

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 7, № 1-2

Volume 7, No. 1-2

Одеса – 2017
Odesa – 2017

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

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:

Г.В. Ахмаметєва

Редакційна колегія:

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,
А.Ф. Верлань, Г.М. Востров, В.Б. Дудикевич,
Л.Є. Євтушик, М.Б. Копитчук, С.В. Ленков,
І.І. Маракова, А.Д. Мілка, С.А. Нестеренко,
М.С. Никитченко, С.А. Положаєнко,
О.В. Рибальський, Х.М.М. Рубіо, В.Д. Русов,
І.М. Ткаченко-Горський, А.В. Усов,
В.О. Хорошко, М.Є. Шелест, М.С. Яджак*

Published 4 times a year

Founded by Odessa National Polytechnic
University in 2011

Certificate of State Registration

КВ № 17610 - 6460Р of 04.04.2011

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

Associate editor:

A.A. Kobozeva

Executive editor:

A.V. Akhmametieva

Editorial Board:

*T. Banakh, P. Bidyuk, V. Dudykevich,
L. Evtushik, V. Khoroshko, N. Kopytchuk,
S. Lenkov, I. Marakova, A. Milka, S. Nesterenko,
N. Nikitchenko, S. Polozhaenko, J. Rubio,
V. Rusov, O. Rybalsky, M. Shelest,
I. Tkachenko Gorski, A. Usov, N. Vaysfeld,
A. Verlan, G. Vostrov, 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: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

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

Tel.: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

© **Одеський національний політехнічний університет, 2017**

ЗМІСТ / CONTENTS

АЛГОРИТМІЗАЦІЯ МЕТОДІВ
ТОЧНОСТНОЇ ПАРАМЕТРИЧНОЇ
РЕДУКЦІЇ МАТЕМАТИЧНИХ
МОДЕЛЕЙ

А.Ф. Верлань, А.А. Верлань,
С.А. Положаєнко

7

ALGORITHMIZATION OF THE
METHODS OF THE ACCURATE
PARAMETRIC REDUCTION OF
MATHEMATICAL MODELS

Verlan A.F., Verlan A.A.,
Polozhaenko S.

УДОСКОНАЛЕННЯ
СТЕГАНОГРАФІЧНОГО
АЛГОРИТМУ, ЗАСНОВАНОГО НА
SIGN-НЕЧУТЛИВОСТІ
СИНГУЛЯРНИХ ВЕКТОРІВ БЛОКІВ
МАТРИЦІ ЗОБРАЖЕННЯ

А.А. Кобозєва, В.А. Мокріцький,
Л.Е.М. Батієне, І.І. Бобок

19

IMPROVEMENT OF THE
STEGANOGRAPHY ALGORITHM
BASED ON THE SIGN-
INSENSITIVITY OF THE SINGULAR
VECTORS OF BLOCKS OF THE
DIGITAL IMAGE MATRIX

Kobozeva A., Mokritsky V.,
Batiene L.E.M., Bobok I.

ЕКСПЕРИМЕНТАЛЬНЕ
ДОСЛІДЖЕННЯ ПРОГРАМНОЇ
РЕАЛІЗАЦІЇ СУМІСНОГО
ВИКОНАННЯ АЛГОРИТМУ
ЕВКЛІДА ТА МНОЖЕННЯ

М.М. Касянчук, І.З. Якименко,
І.Р. Паздрій, С.В. Івасьєв

29

EXPERIMENTAL STUDY OF
SOFTWARE IMPLEMENTATION OF
COMBINE REALIZATION OF THE
EUCLID ALGORITHM AND
MULTIPLICATION

Kasianchuk M., Yakymenko I.,
Pazdriy I., Ivasiev S.

ПРОБЛЕМНІ АСПЕКТИ
ДЕПЕРСОНАЛІЗАЦІЇ ЦИФРОВИХ
ЗОБРАЖЕНЬ

О.В. Задерейко, О.В. Троянський,
Н.І. Логінова, О.Г. Трофименко

37

PROBLEMATIC ASPECTS OF
DEPERSONALIZATION DIGITAL
IMAGES

Zadereyko O., Troyanskiy A.,
Loginova N., Trofimenko E.

НЕЧІТКА СИСТЕМА
ДІАГНОСТУВАННЯ
ПАТОЛОГІЧНИХ СТАНІВ
МОЛОЧНОЇ ЗАЛОЗИ НА ОСНОВІ
ГІСТОЛОГІЧНИХ ЗОБРАЖЕНЬ
Л.О. Дубчак, С.О. Вербовий,
Н.А. Максимів, Т.В. Дацко

47

FUZZY SYSTEM DIAGNOSING OF
PATOLOGY CONDITIONS OF THE
BREAST BASED ON
HISTOLOGICAL IMAGES
Dubchak L., Verbovyy S.,
Maksymiv N., Datsko T.

СИНТЕЗ І МОДЕЛЮВАННЯ
РЕГУЛЯТОРА ДЛЯ ОБ'ЄКТА ЗІ
ЗМІННИМИ ПАРАМЕТРАМИ
С.О. Бобріков, Е.Д. Пічугин,
С.І. Кисса

54

SYNTHESIS AND MODELING OF
THE REGULATOR FOR THE
OBJECT WITH CHANGING
PARAMETERS
Bobrykov S., Pichugin E., Kissa S.

ЗАСТОСУВАННЯ
ІНСТРУМЕНТАЛЬНОГО ЗАСОБУ
ЕКСПЕРТИЗИ ЦИФРОВИХ
ФОНОГРАМ І АПАРАТУРИ
ЦИФРОВОГО ЗВУКОЗАПИСУ
«ФРАКТАЛ» ДЛЯ ПРОВЕДЕННЯ
ЕКСПЕРТИЗ АНАЛОГОВИХ
ФОНОГРАМ ТА АНАЛОГОВОЇ
АПАРАТУРИ МАГНІТНОГО
ЗАПИСУ
О.В. Рибальський, В.І. Соловійов,
В.В. Журавель

63

APPLICATION OF TOOL OF
EXAMINATION OF DIGITAL
PHONOGRAMS AND APPARATUS
OF DIGITAL AUDIO RECORDING
«FRACTAL» FOR REALIZATION OF
EXAMINATIONS OF ANALOG
PHONOGRAMS AND ANALOG
APPARATUS OF MAGNETIC
RECORD
Rybalskiy O., Solovyov V., Zhuravel V.

МОДЕЛІ РОЗПОДІЛЕНИХ СИСТЕМ
ІЗ ЗАПІЗНЮЮЧИМ АРГУМЕНТОМ
С.А. Положаєнко

74

MODELS OF DISTRIBUTED
SYSTEMS WITH DELAYED
ARGUMENT
Polozhaenko S.

РОЗРОБКА ІНТЕРФЕЙСУ
АДМІНІСТРАТОРА В СИСТЕМІ
УПРАВЛІННЯ САЛОНОМ КРАСИ
О.Ю. Лебедева, Т.О. Бирченко

81

DEVELOPMENT OF THE
ADMINISTRATOR INTERFACE IN
THE BEAUTY SALON
MANAGEMENT SYSTEM
Lebedeva E., Byrchenko T.

АНАЛІЗ ЧАСОВИХ РЯДІВ
СПОЖИВАННЯ ПАЛИВА
МАНЕВРОВИМ ТЕПЛОВОЗОМ В
ЕКСПЛУАТАЦІЇ
Ю.Є. Калабухін, О.В. Рудковський

87

RESULTS ANALYSIS OF TIME
SERIES FUEL CONSUMPTION OF
USE SHUNTING LOKOMOTIVE
Kalabukhin Y., Rudkovskiy O.

ПОРІВНЯЛЬНИЙ АНАЛІЗ
ЕФЕКТИВНОСТІ
СТЕГАНОАНАЛІТИЧНИХ
АЛГОРИТМІВ ВИЯВЛЕННЯ
НАЯВНОСТІ ВКЛАДЕНЬ
КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У
ЦИФРОВИХ ВІДЕО
Г.В. Ахмаметьєва, А.О. Єфименко

96 COMPARATIVE EFFICIENCY
ANALYSIS OF STEGANALYTIC
ALGORITHMS FOR DETECTING
THE PRESENCE OF ATTACHMENTS
OF CONFIDENTIAL INFORMATION
IN DIGITAL VIDEO
Akhmametieva A., Efimenko A.

НЕЧІТКА МОДЕЛЬ ФОРМУВАННЯ
ІНДИВІДУАЛЬНОЇ ТРАЄКТОРІЇ
НАВЧАННЯ ТА ПОБУДОВА
ОНТОЛОГІЇ НА ЇЇ ОСНОВІ
Т.В. Лендюк, Н.М. Васильків

103 FUZZY MODEL OF INDIVIDUAL
LEARNING PATH FORMING AND
ONTOLOGY DESIGN ON ITS BASIS
Lendyuk T., Vasylykiv N.

МОЖЛИВІСТЬ ОТРИМАННЯ
ФУНКЦІОНАЛЬНИХ
ЗАЛЕЖНОСТЕЙ ЧЕРЕЗ
СТРУКТУРУ БАЗИ ДАНИХ
С.І. Гришин, Л.М. Тимошенко

113 POSSIBILITY OF OBTAINING
FUNCTIONAL DEPENDENCES
FROM DATABASE STRUCTURE
Grishin S., Timoshenko L.

ДОСЛІДЖЕННЯ ОПТИМАЛЬНОГО
КОЕФІЦІЄНТУ ВИТРАТ НА
ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ
ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ
ДІЯЛЬНОСТІ
М.Г. Романюков

119 INVESTIGATION OF OPTIMUM
FLOW COEFFICIENTS TECHNICAL
INFORMATION PROTECTION OF
OBJECT INFORMATION
Romanyukov N.

СИСТЕМА ПІДТРИМКИ
ПРИЙНЯТТЯ РІШЕНЬ ПРИ
ПЛАНУВАННІ ТА
ДИСТАНЦІЙНОМУ КЕРУВАННІ
РУХОМ МОБІЛЬНИХ ОБ'ЄКТІВ
Ю.О. Гунченко, І.В. Ковалець,
С.А. Шворов, Д.С. Комарчук,
В.Є. Лукін

127 DECISION SUPPORT SYSTEM IN
PLANNING AND REMOTE
CONTROL OF MOVEMENT MOBILE
OBJECTS
Gunchenko Yu., Kovalets I., Shvorov S.,
Komarchuk D., Lukin V.

ПОДАННЯ АЛГОРИТМУ
ВИЗНАЧЕННЯ ПОСЛІДОВНОСТІ
РОБІТ МЕРЕЖЕЮ ПЕТРІ
О. М. Тининика

135 SUBMISSION OF ALGORITHM FOR
WORKS SEQUENCES FINDING
WITH PETRI NET
Tynynyka A.

ВИЗНАЧЕННЯ ОЦІНКИ
СУМАРНОГО КОРЕЛЯЦІЙНОГО
ВЗАЄМОВПЛИВУ ПЕРІОДИЧНИХ
ПРОЦЕСІВ З БАГАТОКРАТНИМ
ПОВТОРЕННЯМ ТА
ПРЕДСТАВЛЕННЯМ В ПОЛЯРНІЙ
СИСТЕМІ КООРДИНАТ
А.І. Сегін

139

DETERMINATION THE
GENERALIZED CORRELATION
ESTIMATE THE IMPACT OF
PERIODIC SIGNALS CONSIDERING
MULTIPLE REPETITION AND
REPRESENTATION IN POLAR
COORDINATES
Segin A.

РОЗРОБКА СИСТЕМИ ДЛЯ
ФОРМУВАННЯ ЗВІТНОСТІ ПРО
НАУКОВУ ТА МЕТОДИЧНУ
РОБОТУ КАФЕДРИ
О.Ю. Лебедева, Л.М. Тимошенко,
В.М. Семенченко

145

DEVELOPMENT OF A SYSTEM FOR
FORMING REPORTS ON THE
SCIENTIFIC AND METHODOICAL
WORK OF THE DEPARTMENT
Lebedeva E., Tymoshenko L.,
Semenchenko V.

АЛГОРИТМИЗАЦИЯ МЕТОДОВ ТОЧНОСТНОЙ ПАРАМЕТРИЧЕСКОЙ РЕДУКЦИИ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ

А.Ф. Верлань¹, А.А. Верлань², С.А. Положаенко³

¹ Институт проблем моделирования в энергетике,
ул. Генерала Наумова, 15, Киев, 03164, Украина; e-mail: afverl@gmail.com

² Норвежский университет науки и технологий,
NTNU Gjøvik, Teknologiveien 22, 2815 Gjøvik, Norway; e-mail: andriy.verlan@ntnu.no

³ Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sanp277@gmail.com

На основе излагаемого принципа параметрической редукции предложены подходы к алгоритмизации процессов упрощения математических моделей, а также группа операций, обеспечивающих конструирование и эффективную реализацию соответствующих алгоритмов посредством вычислительных экспериментов.

Ключевые слова: математическая модель, параметрическая редукция, мера погрешности, коэффициент согласованности, вычислительная сложность, неустраняемая погрешность, алгоритм параметрической редукции

Введение

Задача редукции (упрощения) модели ставится как задача минимизации некоторой меры отклонения выходов исходной и упрощенной моделей [1, 2]. При этом, как правило, предполагается, что параметры исходной модели известны точно. Естественно, на практике это обстоятельство не имеет места, в связи с чем вопрос упрощения математических моделей может ставиться как вопрос согласования вида модели с точностными характеристиками исходных данных. Вполне понятно, что не имеет смысла использовать сложные в структурном отношении модели, если их параметры известны с достаточно большой погрешностью. Это обстоятельство обуславливает необходимость согласования таких характеристик моделей, как сложность и точность исходных данных. Несмотря на то, что такая постановка задачи упрощения моделей известна давно, являясь следствием техники приближенных вычислений (см., например, [3, 4, 5]), определение конструктивных путей ее решения имеет важное значение при исследовании сложных объектов и, в частности, при разработке алгоритмического и программного обеспечения вычислительно-управляющих систем различного назначения.

Достаточно общая постановка задачи редукции математических моделей на основе идеи согласования вида модели с точностью исходных данных дана в работе [5], где она формулируется как задача минимизации функционала сложности на классе моделей, формально сопоставимых по точности с наблюдениями (исходными данными). Класс формально сопоставимых моделей определяется ограничением типа неравенства на меру точности. В рамках указанной общей постановки задачи упрощения математических моделей может быть сформулирован ряд частных постановок, одна из которых – точностная параметрическая редукция моделей, и основные подходы к ее решению рассматриваются далее.

Цель работы

Целью работы является получение условий допустимого параметрического упрощения математических моделей исследуемых явлений (точностной параметрической редукции) и разработка алгоритмов решения задачи параметрической редукции в пространстве параметров моделей.

Основная часть

Пусть задано некоторое математическое описание (модель) M моделируемого явления, а исходные данные (обычно это числовые значения параметров) заданы с некоторой погрешностью, мерой которой служит ε_p . Если ε_p велико, то исходное математическое описание M может быть заменено некоторым другим описанием M' (в том числе более простым) с учетом ε_{yp} – меры погрешности выходных переменных исходной модели, обусловленной неточностью исходных данных, т.е. наличием ε_p . Предположим, что $\varepsilon_p = 0$, тогда замена исходного описания каким-либо другим (в том числе более простым) приведет к появлению погрешности приближения $\varepsilon_{yM} \neq 0$. В этом случае вопрос о применимости упрощенной модели должен решаться на основе анализа требований к точности моделирования исследуемого явления. Иначе говоря, применение упрощенной модели допустимо, если $\varepsilon_{yM} \leq \varepsilon_z$, где ε_z – заданное значение меры погрешности моделирования. Если же имеет место строгое неравенство $\varepsilon_{yM} < \varepsilon_z$, то это свидетельствует о возможности дальнейшего упрощения исходной модели.

В общем случае применимость математической модели M или M' определяется условием

$$\varepsilon_{yM} + \varepsilon_{yp} \leq \varepsilon_z. \quad (1)$$

Здесь ε_{yM} – либо мера погрешности описания исследуемого явления моделью M , либо мера погрешности, обусловленной заменой заданной модели M на какую-либо другую M' (в том числе более простую). В дальнейшем под ε_{yM} будет пониматься именно мера погрешности, обусловленной заменой исходной заданной модели более простой.

В качестве характеристики согласованности с погрешностью исходных данных математической модели M' , заменяющей модель M , примем величину

$$\alpha = \varepsilon_{yM} / \varepsilon_{yp}, \quad (2)$$

которую будем называть коэффициентом согласованности. При этом условие применимости (1) модели M' приобретает вид

$$(\alpha + 1)\varepsilon_{yp} \leq \varepsilon_z \quad (3)$$

и модель M' является α -согласованной с погрешностью исходных данных ε_p модели M , если $\varepsilon_{yM} = \alpha\varepsilon_{yp}$ и $\alpha > 0$.

Задача согласования модели M с точностью исходных данных означает получение модели M' с определенным значением коэффициента согласованности. Исходя из практических соображений (например, при решении инженерных задач), в качестве ограничения снизу может быть принято значение $\alpha = 0.01$, так как

дальнейшее уменьшение коэффициента согласованности, означающее использование моделей, мало отличающихся от исходной, не приведет к заметному выигрышу в точности моделирования. С другой стороны, если $\alpha > 10$, то общая погрешность моделирования почти целиком будет определяться ε_{yM} , причем в этом случае при моделировании сложных объектов удовлетворительные значения ε_{yM} практически невозможны. Таким образом, коэффициент согласованности математических моделей практически можно ограничить интервалом $(0.01, 10)$.

При решении конкретных задач максимальное значение коэффициента согласованности определяется условием применимости (3) как

$$\alpha_{\max} = \varepsilon_3 / \varepsilon_{yp} - 1. \quad (4)$$

Пусть теперь N_M – мера вычислительной сложности математической модели M (для динамических объектов, описываемых, например, обыкновенными дифференциальными уравнениями в нормальной форме, в качестве N_M может быть принято число приведенных к одному типу операций, необходимых для вычисления правой части), а μ_α – множество математических моделей, коэффициент согласованности которых с погрешностью исходных данных не превосходит α .

Если $\alpha < \alpha_{\max}$, то все модели из μ_α эквивалентны в смысле применимости, так как для любой модели выполняется условие применимости (3). В то же время, модели из μ_α могут быть не эквивалентными в смысле вычислительной сложности. Именно при этом условии и появляется возможность упрощения заданной модели M путем замены ее на модель $M' \in \mu_\alpha$, для которой мера сложности $N_{M'} < N_M$.

Математическая модель M'_0 будет оптимально упрощенной, если

$$N_{M'_0} = \min_{M' \in \mu_\alpha} N_{M'}. \quad (5)$$

Очевидно, что мера вычислительной сложности $N_{M'}$ является убывающей функцией от коэффициента согласованности. Следовательно, коэффициент согласованности оптимальной упрощенной модели M'_0 превосходит α .

Построение α -согласованных, а также оптимальных упрощенных моделей преследует двоякую цель. С одной стороны – это обоснование тех или иных допущений, позволяющих упростить модель, с другой – снижение требований к быстродействию системы, реализующей модель. Практическое же решение рассматриваемой задачи сталкивается со значительными трудностями, обусловленными в основном сложностью задачи оценки величин ε_{yM} , ε_{yp} , а также трудностями формализации множества μ_α .

Реальным путем преодоления трудностей является использование параметрического подхода к построению упрощенных моделей. Сущность его заключается в замене значений определенных параметров исходной модели M на такие значения, которые уменьшают значение меры вычислительной сложности. Обычно это замена заданных значений некоторых параметров исходной модели на нулевые (как для аддитивных, так и для мультипликативных параметров) или/и единичные (для мультипликативных параметров). Такого рода параметрическое упрощение целесообразно применять в тех случаях, когда математические модели исследуемых процессов или явлений содержат достаточно большое количество параметров, значения которых определяются по экспериментальным данным. К таким

моделям могут быть отнесены модели в виде систем линейных и нелинейных алгебраических уравнений большой размерности, систем дифференциальных уравнений (как в обыкновенных, так и в частных производных) с коэффициентами, являющимися сложными функциями входных и выходных переменных, интегральных уравнений с ядрами, вид которых определяется реальными характеристиками исследуемых объектов и др.

Теоретическое обоснование возможности параметрического упрощения математических моделей для построения α -согласованных и оптимальных упрощенных моделей базируется на результатах теории точности применительно к анализу неустранимой погрешности.

Пусть $M(y, V, \rho)$ – математическая модель; y, V, ρ – векторы выходных, входных переменных и параметров соответственно, принадлежащих нормированным пространствам с метриками ρ_y, ρ_V, ρ_p , определяемыми соответствующими нормами; N_p – мера вычислительной сложности.

Пусть ρ_0 – неизвестный вектор точных значений параметров модели, а ρ_3 – вектор заданных значений параметров. При этом известно, что

$$\rho_p(\rho_3, \rho_0) \leq \varepsilon_p. \quad (6)$$

Условие (6) определяет множество Ω_p такое, что из $\rho \in \Omega_p$ следует $\rho_p(\rho_3, \rho) \leq \varepsilon_p$. Тем самым определено множество μ возможных моделей

$$\mu = \{M(y, V, \rho) : \rho \in \Omega_p, \rho_p(\rho_3, \rho) \leq \varepsilon_p\},$$

причем модель $M(y, V, \rho)$ представляет собой исходное математическое описание.

Пусть, далее, $\rho_y(\rho_3, \rho)$ – мера погрешности в пространстве выходных переменных, обусловленная неточностью задания вектора ρ_3 , $\rho_y(\rho_3, \rho)$ – мера погрешности, обусловленная заменой заданной модели $M(y, V, \rho_3)$ на некоторую, в частности, более простую модель $M(y, V, \rho_r)$; т.е. $\rho_y(\rho_3, \rho)$ – мера погрешности, характеризующая отличие точной модели $M(y, V, \rho_0)$ от модели $M(y, V, \rho_r)$.

Для указанных погрешностей могут быть определены оценки

$$\rho_y(\rho_3, \rho) / \rho \in \Omega_p, V \in \Omega_p \leq \varepsilon_{yp}, \quad (7)$$

$$\rho_y(\rho_3, \rho_r) / V \in \Omega_v \leq \varepsilon_{yM}, \quad (8)$$

$$\rho_y(\rho_0, \rho_r) / V \in \Omega_v \leq \varepsilon_{yr} \quad (9)$$

(Ω_v – область возможных значений входных переменных), а неравенство треугольника определяет связь между ними:

$$\varepsilon_{yr} \leq \varepsilon_{yM} + \varepsilon_{yp} = (\alpha + 1)\varepsilon_{yp}, \quad (10)$$

причем, $\varepsilon_{yr} \leq \varepsilon_{yM}$. Если $\rho_r \in \Omega_p$, то $\varepsilon_{yM} \leq \varepsilon_{yr}$ и, следовательно, множество μ возможных моделей представляет собой множество α -согласованных моделей при $\alpha=1$, т.е. $\mu = \mu_1$. Однако применение параметрического подхода для поиска

упрощенных моделей в множестве μ имеет ограниченные возможности. Действительно, множество Ω_ρ , как правило, не содержит точек, принадлежащих координатным осям, в связи с чем при таком упрощении моделей можно рассчитывать лишь на сокращение числа значащих цифр в представлении заданных параметров. Отметим, что такого рода упрощение находит применение в технике приближенных вычислений, а также может использоваться при организации вычислительных процессов в системах моделирования на этапе выбора вычислительных средств.

В общем случае, если $\rho_r \in \Omega_\rho$, то $\varepsilon_{yM} \leq \varepsilon_{yp}$ и, следовательно, коэффициент согласованности соответствующей модели будет больше единицы. Тем не менее существует принципиальная возможность определения множества α -согласованных моделей при $\alpha \leq 1$ и $\rho_r \notin \Omega_\rho$. Наличие такой возможности обусловлено тем, что погрешность в пространстве выходных переменных, вызванная неточностью задания вектора ρ_3 , оценивается в метрике ρ_y .

Неопределенность значений вектора параметров исходной модели (наличие Ω_ρ) приводит к неопределенности в значениях выходных переменных, количественной мерой которой служит ошибка

$$\Delta y = y(\rho, V) - y(\rho_3, V) / V \in \Omega_{\Delta y}. \quad (11)$$

Область $\Omega_{\Delta y}$ возможных значений ошибки Δy имеет сложную конфигурацию в пространстве выходных переменных, зависящую от вида Ω_ρ , свойств математического описания $M(y, V, \rho)$, и определяется уравнением для неустранимой погрешности. Детальная характеристика $\Omega_{\Delta y}$ методами анализа неустранимой погрешности, развитыми в теории точности, может быть получена лишь для простейших задач. Обычно же область принадлежности ошибки характеризуется некоторым шаром S (в заданной метрике ρ_y), радиус которого (в данном случае ε_{yp}) определяется на основе оценки сверху (7) для соответствующей метрике ρ_y нормы. Вследствие грубости применяемых оценок имеет место соотношение: $S \supset \Omega_{\Delta y}$. Шару S в пространстве выходных переменных соответствует область Ω'_ρ в пространстве параметров такая, что из $\Omega'_\rho \supset \Omega_\rho$ и $\rho \in \Omega'_\rho$ следует $\rho_y(\rho_3, \rho) \leq \varepsilon_{yp}$. Следовательно, если $\rho_r \in \Omega'_\rho$, то $\varepsilon_{yM} \leq \varepsilon_{yp}$ и соответствующее множеству Ω'_ρ множество μ' возможных моделей является множеством согласованных моделей при $\alpha = 1$.

Из-за наличия включения Ω'_ρ применение параметрического подхода к упрощению исходного описания в классе моделей μ' имеет большие возможности по сравнению с классом μ . Объясняется это тем, что для сложных задач с большим числом параметров, задаваемых с не очень высокой точностью, область Ω'_ρ содержит точки, принадлежащие координатным осям пространства параметров. Следовательно, в качестве вектора ρ_r может быть выбран вектор с некоторыми нулевыми компонентами, чем и достигается уменьшение значения меры вычислительной сложности N_{pr} .

В общем случае Ω'_ρ может не пересекаться с координатными осями, однако и при этих условиях, как это можно показать, существует множество $\Omega'_\rho(\alpha) = \{\rho : \rho_y(\rho_3, \rho) \leq \alpha \varepsilon_{yp}, \alpha > 1\}$, содержащее точки координатных осей и определяющее множество моделей μ'_α , согласованных с погрешностью исходных

данных с коэффициентом согласованности $\alpha > 1$. Действительно, пусть $\Omega'_p(\beta) = \{\rho : \rho_p(\rho_3, \rho) \leq \rho \varepsilon_p\}$. Ясно, что $\Omega_p(1) = \Omega_p$ и существует такое значение $\beta_0 = 1$, что при $\beta > \beta_0$ шар $\Omega_p(\beta)$ пересекается, по крайней мере, с одной из координатных осей пространства параметров. Множество $\Omega_p(\beta)$ определяет некоторую область возможных значений ошибок выходных переменных $\Omega_{\Delta y}(\beta)$, которая в метрике ρ_y оценивается шаром S_α радиуса $\alpha(\beta)\varepsilon_{yp}$, т.е.

$$\rho_y(\rho_3, \rho) / \rho \in \Omega'_p(\beta) \leq \alpha(\beta)\varepsilon_{yp}. \quad (12)$$

Здесь $\alpha(\beta)$ – неотрицательная неубывающая функция, причем $\alpha(1) = 1$, т.е. будем считать, что функция $\alpha(\beta)$ – возрастающая и ограниченная. Первое допущение означает, что с ростом погрешности исходных данных погрешность выходных переменных растет (для практических задач можно считать это условие выполняющимся). Второе условие означает корректность всех моделей с параметрами из $\Omega_p(\beta)$, что является ограничением применимости параметрического подхода к упрощению моделей.

Пусть теперь $\Omega'_p(\alpha) = \{\rho : \rho_y(\rho_3, \rho) \leq \alpha(\beta)\varepsilon_{yp}\}$ – прообраз в пространстве параметров шара S_α . Так как $\Omega'(\alpha) \supset \Omega(\beta)$, то множество $\Omega'_p(\alpha)$ также пересекается по крайней мере с одной из координатных осей, что и требовалось показать. Это свидетельствует о следующем: для любого $\Omega_p = \{\rho : \rho_p(\rho_3, \rho) \leq \varepsilon_p, \varepsilon_p > 0\}$ существует $\alpha_0 > 0$ такое, что при $\alpha > \alpha_0$ в множестве μ_α α -согласованных с погрешностью исходных данных корректных моделей $M(y, V, \rho)$, определяемом множеством параметров $\Omega_p(\alpha) = \{\rho : \rho_y(\rho_3, \rho) \leq \alpha \varepsilon_{yp}\}$, содержится непустое подмножество $\bar{\mu}_\alpha$ моделей $M(y, V, \bar{\rho})$, для которых $N_{\bar{p}} < N_p / \rho \in \Omega_p$.

Данный вывод является теоретическим обоснованием возможности применения параметрического подхода к построению упрощенных математических моделей на основе согласования вида модели с точностью исходных данных. А устанавливаемый факт существования α -согласованных моделей с меньшим значением меры вычислительной сложности, чем исходная модель, составляет сущность принципа точностной параметрической редукции математических моделей, который может быть сформулирован следующим образом.

Для любой модели с неточно заданными параметрами при условии, что погрешность выходных переменных является возрастающей и ограниченной функцией от погрешности параметров, существует более простая α -согласованная модель, отличающаяся от исходной значениями некоторых параметров, уменьшающими меру вычислительной сложности.

Естественно, что пригодность параметрически упрощенных моделей, получаемых в результате точностной параметрической редукции, определяется условием (3), так что практический интерес представляет получение более простых, чем исходное, математических описаний с не очень большим значением коэффициента согласованности. Поэтому желательно уметь достаточно просто априори оценивать коэффициент согласованности параметрически упрощаемых моделей.

Оценка неустранимой погрешности в рамках линейной теории точности для широкого класса задач (математические описания которых представляют собой упрощаемые модели) приводит к линейной форме зависимости ε_{yp} от ε_p , т.е.

$$\varepsilon_{yp} = C_M \varepsilon_p, \quad (13)$$

где C_M – константа, определяемая свойствами задачи (для корректных задач – норма обратного оператора линейных уравнений неустраняемой погрешности).

В этом случае нетрудно получить гарантированную оценку сверху для значения α_0 коэффициента согласованности моделей, которые могут быть получены в результате точностной параметрической редукции, т.е. для минимального значения α_0 коэффициента согласованности параметрически упрощенной модели $M(y, V, \bar{\rho})$ справедлива оценка

$$\alpha_0 \leq \frac{\min_{i=1, m} \rho_p(\rho_3, \wp_i)}{\varepsilon \rho} = \alpha_b, \quad (14)$$

где $\wp_i, i = \overline{1, m}$ – координатные оси в пространстве параметров.

Условие (13) означает, что функция $\alpha(\beta)$ имеет вид $\alpha(\beta) = \beta$. Значение β_0 определяется из условия, что шар $\Omega_\rho(\beta)$ радиуса $\beta_0 \varepsilon_p$ касается ближайшей из координатных осей пространства $\wp_i, i = \overline{1, m}$ параметров, т.е.

$$\beta_0 \leq \frac{\min_{i=1, m} \rho_p(\rho_3, \wp_i)}{\varepsilon \rho},$$

или из включения $\Omega'(\alpha(\beta_0)) \supset \Omega(\beta_0)$ следует $\alpha_0 \leq \beta_0$.

Оценка (14) является, по существу, критерием применимости точностной параметрической редукции математических моделей. Так большие значения α_b (порядка десятков) свидетельствуют о нецелесообразности параметрического упрощения моделей и наоборот, малые значения α_b (порядка единиц) означают допустимость применения точностной параметрической редукции для построения приемлемых упрощенных моделей.

Рассмотрим кратко сущность основных подходов к построению алгоритмов точностной параметрической редукции.

1. Алгоритмы построения области $\Omega'(\alpha)$. Строятся на основе непосредственного определения прообраза в пространстве параметров шара S_α , оценивающего в пространстве выходных переменных область возможных значений ошибок. Алгоритмы требуют знания оценок $\varepsilon_{yM}, \varepsilon_{yM}$ и выполнения преобразования шара S_α радиуса $\alpha \varepsilon_{yp}$ в область $\Omega'(\alpha)$.

2. Алгоритмы параметрической редукции в пространстве параметров. Строятся на основе определения эквивалентного вектора параметров $\rho_s \in \Omega(\alpha)$ такого, что реакция редуцированной модели с априори задаваемым вектором параметров ρ_r отличается от реакции исходной модели с вектором параметров ρ_s на величину, которой можно пренебречь по сравнению с ε_{yM} . Алгоритмы требуют знания оценки ε_{yM} и решения задачи минимизации величины $\rho_y(\rho, \rho_r)$ по ρ при условии $\rho \in \Omega(\alpha)$.

3. Алгоритмы параметрической редукции в пространстве выходных переменных. Сущность алгоритмов этой группы состоит в оценивании принадлежности

ошибки редуцированной модели области $\Omega_{\Delta y}$ (или некоторой ее оценки) возможных значений ошибок выходных переменных исходной модели. Алгоритмы требуют построения оценки области $\Omega_{\Delta y}$ и определения ошибки (или ее оценки) редуцированной модели.

При разработке любого алгоритма из указанных групп возникает необходимость решения ряда частных задач, определяющих их вычислительную сложность и практическую применимость.

Для алгоритмов первой группы наиболее сложным в вычислительном отношении является преобразование S_{α} в $\Omega'_{\rho}(\alpha)$. Практическая применимость алгоритмов ограничивается простыми задачами, для которых возможно получение явных аналитических описаний области $\Omega_{\Delta y}$.

Для алгоритмов второй группы наиболее сложным этапом является поиск $\min \rho_y(\rho, \rho_r)$. Практическое применение алгоритмов возможно в случаях, когда могут быть получены в явном виде уравнения для неустранимой погрешности Δy .

Применимость алгоритмов третьей группы определяется возможностью построения оценок области $\Omega_{\Delta y}$.

Существенное влияние на сложность алгоритмов точностной параметрической редукции моделей оказывает решение и таких вопросов, как оценка ε_{yM} (для алгоритмов первой и третьей групп), назначение или определение ρ_r (для алгоритмов второй и третьей групп).

При оценке ε_{yM} преодоление вычислительной сложности достигается путем анализа ε_{yM} в одной точке пространства выходных переменных, соответствующей выбранному режиму моделирования, обладающему экстремальными свойствами.

При оценке реальным путем является использование линейной теории точности, дающей возможность практически оценивать меру погрешности выходных координат модели, обусловленной неточностью задания вектора параметров. При этом может использоваться либо аппарат теории чувствительности, либо организовываться определение частных вкладов в общую погрешность ошибок компонент вектора параметров с последующим их суммированием [4, 5].

Значение функций чувствительности или частных вкладов ошибок компонент вектора параметров позволяет решать задачу назначения или определения ρ_r путем ранжирования компонент вектора ρ_3 по чувствительности или по частному вкладу.

Для алгоритмов второй группы необходимо априори назначать ρ_r . Практическая реализация этой процедуры основывается как на предшествующем опыте исследования моделируемых процессов, так и на априорном анализе значимости отдельных параметров.

Детальный анализ свойств алгоритмов точностной параметрической редукции проведем лишь для алгоритмов второй группы. Структура алгоритмов редукции в пространстве параметров в общем случае определяется совокупностью следующих основных блоков.

1. Определение y_3 – реакции исходной модели с параметрами ρ_3 на выбранном режиме моделирования.

2. Назначение вектора параметров ρ_r такого, что $N_{pr} < N_{p3}$, т.е. априорный выбор редуцированной модели.

3. Определение y_r – реакции редуцированной модели на выбранном режиме моделирования.

4. Определение вектора параметров ρ_r при условии $\|y_r - y_r\| \ll \|y_3 - y_r\|$, где y_3 – реакция исходной модели с параметрами на режиме моделирования.
5. Оценка выполнения условия $\rho_r \in \Omega(\alpha)$, что эквивалентно оценке коэффициента согласованности α при условии малости Ω_{ρ} .

6. Анализ результатов редукции – если результаты удовлетворительны, то «конец», иначе возврат ко второму блоку.

Рассмотрим представленные основные блоки алгоритма точностной параметрической редукции в пространстве параметров с точки зрения их практической реализации.

Первый блок. Практическая реализация зависит от вида модели и сводится к применению соответствующих численных методов анализа.

Второй блок. Основная трудность реализации заключается в отсутствии формализованных приемов определения значений ρ_r .

Использование предшествующего исследовательского опыта позволяет определить варианты структурной редукции исходных математических моделей, сводящиеся, как правило, к замене каких-либо функциональных зависимостей их линейными членами разложения в степенной ряд. Например, применительно к уравнениям динамики полета самолета подобные варианты структурной редукции часто заключаются в замене отдельных тригонометрических функций линейными членами в предположении малости соответствующих величин [6, 7, 8]. В этих случаях решение задачи точностной параметрической редукции дает возможность обосновать допустимость тех или иных структурных упрощений.

Априорный анализ значимости параметров основывается на сравнении порядка величин аддитивных составляющих, входящих в уравнения динамики. Выявленные при таком анализе члены, вклад которых в значение некоторой величины достаточно мал по сравнению с другими членами, образующими ту же величину, определяют соответствующие им коэффициенты, которые могут претендовать на роль незначимых.

Осуществленный каким-либо образом выбор подозреваемых на незначимость параметров определяет и выбор вектора ρ_r априори редуцированной модели. Следует, однако, отметить, что выбор конкретного значения ρ_r неоднозначен, так как формирование ρ_r может осуществляться с помощью любого подмножества априорного множества подозреваемых на незначимость параметров. С практической точки зрения привлекательной является «максималистская» стратегия формирования ρ_r , в результате чего ρ_r назначается с учетом всего априорного множества подозреваемых на незначимость параметров.

Третий блок. Реализуется аналогично первому блоку.

Четвертый блок. Наиболее сложный в вычислительном отношении, так как представляет собой решение задачи восстановления параметров модели $M(y, V, \rho)$. В общем случае реализация блока основывается на использовании алгоритмов минимизации отклонения реакции y_r редуцированной модели на выбранном режиме моделирования от реакции y_3 на том же режиме исходной модели путем варьирования параметров последней.

Для динамических объектов в математическом плане задача часто может быть сведена к решению нелинейных алгебраических уравнений

$$f(y, V, \rho) = 0, \quad (15)$$

вид которых определяется типом модели относительно неизвестных ρ при условии, что $y = y_r$, $V = V_0$ и $\rho \in \Omega(\alpha)$. Последнее условие является принципиальным, так как в

силу самой постановки задачи решение системы (15) существует, единственно и равно $\rho \in \Omega(\alpha)$. Таким образом, видно, что речь идет не просто о восстановлении параметров, а о приближении решения y_r редуцированной системы решением исходной системы при допустимых значениях ее параметров. Иначе говоря, вопрос ставится об эквивалентной замене влияния на точность моделирования подозреваемых на незначимость параметров влиянием допустимых отклонений параметров исходной модели. Именно это обстоятельство обуславливает вычислительную сложность данного блока алгоритма решения задачи параметрической редукции в пространстве параметров.

В предположении малости отклонений $\Delta\rho$ от заданного значения вектора параметров ρ_3 исходной модели уравнение относительно ошибки Δy имеет вид

$$f_y \Delta y + f_p \Delta \rho + \varphi = 0, \quad (16)$$

где f_y , f_p – матрицы Якоби вектор-функции $f(y, V, \rho)$ по соответствующим аргументам, φ – известная функция.

Если $\Delta y_r = y_3 - y_r$ мало, то искомый вектор приращений должен удовлетворять системе

$$f_y \Delta y_r + f_p \Delta \rho + \varphi = 0 \quad (17)$$

и при условии максимальности ранга матрицы f_p , что на практике обычно и бывает, может быть определен из (17) как

$$\Delta \rho = -(f_p^T f_p)^{-1} f_p^T (f_y \Delta y_r + \varphi) = 0, \quad (18)$$

где f_p^T обозначает транспонированную матрицу f_p .

Другой подход к решению задачи базируется на преобразовании заданного множества Ω_ρ в эквивалентное в смысле точности множество $\Omega_{\bar{\rho}}$, где $\bar{\rho}$ – усеченный вектор параметров исходной модели, компоненты которого выбираются с учетом априорной значимости параметров линейности системы (15) относительно $\bar{\rho}$, а также минимальности размерности. При выборе $\bar{\rho}$ полезной может оказаться концепция фиктивных параметров и ряд других идей, используемых при организации контроля процессов моделирования с применением методов параметрической идентификации. Преобразование Ω_ρ в $\Omega_{\bar{\rho}}$ само по себе представляет достаточно сложную задачу, решение которой требует привлечения аппарата теории точности. Тем не менее, его применение может оказаться целесообразным, если данное преобразование выполнено по каким-либо другим причинам (например, в целях организации упоминавшегося выше контроля).

Пятый блок. Оценка выполнения условия $\rho_3 \in \Omega(\alpha)$ не представляет сложности и является очевидной, причем в случае линейной зависимости ε_{yp} от ε_p коэффициент согласованности определяется как

$$\alpha_r = \rho_p(\rho_3, \rho_r) / \varepsilon_p.$$

Шестой блок. Результатом выполнения предыдущих блоков являются значения вектора параметров ρ_r редуцированной модели и коэффициента согласованности α_r

ее с погрешностью исходных данных. Если обозначить нижнюю и верхнюю границы коэффициента согласованности как α_H и α_b , то задача считается решенной, когда $\alpha_H \leq \alpha_r \leq \alpha_b$. В противном случае осуществляется возврат ко второму блоку. При этом, если $\alpha_H < \alpha_r$, то формирование нового значения вектора параметров ρ_r должно осуществляться с увеличением числа априори незначимых параметров и наоборот, если $\alpha_r < \alpha_b$.

Выводы

Оценивая в целом практическую ценность алгоритмов решения задачи параметрической редукции в пространстве параметров, следует отметить, что узловым моментом, определяющим его применимость, является необходимость пересчета отклонений реакции редуцированной модели от реакции, заданной в области исходных данных. Трудоемкость этого процесса в основном и определяет вычислительную сложность алгоритмов.

Список литературы

1. Горбань, А.В. Об упрощении математических моделей сложных систем и о некоторых приложениях теории / А.В. Горбань // Кибернетика и вычислительная техника. — К.: Наукова думка, 1976. — Вып. 37. — С. 10–14.
2. Суздаль, В.С. Редукция модели при синтезе регуляторов для управления кристаллизацией / В.С. Суздаль, Ю.М. Елифанов // Восточно-Европейский журнал передовых технологий. — 2011. — Том 2. — Выпуск №3 (50). — С. 31–34.
3. Иванов, В.В. Методы вычислений на ЭВМ: Справочное пособие / В.В. Иванов. — К.: Наукова думка, 1986. — 584 с.
4. Opmeer, M.R. Model reduction for distributed parameter systems: A functional analytic view / M.R. Opmeer // Proceedings of the American Control Conference. — American Automatic Control Council, 2012. — P. 1418–1423.
5. Тихонов, А.Н. О математических методах автоматизации обработки наблюдений. Проблемы вычислительной математики / А.Н. Тихонов. — М.: Из-во Моск. ун-та, 1980. — С. 3-17.
6. Кваско, М.З. Числові методи комп'ютерного моделювання автоматичних систем. Алгоритми і програми: Навч. посібник. / М.З. Кваско, А.І. Кубрак, А.І. Жученко. — К.: Політехніка, 2003. — 360с.
7. Широкопояс, В.А. О возможности упрощения дифференциальных уравнений движения в задаче о максимальной скороподъемности самолета / В.А. Широкопояс // Ученые записки ЦАГИ. — Жуковский: ЦАГИ им. Н. Е. ЖУКОВСКОГО", 1980. — Вып. 1. — Т. XI. — 1980. — С.127-135.
8. Верлань, А.Ф. Вычислительные процессы в системах управления / А.Ф. Верлань, И.Е. Ефимов, А.В. Латышев. — Л.: Судостроение, 1981 — 248 с.

АЛГОРИТМІЗАЦІЯ МЕТОДІВ ТОЧНОСТНОЇ ПАРАМЕТРИЧНОЇ РЕДУКЦІЇ МАТЕМАТИЧНИХ МОДЕЛЕЙ

А.Ф. Верлань¹, А.А. Верлань², С.А. Положаенко³

¹Інститут проблем моделювання в енергетиці,
Вул. Генерала Наумова, 15, Київ, 03164, Україна; e-mail: afverl@gmail.com

²Норвезький університет науки та технологій,
NTNU Gjøvik, Teknologiveien 22, 2815 Gjøvik, Norway; e-mail: andriy.verlan@ntnu.no

³Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sanp277@gmail.com

На підставі викладеного принципу параметричної редукції запропоновано підходи до алгоритмізації процесів спрощення математичних моделей, а також група операцій, що забезпечує конструювання та ефективну реалізацію відповідних алгоритмів за допомогою обчислювальних експериментів

Ключові слова: математична модель, параметрична редукція, міра похибки, коефіцієнт узгодженості, обчислювальна складність, неліквідована похибка, алгоритм параметричної редукції

ALGORITHMIZATION OF THE METHODS OF THE ACCURATE PARAMETRIC REDUCTION OF MATHEMATICAL MODELS

A.F. Verlan¹, A.A. Verlan², S.A. Polozhaenko³

¹ Institute of Modeling Problems in Power Engineering,
General Naumova Str., 15, Kiev, 03164, Ukraine; e-mail: afverl@gmail.com

² Norwegian University of Science and Technology
NTNU Gjøvik, Teknologiveien 22, 2815 Gjøvik, Norway; e-mail: andriy.verlan@ntnu.no

³ Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: sanp277@gmail.com

On the basis of the presented parametric reduction principle, approaches are proposed to algorithm the processes of simplification of mathematical models, as well as a group of operations that ensure the construction and effective implementation of the corresponding algorithms through computational experiments.

Keywords: mathematical model, parametric reduction, measure of error, coherence coefficient, computational complexity, unrecoverable error, parametric reduction algorithm

УСОВЕРШЕНСТВОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА, ОСНОВАННОГО НА SIGN- НЕЧУВСТВИТЕЛЬНОСТИ СИНГУЛЯРНЫХ ВЕКТОРОВ БЛОКОВ МАТРИЦЫ ИЗОБРАЖЕНИЯ

А.А. Кобозева, В.А. Мокрицкий, Л.Е.М. Батиене, И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: kobozeva@opu.ua

В работе предложен способ обработки цифрового изображения, результатом которой является понижение числа обусловленности большинства блоков его матрицы, полученных путем стандартного разбиения, за счет предобуславливания соответствующих матриц. Обработка сохраняет надежность восприятия искаженного изображения, которая в работе количественно оценивается при помощи пикового отношения «сигнал-шум». Использование предложенного способа обработки в качестве предобработки изображения-контейнера перед стеганообразованием позволяет расширить область применимости устойчивого к атакам против встроенного сообщения, в том числе значительным, стеганографического алгоритма, основанного на sign-нечувствительности сингулярных векторов блоков матрицы цифрового изображения, соответствующих максимальным сингулярным числам, разработанного одним из авторов ранее. Предобуславливание матрицы блока происходит после его предварительного кодирования. Результатом предварительного кодирования являются 2 симметричные положительно определенные разреженные матрицы, которые ставятся в соответствие блоку изображения. Положительная определенность и разреженность полученных матриц дает возможность использовать в качестве предобуславливателя для них неполное разложение Холецкого. Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганографический алгоритм, цифровое изображение, предобуславливатель, неполное разложение Холецкого, число обусловленности

Введение

Развитие и совершенствование комплексной системы защиты информации сегодня невозможно без наличия в ее составе эффективной стеганографической системы. Современная стеганография переживает этап своего бурного развития, при этом требования, выдвигаемые к стеганографическим алгоритмам, используемым при организации скрытого канала связи, становятся все более жесткими: обеспечение надежности восприятия формируемого стеганосообщения (СС), устойчивость к атакам против встроенного сообщения, устойчивость к стеганоанализу, обеспечение достаточной пропускной способности скрытого канала связи, малая вычислительная сложность [1]. В качестве контейнера сегодня чаще всего используются цифровые изображения (ЦИ), видео (ЦВ), цифровые аудио.

С учетом особенностей современной коммуникации, одной из которых является передача информации (ЦИ, ЦВ) в форматах с потерями, одним из самых важных требований к стеганоалгоритмам становится устойчивость к различным возмущающим воздействиям.

Для устойчивого к атакам против встроенного сообщения стеганопреобразования могут использоваться как пространственная область [2,3] контейнера (ЦИ, ЦВ), так и область преобразования [4,5]: частотная, области различных разложений матрицы (матриц) контейнера [6,7]. Однако до настоящего момента окончательного решения упомянутая задача с одновременным обеспечением надежности восприятия формируемого стеганосообщения так и не получила.

Далее в работе в качестве контейнера рассматривается ЦИ.

Подавляющее большинство стеганоалгоритмов, позиционируемых как устойчивые к возмущающим воздействиям, осуществляют погружение дополнительной информации (ДИ) в частотной области изображения [8,9], основываясь на спорном в свете [10] убеждении, что более устойчивыми к разнообразным искажениям являются стеганоалгоритмы, использующие для стеганопреобразования именно частотную область. В [10] показано, что свойства стеганоалгоритмов, в том числе, их устойчивость к возмущающим воздействиям, определяются не областью, используемой для стеганопреобразования, а величинами и локализацией возмущений сингулярных чисел и сингулярных векторов матриц, отвечающих контейнеру, произошедших в ходе стеганопреобразования. С учетом этого в [11,12] на основе sign-нечувствительности к произвольным возмущающим воздействиям сингулярных векторов (СНВ) блоков матрицы ЦИ, отвечающих максимальным сингулярным числам (СНЧ), был разработан устойчивый к атакам, в том числе значительным, против встроенного сообщения стеганографический алгоритм (СА) *SNG*, эффективность которого превышает эффективность современных аналогов, но область применимости которого ограничивается некоторыми особенностями используемого в качестве контейнера изображения, в частности наличием в ЦИ плохо обусловленных (близких к вырожденным) блоков, получаемых после стандартного разбиения матрицы. Такие ограничения снижают практическую ценность предложенного алгоритма.

Цель статьи и постановка исследований

Целью работы является расширение области применимости стеганографического алгоритма *SNG*, устойчивого к атакам против встроенного сообщения, путем разработки алгоритма предобработки ЦИ-контейнера, предшествующей погружению ДИ.

Для достижения цели необходимо решить следующие задачи:

1. Обеспечить понижение числа обусловленности блоков матрицы ЦИ-контейнера в результате предобработки;
2. Обеспечить надежность восприятия ЦИ после его предобработки, с учетом чего выбрать способ предварительного кодирования блока изображения;
3. Обеспечить симметричность, положительную определенность и разреженность матрицы, являющейся результатом предварительного кодирования блока ЦИ;
4. Осуществить выбор преобуславливателя для блока ЦИ с учетом результата его кодирования.

Основная часть

При организации скрытого канала связи часто задействуется одна цветовая составляющая (с учетом особенностей человеческого зрения – синяя) цветного ЦИ-контейнера, хранящегося в соответствии с цветовой схемой RGB. В силу этого, не ограничивая общности рассуждений, в качестве формального представления

контейнера в работе используется $m \times n$ -матрица F . Как ДИ рассматривается случайно сформированная бинарная последовательность $p_1, \dots, p_t$, $p_i \in \{0,1\}$, $i = \overline{1, t}$.

Пусть B – произвольный 8×8 –блок матрицы контейнера, полученный после ее стандартного разбиения [13], элементы которого b_{kl} , $k, l = \overline{1, 8}$.

В ходе стеганопреобразования, осуществляемого алгоритмом SNG , для B строится нормальное сингулярное разложение [11]:

$$B = U \Sigma V^T, \quad (1)$$

где U, V – ортогональные 8×8 –матрицы левых $u_1, \dots, u_8$ лексикографически положительных и правых $v_1, \dots, v_8$ СНВ B соответственно, отвечающих столбцам U, V , $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_8)$ – матрица СНЧ, $\sigma_1 \geq \dots \geq \sigma_8 \geq 0$.

Основная идея СА SNG заключается в том, что погружение ДИ в блок B должно происходить путем такого возмущения СНВ u_1, v_1 (левого и/или правого), отвечающих максимальному СНЧ σ_1 блока, чтобы стеганопреобразование оставляло/делало его (их) близким (близкими) к n -оптимальному вектору $n^o = (1/\sqrt{8}, \dots, 1/\sqrt{8})^T \in R^8$ пространства R^8 .

При погружении очередного бита ДИ в очередной задействуемый для стеганопреобразования блок ЦИ-контейнера происходит отклонение u_1 и/или v_1 от первоначального положения. Для простоты дальнейшего изложения, не ограничивая общности рассуждений, будем считать, что стеганопреобразование происходит за счет модификации u_1 , результат которой обозначим $\bar{u}_1$. Это требует приведение левых СНВ $u_2, \dots, u_8$ блока B к ортонормированному с $\bar{u}_1$ лексикографически положительному виду, для чего в [12] предлагалось решать систему из 28 линейных алгебраических уравнений с неизвестными x_i , $i = \overline{1, 28}$ (рис. 1):

$$\begin{cases} (\bar{u}_1, u_j^o) = 0, j = 2, \dots, 8, \\ (u_i^o, u_j^o) = 0, i = 2, \dots, 8, j = 2, \dots, i-1, \end{cases} \quad (2)$$

где $(\bullet, \bullet)$ – скалярное произведение векторов-аргументов, u_i^o – вектор-столбец, ортогональный векторам $\bar{u}_1$ и u_j^o , $j = 2, \dots, i-1$. Матрица $\bar{U}$, фигурирующая при формировании матрицы $\bar{B}$ блока стеганосообщения при погружении ДИ, включает в себя нормированные векторы-столбцы $u_j^o / \|u_j^o\|$, $j = 2, \dots, 8$:

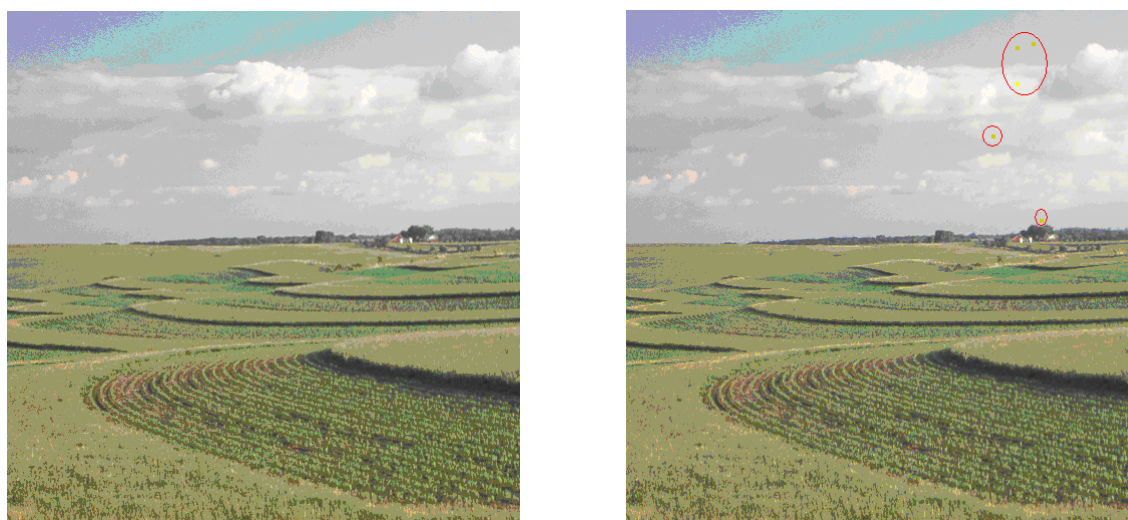
$$\bar{U} = (\bar{u}_1, u_2^o / \|u_2^o\|, \dots, u_8^o / \|u_8^o\|) = (n^o, \bar{u}_2, \dots, \bar{u}_8). \quad (3)$$

Система (2) может оказаться плохо обусловленной для некоторых блоков ЦИ-контейнера, что приводит к возникновению артефактов на ЦИ-стеганосообщении (рис. 2). Установлено, что, как правило, это блоки, отвечающие фоновым областям изображения, перепад значений яркости пикселей в их пределах очень незначительный, а матрица блока близка к вырожденной (плохо обусловлена). Такие блоки в алгоритме SNG не использовались для погружения ДИ. Как показал вычислительный эксперимент, количество таких блоков в пределах изображения невелико, их игнорирование при стеганопреобразовании не приводит к значимому снижению пропускной способности организуемого скрытого канала связи, но все же

ограничивает область применимости алгоритма *SNG*, что можно трактовать как его недостаток.

$$\begin{array}{c}
 \begin{array}{cccccccc}
 u_1^0 & u_2^0 & u_3^0 & u_4^0 & u_5^0 & u_6^0 & u_7^0 & u_8^0 \\
 \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow
 \end{array} \\
 \left(\begin{array}{cccccccc}
 1/\sqrt{8} & u_{12} & u_{13} & u_{14} & u_{15} & u_{16} & u_{17} & u_{18} \\
 1/\sqrt{8} & u_{22} & u_{23} & u_{24} & u_{25} & u_{26} & u_{27} & x_{22} \\
 1/\sqrt{8} & u_{32} & u_{33} & u_{34} & u_{35} & u_{36} & x_{16} & x_{23} \\
 1/\sqrt{8} & u_{42} & u_{43} & u_{44} & u_{45} & x_{11} & x_{17} & x_{24} \\
 1/\sqrt{8} & u_{52} & u_{53} & u_{54} & x_7 & x_{12} & x_{18} & x_{25} \\
 1/\sqrt{8} & u_{62} & u_{63} & x_4 & x_8 & x_{13} & x_{19} & x_{26} \\
 1/\sqrt{8} & u_{72} & x_2 & x_5 & x_9 & x_{14} & x_{20} & x_{27} \\
 1/\sqrt{8} & x_1 & x_3 & x_6 & x_{10} & x_{15} & x_{21} & x_{28}
 \end{array} \right)
 \end{array}$$

Рис.1. Возмущаемая в процессе стеганопреобразования блока *B* алгоритмом *SNG* матрица левых СНВ *U*



а

б

Рис.2. Пример нарушения надежности восприятия СС, формируемого стеганоалгоритмом *SNG*: а – ЦИ-контейнер (формат TIF); б – СС с обозначенными на нем областями, содержащими артефакты (формат TIF)

Одним из возможных способов решения возникшей проблемы является организация предобработки ЦИ-контейнера, предшествующей стеганопреобразованию алгоритмом *SNG*, таким образом, чтобы понизить числа обусловленности матриц (большинства) блоков, сохраняя при этом надежность восприятия результирующего изображения. Одним из широко используемых способов понижения числа обусловленности матрицы является ее предобуславливание [14] за счет выбора подходящей матрицы предобуславливателя, в качестве которого в случае разреженной симметричной и положительно определенной матрицы *A* хорошо зарекомендовало себя ее неполное разложение Холесского [15]. Однако матрица *B* блока ЦИ в общем случае не удовлетворяет ни одному из перечисленных выше свойств. Для обеспечения желаемых свойств проведем кодирование *B* следующим образом.

Поставим B в соответствие бинарную матрицу $\bar{B}$ с элементами $\bar{b}_{kl}$, $k, l = \overline{1,8}$:

$$\bar{b}_{kl} = \begin{cases} 0, & \text{если } b_{kl} < P, \\ 1, & \text{если } b_{kl} \geq P \end{cases} \quad k, l = \overline{1,8}, \quad (4)$$

где

$$P = \left(\min_{1 \leq k, l \leq 8} b_{kl} + \max_{1 \leq k, l \leq 8} b_{kl} \right) / 2 \quad (5)$$

– пороговое значение, вычисляемое для каждого блока B , после чего матрице $\bar{B}$ поставим в соответствие две симметричных матрицы $B^{(V)}$ и $B^{(N)}$, отражая верхний (нижний) треугольник матрицы $\bar{B}$ относительно главной диагонали:

$$B^{(V)} = \begin{pmatrix} \bar{b}_{1,1} & \bar{b}_{1,2} & \bar{b}_{1,3} & \dots & \bar{b}_{1,8} \\ \bar{b}_{1,2} & \bar{b}_{2,2} & \bar{b}_{2,3} & \dots & \bar{b}_{2,8} \\ \bar{b}_{1,3} & \bar{b}_{2,3} & \bar{b}_{3,3} & \dots & \bar{b}_{3,8} \\ \dots & \dots & \dots & \dots & \dots \\ \bar{b}_{1,8} & \bar{b}_{2,8} & \bar{b}_{3,8} & \dots & \bar{b}_{8,8} \end{pmatrix}, \quad B^{(N)} = \begin{pmatrix} \bar{b}_{1,1} & \bar{b}_{2,1} & \bar{b}_{3,1} & \dots & \bar{b}_{8,1} \\ \bar{b}_{2,1} & \bar{b}_{2,2} & \bar{b}_{3,2} & \dots & \bar{b}_{8,2} \\ \bar{b}_{3,1} & \bar{b}_{3,2} & \bar{b}_{3,3} & \dots & \bar{b}_{8,3} \\ \dots & \dots & \dots & \dots & \dots \\ \bar{b}_{8,1} & \bar{b}_{8,2} & \bar{b}_{8,3} & \dots & \bar{b}_{8,8} \end{pmatrix}. \quad (6)$$

Матрицы $B^{(V)}$ и $B^{(N)}$, элементы которых далее обозначаются $b_{kl}^{(V)}$ и $b_{kl}^{(N)}$, $k, l = \overline{1,8}$, соответственно, являясь симметричными, могут не оказаться положительно определенными, более того, они могут оказаться вырожденными. Для обеспечения их положительной определенности положим:

$$b_{kk}^{(V)} = b_{kk}^{(N)} = 8, \quad k = \overline{1,8}, \quad (7)$$

что гарантирует диагональное преобладание, а с учетом того, что после преобразования (7) $b_{kk} > 0$, $k = \overline{1,8}$, то и положительную определенность. Модифицированные таким образом матрицы $B^{(V)}$ и $B^{(N)}$, обозначаемые далее $B_M^{(V)}$ и $B_M^{(N)}$, допускают разложения Холецкого:

$$B_M^{(V)} = L^{(V)} \left(L^{(V)} \right)^T, \quad B_M^{(N)} = L^{(N)} \left(L^{(N)} \right)^T, \quad (8)$$

где $L^{(V)}, L^{(N)}$ – нижние треугольные матрицы с положительными диагональными элементами, элементы которых далее обозначаются $l_{kl}^{(V)}, l_{kl}^{(N)}$, $k, l = \overline{1,8}$.

Неполные разложения Холецкого для $B_M^{(V)}$ и $B_M^{(N)}$, обозначаемые далее

$$M^{(V)} = \bar{L}^{(V)} \left(\bar{L}^{(V)} \right)^T, \quad M^{(N)} = \bar{L}^{(N)} \left(\bar{L}^{(N)} \right)^T \quad (9)$$

соответственно, будут отличаться от классических (8) тем, что нижние треугольные матрицы $\bar{L}^{(V)}, \bar{L}^{(N)}$ с элементами $\bar{l}_{kl}^{(V)}, \bar{l}_{kl}^{(N)}$, $k, l = \overline{1,8}$, соответственно будут иметь нулевые элементы в тех же позициях, что и нижние треугольные части матриц $B_M^{(V)}$ и $B_M^{(N)}$ соответственно, т.е.:

$$\bar{l}_{kl}^{(V)} = \begin{cases} l_{kl}^{(V)}, & \text{если } b_{kl}^{(V)} \neq 0, \\ 0, & \text{если } b_{kl}^{(V)} = 0 \end{cases}, \quad \bar{l}_{kl}^{(N)} = \begin{cases} l_{kl}^{(N)}, & \text{если } b_{kl}^{(N)} \neq 0, \\ 0, & \text{если } b_{kl}^{(N)} = 0 \end{cases}, \quad k > l. \quad (10)$$

Предобусловленные матрицы $B_M^{(V)}$ и $B_M^{(N)}$, обозначаемые далее $W^{(V)}$ и $W^{(N)}$, будут выглядеть следующим образом:

$$W^{(V)} = (M^{(V)})^{-1} B_M^{(V)}, \quad W^{(N)} = (M^{(N)})^{-1} B_M^{(N)}. \quad (11)$$

Числа обусловленности $W^{(V)}$ и $W^{(N)}$, которые не являются бинарными (их элементы в общем случае вещественные числа), практически для всех блоков ЦИ будут меньше чисел обусловленности $B_M^{(V)}$ и $B_M^{(N)}$:

$$\text{cond}(W^{(V)}) < \text{cond}(B_M^{(V)}), \quad \text{cond}(W^{(N)}) < \text{cond}(B_M^{(N)}),$$

что подтверждается результатами вычислительного эксперимента. С учетом полученных предобусловленных матриц $W^{(V)}$ и $W^{(N)}$, отвечающих блоку B , поставим в соответствие B блок ЦИ после предобработки, обозначаемый далее $\bar{B}$ с элементами $\bar{b}_{kl}$, $k, l = \overline{1, 8}$, используя для восстановления элементов нижнего/верхнего треугольника $\bar{B}$ нижний/верхний треугольник матрицы $W^{(V)}/W^{(N)}$ соответственно, учитывая первоначальное соответствие (4) между B и $\bar{B}$ (1/0 в бинарной матрице $\bar{B}$ отвечал элементу оригинального блока B , величина которого превосходила/не превосходила пороговое значение P):

$$\bar{b}_{kl} = \begin{cases} P-1, & \text{если } (m_{kl}^{(V)} < 0.5) \& (b_{kl} \geq P), \\ P+1, & \text{если } (m_{kl}^{(V)} \geq 0.5) \& (b_{kl} < P), \\ b_{kl} & \text{в противном случае} \end{cases}, \quad \bar{b}_{lk} = \begin{cases} P-1, & \text{если } (m_{lk}^{(N)} < 0.5) \& (b_{lk} \geq P), \\ P+1, & \text{если } (m_{lk}^{(N)} \geq 0.5) \& (b_{lk} < P), \\ b_{lk} & \text{в противном случае} \end{cases}, \quad (12)$$

$$l > k.$$

Таким образом, усовершенствованный стеганоалгоритм *SNG* с учетом разработанного алгоритма предобработки блока ЦИ выглядит следующим образом.

Погружение ДИ

Шаг 1. Матрица F ЦИ-контейнера разбивается стандартным образом на непересекающиеся 8×8 – блоки.

Шаг 2. В очередной блок B , используемый в процессе стеганопреобразования, погружается очередной бит p_i ДИ:

2.1 (предобработка блока).

2.1.1. Для блока B вычислить пороговое значение P в соответствии с (5).

2.1.2. Матрице блока B поставить в соответствие бинарную матрицу $\bar{B}$ в соответствии с (4).

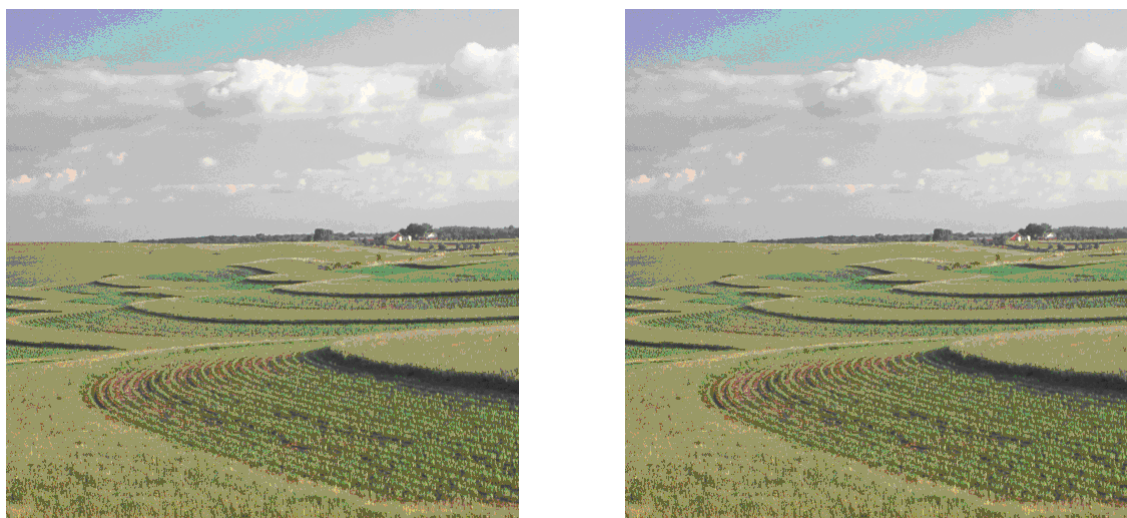
2.1.3. Для матрицы $\bar{B}$ построить матрицы $B^{(V)}$ и $B^{(N)}$ в соответствии с (6).

2.1.4. Модифицировать матрицы $B^{(V)}$ и $B^{(N)}$ в соответствии с (7). Результат – симметричные положительно определенные разреженные матрицы $B_M^{(V)}$ и $B_M^{(N)}$.

- 2.1.5. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить разложения Холецкого в соответствии с (8).
- 2.1.6. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить нижние треугольные матрицы $\bar{L}^{(V)}$, $\bar{L}^{(N)}$ – множители неполного разложения Холецкого в соответствии с (10).
- 2.1.7. Для матриц $B_M^{(V)}$ и $B_M^{(N)}$ построить неполные разложения Холецкого в соответствии с (9).
- 2.1.8. Выполнить предобуславливание матриц $B_M^{(V)}$ и $B_M^{(N)}$ в соответствии с (11). Результат – матрицы $W^{(V)}$, $W^{(N)}$.
- 2.1.9. Матрице B поставить в соответствие блок $\bar{\bar{B}}$, построенный в соответствии с (12). $\bar{\bar{B}}$ – результат предобработки блока B , предшествующей погружению ДИ.
- 2.2. Для $\bar{\bar{B}}$ построить нормальное сингулярное разложение (1): $\bar{\bar{B}} = U\Sigma V^T$.
- 2.3. (погружение p_i):
- Если $p_i = 1$, то
- 2.3.1. $\bar{u}_1 = n^o$, где $\bar{u}_1$ – возмущенный в ходе стеганопреобразования u_1 ;
- 2.3.2. Приведение левых СНВ $u_2, \dots, u_8$ блока $\bar{\bar{B}}$ к ортонормированному с $\bar{u}_1$ лексикографически положительному виду путем решения системы линейных уравнений (2) с последующей нормализацией (3) левых СНВ. Результат – $\bar{u}_2, \dots, \bar{u}_8$.
- иначе
- 2.3.1. $\bar{v}_1 = n^o$, где $\bar{v}_1$ – возмущенный в ходе стеганопреобразования v_1 ;
- 2.3.2. Приведение правых СНВ $v_2, \dots, v_8$ блока $\bar{\bar{B}}$ к ортонормированному с $\bar{v}_1$ виду путем решения соответствующей системы линейных уравнений (2), составленной для правых СНВ, с последующей нормализацией (3) правых СНВ. Результат – $\bar{v}_2, \dots, \bar{v}_8$.
- 2.4. (Формирование блока B_S стеганосообщения, отвечающего блоку B контейнера).
- Если $p_i = 1$, то $B_S = \bar{U}\Sigma V^T$, где $\bar{U} = (n^o, \bar{u}_2, \dots, \bar{u}_8)$
- иначе $B_S = U\Sigma\bar{V}^T$, где $\bar{V} = (n^o, \bar{v}_2, \dots, \bar{v}_8)$.
- Декодирование ДИ** отвечает [12].

Для оценки изменения числа обусловленности блоков ЦИ после предложенной предобработки был проведен вычислительный эксперимент, в котором было задействовано более 200 ЦИ, хранимых как в формате с потерями (Jpeg), так и в формате без потерь (Tif), в ходе которого было установлено, что в среднем для 68% блоков ЦИ число обусловленности соответствующей матрицы уменьшалось (в среднем на 78%), при этом значение пикового отношения «сигнал-шум» PSNR, используемого для оценки искажения ЦИ в результате предобработки, в среднем составило 42 dB, что говорит о большой вероятности сохранения надежности восприятия изображения [16]. Максимально количество блоков изображения, для которых понижалось число обусловленности, составляло 88%, минимально – 52%. Искажения ЦИ в процессе предобработки находились в пределах 38-54 dB. Нарушения надежности восприятия обработанного ЦИ путем субъективного ранжирования в ходе вычислительного эксперимента установлено не было.

Погружение ДИ стеганоалгоритмом *SNG* после предложенной предобработки контейнера позволило значительно расширить область применимости алгоритма, иллюстрацией чего служит рис.3.



а

б

Рис.3. Сохранение надежности восприятия стеганосообщения, формируемого стеганоалгоритмом *SNG* после предобработки контейнера: а – ЦИ-контейнер (формат TIF); б – стеганосообщение (формат TIF)

Замечание. Вычислительная сложность предложенного алгоритма обработки ЦИ определяется количеством блоков его матрицы, полученных в результате ее стандартного разбиения, и составляет $O(n^2)$ для $n \times n$ – матрицы изображения, оставляя СА *SNG* при использовании предобработки контейнера полиномиальным степени 2.

Выводы

В работе предложено усовершенствование устойчивого к атакам против встроенного сообщения, в том числе значительным, стеганографического алгоритма *SNG*, основанного на sign-нечувствительности сингулярных векторов блоков матрицы цифрового изображения, соответствующих максимальным сингулярным числам: предобработка блоков контейнера, осуществляемая перед непосредственным погружением ДИ. Результатом предобработки является понижение числа обусловленности большинства блоков матрицы контейнера, что позволило расширить область применимости алгоритма *SNG*, оставляя его полиномиальным степени 2.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2002. — 272 с.
2. Huang, H.Y. Robust technique for watermark embedding in a video stream based on block matching algorithm / H.Y. Huang, Y.R. Lin, W.H. Hsu // Optical Engineering. — 2008. — Vol. 47, Iss. 3. — PP. 037402-1–037402-14.
3. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения / А.А. Кобозева, О.В. Костырка, Е.Ю. Лебедева // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. — 2014. — № 1(24). — С. 1-12.

4. Subhashini, D. Comparison analysis of spatial Domain and compressed Domain steganographic techniques / D. Subhashini, P. Nalini, G. Chandrasekhar // *International Journal of Engineering Research and Technology*. — 2012. — Vol. 1, Iss. 4. — PP. 1–6.
5. Li, B. A Survey on Image Steganography and Steganalysis / B. Li et al. // *Journal of Information Hiding and Multimedia Signal Processing*. — 2011. — Vol.2, No.2. — PP. 142–172.
6. Veeraswamy, K. Adaptive AC-Coefficient Prediction for Image Compression and Blind Watermarking / K. Veeraswamy, S. Srinivas Kumar // *Journal of Multimedia*. — 2008. — Vol. 3, No. 1. — PP. 16-22.
7. Yongdong, W. On the security of an SVD based ownership watermarking / W. Yongdong // *IEEE Transactions on Multimedia*. — 2005. — Vol. 7, Iss. 4. — PP. 624–627.
8. Fan, C.-H. A robust watermarking technique resistant Jpeg compression / C.-H. Fan, H.-Y. Huang, W.-H. Hsu // *Journal of Information Science and Engineering*. — 2011. — Vol. 27, Iss. 1. — PP. 163–180.
9. Patra, J.C. Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication / J.C. Patra, A.K. Kishore, C. Bornand // *In Proc. of 2011 IEEE International Conference on Systems, Man, and Cybernetics*. — 2011. — P. 2940–2945.
10. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации // *Искусственный интеллект*. — 2007. — № 4. — С. 531–538.
11. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / А.А. Кобозева, М.А. Мельник // *Захист інформації*. — 2013. — №2. — С.49-58.
12. Кобозева, А.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения / А.А. Кобозева, М.А. Мельник // *Системы обработки информации*. — 2013. — Вып. 3(110), том 2. — С.90-94.
13. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. под ред. П.А. Чочиа. — М.: Техносфера, 2005. — 1072 с.
14. Деммель, Дж. Вычислительная линейная алгебра / Дж. Деммель; пер.с англ. Х.Д. Икрамова. — М.: Мир, 2001. — 430 с.
15. Альчиков, В.В. Использование метода неполной факторизации Холецкого — сопряженных градиентов для решения трехмерных уравнений Лапласа / В.В. Альчиков, В.И. Быков // *Вычислительные технологии*. — 2000. — Т.5, № 6. — С.15-19.
16. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф. Конахович, А.Ю. Пузыренко. — К.: МК — Пресс, 2006. — 288 с.

УДОСКОНАЛЕННЯ СТЕГANOГРАФІЧНОГО АЛГОРИТМУ, ЗАСНОВАНОГО НА SIGN-НЕЧУТЛИВОСТІ СИНГУЛЯРНИХ ВЕКТОРІВ БЛОКІВ МАТРИЦІ ЗОБРАЖЕННЯ

А.А. Кобозева, В.А. Мокрицький, Л.Е.М. Батиєне, І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: kobozeva@opu.ua

В роботі запропонований спосіб обробки цифрового зображення, результатом якої є зниження числа обумовленості більшості блоків його матриці, отриманих шляхом стандартного розбиття, за рахунок передобумовлення відповідних матриць. Обробка зберігає надійність сприйняття спотвореного зображення, яка в роботі кількісно оцінюється за допомогою пікового відношення «сигнал-шум». Використання запропонованого способу обробки як передобробки зображення-контейнера перед стеганоперетворенням дозволяє розширити область застосовності стійкого до атак проти вбудованого повідомлення, в тому числі значних, стеганографічного алгоритму, заснованого на sign-нечутливості сингулярних векторів блоків матриці цифрового зображення, які відповідають максимальним сингулярним числам, розробленого одним з автором раніше. Передобумовлення матриці блоку відбувається після його попереднього кодування. Результатом попереднього кодування є 2 симетричні додатно визначені розріджені матриці, які ставляться у відповідність блоку зображення. Додатна визначеність і розрідженість отриманих матриць дає можливість використовувати в якості передобумовника для них неповне розкладання Холеського. Наведено результати обчислювального експерименту.

Ключові слова: стеганографічний алгоритм, цифрове зображення, передобумовник, неповне розкладання Холеського, число обумовленості

IMPROVEMENT OF THE STEGANOGRAPHY ALGORITHM BASED ON THE SIGN-INSENSITIVITY OF THE SINGULAR VECTORS OF BLOCKS OF THE DIGITAL IMAGE MATRIX

A.A. Kobozeva, V.A. Mokritsky, L.E.M. Batiene, I.I. Bobok

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: kobozeva@opu.ua

In this paper the new method for digital image processing is proposed. Application of this method leads to decrease the conditioning number of the majority of matrix blocks obtained by standard partitioning as a result of preconditioning of the corresponding matrices. The proposed method preserves the reliability of the perception of the distorted image, which in the work is quantitatively estimated using the peak signal-to-noise ratio. The application of the proposed method as pre-processing of the cover image before steganography transformation makes it possible to extend the application domain of the steganography algorithm based on the sign-insensitivity of the singular vectors of blocks of the digital image matrix developed by one of the authors earlier. The preconditioning of the block matrix occurred after its precoding. The result of precoding is a symmetric positive-definite sparse matrix, which is mapped to the image block. The positive definiteness and sparsification of obtained matrix make it possible to use as its preconditioner the incomplete Cholesky factorization. The results of the computational experiment are presented.

Keywords: steganographic algorithm, digital image, preconditioner, incomplete Cholesky decomposition, condition number

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СУМІСНОГО ВИКОНАННЯ АЛГОРИТМУ ЕВКЛІДА ТА МНОЖЕННЯ

М.М. Касянчук, І.З. Якименко, І.Р. Паздрій, С.В. Івасьєв

Тернопільський національний економічний університет,
вул. Львівська, 11, м.Тернопіль, 46020, Україна; e-mail: kasyanchuk@ukr.net

Сумісне виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел є досить важливою задачею сучасної теорії чисел, обчислювальної математики та асиметричної криптографії, зокрема, криптосистеми Рабіна. У роботі проведено експериментальне дослідження часових характеристик програмної реалізації вказаних операцій класичним та запропонованим методами із застосуванням мови програмування високого рівня C++. У запропонованому методі передбачено використання проміжних результатів алгоритму Евкліда та звертання до наявної у пам'яті комп'ютера таблиці квадратів. Для дослідження використовувалися числа різної розрядності. Показано, що в переважній більшості розглянутих випадків запропонований метод характеризується більш високою швидкістю, середній час виконання операцій зменшується приблизно в 1.3 рази. Для нівелювання випадкових впливів на час роботи усі обчислення повторювалися 5000 разів. Запропонований метод ефективно можна використовувати для сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел.

Ключові слова: алгоритм Евкліда, множення, асиметрична криптографія, прості числа, середній час, часові характеристики, розрядність чисел

Вступ

На даний час виконання арифметичних операцій над багаторозрядними числами дуже широко використовується в різних галузях науки і техніки, зокрема, при розв'язуванні задач обчислювальної, прикладної та дискретної математики [1]. Кожен з відповідних алгоритмів має свою область ефективного використання залежно від розрядності, моделі обчислень, мови програмування, апаратної або програмної реалізації. Особливо це стосується проблем криптографії [2], де найбільш поширеними є операції множення [3], піднесення до степеня [4], пошуку найбільшого спільного дільника (НСД), використання китайської теореми про залишки [5] тощо. Поєднання перших двох з рештою операцій вимагає строго послідовної реалізації, що істотно зменшує швидкість обчислювальних систем. Прикладом може бути криптосистема Рабіна [6], де для застосування китайської теореми про залишки використовується алгоритм Евкліда, а для формування відкритого ключа ті ж самі числа необхідно перемножити. Тому досить гостро постає питання про можливість розпаралелення виконання подібних операцій [7, 8], зокрема, застосування системи залишкових класів [9, 10], її досконалої [11, 12] та модифікованої досконалої форм [13, 14].

Сучасний математичний запис алгоритму Евкліда має такий вигляд [15]: для будь-якого $a > b = r_0$, де a і b – цілі числа, виконується система рівнянь

[illegible]

НСД (a, b) , обчислений за допомогою алгоритму Евкліда зі складністю $\underline{O}(2 \log_2 \max(a, b))$ [16], дорівнюватиме r_n , тобто останньому ненульовому члену послідовності r_i . Далі відбувається перемноження чисел a і b . Для множення розроблено багато алгоритмів (стандартний, бінарний, Монтгомері, Карацуби-Офмана тощо), які характеризуються різною обчислювальною складністю [17].

Однак теоретичні дослідження не завжди показують реальну картину щодо швидкодії обчислень, оскільки не враховують усіх факторів, які впливають на роботу комп'ютера, зокрема, звертань до пам'яті, особливостей завантаженості процесора, його розрядності та розпаралелення обчислень тощо.

Тому *метою* роботи є визначення, порівняння та аналіз часу сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел, виконаних за допомогою класичного та запропонованих методів для чисел різної розрядності на комп'ютері із заданими параметрами.

Основна частина

У криптосистемі Рабіна задані числа a і b є простими, тому відомо, що в такому випадку $\text{НСД}(a, b) = r_n = 1$. На відміну від виконання алгоритму Евкліда з наступним перемноженням цих самих чисел пропонується, згідно (1), у множенні використати проміжні та кінцеві результати алгоритму Евкліда таким чином:

$$a \cdot b = r_0^2 q_1 + r_1^2 q_2 + r_2^2 q_3 + \dots + r_{n-1}^2 q_n + r_n. \quad (2)$$

Слід відмітити, що кількість доданків у (2) відповідає кількості кроків у алгоритмі Евкліда. Хоча даний метод передбачає виконання більшої кількості арифметичних операцій, однак вони виконуватимуться над числами меншої розрядності. Суттєвим кроком для підвищення швидкодії буде наявність таблиці квадратів у пам'яті комп'ютера, хоча це приводить до збільшення використання ресурсів обчислювальної системи. Блок-схема алгоритму наведена на рис. 1.

Для експериментальних досліджень було обрано портативний комп'ютер Lenovo B50-70 з процесором Intel Pentium 3558U (1.7 ГГц). Об'єм оперативної пам'яті в пристрої становив 4 GB. При проектуванні програмного комплексу, що забезпечував обчислення, було обрано мову програмування високого рівня C++. Для роботи з багаторозрядними числами використовувалась бібліотека спеціального призначення, написана А. Ленстрою. Це дозволило забезпечити гнучкі можливості роботи з багаторозрядними числами, розмір яких залежить лише від доступних ресурсів системи. Обрана мова програмування та кросплатформенність спеціалізованої бібліотеки дозволяють трансформувати коди під різні архітектури та операційні системи.

Найбільш розповсюдженим методом програмної реалізації алгоритму Евкліда є послідовне віднімання меншого числа від більшого, поки різниця не стане меншою від'ємника. Тоді цю ж саму процедуру потрібно виконати з від'ємником та різницею.

Процес віднімання буде тривати до тих пір, поки від'ємник та різниця не стануть однакові.

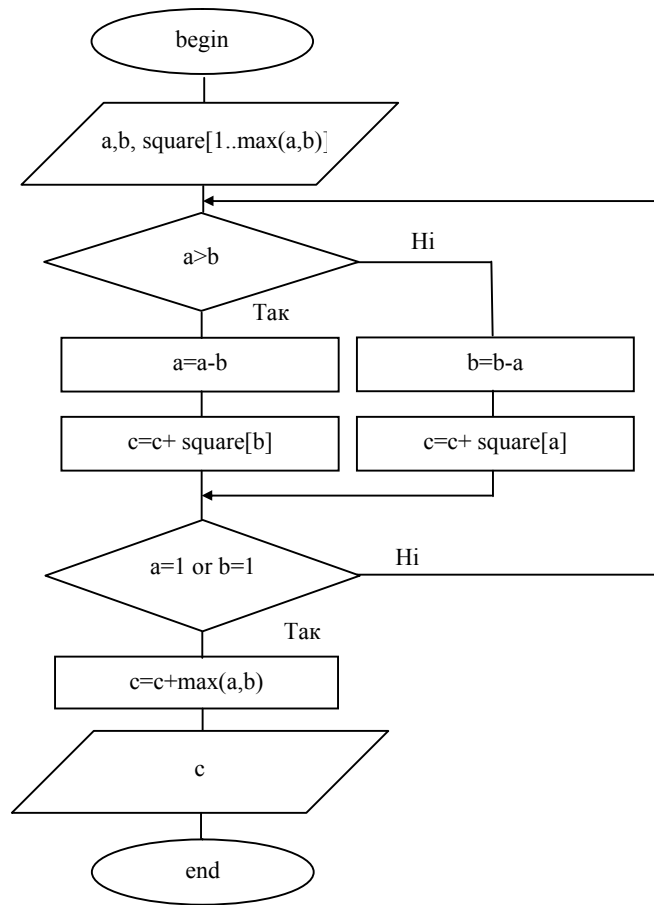


Рис. 1. Блок-схема запропонованого алгоритму

В табл. 1 представлено час сумісного виконання алгоритму Евкліда та перемноження чисел класичним (t_1) та запропонованим (t_2) методами для $b=2, 3, \dots, 70$ при $a=71$, а на рис. 2 – відповідна графічна залежність (t_1 та $t_{1\text{сеп}}$ – пунктирна лінія, t_2 та $t_{2\text{сеп}}$ – суцільна).

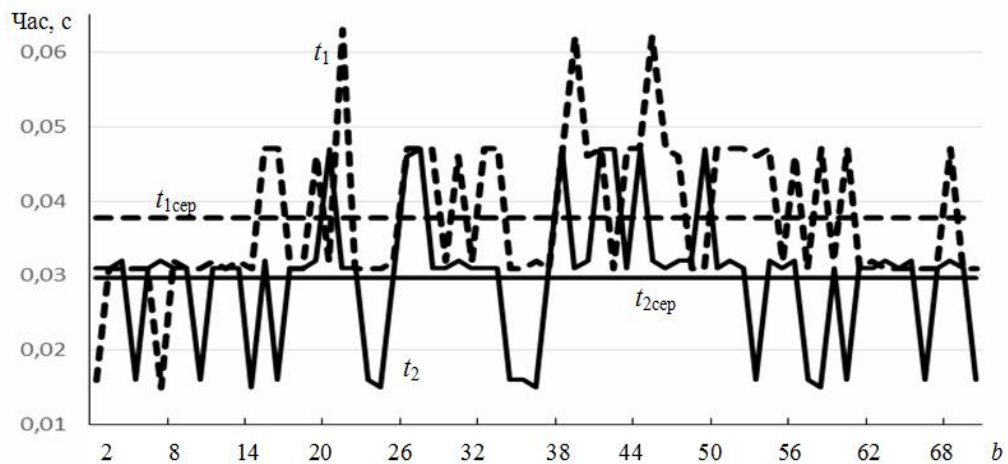


Рис. 2. Графічна залежність часу сумісного виконання алгоритму Евкліда та перемноження чисел класичним (t_1) та запропонованим (t_2) методами

Таблиця 1.

Час сумісного виконання алгоритму Евкліда та перемноження чисел класичним (t_1) та запропонованим (t_2) методами

b	2	3	4	5	6	7	8	9	10	11	12
t_1, c	0.016	0.031	0.031	0.031	0.031	0.015	0.032	0.031	0.031	0.032	0.031
t_2, c	0.031	0.031	0.032	0.016	0.031	0.032	0.031	0.031	0.016	0.031	0.031
b	13	14	15	16	17	18	19	20	21	22	23
t_1, c	0.032	0.031	0.047	0.047	0.031	0.031	0.046	0.032	0.063	0.031	0.031
t_2, c	0.031	0.015	0.032	0.016	0.031	0.031	0.032	0.047	0.031	0.031	0.016
b	24	25	26	27	28	29	30	31	32	33	34
t_1, c	0.031	0.032	0.047	0.047	0.047	0.032	0.046	0.032	0.047	0.047	0.031
t_2, c	0.015	0.031	0.046	0.047	0.031	0.031	0.032	0.031	0.031	0.031	0.016
b	35	36	37	38	39	40	41	42	43	44	45
t_1, c	0.031	0.032	0.031	0.047	0.062	0.046	0.047	0.031	0.047	0.047	0.062
t_2, c	0.016	0.015	0.032	0.047	0.031	0.032	0.047	0.047	0.031	0.047	0.032
b	46	47	48	49	50	51	52	53	54	55	56
t_1, c	0.047	0.046	0.031	0.031	0.047	0.047	0.047	0.046	0.047	0.032	0.046
t_2, c	0.031	0.032	0.032	0.047	0.031	0.032	0.031	0.016	0.032	0.031	0.032
b	57	58	59	60	61	62	63	64	65	66	67
t_1, c	0.031	0.047	0.032	0.047	0.031	0.032	0.031	0.031	0.031	0.031	0.031
t_2, c	0.016	0.015	0.031	0.016	0.031	0.031	0.032	0.031	0.032	0.016	0.031
b	68	69	70								
t_1, c	0.047	0.031	0.031	Середній час: $t_{1\text{сеп}}=0.037783$ с.							
t_2, c	0.032	0.031	0.016	Середній час: $t_{2\text{сеп}}=0.029754$ с.							

Графіки (рис. 2) носять осцилюючий характер, що пояснюється різною кількістю кроків у алгоритмі Евкліда для різних чисел. В 44 випадках із 69, що становить 64%, обчислення запропонованим методом виконуються швидше, у 10 (14%) – повільніше, в 15 випадках (22%) час виконання обома методами однаковий. Середні значення часу становлять відповідно $t_{1\text{сеп}}=0.037783$ с та $t_{2\text{сеп}}=0.029754$ с, що також представлено на графіку. Отже, швидкодія збільшилася в середньому в 1.27 рази.

В табл. 2 представлено середній час сумісного виконання алгоритму Евкліда та множення класичним (t_3) та запропонованим (t_4) методами у випадку, коли прості числа a перебувають в межах однієї розрядності від 67 до 127, а на рис. 3 – відповідні графіки залежності від номера числа. При цьому b змінюється від 2 до $a-1$.

Таблиця 2.

Середній час сумісного виконання алгоритму Евкліда та перемноження класичним (t_3) та запропонованим (t_4) методами

№	1	2	3	4	5	6	7
a	67	71	73	79	83	89	97
t_3, c	0.036369	0.037783	0.037268	0.038416	0.038519	0.038299	0.037137
t_4, c	0.03	0.029754	0.030099	0.029987	0.030926	0.030195	0.030947
№	8	9	10	11	12	13	
a	101	103	107	109	113	127	
t_3, c	0.038798	0.038485	0.040181	0.039243	0.039541	0.039544	
t_4, c	0.032222	0.031248	0.030429	0.030822	0.030568	0.03144	

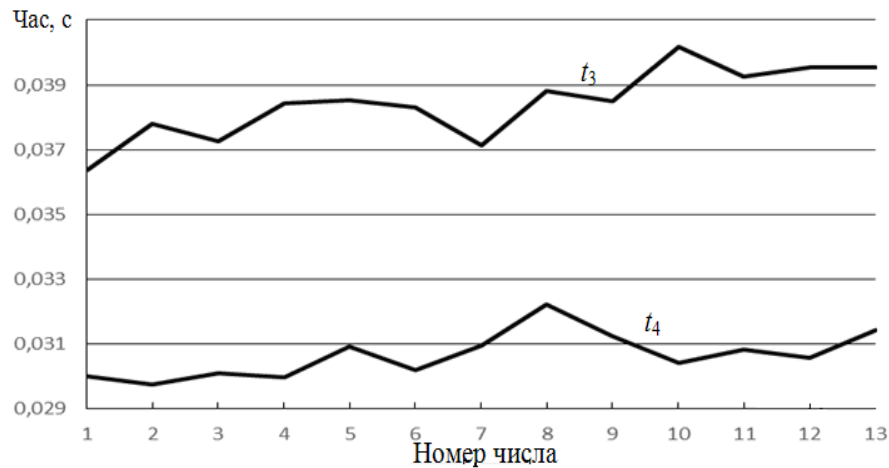


Рис. 3. Графічна залежність середнього часу сумісного виконання алгоритму Евкліда та перемноження класичним (t_3) та запропонованим (t_4) методами від номера числа згідно табл. 2

З рис. 3 видно, середній час роботи запропонованим методом у всіх випадках менший, ніж класичним. Загальний тренд показує зростання часу при збільшенні заданих чисел, причому графік для класичного методу зростає інтенсивніше.

В табл. 3 представлено середній час сумісного виконання алгоритму Евкліда та перемноження класичним (t_5) та запропонованим (t_6) методами у випадку, коли розрядність n простих чисел a перебуває в межах від 7 до 16 біт, а на рис. 4 – відповідні графічні залежності у логарифмічній шкалі. Число b змінюється аналогічно до попереднього випадку.

Таблиця 3.

Середній час сумісного виконання алгоритму Евкліда та перемноження класичним (t_5) та запропонованим (t_6) методами

a	131	181	257	359	521	727
$\log_2 a$	7	7.5	8	8.5	9	9.5
$t_5, \text{с}$	0.040612	0.039525	0.041859	0.043527	0.044844	0.046127
$t_6, \text{с}$	0.031426	0.032223	0.032906	0.034521	0.034865	0.035659
a	1031	1447	2053	2897	4099	5791
$\log_2 a$	10	10.5	11	11.5	12	12.5
$t_5, \text{с}$	0.048333	0.049314	0.051011	0.051922	0.05336	0.054791
$t_6, \text{с}$	0.037083	0.037722	0.039205	0.039943	0.040651	0.041505
a	8209	11587	16411	23173	32771	46337
$\log_2 a$	13	13.5	14	14.5	15	15.5
$t_5, \text{с}$	0.056475	0.05788	0.059334	0.060874	0.062263	0.063511
$t_6, \text{с}$	0.042528	0.043577	0.044608	0.045555	0.04639	0.047953

Видно, що усереднений час роботи збільшується майже лінійно із збільшенням розрядності числа a , причому графік для класичного методу зростає інтенсивніше.

В табл. 4 представлено середній час сумісного виконання алгоритму Евкліда та перемноження класичним (t_7) та запропонованим (t_8) методами у випадку, коли розрядність n простих чисел a (параметру a присвоювалося значення найменшого простого числа, яке перевищувало 2^n) перебуває в межах від 16 до 44 біт, а на рис. 5 –

відповідні графічні залежності у логарифмічній шкалі. Число b набувало 10000 різних значень.

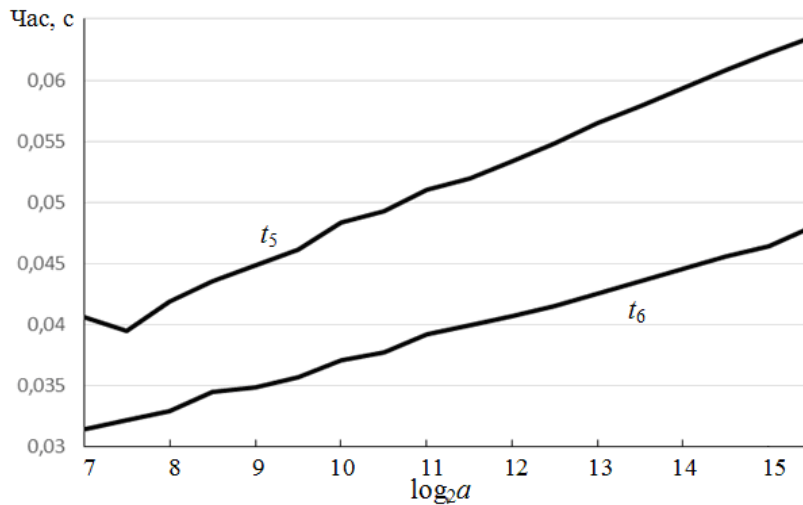


Рис. 4. Графічна залежність середнього часу сумісного виконання алгоритму Евкліда та перемноження класичним (t_5) та запропонованим (t_6) методами від розрядності числа a

Таблиця 4.

Середній час сумісного виконання алгоритму Евкліда та перемноження класичним (t_7) та запропонованим (t_8) методами

$\log_2 a$	16	20	24	28	32	36	40	44
t_7, c	0.06722	0.07799	0.08828	0.09779	0.10631	0.11857	0.12602	0.13206
t_8, c	0.05012	0.05857	0.06734	0.07577	0.08644	0.09782	0.10525	0.10915

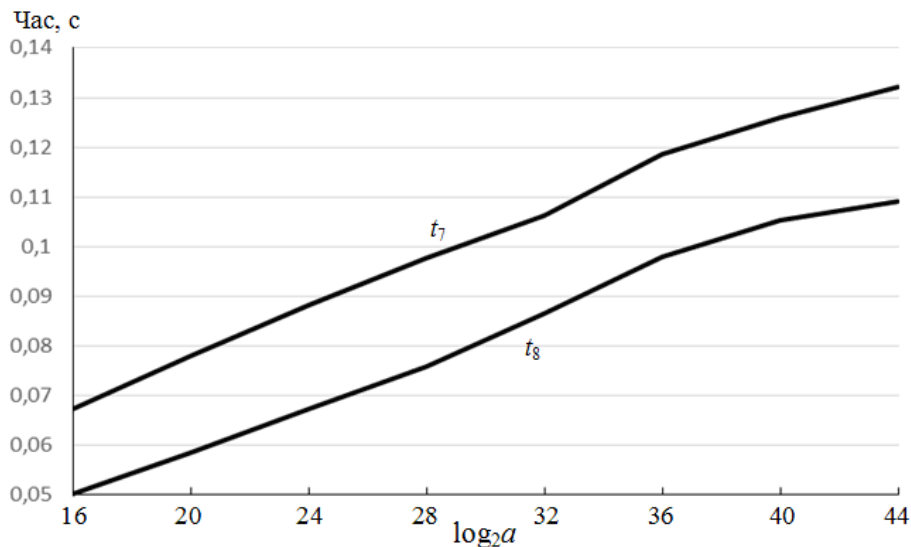


Рис. 5. Графічна залежність середнього часу сумісного виконання алгоритму Евкліда та перемноження класичним (t_7) та запропонованим (t_8) методами від розрядності числа a

Як видно з рисунка, графіки розміщені практично паралельно. При великих розрядностях ($n \geq 40$) інтенсивність зростання t_8 зменшується.

Для нівелювання випадкових впливів на час роботи усі обчислення повторювалися 5000 разів.

Висновки

У роботі проведено експериментальне дослідження часових характеристик програмної реалізації сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел класичним та запропонованим методами із застосуванням мови програмування високого рівня C++. У запропонованому методі передбачено використання проміжних результатів алгоритму Евкліда та звертання до наявної у пам'яті комп'ютера таблиці квадратів. Для дослідження використовувалися числа різної розрядності. Показано, що в переважній більшості розглянутих випадків запропонований метод характеризується більшою швидкістю, середній час виконання операцій зменшується приблизно в 1.3 рази.

Список літератури

1. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел. / В.К. Задірака, О.С. Олексюк. – К.: 2003. – 264 с.
2. Задірака, В.К. Комп'ютерна криптологія / В.К. Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
3. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, M. Kasianchuk, I. Yakymenko, S. Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2015). - Warsaw, Poland. - V.1, September – 2015. – PP.161–163.
4. Касянчук, М.М. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання / М.М. Касянчук, І.З. Якименко, Т.М. Долинюк, Н.А. Рендзеняк // Інформатика та математичні методи в моделюванні. – 2015. – Т.5, №4. – С. 376–382.
5. Николайчук, Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль: ТзОВ „Тернограф”, 2010. – 536 с.
6. Jeffrey, H. An Introduction to Mathematical Cryptography / H. Jeffrey, P. Jill, H. Joseph. – Berlin: Springer, 2008. – 540 p.
7. Чернобровкин, В.В. Распараллеливание представлений многоразрядных чисел на модулярных структурах данных / В.В. Чернобровкин // Фундаментальные исследования. – 2013. – №11. – С. 910-914.
8. Iakymenko, I. Construction of distributed thermal or piezoelectric sensor based on residue systems / I. Iakymenko, M. Kasianchuk, Ia. Kinakh, M. Karpinski // Przegląd Elektrotechniczny. – 2017. – №1. – PP. 290-294.
9. Omondi, A. Residue number systems: theory and implementation / A. Omondi, B. Premkumar. – London: Imperial College Press, 2007. – 296 p.
10. Kasianchuk, M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy // Proceedings of the XIII-th International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)”. – Polyana-Svalyava (Zakarpattia), Ukraine. - 2015. – PP. 168-171.
11. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозиуму „Питання оптимізації обчислень (ПОО–XXXV)”. Т.1. – Київ–Кацивелі.– 2009.– С. 306–310.
12. Kasianchuk, M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasianchuk // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN-2009). – L'viv. – 2009. – PP. 299–301.
13. Nykolaychuk, Ya.M. Theoretical Foundations of the Modified Perfect form of Residue Number System / Ya.M. Nykolaychuk, M.M. Kasianchuk, I.Z. Yakymenko // Cybernetics and Systems Analysis. – 2016. – Vol. 52, №2. – PP. 219-223.
14. Kasianchuk, M.N. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes / M.N. Kasianchuk, Y.N. Nykolaychuk, I.Z. Yakymenko // Journal of Automation and Information Sciences. – 2016. – Vol.48, №8. – PP. 56-63.
15. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
16. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань: Казан. ун., 2011. – 190 с.

17. Николайчук, Я.М. Эффективный метод модулярного умножения в теоретико-числовому базисі Радемахера-Крестенсона / Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, С.В. Івасьєв // Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». – 2014. – №806. – С. 195–199.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ СОВМЕСТНОГО ВЫПОЛНЕНИЯ АЛГОРИТМА ЕВКЛИДА И УМНОЖЕНИЯ

М.Н. Касянчук, И.З. Якименко, И.Р. Паздрій, С.В. Івасьєв

Тернопольский национальный экономический университет,
ул. Львовская, 11, г.Тернополь, 46020, Украина; e-mail: kasyanchuk@ukr.net

Совместное выполнение алгоритма Евклида и умножения двух многоразрядных чисел является весьма важной задачей современной теории чисел, вычислительной математики и асимметричной криптографии, в частности, криптосистемы Рабина. В работе проведено экспериментальное исследование временной сложности программной реализации указанных операций классическим и предложенным методами с применением языка программирования высокого уровня C++. В предложенном методе предусмотрено использование промежуточных результатов алгоритма Евклида и обращение к имеющейся в памяти компьютера таблицы квадратов. Для исследования использовались числа различной разрядности. Показано, что в подавляющем большинстве рассмотренных случаев предложенный метод характеризуется более высоким быстродействием, среднее время выполнения операций уменьшается примерно в 1.3 раза. Для нивелирования случайных воздействий на время работы все вычисления повторялись 5000 раз. Предложенный метод эффективно можно использовать для совместного выполнения алгоритма Евклида и умножения двух многоразрядных чисел.

Ключевые слова: алгоритм Евклида, умножение, асимметричная криптография, простые числа, среднее время, временная сложность, разрядность чисел.

EXPERIMENTAL STUDY OF SOFTWARE IMPLEMENTATION OF COMBINE REALIZATION OF THE EUCLID ALGORITHM AND MULTIPLICATION

M.M. Kasianchuk, I.Z. Yakymenko, I.R. Pazdriy, S.V. Ivasiev

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: kasyanchuk@ukr.net

The joint realization of the Euclid algorithm and multiplication of two numbers is important task of modern number theory, computational mathematics and asymmetric cryptography, including Rabin cryptosystem. The present work provide results of experimental investigation of time characteristics of software implementation these operations by standard and proposed methods using high-level programming language C++. The proposed method provides intermediate results using Euclidean algorithm and reference to computer memory available to the table of squares. In present study we used numbers of different digits. It has been shown that in most cases the proposed method is characterized by a higher speed and reduce average time of operations by 1.3 times. For leveling random effects on the working time all calculations were repeated 5000 times. The proposed method should be used effectively for compatible using Euclidian algorithm and multiplying of two multidigital numbers.

Keywords: Euclidean algorithm, multiplication, asymmetric cryptography, simple numbers, the average time, time characteristics, bit numbers.

ПРОБЛЕМНЫЕ АСПЕКТЫ ДЕПЕРСОНАЛИЗАЦИИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

А.В. Задерейко¹, А.В. Троянский¹, Н.И. Логинова², Е.Г. Трофименко³

¹ Одесский национальный политехнический университет,
пр. Шевченко, 1, г. Одесса, 65044, Украина; e-mail: alexander.zadereyko@onu.ua

² Национальный университет «Одесская юридическая академия»,
Фонтанская дорога, 23, г. Одеса, 65009, Украина

³ Одесская национальная академия связи им. А.С. Попова,
ул. Кузнечная, 1, г. Одесса, 65029, Украина

В статье рассмотрены индивидуальные признаки цифровых оптоэлектронных устройств, которые позволяют выполнить их однозначную идентификацию по сформированным ими цифровым образам (цифровым изображениям). Проанализированы возможности противодействия идентификации цифровых оптоэлектронных устройств. Показано, что эффективным способом, который позволяет противодействовать идентификации цифровых оптоэлектронных устройств, является постобработка цифровых образов с использованием специализированного программного обеспечения. Выполнен анализ специализированного программного обеспечения, которое применяется для деперсонализации цифровых образов, и предложен алгоритм их постобработки, что позволяет противодействовать идентификации цифровых оптоэлектронных устройств.

Ключевые слова: цифровые изображения, цифровое оптоэлектронное устройство, идентификация цифровых оптоэлектронных устройств, EXIF-данные, фотосенсор, цифровой шум, деперсонализация цифрового изображения

Постановка проблемы

В различных сферах профессиональных обязанностей человека возникает необходимость соблюдать меры личной безопасности по обеспечению своей конфиденциальности при создании с помощью различных фото- и веб-камер цифровых контентов, в частности, цифровых изображений.

При создании цифровых изображений всегда существует возможность идентификации цифровых оптоэлектронных устройств (ЦОЭУ) (фото-, видео-, веб-камер и сканеров) по создаваемым ими цифровым образам (цифровым изображениям). В общем случае решение задачи идентификации ЦОЭУ существенно зависит от его индивидуальных характеристик и применяемых алгоритмов постобработки создаваемого цифрового изображения.

Анализ последних исследований и публикаций

Методы анализа цифровых изображений и идентификации ЦОЭУ начали разрабатываться сравнительно недавно. В своих работах проблемы неоднозначности идентификации цифровых образов и применяемых алгоритмов постобработки исследовали Лукас Ян, Фридрих Дж., Голян М., Мехди К.Л., Сенсар К.Л., Метон Н., Кобозева А.А., Малюка А.А., Рублёв Д.П., Фёдоров В.М., Чумаченко А.Б., Макаревич О.Б., Молодяков С.А. и другие ученые. Однако имеется ещё много проблем, требующих своего разрешения. В большинстве известных случаев экспертиза

цифрового изображения может быть выполнена с использованием эффективных методик [1, 2]. Поэтому разработка методик деперсонализации ЦОЭУ, основанных на алгоритмах постобработки цифровых изображений, является актуальной и востребованной.

Целью статьи является проведение анализа признаков цифровых изображений, позволяющих однозначно идентифицировать ЦОЭУ, с помощью которых они были получены, и разработка алгоритма деперсонализации, позволяющего посредством удаления идентификационных признаков ЦОЭУ из создаваемого им цифрового изображения защитить свое оборудование от идентификации сторонними лицами.

Изложение основного материала

Одной из актуальных задач защиты информации является разработка методов обеспечения конфиденциальности пользователя, в первую очередь автора, при создании им цифровых изображений

В традиционной фототехнической экспертизе исследование цифровых изображений выполняется в двух направлениях:

- исследование непосредственно цифровых изображений;
- исследование фотографических материалов, применявшихся для изготовления фотоснимка.

В любом случае каждое из этих направлений связано с решением определенного круга задач, которые можно разделить на идентификационные и диагностические. К идентификационным задачам можно отнести следующие [3]:

- идентификация ЦОЭУ, используемого для создания изображения;
- идентификация фотоматериалов, применявшихся для изготовления фотоснимка;
- идентификация предметов, помещений и участков местности, изображенных на цифровых снимках.

К диагностическим задачам можно отнести:

- установление условий съемки и обработки цифровых изображений;
- определение времени создания снимка;
- восстановление первоначального изображения на фото снимках.

Если представленное на экспертизу цифровое изображение пригодно для идентификационного исследования, то в результате экспертизы можно получить следующие идентификационные данные:

- установление условий съемки;
- определение времени создания изображения;
- восстановление первоначального изображения;
- тип ЦОЭУ, которое применялось для получения изображения;
- наличие последующей цифровой обработки изображений (в графических редакторах и медиаконвертерах);
- программное обеспечение (ПО), применяемое для обработки изображения;
- оценка степени изменения изображения при графической обработке.

К общим признакам документирования характеристик ЦОЭУ, которые отражаются в создаваемом им цифровом изображении, относят размеры кадра и EXIF (Exchangeable Image File Format) данные. EXIF является стандартом, позволяющим добавлять к цифровым изображениям дополнительную информацию (метаданные) [4]. Информация, записанная в EXIF-файл может быть использована, как для идентификации ЦОЭУ, так и различными устройствами и системами, имеющими элементы искусственного интеллекта (например, принтером для прямой печати с ЦОЭУ или нейронными сетями, являющимися составной частью интернет-платформ:

социальных сетей, фотохостингов, файлообменных систем и т.д. при условии размещения в них цифрового изображения) [5, 6].

Для цифровых изображений JPEG-формата алгоритм создания основан на дискретном косинусном преобразовании (ДКП), применяемом к матрице исходного изображения для получения некоторой новой матрицы коэффициентов (цифрового изображения в новом формате). Коэффициенты ДКП получаемой матрицы цифрового изображения можно отнести к групповым признакам ЦОЭУ. Они являются индивидуальными для его модели или серии моделей [7]. ДКП матрицы исследуемого цифрового изображения и полная информация о нем называется EXIF данными.

В общем случае к EXIF данным относятся:

- название модели ЦОЭУ;
- ориентация ЦОЭУ (вертикальная/горизонтальная для устройств со встроенным акселерометром);
- адрес места съёмки – географические координаты (положение точки на земной поверхности);
- дата и время съёмки;
- размеры цифрового изображения;
- разрешение цифрового изображения;
- глубина цвета в битах;
- тип баланса белого;
- фокусное расстояние;
- эквивалентное фокусное расстояние – условная характеристика оптической системы и светочувствительного элемента, дающая информацию об угле обзора этой системы;
- диафрагма;
- использование вспышки;
- ISO – светочувствительность ЦОЭУ;
- светочувствительность сенсора (матрицы), которая была установлена при съёмке;
- ПО, в котором было сделано цифровое изображение (если изображение делается в JPEG-формате, то будет указано ПО ЦОЭУ, которое обработало изображение, если изображение делается в RAW формате, то будет указано ПО, с помощью которого был совершен экспорт в JPEG-формат, например, Adobe Photoshop Camera RAW);
- выдержка в секундах, с которой снято цифровое изображение, интервал времени, в течение которого оптическая система передает изображение на светочувствительную матрицу;
- компенсация выдержки;
- информация о право обладании.

Дополнительно для медиафайлов можно отнести следующие EXIF данные:

- видеоданные;
- аудиоданные;
- flash-содержимое (SWF-формат);
- категории – информация по классификатору агентства Associated Press.

Анализ EXIF данных цифрового изображения, включая цветность и яркость, цветность подвыборки, качество JPEG-настройки, параметры разрешения и многое другое, позволяет осуществить специализированное ПО JPEGsnoop. Оно позволяет определить подлинность цифрового изображения в форматах: JPEG, JPG, THM, AVI, DNG, CRW, CR2, NEF, ORF, PEF, RAW, MOV, PDF, PSD [8]. Одним из важных преимуществ ПО JPEGsnoop является наличие внутренней базы данных, которая сравнивает исследуемое цифровое изображение с большим количеством подписей сжатия (цифровых подписей в шумовых составляющих, которыми маркируется

создаваемое цифровое изображение при его сжатии различными алгоритмами). Это позволяет однозначно определить, какое именно ЦОЭУ применялось для формирования цифрового изображения. ПО JPEG Snoor извлекает из цифрового изображения следующую информацию:

- квантование матрицы (таблицы цветности и яркости);
- цветность подвыборки;
- качество JPEG-контейнера;
- настройки разрешения JPEG-контейнера;
- таблицы Хаффмана, используемые в алгоритмах кодирования для сжатия графической информации;
- Maker notes – примечания производителя фотокамеры, к которым относятся, например, метаданные предустановки баланса белого или сюжетные режимы, применяющиеся во время экспонирования;
- RGB-гистограмма, которая использует все три канала цветности и описывает распределение яркостей в отдельно взятом канале. Гистограмма RGB может показать, есть ли потери в отдельном канале цветности, но она не покажет, в одном канале имеют место потери или во всех. Гистограммы цвета усиливают этот эффект и четко демонстрируют наличие потерь;
- маркеры JPEG (JFIF), каждый из которых начинается с байта 0xFF, свидетельствующего о начале маркера, и байта-идентификатора. Структура JPEG-файла позволяет быстро отыскать маркер с необходимыми данными (например, с длиной строки, числом строк и числом цветовых компонентов сжатого изображения);
- тип VLC декодирования – способ адаптивного кодирования переменной длины (VLC) с эффективным использованием памяти и пониженной сложностью в отношении данных для множества применений, таких как кодирование цифровых видеоданных, данных изображений, звуковых или речевых данных;
- параметры качества, используемые в ПО Adobe Photoshop;
- встроенные в PDF-документы изображения.

В результате проведенного анализа для ЦОЭУ можно выделить следующие аппаратные признаки, на основе которых возможно провести его идентификацию:

1. Для цифровых фото-, видео-, веб-камер:
 - 1.1. Среднеустойчивые признаки объектива и системы крепления байонет (разновидности механического и электронного интерфейса крепления оправы оптической системы (микропроцессоров объектива) к цифровому оптоэлектронному устройству);
 - 1.2. Средне- и высокочастотные устойчивые признаки размытия – необратимой операции, при которой цифровое изображение или его части перераспределяются по некоторому закону. На силу размытия влияют такие физические параметры:
 - геометрическая светосила объектива (диафрагма) – F . Чем меньше число F , тем тоньше глубина резко изображаемого пространства и тем сильнее размыт передний и задний фон изображения;
 - фокусное расстояние объектива. Чем больше фокусное расстояние объектива, тем сильнее будет размыт фон изображения;
 - дистанция фокусировки до объекта съемки (расстояние между фотоаппаратом и снимаемым объектом). Чем меньше дистанция фокусировки, тем сильнее размыт фон изображения;
 - дистанция между объектом съемки и задним фоном. Чем дальше задний фон от объекта съемки, тем сильнее он размыт;
 - оптическая схема (больше влияет именно на характер размытия);
 - размер модуля фотосенсора – светочувствительной матрицы, состоящей из миллионов миниатюрных ячеек-пикселей для получения изображения.

Чем больше его размер, тем больше угол обзора и тем ближе нужно подойти к объекту съемки. Поэтому полноформатные ЦОЭУ сильнее размывают фон изображения;

- специальные насадки и фильтры на объектив;
- фотосенсор (формирует устойчивые признаки всех частот);

2. Для цифровых сканеров изображений:

2.1. Неоднородности светочувствительных элементов линейки сканера;

2.2. Отклонения перемещения каретки сканера от линейного;

2.3. Неравномерность засветки и прижатия к стеклу сканируемого оригинала и т.д.

Кроме перечисленных выше признаков ЦОЭУ, их индивидуальные признаки в значительной степени определяются применяемыми встроенными алгоритмами обработки создаваемых цифровых изображений:

- алгоритмы восстановления изображения из мозаичной структуры фотосенсора, которая основана на принципе измерения только одного цветового компонента в каждой точке фотосенсора, а недостающие вычисляются на основе данных соседних точек. Такая технология позволяет создать фотосенсор, который измеряет три цвета одновременно в каждом пикселе;

- алгоритмы повышения контурной резкости (алгоритм воспроизводит традиционную технику пленочного фотошаблона, используемую для увеличения резкости краев изображения и корректировки размытости, возникшей в результате сканирования, интерполяции или печати) и шумоподавления (алгоритм подавления всех обнаруженных шумов в создаваемом цифровом изображении перед тем, как выполнить его запись на носитель).

В цифровых фото-, видео- и веб-камерах алгоритмы постобработки создаваемых цифровых изображений могут быть как отключаемыми, так и не отключаемыми. В цифровых сканерах получаемое изображение может проходить двухуровневую обработку – в самом сканере на основе калибровочных кривых, подавления следов пыли на (сканируемом носителе и стекле сканера) и на уровне драйвера, где осуществляется субъективное повышение качества цифрового изображения.

Каждому ЦОЭУ (не зависимо от формата создаваемого цифрового изображения) соответствует своя частотно-контрастная характеристика, которая является своеобразной амплитудно-частотной характеристикой (АЧХ) оптической системы и фотосенсора. На разных участках цифрового изображения АЧХ не постоянна, и ее корректное сравнение лучше всего проводить по снимкам радиальной миры (от фр. *mire*, тест-объект для количественного определения разрешающей способности и функции передачи модуляции объектива и светочувствительной матрицы), что на практике не всегда осуществимо. Поэтому к индивидуальным признакам ЦОЭУ можно отнести его паттерн неоднородности световой чувствительности фотосенсора (*photo-response non-uniformity – PRNU*).

Также индивидуальным признаком ЦОЭУ является наличие и расположение загрязнений на его фотосенсоре (фотоматрице), переносимое на цифровые изображения. Этот признак присущ ЦОЭУ зеркального типа, так как на фотосенсор неизбежно попадает пыль вовремя замены объектива. Кроме этого, нередки случаи поверхностного загрязнения оптической системы на неразборных фото-, видео-, веб-камерах и сканерах.

К числу распространенных методов защиты от несанкционированного копирования цифрового контента является применение видимых и невидимых цифровых водяных знаков (ЦВЗ), что также позволяет однозначно идентифицировать ЦОЭУ по создаваемому им цифровому изображению [9]. Внедрение ЦВЗ выполняется с помощью обязательного применения следующих критериев:

- в цифровое изображение внедряется ЦВЗ по специальному алгоритму, который не даёт ему определить – содержатся получаемые изображения ЦВЗ или нет;
- определить наличие ЦВЗ в цифровом изображении можно при наличии секретного ключа;
- возможно доказательство наличия ЦВЗ третьей стороне без раскрытия секретного ключа;
- ЦВЗ выдерживает все типы искажений изображения или максимально возможное их количество, кроме тех, которые делают его практически непригодным к использованию;
- разработаны модели ЦВЗ, стойкие к обрезанию значительной части цифрового изображения, уменьшения размера, разным фильтрам и т.д.

Цифровой шум также является идентификационным признаком цифрового изображения, вносимым фотосенсором ЦОЭУ и с его помощью можно также идентифицировать ЦОЭУ. Под цифровым шумом обычно понимается электрическая погрешность фотосенсора ЦОЭУ. Это явление возникает в результате особенностей преломления света – на фотосенсоре появляются не качественные разноцветные пиксели. Чем больше пикселей содержит фотосенсор, тем меньше их размер. Количество светового потока, принимаемого пикселем, определяется его размером. Поэтому, при повышении количества пикселей приходится повышать их чувствительность, что в свою очередь приводит к увеличению цифрового шума фотосенсора. Цифровой шум проявляется в виде хаотично расположенных точек различных по яркости и цвету. Особенно он заметен на однотонных поверхностях – небо, кожа, участки теней. Цифровой шум придает цифровому изображению неестественный вид – оно кажется «присыпанным» песком [10]. Уровень цифрового шума зависит от технических характеристик фотосенсора и длительности (времени) экспонирования. Цифровой шум характерен для каждого фотосенсора оптоэлектронного цифрового устройства. Особенно, он становится отчетливо виден при увеличении чувствительности: ISO 400, 800, 1600 и т.д., так как возрастает температура фотосенсора. Цифровой шум разделяется на: постоянный, яркостной и хроматический.

Постоянный цифровой шум проявляется одинаково на всех цифровых изображениях, создаваемых ЦОЭУ, и связан с наличием «горячих» и «битых» пикселей его фотосенсора. Формирование «горячих» пикселей связано с тем, что их проявление напрямую зависит от температуры фотосенсора (сигнал с них в разы может отличаться и быть ярче или темнее). «Битые» пиксели, независимо от режима съёмки, могут быть яркими или тёмными, в зависимости от того, в каком режиме они потеряли свою работоспособность: во включённом (яркий, обычно белый пиксель) или выключенном (тёмный, практически чёрный пиксель). На месте «битых» пикселей постоянно присутствуют светлые или темные точки. «Горячие» пиксели проявляются в виде цветных точек, расположенных на одном и том же месте от кадра к кадру при длительных выдержках, когда фотосенсор сильно нагревается. Для того чтобы выявить «горячие» пиксели ЦОЭУ, необходимо закрыть пылезащитной крышкой фотообъектив, выбрать максимальное значение чувствительности ISO, выставить выдержку 30 секунд, отключить встроенное шумоподавление (если оно есть) и сделать несколько контрольных цифровых изображений. Их визуальный анализ покажет наличие или отсутствие «горячих» пикселей.

Яркостной цифровой шум (luminance noise), проявляющийся на изображении в виде маленьких темных точек (или пятен) и напоминающий зерно фотопленки, причем повышение светочувствительности фотопленки сопровождается ростом размеров зерна, из которого состоит изображение. Крупное зерно снижает разрешающую способность фотопленки.

Хроматический цифровой шум (chrominance noise) – шум цветности выглядит неестественно и может сделать изображение непригодным. Проявляется в виде маленьких пятен (точек) другого цвета, отличного от цвета той области, где такой шум проявляется. Хроматический цифровой шум сильно бросается в глаза и неприятен для восприятия.

Относительное количество хроматического и яркостного шума может значительно варьироваться в зависимости от модели камеры.

Проанализировав идентификационные признаки цифровых изображений, авторами работы был разработан алгоритм деперсонализации цифровых изображений (рис. 1), позволяющий защитить от идентификации ЦОЭУ сторонними лицами.

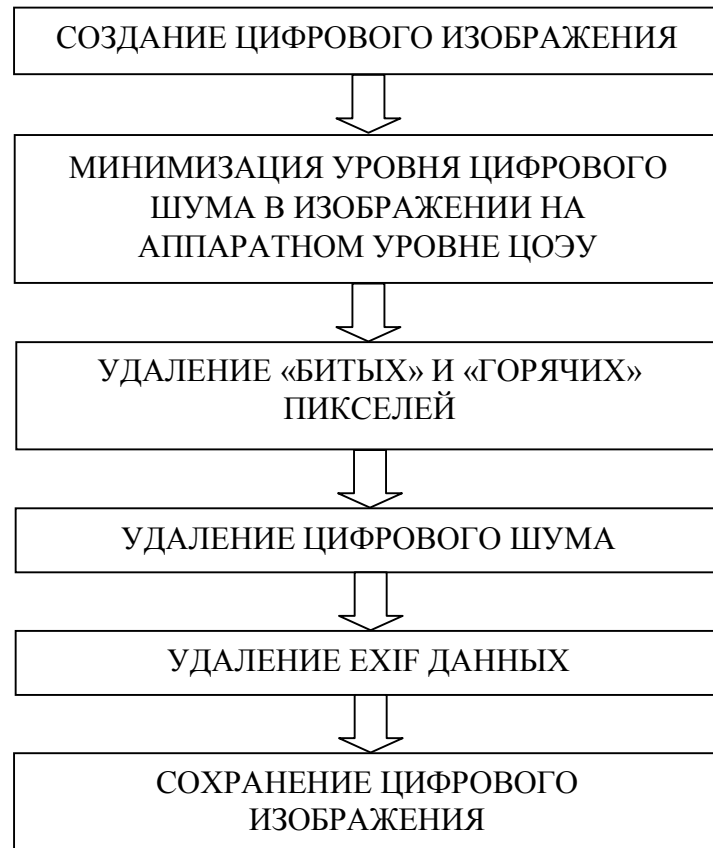


Рис. 1. Алгоритм деперсонализации цифровых изображений

На этапе создания цифрового изображения с минимально возможным уровнем цифрового шума к числу первостепенных рекомендаций относятся [11]:

- уменьшение чувствительности ISO;
- уменьшение выдержки;
- применение более светосильных объективов. Поскольку светосила объектива характеризует способность оптической системы (объектива) пропускать свет, то чем шире будет открыта диафрагма, тем меньше можно сделать выдержку;
- выполнение съемки при хорошем освещении (или с применением вспышки);
- использование встроенной функции шумоподавления;
- следует избегать длительной работы ЦОЭУ без выключения, поскольку может произойти нагрев фотосенсора, особенно в зеркальных фотоаппаратах в режиме фокусировки по ЖК-дисплею);
- сохранение цифровых изображений в RAW-формате, содержащем необработанные данные, полученные с фотосенсора.

Реализация следующих этапов в предлагаемом авторами алгоритме деперсонализации цифровых изображений выполняется с применением специализированного ПО.

На этапе удаления «битых» и «горячих» пикселей для цифровых изображений в RAW-формате применялось специализированное ПО Hot Pixel Eliminator [12], Pixel Fixer [13]. Это ПО способно отличать «горячие» и «битые» пиксели от ярких бликов и источников света и автоматически удалять эти пиксели из необработанных цифровых изображений. Если с помощью специализированного ПО невозможно удалить «битые» и «горячие» пиксели или если создаваемое цифровое изображение сохранено в JPEG-формате, то их удаление можно выполнить вручную в ПО Adobe Photoshop с использованием инструмента Patch Tool.

На этапе удаления цифрового шума пока не существует универсальных алгоритмов. Специализированное ПО, реализующее подобные алгоритмы, не всегда может отличить мелкие детали цифрового изображения от цифрового шума. Вследствие этого, сильное подавление цифрового шума в большинстве случаев приводит к частичной потере мелких деталей и проявляется в виде размытости цифрового изображения. ПО для удаления/подавления цифрового шума должно учитывать следующие факторы:

- модель ЦОЭУ;
- причины возникновения цифрового шума фотосенсора;
- наличие мелких деталей на цифровом изображении.

Такое специализированное ПО должно позволять вручную задавать режимы удаления/подавления цифрового шума, так как восприятие человеческим глазом цифровых изображений субъективно. Практическое использование подобного ПО показало, что пользователь, обладая соответствующими навыками работы, именно в ручных режимах может достигнуть гораздо лучших результатов, чем с применением автоматических режимов. К общим рекомендациям применения специализированного ПО следует отнести применение процедуры удаления/подавления шума до выполнения других операций, таких как: цветокоррекция, изменение яркости/контраста, корректировка размеров и т.д.

В качестве примеров специализированного коммерческого ПО, позволяющего эффективно подавлять цифровой шум изображений, можно применять Adobe Camera RAW и Adobe Light Room. Авторская апробация операции удаления цифрового шума выполнялась с применением специализированного коммерческого ПО Movavi Photo Denoise [14].

Заключительный этап удаления EXIF данных позволяет деперсонализировать ЦОЭУ по вносимым им метаданным в цифровое изображение при его создании, а также скрыть информацию о том, каким специализированным ПО выполнялась постобработка цифрового изображения.

Специализированное ПО, применяемое для выполнения операций с EXIF данными цифровых изображений можно разделить на три группы, каждая из которых состоит из набора характерных функций:

- просмотр метаданных;
- редактирование отдельных тегов метаданных;
- полное удаление метаданных.

Следует отметить, что операция удаления EXIF данных реализуется по тому же принципу, что и их редактирование. Для выполнения этой операции авторами применялось наиболее эффективное специализированное ПО ExifTool, которое доступно для всех платформ. ПО ExifTool распознает дополнительные теги (EXIF чанки, от англ. *chunk* – ячейка, кусок) большинства ЦОЭУ и ПО, применяемое для постобработки цифровых изображений [15].

Выводы и дальнейшие перспективы исследований

Проведенный анализ признаков, однозначно определяющих идентификацию ЦОЭУ по создаваемым ими цифровым изображениям, позволил разработать алгоритм, с помощью которого можно выполнить деперсонализацию цифровых изображений.

Практическое применение разработанного алгоритма деперсонализации цифровых изображений позволяет однозначно защитить свое оборудование от идентификации сторонними лицами посредством разрыва прямой связи между ЦОЭУ и создаваемым им цифровым изображением.

Алгоритм деперсонализации цифровых изображений может быть полезен тем категориям лиц, которые в силу исполнения своих профессиональных обязанностей должны соблюдать повышенные меры личной безопасности по обеспечению своей конфиденциальности при использовании различных ЦОЭУ, в особенности фото-, веб-камер и сканеров.

Список литературы

1. Рублёв, Д.П. Установление авторских прав по неоднородностям цифровых образов / Д.П. Рублёв, В.М. Фёдоров, А.Б. Чумаченко, О.Б. Макаревич // Известия Южного федерального университета. Технические науки. – 2008. – №8. – Т.85. – С. 141-147.
2. Фототехническая экспертиза. URL: <http://www.expertsud.ru/content/view/173/>. (Дата обращения: 3.04.2017).
3. Малюка, А.А. Цифровое изображение как объект судебной фототехнической экспертизы / А.А. Малюка // Актуальные проблемы права. – 2010. – №2. – С. 431-441.
4. Что такое Exif цифрового фотоснимка. URL: <https://profotovideo.ru/polezno-znat/chto-takoe-exif-tsifrovogo-fotosnimka>. (Дата обращения: 3.04.2017).
5. Как Google распознаёт номера домов при помощи нейросети. URL: <http://www.computerra.ru/92627/streetview-goodfellow/> (Дата обращения: 3.04.2017).
6. Другая сторона Цукерберга: чем еще занят основатель Facebook, помимо самой соцсети. URL: <https://bit.ua/2016/03/zuck/> (Дата обращения: 3.04.2017).
7. Khanna, N. Forensic Camera Classification: Verification of Sensor Pattern Noise Approach / N. Khanna, A.K. Mikkilineni, E.J. Delp // Forensic Science Communications (FSC). – 2009. - № 11(1). URL: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/jan2009/research/2009_01_research01.htm (Дата обращения: 3.04.2017).
8. JPEGsnoop 1.7.5 – JPEG File Decoding Utility. URL: <http://www.impulseadventure.com/photo/jpeg-snoop.html>. (Дата обращения: 3.04.2017).
9. Эффективные решения для защиты от мошенничества в цифровом мире. URL: <http://www.smtdp.com>. (Дата обращения: 3.04.2017).
10. Цифровой шум. Цифровой шум – что это такое? Способы борьбы с цифровым шумом. URL: <http://lepser.ru/teoriya-fotografii/tsifrovoy-shum-chto-eto-takoe-sposobyi-borbyi-s-tsifrovym-shumom.html> (Дата обращения: 3.04.2017).
11. Цифровой шум на фотографии. URL: http://www.colorpilot.ru/reduce_noise.html. (Дата обращения: 3.04.2017).
12. HotPixels Eliminator. URL: <http://www.mediachance.com/digicam/hotpixels.htm> (Дата обращения: 3.04.2017).
13. Pixel Fixer. URL: <http://pixelfixer.org> (Дата обращения: 3.04.2017).
14. Movavi Photo Denoise. URL: <https://www.movavi.ru/noise-reduction-software/> (Дата обращения: 3.04.2017).
15. Read, Write and Edit Meta Information! URL: <http://www.sno.phy.queensu.ca/~phil/exiftool/> (Дата обращения: 3.04.2017).

ПРОБЛЕМНІ АСПЕКТИ ДЕПЕРСОНАЛІЗАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ

О.В. Задерейко¹, О.В. Троянський¹, Н.І. Логінова², О.Г. Трофименко³

¹ Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alexander.zadereyko@opu.ua

² Національний університет «Одеська юридична академія»,
Фонтанська дорога, 23, м. Одеса, 65009, Україна

³ Одеська національна академія зв'язку ім. О.С. Попова,
вул. Кузнечна, 1, Одеса, 65029, Україна

У статті розглянуто індивідуальні ознаки цифрових оптоелектронних пристроїв, які дозволяють виконати їх однозначну ідентифікацію за сформованими ними цифровими образами (цифровими зображеннями). Проаналізовано можливості протидії ідентифікації цифрових оптоелектронних пристроїв. Показано, що ефективним способом, який дозволяє протидіяти ідентифікації цифрових оптоелектронних пристроїв є післяопрацювання цифрових образів з використанням спеціалізованого програмного забезпечення. Виконано аналіз спеціалізованого програмного забезпечення, яке застосовується для деперсоналізації цифрових образів, і запропоновано алгоритм їх післяопрацювання, що дозволяє протидіяти ідентифікації цифрових оптоелектронних пристроїв.

Ключові слова: цифрові зображення, цифровий оптоелектронний пристрій, ідентифікація цифрових оптоелектронних пристроїв, EXIF дані, фотосенсор, цифровий шум, деперсоналізація цифрового зображення

PROBLEMATIC ASPECTS OF DEPERSONALIZATION DIGITAL IMAGES

O.V. Zadereyko¹, A.V. Troyanskiy¹, N.I. Loginova², E.G. Trofimenko³

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: alexander.zadereyko@opu.ua

² National University «Odessa Academy Of Law»,
23, Fontanskaya road, Odesa, 65009, Ukraine

³ Odessa National O.S. Popov Academy of Telecommunications,
1, Kuznechna str., Odessa, 65029, Ukraine

The article describes individual attributes of digital optoelectronic devices. These features make it possible to uniquely identify the devices by their digital images. Authors analysed the possibility of countering the identification of the digital optoelectronic devices and showed that the effective way of their countering is the post-processing of digital images with the use of specialized software. Authors Having analysed its use for the digital image depersonalization, we proposed the algorithm of their post-processing to counter the identification of the digital optoelectronic devices.

Key words: digital images, digital optoelectronic devices, digital optoelectronic device identification, EXIF data, photo sensor, digital noise, depersonalization of the digital image

НЕЧІТКА СИСТЕМА ДІАГНОСТУВАННЯ ПАТОЛОГІЧНИХ СТАНІВ МОЛОЧНОЇ ЗАЛОЗИ НА ОСНОВІ ГІСТОЛОГІЧНИХ ЗОБРАЖЕНЬ

Л.О. Дубчак¹, С.О. Вербовий¹, Н.А. Максимів¹, Т.В. Дацко²

¹ Тернопільський національний економічний університет,

вул. Львівська, 11, м.Тернопіль, 46020, Україна; e-mail: dlo@tneu.edu.ua

² Тернопільський державний медичний університет ім. І.Я. Горбачевського,
майдан Волі, 1, м.Тернопіль, 46001, Україна; e-mail: datskotv@gmail.com

Розповсюдженість раку молочної залози посідає перше місце в структурі онкологічних захворювань жінок. Експертна постановка діагнозу таких патологічних станів базується на якісних показниках аналізу гістологічних зображень, тому розробка засобів їх опрацювання дозволяє зробити процес постановки правильного діагнозу швидшим та точнішим для експерта. У даній статті запропоновано нечітку систему діагностування передракових та ракових станів молочної залози, що базується на ознаках, отриманих від лікаря-діагноста. Розроблена система може застосовуватися в онкомедицині, що дозволить здійснювати постановку діагнозу в реальному часі та виключаючи суб'єктивний характер постановки діагнозу лікарем.

Ключові слова: нечітка логіка, нечітка система, гістологічне зображення, молочна залоза, передракові стани, діагноз

Вступ

Рак молочної залози в Україні, так само, як і в більшості країн світу, з кожним роком розповсюджується і на сьогоднішній день посідає одне із передових місць в базі захворюваності і смертності від злоякісних новоутворень серед жінок (25% від усіх випадків раку). В Україні рак молочної залози є однією з основних медико-соціальних проблем сучасної системи охорони здоров'я внаслідок значної поширеності та високого рівня інвалідності та смертності від нього [1, 2].

Визначення діагнозу базується на достовірних показниках синтезу гістологічних зображень, а оцінка передракових станів зазвичай ґрунтується на кількісних ознаках.

Розповсюдженість програмних засобів опрацювання гістологічних зображень допускає створення процесу утвердження точного діагнозу найшвидшим та найточнішим для експерта. Для постановки точного діагнозу, базуючись на якісних ознаках зображень, виключаючи суб'єктивність суджень експерта, варто використати апарат нечіткої логіки. Нечіткі системи можуть оперувати вхідною інформацією, яка задана нечітко, наприклад, словесно, лікарем-експертом, здійснювати нечіткі формалізації критеріїв оцінки і порівняння, проводити якісні оцінки вхідних даних і виведених результатів за їхнім ступенем вірогідності та розподілом, проводити швидке моделювання складних динамічних систем і їхній порівняльний аналіз із заданим ступенем точності. Такий підхід дозволить побудувати систему постановки діагнозу патологічних станів молочної залози, яка працюватиме в режимі реального часу та буде здатною до швидкого переналаштування.

Основна частина

Нечіткі множини зазначаються через певну базову шкалу B і функцію належності $\mu(x)$, $x \in B$, яка набуває значення на інтервалі $[0...1]$. Таким чином, нечітка множина B – сукупність пар типу $(x, \mu(x))$, де $x \in B$. Часто зустрічається такий запис:

$$B = \sum_{i=1}^n \frac{x_i}{\mu(x_i)}, \quad (1)$$

де x_i – i -те значення базової шкали.

Функція належності визначає суб'єктивний степінь впевненості експерта в тому, що дане конкретне значення базової шкали відповідає значенню нечіткої множини.

Задання продукційних правил базується на визначенні таких нечітких правил, щоб побудований на їх основі модуль керування при одержанні вхідних сигналів генерував певні вихідні сигнали. Через це потрібно розділити простір вхідних і вихідних сигналів на множини та задати відповідні для них функції належності; записати нечіткі правила на базі експериментальної вибірки, створити таблицю для запису бази продукційних правил та таблицю істинності правил (присутність або відсутність ознак); надати усім правилам степінь істинності та згенерувати відповідні правила, сформувати базу нечітких правил.

Нечітке моделювання в середовищі Matlab відбувається на основі застосування пакету розширень Fuzzy Logic Toolbox, в якому представлена велика кількість функцій нечіткої логіки і нечіткого виводу [3].

При нечіткому моделюванні зазвичай застосовують апарат нечіткого висновку Мамдані, в якому база знань складається з правил виду: «якщо, то». Нечіткі моделі на основі такого підходу є доступними, їх будова змістовно трактується в термінах, зрозумілих як розробникам з високою математичною кваліфікацією, так і замовникам – лікарям, економістам, менеджерам. Доступність нечітких моделей Мамдані – одна з найголовніших переваг, адже завдяки нечіткій логіці вони успішно конкурують з іншими методами, особливо для тих прикладних задач, де можливість змістовної інтерпретації важливіша точності моделювання [4-7].

В якості експериментальних досліджень використано тестову вибірку гістологічних зображень, отриману від експерта. Вхідними змінними є геометричні ознаки даних зображень [8].

Гістологічні зображення – це зображення зрізів біологічної тканини, як показано на рис. 1.

У гістології використовуються різні способи проведення експериментів, які дають змогу різносторонньо аналізувати процеси прогресу, побудови і функціонування мікрооб'єктів, матерій та органів. Найважливішими кроками гістологічного синтезу є селекція об'єктів експерименту, процес підготовки його для вивчення в мікроскопі та використання способів мікрокопіювання.

Діагностика передракових станів, як правило, вимагає саме біомедичних експериментів. Зібрання гістологічних зрізів – один із найточніших методів контролювання якостей досліджень.

Синтез злоякісних утворень на базі біомедичних зображень здійснюється наглядно, що є вагомим, проте не вирішальним, адже для всебічного опису утворень необхідні кількісні ознаки, що одержуються методом числового морфометричного синтезу, що знижує суб'єктивність експерта.

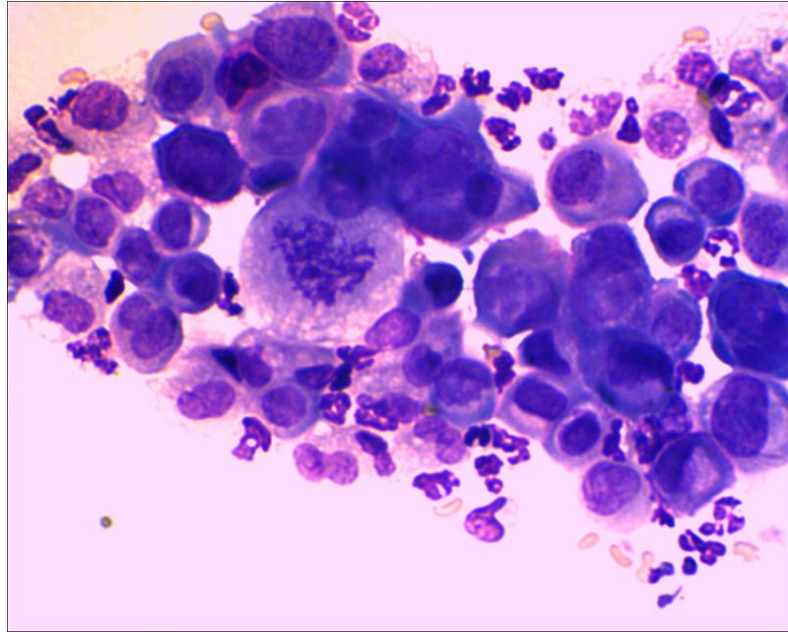


Рис. 1. Гістологічне зображення

Для задання якісних ознак необхідно підсумувати досвід експерта-морфолога: логічні дерева рішень, опис клітини та постановки діагнозу. Описові знання дозволено задавати у формі особливої онтології опису клітин, котра вміщає усі дані про ракові клітини. Відлагодження та послідовна онтологія налічується з всіх вказаних морфологічних ознак, котрі досліджуються в окремий спосіб. Морфологічні показники мають задаватись і «замірятися» підсвідомо таким чином, щоб онтологія використовувалась для автоматичного і для ручного морфологічного дослідження.

Вихідна змінна формується з умовиводів фахівця на базі вхідних змінних про наявність виявлення діагнозу та складається з п'яти нечітких множин, а саме: проліферативна мастопатія (proliferative breast disease), непроліферативна мастопатія (nonproliferative breast disease), фіброаденома (fibroadenoma), внутрішньопротоковий та інвазивний рак (intraductal and invasive cancer).

Функції належності пропонованої нечіткої системи засновані на одержаних фахівцем знаннях з ознак передракових та ракових діагнозів. Наприклад, діагностування внутрішньопротокового раку відбувається на основі наявності таких ознак:

- поліморфізм клітин;
- різке збільшення розмірів клітин;
- атипові мітози;
- накопичування пухлинних клітин в просвітах протоків;
- поодинокі некрози клітин;
- клітини не інфільтрують через базальну мембрану протоків.

Інвазивний рак, в свою чергу, може діагностуватися, якщо на гістологічному зображенні лікар-експерт відмітить:

- різке збільшення розмірів клітин;
- поліморфізм клітин;
- атипові мітози;
- інвазивний ріст в навколишню тканину (в жирову клітковину);
- стертість базальних мембран;
- проникнення пухлинних клітин через базальну мембрану;
- наявність мікроальвеолярних або тубулярних структур;

- множинні некрози клітин;
- мікрокальцифікації.

Ознаки діагностування фіброаденоми:

- проліферація альвеол;
- проліферація внутрішньодолькових протоків;
- наявність рихлої базофільної сполучної тканини;
- наявність грубої оксифільної сполучної тканини;
- протоки вистелені епітелієм та міоепітелієм різного функціонального стану;
- мікроепітелій (видовжені темні клітини, або світлі із шаровидними

включеннями);

- формування химерних залозистих структур;
- гіаліноз сполучної тканини та атрофія епітелію.

Ознаки, які підтверджують діагноз непроліферативної мастопатії, наступні:

- мілкі кісти із альвеол однієї дольки;
- кісти розташовуються гніздами;
- кістозно розширені протоки;
- гіаліноз сполучної тканини;
- проліферація сполучної тканини;
- метаплазія темного епітелію в блідий (світлий);
- наявність великої кількості сполучної тканини навколо залоз і протоків

свідчить про їх атрофію;

- утворення псевдососочків;
- атрофія залозистих ділянок і утворення кіст.

Ознаки діагностування проліферативної мастопатії:

- проліферація міоепітелію та ендотелію дрібних протоків;
- розширення між часточкових протоків;
- проліферація дрібних протоків і альвеол;
- незначна частинна строма;
- відсутня базальна мембрана;
- проліферуючі міоепітеліальні клітини переміщуються у внутрішню часточкову сполучну тканину і стають схожі на гладенькі м'язи.

Використовуючи навчальну вибірку гістологічних зображень та їхні якісні ознаки необхідно побудувати функції належності.

Для побудови нечіткої системи постановки діагнозу патологічних станів молочної залози використано засіб FuzzyLogicToolbox середовища Matlab. Якісні ознаки виступають вхідними даними, а вихідними – поставлений діагноз (рис. 2).

Вхідні дані, якими виступають описані вище ознаки патологічних станів, задаються у вигляді дзвоноподібної функції належності. Варто зазначити, що усі вхідні змінні можуть бути лише присутні або відсутні на гістологічному зображенні, тому вони задаються нечіткими множинами, поданими на рис. 3.

Вихідні дані виступають власне діагнозом, отриманим з продукційних правил, тому вони матимуть вигляд трикутної функції належності, як зображено на рис. 4.

Продукційні правила є невід'ємною частиною бази знань. Кожне продукційне правило відображає окрему частину знань, отриманих від експерта. Продукційні правила можна модифікувати як окрему одиницю незалежно від інших правил.

В медичній експертній системі такі правила використовуються для встановлення зв'язків між симптомами, чи якісними ознаками, та діагнозом.

В запропонованій нечіткій системі є 187 продукційних правил, частина яких показана на рис. 5.

Перевірка роботи нечіткої системи здійснюється шляхом аналізу бази продукційних правил (рис. 6).

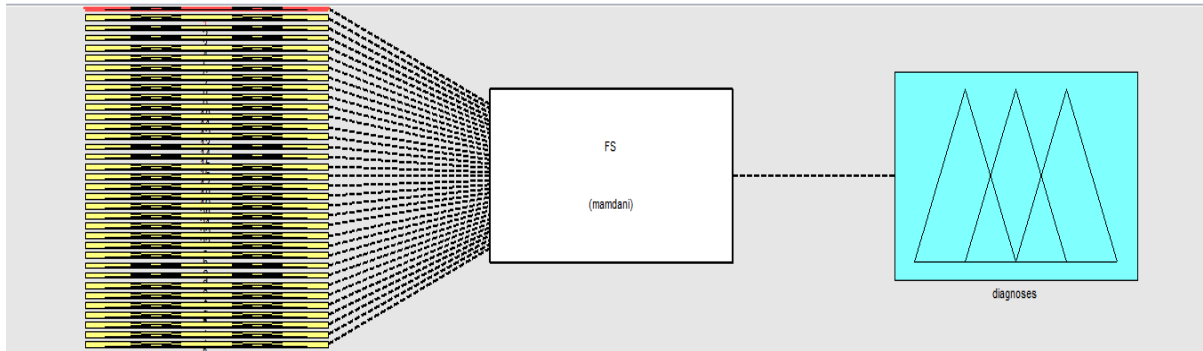


Рис. 2. Схема розробленої нечіткої системи в редакторі «Fuzzy Logic Toolbox»

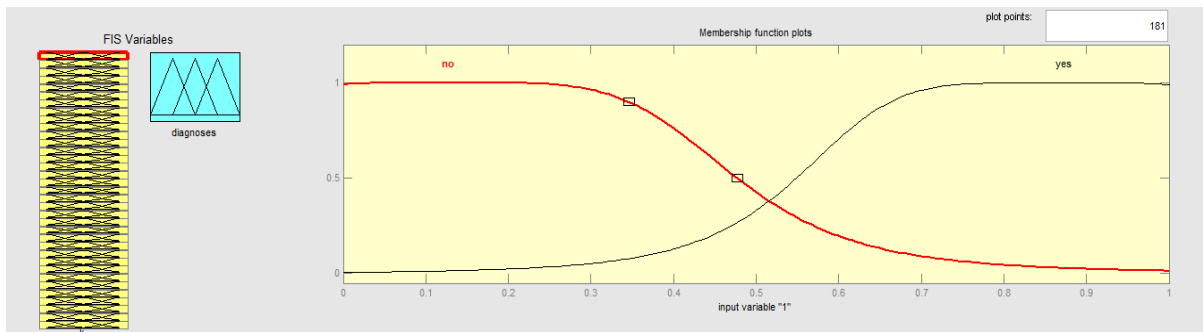


Рис. 3. Функції належності входних змінних нечіткої системи постановки діагнозу

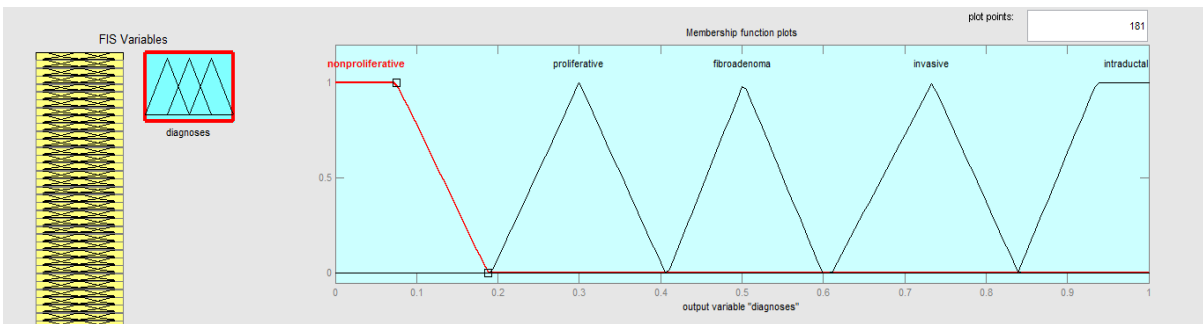


Рис. 4. Функції належності вихідних даних

```

171. If (a is yes) and (b is yes) and (c is yes) and (j is yes) and (l is yes) then (diagnoses is intraductal) (1)
172. If (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
173. If (b is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
174. If (a is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
175. If (a is yes) and (b is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
176. If (c is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
177. If (b is yes) and (c is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
178. If (a is yes) and (c is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
179. If (a is yes) and (b is yes) and (c is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
180. If (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
181. If (b is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
182. If (a is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
183. If (a is yes) and (b is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
184. If (c is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
185. If (b is yes) and (c is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
186. If (a is yes) and (c is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)
187. If (a is yes) and (b is yes) and (c is yes) and (j is yes) and (k is yes) and (l is yes) then (diagnoses is intraductal) (1)

```

Рис. 5. Приклад запису продукційних правил в редакторі «Rule editor»

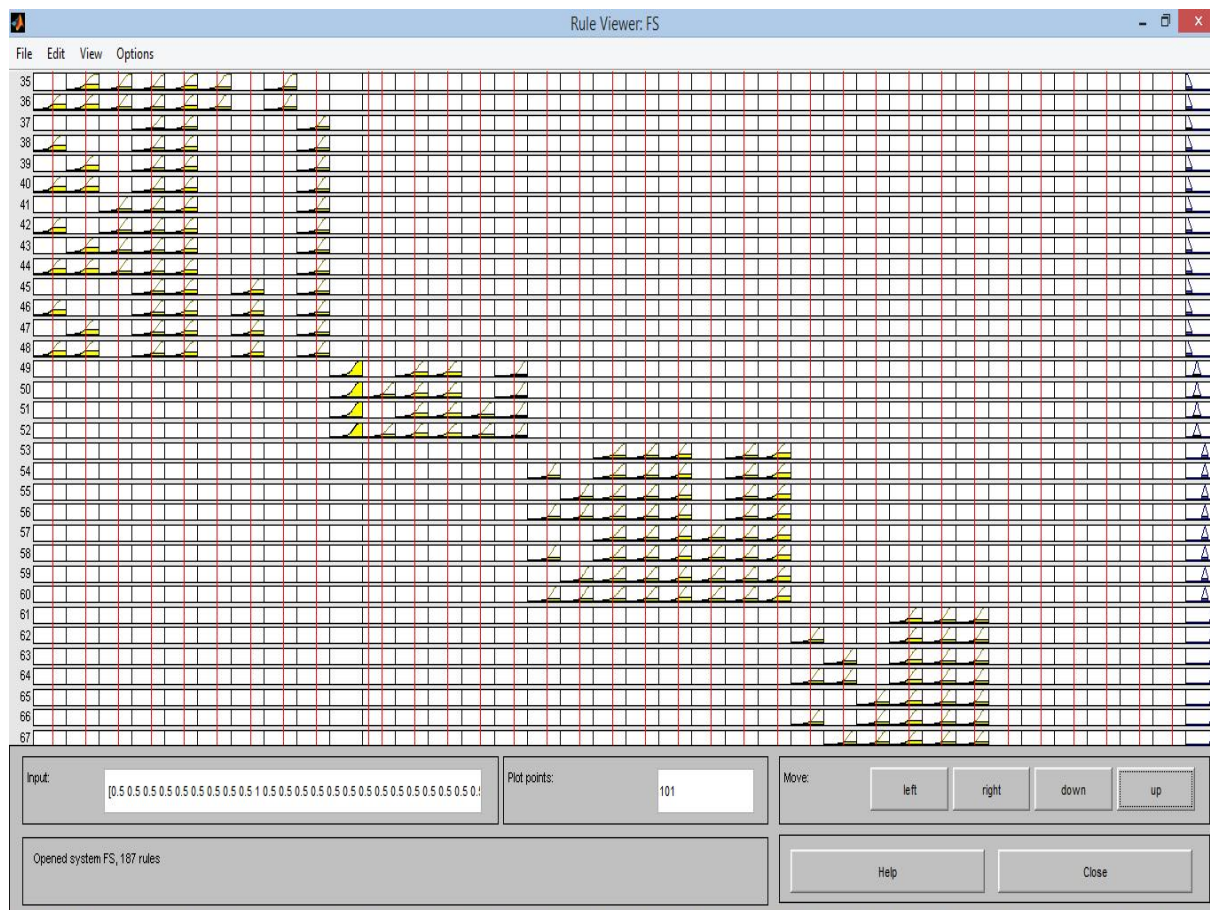


Рис. 6. Приклад роботи бази продукційних правил розробленої нечіткої системи

Аналіз роботи нечіткої системи свідчить про її працездатність та правильність роботи, тому можна стверджувати, що розроблена нечітка система діагностування патологічних станів молочної залози може реалізовуватись апаратно чи програмно і застосовуватись в онкотелемедицині.

Висновки

У роботі проведено розробку нечіткої системи діагностування патологічних станів молочної залози на основі аналізу гістологічних зображень. Робота запропонованої нечіткої системи базується на опрацюванні бази 187 продукційних правил. Для дослідження використовувалися ознаки патологічних станів на гістологічних зображеннях, отримані від лікаря-експерта. Розроблена нечітка система може застосовуватися для постановки точного діагнозу патологічного стану молочної залози в режимі реального часу, виключаючи суб'єктивний характер постановки діагнозу лікарем.

Список літератури

1. Berezsky, O. Fuzzy system diagnosing of precancerous and cancerous conditions of the breast / O. Berezsky, S. Verbovy, L. Dubchak, T. Datsko // XIth International Scientific and Technical Conference "Computer Sciences and Information Technologies (CSIT), 2016. – Pp. 200-203.
2. Berezsky, O. Fuzzy System of Diagnosing in Oncology Telemedicine / O. Berezsky, S. Verbovy, L. Dubchak, T. Datsko // Sensors & Transducers. – 2017. – Pp. 32-38.

3. Штовба, С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д. Штовба // Проблемы управления. – 2007. – №4. – С. 102-104.
4. Дубчак, Л.О. Метод обробки нечітких даних на основі механізму Мамдані / Л.О. Дубчак // Системи обробки інформації. – 2012. – №7(105). – 131 с.
5. Дубчак, Л.О. Спосіб обробки нечіткої інформації / Л.О. Дубчак // Вісник Східноукраїнського національного університету ім. В.Даля. – 2012. – №8 (179), Ч.1. – С. 306-309.
6. Abadeh, M.S. Intrusion Detection Using a Fuzzy Genetics-Based Learning Algorithm / M.S. Abadeh, J. Habibi, C. Lucas // Journal of Network and Computer Applications. – 2007. – №30. – Pp. 414-428.
7. Ross, T.J. Fuzzy Logic with Engineering Applications / T.J. Ross. – McGraw-Hill Inc.(USA), 1995. – 600 p.
8. Berezhsky, O. Computer diagnostic tools based on biomedical image analysis / O. Berezhsky, O. Pitsun, S. Verbovyi, T. Datsko, A. Bodnar // XIV-th of the International Conference on The Experience of Designing and Application of CAD Systems in Microelectronics, CADSM'2017. – Pp. 388-391.

НЕЧЕТКАЯ СИСТЕМА ДИАГНОСТИКИ ПАТОЛОГИЧЕСКИХ СОСТОЯНИЙ МОЛОЧНОЙ ЖЕЛЕЗЫ НА ОСНОВАНИИ ГИСТОЛОГИЧЕСКИХ ИЗОБРАЖЕНИЙ

Л.О. Дубчак¹, С.О. Вербовой¹, Н.А. Максимив¹, Т.В. Дацко²

¹ Тернопольский национальный экономический университет,

ул. Львовская, 11, Тернополь, 46020, Украина; E-mail: dlo@tneu.edu.ua

² Тернопольский государственный медицинский университет им. И.Я. Горбачевского, площадь Воли, 1 Тернополь, 46001, Украина; E-mail: datskotv@gmail.com

Распространенность рака молочной железы занимает первое место в структуре онкологических заболеваний женщин. Экспертная постановка диагноза таких патологических состояний базируется на качественных показателях анализа гистологических изображений, поэтому разработка средств их обработки позволяет сделать процесс постановки правильного диагноза быстрее и точнее для эксперта. В данной статье предлагается нечеткую систему диагностирования раковых состояний молочной железы, основанной на признаках, полученных от врача-диагноста. Разработанная система может применяться в онкологии, что позволит осуществлять постановку диагноза в реальном времени и исключая субъективный характер постановки диагноза врачом.

Ключевые слова: нечеткая логика, нечеткая система, гистологическое изображение, молочная железа, патологические состояния, диагноз

FUZZY SYSTEM DIAGNOSING OF PATOLOGY CONDITIONS OF THE BREAST BASED ON HISTOLOGICAL IMAGES

L.O. Dubchak¹, S.O. Verbovyi¹, N.A. Maksymiv¹, T.V. Datsko²

¹ Ternopil National Economic University,

ul. Lviv, 11, Ternopil, 46020, Ukraine; E-mail: dlo@tneu.edu.ua

² I.Ya. Horbachevsky Ternopil State Medical University, Freedom Square, 1 Ternopil, 46001, Ukraine; E-mail: datskotv@gmail.com

Prevalence of breast cancer ranks first in the structure of women cancer. Expert diagnosis of pathological states based on qualitative performance analysis of histological images, so development processing allows making the correct diagnosis process faster and more accurate for the expert. This paper proposes a fuzzy system diagnosing of precancerous and cancerous breast conditions based on attributes obtained from the doctor-diagnostician. The system can be used in cancer medicine that will allow diagnosing in real time and eliminating subjective diagnosis by a doctor.

Keywords: fuzzy logic, fuzzy system, microscopic images, breast, pathology conditions, diagnosis

СИНТЕЗ И МОДЕЛИРОВАНИЕ РЕГУЛЯТОРА ДЛЯ ОБЪЕКТА С ИЗМЕНЯЮЩИМИСЯ ПАРАМЕТРАМИ

С.А. Бобриков, Е.Д. Пичугин, С.И. Кысса

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: Bobrikov1932@gmail.com

Проведен синтез регулятора для объекта, параметры которого – коэффициент усиления и постоянная времени, могут изменяться в широких пределах. Заданная часть системы включает в себя исполнительный механизм (звено первого порядка) с неизменяющимися параметрами и двигатель – звено второго порядка с изменяющимися параметрами. Регулятор обеспечивает постоянство показателей качества системы при любых значениях переменных параметров объекта в заданном диапазоне их значений. В качестве показателей процесса приняты максимальное перерегулирование в переходной характеристике и время переходного процесса. Разработана структурная схема регулятора и метод расчета его параметров. Работа выполнена путём моделирования системы в пакете MATLAB-Simulink.

Ключевые слова: регулятор, система управления, передаточные функции, моделирование, переходная характеристика, показатели качества управления, объект управления, исполнительный механизм, усилитель, обратная связь, адаптивная система

Введение

Известны системы управления объектами, в которых параметры могут изменяться в широких пределах (нестационарные объекты), например, крупнотоннажные морские суда (с грузом и без груза), управляемая ракета и др. Для обеспечения высоких показателей качества процесса управления при построении подобных систем используют методы адаптивного управления, что приводит, как правило, к существенному усложнению управляющего устройства [1-5]. В данной работе рассматривается система управления нестационарным объектом, построенная без использования методов, свойственных адаптивным системам, и, вместе с тем, позволяющая получить требуемые показатели качества управления при условии, что параметры объекта управления изменяются в широких пределах ($1 \div 10$).

Цель работы

Целью работы является моделирование и синтез управляющего устройства для нестационарного объекта без использования методов адаптивного управления. Устройство обеспечивает заданные показатели качества в пределах заданного диапазона изменения параметров объекта. В качестве показателей принято минимальное перерегулирование при заданной верхней границе времени переходного процесса.

Обобщенная структурная схема разрабатываемой системы показана на рис. 1, где приняты следующие обозначения: $K_{yy}(p)$ – передаточная функция управляющего устройства, $K_{ym}(p)$ – передаточная функция усилителя мощности (исполнительного

устройства), $K_{oy}(p)$ – передаточная функция объекта управления. Полагаем, что заданная часть системы (исполнительное устройство и объект управления) описываются следующими передаточными функциями:

$$K_{ym}(p) = \frac{K_1}{T_1 p + 1}, \quad K_{oy}(p) = \frac{K_2}{(T_2 p + 1)p},$$

где K_1, T_1, K_2, T_2 – параметры.

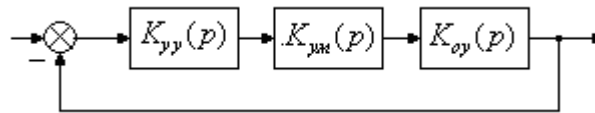


Рис. 1. Обобщенная структурная схема системы управления

Принимаем условие, что параметры объекта K_2 и T_2 в процессе работы системы могут изменяться в заданных пределах.

Разрабатываемое управляющее устройство должно обеспечить работу системы с заданными показателями качества при любых возможных значениях параметров объекта.

Основная часть

Структурная схема системы с управляющим устройством, обеспечивающим независимость принятых показателей качества от параметров объекта, изменяющихся в заданных пределах ($K_{2min} \leq K_2 \leq K_{2max}$, $T_{2min} \leq T_2 \leq T_{2max}$), приведена на рис. 2.

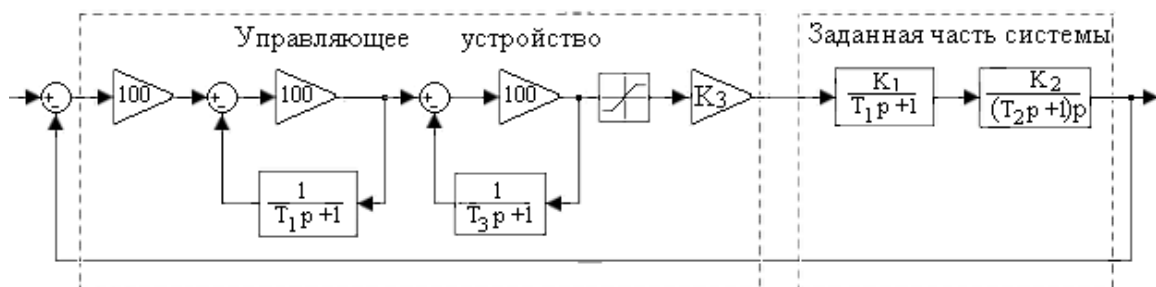


Рис. 2. Структурная схема разрабатываемой системы

Особенностью управляющего устройства в системе (рис. 2) является наличие двух усилителей, каждый из которых охвачен обратной связью через апериодическое звено первого порядка. Управляющее устройство содержит также нелинейное звено типа «насыщение». Величину насыщения примем равной ± 1 , а коэффициент усиления в линейной части характеристики примем равным 1.

Определим передаточную функцию усилителя, охваченного отрицательной обратной связью через апериодическое звено (рис. 3):

$$K(p) = \frac{K}{1 + \frac{K}{Tp+1}} = \frac{K(Tp+1)}{Tp+1+K} = \frac{K(Tp+1)}{(1+K)(\frac{T}{1+K}p+1)}.$$

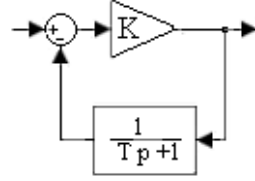


Рис. 3. Структурная схема усилителя с обратной связью через апериодическое звено

Приняв условие, что $K=100$, получим:

$$K(p) = \frac{0.99(Tp+1)}{0.0099Tp+1} \approx \frac{Tp+1}{0.01Tp+1}. \quad (1)$$

Запишем передаточную функцию разомкнутой системы (рис. 2), учитывая (1) и рассматривая нелинейное звено как пропорциональное с коэффициентом 1:

$$\begin{aligned} K(p) &= \frac{100(T_1p+1)(T_3p+1)K_3K_1K_2}{(0.01T_1p+1)(0.01T_3p+1)(T_1p+1)(T_2p+1)p} = \\ &= \frac{100K_c(T_3p+1)}{(0.01T_1p+1)(0.01T_3p+1)(T_2p+1)p}. \end{aligned} \quad (2)$$

где $K_c = K_1K_2K_3$.

Передаточная функция замкнутой системы (без учёта насыщения в нелинейном звене) равна:

$$\begin{aligned} W(p) &= \frac{100K_c(T_3p+1)}{(0.01T_1p+1)(0.01T_3p+1)(T_2p+1)p + 100K_c(T_3p+1)} = \\ &= \frac{100K_c(T_3p+1)}{a_0p^4 + a_1p^3 + a_2p^2 + a_3p + a_4}, \end{aligned}$$

где

$$\begin{aligned} a_0 &= 10^{-4}T_1T_3T_2; \quad a_1 = 10^{-4}T_1T_3 + 0.01T_2(T_1 + T_3); \quad a_2 = 0.01(T_1 + T_3) + T_2; \\ a_3 &= 1 + 100K_cT_3; \quad a_4 = 100K_c. \end{aligned} \quad (3)$$

Отметим некоторые особенности рассматриваемой системы. Управляющее устройство представляет собой два реальных дифференцирующих звена, усилитель и нелинейное звено типа насыщение, включенных последовательно. Постоянная времени дифференцирования первого звена выбирается равной постоянной времени усилителя в заданной части системы. Полагаем, что этот параметр известен и не меняется в процессе работы системы. Постоянная времени дифференцирования

второго звена T_3 определяется диапазоном возможных значений параметров объекта управления T_2 и K_2 . Вопрос о выборе её величины рассмотрен далее.

Наличие в управляющем устройстве двух дифференцирующих звеньев, включенных последовательно, приводит к тому, что при ступенчатом входном воздействии на выходе этих звеньев сигнал может принимать очень большую величину, что в последующих звеньях не может быть реализовано. Для подтверждения этого определим начальное значение сигнала на выходе регулятора при ступенчатом единичном входном сигнале.

Передаточная функция цепи, состоящей из двух дифференцирующих звеньев и линейного усилителя с коэффициентом 100, включенных последовательно (рис. 2) равна:

$$K_1(p) = \frac{100(T_1 p + 1)(T_3 p + 1)}{(0.01 T_1 p + 1)(0.01 T_3 p + 1)} = \frac{Y_{yy}(p)}{G(p)},$$

где $Y_{yy}(p)$ – изображение сигнала на выходе управляющего устройства, $G(p)$ – изображение входного сигнала.

Пусть входной сигнал – единичное ступенчатое воздействие, тогда $G(p) = \frac{1}{p}$.

При этом

$$Y_{yy}(p) = \frac{100(T_1 p + 1)(T_3 p + 1)}{p(0.01 T_1 p + 1)(0.01 T_3 p + 1)}.$$

Начальное значение сигнала на выходе управляющего устройства определим, используя теорему о связи между значениями изображения и оригинала при $t = 0$ [8]:

$$y_{yy}(0) = \lim_{p \rightarrow \infty} p Y_{yy}(p) = \lim_{p \rightarrow \infty} \frac{100(T_1 p + 1)(T_3 p + 1)}{(0.01 T_1 p + 1)(0.01 T_3 p + 1)} = 10^6.$$

Никакое реальное линейное звено, стоящее за управляющим устройством с такой передаточной функцией, отреагировать адекватно на ступенчатый входной сигнал не может. Поэтому после дифференцирующих звеньев включен нелинейный элемент типа «насыщение». Принято условие, что в линейной части характеристики этого звена коэффициент усиления равен 1, а максимальное значение на выходе равно 1.

Принимаем условие, что регулятор должен обеспечить заданные динамические свойства системы при условии, что параметры объекта в процессе нормальной работы системы могут изменяться в заданных интервалах: $K_{2\min} \leq K_2 \leq K_{2\max}$, $T_{2\min} \leq T_2 \leq T_{2\max}$.

В качестве заданных динамических свойств принимаем минимальное перерегулирование в переходной характеристике ($\sigma_{\max} \leq 5\%$), и время регулирования $t_p \leq T_{2\max}$. Время регулирования определим, как интервал времени от начала подачи на вход системы единичного ступенчатого сигнала до момента, после которого ошибка управления не превышает 1%.

Расчетными параметрами регулятора являются T_3 и K_3 . Для определения зависимости показателей качества от параметров регулятора и заданной части системы были проведены исследования системы путём моделирования в пакете

MATLAB-Simulink [10]. Схема набора модели приведена на рис. 4. По результатам моделирования построены графики, приведенные на рис. 5. Для удобства пользования графиками масштабы величины $T_{0\min}$ (ось абсцисс) различны: на рис. 5, а – $0 < T_{0\min} \leq 1$, на рис. 5, б – $0 < T_{0\min} \leq 15$. По оси ординат отложены значения T_3 , соответствующие минимуму перерегулирования и времени переходного процесса $t_p \leq T_{2\max}$. Графики построены для случая, когда коэффициент системы $K_c = 1$, а коэффициент усиления объекта имеет наименьшее значение.

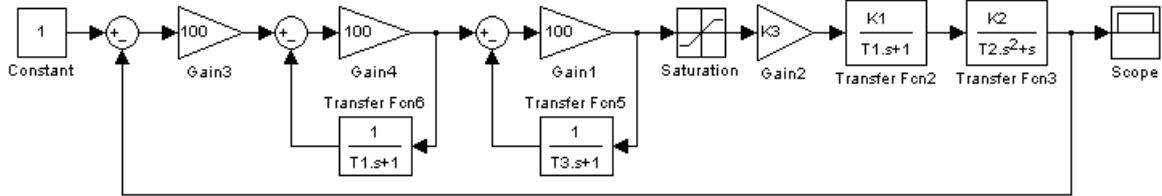


Рис. 4. Схема набора модели в системе Simulink

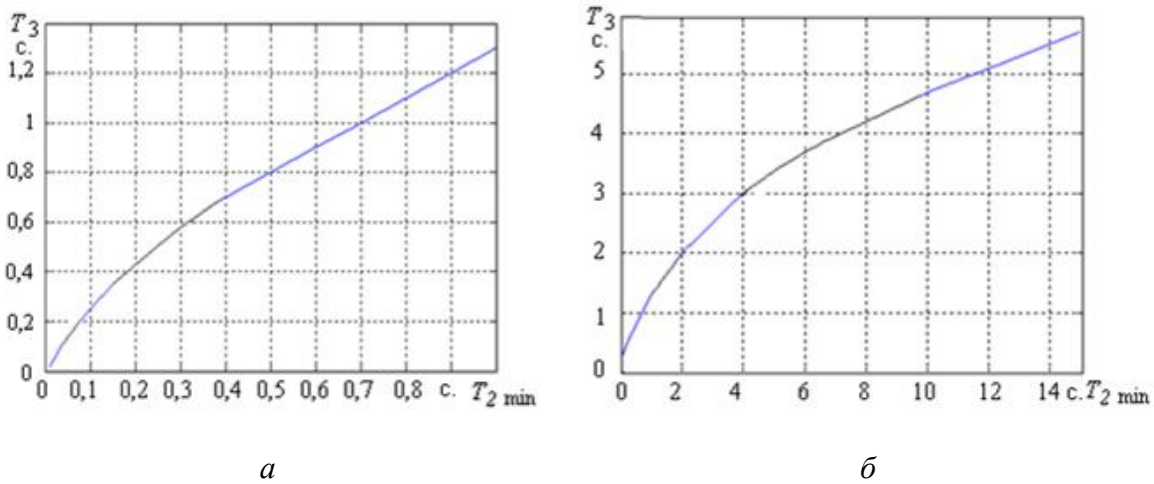


Рис. 5. Зависимость T_3 от минимального значения постоянной времени объекта управления $T_{2\min}$: а – в диапазоне $0 < T_{0\min} \leq 1$; б – в диапазоне $0 < T_{0\min} \leq 15$

Принимаем, что коэффициент усиления системы K_c равен:

$$K_c = K_1 K_{2\min} K_3 = 1. \quad (4)$$

Как показали экспериментальные исследования, увеличение коэффициента усиления, а также постоянной времени объекта в 10 раз практически не влияет на величины принятых показателей качества ($\sigma_{\max} \leq 5\%$, $t_p \leq T_{2\max}$).

Определим условие устойчивости замкнутой системы (рис. 2), полагая, что насыщение в нелинейном элементе отсутствует. При этом коэффициент усиления нелинейного звена равен 1. При увеличении амплитуды входного сигнала выше зоны насыщения коэффициент усиления звена будет уменьшаться, следовательно, коэффициент усиления нелинейного звена, равный 1, есть его наибольшее значение а, значит, для устойчивости условия наихудшие.

Для исследования системы на устойчивость воспользуемся критерием устойчивости Гурвица. В соответствии с критерием условия устойчивости определяются следующими неравенствами:

$$\Delta_3 = \begin{vmatrix} a_1 & a_3 & 0 \\ a_0 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{vmatrix} > 0; \quad \Delta_2 = \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix} > 0. \quad (5)$$

Подставив значения коэффициентов уравнения (3) в неравенства (5) находим условие устойчивости для коэффициента усиления системы K_c :

$$K_c < \frac{(T_1 + T_3)[10^{-4}T_1T_3 + T_2(0,01(T_1 + T_3) + T_2)]}{T_3^2T_2T_1}.$$

Для оценки предельного значения коэффициента K_c можно пользоваться упрощенным выражением:

$$K_c < K_{kp} \approx \frac{(T_1 + T_3)T_2}{T_3^2T_1}, \quad (6)$$

где K_{kp} – критическое значение коэффициента, соответствующее границе устойчивости.

Расчет управляющего устройства проводим в такой последовательности. Пусть заданы следующие величины: параметры усилителя мощности – K_1 , T_1 , и параметры объекта управления – $K_{2\min} \leq K_2 \leq K_{2\max}$, $T_{2\min} \leq T_2 \leq T_{2\max}$. Полагаем, что $K_{2\max} \leq 10K_{2\min}$ и $T_{2\max} \leq 10T_{2\min}$. По кривым рис. 3 для заданной величины $T_{2\min}$ находим соответствующее значение T_3 . Затем определяем величину коэффициента K_3 из условия (4): $K_3 = \frac{1}{K_1K_{2\min}}$.

По формуле (6) проверяем критическое значение коэффициента усиления системы K_{kp} . Так как графики рис. 5 построены для значения $K_c = 1$, очевидно, что для обеспечения запаса устойчивости должно выполняться условие $K_{kp} > 1$.

Примеры.

1. Заданная часть системы.

Коэффициент усиления и постоянная времени исполнительного устройства: $K_1 = 10$, $T_1 = 0.02$ с.

Коэффициент усиления и постоянная времени объекта управления: $K_2 = 0.2 - 2$, $T_2 = (0.15 - 1.5)$ с.

По графику рис. 5, а для $T_{2\min} = 0.15$ находим T_3 : $T_3 = 0.35$. Из условия (6) находим K_3 :

$$K_3 = \frac{1}{K_1K_{2\min}} = \frac{1}{10 \times 0.2} = 0.5.$$

Определяем критическое значение коэффициента усиления (6):

$$K_{kp} \approx \frac{(0.02 + 0.35)0.15}{0.35^2 \cdot 0.02} = 22.6 > 1.$$

Условие устойчивости выполнено.

На рис. 6 приведены результаты моделирования системы с параметрами по примеру 1.

2. В качестве объекта управления рассмотрим большегрузное морское судно. Как показано в [6] передаточная функция судна в системе управления курсом движения имеет вид:

$$K_2(p) = \frac{K_2}{(T_2 p + 1)p}.$$

Передаточная функция усилителя мощности (гидравлическая рулевая машина) равна

$$K_1(p) = \frac{K_1}{T_1 p + 1}.$$

Одним из возможных вариантов значений параметров передаточных функций судна и рулевой машины указаны в [6,7]: $K_2=0.012$ и $T_2=150$ с. (судно с полным грузом) и $K_2=0.12$, $T_2=15$ с. (движение судна порожняком). Параметры передаточной функции рулевой машины равны: $K_1=1$, $T_1=3$ с.

Определим параметры авторулевого, выполненного по схеме рис. 2.

По графику рис. 5 для $T_{2\min}=15$ с находим: $T_3=5.8$ с. Коэффициент усиления K_3 равен (4):

$$K_3 = \frac{1}{0.012} = 83.$$

Определяем условия устойчивости (6):

$$K_{kp} \approx \frac{(3+5.8)15}{5.8^2 \cdot 3} = 1.3$$

– условие устойчивости выполнено.

На рис. 7 приведены результаты моделирования системы по примеру 2.

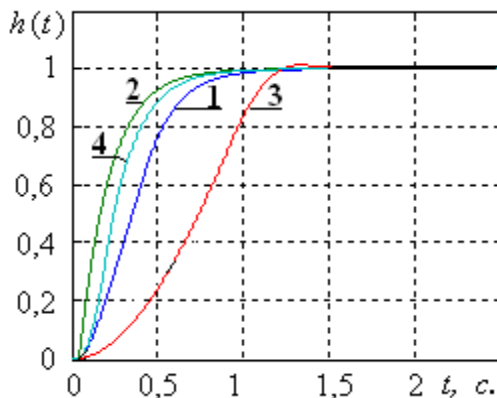


Рис. 6. Переходные характеристики по примеру 1: 1 – $T_2 = 0.15$ с, $K_2 = 0.2$; 2 – $T_2 = 0.15$ с, $K_2 = 2$; 3 – $T_2 = 1.5$ с, $K_2 = 0.2$; 4 – $T_2 = 1.5$ с, $K_2 = 2$

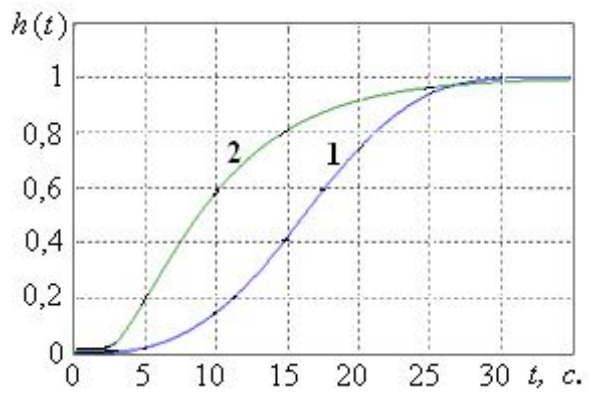


Рис. 7. Переходные характеристики по примеру 2: 1 – $K_2 = 0.012$, $T_2 = 150$ с; 2 – $K_2 = 0.12$, $T_2 = 15$ с

Выводы

Разработана структурная схема регулятора для системы управления, заданная часть которой состоит из исполнительного устройства с неизменяющимися параметрами и объекта управления, параметры которого (постоянная времени и коэффициент усиления) могут изменяться в процессе работы системы в пределах от 1 до 10. При этом показатели качества процесса управления остаются неизменными. В качестве показателей приняты: максимальное перерегулирование в переходной характеристике и время переходного процесса. Разработана структурная схема и метод расчета параметров регулятора. Проведено моделирование системы в пакете MATLAB-Simulink. Разработанный метод расчета подтвержден двумя примерами.

Список литературы

1. Ядыкин, И.Б. Оптимальное адаптивное управление на основе беспоисковой самонастраивающейся системы с обучаемой эталонной моделью / И.Б. Ядыкин // Автоматика и телемеханика. – 1979. – № 2. – С. 65–79.
2. Уткин, В.А. Задача слежения в линейных системах с параметрическими неопределенностями при неустойчивой нулевой динамике / В.А. Уткин, А.В. Уткин // Автоматика и телемеханика. – 2014. – № 9. – С. 45–64.
3. Рутковский, В.Ю. Стабилизация упругих колебаний конструкции крупногабаритных спутников с переменными параметрами методами адаптации / В.Ю. Рутковский, В.М. Суханов, В.М. Глумов // Автоматика и телемеханика. – 2011. – № 12. – С. 91–103.
4. Земляков, С.Д. Алгоритм функционирования адаптивной системы с эталонной моделью, гарантирующей заданную динамическую точность управления нестационарным динамическим объектом в условиях неопределенности / С.Д. Земляков, В.Ю. Рутковский // Автоматика и телемеханика. – 2009. – № 10. – С. 35–44.
5. Глумов, В.Ю. Адаптивное управление ориентацией деформируемых космических аппаратов с изменяющимися параметрами / В.М. Глумов, В.Ю. Рутковский, В.М. Суханов // Автоматика и телемеханика. – 1999. – № 4. – С. 90–102.
6. Кринецкий, И.И. Исследование автоматического управления курсом судна с учетом нелинейных характеристик системы / И.И. Кринецкий, Е.Д. Пичугин // Судовождение и связь. Труды ЦНИИ морского флота. – 1967. – № 83. – С. 13–16.
7. Бобриков, С.А. Коррекция нелинейной характеристики рулевой машины с учетом запаздывания в системе управления курсом морского судна / С.А. Бобриков, Е.Д. Пичугин // Электротехнические и комплексные системы. – 2011. – № 02 (78). – С. 26–29.
8. Батоврин, А.А. Цифровые следящие системы судовой автоматики / А.А. Батоврин, П.Г. Дашевский, В.Д. Лебедев и др. – Л.: Судостроение, 1972. – 445 с.
9. Бесекерский, В.А. Теория систем автоматического регулирования / В.А. Бесекерский, Е.П. Попов. – М.: Наука, 1972. – 719с.
10. Краснопрошина, А.А. Современный анализ систем управления с применением MATLAB, Simulink, ControlSistem / А.А. Краснопрошина, Н.Б. Репникова, А.А. Ильченко. – К: Корнійчук, 1999. – 141 с.

СИНТЕЗ І МОДЕЛЮВАННЯ РЕГУЛЯТОРА ДЛЯ ОБ'ЄКТА ЗІ ЗМІННИМИ ПАРАМЕТРАМИ

С.О. Бобриков, Е.Д. Пічугин, С.І. Кысса

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: bobrikov1932@gmail.com

Проведено синтез регулятора для об'єкта, параметри якого – коефіцієнт посилення і постійна часу, можуть змінюватися в широких межах. Задана частина системи включає в себе виконавчий пристрій (ланка першого порядку) з параметрами, які не змінюються, і двигун – ланка другого порядку зі змінними параметрами. Регулятор забезпечує сталість показників якості системи при будь-яких значеннях змінних параметрів об'єкта в заданому діапазоні їх значень. Як показники процесу прийняті максимальне перерегулювання в перехідній характеристиці і час перехідного процесу. Розроблено структурну схему регулятора і метод розрахунку його параметрів. Робота виконана шляхом моделювання системи в пакеті MATLAB-Simulink.

Ключові слова: регулятор, система управління, передавальні функції, моделювання, перехідна характеристика, показники якості управління, об'єкт управління, виконавчий механізм, підсилювач, зворотний зв'язок, адаптивна система

SYNTHESIS AND MODELING OF THE REGULATOR FOR THE OBJECT WITH CHANGING PARAMETERS

S.A. Bobrykov, E.D. Pichugin, S.I. Kissa

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: bobrikov1932@gmail.com

Has been done synthesis of controller for object, with parameters – gain and time constant which can vary over a wide range. The predetermined portion of the system includes an actuator (first-order unit) with unchanging parameters and an engine-second-order link with varying parameters. The controller ensures the consistency of the system's quality indicators for any values of the object's variables in a given range of values. As indicators of the process, the maximum overshoot in the transient response and the transient time are taken. Have been developed a structural diagram of the regulator and a method for calculating its parameters. The work was done by modeling the system in the MATLAB-Simulink package.

Keywords: regulator, control system, transfer functions, simulation, transient response, control quality indicators, control object, actuator, amplifier, feedback, adaptive system

ПРИМЕНЕНИЕ ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ЭКСПЕРТИЗЫ ЦИФРОВЫХ ФОНОГРАММ И АППАРАТУРЫ ЦИФРОВОЙ ЗВУКОЗАПИСИ «ФРАКТАЛ» ДЛЯ ПРОВЕДЕНИЯ ЭКСПЕРТИЗ АНАЛОГОВЫХ ФОНОГРАММ И АНАЛОГОВОЙ АППАРАТУРЫ МАГНИТНОЙ ЗАПИСИ

О.В. Рыбальский¹, В.И. Соловьев², В.В. Журавель³

¹ Национальная академия внутренних дел,

пл. Соломянская, 1, Киев, 03056, Украина; e-mail: gov_1946@ukr.net

² Восточноукраинский национальный университет имени Владимира Даля,
ул. Советская, 51, г. Северодонецк, 93400, Украина

³ Государственный научно-исследовательский экспертно-криминалистический центр,
ул. Б. Окружная, 4а, м. Киев, 01601, Украина

Проведена проверка возможности использования программного комплекса «Фрактал» и методики ее применения, предназначенных для проведения диагностических экспертных исследований цифровых фонограмм и аппаратуры цифровой звукозаписи, для аналогичных исследований аналоговых фонограмм и аналоговой аппаратуры магнитной записи. Экспериментально показано, что эта программное средство и методика его применения могут использоваться для проведения таких экспертиз, при этом корректировка программы и методики не требуется.

Ключевые слова: аппаратура магнитной записи, аппаратура цифровой звукозаписи, аналоговая звукозапись, аналоговая фонограмма, цифровая звукозапись, цифровая фонограмма, экспертиза

Введение

В процессе разработки инструментального средства экспертизы (ИСЭ) «Фрактал», предназначенного для проведения экспертиз аутентичности цифровых фонограмм (ЦФ) и идентификации аппаратуры цифровой звукозаписи (АЦЗЗ) в первую очередь исследовался механизм слеодообразования, возникающий при цифровой обработке таких фонограмм. Естественно, что эти исследования проводились путем постепенного усложнения задач и моделей, связанных с монтажом ЦФ. По мере построения новых моделей появлялось более полное понимание процессов слеодообразования, происходящих при записи и монтаже ЦФ. Исследования этих процессов для ЦФ и АЦЗЗ в своей динамике отражены в ряде наших предыдущих работ, например, [1-2]. Затем был предложен фрактальный подход к построению ИСЭ (программных средств и методик), предназначенных для проведения экспертизы ЦФ и АЦЗЗ. Попутно возник вопрос пригодности фрактального подхода для построения ИСЭ для аналоговых фонограмм (АФ) и аналоговой аппаратуры магнитной записи (ААМЗ), поскольку старые ИСЭ, предназначенные для этих целей, уже морально и физически устарели. Поэтому в первую очередь была исследована теоретическая возможность

применения такого подхода к проявлению механизма образования следов цифровой обработки в АФ в виде различия самоподобных структур для обработанной и аутентичной АФ [3-4]. Однако вернуться к этим исследованиям пришлось уже после завершения разработки ИСЭ «Фрактал». При этом были определены цели и поставлены задачи экспериментальных исследований пригодности ИСЭ «Фрактал» [5] и проведены первые исследования. Осмысление их результатов является предметом данной статьи.

Основная часть

В работах [4-5] нами на предложенной модели было показано различие между сигналами, записанными на ААМЗ и сигналами, сначала записанными на АЦЗЗ, затем обработанными в цифровой форме и переписанными на ААМЗ. Это различие обусловлено влиянием различия истинных (а не номинальных) значений периодов дискретизации в аналого-цифровых и цифроаналоговых преобразователях (АЦП и ЦАП соответственно) АЦЗЗ и экспертного компьютера, т.к. сигнал на ААМЗ из АЦЗЗ может быть переписан (как и введен в компьютер) только в аналоговой форме через аналоговые вход и выход [1; 2]. В частности, во временной области обработанный сигнал представляется как

$$s_{14}(t) = \frac{\sum_{n_2=-\infty}^{\infty} \sum_{n_3=-\infty}^{\infty} \text{rect}\left(\frac{t-n_2T_2}{T_2}\right) \text{rect}\left(\frac{n_2T_2-n_3T_3}{T_3}\right) A_{m13} \cos \omega_{11}(n_3T_3)}{2\pi d\Delta} \times \left[\text{arctg} \frac{2a_B d}{a_B^2 + x^2 - \Delta^2} - \text{arctg} \frac{2(a_B + d)\Delta}{a_B^2 + x^2 - \Delta^2} \right], \quad (1)$$

где A_{m13} – максимальное значение шкалы преобразования АЦП экспертного компьютера,

T_2 – период дискретизации в ЦАП на аналоговом выходе АЦЗЗ,

T_3 – период дискретизации в экспертном компьютере, в который вводится АФ,

n_2 – номер отсчета (выборки) в ЦАП на аналоговом выходе АЦЗЗ,

n_3 – номер отсчета (выборки) в АЦП экспертного компьютера,

a_B – величина неконтакта между магнитной головкой и носителем при воспроизведении сигнала на ААМЗ,

d – толщина рабочего слоя магнитного носителя ААМЗ,

Δ – половина ширины рабочего зазора головки воспроизведения ААМЗ,

$x = Vt$, где V – скорость транспортирования носителя в ААМЗ, t – текущее время [4-5].

При этом в соотношении (1) учитывается влияние всех основных факторов, действующих на воспроизводимый сигнал в ААМЗ, в частности, влияние неконтакта и щелевой функции.

Сигнал, введенный в экспертный компьютер с аутентичной АФ, запишется как

$$s_3(t) = \frac{\sum_{n_3=-\infty}^{\infty} \text{rect}\left(\frac{t-T_3n_3}{T_3}\right) A_{m3} \cos \omega(n_3T_3)}{2\pi d\Delta} \left[\text{arctg} \frac{2a_B d}{a_B^2 + x^2 - \Delta^2} - \text{arctg} \frac{2(a_B + d)\Delta}{a_B^2 + x^2 - \Delta^2} \right]. \quad (2)$$

Наличие повторяющихся в разных масштабах функций в соотношениях (1) и (2) говорит о том, что обе фонограммы содержат самоподобные структуры, возникающие как за счет влияния тракта воспроизведения ААМЗ, так и за счет оцифровки воспроизводимого сигнала.

Возможна еще одна схема обработки аутентичной АФ, при которой первичная запись производится на ААМЗ, запись вводится в компьютер с аналогового входа/выхода, обрабатывается и переписывается в аналоговой форме на ААМЗ. Однако при этом в обработанной фонограмме все равно остаются следы обработки, но уровень собственных шумов АФ значительно (не менее чем на 4 дБ) возрастает за счет повторной перезаписи на ААМЗ.

При проведении дальнейших исследований требовалось, во-первых, установить, действует ли закономерность наличия аномальной зоны в плотностях вероятностей меры близости фрактальных характеристик двух АФ, записанных на одной АЦЗЗ и введенных в одинаковых условиях в один и тот же экспертный компьютер [6]. Как, впрочем, и закономерность отсутствия такой зоны для двух разных (записанных на разной ААМЗ или обработанной и аутентичной) АФ.

Конечно, наличие такой зоны для двух аутентичных АФ, введенных в экспертный компьютер, сомнений не вызывает, поскольку сама операция их аналогового ввода есть не что иное, как процесс цифровой записи аналогового сигнала, и ничем не отличается от записи такого сигнала на АЦЗЗ. Правда, уровень собственных шумов АФ значительно выше, что может вызвать некоторые затруднения. Возможно, потребуются как уточнение доверительного интервала для принятия решения о выборе области близости или несоответствия фрактальных характеристик сравниваемых АФ при проверке аутентичности АФ и идентификации ААМЗ, так и уточнение максимального порогового значения величины ошибки I рода, задаваемого при выборе этих областей.

Исследования также требуют наличия закономерности отсутствия такой зоны для разных записей, поскольку эта зависимость, хотя и будет существовать, может быть замаскирована в собственных шумах АФ так, что ИСЭ «Фрактал» не сможет обеспечить выделения различия в самоподобных структурах.

Разумеется, что обеспечить эти исследования можно было только экспериментальным путем. Однако организация этих экспериментов столкнулась с рядом сложностей, связанных с «раритетностью» ААМЗ. Хорошо, что осталась большая экспертная база аналоговых записей, полученных при проведении экспертиз в предыдущие годы и сохранившаяся в экспертных компьютерах, что и позволило провести эксперименты с аналоговыми записями, сделанными на различных типах ААМЗ.

Ниже проиллюстрированы проведенные эксперименты. Рассмотрим записи, сделанные при экспертизе 2003 г., выполненные на ААМЗ марки Panasonic типа RQ-L319 зав. № BE7G858937. По экспертизе проходили фонограммы, записанные на 23 кассетах. Экспертиза проводилась с применением ИСЭ «Теорема-1», разработанного для проведения экспертиз ААМЗ одним из соавторов. При проведении экспертизы было установлено, что часть фонограмм, представленных на экспертизу (кассеты 6 и 15) содержат следы цифровой обработки и являются перезаписями, произведенными на ААМЗ, представленной на экспертизу. На ИСЭ «Фрактал» была проведена проверка результатов предыдущих экспертных исследований. Результаты этой проверки представлены на рис. 1-3, иллюстрирующих проведенные исследования.

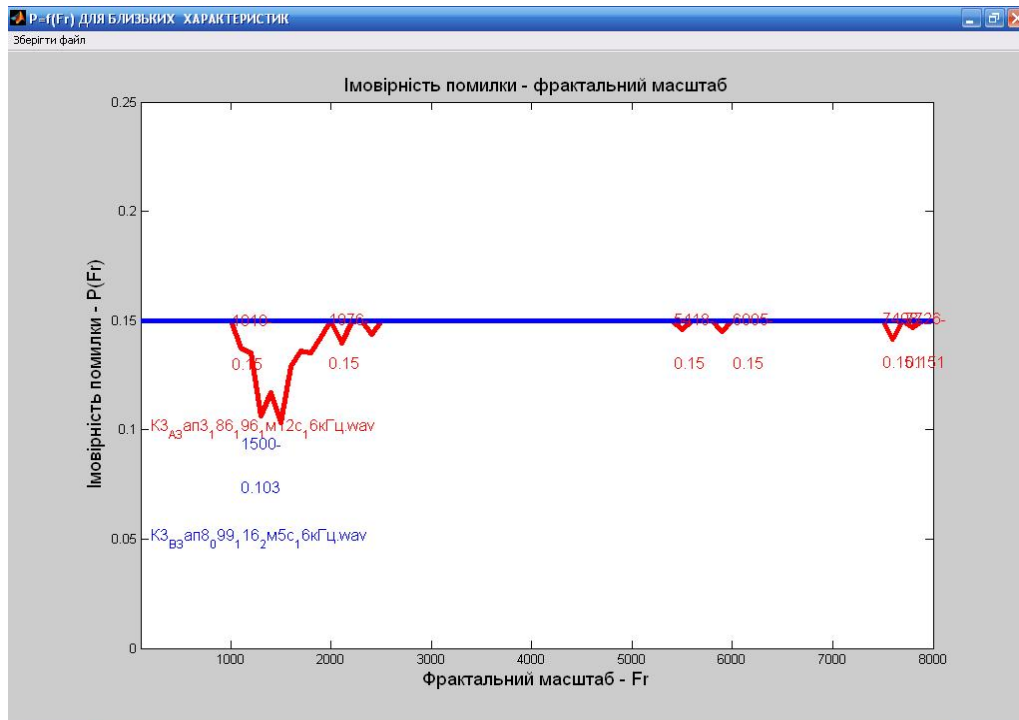


Рис. 1. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на сторонах А и В кассеты № 3 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 1010

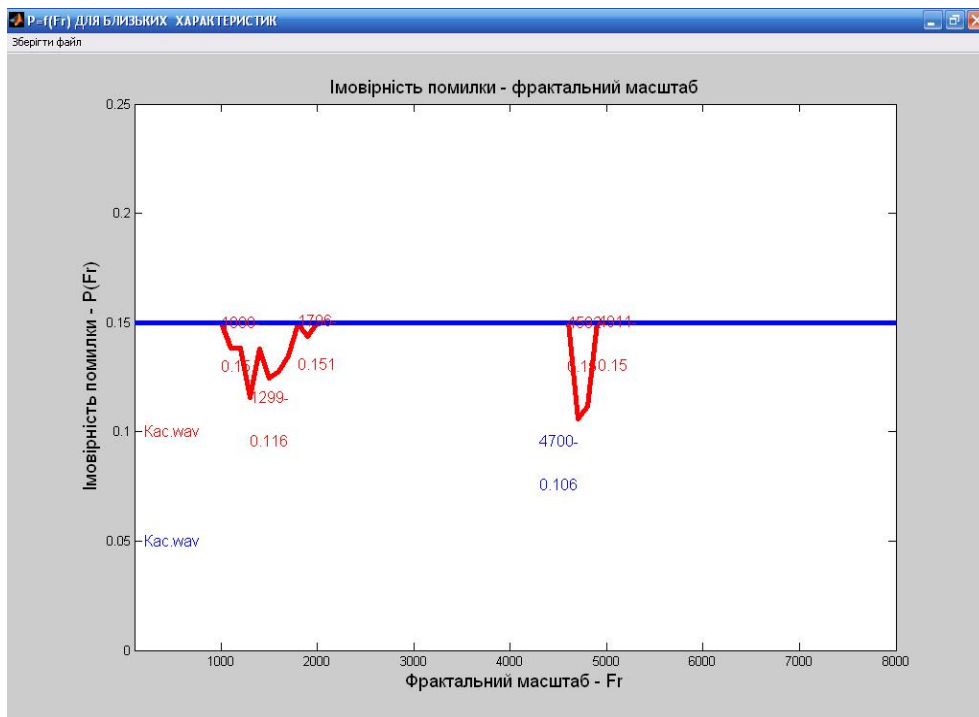


Рис. 2. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на сторонах А и В кассеты № 2 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 1000

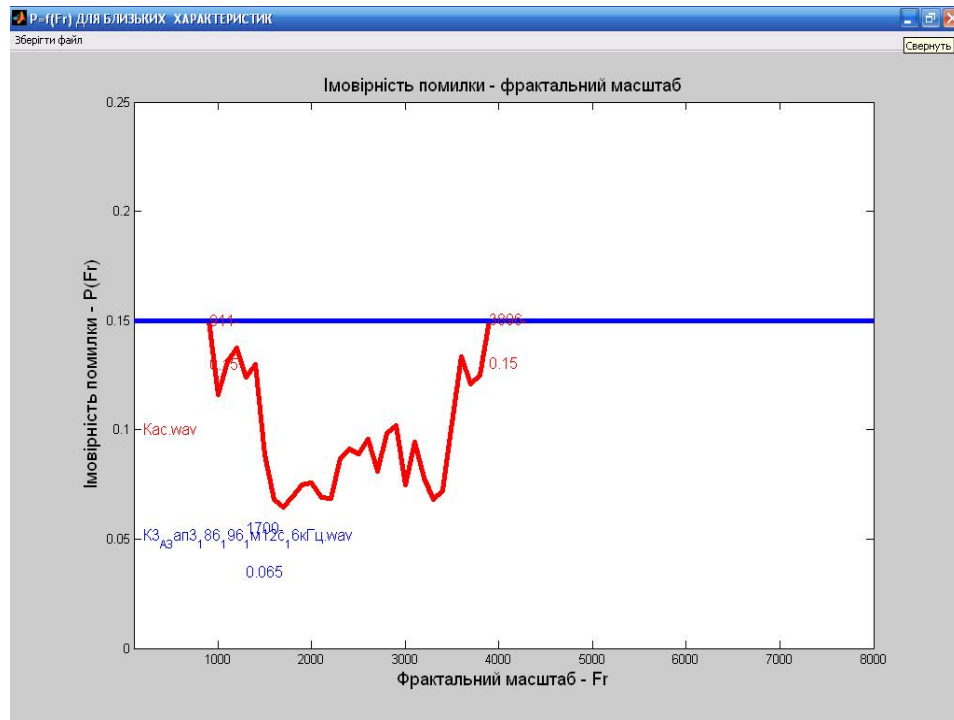


Рис. 3. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на стороне А кассет № 2 и № 3 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 911

Из рассмотрения положений крайней левой (критериальной) точки границ перехода, представленных на рис. 1-3 видно, что они укладываются в доверительный интервал для критериальных точек, определяемый как

$$l_{\beta} = [(a_{\min} - 0.2a_{\min}), (a_{\max} + 0.2a_{\max})],$$

где $a_{\min}$ и $a_{\max}$ – минимальное и максимальное значения критериальной точки [6].

Разумеется, что аналогичные результаты были получены и на АФ, записанных на других типах одной и той же ААМЗ. Всего были проверены записи, выполненные 6 экземплярах ААМЗ разных типов и марок.

Таким образом, из исследований, проведенных на этом этапе, мы сделали вывод, что ИСЭ «Фрактал» пригодно для идентификации ААМЗ и проверки оригинальности АФ в случае, если исследуемые фонограммы записаны на одной ААМЗ. При этом коррекция как доверительного интервала для принятия решения о выборе области близости или несоответствия фрактальных характеристик сравниваемых АФ при проверке аутентичности АФ и идентификации ААМЗ, так и уточнение максимального порогового значения величины ошибки I рода, задаваемого при выборе этих областей, не требуется.

Для принятия решения о пригодности ИСЭ «Фрактал» для идентификации ААМЗ и установления оригинальности АФ необходимо было проверить его способность к определению фонограмм, записанных на различной ААМЗ. Результаты этих экспериментов, проведенных путем сравнения записей, сделанных на одной и разной ААМЗ, иллюстрируются рис. 4. Показаны результаты вычисления фрактальных масштабов для области совпадения фрактальных характеристик для фонограммы № 3, записанной на стороне А кассеты № 3 на ААМЗ Panasonic типа RQ-L319 зав. № BE7G858937 и образцовой фонограммы, записанной на ААМЗ Marantz Model NO PMD 222 сер. № MZ03994810369 PCC REG NO. AKE9T2-14893-RC-N.

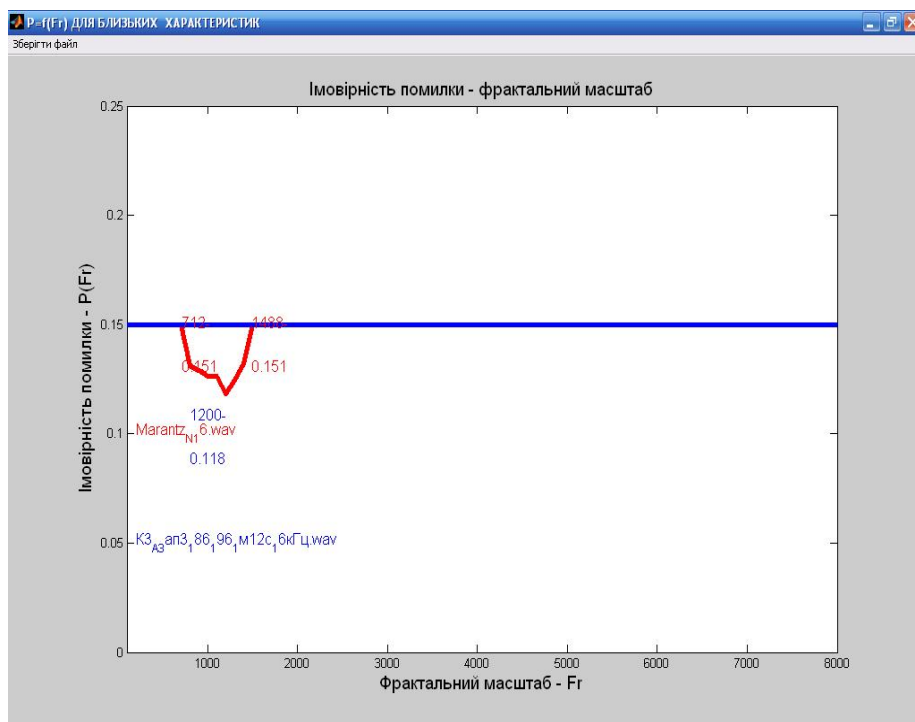


Рис. 4. Результаты расчета величины фрактальных масштабов для области совпадения характеристик фонограммы № 3, записанной на стороне А кассеты № 3 на ААМЗ Panasonic типа RQ-L319 и образцовой фонограммы, записанной на ААМЗ Marantz Model NO PMD 222 при значении критериальной точки границы перехода – 712

На рис. 4 видно, что значение критериальной точки составляет 712. Эта величина не укладывается в доверительный интервал, рассчитанный для фонограмм, записанных на ААМЗ Panasonic типа RQ-L319, т.к. минимальное значение критериальной точки для АФ, записанных на этом аппарате, составляет 729. Как и на предыдущем этапе, исследования были проведены на 6 экземплярах ААМЗ разных типов и марок.

На основании проведенных исследований нами был сделан вывод о том, что ИСЭ «Фрактал» пригодно для выявления факта записи фонограмм на разной ААМЗ. Как и на предыдущем этапе экспериментов, коррекция как доверительного интервала для принятия решения о выборе области близости или несоответствия фрактальных характеристик сравниваемых АФ при проверке аутентичности АФ и идентификации ААМЗ, так и уточнение максимального порогового значения величины ошибки I рода, задаваемого при выборе этих областей, не потребовалась.

Таким образом, на основании исследований, проведенных на представленных двух этапах экспериментов, можно сделать общий вывод о том, что ИСЭ «Фрактал» пригодно для идентификационных исследований ААМЗ и определения оригинальности АФ.

На следующем этапе экспериментов следовало определить возможность выявления с применением ИСЭ «Фрактал» следов цифровой обработки в АФ. Для этого были использованы записи, изготовленные на той же ААМЗ, что использовалась в предыдущих экспериментах, и записи, сделанные на АЦЗЗ трех типов, переписанные затем на используемой ранее ААМЗ. При этом были проведены два вида экспериментов:

- эксперимент по выявлению заранее известных по результатам экспертизы следов цифровой обработки в АФ;
- эксперимент по выявлению следов цифровой обработки в АФ, переписанных с ЦФ.

Результаты проведенных исследований проиллюстрированы на рис. 5-9. Отметим, что согласно актам проведенной в 2003 г. экспертизы, АФ, записанные на кассетах № 6 и № 15, подвергались цифровой обработке.

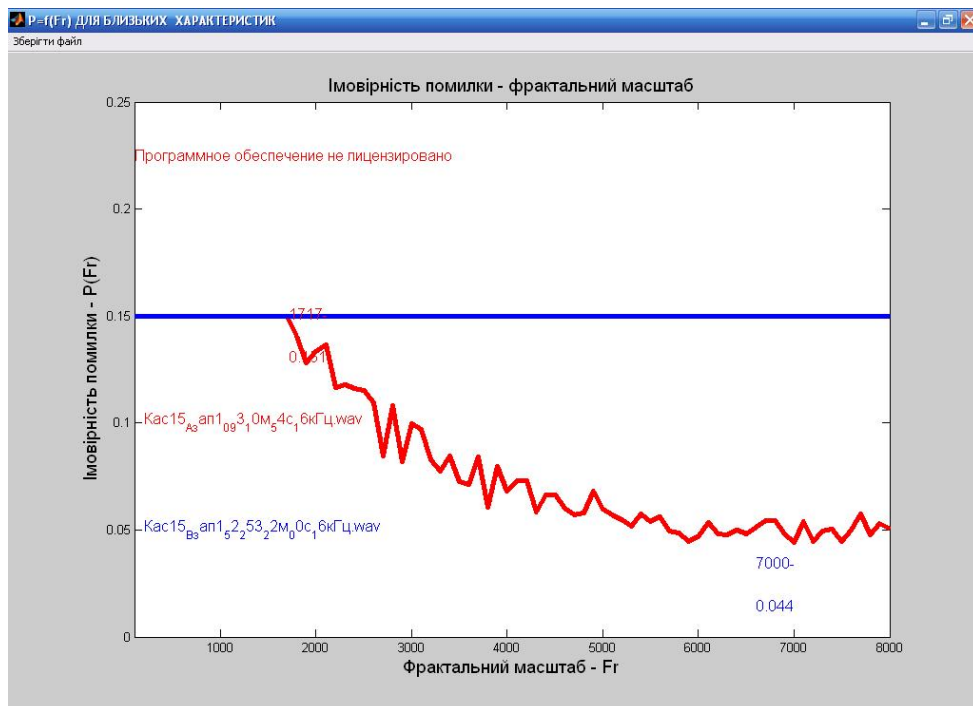


Рис. 5. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на сторонах А и В кассеты № 15 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 1717

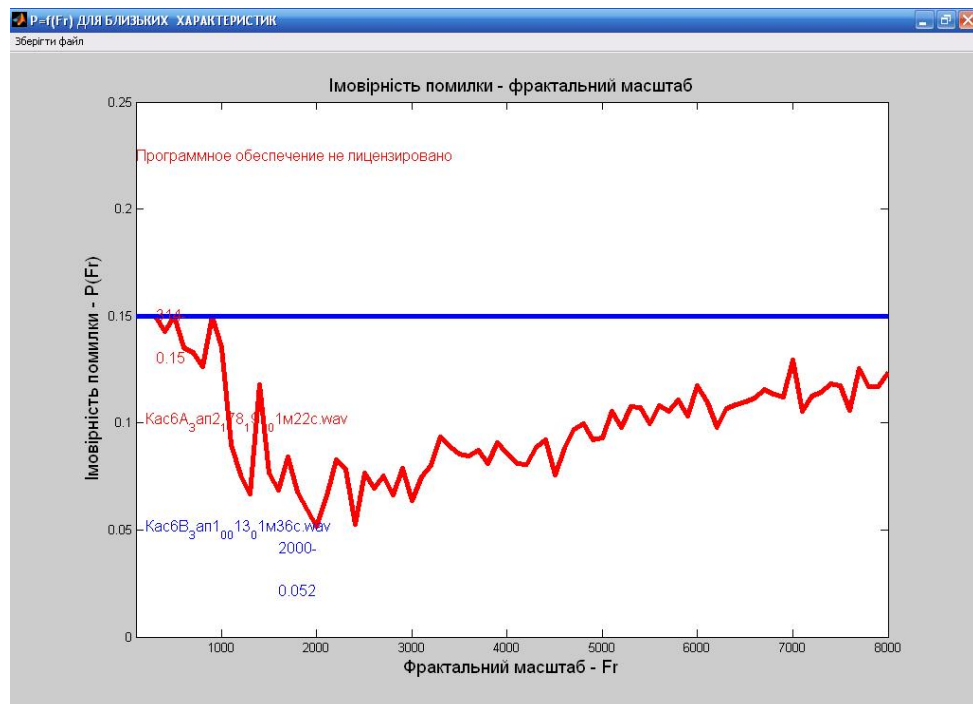


Рис. 6. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на сторонах А и В кассеты № 6 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 314

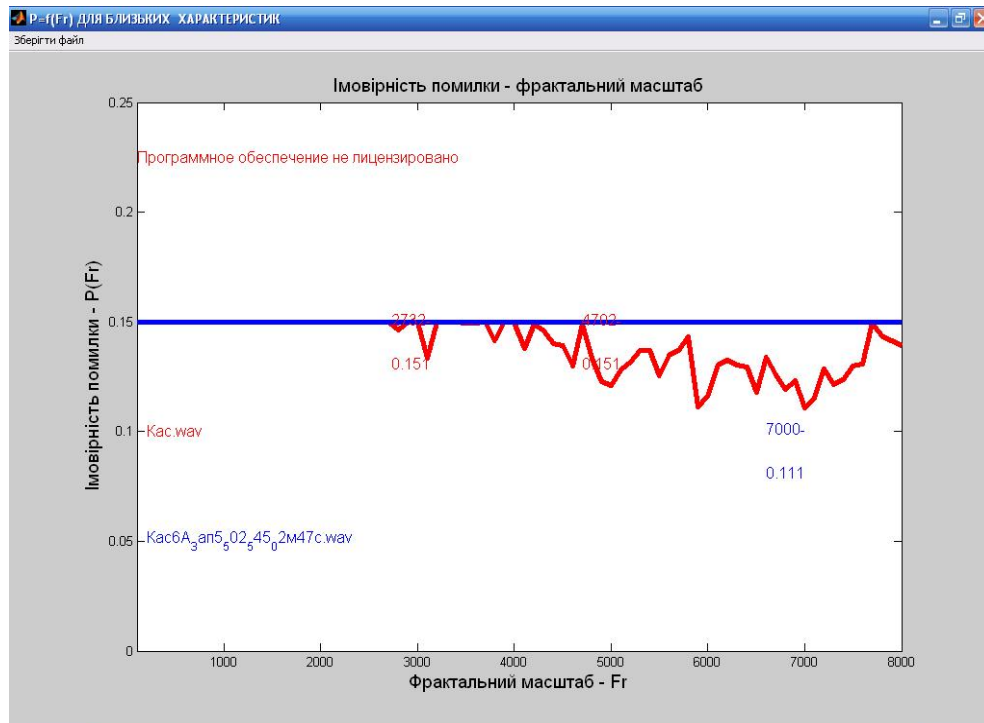


Рис. 7. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на стороне А кассеты № 2 и стороне А кассеты № 6 на ААМЗ Panasonic типа RQ-L319 при значении критериальной точки границы перехода – 2732

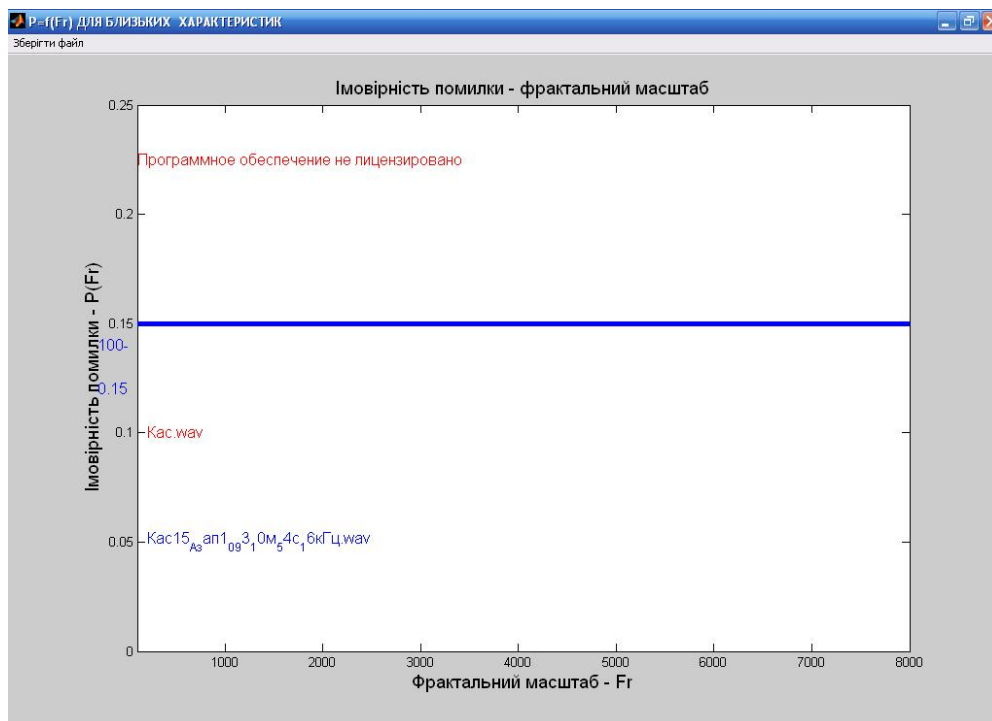


Рис. 8. Результаты расчета величины фрактальных масштабов для области совпадения характеристик двух фонограмм, записанных на стороне А кассеты № 2 и стороне А кассеты № 15 на ААМЗ Panasonic типа RQ-L319

Из графиков на рис. 5 и рис. 6 видно, что критериальные точки для записей, подвергнутых цифровой обработке, значительно отклоняются от допустимого предельного значения в доверительном интервале, определенном для АФ, записанных без такой обработки (см. рис. 1 и рис. 2).

Соответственно, и результаты сравнения фонограмм, записанных без цифровой обработки на, например, кассете № 2, и фонограмм со следами такой обработки, записанными на кассетах № 6 и № 15, показали явное отклонение критериальных точек (см. рис. 7 и рис. 8).

При этом на рис. 8 видно, что различие в записях, зафиксированных на АФ № 2 и № 15 вообще превышает предельную величину ошибки I рода, принятую на уровне 0.15.

Проведение этого этапа экспериментов показало, что коррекция как доверительного интервала для принятия решения о выборе области близкости или несоответствия фрактальных характеристик сравниваемых АФ при проверке аутентичности АФ и идентификации ААМЗ, так и уточнение максимального порогового значения величины ошибки I рода, задаваемого при выборе этих областей, не требуется.

Аналогичные результаты были получены и для перезаписей ЦФ, записанных на АЦЗЗ и переписанных на ААМЗ. Иллюстрация результатов этих экспериментов на примере перезаписи ЦФ, записанной на АЦЗЗ Fictonic зав. № 005, на ААМЗ Marantz Model NO PMD 222, приведена на рис. 9.

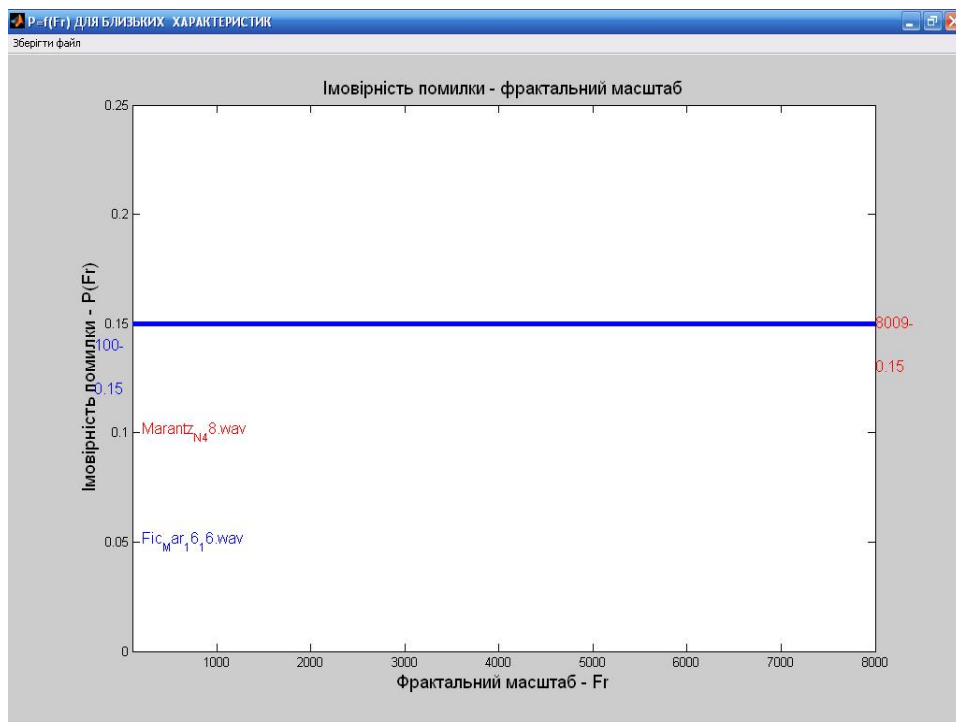


Рис. 9. Результаты расчета величины фрактальных масштабов для области совпадения характеристик фонограммы, записанной на ААМЗ Marantz Model NO PMD 222 и фонограммы, переписанной с аналогового выхода АЦЗЗ Fictonic на ААМЗ Marantz Model NO PMD 222

Эксперименты показали, что ИСЭ «Фрактал» пригодно для выявления следов перезаписи ЦФ на ААМЗ. При этом коррекция как доверительного интервала для принятия решения о выборе области близкости или несоответствия фрактальных характеристик сравниваемых АФ при проверке аутентичности АФ и идентификации

ААМЗ, так и уточнение максимального порогового значения величины ошибки I рода, задаваемого при выборе этих областей, не требуется.

Таким образом, в результате проведенных экспериментов установлено, что специализированное программное средство «Фрактал» и методика его применения при проведении экспертизы, отвечают условиям выявления следов цифровой обработки в АФ.

Выводы

1. Экспериментально установлено, что ИСЭ «Фрактал», разработанное для проведения идентификационных экспертных исследований АЦЗЗ и диагностических экспертных исследований ЦФ, пригодно для проведения аналогичных экспертиз ААМЗ и ЦФ.

2. Экспериментально установлено, что коррекция методики применения программного средства «Фрактал» при проведении экспертизы ААМЗ и АФ по отношению к этой методике для АЦЗЗ и ЦФ, не требуется.

3. Специализированное программное средство «Фрактал» и методика его применения могут быть использованы для проведения экспертиз материалов и средств аналоговой звукозаписи.

Список литературы

1. Рыбальский, О.В. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К. : Нац. акад. внутр. справ України, 2003. – 300 с.
2. Рибальський, О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі / О.В. Рибальський. – К. : Нац. акад. внутр. справ України, 2004. – 167 с.
3. Рыбальский, О.В. Проявление следов цифровой обработки в аналоговых сигналаграммах / О.В. Рыбальский // Інформаційна безпека. – 2010. – № 1 (3). – С. 79-83.
4. Рыбальский, О.В. Модель выявления следов цифровой обработки аналоговых сигналаграмм с применением мультимасштабного анализа / О.В. Рыбальский, В.И. Соловьев // Інформаційна безпека. – 2011. – № 1 (5). – С. 27-32.
5. Рыбальский, О.В. Фрактальный подход к выявлению следов цифровой обработки в аналоговых фонограммах / О.В. Рыбальский, В.И. Соловьев, В.В. Журавель // Сучасна спеціальна техніка. – 2017. – № 1. – С. 3-8.
6. Рыбальский, О.В. Методология построения системы экспертной проверки цифровых фонограмм и идентификации аппаратуры цифровой звукозаписи с применением программы «Фрактал» / О.В. Рыбальский, В.И. Соловьев, В.В. Журавель // Інформатика та математичні методи в моделюванні. – 2016. – Т. 6, № 2. – С. 105-115.

ЗАСТОСУВАННЯ ІНСТРУМЕНТАЛЬНОГО ЗАСОБУ ЕКСПЕРТИЗИ ЦИФРОВИХ ФОНОГРАМ І АПАРАТУРИ ЦИФРОВОГО ЗВУКОЗАПИСУ «ФРАКТАЛ» ДЛЯ ПРОВЕДЕННЯ ЕКСПЕРТИЗ АНАЛОГОВИХ ФОНОГРАМ ТА АНАЛОГОВОЇ АПАРАТУРИ МАГНІТНОГО ЗАПИСУ

О.В. Рибальський¹, В.І. Соловйов², В.В. Журавель³

- ¹ Національна академія внутрішніх справ,
пл. Солом'янська, 1, Київ, 03056, Україна; e-mail: rov_1946@ukr.net
² Східноукраїнський національний університет імені Володимира Даля
вул. Радянська, 51, 93400 м. Сєвєродонецьк Україна
³ Державний науково-дослідний експертно-криміналістичний центр,
вул. В. Окружна, 4 а, м. Київ, 01601, Україна

Проведена перевірка можливості використання програми «Фрактал» і методики її застосування, призначених для проведення діагностичних експертних досліджень цифрових фонограм і апаратури цифрового звукозапису, для аналогічних досліджень аналогових фонограм та аналогової апаратури магнітного запису. Експериментально показано, що ця програма і методика її застосування можуть використовуватися для проведення таких експертиз. При цьому коригування програми та методики не потрібно.

Ключові слова: апаратура магнітного запису, апаратура цифрового звукозапису, аналоговий звукозапис, аналогова фонограма, цифровий звукозапис, цифрова фонограма, експертиза

APPLICATION OF TOOL OF EXAMINATION OF DIGITAL PHONOGRAMS AND APPARATUS OF DIGITAL AUDIO RECORDING «FRACTAL» FOR REALIZATION OF EXAMINATIONS OF ANALOG PHONOGRAMS AND ANALOG APPARATUS OF MAGNETIC RECORD

O.V. Rybalskiy¹, V.I. Solovyov², V.V. Zhuravel³

- ¹ National Academy of Internal Affairs,
1, Solomenskaya Sq., Kiev, 03056, Ukraine; e-mail: rov_1946@ukr.net
² Volodymyr Dahl East Ukrainian National University,
51, Radyanska str., 93400, Severodonetsk, Ukraine,
³ The State Research Expertly-Criminalistics Center of Ministries of Internal Affairs of Ukraine,
4a, Velyka Okruzhna str., Kyiv, 01601, Ukraine

Verification of possibility of the use of the program «Fractal» and methodology of her application is conducted, diagnostic expert researches of digital phonograms and apparatus of the digital audio recording intended for realization, for analogical researches of analog phonograms and analog apparatus of magnetic record. It is experimentally shown that this program and methodology of her application can be used for realization of such examinations. Adjustment of the program and methodology is not required thus.

Keywords: apparatus of magnetic record, apparatus of the digital audio recording, analog audio recording, analog phonogram, digital audio recording, digital phonogram, examination

МОДЕЛІ РОЗПОДІЛЕНИХ СИСТЕМ ІЗ ЗАПІЗНЮЮЧИМ АРГУМЕНТОМ

С.А. Положаєнко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sanp277@gmail.com

Запропоновано математичні моделі систем з розподіленими параметрами, які характеризуються запізнюваннями по аргументу за часом. Моделі отримано для систем k -го порядку, що дозволяє застосовувати їх у більшості прикладних задач математичної фізики. Виконано якісне дослідження запропонованих моделей, в результаті чого строго доведено існування та єдиність розв'язків відповідних диференціальних рівнянь у частинних похідних, які утворюють ці моделі.

Ключові слова: математична модель, аргумент із запізнюванням, основна початкова задача, метод кроків, метод стислих відображень, аналітичні розв'язки диференціальних рівнянь

Вступ

Стрімкий розвиток спеціальних розділів теорії автоматичного управління зумовив останнім часом підвищений інтерес до вивчення диференціальних рівнянь у частинних похідних (ДРЧП), що мають аргумент t із запізненням, і які розглядаються в якості математичного опису (математичних моделей) систем з розподіленими параметрами (РП-систем), що характеризуються властивостями післядії.

У найбільш загальному випадку ДРЧП у «нормальній» формі з частинними похідними k -го порядку та із запізнюванням по одному виділеному аргументу t має вигляд

$$\frac{\partial^k \Phi(t, x)}{\partial t^k} = F \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial t}, \dots, \frac{\partial^{k-1} \Phi(t, x)}{\partial t^{k-1}}, \dots, \frac{\partial \Phi(t - \tau, x)}{\partial t}, \dots, \frac{\partial^{k-1} \Phi(t - \tau, x)}{\partial t^{k-1}}, \frac{\partial \Phi(t, x)}{\partial x}, \dots, \frac{\partial^{k-1} \Phi(t, x)}{\partial x^{k-1}}, \frac{\partial \Phi(t - \tau, x)}{\partial x}, \dots, \frac{\partial^{k-1} \Phi(t - \tau, x)}{\partial x^{k-1}} \right], \quad (t - \tau > 0). \quad (1)$$

При $\tau = 0$ рівняння (1) переходить у звичайне ДРЧП (без запізнювання).

Рівняння першого та другого порядків із запізнюванням по одному аргументу може бути представлено у вигляді

$$\frac{\partial \Phi(t, x)}{\partial t} = F \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial x}, \frac{\partial^{k-1} \Phi(t, x)}{\partial t^{k-1}}, \frac{\partial \Phi(t - \tau, x)}{\partial x} \right], \quad (2)$$

$$\frac{\partial^2 \Phi(t, x)}{\partial t^2} = F \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial t}, \frac{\partial \Phi(t - \tau, x)}{\partial x}, \frac{\partial \Phi(t, x)}{\partial x}, \frac{\partial \Phi(t - \tau, x)}{\partial t}, \frac{\partial^2 \Phi(t, x)}{\partial x^2}, \frac{\partial^2 \Phi(t, x)}{\partial x \partial t}, \frac{\partial^2 \Phi(t - \tau, x)}{\partial x^2} \right]. \quad (3)$$

При цьому вважається, що рівняння визначено в обмеженій зв'язаній області Ω n -мірного евклідова простору змінних $x = \{x_1, x_2, \dots, x_n\}$ при $t_0 \leq t \leq t_f$; $\Phi = \{\Phi_1, \Phi_2, \dots, \Phi_m\}$ – шукана вектор-функція; F – задані функції своїх аргументів, які можуть характеризувати собою просторово визначений диференціальний оператор; $\tau = \text{const} > 0$ – запізнювання по аргументу t .

Типовою лінійною формою рівняння (2) є система

$$\frac{\partial \Phi(t, x)}{\partial t} = L_0 \Phi(t, x) + L_1 \Phi(t - \tau, x) + \Phi(t, x), \quad (4)$$

де L_0 та L_1 – лінійні просторово визначені диференціальні оператори.

В задачах математичної фізики запізнювання з'являються лише за часом (хоча в інших задачах не виключена можливість наявності запізнювання і по просторових змінних); тоді змінній t слід приписати зміст часової координати.

Такими диференціальними рівняннями описуються процеси в замкнених регульованих системах з розподіленими параметрами та зі зворотними зв'язками [1-3]. Поява запізнювання за часом τ зумовлено кінцевою швидкістю розповсюдження сигналів в каналах зворотних зв'язків та інерційних регуляторів.

Аналогічні рівняння можна отримати у випадку, коли Φ та її похідні входять у диференціальне рівняння при більшій кількості запізнювань, ніж у наведених рівняннях [4].

В фундаментальних роботах [5-8] отримано певні теореми, що встановлюють існування та єдиність розв'язку задачі Коші, причому в [5] – для випадку, коли диференціально-різницева рівняння у частинних похідних може бути зведено до рівняння у частинних похідних без запізнювання.

В теорії ДРЧП із запізнюваннями слід розглядати як основну початкову задачу (задачу Коші), так різноманітні крайові задачі.

Мета роботи

Мета роботи полягає у дослідженні окремих питань загальної теорії (теорем існування, неперервної залежності від параметру та початкової точки тощо) для основної початкової задачі (ОПЗ) для розподілених систем, які характеризуються аргументом із запізнюванням.

Основна частина

Основна початкова задача, наприклад, для рівнянь (2), (3) полягає у визначенні функції $\Phi(t, z)$, що має неперервні диференціали, задовольняє відповідно рівнянням (2), (3) при $t > t_0$, та умові $\Phi(t, z) = \varphi(t, z)$ при $t - \tau \leq t \leq t_0$ у випадку рівняння (2) та додатково умові $\frac{\partial \Phi(t, x)}{\partial t} = \psi(t, x)$ при $t - \tau \leq t \leq t_0$ у випадку рівняння (3), де $\varphi(t, z)$ та $\psi(t, x)$ – задані безперервні функції, що мають назву початкових. Відрізок часової осі $[t_0 - \tau, t_0]$, на якому задано початкові функції, має назву початкової множини та позначається E_t . При цьому $\Phi(t, z)$ повинно переходити в $\varphi(t, z)$ неперервно.

Існування та єдиність розв'язку. Доведення існування та єдиності розв'язку ОПЗ для рівнянь у частинних похідних із запізнюваннями можна провести для певних форм рівнянь різноманітними прийомами та методами, одні з яких полягають у

безпосередній побудові розв'язків за допомогою інтеграції, інші – засновано на представленні розв'язків рядами, на дослідженні топологічної структури розв'язків диференціальних рівнянь та формулюванні і доведенні відповідних теорем.

Метод кроків. Найбільш природним методом розв'язування цього питання є метод послідовних наближень – метод кроків, який полягає в тому, що ОПЗ на кожному кроці зводиться до розв'язування задачі Коші для частинних похідних без відхилення аргументу [9]. Наприклад, для рівняння (2) на першому кроці $(t_0, t_0 + \tau)$ маємо

$$\frac{\partial \Phi(t, x)}{\partial t} = F \left[t, \Phi(t, x), \frac{\partial \Phi(t, x)}{\partial x}, \varphi(t - \tau, x), \frac{\partial \varphi(t - \tau, x)}{\partial x} \right]. \quad (5)$$

Існування та єдиність розв'язку рівняння (5) при $t_0 < t \leq t_0 + \tau$ безпосередньо випливає з теорем, які подано в [10] для нелінійних рівнянь без запізнювання.

Розглядаючи розв'язок на інтервалі $[t_0, t_0 + \tau]$ як початкове значення рівняння (2), визначеного для $t \geq t_0 + \tau$, можна поширити розв'язок на інтервал $[t_0 + \tau, t_0 + 2\tau]$, використовуючи ті ж самі теореми. Продовжуючи цей процес, можна отримати розв'язки для інтервалів $[t_0 + 2\tau, t_0 + 3\tau]$, $[t_0 + 3\tau, t_0 + 4\tau]$ тощо.

Цей метод, таким чином, дає можливість побудувати розв'язок $\Phi(t, z)$ рівняння (2) та більш загального рівняння (1) на деякому кінцевому відрізку часової осі та одночасно доводить:

- існування розв'язку в околі точки $(t_0, \varphi(t_0, x), x)$, якщо функції φ та F неперервні в області зміни своїх аргументів t та x , яка розглядається (а функція φ ще така, що диференціюється по x у випадку рівняння (2) та $k-1$ раз диференціюється по t та x у випадку рівняння (1));

- його єдиність, якщо функція F задовольняє одній з умов, що забезпечує єдиність розв'язку звичайного ДРЧП без відхилень аргументу, наприклад, умові Гельдера-Ліпшиця по всіх аргументах, починаючи з третього, або більш жорсткій умові – умові аналітичності.

Теорема існування та єдиності розв'язків аналітичних диференціальних рівнянь. Будемо вважати, що праві частини диференціального рівняння виду

$$\frac{\partial \Phi_i(t, x)}{\partial t} = F_i \left[t, x, \Phi_1, \dots, \Phi_m, \Phi_1(t - \tau, x), \dots, \Phi_m(t - \tau, x), \dots, \frac{\partial \Phi_m(t - \tau, x)}{\partial x} \right], \quad (6)$$

і початкові функції $\Phi_i(t, z) = \varphi_i(t, z)$ на E_{t_i} ($i = 1, 2, \dots, m$) є регулярними функціями своїх аргументів в деякому околі точки $t = t_0 \in E_{t_i}$, $x = x_0 \in \Omega$. Аналітичність рівнянь та початкових функцій означає, що функції F_i та φ_i можуть бути задані степеневими рядами

$$\begin{aligned} \varphi_i(t, z) &= \sum_{\nu_1, \nu_2=0}^{\infty} a_{\nu_1, \nu_2}^i(\tau) (t - t_0)^{\nu_1} (x - x_0)^{\nu_2}, \\ F_i(t, x, \Phi_1, \dots) &= \sum_{\nu_1, \nu_2, \dots, \nu_{m+2}=0}^{\infty} b_{\nu_1, \nu_2, \dots, \nu_{m+2}}^i(\tau) (t - t_0)^{\nu_1} (x - x_0)^{\nu_2} \times \\ &\times \prod_{i=1}^m (\Phi_i - \Phi_{i0})^{\nu_i+2} \cdot (\bar{\Phi}_i - \bar{\Phi}_{i0})^{\nu_i+2} \cdot (q_i - q_{i0})^{\nu_i+2} \cdot (\bar{q}_i - \bar{q}_{i0})^{\nu_i+2}, \end{aligned} \quad (7)$$

що збігаються у відповідних областях. Тут позначено:

$$\Phi_{i0} = \Phi_i(t_0, x_0), \quad \bar{\Phi}_i = \Phi_i(t - \tau, x), \quad \bar{\Phi}_{i0} = \Phi_i(t_0 - \tau, x_0),$$

$$q_i = \frac{\partial \Phi_i(t, x)}{\partial x}, \quad q_{i0} = \frac{\partial \Phi_i(t_0, x_0)}{\partial x}, \quad \bar{q}_i = \frac{\partial \Phi_i(t - \tau, x)}{\partial x}, \quad q_{i0} = \frac{\partial \Phi_i(t_0 - \tau, x_0)}{\partial x}.$$

При цьому

$$a_{\nu_1, \nu_2}^i = \frac{1}{\nu_1! \nu_2!} \left(\frac{\partial^{\nu_1 + \nu_2} \varphi_i}{\partial t^{\nu_1} \partial x^{\nu_2}} \right)_{t=t_0, x=x_0}, \quad b_{\nu_1, \nu_2, \dots, \nu_{m+2}}^i = \frac{1}{\nu_1! \nu_2! \dots \nu_{m+2}!} \left(\frac{\partial^{\nu_1 + \nu_2 + \dots + \nu_{m+2}} F_i}{\partial t^{\nu_1} \partial x^{\nu_2} \dots \partial q_m^{\nu_{m+2}}} \right)_{t=t_0, x=x_0, \dots, \bar{q}_m = \bar{q}_{m0}}.$$

Стверджується, що задача Коші для такої системи із запізнюванням має єдиний розв'язок у класі аналітичних функцій, який тому може бути представлено степеневим рядом

$$\Phi_i(t, x) = \sum_{i=0}^{\infty} \sum_{k=0}^{\infty} C_{ik}^i (t - t_0)^i (x - x_0)^k. \quad (8)$$

Це твердження є аналогом теореми Ковалевської для рівнянь виду (6). Доведення цього положення може бути виконано за допомогою методу «мажорант» так само, як це виконано для звичайних ДРЧП [10]. Слід лише зазначити наступне. При доведенні теореми Ковалевської в випадку, який розглядається, для спрощення бажано будувати розкладення розв'язків, функцій F_i і початкових функцій φ_i в степеневі ряди в околі t_0 , тобто в околі правої границі області E_{t_i} та $x = x_0 \in \Omega$. Більш того, без втрати загальності, можна будувати розкладання в околі точки $t_0 = 0 \in E_{t_i}$, $x = x_0 \in \Omega$ за припущення, що початкові функції на E_{t_i} задовольняють умові $\varphi_i(t, x) \equiv 0$. Якщо б це було не так, то можна було б увести різниці $t - t_0$, $x - x_0$ в якості нових незалежних змінних, а різниці $\Phi_i - \varphi_i$ – в якості нових невідомих функцій V_i , для яких всі початкові значення тотожно дорівнюють нулю, в той час, як загальний вигляд рівнянь залишається незмінним, тобто розглядати основну початкову задачу з нульовими початковими умовами.

Принцип стислих відображень. Як вже зазначалося, метод кроків дає розв'язок задачі у досить широкому класі неперервних функцій, однак він (метод) не може бути застосований у випадку дуже малого τ , тобто у випадку, коли початкова множина E_{t_i} збігається до однієї точки.

Аналог теореми Ковалевської стверджує існування аналітичного розв'язку задачі Коші для аналітичних рівнянь. Виникає питання, чи існують в цьому випадку інші розв'язки? Дійсно, для того, щоб система функцій $\Phi_1, \dots, \Phi_m$ була розв'язком задачі, немає потреби вимагати, щоб вони мали похідні тих порядків, які входять у рівняння (6), які розглядаються.

У загальному випадку, а також для випадків, коли метод кроків не можна застосовувати, а необхідно визначити існування та єдиність розв'язку у класі неаналітичних функцій, відповідь можуть дати теореми, засновані на розгляді топологічної структури диференціальних рівнянь, зокрема принципу стислих відображень.

Розглянемо, наприклад, задачу Коші для рівнянь гіперболічного типу другого порядку із запізнюванням

$$\frac{\partial^2 \Phi(t, x)}{\partial t \partial x} = f \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial x}, \frac{\partial \Phi(t - \tau, x)}{\partial x} \right], \quad (9)$$

та початковою умовою $\Phi(t, x)|_{t \in E_{t_0}} = \varphi(t, x)$, де $\varphi(t, x)$ – неперервна по t і x та така, що один раз диференціюється по x , функція.

Тоді справедлива наступна *теорема*: якщо в рівнянні (9) функція f неперервна в околі точки $\left(t_0, x_0, \varphi(t_0, x_0), \varphi(t_0 - \tau, x_0), \frac{\partial \varphi(t_0, x_0)}{\partial x}, \frac{\partial \varphi(t_0 - \tau, x_0)}{\partial x} \right)$ за сукупністю всіх аргументів, а по аргументах, починаючи з третього, задовольняє умовам Ліпшиця рівномірно відносно t і x , то існує єдиний неперервний по t і x , та такий, що один раз диференціюється по x розв'язок рівняння (9), і такий, що задовольняє на E_{t_0} початковій умові.

Доведення теореми. Виконаємо заміну рівняння (9) на еквівалентне інтегральне рівняння (в силу зауваження початкові умови вважаються нульовими $\varphi \equiv 0$)

$$\Phi(t, x) = \iint_D f \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial x}, \frac{\partial \Phi(t - \tau, x)}{\partial x} \right] dx dt, \quad (10)$$

де область D – область визначення функції f на площині xOt , яка містить в собі значення $t_0 \leq t \leq t_0 + h$, $x_0 \leq x \leq x_0 + \sigma$ та графічно являє собою криволінійний трикутник. Теорему буде доведено, якщо буде показано, що оператор A

$$A[\Phi(t, x)] = \iint_D f \left[t, x, \Phi(t, x), \Phi(t - \tau, x), \frac{\partial \Phi(t, x)}{\partial x}, \frac{\partial \Phi(t - \tau, x)}{\partial x} \right] dx dt,$$

завданий у повному метричному просторі M :

- переводить елементи простору M в елементи того ж самого простору;
- $\rho[A(y), A(z)] \leq \alpha \rho(y, z)$, де y та z – будь-які точки простору M ; $0 < \alpha < 1$ і не залежить від вибору точок y та z , а $\rho(y, z)$ – відстань між точками y та z у просторі M .

Зауважимо, що виконання цих двох умов гарантує існування єдиної нерухомої при дії оператора A точки Φ^* простору M . Цю точку може бути віднайдено методом послідовних наближень, тобто $\Phi^* = \lim_{n \rightarrow \infty} \Phi_n^*$ де $\Phi_n^* = A(\Phi_{n-1}^*)$ ($n = 1, 2, \dots$). При цьому точка Φ_0^* – обирається довільно в просторі M .

Таким чином, розглянемо простір M , елементами якого є функції $\Phi(t, x)$, неперервні по t і x та такі, що один раз диференціюються по x при $t_0 \leq t \leq t_0 + h$, $x_0 \leq x \leq x_0 + \sigma$, причому на E_{t_0} всі ці функції дорівнюють початковим функціям. Відстань задамо формулою

$$\rho[y(t, x), z(t, x)] = \sup_D |y(t, x) - z(t, x)| + \sup_D \left| \frac{\partial y(t, x)}{\partial x} - \frac{\partial z(t, x)}{\partial x} \right|. \quad (11)$$

При такому визначенні відстані M буде повним метричним простором, збіжність в якому означає рівномірну в D збіжність послідовності функцій Φ_n^* та послідовності їх частинних похідних $\frac{\partial \Phi_n^*}{\partial x}$ до граничної функції Φ^* та її похідної $\frac{\partial \Phi^*}{\partial x}$.

Очевидно, при достатньо малих h та σ перша умова принципу стислих відображень буде виконаною: $A[\Phi(t, x)]$ неперервна, якщо $\Phi(t, x)$, а також визначена при $t_0 \leq t \leq t_0 + h_1$, $x_0 \leq x \leq x_0 + \sigma_1$ за достатньо малих h_1 та σ_1 .

Перевіримо виконання другої умови принципу стислих відображень. В силу виконання умов Ліпшиця з постійною Ліпшиця L маємо:

$$\begin{aligned} \sup_D |A[y(t, x)] - A[z(t, x)]| &= \sup_D \left| \iint_D \left\{ f[t, x, y(t, x), y(t - \tau, x), \frac{\partial y(t, x)}{\partial x}, \frac{\partial y(t - \tau, x)}{\partial x}] - \right. \right. \\ &\quad \left. \left. f[t, x, z(t, x), z(t - \tau, x), \frac{\partial z(t, x)}{\partial x}, \frac{\partial z(t - \tau, x)}{\partial x}] \right\} dx dt \right| \leq \\ &\leq L \sup_D \left| \iint_D \left\{ |y(t, x) - z(t, x)| + |y(t - \tau, x) - z(t - \tau, x)| + \left| \frac{\partial y(t, x)}{\partial x} - \frac{\partial z(t, x)}{\partial x} \right| + \right. \right. \\ &\quad \left. \left. + \left| \frac{\partial y(t - \tau, x)}{\partial x} - \frac{\partial z(t - \tau, x)}{\partial x} \right| \right\} dx dt \right| \leq \\ &\leq 2Lh\sigma \left\{ \sup_D |y(t, x) - z(t, x)| + \sup_D \left| \frac{\partial y(t, x)}{\partial x} - \frac{\partial z(t, x)}{\partial x} \right| \right\} = 2Lh\sigma\rho[y(t, x), z(t, x)]. \end{aligned}$$

Тоді при $h\sigma + h \leq \frac{\alpha}{2L}$, де $0 < \alpha < 1$, другу умову принципу стислих відображень буде

виконано. Таким чином, при $h \leq \min \left\{ \frac{\alpha}{4L}, h_1 \right\}$, $\sigma \leq \min \{1, \sigma_1\}$ можна стверджувати, що

існує єдина нерухома точка оператора A , тобто єдиний неперервний і такий, що один раз диференціюється по x розв'язок основної початкової задачі для рівняння (10).

Висновки

У випадку ОПЗ для рівняння більш загального виду, ніж (10), доведення за допомогою принципу стислих відображень конструктивно нічим не відрізняється від наведеного вище доведення, якщо належним чином задати відстань в метричному просторі та увести додаткові обмеження такі, як гіперболічний тип рівняння. Розглянута теорема має місце і у випадках змінного запізнювання $\tau = \tau(t, x)$, якщо накласти додаткову умову неперервності по t та x функції $\tau(t, x)$. Доведення цього твердження можна здійснити за допомогою принципу стислих відображень в просторі з тою ж самою метрикою.

Список литературы

1. Бутковский, А.Г. Методы управления системами с распределенными параметрами / А.Г. Бутковский. — М.: Наука, 1975. — 368 с.
2. Мацевитый, Ю.М. Моделирование нелинейных процессов в распределенных системах / Ю.М. Мацевитый, В.Е. Прокофьев. — К.: Наукова думка, 1985. — 303 с.

3. Бессекерский, В.А. Теория систем автоматического регулирования / А.В. Бессекерский, Е.П. Попов. — М.:1975. — 768 с.
4. Верлань, А.Ф. Математическое моделирование аномальных диффузионных процессов / А.Ф. Верлань, С.А. Положаенко, Н.Г. Сербов. — К.: Наукова думка, 2011. — 416 с.
5. Гуль, И.М. Задача коши для некоторых дифференциальных уравнений в частных производных с функциональными аргументами / И.М. Гуль // УМН. — 1985. — №2. — С. 153 — 156.
6. Петухов, Р.В. О задаче Коши для дифференциальных уравнений в частных производных с запаздывающим аргументом в гильбертовом пространстве / В.Р. Петухов // Изв. ВУЗов. — Математика. — 1990. — Вып. 6. — С.195-202.
7. Wang, P.R.C. Stability of distributed-parameter processes with time-delays / P.R.C. Wang, M.L. Bandy // Electron. and Control. — 2003. — Vol. 15, №4. — P. 343-362.
8. Азбелев, Н.В. Введение в теорию функционально-дифференциальных уравнений / Н.В. Азбелев, В.П. Максимов. — М.: Наука, 1991. — 280 с.
9. Корн, Г. Справочник по математике / Г. Корн, Т. Корн. — М.: Наука, 1989. — 831 с.
10. Петровский, И.Г. Лекции по уравнениям в частных производных / И.Г. Петровский. — М.: Физматгиз, 1961. — 400 с.

МОДЕЛИ РАСПРЕДЕЛЕННЫХ СИСТЕМ С ЗАПАЗДЫВАЮЩИМ АРГУМЕНТОМ

С. А. Положаенко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sanp277@gmail.com

Предложены математические модели систем с распределенными параметрами, которые характеризуются запаздывающим аргументом по времени. Модели получены для систем k -го порядка, что позволяет использовать их для большинства прикладных задач математической физики. Выполнено качественное исследование предложенных моделей, в результате чего строго доказано существование и единственность решений соответствующих дифференциальных уравнений, которые образуют данные модели.

Ключевые слова: математическая модель, запаздывающий аргумент, основная начальная задача, метод шагов, метод сжатых отображений, аналитические решения дифференциальных уравнений

MODELS OF DISTRIBUTED SYSTEMS WITH DELAYED ARGUMENT

S. A. Polozhaenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odessa, 65044, Ukraine; e-mail: sanp277@gmail.com

Mathematical models of systems with distributed parameters that are characterized by a delayed time argument are proposed. The models are obtained for systems of the k -th order, which makes it possible to use them for the majority of applied problems of mathematical physics. A qualitative study of the proposed models is carried out, as a result of which the existence and uniqueness of the solutions of the corresponding differential equations that form the model data is rigorously proved.

Keywords: mathematical model, delayed argument, basic initial problem, step method, compressed mapping method, analytical solutions of differential equations

РОЗРОБКА ІНТЕРФЕЙСУ АДМІНІСТРАТОРА В СИСТЕМІ УПРАВЛІННЯ САЛОНОМ КРАСИ

О.Ю. Лебедєва, Т.О. Бирченко

Одеський національний політехнічний університет
пр. Шевченко 1, Одеса, 65044, Україна; e-mail: whiteswanhl@yahoo.com

У роботі розроблено інтерфейс адміністратора в системі управління салоном краси. Представлено модифікація системи управління салоном краси для автоматизації роботи персоналу. Визначені напрями автоматизації роботи адміністратора салону та структура інтерфейсу адміністратора.

Ключові слова: інтерфейс, розробка інтерфейсу, салон краси, система управління салоном краси.

Вступ

Раніше в салонах краси використовувались паперові журнали для управлінського обліку та для організаційної роботи, тобто для запису клієнтів, витрат матеріалів, розрахунку заробітної плати тощо, вважалися найбільш прийнятним варіантом паперові носії. Але коли на зміну паперовим документам прийшли автоматизовані системи управління (АСУ), оцінити діяльність салону стало набагато простіше та швидше.

Програма автоматизації серйозно полегшує аналіз роботи салону краси, тому що систематизує багато параметрів діяльності салону, підвищуючи загальну ефективність його роботи. Раніше коли у салоні вівся паперовий журнал обліку наданих послуг та клієнтів, потрібно було багато часу, щоб відповісти на такі питання власника або директора: які клієнти приносять дохід салону, який прибуток приносить кожен майстер, які услуги найбільш популярні та затребувані та інші. Використання систем управління салоном краси дозволяє отримати відповіді на ці запитання за лічені хвилини.

Серед основних задач салону краси, що стоять перед власниками, також можна виділити такі: поліпшення якості обслуговування, допомога в управлінні підприємством, боротьба з крадіжками персоналу тощо. Правильно спроектований та розроблений інтерфейс системи управління салоном краси дозволить вирішити вказані задачі, що робить дану роботу актуальною.

Мета та задачі роботи

Метою роботи є розробка інтерфейсу адміністратора в системі управління салоном краси для підвищення ефективності роботи персоналу.

Ефективність роботи персоналу будемо обчислювати за допомогою кількісного аналізу інтерфейсу – моделі GOMS.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

– визначення можливих напрямків автоматизації роботи адміністратора в салоні краси;

- визначення структури та проектування інтерфейсу адміністратора салону краси;
- програмна реалізація інтерфейсу адміністратора в системі управління салоном краси.

Під автоматизацією роботи персоналу в салоні краси у даній роботі будемо розуміти автоматизацію роботи з документами та довідниками для прискорення процесу їх створення та заповнення, скасування зберігання інформації на паперових носіях.

Основна частина

Інтерфейс – сукупність можливостей, способів і методів взаємодії двох систем.

Людино-машинний інтерфейс – це методи і засоби забезпечення безпосередньої взаємодії між оператором і технічною системою, що представляють можливості оператору керувати цією системою і контролювати її роботу.

Інтерфейс користувача – різновид інтерфейсів, в якому одна сторона представлена людиною (користувачем), інша – машиною (пристроєм), і являє собою сукупність засобів і методів, за допомогою яких користувач взаємодіє з різними пристроями та апаратурою. Зазвичай саме цей термін використовується по відношенню до взаємодії між оператором ЕОМ і програмним забезпеченням, з яким він працює.

Будь-який інтерфейс, незалежно від сфери його застосування, має п'ять основних характеристик, а саме:

- продуктивність користувачів;
- кількість людських помилок;
- швидкість навчання роботи з системою;
- суб'єктивне задоволення користувачів;
- здатність збереження користувачами навичок роботи з системою протягом тривалого часу.

Існують декілька концепцій хорошого інтерфейсу. По-перше, дизайн, орієнтований на користувачів (ДОК), де необхідно визначити, хто цільова аудиторія та в чому конкретно інтерфейс, що розроблюється, їм допоможе. Але ДОК не враховує того факту, що людина – дуже адаптивна система. Користувачі здатні до адаптації в дуже широких межах. ДОК не відображає того, що роблять користувачі в системі та заради чого вони з системою взаємодіють.

Згідно дизайну, орієнтованого на завдання користувачів (ДОЗ), той інтерфейс гарний, в якому ефективно виконуються завдання користувачів. Тобто необхідно вибрати найбільш ефективне рішення задачі та забезпечити її виконання. Але ДОЗ не дозволяє визначити, яке саме число розв'язуваних системою завдань є необхідним та достатнім. Завжди є завдання, які система ще не вирішує. Всі задачі необхідно реалізувати в системі, а це веде до нескінченного зростання функціональності.

Згідно дизайну, орієнтованому на мотиви користувачів (ДОМ), користувачі роблять щось для задоволення особистих потреб, інакше – мотивів; упізнавши ці потреби та порівнявши їх із завданнями користувачів, ми отримуємо можливість краще зрозуміти, що потрібно робити. На жаль, ДОМ, як і ДОК, ДОЗ досить фрагментарний, оскільки концентрується тільки на якомусь одному аспекті інтерфейсу.

Сьогодні найбільш поширеним критерієм хорошого інтерфейсу є юзабіліті. Юзабіліті – це показник кількості операторських помилок, швидкості взаємодії з продуктом, швидкості навчання навичкам взаємодії та суб'єктивної задоволеності певних користувачів продукту, що досягають певних цілей/мотивів в певному середовищі.

Процес проектування та розробки призначеного для користувача інтерфейсу складається з чотирьох основних етапів: збір та аналіз інформації від користувачів, розробка користувацького інтерфейсу, побудова користувацького інтерфейсу, підтвердження якості створеного користувацького інтерфейсу.

Розглянемо перший етап – збір та аналіз інформації. Можна виділити два основних користувача системи «салон краси» – адміністратор та управляючий.

Управляючий займається веденням складського обліку (прихід, списання, оприбуткування, переміщення матеріалів), визначає ціну матеріалів та послуг, фінансового обліку (прибутковий та видатковий касові ордери), нарахування заробітної плати та табеля робочого часу. Управляючий – це людина, яка має знання та досвід роботи з комп'ютером. Інтерфейс управляючого має бути націленим на функціональність, а не на простоту.

Робота салону починається з адміністратора. Він зустрічає відвідувачів, допомагає їм підібрати відповідні процедури та додаткові послуги, здійснює грошові розрахунки, супроводжує до знайомства з майстрами салону. Адміністратор координує роботу майстрів салону: перукарів, візажистів, косметологів, масажистів та інших. Від грамотної та ефективної взаємодії адміністраторів з клієнтами залежить успішність та процвітання салону. Частіше адміністратори – це люди, які не мають вищої освіти та є дуже поганими користувачами комп'ютерів. Тому інтерфейс адміністратора потрібен бути простим для розуміння його роботи та швидким для виконання поставлених завдань та потребує більш уваги при його розробці.

Основними завданнями адміністратора є ведення розпису відвідувань клієнтів, робота з клієнтами, створення рахунків з наданими послугами та витраченими матеріалами, фінансовий облік. Згідно з критерієм юзабіліті, необхідно розробити інтерфейс адміністратора, який би виконував швидко та без помилок завдання адміністратора та був простий та зручний у роботі.

Було розроблено інтерфейс адміністратора, який складається з двох форм. Перша – для ведення розпису та роботи з клієнтами (рис. 1), друга – для створення рахунків та фінансового обліку (рис. 2).

При відкритті форми для ведення розпису у інтерфейсі адміністратору доступно розклад відвідувань клієнтів на поточний день. При зміні дати у верху інтерфейсу розклад зміниться і покаже дані на обраний день. Для додавання нового запису у розклад або редагування існуючого запису необхідно обрати колонку бажаного майстра та рядок необхідного часу та подвійним клацанням миші обрати комірку. Далі відкриється вікно для подальшої роботи з клієнтом. Подальша робота з клієнтом – це список дій, які виконує адміністратор при роботі з клієнтом, а саме:

- створення нового запису у розкладі – коли клієнт дзвонить по телефону до салону та бажає записатися до майстра;
- дзвінок клієнту – дзвінок адміністратора клієнту для нагадування та уточнення візиту;
- створення рахунку – коли клієнт приходить до салону на обслуговування;
- відміна відвідування – коли клієнт дзвонить та просить відмінити відвідування.

Зміна статусу запису відображається в розкладі зміною кольору.

При відкритті форми для створення рахунків аналізуються такі дані:

- послуги салону – знайдені послуги сортуються за категоріями та на формі створюються кнопки з назвами категорій послуг для більш зручного пошуку необхідної послуги для заповнення поточного рахунку;
- матеріали, які використовуються у салоні – знайдені матеріали сортуються за категоріями та на формі створюються кнопки з назвами категорій матеріалів для більш зручного пошуку необхідного матеріалу для заповнення поточного рахунку;

– наявність створених, не розрахованих рахунків на поточний день – знайдені рахунки відображаються у інтерфейсу у вигляді закладок, при виборі яких на формі можна побачити дані рахунку, а саме прізвище клієнта, суму рахунку, надані послуги та витрачені матеріали.

а

б

Рис. 1. Інтерфейс адміністратора: а – форма для ведення розпису; б – форма для роботи з клієнтами

Рис. 2. Форма для створення рахунків та фінансового обліку

Розрахувати ефективність розробленого інтерфейсу можна за допомогою моделі GOMS. Модель GOMS дозволяє передбачити час, необхідний для виконання завдання за допомогою конкретного інтерфейсу. Було виявлено, що для вирішення поставленого завдання при роботі з комп'ютером користувач робить певний набір жестів. Таким чином, час виконання завдання складається з часу виконання цих жестів та з проміжків

між жестами, які потрібні для обмірковування. Для опису жестів використовуються наступні позначки:

- $K = 0.2$ с – час, необхідний для натискання клавіші клавіатури або миші;
- $P = 1.1$ с – час, необхідний для переміщення покажчика миші до певної позиції на моніторі;
- $H = 0.4$ с – час, необхідний для переміщення руки користувача з клавіатури на мишу та з миші на клавіатуру;
- $M = 1.35$ с – ментальна пауза, тобто час, необхідний користувачу на обмірковування наступного кроку.

Вказаний час – це середній час виконання різних жестів для будь-якої людини.

Для оцінки виконання завдання за допомогою конкретного інтерфейсу, необхідно описати послідовність жестів, які виконує користувач при роботі з інтерфейсом, застосувати правила GOMS та обчислити час, необхідний для виконання завдання.

Для порівняння візьмемо задачу «Оплатити рахунок». Форма оплати рахунку у розробленому інтерфейсі адміністратора продемонстрована на рис. 3, оплата рахунку у документі «Рахунок» на рис. 4.

000000024
Кондратьева Інна Валеріївна
Сума: 100.00

Мастер1	Услуга	Количество
Мастер2	Материал	Ед.
Абрамова А.С.		
Нет мастера	Получен 1 категория	

Материал Единица Кол

Всего к оплате (грн): 100,00

Способ оплаты:

Наличными

Кредитка

Долг

Отмена

Оплатить Выход

Косметология

Маникюр/Педикюр

Парикмахерские услуги

Продажи

Рис. 3. Оплата рахунку в інтерфейсі адміністратора

Счет: Счет 000000019 от 26.06.2017 00:00:00

Провести и закрыть Провести

Номер: 000000019 Дата: 26.06.2017 00:00:00

Организация: Спа-салон

Контрагент: Шмиль Надежда Алексеевна

Инфо карточка: Шмиль Надежда Алексеевна

Администратор:

Начало оформ.: 26.06.2017 10:56:26

Дата создания: 26.06.2017 10:56:26

Время оплаты:

Дата сохранения: 26.06.2017 11:00:55

Сумма чека: 300.00

Сумма оплаты:

Программист

Комментарий:

Услуги / товары Материалы Оплата

Добавить

N	Вид оплаты	Касса	Валюта	Курс	Сумма	Сумма учета
1	Наличными	Касса гривня	Гривна	1.00000	300,00	300,00

Рис. 4. Оплата рахунку в документі «Рахунок»

Для форми оплати рахунку у розробленому інтерфейсі адміністратора послідовність жестів складається з *НРКРК*, після використання правил GOMS

послідовність трансформується у *НМРКМРК*. Для форми оплати рахунку в документі «Рахунок» складається з *НРКРКРКРКРК*, після використання маємо послідовність *НМРКМРКМРКМРКМРК*. Обчислимо отримані послідовності:

$$НМРКМРК = 0.4 + 1.35 + 1.1 + 0.2 + 1.35 + 1.1 + 0.2 = 5.7 \text{ с};$$

$$НМНКМРКМРКМРКМРКМРК = 0.4 + 1.35 + 1.1 + 0.2 + 1.35 + 1.1 + 0.2 + 1.35 + 1.1 + 0.2 + 1.35 + 1.1 + 0.2 = 13.62 \text{ с}.$$

Результати порівняння показують, що задача оплати рахунку у розробленому інтерфейсі виконується швидше, чим у документі «Розрахунок» у 2.4 рази.

Висновки

У роботі були визначені основні користувачі системи «Салон краси» – управляючий та адміністратор. Робота адміністратора вимагає від інтерфейсу виконувати завдання швидко та без помилок, зручним та простим способом. Визначені можливі напрямки автоматизації роботи адміністратора в салоні краси. Автоматизації підлягає ведення розкладу, робота з клієнтами, створення рахунків та фінансовий облік. В роботі визначена структура інтерфейсу. Було спроектовано та реалізовано інтерфейс адміністратора в системі управління салоном краси.

Список літератури

1. Мандел, Т. Разработка пользовательского интерфейса: Пер. с англ. – М.: ДМК Пресс, 2001. – 416 с.
2. Алан Купер об интерфейсе. Основы проектирования взаимодействия. – СПб.: Символ-Плюс, 2009. – 688 с.
3. Тидвелл, Дж. Разработка пользовательских интерфейсов. – СПб.: Питер, 2008. – 416 с.

РАЗРАБОТКА ИНТЕРФЕЙСА АДМИНИСТРАТОРА В СИСТЕМЕ УПРАВЛЕНИЯ САЛОНОМ КРАСОТЫ

Е. Ю. Лебедева, Т.А. Бырченко

Одесский национальный политехнический университет
пр. Шевченко 1, Одесса, 65044, Украина; e-mail: whiteswanhl@yahoo.com

В работе разработан интерфейс администратора в системе управления салоном красоты. Представлена модификация системы управления салоном красоты для автоматизации работы персонала салона. Определены направления автоматизации работы администратора салона и структура интерфейса администратора.

Ключевые слова: интерфейс, разработка интерфейса, салон красоты, система управления салоном красоты.

DEVELOPMENT OF THE ADMINISTRATOR INTERFACE IN THE BEAUTY SALON MANAGEMENT SYSTEM

E. Lebedeva, T. Byrchenko

Odessa National Polytechnic University
Shevchenko Avenue 1, Odessa, 65044, Ukraine; e-mail: whiteswanhl@yahoo.com

In work the interface of the manager in system of management of a beauty salon is developed. A modification of the beauty salon management system is presented to automate the work of the salon staff. The directions of automation of the salon administrator's work and the structure of the administrator's interface are determined.

Keywords: interface, interface development, beauty salon, beauty salon management system.

АНАЛІЗ ЧАСОВИХ РЯДІВ СПОЖИВАННЯ ПАЛИВА МАНЕВРОВИМ ТЕПЛОВОЗОМ В ЕКСПЛУАТАЦІЇ

Ю.Є. Калабухін, О.В. Рудковський

Український державний університет залізничного транспорту,
вул. Фейербаха, 7, Харків, 61050, Україна; e-mail: Od.is@rambler.ru

Описується алгоритм R/S аналізу для часових рядів споживання палива маневровим тепловозом при різних умовах експлуатаційної роботи, що виконується. Визначено основні положення методу оцінок показника Херста. На основі розрахунку та аналізу показника Херста зроблено висновок про антиперсистентність часових рядів споживання палива маневровим тепловозом в експлуатації.

Ключові слова: R/S аналіз, показник Херста, фрактал, часовий ряд, маневровий тепловоз, експлуатація, витрата палива.

Вступ

Сучасні умови оновлення або модернізації тягового рухомого складу вимагають необхідності визначення його життєвого циклу. Однією із важливіших енергетичних складових життєвого циклу маневрових тепловозів є споживання палива для здійснення експлуатаційної роботи, яка характеризується стохастичним чергуванням станів «холодного» та «гарячого» простою, виконання маневрової роботи. Споживання палива залежить як від багатьох експлуатаційних факторів, так і від технічного стану тепловоза і має змінний характер за часом. Таким чином, вивчення життєвих циклів маневрових тепловозів неможливе без дослідження та аналізу часових рядів споживання палива. Найбільш адекватним математичним апаратом для дослідження динаміки та структури стохастичних процесів, які володіють довгостроковою залежністю та фрактальною структурою є фрактальний аналіз.

У теперішній час зростає кількість робіт, що присвячені дослідженню часових рядів за допомогою методу нормованого розмаху. За цим методом досліджуються послідовності вимірювань температури атмосферного повітря, кількість опадів, товщина кілець річного приросту деревини та інших природних явищ [1, 2], вартості компанії, коливань обмінних курсів валют та інших економічних показників [3, 4]. В роботі [5] запропонована організація моніторингу технічного стану й створено метод для розрахунку залишкового ресурсу паливної апаратури тепловозів на основі розрахунку й оцінки показника Херста.

Мета роботи

Метою роботи є виклад результатів дослідження часових рядів споживання палива маневровим тепловозом за різних умов експлуатаційної роботи на основі використання методів фрактального аналізу.

Основна частина

Протягом i -ї робочої зміни маневровий тепловоз може знаходитись у стані «холодного» та «гарячого» простою, лінійного пробігу та виконання маневрової роботи.

Тривалість споживання палива маневровим тепловозом протягом i -ї робочої зміни (без урахування часу простою локомотива в «холодному» стані) визначається тривалістю знаходження локомотива в стані «гарячого» простою $\tau_{\text{г.пр.}}(i)$, лінійного пробігу $\tau_{\text{л.пр.}}(i)$, виконання маневрової роботи $\tau_{\text{м.р.}}(i)$, тобто

$$\tau(i) = \tau_{\text{г.пр.}}(i) + \tau_{\text{л.пр.}}(i) + \tau_{\text{м.р.}}(i). \quad (1)$$

Річна тривалість споживання палива маневровим тепловозом визначається за формулою

$$T = \sum_{i=1}^n \tau(i). \quad (2)$$

Кількість палива, що споживається маневровим тепловозом $G(i)$ залежить від стану, в якому він знаходиться протягом i -ї робочої зміни, та багатьох експлуатаційних факторів, характерних при виконанні тієї чи іншої експлуатаційної роботи.

Годинне споживання палива маневровим тепловозом протягом i -ї робочої зміни визначається за формулою

$$b(i) = \frac{G(i)}{\tau(i)}. \quad (3)$$

На рис. 1-4 наведено часові ряди годинного споживання палива маневровим тепловозом при різних умовах експлуатаційної роботи протягом року.

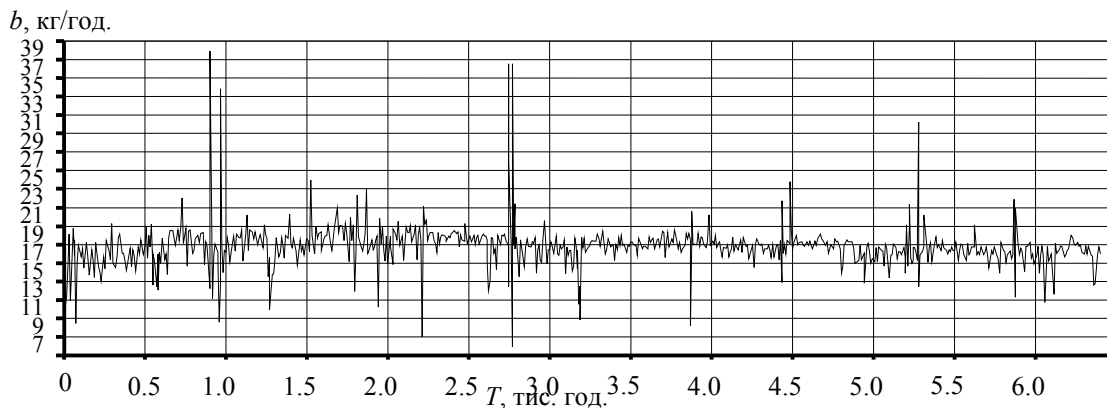


Рис. 1. Часовий ряд годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання сортувальної роботи

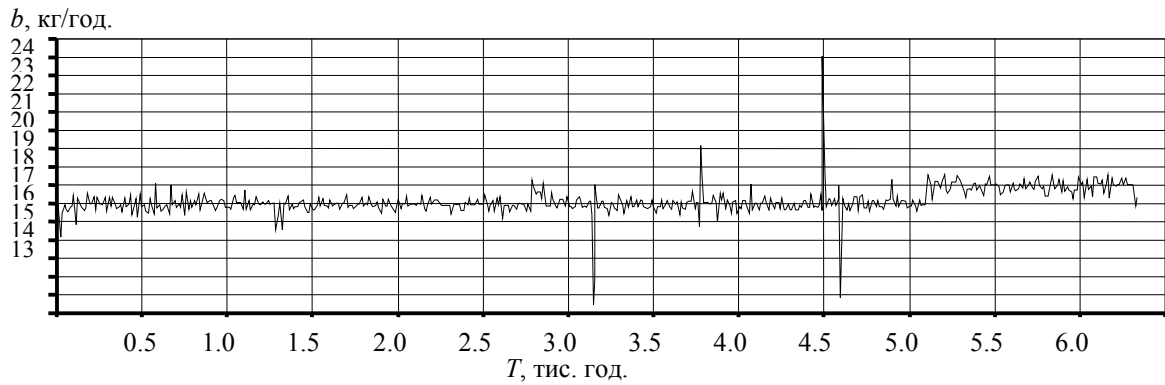


Рис. 2. Часовий ряд годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи по депо

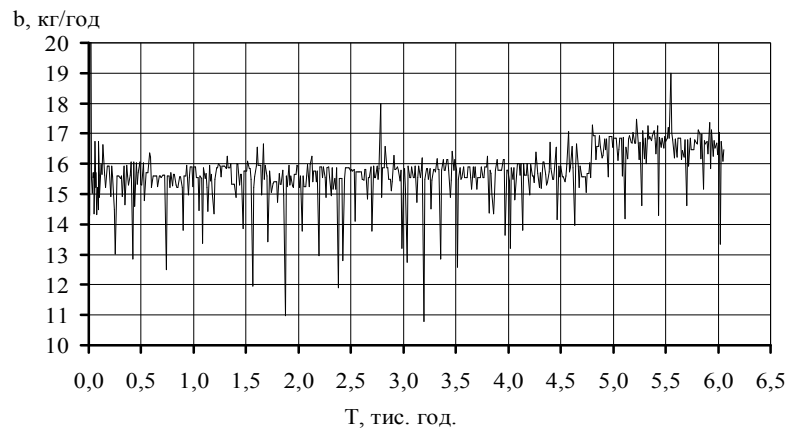


Рис. 3. Часовий ряд годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи по станції

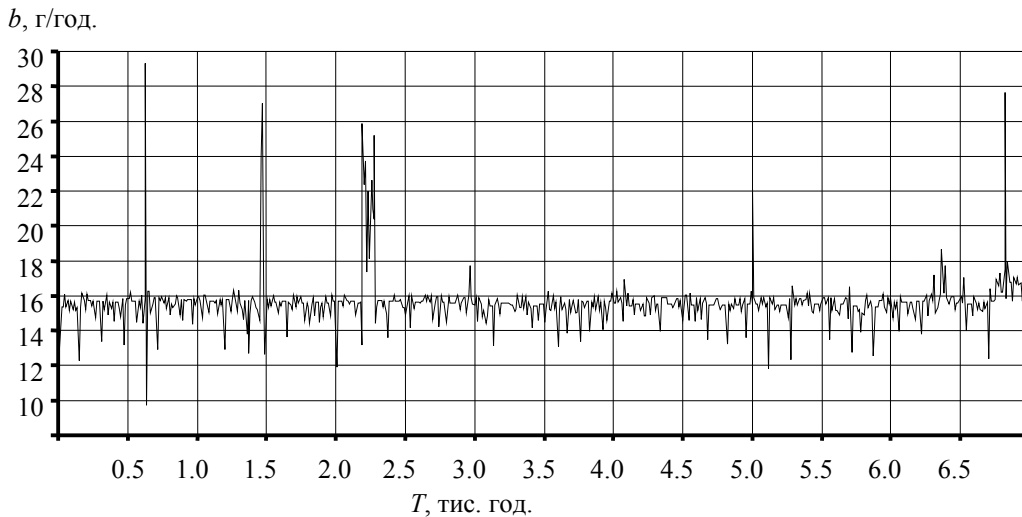


Рис. 4. Часовий ряд годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи на маневровій горці

Розглянемо одномірний часовий ряд годинного споживання палива маневровим тепловозом: $b(1), b(2), \dots, b(n)$. Кожне визначення $b(i)$ відповідає моменту часу $t(i)$ заміру споживання палива $G(i)$, що параметрично визначає функцію дійсної змінної $b(t)$ на деякій дискретній множині точок.

Показник Херста для ряду $b(n)$ визначається наступним чином [1, 6]. Вводиться змінна середня приростів $b(n)$ на кроці n по вибірці довжини k

$$\bar{b}(n, k) = \frac{1}{k} \cdot \sum_{i=n-k+1}^n b(i) \quad (4)$$

або з урахуванням формули (3)

$$\bar{b}(n, k) = \frac{1}{k} \cdot \sum_{i=n-k+1}^n \frac{G(i)}{\tau(i)}$$

та розраховується накопичене відхилення від середнього для вибірки довжиною k

$$R(n, k) = \max_{j \leq n} \left\{ \sum_{i=n-k+1}^j (b(i) - \bar{b}(n, k)) \right\} - \min_{j \leq n} \left\{ \sum_{i=n-k+1}^j (b(i) - \bar{b}(n, k)) \right\}. \quad (5)$$

Розраховується також змінна дисперсія часового ряду, що розглядається по вибірці довжини k

$$\sigma_b^2(n, k) = \frac{1}{k} \cdot \sum_{i=n-k+1}^n [b(i) - \bar{b}(n, k)]^2, \quad (6)$$

після чого розраховується логарифм відношення розмаху до шуму

$$\zeta(n, k) = \ln \left(\frac{R(n, k)}{\sigma_b^2(n, k)} \right). \quad (7)$$

Фіксується мінімальна довжина вибірки k_0 та максимальна довжина N , яка відповідає часовому горизонту аналізу. Встановлений порядок визначення (4)-(7) робиться для вибірок довжин k таких, що $1 < k_0 \leq N$.

Показник Херста $H_N(n)$ за вибіркою довжиною N на кроці n визначається як коефіцієнт регресії величини $\zeta(n, k)$ на логарифм довжини вибірки

$$\zeta(n, k) - \bar{\zeta}_N(n) = H_N(n) \cdot \left\{ \ln k - \frac{\ln \frac{N!}{(k_0 - 1)!}}{N - k_0 + 1} \right\} + \varepsilon(k), \quad (8)$$

$$\bar{\zeta}(n) = \frac{1}{N - k_0 + 1} \cdot \sum_{k=k_0}^N \zeta(n, k), \quad (9)$$

де $\varepsilon(k)$ – являє собою залишок регресії.

Кут ухилу прямої регресії дорівнює показнику Херста. Співвідношення $\frac{R(n, k)}{\sigma_b^2(n, k)}$ в літературних джерелах позначається як R/S . На рис. 5-8 наведено співвідношення R/S у логарифмічному масштабі при різних умовах експлуатаційної роботи маневрового тепловоза.

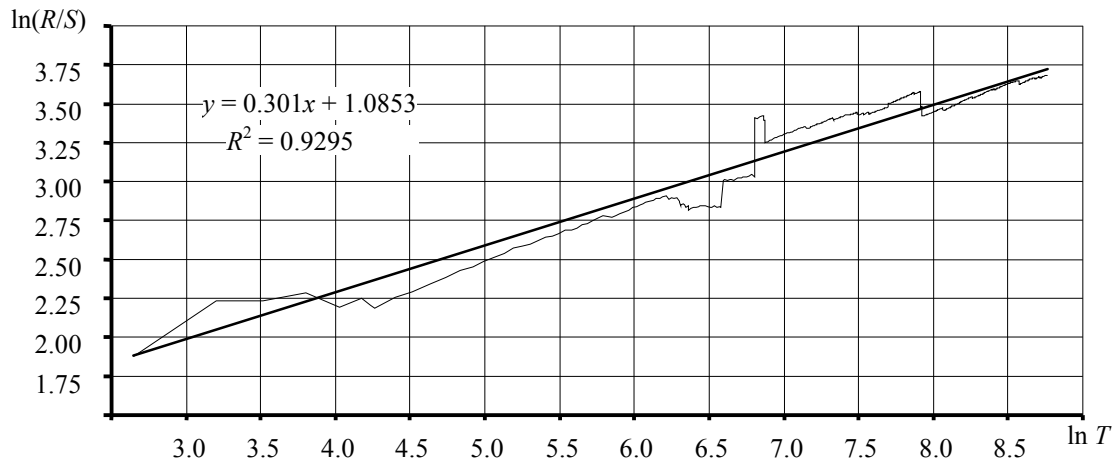


Рис. 5. Співвідношення R/S у логарифмічному масштабі за умови виконання маневровим тепловозом сортувальної роботи

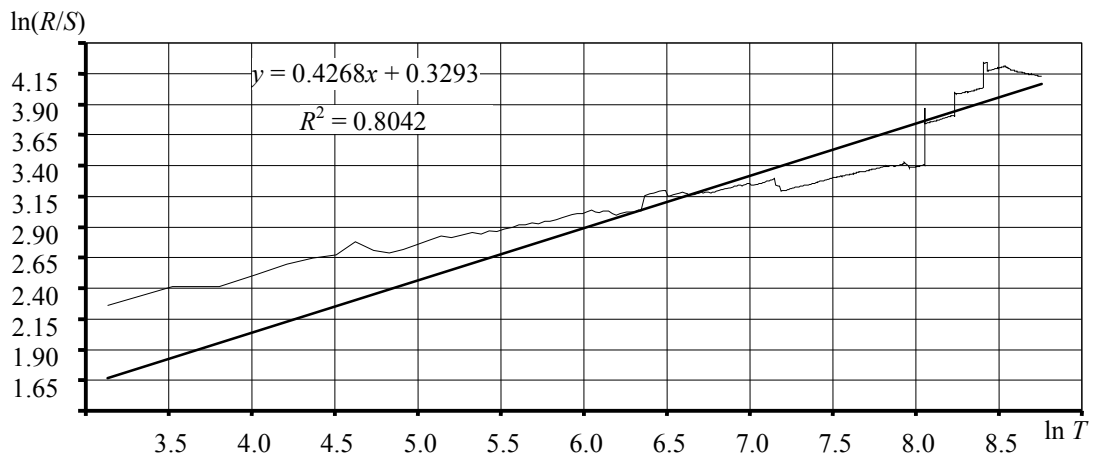


Рис. 6. Співвідношення R/S у логарифмічному масштабі за умови роботи маневрового тепловоза по депо

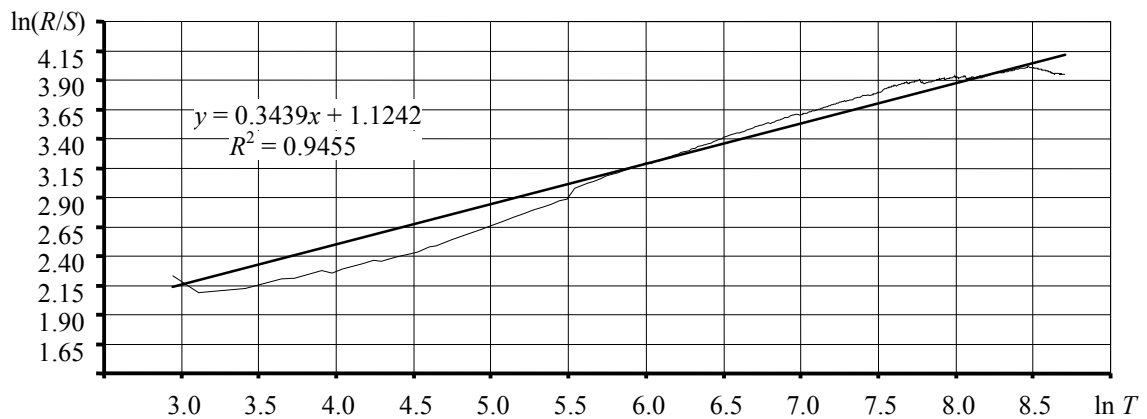


Рис. 7. Співвідношення R/S у логарифмічному масштабі за умови роботи маневрового тепловоза на станції

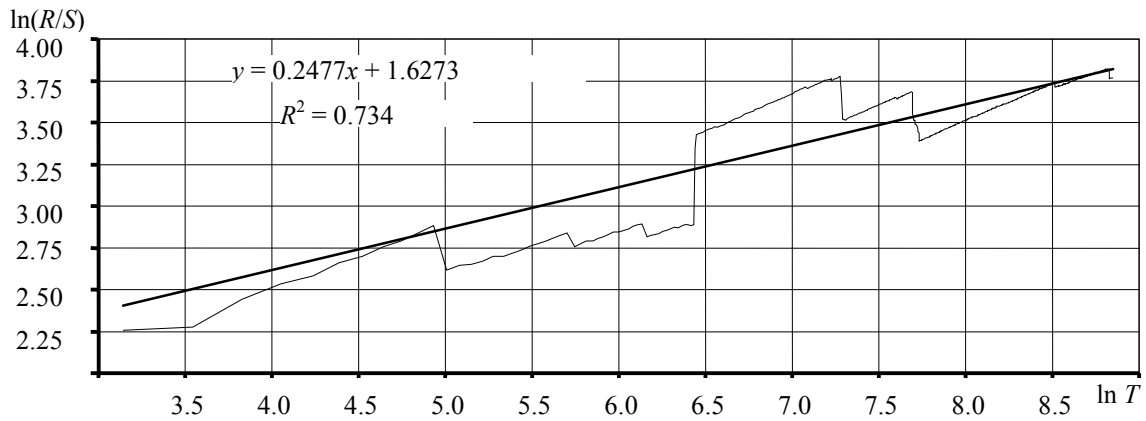


Рис. 8. Співвідношення R/S у логарифмічному масштабі за умови роботи маневрового тепловоза на маневровій горці

Приймаючи для всіх видів експлуатаційної роботи маневрового тепловоза мінімальну довжину вибірки $k_0 = 2$, отримаємо

$$H_N(n) = \frac{\sum_{k=2}^N \left\{ (\zeta(n, k) - \bar{\zeta}_N(n)) \cdot \left(\ln k - \ln \frac{N!}{N-1} \right) \right\}}{\sum_{m=2}^N \left\{ \left(\ln m - \ln \left(\frac{N!}{N-1} \right) \right) \right\}}. \quad (10)$$

Оскільки для всіх видів експлуатаційної роботи маневрового тепловоза $N \gg 1$, то у формулі (10) можливо використати формулу Стірлінга для апроксимації факторіала, та, нехтуючи різницею $N-1$ від N , отримаємо більш зручний вираз показника Херста:

$$H_N(n) = \frac{1}{N} \sum_{k=1}^N \left\{ (\zeta(n, k) - \bar{\zeta}_N(n)) \cdot \left(1 + \ln \frac{k}{N} \right) \right\}. \quad (11)$$

В результаті при фіксованій довжині вибірки N отримаємо набір показників Херста на послідовності кроків з номерами n .

На рис. 9-12 наведено зміну показника Херста в залежності від довжини часового ряду годинної витрати палива маневровим тепловозом ЧМЕЗ при різних умовах експлуатаційної роботи.

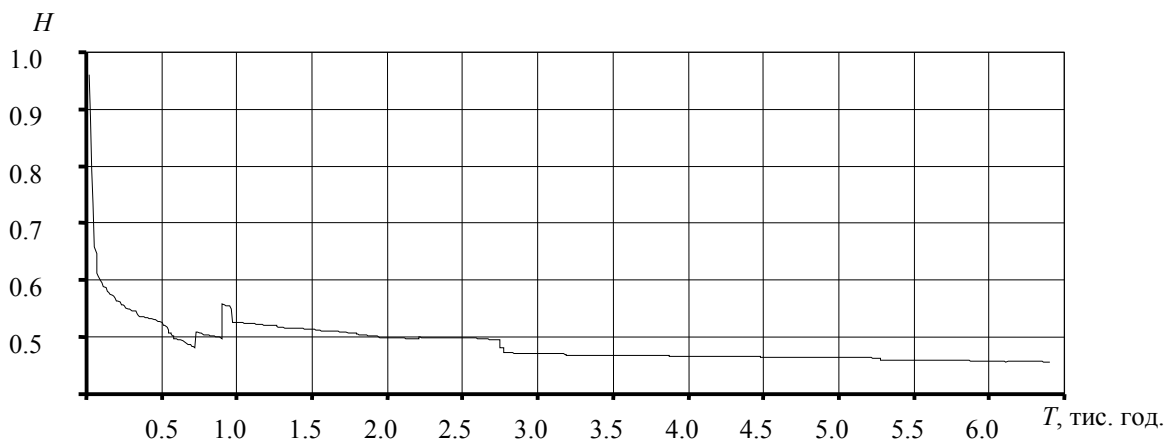


Рис. 9. Зміна показника Херста в залежності від довжини часового ряду годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання сортувальної роботи

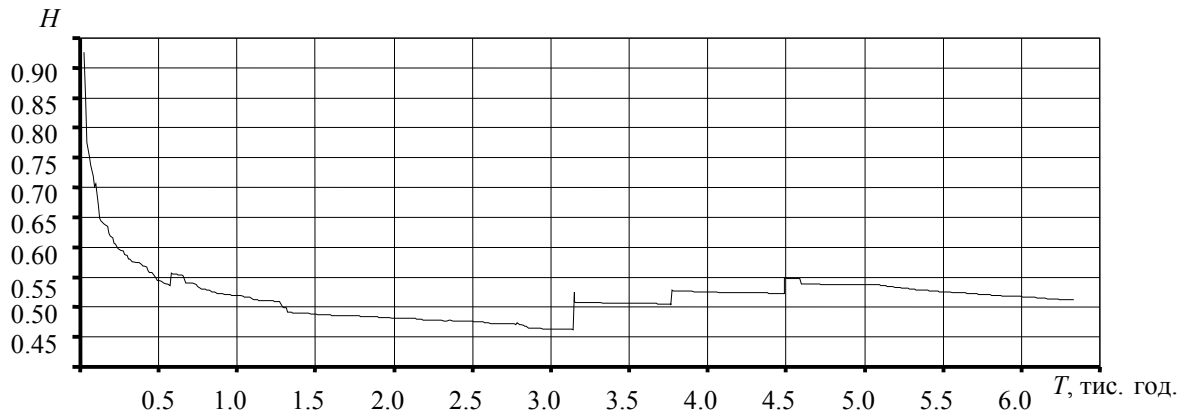


Рис. 10. Зміна показника Херста в залежності від довжини часового ряду годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи по депо

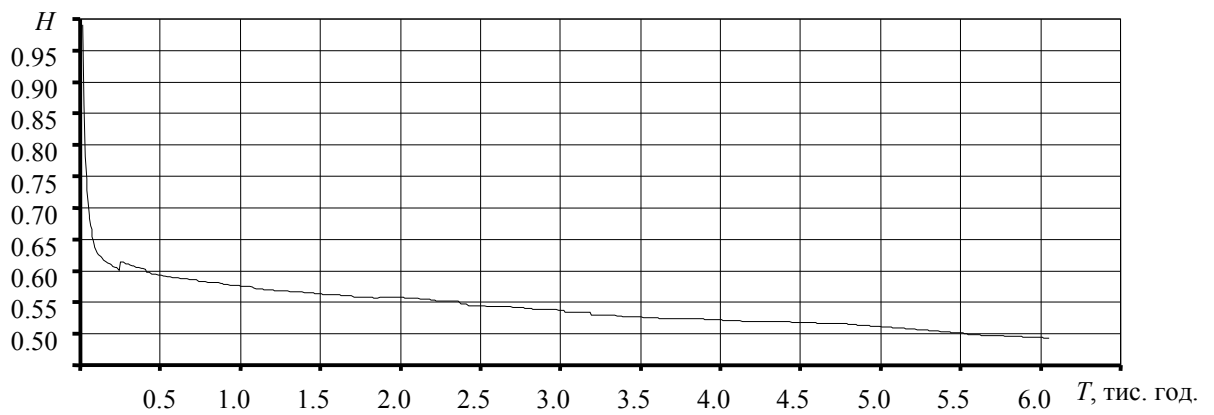


Рис. 11. Зміна показника Херста в залежності від довжини часового ряду годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи по станції

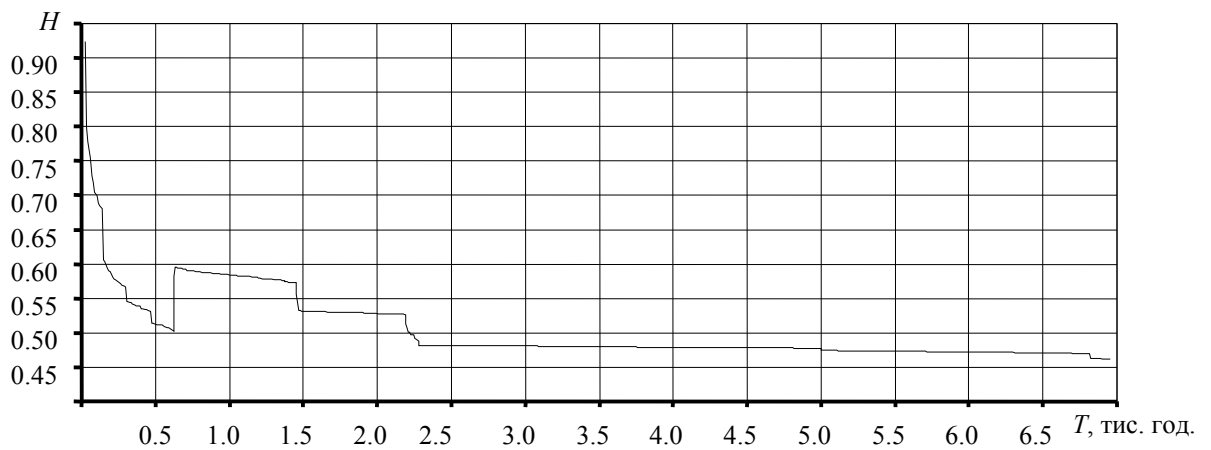


Рис. 12. Зміна показника Херста в залежності від довжини часового ряду годинного споживання палива маневровим тепловозом ЧМЕЗ для виконання роботи на маневровій горці

Результати дослідження часових рядів витрати палива маневровим тепловозом за різних умов експлуатаційної роботи на основі використання методів фрактального аналізу зведено до табл. 1.

Таблиця 1.

Часові ряди та їх параметри за різних умов експлуатаційної роботи маневрового тепловоза ЧМЕЗ

Вид експлуатаційної роботи	Максимальна довжина вибірки, N	Середнє значення варіанти, кг/год.	Середня довжина кроку, год.	$\frac{R(n,k)}{\sigma_b^2(n,k)}$	H
Сортувальна робота	687	16.7	9.3	39.84	0.301
Маневрова робота по депо	559	15.2	11.3	61.96	0.4268
Маневрова робота по станції	536	15.7	11.3	51.88	0.3439
Маневрова гірка	613	15.6	11.3	43.29	0.2477

Згідно класифікації для різних показників Херста:

- при $0 < H < 0.5$ – антиперсистентний часовий ряд, тобто ряд, при котрому відбувається так зване «повернення до середнього»: якщо система зростає в якийсь період, то в наступний період слід чекати падіння. Чим ближче H до 0, тим стійкіше ці коливання. Антиперсистентний часовий ряд називають «рожевим шумом»;
- при $H = 0.5$ – часовий ряд стохастичний. Такий процес називають «рожевим шумом»;
- при $0.5 < H < 1$ – персистентний часовий ряд (ці процеси ще називають «чорним шумом» і це тренд стійкі ряди). Часовий ряд характеризується довгостроковою пам'яттю. Якщо ряд почав зростати, то він буде зростати і подаль [3]. Тренд стійкість тим більше, чим ближче H до 1.

Висновки

Таким чином, аналіз часових рядів споживання палива маневровим тепловозом в експлуатації вказує на їх антиперсистентність, що означає зміну періодів зростання споживання палива на періоди його спаду та навпаки. Використання властивості антиперсистентності дозволяє достатньо просто та надійно прогнозувати подальший розвиток процесу споживання палива маневровим тепловозом на основі даних його історії.

Список літератури

1. Hurst, H. Long-term Storage. An Experimental Study / H. Hurst, R. Black, Y. Simaika. – London: Constamle, 1965. – 185 p.
2. Калущ, Ю.А. Показатель Херста и его скрытые свойства / Ю.А. Калущ, В.М. Логинов. // Сиб. журн. индустр. матем. – 2002. – Том 5, №4. – С. 29-37.
3. Петерс, Э. Фрактальный анализ финансовых рынков / Э. Петерс. – М.: Интернет-трейдинг, 2004. – 304с.
4. Никольчев, Е.В. Модели хаоса для процессов изменения курса акций / Е.В. Никольчев // Методы. Алгоритмы. Программы. – 2003. – №1(1). – С. 4.
5. Дробаха, В.І. Аналіз технічного стану та паливної економічності тепловоза з використанням методу Херста / В.І. Дробаха, О.Д. Трихліб // Восточно-Европейский журнал передовых технологий. – 2014. – 6/8 (72). – С. 25-28.
6. Распределение показателя Херста нестационарного маркированного ряда. / Д.С. Кирилов и др. // Препринты ИПМ им. М.В. Келдыша. – 2013. – №11. – 16 с.

РЕЗУЛЬТАТЫ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ ПОТРЕБЛЕНИЯ ТОПЛИВА МАНЕВРОВЫМ ТЕПЛОВОЗОМ В ЭКСПЛУАТАЦИИ

Ю.Е. Калабухин, О.В. Рудковский

Украинский государственный университет железнодорожного транспорта,
пл. Фейербаха, 7, Харьков, Украина; e-mail: Od.is@rambler.ru

Описывается алгоритм R/S анализа для временных рядов потребления топлива маневровым тепловозом при различных условиях выполняемой эксплуатационной работы. Определены основные положения метода оценок показателя Херста. На основе расчета и анализа показателя Херста сделан вывод об антиперсистентности временных рядов потребления топлива маневровым тепловозом в эксплуатации.

Ключевые слова: R/S анализ, показатель Херста, интервал, фрактал, временной ряд, маневровый тепловоз, эксплуатация, расход топлива

RESULTS ANALYSIS OF TIME SERIES FUEL CONSUMPTION OF USE SHUNTING LOKOMOTIVE

Y.E. Kalabukhin, O.V. Rudkovskiy

Ukrainian state university of railway transport,
Feuerbach area, 7, Kharkov, Ukraine; e-mail: Od.is@rambler.ru

An algorithm R/S analysis of time series of fuel consumption shunting locomotive carried out under different conditions of operational work. The main provisions of the method of the Hurst exponent estimates. Based on the calculation and analysis of the Hurst exponent concluded that fuel consumption antipersistent time series shunting locomotive in operation.

Keywords: R/S analysis, Hurst exponent, interval, fractal time series, shunting locomotive, maintenance, fuel consumption

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СТЕГАНОАНАЛІТИЧНИХ АЛГОРИТМІВ ВИЯВЛЕННЯ НАЯВНОСТІ ВКЛАДЕНЬ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ЦИФРОВИХ ВІДЕО

Г.В. Ахмаметьєва, А.О. Єфименко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: a.v.akhmametieva@opu.ua

В роботі проводиться порівняльний аналіз ефективності алгоритмів для виявлення вкладень конфіденційної інформації у цифрових відео, що реалізують розроблені раніше автором стеганоаналітичні методи, з сучасними аналогами. Запропоновані алгоритми засновані на аналізі просторової області цифрових контентів, що дозволило уникнути додаткового накопичення обчислювальної похибки і, як наслідок, підвищити ефективність стеганоаналізу цифрових відео в умовах малих значень пропускну здатності прихованого каналу зв'язку.

Ключові слова: стеганоаналіз, цифрові відео, аналіз ефективності

Вступ

Широке розповсюдження інформаційних технологій в усіх сферах суспільства сприяє накопиченню та зберіганню великих обсягів електронної інформації в різноманітних організаціях, підприємствах, державних установах, яка може містити конфіденційні відомості як окремих особистостей, так і державну та комерційну таємницю, які потребують захисту від розголошення та крадіжки, що може призвести до використання особистих даних шахраями, значних збитків для компаній тощо. Зокрема, крадіжка конфіденційних даних може здійснюватися за допомогою стеганографії, яка забезпечує передачу та зберігання секретної інформації у непомітному на перший погляд контейнері, в якості якого можуть виступати цифрові зображення, аудіо, відео. Використання певного виду контейнеру залежить від об'єму конфіденційних даних: дійсно, для передачі відносно невеликого повідомлення достатньо цифрового зображення, у випадку значного обсягу секретних даних перевага надається цифровим відео (ЦВ), адже стеганоповідомлення, яке є результатом вбудови додаткової інформації (ДІ) у контейнер, не повинно привертати увагу ні з точки зору непомітності для людського ока, ні з точки зору порушення статистичних характеристик самого контейнера, що часто забезпечується малими значеннями пропускну здатності прихованого каналу зв'язку (ППС).

Використання ЦВ в якості контейнера в стеганографії має ряд переваг у порівнянні з цифровими зображеннями, зокрема за рахунок великої кількості кадрів можна передати значний обсяг даних навіть за умови малої ППС, що значно ускладнює процес стеганоаналізу, основною задачею якого є виявлення факту наявності або констатація відсутності прихованих даних у контейнері. Однак, незважаючи на зазначені переваги, стеганоаналіз цифрових відео менш розвинений, ніж стеганоаналіз цифрових зображень, що пояснюється складністю задачі і неспроможністю існуючих

підходів до її рішення. Тому розвиток і підвищення ефективності стеганоаналізу відео є важливою і актуальною задачею.

Для сучасних розробок в області стеганоаналізу відеопослідовностей [1-3] властиві наступні недоліки:

- спостерігається невисока ефективність виявлення стеганоповідомлень, сформованих при малих значеннях ППС, що обумовлено аналізом області перетворень цифрових контентів, перехід до якої супроводжується додатковим накопиченням обчислювальної похибки;

- авторами сучасних розробок в області відеостеганоаналізу експерименти, як правило, проводяться на основі малої кількості тестових відео (до 26 ЦВ), що ускладнює об'єктивну оцінку реального стану стеганоаналізу відео послідовностей;

- сучасні стеганоаналітичні розробки майже не розглядають питання покадрового аналізу ЦВ у випадку, коли вбудова ДІ здійснюється лише у частину кадрів відеопослідовності.

В роботах [4-7] були запропоновані ефективні стеганоаналітичні методи виявлення факту наявності/відсутності додаткової інформації у цифрових контенті: ЦВ [4-6] та цифрових зображеннях [7], які аналізують просторову область цифрових контентів, що дозволило уникнути додаткового накопичення обчислювальної похибки, завдяки чому були отримані високі результати виявлення стеганоповідомлень.

Метою роботи є проведення порівняльного аналізу ефективності стеганоаналітичних алгоритмів для цифрових відео, що реалізують розроблені раніше [4-7] стеганоаналітичні методи, з сучасними аналогами.

Основна частина

В основі стеганоаналітичних методів [4-6] лежить аналіз кількості блоків з однаковими значеннями яскравості в матрицях кольорних складових цифрових контентів. Було встановлено, що $n \times n$ -блоки виду

$$A = \begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \ddots & \dots \\ a & a & \dots & a \end{pmatrix}, \quad a \in \{1, 2, 3, \dots, 255\}, \quad (1)$$

мають єдине ненульове сингулярне число $\sigma_1 > 0, \sigma_2 = \dots = \sigma_n = 0$, причому таке, що належить множині натуральних чисел ($\sigma_1 \in \mathbb{N}$) і кратне розміру блока n ($\sigma_1 : n$). Така особливість є чутливою до малих збурень, адже в загальному випадку сингулярні числа для довільної матриці є невід'ємними дійсними числами [8]. Зміна лише одного елементу матриці (1), яка може виникнути в результаті стеганоперетворення, призведе до того, що $\sigma_1 \notin \mathbb{N}$. На основі встановленої особливості збурення єдиного ненульового сингулярного числа σ_1 $n \times n$ -блоків виду (1) визначено відповідність між областю сингулярного розкладання відповідних матриць та просторовою областю цифрових контентів, що не тільки дозволило уникнути додаткового накопичення обчислювальної похибки, а й додаткових обчислювальних витрат, пов'язаних з переходом в область перетворень і назад, при розробці стеганоаналітичних алгоритмів.

Стеганоаналітичний метод [4] та його удосконалення [5] засновані на аналізі відносної (по відношенню до загальної кількості $n \times n$ -блоків у матриці кольорної складової кадру ЦВ) кількості блоків з однаковими значеннями яскравості в матрицях цифрових контентів в результаті первинного і повторного стеганоперетворення, що

обумовлено гіпотезою, що кількість $n \times n$ -блоків виду (1) у стеганоповідомленні буде незначною (можливо такі блоки будуть відсутні), що призведе до малих значень відносної кількості таких блоків після повторної вбудови ДІ у порівнянні з первинною вбудовою ДІ. Основні кроки алгоритму САА1, що реалізує запропонований метод, співпадають з наведеними в [4-5] при порогових значеннях $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$ для ЦВ в форматі з втратами, $T_R = 1.6$, $T_G = 1.7$, $T_B = 1.6$ для ЦВ в форматі без втрат.

Метод, розроблений в [6], заснований на врахуванні характеру зміни кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення. Встановлено, що в результаті первинної вбудови ДІ у більшості матриць кольорних складових кадрів ЦВ (не залежно від формату оригінального контейнеру) спостерігається зменшення кількості блоків з однаковими значеннями яскравості (аж до 0, особливо, якщо ППС при первинній вбудові ДІ складала 0.25-0.5 біт/піксель), а в результаті повторної вбудови ДІ у стеганоповідомлення – або незначне збільшення таких блоків, або їх незмінність. Основні кроки алгоритму САА2, що реалізує розроблений метод, співпадають з наведеними в [6] при пороговому значенні $T = 3$. Даний алгоритм, на відміну від САА1, дозволив ефективно виявляти стеганоповідомлення, сформовані вбудовою ДІ у ЦВ з малим розміром кадрів при значеннях ППС, не менше 0.167 біт/піксель.

В роботі [7] запропонований стеганоаналітичний алгоритм (далі САА3) виявлення стеганоповідомлень, сформованих вбудовою ДІ лише в одну будь-яку кольірну складову цифрових зображень в форматі з втратами, заснований на врахуванні кількості послідовних тріад кольорних триплетів в матриці унікальних кольорів UCT розміром $U \times 3$, яка містить унікальні кольірні триплети (r_i, g_i, b_i) , $i = \overline{1, U}$, що містяться в зображенні. Розроблений алгоритм був адаптований для ЦВ (САА3v), для аналізу окремих кадрів відео послідовності слід використовувати алгоритм САА3, основні кроки якого наведені в [7].

Для оцінки ефективності розроблених алгоритмів були проведені обчислювальні експерименти для 200 відеопослідовностей розміром кадру 320×240 , отриманих камерами мобільних пристроїв, з розширенням *.3gp або *.mp4 (при стиску використовуються кодеки H.263 або H.264) – набір 1, та 167 відео послідовностей розміром кадру 320×240 , отриманих відеокамерою з розширенням *.avi (при стиску використовується кодек Xvid) – набір 2. По результатам експериментів, направлених на апробацію розроблених алгоритмів, були визначені помилки першого та другого роду, наведені в табл. 1.

З табл. 1 видно, що найкращі результати детектування наявності ДІ досягаються методом САА3v, однак, як було зазначено вище, даний алгоритм може використовуватися лише у випадку, коли ДІ вбудовується лише в одну кольірну складову кольорових контейнерів. На відміну від САА3v, алгоритми САА1 та САА2 можуть використовуватися як для кольорових ЦВ, так і ЦВ в градаціях сірого, крім того вони спроможні виявляти наявність ДІ, вбудованої у дві або три кольірні складові, оскільки аналіз кольорних матриць відбувається окремо для кожної кольірної складової.

Порівняльний аналіз ефективності розроблених алгоритмів САА1, САА2, САА3v та САА3 для виявлення вкладень ДІ в окремих кадрах ЦВ з сучасними аналогами здійснюється шляхом оцінки точності детектування AD , що характеризує долю правильно виявлених подій [9-11]:

$$AD = \frac{TP + TN}{TP + FN + TN + FP}, \quad (2)$$

де FN – помилки першого роду; FP – помилки другого роду; TP – відсоток правильно виявлених стеганоповідомлень, $TP=100-FN$; TN – відсоток правильно виявлених незаповнених контейнерів, $TN=100-FP$.

Таблиця 1.

Ефективність детектування вкладень ДІ у ЦВ алгоритмами САА1, САА2, САА3v, %

Алгоритм	Помилки	ППС, біт/піксель					
		0.5	0.25	0.167	0.125	0.1	0.05
ЦВ з набору 1							
CAA1	1-го роду	0	0	2.19	11.68	51.09	90.88
	2-го роду	0.36	0.36	0.36	0.36	0.73	6.14
CAA2	1-го роду	0	0	0	64.23	97.08	100
	2-го роду	0	0	0	0	0	0
CAA3v	1-го роду	0	0	0	0.73	2.19	32.12
	2-го роду	0	0	0	0	0	0
ЦВ з набору 2							
CAA1	1-го роду	0	0	19.56	98.26	100	100
	2-го роду	0	0	0	0	0	0
CAA2	1-го роду	0	0	0	80	100	100
	2-го роду	0	0	0	0	0	0
CAA3v	1-го роду	0	0	0	0	0	10
	2-го роду	0	0	0	0	0	0

Для порівняльного аналізу ефективності розроблених стеганоаналітичних алгоритмів, направлених на виявлення наявності/відсутності ДІ в ЦВ, використовуються ефективні сучасні аналоги:

- $V1$ (2005) [12] (10 відео по 124 кадри);
- $V2$ (2005) [13] (10 відео по 124 кадри);
- $V3$ (2007) [1] (10 відео по 124 кадри);
- $V4$ (2013) [2] (9 відео по 150-300 кадрів);
- $V5$ (2015) [3] (26 відео по 100 кадрів).

У дужках представлена інформація про обсяг обчислювальних експериментів, що використовувались авторами відповідних алгоритмів при оцінці їх ефективності. Результати порівняння точності детектування AD розроблених стеганоаналітичних алгоритмів для 367 ЦВ з наборів 1-2 з обраними аналогами наведені в табл. 2, при цьому ДІ вбудовувалась в одну постійну кольірну складову всіх кадрів ЦВ.

В результаті порівняння значень точності детектування AD (табл. 2) можна зробити висновок, що розроблені стеганоаналітичні алгоритми є ефективнішими, ніж сучасні аналоги. Якщо вбудова ДІ здійснювалась з ППС 0.167-0.5 біт/піксель, алгоритмами САА3v і САА2 досягнутий абсолютний результат для точності детектування $AD=1$. У випадку малих значень ППС найбільш ефективним є алгоритм САА3v: результати детектування за допомогою САА3v на 2.3% перевищують аналог $V5$ і більше ніж на 10% аналоги $V1-V3$ (для ППС 0.1 біт/піксель). Найбільше підвищення ефективності досягається при виявленні вкладень ДІ, вбудованої зі значеннями ППС, меншими за 0.1 біт/піксель: точність детектування САА3v на 14.93% перевищує аналог $V4$ при значенні ППС 0.0625 біт/піксель; у випадку ППС 0.05 біт/піксель сучасні аналоги навіть не тестувалися, для алгоритму САА3v точність детектування складає $AD=0.9391$. Точність детектування алгоритмів САА1 і САА2 при ППС 0.125 біт/піксель і менше нижче аналогів, оскільки порівняльний аналіз враховує результати аналізу ЦВ з наборів 1 і 2, однак у випадку використання САА1 для стеганоаналізу ЦВ, отриманих камерами мобільних пристроїв (набір 1), точність

детектування при ППС 0.125 біт/піксель досягає $AD = 0.94$, що на 1.2% перевищує аналог $V4$.

Таблиця 2.

Порівняння AD для розроблених стеганоаналітичних методів і сучасних аналогів

ППС, біт/піксель	$V1$ 2005 (10)	$V2$ 2005 (10)	$V3$ 2007 (10)	$V4$ 2013 (9)	$V5$ 2015 (26)	CAA1 (367)	CAA2 (367)	CAA3v (367)
0.5	0.925	0.955	0.98	1	0.9991	0.9991	1	1
0.4	0.885	0.94	0.97	–	–	0.9991	1	1
0.3	0.825	0.92	0.945	–	–	0.9991	1	1
0.25	–	–	–	0.996	0.9988	0.9991	1	1
0.2	0.68	0.875	0.925	–	–	0.9691	1	1
0.167	–	–	–	–	–	0.9537	1	1
0.125	–	–	–	0.928	–	0.7757	0.7530	0.9991
0.1	0.555	0.755	0.89	–	0.9744	0.7139	0.6703	0.9973
0.0625	–	–	–	0.794	–	0.5157	0.5	0.9433
0.05	–	–	–	–	–	0.5074	0.5	0.9391

Для випадку, коли вбудова ДІ здійснюється лише в деякі окремі кадри ЦВ (часткова вбудова), проводиться покадровий аналіз ЦВ за допомогою алгоритму САА3. Результати порівняння ефективності алгоритму САА3 з єдиним сучасним аналогом $V5$, для якого наводяться результати покадрового аналізу ЦВ, в умовах часткової вбудови ДІ наведені в табл. 3.

Таблиця 3.

Порівняння AD для стеганоаналітичного алгоритму САА3 і сучасного аналогу $V5$ за умови часткового заповнення кадрів ЦВ

ППС окремих кадрів ЦВ, біт/піксель	Кількість заповнених кадрів							
	80%		60%		40%		20%	
	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)	$V5$ 2015 (26)	CAA3 (367)
0.5	1	1	0.9978	1	1	1	0.9932	1
0.25	1	1	1	1	0.9926	1	0.9843	0.9999
0.167	–	0.9998	–	0.9998	–	0.9998	–	0.9999
0.125	–	0.9959	–	0.9948	–	0.9948	–	0.9991
0.1	0.9381	0.9897	0.9276	0.9867	0.7974	0.9867	0.6688	0.9974
0.05	–	0.9232	–	0.9048	–	0.9048	–	0.9811

З табл. 3 видно, що у випадку часткової вбудови ДІ розроблений алгоритм САА3 (стосовно до кадрів ЦВ) значно ефективніше сучасного аналогу $V5$ при вбудові ДІ з малою ППС: при ППС 0.1 біт/піксель при степені заповнення кадрів 60-80% результати САА3 на 5.5% перевищують аналог $V5$, при степені заповнення кадрів 40% і 20% відповідно на 18% і 32%. В умовах ППС 0.05 біт/піксель сучасний аналог не тестувався, однак для алгоритму САА3 при будь-якій степені заповнення кадрів точність детектування перевищує 0.9, що є досить високим результатом.

Висновки

В роботі проведено порівняльний аналіз алгоритмів, що реалізують розроблені раніше стеганоаналітичні методи, з сучасними аналогами. Показано, що розроблені алгоритми є ефективнішими за сучасні аналоги, особливо при значеннях ППС 0.167 біт/піксель та вище. Для менших значень ППС найбільш ефективним є алгоритм САА3 та його адаптація САА3v, які дозволяють ефективно виявляти вкладення ДІ навіть при ППС 0.05-0.1 біт/піксель. Проведено покадровий аналіз ЦВ, в результаті якого також отримані високі результати детектування стеганоповідомлень.

Отримані результати підтверджуються масштабними обчислювальними експериментами, які дозволили отримати об'єктивно високу оцінку для розроблених стеганоаналітичних методів.

Результати отриманих оцінок ефективності алгоритмів, що реалізують розроблені методи, та аналіз області застосування розроблених методів на основі отриманих помилок першого та другого роду дозволяють розробити комплексний метод виявлення вкладень ДІ у ЦВ, такий, що аналізує просторову область цифрових контентів та спроможний ефективно виявляти стеганоповідомлення, сформовані за різних умов вбудови ДІ.

Список літератури

1. Vinod Pankajaksan. Improving video steganalysis using temporal correlation / Vinod Pankajaksan, A.T.S. Ho // Third international conference on intelligent information hiding and multimedia signal processing, 2007. – Vol. 1. – Pp. 287-290.
2. Songbin Li. Detection of Information Hiding by Modulating Intra Prediction Modes in H.264/AVC / Songbin Li, Peng Liu, Qiongxing Dai, Xiuhua Ma, Haojiang Deng // Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013). – Pp. 590-593.
3. Kaicheng Wu. Research of Video Steganalysis Algorithm Based on H265 Protocol / Kaicheng Wu // MATEC Web of Conferences 25, 2015. – Pp. 03003-1 - 03003-7.
4. Кобозева, А.А. Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь / А.А. Кобозева, А.В. Ахметьева, А.А. Ефименко // Інформаційна безпека. – 2014. – №1(13). – С. 31-42.
5. Ахметьева, А.В. Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров / А.В. Ахметьева // Інформатика та математичні методи в моделюванні. – 2015. – Т.5. – № 4. – С. 367-375.
6. Маєвський, Д.А. Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів / Д.А. Маєвський, Г.В. Ахметьева // Інформатика та математичні методи в моделюванні. – 2016. – Т.6. – №1. – С. 52-60.
7. Ахметьева, А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями / А.В. Ахметьева // Захист інформації. – 2016. – Випуск 23. – С.135-145.
8. Деммель, Дж. Вычислительная линейная алгебра. Теория и приложения. / Дж. Деммель. – Пер. с англ. – М.: Мир, 2001. – 430 с.
9. Fawcett, T. An introduction to ROC analysis / Tom Fawcett // Pattern Recognition Letters. – 2006. – No. 27. – Pp. 861–874.
10. Bin Li. A Survey on Image Steganography and Steganalysis / Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi // Journal of Information Hiding and Multimedia Signal Processing. – 2011. – Vol. 2. – No. 2. – Pp. 142-172.
11. Receiver operating characteristic [Electronic resource] // From Wikipedia, the free encyclopedia. On-line: https://en.wikipedia.org/wiki/Receiver_operating_characteristic
12. Xuan, G. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions / G. Xuan // Lecture Notes in Computer Science – 2005. – Vol. 3727. – Pp. 262–277.
13. Shi, Y.Q. Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network / Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, C. Chen // Proceedings of the IEEE International Conference on Multimedia and Expo, July 2005. – 4 p.

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ СТЕГАНОАНАЛИТИЧЕСКИХ
АЛГОРИТМОВ ВЫЯВЛЕНИЯ НАЛИЧИЯ ВЛОЖЕНИЙ КОНФИДЕНЦИАЛЬНОЙ
ИНФОРМАЦИИ В ЦИФРОВЫХ ВИДЕО**

А.В. Ахматетьева, А.А. Ефименко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: a.v.akhmametieva@opu.ua

В работе проводится сравнительный анализ эффективности алгоритмов для выявления вложений конфиденциальной информации в цифровых видео, реализующих разработанные ранее автором стеганоаналитические методы, с современными аналогами. Предложенные алгоритмы основаны на анализе пространственной области цифровых контентов, что позволило избежать дополнительного накопления вычислительной погрешности и, как следствие, повысить эффективность стеганоанализа цифровых видео в условиях малых значений пропускной способности скрытого канала связи.

Ключевые слова: стеганоанализ, цифровые видео, анализ эффективности

**COMPARATIVE EFFICIENCY ANALYSIS OF STEGANALYTIC ALGORITHMS FOR DETECTING
THE PRESENCE OF ATTACHMENTS OF CONFIDENTIAL INFORMATION IN DIGITAL VIDEO**

A.V. Akhmametieva, A.A. Efimenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: a.v.akhmametieva@opu.ua

The paper presents a comparative efficiency analysis of algorithms for detecting the presence of attachments of confidential information in digital video, that implement the author's previously developed steganalytic methods, with modern analogs. Proposed algorithms are based on the analysis of the spatial domain of digital contents, that allowed to avoid additional accumulation of computational error and, as a result, to increase the efficiency of steganalysis of digital video in conditions of low hidden capacity.

Keywords: steganalysis, digital video, efficiency analysis

НЕЧІТКА МОДЕЛЬ ФОРМУВАННЯ ІНДИВІДУАЛЬНОЇ ТРАЄКТОРІЇ НАВЧАННЯ ТА ПОБУДОВА ОНТОЛОГІЇ НА ЇЇ ОСНОВІ

Т.В. Лендюк, Н.М. Васильків

Тернопільський національний економічний університет,
вул. Львівська, 11, м.Тернопіль, 46020, Україна; e-mail: tl@tneu.edu.ua

У статті запропоновано реалізацію моделі формування навчального матеріалу на основі рівня знань студентів і складності завдань (побудови індивідуальної траєкторії навчання), яка базується на апараті нечіткої логіки. Побудовано базу правил нечіткої моделі та перевірено її на правильність роботи. Сформовані нечіткі правила використано в онтології навчальної дисципліни.

Ключові слова: індивідуальна траєкторія навчання, навчальний фрагмент, нечітка логіка, нечітка онтологія

Вступ

Однією з переваг застосування інформаційних технологій у навчальному процесі є можливість використання адаптивного навчання. Система дистанційного навчання з можливістю адаптації готує для студента навчальний матеріал з врахуванням його індивідуальних особливостей і формує індивідуальну траєкторію навчання з використанням навчальних фрагментів заданого рівня складності та додаткового навчального матеріалу відповідно до результатів проміжного тестування.

Існує ряд підходів щодо індивідуальної траєкторії навчання. Наприклад, П. Брусіловський вважає, що послідовність курсу спрямована на допомогу студенту знайти оптимальний шлях «в навчальному матеріалі» [1]. Карла Лімонгеллі вважає, що генерування курсу для студента може розглядатися як індивідуальна траєкторія навчання (набір дій), які студент має вивчити (виконати) для досягнення цільового рівня знань [2]. Грецькі вчені Карампіперіс та Сампсон розглядають визначення послідовності навчальних ресурсів як навчальний шлях [3].

Актуальною в даний час є така побудова індивідуальної навчальної траєкторії, при якій студент забезпечується теоретичним матеріалом, вправами для вивчення теорії, інструктивними матеріалами для виконання вправ відповідно до його моделі, тобто студент забезпечується навчальним матеріалом відповідно до його індивідуальних особливостей [4, 5].

В рамках навчальних процесів специфікувати основні компоненти навчальних дисциплін – лекції, практичні, лабораторні роботи, навчальні матеріали дає змогу застосування онтологій, які забезпечують можливість організації ефективного розподіленого доступу до навчальних ресурсів шляхом створення єдиної бази знань, яка поєднує в собі навчальні дисципліни і може бути розподіленою в мережі Інтернет, що зробить її незалежною від інтерпретації конкретного навчального процесу. Внаслідок цього роль навчальної системи зводиться до ролі інтелектуального агента, що проводить вибірку з бази знань або її зміну залежно від контексту навчання. Також можливо проводити тестування, генеруючи контрольні завдання відповідно до семантики описаних онтологій конкретних навчальних курсів [6].

В даний час онтології використовуються разом з нечіткими множинами для усунення невизначеної інформації в різних областях, наприклад, для пошуку в документах або для підбору навчальних фрагментів для вивчення.

Одне з можливих рішень для обробки невизначених даних полягає в тому, щоб забезпечити включення нечіткої логіки в онтологію [7-8]. Зараз активно ведуться дослідження, і навіть є деякі напрацювання застосування теорії нечіткої логіки в онтологіях [9-11].

Метою даної роботи є побудова моделі формування індивідуальної траєкторії навчання з використанням нечіткої логіки та створення на її основі онтології навчальної дисципліни.

Основна частина

Введення нечітких характеристик щодо оцінки навчального матеріалу може допомогти в підготовці завдань і розробці тестів. Наприклад, викладач може достатньо швидко визначити, є завдання складним чи ні. Але сказати точно, наскільки воно є складним за 100-бальною шкалою або оцінити різницю складності двох завдань, буде досить важко [12, 13].

З точки зору студента, нечітка оцінка знань у вигляді «відмінно», «дуже добре», «добре», «задовільно» і «незадовільно» є зрозумілішою, ніж кількість балів, яка набрана в результаті тестування [14].

При адаптивному навчанні складність завдання, яке є складовою індивідуальної траєкторії навчання, може бути визначена у вигляді певної кількості балів або відсотків, або ж з використанням нечіткої логіки, за рішенням експерта [15]. Нечіткі моделі є достатньо прозорими та зрозумілими і тому не поступаються іншим методам, особливо там, де змістовна інтерпретація важливіша за точність моделювання [4, 16].

В нечітких множинах для побудови математичних моделей формалізують лінгвістичну інформацію за допомогою поняття лінгвістичної змінної, значеннями якої є слова або вирази. Лінгвістичні значення називаються термами, а набір усіх можливих термів формує терм-множину [13, 17].

Функцією належності в нашому випадку буде функція $\mu^A(u): U \rightarrow [0;1]$, що дає змогу для кожного елемента u універсальної множини U розрахувати ступінь його належності до нечіткої множини $\tilde{A}$. Універсальна множина U містить повну множину значень, що охоплює всю проблемну область [18]. В якості функції належності для термів вхідних змінних використано трапецієвидну функцію (рис. 1) [4].

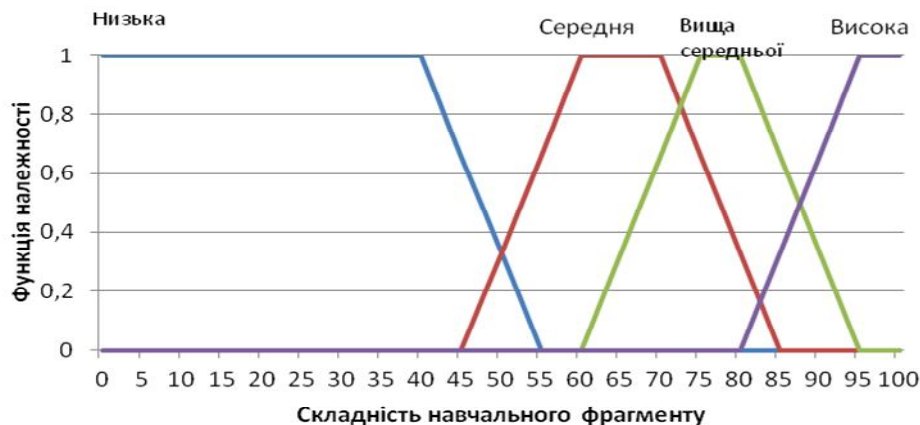


Рис. 1. Функція належності для термів вхідних змінних

Для проведення розрахунків використано формулу, що відповідає трапецієподібній функції належності. У результаті одержано систему рівнянь для розрахунку значень функції належності кожного з термів вхідних змінних [5]:

$$\mu_{ns}(a) = \begin{cases} 1, & a \leq 40 \\ \frac{55-a}{40}, & 40 \leq a \leq 55 \\ 0, & a \geq 55 \end{cases}, \quad \mu_s(a) = \begin{cases} 0, & a \leq 65 \text{ або } a \geq 95 \\ \frac{a-75}{60}, & 60 \leq a \leq 75 \\ 1, & 70 \leq a \leq 80 \\ \frac{95-a}{80}, & 80 \leq a \leq 95 \end{cases}, \quad (1)$$

$$\mu_{vs}(a) = \begin{cases} 0, & a \leq 45 \text{ або } a \geq 85 \\ \frac{a-60}{45}, & 45 \leq a \leq 60 \\ 1, & 60 \leq a \leq 70 \\ \frac{85-a}{70}, & 70 \leq a \leq 85 \end{cases}, \quad \mu_v(a) = \begin{cases} 0, & a \leq 80 \\ \frac{a-95}{80}, & 80 \leq a \leq 95 \\ 1, & 90 \leq a \leq 100 \end{cases}$$

де $\mu_{ns}(a)$ – функція належності для складності нижчої від середньої, $\mu_s(a)$ – функція належності для середньої складності, $\mu_{vs}(a)$ – функція належності для складності вищої від середньої, $\mu_v(a)$ – функція належності для високої складності.

База нечітких знань моделі нечіткого формування індивідуальної траєкторії навчання містить два входи: «Рівень знань студента» та «Складність навчального фрагмента» і один вихід – «Час вивчення навчального фрагмента». В загальному, нечітка модель підбору завдань для індивідуальної траєкторії навчання має вигляд, поданий на рис. 2.



Рис. 2. Загальна схема нечіткої моделі побудови індивідуальної траєкторії навчання

Лінгвістична змінна «Рівень знань студента» містить терми {Низький; Нижчий від середнього; Середній; Вищий від середнього; Високий}. Лінгвістична змінна «Складність навчального фрагмента» містить терми {Нижча від середньої; Середня; Вища від середньої; Висока}. Лінгвістична змінна «Час вивчення навчального фрагмента» містить терми {Малий; Середній; Тривалий}.

Мета теорії нечітких множин полягає в тому, щоб описати невизначене поняття через узагальнене поняття множини, відповідно до якого об'єкт може належати до певної міри множині (як правило, дійсне число з інтервалу $[0,1]$). Наприклад, семантичний зміст твердження, що «Студент із високим рівнем знань може вивчити навчальний фрагмент із складністю нижчою за середню за малий час», може матиступінь або значення істинності 0.6.

Для побудови нечіткої моделі та з метою пришвидшення її роботи потрібно описати рівень знань студентів (табл. 1) та складність навчального фрагмента, що буде

використовуватись (табл. 2). Саме такий розподіл використовується для задання вхідних змінних, тобто для побудови їх функцій належності.

Таблиця 1.

Шкала оцінювання рівня знань студента

Рівень знань студента в логітах Раша	Позначення
Високий, 4.1 – 5.0	В
Вище від середнього, 3.1 ... 4.0	ВС
Середній, 2.1 ... 3.0	С
Нижче від середнього, 1.1 ... 2.0	НС
Низький, -5.0 ... 1.0	Н

Таблиця 2.

Складність навчального фрагмента

Складність навчального фрагмента в логітах Раша	Позначення
Висока, 4.1 – 5.0	В
Вища від середньої, 3.1 ... 4.0	ВС
Середня, 2.1 ... 3.0	С
Нижча від середньої, 1.1 ... 2.0	НС
Низька, 0.1 ... 1.0	Н

Виходом розробленої нечіткої моделі формування індивідуальної траєкторії навчання є час вивчення навчального фрагмента, який позначається відповідно до змінних, поданих у табл. 3.

Таблиця 3.

Час вивчення навчального фрагмента

Опис	Позначення
Малий час вивчення, 0 ... 3 хв.	М
Середній час вивчення, 3 ... 6 хв.	С
Тривалий час вивчення, 7 ... 15 хв.	Т

Для моделювання бази нечітких знань використано Fuzzy Logic Toolbox – пакет прикладних програм, що входить в склад середовища MatLab. На основі даного пакету створено модель нечіткого логічного висновку і нечіткої класифікації.

При розробці нечіткої моделі необхідно врахувати значення вхідних та вихідних змінних, а також правильно побудувати базу правил, за якою здійснюватиметься нечіткий висновок.

Входи і виходи, а також функції належності нечіткої системи побудови індивідуальної траєкторії навчання наведено на рис. 3-5.

Робота запропонованої нечіткої моделі побудови індивідуальної траєкторії навчання залежить від бази правил. Оскільки кожна вхідна змінна задана різною кількістю функцій належності і враховуючи неможливість ситуації, коли вхідна змінна не задана, база правил складається з $R = 6 \cdot 6 - 1 = 35$ правил типу «якщо – то» і будується відповідно до даних табл. 4.

У процесі роботи системи сформовано набір правил визначення часу вивчення навчального матеріалу (рис. 6).

Поверхня (рис. 7) відображає залежність часу вивчення навчального матеріалу від рівня знань студента і складності навчального матеріалу.

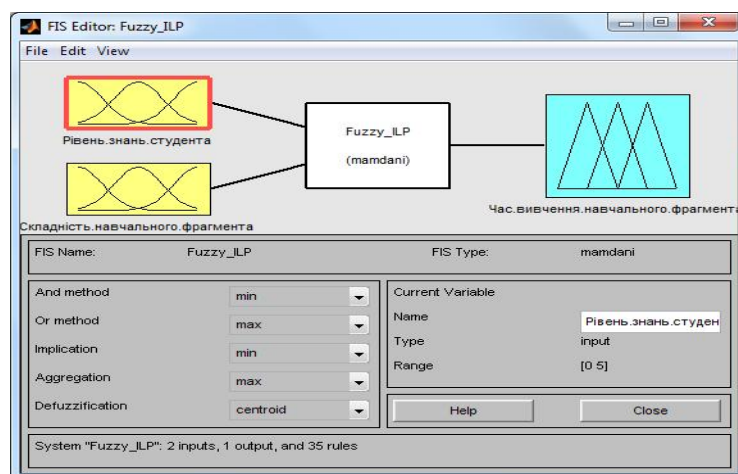


Рис. 3. Входи і виходи нечіткої системи

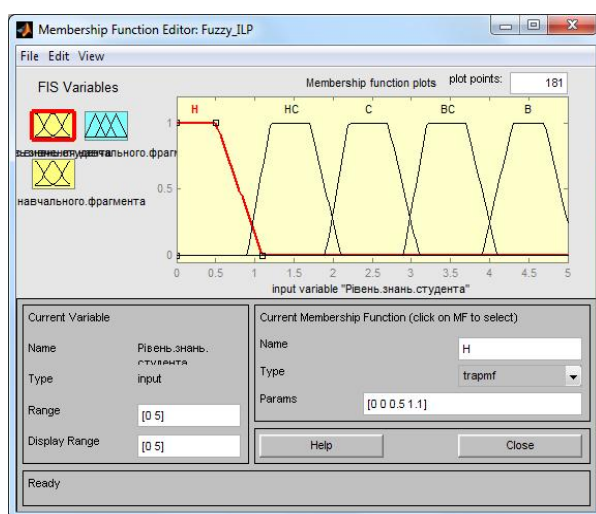


Рис. 4. Функції належності вхідної змінної «Рівень знань студента»

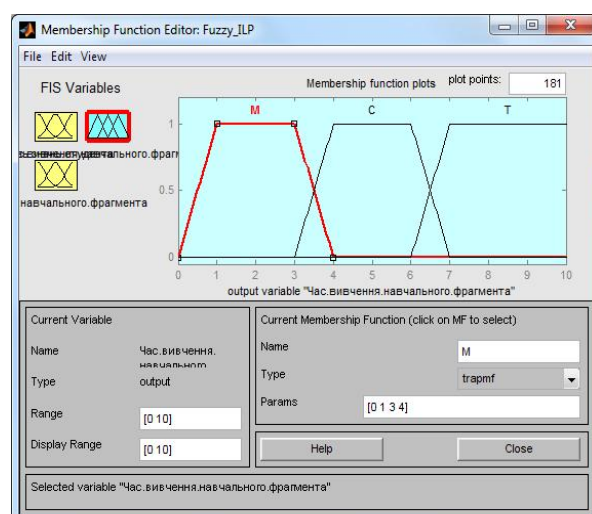


Рис. 5. Функції належності вихідної змінної «Час вивчення навчального фрагмента»

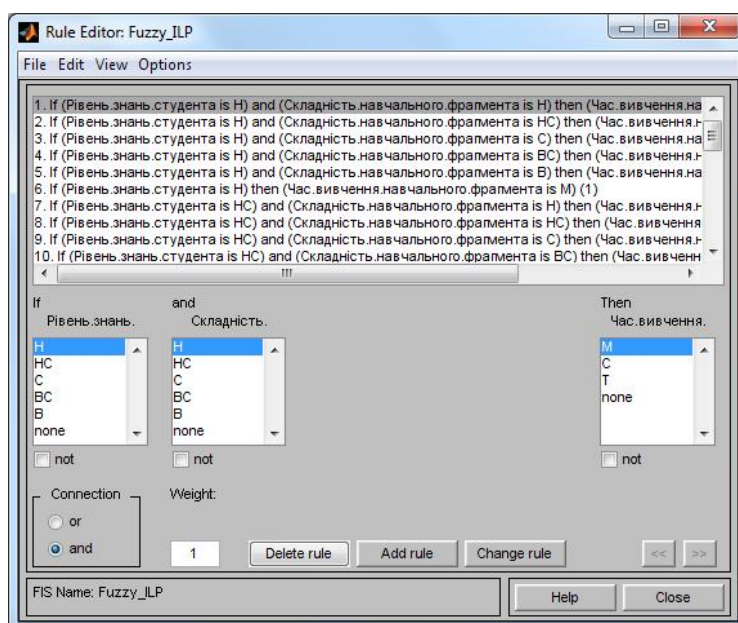


Рис. 6. Набір нечітких правил визначення часу вивчення навчального фрагмента

Таблиця 4.

Відповідність вхідних та вихідної змінних

№ пра-вила	Рівень знань студента	Складність навчального фрагмента	Час вивчення навчального фрагмента	№ пра-вила	Рівень знань студента	Складність навчального фрагмента	Час вивчення навчального фрагмента
1	Н	Н	М	19	ВС	Н	М
2	Н	НС	С	20	ВС	НС	М
3	Н	С	С	21	ВС	С	М
4	Н	ВС	Т	22	ВС	ВС	С
5	Н	В	Т	23	ВС	В	С
6	Н	Не задано	М	24	ВС	Не задано	М
7	НС	Н	М	25	В	Н	М
8	НС	НС	С	26	В	НС	М
9	НС	С	С	27	В	С	М
10	НС	ВС	Т	28	В	ВС	С
11	НС	В	Т	29	В	В	С
12	НС	Не задано	М	30	В	Не задано	С
13	С	Н	М	31	Не задано	Н	М
14	С	НС	М	32	Не задано	НС	М
15	С	С	С	33	Не задано	С	С
16	С	ВС	Т	34	Не задано	ВС	С
17	С	В	Т	35	Не задано	В	Т
18	С	Не задано	С				

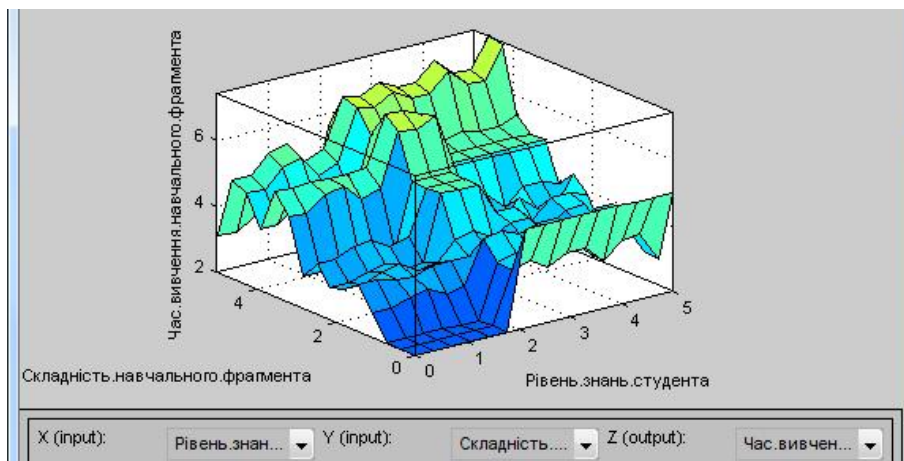


Рис. 7. Залежність часу вивчення навчального матеріалу від рівня знань студента і складності навчального матеріалу

У табл. 5 наведено залежність вихідної змінної від вхідних.

Як видно з рис. 7 та табл. 5, час вивчення навчального матеріалу залежить як від рівня знань студента, так і від складності навчального матеріалу.

Нечітку базу знань, розроблену в середовищі MatLab, можна використати у редакторі онтологій Protégé. Для цього використовується плагін Fuzzy OWL. Розглянемо алгоритм задання нечіткого відношення відповідно до методики FuzzyOWL:

1. Створюється нова властивість-анотація fuzzyLabel, в якій будуть задаватися параметри нечіткості кожного елемента онтології.

2. Лінгвістичні змінні визначаються в формі нових створених типів даних (Datatype).

3. Для кожного створеного типу даних задаються верхня і нижня межа прийнятих значень, вибирається тип функції приналежності і для неї задаються параметри відповідності.

Таблиця 5.

Відповідність вхідних та вихідної змінних

Рівень знань студента	Складність навчального матеріалу	Час вивчення навчального матеріалу, хв
-4.096	4.337	8.26
-4.179	1.592	4.5
4.458	3.735	7.5
0.251	5.1	8.09
-2.189	1.99	6.25
5	1.566	1.41
2.786	1.99	3.4
2.786	3.582	8.24
3.976	5	6.39
2.388	1.94	2.49
4.08	2.687	1.38
2.786	2.388	4.5
-1.928	2.771	8.22

Методологія FuzzyOWL передбачає аналітичне визначення декількох можливих типів функцій належності:

- трикутні (triangular);
- трапецієвидні (trapezoidal);
- лінійні (linear);
- кусково-лінійні: лівобічні і правобічні (left-shoulder and right-shoulder).

Приклад визначення лінгвістичної змінної «навчальний фрагмент рівня складності вищої за середню» і відповідної функції належності:

```

<AnnotationAssertion>
  <AnnotationProperty IRI="#fuzzyLabel"/>
  <IRI>#СкладністьВищаСередньої</IRI>
  <Literal
    datatypeIRI="&rdf;PlainLiteral">&lt;fuzzyOwl2
fuzzyType="&quot;datatype&quot;&gt;
&lt;Datatype type="&quot;trapezoidal&quot; a=2.5; b=3; c=4; d=4.5; /&gt;
&lt;/fuzzyOwl2&gt;</Literal>
</AnnotationAssertion>

```

Розглянемо реалізацію нечіткої онтології побудови індивідуальної траєкторії навчання для дисципліни «Теорія прийняття рішень».

Онтологія навчальної дисципліни містить класи: лекцій, практичних та лабораторних занять. Лекції містять навчальні фрагменти, які є їх складовими частинами. Використовуючи дану онтологію і беручи до уваги метадані навчальних фрагментів здійснюється підбір навчальних фрагментів для побудови індивідуальної траєкторії навчання.

Зазвичай онтологія навчального фрагменту включає наступні метадані: автор, тема, опис, дата, тип, формат, ідентифікатор, джерело, мова, зв'язки, охоплення, права.

Клас «тип» навчального матеріалу містить дані про його тип (базовий теоретичний матеріал, додатковий теоретичний матеріал, роз'яснюючий матеріал, задачі на виконання). Дуже важливим класом для побудови індивідуальної траєкторії навчання є клас складності, за допомогою якого і формується набір навчального матеріалу. Суттєве значення має час вивчення навчального фрагмента при відомій складності і рівні знань, тобто коли складність навчального фрагмента вища від рівня знань – час вивчення зростає, в протилежному випадку – зменшується.

На рис. 8 наведено приклад індивіда онтології індивідуальної траєкторії навчання, а на рис. 9 подано нечітку онтологію в складі онтології індивідуальної траєкторії навчання.

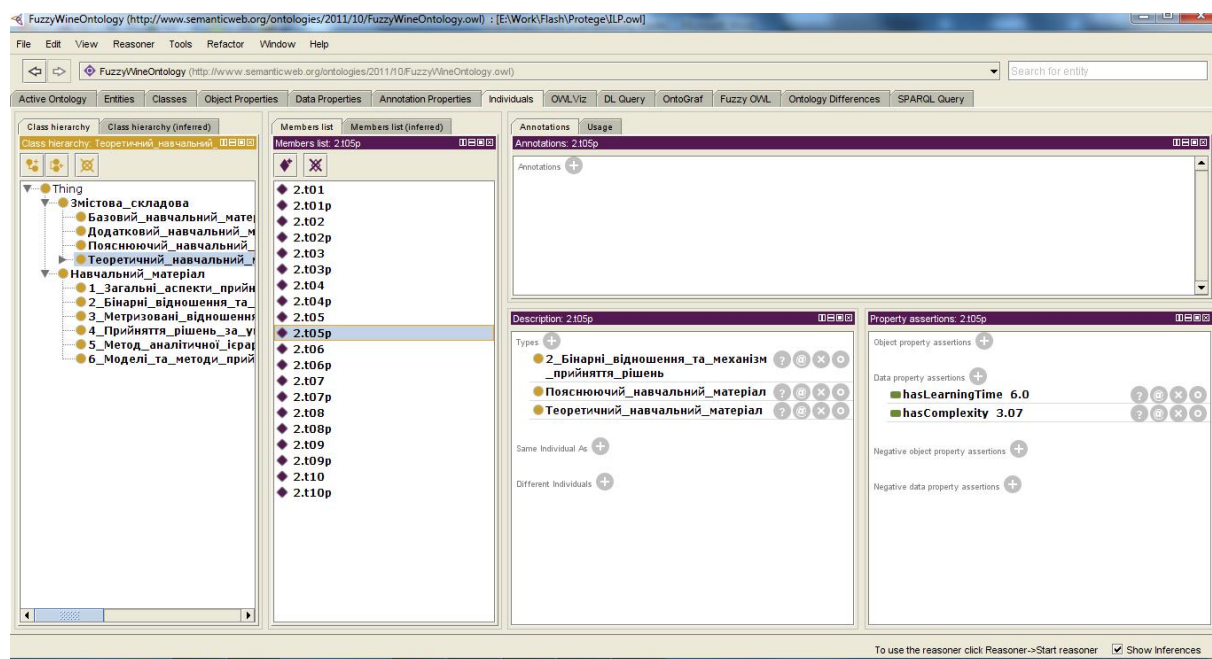


Рис. 8. Індивіди онтології індивідуальної траєкторії навчання

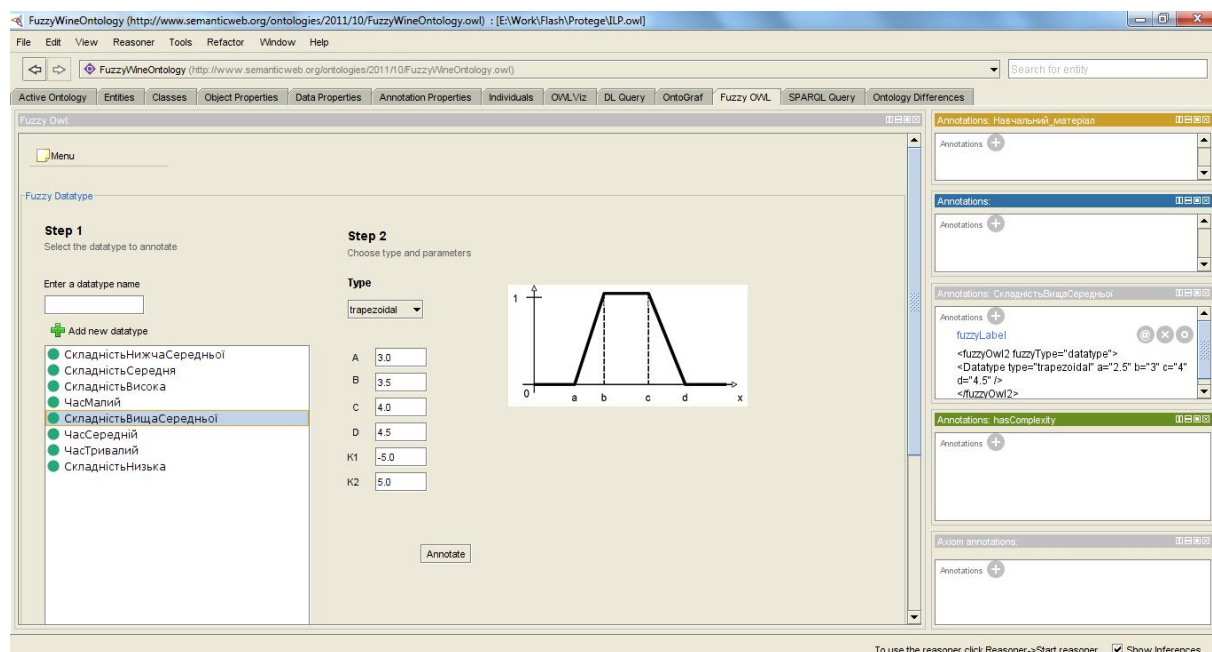


Рис. 9. Нечітка онтологія в онтології індивідуальної траєкторії навчання

Таким чином, даний підхід використовується для інтеграції нечіткого онтологічного та логічного висновку.

Висновки

Вирішено актуальну наукову задачу формування індивідуальної траєкторії навчання студента із застосуванням нечіткого підходу. Розроблено базу нечітких правил для визначення часу вивчення навчального фрагменту залежно від рівня знань студента та складності навчального матеріалу. База правил нечіткої моделі формування індивідуальної траєкторії навчання використовується для створення онтології навчальної дисципліни шляхом введення характеристик складності навчальних фрагментів та часу їх вивчення.

Список літератури

1. Brusilovsky, P. Adaptive navigation support: from adaptive hypermedia to the adaptive web and beyond / P. Brusilovsky // *PsychNology Journal*. – 2004. – Vol. 2. – No. 1. – pp. 7-23.
2. Limongelli, C. Configuration of Personalized e-Learning Courses in Moodle / Carla Limongelli, Giuseppe Sampietro, Marco Temperini // *EUROCON 2007 The International Conference on «Computer as a Tool»*, Warsaw, September 9-12, 2007. – Pp. 2680-2686.
3. Karampiperis, P. Adaptive Learning Resources Sequencing in Educational Hypermedia Systems / P. Karampiperis, D. Sampson // *Educational Technology & Society*. – 2005. – Vol. 8. – Issue 4. – Pp. 128-147.
4. Лендюк, Т.В. Формування індивідуальної траєкторії навчання з використанням знання-орієнтованого і нечіткого підходів / Т.В. Лендюк, С.П. Ріппа, С.І. Саченко // *Сучасні проблеми інформатики в управлінні, економіці, освіті та подоланні наслідків Чорнобильської катастрофи [матеріали XV Міжнародного наукового семінару, Київ – оз. Світязь, 4–8 липня 2016 року]*. – С. 279-283.
5. Лендюк, Т.В. Використання нечіткої логіки для формування індивідуальної траєкторії навчання / Т.В. Лендюк // *Матеріали XVII Міжнародної науково-практичної конференції «Українська наука: проблеми сьогодення та перспективи розвитку»*, Київ, 24-25.07.2015. – С. 44-47.
6. Коваль, В.С. Система дистанційного навчання як інформаційний портал в середовищі семантичного Вебу / В.С. Коваль, Т.В. Лендюк, С.П. Ріппа // *Сучасні комп'ютерні інформаційні технології: Матеріали II Всеукраїнської школи-семінару молодих вчених і студентів АСІТ'2012*. – Тернопіль: ТНЕУ, 2012. – С. 179-180.
7. Асаки, К. Прикладные нечеткие системы / К. Асаки, Д. Ватада, С. Иваи и др. Пер. с япон.; под ред. Тэрано Т., Сугэно М. – М.: Мир, 1993. – 368 с.
8. Zadeh, L.A. Generalized theory of uncertainty (GTU) – principal concepts and ideas / Lotfi A. Zadeh // *Computational statistic & Data analysis*. – 2006. – № 51. – pp. 15-46.
9. Хала, К.А. Один из подходов использования нечеткой логики в построении предметно-ориентированных онтологий на основе текстового контента / К.А. Хала // *Международная научная конференция имени Т.А. Таран «Интеллектуальный анализ информации» ИАИ-2013*, Киев, 15–17 мая 2013 г. : сб. тр. – К. : Просвіта, 2013. – С. 21-27.
10. García-Cerdaña Á. Fuzzy Description Logics and t-norm based fuzzy logics / Á. García-Cerdaña, E. Armengol, F. Esteva // *International Journal of Approximate Reasoning*. – 2010. – Vol. 51. – Pp. 632-655.
11. Lukasiewicz, T. Description logic programs under probabilistic uncertainty and fuzzy vagueness / T. Lukasiewicz, U. Straccia // *International Journal of Approximate Reasoning*. – 2009. – Vol. 50. – Pp. 837-853.
12. Aajli, A. A new approach of learning hierarchy construction based on fuzzy logic / A. Aajli, K. Afdel // *International Journal of Engineering Research and Applications*. – 2014. – Vol. 4. – Issue 10 (Part – 3). – Pp. 58-66.
13. Szentes, D. Enhanced test evaluation for web based adaptive learning paths / D. Szentes, B.-A. Bargel, A. Streicher, W. Roller // in *Proceedings of the 7th International Conference on Next Generation Web Services Practices, NWeSP, Salamanca, Spain, 19-21 October 2011*. – Pp. 352-356.

14. Gokmen, G. Evaluation of Student Performance in Laboratory Applications Using Fuzzy Logic / G. Gokmen, T.C. Akinci, M. Tektas, N. Onat. G. Kocyigit, N. Tektas // *Procedia Social and Behavioral Science*. – 2010. – Vol. 2. – Issue 2. – Pp. 902-909.
15. Voskoglou, M.Gr. Fuzzy Methods for Student Assessment / M.Gr. Voskoglou, I.Ya. Subbotin // *International Journal of Education and Information Technology*. – 2015. – Vol. 1. – No. 1. – Pp. 20-28.
16. Заде, Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений: Пер. с англ. / Л. Заде. – М.: Мир, 1976. – 167 с.
17. Zadeh, L.A. Fuzzy sets as a basis for a theory of possibility / L.A. Zadeh // *Fuzzy Sets and Systems*. – 1999. – Vol. 100. – No. supp. – Pp. 3-28.
18. Штовба, С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д. Штовба // *Проблемы управления и информатики*. – 2007. – №4. – С. 102-114.

НЕЧЕТКАЯ МОДЕЛЬ ФОРМИРОВАНИЯ ИНДИВИДУАЛЬНОЙ ТРАЕКТОРИИ ОБУЧЕНИЯ И ПОСТРОЕНИЕ ОНТОЛОГИИ НА ЕЕ ОСНОВЕ

Т.В. Лендюк, Н.М. Васильків

Тернопольский национальный экономический университет,
ул. Львовская, 11, г. Тернополь, 46020, Украина; e-mail: tl@tneu.edu.ua

В статье предложена реализация модели формирования учебного материала на основе уровня знаний студентов и сложности задач (построения индивидуальной траектории обучения), которая базируется на аппарате нечеткой логики. Построена база правил нечеткой модели и проверена на правильность работы. Сформированные нечеткие правила использованы в онтологии учебной дисциплины.

Ключевые слова: индивидуальная траектория обучения, учебный фрагмент, нечеткая модель, нечеткая онтология

FUZZY MODEL OF INDIVIDUAL LEARNING PATH FORMING AND ONTOLOGY DESIGN ON ITS BASIS

T.V. Lendyuk, N.M. Vasylykiv

Ternopil National Economic University,
11 Lvivska street, Ternopil, 46020, Ukraine; e-mail: tl@tneu.edu.ua

The article proposes the implementation of model for the forming of educational material based on the students knowledge level of and the tasks complexity (the construction of individual learning path), which is based on the fuzzy logic approach. The basis of fuzzy model rules was constructed and it was checked for work correctness. Formed fuzzy rules are used in the discipline ontology.

Key words: individual trajectory of training, training fragment, fuzzy model, fuzzy ontology

POSSIBILITY OF OBTAINING FUNCTIONAL DEPENDENCES FROM DATABASE STRUCTURE

S.I. Grishin¹, L.N. Timoshenko²

¹ Odessa National Maritime University,
Mechnikov 34, Odessa, 65404, Ukraine, e-mail: grishin_si@ukr.net

² Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine

We study the possibility of obtaining functional dependencies from the scheme of the existing database, as well as the data contained in it. Statistical methods for finding dependencies between data were used to generate probability dependencies. Software implementation of the developed algorithm for generating dependencies provides connection to various data providers. Application testing showed that the correct results can be obtained with a sufficiently large amount of data in the source.

Keywords: functional dependence of attributes, normal form, probability, class C#, SQL query

Introduction

Normalization is an obligatory stage of database design. Knowledge of the violation of certain rules of normal forms allows foresee the occurrence of anomalies and redundancy and apply appropriate measures for their preliminary elimination. Despite the fact that the normalization stage is repeated a huge number of times in various developments, in most cases it is performed manually by an experienced specialist. Normalization process is completely formalized, however it is described in terms of the functional dependences which are, in fact, mathematical representation of some rules and regularities of the real world. Since they are completely determined by the subject domain, there is no possibility to automate their search at the design stage. That is why there are no mechanisms of normalization in modern modeling tools, such as Sybase Power Designer or IBM Rational Software Architect.

At the same time, the use of functional dependencies may be required not only at the design stage of OLTP information systems. For example, to extend an OLTP system or design a business intelligence system without creating a data warehouse, you may need an existing database that is not supported by the developer. Another possible situation is operation with the ROLAP data warehouse. The dimensional model that is used for ROLAP database design, include means of denormalization and data division to enhance speed of request execution. The use of outtrigger tables in the dimensional model bring to partial or complete normalization of dimension tables. Thus, the level of normalization of ROLAP data warehouse can be different. If there are problems with the operation laboriousness in such systems, it may be necessary to check their normalization.

Objective and task

In this work, we investigated the possibility of obtaining functional dependencies from the scheme of the existing database, as well as the data contained in it.

To achieve this goal in the paper we solve such *problems*:

- software has been developed for constructing functional dependencies;
- the program is tested and its scope is determined.

Main part

Finding functional dependencies in the database is not a trivial task. First, the regularities found in particular relationship variable not always valid for whole relation. Secondly, required functional dependences are not reflected at design of the database, so the corresponding restrictions of integrity are not respected. Therefore, the studied tables can contain mistakes. The way out of this situation is the probabilistic approach in the search for functional dependencies [1].

The developed software is designed to obtain probabilistic functional dependencies from the data contained in the tables. Statistical methods intended for search of dependences between data are used for generation of probabilistic functional dependencies. Such a search is carried out in each separate data source. Then obtained data are combined into a general scheme by searching for the minimum coverage for the found set of probabilistic functional dependencies. Further, results that do not meet the requirements of the obtained scheme are eliminated.

Let relation R be given, X is a subset of its attributes, and A is an attribute of this relation. A probabilistic functional dependence is the triplet $\langle X, A, p \rangle$, where p indicates the probability of the existence of a functional dependence $X \rightarrow A$. It is proposed to calculate the probability p for all possible combinations X, A of the R relation. We excepted from calculation the functional dependencies that already found, as well as those sets X that are supersets of some potential keys. If probability of dependence existence is greater than some parameter p_0 , the dependence is included in the model and analyzed together with previously constructed dependencies.

The following algorithm is proposed to find the probability p of the existence of the functional dependence of the attribute A on the set of attributes X :

1. The most common value V_a of attribute A is found for each unique value V_x of the set of attributes X .
2. The probability of the functional dependence $X \rightarrow A$ among the tuples with the value V_x of the X attributes is calculated. It is calculated as the ratio of the number of tuples in which V_x corresponds to the value V_a , to the number of tuples with the V_x value of the X attribute:

$$P(X \rightarrow A, V_x) = \frac{|V_x, V_a|}{|V_x|},$$

where $|V_x, V_a|$ is the number of tuples in which the value V_a corresponds to the value V_x , $|V_x|$ is the number of tuples with the V_x value of the X attribute.

3. The probability p is calculated as the average of all probabilities obtained in step 2.

Formally, if D_x – a set of unique values of a set of attributes X , then the probability of existence of the functional dependence is described as follows:

$$P(X \rightarrow A, R) = \frac{\sum_{V_x \in D_x} P(X \rightarrow A, V_x)}{|D_x|}.$$

The application for constructing functional dependencies in the above ways and dependencies analysis is performed in C # and the .NET 4.0 platform.

After connecting to the database, the user is asked to select the tables he wants to analyze.

Next, he has to specify the minimum probability value, which is significant for probabilistic functional dependence existence.

The following information is displayed for each table:

1. Name of the table being analyzed.
2. A list of all the probabilistic functional dependencies found and their corresponding probabilities.
3. Graph of functional dependencies.
4. The arrows with solid lines in this graph show the functional dependencies obtained as a result of the analysis of the database schema. The dotted lines correspond to probabilistic functional dependencies calculated on the basis of the data contained in the table.
5. Estimated normal form.

The following classes were created to represent information about the structure of the database:

Database – represents the database. Contains its name and a list of tables.

DatabaseTable – represents the database table. Contains the name of the table, the name of the schema that contains the table, and lists of potential and foreign keys.

Column – represents the table attribute. Contains the name and type of the attribute.

Constraint – base class for database integrity constraints. Contains the name and type of the constraint (potential or foreign key).

ForeignKey – represents the foreign key of the table. Contains the referencing attribute, as well as information about the table and the potential key, to which this attribute refers. This class inherits the Constraint class.

CandidateKey – represents the potential key of the table. Contains a list of attributes that are part of this potential key. Inherits the Constraint class.

An abstract class called DatabaseProxy was developed to obtain information about the structure of the database. It contains the connection string to the database under investigation and the following methods for obtaining the data required for analysis:

List <DatabaseTable> GetDatabaseTables() – returns a list of database tables, including only information about table name and schema name.

Database GetDatabaseSchema(List <DatabaseTable> tables) – the method returns full information about the database and those tables that are specified in the tables parameter. It includes a list of attributes and their types, primary and foreign keys, unique indexes.

bool CheckIfColumnIsUnique(DatabaseTable table, Column column) – checks whether the values of the specified attribute are unique. Used to search for potential keys not listed in the conceptual diagram.

double GetFDProbability(DatabaseTable table, List<Column> determinant, Column dependentColumn) – receives the probability of the existence of a functional relationship with the determinant and the dependent part specified in the determinant and dependentColumn parameters.

Various implementations of this abstract class can be used to study databases presented in different DBMSs. We use Microsoft SQL Server. The appropriate class is called MSSQLServerProxy. Let us consider its implementation in more detail.

The queries to the service tables of the INFORMATION_SCHEMA schema were created to get information about the database schema. After receiving necessary data on a database structure, we pass to the analysis of its contents. The DatabaseDataAnalyzer class is responsible for it. This class realizes search of all probable functional dependences having only one attribute as a determinant. The main analysis algorithm of one table is shown below:

1. The list of all non-key table attributes is formed.

2. Attributes which all values are unique are deleted from this list. These attributes are marked as possible potential keys that are not reflected in the database schema.

3. All possible probable functional dependences are formed. The determinant of each of them will be the element of the set obtained on step 2. Dependent part will be any attribute of the table, other than a determinant.

4. For each of the probabilistic functional dependencies obtained from the data contained in the database, the probability of their existence is calculated.

5. Probable functional dependences are selected if probability exceeds some value of p_0 . This value is algorithm parameter.

It is necessary to be able to quickly check the set of attribute values for uniqueness, and also to calculate the probability of existence of functional dependencies between some sets of attributes for effective operation of the algorithm.

To implement such checks, it is proposed to generate an SQL-query that solves the task and transfer it for execution to an SQL server. This approach allows you to efficiently examine remote databases. Import database content to local storage can take a long time. At an execution stage we don't know the schema of the database under investigation. It will be necessary to generate a separate query for check of uniqueness of values or computation of probable functional dependence for each set of attributes

Here are some examples of SQL queries that solve the set tasks. The request to verify the uniqueness of the values of the attribute *A* of the *TABLE* table of the *SCHEMA* schema will look like this

```
SELECT [A]
FROM [SCHEMA].[TABLE]
GROUP BY [A]
HAVING COUNT(1) >=2
```

The calculation of probabilistic functional dependencies requires a series of calculations. Let it be necessary to calculate the probability of the existence of a functional dependence of the attribute *B* on the attribute *A* in the table 1. The SQL query that solves this problem has the following syntax:

```
select AVG(probability)
from
(select
(select MAX(count)/CAST(SUM(count) As REAL)
from
(select COUNT(y.B) as count
from
(select t1.B
from TABLE as t1
where t1.A = t.A and
A is not null and
B is not null ) as x
join
(select t1.B
from TABLE as t1
where t1.A = t.A and
A is not null and
B is not null) as y
on x.B = y.B
group by x.B
) as tempTable
```

) as probability
 from TABLE as t
 where A is not null and B is not null
 group by A
) as distinctProbabilities.

The Microsoft sample database Adventure Works [2] was used for testing of the created application. Examples of testing are given in the table 1.

Table 1.

Examples of Adventure Works database testing

Table name	Number of records	Amount of dependences	Normalization assessment
CreditCard	19118	0	3NF
Address	19614	2	2NF
EmployeePayHistory	316	3	2NF

The program found no probabilistic functional dependencies, except dependencies from the primary key. It correctly defined the normal form of the CreditCard table.

There are dependencies of the city and the state ID from the zip code in the Address table. That is quite logical – the same zip code always points to a certain state and city, while in one city there can be many different postal codes. The program successfully defined both dependences, displayed them on the chart and in specified that the table is only in the second normal form.

For the EmployeePayHistory table, all the dependencies obtained were found to be incorrect. The first functional dependence in terms of the subject area indicates that each employee is inclined to receive a salary with a certain frequency convenient for him. Although this statement is rather plausible, it is not a restriction on the integrity of the database. In the process of work, an employee or an employer may revise an employment contract. Thus, a false result was obtained though it was based on the correct data. Unfortunately, there is no way to identify such cases programmatically – you need a manual analysis by an expert. The second probabilistic functional dependence (the periodicity of payment from its hourly rate), unlike the first one, has no semantic meaning. The error is due to insufficient data in this case. The number of accidental coincidence of two attributes values increases in case of a small amount of records. That is shown especially strongly in this case as the “periodicity of payment” attribute accepts only 2 different values in all tables. This error can be eliminated by some modification of the calculation method for the case of a small number of records, or by searching for a more suitable data source. There is the dependence of the date of changing the line on the frequency of payment in the third case. This dependence also does not make any sense. The detailed analysis of basic data showed that the high percent of identical values of “date of change” attribute is a cause of error in this case. 277 records of 316 have identical values. This situation can also be resolved programmatically by means of a preliminary analysis of the researched data.

Conclusion

A large amount of data is needed to obtain a qualitative result using the probabilistic approach in the search for functional dependencies.

In case of dominance of the correct data the considered algorithms are capable to process even the sources containing erratic or inexact information.

References

1. Wang, D.Z. Functional dependency generation and applications in pay-as-you-go data integration systems [Electronic Resource]. / D.Z. Wang, L. Dong, A.D. Sarma, M. Franklin, A. Halevy. - Mode of access: <http://webdb09.cse.buffalo.edu/papers/Paper18/webdb09.pdf>.
2. AdventureWorks. Data Dictionary. Dataedo. 2017-05-30 [Electronic Resource]. - Mode of access: <https://dataedo.com/download/AdventureWorks.pdf>

МОЖЛИВІСТЬ ОТРИМАННЯ ФУНКЦІОНАЛЬНИХ ЗАЛЕЖНОСТЕЙ ЧЕРЕЗ СТРУКТУРУ БАЗИ ДАНИХ

С.І. Гришин¹, Л.М. Тимошенко²

¹ Одеський національний морський університет,
Мечникова 34, Одеса, 65404, Україна, e-mail: grishin_si@ukr.net

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

Наведено результати дослідження можливості отримання функціональних залежностей зі схеми існуючої бази, а також даних, що містяться в ній. Для генерації ймовірнісних функціональних залежностей використані статистичні методи пошуку залежностей між даними. Програмна реалізація розробленого алгоритму генерації залежностей забезпечує підключення до різних постачальників даних. Тестування додатка показало, що коректні результати можна отримати при досить великому обсязі даних в джерелі.

Ключові слова: функціональна залежність атрибутів, нормальна форма, ймовірність, клас C#, запит SQL

ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ФУНКЦИОНАЛЬНЫХ ЗАВИСИМОСТЕЙ ИЗ СТРУКТУРЫ БАЗЫ ДАННЫХ

С.И. Гришин¹, Л.Н. Тимошенко²

¹ Одесский национальный морской университет,
Мечникова 34, Одесса, 65404, Украина, e-mail: grishin_si@ukr.net

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

Приведены результаты исследования возможности получения функциональных зависимостей из схемы существующей базы, а также данных, содержащихся в ней. Для генерации вероятностных функциональных зависимостей использованы статистические методы поиска зависимостей между данными. Программная реализация разработанного алгоритма генерации зависимостей обеспечивает подключение к различным поставщикам данных. Тестирование приложения показало, что корректные результаты можно получить при достаточно большом объеме данных в источнике.

Ключевые слова: функциональная зависимость атрибутов, нормальная форма, вероятность, класс C#, запрос SQL

ДОСЛІДЖЕННЯ ОПТИМАЛЬНОГО КОЕФІЦІЄНТУ ВИТРАТ НА ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

М.Г. Романюков

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: nikolay.romanyukov@gmail.com

Концепцією технічного захисту інформації в Україні визначено злочинну діяльність, спрямовану на незаконне отримання інформації, закритої для доступу сторонніх осіб, з метою досягнення матеріальної вигоди або нанесення шкоди юридичним або фізичним особам, як одне з основних джерел інформаційної небезпеки. Звідси виникає необхідність на прикладі побудови моделі порушника розрахувати оптимальний варіант витрат на організацію технічного захисту інформації віброакустичним каналом витоку та встановити величину витрат для надійного захисту інформації залежно від витрат на несанкціонований доступ до неї. Розглянути організаційно-технічні заходи та порядок їх проведення під час побудови системи технічного захисту інформації з обмеженим доступом з урахуванням державних нормативних документів.

Ключові слова: технічні канали витоку інформації, комплекс технічного захисту інформації, віброакустичні канали витоку

Вступ

Одним з найважливіших організаційно-технічних заходів в галузі технічного захисту інформації (ТЗІ) є протидія технічним розвідкам. Організація протидії та своєчасне проведення необхідних заходів покладається на Керівника органу державної влади, органу місцевого самоврядування, органу управління Збройних Сил України, утворених згідно із законодавством України. Безпосереднє проведення заходів протидії здійснює штатний чи позаштатний підрозділ ТЗІ або призначена відповідальна особа. В даному випадку оборона має два аспекти: захист від інформаційного впливу та захист особистої інформації. Захист особистої інформації частіше має вирішальне значення [1].

Концепцією технічного захисту в Україні [2] визначено одним з основних принципів формування і проведення політики у сфері ТЗІ обов'язкову вимогу захисту інформаційно-технічними заходами інформації, яка становить державну та передбачену законом таємницю, службової інформації, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах місцевого самоврядування та органах державної влади. Фінансове забезпечення системи ТЗІ здійснюється за рахунок Державного бюджету України, місцевих бюджетів та інших джерел. Звідси виникає питання оптимальності витрат на організацію захисту інформації по технічних каналах.

Постановка задачі

На прикладі побудови моделі порушника розробити методику розрахунку витрат на організацію технічного захисту інформації віброакустичним каналом витоку. Використовуючи математичний апарат теорії ігор, вирішити задачу оптимальних витрат на організацію технічного захисту інформації віброакустичним каналом витоку, що постає перед Власником (підрозділу організації).

Основна частина

Особливі вимоги щодо захисту висуваються до інформації з обмеженим доступом (далі ІзОД) від загроз, що можуть бути реалізовані каналами спеціального впливу на технічні засоби інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем (далі – ІТС) та на інші технічні засоби. Захист мовної інформації потребує особливої організації проектно-архітектурних рішень та проведення організаційних та технічних заходів.

Перед Власником (підрозділу організації) постає задача оптимальних витрат для вирішення питання захисту. В даному випадку виникає конфліктна ситуація, коли два суб'єкти інформаційної діяльності мають протилежні цілі та інтереси, при чому результат дії кожної зі сторін залежить від дії супротивника. На практиці будують моделі конфліктних ситуацій, які називають іграми.

Для розв'язування даного роду задач використовують математичний апарат теорії ігор. В нашому випадку учасниками ігрової ситуації, які мають протилежні цілі, є штатний чи позаштатний підрозділ з ТЗІ або призначена відповідальна особа з одного боку та зловмисник (порушник), дії якого передбачено у моделі загроз. Характерною особливістю даної ситуації є взаємодія протилежних інтересів двох суперників, кожний з яких намагається оптимізувати свої рішення. У такій грі джерелом невизначеності є відсутність інформації про стратегію суперників. Кожна протидіюча сторона має можливість вибору одного (або декількох) варіантів стратегій. Кожному крокові гравця відповідає певний програш (виграш), який він отримує. Завдання кожного гравця – знайти оптимальну стратегію гри, яка забезпечує йому максимально можливий виграш. Результати за всіма можливими варіантами гри задаються у вигляді платіжної матриці (матриці гри):

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad (1)$$

рядки якої відповідають стратегіям A_1 , A_2 , а стовпці – стратегіям B_1 та B_2 . Елементи цієї матриці a_{11} та a_{21} – виграші гравця A (далі захисник), якщо він вибрав стратегію A_1 та A_2 відповідно, а гравець B (далі зловмисник) – стратегію B_1 ; елементи a_{12} та a_{22} – виграші захисника A , якщо він вибрав стратегії A_1 та A_2 відповідно, а зловмисник – стратегію B_2 .

Система віброакустичного захисту інформації згідно діючого НДТЗІ реалізована на базі генератора шуму, де в якості захисного сигналу використовуються виключно найпростіші однокомпонентні захисні завади типу «білий шум» та «рожевий шум». Діапазон робочих частот вихідного сигналу повинен охоплювати не менше п'яти октав з частотами 18-5600 Гц [6]. Відповідно до Переліку засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (станом на

1 січня 2017 року), оберемо наступний комплект техніки для обладнання об'єкту інформаційної діяльності:

- генератор акустичного шуму «Ріас-2ГМ» ТУ У 33.2-33694400001:2006 (ПП „РІАС” 02660, м. Київ,). Експертний висновок №627 дійсний з 05.02.2016 до 05.02.2019, виданий на партію продукції зав. № 37300-37499;
- вібровипромінювачі п'єзоелектричні «Ріас-2ВП» ТУ У 33.2-33694400-001:2006 (ПП „РІАС” 02660, м. Київ,). Експертний висновок №629 дійсний з 05.02.2016 до 05.02.2019, виданий на партію продукції зав. № 38000-45499;
- випромінювачі акустичні «Ріас-2ВА» ТУ У 33.2-33694400-001:2006 (ПП „РІАС” 02660, м. Київ,). Експертний висновок №630 дійсний з 05.02.2016 до 05.02.2019, виданий на партію продукції зав. 46000-46999.

Для обладнання середньостатистичного приміщення, де циркулює акустична ІзОД з двома вікнами та двома батареями опалення, необхідно встановити техніку віброакустичного захисту, представлена у табл.1.

Таблиця 1

Техніка віброакустичного захисту

Найменування приладу	Кількість, шт.	Вартість на момент написання статті, тис. грн
Генератор акустичного шуму «Ріас-2ГМ»	1	8000
Вібровипромінювачі п'єзоелектричні «Ріас-2ВП»	8	7150
Випромінювачі акустичні «Ріас-2ВА»	10	6840

Налаштування системи захисту та оцінка ефективності її застосування проводиться згідно вимог НД ТЗІ 2.2-006-08 [7] та НД ТЗІ 2.2-017-08 [8].

На основі оцінки імовірності використання порушником тих чи інших засобів несанкціонованого знімання інформації припустимо використання стетоскопу як інструменту технічної розвідки. Іноземними фірмами випускаються різні варіанти стетоскопів: від простіших портативних малогабаритних до складних конструкцій, обладнаних високочастотними та низькочастотними підсилювачами та набором вбудованих еквалайзерних фільтрів. Вартість професійного комплексу становить в межах 700 у.о. (17220 грн. по курсу НБУ на момент написання статті) [9].

Всі елементи вказаної платіжної матриці є вартості гри засобів технічного захисту інформації: a_{11} – стетоскопа, a_{12} – генератора та вібровипромінювачів, a_{21} – генератора та акустичних випромінювачів, a_{22} – генератора, акустичних випромінювачів, вібровипромінювачів. Отже, матричну гру можна представити у вигляді:

$$\begin{array}{cc}
 & \text{Гравець } B \\
 & \begin{array}{cc} B_1 & B_2 \end{array} \\
 \text{Гравець } A & \begin{array}{cc} A_1 & A_2 \end{array} \\
 & \begin{array}{cc} 17220 & 15150 \\ 14840 & 21990 \end{array}
 \end{array} \quad (2)$$

Для вибору раціональних варіантів рішень використаємо максиміно-мінімакський критерій [10]. Суть критерію полягає в тому, що гравець A намагається максимізувати свій мінімальний виграш, незалежно від дій гравця B . В той час як гравець B намагається мінімізувати свій програш, незалежно від дій гравця A . При цьому

захиснику необхідно здійснити вибір по виграшу, який він отримає незалежно від дій зловмисника, тобто незалежно від вибору дій зловмисника захисник інформації отримує певний мінімальний виграш. Захисник допускає, що зловмисник знає, який буде його вибір, і зробить спробу, щоб мінімізувати виграш захисника. Виходячи з цього, захисник аналізує всі свої стратегії та відмічає мінімальний виграш у кожному рядку. Зрозуміло, що він вибере стратегію, яка забезпечить максимальний виграш серед цих мінімальних виграшів. З другого боку зловмисник зробить спробу мінімізувати свій максимальний програш незалежно від вибору стратегії захисником. Тому він відмічає максимальний програш у кожному стовбці, та обирає стратегію, яка мінімізує його максимально можливий програш за всіма варіантами дій захисника. Оскільки захисник не може виграти більше, ніж може програти зловмисник, то маємо:

$$\max_j \min_i a_{ij} \leq \min_i \max_j a_{ij}, \text{ де } i = 1, 2; j = 1, 2; \quad (3)$$

Оптимальний розв'язок досягається тоді, коли жодному гравцю не вигідно змінювати обрану стратегію, оскільки суперник може у відповідь обрати іншу стратегію, яка дасть йому кращий результат, якщо:

$$\max_j \min_i a_{ij} = \min_i \max_j a_{ij} = v, \quad (4)$$

тобто $\alpha = \beta = v$, гра є цілком визначеною із сідловою точкою (характеризує оптимальний вибір стратегій обох гравців, при цьому зміна оптимальної стратегії одного з гравців приводить до можливих втрат з його боку), тобто в цьому випадку захисник отримує позитивний результат своїх дій в той час як зловмисник при аналогічних затратах не досягає своєї мети. У цій ситуації оптимальним для обох сторін є вибір чистих стратегій (вибір стратегії з ймовірністю, що дорівнює 1) – максимінної для захисника (незалежно від вибору стратегії зловмисником, захисник отримує певний мінімальний виграш) та мінімаксної для зловмисника (незалежно від вибору стратегії захисника, зловмисник отримує мінімальний програш). Адже якщо один з гравців дотримується оптимальної стратегії, то для іншого відхилення від його оптимальної стратегії не може бути вигідним. У нашому випадку у разі вибору захисником стратегії A_1 , залежно від дії зловмисника він може отримати виграш 17220 грн. або 15150 грн. Але його виграш завжди буде не меншим за $\min[17220, 15150] = 15150$ грн., тобто незалежно від дій зловмисника. Якщо розглянути можливі наслідки вибору захисником стратегії A_2 , то аналогічно його гарантований виграш становитиме $\min[14840, 21990] = 14840$ грн. Отже, нижня ціна гри $\alpha = \max[15150, 14840] = 15150$ грн., і захисник для максимізації мінімального виграшу має обрати стратегію A_1 . Зловмисник, який намагається мінімізувати свій програш, обираючи стратегію B_1 , може програти 17220 грн. або 14840 грн. Але за будь-яких варіантів захисника він може програти не більше ніж $\max[17220, 14840] = 17220$ грн. Для стратегії B_2 маємо $\max[15150, 21990] = 21990$ грн.. Отже, верхня ціна гри $\beta = \min[21990, 17220] = 17220$ грн., і зловмисник для мінімізації свого програшу має обрати стратегію B_1 . Оскільки $\alpha \neq \beta$, то гра не має сідлової точки та $\alpha \leq \beta \leq v$, тобто максимінно-мінімаксні стратегії не є оптимальними, кожна зі сторін може поліпшити свій результат, обираючи інший підхід.

При відсутності сідлової точки (кожний з учасників конфлікту може поліпшити свій результат, обираючи так звані змішані стратегії) суттєво, щоб стратегії визначались певною схемою, яка реалізує випадковий вибір з метою маскування свідомого вибору ходу гравцем. Саме тоді гравець буде прагнути до максимізації

очікуваного виграшу. Оптимальний розв'язок такої гри знаходять, застосовуючи змішані стратегії, які є певними комбінаціями початкових чистих стратегій, тобто кожна з них обирається з певною ймовірністю. Ймовірності (частоти) вибору кожної стратегії задаються відповідними векторами. Для гравця $A: X = (x_1, x_2)$, де $\sum_{i=1}^2 x_i = 1$;

для гравця $B: Y = (y_1, y_2)$, де $\sum_{j=1}^2 y_j = 1$. Очевидно, що $x_i \geq 0$; $y_j \geq 0$.

Якщо гравець A використовує стратегію X , а гравець B стратегію Y , то очікуваний виграш для гравця буде XAY , де A – платіжна матриця. Це простий вираз для суми, доданками для якої є добутки виграшу і двох ймовірностей того, що кожний з гравців обере стратегію, яка призведе до цього виграшу.

Так як сідлова точка відсутня ($\alpha \neq \beta$), то переходимо до розгляду гри двох гравців A та B з ненульовою сумою (виграш гравця A відрізняється по величині від програшу гравця B та дозволяє при певному виборі стратегій отримати для себе максимально-можливий результат) [11]. При такій грі кожний елемент платіжної матриці повинен складатись із a_{ij} та b_{ij} виграшів гравців A та B , що відповідають стратегіям A_i та B_j . При цьому вводиться стратегія S , яка є точкою рівноваги стратегій S_A і S_B . В точці рівноваги змішана стратегія гравця максимізує його виграш при умові, що гравці дотримуються рівноважних стратегій S_A і S_B (стратегії, вибір яких не дозволяє погіршувати результати виграшу для гравців A та B). Вибір стратегії рівноваги S_A для гравця A здійснюється наступним чином: він повинен обрати таку стратегію, щоб при будь-яких діях гравця B останній отримав би однаковий програш. Відмова одного з гравців від рівноважної стратегії виключає для нього можливість отримання більшого виграшу при умові, що другий гравець продовжує дотримуватись своєї стратегії рівноваги.

Так як у нашому випадку маємо гру з ненульовою сумою, то вихідна матриця A приймає вигляд:

$$\begin{array}{ccccc}
 & & \text{Гравець } B & & \\
 & & B_1 & & B_2 \\
 \text{Гравець } A & A_1 & (9680, 7540) \rightarrow (7310, 7840) & & (5) \\
 & & \uparrow & & \downarrow \\
 & A_2 & (9550, 5290) \leftarrow (16740, 5250) & &
 \end{array}$$

де перша цифра в дужках вказує виграш гравця A , а друга виграш гравця B . Вертикальні стрілки вказують на перевагу, яка надається гравцем A стратегії, на яку вказує стрілка, через більший, зв'язаний з нею виграш. Аналогічно горизонтальні стрілки вказують на виграш гравця B . Точка рівноваги повинна бути такою, щоб обидві стрілки вказували на неї (стрілка від A_2 до B_1 і стрілка від B_2 до B_1 , стрілка від A_2 до B_2 та від B_2 до A_2). В нашому випадку стрілки показують, що в чистих стратегіях точка рівноваги відсутня, саме тому виникає необхідність шукати її у змішаних стратегіях, які дають очікуване значення виграшу. В загальному випадку

необхідно перевірити наявність у платіжній матриці точки рівноваги, а також застосовувати до неї правило домінування. Домінуючі стратегії для гравців A та B відсутні, так як елементи, що відповідають стратегіям A_1 і A_2 , B_1 і B_2 не перевищують значень елементів інших стратегій. Для гравця A платіжна матриця має наступний вигляд:

$$\begin{array}{cc} A_1 & 9680 & 7310 \\ A_2 & 9550 & 16740 \end{array} \quad (6)$$

Для гравця B платіжна матриця має наступний вигляд:

$$\begin{array}{cc} B_1 & B_2 \\ 7540 & 7840 \\ 5290 & 5250 \end{array} \quad (7)$$

Щоб гарантувати однаковий виграш гравця A незалежно від його дій, гравець B зосереджує свою увагу на виграші гравця A і обчислює його змішані стратегії. Отже, якщо гравець B обирає стратегію B_1 з імовірністю q і стратегію B_2 з імовірністю $1 - q$, то математичні сподівання для обох рядків в платіжній матриці гравця A повинні бути рівними, тобто:

$$\begin{aligned} 9680q + 7310(1 - q) &= 9550q + 16740(1 - q); \\ 9680q + 7310 - 7310q &= 9550q + 16740 - 16740q; \\ 2370q + 7310 &= -7190q + 16740; \\ 9560q &= 9430; q = 0.99; (1 - q) = 1 - 0.99 = 0.01. \end{aligned} \quad (8)$$

Таким чином, гравець B повинен обирати стратегію B_1 з імовірністю 0.99 та стратегію B_2 з імовірністю 0.01. Аналогічно, якщо гравець A обирає стратегію A_1 з імовірністю p і стратегію A_2 з імовірністю $1 - p$, то математичні сподівання (середні значення випадкових виграшів гравців A та B) для обох стовпців в платіжній матриці гравця B повинні бути рівними, тобто:

$$\begin{aligned} 7540p + 5290(1 - p) &= 7840p + 5250(1 - p); \\ 7500p + 5290 - 5290p &= 7840p + 5250 - 5250p; \\ 2250p + 5290 &= 2590p + 5250; \\ 340p &= 40; p = 0.12; (1 - p) = 1 - 0.12 = 0.88. \end{aligned} \quad (9)$$

Таким чином, гравець A повинен обирати стратегію A_1 з імовірністю 0.12 та стратегію A_2 з імовірністю 0.88. Отже, маємо рівноважну стратегію:

$$S = (S_1, S_2) = (0.12A_1 + 0.88A_2, 0.99B_1 + 0.01B_2). \quad (10)$$

Очікуваний виграш гравця A складає:

$$V_1 = 9680 \cdot 0.12 \cdot 0.99 + 0.12 \cdot 7310 \cdot 0.01 + 0.88 \cdot 9550 \cdot 0.99 + 0.88 \cdot 16740 \cdot 0.01 = 1149.98 + 8.77 + 8319.96 + 147.31 = 9626.02. \quad (11)$$

Очікуваний виграш гравця B складає:

$$V_2 = 0.99 \cdot 7540 \cdot 0.12 + 0.99 \cdot 5290 \cdot 0.88 + 0.01 \cdot 7840 \cdot 0.12 + 0.01 \cdot 5250 \cdot 0.88 = 895.75 + 4608.65 + 9.41 + 46.20 = 5560.01. \quad (12)$$

Отже, рівноважний виграш гравців A та B :

$$\omega = (\omega_1; \omega_2) = (9626.02, 5560.01). \quad (13)$$

Оскільки в процесі віртуальної взаємодії гравців A та B з математичної точки зору нас цікавлять їх програші (витрати), то можна допустити, що їх програші обернено пропорційні до відповідних виграшів [12]. Для гравця A ця величина складає $\frac{1}{9626.02}$, а для гравця B $\frac{1}{5560.01}$. Порівнюючи ці величини, маємо:

$$\frac{1}{9626.02} \div \frac{1}{5560.01} = \frac{5560.01}{9626.02} = 0.58. \quad (14)$$

Висновки

Використовуючи математичний апарат теорії ігор, у даній статті вирішена задача оптимальних витрат для вирішення питання захисту інформації, що постає перед Власником (підрозділу організації). На прикладі побудови моделі порушника розраховано оптимальний варіант витрат на організацію технічного захисту інформації віброакустичним каналом витоку та встановлено, що для надійного захисту інформації з обмеженим доступом достатньо 55-60% витрат несанкціонованого доступу до неї. Використовуючи даний математичний апарат теорії ігор, можна вирішувати питання розрахунку оптимальних витрат на технічний захист інформації з обмеженим доступом для будь-яких каналів витоку.

Список літератури

1. Торокин, А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005.
2. Концепція технічного захисту інформації в Україні [Текст]: постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126 // Урядовий кур'єр. – 1997. 12 листопада. – С.3. [Електронний ресурс] – Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1126-97-%EF>.
3. Захист інформації. Технічний захист інформації Основні положення [Текст]: ДСТУ 3396.0. – [Чинний від 1997-01-01]. – ДСТУ 3396.0-96-ДСТУ 3396.2-97 : Вид. офіційне. К. : Держстандарт України, 1997. – 80 с. (Державний стандарт України).
4. Місюра, С.М. Варіант захисту мовної інформації на об'єктах інформаційної діяльності / С.М. Місюра, В.В. Овсянніков, І.Р. Мальцева // Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2011. – №2. – С.84-93.
5. Сабынин, В.Н. Защита информации в выделенных помещениях / В.Н. Сабынин // “ИНФОРМОСТ” – “Радиоэлектроника и телекоммуникации”. – 2002. – №1. – С. 25-28.

6. НДТЗИ Р-001-2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги.
7. Захист інформації на об'єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку мовної інформації [Текст]: НД ТЗІ 2.2-006-08. [Чинний від 2008-08-26]. – К.: Державна служба спеціального зв'язку та захисту інформації України, 2008. – 6 с. – (Нормативний документ системи технічного захисту інформації).
8. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами [Текст]: НД ТЗІ 2.3-017-08. [Чинний від 2008-08-26]. – К.: Державна служба спеціального зв'язку та захисту інформації України, 2008. – 18 с. – (Нормативний документ системи технічного захисту інформації).
9. Хорев, А.А. Средства акустической разведки: проводные микрофонные системы и электронные стетоскопы / А.А. Хорев // Специальная техника. – М.: 2010. – № 5. – С.2-15.
10. Нейман, Дж. Теория игр и экономическое поведение / Дж. Нейман, О. Моргенштерн. – М.: Наука, 1970. – 983 с.
11. Саати, Т.Л. Математические модели конфликтных ситуаций. – М.: Советское радио, 1977. – 300 с.
12. Вітлінський, В.В. Математичне програмування / В.В. Вітлінський, С.І. Наконечний, Т.О. Терещенко. – К.: КНЕУ, 2006. – 248 с.

ИССЛЕДОВАНИЕ ОПТИМАЛЬНОГО КОЭФФИЦИЕНТА ЗАТРАТ НА ТЕХНИЧЕСКУЮ ЗАЩИТУ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Н.Г. Романюков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: nikolay.romanyukov@gmail.com

Концепцией технической защиты информации в Украине определено преступную деятельность, направленную на незаконное получение информации, закрытой для доступа посторонних лиц, с целью достижения материальной выгоды или нанесения вреда юридическим или физическим лицам, как одним из основных источников информационной безопасности. Отсюда возникает необходимость на примере построения модели нарушителя, рассчитать оптимальный вариант затрат на организацию технической защиты информации по виброакустическому каналу утечки, и установить, величину расходов для надежной защиты информации в зависимости от расходов на несанкционированный доступ к ней. Рассмотрим организационно-технические мероприятия и порядок их проведения при построении системы технической защиты информации с ограниченным доступом с учетом государственных нормативных документов.

Ключевые слова: технические каналы утечки информации, комплекс технической защиты информации, виброакустические каналы утечки

INVESTIGATION OF OPTIMUM FLOW COEFFICIENTS TECHNICAL INFORMATION PROTECTION OF OBJECT INFORMATION

N.G. Romanyukov

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: nikolay.romanyukov@gmail.com

Technical Information Protection of Ukraine defines criminal activity aimed at illegally obtaining information closed to access by unauthorized persons in order to achieve material benefit or harm to individuals or legal entities as a major source of information security. Hence the need, the example of model building offender, to calculate the best option expenses for the organization of technical protection of information channel leakage vibroacoustic and determine the amount of expenditure for reliable protection of information depending on the cost of unauthorized access. Consider organizational and technical measures and how they conduct during the construction of technical protection of information with restricted access on the basis of state regulations.

Keywords: technical information leakage, complex technical information security, vibroacoustic channel leakage

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПЛАНУВАННІ ТА ДИСТАНЦІЙНОМУ КЕРУВАННІ РУХОМ МОБІЛЬНИХ ОБ'ЄКТІВ

Ю.О. Гунченко¹, І.В. Ковалець², С.А. Шворов³, Д.С. Комарчук³, В.Є. Лукін³

¹ Одеський національний університет імені І. І. Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна

² Інститут проблем математичних машин та систем НАН України,
пр. Глушкова, 42, м.Київ, 03680, Україна

³ Національний університет біоресурсів і природокористування України,
вул. Героїв Оборони, 15, м. Київ, 03041, Україна; e-mail:dmitruy@mail.ru

У статті з метою підвищення ефективності планування траєкторій руху мобільних об'єктів на складній місцевості запропоновано використовувати систему підтримки прийняття рішень при плануванні та дистанційному керуванні рухом мобільних роботів. Джерелом інформації для системи підтримки прийняття рішень є система технічного збору, що знаходиться на мобільному роботі та безпілотному літальному апараті. Відеоінформація, яка приймається системами технічного зору, передається на диспетчерський пункт в реальному часі. Розглянуті методи навігації мобільних роботів, які поділяються на три групи: глобальні, тактичні і локальні. Глобальний метод використовується перед початком руху мобільного робота на основі застосування карти місцевості. На тактичному рівні інформація про особливості різних ділянок місцевості та перешкоди на шляху руху робота постійно оновлюється за допомогою систем технічного зору. Для уникнення зіткнень з різними видами перешкод, які можуть з'являтися і зникати або змінювати своє місце розташування на шляху мобільного робота, застосовується локальний метод навігації. Показано, що використання систем технічного зору на базі безпілотного літального апарату істотно збільшує зони огляду мобільних роботів і дозволяє підвищити ефективність оперативного керування рухом та планування маршрутів мобільних роботів з урахуванням особливостей ділянок місцевості та різних перешкод. Розглянуті можливості застосування сучасних інформаційних систем і технологій, які включають в себе велику кількість процедур, що моделюють або підтримують процес інтелектуального планування руху мобільних об'єктів на основі даних, отриманих з безпілотного літального апарату. До простих процедур такого типу відноситься будь-яка класифікація кількісних даних по заданим користувачами критеріям, аналіз ділянок місцевості та перешкод з метою планування маршрутів мобільних роботів на складній місцевості. Процедури подібного типу присутні не тільки в задачах аналізу фотозображень, а й при їх обробці за допомогою геоінформаційних систем. Описано принципи використання і методи обробки навігаційної та зорової інформації при вирішенні основних завдань автономного руху мобільних роботів і польоту безпілотного літального апарату. Наведено структуру системи підтримки та прийняття рішень з застосуванням програмно-апаратних засобів систем технічного зору в складі мобільних роботів і безпілотного літального апарату в реальних середовищах.

Ключові слова: мобільна робототехніка, система технічного зору, мобільний робот, геоінформаційна система (ГІС), безпілотний літальний апарат (БПЛА)

Вступ

Системи підтримки та прийняття рішень (СППР) є якісно новим рівнем автоматизації управлінських рішень при плануванні маршрутів або навігації мобільних

роботів (МР). Під навігацією розуміється теорія і практика спрямування по заданій траєкторії рухомих об'єктів. Мета навігації МР полягає в знаходженні оптимальних (відповідно до заданих критеріїв) маршрутів його переміщення між заданими точками простору з урахуванням стаціонарних (пасивних) та рухомих (активних) перешкод. Виходячи з цього, розробка нових моделей, методів і алгоритмів навігації автономних мобільних роботів з урахуванням різних видів перешкод є актуальною науково-технічною задачею.

Аналіз останніх досліджень та публікацій [1-8] показує, що на даний час в СППР широко застосовуються глобальні і локальні методи навігації МР. Глобальні методи засновані на тому, що перед початком руху МР повністю відома карта місцевості. Знаючи своє місцезнаходження, точку фінішу, а також розташування всіх перешкод, МР, користуючись заданим алгоритмом дій, забезпечує знаходження найкоротшого шляху від старту до фінішу і після цього долає цей шлях. На практиці найбільш часто використовуються методи фронту хвилі, A^* , дерева квадратів, видимого графа [1-4]. До недоліків таких методів відноситься необхідність збереження карти місцевості (найчастіше великих розмірів) і підвищена обчислювальна складність. Локальні методи навігації використовуються в тих випадках, коли МР не відомі стаціонарні (пасивні) та рухомі (активні) перешкоди, які можуть з'являтися і зникати та змінювати своє місце розташування. У такому випадку МР отримує навігаційну інформацію про локальну область зовнішнього середовища, перебуваючи в межах дії його датчиків. До таких методів навігації МР можна віднести: методи, засновані на використанні потенційних полів перешкод [2], методи сімейства BUG [5, 6], що використовують для отримання навігаційної інформації тактильні датчики, а також методи сімейства VisBUG [6-8], які припускають отримання навігаційної інформації від ультразвукових датчиків. До переваг методів локальної навігації слід віднести їх обчислювальну простоту. Недоліки цих методів порівняно з методами глобальної навігації складаються у відхиленні реальної траєкторії руху МР від оптимального маршруту і більш складною процедурою локалізації МР в просторі. Для обох груп методів навігації МР характерна проблема своєчасного визначення пасивних та, особливо, активних перешкод на шляху руху МР. Крім того, існуючі методи та алгоритми розв'язання задач планування траєкторій руху наземного МР, застосовуються в два етапи: спочатку знаходиться глобальна траєкторія по картографічних даних, яка потім в процесі руху періодично уточнюється за даними бортової системи технічного зору (СТЗ) МР. Такому підходу властиві суперечності і недоліки, обумовлені суттєвою відмінністю масштабів подання інформації на цих двох етапах. Використання СТЗ на базі БПЛА, що поставляє проміжну між етапами планування інформацію про ділянки місцевості, дозволяє з одного боку оперативно уточнювати картографічні дані, а з іншого – на порядок розширити зону огляду бортової СТЗ МР, що підвищує ефективність вирішення всіх цільових завдань МР. Незважаючи на значний обсяг досліджень в даній області, проблема розробки СППР для навігації МР з урахуванням різних видів перешкод на шляху руху МР, залишається відкритою.

Мета досліджень – розробка структури системи підтримки та прийняття рішень при плануванні маршрутів руху і керуванні МР в залежності від перешкод, визначених за допомогою систем технічного зору.

Методи досліджень

Процес планування змісту та часу планування траєкторій руху МР поділяється на декілька етапів, а саме: формування електронної карти місцевості та визначення усіх видів перешкод на кожній ділянці з БПЛА на основі застосування методів статистичного аналізу та штучного інтелекту, а також визначення оптимальних

маршрутів руху МР з урахуванням перешкод з використанням методу ситуаційного керування.

Результати досліджень

У СППР використовується комбінований метод навігації МР, заснований на комплексному застосуванні глобальних, тактичних та локальних методів навігації. При наявності СТЗ на базі БПЛА можливий варіант трьохетапного планування траєкторій руху МР з використанням картографічних даних (глобальна траєкторія), даних з СТЗ на базі БПЛА (тактична траєкторія) і даних СТЗ МР (локальна траєкторія). Тактична траєкторія, яка побудована за даними з СТЗ на базі БПЛА, являє собою замкнуту траєкторію, що проходить по складкам місцевості. Цільовою точкою на глобальному рівні планування передбачається кінцева точка маршрутного завдання МР, цільовими точками на тактичному рівні планування буде послідовність точок, що належать глобальній траєкторії, а цільовими точками на локальному рівні планування будуть послідовності точок, що належать траєкторіям, побудованим на тактичному рівні планування. При цьому, місцевість, по якій пересувається МР, складається з ділянок двох видів: відкритих ділянок і перешкод, які МР не може прямо подолати. Якщо перешкода виявляється на шляху МР, то він повинен її об'їхати.

Система підтримки та прийняття рішень включає в себе необхідну кількість процедур, що моделюють або підтримують процес інтелектуального планування руху мобільних об'єктів (МО). До простих процедур такого типу відноситься будь-яка класифікація кількісних даних по заданим користувачами критеріям, більш складні забезпечують аналіз сцен, процесів, явищ з метою планування маршрутів МО на складній місцевості. Процедури подібного типу присутні не тільки в задачах аналізу фотозображень, а й при обробці даних за допомогою ГІС. У міру розширення сфери застосування геоінформаційних технологій та ускладнення процедур геоінформаційного моделювання процедури аналізу і класифікації сукупностей даних, об'єктів і структур займають все більш значуще місце і в ГІС нового покоління.

У СППР практично весь процес тематичного дешифрування фотозображень складається з поетапного угруповання і подальшого перетворення даних з метою створення абсолютно визначеною, проблемно-орієнтованої картини ділянки земної поверхні. Значна частина цих етапів забезпечується методами і алгоритмами, що входять в спеціалізовані інструментальні пакети, і завдання обробника полягає у створенні найбільш ефективної схеми класифікації даних.

Центральним елементом СППР (рис. 1) є спеціалізована база знань, яка здійснює ідентифікацію технологічних процесів керування МР. Під ідентифікацією надалі розуміється побудова математичної моделі, яка встановлює взаємозв'язок між вхідними змінними СТЗ і вихідними змінними щодо керування рухом МР. В основу математичної моделі ідентифікації покладена нечітка база знань, що представляє собою сукупність продукційних правил "ЯКЩО-ТО".

Обробка вхідних змінних СППР здійснюється на основі розпізнавання образів, що включає в себе ряд кроків:

1. Сприйняття образу від СТЗ (технічне вимірювання).
2. Фільтрація отриманого сигналу.
3. Визначення необхідних характеристик (індексація).
4. Прийняття рішення щодо класифікації образу.

На першому кроці забезпечується обробка інформації від радарів, камер спостереження, 3D-лазерних сканерів, тепловізорів.

Фільтрація отриманого сигналу та первинне опрацювання вхідних образів здійснюється на основі використання Вейвлет-аналізу [9].

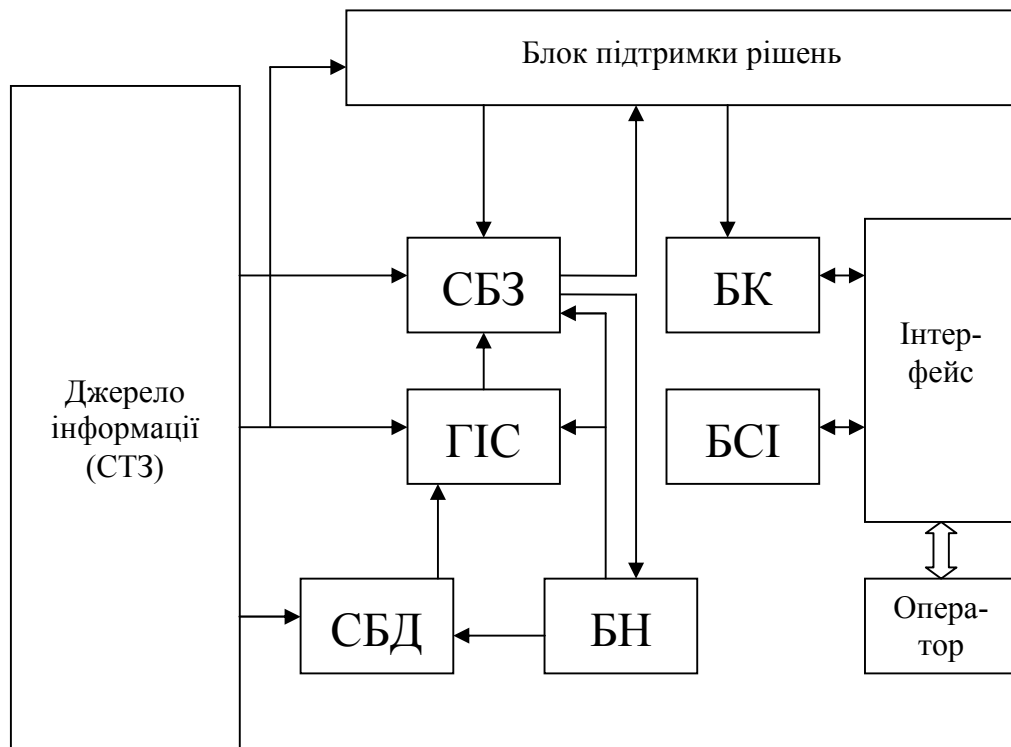


Рис. 1. Структурна схема СПДР: СБД – ситуативна база даних, СБЗ – спеціалізована база знань, ГІС – геоінформаційна система, БН – блок навчання, БК – блок коментарів, БСІ – блок синтезу інформаційної моделі

Розпізнавання образів (на третьому та четвертому кроках) здійснюється у системі розпізнавання образів (СРО). Синтез СРО включає наступні кроки: визначення тренувальної вибірки, представлення даних та значимих характеристик у необхідному вигляді, обґрунтування класифікуючого критерію та навчання СРО, повернення до кроку 2 (або навіть і до кроку 1) при незадовільній якості роботи СРО, оптимізація та налаштування СРО [9].

За допомогою СТЗ забезпечується отримання даних про ділянку місцевості з безпілотного літального апарату і МР та відображення перешкод на шляху руху МР за допомогою ГІС. Фотографування визначеної поверхні проводиться з висоти від 1 до 250 м з можливістю одержання знімків з високою роздільною здатністю.

Як показують результати експериментальних досліджень, отримані дані від звичайних цифрових фотокамер з БПЛА можна ефективно використовувати при визначенні різних перешкод на шляху руху МР. Після проведення фотозйомки на електронній карті місцевості на основі статистичної обробки RGB-сигналів визначається декілька контрастних за оптичними характеристиками зон (ділянок). Для кожної з цих зон експериментально визначаються контрольні розміри та спектральні характеристики різних видів перешкод, які використовуються для навчання нейронної мережі в БН. Таким чином, на основі статистичної обробки спектральних характеристик цифрових знімків кожної ділянки місцевості та за допомогою апарату нейронних мереж визначаються перешкоди на шляху руху МР, що забезпечує оперативне прийняття рішень для планування маршрутів руху МР.

За результатами фотозйомки з БПЛА проводиться статистична обробка отриманих даних. Оскільки стандартний формат Jpeg визначає значення RGB не для кожного конкретного пікселя, а для ділянок з однаковими параметрами, виникає необхідність у перетворенні даних із формату Jpeg в формат BMP, в якому значення яскравості складових адитивної моделі кольору утворення визначаються для кожного

пікселя. Таким чином, є можливість визначення координат перешкод на електронній карті місцевості, значення RGB яких відрізняються від середнього на відповідний відсоток.

Протягом всього польоту фотоапарат проводить серії знімків, що забезпечує їх перекриття для подальшої обробки. Дані про знімки завантажуються в СБД, СБЗ, ГІС та блок підтримки рішень, де обробляються, причому робота зі знімками може вестися як до приземлення апарату, так і після неї. Якщо контрольована територія має більший розмір ніж площа, яка відображена на знімку, тоді знімки «зшиваються» у панораму за допомогою програмного забезпечення «Panorama Factory». В результаті застосування цього програмного пакету отримуємо зведену панораму, до якої вже можна «прив'язати» географічні координати місцевості. В результаті чого отримуємо карту з прив'язкою по реперним точкам. Після прив'язки з'являється можливість обробляти знімок стандартним географічним інструментарієм.

Для планування руху МР відомою інформацією є початкове місце його знаходження та кінцева точка маршруту руху МР, координати перешкод, що отримані за допомогою СТЗ. Необхідно знайти такі оптимальні маршрути руху МР, при яких забезпечується:

- мінімальний шлях руху МР;
- об'їзд пасивних та активних перешкод.

Відправна задача приводиться до дискретного вигляду. Для цього область простору станів, що нас цікавить, накривається Q -ою мережею $L^{(1)} \times L^{(2)} \times \dots L^{(Q)}$. При цьому вважається, що МР може переміщуватися тільки з одного вузла цієї мережі до іншого.

Задача керування рухом в заданих умовах розв'язується за допомогою методу ситуаційного керування та апарату штучного інтелекту, що включає комбінацію нейронних мереж і продукційних правил, при застосуванні яких при переході від одного вузла до іншого мінімізується траєкторія руху МР [10].

Геометричні характеристики зони маневрування дистанційно визначаються СТЗ, створеної на базі 3D-лазерного сенсора, який дозволяє отримувати зображення зовнішнього середовища перед МР, в діапазоні відстаней 0...50 м, з точністю до 5 см. За результатами отриманих зображень відповідно до законів сканування з урахуванням кутових і лінійних переміщень МР будуються локальні траєкторії руху МР.

При плануванні глобальних траєкторій використовується картографічна база даних ГІС, що дозволяє не тільки зберігати інформацію про великі зони можливого маневрування, а й коригувати її в процесі руху за даними СТЗ БПЛА.

Таким чином навігаційна система створюється на основі комплексування ГІС, засобів супутникової навігації, датчиків БПЛА та МР. Комплексне використання різних датчиків і методів навігації (рис. 2), дозволило достовірно вирішувати навігаційну задачу бортовими засобами при функціонуванні МР в умовах пересіченій місцевості, а виконавча система відпрацьовувати знайдені траєкторії з урахуванням кінематичних і динамічних характеристик МР.

Експериментальне дослідження показало переваги в оперативності та достовірності отриманих результатів запропонованої СППР та в застосуванні комбінованого методу в порівнянні з традиційними методами навігації.

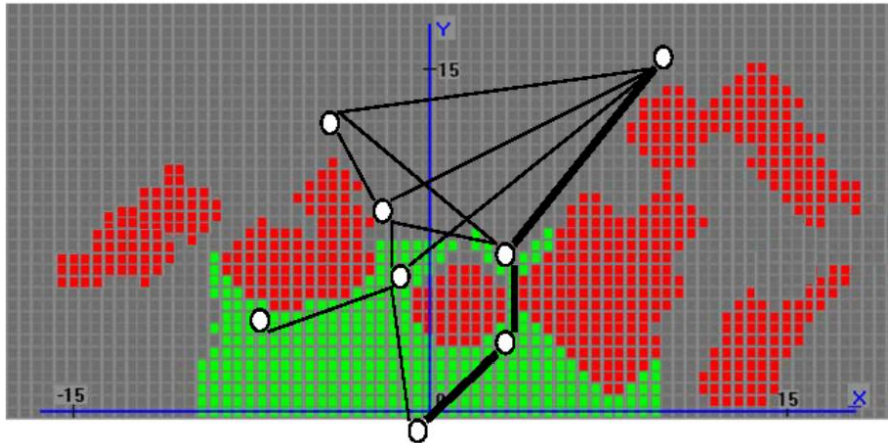


Рис. 2. Комплексне використання різних датчиків і методів навігації: червоним кольором зображені заборонені місця руху МР

Висновки і перспективи

Таким чином, запропонована СППР при плануванні маршрутів руху МР в залежності від наявності перешкод на шляху їх руху, визначених за допомогою СТЗ, передбачає більш високу достовірність і оперативність отримання інформації та точність керування МР, а також зменшення загальної довжини руху МР та витрат пального. Одержані дані з БПЛА дають можливість на основі використання розробленої технології оперативно визначати перешкоди на шляху руху МР, що скорочує часові витрати планування маршрутів руху групи мобільних роботів. Комплексне використання різних датчиків СТЗ і методів навігації МР є перспективним напрямом подальших досліджень.

Список літератури

1. Защелкин, К.В. Реализация комбинированного способа навигации автономного мобильного робота / К.В. Защелкин, В.В. Калиниченко, Н.О. Ульченка // Электротехнические и компьютерные системы. – 2013. – № 09 (85). – С. 102-109.
2. Адамів, О.П. Моделі та інтелектуальні засоби адаптивного керування автономним мобільним роботом [Текст] дис. ... канд.техн. наук: захищена 12.12.2007 / Адамів Олег Петрович. – Одеса, 2007. – 124 с.
3. Fahimi, F. Autonomous Robots. Modeling, Path Planning and Control / F. Fahimi –New York: Springer, 2009. – 348 p.
4. Hachour, O. Pathplanning of Autonomous Mobile robot / O. Hachour // International Journal of Systems Applications, Engineering and Development. – 2009. – Issue 4. – PP. 178 –190.
5. Lumelsky, V. Sensing, intelligence motion / V. Lumelsky – New Jersey: Wiley-Interscience, 2006. – 456 p.
6. Song, H. Research on Path Planning for the Mobile Intelligent Robot / H. Song, L. Hu // World Congress on Computer Science and Information Engineering. – 2009. – № 1. – P. 121-144.
7. Siegwart, R. Introduction to Autonomous Mobile Robots / R. Siegwart, I. Ourbakhsh. – Boston: MIT Press, 2004. – 336 p.
8. Jian, Y. Comparison of Optimal Solutions to Realtime Path Planning for a Mobile Vehicle / Y. Jian, Q. Zhihua, W. Jing, C. Kevin // IEEE Transactions on Systems, Man and Cybernetics. Part A: System and Humans. – 2010. – Vol. 40. – PP. 721-725.
9. Шворов С.А. Нейромережеве розпізнавання оптичних образів у системах спеціального призначення / Шворов С.А., Штепа В.М., Заяць Н.А. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2014. – Вип. 45. – С. 102-108.

10. Гунченко, Ю.О. Метод побудови інтелектуальних систем планування переміщення мобільного робота в невідомому середовищі / Ю.О. Гунченко, І.В. Муляр, П.М. Дубина // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2015. – Вип. 50. – С. 23-28.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПЛАНИРОВАНИИ И ДИСТАНЦИОННОМ УПРАВЛЕНИИ ДВИЖЕНИЕМ МОБИЛЬНЫХ ОБЪЕКТОВ

Ю.А. Гунченко¹, И.В. Ковалец², С.А. Шворов³ С.А., Д.С. Комарчук³, В.Е. Лукин³

¹ Одесский национальный университет имени И. И. Мечникова
ул. Дворянская, 2, Одесса, 65082, Украина

² Институт проблем математических машин та систем НАН Украины,
пр. Глушкова, 42, г. Киев, 03680, Украина

³ Национальный университет биоресурсов и природопользования Украины,
ул. Героев Оборона, 15, г. Киев, 03041, Украина; e-mail: dmitruy@mail.ru

В статье с целью повышения эффективности планирования траекторий движения мобильных объектов на сложной местности предложено использовать систему поддержки принятия решений при планировании и дистанционном управлении движением мобильных роботов. Источником информации для системы поддержки принятия решений являются системы технического зрения, которые находятся на мобильном роботе и беспилотном летательном аппарате. Видеоинформация, регистрируемая системами технического зрения, передается на диспетчерский пункт в реальном времени. Рассмотрены методы навигации мобильных роботов, которые делятся на три группы: глобальные, тактические и локальные. Глобальный метод используется перед началом движения мобильного робота на основе применения карты местности. На тактическом уровне информация об особенностях различных участков местности и препятствий на пути движения робота постоянно обновляется с помощью систем технического зрения. Во избежание столкновений с различными видами препятствий, которые могут появляться и исчезать или сменять свое местоположение на пути мобильного робота, применяется локальный метод навигации. Показано, что использование систем технического зрения на базе беспилотного летательного аппарата существенно увеличивает зоны обзора мобильных роботов и позволяет повысить эффективность оперативного управления движением и планирования маршрутов мобильных роботов с учетом особенностей участков местности и различных препятствий. Рассмотрены возможности применения современных информационных систем и технологий, которые включают в себя большое количество процедур, моделирующих или поддерживающих процесс интеллектуального планирования движения мобильных объектов на основе данных, полученных с беспилотного летательного аппарата. К простым процедурам такого типа относится любая классификация количественных данных по заданным пользователями критериям, анализ участков местности и препятствий с целью планирования маршрутов мобильных роботов на сложной местности. Процедуры подобного типа присутствуют не только в задачах анализа фотоизображений, но и при их обработке с помощью геоинформационных систем. Описаны принципы использования и обработки навигационной и зрительной информации при решении основных задач автономного движения мобильных роботов и полета беспилотного летательного аппарата. Приведена структура системы поддержки и принятия решений с применением программно-аппаратных средств систем технического зрения в составе мобильных роботов и беспилотного летательного аппарата в реальных средах.

Ключевые слова: мобильная робототехника, система технического зрения, мобильный робот, дрон, геоинформационная система, беспилотный летательный аппарат

DECISION SUPPORT SYSTEM IN PLANNING AND REMOTE CONTROL OF MOVEMENT MOBILE OBJECTS

Yu. A. Gunchenko¹, I.V. Kovalets², S.A. Shvoro³, D.S. Komarchuk³, V.E. Lukin³

¹ Odessa I.I.Mechnikov National University,
Dvoryanskaya str., 2, Odessa, 65082, Ukraine

² The Institute of Mathematical Machines and Systems Problems National Academy of Science of Ukraine,
Academician Glushkova Avenue 42, 03680, Kiev, Ukraine

³ National University of Life and Environmental Sciences of Ukraine,
Heroyiv Oborony st., 15, Kyiv, 03041, Ukraine; e-mail:dmitrui@mail.ru

In the article, in order to improve the efficiency of planning the trajectories of mobile objects on a difficult terrain, was suggested to use a decision support system for planning and remote control of the mobile robots movement. The source of information for the decision support system is a vision system that is on mobile objects and an unmanned aerial vehicle. Video information recorded by vision systems is transmitted to the control room in real time. The methods of navigation of mobile robots are considered, which are divided into three groups: global, tactical and local. The global method is used before the mobile robot moves on the basis of the map application. At the tactical level, information about the characteristics of different terrain areas and obstacles to the movement of the robot is constantly updated by the vision systems. To avoid collisions with various types of obstacles that can appear and disappear or change their location in the path of the mobile robot, a local navigation method is used. It is shown that the use of vision systems on the basis of an unmanned aerial vehicle significantly increases view areas of mobile robots and makes it possible to increase the efficiency of operational traffic control and route planning for mobile robots, taking into account the characteristics of terrain and various obstacles. The possibilities of application of modern information systems and technologies that include a large number of procedures that simulate or support the process of intellectual planning of the movement of mobile objects on the basis of data obtained from an unmanned aerial vehicle are considered. Simple procedures of this type include any classification of quantitative data for given users criteria, analysis of terrain and obstacles to plan routes for mobile robots in difficult terrain. Procedures of this type are present not only in problems of analyzing photo images, but also in their processing with the help of geoinformation systems. The principles of using and processing navigation and visual information in solving the main tasks of the autonomous movement of mobile robots and the flight of an unmanned aerial vehicle are described. The structure of the system of support and decision-making with the use of software and hardware for vision systems in mobile robots and an unmanned aerial vehicle in real environments is given.

Keywords: mobile robotics, technical vision system, UAV, mobile robot, geoinformation system, GIS, unmanned aerial vehicle

SUBMISSION OF ALGORITHM FOR WORKS SEQUENCES FINDING WITH PETRI NET

A.N. Tynynyka

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: lorans53@mail.ru

An easy and close to the optimal heuristic algorithm to solve a problem of scheduling theory with some restriction is offered. Such algorithms it is useful to represent of a secure Petri net. The figure steps for solving the problem are present using graphic notation in classical Petri nets plus additional extensions. The reasons for the fall in popularity of Petri nets and the ways of development of its expressive possibilities analyzed. In particular, it will contribute to creating a more complete standard models library with a clear graphical representation.

Keywords: theory of schedules, the sequence of works, algorithm, Petri net

Introduction

Separate process describes by a program that can be written in many languages. Petri nets successfully represent the structure of the control programs, convenient for program. To calculate values they are not designed, but they are designed to simulate instructions and the flow of information.

The standard way of presenting control programs structure is a block diagram algorithms. Block diagram represents the flow of control in a program.

Each algorithm can be depicted as a flowchart and then programmed. Thus, describing the proposed algorithm in the article as a Petri net, we represent and Petri net and, indeed, the follow-up program.

But first, let's solve one application task.

Task formulation

State the task of scheduling theory with this formulation.

One performer must perform n works with known duration of $l_i, i = 1...n$. In the specified calendar dates inspection work carried out, and only completed work accepts. Fix the following sequence works to minimize performed but not accepted works (not performed as a whole at the time of acceptance). This problem makes sense if unfinished deadline work fined.

For the sake of simplicity (not narrowing its mission), assume all integer values. Works will be planning as a whole, without gaps in the performance of any work.

Main body

To solve the problem proposed heuristic (not strict) algorithm acceptable computational complexity.

Sequence of operations when solving:

1. Distribute all upcoming work in order of duration l_i .
 2. First step: $k = 1$. Time step (the moment) $t = 0$. When this $U_1 = W, V_1 = \emptyset$, where W is the quantity of numbers all works; V_k – the quantity of numbers planned activities; U_k – the quantity of numbers have not yet scheduled works.
 3. Define the quantity of candidates B_k (step k) among the unplanned works: $i \in B_k$; if $t + l_i < c_i, i \in U_k$; c_i – planned completion date.
 4. If $B_k = \emptyset$, turn to p. 9.
 5. Calculate the value of the reserve q_i and the amount of losses (fine) s_i : $q_i = c_i - (t + l_i)$ and $s_i = (t + l_i) - c_i$, i.e. if $c_i > (t + l_i)$, include the difference to the reserve, and if $c_i < (t + l_i)$ – add to the amount of losses.
 6. Calculate the index value for each work candidate: $J_i = d \cdot s_i + (1 - d)q_i, i \in B_k$, where $d \in [0,1]$ – weighting factor.
 7. Choose the following work in according to minimum index: $v_k = \min\{J_i\}, i \in B_k$.
 8. Eliminate the planned work of the unplanned for the next step: $U_{k+1} = U_k \setminus \{v_k\}$. Increase the next step time on the duration of planed work: $t = t + l_{v_k}$. Turn to step 11.
 9. When there are no candidates, find an unplanned work with minimum time delay in the end (a fine proportional to the duration of delay).
 10. Repeat pp. 3, 5, 6, 7, 8.
 11. If the scheduled less than $n-1$ work, perform the following step: $k = k + 1$, referring to p. 3. Otherwise, proceed to the next item.
 12. At the final step plan to the rest of unplanned last work.
- Submitted algorithm requires less on average than n^3 elementary action.
- After obtaining sequences of operations typically to build a graphic block diagram of the algorithm.

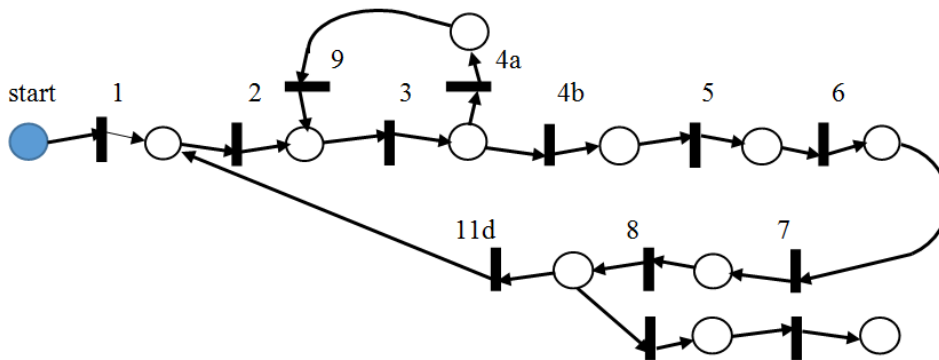


Fig. 1. Modeling with right secure Petri net of operations sequence when solving the task

Block diagram much like Petri nets [1]. Block diagram is visualized in the form of two types nodes (the decision and computation) and arcs between them (like Petri nets). However, in Petri nets transitions modeled actions, whereas in flowcharts nodes modeled actions. Thus, the correct translation of flowcharts in network nodes replaces on transitions network, and arc flowchart – on position of the network. Each arc flowchart corresponds exactly one position network. Flowchart nodes appear differently depending on the type: calculation or decision.

The fig. 1 shows these rules based Petri net that is equivalent to a possible flowchart for the proposed solution algorithm formulated task. Transitions numbering corresponds to the rows numbering of operations sequence when solving. Each position here has only one output

transition, except the one that preceded the adoption of the decision; such positions have two output transitions corresponding to the true and the false value of the predicate.

Transitions are associated with the actions of the program: computing and acceptances of decisions. To interpret the Petri net must interpret each passage. It should also be noted that transitions for calculations have one input and one output; the transition represents a calculation could not be in conflict, because his input position is not input for any other transition. The same action that is associated with the adoption of the decision, introduces a network conflict.

From the perspective of semantic interpretation in terms of simulated problem positions are associated with data, states or goals, while transitions are associated with operations (processes, procedures), that perform data conversion, implement response to input events, etc. Assumed that the transitions are performed instantly.

In Petri nets to represent the momentum used markers (tags, chips), which can be placed in position. Making a marker in the starting position breeds chain positives transitions. Move of marker from position to position reflects the dynamics of the network, and their initial location determines the specific process instance. The current distribution of markers in the positions sets the current state of the execution process modeled with Petri net.

One of the most important properties of Petri nets which simulates a real device or process is safety. The position of the Petri net is safe if the number of markers it never exceeds one. Petri net is safe if all net positions are safe.

The position is interpreted as a condition. The condition of being a logical expression is or true (represented with the token at position), or false (no token); multiple markers have no interpretation [2]. Thus, if network interpreted as conditions and events, marking each position must be safe.

Summation of the algorithm construction. The proposed algorithm is heuristic and does not guarantee an optimal solution, but studies with Monte-Carlo method indicate that decisions are close to optimal.

The average efficiency of the algorithm depends on the weighting factor d . Analysis made it possible to give a general recommendation: at low tension works expedient $d \approx 0.75$, at high – $d \approx 0.4$. Low tension corresponds to the more lengthy execution of works (when someone has time any delay to catch up later).

Conclusion

Historically, the Petri net was one of the first formal models intended for processes model specification. The popularity of the Petri net model, which was very high before the 1990's, is now dropped. The main reason for this is, apparently, in the weakness of submission means operational semantics. And the model does not disclose the questions relating to the execution environment. In view of the insufficiency of expressive possibilities Petri net and its available extensions, for example, chromatic, inhibitory, hierarchical Petri nets, etc., should be thinking about further expansion of models and use it as the basis for other languages, such as language YAWL (Yet Another Workflow) for modeling business processes first of all [3, 4, 5] or in language Workflow Net, where for some of the transitions require explicit writing expressions to complement the structural model of Petri nets. This, in particular, is in need of unambiguous choice of transitions requiring control logic, relevant operations “or” and “exclusive or”. Workflow Net language allows to express the formal semantics of workflows, i.e. clearly defines the rules of transition between nodes. But in all cases, when there are preconditions to the model of Petri nets refuse is not worth it.

Representation of the actions sequence in the fig. 1 uses graphic notation in classical Petri nets with small additional extensions, namely [5]:

1. It is present position in it, which does not have input arcs (initial position);
2. It is present position in it, which does not have output of arcs (end position).

The formal apparatus of Petri nets and their extensions [1] gives the possibility to create a library of generic models with a clear graphic representation. This last, in our view, the most important thing is – for the elements of Petri nets offered clear and easy-to-use graphic notation, satisfying aesthetic orientation of different users that largely determined the attraction of this model for developers, at least because of this model deserves no constriction and increased use. This article, in particular, performs such role.

References

1. Котов, В.Е. Сети Петри / В.Е. Котов. – М.: Наука, 1984. – 160 с.
2. Sheer, A. ARIS-Business Process Frame / A. Sheer. – Springer, 1999. – 170 p.
3. Aalst, W. Yet Another Workflow Language / W. Aalst, A. YAWL Hofstede // Information Systems. – 2005. – No.30(4). – PP. 245-275.
4. Aalst, W. The application of Petri Nets to Workflow management / W. Aalst // Journal of Circuits, System and Computers. – 1998. – No.8(1). – PP. 21-66.
5. Yet Another Workflow Language. <http://www.Yawl-system.com>.

ПОДАННЯ АЛГОРИТМУ ВИЗНАЧЕННЯ ПОСЛІДОВНОСТІ РОБІТ МЕРЕЖЕЮ ПЕТРІ

О. М. Тининика

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: lorans53@mail.ru

Запропоновано недалеко від оптимального евристичний алгоритм для розв'язання однієї задачі теорії розкладу з обмеженням припустимої обчислювальної складності. Такі алгоритми зручно і подавати безпечною мережею Петрі. Звернута увага на доцільність використання традиційних і розширених мереж Петрі для зображення подібних структур. На рисунку послідовність дій при рішенні задачі зображена за допомогою графічної нотації класичної мережі Петрі плюс додаткові розширення. Обговорені причини падіння популярності мереж Петрі і шляхи розвитку її виразних можливостей. Зокрема, цьому буде сприяти створення більш повної бібліотеки типових моделей з наочним графічним представленням.

Ключові слова: теорія розкладу, послідовність робіт, алгоритм, мережа Петрі

ПРЕДСТАВЛЕНИЕ АЛГОРИТМА ОПРЕДЕЛЕНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ РАБОТ СЕТЬЮ ПЕТРИ

А.Н. Тыныныка

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lorans53@mail.ru

Предложен несложный и близкий к оптимальному эвристический алгоритм решения одной задачи теории расписаний с ограничением. Алгоритмы такого рода удобно представлять безопасной сетью Петри. Обращено внимание на целесообразность использования традиционных и расширенных сетей Петри для изображения подобных структур. На рисунке последовательность действий при решении задачи представлена с использованием графической нотации классической сети Петри плюс дополнительные расширения. Обсуждены причины падения популярности сетей Петри и пути развития её выразительных возможностей. В частности, этому будет способствовать создание более полной библиотеки типовых моделей с наглядным графическим представлением.

Ключевые слова: теория расписаний, последовательность работ, алгоритм, сеть Петри

ВИЗНАЧЕННЯ ОЦІНКИ СУМАРНОГО КОРЕЛЯЦІЙНОГО ВЗАЄМОВПЛИВУ ПЕРІОДИЧНИХ ПРОЦЕСІВ З БАГАТОКРАТНИМ ПОВТОРЕННЯМ ТА ПРЕДСТАВЛЕННЯМ В ПОЛЯРНІЙ СИСТЕМІ КООРДИНАТ

А.І. Сегін

Тернопільський національний економічний університет,
вул. Львівська, 1, м.Тернопіль, 46020, Україна; e-mail: scs.kafedra@gmail.com

Запропонована сумарна оцінка кореляційних взаємовпливів періодичних процесів з врахуванням багатократного повторення та представлення кореляційних функцій в полярній системі координат.

Ключові слова: кореляційна функція, полярна система координат, періодичні процеси

Вступ

Сучасний рівень інформаційно-обчислювальної техніки дав значний поштовх розвитку та реалізації складних алгоритмів прогнозування та аналізу поведінки об'єктів і процесів в промисловості, радіоелектроніці, наукових дослідженнях, техніці, економіці та інших галузях. В той же час, потужність та швидкодія комп'ютерної техніки обумовили подальший розвиток класичних методів досліджень та аналізу складних систем. Одним з таких методів є кореляційний аналіз, який для певного класу об'єктів залишається незамінним потужним математичним апаратом для вирішення ряду прикладних задач [1-2].

В природі і техніці часто зустрічаються процеси, які мають циклічний характер з точною або приблизною періодичністю, слабо вираженими кореляційними зв'язками і протікають з великою кількістю повторень періодів. Як правило, такі процеси вважаються або слабокорельованими, в яких взаємозв'язками нехтують як не суттєвими, або вважаються взагалі не корельованими, оскільки кореляційні зв'язки не перевищують певного порогу. Проте за рахунок багатократної повторюваності навіть дуже слабкі кореляційні зв'язки можуть мати суттєвий вплив на протікання процесів, зміни станів об'єктів та розвиток систем. Крім того, в процесах, коли кореляційні зв'язки є досить сильними і їх враховують, все одно вони часто є недооціненими, оскільки не врахована їх багатократна повторюваність.

Визначення сумарного ефекту кореляційного впливу періодичних процесів

При традиційному кореляційному аналізі періодичних стаціонарних процесів для обчислень коваріаційної, кореляційної та нормованої кореляційної функцій [2] використовується відповідно вирази:

$$K(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} x(t)x(t+\tau) dt,$$

$$R(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} (x(t) - m_x)(x(t+\tau) - m_x) dt,$$

$$\rho(\tau) = \frac{R_x(\tau)}{D_x},$$

де T – період, $x(t)$ – сигнал, τ – зсув, m_x – математичне очікування сигналу $x(t)$, D_x – дисперсія сигналу $x(t)$. Для сигналів з нульовим математичним очікуванням коваріаційна та кореляційна функції співпадають.

В залежності від умов дослідження застосовується одна з наведених оцінок, які використовуються для визначення подібності сигналу до його зсунутої в часі копії – автокореляційна функція, чи зсунутих в часі двох різних сигналів – взаємкореляційна функція [1].

Проте, для визначення взаємовпливу періодичних сигналів часто необхідно враховувати їх повторюваність. Тоді навіть при незначних амплітудах кореляції в сумарному підсумку за рахунок великої кількості повторень це може призводити до значного взаємовпливу процесів, які значно недооцінені.

В подальшому будемо користуватись для спрощення розрахунків взаємоковаріаційною функцією, яка для дискретних сигналів представляється виразом:

$$K_{xy}(j) = \frac{1}{n} \sum_{i=1}^n x_i \cdot y_{i+j}, \quad (1)$$

де $n = \frac{T}{\Delta t}$, Δt – крок дискретизації, $x_i = x(i \cdot \Delta t)$ – дискретне значення сигналу $x(t)$, j – дискретний часовий зсув, що відповідає $j \cdot \Delta t$.

Загальний вплив періодичних процесів пропонується визначати як залежність від степеня корельованості $K_{xy}(j)$ та кількості повторень N :

$$K_{\Sigma}(j) = f(N)K_{xy}(j). \quad (2)$$

Якщо на деякому відрізку спостереження $(0, t)$ досліджувався процес з періодичністю T , то кількість повторень буде дорівнювати $N = \frac{t}{T}$. При цьому, якщо залежність сумарного кореляційного ефекту від кількості повторень не носить пропорційний характер з коефіцієнтом k , то вираз сумарного кореляційного впливу можна записати у вигляді:

$$K_{\Sigma}(j) = kNK_{xy}(j),$$

де k – коефіцієнт пропорційності, N – кількість повторень за досліджуваний період, $K_{xy}(j)$ – кореляційна залежність між процесами.

Очевидно, що залежність K_{Σ} від N може мати будь-який характер: гіперболічний, експоненціальний, логарифмічний та інші, набагато складніші. Функцію $f(N)$ можна визначити з виразу (2)

$$f(N) = \frac{K_{\Sigma}(j)}{K_{xy}(j)}.$$

Проте це далеко не завжди можливо, оскільки K_{Σ} , як правило, невідоме. В такому випадку, залежність $f(N)$ визначається емпірично або методами апроксимації.

Кореляційні моделі в декартовому просторі

Одним з найпростіших прикладів таких процесів може служити об'єкт, поведінка якого описується функцією: $x(t) = A_0 + A \sin(\omega t + \varphi)$, при чому постійна складова A_0 є набагато більшою в порівнянні з амплітудою синусоїдальної складовою A (рис. 1).

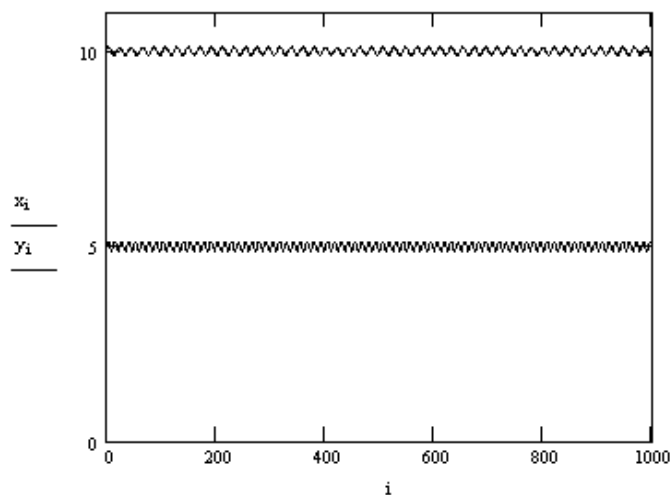


Рис. 1. Приклад сигналів з корельованими складовими малої амплітуди

В таких випадках часто синусоїдальною складовою знехтують і вважають сигнал постійним, що дорівнює A_0 . Подібна ситуація відбувається і для інших слабкорельованих процесів, які включають періодичні або майже періодичні корельовані складові малої амплітуди.

При дослідженні самого процесу таке спрощення можливо допустиме, але при дослідженні взаємозв'язку між процесами це може привести до хибних результатів. Особливо це стосується процесів із кратною періодичністю або квазіперіодичних процесів, у яких спостерігається повторюваність співпадіння фаз велику кількість разів.

Такий підхід можна застосовувати і для звичайних корельованих процесів, внаслідок чого сумарний ефект кореляції може бути набагато значнішим і впливовішим ніж при звичайному однократному впливі.

В багатократних циклічних процесах слабкі кореляційні зв'язки розподілені рівномірно по всій протяжності процесів і не приводять до видимих впливів. Проте, у випадку багатократних повторень кореляційних впливів на одну і ту ж ділянку процесу може привести до значних ефектів в зміні формування об'єктів чи протікання процесів.

Побудова взаємкореляційних моделей циклічних процесів, що багатократно повторюються в декартовому просторі, здійснюється за виразом

$$R_{xy}(j) = \frac{1}{n} \sum_{i=1}^n \hat{x}_i \cdot \hat{y}_{i+j},$$

де $\hat{x}_i, \hat{y}_{i+j}$ – дискретні центровані значення процесів.

Для спрощення процедур обчислення можна використати взаємоковаріаційну модель, в якій немає операції центрування значень процесів і яка розраховується за виразом (1).

В результаті, для процесів, представлених на рис. 1, отримаємо коваріаційну функцію, представлену на рис. 2.

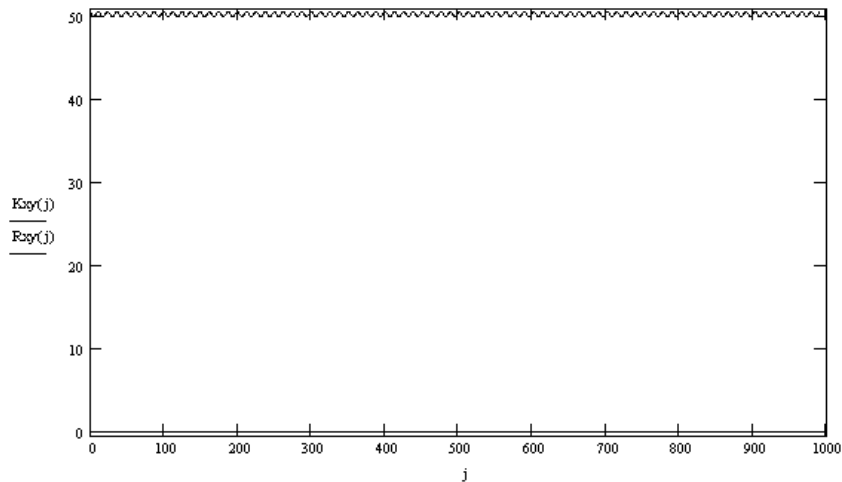


Рис. 2. Графік коваріаційної функції (верхня крива) та кореляційної функції (нижня крива) процесів, представлених на рис. 1

Як видно з графіків, представлених на рис. 2, коваріаційна функція в декартовому просторі має слабо виражений синусоїдальний характер, а кореляційна функція взагалі виглядає прямою лінією, хоча при більшому масштабі вона теж має синусоїдальний характер. Це, як правило, справедливо сприймається як відсутність кореляційних зв'язків, якими можна знехтувати. Проте, при довготривалому повторенні таких взаємокореляційних зв'язків вони можуть привести до суттєвих впливів.

Очевидно, що в декартовому просторі кожне з таких повторень відображаються окремим періодом графіку, і збільшення кількості повторень приводить тільки до розтягнення графіку в часі.

Кореляційні моделі в полярній системі координат

Представлення кореляційних моделей в полярній системі координат [3] для процесів, що розглядалися на рис. 1, буде мати вигляд, представлений на рис. 3.

Як і слід було очікувати, кореляційна функція теж практично дорівнює нулю, хоча при більшому масштабі буде мати вигляд, представлений на рис 4.

Фактично, при розгляді коваріаційних і кореляційних функцій в декартовому і полярному просторі отримані однакові результати. Хоч представлення в полярній системі координат має певні переваги [1], проте в даному випадку можна отримати наглядне представлення сумарного ефекту, якщо здійснити додавання значень кожного циклу повторень. В результаті отримаємо сумарний ефект кореляції (рис. 5).

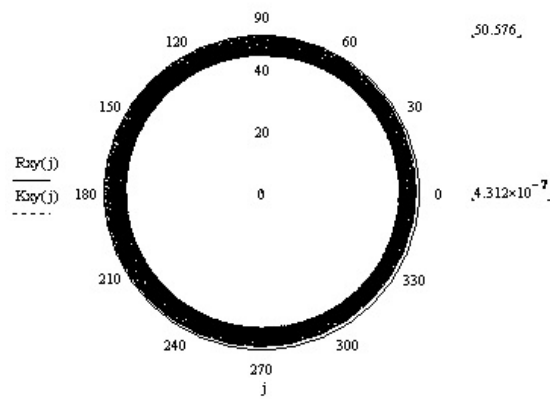


Рис. 3. Представлення коваріаційної функції (зовнішнє коло) і кореляційної функції (практично точка в значенні нуль)

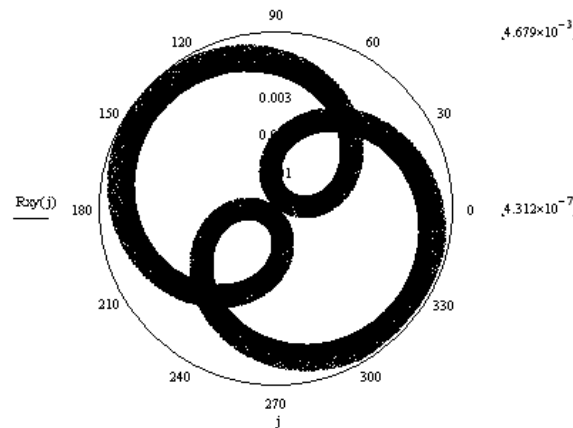


Рис. 4. Представлення кореляційної функції в полярній системі координат у збільшеному масштабі

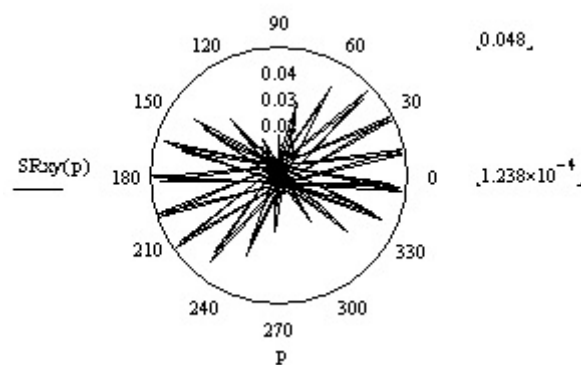


Рис. 5. Представлення оцінки сумарного ефекту кореляції в полярній системі координат

Як видно з рис. 5, порядок сумарного ефекту кореляційних зв'язків є на порядок більшим ніж на кожному циклі повторення. Крім того, можна встановити з даних графіків, на якій фазі процесів відбувається накопичення цих кореляційних ефектів і взаємний вплив є найбільшим чи найменшим.

Висновки

Аналіз сумарного ефекту кореляції може мати надзвичайне важливе значення при аналізі синусоїдальних процесів з деякими спотвореннями, наприклад, значень струмів в електромережах чи електроприладах для виявлення найбільш імовірних місць можливого пробиття ізоляції, в обертових процесах, для виявлення особливих місць навантаження та багатьох інших випадках.

Таким чином, можна досліджувати та встановлювати закономірності для процесів, які мають слабкі кореляційні зв'язки, але за рахунок великої кількості повторень протягом довгого часу можуть створювати значні сумарні впливи одні на одних, які зачасто нехтуються.

Список літератури

1. Сегін, А. І. Побудова алгоритмів формування моделей джерел інформації для автоматизованих систем реального часу / А. І. Сегін // Розвідка і розробка нафтових і газових родовищ. – Івано-Франківськ: ІФДТУНГ. Серія: методи і засоби технічної діагностики. – 1999. – Т. 8, № 36. – С. 84-93.
2. Сергиенко, А. Б. Цифровая обработка сигналов. Учебник для вузов. 2-е изд. / А. Б. Сергиенко. – СПб.: Питер, 206 – 751 с.
3. Сегін, А. І. Перспективи побудови кореляційних моделей в полярній системі координат / А. І. Сегін // Штучний інтелект, Національна академія наук України Інститут проблем штучного інтелекту. – 2009. – № 1. – С. 305-315.

ОПРЕДЕЛЕНИЕ ОЦЕНКИ СУММАРНОГО КОРРЕЛЯЦИОННОГО ВЗАИМОВЛИЯНИЯ ПЕРИОДИЧЕСКОГО ПРОЦЕССА С МНОГОКРАТНЫМ ПОВТОРЕНИЕМ И ПРЕДСТАВЛЕНИЕМ В ПОЛЯРНОЙ СИСТЕМЕ КООРДИНАТ

А.И. Сегин

Тернопольский национальный экономический университет,
ул. Львовская, 1, г. Тернополь, 46020, Украина; e-mail: scs.kafedra@gmail.com

Предложена суммарная оценка корреляционных взаимовлияний периодических процессов с учетом многократного повторения и представления корреляционных функций в полярной системе координат.

Ключевые слова: корреляционная функция, полярная система координат, периодические процессы

DETERMINATION THE GENERALIZED CORRELATION ESTIMATE THE IMPACT OF PERIODIC SIGNALS CONSIDERING MULTIPLE REPETITION AND REPRESENTATION IN POLAR COORDINATES

A.I. Segin

Ternopil national economical university
1, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: scs.kafedra@gmail.com

The proposed the generalized correlation estimate the impact of periodic signals considering multiple repetition and representation of correlation functions in polar coordinates.

Keywords: correlation function, polar coordinate system, periodic processes

РОЗРОБКА СИСТЕМИ ДЛЯ ФОРМУВАННЯ ЗВІТНОСТІ ПРО НАУКОВУ ТА МЕТОДИЧНУ РОБОТУ КАФЕДРИ

О.Ю. Лебедєва, Л.М. Тимошенко, В.М. Семенченко

Одеський національний політехнічний університет
пр. Шевченко 1, Одеса, 65044, Україна; e-mail: whiteswanhl@yahoo.com

У роботі розроблено систему для формування звітності про наукову та методичну роботу кафедри. Спроектвана база даних для формування звітності кафедри у вигляді ER-діаграм. Розроблена система для формування звітності, яка автоматизує одержання вхідних даних за допомогою excel-файлів.

Ключові слова: база даних, розробка системи, звітність про наукову та методичну роботу кафедри

Вступ

Головне завдання інформаційних систем підтримки діяльності вищих навчальних закладів (ВНЗ) полягає у створенні інформаційного середовища на базі мережевих, комп'ютерних, програмно-технічних засобів та сучасних технологій, які забезпечують ефективні процеси управління та прийняття рішень в умовах активного розвитку суспільства. Основним об'єктом, який, з одного боку, визначає діяльність ВНЗ, а з іншого – відображає і фіксує результати цієї діяльності, є документ. Оскільки організація роботи з документами є важливою частиною процесів керування і прийняття управлінських рішень, то завдання інформаційних технологій підтримки діяльності ВНЗ полягає у забезпеченні ефективних і гнучких засобів роботи з цим об'єктом на всіх етапах його життєдіяльності.

На кафедрах, як основних освітніх підрозділах ВНЗ, виконують значний обсяг рутинної роботи. Один із прикладів такої роботи – формування різноманітних видів та типів звітів, що мають типову структуру. Кожного разу така звітність формується вручну. Звичайно, ввід та друк документів виконують з застосуванням офісної техніки та програм, наприклад, текстових редакторів та електронних таблиць, які однак не позбавляють співробітників від необхідності формувати таблиці звітності з великими витратами часу порівняно з автоматизованим процесом. Тому автоматизація управління процесами у вищому навчальному закладі є виключно актуальним завданням.

Розробка системи для формування звітності про наукову та методичну роботу кафедри є особливо актуальною, тому що виникаючі проблеми з пошуком інформації й створенням звітів призводять до втрати робочого часу викладача, зупинки робочого процесу, та навіть втрати інформації. Тому швидка й безперебійна робота автоматизованої системи є однією з головних завдань.

Мета та задачі роботи

Метою роботи є розробка системи для автоматизації формування звітності про наукову та методичну роботу кафедри.

Для досягнення поставленої мети необхідно розв'язати наступні *задачі*:

- проаналізувати склад звітів про наукову та методичну роботу кафедри та визначити можливі напрями автоматизації процесу створення цих документів;
- визначити об'єкти бази даних;
- спроектувати базу даних;
- розробити систему для автоматизації формування звітності про наукову та методичну роботу кафедри.

Основна частина

Кафедра, як відомо, – базовий структурний підрозділ вищого навчального закладу, що проводить навчально-виховну, наукову і методичну роботу з однієї або кількох споріднених спеціальностей, спеціалізацій чи навчальних дисциплін і здійснює наукову, науково-дослідну та науково-технічну діяльність за певним напрямом. Основними завданнями кафедри є: створення умов для задоволення потреб студентів у підвищенні рівня професійних і культурних знань; підготовка висококваліфікованих фахівців з глибокими теоретичними і необхідними практичними знаннями; підвищення кваліфікації персоналу кафедри; підвищення якості методичного забезпечення навчального процесу; розробка нових технологій навчання; організація і проведення за замовленнями підприємств і організацій наукових досліджень і виконання пошуково-конструкторських робіт; поширення наукових, технічних і культурних знань серед населення.

Одним з процесів, необхідних для роботи кафедри, є складання звітів з наукової та методичної роботи викладачів кафедри. Звіти з наукової та методичної роботи кафедри повинні містити відповідні розділи та мати визначену структуру. Крім того, існують певні вимоги, визначені ВНЗ, не тільки до змісту, але й до оформлення зазначених документів. Складання таких звітів є досить трудомістким процесом, з яким мають справу викладачі усіх кафедр ВНЗ.

Розгляд існуючих програмних засобів ведення документації доводить необхідність створення універсальної автоматизованої системи, котра зможе формувати звіти з наукової та методичної роботи з різних дисциплін, що спростить і покращить роботу співробітників кафедри, зробить підготовку до навчального процесу ефективнішою та простішою. Такий підхід дозволить уникнути багатьох помилок, що зазвичай зустрічаються під час організації роботи кафедри.

Таким чином, модуль автоматизації звітності про наукову та методичну роботу кафедри ВНЗ дозволить автоматизувати певне коло завдань, яке виконують працівники кафедри.

Для розв'язання даної задачі доцільно використовувати технологію баз даних, а весь процес реєстрації та обробки даних повинен бути автоматизованим, швидко здійснювати пошук необхідної інформації в базі даних, формувати вихідні документи, проводити зміни в записах бази даних.

Першим етапом при проектуванні інформаційної бази даних є дослідження особливостей обраної предметної області, виявлення і аналіз вхідних та вихідних документів та повідомлень. Наступним є етап розробки концептуальної моделі, що є описом предметної області певного рівня абстракції, виконаним з використанням спеціальних мовних засобів, які не залежать від програмних засобів, що будуть використовуватись надалі, та містить необхідну та достатню інформацію для подальшого проектування. Результатом є семантичні моделі, що відображають інформаційний зміст конкретної предметної області та створюються на основі аналізу інформації, записаної в специфікації користувача. Моделі визначають об'єкти, властивості і зв'язки об'єктів, які реалізуються при проектуванні бази даних.

В якості інструмента для побудови семантичних моделей даних та уніфікованого представлення даних застосовують неформальну модель «сутність-зв'язок» (ER-модель). З моделі «сутність-зв'язок» можуть бути породжені всі існуючі моделі даних (ієрархічна, мережна, реляційна, об'єктна). Моделювання предметної області базується на використанні графічних діаграм, що включають певні різномірні компоненти. ER-модель не визначає операцій над даними й обмежується описом тільки їх логічної структури.

Після аналізу предметної області системи «Звітність кафедри» були визначені такі сутності: викладач, посада, звання та ступені, види публікацій, наукові публікації, міста, роки, методичні публікації, види методичних робіт, дисципліни, спеціальності, інститути, шифри груп, рівні освіти, методична робота викладача, публікації викладача.

Для визначених сутностей опишемо їх атрибути. Для запису використаємо мову інфологічного моделювання (МІМ), в якій сутності представляються у вигляді речень.

Для системи «Звітність кафедри» маємо наступні сутності та їх атрибути:

- ВИКЛАДАЧ (код, ПІБ, прізвище, ім'я, батькові, посада, ступень, звання, ПІБ_укр, ПІБ_рос, ПІБ_анг);
- ПОСАДА (код, назва);
- ЗВАННЯ_СТУПЕНІ (код, назва);
- ВИДИ_ПУБЛІКАЦІЙ (код, назва);
- НАУКОВІ_ПУБЛІКАЦІЇ (код, назва, вид_публікації, рік, назва_видання, автор, список_авторів, місто, номер, том, сторінки, кількість_сторінок, кількість_сторінок_вклад, зарубіжна, зі_студентом, назва_ГОСТ);
- МІСТА (код, назва);
- РОКИ (код, назва);
- ДИСЦИПЛІНИ (код, назва, інститут, групи, спеціальність, рівень_освіти);
- СПЕЦІАЛЬНОСТІ (код, назва);
- ІНСТИТУТИ (код, назва);
- ШИФРИ_ГРУП (код, назва);
- РІВНІ_ОСВІТИ (код, назва);
- ВИДИ_МЕТОДИЧНИХ_РОБІТ (код, назва);
- МЕТОДИЧНІ_ПУБЛІКАЦІЇ (код, назва, вид_методичних_робіт, автор, список_авторів, рік, дисципліна, форма_навчання, номер_реєстрації, дата_реєстрації, кількість_сторінок, кількість_сторінок_вклад);
- ПУБЛІКАЦІЇ_ВИКЛАДАЧА (номер, дата, викладач, наукова_публікація);
- МЕТОДИЧНА_РОБОТА_ВИКЛАДАЧА (номер, дата, викладач, методична_публікація).

Як інструмент семантичного моделювання використовуються різні варіанти діаграм «сутність-зв'язок» (ERD – Entity-Relationship diagram). Існують різні варіанти відображення ERD, але всі варіанти діаграм «сутність-зв'язок» виходять з однієї ідеї – рисунок завжди наочніше текстового опису.

ER-діаграми використовують графічне зображення сутностей предметної області, їх властивостей (атрибутів), і взаємозв'язків між сутностями. ER-діаграма для системи «Звітність кафедри» представлена на рис. 1 та 2.

На основі аналізу вимог до змісту та оформлення звітів про наукову та методичну роботу кафедри можна визначити два можливі шляхи автоматизації процесу формування звітності. Перший напрям пов'язаний із заповненням даних у системі, а другий – з одержанням звітів у необхідному вигляді.

Автоматизація процесу заповнення даних у системі можлива з використанням excel-файлів. Система формує excel-файли з необхідними полями для заповнення для наукових публікацій та методичних робіт (рис. 3 та 4). Такий файл передається викладачам кафедри для заповнення. Після заповнення викладачами переданого файлу,

система зчитує дані з файлу та автоматично зберігає їх у базі. Цей крок дозволяє прискорити заповнення бази необхідними даними та запобігати зменшенню користувацьких помилок.

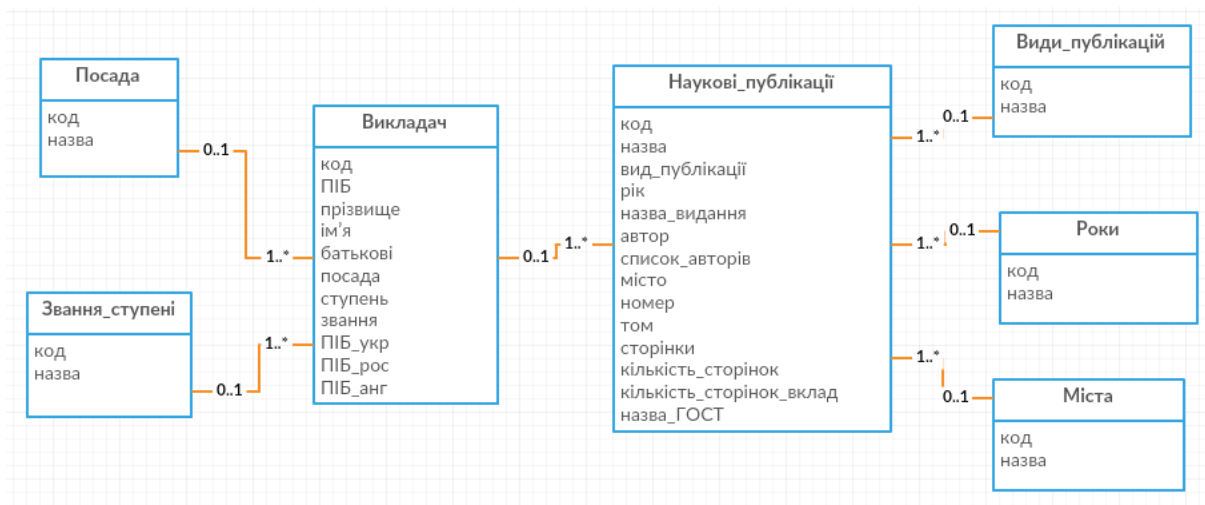


Рис. 1. Наукові публікації

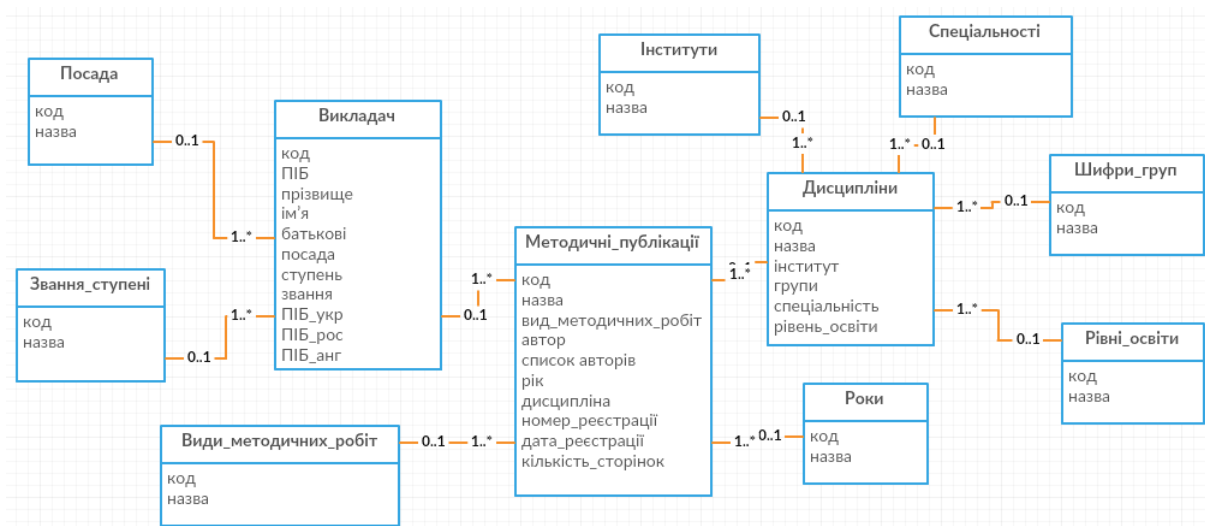


Рис. 2. Методичні роботи

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Назва (мовою оригіналу)	Характер праці (обирається зі списку: Стаття у фаховому виданні, Стаття у провідному закордонному виданні, Тези, Монографія, Підручник, Навчальний посібник, Методичні рекомендації, Патент, Програма)	Вид конференції, семінару: Міжнародна, Всеукраїнська, Регіональна	Список авторського колективу (мовою оригіналу в послідовності, як в публікації)	Співавтори праці (державною мовою в послідовності, як в публікації)	Вихідні дані мовою оригіналу	Місто	Номер	Том	Рік	Діапазон сторінок	Обсяг сторінок	Обсяг власних сторінок	Праця у зарубіжному виданні: 1 - так, 0 - ні	Праця зі студентом: 1 - так, 0 - ні
2															

Рис. 3. Поля excel-файлу для наукових публікацій

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Назва (мовою оригіналу)	Характер роботи (обирається зі списку: Конспект лекцій, Підручник, Навчальний посібник, Методичні рекомендації, Програма)	Дисципліна (обирається зі списку)	Інститут, факультет (обирається зі списку)	Вид методичної роботи (обирається зі списку: Лекція, Лабораторна, Практична, Виробнича практика, Переддипломна практика)	Форма навчання: 1 - очна, 2 - заочна	Список авторського колективу (мовою оригіналу в послідовності, як в роботі)	Співавтори праці (державною мовою в послідовності, як в роботі)	Вихідні дані мовою оригіналу	Спеціальність	Рік	Обсяг сторінок	Обсяг власних сторінок
2													

Рис. 4. Поля ексел-файлу для методичних робіт

У розробленій системі такі об'єкти, як викладач, посада, звання та ступені, міста, роки, дисципліни, спеціальності, інститути, шифри груп створені у вигляді довідників (рис. 5), наукові публікації та методичні публікації – у вигляді документів (рис. 6).

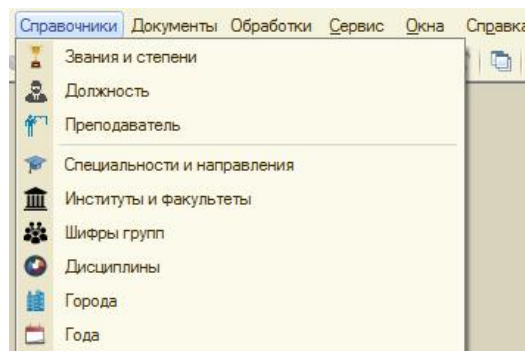


Рис. 5. Довідники системи «Звітність кафедри»

Публікації: Публікації 000000003 от 15.06.2017 13:58:28

Действия       Перейти 

Номер: 000000003 Дата: 15.06.2017 13:58:28 

Преподаватель: Лебедева Е.Ю. 

N	Название	Вид публикации	Соавторы	Где	Номер	Том	Год	Стр...	Количество ...	Со студ...	Зар...
		Вид конференции	Соавторы укр.	Место публикации					Количество ...		
1	Алгоритм створення аналіфа з двох зображень	Тези	В.В. Гусін, О.Ю. Лебедева	XIII всеукраїнська конференція студентів...			2016	30 - 32	3	☒	☐
		Всеукраїнська	В.В. Гусін, О.Ю. Лебедева	Одеса					1,50		
2	Розробка веб-сайту інтернет-магазину для виробів з металу	Тези	В.Г. Кагалак, О.Ю. Лебедева	XIII всеукраїнська конференція студентів...			2016	46 - 48	3	☒	☐
		Всеукраїнська	В.Г. Кагалак, О.Ю. Лебедева	Одеса					1,50		
3	Алгоритм покращення чіткості цифрового зображення	Стаття у фаховому виданні	В.В. Зоріло, А.С. Матвеева, О.Ю. Лебед...	Інформатика та математичні методи в ...	3	6	2016	41 - 49	9	☒	☐
			В.В. Зоріло, А.С. Матвеева, О.Ю. Лебедева						2,25		
4	Уточнення області застосування алгоритму виявлення фотомонтажу	Стаття у фаховому виданні	В.В. Зоріло, О.Ю. Лебедева, М.О. Козін...	Праці Одеського політехнічного універс...	2(49)		2016	101 - 108	8	☒	☐
			В.В. Зоріло, О.Ю. Лебедева, М.О. Козін...						2,00		
5	Analysis of the digital image in terms of different types of blur tools Adobe Photoshop	Тези	К. Каман, Е. Lebedeva, V. Zorilo	II Міжнародна конференція «Комп'ютер...			2016	19 - 20	2	☒	☐
		Міжнародна	К. Каман, О.Ю. Лебедева, В.В. Зоріло	Одеса					0,67		
6	Уточнення області застосування алгоритму виявлення фотомонтажу	Тези	В.В. Зоріло, О.Ю. Лебедева, М.О. Козін...	Матеріали міжнародної науково-практич...			2016	170 - 171	2	☒	☐
		Міжнародна	В.В. Зоріло, О.Ю. Лебедева, М.О. Козін...	Одеса					0,50		
7	Accuracy improvement of cloning area detection	Стаття у фаховому виданні	Ye. Yu. Lebedeva, A.A. Kobozova, V.V. Zorilo	Праці Одеського політехнічного універс...	3(50)		2016	47 - 53	7	☐	☐
			О.Ю. Лебедева, А.А.Кобозова, В.В. Зоріло						2,33		

Рис. 6. Приклад документу «Наукові публікації»

Висновки

В роботі були проаналізовані звіти про наукову та методичну роботу кафедри та визначені основні об'єкти для створення бази даних та можливі напрями автоматизації формування звітності кафедри. Була спроектована база даних та результати цього етапу представлені у вигляді ER-діаграм. Була розроблена система, яка дозволяє сформувати ексел-файли с полями для заповнення науковими публікаціями та методичними роботами викладача. Система зберігає інформацію з ексел-файлів, які були заповнені викладачами в базі даних для подальшого формування з них звітності кафедри.

Список літератури

1. Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика / Т. Коннолли, К. Бегг. – М.: Вильямс, 2003. – 421 с.
2. Пасічник, В.В. Організація баз даних та знань. / В.В. Пасічник, В.А. Резніченко. – К.: Видавнича група BHV, 2006. – 384 с.
3. Дейт К.Дж. Введение в системы баз данных, 8-е изд.: Пер. с англ. – М.: Издательский дом „Вильямс”, 2005. – 1328 с.
4. Тарасов, О.В. Проектування баз даних : навч. посіб. / О.В. Тарасов, В.В. Федько, М.Ю. Лосєв. – Х.: Вид, ХНЕУ, 2011. – 200 с.

РАЗРАБОТКА СИСТЕМЫ ДЛЯ ФОРМИРОВАНИЯ ОТЧЕТНОСТИ ПРО НАУЧНУЮ И МЕТОДИЧЕСКУЮ РАБОТУ КАФЕДРЫ

Е. Ю. Лебедева, Л.Н. Тимошенко, В.М. Семенченко

Одесский национальный политехнический университет
пр. Шевченко 1, Одесса, 65044, Украина; e-mail: whiteswanhl@yahoo.com

В работе разработано систему для формирования отчетности про научную и методическую работу кафедры. Спроектирована база данных для формирования отчетности кафедры в виде ER-диаграмм. Разработана система для формирования отчетности, которая автоматизирует получение входных данных с помощью excel-файлов.

Ключевые слова: база данных, разработка системы, отчетность про научную и методическую работу кафедры

DEVELOPMENT OF A SYSTEM FOR FORMING REPORTS ON THE SCIENTIFIC AND METHODOLOGICAL WORK OF THE DEPARTMENT

E. Lebedeva, L. Tymoshenko, V. Semchenko

Odessa National Polytechnic University
Shevchenko Avenue 1, Odessa, 65044, Ukraine; e-mail: whiteswanhl@yahoo.com

A system has been developed for the formation of reports on the scientific and methodical work of the department. A database was developed for the formation of the Department's reports in the form of ER-diagrams. A system has been developed for generating reports, which automates the receipt of input data using excel files.

Keywords: database, system development, reporting on the scientific and methodical work of the department

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 7, номер 1-2, 2017. Одеса – 151 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 7, номер 1-2, 2017. Одесса – 151 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 7, No. 1-2, 2017. Odesa – 151 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 №8 від 25.04.2017)

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, 2017