УДК 621.396.6

МЕТОД ДИНАМІЧНИХ ХАРАКТЕРИСТИК В ЗАДАЧІ АВТЕНТИФІКАЦІЇ. ФРАКТАЛЬНІ СТРУКТУРИ В БІОМЕТРИЦІ

В.М. РИФА

Досліджуються рухи курсору під керуванням суб'єкта. Експериментально показано існування атракторів, які мають фрактальну структуру, індивідуальних для кожного суб'єкта оператора ПК.

ВСТУП

Кожного ранку, коли службовець входить до офісу і показує свою перепустку охороннику, вирішується задача автентифікації службовця охоронником через деякий документ, що називається перепусткою.

З доступом до електронних інформаційних ресурсів все дещо складніше. З новин преси та інших джерел часто дізнаємось про те, що затриманий та переданий до суду дехто X1, котрий «зламав» сервер X2 і спричинив таким чином компанії X3 збитки на суму X4. Яка користь компанії X3 від того, що цей X1 затриманий та просидить за гратами X5 років? Інформація «сплила» разом з грошима. І, як правило, у того хакера X1 за душею нема нічого, окрім комп'ютера. А це означає, що відшкодувати збитки нема жодної можливості. Ті ж панове, котрі скористалися з одержаної інформації і частіше всього були ініціаторами «зламування», на жаль, нікому не відомі. Саме тому ніхто не зможе дати гарантії того, що ізоляція десятків чи сотень X1 від суспільства позбавить його від хакінгу як явища. Одним із шляхів подолання таких негативних явищ є розробка та впровадження ефективних систем автентифікації.

Задача автентифікації полягає у підтвердженні даних (ім'я, пароль тощо), які вводить користувач комп'ютера, щоби отримати дозвіл на роботу з операційною системою. Простіше кажучи, задача автентифікації — це задача ідентифікації суб'єкта.

Сьогодні, в еру Інтернету та бурхливого розвитку телекомунікаційних технологій, у всьому світі гостро постає проблема автентифікації користувача інформаційних ресурсів. Широко розповсюджені системи автентифікації типу login+password явно пережили свій час. Час на зламування найскладнішого паролю обернено пропорційний потужності застосованих

© *В.М. Рифа*, 2007

обчислювальних засобів. Прослуховування мереж та перехоплення пакетів для деяких офіційних, і не зовсім, організацій на сьогодні — буденна робота. Навіть прочитати пароль, що вводить з клавіатури оператор чужого комп'ютера, вже не проблема.

Існують також системи автентифікації з використанням біометричних даних: відбитки пальців, райдужна оболонка ока і т.п. Однак такі системи мають той же недолік — відсутність явного зв'язку між login+password і суб'єктом, котрий його вводить. Тобто пароль може бути введений, але хто саме його вводить, залишається невідомим.

Таким чином, особливо актуальною постає задача пошуку методу автентифікації, який дасть змогу бути певним в тому, що login+password вводиться саме тією особою, котра має на це право. Такі системи автентифікації базуються на вимірюванні динаміки біометричних характеристик суб'єкта. В Інтернеті зустрічаються публікації, з яких можна зробити висновок, що подібні дослідження ведуться у Росії, Японії та США.

Труднощі, з якими мають справу дослідники на цьому шляху, пов'язані, перш за все, з проблемою вибору методів опису системи з суб'єктом, і як наслідок, з проблемою методів доведення істинності результатів. У своїх дослідженнях автор зіткнувся з тими ж проблемами.

Результатом досліджень, на думку автора, є один з ключових принципів побудови сучасної системи автентифікації — метод динамічних характеристик (назвемо його так).

ПОСТАНОВКА ЗАДАЧІ

Напевне, ні в кого не викличе заперечень твердження про те, що кожна людина має свої, тільки їй притаманні, особливі риси у поведінці: хода, жести чи міміка і т. ін. Тому можна сподіватись на те, що рухи оператора комп'ютера, а точніше управління курсором на екрані монітору за допомогою мишки, якимось чином несуть на собі інформацію про його психофізичні особливості як суб'єкта.

Множина траєкторій руху курсору $M\{f_i(t) = (x_i(t), y_i(t))\}$, якщо їх окремо виділити, являє собою деяке павутиння (рис. 1). На перший погляд, ця множина M, у двомірному фазовому просторі $M \subset R^2$ (екран монітору) являє собою цілком випадкові криві і не містить жодного атрактору.

Задача полягає в тому, щоб побудувати для траєкторії таке відображення $\Phi : f_i \to \phi_i = \phi(f_i)$, $\phi_i \in R^m$, а значить і для всієї множини $\Phi : M\{f_i(t) \in R^2\} \to \Lambda\{\phi_i \in R^m\}$ таке, що Λ буде мати атрактор для ϕ_i.

ТЕОРЕТИЧНІ ДЖЕРЕЛА

Як було сказано вище, оператор *керує* курсором за допомогою мишки для досягнення деякої цілі. При цьому підсвідомо на рухи руки накладені обмеження, обумовлені його психофізичним станом. Тобто можна сказати, що траєкторії руху курсору відповідають умовам деякого нам невідомого функціонала.

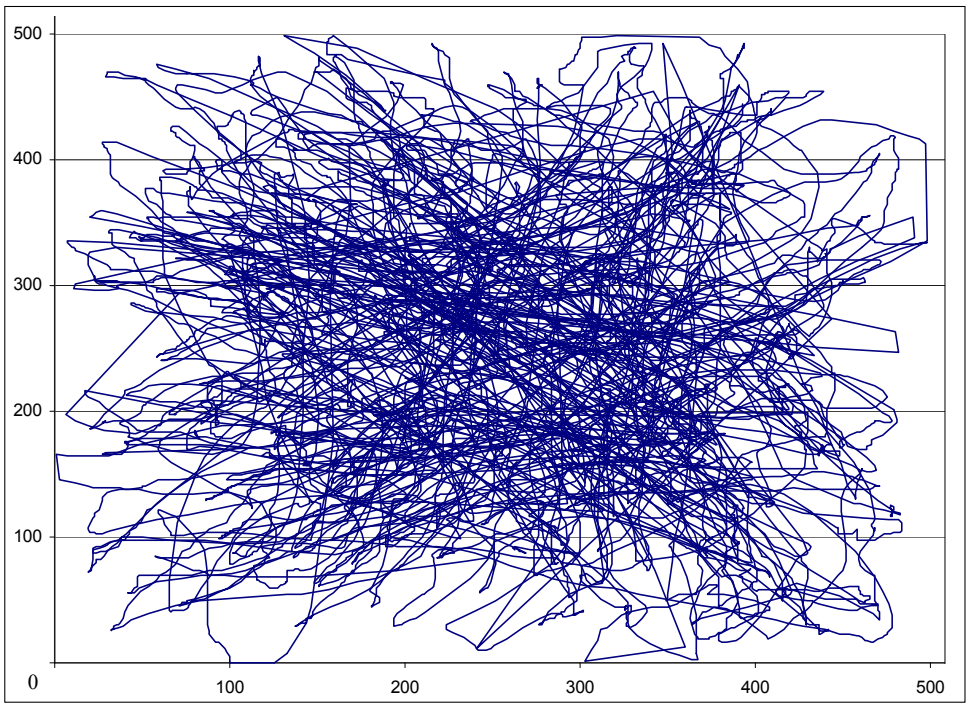

Рис. 1. Загальний вигляд траєкторій руху курсору

У теорії оптимального керування добре відомий розв'язок для лінійно-квадратичної задачі — системи диференціальних рівнянь з квадратичним функціоналом. Розглянемо розв'язок дещо складнішої задачі оптимального керування для лінійної стаціонарної системи

$$\dot{x}(t) = Ax(t) + Bu(t);\ x \in D \subset R^n;\ x(t_0) = x_0;\ u \in R^m, \tag{1а}$$

але з функціоналом якості четвертого порядку

$$J = \int_{t_0}^{t} (x^* Qx + x^* Rx\, x^* Sx + u^* Lu + F(x))dt, \tag{1б}$$

де A, B — const, відповідно розмірності $n \times n$ та $n \times m$; $D \subset R^n$ — область рівноваги системи; Q, R, S — невід'ємно визначені матриці $n \times n$; L — додатньо визначена матриця $m \times m$, а $F(x) \geq 0, \forall x \in D$ буде визначена далі; * — знак транспонування.

Покладемо, що для розв'язків задачі (1) існує функція Ляпунова у вигляді

$$V(x) = x^* V_0 x + x^* V_1 x x^* V_2 x,$$

де V_0, V_1, V_2 — додатньо визначені матриці констант розмірності $n \times n$.

Рівняння Беллмана

$$\min_u \left\{ \frac{d}{dt} V(x) + \omega(x,u) \right\} = 0,$$

де $\omega(x,u)$ — підінтегральний вираз функціоналу, опускаючи F для спрощення викладок і замінюючи $\dot{x}$ правою частиною з (1а), для нашої системи приймає вид

$$\min_u \{x^* A^* V_0 x + u^* B^* V_0 x + x^* V_0 A x + x^* V_0 B u + x^* A^* V_1 x x^* V_2 x +$$

$$+ u^* B^* V_1 x x^* V_2 x + x^* V_1 A x x^* V_2 x + x^* V_1 B u x^* V_2 x + x^* V_1 x x^* A^* V_2 x +$$

$$+ x^* V_1 x u^* B^* V_2 x + x^* V_1 x x^* V_2 A x + x^* V_1 x x^* V_2 B u +$$

$$+ x^* Q x + x^* R x x^* S x + u^* L u\} = 0 . \qquad (2)$$

Використовуючи стандартну процедуру мінімізації, одержимо

$$u = -L^{-1} B^* (V_0 + V_1 x x^* V_2 + V_2 x x^* V_1) x . \qquad (3)$$

Далі, після підстановки u в (2) і прирівнюючи результат до нуля, одержимо рівняння

$$A^* V_0 + V_0 A - V_0 B L^{-1} B^* V_0 + Q + (A^* - V_0 B L^{-1} B^*)(V_1 Y V_2 + V_2 Y V_1) +$$

$$+ (V_1 Y V_2 + V_2 Y V_1)(A - B L^{-1} B^* V_0) + RYS -$$

$$- (V_1 Y V_2 + V_2 Y V_1) B L^{-1} B^* (V_1 Y V_2 + V_2 Y V_1) = 0 ,$$

де $Y \equiv x x^*$ — так звана матриця розсіювання.

Треба відмітити, що коли прирівняти перші чотири доданки до нуля, одержимо загальновідоме матричне рівняння Ріккаті для лінійної системи з квадратичним функціоналом.

Тоді, поклавши

$$x^* (V_1 Y V_2 + V_2 Y V_1) B L^{-1} B^* (V_1 Y V_2 + V_2 Y V_1) x = F(x) ,$$

отримаємо систему матричних рівнянь

$$\begin{cases} A^* V_0 + V_0 A - V_0 B L^{-1} B^* V_0 + Q = 0; \\ (A^* - V_0 B L^{-1} B^*) W + W (A - B L^{-1} B^* V_0) + RYS = 0, \end{cases} \qquad (4)$$

яка має єдиний розв'язок: перше рівняння як матричне рівняння Ріккаті, а друге — як матричне рівняння Ляпунова відносно матриці $W = V_1 Y V_2 + V_2 Y V_1$. До того ж функція $F(x)$ відповідає всім вище поставленим до неї вимогам.

Також треба відмітити, що для обчислення вектора керування u з (3) в заданій точці x зовсім не обов'язково обчислювати V_1, V_2.

Далі розглянемо друге рівняння системи (4), позначивши

$$C = A - B L^{-1} B^* V_0 \; : \; C^* (V_1 Y V_2 + V_2 Y V_1) + (V_1 Y V_2 + V_2 Y V_1) C + RYS = 0 . \qquad (5)$$

Беручи до уваги, що точка $x = 0$ є точкою стійкої рівноваги системи (1), а також припускаючи, що математичне сподівання траєкторії $Ex(t) = 0$,

знайдемо математичне сподівання рівняння (5) вздовж траєкторії $x(t)$. Зважаючи на те, що траєкторія $x(t)$ представлена у вигляді множини послідовних значень $\{x(t_i),\ i = 0 \div N\}$, маємо

$$C^*(V_1 \Sigma V_2 + V_2 \Sigma V_1) + (V_1 \Sigma V_2 + V_2 \Sigma V_1)C + R\Sigma S = 0, \qquad (6)$$

де Σ — коваріаційна матриця траєкторії $\{x(t_i),\ i = 0 \div N\}$.

Тоді для Σ існує матриця T така, що $T^* = T^{-1}$, $TT^* = T^*T = I$, де I — одинична матриця. Тоді $T^*\Sigma T = \Lambda$ — діагональна матриця, на головній діагоналі якої розміщено спектр $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ — власні числа Σ.

Таким чином рівняння (6) можна звести до виду

$$C^{*+}(V_1^+ \Lambda V_2^+ + V_2^+ \Lambda V_1^+) + (V_1^+ \Lambda V_2^+ + V_2^+ \Lambda V_1^+)C^+ + R^+ \Lambda S^+ = 0, \qquad (7)$$

де $[\bullet]^+ = T^*[\bullet]T$.

Оскільки Σ додатньо визначена за побудовою, то всі її власні числа додатні і як наслідок можливе представлення $\Lambda = \Lambda^{\frac{1}{2}} \cdot \Lambda^{\frac{1}{2}}$ в дійсних числах. Тож далі можна побудувати процедуру декомпозиції матриці W, щоб одержати V_1 і V_2.

Гіпотеза. Як бачимо, для досить простої нелінійної замкнутої системи, коваріаційна матриця Σ і функція Ляпунова $V(x)$ мають тісний зв'язок (7). Тобто, можна припустити, що коли побудувати відображення Φ фазового простору $x(t) \in R^n$ системи керування з суб'єктом у деякий простір R^m такий, що буде мати атрактор, то спектр коваріаційної матриці траєкторії може виконувати роль ідентифікатора.

УМОВИ ПРОВЕДЕННЯ ЕКСПЕРИМЕНТІВ

На екрані монітору визначаємо вікно і у вікні формуємо ціль. Оператор повинен досягнути цілі і «клікнути» мишкою. Положення цілі генерується за допомогою рівномірного розподілу. Числові координати кожної точки $\{x(t_i), y(t_i)\}$ траєкторії руху курсору заносяться у базу даних. Після проведення вимірів обчислюється коваріаційна матриця Σ для кожної траєкторії досягнення цілі. Загальна кількість точок для одного експерименту близько 5000.

Сукупність таких параметрів, як швидкість, прискорення та інші (всього шість) в кожній точці траєкторії, є динамічними характеристиками і виконують роль вимірів простору R^6. Далі експериментально показано існування аттрактора в просторі R^6, індивідуального для кожного оператора.

Далі проводиться обчислення власних чисел матриці коваріацій (рис. 2–4).

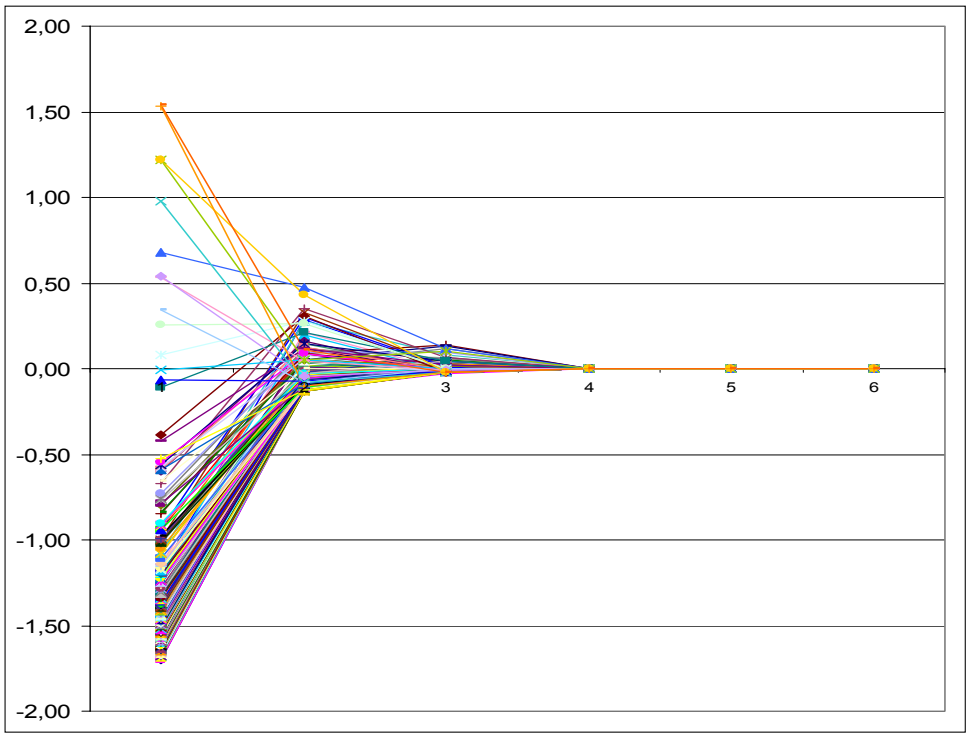

Рис. 2. Власні числа матриці коваріацій (усереднені) для одного з операторів

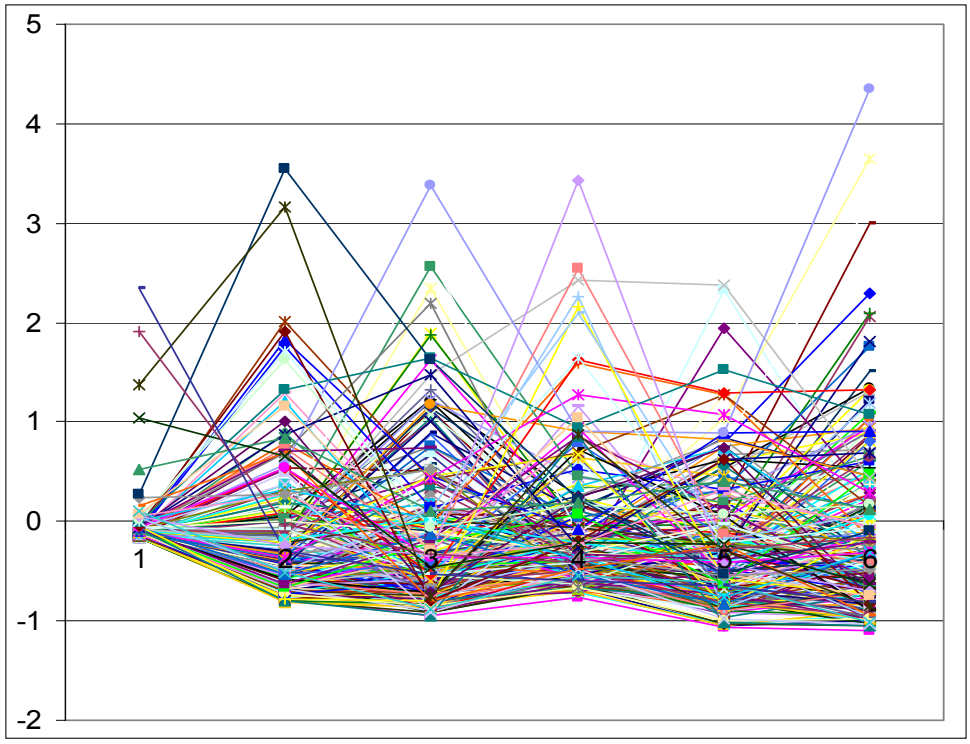

Рис. 3. Власні числа матриці коваріацій, нормовані за стандартним відхиленням

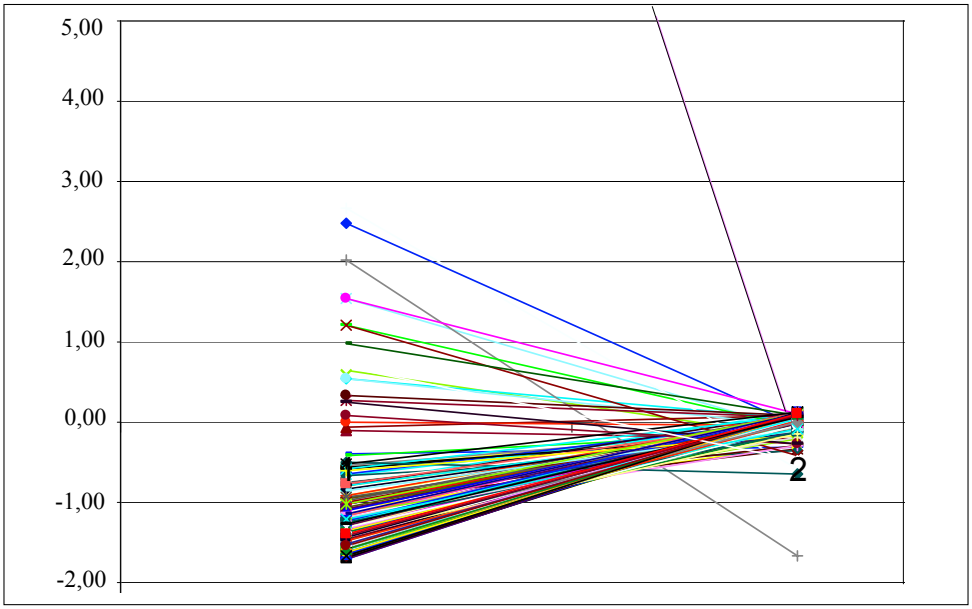

Рис. 4. Відображення множини власних чисел матриці коваріацій методом головних компонент на простір з двох власних чисел

Множина, позначена трикутниками на рис. 6, відповідає тому ж оператору, що і на рис. 5. Дані одержані з інтервалом 8 місяців.

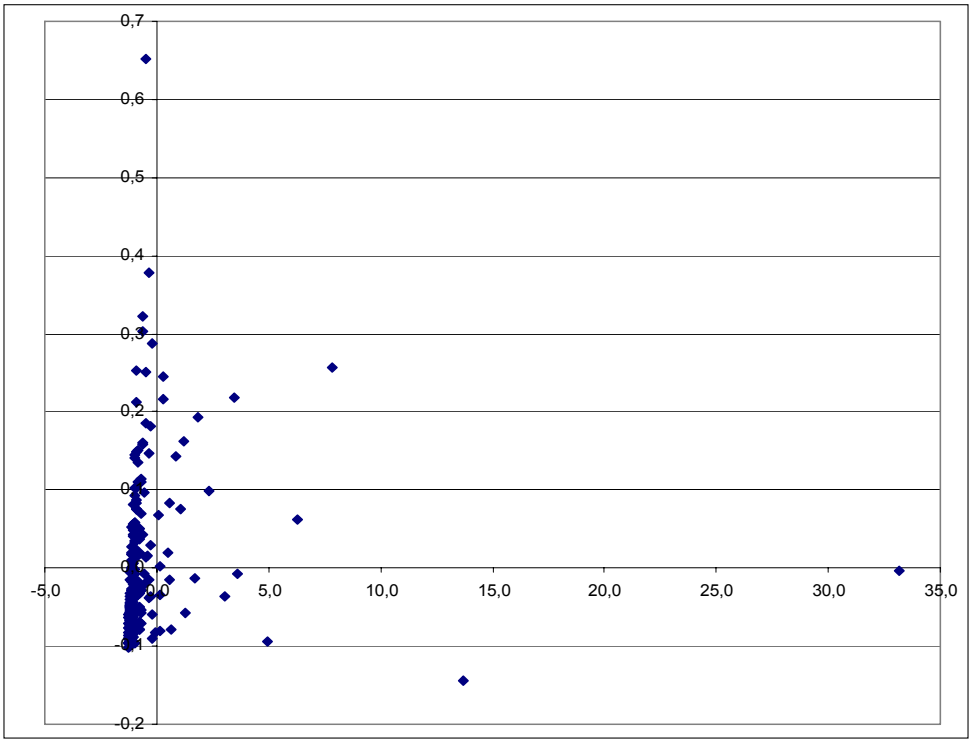

Рис. 5. Відображення множини власних чисел у двомірний простір методом головних компонент. Кожна точка має координати: по горизонталі перше власне число, по вертикалі — друге

Як бачимо, що тільки на рис. 6 є можливість говорити про атрактор спектра коваріаційної матриці для кожного з суб'єктів. Якщо розглянути внутрішню структуру атрактора, то виявляється, що зображення має фрактальну природу.

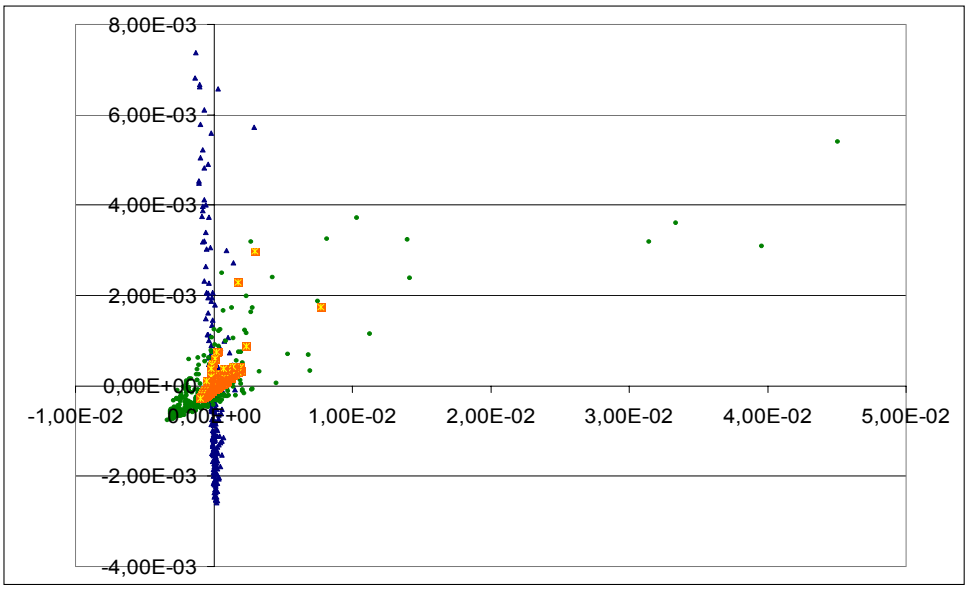

Рис. 6. Відображення множини власних чисел у двомірний простір для трьох операторів

Обчислення показника Херста (рис. 7) проводились для часового ряду найбільшого власного числа коваріаційної матриці відповідно до траєкторій, наведених на рис. 1.

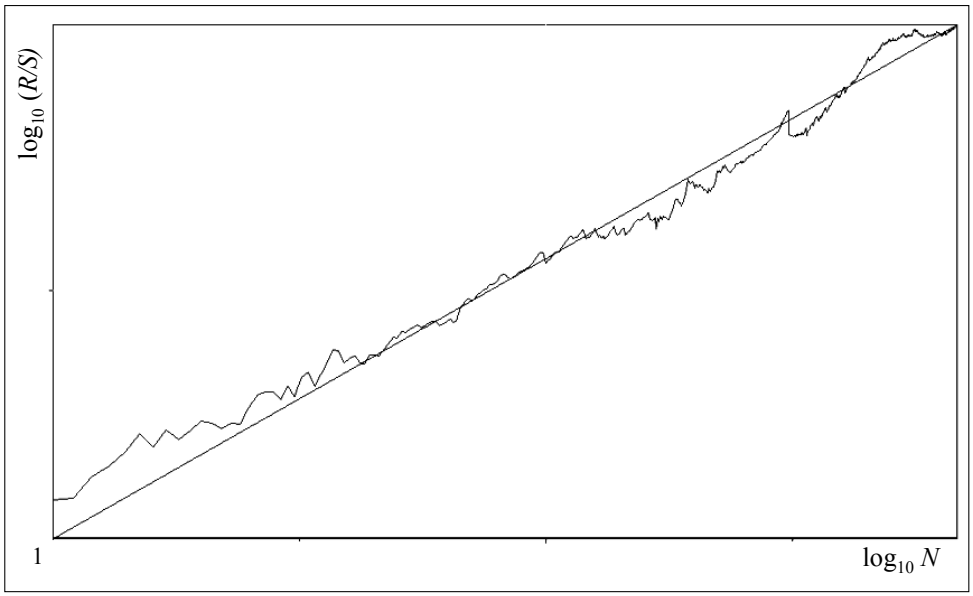

Рис. 7. Показник Херста для часового ряду власних чисел $H = 0{,}8696 \pm 0{,}1030$; фрактальна розмірність $D = 2 - H = 1{,}1304 \pm 0{,}1030$

ВИСНОВОК

Таким чином, використовуючи метод динамічних характеристик, експериментально доведено існування атракторів для кожного суб'єкта оператора ПК. Одержані атрактори мають фрактальну структуру. Результати досліджень можуть бути покладені в основу нових принципів розробки методів автентифікації і доступу до інформаційних ресурсів.

Примітка. Розрахунки показника Херста та фрактальної розмірності проводились за допомогою програми ФРАКТАЛЬНЫЙ АНАЛИЗ. (Copyright © 1998-2003, Вячеслав Сычев, Лаборатория обработки данных, Институт математических проблем биологии, РАН, Пущино, Московская обл., Россия sychyov@mail.ru http://impb.psn.ru/~sychyov/.)

Програму для одержання даних розробив Дмитро Долгов (dm_dds@mail.ru.).

ЛІТЕРАТУРА

1. *Рифа В.Н., Баклан Я.И., Баклан И.В.* Метод главных компонент в задачах аутентификации // Тр. VI Всеукр. междунар. конф. — Киев: Укр'ОБРАЗ 2002. — С. 215–218.
2. *Рифа В.Н.* Методы оптимального управления в задаче аутентификации // Вестник ун-та Туран. — 2004. — **22**, № 1-2. — С. 194–197.
3. *Рифа В.Н.* Метод динамических характеристик в задаче биометрической аутентификации. Фракталы в биометрии // Тез. докл. Междунар. 11-й межвуз. конф. по математике и механике Евразийского национального ун-та им. Л.Н. Гумилева. — Астана, 2006. — 212 с.

Надійшла 07.02.2007