

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 6, № 1

Volume 6, No. 1

Одеса – 2016
Odesa – 2016

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:

А.Л. Іванова

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 - 6460P of 04.04.2011

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

Associate editor:

A.A. Kobozeva

Executive editor:

A.L. Ivanova

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, 2016

ЗМІСТ / CONTENTS

АЛГОРИТМ ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ, ОТРИМАНИХ З БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В.О. Хорошко, Н.А. Дуксенко	5	ALGORITHM FOR IMAGE RESTORATION OBTAINED FROM UNMANNED AERIAL VEHICLES Khoroshko V., Duksenko N.
ПЕРЕМІШУВАННЯ, ЯК СПОСІБ УПРАВЛІННЯ ХАОСОМ Д.В. Дмитришин, І.М. Скринник	11	MIXING AS A METHOD OF CHAOS CONTROL Dmitrichin D., Skrinnik I.
ПОБУДОВА ТРЬОХМОДУЛЬНОЇ МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ РОЗВ'ЯЗКУ КВАДРАТНОГО РІВНЯННЯ М.М. Касянчук	19	CONSTRUCTION OF THREE MODULAR MODIFIED PERFECT FORMS OF SYSTEM OF RESIDUAL CLASSES BASED SOLUTION OF QUADRATIC EQUATION Kasianchuk M.
ГІПОТЕЗА І ФОРМАЛЬНА МОДЕЛЬ СИНГУЛЯРНОЇ ДИНАМІКИ ІНЦИДЕНТІВ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ О.М. Герега, С.О. Гнатюк, В.Г. Кононович, І.В. Кононович	26	HYPOTHESIS AND FORMAL MODEL FOR SINGULAR DYNAMIC OF CYBERSECURITY INCIDENTS Herega O., Gnatyuk S., Kononovich V., Kononovich I.
ПОБУДОВА МІНІМАКСНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШТОК ПОРЯДКУ $N=6$ ДЛЯ БАГАТОКАНАЛЬНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ Н.І. Кушніренко, В.Я. Чечельницький, Л.А. Кузнецова	38	CONSTRUCTING OF MINIMAX CLASS OF PERFECT BINARY ARRAYS OF ORDER $N = 6$ FOR MULTI-CHANNEL CRYPTOGRAPHIC INFORMATION TRANSFER SYSTEM Kushnirenko N., Chechelnytskyi V., Kuznetsova L.
АНАЛІЗ МЕХАНІЗМУ ВИНИКНЕННЯ ПАРАЗИТНИХ ПРОЦЕСІВ В АПАРАТУРІ ЦИФРОВОГО ФОТО ТА ВІДЕОЗАПИСУ, ПРИДАТНИХ ДЛЯ ВИКОРИСТАННЯ ПРИ ЕКСПЕРТИЗИ ТАКИХ ПРИСТРОЇВ О.В. Рибальський, В.В. Журавель	46	THE ANALYSIS OF MECHANISM OF ORIGIN OF PARASITE PROCESSES IN AN APPARATUS IS DIGITAL PHOTO AND VIDEOTAPE RECORDING, SUITABLE FOR USING FOR TO EXAMINATION OF SUCH DEVICES Rybalsky O., Zhuravel V.

СТЕГАНОАНАЛІТИЧНИЙ
АЛГОРИТМ, ЗАСНОВАНИЙ НА
АНАЛІЗІ ПРОСТОРОВОЇ ОБЛАСТІ
ЦИФРОВИХ КОНТЕЙНЕРІВ
Д.А. Маєвський, Г.В. Ахмамет'єва

52

STEGANALYTIC ALGORITHM,
BASED ON THE ANALYSIS OF THE
SPATIAL DOMAIN OF DIGITAL
CONTAINERS
Maevsky D., Akhmamet'ieva A.

ІНФОРМАТИЗАЦІЯ ДИСТАНЦІЙНОГО
ДІАГНОСТУВАННЯ СТАНУ
СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ
С.Н. Коновалов, В.В. Вичужанін

61

INFORMATIZATION OF THE
CONTROLLED FROM DISTANCE
DIAGNOSTICATING OF THE STATE
OF THE DIFFICULT TECHNICAL
SYSTEMS
Konovalov S., Vychuzhanin V.

ПРОГНОЗУВАННЯ
НЕСАНКЦІОНОВАНОГО ДОСТУПУ З
ВИКОРИСТАННЯМ КАНОНІЧНОГО
ПРЕДСТАВЛЕННЯ ВЕКТОРНОГО
АПОСТЕРІОРНОГО ПРОЦЕСУ
І.Р. Опірський

71

UA PREDICTION USING CANONICAL
REPRESENTATION OF VECTOR
POSTERIORI
Opirskyy I.

ФРАКТАЛЬНИЙ АНАЛІЗ РЕОЛОГІЇ
БАГАТОКОМПОНЕНТНИХ ТА
ГЕТЕРОГЕННИХ ПЛАСТОВИХ
СИСТЕМ
С. А. Положаєнко,
Мухіалдін Хасан Моха

78

FRACTAL ANALYSIS OF REOLOGY
OF MULTICOMPONENT AND
HETEROGENEOUS STRATAL
SYSTEMS
Polozhaenko S.,
Muhialdin Hassan Moha

МОДИФІКАЦІЯ СТІЙКОГО ДО
ЗБУРНИХ ДІЙ
СТЕГАНОПЕРЕТВОРЕННЯ
ПРОСТОРОВОЇ ОБЛАСТІ
ЗОБРАЖЕННЯ-КОНТЕЙНЕРА
О.В. Костирка

85

MODIFICATION OF RESISTANCE TO
DISTURBANCE QUILTED
TRANSFORMATION OF SPATIAL
IMAGE CONTAINER
Kostyrka O.

АНАЛІЗ ЯКОСТІ ОЦІНЮВАННЯ
СТУДЕНТІВ В СИСТЕМАХ
КОМП'ЮТЕРИЗОВАНОЇ
ПІДГОТОВКИ ЗА ДОПОМОГОЮ
СТАТИСТИЧНИХ МЕТОДІВ
Т. І. Трояновська, М. А. Котолуп

94

ANALYSIS OF QUALITY OF
EVALUATION OF STUDENTS IN
SYSTEMS OF THE COMPUTERIZED
PREPARATION BY MEANS OF
STATISTICAL METHODS
Trojanovs'ka T., Kotolup M.

АЛГОРИТМ ВОССТАНОВЛЕНИЯ ИЗОБРАЖЕНИЙ, ПОЛУЧАЕМЫХ С БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

В.А. Хорошко, Н.А. Дуксенко

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

Рассматриваются вопросы, связанные с работой беспилотных летательных аппаратов (БПЛА) в условиях активного радиоэлектронного противодействия. Важным фактором работы БПЛА является восстановление переданного им изображения на землю. Предложен алгоритм, который для полученного изображения в результате обработки его рецепторного поля позволяет на каждую из фигур распространить свой обобщенный признак, причем он распространяется одновременно на все фигуры видеокартинки. Таким образом можно легко восстановить и отдельно выделить любое изображение из представленных на рецепторном поле, что позволяет распознать и классифицировать изображение в реальном масштабе времени.

Ключевые слова: беспилотный летательный аппарат, алгоритм восстановления, видеоизображение, рецепторное поле

Введение

Широкое применение беспилотных летательных аппаратов (БПЛА) для проведения разведывательных операций различного назначения поставило большое количество вопросов, на которые необходимо отвечать:

- какую систему видеонаблюдения следует использовать?
- как работать в условиях активного применения различных типов помех?
- как обрабатывать изображения, получаемые с БПЛА?

В последнее время все большее распространение получают цифровые, а не аналоговые системы видеонаблюдения. С одной стороны, за последние годы компьютерные технологии сделали качественный скачок в своем развитии, и в настоящее время цифровые системы видеонаблюдения, как по техническим, так и по ценовым характеристикам теснят аналоговые. С другой стороны, современные комплексы разведки и наблюдения все больше начинают напоминать интегрированные распределенные сетевые системы, где устаревшему аналоговому оборудованию видеоразведки все труднее качественно и эффективно выполнять свои функциональные обязанности [1,2,3] и по качеству видеоотображения, и по реально достигаемому разрешению канала записи/воспроизведения, и по удобству формирования и дальнейшего оперативного использования видеоархива в режиме триплекса (одновременного видеоотображения, записи и просмотра видеоархива). Кроме того, современное цифровое оборудование видеоконтроля по своим характеристикам все больше приближается к современным интеллектуальным компьютерным системам, что позволяет строить очень гибкую политику обеспечения разведанными, приближенную по своим функциям к механизмам принятия решения, близким к человеческой логике. Именно поэтому некоторые из современных цифровых систем видеоконтроля по праву можно назвать интеллектуальными, а их возможности не могут быть реализованы в полной мере никаким аналоговым оборудованием видеоконтроля.

В статье рассматриваются вопросы, связанные с работой БПЛА в условиях активного радиоэлектронного противодействия.

Очень важным фактором работы БПЛА является восстановление изображения. Эта процедура, связанная с концепцией распознавания сложных изображений, заключается в том, что сложное изображение разделяется на простые фигуры, а затем анализируются взаимоположения отдельных фигур. Анализ таких взаимоположений позволяет составлять трехмерное описание изображения, представленное двухмерным сложным изображением, и складывается из процесса нахождения общих контурных линий отдельных фигур, разметки вершин и линий, объединения фигур в объекты.

Целью работы является разработка алгоритма обработки рецепторного поля, позволяющего восстанавливать и отдельно выделять любое изображение, представленное на рецепторном поле.

Основная часть

Метод восстановления несвязанных объектов основывается на использовании понятия общих отрезков [4]. Эта задача является весьма важной при распознавании видеоизображений в условиях помех.

Рассмотрим возможность восстановления изображения объекта для его последующего анализа.

Отрезком p будем называть последовательность идущих подряд элементов. Отрезок, принадлежащий изображению объекта, на любой строке рецепторного поля характеризуется координатами левой и правой точек или длиной отрезка и одной из координат. На любой строке может находиться несколько отрезков, причем некоторые из них могут принадлежать одному объекту, а некоторые – другому, либо все отрезки принадлежат разным объектам [5].

Пусть на рецепторном поле R размерностью $n \times n$ имеется сложное изображение, которое представляется уровнем яркости:

$$G^* = \{\tilde{m}_0, \tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_m\},$$

где $\tilde{m}_s$ – уровень яркости, $0 \leq s \leq m$; $\tilde{m}_0$ – уровень фона.

Определение 1. Сегментом $R_{ks}(i)$ назовем i -ю последовательность элементов уровня яркости $\tilde{m}_s$ на k -той строке.

В свете определения 1 фигура рассматривается как совокупность перекрывающихся по вершинам сегментов. Множество сегментов на k -той строке по каждому уровню яркости представляет собой k -ю строку рецепторного поля:

$$R_k = \bigcup_s \bigcup_i R_{ks}(i);$$

$$i = \overline{1, I_{ks}}; s = \overline{1, m}; k = \overline{1, n},$$

где I_{ks} – общее число сегментов s -й градации яркости на k -той строке.

Для характеристики отрезка p некоторой строки, принадлежащей объекту, кроме координат вводится понятие «список признаков PR».

Определение 2. Каждому сегменту $R_{ks}(i)$ ставится в соответствие по заданным правилам список признаков $PR_{ks}(i)$, элементы которого являются признаками алфавита признаков для каждой градации:

$$R_{ks}(i) \rightarrow PR_{ks}(i) = \{a_x^s, a_y^s, a_z^s, \dots\};$$

$$a_x^s, a_y^s, a_z^s \in A_s = \{a_x^s, a_y^s, a_z^s, \dots\},$$

где A_s – алфавит с бесконечным числом элементов (например, натуральный ряд чисел).

В результате образуются пары: $S_{ks}^i = \{R_{ks}(i), PR_{ks}(i)\}$.

Определение 3. Классом s -й градации k -й строки называются пары s -й градации на k -й строке:

$$K_{ks} = \{S_{ks}^1, S_{ks}^2, S_{ks}^3, \dots, S_{ks}^{I_{ks}}\}.$$

Определение 4. Классом k -й строки называются классы градаций k -й строки:

$$K_k = \{K_{k1}, K_{k2}, K_{k3}, \dots, K_{km}\},$$

где условие $K_{ks} = 0$ обозначает, что на k -й строке нет ни одного сегмента s -й градации.

Определение 5. Общим классом поля называются классы строк:

$$K = \{K_1, K_2, K_3, \dots, K_n\}.$$

Будем считать, что на первой и n -й строках имеется хотя бы по одному сегменту любой градации, т.е. $K_1 \neq 0$ и $K_n \neq 0$; в противном случае можно отбросить пустые строки и обрабатывать остальные.

В списке признаков $PR_{ks}(i)$ признаки a_x^s из алфавита A_s будут записываться по следующему алгоритму. На первой строке ($k \neq 1$) каждому сегменту s -й градации последовательно присваиваются признаки из алфавита A_s по всем s , для которых есть сегменты на первой строке:

$$k = 1; s = \overline{1, m}; PR_{1s}(i) = a_i^s \in A_s, i = \overline{1, I_{1s}}. \quad (1)$$

Для $1 < k \leq n$ проводим сравнения по классам $K_{k-1,s}$ и K_{ks} между сегментами $R_{k-1,s}(j)$ и $R_{ks}(i)$ на перекрытие по вертикали сегментов двух смежных строк:

$$1 < k \leq n; s = \overline{1, m}; e_{ij} = R_{k-1,s}(j) \wedge R_{ks}(i); E_i = \bigvee_j e_{ij}; j = \overline{1, i_{k-1,s}}; \quad (2)$$

$$PR_{ks}(i) = \begin{cases} PR_{ks}(i) \oplus PR_{k-1,s}(j) & \text{по тем } j, \text{ для которых } e_{ij} = 1 \\ E_i = 0 \vee K_{k-1,s} = 0, & \end{cases}$$

где $\wedge, \vee$ – обычные логические операции конъюнкции и дизъюнкции; операция $\oplus$ означает дополнение из $PR_{k-1,s}(j)$ в $PR_{ks}(i)$ признаков, которых нет в $PR_{ks}(i)$; a_f^s – очередной признак из A_s (очередной – следующий после последнего выбранного признака, $f \in \{1, 2, 3, \dots\}$).

После присвоения признаков всем сегментам последней строки ($k = n$) поля R необходимо провести замену списков признаков обобщенными признаками из алфавита обобщенных признаков $\tilde{A}_s = \{\tilde{a}_1^s, \tilde{a}_2^s, \tilde{a}_3^s, \dots\}$, так как при обработке изображения от первой строки до последней происходит «накапливание» признаков в списках признаков сегментов одного и того же объекта. Поэтому замена списков признаков обобщенными признаками производится от n -й строки до первой.

При $k = n$ по $s = \overline{1, m}$ для классов $K_{nk} \neq 0$ производится замена первых списков признаков каждой градации обобщенными признаками:

$$i = 0, PR_{ks}(1) = \{a_x^s, a_y^s, a_z^s, \dots\} = a_1^s \in \tilde{A}_s. \quad (3)$$

Затем сравниваем последовательно списки признаков той же строки, осуществляя поиск хотя бы одного одинакового признака в списках признаков. Если такой признак имеется, то список признаков заменяется тем же обобщенным признаком, который был присвоен сравниваемому списку признаков. Если же такого признака нет, то списку признаков присваивается очередной обобщенный признак:

$$k = n, s = \overline{1, m}, K_{nk} \neq 0, i = \overline{2, I_{ns}}, \tilde{e}_{ir} = PR_{ns}(i) \cap PR_{ns}(r); \quad (4)$$

$$\tilde{E}_i = V_r \tilde{e}_{ir}, r = \overline{1, i-1}, PR_{ns}(i) = \begin{cases} \tilde{a}[PR_{ns}(r)], \tilde{e}_{ir} = 1; \\ \tilde{a}_f^s, \tilde{E}_i = 0 \end{cases}, \quad (5)$$

где логическая операция сравнения $\tilde{e}_{ir} = PR_{ns}(i) \cap PR_{ns}(r)$ может быть представлена как поразрядное произведение, в котором единица в первом разряде означает наличие признака $a_s^s (a_s^s \in A_s)$, а ноль – его отсутствие; $\tilde{e}_{ir} = 1$, если хотя бы в одном одинаковом разряде $PR_{ns}(i)$ и $PR_{ns}(r)$ имеется единица, и $\tilde{e}_{ir} = 0$, если нет ни одного такого разряда; операция присваивания $PR_{ns}(i) = \tilde{a}[PR_{ns}(r)]$ означает, что списку признаков $PR_{ns}(i)$ присваивается тот же обобщенный признак, который был присвоен списку признаков $PR_{ns}(r)$, а $\tilde{a}_f^s$ – очередной признак из $\tilde{A} (f \in \{1, 2, 3, \dots\})$.

После окончания процедуры присваивания на последней строке переходим к сравнению списков признаков s -й градации $(n-1)$ -й строки со списками признаков n -й строки. При наличии хотя бы одного одинакового признака обобщенный признак, присваиваемый списку n -й строки, присваивается и списку $(n-1)$ -й строки, при отсутствии такого сравниваем списки признаков последовательно (s) на $(n-1)$ -й строке (как и на n -й строке). Для строк k и $k+1$ рассуждения аналогичны:

$$1 \leq k \leq n; s = \overline{1, m}; K_{ks} \neq 0, K_{k+1,s} \neq 0, \quad (6)$$

$$\tilde{e}_{ij}^k = PR_{ks}(i) \cap PR_{k+1,s}(j); \tilde{E}_i^k = V_j \tilde{e}_{ij}^k; j = \overline{1, I_{k+1,s}};$$

Если $\tilde{E}_i^k = 0$, то необходимо провести следующие вычисления:

$$\tilde{e}_{ir} = PR_{ks}(i) \cap PR_{ks}(r); \tilde{E}_i = V_r \tilde{e}_{ir}; r = \overline{1, i-1}; \quad (7)$$

$$PR_{ks}(i) = \begin{cases} \tilde{a}[PR_{k+1,s}(j)], \tilde{e}_{ij}^k = 1; \\ \tilde{a}[PR_{ks}(r)], \tilde{E}_i^k = o \wedge \tilde{e}_{ir} = 1; \\ \tilde{a}_j^s, \tilde{E}_i^k = o \wedge \tilde{E}_i = 0 \end{cases} \quad (8)$$

Если $K_{l+1,s_1} = 0 (1 < l < n, s_1 \in s)$, то для $K_{l,s_1} \neq 0$ присваивается очередной признак и для $PR_{l,s_1}(i) (i = \overline{2, I_{l,s_1}})$ проводятся замены обобщенными признаками по формуле (7). Если провести обобщение для формул (1)-(2) и (3)-(8), то получим следующее:

1 этап:

$$k = \overline{1, n}, s = \overline{1, m}, e_{ij} = R_{k-1,s}(j) \wedge R_{ks}(i); \quad (9)$$

$$PR_{ks}(i) = \begin{cases} a_i^s, k=1 \\ PR_{ks}(i) \oplus PR_{k-1,s}(j) \text{ по тем, для которых } e_{ij} = 1; \\ a_i^s, E_i = O \vee K_{k-1,s} = 0; \end{cases} \quad (10)$$

2 этап:

$$k = \overline{n, 1}, s = \overline{1, m};$$

$$\tilde{e}_{ij}^k = PR_{ks}(i) \cap PR_{k-1,s}(j); \quad (11)$$

$$\tilde{E}_i^k = \bigvee_j \tilde{e}_{ij}^k, j = \overline{1, I_{k+1,s}};$$

$$\tilde{e}_{ir} = PR_{ks}(i) \cap PR_{ks}(r); \quad (12)$$

$$\tilde{E}_i = \bigvee_r \tilde{e}_{ir}, r = \overline{1, i-1};$$

$$PR_{ks}(i) = \begin{cases} \tilde{a}[PR_{k+1,s}(j)], \tilde{e}_{ij}^k = 1; \\ \tilde{a}[PR_{ks}(r)], \tilde{E}_i^k = O \wedge \tilde{e}_{ir} = I \vee K = n \wedge \tilde{e}_{ir} = 1; \\ \tilde{a}_f^s, \tilde{E}_i^k = O \wedge \tilde{E}_i = O \vee K_{k+1,s} = O \wedge i = 1; \\ \vee K_{k+1,s} = O \wedge \tilde{E}_i = 0; \\ \vee K = n \wedge i = 1; \\ \vee K = n \wedge \tilde{E}_i = 0 \end{cases} \quad (13)$$

Упрощая логические условия в выражении (13) получаем:

$$PR_{ks}(i) = \begin{cases} \tilde{a}[PR_{k+1,s}(j)], \tilde{e}_{ij}^k = 1; \\ \tilde{a}[PR_{ks}(r)], (\tilde{E}_i^k = O \vee K = n) \wedge \tilde{e}_{ir} = 1; \\ \tilde{a}_f^s, \tilde{E}_i^k = \wedge \tilde{E}_i = O \vee (K_{k+1,s} = O \wedge K = n) \wedge (i = I \wedge E_i = 0) \end{cases} \quad (14)$$

Следует отметить, что на первом этапе обработки – (9), (10) – анализируются сегменты на перекрытие по вертикали, а на втором – (11) – (14) списки признаков на наличие одинаковых признаков. Каждому сегменту одной и той же фигуры будет присвоен один и тот же обобщенный признак, но свой для данной фигуры, так как перекрывающимся сегментам присваиваются одинаковые признаки в списке признаков, последние же заменяются одним обобщенным признаком, поскольку имеют хотя бы по одному одинаковому признаку.

Выводы

В результате обработки рецепторного поля по предложенному алгоритму на каждую из фигур распространяется свой обобщенный признак, причем он распространяется одновременно на все фигуры видеокартинки.

Таким образом, можно легко восстановить и отдельно выделить любое изображение, представленное на рецепторном поле, построить алгоритм, дающий

возможность анализировать каждое отдельно взятое изображение, поступающее с борта БПЛА, и тем самым восстанавливать и выделять интересное оператора изображение или часть изображения, а также изображения, которые являются помехами при применении средств радиоэлектронного противодействия. Этот подход может быть эффективно использован для обработки изображений в цифровых системах видеонаблюдения беспилотников для распознавания и классификации изображений в реальном масштабе времени.

Список литературы

1. Браиловский, Н.Н. Особенности распознавания изображений в цифровых системах видеонаблюдения / Н.Н. Браиловский, С.В. Моржов, В.А. Хорошко, Д.В. Чирков // Радиотехника. – 2004. – Вып.139. – С. 77 – 82.
2. Колпаков, А. Критерии сравнения и выбор цифровых систем видеоконтроля. Часть 1 / А. Колпаков // Бизнес и безопасность. – 2001. – №4. – С. 14 – 20.
3. Колпаков, А. Критерии сравнения и выбора цифровых систем видеоконтроля. Часть 2 / А. Колпаков // Бизнес и безопасность. – 2001. – №6. – С. 10 – 18.
4. Graham, R.L. Bounds on multiprocessing timing anomalies / R.L. Graham // SIAM J. Appl. Math. – 2009. – №2. – P. 416 – 429.
5. Attneave, F. Some informational aspects in visual perception / F. Attneave // Psychol. Rev. – 2000. – P. 23 – 29.

АЛГОРИТМ ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ, ОТРИМАНИХ З БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

В.О. Хорошко, Н.А. Дуксенко

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

У роботі розглядаються питання, пов'язані з роботою безпілотних літальних апаратів (БПЛА) в умовах активної радіоелектронної протидії. При цьому важливим фактором роботи БПЛА є відновлення переданого ними зображення на землю. Це зображення в результаті обробки його рецепторного поля за допомогою запропонованого алгоритму дозволяє на кожну з фігур поширити свій узагальнену ознаку, причому вона поширюється одночасно на всі фігури відеокартинки. Таким чином можна легко відновити і окремо виділити будь-яке зображення з представлених на рецепторном полі, що дозволяє розпізнати і класифікувати зображення в реальному масштабі часу.

Ключові слова: безпілотний літальний апарат, алгоритм відновлення, відеозображення, рецепторне поле

ALGORITHM FOR IMAGE RESTORATION OBTAINED FROM UNMANNED AERIAL VEHICLES

V.O. Khoroshko, N.A. Duksenko

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

In this paper, issues related to the operation of unmanned aerial vehicles (UAVs) in the conditions of active electronic countermeasures are discussed. An important factor in UAV's work is to restore the image which it gives on the ground. In consequence of processing the receptor field of this image using proposed algorithm allows for each of the figures to extend its generic feature, and it is distributed its generic feature and it is distributed simultaneously to all the pieces of a video image. Thus, it is possible to easily recover and isolate separately from any image presented on the receptor field, which allows to recognize and classify the image in real time.

Keywords: unmanned aerial vehicle, recovery algorithm, video image, receptor field

ПЕРЕМЕШИВАНИЕ КАК СПОСОБ УПРАВЛЕНИЯ ХАОСОМ

Д.В. Дмитришин, И.М. Скринник

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

В статье рассматривается возможность управления динамикой нелинейных дискретных систем. Предложен новый способ управления хаосом через перемешивания состояний системы (или функций от этих состояний), вычисленных в предыдущий момент времени. Это позволяет локально стабилизировать наперед неизвестные циклы заданной длины. Как частный случай, этот способ включает в себя метод стабилизации цикла при помощи нелинейной запаздывающей обратной связи. Приведены примеры.

Ключевые слова: нелинейные дискретные системы, управление хаосом, перемешивание состояний системы.

Введение

Проблема оптимального воздействия на хаотический режим является одной из фундаментальных в нелинейной динамике. Целью таких воздействий являются синхронизация хаотических движений или, наоборот, хаотизация регулярных движений. Кроме того, в теории управления нелинейными системами считают допустимыми лишь малые управления, которые, тем не менее, полностью изменяют характер движения. Известны разнообразные подходы к построению систем управления хаосом [1-13], каждый из которых имеет существенные недостатки [14]. Поэтому задача разработки новых методов управления хаосом является актуальной.

В статье предлагается новый метод решения задачи оптимальной стабилизации циклов в семействах дискретных автономных систем, а именно, метод, использующий процедуру перемешивания предыдущих состояний системы или функций этих состояний. В частных случаях метод перемешивания совпадает с управлением по принципу запаздывающей обратной связи [2, 15, 16].

Цель работы состоит в построении алгоритмов подавления хаоса в нелинейных дискретных системах, основанных на новых для рассматриваемого в работе класса задач физических принципах.

Задача состоит в выборе структуры и параметров системы управления, при которых наперед неизвестные циклы заданной длины были бы локально асимптотически устойчивыми.

Постановка задачи и предварительные результаты

Рассматривается векторная нелинейная дискретная система, которая при отсутствии управления имеет вид

$$x_{n+1} = f(x_n), \quad x_n \in R^H, \quad n = 1, 2, \dots, \quad (1)$$

12

Подставим решение (4) в (3), считая, что в окрестности цикла величины $u_m^1, \dots, u_m^T$ малы настолько, что выполняются условия теоремы об устойчивости по первому приближению [1].

Пусть $n = Tm$. Тогда $x_{n+1} = x_{Tm+1} = \eta_2 + u_m^2$, $x_{n+2} = x_{Tm+2} = \eta_3 + u_m^3$, $\dots$, $x_{n+T} = x_{T(m+1)} = \eta_1 + u_{m+1}^1$.

Выделяя линейную часть и учитывая, что $\eta_1 = f(\eta_2), \dots, \eta_T = f(\eta_1)$, получаем

$$\begin{aligned} u_m^2 &= f'(\eta_1)(a_1 u_m^1 + \dots + a_N u_{m-N+1}^1) \\ u_m^3 &= f'(\eta_2)(a_1 u_m^2 + \dots + a_N u_{m-N+1}^2) \\ &\vdots \\ u_m^T &= f'(\eta_T)(a_1 u_m^{T-1} + \dots + a_N u_{m-N+1}^{T-1}) \\ u_{m+1}^1 &= f'(\eta_1)(a_1 u_m^T + \dots + a_N u_{m-N+1}^T) \end{aligned} \quad (5)$$

где

$$a_i = \sum_{j=1}^M \alpha_{ij} \gamma_j, i = 1, \dots, N, \quad (6)$$

Система (5) линейная, поэтому ее решения представляются в виде
$$\begin{pmatrix} u_m^1 \\ \dots \\ u_m^T \end{pmatrix} = \begin{pmatrix} c_1 \\ \dots \\ c_T \end{pmatrix} \lambda^m,$$

где λ - комплексное число, подлежащее определению из системы

$$\begin{pmatrix} -f'(\eta_1) \cdot p(\lambda^{-1}) & I & 0 & \dots & 0 & 0 \\ 0 & -f'(\eta_2) \cdot p(\lambda^{-1}) & I & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -f'(\eta_{T-1}) \cdot p(\lambda^{-1}) & I \\ \lambda I & 0 & 0 & \dots & 0 & -f'(\eta_T) \cdot p(\lambda^{-1}) \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_{T-1} \\ c_T \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 0 \end{pmatrix}, \quad (7)$$

В (7) $f'(\eta_j)$, $j=1, \dots, T$, - матрицы Якоби, I - единичная матрица, O - нулевая матрица (все матрицы размерности H), $p(\lambda^{-1}) = (a_1 + a_2 \lambda^{-1} + \dots + a_N \lambda^{-N+1})$.

Стандартная методика исследования устойчивости T -цикла заключается в проверке расположения всех нулей определителя матрицы системы (7) в центральном единичном круге комплексной плоскости $\Delta = \{z : |z| < 1\}$. В рассматриваемом случае определитель матрицы системы (7) равен

$$\det \left((-1)^{T-1} \lambda I + \prod_{j=1}^T (-f'(\eta_j) p(\lambda^{-1})) \right) = \det \left(\lambda I - (p(\lambda^{-1}))^T \prod_{j=1}^T f'(\eta_j) \right) = \prod_{j=1}^H (\lambda - \mu_j (p(\lambda^{-1}))^T),$$

где $\mu_1, \dots, \mu_H$ — собственные значения матрицы $\prod_{i=1}^T f'(\eta_j)$.

Задача оптимального перемешивания

Условие устойчивости T - цикла системы (2) состоит в том, что все корни уравнения

$$\prod_{j=1}^N \left(\lambda^{(N-1)T} - \mu_j (a_1 \lambda^{N-1} + \dots + a_N) \right)^T = 0, \quad (8)$$

должны лежать в центральном единичном круге комплексной плоскости. Соответственно, задача управления хаосом в системе (1) путем перемешивания значений состояния системы и функций от этих значений в предшествующие моменты времени формулируется следующим образом: для заданной длины цикла T и заданного множества локализации мультипликаторов найти коэффициенты внутреннего перемешивания α_{ij} , $i=1, \dots, N$, $j=1, \dots, M$, и внешнего перемешивания γ_j , $j=1, \dots, M$, так, чтобы цикл длины T был бы локально асимптотически устойчивым; при этом величина используемой предыстории должна быть минимально возможной.

Другими словами, в уравнении (8) необходимо найти коэффициенты $a_1, \dots, a_N$ так, чтобы все корни этого уравнения лежали бы в центральном единичном круге комплексной плоскости, и величина N была бы минимально возможной.

Естественно, что решение поставленной задачи зависит от области локализации мультипликаторов $\{\mu_1, \dots, \mu_N\}$. Будем рассматривать две возможности: все мультипликаторы вещественны $\{\mu_1, \dots, \mu_N\} \subset \{\mu \in \mathbb{R} : \mu \in (-\mu^*, 1)\}$; все мультипликаторы принадлежат левой полуплоскости $\{\mu_1, \dots, \mu_N\} \subset \{\mu \in \mathbb{C} : |\mu + R| < R\}$, $\mu^* > 1$, $R > 1/2$. Для каждого из этих случаев алгоритм нахождения минимального N и оптимальных коэффициентов $\{a_1, \dots, a_N\}$ состоит из следующих шагов [19].

- вычисляются узлы: $\psi_j = \frac{\pi(\sigma + T(2j-1))}{\sigma + (N-1)T}$, $j=1, 2, \dots, \frac{N-2}{2}$, если N – четное, $j=1, 2, \dots, \frac{N-1}{2}$, если N – нечетное; при этом в случае $\{\mu_1, \dots, \mu_N\} \subset \{\mu \in \mathbb{R} : \mu \in (-\mu^*, 1)\}$ следует полагать $\sigma = 2$, а в случае $\{\mu_1, \dots, \mu_N\} \subset \{\mu \in \mathbb{C} : |\mu + R| < R\}$ – $\sigma = 1$;

- строятся полиномы $\eta_N(z) = z(z+1) \prod_{j=1}^{\frac{N-2}{2}} (z - e^{i\psi_j}) (z - e^{-i\psi_j})$, если N – четное, $\eta_N(z) = z \prod_{j=1}^{\frac{N-1}{2}} (z - e^{i\psi_j}) (z - e^{-i\psi_j})$, если N – нечетное;

- вычисляются коэффициенты полинома $\eta_N(z) = \sum_{j=1}^N c_j z^j$;

- определяются оптимальные коэффициенты $a_j = \frac{\left(1 - \frac{1+(j-1)T}{2+(N-1)T}\right) c_j}{\sum_{j=1}^N \left(1 - \frac{1+(j-1)T}{2+(N-1)T}\right) c_j}$,

$j=1, \dots, N$;

- в случае $\{\mu_1, \dots, \mu_N\} \subset \{\mu \in \mathbb{R} : \mu \in (-\mu^*, 1)\}$ вычисляются величины

$$I_N^{(T)} = \left[\frac{T}{2+(N-1)T} \prod_{k=1}^{\frac{N-2}{2}} \operatorname{ctg}^2 \frac{\pi(2+T(2j-1))}{2(2+(N-1)T)} \right]^T \text{ при } N - \text{четном},$$

$$I_N^{(T)} = \left[\prod_{k=1}^{\frac{N-1}{2}} \text{ctg}^2 \frac{\pi(2+T(2j-1))}{2(2+(N-1)T)} \right]^T \quad \text{при } N - \text{нечетном; оптимальное значение } N$$

вычисляется, как минимальное натуральное число, удовлетворяющее неравенству

$$\mu^* \leq \frac{1}{|I_N^{(T)}|};$$

▪ в случае $\{\mu_1, \dots, \mu_H\} \subset \{\mu \in C : |\mu + R| < R\}$ вычисляются величины

$$I_N^{(T)} = \left[\frac{T}{1+(N-1)T} \prod_{k=1}^{\frac{N-2}{2}} \text{ctg}^2 \frac{\pi(1+T(2j-1))}{2(1+(N-1)T)} \right]^T \quad \text{при } N - \text{четном,}$$

$$I_N^{(T)} = \left[\prod_{k=1}^{\frac{N-1}{2}} \text{ctg}^2 \frac{\pi(1+T(2j-1))}{2(1+(N-1)T)} \right]^T \quad \text{при } N - \text{нечетном; оптимальное значение } N$$

вычисляется, как минимальное натуральное число, удовлетворяющее неравенству

$$R \leq \frac{1}{2|I_N^{(T)}|}.$$

Если оптимальные коэффициенты найдены, то коэффициенты перемешивания можно найти из системы (6), которую удобно представить в матричной форме:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1M} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2M} \\ \dots & \dots & \dots & \dots \\ \alpha_{N1} & \alpha_{N2} & \dots & \alpha_{NM} \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \dots \\ \gamma_M \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_N \end{pmatrix}. \quad (9)$$

К системе (9) необходимо добавить условия нормировки, тогда она примет вид:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1M} \\ \dots & \dots & \dots & \dots \\ \alpha_{N-1,1} & \alpha_{N-1,2} & \dots & \alpha_{N-1,M} \\ 1 & 1 & \dots & 1 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \dots \\ \dots \\ \gamma_M \end{pmatrix} = \begin{pmatrix} a_1 \\ \dots \\ a_{N-1} \\ 1 \end{pmatrix}.$$

Заметим, что оптимальные коэффициенты определяются единственным образом, однако коэффициенты перемешивания не обязательно определяются единственным образом.

Оптимальная стабилизация хаоса

$$\text{Рассмотрим отображение [20] } f(x) = (1 + \sqrt{2}) \left(\frac{1}{2} - \left| x - \frac{1}{2} \right| \right) + x,$$

порождающее динамическую систему «внезапного возникновения хаоса» (SOC).

$$x_{n+1} = f(x_n), \quad (10)$$

В [20] для стабилизации (нахождения) циклов длин от 1 до 6 было использовано прогнозирующее управление [3]. Ниже иллюстрируется применение метода перемешивания для стабилизации 3-цикла (рис. 1), 7-циклов (рис. 2) в системе SOC.

Для системы (10) инвариантным является множество $\left[0, 1 + \frac{\sqrt{2}}{2}\right]$; положением

равновесия – точка $z = 1$.

Найдем 3-цикл системы (10). Для этого рассмотрим систему управления

$$x_{n+1} = f \left(f \left(f \left(\sum_{j=1}^N a_j x_{n-jT+T} \right) \right) \right) \quad (11)$$

при $T = 1$, $N = 8$, $\{a_1, \dots, a_8\} = \{0.107, 0.176, 0.204, 0.193, 0.154, 0.102, 0.050, 0.013\}$.

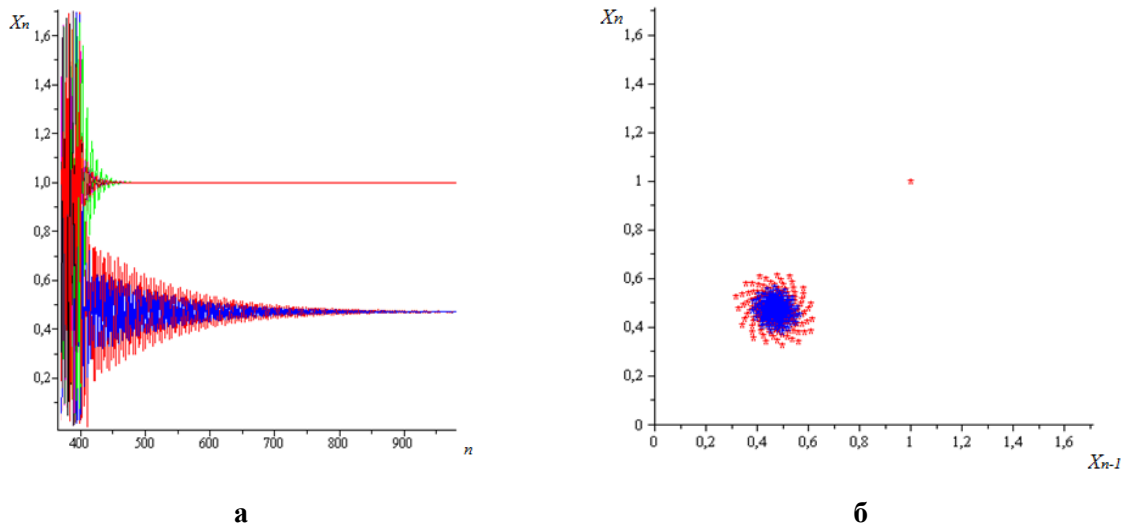


Рис. 1. Динамика решений системы (11); а – в плоскости (n, x_n) ; б – в плоскости (x_{n-1}, x_n)

Видно, что в системе (11) имеется два положения равновесия: $z_1 = 1$ и $z_2 \approx 0.471$. Первое положение равновесия является положением равновесия и для исходной системы (10), а вот второе – определяет 3-цикл системы (10): $\{0.471, 1.609, 0.138\}$.

Аналогично находим 7-цикл системы (10). Систему управления

$$x_{n+1} = f \left(f \left(f \left(f \left(f \left(f \left(\sum_{j=1}^N a_j x_{n-jT+T} \right) \right) \right) \right) \right) \right), \quad (12)$$

используем при $T = 1$, $N = 12$,

$\{a_1, \dots, a_{12}\} = \{0.054, 0.095, 0.124, 0.138, 0.139, 0.130, 0.111, 0.087, 0.061, 0.037, 0.017, 0.004\}$.

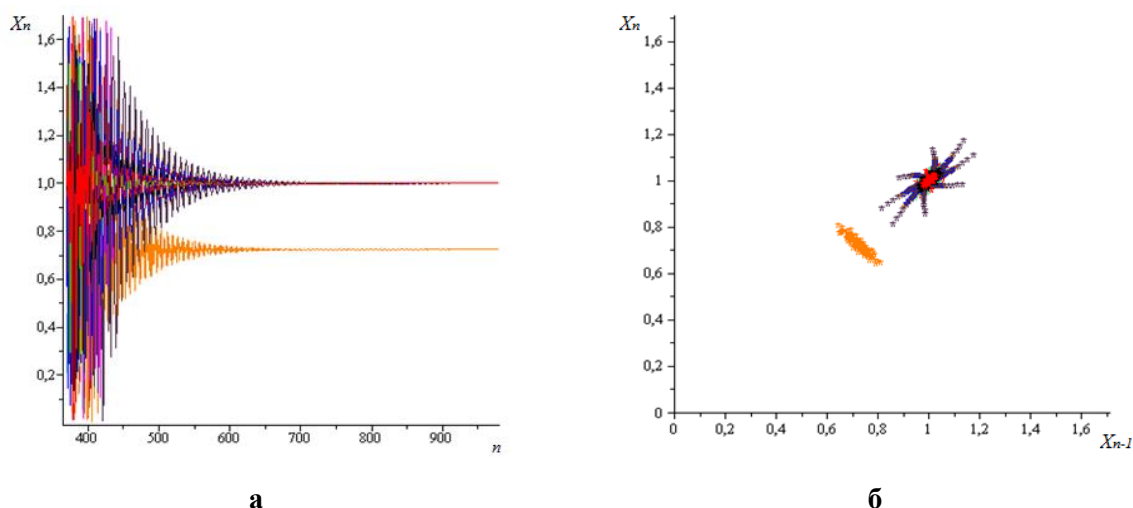


Рис. 2. Динамика решений системы (12); а – в плоскости (n, x_n) ; б – в плоскости (x_{n-1}, x_n)

Положение равновесия в системе (12) $z \approx 0.723$ определяет искомый 7-цикл системы (10): $\{0.723, 1.391, 0.448, 1.529, 0.252, 0.862, 1.195\}$.

Заключение

В статье рассмотрена актуальная проблема стабилизации наперед не известных неустойчивых периодических орбит дискретных систем с хаотической динамикой. Подход для решения задачи стабилизации связан с использованием системы управления, построенной на перемешивании координат предыстории или функций этих координат. Этот подход обобщает предложенный в [14, 15] метод стабилизации с использованием нелинейной запаздывающей обратной связи (DFC). Он сохраняет все преимущества метода DFC и дает дополнительные возможности выбора параметров перемешивания, что чрезвычайно важно для нелинейных систем, позволяя расширять бассейны притяжения стабилизируемых периодических орбит. Также использование внутреннего перемешивания существенно сокращает объем вычислений, т.к. отпадает необходимость вычислять значение функции, которая задает динамическую систему, большее число раз, чем в системе без перемешивания. Также мы надеемся, что использование внутреннего перемешивания облегчит физическую реализацию предложенной схемы управления хаосом в нелинейных дискретных системах.

Список литературы

1. Ott, E. Controlling chaos Phys. Rev. / E. Ott, C. Grebogi, J.A. Yorke. – 1990. - Lett. 64. - P. 1196 - 1199.
2. Vieira, D.S. Controlling chaos using nonlinear feedback with delay / D.S. Vieira, A.J. Lichtenberg, // Phys.Rev. – 1996. - E 54. – PP. 1200 – 1207.
3. Polyak, B.T. Stabilizing chaos with predictive control. Automation and Remote Control.66(11) / B.T. Polyak. – 2005. – PP. 1791 - 1804.
4. Morgul, O. On the stability of delayed feedback controllers / O. Morgul // Phys. - 2003. - Lett. A 314. – PP. 278 – 285.
5. Pyragas, K. Delayed feedback control of chaos / K. Pyragas // Phil. Trans. R. Soc. A 364. – 2006. – No.1846, PP. 2309 – 2334.
6. Calvo, O. Fuzzy control of chaos /International Journal of Bifurcation and Chaos / O. Calvo, J. H. Cartwright. - 1998. - Vol.8. –No.8. - PP. 1743 – 1747.

7. Wu, X.Q. Parameter identification and backstepping control of uncertain Lu system, *Chaos, Solitons, Fractals* 18 / X.Q. Wu, J.A. Lu. – 2003. – PP. 721 - 729.
8. Lima, R. Supression of chaos by resonant parametric perturbation. / R. Lima, M. Pettini // *Phys. – 1990. - Rev. A, 41: PP. 726 – 733.*
9. Astrom, K.J. Adaptive control. Dover Publications / K.J. Astrom, B. Wittenmark // INC. Mineola, N.-Y. - 578 p.
10. Wang, H. O. Fuzzy modeling and control of chaotic systems / H. O. Wang, K. Tanaka, T. Ikeda // *Proc. IEEE Int. Symp. Circuits and Systems. – 1996. - Vol.3. - PP. 209 - 212.*
11. Kokame, H. Difference feedback can stabilize uncertain steady states / H. Kokame, K. Hirata, K. Konishi, T. Mori // *IEEE Trans. on Automatic Control. - 2001. - Vol.46. - No.12. - PP. 1908 - 1913.*
12. Zelinka, I. Motivation for Application of Evolutionary Computation to Chaotic Systems. *Evolutionary Algorithms and Chaotic Systems* / I. Zelinka, G. Chen // Springer., series Studies in Computational Intelligence. – 2000. – Vol.267. - PP. 3 - 36.
13. Gauthier, D. J. / Resource letter / D. J. Gauthier // *Controlling chaos, Am. J. Phys. – 2003. – 71 p.*
14. Андриєвський, Б.Р. Управление хаосом: методы и приложения, часть I / Б.Р. Андриєвський, А.Л. Фрадков // *АиТ. – 2003. – Т.5. – С. 3-45.*
15. Dmitrishin, D. Methods of harmonic analysis in nonlinear dynamics / D. Dmitrishin, A. Khamitova // *Comptes Rendus Mathematique. - 2013. - Vol.351. – PP. 367 - 370.*
16. Dmitrishin, D. Fejer polynomials and Chaos / D. Dmitrishin, A. Khamitova, A. Stokolos // *Springer Proceedings in Mathematics and Statistics. – 2014. - PP. 49 - 75.*
17. Dmitrishin, D. On the stability of cycles by delayed feedback control / D. Dmitrishin, P. Hagelstein, A. Khamitova, A. Stokolos // *arXiv:1501.04573. Published online in Linear and multilinear Algebra. – 2014. – 256 p.*
18. Khamitova, A. About the characteristic polynomial of product Frobenius' matrix, *Visnyk Odeskoho Natsionalnoho Universytetu* / A. Khamitova. - 2015. - Vol.20. - PP. 71 - 80.
19. Dmitrishin, D. Finding cycles in nonlinear autonomous discrete dynamical systems, in preparation / D. Dmitrishin, A. Khamitova, A. Stokolos, M. Tohaneanu // *Tian L., Dong G. Predictive control of sudden occurrence of chaos. – 2008. – PP. 99 - 105.*
20. Tian, L. Predictive control of sudden occurrence of chaos / L. Tian // *Int. J. Nonlinear Science. – 2008. – PP. 99 – 105.*

ПЕРЕМІШУВАННЯ, ЯК СПОСІБ УПРАВЛІННЯ ХАОСОМ

Д.В. Дмитришин, І.М. Скринник

Одеський Національний Політехнічний Університет
пр. Шевченка, 1, Одеса, 65044, Україна; e-mail: anton_dora@mail.ru

У статті розглядається можливість управління динамікою нелінійних дискретних систем. Запропоновано новий спосіб управління хаосом через перемішування станів системи (або функцій від цих станів) визначених в попередній момент часу. Це дозволяє локально стабілізувати наперед невідомі цикли заданої довжини. Як окремий випадок, цей спосіб включає в себе метод стабілізації циклу за допомогою нелінійного зворотного зв'язку із запізненням. Наведені приклади.

Ключові слова: нелінійні дискретні системи, управління хаосом, перемішування станів системи

MIXING AS A METHOD OF CHAOS CONTROL

D.V. Dmitrichin, I.M. Skrinnik

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

In the article we consider the possibility of controlling the dynamics of nonlinear discrete systems. A new way to chaos control by mixing states of the system (or the functions of these states) calculated in the previous time. This approach allows to locally stabilize beforehand unknown cycles of a given length. As a special case, the method includes a cycle stabilization method using nonlinear feedback retarded.

Keywords: linear discrete systems, chaos control, mixed of system's states

ПОБУДОВА ТРЬОХМОДУЛЬНОЇ МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ РОЗВ'ЯЗКУ КВАДРАТНОГО РІВНЯННЯ

М.М. Касянчук

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

Виконання арифметичних операцій над багаторозрядними числами є досить важливою задачею сучасної теорії чисел, прикладної і обчислювальної математики, а також асиметричної криптографії. Тому велика увага приділяється розпаралелюванню процесу обчислень, що реалізується, зокрема, при використанні системи залишкових класів. Дана стаття присвячена розробці аналітичного методу побудови трьохмодульної модифікованої досконалої форми системи залишкових класів, яка дозволяє уникнути виконання громіздкої процедури пошуку оберненого елемента за модулем та множення на базисні числа, на основі розв'язку квадратного рівняння, отриманого за допомогою теореми Вієта. Визначено умову, при виконанні якої існує набір шуканих модулів, та проведено її дослідження. Показано, що відповідна заміна змінних дозволяє суттєво скоротити перебір усіх можливих варіантів та зменшити обчислювальну складність для знаходження модулів. Побудовано та проаналізовано графічні залежності абсолютних величин отриманих модулів та визначено ділянки їх монотонності. Наведено приклад обчислення можливих значень шуканих модулів за допомогою розробленого алгоритму.

Ключові слова: система залишкових класів, модифікована досконала форма, модуль, квадратне рівняння, теорема Вієта, обернений елемент за модулем, базисні числа

Вступ

Відомо [1], що найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелювання процесу обробки інформації. Цією властивістю, на відміну від найпоширенішого на даний час двійкового представлення чисел, володіють деякі непозиційні системи числення, зокрема система залишкових класів (СЗК) [2]. Хоча вона має певні недоліки (відсутність операцій ділення та порівняння, труднощі у виявленні переповнення розрядної сітки тощо), однак дозволяє ефективно виконувати додавання, віднімання, множення, піднесення до степеня над великорозрядними числами [3], що є дуже важливим у наш час, зокрема, у асиметричній криптографії (алгоритми RSA, Ель-Гамала, електронного цифрового підпису тощо) [4], при великих матричних обчисленнях, інших задачах прикладної математики [3].

Представленню десяткового числа N у СЗК відповідають найменші невід'ємні залишки b_i цього числа у системі взаємно простих модулів p_i , тобто $b_i = N \bmod p_i$ [1].

При цьому діапазон обчислень має лежати в межах $0 \leq N \leq P-1$, де $P = \prod_{i=1}^n p_i$. Зворотнє перетворення у десяткову систему числення відбувається на основі китайської теореми

про залишки [5]: $N = \left(\sum_{i=1}^n b_i B_i \right) \bmod P$, де $B_i = M_i m_i$, $M_i = \frac{P}{p_i}$, базисні числа m_i шукаються з виразу:

$$m_i = M_i^{-1} \bmod p_i. \quad (1)$$

Необхідність обчислення оберненого елемента в (1) істотно збільшує складність переведення чисел з СЗК у десяткову систему. Спрощення цієї задачі відбувається у досконалішій формі СЗК (ДФ СЗК), коли усі $m_i = 1$ [1], що дозволяє уникнути процедури пошуку оберненого елемента і множення на базисні числа. В [6] визначені умови для аналітичного визначення m_i . Але в обох випадках значення p_i швидко збільшуються, що неприйнятно при необхідності використання модулів приблизно однакової розрядності.

У роботі [7] описана модифікована ДФ СЗК (МДФ СЗК), у якій базисні числа $m_i = \pm 1$, що також виключає необхідність пошуку оберненого числа. У [8] розроблений метод побудови трьохмодульної МДФ СЗК на прикладі $p_2 - p_1 = 5$. Однак на даний час відсутні аналітичні методи пошуку модулів, які задовольняють умовам МДФ СЗК.

Метою роботи є розробка алгоритму знаходження системи з трьох модулів для МДФ СЗК на основі побудови та розв'язку квадратного рівняння, побудованого за допомогою теореми Вієта.

Основна частина

У працях [9], [10] за допомогою розв'язування систем конгруенцій було отримано вираз для пошуку набору модулів ДФ СЗК. Аналогічні міркування приводять до умови, яка має виконуватися для МДФ СЗК:

$$\sum_{i=1}^n \frac{1}{p_i} = h \pm \frac{1}{\prod_{i=1}^n p_i}, \quad (2)$$

де $h = 0, \pm 1, \pm 2, \pm 3, \dots$.

Для спрощення обмежимося трьома взаємно простими значеннями модулів та приймемо $h = 0$, що відповідає найбільшому діапазону обчислень при заданій кількості модулів. Рівняння (2) буде мати вигляд:

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} = \pm \frac{1}{p_1 p_2 p_3}. \quad (3)$$

Потрібно відмітити, що умова $m_i = 1$ визначає додатній знак модулів, а $m_i = -1$ – від'ємний. Після відповідних перетворень, вважаючи відомим перший модуль, вираз (3) набуде такого вигляду:

$$p_2 p_3 + p_1 (p_2 + p_3) = \pm 1. \quad (4)$$

У рівняння (4) входять добуток та сума невідомих модулів p_2 та p_3 . Для їх пошуку введемо позначення $p_2 p_3 = k p_1 \pm 1$. Тоді відповідно $p_2 + p_3 = -k$. За допомогою теореми Вієта можна побудувати квадратне рівняння, цілочисельними коренями якого будуть значення шуканих модулів:

$$x^2 + kx + kp_1 \pm 1 = 0. \quad (5)$$

Розв'язавши (5), невідомі модулі можна записати таким чином:

$$p_{2,3} = \frac{1}{2} \left(-k \pm \sqrt{k^2 - 4(kp_1 \pm 1)} \right) \quad (6)$$

З (6) видно, що розв'язки (5) будуть цілочисельні, коли дискримінант рівняння (5) являтиме собою повний квадрат деякого числа, яке зручно представити в такому вигляді:

$$k^2 - 4(kp_1 \pm 1) = (k - 2(p_1 + a))^2. \quad (7)$$

Парність другого доданку в дужках в правій частині виразу впливає з вигляду дискримінанта у лівій частині (7). Після відповідних перетворень з (7) отримується:

$$k = 2p_1 + a + \frac{p_1^2 \pm 1}{a}. \quad (8)$$

Отже, МДФ СЗК з трьох модулів існує, коли виконується умова $(p_1^2 \pm 1) \bmod a = 0$. Це означає, що параметр a обмежується інтервалом $[-p_1^2 - 1; p_1^2 + 1]$, $a \neq 0$. Дослідивши (8), можна побачити, що екстремуми k визначаються з умови $a = \pm \sqrt{m^2 \pm 1}$. На рис.1 представлено графік залежності величини k від a , що змінюється від -26 до 26, при $p_1 = 5$.

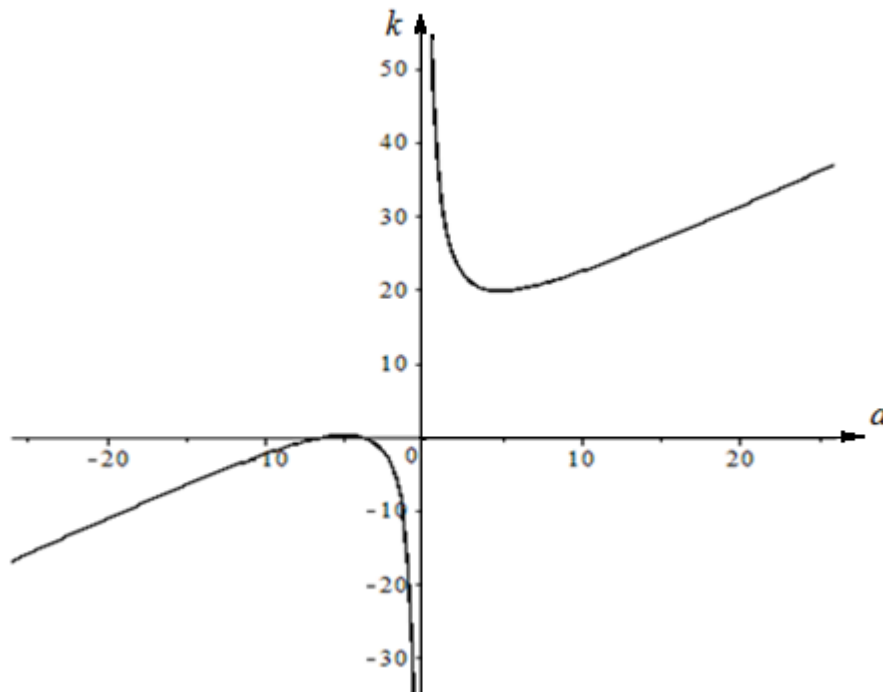


Рис. 1. Графік залежності величини k від параметра a

Графік та побудоване з (7) відносно a квадратне рівняння $a^2 + a(2p_1 - k) + p_1^2 \pm 1 = 0$ показують, що фіксованій величині k відповідають два значення параметра a , причому, згідно теореми Вієта, якщо одне з них є цілочисельне,

то і друге теж повинно бути цілим числом. Це дозволяє зменшити діапазон дослідження a до таких меж: $[-p_1+1; p_1-1]$, $a \neq 0$. На рис.2 для прикладу показана поверхня, яка, згідно виразу $k = 2p_1 + a + \frac{p_1^2 - 1}{a}$, характеризує залежність параметра k від значень $p_1 = 2 \dots 10$ та $a = 1 \dots p_1 - 1$.

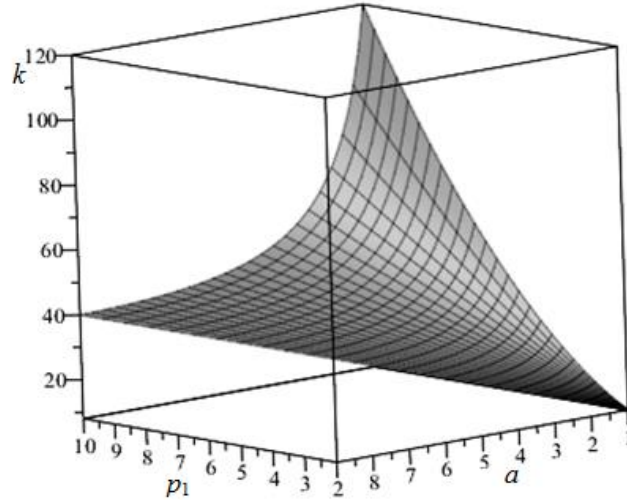


Рис. 2. Графік залежності параметра k від значень $p_1 = 2 \dots 10$ та $a = 1 \dots p_1 - 1$

Як видно з графіка, величина k досягає максимуму при найбільшому значенні модуля p_1 та найменшому значенні параметра a . Мінімум k знаходиться при мінімальних значеннях p_1 і a .

На рис.3,4 показано відповідно графіки залежності модулів $p_2 = \frac{1}{2} \left(-k + \sqrt{k^2 - 4(kp_1 - 1)} \right)$ та $p_3 = \frac{1}{2} \left(-k - \sqrt{k^2 - 4(kp_1 - 1)} \right)$ від значень модуля $p_1 = 2 \dots 10$ і параметра $a = 1 \dots p_1 - 1$.

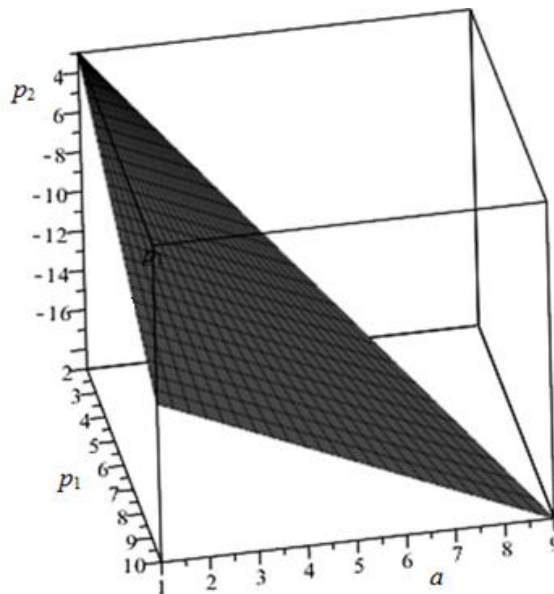


Рис. 3. Графік залежності модуля p_2 від значень модуля p_1 і параметра a

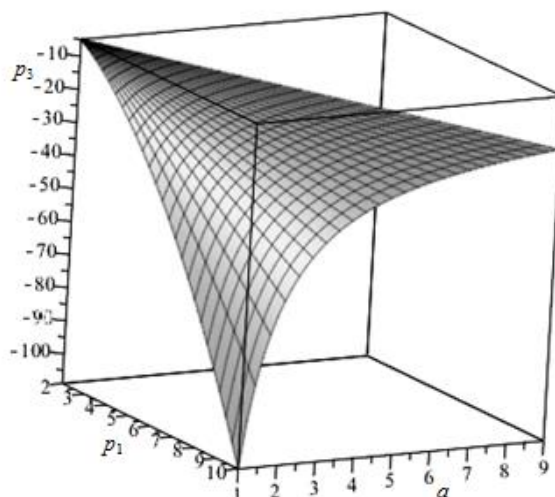


Рис. 4. Графік залежності модуля p_3 від значень модуля p_1 і параметра a

З рис.3,4 видно, що графіком залежності модуля p_2 від значень p_1 і a є площина, а модуля p_3 - гіперboloїд. Мінімального абсолютного значення модулі p_2 та p_3 набувають при найменших величинах p_1 та a . Максимальне абсолютне значення p_2 буде у випадку, коли $p_1 \rightarrow \max$, $a \rightarrow \max$, відповідно $|p_3| \rightarrow \max$, якщо $p_1 \rightarrow \max$, $a \rightarrow \min$.

В табл.1 представлено можливі значення p_2 , p_3 , відповідних їм параметрів a , k , а також абсолютних величин модулів для $p_1 = 5$.

Таблиця 1.

Можливі значення p_2 , p_3 , відповідні їм значення параметрів a , k , а також абсолютні величини модулів для $p_1 = 5$.

№	a	k	p_2	p_3	$ p_2 $	$ p_3 $
1	-3	-1	-2	3	2	3
2	-2	-4	-3	7	3	7
3	-2	-5	-3	8	3	8
4	-1	-15	-4	19	4	19
5	-1	-17	-4	21	4	21
6	1	37	-6	-31	6	31
7	1	35	-6	-29	6	29
8	2	25	-7	-18	7	18
9	2	24	-7	-17	7	17
10	3	21	-8	-13	8	13
11	4	20	-9	-11	9	11

З табл.1 видно, що модуль p_2 набуває тільки від'ємних значень. При $a < 0$ модуль p_3 додатний і навпаки, якщо $a > 0$, то $p_3 < 0$. Слід зазначити, що в табл.1 відсутнє значення $a = -4$, оскільки в цьому випадку, як впливає з виразу (6), p_2 , $p_3 = \pm 1$. Однак такий набір модулів суперечить початковим умовам задачі. На рис.5 зображено графіки залежності абсолютних величин модулів p_2 та p_3 від їх номера згідно табл.1.

Як видно з рис.5, абсолютна величина модуля p_2 повільно збільшується. На відміну від цього, графік для $|p_3|$ швидко зростає, досягає максимуму посередині номерного діапазону, потім спадає з меншою швидкістю до значення $|p_2|$.

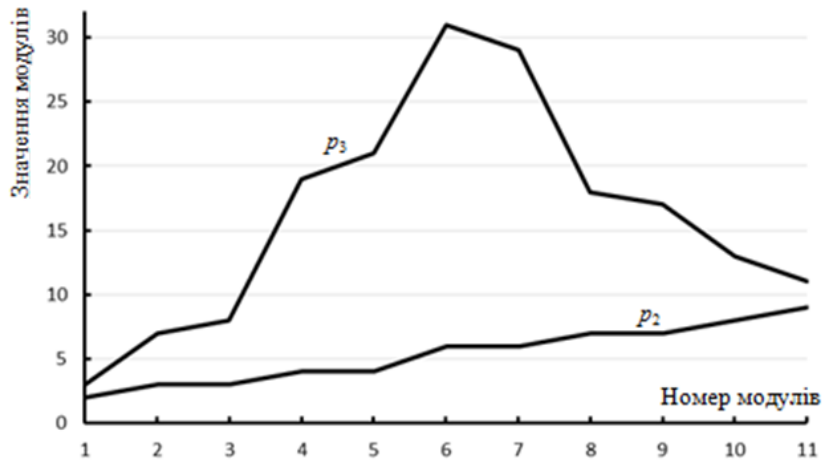


Рис. 5. Графіки залежності абсолютних величин модулів p_2 та p_3 від їх номера згідно табл.1

Висновки

Дана стаття присвячена розробці аналітичного методу побудови трьохмодульної модифікованої досконалої форми системи залишкових класів, яка дозволяє уникнути виконання громіздкої процедури пошуку оберненого елемента за модулем, на основі розв'язку квадратного рівняння, отриманого за допомогою теореми Вієта. Визначено умову, при виконанні якої існує набір шуканих модулів, та проведено її дослідження. Показано, що відповідна заміна змінних дозволяє суттєво скоротити перебір усіх можливих варіантів та зменшити обчислювальну складність для знаходження модулів. Побудовано та проаналізовано графічні залежності абсолютних величин отриманих модулів та визначено ділянки їх монотонності. Наведено приклад обчислення можливих значень шуканих модулів за допомогою розробленого алгоритму.

Список літератури

1. Николайчук, Я.М. Теория джерел інформації / Я.М. Николайчук. – Тернопіль: ТЗОВ «Терно–граф», 2010. – 536 с.
2. Червяков, Н.И. Нейрокомпьютеры в остаточных классах / Н.И.Червяков, П.А. Сахнюк, А.В. Шапошников, А.И. Макоха. - М: Радиотехника, 2003. - 272 с.
3. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел / В.К. Задірака, О.С. Олексюк. – К.: 2003. – 264 с.
4. Задірака, В.К. Комп'ютерна криптологія / В.К. Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
5. Виноградов, И.М. Основы теории чисел/ И.М. Виноградов. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
6. Nykolaychuk, Ya. M. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. // Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko / Cybernetics and Systems Analysis. – 2014. – Vol.50. – Issue 5. – P. 649 - 654.
7. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозіуму «Питання оптимізації обчислень (ПОО–XXXV)». Т.1. – Київ–Кацивелі. – 2009. – С. 306–310.

8. Николайчук, Я.Н. Теоретические основы модифицированной совершенной формы системы остаточных классов / Я.Н. Николайчук, М.Н. Касянчук, И.З. Якименко // Кибернетика и системный анализ. – 2016. – Том 52. – № 2. – С. 51 – 55.
9. 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 (Zakarpattya), Ukraine. - 2015. – P. 168 - 171.
10. Касянчук, М.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх використання в китайській теоремі про залишки / М.М. Касянчук, І.З. Якименко, І.Р. Паздрій, Я.М. Николайчук // Вісник Хмельницького національного університету: Технічні науки. – 2015. - №1. – С. 170 - 176.

ПОСТРОЕНИЕ ТРЁХМОДУЛЬНОЙ МОДИФИЦИРОВАННОЙ СОВЕРШЕННОЙ ФОРМЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ НА ОСНОВЕ РЕШЕНИЯ КВАДРАТНОГО УРАВНЕНИЯ

М.Н. Касянчук

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

Выполнение арифметических операций над многоразрядными числами является весьма важной задачей современной теории чисел, прикладной и вычислительной математики, а также асимметричной криптографии. Поэтому большое внимание уделяется распараллеливанию процесса вычислений, что реализуется, в частности, использованием системы остаточных классов. Данная статья посвящена разработке аналитического метода построения трёхмодульной модифицированной совершенной формы системы остаточных классов, которая позволяет избежать выполнения громоздкой процедуры поиска обратного элемента по модулю и умножения на базисные числа, на основе решения квадратного уравнения, полученного с помощью теоремы Виета. Определено условие, при выполнении которого существует набор искомых модулей, и проведено его исследование. Показано, что соответствующая замена переменных позволяет существенно сократить перебор всех возможных вариантов и уменьшить вычислительную сложность для нахождения модулей. Построены и проанализированы графические зависимости абсолютных величин полученных модулей и определены участки их монотонности. Приведён пример вычисления возможных значений искомых модулей с помощью разработанного алгоритма.

Ключевые слова: система остаточных классов, модифицированная совершенная форма, модуль, квадратное уравнение, теорема Виета, обратный элемент по модулю, базисные числа

CONSTRUCTION OF THREE MODULAR MODIFIED PERFECT FORMS OF SYSTEM OF RESIDUAL CLASSES BASED SOLUTION OF QUADRATIC EQUATION

M.M. Kasianchuk

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

Perform of arithmetic operations with multidigital numbers are quite important task of modern numbers theory, applied and computational mathematics and asymmetric cryptography. So much attention is paid for paralleling computation process, which is implemented particularly in the system of residual classes usage. This article is focused on the development of the analytical method of construction of triple-modular modified perfect form of the system of residual classes, which allows to avoid the cumbersome execution procedure of search of inverse element by module and multiplying by the basis number, based on the solution of the quadratic equation obtained with using of Vieta's formula. The condition which is required for existence of set of modules is defined and investigated. It is shown that the corresponding change of variables allows to reduces significantly of all possible options and to exhausts the computational complexity for finding modules. The image depending of absolute values of obtained modules is constructed and analyzed and the areas of monotony are identified. An example of the possible values of the calculation modules using the algorithm is launched.

Keywords: system of residual classes, modified perfect form, module, quadratic equations, Vieta's formula, inverse element for the module, the basis number

ГІПОТЕЗА І ФОРМАЛЬНА МОДЕЛЬ СИНГУЛЯРНОЇ ДИНАМІКИ ІНЦИДЕНТІВ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

О.М. Гергега¹, С.О. Гнатюк², В.Г. Кононович³, І.В. Кононович¹

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

²Національний авіаційний університет,
просп. Космонавта Комарова, 1, м. Київ, 03680, Україна; e-mail: s.gnatyuk@nau.edu.ua

³Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net

Статистика свідчить про високі темпи зростання кількості деструктивних інцидентів інформаційної безпеки. Але чинники, що спричиняють це явище, досліджені недостатньо. Вони не охоплюють широкий спектр характеристик і не розкривають повний формальний та системний підхід до вирішення задач кібербезпеки. У зв'язку з цим, сформульована гіпотеза щодо сингулярності динаміки інформаційного потоку з деструктивними та корисними характеристиками. Розроблена проста математична модель багатовступової обробки та фільтрації інформаційного потоку із зворотними зв'язками для забезпечення кібербезпеки. Проведене дослідження чотирьох-ступеневої динамічної системи показало, що в ній можуть виникати стаціонарні, квазіперіодичні коливання та динамічний хаос. У перехідний період можливі турбулентність та сингулярність. Використання механічних аналогій сприяло більш точному розумінню результатів дослідження. Зроблено висновок щодо об'єктивності турбулентних та сингулярних явищ перехідного періоду та щодо необхідних позасистемних заходів забезпечення кібербезпеки.

Ключові слова: кібернетична безпека, модель динамічної системи, турбулентність, сингулярність, біфуркації, інциденти кібербезпеки

Вступ

Одночасно із бурхливим розвитком інформаційних та інших технологій фіксуються високі темпи зростання кількості інцидентів інформаційної та кібернетичної безпеки (кібербезпеки). Серед теоретичних методів досліджень таких явищ важливе місце займають математичне моделювання і математичні методи інформаційної та кібернетичної безпеки. Проблемою є розуміння причин та пошук засобів припинення зростання кількості інцидентів кібернетичної безпеки.

Аналіз існуючих досліджень. Статика процесів забезпечення кібербезпеки, моделі загроз, моделі порушників, моделі захисту, статичні моделі ризиків тощо досліджені досить глибоко [1, 2]. Що стосується динаміки процесів кібербезпеки, то розроблені аналітичні моделі розповсюдження вірусів і мережевих черв'яків [3, 4], авторами цієї роботи та іншими дослідниками розпочато застосування біологічних моделей в сфері динаміки процесів забезпечення інформаційної безпеки [5], оцінки впливу затримки в реагуванні на інциденти кібербезпеки [6]. У цілому, подібних робіт поки що мало і систематичних досліджень не проводиться. Як правило, моделі динамічних систем аналізуються в усталених режимах. Перехідні процеси, які цікавлять авторів, часто ігноруються. Крім того, недостатньо детальних статистичних даних.

Сучасна епоха характеризується збігом у найближчому майбутньому кризових прискорень декількох загально планетарних процесів. Серед таких процесів, що несуть загрозу всьому людству, є прискорення зростання кількості інцидентів кібербезпеки.

На рис.1(а) представлено динаміку деструктивних інцидентів щодо державних інформаційних ресурсів в Україні [2], а рис.1(б) містить зростання інцидентів за даними державного відомства США. У нашій державі відсутня загальна статистика інцидентів кібербезпеки, а реагування на них покладено на єдиний у державі спеціалізований центр CERT-UA. Темпи зростання кількості інцидентів складають мінімум 30-40 % на рік, за іншими даними – 400 %. До того ж, більшість приватних компаній не схильні до розголошення фінансових втрат від інцидентів, оскільки іміджеві втрати теж можуть бути значними.

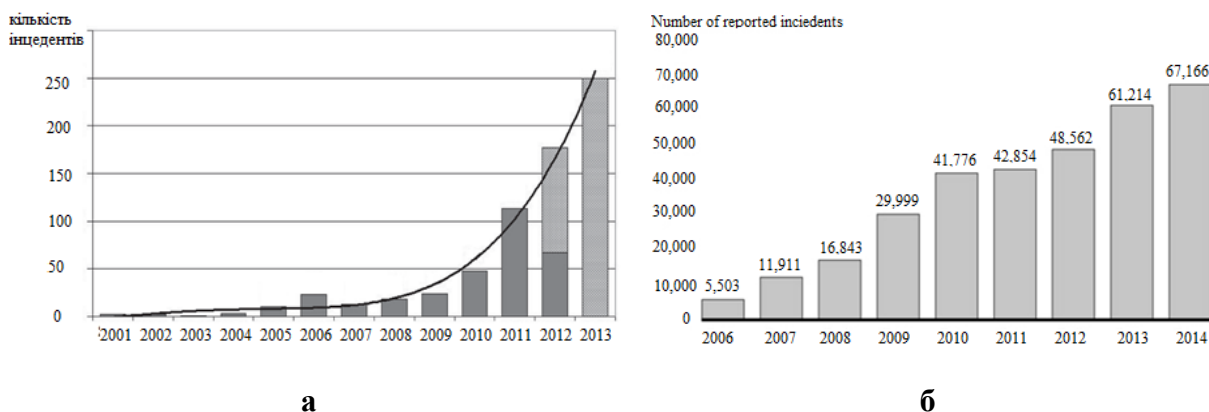


Рис. 1. Статистика інцидентів кібербезпеки: а - пов'язаних з державними інформаційними ресурсами України; б - за даними U.S. Government Accountability Office

Приймаючи до уваги цю статистику, можна висловити гіпотезу щодо сингулярного характеру динаміки кількості інцидентів кібербезпеки. Представляє інтерес дослідження цієї динаміки окіл точок сингулярності та після сингулярного періоду. Тому необхідна розробка відповідної адекватної моделі. Актуальність проблеми обумовлена успішним застосуванням якісних методів дослідження нелінійної динаміки у техніці, системах кібербезпеки, «радіоелектроніці, медицині, біофізиці, хімічних технологіях, психології та ще у десятих інших областях [8]».

Метою роботи є обґрунтування гіпотези щодо сингулярного характеру динаміки кількості інцидентів кібербезпеки, розроблення та дослідження математичної моделі циклічного поетапного процесу обробки інформаційного потоку з включеними до нього етапами забезпечення кібербезпеки, а також пошук методів забезпечення кібербезпеки.

Математична модель циклічного інформаційного процесу управління з включеними до нього етапами забезпечення кібербезпеки

Ця задача виходить далеко за межі систем забезпечення кібербезпеки і досліджувалась авторами стосовно циклічного управління кібербезпекою в [9] і стосовно управління колективною та індивідуальною свідомістю громадян у [10]. Тут розглянемо найпростішу модель циклового інформаційного процесу управління узагальненим інформаційним виробництвом у високотехнологічному суспільстві.

«Інформація на сьогодні набуває характер стратегічного ресурсу сучасних розвинутих суспільств. Основою цього являється той факт, що будь-який речовинний процес, який підлягає контролю та управлінню, має своє ізоморфне відображення... Ефективність людської дії здебільшого залежить від правильного управлінського рішення, що, у свою чергу, залежить від інформаційного моделювання ситуації, від пошуку потрібної інформації та її переробки. Лавиноподібне зростання інформаційних

потоків, у яких змішувались потрібна і непотрібна інформація («інформаційні шуми»). У значній мірі утруднив поведінку людини та висунув на передній план вибіркового пошук потрібної інформації з наступною її редукцією для прийняття тих чи інших рішень [11]». Нехай цикл управління інформаційним потоком складається із чотирьох етапів: фільтрація вхідного інформаційного потоку – x_{in} засобами забезпечення кібербезпеки; аналіз інформаційного потоку (відбір потрібної інформації, редукція, консолідація, переробка); прийняття рішень (формування управлінського рішення); обробка вихідного інформаційного потоку для забезпечення кібербезпеки перед видачею управлінського рішення – x_{out} . Тоді, математична модель динамічної системи буде мати такий вигляд:

$$\Phi(x, y, z, w) = \begin{cases} x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} \\ y_{n+1} = y_n + k_{xy} p x_n^2 - (k_{yx} + k_{yz}) q y_n^2 + k_{zy} r z_n^2 \\ z_{n+1} = z_n + k_{yz} q y_n^2 - (k_{zy} + k_{zw}) r z_n^2 + k_{wz} s w_n^2 \\ w_{n+1} = w_n + k_{zw} r z_n^2 - (k_{wz} + k_{out}) s w_n^2 \end{cases} \quad (1)$$

де x, y, z, w – динамічні змінні, які визначають інтенсивність інформаційних елементів потоку на етапах обробки інформації; k_{ij} – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації; p, q, r, s – розподільчі коефіцієнти, x_{in} – інтенсивність інформаційних елементів потоку, що поступають на перший етап обробки; причому, k_{ij} и $p, q, r, s \in (0,1)$, $x, y, z, w \in R$, $x_{in} = const \in R^+$.

Наявність у системі двох груп коефіцієнтів (k_{ij} та p, q, r, s) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку переходить на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q, r, s описують розподіл елементів інформаційного потоку за їх видами по семантичним ознакам, наприклад, по змісту. Перехід між етапами обробки визначається добуток коефіцієнтів обох груп.

Слідуючи методам відпрацьованої в теорії нелінійної динаміки досліджень, знайдемо нерухомі точки системи та проаналізуємо їх стійкість. При цьому, буде продемонстровано метод графічного відображення проекцій об'єктів чотирьохмірного простору на двохмірний та трьохмірний простір. Для знаходження нерухомих точок необхідно й достатньо розв'язати систему рівнянь, які отримуються із системи (1) при $x_{n+1}^* = x_n^*$, $y_{n+1}^* = y_n^*$, $z_{n+1}^* = z_n^*$, $w_{n+1}^* = w_n^*$. Маємо систему рівнянь

$$\Phi^*(x, y, z, w) = \begin{cases} -k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} = 0 \\ k_{xy} p x_n^2 - (k_{yx} + k_{yz}) q y_n^2 + k_{zy} r z_n^2 = 0 \\ k_{yz} q y_n^2 - (k_{zy} + k_{zw}) r z_n^2 + k_{wz} s w_n^2 = 0 \\ k_{zw} r z_n^2 - (k_{wz} + k_{out}) s w_n^2 = 0 \end{cases} \quad (2)$$

яка шляхом заміни змінних перетворюється в систему рівнянь зі змінними у першій степені. Система рівнянь (2) має тривіальний нульовий розв'язок: $x_0^* = 0$; $y_0^* = 0$; $z_0^* = 0$; $w_0^* = 0$. Для аналізу стійкості нульового розв'язку використовуємо метод першого наближення. Розкладемо змінні рівняння (2) в ряд

Тейлора та відкинемо члени другого порядку малості. Тоді отримуємо сукупність частинних похідних типу $\mu = f'(x_0^*)$, які називаються у випадку дискретних відображень мультиплікаторами. Із частинних похідних складається матриця Якобі, знаходиться визначник матриці (якобіан) у нульовій нерухомій точці і корені характеристичного рівняння. Для цього розв'язуємо матричне рівняння виду $\det(A - \mu E) = 0$ і знаходимо, що чотири корені характеристичного рівняння і якобіан у нульовій нерухомій точці дорівнюють одиниці, $J=1$. Усі корені є дійсними. Таким чином, у нульовій нерухомій точці система (1) консервативна, не стискає і не розширює фазовий простір. Для визначення стійкості нульової нерухомої точки необхідні додаткові дослідження.

У загальному випадку, для знаходження нерухомих точок системи (1) необхідно знайти корені системи (2). Розв'язання може бути знайдено чисельним способом, наприклад, за допомогою алгоритму Ньютона-Рафсона [12]. У нашому випадку розв'язання знаходимо аналітичним методом. Враховуючи симетричний характер взаємодії етапів, отримуємо вирази для координат нерухомих точок:

$$w_0 = \pm \sqrt{\frac{x_{in}}{k_{out}s}}, \quad z_0 = \pm \sqrt{\frac{x_{in}}{k_{zw}r}} L, \quad y_0 = \pm \sqrt{\frac{x_{in}}{k_{yz}q}} M, \quad x_0 = \pm \sqrt{\frac{x_{in}}{k_{xy}p}} N, \quad (3)$$

$$\text{де } L = \left(\frac{k_{wz}}{k_{out}} + 1 \right), \quad M = \left(\frac{k_{zy}}{k_{zv}} L + 1 \right), \quad N = \left(\frac{k_{yx}}{k_{yz}} M + 1 \right).$$

Координати (3) за умов, наприклад, коли коефіцієнти $k_{xy} = 0.5$; $k_{yx} = 0.4$; $k_{yz} = 0.3$; $k_{zy} = 0.3$; $k_{zw} = 0.5$; $k_{wz} = 0.5$; $k_{out} = 0.4$; і $p = 0.08$; $q = 0.02$; $r = 0.015$; $s = 0.015$; $x_{in} = 5.0$ приймають значення: $x_0 = \pm 22.7303$; $y_0 = \pm 44.2531$; $z_0 = \pm 38.7298$; $w_0 = \pm 28.8675$.

Маємо 16 коренів, а значить 16 нерухомих точок. Усі корені (3) системи рівнянь (2) дійсні. Координати рухомих точок залежать від параметрів системи. Розташування нерухомих точок у чотирьохвимірному просторі можна оцінити за допомогою проєкцій цих координат на координатні площини та проєкції на трьохвимірний простір. Об'єкт чотирьохвимірного простору повністю визначають його проєкції на чотири трьохвимірні простори (з чотирьох «сторін») або його проєкції на відповідні чотири координатні площини. Для прикладу, на рис.2(а) показано рух від центра до периферії проєкцій координат нерухомих точок на площині Oxy (Oab), коли параметр x_{in} приймає значення, відповідно, 1, 2, ... 8. На рис.2(б) представлені проєкції тих же точок на трьохмірний простір $Oxyz$ ($Oaiv$).

У кожному з чотирьох квадрантів координатних площин є по одній проєкції нерухомих точок. У кожному з восьми октантів трьохвимірних просторів є по одній проєкції нерухомих точок. У кожному з шістнадцяти седетантів чотирьохвимірного простору є також по одній нерухомій точці. Стійкість нерухомих точок перевірялась шляхом обчислення якобіану матриці збурення. Матриця збурення складена із відповідних частинних похідних правих частин системи рівнянь (1). Маємо додатний якобіан для восьми відповідних нерухомих точок і від'ємний для інших восьми точок. «Якобіан, обчислений у нерухомій точці, визначає еволюцію малого елемента площі при дії відображення. При $|J| < 1$ цей елемент стискається, і відображення буде дисипативним [13, 14]». У іншому випадку система стає консервативною ($J = 1$), або ця нерухома точка нестійка.

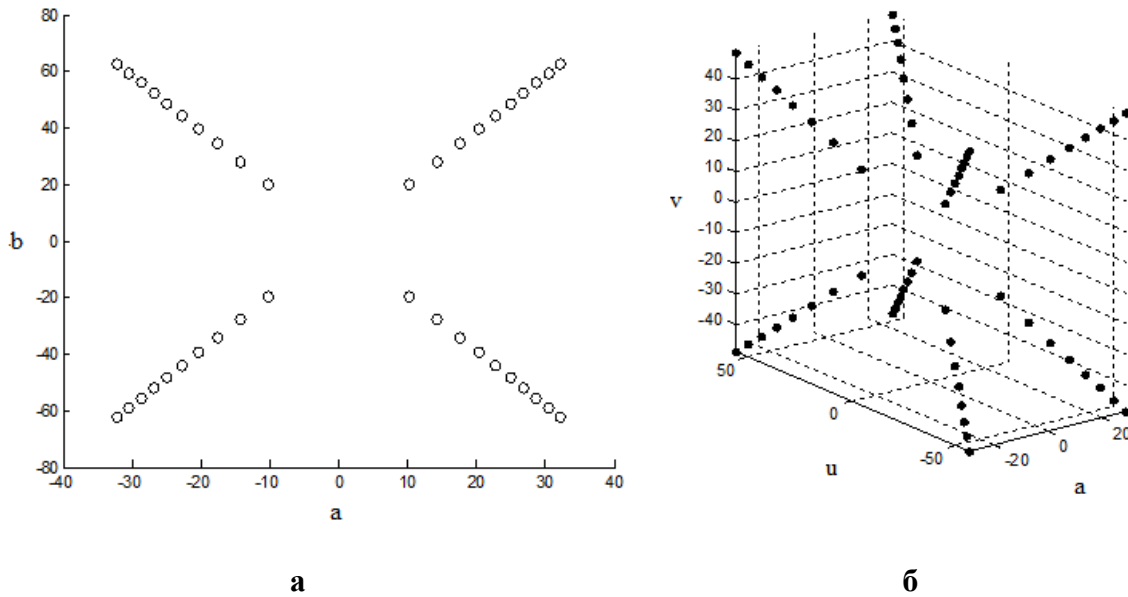


Рис. 2. Проекції координат нерухомих точок на: а - координатну площину; б - трьохвимірний простір

Аналіз рівнянь руху та виникаючої турбулентності

Процедури аналізу динамічних систем включають перевірку всіх траєкторій на стійкість та виявлення початкових умов, за яких траєкторії потрапляють в околиці кожної з нерухомих точок. У наслідок складності представлення об'єктів у чотирьохвимірному просторі та великої кількості варіантів, у даному випадку доцільно встановлювати початкові умови, виходячи із практичних міркувань, – на початку моделювання на всіх етапах обробки інформації руху немає і здійснюється включення вхідного потоку заданої інтенсивності. Тому для відображення рівнянь руху чисельно вирішуємо систему рівнянь (1) при початкових умовах: $x_0 = 0$; $y_0 = 0$; $z_0 = 0$; $w_0 = 0$. Графіки рівнянь руху у вигляді проекцій на площини $0xt$, $0yt$, $0zt$, $0wt$ при тих же значеннях коефіцієнтів системи рівнянь (1), інтенсивності вхідного потоку $x_{in} = 4.94$ показані на рис.3.

Рішення мають три характерні ділянки: початкова, турбулентна і усталена (при заданих значеннях параметрів – квазіперіодична). Початкова ділянка (модельний час t у проміжку від 0 до 30 одиниць) відрізняється плавним зростанням величини інтенсивності потоку. Початкова ділянка тим довша, чим менша інтенсивність вхідного потоку. Турбулентна ділянка на графіках рис.3 триває у проміжку від 30 до 70 модельних одиниць, характеризується хаотичними коливаннями, викиди досягають великих значень і при збільшенні інтенсивності вхідного потоку прямують до нескінченності. Сингулярності у цій моделі, за даних параметрів виникають при $x_{in} > 4.94$. Але якщо сингулярність не досягається, то поступово хаотичні коливання затухають і замінюються стаціонарними квазіперіодичними коливаннями. В усталеній ділянці, в залежності від величин параметрів системи, відбуваються біфуркації подвоєння періоду Фейгенбаума. Періодичні коливання змінюються на квазіперіодичні а потім – динамічним хаосом [12].

Причиною виникнення коливань і турбулентності є зворотні зв'язки у кожному з етапів обробки інформації та перехідні процеси при включенні потоку. Потік не може вирости миттєво і наростає плавно. На рис.4 показано, як проходить взаємодія потоків на межі двох етапів обробки інформаційного потоку.

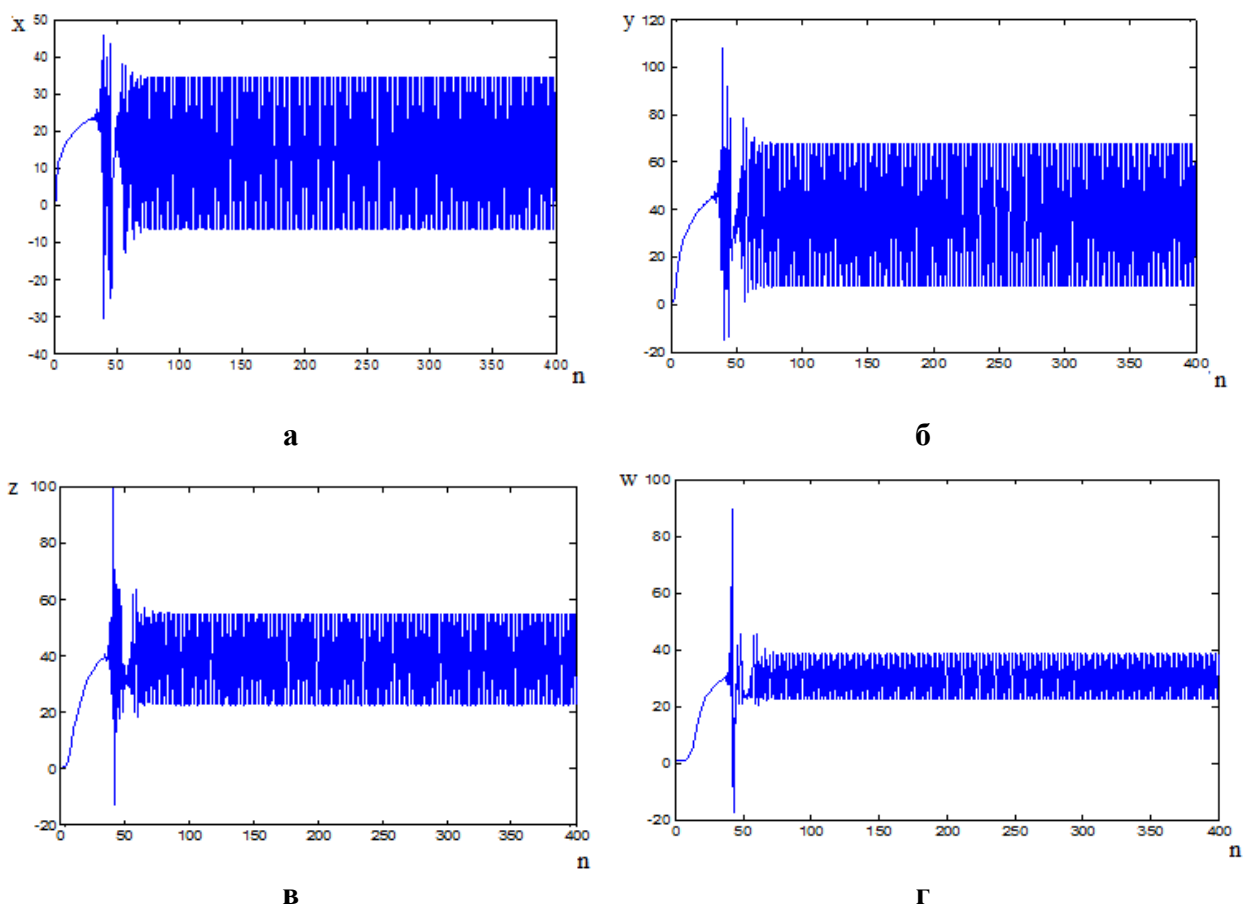


Рис. 3. Графіки рівнянь руху в проекціях на площини: а - $0xy$; б - $0yz$; в - $0zw$; г - $0wx$

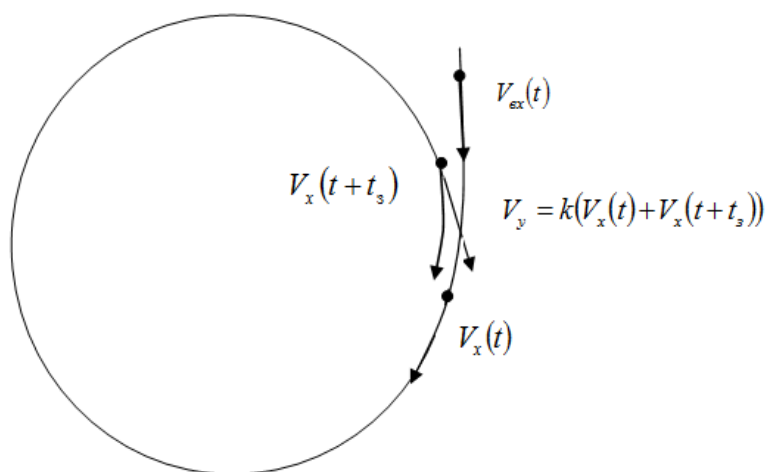


Рис. 4. Векторна діаграма швидкостей потоку на границі двох етапів обробки

Кожен етап обробки інформаційного потоку у загальному вигляді можна вважати циркуляційним процесом. Інформаційні елементи циркулюють «по колу» і приймають участь у різних операціях обробки інформації. Вхідний потік поступає на циркуляцію із миттєвою швидкістю $V_{BX}(t)$. Пройшовши за час t_3 по колу послідовні операції обробки інформації на стику етапів, інформаційний потік розділяється. Частина потоку поступає до наступного етапу обробки з інтенсивністю $V_y = k(V_x(t) + V_x(t+t_3))/2$, а інша частина продовжує циркуляцію, змішуючись із вхідним потоком, який має більшу миттєву швидкість внаслідок перехідного процесу. Швидкі інформаційні елементи у спільному

поточи уповільнюються, а повільні пришвидшуються. Наявність інерційних ефектів сприяє виникненню коливальних.

Фізичні аналогії

Для більш повного розуміння процесів корисно застосувати метод фізичних аналогій, порівнявши цю модель, наприклад, з математичною моделлю повітряного відцентрового фільтра. Таку модель запропонував О. Герега в [15] і її адекватність підтверджена експериментально. Повітряний фільтр моделюється як трьох- або чотирьох рівнева динамічна дисипативна система із суміжно взаємодіючими рівнями. У моделі вивчається динаміка газового потоку (аналог інформаційного потоку) з пилом (аналог деструктивної інформації) у повітряних фільтрах зі зворотними зв'язками між сусідніми рівнями (аналог багатоетапної обробки інформації). Комп'ютерна модель фільтра описується як система (1). Фізична інтерпретація коефіцієнтів системи (1) інша. «Коефіцієнти k_{ij} описують відносну величину зміщення послідовних криволінійних каналів (труб) інженерної конструкції та задають долю потоку, які переходять з одного каналу в інший. Коефіцієнти p, q, r, s описують розподіл часток по ширині каналу конструкції. Перехід між каналами також визначається добутком коефіцієнтів обох груп (див. [15])». Виникнення коливальних і турбулентності в моделі повітряного фільтра можна пояснити за допомогою рис.4.

Вхідний потік поступає на циркуляцію з миттєвою швидкістю потоку $V_{ex}(t)$. Пройшовши за інтервал часу t_s шлях у криволінійному (коловому) каналі, на стику фаз потік поділяється. Високо орбітальна частина потоку з важкими частками пилу поступає до наступної фази очистки, а низькоорбітальна частина продовжує свій шлях у криволінійному каналі, змішуючись із вхідним потоком. В один потік потрапляють частки пилу і газу, які рухаються з різною швидкістю: $V_x(t) > V_x(t+t_s)$. За повільними частками виникає згущення потоку, а за швидкими – розрідження. Тим самим у середовищі пружного газу виникають сили прискорення й уповільнення, а значить виникають коливання швидкості навколо деякого середнього значення. Стійкі коливання виникають за певного співвідношення фаз

$$\varphi_{зд} = \arcsin\left(\frac{a}{A}\right) - \omega_0 t_{зп} \pmod{2\pi}, \quad (4)$$

де ω_0 – кутова частота коливальних (резонансна частота); a – поточна швидкість потоку; A – амплітуда коливальних.

Кутова частота повинна бути такою, щоб потоки зустрічались у протилежних фазах. Тоді на швидкі частки діють сили уповільнення, а на повільні – сила прискорення. Коливання повздовжні та не приводять до перемішування орбіт, тобто не заважають роботі повітряного фільтра. Наведені міркування пояснюють результати моделювання і можуть бути перенесені на обробку інформаційного потоку. На рис.5(а) і рис.5(б) показані спектри коливальних у стаціонарному режимі, які отримані за допомогою одномірного швидкого дискретного перетворення Фур'є:

$$X(k) = \sum_{n=1}^N x(n) e^{-j2\pi(k-1)(n-1)/N}, \quad (5)$$

де $1 \leq k \leq N$; N – довжина аналізованої часової послідовності, яка генерується системою (1).

Графіки отримані при наступних параметрах моделі: $q = 0,032 q$; x_{in} змінювалось в інтервалі від 4,5 до 4,7. Частота несучої 1500 у.о. відповідає несучому коливальню на

атракторі, яке визначається властивостями відображення (1). Модуючі частоти (рис.5(а)) відповідають резонансам у колових каналах повітряного фільтру. Ці частоти змінюються стрибками, у залежності від того, скільки цілих періодів модулюючого коливання вкладається в інтервал часу затримки t_z . З результатів моделювання слідує, що в стаціонарному режимі усі змінні коливаються з однаковою частотою і фазою, представляючи собою єдину хвилю.

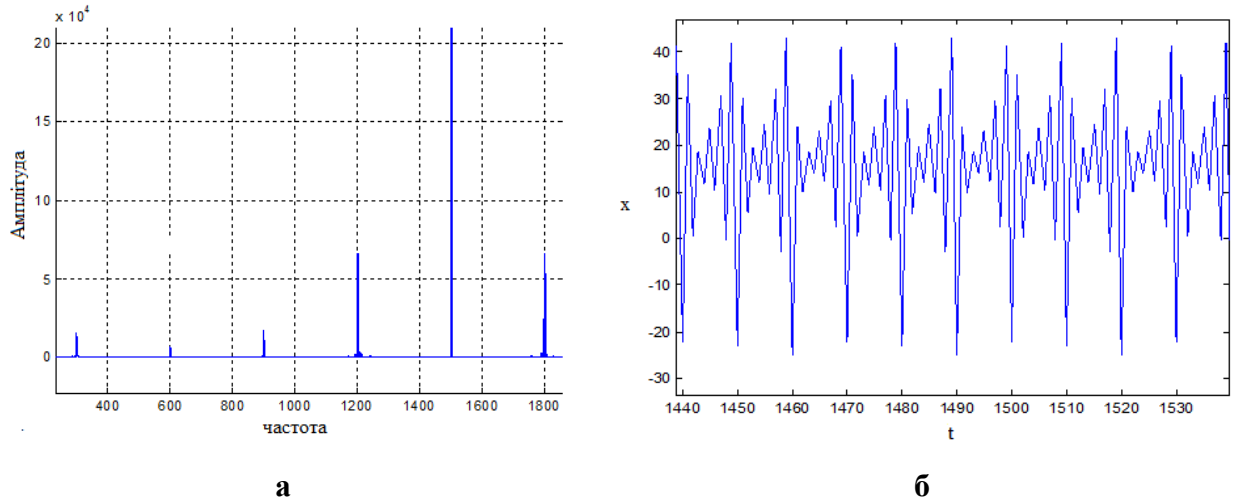


Рис. 5. Коливання в стаціонарному режимі при $N = 3000$: а - спектр для змінної x ; б - графік часової залежності змінної x

Зауважимо що співвідношення (5) не визначає явну частоту коливань. Частота дана відносно розподілів вектора вхідного сигналу й вимірюється в безрозмірних умовних одиницях, зворотних тривалості одного такту моделювання, яка, у свою чергу, у цьому дослідженні не співвідноситься з реальним часом процесу. Таким чином, розглянута динамічна система об'єднує в собі, у крайньому випадку в межах загального модельного часу, глобальну стійкість із локальною нестійкістю.

Турбулентні перехідні процеси

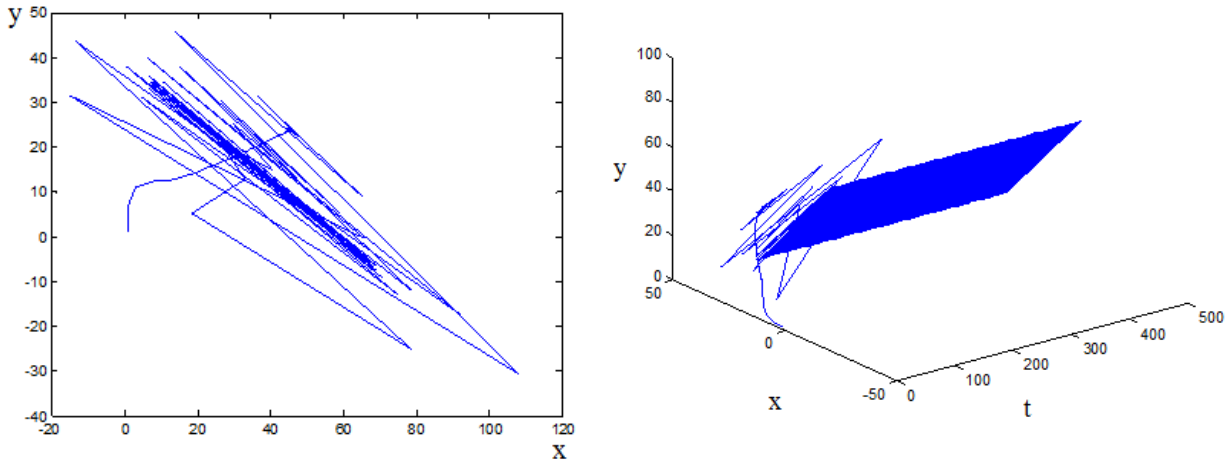
Коливальний характер процесів системи (1) тісно пов'язаний з турбулентними явищами перехідного періоду. Ці явища мають в своїй основі одну причину – наявність у системі позитивних зворотних зв'язків. Для більш детального аналізу турбулентної ділянки процесу обробки інформаційного потоку в системі (1) розглянемо фазовий портрет системи у перехідному і стаціонарному режимах. Значення коефіцієнтів системи та початкові умови залишаються тими ж. На рис.6(а) представлена проекція багатовимірний фазового портрета на площину $0xy$, а на рис.6(б) – його проекція на трьохвимірний простір $0xyt$. Останнє дозволяє прослідкувати еволюцію траєкторії до атрактору.

У турбулентному режимі спостерігаються хаотичні траєкторії. У стаціонарному режимі маємо атрактор. Згідно попередніх досліджень [15] мають місце дивні атрактори у вигляді тонкого сильно витягнутого еліпсоїдного тора.

Розглянемо структурну стійкість системи. Для дослідження структурної стійкості системи вивчені біфуркаційні діаграми, приклад яких показано на рис.7. Перша біфуркація співпадає з виникненням турбулентності. Навколо стійкої і нестійкої гілок біфуркації виникають хаотичні коливання (так званий «чубчик»).

Деякі траєкторії мають сингулярність. Координати точок сингулярної траєкторії спрямовуються до нескінченності. У моделі вони досягають – NaN або +NaN (мінус і

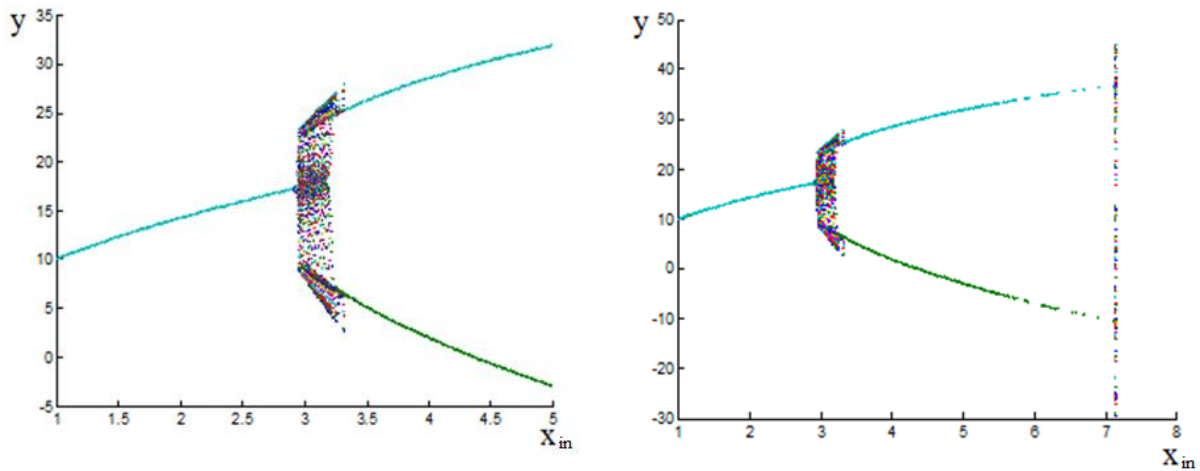
плюс машинної нескінченності). Такі траєкторії в моделі «гинуть». Траєкторії, що вижили, можуть існувати і при другій біфуркації подвоєння періоду. Але при збільшенні інтенсивності вхідного потоку траєкторій, які вижили, стає все менше. Тому дослідження другої біфуркації у цій моделі, з наявними комп'ютерними ресурсами, практично неможливо. Можна припустити, що друга біфуркація також супроводжується турбулентністю. На рис.7(б) видно залишки «чубчика» на другій біфуркації.



а

б

Рис. 6. Перехідний процес і атрактор системи (а) та його еволюція (б)



а

б

Рис. 7. Біфуркаційна діаграма: а - при x_{in} в інтервалі $[1, 5]$; б - при x_{in} в інтервалі $[1, 8]$

Таким чином, турбулентність і сингулярність динамічних систем типу системи (1), для яких характерна наявність позитивних зворотних зв'язків, визначаються природними властивостями цих систем. Турбулентність виникає як при включенні вхідного інформаційного потоку, так і при його виключенні. Управління вхідним потоком не змінює якісний характер турбулентності, який визначається властивостями системи (1), але дозволяє зменшити величину викидів та сингулярності.

Отримані в даній роботі результати, застосовні у багатьох областях. Наприклад, силова установка автомобіля на холостих обертах може викликати сильні коливання корпусу автомобіля, навіть якщо він стоїть на місці. Під час руху збільшуються потужність і обороти двигуна, а трясіння корпусу зникає і далі залежить лише від

нерівностей дороги. Процеси виводу на повну потужність крупних енергетичних агрегатів, атомних реакторів тощо та їх зупинка також проявляють ознаки нестійкості.

Формулювання гіпотези сингулярності динаміки інцидентів кібербезпеки

Сфера забезпечення кібербезпеки, технології і техніки її забезпечення в історичному сенсі є молодими, але вже складними системами. Вони, як і сфера інформаційних технологій, а також як інформаційне суспільство, знаходяться в стадії становлення, ще не завершили свого етапу бурхливого розвитку. Більшість процедур руху, обробки й використання інформаційних потоків є циклічними. Як і в будь-якій складній системі з позитивними зворотними зв'язками, процеси обробки інформації та забезпечення кібербезпеки можуть мати області нестійкості, в них можуть мати місце турбулентність і сингулярність.

Гіпотеза обґрунтована завдяки створенню моделі процесу циклічної обробки інформаційного потоку системою, складеною із послідовності етапів обробки, пов'язаних прямими й зворотними взаємозв'язками, і кожен з етапів виконується циклічним повторенням операцій обробки інформаційного потоку. Гіпотеза підтверджується характером перехідного процесу від моменту включення на вході інформаційного потоку до встановлення стаціонарного режиму. На протязі перехідного процесу при певних параметрах моделі виникають біфуркації, турбулентності і сингулярність. Сингулярність є природною властивістю такого роду систем.

Для усунення сингулярності вирішальне значення мають методи управління перехідним процесом, методи обмеження інтенсивності інформаційних потоків в їх деструктивній частині та методи планування продуктивності систем обробки інформаційних потоків. Що стосується систем кібербезпеки, вказані методи лежать не лише в технічній і технологічних сферах, а в значній мірі в організаційній, соціальній та психологічних сферах.

Висновки

Гіпотеза щодо сингулярного характеру динаміки кількості інцидентів кібербезпеки обґрунтована завдяки застосуванню математичної моделі циклічного поетапного процесу обробки інформаційного потоку з включеними до нього етапами забезпечення кібербезпеки. Проведене дослідження моделі динамічних систем з чотирьохрівневим потоком показало, що в них можуть виникати стаціонарні квазіперіодичні коливання, біфуркації, а в перехідний період можливі турбулентність і сингулярність. Для усунення впливу сингулярностей необхідні додаткові позасистемні заходи, зокрема в організаційній, соціальній та психологічних сферах.

Список літератури

1. Обзор кибербезопасности / Рекомендация МСЭ-Т X.1205 // Безопасность электросвязи. – Женева: 2008. – 56 с.
2. Бурачок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурачок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа, за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
3. Захарченко, А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. – 2004. – № 2. – С. 50 – 55.
4. Котенко, И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. – СПб.: Наука, 2007. – Вып. 4 – С. 208-224. – Режим доступа: <http://www.proceedings.spiras.nw.ru/data/src/2007/04/00/spyproc-2007-04-00-15.pdf>.
5. Кононович, І.В. Динаміка кількості інцидентів інформаційної безпеки / І.В. Кононович // Інформатика та математичні методи в моделюванні. – 2014. – Т.3. – №3. – С. 35 - 43.

6. Кононович, В.Г. Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки / В.Г. Кононович, І.В. Кононович, Ю.В. Копитін, С.В. Стайкуца // Безпека інформації. – 2014. – Том 20. – № 1. – С. 83 - 91.
7. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world: [Електронний ресурс] // Cabinet Office 22 Whitehall London SW1A 2WH. Режим доступу: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
8. Малинецкий, Г.Г. Нелинейная динамика и хаос. Основные понятия: Учебное пособие. / Г.Г. Малинецкий, А.Б. Потапов. – М.: КомКнига, 2006. – 240 с.
9. Кононович, В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // Інформаційні управляючі системи та технології. – 2015. – С. 171 – 173.
10. Кононович, В.Г. Модель системы информационной безопасности консолидированной информации при информационном противоборстве (Раздел 16) / В.Г. Кононович, И.В. Кононович // Информационные технологии и защита информации в информационно-коммуникационных системах : монография / под редакцией В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – С. 220 – 233.
11. Кузнецов, Н.А. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба]; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. – Т.1 – 495 с.
12. Табор, М. Хаос и интегрируемость в нелинейных системах / М. Табор . Пер. с англ. – М.: Эдиториал УРСС, 2001. – 320 с.
13. Кузнецов, А.П. Введение в физику нелинейных отображений / А.П. Кузнецов, А.В. Савин, Л.В. Тюркина. – Саратов: изд-во «Научная книга», 2010. – 134 с.
14. Постнов, Д.Э. Методы нелинейной динамики: Учеб. Пособие для студ. физ. фак. / Д.Э. Постнов, А.Н. Павлов, С.В. Астахов. – Саратов, 2008. – 120 с.
15. Герега, А.Н. Моделирование самоорганизации динамических дисперсных систем. Спонтанная организация двухфазного потока / А.Н. Герега, Т.Л. Лозовский // Электронное моделирование. – 2008. – № 3. – Т. 30. – С. 3 - 12.

ГИПОТЕЗА И ФОРМАЛЬНАЯ МОДЕЛЬ СИНГУЛЯРНОЙ ДИНАМИКИ ИНЦИДЕНТОВ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

А.Н. Герега¹, С.А. Гнатюк², В.Г. Кононович³, И.В. Кононович¹

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

²Национальный авиационный университет
просп. Космонавта Комарова, 1, м Київ, 03680, Україна; e-mail: s.gnatyuk@nau.edu.ua

³Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net

Статистика свидетельствует о высоких темпах роста количества деструктивных инцидентов информационной безопасности. Но факторы, вызывающие это явление, исследованы недостаточно. Они не охватывают широкий спектр характеристик и не раскрывают полного формального и системного подхода к решению задач кибербезопасности. В связи с этим, сформулирована гипотеза относительно сингулярности динамики информационного потока с деструктивными и полезными характеристиками. Разработана простая математическая модель многоступенчатой обработки и фильтрации информационного потока с обратными связями для обеспечения кибербезопасности. Проведенное исследование четырех ступенчатой динамической системы показало, что в них могут возникать стационарные, квазипериодические колебания и динамический хаос. В переходной период могут возникать турбулентность и сингулярность. Использование механических аналогий способствовало более точному пониманию результатов исследования. Сделан вывод относительно объективности турбулентных и сингулярных явлений переходного периода и относительно необходимых внесистемных мероприятий обеспечения кибербезопасности.

Ключевые слова: кибернетическая безопасность, модель динамической системы, турбулентность, сингулярность, бифуркации, инциденты кибербезопасности

HYPOTHESIS AND FORMAL MODEL FOR SINGULAR DYNAMIC OF CYBERSECURITY INCIDENTS

O.M.Herega¹, S.O. Gnatyuk², V.G. Kononovich³, I.V. Kononovich¹

¹Odessa National Academy of Food Technologies

112, Kanatna Str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

²National Aviation University

1, Kosmonavta Komarova Ave, 03680 Kyiv, Ukraine; e-mail: s.gnatyuk@nau.edu.ua

³Odessa National Polytechnic University,

1, Shevchenko Str, Odessa, 65044, Ukraine; e-mail: konrac1993@gmail.com

Statistics show high rates of increase in the number of destructive information security incidents. But the factors that cause this phenomenon, investigated enough. They cover a wide range of characteristics and do not reveal the full formal and system approach to solving cyber security tasks. Accordingly, a hypothesis on the dynamics of information flow singularity of destructive and beneficial characteristics was formulated. A simple mathematical model of multi-processing and filtering the information flow with feedback to ensure cybersecurity was developed. The study of four-stage dynamic system showed that it may have fixed quasi-periodic oscillations and dynamic chaos. In the transition period turbulence and singularity are possible. The use of mechanical analogies contributed to a more accurate understanding of research results. The conclusion was made about objectivity and singularity phenomena of turbulent transition and exogenous on the necessary measures to ensure cybersecurity.

Keywords: cybernetic security, model of dynamic system, turbulent, singularly, bifurcation, cybersecurity incident

CONSTRUCTING OF MINIMAX CLASS OF PERFECT BINARY ARRAYS OF ORDER $N = 6$ FOR MULTI-CHANNEL CRYPTOGRAPHIC INFORMATION TRANSFER SYSTEM

N.I. Kushnirenko, V.Y. Chechelnytskyi, L.A. Kuznetsova

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

This paper presents a method for constructing of the minimax class of perfect binary arrays with order $N = 6$. Maximum peak level of the two-dimensional periodic cross-correlation function between perfect binary arrays of minimax class has been evaluated. Power of the minimax class has been determined. Development of method is based on analysis of structural and correlation properties of thinned matrices. Paper proposes the method for single-channel and multi-channel cryptographic information transfer systems design. These systems are based on codes designed on the basis of minimax class of perfect binary arrays. Limits on the number of channels in multi-channel system determined. The method for overcoming of these limitations proposed.

Keywords: the minimax class, the perfect binary array, error-correcting codes, cryptographic information transfer systems, information security

Introduction

At the present time the heightened attention is paid to the effective application of perfect binary arrays (PBAs). Such structures can be used to solve problems of information security, error-correcting coding, radar and other related areas that directly reflected in contemporary scientific papers. PBAs have attractive correlation properties and allow simple technical implementation of devices for their formation and processing.

As shown in [1] the new classes of error-correcting codes can be built on the basis of the PBAs. Such codes have attractive properties and a number of advantages in comparison to many well-known codes, including BCH codes. Moreover, these codes can be processed using majority decoding. On the other hand, the PBA classes have a very large power which riches billion of arrays depending on the order of PBAs. Owing to this the PBAs can find wide application in the cryptographic information transfer systems design [2-3].

Properties of PBAs of order $N = 2^k$, where k is arbitrary integer, and algorithms for their constructing are well known and widely discussed in domestic and foreign papers. However, PBAs of order $N = 3 \cdot 2^k$ require detailed consideration. There are no known algorithms for constructing of PBAs classes of these orders with desired properties, such as minimax class and classes with constant level of cross-correlation.

The aim of the research

Search of the minimax class on the basis of complete PBA class is fairly complex computational task. The aim of this study is to develop a constructive algorithm for formation of the minimax class of PBA with order $N = 6$ based on the properties of the PBAs and their thinned matrices.

The following problems must be solved to achieve this:

- consider the structural and correlation properties of PBAs' thinned matrices;
- determine the imbalance parameter for PBA of order $N = 6$ and its influence to PBA construction;
- formulate and substantiate rules for formation of minimax class of PBA with order $N = 6$;
- determine magnitude of side lobe of two-dimensional periodic cross-correlation function and power of minimax class for PBAs of order $N = 6$;
- evaluate the effect of inversion and cyclic shift of rows and/or columns of any PBA from minimax class on magnitude of side peaks of two-dimensional periodic cross-correlation function between the given PBA and the rest of the PBAs in this class;
- evaluate the effect of the thinned matrices location in PBAs on formation of minimax class.

Main Body

Minimax class contains all possible combinations of different PBAs for which the two-dimensional periodic cross-correlation function (2D PCCF) between any two PBAs $P^0(N)$ and $P^1(N)$ from this class has minimum modulus of maximum peak. Such class is known as $M(N)$ - class of PBAs [1].

The two-dimensional periodic autocorrelation function (2D PACF) of PBA always has peak of value N^2 . Level of interfering signals or level of maximum 2D PCCF peaks (ρ) for PBAs of minimax class required for correct detection of PBA in receiver under the influence of signals constructed on the basis of PBAs is given below

$$\rho < N^2 / 2. \quad (1)$$

As stated in [4], each PBA $P(N)$ by its thinning in spatial coordinates can be presented as four thinned matrices of order $N / 2$.

For example, for an arbitrary array $P^0(6)$

$$P^0(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & - & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix} \quad (2)$$

the thinned matrices are given below

$$A(3) = \begin{bmatrix} - & - & - \\ + & + & + \\ + & + & + \end{bmatrix}, \quad B(3) = \begin{bmatrix} - & + & + \\ - & + & + \\ - & + & + \end{bmatrix}, \quad C(3) = \begin{bmatrix} - & + & + \\ + & - & + \\ + & + & - \end{bmatrix}, \quad \bar{D}(3) = \begin{bmatrix} - & - & + \\ - & + & - \\ + & - & - \end{bmatrix}.$$

It was found that for PBA of order $N = 6$ there is a finite number of thinned matrices of order $N/2 = 3$ [5], whose $4! = 24$ permutations lead to the construction of the PBA. Such structures are shown in Table 1.

Table 1.

Thinned matrices of order $N/2=3$

$A_0(3)$	$A_1(3)$	$A_2(3)$	$\bar{A}_0(3)$	$\bar{A}_1(3)$	$\bar{A}_2(3)$
$\begin{bmatrix} - & - & - \\ + & + & + \\ + & + & + \end{bmatrix}$	$\begin{bmatrix} + & + & + \\ - & - & - \\ + & + & + \end{bmatrix}$	$\begin{bmatrix} + & + & + \\ + & + & + \\ - & - & - \end{bmatrix}$	$\begin{bmatrix} + & + & + \\ - & - & - \\ - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - \\ + & + & + \\ - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - \\ - & - & - \\ + & + & + \end{bmatrix}$
$B_0(3)$	$B_1(3)$	$B_2(3)$	$\bar{B}_0(3)$	$\bar{B}_1(3)$	$\bar{B}_2(3)$
$\begin{bmatrix} - & + & + \\ - & + & + \\ - & + & + \end{bmatrix}$	$\begin{bmatrix} + & - & + \\ + & - & + \\ + & - & + \end{bmatrix}$	$\begin{bmatrix} + & + & - \\ + & + & - \\ + & + & - \end{bmatrix}$	$\begin{bmatrix} + & - & - \\ + & - & - \\ + & - & - \end{bmatrix}$	$\begin{bmatrix} - & + & - \\ - & + & - \\ - & + & - \end{bmatrix}$	$\begin{bmatrix} - & - & + \\ - & - & + \\ - & - & + \end{bmatrix}$
$C_0(3)$	$C_1(3)$	$C_2(3)$	$\bar{C}_0(3)$	$\bar{C}_1(3)$	$\bar{C}_2(3)$
$\begin{bmatrix} - & + & + \\ + & - & + \\ + & + & - \end{bmatrix}$	$\begin{bmatrix} + & - & + \\ + & + & - \\ - & + & + \end{bmatrix}$	$\begin{bmatrix} + & + & - \\ - & + & + \\ + & - & + \end{bmatrix}$	$\begin{bmatrix} + & - & - \\ - & + & - \\ - & - & + \end{bmatrix}$	$\begin{bmatrix} - & + & - \\ - & - & + \\ + & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & + \\ + & - & - \\ - & + & - \end{bmatrix}$
$D_0(3)$	$D_1(3)$	$D_2(3)$	$\bar{D}_0(3)$	$\bar{D}_1(3)$	$\bar{D}_2(3)$
$\begin{bmatrix} + & + & - \\ + & - & + \\ - & + & + \end{bmatrix}$	$\begin{bmatrix} - & + & + \\ + & - & + \\ + & - & + \end{bmatrix}$	$\begin{bmatrix} + & - & + \\ - & + & + \\ + & + & - \end{bmatrix}$	$\begin{bmatrix} - & - & + \\ + & - & - \\ + & - & - \end{bmatrix}$	$\begin{bmatrix} + & - & - \\ - & - & + \\ - & + & - \end{bmatrix}$	$\begin{bmatrix} - & + & - \\ + & - & - \\ - & - & + \end{bmatrix}$

The 2D PACFs for thinned matrices from Table 1 are given in Table 2.

Table 2.

2D PACFs of thinned matrices of order $N/2=3$

Types of thinned matrices	$A_0(3), A_1(3), A_2(3), \bar{A}_0(3), \bar{A}_1(3), \bar{A}_2(3)$	$B_0(3), B_1(3), B_2(3), \bar{B}_0(3), \bar{B}_1(3), \bar{B}_2(3)$	$C_0(3), C_1(3), C_2(3), \bar{C}_0(3), \bar{C}_1(3), \bar{C}_2(3)$	$D_0(3), D_1(3), D_2(3), \bar{D}_0(3), \bar{D}_1(3), \bar{D}_2(3)$
2D PACF of thinned matrices	$R_A = \begin{bmatrix} 9 & 9 & 9 \\ -3 & -3 & -3 \\ -3 & -3 & -3 \end{bmatrix}$	$R_B = \begin{bmatrix} 9 & -3 & -3 \\ 9 & -3 & -3 \\ 9 & -3 & -3 \end{bmatrix}$	$R_C = \begin{bmatrix} 9 & -3 & -3 \\ -3 & 9 & -3 \\ -3 & -3 & 9 \end{bmatrix}$	$R_D = \begin{bmatrix} 9 & -3 & -3 \\ -3 & -3 & 9 \\ -3 & 9 & -3 \end{bmatrix}$

Statement 1. Value of elements imbalance in thinned matrices of order $N/2=3$

$$\Delta = K^{(+)} - K^{(-)} = \pm N ,$$

where $K^{(+)}$ and $K^{(-)}$ is number of symbols +1 and -1 respectively, is given below

$$\Delta_{A(3)} = \Delta_{B(3)} = \Delta_{C(3)} = \Delta_{D(3)} = N / 2 = 3 ,$$

$$\Delta_{\bar{A}(3)} = \Delta_{\bar{B}(3)} = \Delta_{\bar{C}(3)} = \Delta_{\bar{D}(3)} = -N / 2 = -3 .$$

If the element imbalance of PBA has a positive value such a PBA is called direct. For the negative value of the element imbalance the PBA is called inverse.

Property 1. The PBA can be constructed from three direct matrices and one inverse and vice versa. Only in this case element imbalance of resulting PBA is equal to $\Delta = \pm 6$.

For development of minimax class constructing method the 2D PCCF calculated for $P^1(N)$ и $P^2(N)$ PBAs will be used. It is denoted as follows

$$B(N) = \|b_{m,n}\|, \quad (3)$$

where $m = \overline{0, N_1 - 1}$ — numbers of 2D PCCF rows; $n = \overline{0, N_2 - 1}$ — numbers of 2D PCCF columns.

Elements of 2D PCCF (3) between PBAs $P^1(N)$ and $P^2(N)$ are calculated using an equation

$$b_{m,n} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} p_{i,j}^1 p_{i+m,j+n}^2 ,$$

where $p_{i,j}^1$ — elements of $P^1(N)$ PBA; $p_{i,j}^2$ — elements of $P^2(N)$ PBA; while values $i+m$ and $j+n$ are calculated modulo N .

The following task must be solved for construction of minimax class. Suppose that an arbitrary PBA is given. It will be used as the base PBA for minimax class formation.

Let use for our purpose the PBA (2). It is known [4] that for new PBA constructing from thinned matrices of the base PBA the next methods can be used:

- cyclic shifts of rows and/or columns of thinned matrices;
- inverse of thinned matrices elements;
- permutation of thinned matrices.

Consider all these methods in detail.

2D PCCF between the base PBA of size 6×6 and PBA with cyclically shifted rows and/or columns of thinned matrices was analyzed. It was found that magnitude of 2D PCCF side lobe maximum peak is 24 and it contradicts (1).

Consider an inverse of PBA's thinned matrices elements. Base array (2) consists of thinned matrices

$$A(3)B(3)C(3)\bar{D}(3). \quad (4)$$

Property 1. Can be accomplished if PBA will be formed without thinned matrices permutation and using the following rules

$$\left. \begin{aligned} P^0(6) &= A(3)B(3)C(3)\bar{D}(3), P^1(6) = A(3)B(3)\bar{C}(3)D(3), \\ P^2(6) &= A(3)\bar{B}(3)C(3)D(3), P^3(6) = \bar{A}(3)B(3)C(3)D(3), \\ P^4(6) &= \bar{A}(3)\bar{B}(3)\bar{C}(3)D(3), P^5(6) = \bar{A}(3)\bar{B}(3)C(3)\bar{D}(3), \\ P^6(6) &= \bar{A}(3)B(3)\bar{C}(3)\bar{D}(3), P^7(6) = A(3)\bar{B}(3)\bar{C}(3)\bar{D}(3). \end{aligned} \right\}. \quad (5)$$

Calculation of 2D PCCF between all PBAs constructed on the basis of rules (5) gives the following combinations of PBAs for which the maximum magnitude of 2D PCCF side lobe is $\rho = \pm 12$

$$\left. \begin{aligned} P^0(6) &= A(3)B(3)C(3)\bar{D}(3) \\ P^1(6) &= A(3)B(3)\bar{C}(3)D(3) \\ P^2(6) &= A(3)\bar{B}(3)C(3)D(3) \\ P^3(6) &= \bar{A}(3)B(3)C(3)D(3) \end{aligned} \right\}. \quad (6)$$

However, more combinations from (5) can lead to appropriate maximum peaks.

Property 2. The inverse of one PBA from minimax class does not lead to increasing of 2D PCCF side peaks for given PBA and other PBAs from minimax class.

Other combinations can be obtained by replacing each row in (6) with its inverted form. The expression (6) is a combination of direct thinned matrices for which the 2D PCCF has maximum peaks no greater than $\rho = \pm 12$ and this expression it taken as a base.

Further research allowed revealing of the following property.

Property 3. Cyclic shift by rows and/or columns of one PBA from minimax class does not lead to increasing of 2D PCCF side peaks for given PBA and other PBAs from minimax class.

The matrices (7) are constructed on the basis of rule (6).

Maximum magnitude of 2C PCCF side lobes between PBAs from (6) is not greater than $\rho = \pm 12$ which is acceptable (1) for a minimax class.

$$\begin{aligned}
 P^0(6) &= \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}, \quad P^1(6) = \begin{bmatrix} - & - & - & + & - & + \\ + & + & - & + & - & - \\ + & - & + & + & + & + \\ - & + & + & - & - & + \\ + & - & + & + & + & + \\ - & - & - & + & + & + \end{bmatrix}, \\
 P^2(6) &= \begin{bmatrix} - & + & - & - & - & - \\ - & + & + & + & + & - \\ + & + & + & - & - & + \\ + & + & - & - & + & + \\ + & + & + & - & - & - \\ + & - & + & + & - & + \end{bmatrix}, \quad P^3(6) = \begin{bmatrix} + & - & + & + & + & + \\ - & + & + & + & + & - \\ - & - & - & + & - & + \\ + & + & - & - & + & + \\ - & - & - & + & - & + \\ + & - & + & + & - & + \end{bmatrix}.
 \end{aligned} \tag{7}$$

Evaluate an effect of thinned matrices permutation in the PBA $P^1(6)$ on 2D PCCF between $P^0(6)$ and $P^1(6)$. Permute thinned matrices $B(3)$ and $C(3)$ in PBA $P^1(6)$

$$A(3)C(3)B(3)\bar{D}(3) \tag{8}$$

and calculate 2D PCCF for PBAs $P^0(6)$ and $P^1(6)$

$$\begin{aligned}
 P^0(6) &= \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}, \quad P^1(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & + & + & - & + & + \\ - & - & + & + & + & - \\ + & + & + & + & + & - \\ - & + & + & - & + & - \end{bmatrix}, \quad B(6) = \begin{bmatrix} 20 & 0 & 8 & 0 & 8 & 0 \\ 0 & 4 & 0 & -8 & 0 & 4 \\ -4 & 0 & -4 & 0 & 8 & 0 \\ 0 & 16 & 0 & -8 & 0 & -8 \\ -4 & 0 & 8 & 0 & -4 & 0 \\ 0 & 4 & 0 & 4 & 0 & -8 \end{bmatrix}.
 \end{aligned} \tag{9}$$

Two thinned matrices $A(3)$ and $\bar{D}(3)$ keep initial locations (4) and (8). Magnitude of 2D PCCF maximum peak (9) is quite high. It can be concluded that for the creation of new PBAs for the minimax class the thinned matrices should not be repeated in their places. It is possible, for example, in case of following thinned matrices permutations

$$\begin{aligned}
 &A(3)B(3)C(3)\bar{D}(3), \\
 &A(3)C(3)\bar{D}(3)B(3), \\
 &A(3)\bar{D}(3)B(3)C(3).
 \end{aligned}$$

2D PCCF for these thinned matrices presented in Table 3.

The above approach and the properties of thinned matrices of PBA with order $N = 6$ allow creation of a stepwise algorithm for constructing of minimax arrays on the basis of any arbitrary base PBA.

Algorithm

Step 1. Construct by any known method the base PBA of order $N = 6$ and present it in the form of thinned matrices of order $N / 2 = 3$ by thinning in the spatial coordinates.

Step 2. Calculate 2D PCCF for each matrix.

Step 3. Taking into account the Property 1 determine which of thinned matrices is inverted in relation to the other. Denote inverted matrix as $\bar{D}(3)$ and other as $A(3)$, $B(3)$ and $C(3)$ in any order.

Step 4. Construct PBAs using equations

$$\left. \begin{array}{lll} A(3)B(3)C(3)\bar{D}(3), & A(3)B(3)\bar{C}(3)D(3), & A(3)\bar{B}(3)C(3)D(3), \\ \bar{A}(3)B(3)C(3)D(3), & A(3)D(3)B(3)\bar{C}(3), & A(3)D(3)\bar{B}(3)C(3), \\ A(3)\bar{D}(3)B(3)C(3), & \bar{A}(3)D(3)B(3)C(3), & A(3)C(3)D(3)\bar{B}(3), \\ A(3)C(3)\bar{D}(3)B(3), & A(3)\bar{C}(3)D(3)B(3), & \bar{A}(3)C(3)D(3)B(3). \end{array} \right\}.$$

Table 3.

Two-dimensional periodic cross-correlation functions

PBA 1	PBA 2	2D PCCF
$A(3)B(3)C(3)\bar{D}(3)$	$A(3)C(3)\bar{D}(3)B(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & + & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & + \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} 8 & 12 & 8 & 0 & 8 & 0 \\ 8 & -4 & -4 & -4 & -4 & 8 \\ -4 & 0 & -4 & 0 & -4 & 12 \\ 8 & 8 & -4 & -4 & -4 & -4 \\ -4 & 0 & -4 & 12 & -4 & 0 \\ 8 & -4 & -4 & 8 & -4 & -4 \end{bmatrix}$
$A(3)B(3)C(3)\bar{D}(3)$	$A(3)\bar{D}(3)B(3)C(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & + & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & + & + & - & + & - \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} 8 & -4 & 8 & -4 & 8 & 8 \\ 12 & 8 & 0 & -4 & 0 & -4 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ 0 & 8 & 0 & -4 & 12 & -4 \\ -4 & -4 & -4 & 8 & -4 & -4 \\ 0 & 8 & 12 & -4 & 0 & -4 \end{bmatrix}$
$A(3)C(3)\bar{D}(3)B(3)$	$A(3)\bar{D}(3)B(3)C(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & + \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & + & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & + & + & - & + & - \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} 8 & 8 & 8 & -4 & 8 & -4 \\ -4 & 0 & 8 & 0 & -4 & 12 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ -4 & 0 & -4 & 12 & 8 & 0 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ 8 & 12 & -4 & 0 & -4 & 0 \end{bmatrix}$

Thus, it was found that the power of PBA minimax class is $\Psi_M(6)=12$ perfect binary arrays, while the magnitude of the maximum peak is $\rho=\pm 12$.

Minimax class of PBA is given in Table 4.

Table 4.

 Minimax class of PBA with order $N = 6$

$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ + & + & - & + & - & - \\ + & - & + & + & + & + \\ - & + & + & - & - & + \\ + & - & + & + & + & + \\ - & - & - & + & + & + \end{bmatrix}$	$\begin{bmatrix} - & + & - & - & - & - \\ - & + & + & + & + & - \\ + & + & + & - & + & - \\ + & + & + & - & + & + \\ + & + & + & - & + & + \\ + & + & + & - & + & + \end{bmatrix}$	$\begin{bmatrix} + & - & + & + & + & + \\ - & + & + & + & + & - \\ - & - & + & + & - & + \\ + & + & - & - & + & + \\ - & - & - & + & - & + \\ + & - & + & + & - & + \end{bmatrix}$
$\begin{bmatrix} - & + & - & + & - & - \\ - & + & + & - & + & - \\ + & + & + & - & + & + \\ - & - & + & + & + & - \\ + & - & + & + & + & + \\ - & - & + & + & + & + \end{bmatrix}$	$\begin{bmatrix} - & + & - & + & - & - \\ + & - & - & + & + & - \\ + & + & + & - & + & + \\ + & + & + & - & + & + \\ + & + & + & - & + & + \\ + & + & + & - & + & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & - & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & + & + & - & + & + \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} + & + & + & + & + & - \\ - & - & + & + & + & + \\ - & + & - & - & + & + \\ - & + & + & - & + & + \\ - & - & - & + & - & + \\ - & + & + & + & + & - \end{bmatrix}$
$\begin{bmatrix} - & - & - & + & - & + \\ + & + & + & - & + & + \\ + & + & + & - & + & + \\ + & + & + & - & + & + \\ + & + & + & + & - & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & - \\ + & + & + & + & - & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & + & - & - & - & - \\ - & + & + & + & + & - \\ + & - & + & + & + & - \\ + & - & - & + & + & + \\ + & - & + & - & + & + \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} + & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & - & - & + & + \\ + & - & - & + & + & + \\ - & + & - & + & - & + \\ - & - & + & + & + & + \end{bmatrix}$

It is possible to develop a new class of multiparametric error-correcting $M(n)$ -codes of length $n = N^2$ on the basis of minimax class of PBA. Their properties and procedures of coding and decoding studied in [1].

It is assumed that the encoder and decoder of authorized users utilize for coding and decoding of each next symbol the same PBA from the equivalence class. Such PBA is constructed on the basis of one PBA (base PBA) from minimax class by means of cyclic shifts of rows and/or columns. Base PBAs are operatively changed for each symbol according to some algorithm, which managed by a secret key. It is this array determines a code word of $M(n)$ -code which will be applied for the transmission of next message.

An attacker is not able to determine which PBA from minimax class determined parameters of message transmission in system. Only fact of message transmission can be revealed. Thus, it is possible to create a single-channel cryptographic information transfer system on the basis of single PBA of minimax class. For all other PBAs from minimax class similar systems can be built.

Due to the fact that the signals based on the PBA of the minimax class are the minimax as well, they have a minimal impact on the other signals, which are built on the basis of other PBAs from minimax class. Therefore, the single-channel cryptographic information transfer systems can be used to transmit information in a single communication channel on condition that all the signals are constructed on the basis of the same minimax class. The number of channels of multi-channel cryptographic information transfer system is determined by the power of minimax class of PBAs.

Hypothetically, it is clear that with the growth of the PBA order the power of minimax class and number of channels in multi-channel cryptographic information transfer system grows as well. However, the redundancy of $M(n)$ -code which is used for a single character of the original message transmission increases correspondingly. Thus, it is possible to provide any desired number of channels in a multi-channel cryptographic information transfer system by reducing the transmission rate, since the growth of minimax class power causes an increase of $M(n)$ -code redundancy.

Conclusions

This paper presents an algorithm for constructing of minimax class of PBAs with order $N = 3 \cdot 2^k$ which can become the basis for creation of recurrent algorithms for constructing of $M(N)$ -classes for PBAs of arbitrary orders.

A method of constructing a single-channel cryptographic information transfer system proposed. It is shown how a multi-channel system can be organized. Limits on the number of channels in this information transfer system determined. The way and cost of an increase in number of channels discussed.

References

1. Мазурков, М.И. Класс минимаксных корректирующих кодов на основе совершенных двоичных решеток / М.И. Мазурков // Радиоэлектроника (Изв. вузов). – 2011. – №9. – С. 24-39.
2. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника (Изв. вузов). – 2008. – № 11. – С. 53-57.
3. Кушниренко, Н.И. Метод криптографической передачи информации на базе эквивалентного класса совершенных двоичных решеток / Н.И. Кушниренко, В.Я. Чечельницкий // Информатика та математичні методи в моделюванні. — 2014. — Т.4. — №3. — С. 210-218.

4. Чечельницький, В.Я. Метод построения полного класса совершенных двоичных решеток порядка $N = 2^k$ / В.Я. Чечельницький // Радиоэлектроника (Изв. вузов). – 2006. – №9. – С. 44-53.
5. Мазурков, М.И. Свойства полного класса совершенных двоичных решеток на 36 элементов / М.И. Мазурков, В.Я. Чечельницький // Радиоэлектроника (Изв. вузов). – 2004. – № 6. – С. 56-64.

ПОБУДОВА МІНІМАКСНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШІТОК ПОРЯДКУ $N=6$ ДЛЯ БАГАТОКАНАЛЬНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Н.І. Кушніренко, В.Я. Чечельницький, Л.А. Кузнецова

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

У роботі представлено метод побудови мінімаксного класу досконалих двійкових решіток порядку $N=6$, встановлена його потужність, визначено рівень максимальних піків двовимірної періодичної взаємкореляційної функції між досконалими двійковими решітками мінімаксного класу. Даний метод розроблений на основі аналізу структурних і кореляційних властивостей проріджених матриць досконалих двійкових решіток. Запропоновано метод побудови одноканальної і багатоканальної криптографічних систем передачі інформації на основі кодів, які розроблені на базі мінімаксного класу досконалих двійкових решіток. Наведено обмеження на кількість каналів багатоканальної системи і зазначений спосіб подолання цих обмежень.

Ключові слова: мінімаксний клас, досконала двійкова решітка, проріджена матриця, коректувальні коди, криптографічна система передачі інформації, захист інформації

ПОСТРОЕНИЕ МИНИМАКСНОГО КЛАССА СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК ПОРЯДКА $N=6$ ДЛЯ МНОГОКАНАЛЬНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Н.И. Кушниренко, В.Я. Чечельницький, Л.А. Кузнецова

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

В работе представлен метод построения минимаксного класса совершенных двоичных решеток порядка $N=6$, установлена его мощность, определен уровень максимальных пиков двумерной периодической взаимокорреляционной функции между совершенными двоичными решетками минимаксного класса. Данный метод разработан на основе анализа структурных и корреляционных свойств прореженных матриц совершенных двоичных решеток. Предложен метод построения одноканальной и многоканальной криптографической системы передачи информации на основе кодов, которые построены на базе минимаксного класса СДР. Приведены ограничения на количество каналов многоканальной системы и указан способ преодоления этих ограничений.

Ключевые слова: минимаксный класс, совершенная двоичная решетка, прореженная матрица, корректирующие коды, криптографическая система передачи информации, защита информации

АНАЛИЗ МЕХАНИЗМА ВОЗНИКНОВЕНИЯ ПАРАЗИТНЫХ ПРОЦЕССОВ В АППАРАТУРЕ ЦИФРОВОЙ ФОТО И ВИДЕОЗАПИСИ, ПРИГОДНЫХ ДЛЯ ИСПОЛЬЗОВАНИЯ ПРИ ЭКСПЕРТИЗЕ ТАКИХ УСТРОЙСТВ

О.В. Рыбальский, В.В. Журавель

Национальная академия внутренних дел,
пл. Соломянская, 1, Киев, 03056, Украина; e-mail: rybalsky_ol@mail.ru

Проведен анализ конструктивных и технологических особенностей модели аппаратуры цифровой фото и видеозаписи. Показано, что паразитные процессы, возникающие в элементах матриц и аналого-цифровых преобразователей, носят устойчивый индивидуальный характер. Предложено использование этих процессов для получения идентификационных признаков, пригодных для использования в экспертизе целостности и достоверности информации, содержащейся в видеограммах. Данные признаки носят фрактальный характер, что может быть использовано при их выделении из шумов цифровых изображений и последующей статистической обработке. Применение этих признаков в экспертизе соответствует теории криминалистической идентификации.

Ключевые слова: аппаратура цифровой фото и видео записи, цифровое изображение, светочувствительный элемент, аналого-цифровой преобразователь, фрактал, целостность информации, экспертиза

Введение

Материалы фото и видеозаписи давно используются в правоохранительной деятельности при расследовании преступлений. Порядок их использования при формировании доказательной базы основан на ряде процессуальных требований, предусматривающих, в частности, обязательное проведение экспертизы. Цель такой экспертизы – проверка целостности и достоверности информации, предоставляемой следствию и суду на фотоснимках и видеозаписях.

Появление цифровых методов и аппаратуры фиксации изображений потребовало создания новой инструментальной базы, необходимой для проведения экспертизы материалов и средств цифровой фото и видеозаписи.

Для создания такого инструментария необходимо провести системный анализ конструктивного и технологического устройства аппаратуры для такой записи [1]. На основании проведенного анализа можно установить идентификационные признаки, пригодные для создания такого инструментария. Наиболее пригодными для получения таких признаков являются паразитные процессы, возникающие в аппаратуре записи, и фиксируемые на носителях в шумах записываемых видеограмм. Такие процессы возникают за счет технологических погрешностей изготовления деталей и узлов аппаратуры записи, определяемых установленными для них полями допусков.

Цель статьи – проведение системного анализа конструктивных и технологических особенностей аппаратуры цифровой фото и видеозаписи (АЦФВЗ), установления

механизма возникновения в них паразитных процессов и выбора процессов, пригодных для использования в качестве базовых для получения идентификационных признаков. При этом такие признаки должны отвечать требованиям теории криминалистической идентификации [1].

Основная часть

Для анализа механизма возникновения процессов, происходящих при цифровой видеозаписи, необходимо рассмотреть устройство аппаратуры видео и фотозаписи сигналов в цифровой форме. Отметим, что принципиальных отличий в устройстве цифровых видеокамер и фотоаппаратов с точки зрения преобразования изображения в цифровую форму и его последующей записи нет. Цифровая видеозапись состоит из цифровых фотографий, размещенных и воспроизводимых во времени в последовательном порядке с определенной скоростью смены изображений (кадров). Нижний предел этой скорости, как правило, определяется возможностью восприятия человеком изображения как отдельного фотоснимка. Поэтому рассматриваемое ниже устройство такой аппаратуры в равной степени относится и к цифровым фотоаппаратам, и к видеокамерам. Схематично это устройство представлено на рис. 1.

В такую аппаратуру входят: объектив с сопряженной с ним створкой затвора и регулируемой диафрагмой (оптическая система); световоспринимающая матрица, состоящая из изолированных светочувствительных элементов; аналого-цифровой преобразователь (АЦП) считывания и преобразования в цифровой код уровня электрического заряда светочувствительных элементов; генератор тактовой частоты для синхронизации процессов преобразования, обработки и запоминания записанных сигналов. Кроме того, в такой аппаратуре имеется оперативное запоминающее устройство, твердотельный носитель записанной цифровой информации и дисплей. Разумеется, в аппаратуру входит блок управления, но оценка его влияния на рассматриваемые процессы будет проведена ниже. Ранее необходимо рассмотреть работу такой аппаратуры и оценить функции, выполняемые каждым из ее узлов и блоков, приведенных на рис.1. Рассмотрим их функциональное взаимодействие при записи цифрового изображения.

Объектив с регулируемой диафрагмой увеличивает и фокусирует изображение, подлежащее записи, а затвор обеспечивает необходимое время экспозиции. Таким образом, аналогами процессов, происходящих в оптической системе АЦФВЗ, являются аналоговое усиление и дискретизация светового потока. Дискретный световой поток поступает на светочувствительную матрицу, где его интенсивность фиксируется на его элементах. При этом дискретный световой поток подвергается повторному процессу дискретизации (передискретизации), поскольку разбивается по отдельным элементам матрицы. Частота этой передискретизации определяется количеством изолированных светочувствительных элементов, но она не является окончательной.

Окончательный период дискретизации определяется периодом сканирования светочувствительных элементов матрицы в АЦП, где происходит преобразование уровней аналоговых электрических зарядов, пропорциональных световому потоку, в цифровой код, подлежащий последующему запоминанию. Эти процессы представлены на временной диаграмме (рис.2).

На диаграмме (рис.2) показано, что на весь процесс преобразования изображения в цифровую форму отводится временной промежуток, не превышающий время между двумя экспонированиями (время смены кадра). Тогда период дискретизации АЦП определится как

$$T_{дэ} = \frac{T_{СКМ}}{N} = \frac{T_{ЭКС} - T_{ВЫД}}{N}, \quad (1)$$

где N – количество светочувствительных элементов матрицы, $T_{дэ}$, $T_{СКМ}$, $T_{ЭКС}$, $T_{ВЫД}$ определяются в соответствии с рис.2.



Рис. 1. Функциональная схема цифрового аппарата записи изображений

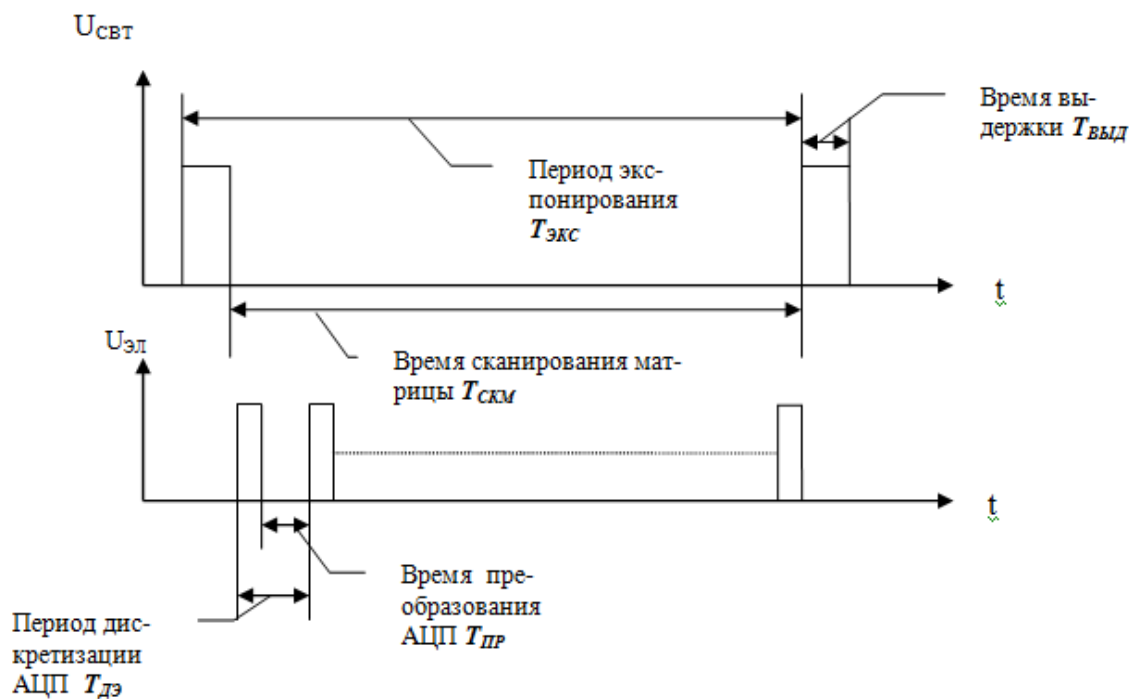


Рис. 2. Временная диаграмма процессов экспонирования и преобразования светового потока в цифровую форму

За это время в АЦП происходит процесс выборки с длительностью $\Delta_{\text{ВЫБ}}$ и последующий процесс преобразования выбранной величины сигнала в двоичный код. При этом время преобразования АЦП определяется как

$$T_{\text{ПР}} = T_{\text{ДЭ}} - \Delta_{\text{ВЫБ}}. \quad (2)$$

Для определения идентификационных признаков, возникающих в течение экспонирования и аналого-цифрового преобразования изображений, необходимо исследовать паразитные процессы, протекающие в это время. При этом воспользуемся методом суперпозиции, и будем рассматривать отдельно процессы, протекающие в каждом из узлов и блоков, показанных на рис. 1.

Рассмотрим паразитные процессы, возникающие в оптической системе в процессе экспонирования. Мы полагаем, что к таким процессам следует отнести нестабильность периода экспонирования $T_{\text{ЭК}}$, возникающую за счет, например, нестабильности генератора сигнала управления или механического затирания шторки затвора. Такая нестабильность носит индивидуальный характер в силу индивидуальности технологических погрешностей (в пределах полей допусков) деталей и узлов, входящих в оптическую систему АЦФВЗ. Однако ее использование, по нашему мнению, не представляется возможным, т.к. сигнал этой нестабильности никак не проявляется в конечном изображении, представленном в цифровой форме.

Нестабильность периода дискретизации АЦП $T_{\text{ДЭ}}$ также никак не фиксируется в цифровом изображении и поэтому непригодна для использования в качестве идентификационного признака.

Рассмотрим светочувствительную матрицу. Она состоит из миллионов изолированных светочувствительных элементов (пикселей), имеющих технологические допуски на свои характеристики преобразования уровня освещенности и цвета в уровни электрического заряда. Также допусками предусматривается наличие некоторого количества «пустых» пикселей. Расположение таких дефектных пикселей на каждом экземпляре матрицы носит устойчивый индивидуальный характер. И, что самое главное, эти индивидуальные особенности матриц фиксируются в цифровых изображениях. Более того, шумы, создаваемые влиянием таких технологических дефектов, носят фрактальный характер и, следовательно, могут быть выделены и обработаны [2]. Таким образом, они пригодны для проведения сравнительных исследований и могут быть приняты в качестве идентификационных признаков.

В АЦФВЗ, в отличие от аппаратуры цифровой звукозаписи, используются АЦП с параллельным способом преобразования. Однако, поскольку и при этом способе преобразования в АЦП обязательно используется квантователь уровня (КУ), то в них возникают те же погрешности передачи, что и в АЦП последовательных приближений. Поэтому все положения, связанные с проявлением немонотонности статической характеристики (НСХ) КУ в оцифрованных звуковых сигналах, полностью относятся и к цифровым изображениям [3]. Исходя из этого, НСХ КУ АЦП также следует признать идентификационным признаком. Поскольку эти проявления также носят фрактальный характер, то и они могут использоваться для проведения сравнительных исследований [2].

Разумеется, что эти две группы признаков носят независимый характер и фиксируются в цифровом изображении. Поэтому сравнение двух цифровых изображений будет проводиться по интегральному признаку, связанному с образованием в их шумах самоподобных структур. Исходя из независимости событий [4], вероятность совпадения расположения и количества дефектных мест матриц и дефектных уровней КУ для двух черно-белых видеокамер среднего качества одного типа составляет

$$P_{\Sigma} = P_M^2 \cdot P_{HCK}^2 = \frac{1}{M^2} \cdot \frac{1}{K^2} \approx 2,2 \cdot 10^{-30}, \quad (3)$$

где P_M^2 – вероятность совпадения положения пикселей в двух однотипных матрицах, P_{HCK}^2 – вероятность совпадения положения в двух КУ двух уровней квантования, M – объем матрицы для видеокамеры среднего качества (2400x1200 пикс.), $K = 2^{16}$ – количество уровней квантования для 16-разрядного КУ.

При такой вероятности совпадения идентификационных признаков для двух видеокамер, очевидно, что образовавшиеся в их шумах фрактальные структуры будут принадлежать к различным совокупностям, поскольку вид этих фракталов зависит от положения дефектных участков, как в матрицах, так и в КУ АЦП [5].

Это, в свою очередь, означает возможность их получения из шумов цифровых изображений и статистическую обработку, что обеспечивает сравнительные исследования их принадлежности к одному распределению.

Таким образом, паразитными процессами, пригодными для выделения их из идентификационных признаков АЦФВЗ, следует признать шумы, возникающие в цифровых изображениях, обусловленные технологическими погрешностями изготовления светочувствительных элементов светопреобразующих матриц и квантователей уровня АЦП.

Индивидуальность и устойчивость их характера определяются ничтожной вероятностью совпадения местоположения дефектных мест в светопреобразующих матрицах и КУ АЦП.

Выводы

1. Проведенный системный анализ конструктивного строения и технологических погрешностей изготовления аппаратуры цифровой фото и видеозаписи показал, что паразитные процессы, возникающие в светопреобразующих матрицах и квантователях уровня АЦП, пригодны для получения из них идентификационных признаков, предназначенных для проведения экспертизы.

2. Эти идентификационные признаки являются фрактальными образованиями, носящими устойчивый индивидуальный характер. Они могут быть выделены из шумов цифровых изображений и подвергнуты статистическому анализу.

3. Эти идентификационные признаки отвечают требованиям теории криминалистической идентификации.

Список литературы

1. Рыбальский, О.В. Применение системного анализа для разработки методик и средств экспертизы технических объектов / О. В. Рыбальский, В. И. Соловьев, Т. А. Татарникова // Теорія та практика судової експертизи і криміналістики. – 2011. – Вип.11. – С. 348 – 353.
2. Рыбальський, О.В. Новий напрям рішення комплексу проблем фоновоскопії / О.В. Рыбальський, В.І. Соловйов, О.М. Шабля, В.В. Журавель // Захист інформації і безпека інформаційних систем: Матеріали 2-ої міжнародної науково-технічної конференції. – Львів: УАД. – С. 122 – 123.
3. Рыбальський, О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі / О.В. Рыбальський. – К. : Нац. акад. внутр. справ України, 2004. – 167 с.
4. Корн, Г. Справочник по математике для научных работников и инженеров / Г. Корн, Т. Корн. – М.: Наука. Гл. ред. физ.-мат. лит., 1972. – 720 с.

5. Белозьоров, Є. В. Методологія аналізу автентичності цифрового зображення на основі фрактального підходу / Є. В. Белозьоров // Проблеми інформатизації та управління. – 2012. – № 4 – С. 13 – 18.

АНАЛІЗ МЕХАНІЗМУ ВИНИКНЕННЯ ПАРАЗИТНИХ ПРОЦЕСІВ В АПАРАТУРІ ЦИФРОВОГО ФОТО ТА ВІДЕОЗАПИСУ, ПРИДАТНИХ ДЛЯ ВИКОРИСТАННЯ ПРИ ЕКСПЕРТИЗІ ТАКИХ ПРИБОРІВ

О.В. Рибальський, В.В. Журавель

Національна академія внутрішніх справ,
пл. Солом'янська, 1, Київ, 03056, Україна; e-mail: rybalsky_ol@mail.ru

Проведено аналіз конструктивних і технологічних особливостей моделі апаратури цифрового фото та відеозапису. Показано, що паразитні процеси, що виникають в елементах матриць та аналого-цифрових перетворювачів, носять стійкий індивідуальний характер. Запропоновано використання цих процесів для отримання ідентифікаційних ознак, придатних для використання в експертизі цілісності та достовірності інформації, що міститься у відеограмах. Ці ознаки носять фрактальний характер, що може бути використано при їх виділенні з шумів цифрових зображень і подальшій статистичній обробці. Застосування цих ознак в експертизі відповідає теорії криміналістичної ідентифікації.

Ключові слова: апаратура цифрового фото та відео запису, цифрове зображення, світлочутливий елемент, аналого-цифровий перетворювач, фрактал, цілісність інформації, експертиза

THE ANALYSIS OF MECHANISM OF ORIGIN OF PARASITE PROCESSES IN AN APPARATUS IS DIGITAL PHOTO AND VIDEOTAPE RECORDING, SUITABLE FOR USING FOR TO EXAMINATION OF SUCH DEVICES

O.V. Rybalsky, V.V. Zhuravel

National Academy of Internal Affairs,
1, Solomenskaya Sq., Kiev, 03056, Ukraine; e-mail: rybalsky_ol@mail.ru

The analysis of structural and technological features of model of apparatus is conducted by digital to the photo and videotape recording. It is shown that parasite processes arising up in the elements of matrices and ADCS carry steady individual character. The use of these processes is offered for the receipt of identification signs, suitable for the use in examination of integrity and authenticity of the information contained in videogrammes. These signs carry fractal character, that it can be used for their selection from noises of images and subsequent statistical treatment. Application of these signs in examination corresponds to the theory of criminalistics authentication.

Keywords: apparatus digital photo and video of record, digital representation, photosensitive element, ADC, fractal, integrity of information, examination

СТЕГАНОАНАЛІТИЧНИЙ АЛГОРИТМ, ЗАСНОВАНИЙ НА АНАЛІЗІ ПРОСТОРОВОЇ ОБЛАСТІ ЦИФРОВИХ КОНТЕЙНЕРІВ

Д.А. Маєвський, Г.В. Ахметьєва

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

В роботі запропонований стеганоаналітичний алгоритм, заснований на врахуванні відмінностей характеру змін кількості блоків з однаковими значеннями яскравості колірних матриць послідовності зображень/кадрів відео послідовності в результаті первинної та повторної вбудови додаткової інформації. Запропонований стеганоаналітичний алгоритм здійснює аналіз просторової області цифрових контентів (як у форматах з втратами, так і у форматах без втрат) та направлений на виявлення наявності вбудови додаткової інформації методом модифікації найменшого значущого біта з незначною пропускнуою спроможністю прихованого каналу зв'язку (не більше 0.5 біт/піксель). Наведені результати обчислювального експерименту.

Ключові слова: стеганоаналітичний метод, метод модифікації найменшого значущого біта, просторова область контейнера, цифрове зображення, цифрова відеопослідовність, формат зберігання з втратами, формат зберігання без втрат

Вступ

Бурхливий розвиток інформаційних і комунікативних технологій сприяє їх широкому розповсюдженню як у державних та суспільних сферах, так і у повсякденному житті кожної людини, коли непомітними стають великі відстані і будь-яку інформацію можна передати за декілька хвилин, можна спілкуватися з людьми, які знаходяться у різних країнах. Але такий розвиток має й зворотну сторону – багато злочинів, у тому числі терористичні акти, організовані за допомогою таємної комунікації, такої як стеганографія. Використання стеганографічних систем дозволяє передати конфіденційну інформацію по відкритому каналу зв'язку, приховуючи сам факт її присутності у контейнері [1, 2], в ролі якого можуть виступати цифрові зображення (ЦЗ), відео послідовності (ЦВ). Результат вбудови додаткової інформації (ДІ) у контейнер далі будемо називати стеганоповідомленням (СП).

З метою запобігання злочинних дій з використанням стеганографії актуальним є розвиток стеганоаналізу, основною задачею якого є виявлення факту наявності/відсутності прихованої інформації у будь-якому контейнері [2, 3].

Найбільш розповсюдженим стеганографічним методом є метод модифікації найменшого значущого біта (LSB) [2] завдяки простоті реалізації, можливості забезпечення високої пропускнуої спроможності прихованого каналу зв'язку (ППС), використанню як у просторовій області, так і в області перетворень цифрового контейнера. Але сьогодні найчастіше метод LSB використовують саме з малою ППС (не більше 0.5 біт/піксель), що значно ускладнює виявлення факту наявності прихованої інформації.

Більшість сучасних стеганоаналітичних методів та алгоритмів [1, 4-7] виконують аналіз цифрових контентів в області перетворень (частотній області, областях

сингулярного / спектрального розкладання відповідних матриць, тощо), що сприяє накопиченню обчислювальної похибки, особливо цей недолік впливає на ефективність стеганоаналізу при малій ППС стеганографічного каналу зв'язку. Стеганоаналітичні методи, що аналізують просторову область контейнерів [8], дозволяють уникнути як додаткового накопичення похибок обчислень, так і додаткових часових витрат при переході в область перетворень.

Таким чином, підвищення ефективності стеганоаналізу за рахунок забезпечення можливості його проведення в просторовій області при вбудові ДІ методом LSB з незначною ППС в цифрові контейнери (ЦЗ, ЦВ) є актуальною задачею для сучасної стеганографії.

Мета та постановка задач

Метою роботи є покращення ефективності стеганоаналізу при виявленні наявності/відсутності ДІ, вбудованої методом LSB з незначною ППС (не більше 0.5 біт/піксель) у послідовність ЦЗ/кадрів відеопослідовності шляхом розробки універсального стеганоаналітичного алгоритму, заснованого на аналізі характеру змін кількості блоків з однаковими значеннями яскравості в кольорних компонентах цифрових контентів після повторної вбудови ДІ.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Установити в просторовій області характерні зміни кількості блоків з однаковими значеннями яскравості пікселів блоків матриці оригінального ЦЗ у порівнянні з СП, а також СП у порівнянні з СП, отриманим у результаті повторної вбудови ДІ в СП методом LSB;
2. Визначити порогове значення відсотку кольорних складових зі зменшеною кількістю блоків з однаковими значеннями яскравості у послідовності ЦЗ/ЦВ, сформованих первинною вбудовою ДІ, у порівнянні з цифровим контентом, отриманим повторним впровадженням ДІ у СП;
3. Розробити основні кроки стеганоаналітичного алгоритму детектування наявності/відсутності ДІ, вбудованої методом LSB з незначною ППС (не більше 0.5 біт/піксель), у цифрових контентях;
4. Оцінити ефективність розробленого стеганоалгоритму шляхом визначення помилок 1-го та 2-го роду на основі детектування набору відеопослідовностей.

Основна частина

В роботах [9, 10] були сформульовані стеганоаналітичні методи для форматів без втрат та форматів з втратами, направлені на детектування наявності/відсутності ДІ, вбудованої в контейнер методом LSB з малою ППС (не більше 0.5 біт/піксель), шляхом порівняння відносної зміни кількості блоків в контенті, що аналізується, у порівнянні з СП, отриманим повторним впровадженням ДІ у цей контент.

У поточній роботі проводиться дослідження характеру зміни кількості 4×4-блоків з однаковими значеннями яскравості у послідовності ЦЗ/відеопослідовності в результаті первинного та повторного впровадження ДІ. В обчислювальному експерименті використовується база зображень, яка містить 1000 кольорових ЦЗ (схема RGB):

- група 1: 200 ЦЗ із бази NRCS Photo Gallery [11] у форматі TIFF;
- група 2: 200 зображень, отриманих непрофесіональними фотокамерами в форматі TIFF;
- група 3: 200 ЦЗ із бази NRCS Photo Gallery [11] в форматі JPG;
- група 4: 200 високоякісних ЦЗ із [12], в форматі JPG;

група 5: 200 зображень, отриманих непрофесіональними фотокамерами в форматі JPG.

На першому етапі обчислювального експерименту проводилась оцінка характеру зміни (зменшення, збільшення чи незмінність) кількості 4×4 -блоків з однаковими значеннями яскравості в колірних складових оригінальних ЦЗ та СП, отриманих первинним впровадженням ДІ у контейнер методом LSB. Кожна колірна компонента контейнера досліджувалась окремо, однак характер змін для будь-яких колірних складових аналогічний, тому в подальшому будемо мати на увазі, що результати обчислювального експерименту застосовні як для червоної, так і для зеленої та синьої колірних матриць. Результати першого етапу експерименту представлені у табл.1. Тут характер змін визначається за формулами

$$P_{\text{зменш}} = \frac{k_{\text{зменш}}}{N} \cdot 100\%, P_{\text{збільш}} = \frac{k_{\text{збільш}}}{N} \cdot 100\%, P_{\text{незмін}} = \frac{k_{\text{незмін}}}{N} \cdot 100\%, \quad (1)$$

де $P_{\text{зменш}}$, $P_{\text{збільш}}$, $P_{\text{незмін}}$ – відсоток матриць, у яких кількість 4×4 -блоків з однаковими значеннями яскравості при впровадженні ДІ зменшується, збільшується та залишається незмінною відповідно;

$k_{\text{зменш}}$, $k_{\text{збільш}}$, $k_{\text{незмін}}$ – кількість матриць у послідовності ЦВ/кадрах ЦВ, у яких кількість 4×4 -блоків з однаковими значеннями яскравості при впровадженні ДІ зменшується, збільшується та залишається незмінною відповідно;

N – загальна кількість матриць у послідовності, що аналізується.

Таблиця 1.

Характер зміни кількості 4×4 -блоків з однаковими значеннями яскравості при первинному впровадженні ДІ по всьому набору зображень, %

ППС при первинному впровадженні ДІ	Характер зміни	Група 1 (TIFF)	Група 2 (TIFF)	Група 3 (JPG)	Група 4 (JPG)	Група 5 (JPG)
0.5	Зменшення	34.9301	40.3134	92.2824	82.2554	91.6279
	Збільшення	40.9182	47.1510	4.9261	12.2720	7.9070
	Незмінність	24.1517	12.5356	2.7915	5.4726	0.4651
0.25	Зменшення	39.7206	43.4473	92.7750	86.2355	93.9535
	Збільшення	33.9321	40.5983	4.5977	8.4577	5.4264
	Незмінність	26.3473	15.9544	2.6273	5.3068	0.6201
0.1	Зменшення	43.7126	46.0114	92.7750	88.8889	96.2791
	Збільшення	27.3453	34.4729	3.4483	4.8093	2.6356
	Незмінність	28.9421	19.5157	3.7767	6.3018	1.0853

Як видно з табл. 1 при первинному впровадженні ДІ у контейнери в форматах без втрат (групи 1 і 2) незалежно від ППС у середньому в 40% матриць спостерігається зменшення кількості 4×4 -блоків з однаковими значеннями яскравості. У зображеннях в форматах з втратами (групи 3, 4, 5) доля матриць зі зменшеною кількістю 4×4 -блоків досягає 80% та вище.

На другому етапі обчислювального експерименту проводилась оцінка характеру змін кількості 4×4 -блоків з однаковими значеннями яскравості у колірних складових СП, отриманих первинним впровадженням ДІ у контейнер методом LSB, та СП, отриманих в результаті повторної вбудови ДІ у дане СП. Результати експерименту представлені у табл.2. Характер змін визначається за формулами (1).

Таблиця 2.

Характер зміни кількості 4×4 -блоків з однаковими значеннями яскравості при повторному впровадженні ДІ по всьому набору зображень, %

ППС при первинній вбудові ДІ	ППС при повторній вбудові ДІ	Характер зміни	Гр. 1 (TIFF)	Гр. 2 (TIFF)	Гр. 3 (JPG)	Гр. 4 (JPG)	Гр. 5 (JPG)
0.5	0.5	Зменшення	0	0	0	0	0
		Збільшення	55.8882	72.0798	71.5928	73.6318	81.7054
		Незмінність	44.1118	27.9202	28.4072	26.3682	18.2946
	0.25	Зменшення	0	0	0	0	0
		Збільшення	52.4950	65.6695	33.9901	63.1841	56.8992
		Незмінність	47.5050	34.3305	66.0099	36.8159	43.1008
	0.1	Зменшення	0	0	0	0	0
		Збільшення	46.5070	60.2564	26.7652	55.7214	51.1628
		Незмінність	53.4930	39.7436	73.2348	44.2786	48.8372
0.25	0.5	Зменшення	0.1996	0	0.1642	0	2.0155
		Збільшення	57.2854	73.7892	41.2151	71.4760	67.1318
		Незмінність	42.5150	26.2108	58.6207	28.5240	30.8527
	0.25	Зменшення	0.3992	0	0.1642	0	1.7054
		Збільшення	54.0918	68.0912	39.4089	67.1642	65.8915
		Незмінність	45.5090	31.9088	60.4269	32.8358	32.4031
	0.1	Зменшення	0.1996	0	0	0	1.7054
		Збільшення	49.1018	60.8262	29.5567	55.2239	54.2636
		Незмінність	50.6986	39.1738	70.4433	44.7761	44.0310
0.1	0.5	Зменшення	20.3593	20.2279	64.5320	41.4594	63.4109
		Збільшення	50.4990	62.9630	18.8834	45.2736	31.6279
		Незмінність	29.1417	16.8091	16.5846	13.2670	4.9612
	0.25	Зменшення	21.7565	22.6496	68.1445	48.0929	67.4419
		Збільшення	46.7065	55.6980	13.7931	35.1575	25.8915
		Незмінність	31.5370	21.6524	18.0624	16.7496	6.6666
	0.1	Зменшення	15.7685	17.6638	41.3793	34.1625	44.1860
		Збільшення	46.9062	54.2735	45.8128	50.9121	51.4729
		Незмінність	37.3253	28.0627	12.8079	14.9254	4.3411

З табл.2 видно, що після повторного впровадження ДІ у стеганоповідомлення помітно знижується відсоток колірних матриць зі зменшеною кількістю 4×4 -блоків з однаковими значеннями яскравості (аж до 0%, особливо, якщо ППС при первинному впровадженні складала 0.5 та 0.25 біт/піксель), що призводить до зростання відсотку матриць зі збільшеною та незмінною кількістю 4×4 -блоків з однаковими значеннями яскравості. Притому, це спостереження характерне як для контейнерів в форматах без втрат, так і для контейнерів в форматах з втратами.

Таким чином, на основі характеру змін більшості елементів (ЦЗ, кадрів) послідовності можна зробити висновок про наявність/відсутність ДІ у контенті, який аналізується. З цією метою визначимо порогове значення відсотку зменшення кількості 4×4 -блоків з однаковими значеннями яскравості. У випадку, якщо первинна ППС складає 0.1 біт/піксель, порогове значення точно визначити не представляється можливим у зв'язку з розкидом значень табл. 2 для різних груп, оскільки завжди знайдеться оригінальна послідовність, яка має менший відсоток елементів зі зменшеною кількістю 4×4 -блоків з однаковими значеннями яскравості. Для первинної

ППС 0.5 та 0.25 біт/піксель для контейнерів в форматах без втрат приймемо порогове значення $T_{uncompressed} = 0.4$ та для контейнерів в форматах з втратами $T_{compressed} = 3$.

Для послідовності з P ЦЗ/кадрів ЦВ $C_1, C_2, \dots, C_P$ з колірними складовими $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ основні кроки стегааноаналітичного алгоритму детектування наявності/відсутності ДІ, вбудованої методом LSB, наступні.

Крок 1. Вбудова ДІ (випадково сформованої бінарної послідовності).

Для кожного $C_i, i = \overline{1, P}$:

- 1.1. Вбудувати у $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ - колірні складові C_i методом LSB ДІ – випадково сформовану бінарну послідовність з ППС 0.5 біт/піксель. Результат - $S_i^{0.5}$ з колірними складовими $R_i^{(0.5)}, G_i^{(0.5)}, B_i^{(0.5)}$;
- 1.2. Вбудувати у $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ - колірні складові C_i методом LSB ДІ – випадково сформовану бінарну послідовність з ППС 0.25 біт/піксель. Результат - $S_i^{0.25}$ з колірними складовими $R_i^{(0.25)}, G_i^{(0.25)}, B_i^{(0.25)}$;
- 1.3. Вбудувати у $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ - колірні складові C_i методом LSB ДІ – випадково сформовану бінарну послідовність з ППС 0.1 біт/піксель. Результат - $S_i^{0.1}$ з колірними складовими $R_i^{(0.1)}, G_i^{(0.1)}, B_i^{(0.1)}$.

Крок 2. Визначення кількості 4×4 -блоків з однаковими значеннями яскравості у кожній колірній складовій.

Для кожного $C_i, i = \overline{1, P}$:

- 2.1. Визначити $kr_i^{(C)}, kg_i^{(C)}, kb_i^{(C)}$ - кількість 4×4 -блоків у $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ відповідно;
- 2.2. Визначити $kr_i^{(0.5)}, kg_i^{(0.5)}, kb_i^{(0.5)}$ - кількість 4×4 -блоків у $R_i^{(0.5)}, G_i^{(0.5)}, B_i^{(0.5)}$ відповідно;
- 2.3. Визначити $kr_i^{(0.25)}, kg_i^{(0.25)}, kb_i^{(0.25)}$ - кількість 4×4 -блоків у $R_i^{(0.25)}, G_i^{(0.25)}, B_i^{(0.25)}$ відповідно;
- 2.4. Визначити $kr_i^{(0.1)}, kg_i^{(0.1)}, kb_i^{(0.1)}$ - кількість 4×4 -блоків у $R_i^{(0.1)}, G_i^{(0.1)}, B_i^{(0.1)}$ відповідно.

Крок 3. Визначення характеру змін кількості 4×4 -блоків з однаковими значеннями яскравості у кожній колірній складовій.

Для кожного $C_i, i = \overline{1, P}$ обчислити:

$$\begin{aligned} dR_i^{(0.5)} &= kr_i^{(C)} - kr_i^{(0.5)}, \quad dG_i^{(0.5)} = kg_i^{(C)} - kg_i^{(0.5)}, \quad dB_i^{(0.5)} = kb_i^{(C)} - kb_i^{(0.5)}; \\ dR_i^{(0.25)} &= kr_i^{(C)} - kr_i^{(0.25)}, \quad dG_i^{(0.25)} = kg_i^{(C)} - kg_i^{(0.25)}, \quad dB_i^{(0.25)} = kb_i^{(C)} - kb_i^{(0.25)}; \\ dR_i^{(0.1)} &= kr_i^{(C)} - kr_i^{(0.1)}, \quad dG_i^{(0.1)} = kg_i^{(C)} - kg_i^{(0.1)}, \quad dB_i^{(0.1)} = kb_i^{(C)} - kb_i^{(0.1)}. \end{aligned}$$

Крок 4. Визначити загальну кількість матриць ЦЗ/кадрів відео послідовності, у яких спостерігається зменшення кількості 4×4 -блоків з однаковими значеннями яскравості у кожній колірній складовій.

- 4.1. Якщо $dR_i^{(0.5)} > 0$, то $kR^{(0.5)} = kR^{(0.5)} + 1$ ($kR^{(0.5)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);

- 4.2. Якщо $dR_i^{(0.25)} > 0$, то $kR^{(0.25)} = kR^{(0.25)} + 1$ ($kR^{(0.25)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.3. Якщо $dR_i^{(0.1)} > 0$, то $kR^{(0.1)} = kR^{(0.1)} + 1$ ($kR^{(0.1)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.4. Якщо $dG_i^{(0.5)} > 0$, то $kG^{(0.5)} = kG^{(0.5)} + 1$ ($kG^{(0.5)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.5. Якщо $dG_i^{(0.25)} > 0$, то $kG^{(0.25)} = kG^{(0.25)} + 1$ ($kG^{(0.25)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.6. Якщо $dG_i^{(0.1)} > 0$, то $kG^{(0.1)} = kG^{(0.1)} + 1$ ($kG^{(0.1)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.7. Якщо $dB_i^{(0.5)} > 0$, то $kB^{(0.5)} = kB^{(0.5)} + 1$ ($kB^{(0.5)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.8. Якщо $dB_i^{(0.25)} > 0$, то $kB^{(0.25)} = kB^{(0.25)} + 1$ ($kB^{(0.25)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості);
- 4.9. Якщо $dB_i^{(0.1)} > 0$, то $kB^{(0.1)} = kB^{(0.1)} + 1$ ($kB^{(0.1)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків з однаковими значеннями яскравості).

Крок 5. Обчислити:

$$pR^{(0.5)} = \frac{kR^{(0.5)}}{P} \cdot 100\%, \quad pR^{(0.25)} = \frac{kR^{(0.25)}}{P} \cdot 100\%, \quad pR^{(0.1)} = \frac{kR^{(0.1)}}{P} \cdot 100\%;$$

$$pG^{(0.5)} = \frac{kG^{(0.5)}}{P} \cdot 100\%, \quad pG^{(0.25)} = \frac{kG^{(0.25)}}{P} \cdot 100\%, \quad pG^{(0.1)} = \frac{kG^{(0.1)}}{P} \cdot 100\%;$$

$$pB^{(0.5)} = \frac{kB^{(0.5)}}{P} \cdot 100\%, \quad pB^{(0.25)} = \frac{kB^{(0.25)}}{P} \cdot 100\%, \quad pB^{(0.1)} = \frac{kB^{(0.1)}}{P} \cdot 100\%.$$

Крок 6. Детектування наявності/відсутності ДІ.

6.1. Якщо

$$\begin{aligned} & (pR^{(0.5)} \leq T \text{ AND } pR^{(0.25)} \leq T) \text{ OR } (pR^{(0.5)} \leq T \text{ AND } pR^{(0.1)} \leq T) \text{ OR} \\ & (pR^{(0.25)} \leq T \text{ AND } pR^{(0.1)} \leq T) \text{ OR} \\ & (pR^{(0.5)} \leq T \text{ AND } pR^{(0.25)} \leq T \text{ AND } pR^{(0.1)} \leq T), \end{aligned}$$

то $C_1, C_2, \dots, C_P$ містять вбудовану ДІ у червоній колірній складовій;

6.2. Якщо

$$\begin{aligned} & (pG^{(0.5)} \leq T \text{ AND } pG^{(0.25)} \leq T) \text{ OR } (pG^{(0.5)} \leq T \text{ AND } pG^{(0.1)} \leq T) \text{ OR} \\ & (pG^{(0.25)} \leq T \text{ AND } pG^{(0.1)} \leq T) \text{ OR} \\ & (pG^{(0.5)} \leq T \text{ AND } pG^{(0.25)} \leq T \text{ AND } pG^{(0.1)} \leq T), \end{aligned}$$

то $C_1, C_2, \dots, C_P$ містять вбудовану ДІ у зеленій колірній складовій;

6.3. Якщо

$$\begin{aligned} & (pB^{(0.5)} \leq T \text{ AND } pB^{(0.25)} \leq T) \text{ OR } (pB^{(0.5)} \leq T \text{ AND } pB^{(0.1)} \leq T) \text{ OR} \\ & (pB^{(0.25)} \leq T \text{ AND } pB^{(0.1)} \leq T) \text{ OR} \\ & (pB^{(0.5)} \leq T \text{ AND } pB^{(0.25)} \leq T \text{ AND } pB^{(0.1)} \leq T), \end{aligned}$$

то $C_1, C_2, \dots, C_p$ містять вбудовану ДІ у синій колірній складовій.

Для оцінки ефективності розробленого алгоритму у середовищі MatLAB був проведений обчислювальний експеримент на базі наступних цифрових контентів:

- 367 відеопослідовностей розміром кадру 320×240 , збережених в форматі з втратами, які отримані непрофесійною камерою, а також роліки, зняті на мобільний телефон (набір 1);
- 49 відеопослідовностей розміром кадру 176×144 , збережених в форматі з втратами, які отримані камерою застарілої моделі мобільного телефону (набір 2);
- 60 послідовностей ЦЗ з [13] розміром 256×256 , збережених в форматі без втрат (набір 3).

Слід зауважити, що перевага надається відеоролікам, які зняті камерами мобільних пристроїв, оскільки вони є найрозповсюдженими. Такі ЦВ зберігаються в форматах з втратами та мають розширення *.3gp або *.mp4. ЦВ в форматах без втрат у просторі Internet майже не зустрічаються.

Первинна вбудова ДІ здійснювалась лише в одну колірну складову, випадково обрану для кожного ЦВ (кожної послідовності ЦЗ) з ППС 0.5 біт/піксель (в кожний другий біт), 0.25 біт/піксель (в кожний четвертий біт), 0.167 біт/піксель (в кожний шостий біт), 0.125 біт/піксель (в кожний восьмий біт), 0.1 біт/піксель (в кожний десятий біт). Вбудова в одну постійну колірну складову обумовлена тим, що у сусідніх кадрах ЦВ можуть відрізнятися лише ті ділянки, які відповідають руху, а фон майже не змінюється, тому якщо здійснювати вбудову ДІ у різні компоненти кадрів, можна запідозрити наявність ДІ у ЦВ простим порівнянням колірних компонент сусідніх кадрів.

На основі детектування наявності/відсутності ДІ у цифровому контенті визначені помилки першого та другого роду для порогових значень $T=0.4$ та $T=3$, які представлені у табл. 3, 4 відповідно.

Таблиця 3.

Ефективність детектування наявності/відсутності ДІ у цифрових контентях при $T=0.4$, %

Набір цифрових контентів	Помилки	ППС, біт/піксель				
		0.5	0.25	0.167	0.125	0.1
Набір 1	1-го роду	0	0	4.63	97	100
	2-го роду	0	0	0	0	0
Набір 2	1-го роду	0	0	6.12	53.06	87.75
	2-го роду	0	0	0	1.02	0
Набір 3	1-го роду	0	0	0	5	48.33
	2-го роду	5.83	5.87	6.67	6.67	5.83

Як видно з табл.3,4 запропонований стеганоаналітичний алгоритм є ефективним для ППС 0.5, 0.25 та 0.167 біт/піксель, на відміну від ППС 0.125 та 0.1 біт/піксель.

Таблиця 4.

Ефективність детектування наявності/відсутності ДІ у цифрових контентах при
 $T = 3, \%$

Набір цифрових контентів	Помилки	ППС, біт/піксель				
		0.5	0.25	0.167	0.125	0.1
Набір 1	1-го роду	0	0	0	74.11	98.91
	2-го роду	0	0	0	0	0
Набір 2	1-го роду	0	0	0	6.12	40.82
	2-го роду	5.10	5.10	5.10	5.10	5.10
Набір 3	1-го роду	0	0	0	0	0
	2-го роду	49.17	45.83	49.17	48.33	50.83

Окремого зауваження потребують результати детектування для набору 3 при $T = 3$ (табл. 4), де помилки першого роду складають 0% навіть при малій ППС. ЦЗ набору 3 збережені в форматі без втрат, крім того завдяки невеликому розміру зображень відсоток елементів зі зменшеною кількістю 4×4 -блоків з однаковими значеннями яскравості в незаповненій колірній матриці знаходиться у діапазоні від 0.6 до 6 (при ППС 0.167, 0.125 та 0.1 біт/піксель), та від 0.5 до 11 (при ППС 0.5 та 0.25 біт/піксель), саме тому при $T = 3$ у наборі 3 не спостерігається пропуск наявності ДІ, але значно зростає відсоток помилок другого роду. Тому порогове значення $T = 3$ може використовуватися лише для цифрових контентів, збережених в форматах з втратами.

Висновки

У роботі запропонований стеганоаналітичний алгоритм детектування наявності/відсутності вбудови ДІ у послідовності ЦЗ/відео послідовності, сформованої методом LSB з малою ППС (не більше 0.5 біт/піксель).

Встановлено порогове значення для контейнерів в форматах з втратами $T = 3$ незалежно від колірної складової, однак алгоритм може бути використано як універсальний (як для контейнерів в форматах з втратами, так і в форматах без втрат) з пороговим значенням $T = 0.4$. Для ППС 0.5 та 0.25 біт/піксель стеганоалгоритм є ефективним, помилки першого роду складають 0%.

Список літератури

1. Бобок, И.И. Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями / И.И. Бобок // Сучасний захист інформації. – 2011. – №2. – С. 50 - 60.
2. Аграновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.
3. Bohme, R. Advanced statistical steganalysis / R. Bohme. – Springer, 2010. – 302 p.
4. Alimoradi, D. The effect of correlogram properties on blind steganalysis in JPEG images / D. Alimoradi, M. Hasanzadeh // Journal of computing and security. – 2014. – Vol. 1, No.1. – PP. 39-46.
5. Visavalia, S.R. Improving blind image steganalysis using genetic algorithm and fusion technique / S.R. Visavalia, Amit Ganatra // Journal of computer science. – 2014. – Vol. 1. – PP. 40-46.
6. Yamini, B. Blind steganalysis: to analyse the detection rate of stego images using different steganalytic techniques with support vector machine classifier / B. Yamini, R. Sabitha // International journal of computer applications. – 2014. – No. 2. – PP. 22-25.

7. Manjunath, C. Added and subtracted feature level video steganalysis in neighbor adaptive embedded / C. Manjunath, Mis.B. Sowjanya // International journal of professional engineering studies. – 2015. – Vol.5. – Issue 2. – PP. 308-316.
8. Xikai, Xu. Universal spatial feature set for video steganalysis / Xu. Xikai, Jing Dong, Tieniu Tan // Image Processing (ICIP), 2012 19th IEEE International Conference on Sept. 30 - Oct. 3, 2012. – PP. 245-248.
9. Кобозева, А.А. Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь / А.А. Кобозева, А.В. Ахматєєва, А.А. Ефименко // Інформаційна безпека. – 2014. – №1(13). – С. 31 - 42.
10. Ахматєєва, А.В. Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров / А.В. Ахматєєва // Інформатика та математичні методи в моделюванні. – 2015. – Т.5. – № 4. – С. 367 - 375.
11. NRCS Photo Gallery: [Электронный ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата звертання: 26.07.2012).
12. WallpapersCraft: [Электронный ресурс] // Широкоформатные обои на рабочий стол, картинки, фото. Режим доступа: <http://wallpaperscraft.ru/> (Дата обращения: 21.11.2014).
13. Never-compressed image database: [Электронный ресурс] // Sam Houston State University, USA. Режим доступа: <http://www.shsu.edu/~qxl005/New/Downloads/> (Дата звертання: 21.12.2015).

СТЕГАНОАНАЛИТИЧЕСКИЙ АЛГОРИТМ, ОСНОВАННЫЙ НА АНАЛИЗЕ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ЦИФРОВЫХ КОНТЕЙНЕРОВ

Д.А. Маевский, А.В. Ахматєєва

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: anna-odessitka@mail.ru

В работе предложен стеганоаналитический алгоритм, основанный на учете различий характера изменений количества блоков с одинаковыми значениями яркости цветковых матриц последовательности изображений/кадров видеопоследовательности в результате первичного и повторного внедрения дополнительной информации. Предложенный стеганоаналитический алгоритм осуществляет анализ пространственной области цифровых контентов (как в форматах с потерями, так и в форматах без потерь) и направлен на выявление наличия вложения дополнительной информации методом модификации наименьшего значащего бита с незначительной скрытой пропускной способностью (не более 0.5 бит/пиксель). Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганоаналитический алгоритм, метод модификации наименьшего значащего бита, пространственная область контейнера, цифровое изображение, цифровая видеопоследовательность, формат хранения с потерями, формат хранения без потерь

STEGANALYTIC ALGORITHM, BASED ON THE ANALYSIS OF THE SPATIAL DOMAIN OF DIGITAL CONTAINERS

D.A. Maevsky, A.V. Akhmet'eva

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

The paper presents the steganalytic algorithm, based on the accounting of differences of character in the change of the number of blocks with the equal color brightness values of color matrices of sequence of images / frames of a video sequence as a result of primary and repeated insertion of additional information. The proposed steganalytic algorithm analyzes digital content in the spatial domain and is aimed to detect the presence of the embedding of additional information by modification of the least significant bits with a small hidden capacity (not more than 0.5 bit / pixel). Results of computational experiment are shown.

Keywords: Steganalytic algorithm, method of the modification of the least significant bit, the spatial domain of the container, a digital image, a digital video sequence, losses format, lossless storage format

ИНФОРМАТИЗАЦИЯ ДИСТАНЦИОННОГО ДИАГНОСТИРОВАНИЯ СОСТОЯНИЯ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

С.Н. Коновалов, В.В. Вычужанин

Одесский национальный морской университет,
ул. Мечникова 34, Одесса, 65404, Украина, e-mail: vint532@yandex.ru

Приведены результаты разработки и информатизации метода дистанционного мониторинга, диагностики сложных технических систем, установленных на судах. Проведен анализ используемых методов мониторинга, диагностики технических систем. Описан метод дистанционного мониторинга, диагностики, основывающийся на экспертном анализе состояния сложных технических систем. Приведены результаты разработки нечеткой модели для диагностирования сложной технической системы, а также результаты ее исследования. Применение разработанного метода и его информатизация позволяет оценить работоспособность сложной технической системы в различных условиях и режимах ее эксплуатации, а также прогнозировать состояние системы в аварийных экстремальных ситуациях.

Ключевые слова: сложная техническая система, мониторинг, диагностика, прогнозирование, экспертный анализ, нечеткая модель

Введение

Безопасность мореплавания связана с обеспечением работоспособности, а значит надежности эксплуатации судовых сложных технических систем (СТС). В результате переменных режимов и условий эксплуатации СТС их работоспособность снижается, возрастает вероятность возникновения отказов систем [1,2]. Переход к обеспечению эксплуатационной надежности технологического оборудования по его «фактическому состоянию» вызывает необходимость предпринимать меры по предупреждению и обнаружению причин возникновения отказов СТС, обязательного создания систем технического мониторинга и диагностики их состояния.

Оценка работоспособности оборудования непосредственно на судне осуществляется на основе измерений и анализа диагностических параметров СТС, число которых, а также их взаимосвязей велико. Решение проблемы заключается в применении информационных систем дистанционного мониторинга и диагностирования (ДМД) состояния СТС. При этом имеется возможность учитывать диагностические признаки различной природы, получать решения в условиях неполной, нечеткой информации.

В настоящее время проектируются и эксплуатируются информационные системы ДМД, основывающиеся на различных методах мониторинга, диагностики состояния СТС [3-8]. Сложность технических систем, разнообразие условий эксплуатации требуют пересмотра существующих концепций построения систем ДМД и поиска новых. Информация, используемая для постановки диагноза, в большинстве случаев является нечеткой. Для развития методов диагностики СТС в последние годы установлена целесообразность применения математического аппарата нечеткой логики для определения критериев оценки состояния оборудования и принятия диагностических решений. Данный метод базируется на сочетании традиционных

средств оперативного контроля с экспертными системами, построенными с использованием методов нечеткой логики [1,2]. Хотя средства автоматизации контроля технического состояния СТС появились давно, в настоящее время еще не создана такая система ДМД, которая бы комплексно оценивала текущее состояние судовых СТС, обеспечивала раннее обнаружение дефектов и прогнозировала развитие процессов. Существующие диагностические методы базируются на математических моделях, способных отображать лишь часть свойств и режимов работы судовых СТС. Отсутствие научных методов, позволяющих решать задачи создания систем ДМД на базе информационных технологий, объясняет причину того, что в морехозяйственном комплексе процент успешных внедрений таких систем очень низкий. Несмотря на многообразие существующих методов ДМД, они нуждаются в дальнейшем развитии для судовых СТС.

Таким образом, решение задачи обеспечения эксплуатационной надежности судовых СТС по их «фактическому состоянию» путем создания и внедрения экспертной системы с использованием нечеткой логики актуально. От решения задачи зависит эффективность функционирования удаленных от диагностических центров СТС в экстремальных условиях эксплуатации.

Цель статьи

Целью статьи является создание нечеткой экспертной системы мониторинга и диагностики состояния судовых СТС для качественной оценки их состояния.

Основная часть

Алгоритм построения информационной системы ДМД СТС приведен на рис.1. Его реализация позволяет систематизировать метод диагностики с разделением процесса разработки на логически завершённые этапы. Динамика изменений в экспертной системе СТС отображается при задании множеств лингвистических переменных, терм-множеств, нечетких переменных, базовых множеств, функций принадлежности, баз данных в задании нечетких критериев и нечетких отношений.

Входные данные:

1. Нелингвистические (точные) переменные: $x_1; x_2; x_3$. $\{x_1, x_2, x_3\} \in X$ – множество нелингвистических переменных. Нелингвистические переменные задаются как показатели работы СТС, по которым, используя вывод Сугено, определяется работоспособность системы.

2. Лингвистические переменные: $y_1; y_2; y_3$ – комплексный критерий качества, построенный на основе функций желательности Харрингтона. $D = y_3$ – лингвистические переменные. $\{y_1, y_2, y_3\} \in Y$ – множество лингвистических переменных.

Значение каждого из лингвистических параметров диагностики y_u , которых в задаче может быть сколь угодно много, переводится в соответствующую желательность d_u :

$$d_u = \exp[-\exp(-y_u)].$$

Значения лингвистических переменных определяются по выводу Мамдани. Функция желательности D – среднее геометрическое желательностей отдельных оценочных параметров: $D = \sqrt[q]{y_1 \cdot y_2 \cdot y_3}$, где q – число параметров диагностики. Все

параметры, как лингвистические, так и нелингвистические, получены динамическим мониторингом СТС.

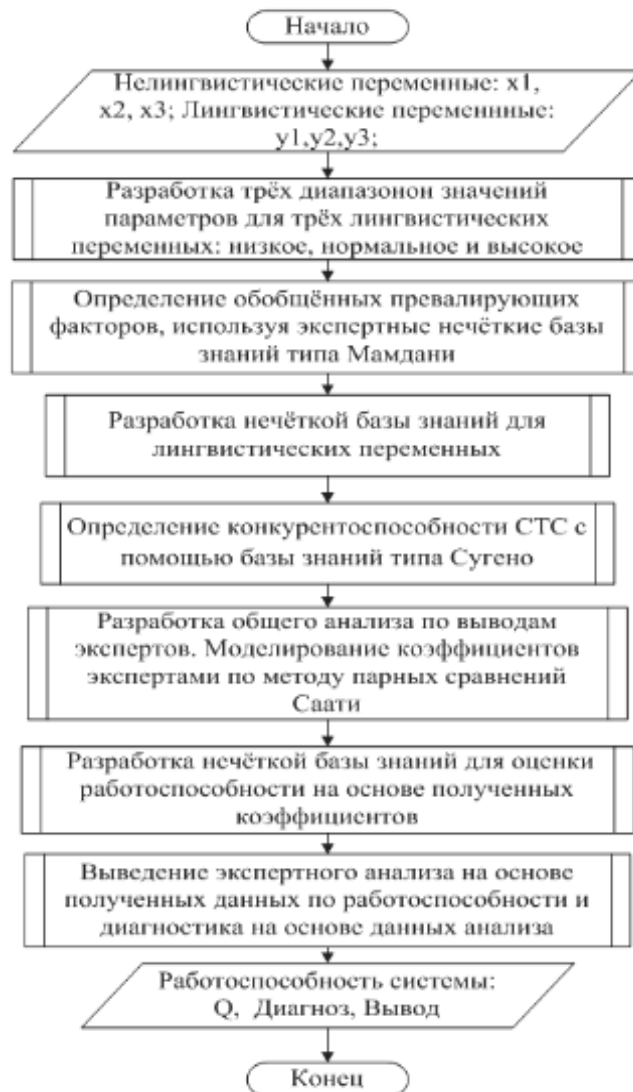


Рис. 1. Алгоритм построения информационной системы ДМД СТС

Выходные данные:

Q – работоспособность системы; $Q \in [0,100]$.

Модель работоспособности СТС представляет собой функциональное отображение вида

$$X = (x_1, x_2, x_3) \cap Y = (y_1, y_2, y_3) \rightarrow Q \in [0,100].$$

Нечёткое множество

$$\mu(X) \cap \mu(Y) = \mu_{\tilde{A} \rightarrow B}(Q) \mu(X) \cap \mu(Y) = \mu_{\tilde{A} \rightarrow B}(Q),$$

где $\tilde{A}$ – нечёткое множество, B – чёткое множество.

При разработке базы знаний экспертной системы использованы результаты индентификации, преобразованных в три диапазона значений параметров соответственно для трёх лингвистических переменных: низкие (H), средние (C) и высокие (B), представленных в табл.1.

Таблица 1.

Значения параметров в диапазонах лингвистических переменных

Лингвистическая переменная	Значение параметров		
	низкое	среднее	высокое
y_1	$[a_1...b_1]$	$[b_1...c_1]$	$[c_1...d_1]$
y_2	$[a_2...b_2]$	$[b_2...c_2]$	$[c_2...d_2]$
y_3	$[a_3...b_3]$	$[b_3...c_3]$	$[c_3...d_3]$

В табл.1 $a_i, b_i, c_i, d_i, i = \overline{1,3}$ – граничные значения параметров лингвистических переменных. Промежуточные значения параметров определяются как отклонения от усредненных показателей.

При моделировании укрупненных влияющих факторов используются экспертные нечёткие базы знаний типа Мамдани. Элементы antecedentes нечётких правил, основанных на опыте экспертов, связаны логической операцией «И», представлены в табл.2.

Таблица 2.

Нечёткая база знаний для лингвистических переменных

y_1	y_2	y_3	Y
В	В	В	В
В	В	С	В
В	С	В	В
В	С	С	В
С	В	В	В
Н	Н	Н	Н
Н	Н	С	Н
Н	С	Н	Н
Н	С	С	Н
С	Н	Н	Н
В	Н	С	С
В	С	Н	С
Н	В	С	С
Н	С	В	С
С	В	Н	С
С	Н	В	С
С	С	С	С

Работоспособность судовой СТС исследуется с учётом трёх типов показателей лингвистических переменных. Границы подобластей с постоянными эластичностями работоспособности – нечёткие, что обусловлено плавным переходом одного типа показателей в другой.

Предлагается нечёткая база знаний типа Сугено для моделирования конкурентоспособности ТС. Каждое правило базы знаний моделирует один тип. Коэффициенты в заключениях правил задают чувствительность конкурентоспособности по соответствующим факторам.

Каждому элементу множества соответствует своя степень принадлежности: чем выше степень принадлежности, тем больше вероятность того, что значение параметра в

норме. Функции принадлежности или информация для их построения задаются экспертами на основе субъективных предпочтений и не носят случайного характера.

По нелингвистическим и лингвистическим переменным, осуществляется общий анализ по выводам экспертов. Коэффициенты уравнения определения работоспособности выбираются экспертами по методу парных сравнений Саати, результаты которых (в общем виде) для первой нелингвистической переменной x_1 в табл.3.

Таблица 3.

Результат парных сравнений экспертов для первой нелингвистической переменной x_1

	B	C	H
B	1/1	$f/1$	$g/1$
C	$1/f$	1/1	$f/1$
H	$1/g$	$1/f$	1/1

В табл.3 f – значение отношения В к С, g – значение отношения В к Н для первой нелингвистической переменной. Действия над дробями для первой нелингвистической переменной приведены в табл.4.

Таблица 4.

Действия над дробями для первой нелингвистической переменной x_1

	B	C	H	$\sum_{x1}$	Отношение
B	1	f	g	$\sum_{x11} = 1 + f + g$	$\sum_{x11} / \sum_{x1}$
C	$1/f$	1	f	$\sum_{x12} = 1/f + 1 + f$	$\sum_{x12} / \sum_{x1}$
H	$1/g$	$1/f$	1	$\sum_{x13} = 1/g + 1/f + 1$	$\sum_{x13} / \sum_{x1}$
				$\sum_{x1} = \sum_{x11} + \sum_{x12} + \sum_{x13}$	$\sum_{x1} / \sum_{x1}$

В табл.4 $\sum_{x11}$ – строчная сумма для значения В, $\sum_{x12}$ – строчная сумма для значения С, $\sum_{x13}$ – строчная сумма для значения Н, $\sum_{x1}$ – общая сумма строчных сумм первой нелингвистической переменной. Подобные расчёты делаются и для лингвистических переменных x_2 и x_3 соответственно. Веса обобщённой лингвистической переменной для разных значений приведены в табл.5.

В табл.5 $\sum_{x21}$ – строчная сумма для значения В, $\sum_{x22}$ – строчная сумма для значения С, $\sum_{x23}$ – строчная сумма для значения Н, $\sum_{x2}$ – общая сумма строчных сумм второй нелингвистической переменной; $\sum_{x31}$ – строчная сумма для значения В, $\sum_{x32}$ – строчная сумма для значения С, $\sum_{x33}$ – строчная сумма для значения Н, $\sum_{x3}$ – общая сумма строчных сумм третьей нелингвистической переменной; $\sum_{\epsilon}$ – строчная сумма для значения В, $\sum_c$ – строчная сумма для значения С, $\sum_n$ – строчная сумма для значения Н, $\sum$ – общая строчная всех значений для всех переменных. С учетом коэффициентов уравнения определения работоспособности которых построена нечёткая база знаний (табл.6).

Таблица 5.

Веса обобщённой лингвистической переменной для разных значений

	x_1	x_2	x_3	Σ	Среднее
B	$\sum_{x11}/\sum_{x1}$	$\sum_{x21}/\sum_{x2}$	$\sum_{x31}/\sum_{x3}$	$\sum_{\epsilon} = \sum_{x11}/\sum_{x1} + \sum_{x21}/\sum_{x2} + \sum_{x31}/\sum_{x3}$	$\sum_{\epsilon}/\sum$
C	$\sum_{x12}/\sum_{x1}$	$\sum_{x22}/\sum_{x2}$	$\sum_{x32}/\sum_{x3}$	$\sum_c = \sum_{x12}/\sum_{x1} + \sum_{x22}/\sum_{x2} + \sum_{x32}/\sum_{x3}$	$\sum_c/\sum$
H	$\sum_{x13}/\sum_{x1}$	$\sum_{x23}/\sum_{x2}$	$\sum_{x33}/\sum_{x3}$	$\sum_h = \sum_{x13}/\sum_{x1} + \sum_{x23}/\sum_{x2} + \sum_{x33}/\sum_{x3}$	$\sum_h/\sum$
				$\Sigma = \sum_{\epsilon} + \sum_c + \sum_h$	Σ/Σ

Таблица 6.

Нечёткая база знаний для оценки работоспособности

x_1	x_2	x_3	Y	Q
x_1	x_2	x_3	Высокое	$\sum_{x11}/\sum_{x1} \cdot x_1 + \sum_{x21}/\sum_{x2} \cdot x_2 + \sum_{x31}/\sum_{x3} \cdot x_3 + \sum_{\epsilon}/\sum \cdot Y$
x_1	x_2	x_3	Среднее	$\sum_{x12}/\sum_{x1} \cdot x_1 + \sum_{x22}/\sum_{x2} \cdot x_2 + \sum_{x32}/\sum_{x3} \cdot x_3 + \sum_c/\sum \cdot Y$
x_1	x_2	x_3	Низкое	$\sum_{x13}/\sum_{x1} \cdot x_1 + \sum_{x23}/\sum_{x2} \cdot x_2 + \sum_{x33}/\sum_{x3} \cdot x_3 + \sum_h/\sum \cdot Y$

Нечёткая модель экспертной системы в Matlab реализована двумя системами нечёткого вывода: *q_y.fis* – нечёткая система моделирования общей оценки лингвистических переменных (Y); *q_q.fis* – нечёткая система прогнозирования работоспособности системы (Q).

Диагностика осуществляется функцией *diagm*. Функция может возвращать два выходных аргумента: первый аргумент – результат прогнозирования работоспособности системы; второй аргумент – общей оценки лингвистических переменных. Функция вызывается с 6 входными аргументами, которые задают значения факторов x_1 , x_2 , x_3 , y_1 , y_2 , y_3 . Значения факторов y_1 , y_2 , y_3 можно задавать как числами, так и термами: «Н» – низкий; «НС» – ниже среднего; «С» – средний; «ВС» – выше среднего; «В» – высокий. Для логического вывода при нечётких входных данных используется функция *qgaussmf*, модифицированная из гауссовской функции принадлежности *gaussmf*. Расчёт степени принадлежности одного нечёткого множества к другому нечёткому множеству осуществляется функцией *qual_inp_gauss*. Логический вывод происходит через функцию *evalfis_ww*, которая аналогична функции *evalfis*, но не выдает предупреждений при использовании нечетких входных данных.

При разработке модуля экспертной системы для идентификации неисправностей на примере судовых паровых котлов. Входными параметрами являются давление пара, уровень воды в котле, давление топлива и температура выпускаемого пара. Выходные параметры – работоспособность котла (низкая работоспособность, средняя

работоспособность, высокая работоспособность). Для каждого параметра в числовом эквиваленте (для типа Сугено): низкое (от 1 до 6), среднее (от 7 до 19) и высокое (от 20 до 100). Правила сгенерированной системы нечёткого вывода для значения общей оценки лингвистических переменных Y приведены на рис.2, а для значения работоспособности системы Q приведены на рис.3. Визуализация соответствующей поверхности нечёткого вывода для значения работоспособности системы Q на рис 4. Поверхность нечёткого вывода позволяет установить зависимость значений работоспособности от значений входных переменных нечёткой модели системы управления объектом при фиксировании остальных переменных на основном уровне. Эта зависимость может послужить основой для программирования контроллера или аппаратной реализации соответствующего нечеткого алгоритма управления в форме соответствующей таблицы решений.

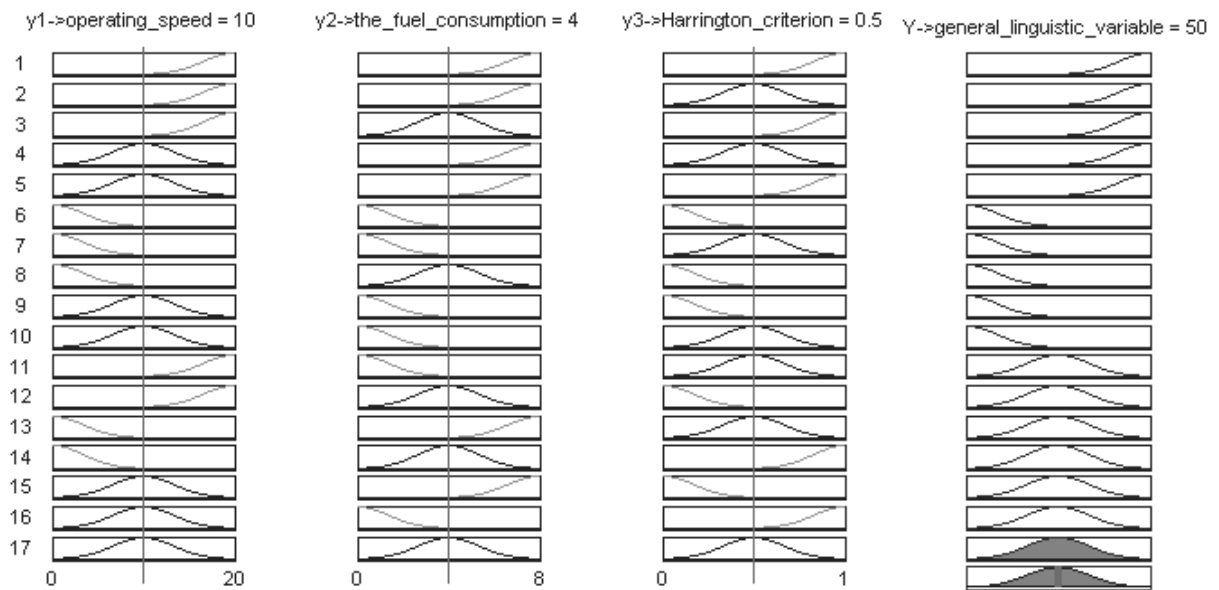


Рис. 2. Правила сгенерированной системы нечёткого вывода для значения общей оценки лингвистических переменных Y

На заключительном этапе производится построение схемы блочной модели в среде интерактивного моделирования Simulink. В качестве компонентов системы используются контроллеры, входами, которых являются параметры рабочего процесса и характеристики (возраст, время эксплуатации) соответствующего компонента. Выходом может быть остаточный ресурс компонента или величина воздействия на ресурс.

На рис.5 приведен возможный вариант компоновки такой схемы с четырьмя входными переменными t (температура), к.п.д., T и P , тремя уровнями нечёткого вывода, дифференциальной оценкой переменной P и интегральной оценкой вывода второго уровня Q_{cp} . На основании значений переменных t , к.п.д. определяется текущее значение переменной Q , которое уточняется на основании значения T . Переменная P - значение срока эксплуатации тестируемого оборудования, дифференциальные оценки, которой позволяют дополнить недостающие значения усредненными значениями переменной Q_{cp} и сброса интегральной оценки к 0 в случае замены оборудования. Последний уровень определяет окончательный вывод о состоянии оборудования в зависимости от накопления (интегральной оценки) значений Q_{cp} и срока службы оборудования.

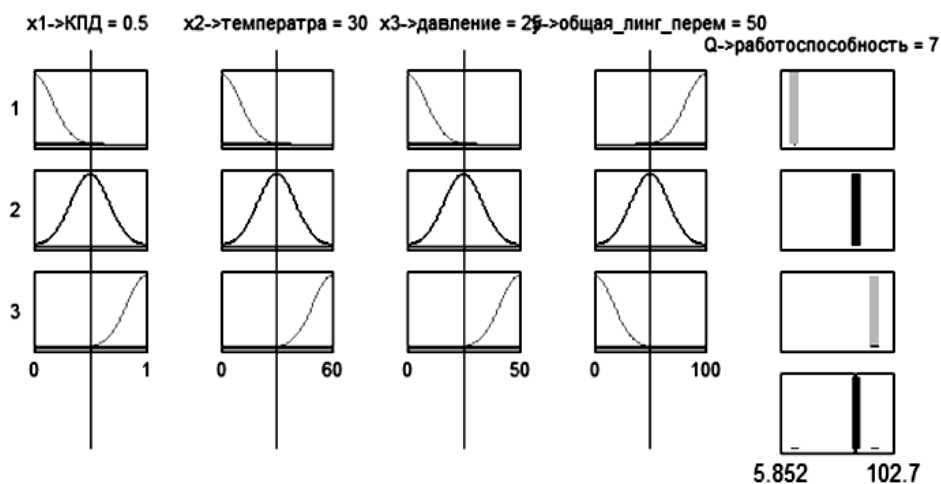


Рис. 3. Правила сгенерированной системы нечёткого вывода для значения работоспособности системы Q

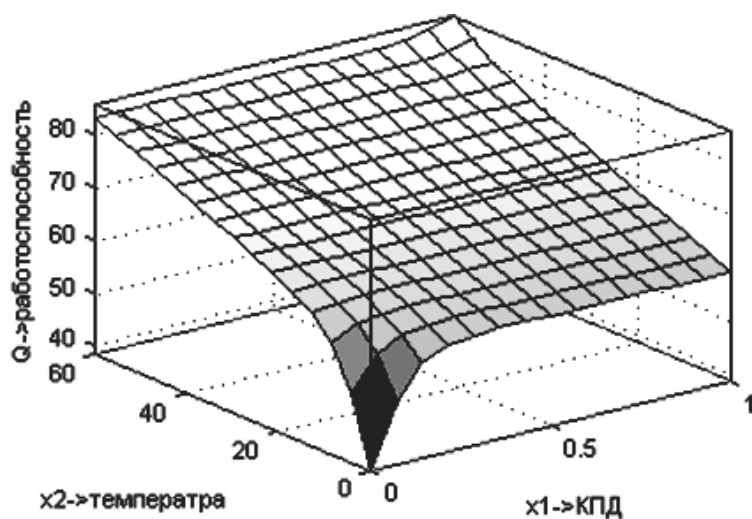


Рис. 4. Визуализация соответствующей поверхности нечёткого вывода для значения работоспособности системы Q

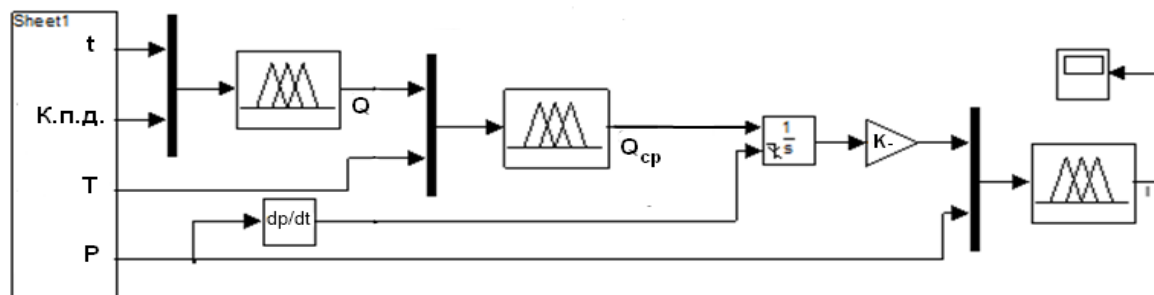


Рис. 5. Пример экспертной системы, построенной в среде Matlab Simulink

На основе данных, полученных при разных критериях, работоспособность СТС зависит как от значений нелингвистических переменных, так и от значения

лингвистических переменных и может колебаться как резко вверх, так и резко вниз в зависимости от комбинации этих переменных.

Практическая ценность полученных результатов состоит в том, что предложенный метод создания системы ДМД СТС по ее фактическому состоянию позволяет повысить эффективность оборудования судовых СТС за счет снижения времени простоев оборудования в ремонте, снизить затраты на ремонты и послеаварийное восстановление оборудования.

Выводы

Впервые разработаны методологические основы и принципы нового для судовых СТС научного направления – реализация интеллектуальных систем контроля и анализа функционирования СТС с использованием экспертной нечеткой информации.

Применение предлагаемого метода позволяет оценить работоспособность любой судовой технической системы при минимальной информации о ней. Результаты работы действующей нечеткой модели, разработанной на основе применения экспертного анализа данных, позволяют с высокой точностью оценить работоспособность судовых технических систем и принимать решение по дальнейшему применению данной системы.

Список литературы

1. Вычужанин, В.В. Метод управления рисками судовых сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Проблемы техники. – 2014. – №2. – С. 138 – 142.
2. Вычужанин, В.В. Технические риски сложных комплексов функционально взаимосвязанных структурных компонентов судовых энергетических установок / В.В. Вычужанин, Н.Д. Рудниченко // Вісник Одеського національного морського університету, збірник наукових праць. – 2014. – В.2(40). – С. 68 – 77.
3. Бакланов, А.И. Системы наблюдения и мониторинга / А.И. Бакланов. – М.: Бином, 2009. – 234 с.
4. Кончаков, Е.И. Техническая диагностика судовых энергетических установок / Е.И. Кончаков. – Владивосток. : ДВГТУ, 2007. – 112 с.
5. Головкин, С.В. Диагностика технического состояния судового электрооборудования на основе интеллектуального анализа данных / С.В. Головкин. // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. – 2009. – С. 90 – 95.
6. Одинцов, В.И. Диагностирование технического состояния дизелей по параметрам рабочего процесса / В.И. Одинцов, С.А. Кабыш. // Вестник Астраханского государственного технического университета. Серия: Морская техника и технология. – 2012. – С. 123 – 128.
7. Andersen, B.A Diagnostic System for Remote Real-Time Monitoring of Marine Diesel-Electric Propulsion Systems / B. Andersen. – Leipzig, 2011. – 45 p.
8. Минаков, А.А. Диагностирование оборудования с использованием параметров технологического контроля / А.А. Минаков, Д.В. Федосеев. // Известия Самарского научного центра Российской академии наук. – 2009. – С. 305 – 309.

ІНФОРМАТИЗАЦІЯ ДИСТАНЦІЙНОГО ДІАГНОСТУВАННЯ СТАНУ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ

С.Н.Коновалов, В.В. Вичужанін

Одеський національний морський університет,
вул. Мечникова 34, Одеса, 65404, Україна; e-mail: vint532@yandex.ru

У статті наведені результати розробки та інформатизації методу дистанційного моніторингу, діагностики складних технічних систем, встановлених на судах. Проведено аналіз використовуваних методів моніторингу, діагностики технічних систем. Описано метод дистанційного моніторингу, діагностики, що ґрунтується на експертному аналізі стану складних технічних систем. Наведено результати розробки нечіткої моделі для діагностування складної технічної системи, а також результати її дослідження. Застосування розробленого методу і його інформатизація дозволяє оцінити працездатність складної технічної системи в різних умовах і режимах її експлуатації, а також прогнозувати стан системи в аварійних екстремальних ситуаціях.

Ключові слова: складна технічна система, моніторинг, діагностика, прогнозування, експертний аналіз, нечітка модель

INFORMATIZATION OF THE CONTROLLED FROM DISTANCE DIAGNOSTICATING OF THE STATE OF THE DIFFICULT TECHNICAL SYSTEMS

S.N. Konovalov, V.V. Vychuzhanin

Odessa National Maritime University,
34, Mechnikov str., Odessa, 65404, Ukraine; e-mail: vint532@yandex.ru

To the article the results of development and informatization of method of remote monitoring, diagnosticians of the difficult technical systems set on courts, are driven. The analysis of the used methods of monitoring, diagnostics of the technical systems is conducted. The method of remote monitoring diagnostics, being base on expert analysis of the state of the difficult technical systems, is described. Results over of development of unclear model are brought for diagnosticating of the difficult technical system, and also results of her research. Application of the worked out method and his informatization allow to estimate the capacity of the difficult technical system under various conditions and modes of her exploitation, and also to forecast the state of the system.

Keywords: difficult technical system, monitoring, diagnostics, forecasting, expert analysis, fuzzy model

ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ КАНОНІЧНОГО ПРЕДСТАВЛЕННЯ ВЕКТОРНОГО АПОСТЕРІОРНОГО ПРОЦЕСУ

І.Р. Опірський

Національний університет «Львівська політехніка»,
вул. Ст.Бандери, 12, Львів, 79000, Україна; e-mail: iopirsky@gmail.com

В роботі проводиться дослідження і опис процесу $X(t)$ для прогнозування несанкціонованого доступу (НСД) з використанням канонічного представлення векторного апостеріорного процесу, приводиться математичне обґрунтування та виведення виразів, що точно описують апостеріорне математичне визначення векторного випадкового процесу $X(t)$ і в рамках зроблених припущень та досліджень дозволяють вирішити задачу прогнозування НСД.

Ключові слова: несанкціонований доступ, інформаційні системи держави, апостеріорний процес, випадковий процес, прогнозування

Вступ

Проблема прогнозування включає в себе ряд численних труднощів, одні з яких власне зв'язані з прогнозуванням, другі характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю.

Прогнозування несанкціонованого доступу (НСД) на інформаційні мережі держави (ІМД) без сумніву повинно ґрунтуватись на вивченні тенденцій, що спостерігаються в зміні її поточного стану під дією НСД. В теорії автоматичного контролю передбачається, що цей стан може бути представлено сукупністю значень деяких контрольних параметрів. Тоді, очевидно, причиною, що викликає зміни стану ІМД, повинні бути зміни значень саме цих параметрів. Таким чином прогнозування НСД в ІМД повинно базуватись на прогнозуванні значень складових контрольних параметрів. Це може здійснюватись на базі математичного апарату екстраполяції процесів, що описує закономірності змін в параметрах. В свою чергу, використання апарату екстраполяції потребує певної формалізації процесів змін контрольних параметрів, тобто потребує створення певної математичної моделі процесів вимірювання параметрів ІМД під впливом НСД.

Прогнозний контроль потребує визначення спеціальних прогнозних параметрів. Такі параметри повинні відрізнятися рядом особливостей [1]. По-перше, вони повинні з відповідною точністю представляти стан контрольованого об'єкту ІМД. По-друге вони повинні відображати основні тенденції в змінах мережі. По-третє, як і всі контрольні параметри, вони повинні допускати зміни з необхідною точністю.

Всі перелічені особливості, як це легко побачити, в той же час є особливостями параметрів якості.

Важливою проблемою є визначення дійсного місця прогнозуючого контролю серед всіх форм контролю в підвищенні ефективності використання системи контролю НСД. Рішенням цієї проблеми в чималому степені залежить від самої можливості

здійснення прогнозу в тих чи інших конкретних умовах застосування в системах та мережах.

Оскільки автоматична система контролю (АСК) має в своєму складі засоби обчислювальної техніки, то ці методи є особливо прийнятними при автоматизації контролю. Ідея їх полягає в тому, що тим чи іншим методом моделюється безліч реалізацій випадкового процесу $X^{PS}(t)$, які використовуються для рішення системи рівнянь і визначення любых необхідних апостеріорних характеристик статистики цим методом. В даному випадку рішення задачі прогнозу складається з наступних етапів:

- перший етап. Отримання з статистичних даних елементів опису досліджуваного випадкового процесу $X(t)$, придатного для відтворення його шляхом моделювання. Від універсальності такого опису в більшій мірі залежить і універсальність методу в цілому.

- другий етап. Розробка алгоритму, що дозволяє враховувати значення конкретної реалізації процесу $X(t)$, вимірювати при контролі і отримувати на цій основі опис апостеріорного випадкового процесу $X^{PS}(t)$. Наявність такого опису дозволяє шляхом моделювання визначити характеристики даного процесу і, таким чином, повністю вирішити задачу прогнозування.

- третій етап. Розробка алгоритму рішення системи стохастичних рівнянь:

$$X^{PS}(t) - a = 0; X^{PS}(t) - b = 0, \quad (1)$$

де, $X^{PS}(t) = X[t/x_w(\Theta), t_1 \leq \Theta \leq t_k]$ – апостеріорний (умовний) випадковий процес, виникаючий із апіорного при врахуванні результатів контролю. Виконання даного етапу дозволяє повністю вирішити задачу прогнозування НСД.

Наведений перелік показує, що основною передумовою до рішення задачі є наявність достатньо зручного опису процесу $X(t)$. При цьому пропонується апроксимувати реальний випадковий процес $X(t)$ лінійною функцією часу $X(t) = A + Bt$, де A і B – випадкові коефіцієнти, ймовірні характеристики яких визначаються за допомогою методу найменших квадратів, виходячи з умови $M \int_T [X(t) - (A + Bt)]^2 dt = \min$, при чому T – інтервал спостереження випадкового процесу $X(t)$.

Мета роботи

Метою даної роботи є дослідження і опис процесу $X(t)$ для прогнозування НСД з використанням канонічного представлення векторного апостеріорного процесу.

В роботі приводиться математичне обґрунтування та виведення виразів, що точно описують апостеріорне математичне визначення векторного випадкового процесу $X(t)$ і в рамках зроблених припущень та досліджень дозволяють вирішити задачу прогнозування НСД.

Основна частина

Стан ІМД характеризується як правило, декількома параметрами, в загальному випадку залежних між собою. У зв'язку з цим велике практичне значення набувають методи, що дозволяють вирішити задачу прогнозу для векторного випадкового процесу

$X(t) = [X_1(t), X_2(t), \dots, X_n(t)]$ з залежними складовими. Одним із найбільших прийнятних є метод, що базується на канонічному представленні даного процесу в дискретному ряді точки $t_i, i = \overline{1, I}$ [1].

Якщо вихідний випадковий процес $X(t)$ заданий у вигляді векторної випадкової послідовності $X(i), i = \overline{1, I}$, то його канонічне представлення може бути зазначено у вигляді:

$$X_h(i) = m_h(i) + \sum_{\lambda=1}^h \sum_{v=1}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i), h = \overline{1, n}, i = \overline{1, I}, \quad (2)$$

де $V_v^{(\lambda)}, v = \overline{1, I}, \lambda = \overline{1, n}$ – випадкові коефіцієнти з властивостями $M[V_v^{(\lambda)}] = 0, M[V_v^{(\lambda)} V_\mu^{(\zeta)}] = 0$, при невиконанні хоча б одної з умов: $v = \mu$ або $\lambda = \zeta$ $M[V_v^{(\lambda)}]^2 = D_v^{(\lambda)}$. Якщо уявити, що одномірна щільність розподілу кожного з цих коефіцієнтів задається d , то для збереження відомостей про них в пам'яті ЕОМ необхідно dnf комірок.

Властивості невинуватих координатних функції процесу визначаються співвідношенням $\varphi_{hv}^{(\lambda)}(i) = 0$ при цьому $i < v$ і $\lambda > h$; $\varphi_{hv}^{(\lambda)} = 1$ при $i = v$ і $\lambda = h$. Об'єм пам'яті, необхідний для їх збереження, оцінюється наступним методом. Для першої складової наявний один масив координатних функцій, об'єм якого рівний $I(I+1)/2$.

Для другої складової таких масивів вже два, для третьої – три, $N_{\kappa\phi} = \frac{n(n+1)}{2} \frac{I(I+1)}{2}$.

З врахуванням математичних очікувань складових процесу мінімальний загальний об'єм пам'яті, необхідний для запису апіорної інформації про нього, складе $N(n, I) = nI + dnI + \frac{n(n+1)}{2} \frac{I(I+1)}{2}$.

Як, показано в [1], випадковий процес $X(t)$ в дискретному вигляді точки $t^i, i = \overline{1, I}$, точно представляється своїм канонічним розкладанням:

$$X(i) = m(i) + \sum_{v=1}^i v_v \varphi_v(i), i = \overline{1, I}, \quad (3)$$

Відповідно для його дисперсії і кореляційної функції можна записати:

$$D(i) = \sum_{v=1}^i D_v \varphi_v^2(i), i = \overline{1, I} \quad (4)$$

$$K(i, j) = \sum_{v=1}^{\min(i, j)} D_v \varphi_v(i) \varphi_v(j), i, j = \overline{1, I}. \quad (5)$$

Елементи виразу (5) визначаються виразами

$$V_1 = \overset{o}{X}(1), V_i = \overset{o}{X}(i) = \sum_{v=1}^i V_v \varphi_v(i), i = \overline{2, I}; \quad (6)$$

$$\varphi_v(i) = \frac{1}{D_v} M \left[V_v \overset{o}{X}(i) \right], v = \overline{1, I}, i = \overline{v, I}; \quad (7)$$

$$D_1 = D(1), D_i = D(1) - \sum_{v=1}^{i-1} D_v \varphi_v^2(i), i = \overline{2, I}. \quad (8)$$

Вирази (6)-(8) описують алгоритм визначення канонічного розкладання процесу по вихідних статистичних даних. Детально цей алгоритм розглянутий в роботі [2]

На підставі канонічного представлення (6) можна отримати вираз для апостеріорного випадкового, враховуючи дані контролю. Нехай з чергового контролю стало відомо значення $X(1)$ конкретної реалізації процесу $X(t)$. Для цього значення, як і для всіх інших, справедливо (3), звідки $X(1) = m(1) + V_1$, $V_1 = X(1) - m(1)$. Тоді з (3) слідує, що апостеріорний випадковий процес, що проходить в момент $i=1$ через точку $X(1)$, описується виразом $X^{(1)}(i) = m(i) + [x(1) - m(1)]\varphi_1(i) + \sum_{v=2}^i V_v \varphi_v(i)$, $i = \overline{1, I}$.

Застосування апаратно математичного очікування, можна визначити математичне очікування цього апостеріорного процесу

$$m^{(1)}(i) = m(i) + [x(1) - m(1)]\varphi_1(i), i = \overline{1, I}. \quad (9)$$

При введенні виразу (9) використано припущення про те, що конкретне значення першого коефіцієнта не змінює математичного очікування решти коефіцієнтів, залишаючи їх вірними нулю. Це припущення не завжди справедливо, оскільки коефіцієнти V_v не тільки некорельовані а й незалежні. Однак припущення, щодо незалежності, доводиться використовувати вже при моделюванні апіорного випадкового процесу, і воно зазвичай не є вагомим, так як стохастичні зв'язки вищих порядків швидко затухають з ростом інтервалу дискретності $t_i - t_{i-1}$. Тому і дане припущення можна вважати цілком прийнятним.

Використовуючи попередні вирази, остаточно отримуємо:

$$X^{(1)}(i) = m^{(1)}(i) + \sum_{v=2}^i V_v \varphi_v(1), i = \overline{1, I}. \quad (10)$$

Тепер припустимо, що при черговому контролі отримано наступні значення $X(2)$ тої ж реалізації процесу. Для цього значення вірним буде вираз (10), звідки $x_2 = m^{(1)}(2) + V_2$. Повторюючи операції зроблені на першому кроці, отримуємо для $i = \overline{1, I}$: $m^{(2)}(i) = m^{(1)}(i) + [x(2) - m^{(1)}(2)]\varphi_2(i)$, $X^{(2)}(i) = m^{(2)}(i) + \sum_{v=3}^i V_v \varphi_v(i)$.

Вираз (10) є основою для математичного опису апостеріорного випадкового процесу, причому методика виведення відповідного виразу повторює використані раніше способи. Нехай в момент $\mu=1$ стало відомо значення першої складової процесу $X_1(\mu) = x(1)$. Для цього значення, як і для всіх решта справедливе представлення (2), звідки $x_1(1) = m_1(1) + v_1^{(1)}$.

Підстановка, визначеного таким шляхом значення коефіцієнта $v_1^{(1)}$, в вираз (1) дає

$$X_h^{(1)}(i) = m_h(i) + [x_1(1) - m_1(1)]\varphi_{h1}^{(1)} + \sum_{v=2}^i V_v^{(1)} \varphi_{hv}^{(1)}(i) + \sum_{\lambda=2}^h \sum_{v=1}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i), h = \overline{1, n}, i = \overline{1, I}. \quad (11)$$

Тут $X_h^{(1)}(i)$; $h = \overline{1, n}$; $i = \overline{1, I}$ - апостеріорний випадковий процес, який проходить в момент $\mu = 1$ через точку з фіксованою координатною $X_1(1) = x_1(1)$.

Вважаючи, що відомого значення $x_1(1)$ не змінює математичних очікувань випадкових коефіцієнтів $V_v^{(\lambda)}$, знайдемо математичне очікування даного процесу

$$m_h^{(1)}(i) = m_h(i) + [x_1(1) - m_1(1)]\varphi_{h1}^{(1)}(i), h = \overline{1, n}, i = \overline{1, I}. \quad (12)$$

Зазначимо, що поява одного відомого значення першої складової процесу привело до зміни математичних очікувань всіх інших складових. Це явище природнім наслідком наявності залежностей між ними.

З врахуванням (12) з (11) кінцево отримуємо

$$X_h^{(1)} = m_h(i) + \sum_{v=2}^i V_v^{(1)} \varphi_{hv}^{(1)}(i) + \sum_{\lambda=2}^h \sum_{v=1}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i), h = \overline{1, n}, i = \overline{1, I}. \quad (13)$$

Вводячи відоме початкове значення другої складової, з (13) отримуємо $x_2(1) = m_2^{(1)}(1) - \nu_1^2$, звідки при $h = \overline{1, n}, i = \overline{1, I}$ $m_h^{(2)}(i) = m_h^{(1)}(i) + [x_2^{(1)}(1) - m_2^{(1)}(1)]\varphi_{h1}^{(2)}(i)$,
 $X_h^{(2)} = m_h^{(2)}(i) + \sum_{\lambda=1}^h \sum_{v=2}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i) + \sum_{\lambda=3}^h \sum_{v=1}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i).$

Послідовно розглядаючи відомі початкові значення складових більш високого порядку, отримуємо можливість узагальнювати отримані результати на випадок довільної кількості $r_1 \leq n$ відомих значень які в момент $\mu = 1$ приймають участь в формуванні апостеріорного процесу:

$$X_h^{(r_1)}(i) = m_h^{(r_1)}(i) + \sum_{\lambda=1}^h \sum_{v=\eta_1}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i). \quad (14)$$

тут при $h = \overline{1, n}, i = \overline{1, I}$: $m_h^{(r_1)}(i) m_h^{(r_1-1)}(i) + [x_{r_1}(1) - m_{r_1}^{(r_1-1)}(1)]\varphi_{h1}^{(r_1)}(i)$, $r_1 = \begin{cases} 2 \text{ при } \lambda \leq r_1 \\ 1 \text{ при } \lambda > r_1 \end{cases}$.

Подальше узагальнення зв'язане з послідовним розглядом нових відомих значень процесу для моментів контролю з номерами $\mu > 1$. Так для першої складової процесу в момент $\mu = 2$ відоме значення $x_1(2)$ визначається з (14) як $x_1(2) = m_1^{(r_1)}(2) + \nu_2^{(1)}$ типові перетворення при $h = \overline{1, n}, i = \overline{1, I}$ дають $m_h^{(r_1,1)}(i) = m_h^{(r_1)}(i) + [x_1(2) - m_1^{(r_1)}(2)]\varphi_{h2}^{(1)}(i)$,

$$X_h^{(r_1,1)}(i) = m_h^{(r_1,1)}(i) + \sum_{v=3}^i V_v^{(1)} \varphi_{hv}^{(1)}(i) + \sum_{\lambda=2}^h \sum_{v=\eta_2}^i V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i).$$

Легко помітити, що з зростанням номера моменту контролю характер одержаних результатів зберігається. Це дозволяє записати загальний вираз для апостеріорного векторного випадкового процесу і його математичного очікування при довільному числі $k < I$ моментів контролю і числа $r_\mu, n \geq r_\mu \geq r_{\mu=1}, \mu = \overline{1, k}$ відомих значення процесу з них:

$$m_h^{(o)}(i) = m_h(i), m_h^{(r_1, r_2, \dots, r_k)}(i) = m_h^{(r_1, r_2, \dots, r_{k-1})}(i) + [x_{r_k}(k) - m_{r_k}^{(r_1, \dots, r_{k-1})}(k)]\varphi_{hk}^{(r_k)}(i) \quad (15)$$

$$X_h^{(r_1, \dots, r_k)} m_h^{(r_1, \dots, r_k)}(i) + \sum_{\lambda=1}^{ih} \sum_{v=\eta_k}^h V_v^{(\lambda)} \varphi_{hv}^{(\lambda)}(i) \quad (16)$$

де $h = \overline{1, n}, i = \overline{1, I}, \eta_k = \begin{cases} k + 1npi\lambda \leq r_k \\ 1npi\lambda > r_k \end{cases}$.

Вираз (15) точно описує апостеріорне математичне визначення векторного випадкового процесу $X(t)$ в рамках зроблених припущень і відповідно дозволяє вирішити задачу прогнозування НСД. Сукупність виразів (15 і 16) повністю описує апостеріорний випадковий процес при тих же припущеннях і забезпечує вирішення задачі прогнозування. Очевидно, що алгоритм вирішення цих задач повинен в більшості нагадувати алгоритм для одномірного процесу, оскільки математичний апарат і методика отримання опису апостеріорного процесу в обох випадках однакові. Схема такого алгоритму для найбільш поширеного на практиці випадку $r_\mu = n, \mu = 1, k, k < I$ детально описано в [2].

Слід відмітити, що для апостеріорного багатомірного процесу, як і для одномірного випадку, представлення у вигляді (16) не є єдиновірним. В [5] отримано канонічне представлення апостеріорного процесу, в якому рекурентному перетворенню піддавались не відомі значення, отримані в результаті контролю, а відповідні координатні функції.

Висновки

На основі математичного обґрунтування та виведення виразів, що точно описують апостеріорне математичне визначення векторного випадкового процесу $X(t)$, і в рамках зроблених припущень та досліджень виведено вирази прогнозування НСД в інформаційних системах держави методом канонічного представлення векторного апостеріорного процесу, що в свою чергу дозволило отримати подальший розвиток вирішенню проблеми прогнозування НСД.

Список літератури

1. Дианов, В.Д. Диагностика и надежность автоматических систем, 2 пособие / В.Д. Дианов. – М.: МГИУ, 2005. – 160 с.
2. Булинский, А.В. Теория случайных процессов / А.В. Булинский, А.Н. Ширяев. – М.: ФИЗ, 2005. – 408 с.
3. Кремер, Н.Ш. Теория вероятностей и математическая статистика / Н.Ш. Кремер // Учебник для ВУЗов. - 2- изд., перераб. и доп.-М:ЮНИТИ-ДАНА. – 2004. – 573 с.
4. Квасов, Б.И. Численные методы анализа и линейной алгебры. Учеб. пособие / Б.И. Квасов / Новосиб. гос. ун-т. Новосибирск. – 2012. – 262 с.
5. Gu, Y. and D.S. Oliver. An interativ ensemble Kalman filter for multiphase fluid flow data assimilation / Gu, Y. and D.S. Oliver. // SPE Journal. – 2005. – Vol.12. – №4. – P. 217-224.
6. Сінчук, О.М. Основи надійності та технічної діагностики електроустаткування промислових підприємств: Монографія / О.М. Сінчук, М.І. Лісний, І.О. Сінчук, Є.І. Скапа, О.О. Удовенко. – Кременчук: Вид. ПП Щербатих О.В., 2012. – 264 с.
7. Булинский, А.В. Теория случайных процессов / А.В. Булинский, А.А Ширяев. – М.: ФИЗ, 2005. — 408 с.

ПРОГНОЗИРОВАНИЕ НСД С ИСПОЛЬЗОВАНИЕМ КАНОНИЧЕСКОГО ПРЕДСТАВЛЕНИЕ ВЕКТОРНОГО АПОСТЕРИОРНОГО ПРОЦЕССА

И.Р. Опирский

Национальный университет «Львовская политехника»,
ул. Бандеры, 12, Львов, 79000, Украина; e-mail: iopirsky@gmail.com

В работе проводится исследование и описание процесса $x(t)$ для прогнозирования НСД с использованием канонического представления векторного апостериорного процесса, приводится математическое обоснование и вывод выражений, точно описывают апостериорное математическое определение векторного случайного процесса $X(t)$ и в рамках сделанных предположений и исследований позволяют решить задачу прогнозирования НСД.

Ключевые слова: несанкционированный доступ, информационные системы государства, апостериорный процесс, случайный процесс, прогнозирование

UA PREDICTION USING CANONICAL REPRESENTATION OF VECTOR POSTERIORI

I.R. Opirskyy

National University "Lviv Polytechnic"
12, St. Bandery str., Lviv, 79000, Ukraine; e-mail: iopirsky@gmail.com

The work is to study and description of $x(t)$ to predict UA using canonical representation vector posteriori process driven mathematical reasoning and output expressions that accurately describe a posteriori mathematical definition of a vector random process $X(t)$ and under the assumptions made and research allow solve the problem of forecasting UA.

Keywords: unauthorized access, information systems of the state, a posteriori process, stochastic process forecasting

ФРАКТАЛЬНЫЙ АНАЛИЗ РЕОЛОГИИ МНОГОКОМПОНЕНТНЫХ И ГЕТЕРОГЕННЫХ ПЛАСТОВЫХ СИСТЕМ

С. А. Положаенко, Мухиалдин Хасан Моха

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

Исследовано условие «гладкости» фронта раздела составляющих многокомпонентных (гетерогенных) систем на основании анализа «скачка» насыщенности в функции Баклея-Левверетта. Показано, что «скачок» насыщенности отсутствует, а фронт раздела продвигается устойчиво и сохраняет «гладкость», если подвижность вытесняющей компоненты не превышает подвижность вытесняемой. Также показано, что нарушение «гладкости» фронта раздела приводит к фрактально-неоднородной структуре процесса реологии. Получены численные значения фрактальной размерности фронта раздела для реологического процесса, развивающегося в реальных геологических условиях.

Ключевые слова: многокомпонентная система, гетерогенная система, процесс реологии, фрактально-неоднородная структура, фрактальный кластер, фрактальная размерность

Введение

В последние годы появился ряд работ (например, [1]), в которых исследуются вопросы ранее не изученного влияния процесса образования фрактальных структур на фильтрацию внутрипластовых жидкостей. Это влияние может осуществляться за счет фрактальной структуры пористой среды [2] или самой системы фильтрующихся жидкостей, имеющих гетерогенный характер [3]. В работе [2] утверждается, что переход от линейного закона фильтрации к нелинейному в сильной степени зависит от распределения пор по размерам или фрактальности структуры пористой среды.

Имеется ряд работ по экспериментальному определению фрактальной размерности пористых сред. В частности, в работе [4] методом сканирующей электронной микроскопии определена пространственная фрактальная размерность реального образца пористой среды, в [5] впервые предложен метод определения фрактальной размерности по экспериментальной изотерме адсорбции газа, который (метод) нашел своё развитие в работах [6, 7]. В работах [8, 9] предложены косвенные способы определения фрактальных характеристик пласта по кривым восстановления давления [8] и реакции пластовой системы на мгновенное изменение давления [9].

Представляется перспективным, с точки зрения временных и ресурсных затрат, использовать средства математического моделирования для исследования фрактальных геологических структур и реологии (фильтрации в пористой среде) фрактально-неоднородных пластовых систем. Для построения адекватной математической модели (ММ) фрактально-неоднородной пластовой системы необходимо выполнить анализ и оценку фрактальной размерности реологической картины в исследуемой пластовой системе. В ряде работ, например [10 – 12] выполнена попытка формализации реологии в пористых средах для случая фрактальной структуры последней, однако приведенные

модели получены для идеального лотка Хелле-Шоу и имеют исключительно теоретическое значение.

Цель работы

Качественное описание процесса реологии многокомпонентной (гетерогенной) системы в пористой среде и получение численной оценки ее фрактальной размерности.

Основная часть

Для фильтрующихся многофазных жидкостей (систем) важным аспектом при моделировании динамики является определение фронта раздела между отдельными компонентами. Данная задача может иметь и самостоятельное прикладное значение, например, когда исследуется процесс вытеснения одной жидкостью другой.

Предположение о «гладкости» фронта раздела компонент в фильтрующейся многофазной (а также гетерогенной) системе возможно лишь в случае «близости» физико-химических свойств этих компонент (или мелкодисперсности и низкой концентрации гетерогенной системы). В противном случае «гладкость» фронта нарушается, а фильтрующийся поток приобретает фрактально-неоднородную структуру со «сложным» фронтом раздела фаз. Ещё более сложную картину реологии приобретает случай, когда с границей Γ области моделирования Ω контактируют разные компоненты многофазной (или гетерогенной) системы.

В пластовой гидро-газодинамике условием, определяющим границу раздела двух (для простоты дальнейшего рассмотрения) фильтрующихся компонент многофазного или гетерогенного потока, может служить «скачок» насыщенности в функции Баклея-Леверетта [13, 14 – 16]

$$J(S) = \frac{k_1^0(S_1)}{\mu_1 k_1^0(S_1) + \mu_2 k_2^0(S_2)}, \quad (1)$$

где $k_1^0(S_1)$ и $k_2^0(S_2)$ — относительные фазовые проницаемости фильтрующихся компонент; μ_1 и μ_2 — их вязкости; S_1 и S_2 — насыщенности порового пространства фильтрующимися компонентами, соответственно.

Физически «скачок» насыщенности обусловлен наличием у одной из компонент многофазной системы напряжения сдвига τ , превышающего предельное значение ($\tau > \tau^*$). В литературе данная компонента получила название «вытесняющей» [13 – 15]. Экспериментально установлено [14], что фронт раздела фильтрующихся компонент многофазной системы продвигается устойчиво (т.е. фрактально-неоднородная структура процесса реологии отсутствует), если подвижность вытесняющей компоненты не превышает подвижность вытесняемой компоненты (рис.1(a)).

$$\frac{k_1(S_1)}{\mu_1} \leq \frac{k_2(S_2)}{\mu_2}. \quad (2)$$

На практике более удобно пользоваться выражением, полученным из (2), делением последнего на усреднённую скорость фильтрации ϖ :

$$\frac{\partial P(t, z)}{\partial \eta} > 0, \quad \frac{\partial P_c(S)}{\partial \eta} > 0, \quad (3)$$

где $P(t, z)$ задает внутрипластовое (усредненное) давление для фильтрующихся компонент многофазной системы; $P_c(S)$ — капиллярное давление, обусловленное наличием различных скоростей фильтрации для компонент в многокомпонентной системе; η — нормаль к градиенту внутрипластового давления $P(t, z)$ на границе Γ .

В противном случае скорость фильтрации вытесняемой компоненты ϖ_2 выше скорости изменения насыщенности вытесняющей компоненты, что приводит к образованию фрактально-неоднородной структуры процесса реологии, т.е. существенному нарушению «гладкости» фронта раздела (рис.1(б)). При этом физическая картина реологического процесса характеризуется появлением «пальцев» вытесняющей компоненты (рис.1(в)). В предельном случае в фильтрующемся потоке возможно даже образование «застойных зон» [13, 14], представляющих собой участки вытесняемой компоненты с нулевой скоростью фильтрации $\varpi_2 = 0$ (рис.1(г)). Иными словами, вытесняемая компонента «отстывает» медленнее, чем продвигается вытесняющая компонента, что физически и определяет механизм образования фрактально-неоднородной структуры и, как следствие, «застойных зон».

Предположим, что в момент времени $t=0$ поверхность фронта раздела представляет собой плоскость $F(z_i) = \Xi_0, i=1, 2$. Нарушение устойчивости фронта раздела учтем в виде нестационарных возмущений, нарушающих постоянство насыщенностей компонент S_j многофазной системы ($j=2$ — для двухфазного случая) в областях распространения фронта и искажающих его «гладкость», что отразится следующим образом

$$F(z_i, t) = \Xi_0(t); i=1, 2, \quad (4)$$

где z_i — соответствуют координатам в невозмущенной плоскости фронта раздела.

Выраженная направленность развития рассматриваемого процесса реологии, о которой говорилось выше, свидетельствует об его отклонении от линейного закона Дарси [14 – 16] (т.е. о пропорциональной линейной зависимости скорости фильтрации ϖ от градиента внутрипластового давления $grad(P)$) и о возможном наличии предельного градиента G , обуславливающего ненулевую скорость продвижения фронта раздела.

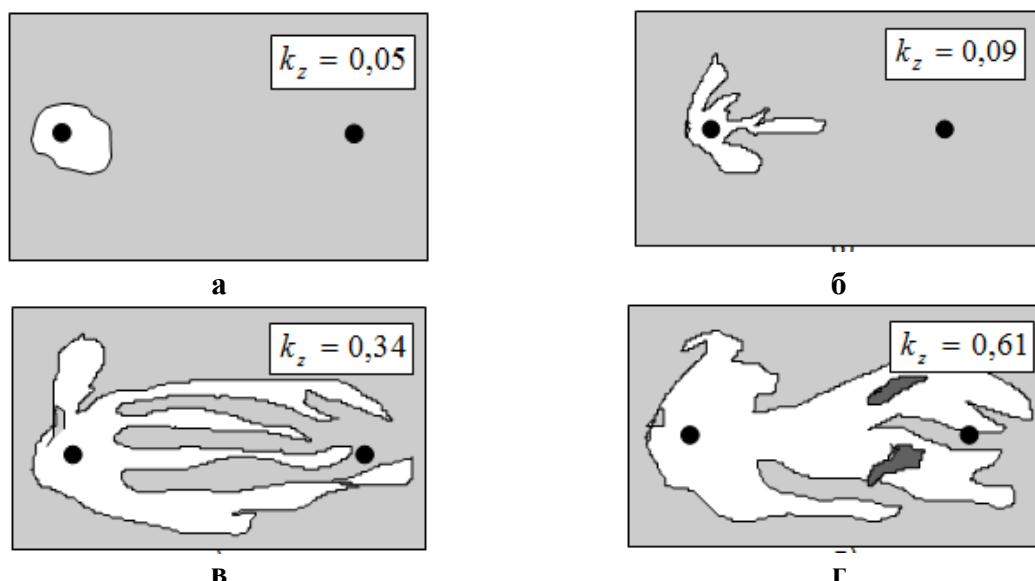


Рис. 1. Картина реологии двухкомпонентной системы на примере водо-нефтяной смеси при различных значениях пропускной способности k_z пористой среды

Формализовано данное предположение представим следующим образом (для двухкомпонентного потока, $j = 1, 2$)

$$\varpi_j = -\frac{k_j(S_j)}{\mu_j} \left[\text{grad}(P_j) - \frac{G_j}{|\text{grad}(P_j)|} \right]; \quad |\text{grad}(P_j)| > G_j, \quad \varpi_j = 0;$$

$$|\text{grad}(P_j)| \leq G_j; \quad j = 1, 2. \quad (5)$$

Уравнения динамики вида (5) дополним уравнениями неразрывности (случай двух компонент в многофазной системе)

$$\text{div}(\varpi_j) - (-1)^j m \frac{\partial S_j}{\partial t} = 0; \quad j = 1, 2. \quad (6)$$

Граничные условия (ГУ) на возмущенной поверхности фронта раздела компонент (4), выражающие равенство давлений перед и за фронтом раздела, а также расходов

$$\frac{\partial Q_1}{\partial \eta} = m \overline{\varpi} (S_1^h - S_1^f); \quad \frac{\partial Q_2}{\partial \eta} = m \overline{\varpi} (S_2^h - S_2^f)$$

определены на невозмущенной поверхности фронта вытеснения Ξ_0 .

Очевидно, что для «гладкости» границы раздела требуется ограниченность возмущений на поверхности Ξ_0 . Тогда для определения возмущений скоростей, давлений и насыщенностей получим следующие выражения (в приведенных ниже выражениях возмущения соответствующих величин обозначены знаком тильда, а невозмущенные величины обозначены индексом 0)

$$\varpi_j = -\frac{k_j(S_j)}{\mu_j} J_0(S_j) \left[\text{grad}(\tilde{P}_j) - \frac{G_j}{|\text{grad}(\tilde{P}_j)|} \right]; \quad |\text{grad}(\tilde{P}_j)| > G_j, \quad \varpi_j = 0;$$

$$|\text{grad}(\tilde{P}_j)| \leq G_j; \quad j = 1, 2, \quad (7)$$

с ГУ, учитывающими ограниченные возмущения (или их отсутствие) на поверхности фронта $F(z_i) = \Xi_0; i = 1, 2$

$$\frac{\partial \tilde{P}(t, z_i)}{\partial \eta} > 0, \quad \frac{\partial \tilde{P}_c(S)}{\partial \eta} > 0; \quad i = 1, 2, \quad (8)$$

$$\frac{\partial \tilde{Q}_j}{\partial \eta} = m \overline{\varpi} (S_j^h - S_j^f); \quad j = 1, 2. \quad (9)$$

Таким образом, формулировка задачи об устойчивости фронта раздела компонент многофазной системы фактически сводится к определению возмущений насыщенности («скачку» насыщенности) из системы (7) с ГУ (8), (9).

Однако возникновение фрактально-неоднородной структуры процесса реологии свидетельствует о значительных возмущениях фронта раздела компонент многофазной системы, что, формализовано, должно быть отражено в граничных условиях, поскольку последние определяют геометрию фронта раздела. В соответствии с одним из свойств,

составляющих основу определения фрактальных систем, фрактальная структура представляет собой систему с дробной размерностью (именуемой в литературе, например [1, 3, 10, 11], фрактальной размерностью), геометрически объединяющая фрактальные кластеры (или агрегаты). При этом фрактальный кластер представляет собой совокупность достаточно большого числа элементов, которые внутри данной совокупности сохраняют свою индивидуальность [3, 10, 11]. С точки зрения реологии многокомпонентных систем, под фрактальным кластером будем понимать совокупность «пальцев» вытесняющей компоненты на фронте раздела (рис.1(в,г)).

Если выполнить аппроксимацию фронта раздела в пределах одного «пальца» ломаной линией, то ее длину можно представить в следующем виде

$$L = a(R/a)^D, \quad (10)$$

где L — линейный размер «пальца» вытесняющей компоненты (по прямой); a — размер звена ломаной линии (усреднённый размер «зерна» порового пространства); R — размер фрактального кластера (радиус сферы, охватывающий «палец»); D — фрактальная размерность, обеспечивающая для кластера определенную область масштабов, в которой выполняется аппроксимация вида (10).

Разрешая (10) относительно фрактальной размерности D получим

$$D = [\ln(L) - \ln(a)] / [\ln(R) - \ln(a)]. \quad (11)$$

Учитывая реальные (усреднённые) геологические значения параметров [8, 14], входящих в (10), и, подставляя их в (11), можно оценить величину фрактальной размерности для пористых сред, в которых осуществляется реология многокомпонентных (или гетерогенных) систем

$$D = [\ln(100) - \ln(0,1)] / [\ln(50) - \ln(0,1)] = [4,605 - (-2,302)] / [3,912 - (-2,302)] = 1,112.$$

Заметим, что фрактальная размерность D является определяющей геометрической характеристикой фрактально-неоднородной структуры реологического процесса для многокомпонентной (гетерогенной) системы в пластовом пространстве, а полученная ее численная оценка позволяет разработать адекватную ММ исследуемого процесса.

Вывод

Выполнено качественное описание и анализ фрактальных свойств процесса реологии многокомпонентной (гетерогенной) системы в пористой среде при значительных возмущениях на фронте раздела компонент. На основании анализа получены формализованное представление фрактальной размерности «возмущенного» фронта и ее числовая оценка.

Список литературы

1. Мандельбот, Б. Фрактальная геометрия природы / Б. Мандельбот. — М.-Ижевск: МКИ, 2002. — 656 с.
2. Сулеманов, Б.А. Экспериментальные исследования образования фрактальных структур при вытеснении нефти / Б.А. Сулеманов // Азербайджанское нефтяное хозяйство. — 2010. — № 5. — С. 29 — 33.
3. Динариев, О.Ю. Движение жидкостей и газов в пористых средах с фрактальной геометрией / О.Ю. Динариев // Известия РАН. Механика жидкости и газа. — 2012. — № 4. — С. 101 — 109.
4. Suleimanov, B.A. Experimental Study of the Formation of Fractal Structures During Oil Displacement / B.A. Suleimanov // Energy Sources. — 2005. — Vol. 17. — № 4. — P. 477 — 483.

5. Bak, P. Self-organized criticality / P. Bak, C. Tang, K. Wiesenfeld // Phys. Rev. A. – 2008. – Vol. 38. – № 1. – P. 364–374.
6. Трубецкой, К. Н. Фрактальная структура нарушенности каменных углей и их предрасположенность к газодинамическому разрушению / К.Н. Трубецкой, А.Д. Рубан, С.Д. Викторов и др. // Доклады РАН. – 2010. – Т. 431. – № 6. – С. 818–821.
7. Булат, А.Ф. Фракталы в геомеханике / А.Ф. Булат, В.И. Дырда. – Киев: «Наукова книга», 2005. – 357 с.
8. Сулейманов, Б.А. Особенности фильтрации гетерогенных систем / Б.А. Сулейманов. – М.-Ижевск: Ин-т компьютерных исследований, 2006. – 354 с.
9. Малинников, В.А. Разработка метода обобщенного локально-глобального мультифрактального анализа изображений для исследования пространственной структуры природно-антропогенных систем / В.А. Малинников, Д.В. Учаев, Д.В. Учаев // Известия вузов. «Геодезия и аэрофотосъемка». – 2010. – № 4. – С. 64–68.
10. Федер, Е. Фракталы / Е. Федер. – М.: Мир, 1991. – 254 с.
11. Паламарчук, Т.А. Кластерно-иерархические структуры в массиве горных пород как одна из форм самоорганизации породного массива / Т.А. Паламарчук, С.И. Скипочка, Б.М. Усаченко и др. // Геотектоническая механика. – 2009. – № 83. – С. 91 – 104.
12. Moulu, J. C. A new model for three-phase relative permeability's based on a fractal representation of the porous media / J.C. Moulu, O. Vizika, F. Kalandjian // SPE Formation Evaluation. – 1997, August. – SPE 38891. – P. 147 – 158.
13. Верлань, А.Ф. Математическое моделирование аномальных диффузионных процессов / А.Ф. Верлань, С.А. Положаєнко, Н.Г. Сербов. – К.: Наука, 2011. – 416 с.
14. Верлань, А.Ф. Метод решения задачи параметрической идентификации процессов фильтрации аномальных жидкостей в пористых средах / А.Ф. Верлань, С.А. Положаєнко // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2010. – Вип. 57. – С. 67-72.
15. Азиз, Х. Математическое моделирование пластовых систем / Х. Азиз, Э. Сеттари. – М.-Ижевск: МКИ, 2008. – 406 с.

ФРАКТАЛЬНИЙ АНАЛІЗ РЕОЛОГІЇ БАГАТОКОМПОНЕНТНИХ ТА ГЕТЕРОГЕННИХ ПЛАСТОВИХ СИСТЕМ

С. А. Положаєнко, Мухіалдін Хасан Моха

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

Досліджено умову «гладкості» фронту поділу складових багатокомпонентних (гетерогенних) систем на основі аналізу «стрибка» насиченості в функції Баклея-Леверета. Показано, що «стрибок» насиченості відсутній, а фронт поділу просувається стало та зберігає «гладкість», якщо рухомість компоненти, яка витискає, не перевищує рухомість компоненти, яка витискається. Також показано, що порушення «гладкості» фронту поділу призводить до фрактально-неоднорідної структури процесу реології. Отримано числові значення фрактальної розмірності фронту поділу для реологічного процесу, який розвивається у реальних геологічних умовах.

Ключові слова: багатокомпонентна система, гетерогенна система, процес реології, фрактально-неоднорідна структура, фрактальний кластер, фрактальна розмірність

FRACTAL ANALYSIS OF REOLOGY OF MULTICOMPONENT AND HETEROGENEOUS STRATAL SYSTEMS

S. A. Polozhaenko, Muhialdin Hassan Moha

Odessa national polytechnic university,

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

The condition «of smoothness» of front of division of the making multicomponent (heterogeneous) systems is investigational on the basis of analysis «of jump» of saturation in the function of Bacley-Leverett. It is shown that «jump» of saturation is absent, and front of division moves up steadily and saves «a smoothness», if mobility of ousting component does not exceed mobility of ousted. It is also shown that over violation «of smoothness» of front of division brings to the fractal-heterogeneous structure of process of reology. The numeral values of fractal dimension of front of division are got for a reology process developing in the real geological terms. The mathematical model of the fractal-heterogeneous multicomponent system is offered in the class of variation inequalities.

Keywords: multicomponent system, heterogeneous system, process of reology, fractal-heterogeneous structure, fractal cluster, fractal dimension

МОДИФІКАЦІЯ СТІЙКОГО ДО ЗБУРНИХ ДІЙ СТЕГАНОПЕРЕТВОРЕННЯ ПРОСТОРОВОЇ ОБЛАСТІ ЗОБРАЖЕННЯ-КОНТЕЙНЕРА

О.В. Костирка

Черкаський інститут пожежної безпеки ім. Героїв Чорнобиля Національного університету цивільного захисту України,
вул. Онопрієнка, 8, Черкаси, 18034, Україна; e-mail: chaykaov@rambler.ru

В роботі запропоновано модифікацію стійкого до атак проти вбудованого повідомлення стеганографічного методу, розробленого автором раніше, який здійснює стеганоперетворення в просторовій області контейнера-зображення, але має обмеження області застосування завдяки можливості порушення надійності сприйняття зображення в результаті вбудови додаткової інформації. Результатом модифікації є усунення будь-яких обмежень на область застосування відповідного алгоритму шляхом забезпечення надійності сприйняття формованого стеганоповідомлення незалежно від специфіки зображення-контейнера. Стійкість алгоритму, що реалізує модифікований метод, до атак проти вбудованого повідомлення при цьому знижується незначно. Як збурні дії розглянуто: накладання на стеганоповідомлення різних шумів з різними параметрами, фільтрація, стиск стеганоповідомлення з втратами з різними коефіцієнтами якості (збереження в формати Jpeg, Jpeg2000). Наведені результати обчислювального експерименту.

Ключові слова: стеганографічний алгоритм, цифрове зображення, просторова область контейнера, надійність сприйняття стеганоповідомлення, стійкість до атак проти вбудованого повідомлення

Вступ

При розробці нових і вдосконаленні існуючих стеганографічних алгоритмів (СА), що використовуються при організації прихованого каналу зв'язку, гостро встають питання забезпечення ними різних вимог, серед яких одною з основних, але не вирішених до кінця залишається задача забезпечення стійкості алгоритму до різних збурних дій — атак проти вбудованого повідомлення [1,2]. До таких атак відносяться, зокрема, накладання різних шумів на стеганоповідомлення (СП), що є результатом вбудови додаткової інформації (ДІ) в контейнер, фільтрація, стиск СП із втратами та ін.

Протягом привалого часу вважалося, що для забезпечення стійкості СА кращою для вбудови ДІ є область перетворення контейнера, в якості якого далі розглядається цифрове зображення (ЦЗ), зокрема, частотна область [3,4]. Завдяки цьому розробки стійких стеганоалгоритмів у просторовій області (ПО) ЦЗ були нечисленними, безсистемними, не мали потрібного математичного фундаменту [5,6].

У результаті сучасних наукових досліджень було показано, що забезпечення стійкості СА не залежить прямо від того, у якій області контейнера — просторовій або перетворення відбувається вбудова ДІ [7,8]. При цьому просторова область ЦЗ має значні переваги перед областями перетворень для організації стеганоперетворення [9]. В [8,10,11] був розроблений стеганографічний метод і реалізуючий його поліноміальний СА, стійкість до атак проти вбудованого повідомлення якого перевищує стійкість сучасних аналогів. Однак недоліком методу і відповідного

алгоритму є можливість порушення надійності сприйняття формованого СП в тому випадку, коли ЦЗ-контейнер має значні по розмірі фонові області, що звужує область його застосування.

Мета статті і постановка досліджень

Метою роботи є модифікація розробленого в [8,10,11] стійкого стеганографічного методу, що здійснює стеганоперетворення в просторовій області контейнера, яка дозволить усунути будь-які обмеження на область застосування модифікованого методу шляхом забезпечення надійності сприйняття формованого їм стеганоповідомлення незалежно від специфіки зображення-контейнера, не знижуючи при цьому значимо його стійкість до атак проти вбудованого повідомлення.

Для досягнення поставленої мети в роботі потрібно вирішити наступні задачі:

1. Забезпечити зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ за рахунок зміни виду матриці збурення блоку контейнера при стеганоперетворенні;
2. Визначити розміри складових частин матриці збурення блоку контейнера при стеганоперетворенні таким чином, щоб вона забезпечувала найкраще співвідношення між кількісними показниками спотворення контейнера в результаті вбудови ДІ й стійкості відповідного алгоритму до збурних дій;
3. Провести порівняльний аналіз властивостей стеганоалгоритмів, що реалізують модифікований метод, і базового алгоритму.

Основна частина

Нехай F , $\bar{F}$ — $m \times m$ -матриці контейнера, СП відповідно, $p_1, p_2, \dots, p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$, - бінарна послідовність, яка є результатом кодування пересилаємої інформації, що розглядається як ДІ. Зауважимо, що хоча для кольорового ЦЗ його формальним представленням в різних схемах буде 3 або 4 двовимірні матриці, запропонована формалізація у вигляді одної матриці не обмежує спільність подальших міркувань, оскільки, по-перше, всі ці міркування можуть бути застосовані для кожної з матриць, по-друге, для збільшення ймовірності збереження прихованості стеганографічного каналу зв'язку при стеганоперетворенні кольорового зображення-контейнера часто використовується лише одна його кольорова складова.

Основним недоліком розробленого автором раніше стійкого стеганографічного методу SA_B [10], що використовується для організації прихованого каналу зв'язку, є обмеження області його застосовності: на фонових ділянках, при їх наявності в зображенні-контейнері, завдяки перепаду значень яскравості пікселів на границі блоків, що використовуються при стеганоперетворенні за допомогою SA_B , виникають артефакти. Звичайно такі області контейнера можна не задіювати в процесі вбудови ДІ, що дасть можливість уникнути порушення надійності сприйняття зображення-стеганоповідомлення, але приведе до зменшення пропускну здатності прихованого каналу зв'язку, що організується за допомогою даного стеганометода, що є вкрай небажаним.

В ході стеганоперетворення методом SA_B $m \times m$ -матриця F ЦЗ розбивається стандартним чином [12] на $l \times l$ -блоки B (в алгоритмічній реалізації SA_B $l=8$, що обґрунтовано в [10,11]). В один блок відбувається вбудова одного біта ДІ шляхом збільшення/зменшення всіх значень яскравості пікселів блоку на одне й те саме значення Δb (в алгоритмічній реалізації SA_B $\Delta b=9$ [10]), що може бути представлене

в матричному виді наступним чином: $\bar{B} = B \pm \Delta B$, де $\bar{B}$ - відповідний блок СП, а ΔB - $l \times l$ -матриця, всі елементи якої дорівнюють Δb . В результаті можливий значний перепад яскравості на спільній границі блоків, що знаходяться поряд і використовуються в процесі стеганоперетворення. Це відбувається тоді, коли в них вбудовуються різні за значенням біти ДІ (див. рис.1(а)). Стрибок функції яскравості пікселів, що відбувається, за значенням порівнянний з $2\Delta b$, і викликає появу артефактів на ЦЗ-стеганоповідомленні, що формується SA_B . Щоб запобігти можливості виникнення таких артефактів, треба зменшити цей перепад значень функції яскравості.

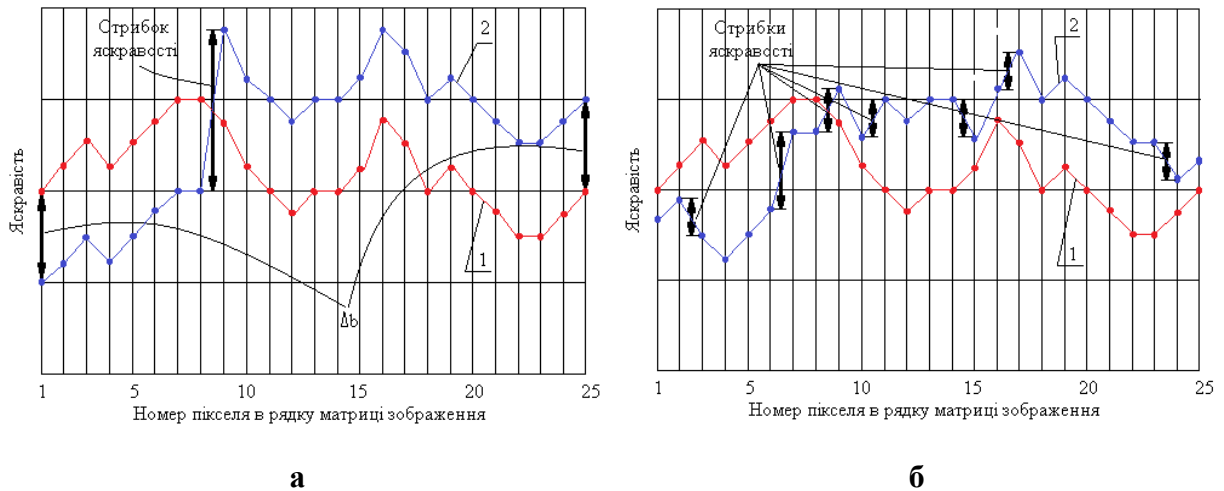


Рис. 1. Графіки залежності значення яскравості пікселя від його номера в рядку ЦЗ: 1 – для ЦЗ-контейнера; 2 – для СП; а – СП, яке сформоване базовим стеганометодом SA_B ; б – СП, яке сформоване з використанням ΔB^M

Для цього змінимо вид $l \times l$ -матриці ΔB наступним чином. Розіб'ємо ΔB на 2 ділянки, як пропонує рис.2. Модифіковану матрицю будемо позначати ΔB^M . При цьому елементи внутрішньої частини матриці збурення блоку контейнера при стеганоперетворенні, що позначимо ΔB_h , будуть залишатися рівними Δb , а елементи зовнішньої області будуть визначатися як $\Delta b/3$ (чи $\lfloor \Delta b/3 \rfloor$ в випадку, коли Δb не є кратним трьом). Таке рішення приймається в силу наступних обставин. При запропонованих змінах матриці ΔB хоча стрибків функції яскравості буде більше, але всі вони не будуть перевищувати Δb (рис.1(б)). Це буде сприяти зменшенню спотворення ЦЗ в процесі стеганоперетворення.

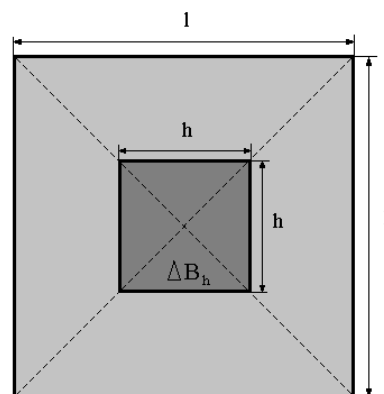


Рис. 2. Розбиття $l \times l$ -матриці збурення блоку ΔB при стеганоперетворенні на 2 ділянки

Основні кроки пропонуємої модифікації стеганографічного методу SA_B , яка далі позначається $SA_B^{(M)}$, виглядають наступним чином.

Вбудова ДІ.

1. Матрицю F ЦЗ-контейнера розбити стандартним чином на $l \times l$ – блоки.
2. Побудувати матрицю ΔB^M .
3. Нехай B — черговий блок контейнеру, що використовується для стеганоперетворення, а p_i — черговий біт ДІ, $\bar{B}$ — відповідний блок СП.

$$\begin{array}{ll} \text{Якщо} & p_i = 1 \\ \text{то} & \bar{B} = B + \Delta B^M \\ \text{інакше} & \bar{B} = B - \Delta B^M. \end{array}$$

Результат – матриця $\bar{F}$ стеганоповідомлення.

Декодування ДІ

1. Матриці F контейнера і $\bar{F}$ можливо зміненого в процесі пересилання стеганоповідомлення розбиваються стандартним чином на непересічні $l \times l$ – блоки.

2. Нехай $\bar{B}$ — черговий блок СП, з якого декодується біт $\bar{p}_i$ ДІ, а B – відповідний йому блок контейнера.

- 2.1. Визначити: $\Delta \bar{B} = \bar{B} - B$.
- 2.2. Визначити кількості додатних k_p і від’ємних k_n елементів в $\Delta \bar{B}$.

$$\begin{array}{ll} \text{Якщо} & k_p > k_n, \\ \text{то} & \bar{p}_i = 1, \\ \text{інакше} & \bar{p}_i = 0. \end{array}$$

Конкретна алгоритмічна реалізація методу $SA_B^{(M)}$ буде визначатися конкретними значеннями параметрів l, h .

Для практичного підтвердження зменшення спотворення ЦЗ в процесі стеганоперетворення $SA_B^{(M)}$ в порівнянні з SA_B був проведений обчислювальний експеримент, у якому були задіяні 400 ЦЗ з бази NRCS [13], що є традиційною для тестування алгоритмів, які працюють з ЦЗ. Далі ця множина зображень називається тестовою множиною (ТМ). Оскільки для алгоритмічної реалізації SA_B в [10,11] обґрунтована доцільність значення $l=8$, далі розглядається саме це значення для розміру блоків, що використовуються при вбудові ДІ.

В ході експерименту в ЦЗ-контейнери із ТМ вбудовувалася ДІ, що представляла із себе бінарну послідовність, методом $SA_B^{(M)}$ з різними значеннями $h \in \{2,4,6,8\}$ (відповідні алгоритми далі позначаються $SA_B^{(M,h)}$). Після цього отримане стеганоповідомлення зберігалось у форматі без втрат. Кількісна оцінка спотворення контейнера за рахунок стеганоперетворення проводилася за допомогою різницевого показника PSNR – пікового відношення «сигнал-шум»:

$$PSNR = 10 \cdot \lg \left(255^2 / \left(\frac{1}{m^2} \sum_{i,j} (f_{ij} - \bar{f}_{ij})^2 \right) \right).$$

Результати цієї частини експерименту наведені на рис.3 (при цьому $h=8$ відповідає алгоритмічній реалізації базового методу SA_B). Необхідно зазначити, що й

для SA_B середнє значення $PSNR > 40dB$, що розглядається в літературних джерелах як значення, яке характеризує прийнятну якість ЦЗ при стеганоперетворенні [3], хоча порушення надійності сприйняття стеганоповідомлення, як було зазначено вище, можливо, що в черговий раз підтверджує недосконалість існуючих кількісних різницевих показників у випадку оцінки візуального сприйняття зміненого ЦЗ.

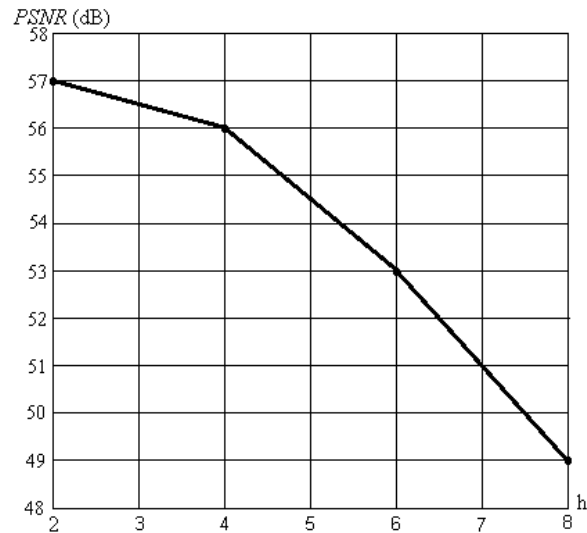


Рис. 3. Залежність значення PSNR, що відображає спотворення контейнера в результаті стеганоперетворення за допомогою $SA_B^{(M,h)}$, від величини h

Виходячи з отриманих результатів для забезпечення візуальної стійкості СП найкращим з погляду значення PSNR після стеганоперетворення є $h=2$, однак експертна оцінка, отримана шляхом суб'єктивного ранжирування, є задовільною вже для $h=6$, в тому числі, для абсолютної більшості тих ЦЗ-контейнерів, для яких для SA_B спостерігалось виникнення артефактів (рис. 4). Однак, з урахуванням мети роботи, вибір h повинен забезпечити відсутність артефактів на СП при незначному зменшенні стійкості модифікованого алгоритму в порівнянні з базовим, яке очевидно відбудеться. Рішенню цієї задачі була присвячена друга частина обчислювального експерименту, у ході якої отримані раніше й збережені без втрат (у відсутності будь-яких збурних дій) стеганоповідомлення піддавалися різним атакам проти вбудованого повідомлення, після чого відбувалося декодування ДІ. Кількісна оцінка ефективності декодування визначалася коефіцієнтом кореляції NC для ДІ [10]:

$$NC = \left(\sum_{i=1}^t p_i' \times \bar{p}_i' \right) / t,$$

де $p_i' = 1, \bar{p}_i' = 1$, якщо $p_i = 1, \bar{p}_i = 1$, і $p_i' = -1, \bar{p}_i' = -1$, якщо $p_i = 0, \bar{p}_i = 0$.

Як атаки використовувалися: накладання різних шумів, фільтрація, збереження СП із втратами (формати Jpeg, Jpeg2000). Результати експерименту наведені в табл.1.

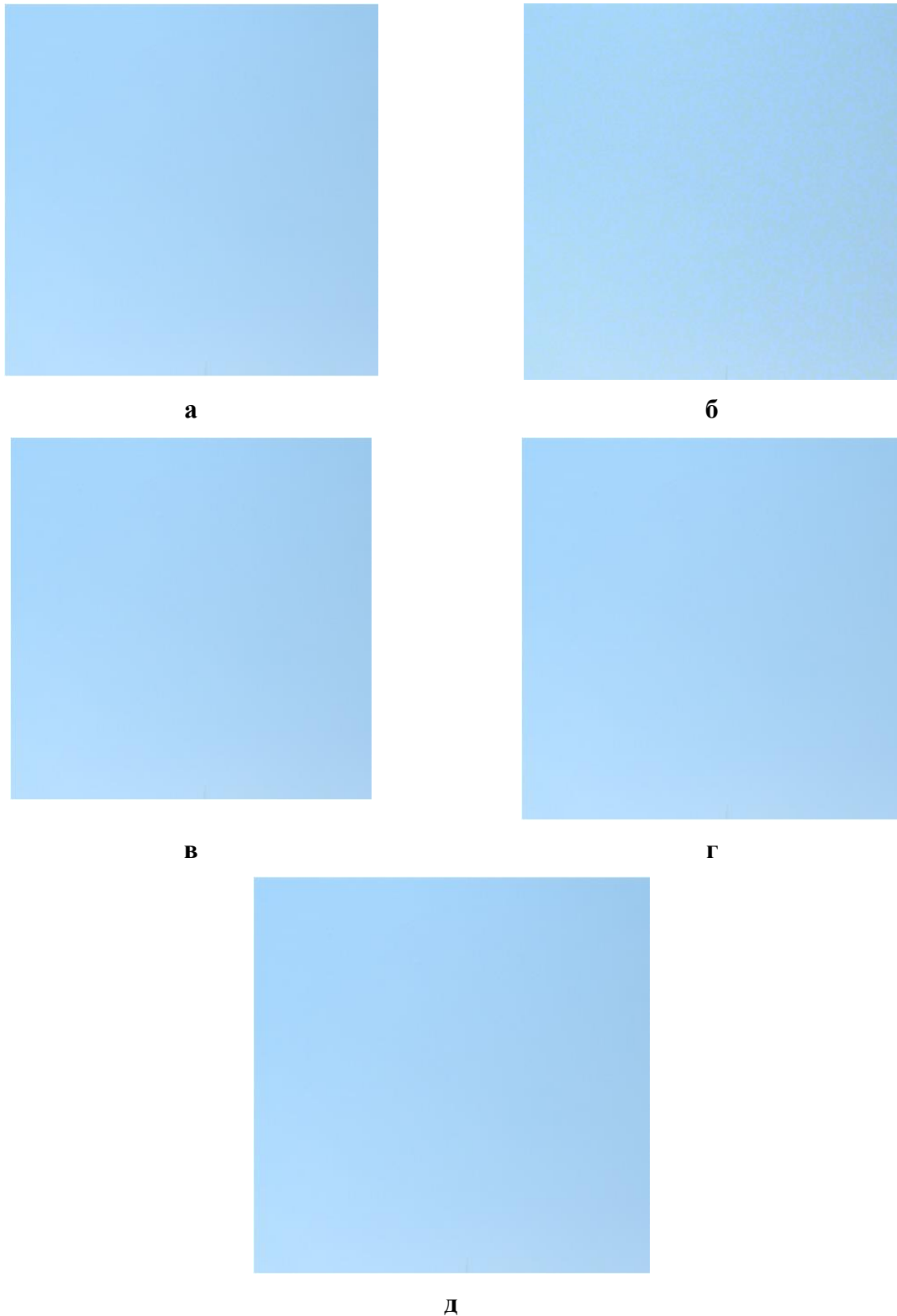


Рис. 4. Результати стеганоперетворення зображення за допомогою SA_B та стеганоалгоритмами, що реалізують $SA_B^{(M)}$: а – контейнер; б – СП, сформоване SA_B ; в – СП, сформоване $SA_B^{(M,6)}$; г – СП, сформоване $SA_B^{(M,4)}$; д – СП, сформоване $SA_B^{(M,2)}$

Таблиця 1.

Кількісні оцінки стійкості до атак проти вбудованого повідомлення алгоритмічних реалізацій методів SA_B та $SA_B^{(M)}$

Збурні дії та їх параметри		Значення NC			
		SA_B	$SA_B^{(6)}$	$SA_B^{(4)}$	$SA_B^{(2)}$
Гауссівський шум з нульовим маточікуванням	$D = 0.0005$	0.994	0.994	0.920	0.834
	$D = 0.001$	0.993	0.992	0.891	0.811
	$D = 0.005$	0.988	0.979	0.874	0.791
	$D = 0.01$	0.962	0.951	0.823	0.715
	$D = 0.1$	0.524	0.508	0.505	0.491
Мультиплікативний шум	$D = 0.0001$	0.995	0.995	0.941	0.854
	$D = 0.001$	0.993	0.993	0.903	0.802
	$D = 0.01$	0.977	0.967	0.873	0.779
	$D = 0.08$	0.822	0.810	0.806	0.721
	$D = 0.5$	0.548	0.533	0.505	0.496
Пуассонівський шум		0.9977	0.9953	0.9211	0.8454
Усереднюючий фільтр розміру $p \times p$	$p=3$	0.994	0.989	0.922	0.834
	$p=5$	0.962	0.943	0.881	0.794
	$p=7$	0.881	0.839	0.709	0.678
Гауссов фільтр розміру $p \times p$ ($\sigma = 0.5$)	$p=3$	0.997	0.982	0.912	0.833
	$p=5$	0.997	0.982	0.912	0.833
	$p=7$	0.997	0.983	0.912	0.833
Медіанний фільтр 3×3		0.997	0.985	0.913	0.836
Збереження СП в форматі Jpeg з коефіцієнтом якості QF	QF=40	0.969	0.920	0.808	0.703
	QF=60	0.987	0.966	0.845	0.737
	QF=70	0.988	0.974	0.890	0.765
	QF=80	0.989	0.980	0.911	0.834
	QF=90	0.991	0.990	0.951	0.884
Збереження СП в форматі Jpeg2000 з коефіцієнтом якості QF	QF=40	0.782	0.739	0.648	0.549
	QF=60	0.947	0.934	0.723	0.623
	QF=70	0.980	0.963	0.867	0.711
	QF=80	0.990	0.972	0.912	0.799
	QF=90	0.992	0.989	0.954	0.888

Виходячи з результатів порівняльного аналізу стійкості алгоритму, що реалізує базовий стеганометод, і його модифікацій, що визначаються значеннями параметра h , і беручи до уваги оцінки спотворень контейнера в результаті стеганоперетворення, можна зробити висновок, що співвідношення між NC и $PSNR$, яке найбільш підходить, досягається для $h=6$, яке й рекомендується використовувати для розробленої модифікації $SA_B^{(M)}$ методу SA_B . Рекомендоване значення параметра знижує стійкість алгоритму до атак проти вбудованого повідомлення незначно - не більше, ніж на 5.5% (див. табл.1).

Висновки

В роботі запропонована модифікація стійкого до атак проти вбудованого повідомлення стеганометода, що здійснює вбудову ДІ в просторовій області зображення-контейнера, яка дозволяє усунути будь-які обмеження на область

застосування, забезпечуючи надійність сприйняття відповідного стеганоповідомлення незалежно від специфіки зображення-контейнера, що не було притаманне базовому стеганометоду і відповідному алгоритму, область застосовності якого обмежувалася зображеннями, що не мали значних за розміром фонових ділянок. Результат модифікації досягається за рахунок зменшення стрибка функції яскравості пікселів на границі блоків матриці ЦЗ-контейнера при вбудові ДІ шляхом зміни виду матриці збурення блоку контейнера при стеганоперетворенні.

Алгоритмічна реалізація побудованої модифікації не знижує значно стійкість модифікованого алгоритму, у порівнянні з базовим, при рекомендованому значенні параметра $h=6$, який визначає вид матриці збурення блоку контейнера при стеганоперетворенні. Максимальне зниження стійкості стеганоалгоритму, яка кількісно оцінювалася коефіцієнтом кореляції для переданої інформації, досягало 5.5%.

Обчислювальна складність запропонованої алгоритмічної реалізації визначається кількістю блоків в $m \times m$ – матриці ЦЗ і складає $O(m^2)$ операцій.

Література

1. Qin, C. A Novel Digital Watermarking Algorithm in Contourlet Domain / C. Qin, X. Wen // Journal of Information & Computational Science. — 2014. — 11(2). — P. 519 – 526;
2. Fang, H. Robust Watermarking Scheme for Multispectral Images Using Discrete Wavelet Transform and Tucker Decomposition / H. Fang, Q. Zhou, K. Li // Journal of Computers. — 2013. — Vol.8. — No.11. — P. 2844 – 2850.
3. Lin, W.H. A blind watermarking method using maximum wavelet coefficient quantization / W.H. Lin, Y.R. Wang, S.J. Horng *et al.* // Expert Systems with Applications. — 2009. — No.36. — P. 11509 – 11516.
4. Doncel, V.R. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics / V.R. Doncel, N. Nikolaidis, I. Pitas // IEEE Transactions on Visualization and Computer Graphics. — 2007. — 13(5). — P. 851 – 863.
5. Nasir, I. A New Robust Watermarking Scheme for Color Image in Spatial Domain / I. Nasir, Y. Weng, J. Jiang // In Proceedings of the 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System (SITIS'07), 16–18 Dec. 2007, Shanghai. — 2007. — P. 942 – 947.
6. Viswanatham, V.M. Novel Technique for Embedding Data in Spatial Domain / V.M. Viswanatham, J. Manikonda // International Journal on Computer Science and Engineering. — 2010. — Vol.2. — P. 233 – 236.
7. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А. Кобозева // Искусственный интеллект. — 2007. — № 4. — С. 531 – 538.
8. Кобозева, А.А. Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. — 2013. — №3(11). — С. 29 – 35.
9. Костырка, О.В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О.В. Костырка // Інформатика та математичні методи в моделюванні. — 2013. — Т.3. — №3. — С. 275 – 282.
10. Костырка, О.В. Стеганографічний алгоритм, стійкий до накладання шуму / О.В. Костырка // Безпека інформації. — 2014. — Т.20. — №1. — С. 71 – 75.
11. Кобозева, А.А. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения Проблемы региональной энергетики. / А.А. Кобозева, О.В. Костырка, Е.Ю. Лебедева // Электронный журнал Академии наук республики Молдова. — 2014. — №1(24). — С. 1 – 12.
12. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
13. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата звернення: 26.07.2012).

МОДИФИКАЦИЯ УСТОЙЧИВОГО К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ СТЕГАНОПРЕОБРАЗОВАНИЯ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ- КОНТЕЙНЕРА

А.В Костырка

Черкасский институт пожарной безопасности им. Героев Чернобыля Национального университета
гражданской защиты Украины,
ул. Оноприенко, 8, Черкассы, 18034, Украина; e-mail: chaykaov@rambler.ru

В работе предложена модификация устойчивого к атакам против встроенного сообщения стеганографического метода, разработанного автором ранее, осуществляющего стеганопреобразование в пространственной области контейнера-изображения, имеющего ограничение области применения в силу возможности нарушения надежности восприятия изображения в результате внедрения дополнительной информации. Результатом модификации является устранение любых ограничений на область применения соответствующего алгоритма путем обеспечения надежности восприятия формируемого стеганосообщения независимо от специфики изображения-контейнера. Устойчивость алгоритма, который реализует модифицированный метод, к атакам против встроенного сообщения при этом снижается незначительно. В качестве возмущающих воздействий рассмотрены: наложение на стеганосообщение различных шумов с различными параметрами, фильтрация, сжатие стеганосообщения с потерями с различными коэффициентами качества (сохранение в форматы Jpeg, Jpeg2000). Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганографический алгоритм, цифровое изображение, пространственная область контейнера, надежность восприятия стеганосообщения, устойчивость к атакам против встроенного сообщения

MODIFICATION OF RESISTANCE TO DISTURBANCE QUILTED TRANSFORMATION OF SPATIAL IMAGE CONTAINER

O.V Kostyrka

Cherkassy Institute of Fire Safety named. Heroes of Chernobyl National University of Civil Defense of Ukraine,
8, Onoprienko st., Cherkasy, 18034, Ukraine; e-mail: chaykaov@rambler.ru

The paper presents a modification resistant to attacks against embedded message steganographic method developed earlier by the author, which provides a spatial region steganoperetvorennaya container image, but is limited to applications with the ability to breach the reliability of the image due to embed additional information. The result of the modification is to eliminate any restriction on the scope of the relevant algorithm by ensuring the reliability of perception formed stehanopovidomlennaya regardless of the specific image container. Resistance algorithm that implements a modified method to attacks against embedded message in this case is reduced slightly. As discussed zburni steps: overlay stehanopovidomlennaya different noises with different parameters, filtering, compression lossy stehanopovidomlennaya with different coefficients of quality (saving in format Jpeg, Jpeg2000). The results of computational experiments.

Keywords: steganography algorithm, digital images, spatial region container perception stehanopovidomlennaya reliability, resistance to attacks against embedded message

АНАЛІЗ ЯКОСТІ ОЦІНЮВАННЯ СТУДЕНТІВ В СИСТЕМАХ КОМП'ЮТЕРИЗОВАНОЇ ПІДГОТОВКИ ЗА ДОПОМОГОЮ СТАТИСТИЧНИХ МЕТОДІВ

Т.І. Трояновська, М.А. Котолуп

Вінницький національний технічний університет,
Хмельницьке шосе, 95, Вінниця, 210021, Україна; e-mail: trtet@mail.ru
Морехідний коледж технічного флоту,
вул. Маразліївська, 42, Одеса, Україна; e-mail: spine 99@mail.ru

Роботу присвячено аналізу якості оцінювання студентів в системах комп'ютеризованої підготовки (СКП) за допомогою статистичних методів. Пропонується використовувати непряме оцінювання (НО) в СКП, яке надає можливість проставляти більш адекватні дійсному рівню студента оцінки. Таким чином, нормальний закон розподілу (НЗР) при оцінюванні в академічній формі буде мати більше відхилення від критичних статистик НЗР, ніж НЗР при оцінюванні студента за допомогою запропонованої СКП.

Ключові слова: система комп'ютеризованої підготовки, непряме оцінювання, нормальний закон розподілу, статистичні методи

Вступ

Існують різні методології оцінювання знань студента, побудовані на якісному аналізі його теоретичних знань та практичних робіт. Всі вони зводяться до певної шкали оцінок. В Україні на теперішній час існує дві загальноприйняті шкали: п'ятибальна та дванадцятибальна. Обидві шкали побудовані на узагальненнях, згідно яких якісні показники роботи студента ранжуються по певній сітці ознак, що відносяться до відповідної оцінки. Ранжувальна сітка потрібна тому, що оцінка завжди цілочисельна і не відображає достатньо реального рівня знань студента, а тільки скориговану відповідно деякого, наперед спрогнозованого, середнього рівня.

Для того, щоб підвищити точність оцінки у якості ранжувальної сітки може бути використана допоміжна шкала, достатньо деталізована, щоб враховувати всі варіанти проміжних випадків при оцінюванні знань. Однак таку допоміжну шкалу можна організувати тільки у випадку статичних засобів оцінювання – наприклад, затвердженого переліку відповідей на кожен варіант, або т. зв. «жорсткі» тести. Тому у більшості випадків використовуються або табличні способи (перевірка наявності в практичній роботі тих чи інших ознак), або приблизні методи оцінювання безпосередньо викладачем. Обидва методи є суб'єктивними.

Актуальність

Експоненціальне зростання обсягів навчального контенту, який необхідно засвоїти, у поєднанні з його постійним старінням породжує необхідність впровадження нових інформаційних технологій (ІТ) у галузь систем комп'ютеризованої підготовки (СКП). Широке впровадження ІТ у навчальний процес та наявність широкого кола

розробників вимагає дотримання міжнародних стандартів для успішного розвитку цієї діяльності.

У своїй суті процес навчання є інформаційним процесом, який полягає в передачі знань, умінь і навичок від об'єкта до суб'єкта підготовки та охоплює процеси формування, зберігання, обробки та передачі інформації, а також контроль засвоєння навчального контенту як невід'ємної частини навчального процесу.

СКП – це комплекс програмно-технічних засобів, моделей, методів та інформаційних ресурсів, що забезпечують доставку контенту суб'єктам підготовки засобами сучасних мережових та інформаційних технологій, а також здійснюють перевірку отриманих знань суб'єкта підготовки.

Мета статті і постановка досліджень

Метою статті є аналіз якості оцінювання студентів у системах комп'ютеризованої підготовки за допомогою статистичних методів.

В роботі поставлено та вирішено наступні *задачі*:

1. Виконати аналіз даних оцінювання студентів за допомогою традиційного підходу та у середовищі СКП;
2. Перевірити гіпотезу, що нормальний закон розподілу (НЗР) при оцінюванні в академічній формі буде мати більше відхилення від критичних статистик НЗР, ніж НЗР при оцінюванні студента за допомогою запропонованої СКП.

Система вищої освіти України впевнено крокує по шляху впровадження Європейської системи трансферу та акумуляції кредитів (залікових балів), ECTS. На рис.1 можна бачити симетричність та одномодальність розподілу успішних студентів по відсотковому рейтингу в межах статистичних критеріїв шкали ECTS. Добре видно те, що медіаною, і одночасно модою розподілу, в цій шкалі успішності є оцінка “С – good”, яка відповідає українській оцінці «добре».

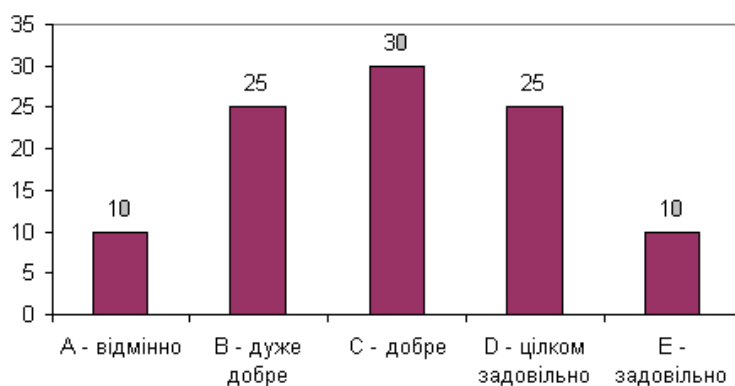


Рис. 1. Розподіл успішних студентів по відсотковому рейтингу в межах статистичних критеріїв шкали ECTS

Таким чином, стверджується, що система оцінювання знань студентів є ефективною при відповідності результатів оцінювання НЗР.

У запропонованій СКП крім прямого, використовується непряме оцінювання, що побудовано на шкалі, яка складається з дійсних значень на протизагу дискретній шкалі. Це дозволить оцінювати студентів з більш високою точністю.

При використанні дискретних шкал оцінювання існує необхідність допуску при оцінюванні знань студента. Критерії кожної оцінки в таких шкалах відповідають лише усередненому рівню знань (еквівалентному точці, яка знаходиться в центрі інтервалу на числовій вісі, що відповідає даній оцінці). Можна припустити, що при оцінюванні студента викладачем виникає залежність від останнього, яка полягає в тому, що

викладач суб'єктивно вирішує, до околу якої саме оцінки відноситься результат даного студента. Така суб'єктивність виникає, коли у випадку результату, недостатнього для потрапляння в інтервал кращої оцінки, але перевищуючого критерій нижчої оцінки, йому може бути виставлена фактично нижча оцінка. Або навпаки, при результаті, який перевищує критерій нижчої оцінки, і недостатній для вищої, йому може бути виставлена вища на 1 бал. Прийняття рішення в цих випадках цілком залежить від того, як саме розглядає відповідність критеріями певної оцінки отриманий студентом результат конкретно узятий викладач.

Запропонована СКП покликана підвищити якість оцінювання студентів та містить механізми для більш точного оцінювання рівня їх знань [1]. Оскільки в даному випадку контакт студента із викладачем обмежений або відсутній взагалі, схеми оцінювання не повинні залежати від прийняття рішень конкретним викладачем, або мати мінімальну таку залежність. Для цього запропонована шкала оцінювання, заснована на дійсних числах, в якій результат студента на основі даних прямого і непрямого оцінювання [2] протягом періоду навчання апроксимується не на множину узагальнених дискретних оцінок, а на неперервну числову вісь.

Виходячи із того, що така шкала надає можливість проставляти більш адекватні дійсному рівню студента оцінки, висунемо гіпотезу, що НЗР при оцінюванні в академічній формі буде мати більше відхилення від критичних статистик НЗР, ніж НЗР при оцінюванні студента за допомогою запропонованої СКП [3].

Для перевірки гіпотези використаємо статистичний аналіз. Виконаємо розрахунки для оцінювання студентів за допомогою СКП та засобами академічного навчання, порівняймо їх та доведемо, або заперечимо висунуту гіпотезу.

Основна частина

Як генеральною сукупністю для першого етапу статистичних розрахунків скористаємось масивом реальних даних, які були зібрані в середовищі СКП під час контролю залишкових знань студентів з дисципліни «Дискретна математика» 3 курсу в 2014 року на кафедрі Обчислювальної техніки ВНТУ. Було проведено тестування 100 студентів з трьох груп. Оберемо для 100 варіантів число інтервалів $N=10$ [4]. В областях максимальної концентрації результатів спостережень слід вибрати більш вузькі інтервали, які визначаються за формулою:

$$\Delta x = (X_{\max} - X_{\min}) / (N - 1), N - 1 = 9. \quad (1)$$

Для оцінювання студентів за допомогою СКП та традиційного оцінювання студентів співпали: $X_{\max}=12$, $X_{\min}=3$. Інтервал: $\Delta x=1$. Визначимо межі інтервального ряду: ліву – 2,5, праву – 12,5. Побудуємо гістограми частот розподілу.

Гістограми частот розподілу наведена на рис.2.

Для СКП обчислимо умовні моменти першого та другого порядків: $M_1 = -0,45$; $M_2 = 4,59$. Обчислимо вибічкові середню $\bar{X} = 4,39$ та дисперсію $S^2 = 2,09$. Для академічного підходу обчислимо умовні моменти першого та другого порядків: $M_1 = 0,98$; $M_2 = 4$. Обчислимо вибічкові середню $\bar{X} = 7,98$ та дисперсію $S^2 = 3,04$.

Для побудови теоретичної кривої розподілу обчислюють теоретичні (вирівнюючі) частоти. Округлені значення теоретичних частот нанесемо в масштабі на гістограму (рис.2) та з'єднаємо плавною кривою (рис.3).

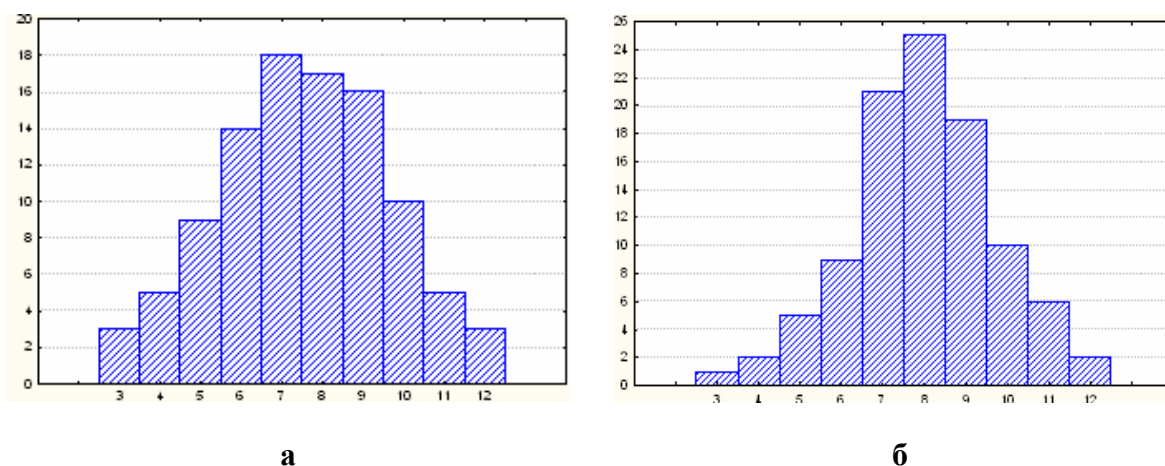


Рис. 2. Гістограма частот розподілу: а - оцінювання за допомогою СКП; б - традиційне оцінювання студентів

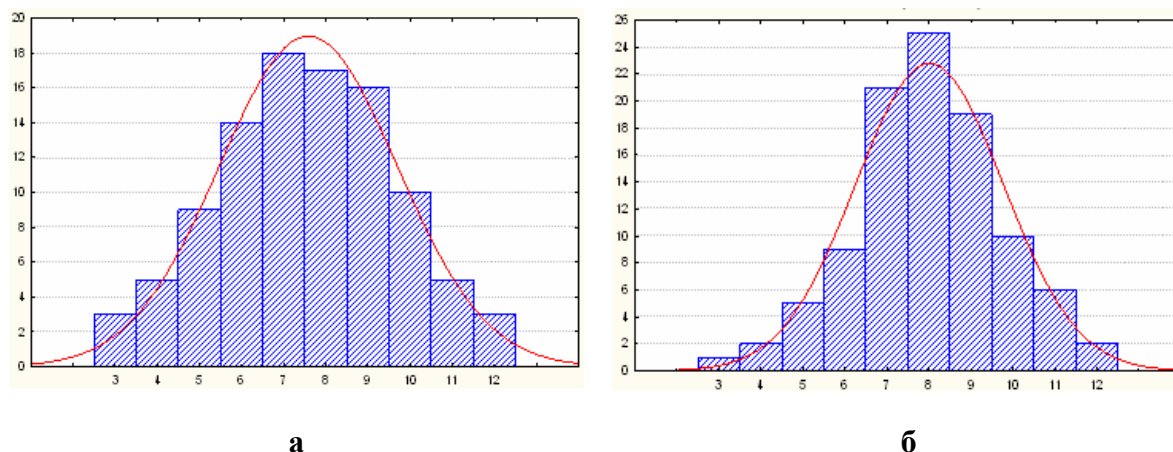


Рис. 3. Теоретичні криві розподілу: а - оцінювання за допомогою СКП; б - традиційне оцінювання студентів

Перевірка правдоподібності статистичної гіпотези

При дослідженні оцінювання студентів припустимо, що значення параметрів дослідження мають нормальний закон розподілу. Це гіпотеза H_0 . Альтернативну гіпотезу позначимо H_1 . Для перевірки гіпотез скористаємось критерієм Пірсона.

Задамо рівень значущості $\alpha = 0,05$; $p = 1 - \alpha = 0,95$. Визначимо число ступенів вільності $f = K - l$, де l - кількість накладених зв'язків (за перший параметр взята вибірка середня арифметична $\bar{X}$, за другий – вибірка дисперсія S^2 та сума емпіричних частот об'єму вибірки $\sum_{i=1}^N m_i = n$). Тоді $l = 3$, число ступенів вільності $f = 6 - 3 = 3$ (СКП) та $f = 5 - 3 = 2$ (традиційне навчання).

Для даних, отриманих за допомогою СКП. За рівнем значущості $\alpha = 0,05$ і числом ступенів вільності $f = 3$ з таблиці додатків знаходимо критичне значення $\chi^2_{\text{крит СКП}} = 7,8$. Порівнюючи $\chi^2_{\text{АСДН}}$ з $\chi^2_{\text{крит СКП}}$, маємо $0,27 < 7,8$, тобто, спостережувані значення критерію згоди менше критичного значення, що відповідає рівню

значущості $\alpha = 0,05$ ($p = 0,95$). Таким чином, відносно нульової гіпотези: дані оцінювання студентів за допомогою СКП, відповідають нормальному закону розподілу із значенням $\chi^2 = 0,27$.

Для даних, отриманих за допомогою академічної форми навчання. Порівнюючи $\chi^2_{Трад.Навч}$ з $\chi^2_{критТрад.Навч}$, маємо $1,26 < 6$, тобто, спостережуване значення критерію згоди менше його критичного значення, і не відповідає рівню значущості $\alpha = 0,05$, ($p = 0,95$).

Висновки

У даній роботі виконано аналіз даних оцінювання студентів за допомогою традиційного підходу (при академічному навчанні, коли студент знаходиться у тісному контакті із викладачем) та у середовищі СКП (коли контакт студента та викладача є віддаленими та часто опосередкованим). За допомогою поставленого експерименту та аналізу його даних статистичними методами виявлено, що значення $\chi^2_{критСКП}$ та $\chi^2_{Трад.Навч}$ лежать в області допустимих значень, немає підстав відкидати нульову гіпотезу. Тобто, розходження емпіричних та теоретичних частот незначне. Відповідно, дані спостережень відповідають гіпотезі про нормальний закон розподілу генеральної сукупності. Таким чином, висунута гіпотеза підтвердилась, що свідчить про ефективність оцінювання студентів в СКП.

Список літератури

1. Гороховський, О.І. Автоматизація роботи викладача дистанційної форми навчання за допомогою непрямих оцінок / О.І. Гороховський, Т.І. Трояновська, Д.В. Кисюк // Міжнародна науково-практична конференція, 14-16 травня: «Наукові дослідження – теорія та експеримент 2007». – 2007. – С. 127-131.
2. Трояновська, Т.І. Метод обробки даних дослідження індивідуальних характеристик суб'єкта СКП спеціалістів / Т.І. Трояновська // Вісник ВПШ. – 2013. – № 4. – С. 140–146.
3. Трояновская, Т.И. Формализация математических моделей системы компьютеризированной подготовки специалистов / Т.И. Трояновская // Научно-теоретический и практический журнал «Оралдыңғылымжаршысы»– Уральск : «Уралнаучкнига». – 2013. – № 18. – С. 28–40.
4. Кондратенко, Н.Р. Дослідження особливостей сприйняття студентами дистанційного курсу навчання на базі кластерного аналізу / Н.Р. Кондратенко, Т.І. Трояновська, Ю.Я. Слободянюк // Вісник Хмельницького національного університету. – 2009. – № 4. – С. 249–253.

**АНАЛИЗ КАЧЕСТВА ОЦЕНИВАНИЯ СТУДЕНТОВ В СИСТЕМАХ
КОМПЬЮТЕРИЗИРОВАННОЙ ПОДГОТОВКИ С ПОМОЩЬЮ СТАТИСТИЧЕСКИХ
МЕТОДОВ**

Т.І. Трояновская, М.А. Котолуп

Винницкий национальный технический университет,
Хмельницкое шоссе, 95, Винница, 210021, Украина; e-mail: trtet@mail.ru
Мореходный колледж технического флота,
Маразлиевская, 42, Одесса, Украина; e-mail: spine 99@mail.ru

Работа посвящена анализу качества оценивания студентов систем компьютеризированной подготовки (СКП) с помощью статистических методов. Предлагается использовать не прямое оценивание в СКП, которое предоставляет возможность проставлять более адекватные действительному уровню студента оценки. Таким образом, нормальный закон распределения (НЗР) при оценивании в академической форме будет иметь большее отклонение от критических статистик НЗР, чем НЗР при оценивании студента с помощью предложенной СКП.

Ключевые слова: система компьютеризированной подготовки (СКП), не прямое оценивание, нормальный закон распределения, статистические методы

**ANALYSIS OF QUALITY OF EVALUATION OF STUDENTS IN SYSTEMS OF THE
COMPUTERIZED PREPARATION BY MEANS OF STATISTICAL METHODS**

T.I. Trojanovs'ka, M.A. Kotolup

Vinnitsa national technical university,
Khmelnitsky highway, 95, Vinnitsa, 210021, Ukraine; e-mail: trtet@mail.ru
Navigated college of technical fleet,
Marazliev str., 42, Odessa, Ukraine; e-mail: spine 99@mail.ru

This work is devoted to quality evaluation analysis in computerized training system (CTS) by statistical methods. The indirect evaluation using in CTS is suggested, which gives possibility of more adequate student estimation. Thus, the normal law of distributing (NLD) in an academic form will have greater deviation from critical statistician NLD, than NLD at the student evaluation by offered CTS.

Keywords: computerized training system (CTS), indirect evaluation, normal law of distributing, statistical methods

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 6, номер 1, 2016. Одеса – 100 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 6, номер 1, 2016. Одесса – 100 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 6, No. 1, 2016. Odesa – 100 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 №3 від 08.12.2015)

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, 2016