

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 2, № 3

Volume 2, No. 3

Одеса – 2012
Odesa – 2012

Інформатика та математичні методи в моделюванні

Науковий журнал

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію
КВ № 17610 - 6460Р від 04.04.2011р.

Головний редактор: *Г.О. Оборський*

Заступник головного редактора:

А.А. Кобозєва

Відповідальний редактор: *І.І. Бобок*

Редакційна колегія:

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,
А.Ф. Верлань, О.Ф. Дащенко, В.Б. Дудикевич,
Л.Є. Євтушик, М.П. Карпінський,
М.Б. Копитчук, С.В. Ленков, Є.В. Малахов,
І.І. Маракова, А.Д. Мілка, С.А. Нестеренко,
М.С. Никитченко, С.А. Положаєнко,
О.В. Рибальський, В.Д. Русов, І.М. Ткаченко,
А.В. Усов, С.В. Філіппова, В.О. Хорошко,
М.Є. Шелест, М.С. Яджак*

Informatics and mathematical methods in simulation

Scientific journal

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration
KB № 17610 - 6460P of 04.04.2011

Editor-in-chief: *G.A. Oborsky*

Associate editor: *A.A. Kobozeva*

Executive editor: *I.I. Bobok*

Editorial Board:

*T. Banakh, P. Bidyuk, A. Daschenko,
V. Dudykevich, L. Evtushik, S. Filippova,
V. Horoshko, M. Karpinski,
N. Kopytchuk, S. Lenkov, E. Malakhov,
I. Marakova, A. Milka, S. Nesterenko,
N. Nikitchenko, S. Polozhaenko, V. Rusov,
O. Rybalsky, M. Shelest, I. Tkachenko, A. Usov,
N. Vaysfeld, A. Verlan, M. Yadzhak*

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 734 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine

Tel.: +38 048 734 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

Sergey A. Polozhaenko, Yuri V. Grigorenko

RESEARCH OF SOLVABILITY OF TASK OF AUTHENTICATION OF
WATER-OIL MIXTURES ON THE PARAMETERS OF TUNING OF
MATHEMATICAL MODEL 199

Ф.И. Егоров, Е.А. Скоробогатько, В.А. Хорошко, В.И. Степаненко

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПЕРЕДАЧИ
И ОБРАБОТКИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ
СЕТЯХ 210

И.И. Бобок

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА РОС-КРИВЫХ ДЛЯ
КОМПЛЕКСНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ
СТЕГАНОАНАЛИТИЧЕСКОГО МЕТОДА 221

Aleksey P. Moyseenok

THE SOLUTION OF THE BOUNDARY VALUE PROBLEMS FOR
LAPLACE EQUATION IN THE WEDGE-LAYERED MEDIUM WITH
THE APPLICATION IN THE HEAT CONDUCTION AND ELASTICITY 231

В.Н. Рудницкий, И.А. Узун

СТЕГАНОАНАЛИТИЧЕСКИЙ АЛГОРИТМ ДЕТЕКТИРОВАНИЯ
МЕТОДА МОДИФИКАЦИИ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА
ДЛЯ КОНТЕЙНЕРОВ, ХРАНИМЫХ В ФОРМАТАХ БЕЗ ПОТЕРЬ 238

Ю.Є. Яремчук

ОТРИМАННЯ ЗАЛЕЖНОСТЕЙ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ
ДЛЯ МОЖЛИВОСТІ ВИКОНАННЯ КРИПТОГРАФІЧНИХ
ПЕРЕТВОРЕНЬ НА ЇХ ОСНОВІ 246

А.А. Кобозева

ТЕОРИЯ ВОЗМУЩЕНИЙ КАК ОСНОВА ОБЩЕГО ПОДХОДА К
ОЦЕНКЕ ЧУВСТВИТЕЛЬНОСТИ СТЕГАНООБЩЕНИЙ 254

В.Д. Бойко

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ
РЕШЕНИЙ ДЛЯ ОЦЕНКИ ЖИВУЧЕСТИ СУДОВЫХ
ТЕХНИЧЕСКИХ СИСТЕМ 268

А.О. Данильченко

РЕЗУЛЬТАТИ ПОРІВНЯЛЬНОГО ОБЧИСЛЮВАЛЬНОГО
ЕКСПЕРИМЕНТУ СКЛАДАННЯ РОЗКЛАДУ ПРИЙМАННЯ
ЛІКУВАЛЬНИХ ПРОЦЕДУР 277

В.С. Михайленко, Р.Ю. Харченко

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ
ЭНЕРГОБЛОКА ТЭС НА ОСНОВЕ АППАРАТА ГИБРИДНЫХ СЕТЕЙ 286

RESEARCH OF SOLVABILITY OF TASK OF AUTHENTICATION OF WATER-OIL MIXTURES ON THE PARAMETERS OF TUNING OF MATHEMATICAL MODEL

Sergey A. Polozhaenko, Yuri V. Grigorenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

The formulation of the problem is set by the parametric identification for oil-water reservoirs in the case when one of the fluids being filtered is anomalous. Therewith, the identification problem is defined as an optimal control problem reduced to finding the extremum of the quality criterion (functional). The conditions of the existence and uniqueness of the solution to identify the mathematical model adjustment are obtained alongside with the differentiability of the quality criterion, and therefore the corresponding theorems are proved.

Keywords: identification, methods of identification, abnormal diffusion processes, parametric identification

In the practice of the geophysical research and oil production the spatial soil medium denotes the layer, which in addition to the geological components of different types of rocks, the horizons of groundwater and fluid minerals, in particular, also includes a number of technological components, such as production and injection wells etc. The reservoir porosity and permeability of its material should be considered as the most important geological characteristics. These characteristics determine, respectively, the relative share of the amount of space occupied by the rock itself, and the penetrating ability of the medium for the intrastratal fluid - phase to be infiltrated (filtrated) through it. It should be noted that the filtering intrastratal fluids in terms of the hydrodynamic theory can be regarded as viscous (ideal), obeying a linear Darcy law of motion, or as viscoplastic (abnormal) whose motion can not be described within the bounds of the mentioned law. [1] Viscoplasticity should be understood in terms of compressibility, which is specified by the oil complex fractional composition in particular. The most common technological mode of oil production is artificially created pressure by pumping water into the injection wells. This filtering is called viscoplastic rheology of viscoplastic (oil) and viscous (water) fluids [1]. The mathematical model (MM) of a physical process in the case of the collaborative filtering of viscoplastic and viscous fluids in the reservoir system can be represented as follows [2,3] (here and hereafter the index or parameters of summation will be denoted by $i, j, j_1, j_2, \dots$ will be for the corresponding variables):

$$-\frac{m\partial S_2}{\partial t}(v-S_2)-\int_{\Omega}\sum_{i=1}^n\left[k_1\frac{\partial^2 P}{\partial z_i^2}|v|\right]dz+\int_{\Omega}\sum_{i=1}^n\left[k_1\frac{\partial^2 P}{\partial z_i^2}|S_2|\right]dz\geq\frac{1}{h}\sum_{j=1}^{K_1}\zeta_j(z)Q_{1_j}(t), \quad (1)$$

$$\forall v, S_2 \in K,$$

$$-\frac{m\partial S_2}{\partial t} - \int_{\Omega} \sum_{i=1}^n \left(k_2 \frac{\partial^2 P}{\partial z_i^2} \right) dz = \frac{1}{h} \sum_{j=1}^{K_2} \zeta_j(z) Q_{2j}(t), \quad (2)$$

$$P(0, z) = P_0(z); \quad S_2(0, z) = S_{2_0}(z), \quad (3)$$

$$\frac{\partial S_2(t, z)}{\partial \eta} \geq 0, \quad S_2(t, z) < S_{2_{\max}}, \quad (4)$$

$$\frac{\partial S_2(t, z)}{\partial \eta} = 0, \quad S_2(t, z) \geq S_{2_{\max}}, \quad (5)$$

where

$P = P(t, z)$ – the distributed function of intratrastal pressure;

$S_2 = S_2(t, z)$ – the distributed function of water saturation;

$v = v(t, z)$ – the distributed test function (with respect to the function of water saturation);

$P_0(z), S_{2_0}(z)$ – the initial values of the functions, of the intrastratal pressure and of water saturation respectively;

$S_{2_{\max}}$ – the maximum value of water saturation;

$k_1 = k_1(z), k_2 = k_2(z)$ – the reservoir permeability of the material for the corresponding phase (index 1 – oil, index 2 – water);

$m = m(z)$ – the porosity of the reservoir material;

h – the bulk of reservoir rock;

$Q_{1j}(t), Q_{2j}(t)$ – the consumption function of the corresponding phases (debits);

$\zeta_j(t)$ – the function determining the nature of fluid withdrawal from the j -th hole;

K_1, K_2 – a number of production and injection wells, respectively;

Ω – the spatial region where a physical process is developing;

t – temporal value;

z – spatial value;

K – the functional space of the function definition for water saturation respectively;

n – the number of spatial variables;

η – normal to the boundary G of the spatial domain Ω .

Solving the direct problem of the research, i.e. tasks of modeling, filtration processes described by the system of the form (1) – (5) suggests that the values of coefficients of the differential operators for the corresponding expressions, defined by the physical parameters of the medium are known — in this case by the porosity $m(z)$ and permeability of the reservoir $k_l(z)$, ($l=1,2$). However, in practice, quite often the values of these parameters are not known and, therefore, the functions describing them are not specified a priori, and, or in other words, the coefficients the differential operators for the corresponding MM are not defined. The given circumstance conditions the necessity to formulate and solve the identification problems of the parameters in the physical environment (inverse problems) – the porosity and permeability of the preceding the solution for managing the process being investigated, and, if the coefficients of the original MM are not completely defined, then the modeling problems as well. Therewith, the porosity and permeability are the parameter settings for the MM of the physical process studied.

The problems of identification of the parameters for the reservoir system have been, for example, earlier solved for oil and oil-gas reservoir [4]. However, their decision was made on

the assumption of ideal filtering liquids. In case of abnormal fluid filtration, a number of important aspects qualitatively change the problem of identification:

- interacting with a porous medium, with specific physical and chemical parameters the filtering fluid can acquire anomalous character that requires the use of adequate MM for solving practical problems;
- the result of solving the problem for water-oil reservoir simulation can be considered when the intrastratal pressure achieves the limiting gradient that leads to the subsequent formulation and solution of problem of determining the therein dead zones, as well as the problem of identification of the physical parameters in the reservoir;
- in case of the multiphase filtration the filterable mixture of anomalous and ideal fluids only partially obeys Darcy's law: for example, when displacing viscoplastic fluid with viscous fluid, the general problem of identification is divided into individual tasks of determining the zones of the parameter fields in preferential rheology of anomalous and viscous fluids that, in general, can have a different setting;
- MM of water drive in oil field development has a clearly pronounced non-linear character, which, in its turn, results in setting a non-trivial problem of identification and finds the required parameter fields in the class of nonlinear functions when being solved.

In what follows, the problem of identification of the filtration processes in porous media will refer to the determination of the fields of the porosity parameters $m(z)$ and permeability of the medium $k_l(z)$, ($l=1,2$) based on the results of measuring the intrastratal pressure $P(t,z)$ and flow rates $Q_j(t)$ in the system of wells which cover the reservoir.

The formalized statement of problem of identifying the anomalous fluids of the filtration processes in porous media as an optimization problem is offered. Let $m'(z)$ and $k_l(z)$, ($l=1,2$) are the exact values of porosity parameters and permeability of the medium, respectively. For the j -th well in the time interval $t \in (0, t_k)$, the measured intrastratal pressure $P(t,z)$ of the filterable fluid is indicated through

$$F_j^P(t) = \int_{\Omega_j} P'(t,z) dz + \varepsilon_j^P(t),$$

$$j = 1, \dots, (K_1 + K_2)$$
(6)

and water saturation $S_2(t,z)$ in the reservoir through

$$F_j^S(t) = \int_{\Omega_j} S_2'(t,z) dz + \varepsilon_j^S(t),$$

$$j = 1, \dots, (K_1 + K_2)$$
(7)

where

$P'(t,z)$, $S_2'(t,z)$ are the values of the intrastratal pressure and water saturation, determined in accordance with a mathematical model for the exact type (1) — (5) of the parameter values $m'(z)$ and $k_l(z)$, ($l=1,2$);

$\varepsilon_j^P(t)$ and $\varepsilon_j^S(t)$ — are respectively, the measurement error of the intrastratal pressure and water saturation in the j -th well. [4]

The functionals are introduced into consideration

$$J_1[m(z), k_1(z)] = \sum_{j=1}^{K_1+K_2} \left\{ \int_{T_j} [P'(t, z_j, m, k_1) - F_j^P(t)]^2 dt + \int_{T_j} [S_2'(t, z_j, m, k_1) - F_j^S(t)]^2 dt \right\} \quad (8)$$

$$J_2[m(z), k_2(z)] = \sum_{j=1}^{K_1+K_2} \left\{ \int_{T_j} [P'(t, z_j, m, k_2) - F_j^P(t)]^2 dt + \int_{T_j} [S_2'(t, z_j, m, k_1) - F_j^S(t)]^2 dt \right\} \quad (9)$$

where T_j is the period of time when the measurement $F_j^P(t)$ and $F_j^S(t)$, is done.

Since the exact values of the pressure $P'(t, z_j, m, k_1)$ and $P'(t, z_j, m, k_2)$, as well as the water saturation $S_2'(t, z_j, m, k_1)$ and $S_2'(t, z_j, m, k_2)$ included in the expressions (8), (9), are physically the same value i.e. mathematically $J_1 = J_2$, then only one of the functionals, e.g. J_1 , will be taken into account in the subsequent arguments.

One possible approach to the solution of formulated problem of identification is representing it in the form of an optimal control problem. Quality criterion for this can be a functional (8), and the problem itself in terms of the optimization will be as follows: to determine $\hat{m}(z)$, $\hat{k}_1(z)$ for which

$$J_1(\hat{m}, \hat{k}_1) \leq J_1(m, k_1), \quad \forall (m(z), k_1(z)) \in \Lambda_d, \quad (10)$$

where Λ_d is the admissible domain to determine the parameter fields $\hat{m}(z)$, $\hat{k}_1(z)$.

The aim to qualitatively analyze the problem of identification for water-oil reservoirs by the parameters of the MM settings in the work conducted is studying the existence and uniqueness of problem solving (10), as well as establishing the fact of differentiability of the functional $J_1[m(z), k_1(z)]$ in (8) by the of porosity and permeability parameters. In this regard, the following theorems are formulated and proved.

Theorem 1. For a set of functions defined by (6), (7) and the admissible domain of the parameters $\forall \Lambda_d^m, \Lambda_d^k \in \Lambda_d$, the problem (10) has, at least, one solution, and this solution is the only one.

Proof. Given the physical meaning of the operators and domain of admissible values of variables included in the system (1) — (5), their affiliation the corresponding class of spaces is written as

$$\begin{aligned} P(t, z) &\in L^2(\Omega) = H(\Omega); \quad S_2(t, z) \in L^2(\Omega) = H(\Omega); \\ \frac{1}{h} \sum_{j=1}^{K_1} \zeta_j(z) Q_{1j}(t) &= f_1(t, z) \in L^2(\Omega); \quad \frac{1}{h} \sum_{j=1}^{K_{21}} \zeta_j(z) Q_{2j}(t) = f_2(t, z) \in L^2(\Omega); \\ \int_{\Omega} \sum_{i=1}^n \left[k_1 \frac{\partial^2 P}{\partial z_i^2} |v| \right] dz &= A_1'(P, v, t, z) \in L^2(\Omega); \quad \int_{\Omega} \sum_{i=1}^n \left[k_1 \frac{\partial^2 P}{\partial z_i^2} |S_2| \right] dz = A_1'(P, S_2, t, z) \in L^2(\Omega); \\ \sum_{i=1}^n \left(k_1 \frac{\partial^2 P}{\partial z_i^2} \right) &= A_1''(P, t, z) \in L^2(\Omega), \end{aligned}$$

where $L^2(\Omega)$ is space of square-integrable functions.

Let a given functional space is $W^p = H^1(\Omega)$, $W^s = H^1(\Omega)$, $H(\Omega) = L^2(\Omega)$, where $H^1(\Omega)$ is Sobolev space of order 1, defined as follows

$$H^1(\Omega) = \left\{ \omega \mid \omega \in L^2(\Omega); \frac{\partial \omega}{\partial z_i} \in L^2(\Omega), \quad i = 1, 2 \right\}.$$

It is assumed that there are sets of elements in spaces W^p and W^s , which are generated by a basis for which the following relations are true

$$((w_j^p, \omega)) = \beta_j^p(w_j^p, \omega), \quad \forall w^p \in W^p, \quad \forall j = 1, 2, \dots, q;$$

$$((w_j^s, \omega)) = \beta_j^s(w_j^s, \omega), \quad \forall w^s \in W^s, \quad \forall j = 1, 2, \dots, q.$$

Since the original system (1) — (5) is infinite, which is impossible to obtain an analytical solution for, it is necessary to pass to a discrete space for its numerical implementation. Then for the discrete space $W : W_n = \{w_1, w_2, \dots, w_n\}$ the system, defining the problem (1) — (5) is written

$$-\left(\frac{m\partial \mathcal{S}_2}{\partial t}, w_j^s\right)(v - S_2, w_j^s) - A_1'(P_q, v, t, z, w_j^p) + A_1'(P_q, v, t, z, w_j^p) \geq f_1(z, w_j^p), \quad (11)$$

$$j = 1, 2, \dots, q;$$

$$\left(\frac{m\partial \mathcal{S}_2}{\partial t}, w_j^s\right) - A_1''(P_q, t, z, w_j^p) = f_2(z, w_j^p), \quad (12)$$

$$j = 1, 2, \dots, q;$$

$$\overline{P_q}(0) = \overline{P_{0_q}} \rightarrow P_0 \in L^2(\Omega),$$

$$\overline{S_{2q}}(0) = \overline{S_{2_{0_q}}} \rightarrow S_{2_0} \in L^2(\Omega), \quad (13)$$

where the set $\{P_q(t, z), S_{2_q}(t, z)\}$ is the approximate solution of (1) — (5), represented as

$$\overline{P_j}(t, z) = \sum_{j=1}^q \beta_j^p(t) w_j^p; \quad \overline{S_{2_j}}(t, z) = \sum_{j=1}^q \beta_j^s(t) w_j^s, \quad \forall t \in [0, t_q];$$

$\beta_j^p(t)$ and $\beta_j^s(t)$ are the weighting coefficients.

The resulting solution is local because it is valid only on the local interval $t \in [0, t_q]$, and t_q is a discrete analog of t_k . It should be proved that $t_q = t_k$, i.e., that the local solution can be extended to the whole time interval $\forall t \in [0, t_k]$.

For this purpose the termwise multiplication of the derivatives of j -th dynamics ratios (11), (12) by $\beta_j^p(t)$ and $\beta_j^s(t)$, respectively, as well as their summation is performed, and as result the system of equations has the form of

$$\begin{aligned}
 & - \left(\frac{m \partial S_{2q}(t, z)}{\partial t}, S_{2q}(t, z) \right) (v - S_{2q}(t, z)) - A_1'(P_q(t, z), v, P_q(t, z)) + \\
 & + A_1'(P_q(t, z), S_{2q}(t, z), P_q(t, z)) \geq f_1(z, P_q(t, z)),
 \end{aligned} \tag{14}$$

$$\left(\frac{m \partial S_{2q}(t, z)}{\partial t}, S_{2q}(t, z) \right) - A_1''(P_q(t, z), P_q(t, z)) = f_2(z, P_q(t, z)), \tag{15}$$

$$P_q(0) = P_0; \quad S_{2q}(0) = S_{2_0}, \tag{16}$$

where it turns out that the solution of $\{P(t, z), S_2(t, z)\}$ systems (1) — (5) exist in the whole interval $[0, t_k]$, i.e. $t_q = t_k$.

Next, some operators Y^P and Y^S are introduced that perform projection H on W^P and H on W^S in n -dimensional space of R^n for the norms of $\|P_q(t, z)\|$ and $\|S_{2q}(t, z)\|$. Then, the expressions of the dynamics (11), (12) can be represented as

$$-Y^P \frac{m \partial S_2}{\partial t} \geq Y^P A_1'(P_q, v, z) - Y^P A_1'(P_q, S_2, z) + Y^P f_1(t), \tag{17}$$

$$Y^S \frac{m \partial S_2}{\partial t} = Y^S A_1''(P_q, z) + Y^S f_2(t), \tag{18}$$

and here (17) and (18) are performed in the spaces of W^P and W^S almost for all $t \in (0, t_k)$. The above arguments imply that the operators $Y^P A_1'(P_q, v, z)$, $Y^P A_1''(P_q, z)$ belong to the space boundary of $L^2(0, t_k, W^P)$, and the operator of $Y^P A_1'(P_q, S_2, z)$ — to the space boundary $L^2(0, t_k, W^S)$.

Finally, it follows that the required solution of $\{P(t, z), S_2(t, z)\}$ can be obtained from the approximate of $\{P_q(t, z), S_{2q}(t, z)\}$, and thus the following conditions for convergence are taken into account:

- $P_q \rightarrow P$ in the space of $L^2(0, t_k, W^P)$ and $S_{2q} \rightarrow S_2$ in the space of $L^2(0, t_k, W^S)$ — weak;
- $\frac{m \partial S_{2q}}{\partial t} \rightarrow \frac{m \partial S_2}{\partial t}$ in the space of $L^2(0, t_k, W^S)$ — weak;
- $P_q \rightarrow P$ in the space of $L^\infty(0, t_k, W^P)$ and $S_{2q} \rightarrow S_2$ in the space of $L^\infty(0, t_k, W^S)$ — weak.

Therefore, the implemented limiting transition is the proof that the set of $\{P(t, z), S_2(t, z)\}$ provided by the specified conditions of convergence, is a solution of the (1) — (5) system for the parameters of $(m(z), k_1(z)) \in \Lambda_d$.

The next phase of the qualitative analysis is the proof of the uniqueness of the problem solving of (1) — (5). Suppose that (1) ... (5) has two solutions, defined by the set of $\{P^1(t, z), S_2^1(t, z)\}$ and $\{P^2(t, z), S_2^2(t, z)\}$. Then it may also be assumed that for each point of the domain Ω there are numbers

$$\eta^P = P^1(t, z) - P^2(t, z), \quad \eta^S = S_2^1(t, z) - S_2^2(t, z).$$

Replacing in terms of the systems dynamics of (1) — (5) the functions of $P(t, z)$, $S_2(t, z)$ respectively by $P^1(t, z)$, $S_2^1(t, z)$ and $P^2(t, z)$, $S_2^2(t, z)$, it is possible to get two systems where the termwise subtraction will lead to the result

$$\begin{aligned} & \left(\frac{m \partial \eta^S}{\partial t} \right) (v - \eta^S) - \left[A_1'(P^1, v, t, z) - A_1'(P^2, v, t, z) \right] + \\ & + \left[A_1'(P^1, S_2, t, z) - A_1'(P^2, S_2, t, z) \right] \geq 0 \end{aligned} \quad (19)$$

$$\left(\frac{m \partial \eta^S}{\partial t} \right) - \left[A_1''(P^1, t, z) - A_1''(P^2, t, z) \right] = 0, \quad (20)$$

$$\eta^P(0) = 0, \quad \eta^S(0) = 0. \quad (21)$$

The expressions in square brackets in (19) and (20), based on the definition of the operators $A_1'(\cdot)$ and $A_1''(\cdot)$, can be presented as

$$A_1'(P^1, v, t, z) - A_1'(P^2, v, t, z) = \int_{\Omega} \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \|v\| \right\} dz,$$

$$A_1'(P^1, S_2^1, t, z) - A_1'(P^2, S_2^2, t, z) = \int_{\Omega} \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \|S_2^1 - S_2^2\| \right\} dz,$$

$$A_1''(P^1, t, z) - A_1''(P^2, t, z) = \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \right\} dz.$$

Thus the system (19) — (21) can be presented as

$$\begin{aligned} & \|S_2^1 - S_2^2\| \left(\frac{m \partial \eta^S}{\partial t} \right) (v - \eta^S) - \int_{\Omega} \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \|P^1 - P^2\| \|v\| \right\} dz + \\ & + \int_{\Omega} \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \|P^1 - P^2\| \|S_2^1 - S_2^2\| \right\} dz \geq 0, \end{aligned} \quad (22)$$

$$\|S_2^1 - S_2^2\| \left(\frac{m \partial \eta^S}{\partial t} \right) - \sum_{i=1}^n \left\{ k_1 \frac{\partial^2}{\partial z_i^2} [\beta(P^1) - \beta(P^2)] \|P^1 - P^2\| \right\} dz = 0, \quad (23)$$

$$\eta^P(0) = 0, \quad \eta^S(0) = 0. \quad (24)$$

It is obvious that implementing the conditions of the system (22) — (24) is possible only under the condition that $P^1(t, z) = P^2(t, z)$, $S_2^1(t, z) = S_2^2(t, z)$ which proves the uniqueness of the solution of initial problem (1) — (5).

Thus, there is the solution of the problem in $L^2(\Omega) \cap L^\infty(0, t_k, H)$ and it is unique.

Now the differentiability of the functional (10) in the form of proving the following theorem is under study.

Theorem 2. For $(m(z), k_1(z)) \in \Lambda_d$ the functional (10) has a weak derivative Λ_d (i.e., the derivative in the sense of Gateaux) in the domain R^n .

Proof. The functional derivative $J_1[m(z), k_1(z)]$ is defined as

$$\begin{aligned} \delta J_1(m, k_1) = & \int_{\Omega} \delta m(z) \left\{ \left[\frac{\partial [P(t, z_j, m, k_1) - F_j^P(t)]}{\partial t} + \right. \right. \\ & + \left. \frac{\partial [S_2(t, z_j, m, k_1) - F_j^S(t)]}{\partial t} \cdot p^* dt \right\} dz + \int_{\Omega} \delta k_1(z) \left\{ \sum_{j=1}^{K_1+K_2} \left[\frac{\partial [P(t, z_j, m, k_1) - F_j^P(t)]}{\partial z_j} + \right. \right. \\ & + \left. \left. \frac{\partial [S_2(t, z_j, m, k_1) - F_j^S(t)]}{\partial z_j} \right] \cdot \frac{\partial p^*}{\partial z_j} dt \right\} dz, \end{aligned} \quad (25)$$

where $\{P(t, z), S_2(t, z)\}$ is the solution of the problem (1) — (5), and $p^*(t, z)$ is the solution of the adjoint system of the form

$$-m(z) \frac{\partial p^*}{\partial t} (v - S_2) - \left[A_1'(P, v, t, z) + A_1'(P, S_2, t, z) \right] \sum_{i=1}^n \left[k_1(z) \frac{\partial p^*}{\partial z_i} \right] \geq 0, \quad (26)$$

$$-m(z) \frac{\partial p^*}{\partial t} - A_1''(P, t, z) \sum_{i=1}^n \left[k_1(z) \frac{\partial p^*}{\partial z_i} \right] = 0, \quad (27)$$

$$\frac{\partial p^*(t, z)}{\partial t} = 0 \text{ for } \Sigma = \mathcal{A}\Omega \times (0, t_k), \quad (28)$$

$$p^*(t_k, z) = 0 \text{ for } \Omega. \quad (29)$$

The conjugate function satisfies the following conditions

$$p^*(t, z) \in L^2(0, t_k, H(\Omega)) \cap L^\infty(0, t_k); \quad \frac{\partial p^*(t, z)}{\partial t} \in L^2(\Omega). \quad (30)$$

Assuming that $(m(z), k_1(z)) \rightarrow P(t, z)$ and $(m(z), k_1(z)) \rightarrow S_2(t, z)$ are continuous on Λ_d and, consequently, have weak derivatives (i.e., derivatives in the sense Gato) on $L^2(\Omega)$, we can prove that the criterion $J_1[m(z), k_1(z)]$ (8) is also Gateaux-differentiable, and its derivative Λ_d is

$$\delta J_1 = - \int_0^{t_k} \int_{\Omega} [e^P(t, z) \delta P(t, z) + e^S(t, z) \delta S_2(t, z)] dz dt,$$

where

$$e^P(t, z) = -2 \sum_{j=1}^{K_1+K_2} \left\{ \frac{1}{|z_j|} \int_{\Omega} [P(t, z_j, m, k_1) - F_j^P(t)] dz \right\},$$

$$e^S(t, z) = -2 \sum_{j=1}^{K_1+K_2} \left\{ \frac{1}{|z_j|} \int_{\Omega} [S_2(t, z_j, m, k_1) - F_j^S(t)] dz \right\};$$

$\delta P(t, z)$ and $\delta S_2(t, z)$ – respectively increment of functions $P(t, z)$ and $S_2(t, z)$.

For the functions $\delta P(t, z) \in L^2(\Omega)$ and $\delta S_2(t, z) \in L^2(\Omega)$, given the accepted symbols, the expressions of the systems dynamics can be written

$$\begin{aligned} & \left(\frac{\delta m(z) \partial \delta S_2}{\partial t} \right) (\delta v - \delta S_2) - A_1'(\delta P, \delta v, t, z) + A_1'(\delta P, \delta S_2, t, z) = \\ & = \left(\frac{\delta m(z) \partial \delta S_2}{\partial t} \right) (\delta v - \delta S_2) - \int_{\Omega} \sum_{i=1}^n \left[\delta k_1(z) \frac{\partial \delta P}{\partial z_j} |\delta v| \right] dz + \int_{\Omega} \sum_{i=1}^n \left[\delta k_1(z) \frac{\partial \delta P}{\partial z_j} |\delta S_2| \right] dz \leq f(t, z), \end{aligned} \quad (31)$$

$$\left(\frac{\delta m(z) \partial \delta S_2}{\partial t} \right) - A_1''(\delta P, t, z) = \left(\frac{\delta m(z) \partial \delta S_2}{\partial t} \right) - \sum_{i=1}^n \delta k_1(z) \frac{\partial^2 \delta P}{\partial z_j^2} \quad (32)$$

Next, the function $\rho(t, z) \in L^2(\Omega)$ which can be defined by the following system is introduced into consideration

$$\begin{aligned} & \left(\frac{m \partial \rho}{\partial t} \right) - A_1'(\rho, v, t, z) + A_1'(\rho, S_2, t, z) = \int_{\Omega} (e^P \rho + e^S \rho) dt; \\ & \rho(t_k) = 0, \end{aligned} \quad (33)$$

and this system has a unique solution (which follows from the proof of Theorem 1), satisfying the conditions

$$\left. \begin{aligned} & \rho \in L^2(\Omega) \cap L^\infty(0, t_k, H), \\ & \frac{\partial \rho}{\partial t} \in L^2(\Omega). \end{aligned} \right\} \quad (34)$$

Using the expressions (31) — (34) the following can be obtained

$$\delta J_1 = \left(\frac{\delta m(z) \partial \delta S_2}{\partial t} \right) (\delta v - \delta S_2) - \int_{\Omega} \sum_{i=1}^n \left[\delta k_1(z) \frac{\partial \delta P}{\partial z_j} |\delta v| \right] dz + \int_{\Omega} \sum_{i=1}^n \left[\delta k_1(z) \frac{\partial \delta P}{\partial z_j} |\delta S_2| \right] dz. \quad (35)$$

By equating in turn $p^* = \delta S_2$ and $p^* = \delta P$, the inequality (26) can be obtained from (35) and the relation (30) from (33). In addition, (35) results from (25). Hence Theorem 2 is proved.

We can write the derivative $J_1(m, k_1)$ by the parameters in the form of $m(z)$ and $k_1(z)$

$$\delta J_1 = J_1(m, k_1) [\delta m(z), \delta k_1(z)] = \int_{\Omega} \left[\delta m(z) \frac{\partial J_1(m, k_1)}{\partial m(z)} + \delta k_1(z) \frac{\partial J_1(m, k_1)}{\partial k_1(z)} \right] dz,$$

where

$$\frac{\partial J_1(m, k_1)}{\partial m(z)} = \int_0^{t_k} \frac{\partial S_2(t, z)}{\partial t} [v - S_2(t, z)] p^*(t, z) dt, \quad (36)$$

$$\frac{\partial J_1(m, k_1)}{\partial k_1(z)} = \int_0^{t_k} \left[A_1'(P, v, t, z) + A_1'(P, S_2, t, z) \right] \sum_{i=1}^n \frac{\partial p(t, z)}{\partial z_i} \frac{\partial p^*(t, z)}{\partial z_i} dt \quad (37)$$

The relations (36), (37) are convenient for the numerical calculation of the gradient of the functional $J_1[m(z), k_1(z)]$ while writing the optimization problem in the form (10).

A qualitative analysis of the problem of identification for water-oil reservoirs by the porosity and permeability parameters, which are the parameter settings of the MM for filtering process of the anomalous fluid, showed that there is a solution for the formulated problem of identification in the optimization setting and it is unique. In addition, the quality criteria in the formulated optimization problem is differentiable with respect to identifiability of the porosity and permeability parameters, which means the possibility to achieve extremum in its decision. In other words, a quality criterion for the optimization problem can be minimized by MM settings, and the initial problem of identification for water-oil reservoirs is the correct solution.

References

1. Бернадинер, М.Г. Гидродинамическая теория фильтрации аномальных жидкостей [Текст] / М.Г. Бернадинер, В.М. Ентов ; АН СССР, Институт проблем механики. — М. : Наука, 1975. — 199 с.
2. Положаенко, С.А. Оптимизационный подход к исследованию моделей объектов, представленных в виде вариационных неравенств // Автоматика, автоматизация, электротехнические комплексы и системы. — 2002. — №1. — С. 6–12.
3. Положаенко, С.А. Математические модели процессов течения аномальных жидкостей // Моделювання та інформаційні технології: Зб. наук. пр. — К.: ИПМЕ, 2001. — Вип. 9. — С. 14–21.
4. Ажогин, В.В. Автоматизированное проектирование математического обеспечения АСУ ТП [Текст] : учеб. для студ. высших учеб. заведений / В.В. Ажогин, М.З. Згуровский. — К. : Вища школа, 1986. — 335 с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ РОЗВ'ЯЗУВАННЯ ЗАДАЧІ ІДЕНТИФІКАЦІЇ ВОДО-НАФТОВИХ СУМІШЕЙ ПО ПАРАМЕТРАХ НАЛАШТУВАННЯ МАТЕМАТИЧНОЇ МОДЕЛІ

С.А. Положаєнко, Ю.В. Григоренко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: polozhaenko@mail.ru

Виконано постановку задачі параметричної ідентифікації для водо-нафтових пластів у випадку, коли одна з рідин, що фільтрується, має аномальний характер. При цьому задачу ідентифікації сформульовано як задачу оптимального управління, що зводиться до відшукування екстремуму критерію якості (функціонала). Одержано умови існування та єдиності розв'язку задачі ідентифікації за параметрами налаштування математичної моделі, а також диференційованості критерію якості, у зв'язку з чим доведено відповідні теореми.

Ключові слова: ідентифікація, методи ідентифікації, аномальні дифузійні процеси, параметрична ідентифікація

ИССЛЕДОВАНИЕ РАЗРЕШИМОСТИ ЗАДАЧИ ИДЕНТИФИКАЦИИ ВОДО-НЕФТЯНЫХ СМЕСЕЙ ПО ПАРАМЕТРАМ НАСТРОЙКИ МАТЕМАТИЧЕСКОЙ МОДЕЛИ

С.А. Положаєнко, Ю.В. Григоренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: polozhaenko@mail.ru

Выполнена постановка задачи параметрической идентификации для водо-нефтяных пластов в случае, когда одна из фильтрующихся жидкостей имеет аномальный характер. При этом задача идентификации сформулирована как задача оптимального управления, которая сводится к отысканию экстремума критерия качества (функционала). Получены условия существования и единственности решения задачи идентификации по параметрам настройки математической модели, а также дифференцируемости критерия качества, в связи с чем доказаны соответствующие теоремы

Ключевые слова: идентификация, методы идентификации, аномальные диффузионные процессы, параметрическая идентификация

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Ф.И. Егоров, Е.А. Скоробогатько, В.А. Хорошко, В.И. Степаненко

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

В статье рассматривается проблема выбора комплекса технических средств организации процесса передачи информации в телекоммуникационных сетях. Предлагается способ моделирования устройств сети с помощью теории массового обслуживания.

Ключевые слова: телекоммуникационные сети, математическое моделирование, процессы передачи, обработка информации

Введение

Современные телекоммуникационные сети (ТКС) представляет собой сложный комплекс технических средств, программного обеспечения, устройств управления и организационной структуры, позволяющей совместно функционировать элементам комплекса и эксплуатировать их территориально распределенными абонентами. Основными задачами проектирования и эксплуатации ТКС является выбор, обоснование, оценка объема загрузки и пропускной способности комплекса технических средств, организации процесса функционирования, обработки и передачи информации по каналам ТКС.

Основной тенденцией развития ТКС во всем мире является цифровизация сетей, предусматривающая построение сети на базе цифровых методов передачи и коммутации с помощью цифровой системы передачи и цифровых систем коммутации. Это объясняется следующими существенными преимуществами:

- высокая помехоустойчивость. Представление информации в цифровой форме позволяет осуществлять восстановление сигналов при передаче их по сетям связи, что резко снижает влияние помех и искажений на качество передачи информации;
- слабая зависимость качества передачи от длины линии связи;
- стабильность параметров сетей связи. Стабильность и идентичность параметров каналов определяется в основном устройствами обработки сигналов в аналоговой форме. Поскольку такие устройства составляют незначительную часть оборудования ТКС, стабильность параметров каналов в таких системах значительно выше, чем аналоговых. Этому способствует также отсутствие в ТКС влияния загрузки системы на параметры отдельных каналов;
- эффективность использования пропускной способности сетей для передачи информационных сигналов;
- возможность построения цифровой сети связи. Цифровые системы передачи в сочетании с цифровыми системами коммуникации являются основой цифровой сети, в которой передача, транзит и коммуникация осуществляются в цифровой форме;

▪ высокие технико-экономические показатели. Передача и коммуникация сигналов в цифровой форме позволяют реализовывать оборудование на единых аппаратных платформах.

Цель статьи и постановка заданий

Целью работы является построение математической модели процессов передачи и обработки информации в ТКС.

Для достижения цели решаются задачи:

- оценки рабочих нагрузок,
- выбора способа управления на этапе разработки и проектирования ТКС,
- анализа качества функционирования существующих ТКС.

Основная часть

Для решения поставленных в работе задач используется аппарат теории массового обслуживания [1-4]. Телекоммуникационная сеть моделируется с помощью сети систем массового обслуживания (ССМО), приборами которой являются модели первичных элементов ТКС – устройств ввода-вывода, источника информации и т.п.

При рассмотрении открытой ССМО, которая моделирует ТКС с последовательным прохождением требованием через первичные элементы сети, основной задачей является определение характеристик выходящего потока из обслуживающего абонента, представляющих собой, очевидно, характеристики входящего потока для следующего обслуживающего абонента в ССМО. Для определения характеристик выходящего потока из обслуживающего абонента ССМО используются результаты доказательства теоремы Берке, приведенные в работе [1], где описывалась ССМО, состоящая из двух узлов с показательными распределениями времени обслуживания и исходных пуассоновских потоков. В данной ситуации рассматривается общая ССМО с произвольным количеством узлов и общим видом плотности распределения вероятностей времени обслуживания, на вход которой поступает поток с общим видом плотности распределения вероятностей между последовательными требованиями (рис. 1).

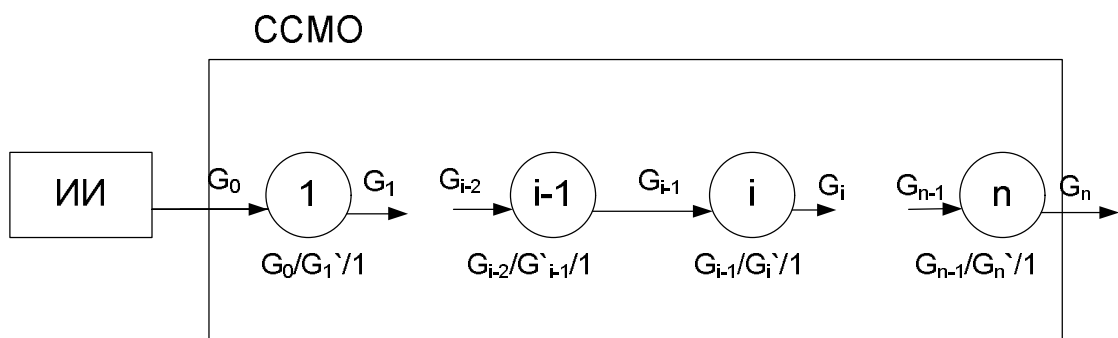


Рис. 1. Принципиальная схема общей сети систем массового обслуживания

Пусть $a_{i-1}(t)$ – плотность распределения вероятностей промежутков времени между моментами поступления последовательных требований на вход $(i-1)$ -го

обслуживающего абонента ССМО, а соответствующее преобразование Лапласа $A_{i-1}^*(S) = \int_0^{\infty} e^{-st} a_{i-1}(t) dt$, где s – комплексная переменная. Пусть также задана $b_{i-1}(x)$ – плотность распределения вероятностей промежутков времени обслуживания последовательных требований в $(i-1)$ -м обслуживающем абоненте ССМО, а соответствующее преобразование Лапласа $B_{i-1}^*(S) = \int_0^{\infty} e^{-sx} b_{i-1}(x) dx$. Введем коэффициент использования $(i-1)$ обслуживающего однолинейного абонента ССМО:

$$P_{i-1} = \lambda_{i-1} \bar{x}_{i-1}, \quad 0 \leq \rho_{i-1} < 1, \quad (1)$$

где λ_{i-1} – интенсивность поступления требований на $(i-1)$ -м абоненте.

Теорема 1. Если задача ССМО с однолинейными обслуживающими абонентами с последовательным прохождением требований через обслуживающие абоненты и со взаимно независимыми временами между моментами появления и временами обслуживания для всех абонентов ССМО, то преобразование Лапласа плотностей распределения вероятностей промежутков времени между моментами поступления последовательных требований на входе i -го обслуживающего абонента определяется рекуррентным соотношением

$$A_i^*(S) = B_{i-1}^*(S) [A_{i-1}^*(S)(1 - \rho_{i-1}) + \rho_{i-1}], \quad i = \overline{2, n}. \quad (2)$$

Пусть x_i – случайная величина, соответствующая промежутку времени между моментами поступления последовательных требований в i -й обслуживающий абонент ССМО. Характеристики потока, входящего в него с последовательным происхождением требованием через однолинейные обслуживающие абоненты, определяются с помощью очевидных следствий, вытекающих из теоремы 1.

Следствие 1. Математическое ожидание случайной величины x_i определяется соотношением

$$\bar{t}_i = (-1) [B_{i-1}^{*(1)}(0) (A_{i-1}^*(0)(1 - \rho_{i-1}) + \rho_{i-1}) + B_{i-1}^*(0) A_{i-1}^{*(1)}(0)(1 - \rho_{i-1})], \quad i = \overline{2, n}, \quad (3)$$

где $B_{i-1}^{*(1)}(0)$ и $A_{i-1}^{*(1)}(0)$ – первые производные по переменной S преобразований Лапласа соответствующих плотностей распределения вероятностей $(i-1)$ -го обслуживающего абонента ССМО, рассмотренные в точке $S = 0$.

Следствие 2. Дисперсия случайной величины x_i определяется соотношением

$$\begin{aligned} S_{ia} = & B_{i-1}^{*(2)}(0) (A_{i-1}^*(0)(1 - \rho_{i-1}) + \rho_{i-1}) + 2B_{i-1}^{*(1)}(0) A_{i-1}^*(0)(1 - \rho_{i-1}) + \\ & + B_{i-1}^*(0) A_{i-1}^{*(2)}(0)(1 - \rho_{i-1}) - (B_{i-1}^{*(1)}(0) A_{i-1}^*(0)(1 - \rho_{i-1}) + \rho_{i-1})^2 - \\ & - 2B_{i-1}^{*(1)}(0) B_{i-1}^*(0) (A_{i-1}^*(0)(1 - \rho_{i-1}) + \rho_{i-1}) A_{i-1}^{*(1)}(0)(1 - \rho_{i-1}) - \\ & - [B_{i-1}^*(0) A_{i-1}^{*(1)}(0)(1 - \rho_{i-1})]^2, \\ & i = \overline{2, n}, \end{aligned} \quad (4)$$

На основании теоремы 1 и следствий 1 и 2 применим рассматриваемый подход и математическому моделированию и определению характеристик процесса функционирования в базовой ТКС, подсистема обмена информацией которой приведена на рис. 2.

Процесс поступления требований из источников информации (ИИ) на вход базовой ССМО предполагается Пуассоновским с плотностью распределения вероятностей времени отступления соседних требований

$$a_{1(t)} = \lambda e^{-\lambda t}, \quad t \geq 0, \quad (5)$$

где λ – интенсивность поступления требований на обслуживание. Соответствующее преобразование Лапласа запишется как

$$A_1^*(t) = \frac{\lambda}{S + \lambda}. \quad (6)$$

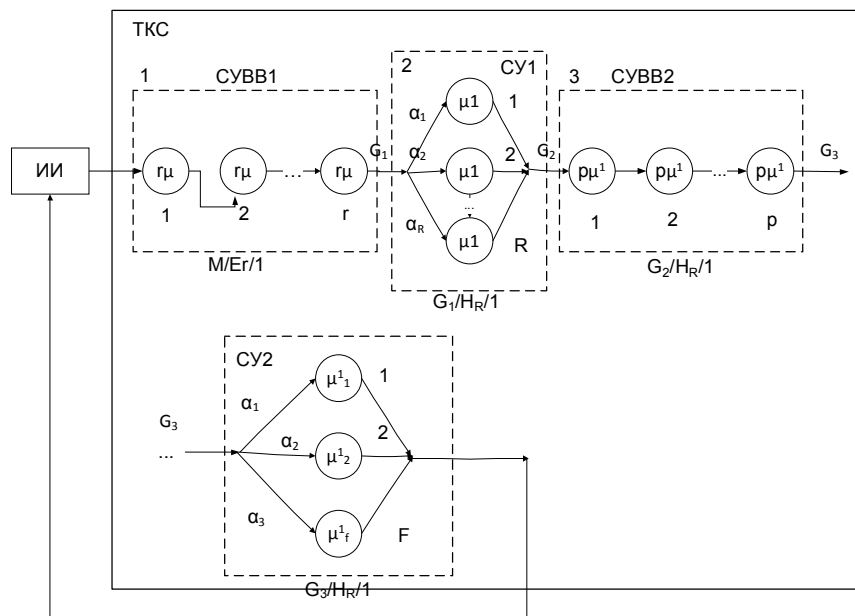


Рис. 2. Базовая ССМО

Результаты измерений и экспериментальных проверок, приведенные в работах [5-7], показали что для аппроксимации обслуживания в большинстве систем устройств ввода-вывода (СУВВ) целесообразно применять этапное эрланговое обслуживание. Таким образом, плотность распределения вероятностей времени обслуживания абонентов, находящихся в узлах 1 и 3 базовой ССМО (рис. 2) и соответственно моделирующих СУВВ1 и СУВВ2 запишем в следующем виде:

$$b_1(x) = \frac{r\mu(r\mu x)^{r-1} e^{-r\mu x}}{(r-1)!}, \quad (7)$$

$$b_3(x) = \frac{p\mu'(r\mu'x)^{p-1} e^{-p\mu'x}}{(p-1)!}, \quad x \geq 0. \quad (8)$$

где

$r\mu$, $p\mu'$ – интенсивности обслуживания требований;

r , p – числа последовательных этапов в эрланговом обслуживающем абоненте.

Соответствующие преобразования Лапласа

$$B_1^*(S) = \left(\frac{r\mu}{S + r\mu} \right)^r, \quad (9)$$

$$B_3^*(S) = \left(\frac{p\mu'}{S + r\mu'} \right)^p. \quad (10)$$

Из результатов измерений и экспериментальных проверок, приведенных в работах [3, 4], следует, что для аппроксимации функционирования работы СУ целесообразно применить гиперэкспоненциальное обслуживание, поэтому плотности распределения вероятностей времени обслуживания абонентов, находящихся в узлах 2 и 4 базовой ССМО (рис. 2) и моделирующих соответственно системы управления (СУ1 и СУ2), запишем в виде:

$$b_2(x) = \sum_{i=1}^R \alpha_i \mu_i e^{-\mu_i x}, \quad (11)$$

$$\sum_{i=1}^R \alpha_i = 1, \quad \alpha_i \geq 0, \quad x \geq 0;$$

$$b_4(x) = \sum_{i=1}^F \alpha'_i \mu'_i e^{-\mu'_i x}, \quad (12)$$

$$\sum_{i=1}^F \alpha'_i = 1, \quad \alpha'_i \geq 0, \quad x \geq 0.$$

где

R , F – числа параллельных этапов обслуживания;

α_i , α'_i – вероятности обслуживания i -м этапом;

μ_i , μ'_i – интенсивности обслуживания на i -м этапе.

Соответствующее преобразование Лапласа запишем в виде

$$B_2^*(S) = \sum_{i=1}^R \frac{\alpha_i \mu_i}{S + \mu_i}. \quad (13)$$

Из работы [2] известны математическое ожидание и дисперсия времени обслуживания в эрланговом и гиперэкспоненциальном обслуживающих абонентах. Применительно к базовой ССМО эти характеристики имеют следующий вид:

$$\bar{x}_1 = \frac{1}{\mu}, \quad \delta_{1b}^2 = \frac{1}{r\mu^2}; \quad (14)$$

$$\bar{x}_2 = \sum_{i=1}^R \frac{\alpha_i}{\mu_i}, \quad \delta_{2b}^2 = \sum_{i=1}^R \frac{2\alpha_i - \alpha_i^2}{\mu_i^2}; \quad (15)$$

$$\bar{x}_3 = \frac{1}{\mu'}, \quad \delta_{3b}^2 = \frac{1}{p\mu'^2}; \quad (16)$$

$$\bar{x}_4 = \sum_{i=1}^F \frac{\alpha'_i}{\mu'_i}, \quad \delta_{4b}^2 = \sum_{i=1}^F \frac{2\alpha'_i - \alpha_i'^2}{\mu_i'^2}. \quad (17)$$

На примере базовой ССМО (рис. 2) рассмотрим методику определения основных характеристик обслуживающих абонентов, находящихся в ее узлах.

Для систем массового обслуживания (СМО) $M/E_r/1$ в обозначениях Кендала, находящейся в 1-м узле базовой ССМО, на основании соотношений (1), (5), (7) и (14) определим коэффициент использования системы

$$\rho_1 = \frac{\lambda}{\mu}, \quad 0 \leq \rho_1 < 1. \quad (18)$$

Теорема 2. Если задана базовая ССМО, в i -м узле которой находится СМО $M/E_r/1$, определяемая соотношениями (5) и (7), и соблюдаются условия теоремы 1, то преобразование Лапласа плотности распределения вероятностей промежуточного времени между моментами поступления последних требований на вход СМО $G_1/H_R/1$, находящейся в узле 2 базовой ССМО, имеет следующий вид:

$$A_2^*(S) = \frac{\lambda}{\mu} \left(\frac{\mu + S}{\lambda + S} \right) \left(\frac{r\mu}{S + r\mu} \right)^r. \quad (19)$$

Доказательство теоремы 2 непосредственно следует из доказательства теоремы 1 при подстановке соотношений (6), (9), (18) в соотношение (2).

Рассмотрим случайную величину x_2 , представляющую собой промежуток времени между моментами поступления последовательно требований на вход СМО $G_1/H_R/1$, находящейся в узле 2 базовой ССМО. Основные характеристики потока G_1 определяются с помощью очевидных следствий, вытекающих из теоремы 2.

Следствие 3. Математическое ожидание случайной величины x_2 определяется из соотношений (3), (6), (9) и (18):

$$i_2 = \frac{1}{\lambda}. \quad (20)$$

Следствие 4. Дисперсия случайной величины x_2 определяется из соотношений (4), (6), (9), (18) и имеет вид:

$$\delta_{2a}^2 = \frac{\lambda^2 - r\lambda^2 + r\mu^2}{r\lambda^2\mu^2}. \quad (21)$$

Для СМО $G_1/H_R/1$, находящейся в узле 2 базовой ССМО, на основании соотношений (1), (15) и (20) определим коэффициент использования системы

$$\rho_2 = \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i}, \quad 0 \leq \rho_2 \leq 1. \quad (22)$$

Теорема 3. Если задана базовая ССМО, в узле 2 которой находится СМО $G_1/H_R/1$, определяемая соотношениями (19) и (11), и выполняется условие теоремы 1, то преобразование Лапласа плотности распределения вероятностей промежутков времени между моментами поступления последовательных требований на вход СМО $G_2/E_p/1$, находящейся в узле 3 базовой ССМО, имеет вид

$$A_3^*(S) = \sum_{i=1}^R \frac{\alpha_i \mu_i}{S + \mu_i} \left[\frac{\lambda}{\mu} \left(\frac{\mu + S}{\lambda + S} \right) \left(\frac{r\mu}{S + r\mu} \right)^r \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) + \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right]. \quad (23)$$

Доказательство теоремы 3 непосредственно следует из доказательства теоремы 1 при подстановке соотношений (12), (19) и (22) в соотношение (2).

Рассмотрим случайную величину x_3 , представляющую собой промежуток времени между моментами поступления последовательных требований на вход СМО $G_2/E_p/1$, находящейся в узле 3 базовой ССМО. Основные характеристики потока G_2 определяются с помощью очевидных следствий, вытекающих из теоремы 3.

Следствие 5. Математическое ожидание случайной величины x_3 определяется из соотношений (3), (13), (19), (22) и имеет вид:

$$\bar{t}_3 = \frac{1}{\lambda}. \quad (24)$$

Следствие 6. Дисперсия случайной величины x_3 определяется из соотношений (4), (13), (19), (22) и имеет вид:

$$\delta_{3a}^2 = 2 \sum_{i=1}^R \frac{\alpha_i}{\mu_i^2} + \frac{2}{\lambda} \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) + \left(\frac{r+1}{2\mu^2} + \frac{2(\mu-\lambda)}{\mu\lambda^2} \right) \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) - \frac{1}{\lambda^2}. \quad (25)$$

Для СМО $G_2/E_p/1$, находящейся в узле 3 базовой ССМО, на основании соотношений (1), (16), (24), определим коэффициент использования системы

$$\rho_3 = \frac{\lambda}{\mu'}, \quad 0 \leq \rho_3 < 1. \quad (26)$$

Теорема 4. Если задана базовая ССМО, в узле 3 которой находится СМО $G_2/E_p/1$, определяемая соотношениями (23), (9), и выполняются условия теоремы 1, то преобразование Лапласа плотности распределения вероятностей промежутков времени между моментами поступления последовательных требований на вход СМО $G_3/H_F/1$, находящейся в узле 4 базовой ССМО, имеет вид

$$A_4^*(S) = \left(\frac{p\mu'}{S + p\mu'} \right)^p \times \quad (27)$$

$$\times \left[\sum_{i=1}^R \frac{\alpha_i \mu_i}{S + \mu_i} \left(\frac{\lambda}{\mu} \left(\frac{\mu + S}{\lambda + S} \right) \left(\frac{r\mu}{S + r\mu} \right)^r \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) + \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) \right] \left[\left(1 - \frac{\lambda}{\mu'} \right) + \frac{\lambda}{\mu'} \right].$$

Доказательство теоремы 4 непосредственно следует из доказательства теоремы 1 при подстановке соотношений (10), (23) и (26) в соотношение (2).

Рассмотрим случайную величину x_4 , представляющую собой промежуток времени между моментами поступления последовательных требований на вход СМО $G_3/H_F/1$, находящейся в узле 4 базовой ССМО. Основные характеристики потока G_3 определяются с помощью очевидных следствий, вытекающих из теоремы 4.

Следствие 7. Математическое ожидание случайной величины x_4 , определяется из соотношений (3), (9), (23), (26) и имеет вид:

$$\bar{t}_4 = \frac{1}{\lambda}. \quad (28)$$

Следствие 8. Дисперсия случайной величины x_4 определяется из соотношений (4), (10), (23), (26) и имеет вид:

$$\begin{aligned} \delta_{4a}^2 = & \left(\frac{1}{\mu'^2} + \frac{1}{p\mu'^2} \right) - \frac{2}{\mu'} \left[- \sum_{i=1}^R \frac{\alpha_i}{\mu_i} + \frac{\lambda - 2\mu}{\mu\lambda} \times \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) \right] \left(1 - \frac{\lambda}{\mu_i} \right) + \\ & + 2 \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) - 2 \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \left(\frac{\lambda - 2\mu}{\mu\lambda} \right) \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) + \left(2 \frac{\mu - \lambda}{\mu\lambda^2} + \frac{2}{\mu^2} + \frac{1}{r\mu^2} \right) \times \\ & \times \left(1 - \lambda \sum_{i=1}^R \frac{\alpha_i}{\mu_i} \right) \left(1 - \frac{\lambda}{\mu_i} \right) - \frac{1}{\lambda^2}. \end{aligned} \quad (29)$$

Для СМО $G_3/H_F/1$, находящейся в узле 4 базовой ССМО, на основании соотношений (1), (17), (28) определим коэффициент использования системы

$$\rho_4 = \lambda \sum_{i=1}^F \frac{\alpha'_i}{\mu'_i}, \quad 0 \leq \rho_4 < 1. \quad (30)$$

Перейдём теперь к решению основной задачи, для обеспечения которой моделировалось обслуживание в ТКС, т.е. найдем среднее время пребывания требования в каждом обслуживающем абоненте, входящем в состав базовой ССМО.

Среднее время пребывания требования СМО $M/E_r/1$ базовой ССМО можно определить по формуле Хинчина-Полагека для СМО вида $M/G/1$ [1]:

$$T_1 = \bar{x}_1 + \frac{\rho_1 \bar{x}_1 [1 + \delta_{1b}^2 (\bar{x}_1)^2]}{2(1 - \rho_1)}, \quad (31)$$

среднее время пребывания требования в СМО $G_1/H_R/1$, $G_2/E_p/1$, $G_3/H_F/1$, – используя оценки для верхней и нижней границ среднего времени обслуживания требований для СМО вида $G/G/1$, [1,2]:

$$\frac{\delta_{ia}^2 + \delta_{ib}^2}{2t_i(1-\rho_i)} + \bar{x}_i \geq T_i \geq \bar{x}_i + \frac{\delta_{ia}^2 + \delta_{ib}^2}{2t_i(1-\rho_i)} - \frac{\rho_i(2-\rho_i) + \delta_{ia}^2(\bar{t}_i)^{-2}}{2\lambda(1-\rho_i)}, \quad (32)$$

или при $\delta_{ib}^2(\bar{x}_i)^{-2} \geq (2-\rho_i)\rho_i^{-1}$:

$$\frac{\delta_{ia}^2 + \delta_{ib}^2}{2t_i(1-\rho_i)} + \bar{x}_i \geq T_i \geq \bar{x}_i + \frac{\rho_i^2 \delta_{ib}^2(\bar{x}_i)^{-2} + \rho_i(\rho_i - 2)}{2\lambda(1-\rho_i)}. \quad (33)$$

Здесь i ($i = \overline{2,4}$) – номер узла базовой ССМО, в котором находится рассматриваемая СМО.

Среднее время пребывания в СМО $M/E_r/1$ базовой ССМО получим, подставляя в соотношение (31) значения из соотношений (18) и (14). Верхние и нижние границы среднего времени пребывания в СМО $G_1/H_R/1$ базовой ССМО получаются при подстановке в соотношения (32) и (33) значений из соотношений (15), (20), (21), (22); в СМО $G_2/E_p/1$, – значений из соотношений (16), (24), (25), (26); в СМО $G_3/H_F/1$ – значений из соотношений (17), (28), (29), (30).

Рассматриваемая ТКС является специализированной и помехоустойчивой, со структурой, не имеющей петель. Следовательно, все стандартные службы сети (управление сетью, передачей, информационным каналом, выбором трафика) объединяются в одну службу управления сетью, чему соответствуют протоколы информационного обмена, свои форматы сообщений и квитанций. Особенностью просматриваемой ТКС является последовательно прохождение требований на обслуживание через устройство сети с порядком обслуживания «первый пришел – первым обслужен», с очередями и без приоритетов, что позволяет применить в данной ТКС изложенный выше метод моделирования с помощью базовой ССМО.

Процесс моделирования данной сети, находящейся в стационарном режиме функционирования, заключается в следующем:

Шаг 1. Определение интенсивности поступления требований на вход сети на основании данных, представленных заказчиков или эксплуатантом ТКС, т.е. определение параметра λ , входящего в соотношение (5), как математического ожидания числа требований на обмен информацией абонентами в единицу времени. При этом предполагается, что процесс поступления требований подчиняется закону Пуассона. Известно, что сумма независимых случайных величин, каждая из которых распределяется по закону Пуассона, подчиняется тому же закону с математическим ожиданием, равным сумме математических ожиданий этих случайных величин.

Шаг 2. Определение интенсивностей обработки требований в базовой ССМО, т.е. определение параметров μ , μ' , μ_i , μ'_i , входящих в соотношения (7), (8), (11), и (12), как среднего числа требований на обмен информацией, которое может обработать за единицу времени.

Шаг 3. Организация сбора статистических данных о функционировании ТКС по обработке требований на обмен информацией для определения эмпирических распределений средних времен требований в ССМО.

Шаг 4. Идентификация в предложенных моделях устройств ТКС – определение тех параметров r , p , R , F , входящих в соотношения (7), (8), (11) и (13), при которых данные теоретические модели наиболее точно аппроксимируют реальные эмпирические распределения, найденные на предыдущем шаге моделирования. Мерой расхождения эмпирической и теоретической функций распределения можно принять построенную методом наименьших квадратов величину

$$b_d = \sum_{j=1}^k \frac{(v_j - mp_j)^2}{v_j}, \quad (34)$$

где

$d, (d = \overline{1,4})$ – номер теоретической плотности распределения из соотношений (7), (8), (11), (12);

m – объем выборки;

k – число интервалов гистограммы;

v_j – число элементов выборки, находящихся в j -м интервале;

$p_j = p_j(\beta_1, \dots, \beta_m)$ – площадь под кривой теоретической плотности распределения, соответствующей j -му интервалу;

$\beta_l, (l = \overline{1, m})$ – параметр теоретической плотности распределения.

Метод наименьших квадратов реализуется программно с учетом того, что в заданных моделях идентифицируемые параметры принимают только целочисленные значения, организуется цикл по применению r, p, R, F , например, от 1 до 100. Значение параметра, при котором величина b_d наименьшая, считается искомым и вводится в исходную модель устройства ТКС.

Шаг 5. Проверка данных гипотез о достаточной точности аппроксимации эмпирических плотностей распределения соотношениями (7), (9), (11) и (12) проводится согласно критерию χ^2 на основании значений, определенных на шаге 4 из соотношения (34).

Шаг 6. Анализ результатов проверки на шаге 5 согласно требованиям технического задания на ТКС к точности аппроксимации; принятие решения о виде теоретической плотности распределения для каждой модели; повторение (в случае необходимости) шагов 4-6 до получения нужной точности аппроксимации.

Шаг 7. Определение среднего времени пребывания требований на обмен информацией в каждом устройстве ТКС на основании соотношений (31)-(33).

Выводы

Задача, для решения которой предлагается использовать рассмотренный метод – оценка качества и выбор организации помехоустойчивого процесса обмена информацией в ТКС с программной реализацией процедур помехозащищенного кодирования и декодирования данных при передаче информации по каналам связи между абонентами. В результате такого моделирования определяются средние времена пребывания требований в обслуживающих абонентах ТКС с аппаратурной и программной реализацией процедур помехозащищенного кодирования. Для программной реализации процедур кодирования-декодирования со средствами организации мультиветвящегося режима среднее время пребывания требования в устройствах ТКС также определяется из соотношений (31)-(33). Разница средних времен и задает количественную меру, которая показывает, насколько изменяется среднее время обработки требований при соответствующем изменении организации функционирования ТКС.

Список литературы

1. Клейнрок, Л. Теория массового обслуживания [Текст] : пер.с англ. / Под ред. В.И. Неймана. — М. : Машиностроение, 1979. — 432 с.

2. Розенберг, В.Я. Что такое теория массового обслуживания [Текст] / В.Я. Розенберг, А.И. Прохоров. — М. : Сов.радио, 1962. — 255 с.
3. Хеллман, О. Введение в теорию оптимального поиска [Текст] / О. Хеллман ; пер. с англ. Е.М. Столяровой ; под ред. Н.Н. Моисеева. — М. : Наука, Гл. ред. физ.-мат. лит., 1985. — 245 с.
4. Авен, О.И. Оценка качества и оптимизация вычислительных систем [Текст] / О.И. Авен, Н.Н. Гурин, Я.А. Коган. — М. : Наука, 1982. — 464 с.
5. Бегма, Т.В. Математичні моделі функціонування складних систем / Т.В. Бегма, М.В. Капустян, В.О. Хорошко // Вісник СНУ ім. В. Даля. — 2011. — №7 (161). — Ч.1. — С. 252–263.
6. Капустян, М.В. Аналіз методів складання оптимальних розкладів роботи складних систем / М.В. Капустян, Л.Т. Пархуць, В.О. Хорошко // Информатика и математические методы в моделировании. — 2012. — Том 2, №1. — С. 46–57.
7. Козюра, В.Д. Методика оценки эффективности систем связи / В.Д. Козюра, И.В. Пискун, В.А. Хорошко // Інформаційна безпека. — 2012. — №1 (7). — С. 8–12.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ ПЕРЕДАЧІ ТА ОБРОБКИ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Ф.І. Єгоров, Є.О. Скоробогатько, В.О. Хорошко, В.І. Степаненко

Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

У даній статті розглядається проблема вибору технічних засобів, організації процесу передачі інформації в телекомунікаційних мережах. Пропонується спосіб моделювання пристроїв мережі за допомогою теорії масового обслуговування.

Ключові слова: телекомунікаційні мережі, математичне моделювання, процеси передачі, обробка інформації

THE MATHEMATICAL MODELING OF TRANSMISSION AND INFORMATION PROCESSING IN TELECOMMUNICATION NETWORKS

Fedor I. Egorov, Eugene A. Skorobogat'ko, Vladimir O. Khoroshko, Viktor I. Stepanenko

National Aviation University,
1 Kosmonavta Komarova Ave., Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

This article discusses the problem of choice of the technical facilities, the organization of the process of information transmission in telecommunication networks. Method is proposed for modeling the network devices using queuing theory.

Keywords: telecommunication networks, mathematical modeling, processes of transmission, processing of information

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА ROC-КРИВЫХ ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ СТЕГАНОАНАЛИТИЧЕСКОГО МЕТОДА

И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: onu_metal@ukr.net

Представлены результаты анализа эффективности и сравнения работы нового стеганоаналитического метода детектирования стеганографических вложений, осуществленных методом модификации наименьшего значащего бита, в цифровое изображение, хранимое в формате с потерями, разработанного автором ранее, с наиболее эффективными существующими аналогами. Оценка работы методов производится при помощи ROC-анализа. Представлены результаты вычислительных экспериментов

Ключевые слова: стеганоанализ, метод модификации наименьшего значащего бита, ROC-анализ, точка отсечения

Введение

Стеганография, один из древнейших способов сокрытия и защиты информации, переживает в настоящий момент очередной виток в своем развитии, результатом чего является активизация работы в области стеганоанализа (СА) [1-6]. Стеганография и СА – два взаимосвязанных и взаимозависимых звена одной цепи: развитие одного звена приводят к адекватному ответу в другом, хотя цели и задачи их различны. Так общим для стеганографирования является организация тайного канала связи внутри открытого канала: в непривлекающий внимание объект – контейнер (или основное сообщение (ОС)) погружается секретная, или дополнительная, информация (ДИ) таким образом, что ее наличие в составе ОС остается незамеченным. Результатом такого погружения, или стеганопреобразования (СП), является стеганосообщение (СС), которое открыто пересылается адресату по каналам связи. Задачей стеганоанализа является детектирование наличия и, возможно, декодирование ДИ в «подозрительном» информационном контенте, или доказательство отсутствия секретного сообщения [1, 2].

Одним из наиболее широко используемых стеганографических методов был и остается до настоящего момента метод модификации наименьшего значащего бита (LSB) [1, 2]. В силу этого значительная часть стеганоаналитических исследований посвящена именно этому методу [7-10]. Но несмотря на то, что разработки здесь ведутся достаточно активно, все они, учитывая главное достоинство LSB – большую скрытую пропускную способность (СПС) [1], разрабатывают стеганоаналитические методы с учетом СПС, как правило, 0.5-1 бит/пиксель и более и даже не рассматривают возможность детектирования секретного вложения при СПС менее 0.25 бит/пиксель в силу сложности получаемой задачи, т.к. возмущения здесь оказываются настолько малыми, что их выявление вызывает значительные затруднения. Однако такая задача является реальной, а применение LSB при малой СПС, значительно повышающее стойкость стеганографической системы, часто используемым, оставляя задачу детектирования малых вложений *актуальной*.

Автором настоящей работы был предложен принципиально новый стегано-аналитический метод *SAVV* детектирования LSB – метод выявления *малых* возмущений матрицы контейнера, в качестве которого рассматривается цифровое изображение (ЦИ), хранимое в формате с потерями, происходящих при стеганопреобразовании, за счет анализа скорости изменения наименьших сингулярных чисел (СНЧ) блоков матрицы, полученных при ее стандартном разбиении [11], дающий принципиальную возможность выявления наличия ДИ даже при малой СПС.

Цель статьи и постановка исследований

Целью настоящей работы является оценка эффективности разработанного автором ранее стеганоаналитического метода *SAVV*.

Для достижения поставленной цели в разделе решаются следующие задачи:

- 1) Выбора метода для оценки эффективности *SAVV*;
- 2) Оценка эффективности разработанного стеганоаналитического метода по детектированию результатов вложения секретной информации методом LSB;
- 3) Сравнение эффективности разработанного стеганоаналитического метода с результатами работы современных методов по детектированию результатов вложения секретной информации методом модификации наименьшего значащего бита.

Основная часть

В соответствии с общим подходом к анализу состояния и технологии функционирования информационных систем (ОПАИС) [12], на основе которого был разработан *SAVV*, произвольная информационная система, в том числе, стеганографическая система (или отдельно рассматриваемые контейнер, СС), формализуется в виде двумерной матрицы (конечного множества двумерных матриц). Результат преобразования информационной системы, ее свойства определяются характерными особенностями совокупности возмущений однозначно определяющих ее формальных параметров – СНЧ и сингулярных векторов (СНВ) соответствующей матрицы (матриц) [12]. Анализ состояния контейнера, формальным представлением которого является матрица F , или анализ СС, в частности, стеганоанализ, в [11] сводится к анализу только СНЧ соответствующей матрицы (матриц), являющихся в соответствии с соотношением [12] $\max_{1 \leq j \leq n} |\sigma_j(F) - \sigma_j(F + \Delta F)| \leq \|\Delta F\|_2$, где $\sigma_j(F)$, $\sigma_j(F + \Delta F)$ – СНЧ матриц F , $F + \Delta F$ соответственно, $\|\Delta F\|_2$ – спектральная норма матрицы возмущения ΔF , нечувствительными к возмущающим воздействиям, или хорошо обусловленными, поскольку реакция СНВ на возмущения различна, а в некоторых случаях – непредсказуема [12]. Хорошая обусловленность СНЧ приводит к тому, что величина их возмущений качественно отвечает величине возмущающего воздействия, характеризуя «силу» этого воздействия, в отличие от СНВ.

В соответствии с ОПАИС, СП, осуществляемое методом LSB, представляется в виде аддитивного погружения некоторой информации в пространственной области: $\bar{F} = F + \Delta F$, где $\bar{F}$ – матрица СС, ΔF – матрица возмущения ОС вследствие СП, ΔF сформирована случайным образом, ее элементы принадлежат множеству $\{-1, 0, 1\}$. Сформированное СС сохраняется в формате без потерь (хотя это принципиально не важно. Важно только чтобы *после* СП не происходило квантование коэффициентов ДКП). Везде ниже для определенности в качестве формата хранения без потерь ЦИ рассматривается TIFF.

Матрицы одного ЦИ до СП (формат JPEG) и после СП отличаются друг от друга. Выявление этого различия в методе *SAVV* происходит при анализе значения скорости изменения минимальных СНЧ 8×8 -блоков, полученных после стандартного разбиения матрицы исходного изображения. В [13] были получены основные качественные отличия сингулярных спектров блоков СС с разными СПС от сингулярных спектров блоков JPEG-контейнеров: с увеличением СПС характер поведения СНЧ блоков СС все больше соответствует характеру СНЧ для ЦИ, хранимого без потерь, в частности, происходит увеличение скорости изменения наименьших СНЧ с ростом СПС. В [11] эмпирическим путем было получено пороговое значение $K = 4$ числового параметра $ih1$, непосредственно связанного с наиболее часто встречаемым значением скорости изменения наименьших СНЧ для совокупности блоков матрицы анализируемого ЦИ, позволяющего отделить СС от ОС по следующему принципу: если $ih1 < K$, то анализируемое ЦИ относится к контейнерам, иначе – к СС. В связи с этим ключевым моментом эффективной работы *SAVV* является определение порогового значения K ; желаемым является подтверждение значения этого параметра, полученного ранее эмпирическим путем, при помощи математически обоснованных методов.

Учитывая все вышесказанное, основным инструментом для анализа эффективности работы метода *SAVV* выбран метод, основанный на анализе так называемых операционных характеристических кривых – ROC-анализе (*ROC – Receiver Operating Characteristic*) [14], и обладающий следующими свойствами:

- он позволяет оценить эффективность анализируемого метода (алгоритма) в целом, с учетом как ошибок первого, так и ошибок второго рода;
- он позволяет формализовать процесс получения порогового значения анализируемого параметра – так называемой точки отсечения (в нашем случае – это значение K), которое даст возможность отделить СС от ОС;
- значение точки отсечения является своеобразным «рычагом» управления чувствительностью исследуемого алгоритма, т.к. позволяет менять соотношение между ошибками первого и второго рода в зависимости от специфики решаемой задачи.

Основная идея метода анализа ROC-кривых в приложении к решению задачи СА заключается в следующем. Необходимо выявить СС (класс V_1) в группе ЦИ, где есть и незаполненные контейнеры (класс V_2). Для выявления СС используется стеганоаналитический метод (САМ), который принимает одно из двух решений: положительное $\delta = 1$ (СС) или отрицательное $\delta = 0$ (ОС). Для оценки эффективности САМ проводится его тестирование на группе ЦИ, для которых известно, какое из них является СС, а какое ОС. Результаты такого тестирования в общем случае можно представить в виде таблицы 1, где приняты следующие обозначения: TP – число правильно выявленных СС; TN – число правильно выявленных ОС; FP – число ОС, ошибочно принятых за СС (ошибка второго рода); FN – число СС, ошибочно признанных ОС (ошибка первого рода).

Таблица 1.
Результаты тестирования репрезентативной группы ЦИ

Истинное состояние ЦИ	Результат тестирования	
	$\delta = 1$ – СС	$\delta = 0$ – ОС
Класс V_1 – СС	TP	FN
Класс V_2 – ОС	FP	TN

По данным табл. 1 результаты тестирования САМ возможно представить точками в двумерном ROC-пространстве, где по оси ординат откладывается значение, несущее в себе информацию об ошибках первого рода (чувствительность): $S_E = TP / (TP + FN)$, а

по оси абсцисс – значение $1 - S_p$, характеризующее ошибки второго рода, где S_p (специфичность [14]) вычисляется в соответствии с формулой: $S_p = TN / (TN + FP)$. ROC-пространство дает наглядное графическое представление об эффективности алгоритма и позволяет сравнивать эффективность различных алгоритмов.

Наиболее распространенным способом построения ROC-кривых является разбиение возможных значений анализируемого параметра (в нашем случае – $ih1$) на группы. Группы могут формироваться по-разному, различным может быть их количество в зависимости от специфики решаемой задачи. В случае небольшого количества различных значений для анализируемого параметра рекомендуется разбиение на группы по значению параметра [14], что и делается в настоящей работе. В этом случае появляется возможность оценить чувствительность и специфичность алгоритма при различных значениях параметра, что будет соответствовать последовательности точек в ROC-пространстве [14].

Количественной оценкой эффективности исследуемого при помощи ROC-анализа алгоритма (метода) является значение интегральной характеристики ρ , определяемой в соответствии с формулой [14]: $\rho = 2A - 1$, где A – площадь под ROC-кривой. Чем больше A , тем выше эффективность исследуемого алгоритма (метода).

Таким образом, очевидна целесообразность выбора в качестве метода для оценки эффективности $SAVV$ метода анализа ROC-кривых.

Вычислительный эксперимент для проверки эффективности разработанного САМ по детектированию результатов вложения LSB-методом проводился в среде *MathWorks MATLAB* на множестве Q из 500 ЦИ, хранимых в формате JPEG, основанном на ДКП, взятых из базы NRCS [15], которая является традиционной при тестировании стеганографических и стеганоаналитических алгоритмов. В ходе эксперимента в каждое из изображений производилось внедрение ДИ одной из современных вариаций LSB – алгоритмом *LSB-matching* [7-10], при этом СПС составляла 0.05, 0.1, 0.2, 0.25, 0.3, 0.4, 0.5, 0.75, 1 бит/пиксель.

Соответствующие ROC-кривые представлены на рис. 1. Значения интегрального параметра ρ в совокупности с непосредственными значениями площади A под ROC-кривой (формула (10)) представлены в табл. 2.

Полученные значения интегрального параметра ρ (табл.2) являются высокими [14], но для окончательной оценки эффективности $SAVV$ необходимо провести сравнение с результатами ROC-анализа для современных аналогов, что делается ниже.

ROC-анализ, как уже было отмечено, используется для нахождения оптимального порогового значения K , или точки отсечения (*cut-off value*). В общем случае, оптимальное значение порога зависит от предъявляемых к алгоритму требований, т.е. от выбранного критерия оптимальности [14]. В настоящей работе в качестве оптимальной рассматривается точка на ROC-кривой, которая имеет наибольшее значение чувствительности. Эта точка может быть найдена с помощью индекса Йодена J [16]: $J = \max(S_E + S_p - 1)$. Для ее нахождения воспользуемся результатами проведенных вычислительных экспериментов. Полученные значения J приведены в табл. 3. Для каждой СПС находится максимальное значение $J - J_{\max}$ (в табл. 3 эти значения выделены жирным шрифтом), для каждого $J_{\max}$ определяется соответствующее значение $ih1$; из полученных значений $ih1 - 4, 5, 6$ выбирается минимальное: $K = 4$, что подтверждает правильность порогового значения, полученного автором ранее эмпирическим путем.

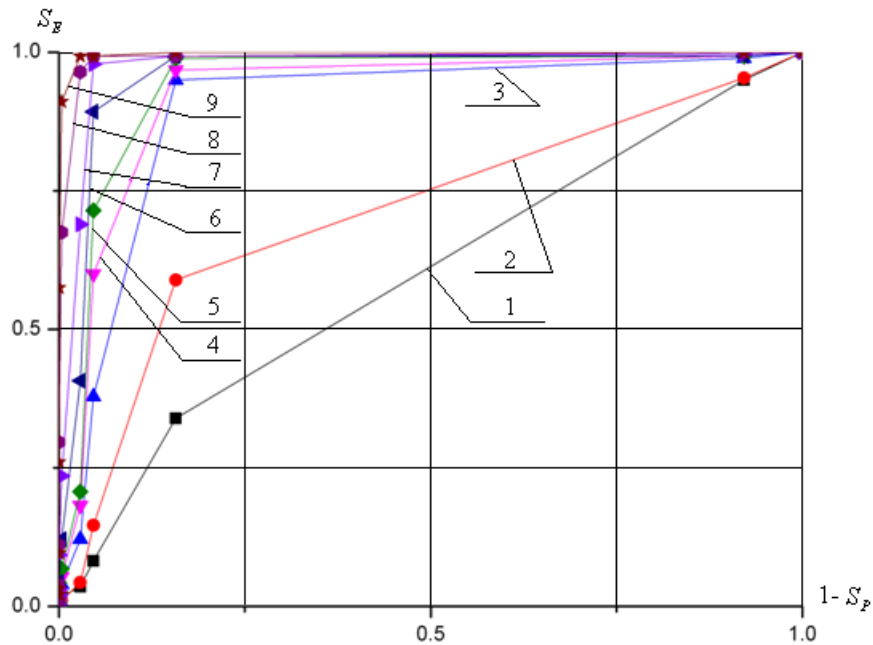


Рис. 1. ROC-кривые, характеризующие работу метода *SAVV* при детектировании результатов *LSB-matching* для различных значений СПС: 1 – 0.05; 2 – 0.1; 3 – 0.2; 4 – 0.25; 5 – 0.3; 6 – 0.4; 7 – 0.5; 8 – 0.75; 9 – 1 бит/пиксель

Таблица 2.

Значения интегрального параметра для оценки эффективности *SAVV* при детектировании результатов *LSB-matching*

СПС, бит/пиксель	A	ρ
0.05	0.594	0.188
0.1	0.710	0.420
0.2	0.89936	0.79872
0.25	0.92442	0.84884
0.3	0.942	0.884
0.4	0.960	0.920
0.5	0.9748	0.9496
0.75	0.98975	0.9795
1	0.99735	0.9947

Необходимо отметить, что часто при использовании ROC-анализа при определении точки отсечения в качестве критерия оптимальности используется требование баланса между чувствительностью и специфичностью, т.е. требование $S_E \approx S_P$ [14]. В этом случае порог есть точка пересечения двух кривых, когда по оси X откладываются значения анализируемого параметра, а по оси Y – S_E и S_P . Проведение такой операции для результатов тестирования метода *SAVV* при СПС 0.05 бит/пиксель представлено на рис. 2. Как видно, определенное выше значение $K = 4$ для *SAVV* является не только оптимальным в смысле чувствительности, но и близко к оптимальному в смысле баланса между чувствительностью и специфичностью.

Важной составляющей ROC-анализа является то, что изменение значения точки отсечения позволяет управлять чувствительностью тестируемого метода в зависимости от требований, выдвигаемых к решению задачи в данный конкретный момент, за счет изменения соотношения между ошибками первого и второго рода.

Таблица 3.

Определение точки отсечения с использованием индекса Йодена

	<i>J</i>									
СПС <i>ih1</i>	5	10	20	25	30	40	50	75	100	
1	0	0	0	0	0	0	0	0	0	
2	0.028571	0.032143	0.067857	0.071429	0.071429	0.071429	0.075	0.078571	0.078571	
3	0.028571	0.032143	0.067857	0.071429	0.071429	0.071429	0.075	0.078571	0.078571	
4	0.182143	0.432143	0.792857	0.810714	0.832143	0.835714	0.835714	0.835714	0.842857	
5	0.035714	0.1	0.332143	0.553571	0.667857	0.846429	0.932143	0.946429	0.946429	
6	0.007143	0.014286	0.092857	0.153571	0.178571	0.378571	0.660714	0.935714	0.964286	
7	0.014286	0.007143	0.035714	0.05	0.064286	0.117857	0.232143	0.671429	0.907143	
8	0	0	0.017857	0.021429	0.042857	0.042857	0.092857	0.296429	0.575	
9	0	0	0.010714	0.003571	0.007143	0.014286	0.032143	0.110714	0.260714	
10	0	0	0	0.003571	0	0.007143	0.021429	0.039286	0.096429	
11	0	0	0	0	0	0	0.017857	0.010714	0.032143	
12	0	0	0	0	0	0	0.003571	0.003571	0.021429	

Для сравнительной оценки работы *SAVV* были выбраны современные стеганоаналитические аналоги, детектирующие LSB-метод: методы Керра, Лю и т.д. [7-10].

Результаты сравнения представлены на рис. 3, в таблице 4.

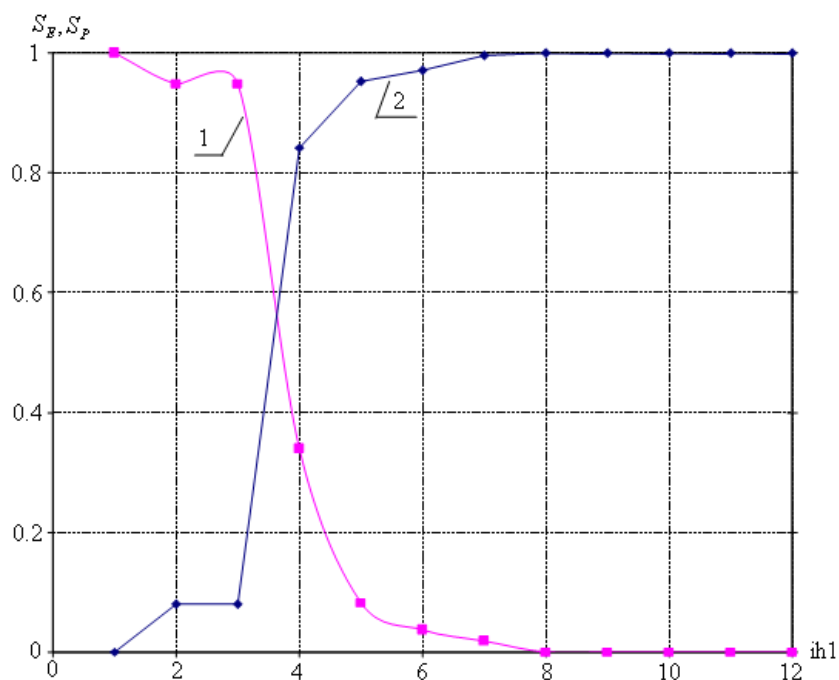


Рис. 2. Построение точки отсечения при требовании баланса между чувствительностью и специфичностью: 1 – кривая чувствительности, 2 – кривая специфичности

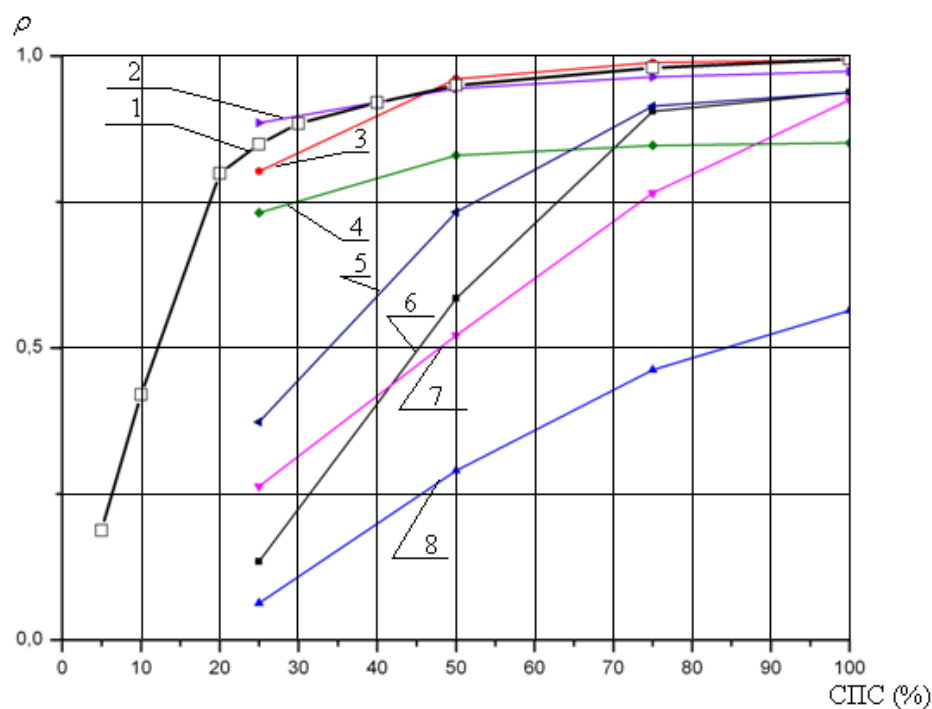


Рис. 3. Результаты сравнения эффективности работы *SAVV* с существующими аналогами: 1 – *SAVV*; 2 – Joint feature set; 3 – Liu's; 4 – RLH COM; 5 – Fused feature; 6 – Ker's; 7 – NDH COM; 8 – HGE

Результаты вычислительного эксперимента показывают, что разработанный САМ *SAVV* имеет высокую эффективность детектирования, в частности, даже при СПС меньше 0.25 бит/пиксель, которая вообще не рассматривается аналогами. Так $\rho=0.79872$ для *SAVV* при СПС 0.2 бит/пиксель, что выше, чем ρ для всех сравниваемых САМ при СПС 0.25 бит/пиксель, за исключением единственного САМ: Joint feature set (эффективность которого для СПС меньшей 0.25 бит/пиксель также неизвестна, однако отсутствие таких данных в результатах эксперимента косвенно указывает на то, что соответствующая эффективность является малой, и по этой причине авторы ее не приводят), кроме того, при СПС 0.5, 0.75, 1 бит/пиксель эффективность Joint feature set уступает *SAVV*. При СПС 0.5, 0.75 бит/пиксель *SAVV* несколько уступает САМ Liu's, но для малой СПС САМ Liu's значительно хуже *SAVV*: его эффективность для СПС 0.25 меньше, чем для разработанного метода при СПС 0.2 бит/пиксель.

Таким образом, исходя из результатов вычислительного эксперимента, можно утверждать, что разработанный САМ *SAVV* является эффективнее своих аналогов, что особенно явно проявляется при малой СПС.

Для полученной выше точки отсечения $K=4$ результаты работы *SAVV* с явным указанием ошибок I и II рода представлены в табл. 5.

Таблица 4.

Значение интегрального параметра ρ для различных САМ детектирования результатов *LSB-matching* при различной СПС

CAM СПС, (%)	Ker's	Liu's	HGE	NDH COM	RLH COM	Fused feature	Joint feature set	<i>SAVV</i>
5	-	-	-	-	-	-	-	0.188
10	-	-	-	-	-	-	-	0.42
20	-	-	-	-	-	-	-	0.79872
25	0.1346	0.7922	0.063	0.2628	0.7316	0.3732	0.8855	0.84884
30	-	-	-	-	-	-	-	0.884
40	-	-	-	-	-	-	-	0.92
50	0.5846	0.9608	0.2898	0.5212	0.8298	0.7324	0.9441	0.9496
75	0.9052	0.9885	0.4622	0.765	0.8468	0.9138	0.9637	0.9795
100	0.9376	0.9931	0.5642	0.9244	0.851	0.9376	0.9732	0.9947

Таблица 5.

Результаты детектирования *LSB-matching* стеганоаналитическим методом *SAVV*

СПС (бит/пиксель)	0.05	0.1	0.2	0.25	0.3	0.4	0.5	0.75	1
Ошибки 1-го рода (%)	33.12	27.87	5	3.21	1.07	0.71	0.71	0.71	0
Ошибки 2-го рода (%)	7.5								

Количество ошибок первого и второго рода (табл. 5), их соотношение объясняется сделанным выше выбором критерия оптимальности для определения точки отсечения: максимизация чувствительности разрабатываемого САМ.

Выводы

В настоящей работе обоснована целесообразность выбора для оценки эффективности разработанного САМ метода анализа ROC-кривых, использование которого позволило получить комплексную оценку *SAVV* с одновременным учетом ошибок первого и второго рода, а также провести формальную проверку правильности установленного ранее эмпирически порогового значения скорости изменения наименьших СНЧ блоков матрицы ЦИ, позволяющего в *SAVV* отделить СС от ОС; установлено, что разработанный САМ *SAVV* является эффективнее своих аналогов по детектированию результатов вложения секретной информации методом модификации наименьшего значащего бита, что особенно явно проявляется при малой СПС.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
3. Gul, G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol.5, No.2. — PP. 349–353.
4. Gul, G. Steganalytic Features for JPEG Compression-Based Perturbed Quantization / G. Gul, A.E. Dirik, I. Avcibas // IEEE Signal Processing Letters. — 2007. — Vol.14, Iss.3. — PP. 205–208.
5. Lyu, S. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines / S. Lyu, H. Farid // Lecture Notes in Computer Science. — New York: Springer-Verlag, 2002. — Vol.2578. — PP. 340–354.
6. Avcibas, I. Image Steganalysis with Binary Similarity Measures / I. Avcibas, M. Kharrazi, *et al.* // EURASIP Journal on Applied Signal Processing. — 2005. — Vol.17. — PP. 2749–2757.
7. Ker, A.D. Steganalysis of LSB matching in grayscale images // IEEE Signal Processing Letters. — 2005. — Vol.12, No.6. — PP. 441–444.
8. Liu, Q.Z. Image complexity and feature mining for steganalysis of least significant bit matching steganography / Q.Z. Liu, A.H. Sung, *et al.* // Information Sciences. — 2008. — Vol.178, No.1. — PP. 21–36.
9. Zhihua Xia. A Learning-Based Steganalytic Method against LSB Matching Steganography / Zhihua Xia, Lincong Yang, *et al.* // Radioengineering. — 2011. — Vol.20, No.1. — PP. 102–109.
10. Natarajan, V. Blind Image Steganalysis Based on Contourlet Transform / V. Natarajan, R. Anitha // International Journal on Cryptography & Information Security. — 2012. — Vol.2, Iss.3. — PP. 77–87.
11. Бобок, И.И. Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукраїнського національного університету ім. В. Даля. — 2011. — №7(161). — С.32–41.
12. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
13. Бобок, И.И. Стеганоанализ как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева // Сучасна спеціальна техніка. — 2011. — №2. — С. 21–34.
14. Файнзильберг, Л.С. Гарантированная оценка эффективности диагностических тестов на основе усиленного ROC-анализа / Л.С. Файнзильберг, Т.Н. Жук // Управляющие системы и машины. — 2009. — №5. — С.3–13.
15. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата звернення: 26.07.2012).
16. Schlisterman, E.F. Optimal cut-point and its corresponding Youden index to discriminate individuals using pooled blood samples / E.F. Schlisterman, N.J. Perkins, *et al.* // Epidemiology. — 2005. — Vol.16, Iss.1. — PP. 73–81.

ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ROC-КРИВИХ ДЛЯ КОМПЛЕКСНОЇ ОЦІНКИ ЕФЕКТИВНОСТІ СТЕГАОАНАЛІТИЧНОГО МЕТОДУ

І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: onu_metal@ukr.net

Представлено результати аналізу ефективності й порівняння роботи нового стеганоаналітичного методу детектування стеганографічних вкладень, здійснених методом модифікації найменшого значущого біта, у цифрове зображення, збережене у форматі із втратами, розробленого автором раніше, з найбільш ефективними існуючими аналогами. Оцінка роботи методів проводиться за допомогою ROC-аналізу. Представлено результати обчислювальних експериментів.

Ключові слова: стеганоаналіз, метод модифікації найменшого значущого біта, ROC-аналіз, точка відсікання

APPLICATION OF ROC-ANALYSIS FOR INTEGRATED ASSESSMENT OF STEGANALYSIS METHOD'S EFFICIENCY

Ivan I. Bobok

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: onu_metal@ukr.net

Results of the analysis of the new LSB-steganalysis method for digital images stored in a lossy format and comparison its efficiency with the best existing analogues. Evaluation of analyzed method is done by ROC-analysis. The results of computational experiments are presented.

Keywords: steganalysis, Least Significant Bit, ROC-analysis, cut-off value

THE SOLUTION OF THE BOUNDARY VALUE PROBLEMS FOR LAPLACE EQUATION IN THE WEDGE-LAYERED MEDIUM WITH THE APPLICATION IN THE HEAT CONDUCTION AND ELASTICITY

Aleksey P. Moyseenok

Odessa I.I. Mechnikov National University,
2 Dvoryanskaya str., Odessa, 65082 Ukraine; e-mail: yogan@ua.fm

With the help of the Mellin integral transformation the problem is reduced to one-dimensional, the explicit solution is found on the recursive scheme for an arbitrary number of layers. The inverse Mellin transform allows to obtain the solution of the problem. The proposed method of solution is illustrated for the case of two-layer wedge.

Keywords: wedge-layered medium, integral Mellin transformation, Laplace equation

Introduction

The relevance of the proposed problem is due to the fact that existing mathematical and technical models developed for classical homogeneous materials not fully cover the mechanical and physical properties of the advanced materials inhomogeneous structure. The development of composite, laminated and functionally gradient materials required the creation of the new mathematical models to determine the integrity of the object without the costly experiments. The construction of such models we can find in [2-4]. The novelty of the proposed work is to construct an exact solution for an elastic wedge-shaped two-layer medium in terms of the antiplane strain.

The formulation of the problem

There is two-layer wedge medium

$$0 < r < \infty, \quad \omega_0 < \varphi < \omega_2 \quad (1)$$

$\mu_j, G_j, j=1,2$ – the Poisson's ratio and shear modulus of each of the elastic wedges. In each of the layers the displacements $W_j(r, \varphi)$, $j=1,2$ satisfy the equilibrium equation

$$r(rW_j'(r, \varphi))' + W_j''(r, \varphi) = 0, \quad (2)$$

$$0 < r < \infty,$$

$$\omega_0 < \varphi < \omega_2.$$

hereinafter bar displays the derivative in the first variable, and the point - in the second, (j - layer number). The boundary conditions are written as follows:

$$\tau_{\varphi z}^{(1)}(r, \omega_0) = G_1 \frac{W_1'(r, \omega_0)}{r} = q(r), \quad (3)$$

$$\tau_{\varphi z}^{(1)}(r, \omega_2) = G_2 \frac{W_2'(r, \omega_0)}{r} = \tilde{q}(r).$$

Stresses $\tau_{\varphi z}^{(j)}(r, \varphi), j=1,2$ and displacements $W_j(r, \varphi), j=1,2$ also satisfy the junction conditions at the intersection of media:

$$\begin{aligned} W_1(r, \omega_1) &= W_2(r, \omega_1), \\ \tau_{\varphi z}^{(1)}(r, \omega_1) &= \tau_{\varphi z}^{(2)}(r, \omega_1). \end{aligned} \quad (4)$$

It is required to find the solution of the boundary problem (2) — (4) in the area (1).

The reduction of the initial boundary value problem to one-dimensional

Reformulate the original problem in terms of displacements. Then the boundary condition (3), (4) will be written in the form:

$$\begin{aligned} r(W_j'(r, \varphi))' + W_j''(r, \varphi) &= 0, \\ 0 < r < \infty, \quad \omega_0 < \varphi < \omega_2, \quad j &= 1, 2; \\ G_1 W_1'(r, \omega_0) &= r q(r); \\ G_2 W_2'(r, \omega_0) &= r \tilde{q}(r); \\ W_1(r, \omega_1) &= W_2(r, \omega_1); \\ G_1 W_1'(r, \omega_1) &= G_2 W_2'(r, \omega_1). \end{aligned} \quad (5)$$

We apply the Mellin integral transformation to the equations and boundary conditions for the reduction of the initial boundary value problem (5) to one-dimensional.

$$W_{js}(\varphi) = \int_0^\infty r^{s-1} W_j(r, \varphi) dr, \quad j = 1, 2, \quad (6)$$

with the inversion formula

$$W_j(r, \varphi) = \frac{1}{2\pi i} \int_{\gamma-i\infty}^{\gamma+i\infty} W_{js}(\varphi) r^{-s} ds. \quad (7)$$

In the space of transforms the boundary problem (5) becomes:

$$\begin{aligned} W_{js}''(\varphi) + s^2 W_{js}(\varphi) &= 0, \\ \omega_0 < \varphi < \omega_2, \quad j &= 1, 2; \end{aligned} \quad (8)$$

$$G_1 W_1'(\omega_0) = q_s ;$$

$$G_2 W_2'(\omega_2) = \tilde{q}_s ;$$

$$G_1 W_{1s}'(\omega_1) = G_2 W_{2s}'(\omega_1) .$$

where

$$q_s = \int_0^\infty r^{s-1} q(r) dr ;$$

$$\tilde{q}_s = \int_0^\infty r^{s-1} \tilde{q}(r) dr .$$

The construction of the solution of one-dimensional boundary value problem

The general solution of the differential equation in (8) has the form

$$W_{js}(\varphi) = C_j^0(s) \sin(s\varphi) + C_j^1(s) \cos(s\varphi), \quad j = 1, 2. \quad (9)$$

Substitute (9) into the junction and boundary conditions

$$\begin{aligned} C_1^0(s) \sin(s\omega_1) + C_1^1 \cos(s\omega_1) &= C_2^0(s) \sin(s\omega_1) + C_2^1 \sin(s\omega_1) \\ sG_1 C_1^0(s) \cos(s\omega_1) - sG_1 C_1^1 \sin(s\omega_1) &= sG_2 C_2^0(s) \cos(s\omega_1) + sG_2 C_2^1 \cos(s\omega_1) \\ sG_1 C_1^0(s) \cos(s\omega_0) + sG_1 C_1^1 \sin(s\omega_0) &= q(s) \\ sG_2 C_2^0(s) \cos(s\omega_2) + sG_2 C_2^1 \cos(s\omega_2) &= \tilde{q}(s) \end{aligned} \quad (10)$$

System (10) of four linear algebraic equations contains four unknown constants C_j^0 , C_j^1 , $j = 1, 2$, which are calculated explicitly. We obtain the representation of integral Mellin transforms of displacements by allowing the system (10):

$$\begin{aligned} W_{1s}(\varphi) &= \left\{ \frac{q_s}{G_1 \Delta} \left(\cos\left(\frac{\pi}{2}s\right) h_1(s) - \sin\left(\frac{\pi}{2}s\right) h_3(s) \right) - \frac{\tilde{q}_s}{G_2 \Delta} \left(\cos\left(\frac{\pi}{2}s\right) h_2(s) + \sin\left(\frac{\pi}{2}s\right) h_1(s) \right) \right\} \sin(s\varphi) + \\ &+ \left\{ \frac{q_s}{G_1 \Delta} s \sin\left(\frac{\pi}{6}s\right) + \frac{\tilde{q}_s}{G_2 \Delta} s \cos\left(\frac{\pi}{6}s\right) \right\} \cos(s\varphi) \\ h_1 &= \sin\left(\frac{\pi s}{4}\right) \cos\left(\frac{\pi s}{4}\right) - \sin\left(\frac{\pi s}{4}\right) \cos\left(\frac{\pi s}{4}\right) \frac{G_1}{G_2} \\ h_2 &= \sin^2\left(\frac{\pi s}{4}\right) + \cos^2\left(\frac{\pi s}{4}\right) \frac{G_1}{G_2} \\ h_3 &= \cos^2\left(\frac{\pi s}{4}\right) + \sin^2\left(\frac{\pi s}{4}\right) \frac{G_1}{G_2} \\ \Delta &= s^2 \cos(\omega_0 s) (\sin(\omega_1 s) \cos(\omega_1 s) - \frac{G_2 - G_1}{G_2} (\cos(\omega_2 s) - \sin(\omega_2 s))) + \end{aligned} \quad (11)$$

$$+ \frac{G_1 - G_2}{G_2} \sin^2(\omega_0 s) (-\sin(\omega_0 s) \cos(\omega_2 s) - \sin(\omega_2 s)) + \frac{G_1}{G_2} \sin(\omega_0 s) \cos(\omega_2 s)$$

The transformant $W_{2s}(\varphi)$ has a similar structure. Thus, in the space of Mellin transforms, we obtain the exact solution of 1D boundary problem (8). In order to obtain the solution of the original boundary problem we apply the inverse Mellin integral transformation (7) to the displacement (11), taking into account that the given shifting loading defines as follows

$$q(r), \tilde{q}(r) = \begin{cases} r, r \in [a, b] \\ 0, r \notin [a, b] \end{cases}$$

Thus displacement $W_1(r, \varphi)$, for example, takes the next form:

$$W_1(r, \varphi) = \frac{1}{2\pi i} \int_{\gamma-i\infty}^{\gamma+i\infty} \int_a^b (H_1(s) \sin(s\varphi) + H_2(s) \cos(s\varphi)) d\rho \left(\frac{r}{\rho}\right)^{-s} ds \quad (12)$$

$$H_1(s) = \frac{s}{G_1 \Delta} (\cos(\omega_2 s) h_1(s) - \sin(\omega_2 s) h_3(s)) - \frac{s}{G_2 \Delta} (\cos(\omega_2 s) h_2(s) + \sin(\omega_2 s) h_1(s))$$

$$H_2(s) = \frac{s \sin(\omega_1 s)}{G_1 \Delta} + \frac{s \cos(\omega_1 s)}{G_2 \Delta} \quad (13)$$

The calculation of the original displacement reduced to evaluating integrals of the form:

$$\frac{1}{2\pi i} \int_{\gamma-i\infty}^{\gamma+i\infty} \int_a^b \left(\frac{r}{\rho}\right)^{-s} H_1(s) \sin(s\varphi) ds d\rho$$

$$\frac{1}{2\pi i} \int_{\gamma-i\infty}^{\gamma+i\infty} \int_a^b \left(\frac{r}{\rho}\right)^{-s} H_2(s) \cos(s\varphi) ds d\rho \quad (14)$$

We calculate these integrals using the residue theorem, for that we find the zeros of the denominator of the under-integral functions and close the contour of the integration so that the Jordan's lemma executes.

Finding the zeros of the denominator $\Delta(s)$

We find the roots of the equation $\Delta(s) = 0$, for which we write it in the form

$$\Delta(s) = s^2 \cos(\omega_0 s) F(s),$$

where

$$F(s) = (\sin(\omega_1 s) \cos(\omega_1 s) \frac{G_2 - G_1}{G_2} (\cos(\omega_2 s) - \sin(\omega_2 s)) +$$

$$+ \frac{G_1 - G_2}{G_2} (\sin(\omega_0 s))^2 (-\sin(\omega_0 s) \cos(\omega_2 s) - \sin(\omega_2 s)) + \frac{G_1}{G_2} \sin(\omega_0 s) \cos(\omega_2 s)) \quad (15)$$

Equation (14) leads to the first root $s = 0$, and a series of roots $s_k = \frac{\pi}{2\omega_0} + \frac{\pi k}{\omega_0}$. The roots of the equation $F(s) = 0$ we will find in the form $\omega_i = \frac{\pi d_i}{e_i}$, $[d_i, e_i] = 1$, $d_i, e_i \in \mathbb{N}$, $i = \overline{0, 2}$, in this case we take $d_i = 1$, then $s = \frac{\pi}{e_i} + tk$, where $t = [e_0, e_1, e_2]$ is least common multiple, then, in our case $12 = [2, 4, 6]$, where t is the period. The final expression for the roots of $\Delta(s)$ we can write as follows: $s = s_i + 12k$, $k \in \mathbb{N}$.

The approximate values s_i of the roots of $\Delta(s)$ were calculated numerically with the help of the package Maple. The calculation of the integrals of the form (14) with the implementation of Jordan's lemma reduced to the next formula:

$$\frac{1}{2\pi i} \int_{\gamma-i\infty}^{\gamma+i\infty} \left(\int_a^b \left(\frac{r}{\rho} \right)^{-s} H_1(s) \sin(s\varphi) \right) d\rho ds = \begin{cases} \sum_{k=1}^{\infty} \operatorname{Res} \left(\frac{r}{\rho} \right)^{-s} H_1(s) \sin(s\varphi) = Q_1^k(r, \rho), r > \rho \\ \sum_{k=0}^{\infty} \operatorname{Res} \left(\frac{r}{\rho} \right)^{-s} H_1(s) \sin(s\varphi) = Q_2^k(r, \rho), r < \rho \end{cases}. \quad (16)$$

A similar formula is used to calculate the second integral in (14). There is the final formula to determine the displacement inside the wedge:

$$W_1(r, \varphi) = \sum_{k=1}^{\infty} \int_a^r Q_1^k(r, \rho) d\rho - \sum_{k=0}^{\infty} \int_r^b Q_2^k(r, \rho) d\rho. \quad (17)$$

Numerical results

It is interesting to consider the values of stresses $\tau_{\varphi z}(r, \varphi)$ and $\tau_{rz}(r, \varphi)$ arising on the orthogonal platforms with the different angles at the points of the applying the shifting loading. The results of the numerical studies are presented for the initial data: $\omega_0 = \frac{\pi}{6}$, $\omega_1 = \frac{\pi}{4}$, $\omega_2 = \frac{\pi}{2}$, $G_1 = 1$, $G_2 = 10$, $a = 5$, $b = 10$. Fig. 1(a) and Fig. 1(b) show plots of the stresses along the line of action of shift loading. Fig. 1(a) shows the values for the stresses $\tau_{\varphi z}(r, \varphi)$. From this figure, we see that in the interval of the loading the stress has the maximum close to the middle. The second figure shows the values of $\tau_{rz}(r, \varphi)$. We can see that the values of $\tau_{rz}(r, \varphi)$ has a maximum at the beginning of the interval of shifting loading, then the value tends to a constant value. Note, that the value $\tau_{rz}(r, \varphi)$ is greater than the corresponding values of $\tau_{\varphi z}(r, \varphi)$ and with approaching to zero the values for both stresses tend to infinity. Note that when you change the values of the shear modulus, stresses varies in proportion to the change. Fig. 1(c) and Fig. 1(d) show the values of $\tau_{\varphi z}(r, \varphi)$ and $\tau_{rz}(r, \varphi)$ depending on the angle. In both figures we can see that with increasing angle the stresses are increased linearly.

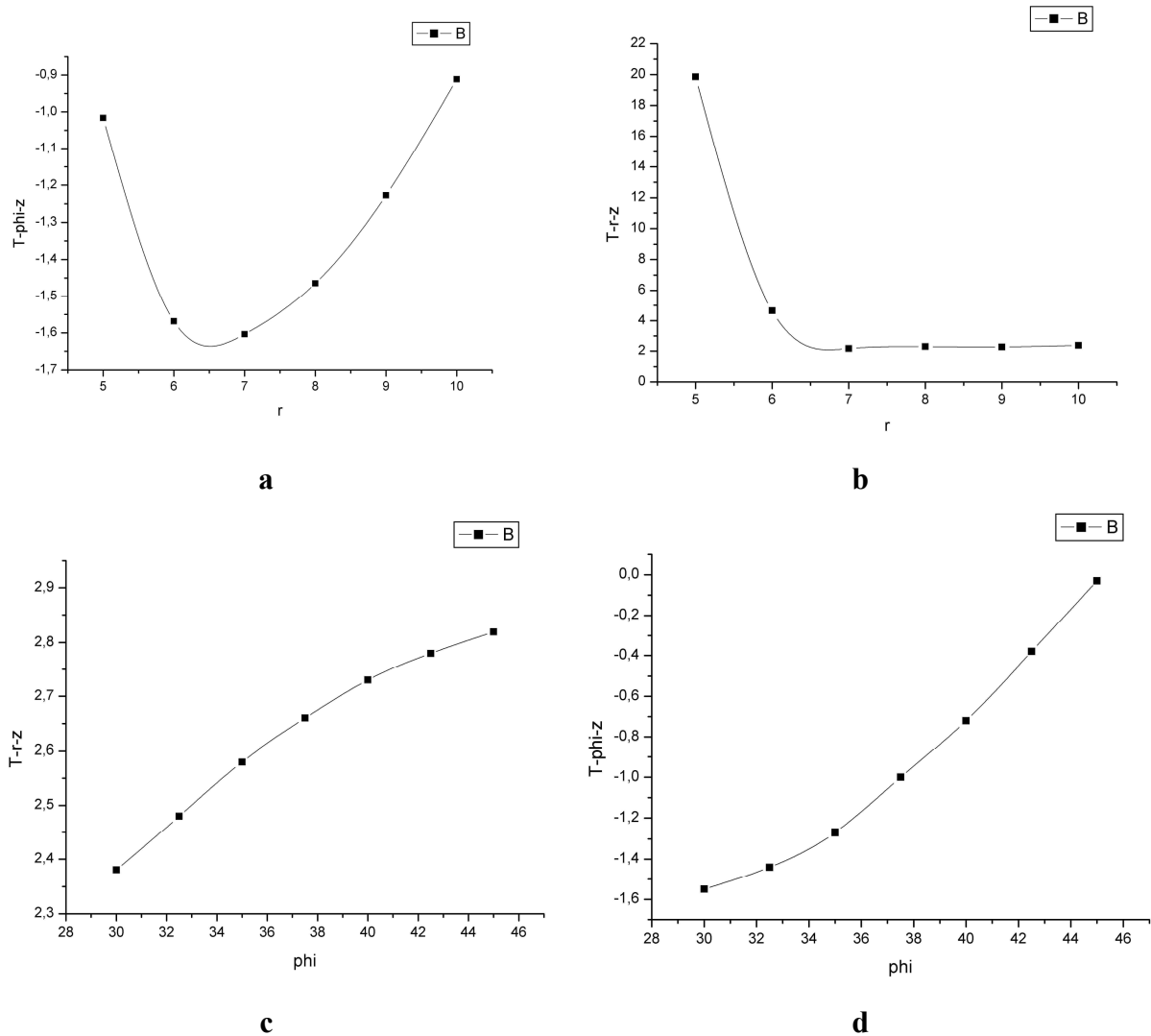


Fig. 1. Plots of the stresses along the line of action of shift loading: a – stresses $\tau_{\phi z}(r, \phi)$, b – $\tau_{rz}(r, \phi)$, c – $\tau_{\phi z}(r, \phi)$, d – $\tau_{rz}(r, \phi)$

Conclusions

- 1) The stated problem is solved exactly using the method proposed in [1].
- 2) The problem for the two-layer wedged medium can be solved in the conditions of plain strain.
- 3) Changes in the relations of the shear modules results in a proportional change in stresses.

References

1. Попов, Г.Я. К решению краевых задач механики и математической физики для слоистых сред / Г.Я. Попов // Известия АН СССР. — 1978. — Т. 31, № 2. — С. 34–47.
2. Акопян, В.С. О продольном сдвиге неоднородно-составного клина / В.С. Акопян // Известия академии наук армянской ССР. — 1994. — Т. 47, № 1-2. — С. 21–27.
3. Прокофьев, А.П. Контактная задача для составного клина / А.П. Прокофьев // Взаимодействие в механике конструкций. — 1980. — С. 52–59.
4. Контактные задачи теории упругости для неоднородных сред [Текст] / С.М. Айзикевич [и др.]. — М. : Физматлит, 2006. — 236 с.

**РІШЕННЯ ДВОВИМІРНОЇ КРАКРАЙОВОЇ ЗАДАЧІ ДЛЯ РІВНЯННЯ ЛАПЛАСА В
КЛИНУВАТО-ШАРУВАТОМУ СЕРЕДОВИЩІ ІЗ ЗАСТОСУВАННЯМ У ТЕПЛОПРОВІДНОСТІ
І ТЕОРІЇ ПРУЖНОСТІ**

О.П. Мойсеєнок

Одеський національний університет імені І.І. Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна; e-mail: yogan@ua.fm

За допомогою інтегрального перетворення Мелліна подана задача зведена до одномірної, явне рішення якої знайдено на основі рекурентної схеми для довільної кількості шарів. Зворотнє перетворення Мелліна дозволило отримати рішення поданої задачі. Запропонований метод рішення задачі проілюстрований для випадку двошарового клину.

Ключові слова: клинувато-шарувате середовище, рекурентні матричні перетворення, теорія пружності

РЕШЕНИЕ ДВУМЕРНОЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ УРАВНЕНИЯ ЛАПЛАСА В КЛИНОВИДНО-СЛОИСТОЙ СРЕДЕ С ПРИМЕНЕНИЕМ В ТЕПЛОПРОВОДНОСТИ И ТЕОРИИ УПРУГОСТИ

А.П. Мойсеенок

Одесский национальный университет имени И.И. Мечникова,
ул. Дворянская, 2, Одесса, 65082, Украина; e-mail: yogan@ua.fm

С помощью интегрального преобразования Меллина исходная задача сведена к одномерной, явное решение которой найдено на основе рекуррентной схемы для произвольного количества слоёв. Обратное преобразование Меллина позволило получить решение исходной задачи. Предложенный метод решения задачи проиллюстрирован для случая двухслойного клина.

Ключевые слова: клиновидно-слоистая среда, рекуррентные матричные преобразования, теория упругости

СТЕГАНОАНАЛИТИЧЕСКИЙ АЛГОРИТМ ДЕТЕКТИРОВАНИЯ МЕТОДА МОДИФИКАЦИИ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА ДЛЯ КОНТЕЙНЕРОВ, ХРАНИМЫХ В ФОРМАТАХ БЕЗ ПОТЕРЬ

В.Н. Рудницкий¹, И.А. Узун²

¹ Черкасский государственный технологический университет,
бул. Шевченко, 460, Черкассы, 18006, Украина; e-mail: rvn_2008@ukr.net

² Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина

Работа посвящена разработке стеганоаналитического алгоритма определения наличия секретного сообщения, погруженного в цифровое изображение, хранимое в формате без потерь. Алгоритм основан на анализе пар цветов с использованием метода модификации наименьшего значащего бита.

Ключевые слова: стеганоанализ, цифровое изображение, метод модификации наименьшего значащего бита

Введение

Повышенный интерес к стеганографии [1, 2] - науке о скрытой передаче информации путём сохранения в тайне самого факта передачи, обусловленный запретом или ограничением на законодательном уровне во многих странах мира использования шифрования после трагических событий 11 сентября 2011 года, привел к появлению огромного количества программных продуктов (Steganos, StegHide, S-tools и др.), многие из которых свободно распространяются в интернете. Используя данные стеганографические средства, можно в любой мультимедиа-объект (цифровое изображение (ЦИ), видео или аудио) внедрить дополнительную, или секретную, информацию (ДИ) таким образом, что это не приведет к каким-либо заметным изменениям этих объектов. Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат погружения – стеганосообщением (СС). ДИ, вносимая в контейнер, может быть предварительно зашифрована, чтобы усложнить задачу стегоаналитика [1]. Основная задача стеганоанализа (СА) [1, 2] – установление факта присутствия в контейнере скрытой информации.

Каждый день во всемирной паутине на сайтах и социальных сетях миллионами публикуются фотографии, которые могут служить каналом передачи скрытой информации. Подобный способ передачи секретной информации не привлекает к себе внимания и может быть легко использован криминальными структурами и террористами [4]. Поэтому развитие методов стеганоанализа на сегодняшний день чрезвычайно актуальная задача.

Одним из широко используемых методов стеганографии для изображений является метод модификации наименьших значащих битов – LSB (*least significant bit*) [1], «долгожевучесть» и популярность которого обусловлена простотой его реализации,

а также возможностью обеспечения при его применении значительной скрытой пропускной способности с одновременным соблюдением надежности восприятия соответствующего СС [1], особенно если в качестве ОС выбрано многоцветное изображение с большим количеством деталей, то есть информационно нагруженное. Если, например, взять ЦИ в формате BMP, на каждую компоненту цвета R , G и B которого отводится 8 бит, и изменить значения наименьших значащих бит (НЗБ) – то подобное искажение будет неуловимо для человеческого восприятия [3] (рис. 1). Это в значительной степени осложняет работу стегоаналитика, если он не обладает специальными средствами СА. В качестве таких средств могут выступать программы, реализующие статистические методы стегоанализа. К таким методам можно отнести алгоритмы, основанные на анализе пар цветов [5-9]. Проводя анализ в данном направлении, было замечено, что эти методы, являясь достаточно эффективными, обладают несогласованностью в определении понятий уникальных цветов ЦИ [6, 7]. Помимо этого, некоторые методы [7, 8] для проведения детектирования наличия ДИ в анализируемом ЦИ требуют выполнение предварительной классификации ЦИ по категориям с целью определения пороговых значений для каждой категории, причем целесообразность предлагаемой авторами классификации является мало убедительной и не выдерживает критики при желании повторить описываемые в работах вычислительные эксперименты. Большинство проанализированных методов применяется лишь в изображениях с количеством уникальных [5, 6] пикселей, не превышающим половину от общего количества пикселей ЦИ.



а



б

Рис. 1. Результат работы метода модификации наименьшего значащего бита: а – изображение-контейнер; б – стеганосообщение

Цель статьи и постановка исследований

Целью работы является повышение эффективности процесса стеганоанализа путем разработки стеганоаналитического алгоритма (САА) детектирования метода LSB, основанного на анализе количества близких пар цветов и уникальных цветов.

Особенностью и ценностью предлагаемого метода является то, что для анализа требуется лишь изображение, которое нужно проверить на факт содержания ДИ. При этом нет необходимости в информации о размере внедренного сообщения. Кроме этого предлагаемое решение не требует предварительной классификации изображений по категориям и последующего определения пороговых значений для каждой категории,

как это требуется в подобных алгоритмах [7, 8]. Данная ситуация является наиболее часто возникающей на практике.

Областью применимости предлагаемого метода являются изображения с количеством уникальных пикселей, превышающим половину общего числа пикселей ЦИ (в качестве таких ЦИ были взяты изображения в формате BMP, не подвергавшиеся операции сжатия), что также отличает его от существующих аналогов. В результате работы алгоритм должен дать ответ, является ли анализируемое ЦИ стеганосообщением, или не содержит никакой внедренной секретной информации.

Для достижения поставленной цели необходимо решить следующие задачи:

- 1) Определить понятие уникального цвета в силу существующих противоречий по поводу данного определения в различных вариациях метода [6, 7];
- 2) Выявить характерные особенности и отличия исходных ЦИ, не подвергавшихся СП, от СС – полученных после внедрения ДИ в ходе СП посредством модификации НЗБ;
- 3) Выявить характерные особенности и отличия изображений, уже подвергавшихся СП посредством модификации НЗБ, от СС, полученных после повторного СП;
- 4) Исходя из результатов решения предыдущих задач, разработать САА для выявления СС, полученных при использовании метода LSB к изображениям в формате BMP.

Основная часть

Введем необходимые обозначения и определения. Под цветом будем понимать в дальнейшем тройку компонент (R, G, B) или пиксель, который также подразумевается как триплет значений (R, G, B) , где R – красная, G – зеленая и B – синяя компонента в цветовой модели RGB [3].

Буквой P обозначим число близких пар цветов в изображении. При этом два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) будем называть близкими [5], если для них справедливо следующее соотношение:

$$\begin{cases} |R_1 - R_2| \leq 1, \\ |G_1 - G_2| \leq 1, \\ |B_1 - B_2| \leq 1 \end{cases} \Leftrightarrow (R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2 \leq 3.$$

Второй статистической величиной, используемой при анализе, является количество уникальных цветов. В отношении уникальных цветов изображения существует несколько подходов. В одном случае [5, 6, 9] под уникальными цветами понимают просто все уникальные пиксели (т.е. различные триплеты значений (R, G, B)) ЦИ. Данная величина обозначается буквой U . Данный подход применяют, когда анализируется ЦИ, в котором количество уникальных пикселей не превышает 50% всех пикселей [5]. Количество всех пар уникальных цветов, представляется как количество сочетаний из U по 2:

$$C_2^U \geq P$$

Будем обозначать R – отношение между числом близких пар цветов и количеством уникальных пар цветов:

$$R = \frac{P}{C_2^U} \quad (1)$$

Согласно второму подходу [7, 8] в определении понятия уникального цвета, два цвета (R_1, G_1, B_1) и (R_2, G_2, B_2) называются уникальными, если выполняется, хотя бы одно из условий: $|R_1 - R_2| \leq 1$, $|G_1 - G_2| \leq 1$, $|B_1 - B_2| \leq 1$. При этом R определяется как отношение количества близких пар цветов к количеству уникальных цветов U :

$$R = \frac{P}{U} \quad (2)$$

Как уже говорилось ранее, в ЦИ в формате BMP каждый цвет состоит из трех компонент, на каждую из которых отведено по 8 бит. Таким образом, в каждом цвете НЗБ содержатся в каждой компоненте триплета значений (R, G, B) . Тогда, можно сказать, что два цвета составляют близкую пару цветов, если они отличаются между собой лишь наименьшими значащими битами. Данное определение было введено исследователями Джонсоном и Яджоди [1], которые указали, что после внедрения ДИ в ЦИ методом LSB полученная цветовая палитра будет иметь отличительную особенность – большое количество пар близких цветов. При этом ими предполагалось, что данный тип артефакта можно наблюдать только в изображениях в градациях серого.

Позже данными особенностями заинтересовались и другие исследователи [6], которыми было замечено, что число уникальных цветов в ЦИ обычно значительно меньше общего числа пикселей ЦИ. Отношение числа уникальных цветов к количеству пикселей составляет примерно от 1:2 для изображений, хранящихся в форматах без потерь (TIF, BMP), до 1:6, или даже ниже, для JPEG изображений. Количество уникальных цветов в JPEG изображениях тем меньше, чем выше параметр сжатия. Данное наблюдение очень важно, поскольку означает, что большинство ЦИ имеет небольшое количество уникальных цветов, относительно общего количества пикселей ЦИ. Таким образом, было показано, что появление большого количества близких пар цветов закономерно и для полноценных цветных изображений.

Отношение R (как для первого (1), так и для второго подхода (2)) дает идею относительно близких пар цветов в ЦИ. Так, после внедрения, число уникальных цветов в ЦИ возрастет до U' , и мы можем посчитать число близких пар цветов P' и отношение R' для полученного СС. Таким образом, идеей является то, что для изображения, которое не содержит секретного сообщения, число близких пар цветов относительно показателя всех возможных пар цветов будет значительно меньше, чем для изображения, которое уже содержит в себе внедренную ДИ. Однако оказывается, что практически невозможно найти порог для отношения R для всех изображений в силу большой вариации уникальных цветов U . Данную проблему помогло решить наблюдение, позволяющее различать изображения, содержащие и не содержащие ДИ. Так, можно заметить, что если изображение уже содержит в себе внедренную информацию, то внедрение другого сообщения в него не изменит отношение R значительно. С другой стороны, если изображение является чистым, то показатель R значительно возрастет после внедрения.

На основании данных наблюдений Д. Фридрих [6] был предложен САА, согласно которому анализируемое изображение подвергается внедрению дополнительной информации. Чтобы ответить на вопрос, являлось ли исходное изображение СС или нет, анализируются показатели R и R' . Если $R \cong R'$ – то делается вывод, что анализируемое изображение содержало дополнительную информацию, в противном

случае если $R' > R$, то считается, что анализируемое изображение было чистым. Подобный вид имеют и алгоритмы, основанные на (2), которые помимо всего еще используют пороговые значения категорий классификации ЦИ.

В настоящей работе рассматриваются изображения в формате BMP, которые не подвергались операции сжатия. Было отобрано 100 изображений размером 300 на 200 пикселей, которые были конвертированы в формат BMP из TIF. Посредством LSB метода было получено еще 100 СС. В качестве дополнительной информации внедрялись Ц. При анализе количества уникальных цветов, было установлено, что у 76% анализируемых чистых изображений уникальными являются более 50% пикселей. А данный факт свидетельствует о том, что приведенные выше алгоритмы не применим к анализируемым изображениям, поскольку количество уникальных пикселей слишком велико.

Согласно вычислениям, полученным при анализе чистых ЦИ, было замечено, что если ЦИ не подвергалось сжатию и количество уникальных цветов в изображении превышает 50% (или близко к 50%) от общего количества пикселей, то это ЦИ уже содержит значительное число близких пар цветов. И при внедрении дополнительной информации LSB методом, данный показатель будет стремительно уменьшаться (от P к P_1). При этом уменьшается и количество уникальных цветов, однако с гораздо меньшей скоростью (от U к U_1).

Если рассмотреть аналогичные значения для изображений, в которые была предварительно внедрена дополнительная информация, то здесь нет такой однозначной тенденции в изменении количества близких пар цветов или уникальных цветов. Изменения коэффициентов P и U происходят как в сторону увеличения, так и уменьшения.

Как уже было сказано ранее, в предлагаемом методе было решено для получения новых статистических данных проводить над анализируемым ЦИ стеганопреобразования, т.е. сначала необходимо получить исходные данные количеств уникальных цветов и близких пар цветов (P и U) в исходном изображении, а потом эти же показатели (P_1 и U_1) должны считываться в СС, получаемых посредством внедрения в НЗБ исходного изображения бит случайного ЦИ. Над каждым изображением из базы (100 чистых и 100 стеганосообщений) производилось по 15 внедрений.

Данные особенности будет удобно рассматривать на графиках (рис. 2).

Анализ подобных графиков для всех тестируемых изображений обратил внимание на различия в разбросе коэффициентов R_1 в чистых изображениях и стеганосообщениях (рис. 2): практически во всех анализируемых изображениях разброс значений R_1 в СС превышает аналогичный показатель, полученный для ЦИ, не содержащих изначально внедренной ДИ. Поэтому в качестве порогового было взято значение разности между максимальным значением коэффициента R_1 и R :

$$\max(R_1) - R$$

Для контейнеров

$$\max(R_1) - R < 0,$$

а для стеганосообщений –

$$\max(R_1) - R \geq 0.$$

На основании проделанных исследований предлагается САА, основными шагами которого являются:

1) Вычисление количеств близких пар цветов (P) и уникальных цветов (U) в анализируемом изображении, а также коэффициента R , равного их отношению.

2) Внедрение случайного изображения в анализируемое ЦИ с использованием LSB-преобразования с последующим подсчетом коэффициентов P_1 , U_1 и R_1 для полученного СС. Данная процедура повторяется 15 раз с различными случайными изображениями.

3) Определение максимального значения в массиве из 15 значений R_1 , полученных на 2 шаге.

4) Результат.

Если

$$\max(R_1) - R < 0,$$

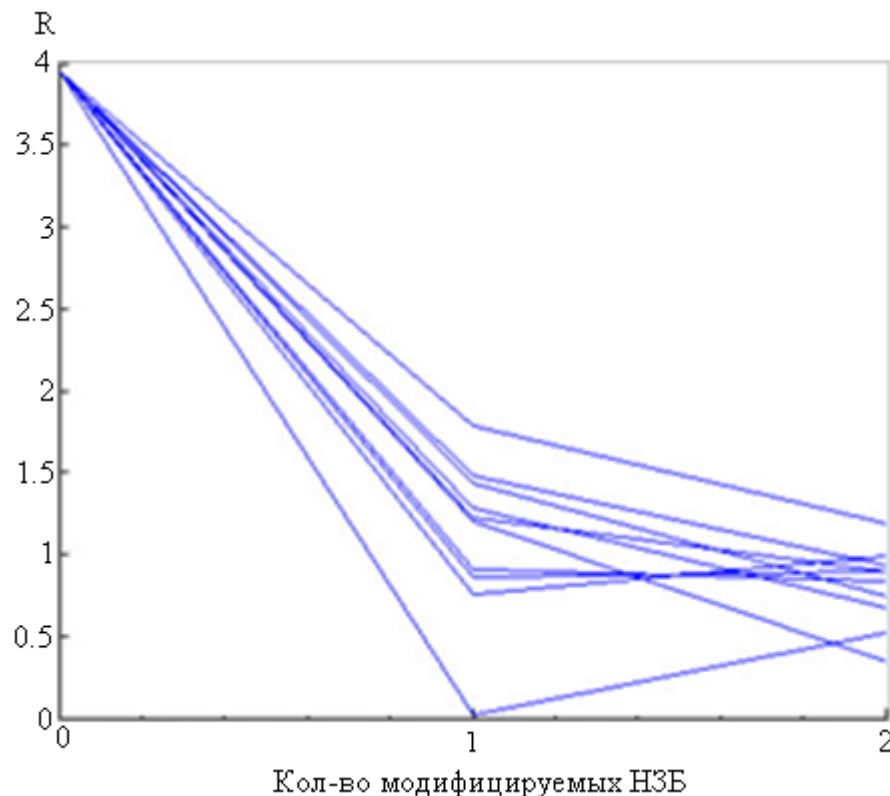
то

анализируемое ЦИ не подвергалось стегопреобразованию,

иначе

анализируемое изображение являлось стегосообщением.

Предлагаемый алгоритм был опробован на 200 ОС и 200 стеганосообщениях в формате BMP размером 300 на 200 пикселей. При этом ошибка второго рода, когда ЦИ изображение было ошибочно принято за стеганосообщение, составила 1%, а ошибка первого рода составила 5%.



а

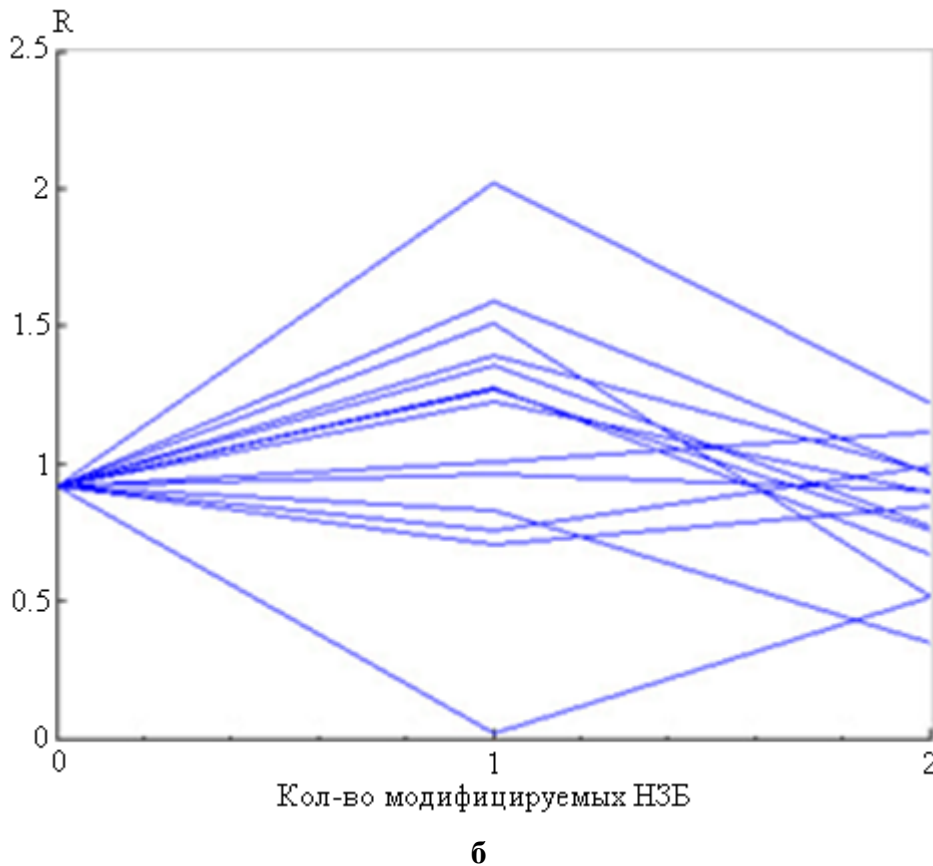


Рис. 2. Графики поведения коэффициентов R при стеганопреобразованиях: над ЦИ, не содержащими ДИ (а); над СС (б)

Выводы

Разработанный алгоритм дал возможность эффективного использования статистических значений близких пар цветов и уникальных цветов в ЦИ с количеством уникальных пикселей, превышающим 50% всех пикселей изображения, что никогда не делалось ранее.

В данный момент исследования авторов направлены на изучение эффективности алгоритма при анализе СС с уменьшением количества погруженной в них информации, поскольку в настоящий момент рассматривалась скрытая пропускная способность в LSB 1 бит/пиксель, а также совершенствование порогового значения.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
2. Конахович, Г.Ф. Компьютерная стеганография [Текст] : теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 283 с.
3. Гонсалес, Р.С. Цифровая обработка изображений [Текст] : научное издание / Р.С. Гонсалес, Р. Вудс ; Пер. с англ. П.А. Чочиа. — М. : Техносфера, 2005. — 1070 с.
4. Бобок, И.И. Стеганоанализ, как частный случай анализа информационной системы / И.И. Бобок, А.А. Кобозева. — Сучасна спеціальна техніка. — 2011. — №1. — С. 25–36.
5. Johnson, N.F. Steganography: Seeing the Unseen / N.F. Johnson, S. Jajodia // IEEE Computer. — 1998. — Vol.31, Iss.2. — PP. 26–34.

6. Friedrich, J. Steganalysis of LSB Encoding in Color Image / J. Friedrich, R. Du, M. Long // IEEE International Conference on Multimedia and Expo. — 2000. — Vol.3. — PP. 1279–1282.
7. Geetha, S. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / S. Geetha, S. Sindhu, and N. Kamaraj // Transactions on Data Privacy. — 2008. — Vol.1, Iss.3. — PP. 140–161.
8. Mitra, S. Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis / S. Mitra, T. Roy, D. Mazumdar and A.B. Saha // IIT Kanpur Hackers' Workshop 2004 (IITKHACK04), 23–24 Feb 2004. — 2004. — PP. 23–24.
9. Seymer, P. Performance Optimization of Close-Color Pair Steganalysis / P. Seymer, G. Dimitoglou // Proceedings of the 2007 International Conference on Security & Management, Las Vegas, USA. — 2007. — PP. 123–127.

СТЕГАНОАНАЛІТИЧНИЙ АЛГОРИТМ ДЕТЕКТУВАННЯ МЕТОДУ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА ДЛЯ КОНТЕЙНЕРІВ, ЗБЕРЕЖЕНИХ У ФОРМАТАХ БЕЗ ВТРАТ

В.М. Рудницький¹, І.О. Узун²

¹ Черкаський державний технологічний університет
бул. Шевченка, 460, Черкаси, 18006, Україна; e-mail: rvn_2008@ukr.net

² Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна

Робота присвячена розробці стеганоаналітичного алгоритму визначення наявності секретного повідомлення, вбудованого в цифрове зображення, яке зберігається в форматі без втрат. Алгоритм заснований на аналізі пар кольорів з використанням методу модифікації найменшого значущого біту.

Ключові слова: стеганоаналіз, цифрове зображення, метод модифікації найменшого значущого біта

METHOD OF LSB STEGANALYSIS FOR LOSSLESS COVER-IMAGES

Vladimir N. Rudnitsky¹, Ija A. Uzun²

¹ Cherkassy State Technological University
460 Shevchenko str., Cherkassy, 18006, Ukraine; e-mail: rvn_2008@ukr.net

² Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine

This paper is devoted to steganalysis algorithm determining presence a secret message embedded into digital image which is stored in uncompressed form. The algorithm is based on the analysis of pairs of colors and uses the method of modifying the least significant bit.

Keywords: steganalysis, digital images, Least Significant Bit

ОТРИМАННЯ ЗАЛЕЖНОСТЕЙ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ МОЖЛИВОСТІ ВИКОНАННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ НА ЇХ ОСНОВІ

Ю.Є. Яремчук

Вінницький національний технічний університет,
вул. Хмельницьке шосе 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

В роботі розглянуто рекурентну послідовність V_k , яка складається з двох послідовностей V_k^+ і V_k^- . Встановлено залежності для V_k^- – послідовності, які забезпечують можливість прискореного обчислення елементів послідовності та безпосереднього обчислення елемента через початкові елементи. Отримані залежності надають можливість виконання криптографічних перетворень на їх основі.

Ключові слова: рекурентні послідовності, аналітичні залежності, захист інформації, криптографія, криптографічні перетворення

Вступ

Рекурентні послідовності отримали широке застосування при побудові різного роду систем [1], для розв'язання різних технічних задач, зокрема в радіотехніці, електрозв'язку [2], криптографії [3]. Математичний апарат рекурентних послідовностей дозволяє за певних умов спрощувати обчислення. В зв'язку з цим цікавим є отримання залежностей рекурентних послідовностей для можливості виконання криптографічних перетворень на їх основі.

Рекурентні послідовності в загальному вигляді можна представити у вигляді [4]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \dots + a_k \cdot u_{n-k},$$

де

$a_1, a_2, \dots, a_k$ – коефіцієнти,

k – порядок послідовності, виходячи з початкових елементів $u_0, u_1, \dots, u_k$.

Далі пропонуються послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Така особливість послідовностей створює передумови для побудови криптографічних перетворень. Для здійснення цієї можливості актуальним залишається отримання відповідних аналітичних залежностей.

Рекурентні послідовності, в яких початкові елементи зав'язані на коефіцієнти

Назвемо V_k^+ – послідовністю послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \quad (1)$$

при початкових значеннях $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \dots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні числа.

Для $k = 2$ послідовність буде мати такий вигляд:

$$\begin{array}{ccccccc}
 \dots & v_{5,2} & v_{4,2} & v_{3,2} & v_{2,2} & v_{1,2} & v_{0,2} \\
 \dots & g_2^5 + 4g_1g_2^3 + 3g_1^2g_2 & g_2^4 + 3g_1g_2^2 + g_1^2 & g_2^3 + 2g_1g_2 & g_2^2 + g_1 & g_2 & 1
 \end{array}$$

Для $k > 2$ послідовність буде мати такий вигляд:

$$\begin{array}{ccccccc}
 & v_{k,k} & v_{k-1,k} & v_{k-2,k} & v_{k-3,k} & \dots & v_{1,k} & v_{0,k} \\
 & g_k^2 & g_k & 1 & 0 & \dots & 0 & 0 \\
 \dots & v_{2k-1,k} & v_{2k-2,k} & v_{2k-3,k} & \dots & v_{k+1,k} \\
 \dots & g_k^{k+1} + 2g_1g_k & g_k^k + g_1 & g_k^{k-1} & \dots & g_k^3
 \end{array}$$

Формула (1) дозволяє отримувати значення для зростаючих n , починаючи з $n = 0$, але певну цікавість становить зворотна процедура, яка складається з того, що елементи обчислюються для спадних n , починаючи з деякого значення $n = l$. Обчислення елементів такої послідовності буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \quad (2)$$

Обчислення за формулою (2) може продовжуватись і для $n < 0$, тобто існує два види послідовностей. Перший вид послідовностей формується для n – додатних за формулою (1). Другий вид послідовностей формується для n – від’ємних за формулою (2).

Назвемо V_k^- – послідовністю послідовність чисел, що обчислюються за формулою (2) для n – від’ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \dots = v_{-k,k} = 0$ для $k > 2$.

Для $k = 2$ послідовність буде мати такий вигляд:

$$\begin{array}{ccccccc}
 v_{-1,2} & v_{-2,2} & v_{-3,2} & v_{-4,2} & v_{-5,2} & v_{-6,2} & \dots \\
 0 & g_1^{-1} & -g_2g_1^{-2} & (g_2^2 + g_1)g_1^{-3} & -(g_2^3 + 2g_1g_2)g_1^{-4} & (g_2^4 + 3g_1g_2^2 + g_1^2)g_1^{-5} & \dots
 \end{array}$$

Для $k > 2$:

$v_{-1,k}$	$v_{-2,k}$	$v_{-3,k}$	$\dots$	$v_{-k,k}$	
0	g_1^{-1}	0	$\dots$	0	
$v_{-((k-1)+2),k}$	$v_{-(k+2),k}$	$v_{-(k+3),k}$	$\dots$	$v_{-2k+1,k}$	
$-g_k g_1^{-2}$	g_1^{-2}	0	$\dots$	0	
$v_{-(2(k-1)+2),k}$	$v_{-2k-1,k}$	$v_{-2k-2,k}$	$v_{-2k-3,k}$	$\dots$	$v_{-3k,k}$
$g_k g_1^{-3}$	$-2g_k g_1^{-3}$	g_1^{-3}	0	$\dots$	0
$\dots$					
$v_{-((k-2)(k-1)+2),k}$	$v_{-((k-2)(k-1)+3),k}$	$\dots$	$v_{-((k-2)(k-1)+k),k}$	$\dots$	
$(-1)^{k-2} g_k^{k-2} g_1^{-(k-1)}$	$(-1)^{k-1} (k-2) g_k^{k-3} g_1^{-(k-1)}$	$\dots$	$g_1^{-(k-1)}$	$\dots$	

Послідовність чисел, яка складається з V_k^+ -послідовності та V_k^- -послідовності назовемо V_k -послідовністю.

Виконання криптографічних перетворень нерозривно пов'язано з необхідністю дослідження криптографічної стійкості протоколів, що базуються на цих перетвореннях. В зв'язку цим, для рекурентної послідовності важливим є отримання залежності безпосереднього обчислення елемента через початкові елементи.

Для будь-яких цілого додатного k та цілого від'ємного n , таких що $k > 2$ та $n \leq -((k-1)(k-2)+2)$ отримано таку аналітичну залежність

$$v_{n,k} = g_1^{-(s+1)} \sum_{i=0}^{\left\lfloor \frac{|n|-2-t(k-1)}{k \cdot (k-1)} \right\rfloor} (-1)^{s-t-ki} C_{s-i}^{t+(k-1)i} g_k^{s-t-ki} g_1^i \quad (3)$$

де

$$s = \left\lfloor \frac{|n|-2}{k-1} \right\rfloor,$$

$$t = (|n|-2) \bmod (k-1).$$

Проведемо аналіз індукцією по n .

Покажемо, що (3) виконується для n , які дорівнюють $-((k-1)(k-2)+2)$, $-((k-1)(k-2)+3)$, $\dots$, $-((k-1)(k-2)+k)$, $-((k-1)(k-2)+k+1)$.

Для $n = -((k-1)(k-2)+2)$

$$s = \left\lfloor \frac{(k-1)(k-2)+2-2}{k-1} \right\rfloor = \lfloor k-2 \rfloor = k-2,$$

$$t = ((k-1)(k-2) + 2 - 2) \bmod (k-1) = 0,$$

$$v_{-((k-1)(k-2)+2),k} = g_1^{-(k-1)} \sum_{i=0}^0 (-1)^{k-2-ki} C_{k-2-i}^{(k-1)i} g_k^{k-2-ki} g_1^i = (-1)^k g_k^{k-2} g_1^{-(k-1)}.$$

Для $n = -((k-1)(k-2) + 3)$

$$s = \left\lfloor \frac{(k-1)(k-2) + 3 - 2}{k-1} \right\rfloor = \left\lfloor k-2 + \frac{1}{k-1} \right\rfloor = k-2,$$

$$t = ((k-1)(k-2) + 3 - 2) \bmod (k-1).$$

враховуючи властивість додавання порівнянь,

$$t = [(((k-1)(k-2) \bmod (k-1)) + (1 \bmod (k-1))) \bmod (k-1) = [0 + 1] \bmod (k-1) = 1;$$

$$v_{-((k-1)(k-2)+3),k} = g_1^{-(k-1)} \sum_{i=0}^0 (-1)^{k-3-ki} C_{k-2-i}^{1+(k-1)i} g_k^{k-3-ki} g_1^i = (-1)^{k-1} (k-2) g_k^{k-3} g_1^{-(k-1)}.$$

Продовжуючи далі таким же чином, отримаємо для $n = -((k-1)(k-2) + k)$

$$s = \left\lfloor \frac{(k-1)(k-2) + k - 2}{k-1} \right\rfloor = \left\lfloor k-2 + \frac{k-2}{k-1} \right\rfloor = k-2,$$

$$t = ((k-1)(k-2) + k - 2) \bmod (k-1),$$

враховуючи властивість додавання порівнянь,

$$t = [(((k-1)(k-2) \bmod (k-1)) + ((k-2) \bmod (k-1))) \bmod (k-1) = [0 + k-2] \bmod (k-1) = k-2;$$

$$v_{-((k-1)(k-2)+k),k} = g_1^{-(k-1)} \sum_{i=0}^0 (-1)^{k-2-k+2-ki} C_{k-2-i}^{k-2+(k-1)i} g_k^{k-2-k+2-ki} g_1^i = g_1^{-(k-1)}.$$

Для $n = -((k-1)(k-2) + k + 1)$

$$s = \left\lfloor \frac{(k-1)(k-2) + k + 1 - 2}{k-1} \right\rfloor = \left\lfloor \frac{(k-1)(k-1)}{k-1} \right\rfloor = k-1,$$

$$t = ((k-1)(k-2) + k + 1 - 2) \bmod (k-1) = (k-1)^2 \bmod (k-1) = 0,$$

$$v_{-((k-1)(k-2)+k+1),k} = g_1^{-k} \sum_{i=0}^0 (-1)^{k-1-ki} C_{k-1-i}^{(k-1)i} g_k^{k-1-ki} g_1^i = (-1)^{k-1} g_k^{k-1} g_1^{-k}.$$

Основа індукції, таким чином, доведена.

Нехай залежність (3) виконується для $n+k$, $n+k-1$. Покажемо, що вона виконується для n .

$$\begin{aligned}
 v_{n,k} &= \frac{v_{n+k,k} - g_k v_{n+k-1,k}}{g_1} = g_1^{-1} v_{(|n|-k),k} - g^k g_1^{-1} v_{(|n|-k+1),k} = \\
 &= g_1^{-(s_1+2)} \sum_{i=0}^{\left\lfloor \frac{|n|-k-2-t_1(k-1)}{k(k-1)} \right\rfloor} (-1)^{s_1-t_1-ki} C_{s_1-i}^{t_1+(k-1)i} g_k^{s_1-t_1-ki} \cdot g_1^i - \\
 &- g_k \cdot g_1^{-(s_2+2)} \sum_{i=0}^{\left\lfloor \frac{|n|-k-1-t_2(k-1)}{k(k-1)} \right\rfloor} (-1)^{s_2-t_2-ki} C_{s_2-i}^{t_2+(k-1)i} g_k^{s_2-t_2-ki} g_1^i,
 \end{aligned}$$

де

$$\begin{aligned}
 s_1 &= \left\lfloor \frac{|n|-k-2}{k-1} \right\rfloor, \\
 t_1 &= (|n|-k-2) \bmod (k-1), \\
 s_2 &= \left\lfloor \frac{|n|-k-1}{k-1} \right\rfloor, \\
 t_2 &= (|n|-k-1) \bmod (k-1).
 \end{aligned}$$

Виразимо t_1 і t_2 через t , та s_1 і s_2 через s .

Знайдемо $t-t_1$, $t-t_2$.

$$t - t_1 = ((|n|-2) \bmod (k-1)) - ((|n|-k-2) \bmod (k-1)).$$

Враховуючи властивість різниці порівнянь

$$t - t_1 = (|n|-2 - |n| + k + 2) \bmod (k-1) = k \bmod (k-1) = 1.$$

Аналогічно

$$\begin{aligned}
 t - t_2 &= ((|n|-2) \bmod (k-1)) - ((|n|-k-1) \bmod (k-1)) = \\
 &= (|n|-2 - |n| + k + 1) \bmod (k-1) = (k-1) \bmod (k-1) = 0.
 \end{aligned}$$

Тоді $t_1 = t-1$, $t_2 = t$.

$$\begin{aligned}
 s_1 &= \left\lfloor \frac{|n|-k-2}{k-1} \right\rfloor = \left\lfloor \frac{|n|-2}{k-1} - \frac{k}{k-1} \right\rfloor = s-1, \\
 s_2 &= \left\lfloor \frac{|n|-k-1}{k-1} \right\rfloor = \left\lfloor \frac{|n|-2}{k-1} - \frac{k-1}{k-1} \right\rfloor = \left\lfloor \frac{|n|-2}{k-1} - 1 \right\rfloor = s-1.
 \end{aligned}$$

Тобто $s_1 = s_2 = s-1$.

Враховуючи отримані результати запишемо

$$\begin{aligned}
v_{n,k} &= g_1^{-(s+1)} \sum_{i=0}^{\left\lfloor \frac{|n|-3-t(k-1)}{k(k-1)} \right\rfloor} (-1)^{s-t-ki} C_{s-1-i}^{t-1+(k-1)i} g_k^{s-t-ki} g_1^i + \\
&+ g_1^{-(s+1)} \sum_{i=0}^{\left\lfloor \frac{|n|-k-1-t(k-1)}{k(k-1)} \right\rfloor} (-1)^{s-t-ki} C_{s-1-i}^{t+(k-1)i} g_k^{s-t-ki} g_1^i = \\
&= g_1^{-(s+1)} \left((-1)^{s-t} C_{s-1}^{t-1} g_k^{s-t} g_1^0 + (-1)^{s-t-k} C_{s-2}^{t-1+(k-1)} g_k^{s-t-k} g_1^1 + \right. \\
&+ (-1)^{s-t-2k} C_{s-3}^{t-1+2(k-1)} g_k^{s-t-2k} g_1^2 + (-1)^{s-t-3k} C_{s-4}^{t-1+3(k-1)} g_k^{s-t-3k} g_1^3 + \dots + \\
&+ (-1)^{s-t} C_{s-1}^t g_k^{s-t} g_1^0 + (-1)^{s-t-k} C_{s-2}^{t+(k-1)} g_k^{s-t-k} g_1^1 + \\
&\left. + (-1)^{s-t-2k} C_{s-3}^{t+2(k-1)} g_k^{s-t-2k} g_1^2 + (-1)^{s-t-3k} C_{s-4}^{t+3(k-1)} g_k^{s-t-3k} g_1^3 + \dots \right).
\end{aligned}$$

Відомо [5], що

$$C_n^r + C_n^{r+1} = C_{n+1}^{r+1} \quad (4)$$

і для будь-яких n та m

$$C_n^0 = C_m^0.$$

Замінюючи доданки попарно з урахуванням (4) отримаємо

$$v_{n,k} = g_1^{-(s+1)} \sum_{i=0}^{\left\lfloor \frac{|n|-2-t(k-1)}{k(k-1)} \right\rfloor} (-1)^{s-t-ki} C_{s-i}^{t+(k-1)i} g_k^{s-t-ki} g_1^i.$$

В основу криптографічних перетворень можна покласти обчислення елементу рекурентної послідовності з великим значенням його індексу. Тоді виникає необхідність отримання залежності, яка могла б забезпечувати можливість прискореного обчислення елементів послідовності за рекурентною формулою (2) для будь-якого k .

Для будь-яких цілих додатних n і m , таких що $1 \leq m < n$ та будь-якого цілого додатного k отримано таку залежність

$$v_{n-m,k} = v_{-m+(k-2),k} v_{n,k} + g_1 \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} v_{n-k+i,k}. \quad (5)$$

Проведемо аналіз індукцією по m .

Покажемо, що (5) виконується для m , які дорівнюють $1, 2, 3, \dots, k$.

$$v_{n-1,k} = v_{k-3,k} v_{n,k} + g_1 v_{k-4,k} v_{n-k+1,k} + \dots + g_1 v_{-1,k} v_{n-2,k} + g_1 v_{-2,k} v_{n-1,k}.$$

Враховуючи значення початкових елементів, отримаємо

$$v_{n-1,k} = g_1 g_1^{-1} v_{n-1,k} = v_{n-1,k}.$$

Знайдемо тепер $v_{n-2,k}$.

$$\begin{aligned}
 v_{n-2,k} &= v_{k-4,k} v_{n,k} + g_1 v_{k-5,k} v_{n-k+1,k} + \dots + \\
 &+ g_1 v_{-1,k} v_{n-3,k} + g_1 v_{-2,k} v_{n-2,k} + g_1 v_{-3,k} v_{n-1,k} = g_1 v_{-2,k} v_{n-2,k} = v_{n-2,k} \\
 &\dots \\
 v_{n-k,k} &= v_{-2,k} v_{n,k} + g_1 v_{-3,k} v_{n-k+1,k} + \dots + g_1 v_{-k,k} v_{n-2,k} + g_1 v_{-k-1,k} v_{n-1,k} = \\
 &= v_{-2,k} v_{n,k} + g_1 v_{-k-1,k} v_{n-1,k} = g_1^{-1} v_{n,k} + g_1 (-g_k g_1^{-2}) v_{n-1,k} = \frac{v_{n,k} - g_k v_{n-1,k}}{g_1} = v_{n-k,k}
 \end{aligned}$$

Нехай залежність (5) виконується для $m+1$, $m+2$, $\dots$, $m+k$. Покажемо, що вона виконується для m .

$$\begin{aligned}
 v_{n-m,k} &= g_k v_{n-m-1,k} + g_1 v_{n-m-k,k} = g_k v_{-m-1+(k-2),k} v_{n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{-m-1+(k-2)-i,k} v_{n-k+i,k} + \\
 &+ g_1 v_{-m-k+(k-2),k} v_{n,k} + g_1^2 \sum_{i=1}^{k-1} v_{-m-k+(k-2)-i,k} v_{n-k+i,k} = \\
 &= g_k v_{-m-1+(k-2),k} v_{n,k} + g_1 g_k v_{-m-1+(k-2)-1,k} v_{n-k+1,k} + \\
 &+ g_1 g_k v_{-m-1+(k-2)-2,k} v_{n-k+2,k} + \dots + g_1 g_k v_{-m-1+(k-2)-(k-1),k} v_{n-1,k} + \\
 &+ g_1 v_{-m-k+(k-2),k} v_{n,k} + g_1^2 v_{-m-k+(k-2)-1,k} v_{n-k+1,k} + g_1^2 v_{-m-k+(k-2)-1,k} v_{n-k+1,k} + \dots + g_1^2 v_{-m-k-1,k} v_{n-1,k} = \\
 &= (g_k v_{-m-1+(k-2),k} + g_1 v_{-m-k+(k-2),k}) v_{n,k} + g_1 (g_k v_{-m-1+(k-2)-1,k} + g_1 v_{-m-k+(k-2)-1,k}) v_{n-k+1,k} + \\
 &+ g_1 (g_k v_{-m-1+(k-2)-2,k} + g_1 v_{-m-k+(k-2)-2,k}) v_{n-k+2,k} + \dots + \\
 &+ g_1 (g_k v_{-m-1+(k-2)-(k-1),k} + g_1 v_{-m-k+(k-2)-(k-1),k}) v_{n-1,k} = \\
 &= v_{-m+(k-2),k} v_{n,k} + g_1 v_{-m+(k-2)-1,k} v_{n-k+1,k} + g_1 v_{-m+(k-2)-2,k} v_{n-k+2,k} + \dots + \\
 &+ g_1 v_{-m+(k-2)-(k-1),k} v_{n-1,k} = v_{-m+(k-2),k} v_{n,k} + g_1 \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} v_{n-k+i,k}
 \end{aligned}$$

Висновки

Розглянуто рекурентну V_k – послідовність, яка складається з двох послідовностей V_k^+ і V_k^- . Отримано залежності для V_k^- – послідовності, які надають можливість виконання криптографічних перетворень на їх основі.

Залежність (5) забезпечує можливість прискореного обчислення елементів для спадних n для будь-якого k . Це може бути використано в криптографічних

перетвореннях для швидкого обчислення елементу V_k – послідовності для спадних n , коли воно представляється як велике значення індексу.

Залежність (3) дає можливість безпосереднього обчислення елементу через початкові елементи. Це створює певні зручності для досліджень рекурентної послідовності щодо криптографічної стійкості протоколів, що можуть бути побудовані на основі цієї послідовності.

Список літератури

1. Сороко, Э.М. Золотые сечения, процессы самоорганизации и эволюции систем [Текст] : введение в общую теорию гармонии систем / Э.М. Сороко. — М. : URSS, 2006. — 264 с.
2. Ясинский, С.А. Прикладная «золотая» математика и ее приложения в электросвязи [Текст] / С.А. Ясинский. — М. : Горячая линия – Телеком, 2004. — 240 с.
3. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — 5th ed. — N.Y.: CRC Press, 1996. — 816 p.
4. Маркушевич, А.И. Возвратные последовательности [Текст] : монография / А.И. Маркушевич. — 3-е изд. — М. : Наука, 1983. — 47 с.
5. Кнут, Д.Э. Искусство программирования для ЭВМ [Текст] : в 7 т.: пер. с англ. / Д.Э. Кнут. — М. : Мир, 1976. — Т.2 : Получисленные алгоритмы. — 724 с.

ПОЛУЧЕНИЕ ЗАВИСИМОСТЕЙ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ВОЗМОЖНОСТИ ВЫПОЛНЕНИЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ИХ ОСНОВЕ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

В работе рассмотрено рекуррентную последовательность V_k , которая состоит из двух последовательностей V_k^+ и V_k^- . Установлены зависимости для V_k^- – последовательности, которые обеспечивают возможность ускоренного вычисления элементов последовательности и непосредственного вычисления элементов через начальные элементы. Полученные зависимости дают возможность выполнения криптографических преобразований на их основе.

Ключевые слова: рекуррентные последовательности, аналитические зависимости, защита информации, криптография, криптографические преобразования

OBTAINING RELATIONS OF RECURRENT SEQUENCES FOR THE POSSIBILITY OF CARRYING OUT CRYPTOGRAPHIC TRANSFORMATIONS ON THEIR BASIS

Yuri E. Yaremchuk

Vinnitsia National Technical University,
95 Khmelnytske shose, Vinnitsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

In this paper we considered a recurrent sequence V_k consisting of two sequences V_k^+ and V_k^- . We established relations for the V_k^- – sequence that allow an accelerated calculation of the sequence elements and a direct computation of the elements through the initial elements. The relations obtained allow a possibility of carrying out cryptographic transformations on their basis.

Keywords: recurrent sequence, analytical relations, information security, cryptography, cryptographic transformations

ТЕОРИЯ ВОЗМУЩЕНИЙ КАК ОСНОВА ОБЩЕГО ПОДХОДА К ОЦЕНКЕ ЧУВСТВИТЕЛЬНОСТИ СТЕГАНОСООБЩЕНИЙ

А.А. Кобозева, Е.В. Нариманова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

Разработан общий математический подход к оценке чувствительности стеганосообщений к возмущающим воздействиям, не зависящий от используемого стеганографического алгоритма, области погружения секретной информации, области анализа стеганосообщения – пространственной или частотной. Основными математическими инструментами являются матричный анализ и теория относительных возмущений. Предлагается способ оценки защищенности секретной информации, внедренной в контейнер, в качестве которого рассматривается цифровое изображение. Разработан способ количественной оценки чувствительности стеганосообщения к возмущающим воздействиям, который используется для решения задачи о выборе контейнера из конечного множества контейнеров для заданного секретного сообщения. Получаемое решение обеспечивает наименьшую чувствительность стеганосообщения к возмущающим воздействиям, т.е. наибольшую эффективность процесса декодирования дополнительной информации, оцениваемую при помощи объема восстановленной информации. Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганосообщение, возмущающее воздействие, чувствительность, матрица, собственное число, собственный вектор

Введение

Жизнедеятельность общества немыслима без накопления, хранения, изменения, передачи информации. Специфика сегодняшнего дня заключается в том, что информация характеризуется не только как ресурс, но и как объект труда. В настоящее время в число защищаемых помимо военных, государственных и ведомственных, включены также секреты промышленные, коммерческие и даже личные. Информация все больше становится товаром, причем одним из самых дорогих. Трудно переоценить важность и актуальность вопросов, связанных с ее защитой [1-3].

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений информационной безопасности сформировали современные методы стеганографии [4-13].

Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов. Особенностью стеганографического подхода является то, что он не предусматривает оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать важные задачи защиты информации ряда прикладных областей, как, например, в [4, 14, 15].

Стеганографирование может осуществляться различными способами, однако общей чертой этих способов является то, что секретное сообщение, или дополнительная информация (ДИ), погружается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается по каналу связи адресату или хранится в таком виде. Процесс погружения ДИ в ОС, или контейнер, будем называть стеганопреобразованием (СП), а результат стеганопреобразования – стеганосообщением (СС).

Постановка задачи и цель исследования

Хотя практические приложения стеганографии в настоящий момент достигли значительного развития, используемые стеганографические методы часто не имеют под собой строгого теоретического обоснования [6, 8-10, 12]. Это затрудняет выделение ограничений для области применимости тех или иных стеганографических алгоритмов (СА), не дает возможности разработки универсальных в некотором смысле стеганографических методов и общих подходов решения актуальных задач стеганографии, в частности, задачи обеспечения одного из основных требований, предъявляемых к любому СА, – требования нечувствительности получаемого СС к возмущающим воздействиям, которое равносильно требованию устойчивости СА к преднамеренным (непреднамеренным) атакам [4, 16, 17]. До настоящего момента активно культивировалась и продолжает культивироваться ошибочная, по мнению авторов, идея о том, что результат СП при помощи СА, работающих в частотной области, менее чувствителен к большинству возмущающих воздействий, чем результат пространственного СП [4-6].

Таким образом, задача создания единого подхода к качественной и количественной оценке чувствительности СС, основы решения которой были заложены авторами настоящей работы в [18], остается актуальной задачей стеганографии.

Целью работы является разработка общего математического подхода к оценке чувствительности СС к возмущающим воздействиям, не зависящего от используемого стеганоалгоритма и области погружения ДИ, который позволит:

- оценивать (сравнивать) устойчивость существующих СА;
- делать выбор контейнера, обеспечивающего для заданного секретного сообщения наименее чувствительное стеганосообщение;
- теоретически обоснованно модифицировать существующие и разрабатывать новые устойчивые к атакам СА, независимо от используемой ими области ОС для СП (пространственной, частотной).

Для достижения поставленной цели в работе решаются следующие *задачи*:

- универсальной (не зависящей от конкретики используемого СА) формализации процесса СП;
- выбора формальных параметров, определяющих СС (ОС), характеризующих его чувствительность к возмущающим воздействиям;
- получения достаточных условий нечувствительности СС к возмущающим воздействиям.

Основными математическими инструментами выступают матричный анализ и теория относительных возмущений. Использование теории возмущений дает принципиальную возможность для определения степени зависимости состояния произвольного ОС (СС) от произвольного возмущающего воздействия; позволяет производить априорную оценку основных свойств СС (ОС); абстрагируясь от конкретики СП, дает возможность анализировать результат этого возмущающего воздействия.

Формализация процесса стеганопреобразования

В качестве контейнера в силу широкого распространения в настоящее время цифровых сигналов часто используются цифровые изображения (ЦИ), аудио (ЦА) и видео (ЦВ). Произвольное ЦИ и ЦВ, рассматриваемое как последовательность видео-кадров, естественным образом представимы в виде матрицы (совокупности матриц). Хотя общеиспользуемой математической формализацией ЦА является вектор, элементарно осуществляется переход к его двумерному матричному представлению [19], что позволяет в качестве математической модели любого из указанных цифровых сигналов использовать матрицу (конечное множество матриц). Таким образом, не ограничивая общности рассуждений, для определенности и простоты изложения везде ниже в роли контейнера выступает цифровое монохромное изображение, $n \times n$ -матрица которого обозначается F ; ДИ – сформированная случайным образом последовательность $p_1, p_2, \dots, p_k$, где $p_i \in \{0,1\}, i = \overline{1,k}$; $\overline{p}_1, \overline{p}_2, \dots, \overline{p}_k$, $\overline{p}_i \in \{0,1\}, i = \overline{1,k}$, – декодированное из СС секретное сообщение. Объем восстановленной при декодировании информации (ОВИ) определяется в соответствии с формулой:

$$\frac{k - \sum_{i=1}^k p_i \oplus \overline{p}_i}{k} \times 100\%,$$

где $\oplus$ – операция логического исключающего ИЛИ.

СС будем называть чувствительным, если чувствительной окажется задача декодирования ДИ, т.е. если незначительные возмущающие воздействия, которым подвергается СС, способны привести к значительному снижению ОВИ, и нечувствительным в противном случае.

Погружение ДИ в ОС, независимо от способа и области (пространственной, частотной) этого погружения, формально представляется как возмущение ΔF матрицы F . Тогда матрица СС $\overline{F}$ удовлетворяет соотношению: $\overline{F} = F + \Delta F$, где $\Delta F = f(F)$, т.е. ΔF является некоторой функцией матрицы контейнера F . Отсюда вытекает, что произвольное СП можно представить в виде аддитивного погружения некоторой информации, формальным представлением которой является матрица ΔF , в пространственной области.

Любые преобразования, которые производятся над СС, формализуются как дополнительные возмущения матрицы ОС F .

Определим набор математических параметров, который полностью характеризует любое ОС (СС). Поскольку формальным представлением ОС (СС) является матрица, то в качестве набора искомых характеристик можно использовать множество сингулярных чисел и ортонормированных лексикографически положительных сингулярных векторов, а также спектр (совокупность собственных значений (СЗ)) и множество ортонормированных лексикографически положительных собственных векторов (СВ) соответствующей матрицы [2]. В случае симметричности матрицы ОС F второй из наборов является предпочтительным в силу следующих замечаний. Во-первых, построение спектрального разложения симметричной матрицы, результатом которого является определение СЗ и СВ, обладает рядом преимуществ в вычислительном смысле по сравнению с построением сингулярного разложения для матрицы произвольной структуры того же размера и уровня заполненности, результатом которого является определение сингулярных чисел и сингулярных векторов [20,21]; во-вторых, СЗ симметричной матрицы (как и сингулярные числа произвольной матрицы) являются хорошо обусловленными [22], т.е.

$$\max_{1 \leq j \leq n} |\lambda_j(F) - \lambda_j(F + \Delta F)| \leq \|\Delta F\|_2 \quad (1)$$

где

$\lambda_j(\cdot)$ – СЗ соответствующей матрицы,

$\|\cdot\|_2$ – спектральная матричная норма [20] (чего нельзя утверждать в общем случае для несимметричных матриц [20]).

Однако, как правило, матрица ОС не удовлетворяет свойству: $F = F^T$. Поставим в соответствие F две симметричные $n \times n$ -матрицы A , B по следующему правилу:

$$F = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \rightarrow A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{12} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{21} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \quad (2)$$

которые будем рассматривать ниже как матрицы ОС (рис. 1).

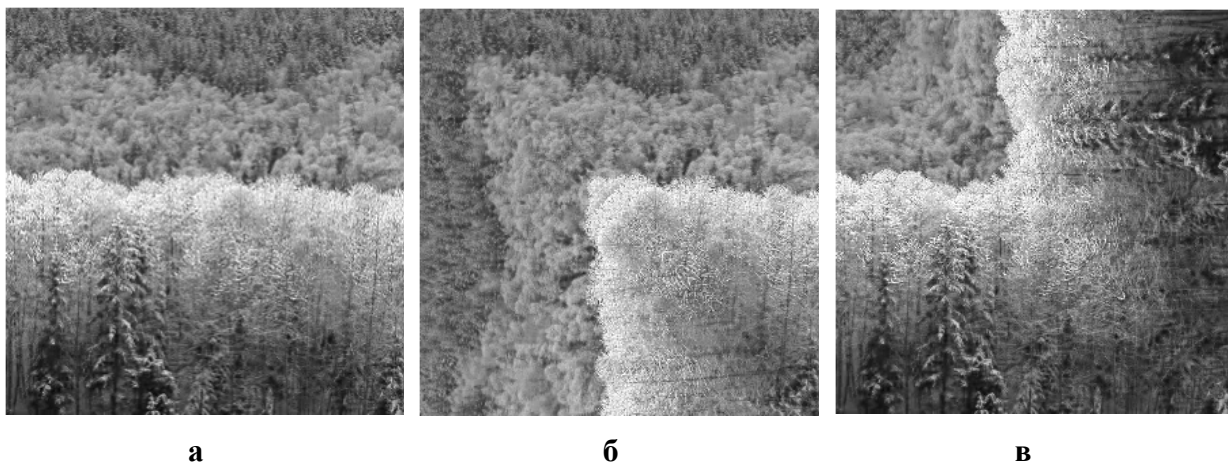


Рис. 1. Исходное цифровое изображение с несимметричной матрицей F (а); соответствующие изображения с симметричными матрицами A (б); B (в)

При встраивании ДИ в исходный контейнер СП представляется в виде погружения в верхний (нижний) треугольник матрицы $A(B)$ с последующим виртуальным симметричным отражением результата относительно главной диагонали $A(B)$. Результат СП обозначим $\bar{A}$ и $\bar{B}$ ($\bar{A} = A^T$, $\bar{B} = B^T$). При окончательном формировании матрицы СС используется верхний треугольник $\bar{A}$ и нижний треугольник матрицы $\bar{B}$. Применение такого подхода, дающего возможность рассматривать матрицы ОС, СС как симметричные и, в силу этого, использовать для их формального описания спектр и соответствующие СВ, было предложено в [23] и используется в настоящей работе.

Пусть E – $n \times n$ -матрица произвольного возмущающего воздействия, которому подвергается ОС (СС). В общем случае $E \neq E^T$. Матрице E поставим в соответствие две симметричных матрицы той же размерности, используя правило (2), рассматривая матрицу, отвечающую верхнему (нижнему) треугольнику E как возмущающую для контейнера (СС), полученного на основе $A(B)$, что дает принципиальную возможность

матрицу произвольного возмущающего воздействия также рассматривать ниже как симметричную.

Пусть A – симметричная $n \times n$ -матрица, элементы которой $a_{ij} \in R$, $i, j = \overline{1, n}$, с $\lambda_i \in R$, $i = \overline{1, n}$, и ортонормированными СВ u_i , $i = \overline{1, n}$, т.е.

$$A = U \Lambda U^T \quad (3)$$

– спектральное разложение (СР) матрицы A [20] (здесь $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$, $U = [u_1, \dots, u_n]$), которое в общем случае определяется неоднозначно. СР (3) назовем нормальным, если элементы матрицы Λ удовлетворяют соотношению: $|\lambda_1| \geq \dots \geq |\lambda_n|$, а СВ u_i , $i = \overline{1, n}$, лексикографически положительны [2]. Если A – невырожденная симметричная $n \times n$ -матрица, модули СЗ которой попарно различны, для нее существует единственное нормальное СР [2].

Далее будем считать, что все матрицы, отвечающие рассматриваемым ОС, симметричны (в силу (2)) и удовлетворяют достаточным условиям, обеспечивающим единственность нормального СР.

Произвольное возмущающее воздействие, в частности, СП матрицы ОС, определенным образом возмутит ее спектр и (или) СВ. В силу этого результат любого СП – завершённое погружение ДИ в контейнер – формально может быть представлен в виде совокупности возмущений спектра и (или) СВ матрицы ОС, однозначно определяемых нормальным СР, которые произошли в ходе СП.

Поскольку согласно (1), все СЗ симметричной матрицы ОС являются нечувствительными к возмущающим воздействиям, независимо от того, чувствительным или нечувствительным окажется полученное СС, целесообразным для оценки чувствительности СС является анализ возмущений СВ матрицы ОС, которые произошли в процессе СП. СС отличается от контейнера содержанием в нем ДИ. Таким образом, совокупность возмущений СВ матрицы контейнера может рассматриваться как формальное представление погруженной ДИ (для $n = 3$ геометрическая интерпретация дана на рис.2, где u_i , $i = \overline{1, 3}$, – СВ матрицы ОС, а u_i , $i = \overline{1, 3}$, – СВ СС).

СП, а также возмущающие воздействия, которым подвергается СС в ходе пересылки и (или) хранения, должны обеспечивать надежность его восприятия [4], т.е. так возмутить матрицу ОС (СС), чтобы зрительно возмущение оказалось незаметным. В силу этого везде ниже рассматриваются малые возмущающие воздействия [2, 4].

Качественная оценка чувствительности стеганосообщения к возмущающим воздействиям

Пусть A – произвольная симметричная матрица контейнера. Назовем абсолютной отделенностью СЗ λ_i матрицы A число, определяемое в соответствии с формулой:

$$gap_{abs}(i, A) = \min_{i \neq j} \|\lambda_j\| - \|\lambda_i\|.$$

Погружение одного и того же секретного сообщения при помощи одного СА в разные контейнеры в общем случае приводит к разным по чувствительности СС. Действительно, спектры матриц различных ОС отличаются друг от друга не только по непосредственным значениям СЗ, но и, что главное, по абсолютным отделенностям СЗ. Поэтому понятие малой (наименее возможной) чувствительности, рассматривается в данном разделе по отношению к конкретному ОС (СС) как качественная характеристика.

Теорема 1. Достаточным условием обеспечения малой (наименьшей из возможных) чувствительности СС к возмущающим воздействиям для используемого контейнера является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы СС, имеющим большие, по сравнению с остальными, (максимальные из всех) абсолютные отделенности.

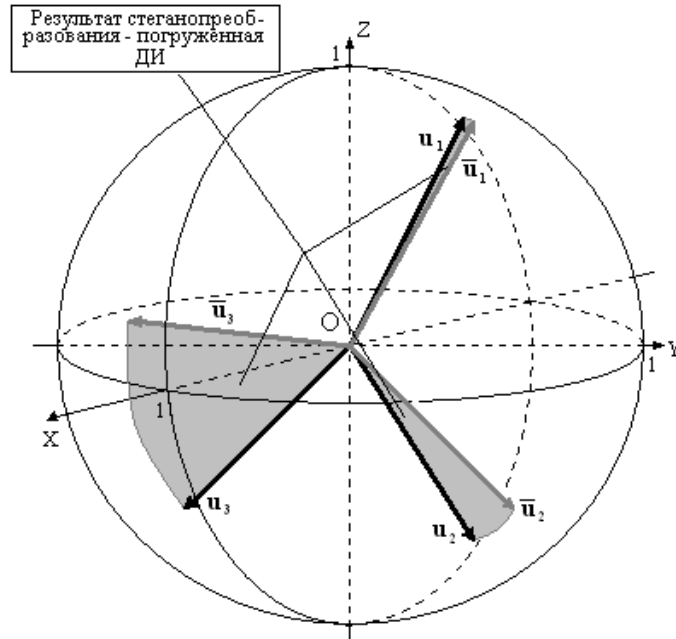


Рис. 2. Формальное представление дополнительной информации, погруженной при стеганопреобразовании

Доказательство. При погружении ДИ в контейнер СВ матрицы A ОС возмущатся, отклонившись от первоначального положения на некоторые углы (рис. 2). Это произойдет всегда, если только алгоритм погружения ДИ не базируется на непосредственной модификации лишь СЗ матрицы ОС, как, например, в [24]. Этот случай требует отдельного обсуждения, которое не проводится в настоящей работе. Поскольку формальным представлением результата СП (погруженной информации) является совокупность возмущений СВ матрицы контейнера, чувствительность полученного СС будет определяться чувствительностью возмущенных при стеганопреобразовании СВ матрицы A . В соответствии с [20] СВ является чувствительным, если малое возмущающее воздействие может привести к значительному возмущению вектора, т.е. значительному углу его поворота от первоначального положения. Очевидно, чтобы сохранить неизменной погруженную ДИ при возмущающем воздействии, направленном на СС, возмущения СВ, возникшие в результате СП, должны остаться неизменными после воздействия.

Пусть $\bar{A}$ – симметричная матрица СС, нормальное СР которой в соответствии с (3) представляется в виде: $\bar{A} = \bar{U} \bar{\Lambda} \bar{U}^T$; E – матрица некоторого возмущающего воздействия, направленного на СС $\bar{A}$, $E = E^T$; $\bar{A} + E = \bar{U} \bar{\Lambda} \bar{U}^T$ – нормальное СР $\bar{A} + E$. Пусть $\bar{u}_i$, $\bar{u}_i$ – нормированные лексикографически положительные СВ $\bar{A}$ и $\bar{A} + E$ соответственно, отвечающие i -му СЗ, а θ_i – угол между ними. Легко показать, опираясь на [20], что:

$$\sin \theta_i \leq \frac{2\|E\|_2}{gap_{abs}(i, \bar{A})}. \quad (4)$$

В соответствии с (4) СВ, возмущенные при СП контейнера, а значит и СС в целом, будут тем менее чувствительными к возмущающим воздействиям, чем большие абсолютные отделенности $gap_{abs}(i, \bar{A})$ имеют соответствующие СЗ матрицы $\bar{A}$, а наименьшая чувствительность СС будет обеспечиваться в том случае, когда возмущению при СП подверглись только те СВ матрицы ОС, которые отвечают СЗ СС с максимальными абсолютными отделенностями.

Таким образом, абсолютная отделенность СЗ является мерой чувствительности соответствующего СВ к возмущающим воздействиям, а абсолютные отделенности СЗ, соответствующих возмущенным при стеганопреобразовании СВ, определяют чувствительность полученного СС. СС будет наименее чувствительным к возмущающим воздействиям, если СП возмутит СВ, соответствующие СЗ матрицы СС, имеющим наибольшие абсолютные отделенности. Более того, как показывает вычислительный эксперимент, наибольшие абсолютные отделенности СЗ, присутствующих в спектре матрицы СС, таковы, если в процессе СП были возмущены только СВ, отвечающие этим СЗ, то они обеспечивают нечувствительность СС в указанном случае: углы поворота соответствующих СВ при возмущающем воздействии, сохраняющем надежность восприятия СС, составляют, как правило, доли секунды.

Следствие 1. Если возмущенные в результате стеганопреобразования ОС СВ соответствуют СЗ матрицы СС с малыми абсолютными отделенностями, то полученное СС оказывается чувствительным к возмущающим воздействиям, что приводит к недостаточной эффективности декодирования ДИ, оцениваемой ОВИ.

Как следует из (1), абсолютные отделенности СЗ матриц $\bar{A}$ и A незначительно отличаются друг от друга, откуда вытекает истинность следствия 2.

Следствие 2. Достаточным условием обеспечения малой (наименьшей из возможных) чувствительности СС к возмущающим воздействиям для используемого контейнера является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы ОС, имеющим большие, по сравнению с остальными, (максимальные из всех) абсолютные отделенности.

Заметим, что на практике для реальных ЦИ наибольшие абсолютные отделенности имеют максимальные по модулю СЗ соответствующих матриц.

Теорема 2. Достаточным условием обеспечения малой чувствительности (нечувствительности) СС к предполагаемому возмущающему воздействию E является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы СС, имеющим абсолютные отделенности, значительно превосходящие $\|E\|_2$.

Доказательство теоремы непосредственно следует из соотношения (4) в случае, когда $gap_{abs}(i, \bar{A}) \gg \|E\|_2$.

Следствие. Достаточным условием обеспечения малой чувствительности (нечувствительности) СС к предполагаемому возмущающему воздействию E является соответствие возмущенных при СП ОС собственных векторов собственным значениям матрицы ОС, имеющим абсолютные отделенности, значительно превосходящие $\|E\|_2$.

Из всего вышесказанного следуют *выводы*:

- чувствительность СС к возмущающим воздействиям определяется характером возмущений СВ матрицы ОС при СП, и не зависит от области погружения ДИ, используемого СА. Исходя из значений возмущений и абсолютных отделенностей соответствующих СЗ возможно сделать качественные априорные оценки чувствительности СС к возмущающим воздействиям;

■ при разработке новых (модификации существующих) устойчивых к возмущающим воздействиям СА, т.е. алгоритмов, формирующих нечувствительные (малочувствительные) СС, необходимо обеспечить следующее требование: СП должно осуществляться так, чтобы при его формальном представлении в виде совокупности возмущений СВ матрицы ОС, возмущенные СВ соответствовали СЗ с большими, по сравнению с другими СЗ, абсолютными отделенностями. Наименьшая чувствительность СС будет достигаться при соответствии возмущенных СВ СЗ с наибольшими абсолютными отделенностями (здесь возможно нарушение надежности восприятия СС [19]). Для обеспечения сформулированного требования не имеет значения используемая СА для погружения ДИ область ОС – пространственная, частотная, что нивелирует так называемое преимущество с точки зрения устойчивости к возмущениям для СА, осуществляющих погружение секретной информации в частотной области.

Замечание. Возмущения СВ, происходящие в результате СП, в частотной и пространственной области изображения одинаковы (независимо от того, в какой области происходит погружение ДИ).

Действительно, если A – симметричная матрица яркости ЦИ, а A_j – соответствующая матрица частотных коэффициентов (например, коэффициентов дискретного косинусного преобразования), то они связаны соотношением [25]:

$$A_j = PAP^T, \quad (5)$$

где P – ортогональная матрица. С учетом (3) формула (5) примет вид:

$$A_j = PAP^T = PU\Lambda U^T P^T = (PU)\Lambda(PU)^T. \quad (6)$$

В силу того, что матрица PU является ортогональной, правая часть (6) дает спектральное разложение A_j , из которого вытекает, что СЗ A_j и A – одинаковые, а СВ $u^{(j)}$ матрицы A_j представляются как

$$u^{(j)} = Pu,$$

где u – соответствующие СВ A . Если $\bar{A}$ и $\bar{A}_j$ – матрицы СС в пространственной и частотной областях соответственно, СВ которых $\bar{u}$ и $\bar{u}^{(j)}$, то

$$(u^{(j)}, \bar{u}^{(j)}) = (Pu, P\bar{u}) = (u, \bar{u}), \quad (7)$$

где (a, b) – скалярное произведение векторов a, b . Из (7) вытекает, что углы между векторами $u, \bar{u}$ и $u^{(j)}, \bar{u}^{(j)}$ одинаковы, что и требовалось показать.

Таким образом, анализ возмущений СВ матрицы ЦИ, происходящих в результате СП, возможно проводить как в пространственной, так и в частотной области изображения в зависимости от специфики конкретной задачи.

Количественная оценка чувствительности стеганосообщения к возмущающим воздействиям

Для получения количественной оценки чувствительности СС вернемся к соотношению (4). Заметим, что если правая часть (4) превзойдет единицу, т.е.

$$\|E\|_2 \geq \frac{gap_{abs}(i, \bar{A})}{2},$$

то оценка возмущения СВ приобретет вид: $\sin \theta_i \leq 1$, превращаясь в тривиальную, и сделать заключение о реальной чувствительности такого вектора не представляется возможным. Кроме того, в этой ситуации в общем случае для θ_i принципиально нельзя найти никакой практической оценки. Для иллюстрации сказанного рассмотрим пример, когда возмущение E таково, что СЗ матрицы $\bar{A} + E$, достаточно отдалившись от СЗ $\bar{A}$ (соотношение (1)), превратились в кратные:

$$\bar{A} = \begin{pmatrix} 1.0005 & 0 \\ 0 & 0.9995 \end{pmatrix}, \text{ а } \bar{A} + E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Поскольку любой ненулевой вектор размерности 2 является СВ для $\bar{A} + E$, то нет никакой принципиальной возможности оценить угол θ_i .

Будем говорить, что СЗ λ_i имеет достаточную (недостаточную) абсолютную отделенность по отношению к возмущению E , если

$$gap_{abs}(i, \bar{A}) > 2\|E\|_2 \quad (gap_{abs}(i, \bar{A}) \leq 2\|E\|_2).$$

СВ, отвечающие СЗ с достаточной (недостаточной) абсолютной отделенностью по отношению к возмущению E , назовем защищенными (незащищенными) от рассматриваемого возмущения. Заметим, что только для защищенных СВ имеется потенциальная возможность численно оценить возмущение при помощи неравенства (4); СВ, отвечающие СЗ с большими (максимальными) абсолютными отделенностями, являются защищенными от любого из рассматриваемых (малых) возмущений. ДИ, результатом погружения которой явилось возмущение защищенных СВ, будем называть дополнительной информацией, защищенной от возмущения E (ЗИ).

Далее будем считать, что при увеличении величины угла отклонения СВ при СП увеличивается и количество ДИ, которая хранится в возмущении этого вектора. СВ «распределяют между собой» погруженную ДИ. Конечно, такое допущение будет не совсем оправданным, если алгоритм погружения связан с определенной непосредственной модификацией СВ, например, с изменением знаков их компонент, как, например, в [23]. Однако это лишь незначительно сужает область рассмотрения и является предметом исследования другой работы одного из авторов.

На основе сделанного выше допущения предположим, что СС тем менее чувствительно, чем большему возмущению при СП подверглись СВ, отвечающие СЗ с максимальными абсолютными отделенностями, чем большая «часть» погруженной ДИ является защищенной от возмущающих воздействий.

В качестве количественной оценки чувствительности СС рассмотрим объем ЗИ, определяемый с учетом возмущений защищенных СВ и абсолютных отделенностей соответствующих СЗ, непосредственное вычисление которого сводится к следующему.

Пусть A и $\bar{A}$ – симметричные $n \times n$ -матрицы контейнера и СС, полученного при помощи некоторого СА, соответственно;

$$A = U \Lambda U^T,$$

$$\bar{A} = \bar{U} \bar{\Lambda} \bar{U}^T$$

– их нормальные СР. Определим вектор $V = (v_1, \dots, v_n)^T$ весовых коэффициентов при учете возмущений СВ матрицы ОС в процессе СП, в соответствии с абсолютными отделенностями СЗ матрицы СС:

$$v_i = \frac{\bar{v}_i}{\|\bar{V}\|}, \quad i = \overline{1, n},$$

где $\bar{V}$ – вектор с элементами $\bar{v}_i = gap_{abs}(i, \bar{A})$, $i = \overline{1, n}$.

Возмущения СВ матрицы контейнера в процессе СП учитываются естественным образом в процессе формирования вектора $P = (p_1, \dots, p_n)^T$:

$$p_i = \frac{\bar{p}_i}{\|\bar{P}\|}, \quad i = \overline{1, n},$$

где

$\bar{P}$ – вектор с элементами $\bar{p}_i = \sin \theta_i$, $i = \overline{1, n}$;

θ_i – угол между СВ u_i , $\bar{u}_i$ матриц A и $\bar{A}$ соответственно.

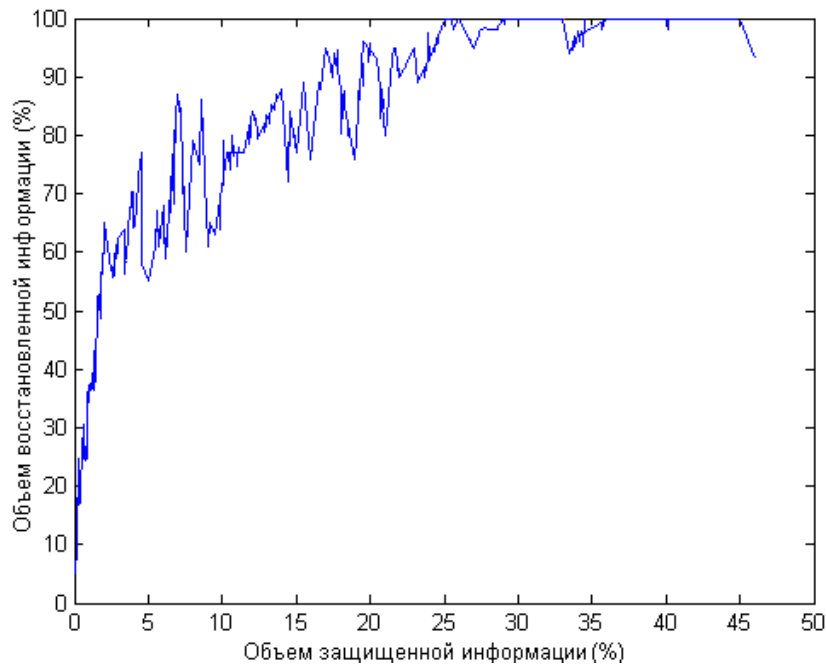
Пусть $\bar{\lambda}_{t_1}, \dots, \bar{\lambda}_{t_p}$ – СЗ $\bar{A}$ с достаточной абсолютной отделенностью по отношению к предполагаемому возмущению E (соответствующие СВ $\bar{u}_{t_1}, \dots, \bar{u}_{t_p}$ – защищенные от E), тогда окончательная формула для объема I ЗИ в СС $\bar{A}$ – количественной оценки чувствительности СС к возмущающему воздействию E – выглядит следующим образом:

$$I = \sum_{j=1}^p p_{t_j} v_{t_j}. \quad (8)$$

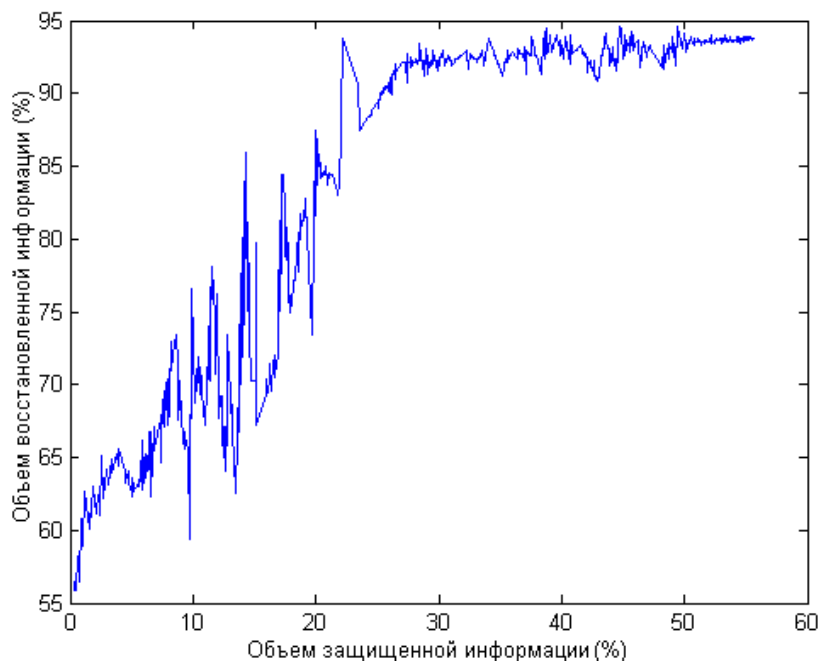
Выдвинем следующую гипотезу: чем больше объем ЗИ в СС, определяемый в соответствии с формулой (8), тем менее это СС будет чувствительным к возмущающим воздействиям, т.е. тем больше будет ОВИ при декодировании ДИ из атакованного (возмущенного) СС. Для проверки этой гипотезы был проведен вычислительный эксперимент.

Результаты вычислительного эксперимента

Вычислительный эксперимент проводился в среде *MathWorks MATLAB* более, чем с 300 монохромными ЦИ одинакового размера (100×100 пикселей), различными по контрастности, текстуре, жанру (пейзажи, портреты, натюрморты и др.), по объему ЗИ. Для СП были взяты два СА, осуществляющих погружение и декодирование ДИ в различных областях: метод квантования изображений (пространственная область) и метод относительной замены величин коэффициентов дискретного косинусного преобразования (частотная область) [5]. Случайным образом генерировалось бинарное секретное сообщение, одинаковое для всех контейнеров, после погружения которого каждое СС подвергалось одному и тому же возмущающему воздействию с матрицей E . Учитывая $\|E\|_2$, в соответствии с формулой (8) вычислялся объем I ЗИ в невозмущенном СС и производилось декодирование ДИ из возмущенных СС с последующим вычислением ОВИ. Результаты проведенных экспериментов, которые в целом подтверждают выдвинутую в предыдущем пункте гипотезу, представлены на рис. 3.



а



б

Рис. 3. Зависимость объема восстановленной при декодировании информации от объема защищенной информации в стеганосообщении: а – метод квантования изображения; б – метод относительной замены величин коэффициентов дискретного косинусного преобразования

Заметим, что имеющиеся различия в ОВИ для СС с близкими значениями объемов ЗИ обязаны существованию в стеганосообщениях СВ, возмущенных в процессе СП, но незащищенных от применяемого возмущающего воздействия. Как было отмечено выше, поведение незащищенных СВ является неконтролируемым. Однако, несмотря на это, из сопоставления всей совокупности полученных результатов, для всех рассмотренных СС, непосредственно вытекает, что наибольшая эффективность

декодирования, независимо от конкретики СА и возмущающего воздействия, отвечает наименее чувствительным стеганосообщениям – стеганосообщениям с наибольшим объемом ЗИ. Такие результаты дают возможность использовать предложенный подход для обоснованного выбора контейнера из данного множества контейнеров, обеспечивающего наибольшую эффективность декодирования ДИ.

Вычислительная сложность количественной оценки чувствительности СС в соответствии с формулой (8) будет определяться вычислительной сложностью процесса получения СР матрицы.

Замечание. Пусть имеется некоторое ОС, которое предварительно подвергается разбиению на блоки фиксированной малой размерности. Предложенный метод оценки чувствительности может быть применен к множеству блоков контейнера, что даст возможность для данного ОС выбрать блоки, которые будут малочувствительными к предполагаемым возмущающим воздействиям, и погружение ДИ производить именно в эти блоки. Заметим, что количество арифметических операций для исследования каждого блока будет определяться некоторой константой, не зависящей от размерности матрицы ОС. Тогда общее количество арифметических операций для обработки всего ОС определится количеством блоков, т.е. как $O(n^2)$, где n – размерность матрицы ОС.

Выводы

На основе теории возмущений и матричного анализа разработан принципиально новый общий математический подход к оценке чувствительности СС к возмущающим воздействиям, в результате которого:

1) Получена универсальная математическая формализация процесса стегано-преобразования в виде совокупности возмущений собственных значений и собственных векторов специального вида матрицы контейнера, рассматриваемой в симметричном виде, позволившая выделить математические параметры, характеризующие чувствительность стеганосообщения;

2) Получены достаточные условия обеспечения нечувствительности (малой чувствительности) стеганосообщения к возмущающим воздействиям, носящие характер качественной оценки чувствительности, не зависящие от используемого при стеганопреобразовании алгоритма и области изображения, используемой для анализа – пространственной, частотной;

3) Разработан способ количественной оценки чувствительности стеганосообщения к возмущающим воздействиям, позволяющий проводить сравнение чувствительностей различных стеганосообщений. Разработанный способ может быть использован для решения одной из широко распространенных задач стеганографии – задачи о выборе контейнера из имеющегося конечного множества контейнеров для заданного секретного сообщения, обеспечивающего наименьшую чувствительность получаемого на его основе стеганосообщения к возмущающим воздействиям, т.е. наибольшую эффективность процесса декодирования дополнительной информации, оцениваемую при помощи объема восстановленной информации.

Список литературы

1. Ленков, С.В. Методы и средства защиты информации : [в 2 томах] / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко ; [под ред. В.А. Хорошко]. — Киев : Арий, 2008.
2. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
3. Гришук, Р.В. Теоретические основы моделирования процессов атак на информацию методами теорий дифференциальных игр и дифференциальных преобразований / Р.В. Гришук. — Житомир: Рута, 2010. — 280 с.

4. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
5. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
6. Cheddad, A. Digital image steganography: Survey and analysis of current methods / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // *Signal Processing*. — 2010. — Vol.90, Iss.3. — PP. 727–752.
7. Cheddad, A. A skin tone detection algorithm for an adaptive approach to steganography / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // *Signal Processing*. — 2009. — Vol.89, Iss.12. — PP. 2465–2478.
8. Luo, X.-Y. A review on blind detection for image steganography / X.-Y. Luo, D.-S. Wang, P. Wang, F.-L. Liu // *Signal Processing*. — 2008. — Vol.88, Iss.9. — PP.2138–2157.
9. Khatirinejad, M. Linear codes for high payload steganography / M. Khatirinejad, P. Lisoněk // *Discrete Applied Mathematics*. — 2009. — Vol.157, Iss.5. — PP. 971–981.
10. Chen, W.-J. High payload steganography mechanism using hybrid edge detector / W.-J. Chen, C.-C. Chang, T. Hoang Ngan Le // *Expert Systems with Applications*. — 2010. — Vol.37, Iss.4. — PP. 3292–3301.
11. Cetin, O. A new steganography algorithm based on color histograms for data embedding into raw video streams / O. Cetin, A. Turan Ozcerit // *Computers & Security*. — 2009. — Vol.28, Iss.7. — PP. 670–682.
12. Eslami, Z. Secret image sharing based on cellular automata and steganography / Z. Eslami, S.H. Razzaghi, J. Zarepour Ahmadabadi // *Pattern Recognition*. — 2010. — Vol.43, Iss.1. — PP. 397–404.
13. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // *Компьютерная оптика*. — 2011. — Том 35, №2. — С. 262–267.
14. Карпинець, В.В. Вирішення проблеми зменшення рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпинець, Ю.Є. Яремчук // *Інформатика та математичні методи в моделюванні*. — 2011. — Том 1, №2. — С. 131–140.
15. Маракова, И.И. Повышение эффективности сокрытия информации для систем с зашумленными каналами связи / И.И. Маракова, А.А. Яковенко // *Информатика та математичні методи в моделюванні*. — 2011. — Том 2, №1. — С. 5–17.
16. Кобозева, А.А. Проблема выбора контейнера в компьютерной стеганографии / А.А. Кобозева // *Захист інформації*. — 2007. — №4. — С. 63–75.
17. Кобозева, А.А. Общий подход к оценке свойств стеганографического алгоритма, основанный на теории возмущений / А.А.Кобозева // *Информационные технологии и компьютерная инженерия*. — 2008. — №1(11). — С.164–171.
18. Кобозева, А.А. Оценка чувствительности стегосообщения к возмущающим воздействиям / А.А. Кобозева, Е.В. Нариманова // *Системні дослідження та інформаційні технології*. — 2008. — №3. — С. 52–65.
19. Кобозева, А.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // *Вісник Східноукраїнського національного університету ім. В. Даля*. — 2008. — №8(126), Ч.1. — С. 62–72.
20. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
21. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студентов физико-математических специальностей вузов / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 8-е изд. — М. : Физматлит ; Л. : Невский диалект, 2000. — 622 с.
22. Парлетт, Б. Симметричная проблема собственных значений: численные методы [Текст] / Б. Парлетт; Пер. с англ. Х.Д. Икрамов, Ю.А. Кузнецов. — М. : Мир, 1983. — 382 с.
23. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах / А.А.Кобозева // *Вісник Східноукраїнського національного університету ім. В. Даля*. — 2006. — №9(103). — С. 74–82.
24. Кобозева, А.А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы / А.А. Кобозева // *Праці УНДІРТ*. — 2006. — №4(48). — С. 44–52.
25. Кобозева, А.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы / А.А. Кобозева, Е.А. Трифонова // *Труды Одесского политехнического университета*. — 2008. — №1(29). — С. 183–190.

ТЕОРІЯ ЗБУРЕНЬ ЯК ОСНОВА ЗАГАЛЬНОГО ПІДХОДУ ДО ОЦІНКИ ЧУТЛИВОСТІ СТЕГАНОВІДОМЛЕНЬ

А.А. Кобозєва, О.В. Наріманова

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

Розроблено загальний математичний підхід до оцінки чутливості стегановідомлень до збурних дій, що не залежить від використовуваного стеганографічного алгоритму, області вбудови секретної інформації, області аналізу стегановідомлення – просторової або частотної. Основними математичними інструментами є матричний аналіз і теорія відносних збурень. Пропонується спосіб оцінки захищеності секретної інформації, вбудованої в контейнер – цифрове зображення. Розроблено спосіб кількісної оцінки чутливості стегановідомлення до збурних дій, що використовується для рішення задачі про вибір контейнера із скінченної множини контейнерів для заданого секретного повідомлення. Отримане рішення забезпечує найменшу чутливість стегановідомлення до збурних дій, тобто найбільшу ефективність процесу декодування додаткової інформації, оцінювану за допомогою об'єму відновленої інформації.

Ключові слова: стегановідомлення, збурна дія, чутливість, матриця, власне значення, власний вектор

PERTURBATION THEORY AS A BASIS OF GENERAL APPROACH TO EVALUATE SENSITIVITY OF STEGO MESSAGES

Alla A. Kobozeva, Elena V. Narimanova

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

The general mathematical approach, based on matrix theory and perturbation theory, to evaluate sensitivity of stego messages is developed. Proposed approach does not depend on the used steganography algorithm, area of hidden information, analyzed domain – spatial or frequency. Method to evaluate immunity of hidden information in cover (for example, image) is developed. The results of computational experiments are presented.

Keywords: stego message, perturbation, sensitivity, matrix, eigenvalue, eigenvector

ИНФОРМАЦИОННАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОЦЕНКИ ЖИВУЧЕСТИ СУДОВЫХ ТЕХНИЧЕСКИХ СИСТЕМ

В.Д. Бойко

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65029, Украина; e-mail: vint532@yandex.ua

В статье описана информационная система поддержки принятия решений, основывающаяся на когнитивно-информационной модели судовых технических систем, позволяющая получать комплексную оценку живучести систем с точки зрения структурной уязвимости и функциональности.

Ключевые слова: судовые технические системы, система поддержки принятия решений, когнитивно-информационная модель

Введение

Качественное информационное обеспечение процессов управления судовыми техническими системами (СТС) в процессе эксплуатации требует использования системы поддержки принятия решений для оценки живучести СТС, основывающейся на новых информационных технологиях.

Современное судно представляет собой сложную совокупность технических систем, подсистем и технического оборудования, влияющих на безопасную эксплуатацию судов и во многом определяющих их живучесть.

Использованием конструктивных решений на стадии проектирования и организационно-технических мероприятий, осуществляемых при эксплуатации, решаются в той или иной мере задачи по обеспечению живучести СТС [1-3].

Актуальность

Из анализа результатов эксплуатации судов следует, что, не смотря на принимаемые меры по обеспечению безопасности мореплавания, количество аварийных случаев на море остается высоким. Соблюдение на стадии проектирования и постройки нормативных требований не является достаточным условием для обеспечения живучести судов при их эксплуатации. Анализ распределения аварий по водоизмещению и возрасту судов показывает, что выход из строя технических систем чаще всего служит одной из самых многочисленных причин аварий на судах большого и среднего тоннажа. Следует отметить, что проблема обеспечения живучести актуальна не только для старых, но и для новейших типов судов и, в особенности, для судов большого водоизмещения, с развитыми системами управления и коммуникациями и, как следствие, с более уязвимыми судовыми подсистемами [4-6]. Существующие информационные системы оценки состояния СТС контролируют, в основном, процессы реального времени, предоставляя информацию о текущем состоянии систем, не обобщая ее и не пытаясь прогнозировать возможные варианты эволюции параметров систем во времени.

Из рассмотренных литературных источников следует, что в настоящее время теория живучести находится в такой стадии развития, когда точно не сформированы основные понятия и определения, не существует единого мнения и о том, что такое живучесть, какова область применения этого понятия. Практически нет апробированных длительным практическим использованием моделей живучести СТС. Большое разнообразие известных показателей живучести скорее свидетельствует о недостаточной ясности в решении этого вопроса, чем о его проработанности. Нет определенных методических разработок и по вопросу о том, для каких судовых технических систем следует оценивать, нормировать и обеспечивать живучесть. До сих пор не создано развитой теории, которая содержала бы, как и теория надежности, общетехнические результаты, позволяющие исследовать это свойство, оценивать его количественно и разрабатывать практические рекомендации проектировщика сложных систем по обеспечению живучести.

Исходя из изложенного, обеспечение живучести судовых технических систем в целях повышения уровня безопасной эксплуатации судов и снижения их аварийности является по-прежнему актуальной научно-технической задачей.

Целью работы является создание информационной системы поддержки принятия решений для оценки и управления живучестью технических систем, обеспечивающих безопасную эксплуатацию судов.

Изложение основного материала

Современные технологии профессионального обучения позволяют оператору эффективно моделировать и оценивать (в первом приближении) происходящее в технических системах. Однако большая (все возрастающая по мере распространения микропроцессорных комплексов реального времени и интеллектуализации судовых систем) информационная нагрузка требует даже на уровне первого приближения оценок все большего ресурса внимания, а также учета все большего количества различных параметров, их значений и взаимосвязи [7].

Судовые технические системы состоят из конечного числа элементов, в которых возможно возникновение конечного числа дефектов. Т.е. подобные системы могут находиться в конечном множестве состояний, оцениваемых по признаку работоспособности и неработоспособности.

Множество состояний СТС можно представить *пространством состояний*. Совокупность тех или иных значений технических параметров для каждого из состояний – *вектор состояний*, характеризующий положение судовых систем в пространстве состояний. Аналогичные рассуждения можно провести для каждого из составных блоков систем. Таким образом, весь комплекс СТС на каждом уровне («совокупность систем» – «комплекс» – «отдельные системы» – «подсистемы» – «узлы») можно характеризовать пространством состояний, каждая точка которого соответствует определенному уровню живучести системы и определяется вектором состояний системы.

Для оценки живучести СТС предлагается использовать систему поддержки принятия решений (СППР). Как известно [8-11] в таких системах в отличие от классических систем искусственного интеллекта осуществляется: моделирование предметной области, а не самого эксперта; применение теории вероятности и теории принятия решений вместо попыток «учета неопределенности» с помощью продукционных правил вида «если..., то...»; замена эксперта (разгрузка его внимания и оказание ему помощи).

Разработанная СППР оценивает: общее состояние систем, используя единую систему параметров узлов; значения характеристик узлов и взаимодействие, основанное на значении и динамике входящих и исходящих параметров. Ядром СППР

является иерархически организованная когнитивно-информационная модель судовых технических систем. Концептуальной единицей модели является объект, рассматриваемый как составная часть информационной модели с индивидуальными характеристиками. Каждый узел подключается к системе, либо как виртуальный компонент библиотеки узлов (модель функционирующего узла системы), либо как реальный компонент, подключаемый через информационный интерфейс, получающий на входе параметры технической диагностики систем, и преобразующий их в системные параметры СППР. При реализации СППР используются аппаратные или программные интерфейсы. Взаимодействие узлов оценивается по их входящим и исходящим параметрам.

Узлы когнитивно-информационной модели объединяются в иерархическую, взаимосвязанную систему, организованную на нескольких уровнях иерархии. Первым уровнем являются технические комплексы, определяющие живучесть корабля в целом. Следующим уровнем являются технические системы образующие комплексы. Нижний уровень включает промежуточные уровни технических систем, отражающие их функционально-структурное распределение на судне, а также работу систем резервирования, в частности – систем и компонентов таких систем. На рис. 1 приведена разработанная обобщенная структурная схема оценки судовых технических систем с учетом их иерархии.

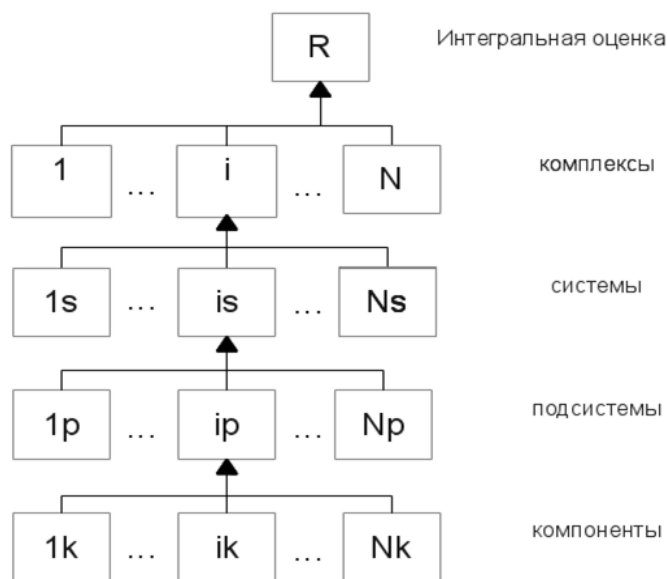


Рис. 1. Иерархическая обобщенная структурная схема оценки СТС

На верхнем уровне иерархии осуществляется общая интегральная оценка живучести всего технического комплекса – R . Она складывается из оценок отдельных комплексов (от 1 до N), каждая из которых в свою очередь включает в себя оценку живучести входящих в его состав: технических систем (от $1s$ до Ns для каждого комплекса); подсистем (от $1p$ до Np для каждой системы); компонентов (от $1k$ до Nk для каждой подсистемы).

Следующий шаг оценки живучести технических систем заключается в использовании логических уравнений связи конъюнктивно-дизъюнктивного типа или средств нечеткой логики и нейронного моделирования. Использование понятия «лингвистической переменной», применение аппарата нечеткой логики позволяет применить графоаналитические методы для построения сетей, в которых, вместо

жестких логических связей конъюнктивно-дизъюнктивного характера используются элементы типа «нейрон-конъюнктор» («нейрон-дизъюнктор»), оперирующие не жесткими бинарными значениями, а комплексом весовых функций и порогом передаточной функции. Такой подход также позволяет использовать системы байесовых оценок правдоподобия, либо аналогичные им и нейронным сетям механизмы свертки нечетких оценок к интегральным показателям. Нейронные и квазинеуронные сети оценок позволяют прогнозировать техническую эволюцию параметров системы и представить возможные сценарии развития событий в ранжированных обобщенных оценках их опасности на различных уровнях иерархии судовых технических систем — как в функционально-структурном виде, так и по временной оси. При этом сохраняется преимущество представления всей системы в «человеко-читаемом виде» — сохраняются функционально-структурные связи. Это позволяет использовать систему в режиме автоматического обучения, а также «ручную» коррекцию параметров системы.

Использованием аппарата нечеткой логики оценивается состояние системы в обобщенных оценках (например, в терминах базы данных OREDA: «исправное», «минимальное», «ухудшающееся», «критическое» [12]) либо в точных значениях функции доверия на всем спектре значений. Такое представление обеспечивает ранжировку событий, как по опасности, так и по времени наступления, позволяя принимать меры для устранения в первую очередь наиболее критичных и неотложных уязвимостей в системе.

Рассмотрим применение разработанной СППР для оценки живучести системы обеспечения электропитанием судовых электропотребителей. Упрощенная структурная схема обеспечения электропитанием судовых электропотребителей приведена на рис.2.

Представленная на рис.2 структурная схема состоит из основного (M) и резервного (R) блоков. Каждый из блоков содержит основной или резервный генератор (Gm и Gr соответственно), основной или резервный привод (Dm и Dr соответственно).

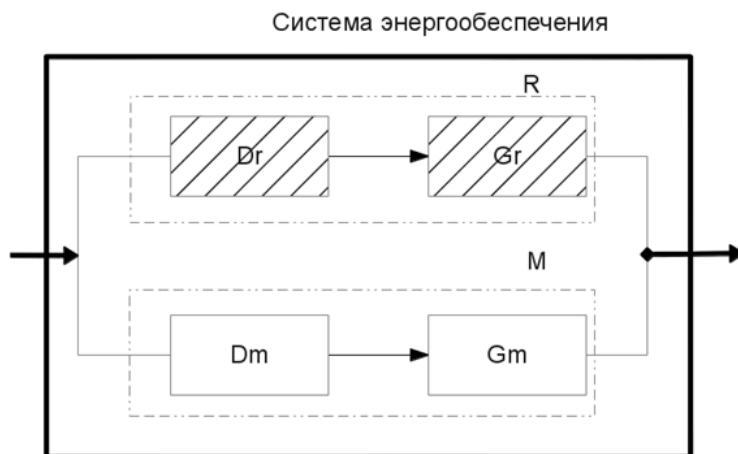


Рис. 2. Обобщенная структурная схема обеспечения электропитанием судовых электропотребителей

Каждый узел характеризуется n состояниями S_n , каждое из которых отражает эволюцию исправности узла. При этом за S_0 принимается абсолютно исправное состояние узла, а S_i , для $i \in 1, \dots, n$ отражают переход узла к все менее исправным состояниям. В простейшем случае у узла два состояния: $n = 0$ — узел исправен; $n = 1$ —

узел неисправен. Характеристика «состояние узла» S_i – отражает его состояние на текущий момент времени. Вектор вероятности состояний узла P отражает вероятности перехода узла в одно из n состояний. Вектор работоспособности узла F указывает на состояние узла в каждом из n состояний и отражает его способность выполнить поставленную задачу за время Δt . Вектор работоспособности узла F определяется по формуле

$$F_i = \frac{P'_1}{P'_0} = \frac{P(S_i | \Delta t)}{P(S_0 | \Delta t)}. \quad (1)$$

Вектор работоспособности узла – качественная характеристика, отражающая отношение вероятности выполнения целевой работы в состоянии S_0 к вероятности выполнения работы в S_i . При двух состояниях узла такой вектор будет иметь всего два значения – $F_0 = 1$ (узел работоспособен) и $F_1 = 0$ (узел неработоспособен). Тогда (1) может быть записана в виде

$$F_0 = \frac{P(S_0 | \Delta t)}{P(S_0 | \Delta t)} = \frac{1}{1} = 1, \quad (2)$$

$$F_1 = \frac{P(S_1 | \Delta t)}{P(S_0 | \Delta t)} = \frac{0}{1} = 0.$$

Ожидаемая работоспособность является математическим ожиданием работоспособности узла и вычисляется по формуле

$$F_\Sigma = \sum_{i=0}^n f_i p_i. \quad (3)$$

Таким образом, состояние системы в логической форме будет описываться уравнением

$$S = S_r \vee S_m = S_{Dr} \wedge S_{Gr} \vee S_{Dm} \wedge S_{Gm}, \quad (4)$$

где состояние S определяется как бинарное (1 – «узел исправен», 0 – «узел неисправен»).

В случае неисправности основного блока питания S_m обратится в ноль, однако, если резервная система продолжит работу – S_r останется равным единице и система продолжит выполнять свою функцию. Этому состоянию будет соответствовать вектор работоспособности системы, принимающий следующие значения

$$F = 1 \text{ для } S = 1$$

$$F = 0 \text{ для } S = 0$$

Обозначив вероятности $P_0(t)$ и $P_1(t)$ как вероятности смены состояния системы в момент времени t с учетом [9], получим следующие характеристики системы

$$\begin{aligned}
 P_{m0}(t) &= P_{Gm0}(t) \cdot P_{Dm0}(t) \\
 P_{m1}(t) &= P_{Gm1}(t) \cdot P_{Dm1}(t) \\
 P_{r0}(t) &= P_{Gr0}(t) \cdot P_{Dr0}(t) \\
 P_{r1}(t) &= P_{Gr1}(t) \cdot P_{Dr1}(t) \\
 P_0(t) &= P_{r0}(t) + P_{m0}(t) = P_{Gr0}(t) \cdot P_{Dr0}(t) + P_{Gm0}(t) \cdot P_{Dm0}(t) \\
 P_1(t) &= P_{r1}(t) + P_{m1}(t) = P_{Gr1}(t) \cdot P_{Dr1}(t) + P_{Gm1}(t) \cdot P_{Dm1}(t)
 \end{aligned} \tag{5}$$

Таким образом, общая усредненная по всем параметрам оценка живучести системы на момент времени t будет равна его работоспособности, определяемой с учетом (3)-(5) по формуле

$$G_{\Sigma} = F_{\Sigma} = \sum_{i=0}^n F_i P_i = SP = (S_{Dr} \wedge S_{Gr} \vee S_{Dm} \wedge S_{Gm}) \cdot (P_{Gr1}(t) \cdot P_{Dr1}(t) + P_{Gm1}(t) \cdot P_{Dm1}(t)). \tag{6}$$

При моделировании работы системы средствами нечеткой логики используем вместо бинарной логики состояний узлов четыре лингвистических термина функции принадлежности, соответствующие состояниям различной степени исправности – «критические неисправности» ($n = 0$), «неисправности средней тяжести» ($n = 0,33$), «незначительные неисправности» ($n = 0,66$), «отсутствие неисправностей» ($n = 1$). В качестве модели взаимовлияния элементов и блоков системы используем нейроподобный решающий элемент (рис. 3). Данный элемент включает в себя сумматор *Sum*, позволяющий получить усредненное значение весов на его входе, пороговое устройство *Lev* для определения влияния данного узла на следующие узлы в иерархии. Параметры влияния рассматриваются, как безразмерные немасштабные величины в диапазоне от 0, 0.33, 0.66, 1, где 0 отражает полное отсутствие связи (выход узла из строя не влияет на смежный узел), а 1 – прямую связь (выход из строя узла, влечет за собой однозначный выход из строя смежного узла). Вектора влияния узла представляют собой комбинацию входящего и исходящего векторов влияния, отражающую взаимодействие узла с другими узлами системы.

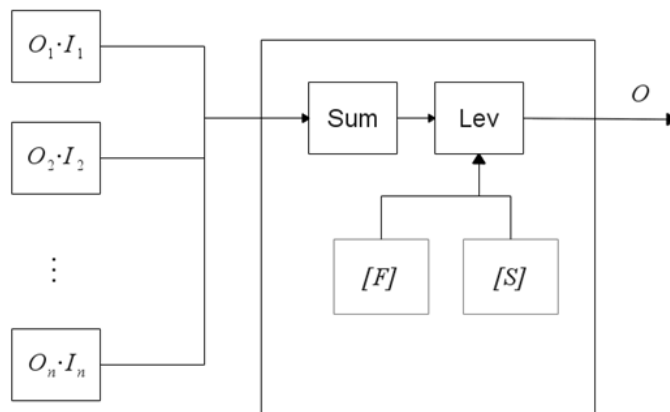


Рис. 3. Нейроподобный решающий элемент

Внутренний вектор влияния $[I]$ отражает параметры влияния на данный узел других узлов системы и зависит от состояния исходящих величин O узлов системы, связанных с данным узлом. Сумматор Sum осуществляет свертку входящих влияний узлов и внутреннего вектора влияния

$$I_{\Sigma} = \sum_{i=1}^n O_i I_i = O_1 I_1 + O_2 I_2 + \dots + O_n I_n \quad (7)$$

Величина свертки оценивается пороговым устройством Lev , которое в зависимости от значения I_{Σ} (7), а также с учетом состояния векторов $[S]$ и $[F]$, либо без такового, формирует исходящее значение O , отражающее параметры влияния данного узла на узлы системы верхней иерархии. Исходящий вектор изменяется по мере перехода системы в каждое из состояний S_n .

В простейшей модели влияние векторов состояний и работоспособности может не учитываться. В этом случае пороговое устройство имеет вид простой решающей системы

$$O = 0, \text{ для } I_{\Sigma} \cdot Lev,$$

$$O = 1, \text{ для } I_{\Sigma} > Lev.$$

Взаимовлияние систем определяется состоянием сигналов на входе. При этом целесообразно описать передаточную функцию при помощи какой-либо из функций, использующихся при моделировании нейронов, например S-образной логистической функцией вида

$$F(S) = \frac{1}{1 + e^{-S/T}}.$$

В этом случае для низкого значения входных сигналов и высокого порога передаточной функции можно получить «нечеткий конъюнктор», а в обратном случае (высокое значение входных сигналов и низкое значение порога) – «нечеткий дизъюнктор». То есть по мере приближения модели к граничным значениям она вырождается в логико-вероятностную модель.

Кроме узлов-объектов, представляющих собой части судовых технических систем, СППР может включать в себя узлы, моделирующие возникающие неисправности (внутренние неблагоприятные воздействия) и порождающие их причины (внешние неблагоприятные воздействия). При этом одно и то же неблагоприятное воздействие может переводить систему в разные режимы состояния с разной долей вероятности.

Разработанная СППР функционирует в следующих режимах поддержки принятия решений. В *режиме интегральной оценки* система указывает на возможные в разные моменты времени неисправности, оценивает их критичность и выдает рекомендации по восстановлению/замене узлов в зависимости от их влияния на систему и экономического эффекта. В *режиме дифференциальной оценки* система оценивает каждую из иерархий технических систем по категории «система – подсистема – узел» и выдает рекомендации аналогичные режиму интегральной оценки. В *поисковом режиме* система моделирует возможные неисправности и выход из строя узлов с различными целевыми функциями поиска. Целями поиска в таком режиме являются поиск критических и уязвимых мест системы, оценка различных вариантов профилактики системы (в зависимости от критичности и экономического эффекта – при этом экономический эффект может выражаться как в ценовой, так и в ресурсозатратной форме), наихудшие

сценарии возможных неисправностей и возможность «аварийных резонансов» – когда выход из строя незначительных элементов может повлечь за собой каскадную цепь поломок и выходов из строя систем.

Выводы

Разработанная информационная система поддержки принятия решений, основанная на когнитивно-информационной модели судовых технических систем, позволяет на стадии проектирования систем осуществить моделирование возможных сценариев неисправностей и устранить уязвимые места конструктивными методами, в частности резервированием уязвимых участков. На стадии эксплуатации СППР позволяет оценить критичность технических узлов и в зависимости от риска выхода из строя этих узлов формировать рекомендации по профилактическому ремонту и замене технических систем. На стадии упреждения аварии СППР позволяет формировать рекомендации по мерам направленным на возможное предотвращение более серьезных аварий

Список литературы

1. Менеджмент риска. Термины и определения : ГОСТ Р 51897-2002. — [Принят и введен с 2003—01—01]. — М.: Издательство стандартов. — 2003. — 8 с.
2. Quality management systems – Requirements : BS EN ISO 9001:2008. — [Принят и введен с 2009—11—12]. — London : BSI Standards, 2009. — 27 p.
3. Risk management — Principles and guidelines : ISO 31000:2009. — [Принят и введен с 2009—07—52]. — Geneva: International Organization for Standardization, 2009. — 24 p.
4. Marine Accident Investigation Branch (MAIB). Annual Report 2011. — United Kingdom, Southampton: Crown. — 2011. — 77 p.
5. Дерменжи, М. Аварийность на море: реальный взгляд на жизнь / М. Дерменжи, А. Гудзь // Материалы XII международного семинара «Качественное судоходство: стандарт XXI века. Безопасность и защита морской среды: грядущие перемены», 21–22 октября 2009, Санкт-Петербург. — Санкт-Петербург, 2009.
6. Wang, J. Formal safety assessment of containerships / J. Wang, P. Foinikis // Marine Policy. — 2001. — Vol.25, Iss.2. — PP. 143–157.
7. Ковтун, Л.И. Интеллектуальный интерпретатор критических событий и их последствий в корабельной АСУ на базе упреждающего имитационного моделирования и ситуационного анализа контролируемых процессов [Текст] / Л.И. Ковтун, Н.А. Шарков // Пятая (юбилейная) всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика ИММОД-2011», 19–21 октября 2011, Санкт-Петербург. — Санкт-Петербург, 2011. — С. 181–188.
8. Терехов, С.А. Введение в байесовы сети / С.А. Терехов // Научная сессия МИФИ-2003. V Всероссийская научно-техническая конференция «Нейроинформатика-2003»: лекции по нейроинформатике. Часть 1. — М.:МИФИ, 2003. — С. 149–187.
9. Korczewski, Z. Application of expert systems in diagnostics, management and logistics / Z. Korczewski // Polish Maritime Research. — 2008. — Nr. 3. — S. 86–91.
10. Saaty, T.L. Decision making with the analytic network process: economic, political, social and technological applications with benefits, opportunities, costs and risks / T.L. Saaty, L.G. Vargas. — New York : Springer, 2006. — 278 p.
11. Горелова, Г.В. О возможности анализа и синтеза структур отказоустойчивых распределенных информационно-управляющих систем, основанной на когнитивном подходе [Текст] / Г.В. Горелова, Э.В. Мельник // Искусственный интеллект. — 2008. — №3. — С. 638–644.
12. OREDA : Offshore Reliability Data Handbook. — 4th Edition. — Høvik, Norway : OREDA Participants, 2002. — 835 p.

ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЖИВУЧОСТІ СУДНОВИХ ТЕХНІЧНИХ СИСТЕМ

В.Д. Бойко

Одеський національний морський університет,
ул. Мечникова, 34, Одесса, 65029, Україна; e-mail: vint532@yandex.ua

У статті описана інформаційна система підтримки прийняття рішень, яка ґрунтується на когнітивно-інформаційній моделі суднових технічних систем, що дозволяє отримувати комплексну оцінку живучості систем з точки зору структурної вразливості і функціональності.

Ключові слова: суднові технічні системи, система підтримки прийняття рішень, когнітивно-інформаційна модель

INFORMATION DECISION SUPPORT SYSTEM FOR ASSESSMENT OF SHIP SURVIVAL TECHNICAL SYSTEMS

Viktor D. Boyko

Odessa National Maritime University,
34 Mechnikova str., Odessa, 65029, Ukraine; e-mail: vint532@yandex.ua

The article describes a decision support system that is based on cognitive-information model ship technical systems, allowing to obtain a comprehensive assessment of survival systems in terms of structural vulnerability and functionality.

Keywords: marine engineering systems, decision support system, cognitive-information model

РЕЗУЛЬТАТИ ПОРІВНЯЛЬНОГО ОБЧИСЛЮВАЛЬНОГО ЕКСПЕРИМЕНТУ СКЛАДАННЯ РОЗКЛАДУ ПРИЙМАННЯ ЛІКУВАЛЬНИХ ПРОЦЕДУР

А.О. Данильченко

Житомирський державний технологічний університет,
вул. Черняхівського, 103, Житомир, 10005, Україна; e-mail: kissann@ukr.net

В статті наведені результати порівняльного обчислювального експерименту складання розкладу приймання лікувальних процедур пацієнтами санаторію різними методами (мурашиним; гілок і меж; пошуку рішення вичерпуванням всіх варіантів) та алгоритмами, що були модифіковані автором для пошуку максимального паросполучення у дводольному графі та враховують обмеження сумісності процедур.

Ключові слова: паросполучення, дводольний граф, генетичний алгоритм, метод гілок і меж, метод повного перебору

Вступ

Санаторій «Дениші» (Житомирська обл.), як цільовий об'єкт дослідження, має популярність в межах України. Основною рисою санаторію є безперервна модернізація комплексу послуг, лікувальних процедур та умов відпочинку і життя пацієнта. В санаторії оздоровлюється більше 500 пацієнтів на зміну (24 дні).

У санаторії розроблені певні комплекси лікувальних процедур, які розраховані на лікування чи профілактику тієї або іншої хвороби. Загалом до послуг хворих надається близько 98 типів процедур. Серед них – використання радонової води, лікувальні грязі, зали лікувальної фізкультури, тренажерні зали, плавальний басейн, нетрадиційні методи лікування (голкорексфлексотерапія, магнітно-вакуумні банки, п'явки, аромотерапія), різні види масажу тощо. Їх вибір залежить від багатьох факторів: основного і супутнього захворювання, мозкового кровообігу, тривалості лікування, яке може собі дозволити пацієнт і т.д. В залежності від стану хворого, йому призначається по 5-7 видів процедур.

Згадуючи загальну кількість пацієнтів, які проходять лікування та індивідуальний підхід до стану кожного пацієнта, стає зрозумілим, що складання розкладу процедур, який зміг би врахувати всі вищезазначені фактори, є проблемою для санаторію більш ніж актуальною. Основною вимогою до розкладу процедур є його гнучкість та швидкість формування.

В загальній постановці задача складання розкладу приймання лікувальних процедур пацієнтами санаторію поширюється на велику кількість споріднених задач складання оптимальних розкладів та може бути вирішена методами комбінаторної оптимізації [1], а також за допомогою теорії графів [2].

Шляхом модифікації класичної задачі теорії графів про паросполучення, прикладна задача складання оптимального розкладу прийому лікувальних процедур пацієнтами санаторію може бути зведена до розширеної математичної задачі пошуку максимального паросполучення у дводольному графі [3, 4].

Задача про паросполучення може бути розв'язана як методом повного перебору всіх можливих варіантів так і більш ефективними методами: мурашиним, генетичним алгоритмом, методом гілок і меж, тощо.

Метою статті є вибір алгоритму з найменшою обчислювальною складністю для прикладного використання його в санаторних закладах України.

Для досягнення мети необхідно вирішити наступні *задачі*:

- оцінити часові витрати на виконання розрахунків різними алгоритмами на обчислювальних платформах, що мають різні обчислювальні потужності: різну кількість ядер мікропроцесора, різний обсяг пам'яті, тощо;
- обрати найбільш ефективний алгоритм вирішення задачі складання розкладу приймання лікувальних процедур пацієнтами санаторію. Критерієм ефективності є мінімізація часу виконання розрахунків щодо пошуку найбільшого паросполучення у дводольному графі зі зникаючими дугами.

Аналіз попередніх досліджень

Метод повного перебору [5] відноситься до класу методів пошуку рішення вичерпування всіх варіантів. Складність повного перебору залежить від кількості можливих рішень, якщо простір рішень дуже великий, тоді перебір може не дати очікуваний результат на протязі великого проміжку часу. Будь-яка задача *NP*-класу може бути вирішена методом повного перебору.

Мурашиний алгоритм [6] – один з ефективних поліноміальних алгоритмів для знаходження наближених рішень задачі комівояжера [7], а також аналогічних завдань пошуку маршрутів на графах. Суть підходу полягає в аналізі та використанні моделі поведінки мурах, що шукають шляхи від колонії до джерела живлення.

Генетичні алгоритми [8] дозволяють розв'язувати широке коло складних задач багатокритеріальної оптимізації шляхом випадкового підбору, комбінування та зміни параметрів моделювання способами, що подібні до біологічної еволюції (наслідування, мутація, відбір). Застосовують ці алгоритми й для розв'язку задач на графах. Існує досить багато модифікацій генетичних алгоритмів. Але всім їм властива універсальність. Тобто від задачі, яку необхідно розв'язати, залежить визначення функції пристосованості й спосіб кодування рішень. Решта же етапів генетичних алгоритмів виконується однаково для будь-яких задач.

Метод гілок і меж [9] є загальним алгоритмічним методом вирішення різноманітних оптимізаційних задач. Він широко застосовується для таких *NP*-повних задач, як задача комівояжера та задача о ранці. В методі гілок і меж використовуються дві процедури: розгалуження та знаходження оцінок (меж).

Основні результати

1) Умови проведення експерименту.

Експеримент проводився на базі санаторію «Деніш» з використанням авторського проблемно-орієнтованого інструментарію – програми ICS_DENISH. Програма має можливість вирішення задачі складання розкладу приймання процедур пацієнтами санаторію п'ятьма алгоритмами: методом повного перебору, оптимальним алгоритмом вирішення задачі пошуку максимального паросполучення у дводольному графі зі зникаючими дугами; модифікованим методом гілок та меж, модифікованим генетичним алгоритмом та модифікованим мурашиним алгоритмом вирішення задачі про паросполучення зі зникаючими дугами.

Обчислювальний експеримент проведено на серії випадкових умов задачі, отриманих від реальних пацієнтів санаторію за часовою вибіркою. Характеристики

комп'ютерів, що були використані для проведення експерименту наведені в табл. 1 та на рис. 1.

Таблиця 1.

Характеристики комп'ютерів, що були використані для проведення порівняльного обчислювального експерименту

№ платформи	Назва процесора	Кіль. ядер	Тактова частота	Обсяг оперативної пам'яті
1	Pentium 4	1	2,42 ГГц	512 МБ
2	Intel Celeron E3300	2	2,50 ГГц	2 ГБ
3	Intel Core i5-3570K	4	3,4 ГГц	4 ГБ

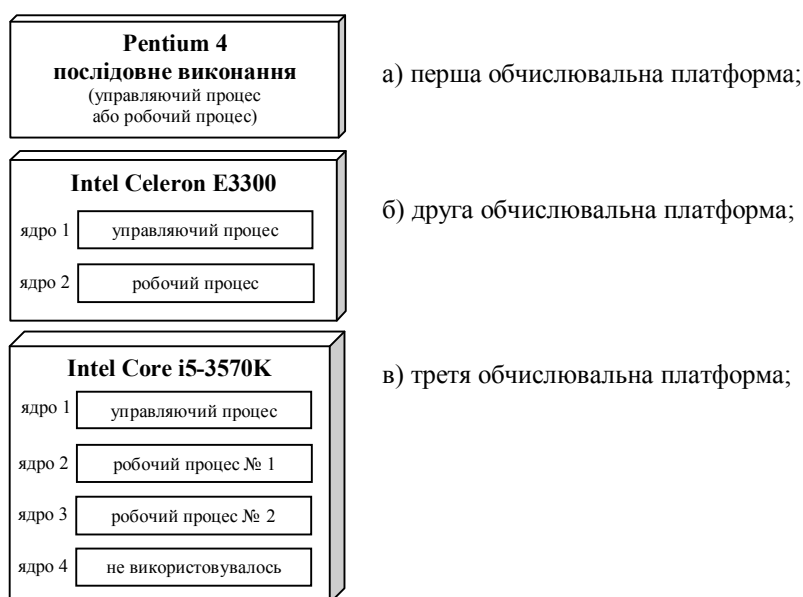


Рис. 1. Структура процесів, що були задіяні на різних обчислювальних платформах

2) Вхідні та вихідні параметри.

Вхідні параметри експерименту (табл. 2) є випадковими та отримані від реальних пацієнтів санаторію за часовою вибіркою і обумовлені організаційною структурою санаторію «Дениші». Вхідні параметри були детермінованими, тобто реєстрованими і керованими (залежними від спостерігача), і випадковими, тобто реєстрованими, але некерованими.

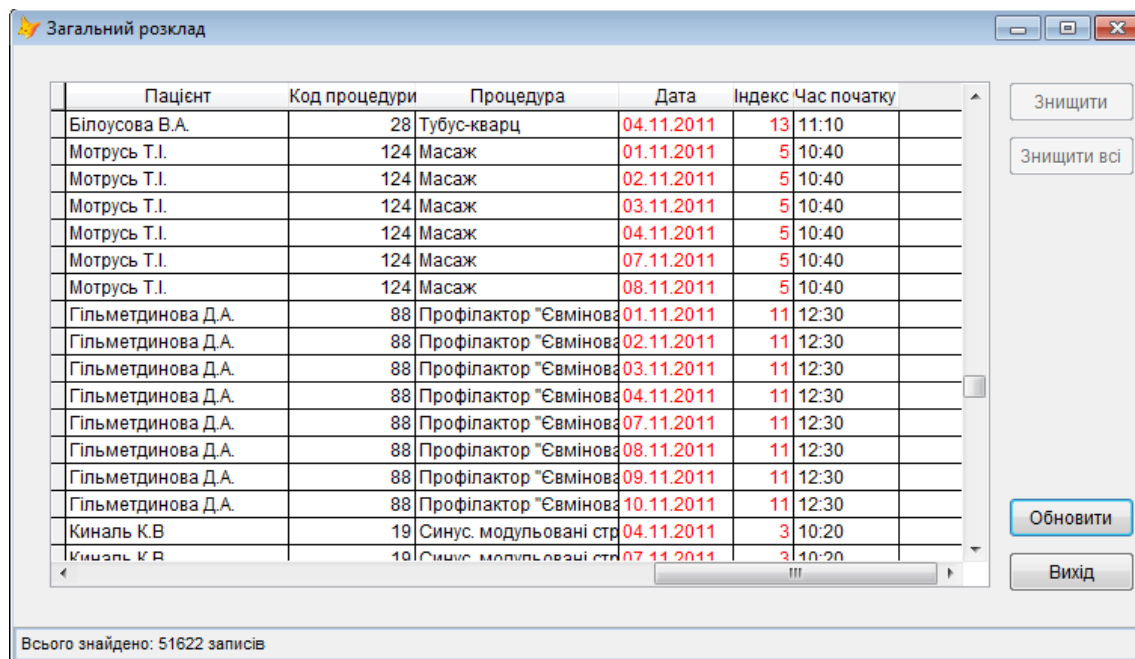
Таблиця 2.

Перелік вхідних параметрів обчислювального експерименту

№ п-ру	Позначка	Назва параметру	Тип параметру
1	$k_{лп}$	кількість лікувальних процедур	детермінований
2	$k_{п}$	кількість пацієнтів	випадковий
3	$k_{пп}$	кількість призначених процедур	випадковий
4	$C_{i,j}$	обмеження прийому процедур	детермінований

Відомі обмеження прийому лікувальних процедур (табл. 2) задаються множиною слідств C , таких, що $(x_i, y_j) \rightarrow C_{i,j} = \{(x_{i1}, y_{j1}), \dots, (x_{ik}, y_{jk})\}$. Ці обмеження враховують, неможливість призначення однієї й той же процедури різним пацієнтам на однаковий час (з урахуванням пропускну здатності процедурного кабінету), а також сумісність процедур. Крім того, враховують послідовність прийняття процедур (наприклад, деяка процедура повинна обов'язково передувати заданій множині інших процедур).

Вихідним параметром для проведення порівняльного обчислювального експерименту є час t_{BP} , що витрачається на виконання розрахунків щодо складання розкладу приймання лікувальних процедур пацієнтами санаторію за допомогою програми ICS_DENISH (рис. 2).



Пацієнт	Код процедури	Процедура	Дата	Індекс	Час початку
Білоусова В.А.	28	Тубус-кварц	04.11.2011	13	11:10
Мотрусь Т.І.	124	Масаж	01.11.2011	5	10:40
Мотрусь Т.І.	124	Масаж	02.11.2011	5	10:40
Мотрусь Т.І.	124	Масаж	03.11.2011	5	10:40
Мотрусь Т.І.	124	Масаж	04.11.2011	5	10:40
Мотрусь Т.І.	124	Масаж	07.11.2011	5	10:40
Мотрусь Т.І.	124	Масаж	08.11.2011	5	10:40
Гільметдинова Д.А.	88	Профілактор "Євмінова"	01.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	02.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	03.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	04.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	07.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	08.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	09.11.2011	11	12:30
Гільметдинова Д.А.	88	Профілактор "Євмінова"	10.11.2011	11	12:30
Киналь К.В.	19	Синус. модульовані стр	04.11.2011	3	10:20
Киналь К.В.	19	Синус. модульовані стр	07.11.2011	3	10:20

Всього знайдено: 51622 записів

Рис. 2. Вікно програми ICS_DENISH складання загального розкладу приймання процедур

Точність експериментальних даних істотно залежить від кількості випробувань – чим випробувань більше, тим вище достовірність результатів [4]. Для нашого випадку (при невеликому числі факторів) можна становити 50-100 випробувань на кожній обчислювальній платформі (табл. 1).

3) Результати розрахункового моделювання розв'язання задачі про паросполучення зі зникаючими дугами.

В кожному випробуванні (табл. 3-5) проводився вимір часу на виконання розрахунків: $t_{МП}$ – методом повного перебору, $t_{ОА}$ – оптимальним алгоритмом вирішення задачі зі зникаючими дугами, $t_{ММ}$ – модифікацією методу гілок та меж, $t_{ГА}$ – модифікацією генетичного алгоритму, $t_{МА}$ – модифікацією мурашиного алгоритму.

Результати обчислювального експерименту (рис. 3-5) для методів, що порівнюються на різних обчислювальних платформах дозволяють зробити наступні висновки:

Таблиця 3.

Результати окремих випробувань обчислювального експерименту на першій обчислювальній платформі

№ випр.	Вхідні параметри			Вихідний параметр				
	$k_{\text{ЛП}}$	$k_{\text{П}}$	$k_{\text{ПП}}$	$t_{\text{МП}}$	$t_{\text{ОА}}$	$t_{\text{ММ}}$	$t_{\text{ГА}}$	$t_{\text{МА}}$
1	74	1584	2974	511.24	57.63	47.13	77.81	68.77
2	74	1312	3217	612.75	96.17	89.43	127.84	111.54
3	80	1723	3343	712	118.8	99.9	144.9	129.8
4	80	1784	3578	811.2	141	119.5	171.1	144.5
5	85	1837	3724	909.2	152.3	135.2	189.2	164.3
...								
86	129	8719	51622	2634.68	587.43	386.72	883.24	783.69

Таблиця 4.

Результати окремих випробувань обчислювального експерименту на другій обчислювальній платформі

№ випр.	Вхідні параметри			Вихідний параметр				
	$k_{\text{ЛП}}$	$k_{\text{П}}$	$k_{\text{ПП}}$	$t_{\text{МП}}$	$t_{\text{ОА}}$	$t_{\text{ММ}}$	$t_{\text{ГА}}$	$t_{\text{МА}}$
87	74	1584	2974	365.17	41.16	33.66	55.58	49.12
88	74	1312	3217	437.68	68.69	63.88	91.31	79.67
89	80	1723	3343	508.57	84.86	71.36	103.50	92.71
90	80	1784	3578	579.43	100.71	85.36	122.21	103.21
91	85	1837	3724	649.43	108.79	96.57	135.14	117.36
...								
172	129	8719	51622	1881.91	419.59	276.23	630.89	559.78

Таблиця 5.

Результати окремих випробувань обчислювального експерименту на третій обчислювальній платформі

№ випр.	Вхідні параметри			Вихідний параметр				
	$k_{\text{ЛП}}$	$k_{\text{П}}$	$k_{\text{ПП}}$	$t_{\text{МП}}$	$t_{\text{ОА}}$	$t_{\text{ММ}}$	$t_{\text{ГА}}$	$t_{\text{МА}}$
173	74	1584	2974	170.41	19.21	15.71	25.94	22.92
174	74	1312	3217	204.25	32.06	29.81	42.61	37.18
175	80	1723	3343	237.33	39.60	33.30	48.30	43.27
176	80	1784	3578	270.40	47.00	39.83	57.03	48.17
177	85	1837	3724	303.07	50.77	45.07	63.07	54.77
...								
258	129	8719	51622	878.23	195.81	128.91	294.41	261.23

1) Час складання розкладу прямо пропорційно залежить від кількості вершин дводольного графу (яка дорівнює сумі кількості процедур та кількості пацієнтів), кількості призначених процедур та обмежень $C_{i,j}$.

2) Найменший час складання розкладу показав модифікований метод гілок та меж, при $k_{\text{ЛП}} = 74$, $k_{\text{П}} = 1584$, $k_{\text{ПП}} = 2974$ на першій платформі – 47.13, на другій – 33.14, та третій – 15.06 секунд.

3) Час складання розкладу за умов вирішення задачі пошуку найбільшого паросполучення методом повного перебору в 6.8 разів більший від часу вирішення цієї ж задачі модифікацією методу гілок та меж.

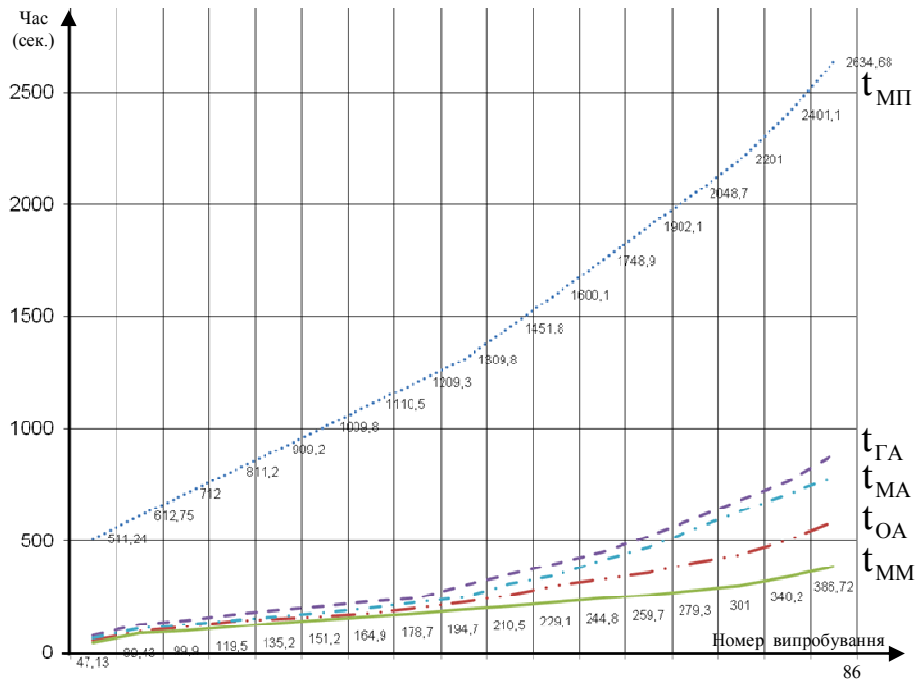


Рис. 3. Графіки залежності часу від розмірності вхідних даних (згідно номера випробування) для методів, що порівнюються на першій обчислювальній платформі

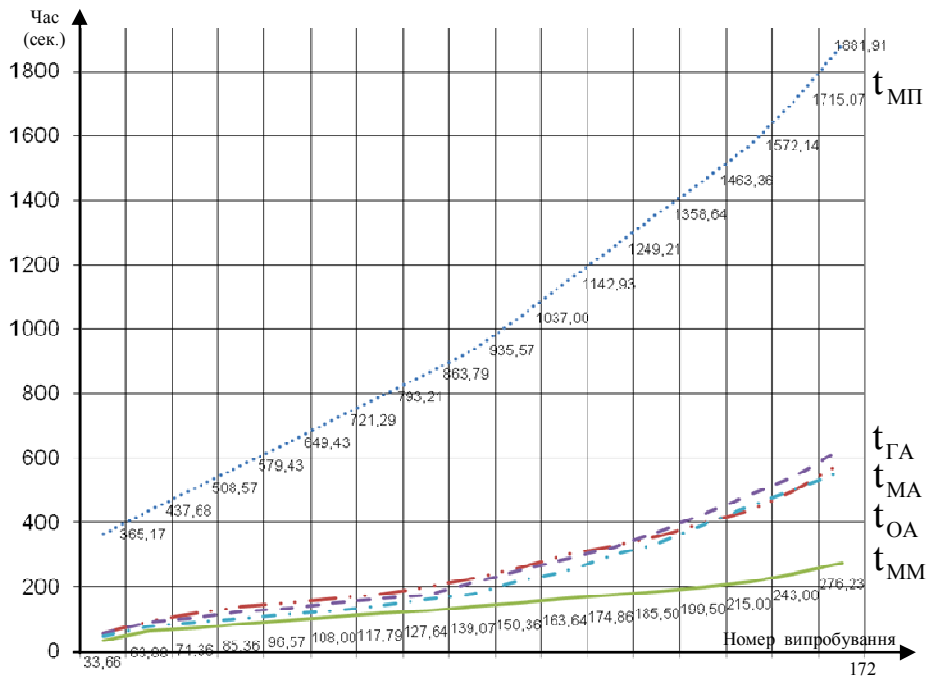


Рис. 4. Графіки залежності часу від розмірності вхідних даних (згідно номера випробування) для методів, що порівнюються на другій обчислювальній платформі

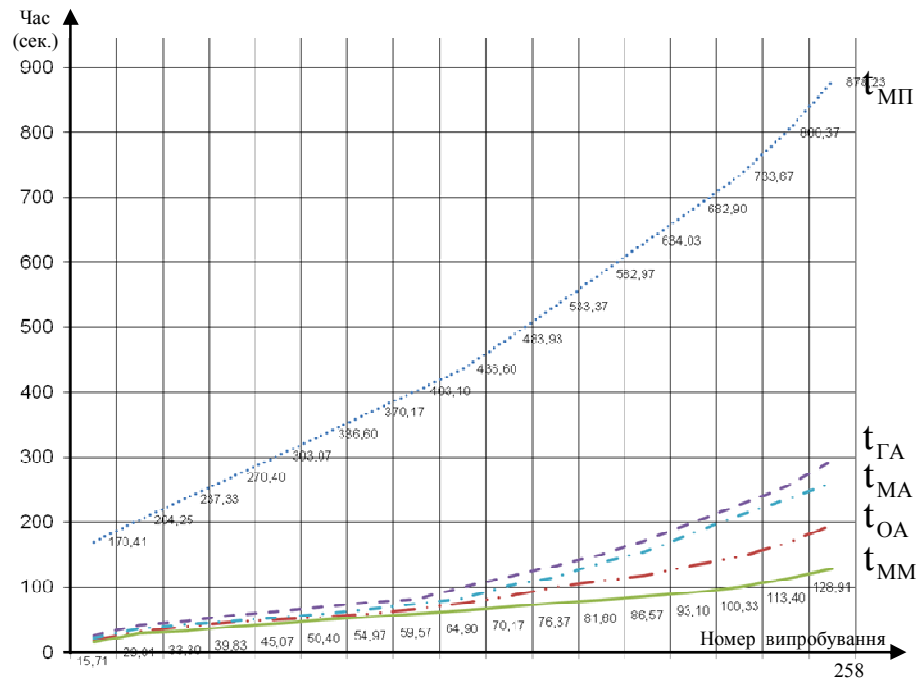


Рис. 5. Графіки залежності часу від розмірності вхідних даних (згідно номера випробування) для методів, що порівнюються на третій обчислювальній платформі

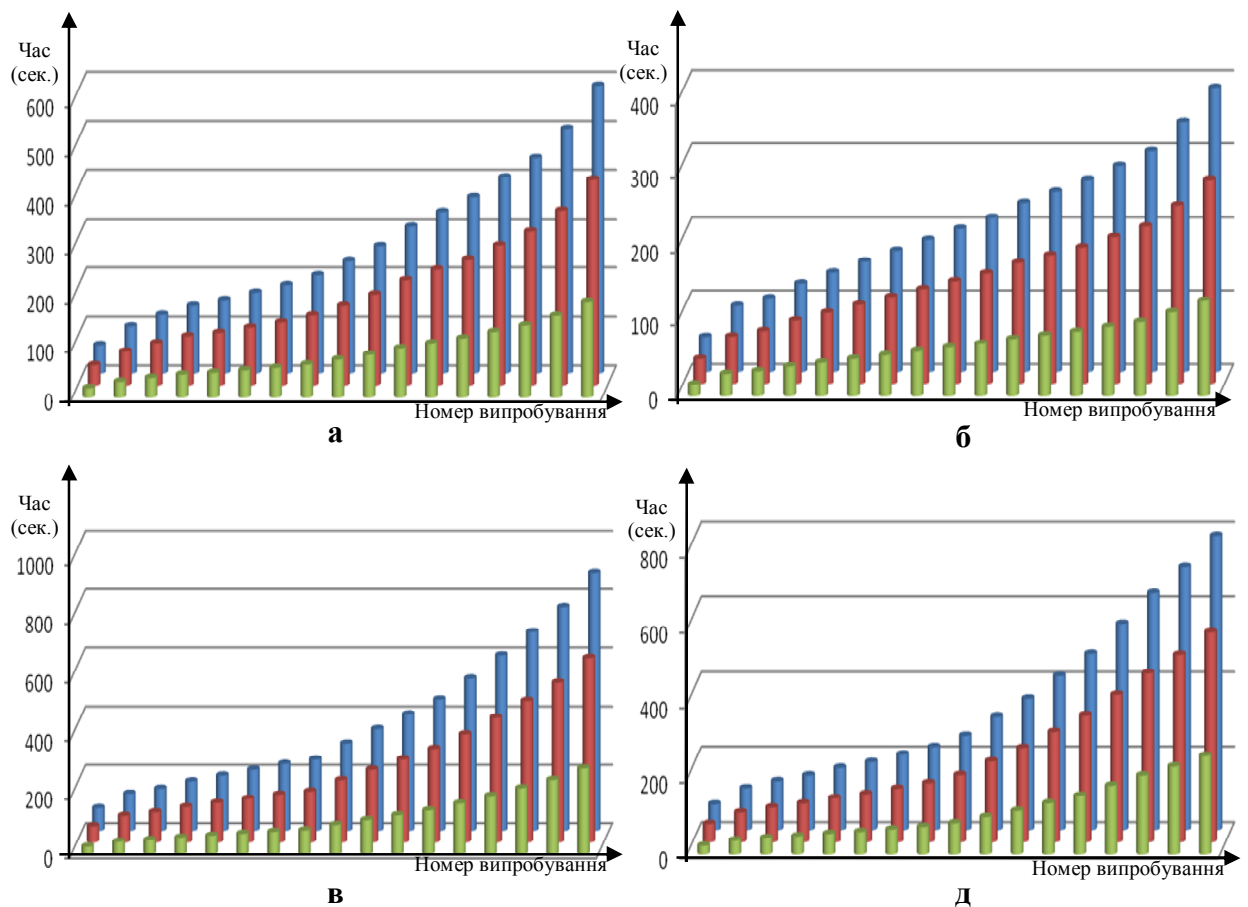


Рис. 6. Час складання розкладу приймання процедур пацієнтами санаторію за допомогою програми ICS_DENISH на різних обчислювальних платформах: а – оптимальним алгоритмом; б – модифікацією методу гілок та меж; в – модифікацією генетичного алгоритму; д – модифікацією мурашиного алгоритму

Якщо розглянути результати обчислювального експерименту (рис. 6) окремо для кожного методу, що порівнюються на кожній обчислювальній платформі можна побачити, при однакових вхідних даних (однаковій кількості процедур, пацієнтів та призначених процедур) час складання розкладу найменший при використанні третьої, найбільш потужної платформи. Так для найбільш ефективного алгоритму модифікації методу гілок та меж приріст часу при $k_{III} = 85$, $k_{II} = 1837$, $k_{III} = 3724$ становить 3 рази.

Висновки

Проведено порівняльний обчислювальний експеримент, який дозволив оцінити часові характеристики методів та алгоритмів розв'язання задачі про паросполучення зі зникаючими дугами та порівняти їх.

За результатами розрахункового моделювання при розв'язанні задачі про паросполучення зі зникаючими дугами на різних обчислювальних платформах за допомогою авторського програмного продукту ICS_DENISH можна визначити, що найбільш ефективним за часом виконання розрахунків є модифікований метод гілок та меж. Час складання розкладу за умов вирішення задачі пошуку найбільшого паросполучення на дводольному графі модифікованим методом гілок та меж на максимально складних вхідних даних $k_{III} = 129$, $k_{II} = 8719$, $k_{III} = 51622$ менший від методу повного перебору в 6.8 разів.

Модифікований метод гілок та меж показує стабільність зменшення часу складання розкладу приймання процедур пацієнтами при збільшенні обчислювальних потужностей ПЕОМ. Так, наприклад, при $k_{III} = 85$, $k_{II} = 1837$, $k_{III} = 3724$ час вирішення задачі на третій платформі зменшується у 3 рази порівняно з першою обчислювальною платформою.

Список літератури

1. Рейнгольд, Э. Комбинаторные алгоритмы [Текст] : теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део ; пер. с англ. Е.П. Липатова ; под ред. В.Б. Алексеева. — Москва : Мир, 1980. — 476 с.
2. Харари, Ф. Теория графов / Ф. Харари; пер. с англ. и предисл. В.П. Козырева ; под ред. Г.П. Гаврилова. — [2-е. изд.] — М.: Едиториал УРСС, 2003. — 296 с.
3. Данильченко, О.М. Розв'язання одного класу задач складання розкладів генетичними алгоритмами на кластерних системах / О.М. Данильченко, А.О. Данильченко, С.А. Ібрагім // Вісник Житомирського державного технологічного університету. — 2004. — №4. — С. 130–135.
4. Данильченко, О.М. Інтелектуальний аналіз даних (Data Mining): навчальний посібник / О.М. Данильченко, А.О. Данильченко. — Житомир: ЖДТУ, 2009. — 405 с.
5. Cormen, T.H. Introduction to Algorithms / T.H. Cormen, et al. — New Delhi : PHI Learning, 2010. — 1292 p.
6. Штовба, С.Д. Муравьиные алгоритмы. Exponenta Pro / С.Д. Штовба // Математика в приложениях. — 2003. — №4. — С. 70–75.
7. Литтл, Дж. Алгоритм для решения задачи коммивояжера / Дж. Литтл, К. Мурти, Д. Суини, К. Кэрел // Экономика и математические методы. — 1965. — Том 1, Вып. 1. — С. 94–107.
8. Гладков, Л.А. Генетические алгоритмы [Текст] : учебное пособие / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик ; под ред. В.М. Курейчика. — Изд. 2-е, испр. и доп. — Москва : Физматлит, 2006. — 320 с.
9. Жолобов, Д.А. Введение в математическое программирование: учебное пособие [Текст] / Д.А. Жолобов. — М.:МИФИ, 2008. — 376 с.

РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА СОСТАВЛЕНИЯ РАСПИСАНИЯ ПРИЕМА ЛЕЧЕБНЫХ ПРОЦЕДУР

А.А. Данильченко

Житомирский государственный технологический университет,
ул. Черняховского, 103, Житомир, 10005, Украина; e-mail: kissann@ukr.net

В статье приведены результаты сравнительного вычислительного эксперимента составления расписания приема лечебных процедур пациентами санатория различными методами (муравьиным; методом ветвей и границ; поиска решения перебором всех вариантов) и алгоритмами, которые были модифицированы автором для поиска максимального паросочетания в двудольном графе и учитывают ограничения совместимости процедур.

Ключевые слова: паросочетания, двудольный граф, генетический алгоритм, метод ветвей и границ, метод полного перебора

ALGORITHM TO SCHEDULE OF RECEIVING SANATORIUM TREATMENTS

Anna A. Danylchenko

Zhytomyr State Technological University,
103 Chernyakhovsky str., Zhytomyr, 10005, Ukraine; e-mail: kissann@ukr.net

The results of the comparative computational experiment to schedule of receiving sanatorium treatments by different methods (ant, branch and borders, exhaustive, etc.) and algorithms that have been modified by the author for finding the maximum matching in a bipartite graph and consider limiting the compatibility of procedures.

Keywords: matching, bipartite graph, genetic algorithms, branches and borders method, exhaustive search method

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ЭНЕРГБЛОКА ТЭС НА ОСНОВЕ АППАРАТА ГИБРИДНЫХ СЕТЕЙ

В.С. Михайленко¹, Р.Ю. Харченко²

¹ Одесская национальная академия пищевых технологий,
ул. Канатная, 112, Одесса, 65039, Украина; e-mail: vlad_mikhailenko@mail.ru

² Одесская национальная морская академия,
ул. Дидрихсона, 8, Одесса, 65029, Украина; e-mail: romannn30@gmail.com

На основе проведенного анализа, показывающего неэффективность традиционных методов адаптации применяемых на энергоблоках ТЭС, авторами предлагается создание нейро-нечеткой гибридной сети (ГС) с интеллектуальной системой идентификации, учитывающей мнение экспертов, способной как к аппроксимации значений параметров математических моделей для всевозможных режимов нагрузки энергоблоков, так и к самообучению методом обратного распространения ошибки. Экспериментально доказано, что спроектированная ГС, реализующая алгоритм Сугено, может быть успешно адаптирована в производственных условиях т.к. является эффективным аппроксиматором, учитывающим мнения экспертов-наладчиков АСУ ТП и нелинейные характеристики объекта.

Ключевые слова: нейро-нечеткая сеть (ННС), гибридная сеть (ГС), аппроксимация, фаззификация, идентификация.

Анализ состояния и постановка проблемы в эффективном управлении работой энергоблоков ТЭС в свете последних исследований и публикаций

Производство электроэнергии на ТЭС проходит в две основные стадии: сжигание топлива в котле, в результате чего образуется пар заданного давления и температуры, и последующее преобразование энергии пара в электрическую энергию в турбогенераторе [1]. Котел и турбогенератор конструктивно объединяются в единый агрегат, который называется энергоблоком «котел — турбина».

Технологическая схема энергоблока «барабанный котел — турбина» в общем виде показана на рис. 1. В топку котла подается топливо и предварительно подогретый в воздухоподогревателе ВП воздух. Выделяемая при сгорании топлива теплота воспринимается поверхностями нагрева — экранными трубами ЭК, пароперегревателем ПП и водяным экономайзером ВЭ, в результате чего поступающая в котел питательная вода превращается сначала в насыщенный, а затем в перегретый пар с давлением $P_{n,n}$ и температурой $\theta_{n,n}$, отделение воды от пара происходит в барабане котла Б. Продукты сгорания топлива — уходящие газы, после соответствующей очистки удаляются через дымовую трубу. Полученный в котле перегретый пар поступает в турбогенератор, где превращается в электрическую энергию трехфазного переменного тока заданной частоты f_c и напряжения.

Цель управления энергоблоком в эксплуатационных режимах состоит в обеспечении выработки в каждый момент времени требуемого количества электрической энергии (мощности). При этом должны выполняться заданные требования к качеству функционирования энергоблока, которые сводятся к минимизации удельного расхода

топлива при сохранении всех эксплуатационных показателей на требуемых правилами технической эксплуатации оборудования и техники безопасности [2].

Общее число управляемых величин энергоблока достигает нескольких сотен, однако из них можно выделить сравнительно небольшое число наиболее важных: электрическую мощность $N_{э}$, давление и температуру перегретого пара $P_{п.п}$ и $\theta_{п.п}$, уровень воды в барабане h_6 , разрежение в топке $P_{т.п}$, параметры, характеризующие качество сгорания топлива.

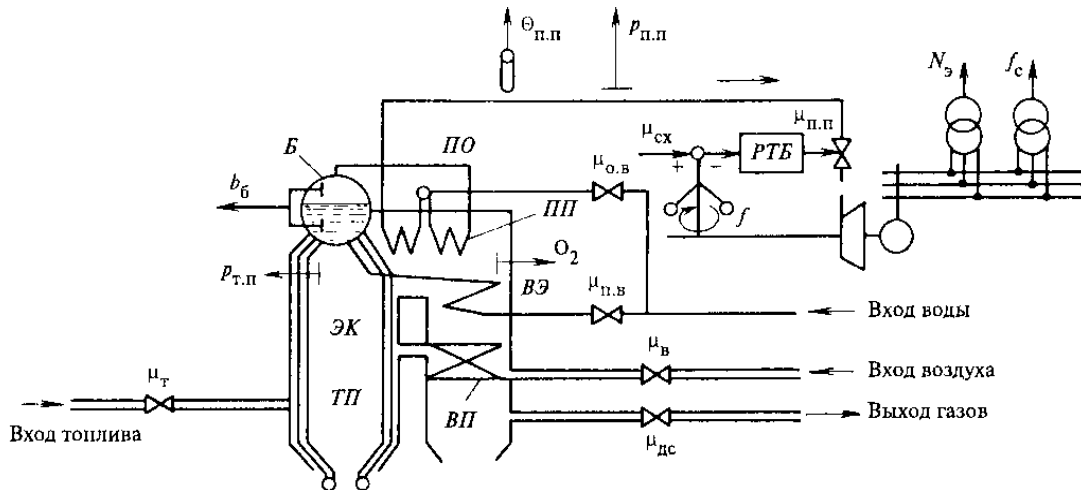


Рис. 1. Технологическая схема энергоблока 200 МВт

Для возможности целенаправленно воздействовать на текущее значение указанных управляемых величин энергоблок снабжается следующими управляющими и регулирующими устройствами:

- задачиком регулятора частоты вращения ротора турбины (синхронизатором), который должен рассматриваться как один из управляющих органов энергоблока, поскольку он является неотъемлемым конструктивным элементом турбины (воздействие $\mu_{сх}$ на рис. 1);
- питателями топлива переменной производительности (воздействие μ_T);
- направляющими аппаратами вентиляторов и дымососов (воздействия μ_6 и $\mu_{дс}$);
- питательным клапаном воды (воздействие $\mu_{п.в}$);
- клапаном на подводе воды к пароохладителю ПО (воздействие $\mu_{о.в}$) и т.д.

На основании анализа ключевых процессов, можно выделить два основных технологических процесса: в паровом котле и турбине. Для процесса в котле главными являются каналы передачи воздействий, связывающие расход топлива, питательной воды и воздуха на входе с давлением и температурой перегрева пара на выходе и в промежуточной точке пароводяного тракта. Для процесса в турбине главным служит воздействие по каналу регулирующие клапаны $h_{кл}$ – мощность N , для энергоблока в целом – по каналу тепловая нагрузка (топливо, вода и воздух) – мощность. Известно, что объект по всем рассматриваемым каналам обладает свойством самовыравнивания и инерцией, которая характеризуется временем запаздывания и постоянной времени T .

Как известно, модели динамики промышленных объектов, используемые в задачах управления, разрабатываются с помощью аппроксимации и методов структурного анализа позволяющих представить сложные системы в виде соединения более простых типовых звеньев [3, 4].

В качестве конкретных примеров моделей динамики приведем передаточные функции отдельных процессов энергоблока ТЭС мощностью 800 МВт при установившихся расходах топлива и воды, полученные в результате аппроксимации экспериментальных усредненных кривых переходного процесса кривыми звена чистого запаздывания и инерционного звена первого порядка [3]:

- для котла (канал топливо B_T – температура пара за потолочным экраном в промежуточной точке тракта)

$$W(s) = \frac{k_1 e^{-20s}}{120s + 1}; \quad (1)$$

- для турбогенератора (канал давление – мощность)

$$W(s) = \frac{150s e^{-2.5s} k_1}{150s + 1}, \quad (2)$$

где $k_1 = 2.5$ МВт см/кгс;

- для энергоблока в целом (канал тепловая нагрузка D – одновременно и согласованное изменение расходов топлива, воды и воздуха – мощность)

$$W(s) = \frac{e^{-17s} k_2}{110s + 1}, \quad (3)$$

где $k_2 = 4.5$ МВт ч/т.

Передаточные функции (1-3) получены при фиксированной нагрузке, равной 300 МВт.

Нерешенные ранее части общих проблем эффективной работы энергоблока

Для математического описания динамики технологических процессов ТЭС в широком диапазоне изменения нагрузок передаточные функции должны быть определены для каждой из установившейся нагрузок. Данная идентификация на современных ТЭС проводится с помощью ступенчатого или синусоидального активного воздействий, что заметно ухудшает качество процессов управления. На действующих в Украине ТЭС экспериментальную информацию необходимую для параметрической идентификации заносят в таблицы, учитывающие изменчивость параметров моделей динамики нагрузок. На основании этих значений выполняется табличная адаптация типовых регуляторов. Вместе с тем, по нашему мнению, данный способ адаптивного управления имеет целый ряд недостатков, связанных с невозможностью получения оптимальных параметров регулятора для всех режимов работы объекта, а также невозможностью учета влияния случайных помех, возмущений и нелинейностей значений нагрузки. Таким образом, существующее адаптивное управление на ТЭС неэффективно.

Цель статьи и постановка задания

В последнее время на зарубежных энергетических предприятиях в системах управления широкое распространение получают интеллектуальные технологии. Использование нейросетевых и нечетких регуляторов позволяет значительно увеличить основные экономические показатели энергоблоков в странах Западной Европы и США [4]. Исходя из перспективности данного направления, а также с учетом экспериментальных характеристик (табл. 1), авторами предлагается создание нейро-нечеткой ННС

или гибридной ГС сети, учитывающей мнение экспертов, способной как к аппроксимации значений параметров математических моделей для всех возможных режимов нагрузки энергоблоков, так и к самообучению на основе опыта экспертов и алгоритма обратного распространения ошибки [5].

Изложение основного материала исследования

Исходя из экспериментальных данных (табл. 1) модель динамики объекта управления может быть дополнена таблицей значений параметров K , T , τ в широком диапазоне изменения паровых нагрузок энергоблока действующего в регулировочном режиме:

Таблица 1.

Параметры математических моделей энергоблока

N , МВт	K , °С/%	τ , с	T , с
400	6.4	45	290
600	1.75	25	126
800	1.46	20	120

ГС, реализующая алгоритм Сугено [5], создается исходя из ряда этапов проектирования:

1) Фаззификация входного параметра «нагрузка энергоблока» (рис. 2).

2) Разработка базы правил вида:

ЕСЛИ «нагрузка низкая» ТО «параметры модели объекта $K_{об}$, $T_{об}$, τ – принимают большие значения» ИНАЧЕ,

«ЕСЛИ «нагрузка средняя» ТО «параметры модели объекта $K_{об}$, $T_{об}$, τ – принимают средние значения» ИНАЧЕ,

ЕСЛИ «нагрузка высокая» ТО «параметры модели объекта $K_{об}$, $T_{об}$, τ – принимают малые значения» и т.д.

Фрагмент базы правил разработанной в программе FTL представлен на рис. 3.

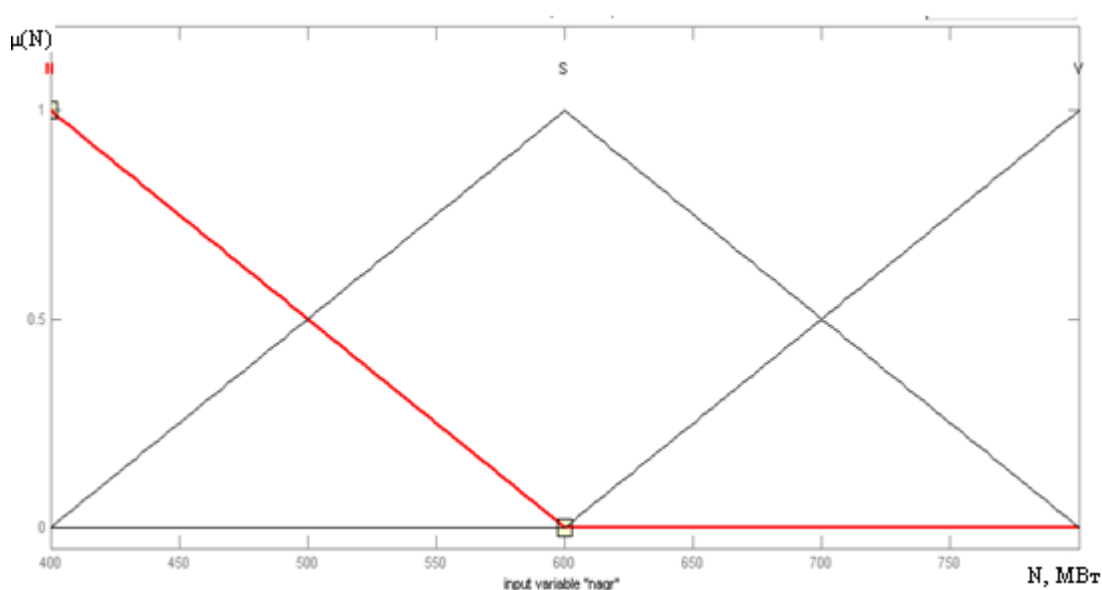


Рис. 2. Фаззификация входного параметра «нагрузка энергоблока»

1. If (nagr is N) and (nagr is N) and (nagr is N) then (Kob is N)(T is N)(z is N) (1)
2. If (nagr is N) and (nagr is S) and (nagr is S) then (Kob is S)(T is S)(z is S) (1)
3. If (nagr is V) and (nagr is V) and (nagr is V) then (Kob is V)(T is V)(z is V) (1)

Рис. 3. База правил системы нечеткого вывода

3) Разработка структуры ГС и ее обучение на основе тестовой выборки (табл. 1). Структура ГС вида ANFIS представлена на рис. 4. Авторами выбрано: количество циклов обучения – 30, метод обучения – обратного распространения ошибки [5].

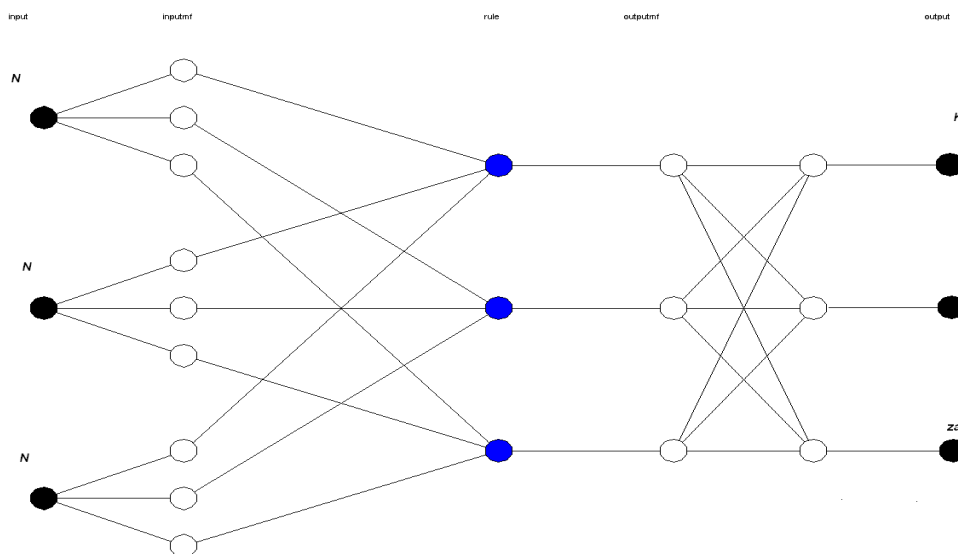
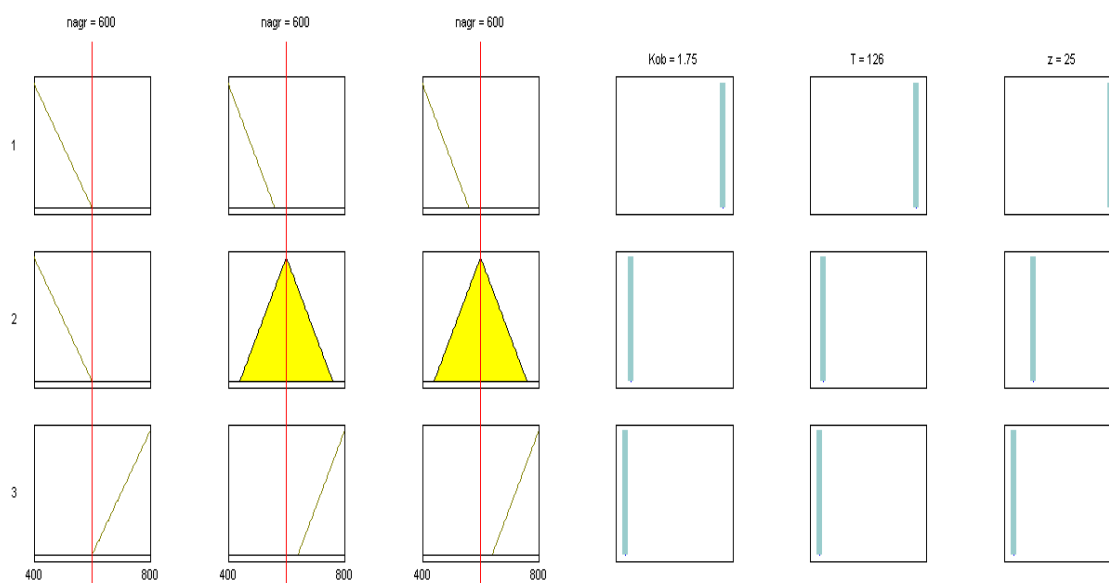


Рис. 4. Структура разрабатываемой ГС

4) Апробация системы нечеткого вывода Сугено представлена на рис. 5.



a

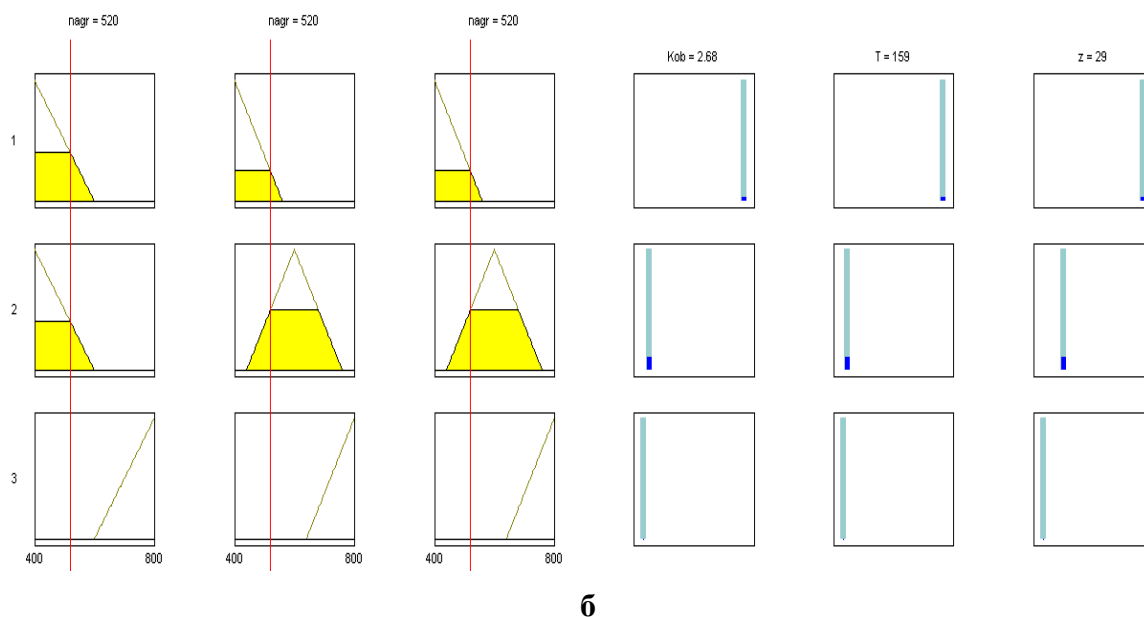


Рис. 5. Окно программы системы вывода заключений FNFIS: а – проверка на соответствие; б – идентификация объекта при изменении нагрузки

Промежуточные значения параметров модели объекта исследования при возможной нагрузке полученные в результате аппроксимации ГС сведены в табл. 2

Таблица 2.
Параметры математической модели энергоблока в регулировочном режиме работы (аппроксимация ГС)

N , МВт	K , °C/%	τ , с	T , с
400	6.4	45	290
500	4.07	35	208
550	1.79	25.2	127
600	1.75	25	126
700	1.52	22.3	123
800	1.46	20	120

Выводы

Таким образом, ГС является эффективным аппроксиматором, учитывающим мнения экспертов наладчиков АСУ ТП и нелинейные характеристики объекта, проявляющиеся при частых изменениях нагрузки. Можно указать, что интеллектуальная система идентификации способна к обучению в отличие от традиционных методов аппроксимации, что также способствует ее успешной адаптации в производственных условиях. Также использование аппарата ГС в системах адаптивного управления технологическими процессами энергоблоков позволит успешно решать задачи перенастройки типовых регуляторов, оптимального перераспределения нагрузки между энергоблоками и прогнозирования остаточного ресурса оборудования.

Список литературы

1. Плетнев, Г.П. Автоматизированное управление объектами тепловых электростанций [Текст] : учеб. пособие для вузов / Г.П. Плетнев. — М. : Энергоиздат, 1981. — 368 с.
2. Ротач, В.Я. Теория автоматического управления [Текст] : учебник для студентов вузов, обучающихся по специальности «Автоматизация технологических процессов и производств (энергетика)» направления подготовки «Автоматизированные технологии и производства» : рек. М-вом образования РФ / В.Я. Ротач. — 3-е изд., стер. — М. : МЭИ, 2005. — 399 с.
3. Ключев, А.С. Наладка систем автоматического регулирования котлоагрегатов [Текст] / А.С. Ключев, А.Г. Товарнов. — М. : Энергия, 1970. — 280 с.
4. Ибрагимов, И.М. Использование систем искусственного интеллекта при эксплуатации энергетических объектов / И.М. Ибрагимов // Надежность и безопасность энергетики. — 2008. — № 1. — С. 51–55.
5. Леоненков, А.Ю. Нечеткое моделирование в среде MATLAB и fuzzyTECH [Текст] : руководство / А.В. Леоненков. — СПб. : БХВ-Петербург, 2003. — 719 с.

ВИЗНАЧЕННЯ ПАРАМЕТРІВ МАТЕМАТИЧНИХ МОДЕЛЕЙ ЕНЕРГОБЛОКУ ТЕС НА ОСНОВІ АПАРАТУ ГІБРИДНИХ МЕРЕЖ

В.С. Михайленко¹, Р.Ю. Харченко²

¹ Одеська національна академія харчових технологій,
вул. Канатна, 112, Одеса, 65039, Україна; e-mail: vlad_mikhailenko@mail.ru

² Одеська національна морська академія,
вул. Дідріхсона, 8, Одеса, 65029, Україна; e-mail: romannn30@gmail.com

На основі проведеного аналізу, який показує неефективність традиційних методів адаптації що застосовують на енергоблоках ТЕС, авторами пропонується створення нейро-нечіткої гібридної мережі з інтелектуальною системою ідентифікації, що враховує думку експертів, здатної як до апроксимації значень параметрів математичних моделей для всіх режимів навантаження енергоблоків, так і до самонавчання методом зворотного поширення помилки. Експериментально доведено, що спроектowana ГМ, що реалізує алгоритм Сугено, може бути успішно адаптована у виробничих умовах, а тому є ефективним апроксиматором й враховує думки експертів-наладчиків АСУ ТП і нелінійні характеристики об'єкта.

Ключові слова: нейро-нечітка мережа, гібридна мережа, апроксимація, фаззифікація, ідентифікація

DEFINING THE PARAMETERS OF MATHEMATICAL MODELS OF POWER BLOCK IN THERMAL POWER STATION BASED ON APPARATUS OF HYBRID NETWORKS

Vladislav S. Mikhailenko¹, Roman Yu. Kharchenko²

¹ Odessa National Academy of Food Technologies,
112 Kanatna str., Odesa, 65039, Ukraine; e-mail: vlad_mikhailenko@mail.ru

² Odessa National Maritime Academy,
8 Didrikhson str., Odesa, 65029, Ukraine; e-mail: romannn30@gmail.com

Based on the analysis, showing the inefficiency of traditional adaptation methods used at power block in thermal power station authors suggest the creation of a hybrid neuro-fuzzy network with intelligent identification, taking into account the opinion of experts, able to approximate how the parameters of mathematical models for various modes of load power units and to self backpropagation. Experimentally proved that the projected GN, which implements algorithm of Sugeno, can be successfully adapted to the operating conditions as approximator is effective, consider the views of expert fitters ACS and non-linear characteristics of the object.

Keywords: Neuro-Fuzzy Network, a hybrid network, approximation, fuzzification, identification

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 2, номер 3, 2012. Одеса – 99 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 2, номер 3, 2012. Одесса – 99 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 2, No. 3, 2012. Odesa – 99 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 31.08.2012)

Адреса редакції: Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044 Україна

Web: <http://www.immm.opu.ua>

E-mail: immm.ukraine@gmail.com

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали

© Одеський національний політехнічний університет, 2012