22553
2	0.4	0.4	0.4	21	302
3	0.6	0.6	0.6	9	31
4	0.8	0.8	0.8	5.5	6.1
5	0.9	0.9	0.9	4.58	1.56
6	0.2	0.4	0.9	13	112
7	0.9	0.4	0.2	39	1323

For a GERT-scheme of the process of steganographic coding based on the stochastic model (Fig. 4), when analyzing the execution time of the system C_1, the following expression was obtained:

$$W_E^{(C_1)}(s)=e^{\left(zs+0.5k\sigma^2s^2\right)}.$$

With $a=7.5$, $\tilde{\sigma}^2=1.56$, $k=0.3$, and a relative value of $\tau/10$, it is possible to calculate W – the function of the execution time of transformation C_1:

$$W_E^{(C_1)}(s)=e^{\left(2.9s+0.2s^2\right)}.$$

Then the equivalent time function of the steganographic transformation is:

$$W_E(s)=$$

$$=\frac{q_1q_2q_3e^{\left(11.6s+0.8s^2\right)}}{1-(p_1+p_2)e^{\left(2.9s+0.2s^2\right)}+p_1p_2e^{\left(5.8s+0.4s^2\right)}-q_1q_2p_3e^{\left(8.7s+0.6s^2\right)}}.$$

The results of our experiment in the form of plots of the distribution function and the distribution density of the random value of the time of the steganographic transformation for the practical case when all operations in the system are performed using the Chinese remainder theorem are shown in Fig. 5.

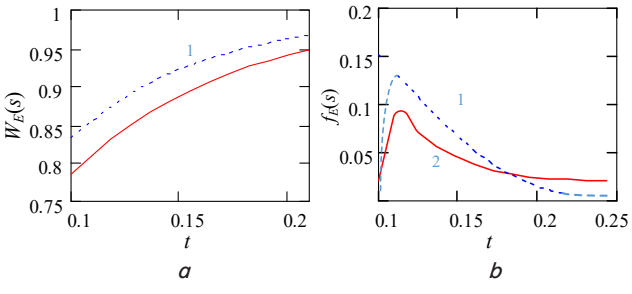

Fig. 5. Fragments of plots of statistical functions of the random value of the time of steganographic transformation: plot 1 – $q_i=0,8$, $i=1..3$; plot 2 – $q_i=0.6$, $i=1..3$: a – probability distribution; b – distribution density

The average time of steganographic conversion at $q_i=0.8$ is 1.18 y. o., and the three-sigma interval is 3.1. The average time of steganographic conversion at $q_i=0.6$ is 1.4 y. o., and the three-sigma interval is 6.6. These results coincide with known ones under the considered conditions.

For this technology, the main criterion is the ability to exchange messages in real time. Our results prove that the proposed approach satisfies this criterion, although it is somewhat inferior to previously known approaches. But according to the security criterion, the proposed approach significantly outweighs the existing ones, which is important for the aerial objects considered in the work.

Thus, the study of the constructed mathematical model has made it possible to calculate the probabilistic time characteristics of the average execution time of steganographic transformations and its variance. In addition, the reported research procedure has made it possible to estimate the probability of the time of steganographic coding falling into a given interval.

6. Discussion of results of the construction of a mathematical model of the process of steganographic embedding of the identifier of an unmanned aerial vehicle

The application of the Chinese remainder theorem and the finite integral ring theorem (power remainders) have been considered. Based on these theorems, a mathematical model of the process of steganographic embedding of the UAV identifier into the ADS-B format data was built. The simulation results have made it possible to estimate the random value of the steganographic data transformation time and the confidence interval.

We have mathematically formalized and described algorithms for steganographic transformation of data using the Chinese remainder theorem and the finite integral ring theorem. The results of the formalization formed the basis of the following models of steganographic data transformation operations.

A model of the steganographic data transformation operation was built, based on the Chinese remainder theorem (ex-

pressions (3) to (5)). The model constructed takes into account the peculiarities of the ADS-B format data. This has made it possible to formalize and evaluate the equivalent *W*-functions of the time of steganographic encoding and decoding of data (Tables 1, 2, formula (7)).

A model of steganographic data transformation operations based on the finite integral ring theorem has been built. This has made it possible to formalize the operations performed in the steganographic transformation algorithm and estimate the equivalent *W*-function for the algorithm of power residues (formula (9) when performing key data partitioning (8)).

The mathematical model of the process of steganographic embedding of the UAV identifier in the ADS-B format data was studied. The main difference of this study is the use of GERT-network modeling technology to find probabilistic time characteristics on the example of the ADS-B format steganographic data conversion system. The results of the study according to GERT-schemes are shown in Fig. 2–4, given in Table 4 and on the plots in Fig. 5.

Our results of the research of the mathematical model of the process of steganographic conversion of ADS-B format data can be explained by the correct choice of data conversion algorithms and the implementation of proven modeling technology using GERT networks.

The following can be noted as a description of directions for further research.

One of the developer's tasks is to estimate the probability that the execution time of the algorithm falls within a given interval. With the help of the presented set of models, this task can be performed. However, it can also be noticed that the results of the calculation of probability-time characteristics and distribution density can be used in models of a higher level of the hierarchy [24–27]. Consideration of delays when encoding steganographic data in the ADS-B format is necessary for building more complex models. These models can be related to the computation of control sequences and the analysis of queues in devices. They are also useful when performing data transfer procedures according to the ADS-B format data exchange protocols.

The use of the developed models is possible only for data exchange protocols in the ADS-B cooperative surveillance technology. At the same time, the models can be used without restrictions for the ADS-B IN service. But for the ADS-B Out service, the use of models is limited to the total volume coming from the information channels FIS-B (Flight Information Services – Broadcast) and TIS-B (Traffic Information Service – Broadcast). The value of this limit depends on the parameters of the equipment used.

As a shortcoming of this study, one should note the lack of an approach to determining the limit, at which both proposed models can give false results. To eliminate the shortcoming, it is necessary to conduct additional research into the nature of change in the vector of characteristics depending on the number of serviced parameters under heavy load. The load at which the hypothesis of the validity of the normal law of distribution of the algorithm's execution time is violated will be the desired value of the limit.

7. Conclusions

1. We have mathematically formalized methods for finding probabilistic-time characteristics of steganographic systems using the Chinese remainder theorem and the theorem on a finite integral ring (power remainders). This formalization has made it possible to embed a message in the image, which ensured a high degree of information protection.

2. A model of steganographic data transformation operations based on the Chinese remainder theorem has been built. The main difference of the model is taking into account the features of the ADS-B format data. This has made it possible to formalize and evaluate the equivalent *W*-time functions of steganographic encoding and decoding of UAV identifiers with an embedded ADS-B system.

3. A model of steganographic data transformation operations based on the finite integral ring theorem has been built. A list of operations performed in the developed algorithm has been compiled. This has made it possible to mathematically formalize them for complex use in the model of steganographic protection of UAV identifiers with a built-in ADS-B system.

4. The mathematical model of steganographic protection of UAV identifiers with a built-in ADS-B system was studied. The results of the study have made it possible to estimate the average time of steganographic conversion of ADS-B format data. This time with the probability of choosing branches of the GERT network equal to 0.8 was 1.18 y. o, and with a probability of 0.6 – 1.4 y. o. The confidence interval for the three-sigma rule was also estimated. In the first case, the estimate was 3.1, in the second case – 6.6. These results coincide with known ones under the considered conditions.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available in the main text of the manuscript.

References

1. Wu, Z., Shang, T., Guo, A. (2020). Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey. IEEE Access, 8, 122147–122167. doi: https://doi.org/10.1109/access.2020.3007182
2. Perkaus, J. (2020). ADS-B Cyber Security alert. Available at: https://www.perkausandfarley.com/wp-content/uploads/2022/01/ADSBCyberSecurity.pdf
3. Alghamdi, F., Alshhrani, A., Hamza, N. (2018). Effective Security Techniques for Automatic Dependent Surveillance-Broadcast (ADS-B). International Journal of Computer Applications, 180 (26), 23–28. doi: https://doi.org/10.5120/ijca2018916598

4. Habibi Markani, J., Amrhar, A., Gagné, J.-M., Landry, R. J. (2023). Security Establishment in ADS-B by Format-Preserving Encryption and Blockchain Schemes. Applied Sciences, 13 (5), 3105. doi: https://doi.org/10.3390/app13053105
5. Semenov, S., Zhang, M. J. (2022). Comparative studies of methods for improving the cyber security of unmanned aerial vehicles with the built-in ADS-B system. Advanced Information Systems, 6 (4), 69–73. doi: https://doi.org/10.20998/2522-9052.2022.4.10
6. Desai, L., Mali, S. (2018). Crypto-Stego-Real-Time (CSRT) System for Secure Reversible Data Hiding. VLSI Design, 2018, 1–8. doi: https://doi.org/10.1155/2018/4804729
7. Shahadi, H. I., Kod, M. S., Qasem, B., Farhan, H. R. (2021). Real-Time Scheme for Covert Communication Based VoIP. Journal of Physics: Conference Series, 1997 (1), 012020. doi: https://doi.org/10.1088/1742-6596/1997/1/012020
8. Kuznetsov, A., Onikiychuk, A., Peshkova, O., Gancarczyk, T., Warwas, K., Ziubina, R. (2022). Direct Spread Spectrum Technology for Data Hiding in Audio. Sensors, 22 (9), 3115. doi: https://doi.org/10.3390/s22093115
9. Kharchenko, V., Kliushnikov, I., Rucinski, A., Fesenko, H., Illiashenko, O. (2022). UAV Fleet as a Dependable Service for Smart Cities: Model-Based Assessment and Application. Smart Cities, 5 (3), 1151–1178. doi: https://doi.org/10.3390/smartcities5030058
10. Semenov, S., Zhang, M., Yenhalychev, S., Smidovych, L. (2022). Generalized model of the ADS-B unmanned aerial vehicle data transmission process in a steganographic system. Innovative Technologies and Scientific Solutions for Industries, 4 (22), 14–19. doi: https://doi.org/10.30837/itssi.2022.22.014
11. Li, J., Chen, J. (2006). The Number Theoretical Method in Response Analysis of Nonlinear Stochastic Structures. Computational Mechanics, 39 (6), 693–708. doi: https://doi.org/10.1007/s00466-006-0054-9
12. Baake, M., Bustos, Á., Huck, C., Lemańczyk, M., Nickel, A. (2020). Number-theoretic positive entropy shifts with small centralizer and large normalizer. Ergodic Theory and Dynamical Systems, 41 (11), 3201–3226. doi: https://doi.org/10.1017/etds.2020.111
13. Alhassan, E. A., Tian, K., Abban, O. J., Ohiami, I. E., Michael Adjabui, M., Armah, G., Agyemang, S. (2021). On Some Algebraic Properties of the Chinese Remainder Theorem with Applications to Real Life. Journal of Applied Mathematics and Computation, 5 (3), 219–224. doi: https://doi.org/10.26855/jamc.2021.09.008
14. Selianinau, M. (2020). An efficient implementation of the Chinese Remainder Theorem in minimally redundant Residue Number System. Computer Science, 21 (2). doi: https://doi.org/10.7494/csci.2020.21.2.3616
15. Chatterjee, R., Bharti, S. (2018). Finding the ring of integers and its algorithms in algebraic number theory. International Journal of Engineering, Science and Mathematics, 7 (4 (1)), 41–44. Available at: https://www.ijesm.co.in/uploads/68/5367_pdf.pdf
16. Kuchuk, N., Mozhaiev, O., Mozhaiev, M., Kuchuk, H. (2017). Method for calculating of R-learning traffic peakedness. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2017.8246416
17. Kovalenko, A., Kuchuk, H., Kuchuk, N., Kostolny, J. (2021). Horizontal scaling method for a hyperconverged network. 2021 International Conference on Information and Digital Technologies (IDT). doi: https://doi.org/10.1109/idt52577.2021.9497534
18. Semenov, S., Davydov, V., Voloshyn, D. (2019). Obfuscated Code Quality Measurement. 2019 XXIX International Scientific Symposium «Metrology and Metrology Assurance» (MMA). doi: https://doi.org/10.1109/mma.2019.8936022
19. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mozhaev, M., Lohvynenko, M. (2017). Multiservice network security metric. 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). doi: https://doi.org/10.1109/aiact.2017.8020083
20. Semenov, S., Zhang, L., Cao, W., Bulba, S., Babenko, V., Davydov, V. (2021). Development of a fuzzy GERT-model for investigating common software vulnerabilities. Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 6–18. doi: https://doi.org/10.15587/1729-4061.2021.243715
21. Zhang, N., Ou, M., Liu, B., Liu, J. (2023). A GERT Network Model for input-output optimization of general aviation industry chain based on value flow. Computers & Industrial Engineering, 176, 108945. doi: https://doi.org/10.1016/j.cie.2022.108945
22. Kuchuk, N., Mozhaiev, O., Semenov, S., Haichenko, A., Kuchuk, H., Tiulieniev, S. et al. (2023). Devising a method for balancing the load on a territorially distributed foggy environment. Eastern-European Journal of Enterprise Technologies, 1 (4 (121)), 48–55. doi: https://doi.org/10.15587/1729-4061.2023.274177
23. Kuznetsov, A., Smirnov, O., Zhora, V., Onikiychuk, A., Pieshkova, O. (2021). Hiding Messages in Audio Files Using Direct Spread Spectrum. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technlogy and Applications (IDAACS). doi: https://doi.org/10.1109/idaacs53288.2021.9660879
24. Mammadov, F. K. (2023). New approach to book cipher: web pages as a cryptographic key. Advanced Information Systems, 7 (1), 59–65. doi: https://doi.org/10.20998/2522-9052.2023.1.10
25. Aleksandrov, E., Aleksandrova, T., Kostianyk, I., Morgun, Y. (2023). Simulation of random external disturbance acting on the car body in the urgent braking mode. Advanced Information Systems, 7 (1), 14–17. doi: https://doi.org/10.20998/2522-9052.2023.1.02
26. Chiocchio, S., Persia, A., Santucci, F., Graziosi, F., Pratesi, M., Faccio, M. (2020). Modeling and evaluation of enhanced reception techniques for ADS-B signals in high interference environments. Physical Communication, 42, 101171. doi: https://doi.org/10.1016/j.phycom.2020.101171
27. Afanasyev, I., Sytnikov, V., Strelsov, O., Stupen, P. (2022). The Applying of Low Order Frequency-Dependent Components in Signal Processing of Autonomous Mobile Robotic Platforms. Intelligent Computing, 882–891. doi: https://doi.org/10.1007/978-3-031-10464-0_61