ЗАКЛЮЧЕНИЕ

Представленный в работе метод вычисления элементов матрицы Хассе – Витта гиперэллиптических кривых, позволяет решить задачу определения якобиана гиперэллиптических кривых. Метод требует для реализации существенно меньших вычислительных затрат по сравнению с известными. Дальнейшие исследования в этом направлении заключаются в совершенствовании формул вычисления биномиальных коэффициентов по модулю большого простого числа, а также в исследовании свойств рациональных гиперэллиптических кривых, соответствующих значениям $k > 1$ в формуле (9).

ПЕРЕЧЕНЬ ССЫЛОК

1. *Colm Ó hÉigeartaigh.* A Comparison of Point Counting methods for Hyperelliptic Curves over Prime Fields and Fields of Characteristic 2 [Электронный ресурс] / Colm Ó hÉigeartaigh: Cryptology ePrint Archive: Report 2004/241, 2004 . – P. 1–12. – Режим доступа: http://eprint.iacr.org/ 2004/241.pdf.
2. *Долгов В. И.* Методы определения порядка якобианов гиперэллиптических кривых / Долгов В. И., Неласая А. В. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – ХНУРЭ, 2007. – Том 6, № 3. – С. 366–369.
3. *Menezes A.* An Elementary Introduction to Hyperelliptic Curves [Электронный ре-сурс] : Published as Technical Report CORR 96–19 Department of C&O University of Waterloo: Ontario: Canada / Menezes A., Wu Y., Zuccherato R. – 1996. – P. 1–35. – Режим доступа: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps.
4. *Манин Ю. И.* О матрице Хассе–Витта алгебраической кривой / Манин Ю. И. // Известия АН СССР. Серия: Математика. – 1961. – Том 25, выпуск 1. – С. 153–172.
5. *Bostan A.* Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator / Bostan A., Gaudry P., Schost É. // Proceedings of Fq7, Lecture Notes in Comput. Sci. – Berlin : Springer-Verlag, 2004. – Vol. 2948. – P. 40–58.
6. *Долгов В. И.* Стойкость криптографических алгоритмов на гиперэллиптических кривых / Долгов В. И., Неласая А. В. // Прикладная радиоэлектроника : тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2006. – Том 5, № 1. – С. 30–34.
7. *Чевардин В. Е.* Метод аутентификации данных на основе ключевого хеширования с использованием арифметики эллиптических кривых : дис. канд. техн. наук : 05.13.21 / Чевардин В. Е. – Полтава, 2006. – 202 с.
8. *Бронштейн И. Н.* Справочник по математике / Бронштейн И. Н. Семендяев К. А. – М. : Наука, 1967. – 608 с.
9. *Ладиков А. В.* Улучшенный алгоритм вычисления факториала / Ладиков А. В. // Математические заметки. – 2008. – Т. 83, № 6. – С. 857–863.

Надійшла 16.09.2008

В статті пропонується метод обчислення елементів матриці Хассе – Вітта гіпереліптичних кривих спеціального виду, що базується на застосуванні формули бінома Ньютона.

The method of calculation of Hasse – Witt matrix for special hyperelliptic curves is proposed. This method is based on using binomial theorem.

УДК 004.93.1

В. М. Заяць

ДОЦІЛЬНІСТЬ ВСТАНОВЛЕННЯ ПРИОРІТЕТУ ПЕРВИННИХ ОЗНАК ПРИ ПОБУДОВІ СИСТЕМ РОЗПІЗНАВАННЯ ТА ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ І ПРОЦЕСІВ НА ОСНОВІ ДЕТЕРМІНОВАНИХ ТА ІМОВІРНІСНИХ МЕТОДІВ

Запропоновано підхід до встановлення пріоритетну первинних ознак при побудованої системи розпізнавання користувачів комп'ютера на основі її опису у вигляді дискретної моделі, що рекурентно зв'язує часові затримки при введені інформації з клавіатури комп'ютера у дискретні відліки часу. Доцільність розроблених підходів проілюстровано при реалізації автоматизованої процедуру ідентифікації користувачів комп'ютера на основі детермінованого та імовірнісного методів.

ПОСТАНОВКА ЗАДАЧІ

При створені нових реальних пристроїв, дослідженні невивчених фізичних явищ чи процесів, побудові систем розпізнавання та ідентифікації, що мають бажані характеристики інформаційного сигналу або невідомі характеристики, які підлягають вивченню, доцільно провести комп'ютерне моделювання та аналіз, створивши адекватні математичної моделі об'єкта, що розробляється чи вивчається. Такий підхід вимагає значно менших часових і технічних засобів порівняно з фізичним експериментом, особливо на попередній стадії розробки, за відсутності достовірної апріорної інформації

Останнім часом в нелінійній динаміці широке застосування знаходять дискретні моделі систем [1–6] для яких дискретність закладена в природі самого

об'єкта досліджень, а не є наслідком дискретизації неперервної системи [7–10]. Доцільність використання дискретних по своїй природі моделей пояснюється такими їх особливостями:

– простотою математичного опису в порівнянні з неперервними моделями;

– наявністю суттєво ширшого спектру динамічних режимів, порівняно з відомими моделями;

– нескінченною вимірністю, що дозволяє моделювати кожну нову гармоніку процесу шляхом її введення у вектор змінних стану, тоді як для неперервних системах для вирішення цієї задачі необхідно підвищувати розмірність системи;

– відсутністю необхідності визначення кроку дискретизації, оцінки локальної і глобальної похибок чисельних методів, областей стійкості та синхронізації;

– кращою адаптованістю до постановки комп'ютерного експерименту, порівняно з неперервними моделями.

Власне моделі, дискретні за своєю природою є застосовні як до побудови пристроїв, що мають бажані режими, так і до розпізнавання та ідентифікації таких режимів у системах зі складною динамікою і поведінкою, що дозволяє підвищити ефективність їх роботи.

При такій постановці задачі актуальною є проблема розроблення надійних підходів до встановлення пріоритету первинних ознак, що формуються в процесі розпізнавання в реальному режимі часу.

Метою даної статті є формування підходу до встановлення пріоритету первинних ознак, які використовуються для опису автоматизованих комп'ютерних систем розпізнавання та достовірної ідентифікації об'єктів і явищ зі складною динамічною природою, для забезпечення достовірного якісного та автоматизованого процесу розпізнавання та ідентифікації досліджуваних систем В роботі також визначено перспективні напрямки розвитку систем розпізнавання складних динамічних систем на основі дискретних моделей та напрямки їх доцільного застосування.

ОСНОВНІ ПРОБЛЕМИ РОЗПІЗНАВАННЯ

При розроблені систем розпізнавання об'єктів і явищ та їх достовірної ідентифікації необхідний системний підхід, суть якого полягає у формуванні первинних ознак про об'єкт розпізнавання, встановленню їх пріоритету та вибору або розробленню та реалізації надійних критеріїв розпізнавання і достовірної ідентифікації об'єктів та процесів.

Перші дослідження у галузі розпізнавання в нашій країні проводилися О. О. Харкевичем [11] – одним з основоположників та фундаторів теорії інформації та сигналів. Значний внесок у розвиток теорії розпізнавання зробили В. М. Глушков, В. С. Міхалєвич, О. Г. Івахненко, Ю. І. Журавльов, Я. З. Ципкін, В. І. Васильєв. Серед іноземних вчених слід згадати роботу Ф. Розенблатта, який у 1957 р. запропонував машину, яка навчалася розпізнавати образи і називалася персептроном). Це була найпростіша модель діяльності людського мозку. Значний вклад у подальший розвиток теорії розпізнавання образів зробили У. Гарднер, Р. Дуда, Г. Себастіан, Дж. Ту, К. Фу, П. Харт, С. Ватанабе та інші.

Перші роботи з розпізнавання образів було присвячено теорії і практиці побудови читальних автоматів (під образом розумівся знак, зображення, буква або цифра). Математичним апаратом для розв'язання задач розпізнавання з моменту їх виникнення була теорія статистичних розв'язків [12].

На сьогоднішній день результати теорії статистичних розв'язків стали базою для побудови алгоритмів розпізнавання, які забезпечували віднесення об'єкта до його класу на підставі експериментальних апостеріорних даних, що характеризують об'єкт та апріорних даних, що описують класи об'єктів. Пізніше математичний апарат розширився за рахунок використання методів алгебри логіки і деяких розділів прикладної математики, теорії інформації, математичного програмування, системотехніки і системного аналізу [13–14].

Незважаючи на те, що методи і алгоритми розпізнавання все більшою мірою стають невід'ємною складовою таких прикладних галузей природознавства, як медична і технічна діагностика, ідентифікація складних коливних динамічних процесів і явищ, екологічний моніторинг та соціальна інформатика, метеорологічне прогнозування і геологічна розвідка, локаційні засоби спостереження та системи введення і виведення текстової, графічної та мовної інформації в комп'ютер [13], інтелектуальні системи прийняття рішень в літературі – як вітчизняній, так і в іноземній – системний підхід до задач розпізнавання поки що не став домінуючим.

Сьогодні, як і півстоліття тому, проблема розпізнавання значною мірою ототожнюється з побудовою оптимальних алгоритмів розпізнавання та дослідженням умов, які дозволяють реалізувати такий алгоритм. Теоретичні дослідження орієнтуються на розв'язання хоча й важливих, але часткових задач здебільш прикладного характеру. До таких задач у першу чергу треба віднести задачі достовірного розпізнавання, суть яких зводиться до поділу простору ознак, мовою яких описуються об'єкти чи процеси розпізнавання, на області, що відповідають класам цих об'єктів, тобто до вибору найкращих границь (правил) розділення класів. Але розв'язання цих задач можливе лише тоді, коли апріорі відомі класи об'єктів і ознаки, мовою яких описуються розпізнавані об'єкти та їх класи. Однак розробник системи

розпізнавання, як правило, не володіє цією інформацією. Навіть в найпростіших випадках розпізнавання букв алфавіту, відбитків пальців, слів мови, екстремумів та особливих точок функцій (де не виникає питання про класи), їх інформативні ознаки та апаратура для їх визначення не є відомими – це є предметом нетрадиційних досліджень.

Виникає питання про причини такої уваги задачам опису класів мовою ознак і побудови оптимальних алгоритмів розпізнавання.

Перша причина в тому, що ці задачі, порівняно, легко піддаються формальному і аналітичному розв'язанню, що й визначає їх привабливість для дослідників. Друга причина полягає у тому, що значна частина дослідників обмежує свою діяльність лише теоретичними дослідженнями. Третя проблема в тому, що традиційно вважається, що системи розпізнавання є автономними. У деяких часткових задачах це виправдано, хоча в загальному випадку таке формулювання питання не є правомірним. Адже і в системах технічної та медичної діагностики, в автоматизованих системах управління виробництвом, розпізнавання дефектів механізмів і машин, визначення діагнозу пацієнта, розпізнавання складних коливних режимів, класифікація виробничих ситуацій не є самоціллю. Їх розпізнавання необхідне для отримання вихідної інформації для підсистеми управління з метою прийняття керівних рішень, адекватних результатам розпізнавання невідомих об'єктів, явищ, ситуацій, станів.

Можна стверджувати, що достовірне розпізнавання конкретних ситуацій не є достатньою умовою потенціально можливої ефективності системи управління. Але це є необхідна умова. Важко уявити, що лікар, який поставив неправильний діагноз, знайде правильний метод лікування чи не виявлення нестійких коливних режимів забезпечить надійну роботу технічного пристрою.

При розробці будь-яких систем розпізнавання необхідний системний підхід, суть якого полягає в тому, щоб в умовах неминучих фінансових і технічних обмежень система розпізнавання забезпечила системі управління реалізацію потенціально можливої ефективності. Вибору чи створенню критеріїв розпізнавання повинна передувати процедура вимірювання первинних ознак про процес розпізнавання, встановлення пріоритету цих ознак та їх впливу на інтегральні характеристики досліджуваного процесу чи об'єкту. З математичної точки зору опис такої системи має забезпечувати мінімальну похибку розпізнавання та достовірну ідентифікацію об'єкта розпізнавання за певними ознаками та критеріями прийняття рішення.

Метод ідентифікації користувача шляхом виділення первинних дискретних інформативних ознак

Суть методу полягає у тому, щоб забезпечити процедуру розпізнавання конкретного користувача при його роботі за клавіатурою комп'ютера. Деякі загальні міркування щодо створення такої системи подані в роботі [13–15].

Очевидно, для організації процесу розпізнавання у пам'ять комп'ютера необхідно ввести текст (зразок) кожного із об'єктів розпізнавання. При відсутності зразка об'єкт не розпізнається або пропонується створити новий клас об'єктів шляхом завдання зразку почерку (це можна використати для забезпечення санкціонованого доступу до ресурсів комп'ютера). Паралельно при створенні зразка за рукомоторними ознаками об'єкту формується інформаційна модель об'єкту шляхом визначення функцій розподілу часових затримок при введенні інформації в комп'ютер. У якості первинних ознак про об'єкт о використано різні часові затримки при роботі об'єкта з клавіатурою комп'ютера. Встановити пріоритет кожної із первинних ознак можна експериментальним шляхом, що запропоновано в роботі [16]. При ідентифікації об'єкта знову реалізуємо процедуру вибору або розроблення критеріїв прийняття рішення і на основі цих критеріїв [14–16] і приймаємо рішення про віднесення об'єкта до певного класу. У випадку неоднозначного рішення можна застосувати функції відстані (детермінований підхід) і однозначно обрати клас (з найменшим середньоквадратичним відхиленням ознак). Відзначимо, що різні інформаційні ознаки можуть мати різний пріоритет, який також можна встановити експериментально. З метою підвищення ефективності системи доцільно відсікати не детерміновані хаотичні рухи руки особи шляхом попередньої фільтрації інформації, що вводиться користувачем в режимі реального часу, створюючи тим самим неперервні послідовності (набори) символів.

У роботах [15–17] сформульовано і проаналізовано велику кількість характеристик. Приведемо лише найбільш інформативні та доступні для швидкого формування. Отже, для побудови системи розпізнавання особи за її рукомоторними реакціями було обрано наступні характеристики:

1) відносна девіація паузи перед клавішем – розподіл відносних відхилень паузи перед даним клавішем до середнього значення паузи перед всіма клавішами у даній неперервній послідовності набору

$$\mathrm{Dev}B = \frac{t_i - t_{\mathrm{ср}}}{t_{\mathrm{ср}}} \cdot 100\ \%, \qquad (1)$$

де t_i – тривалість паузи перед i-м клавішем, $t_{\text{ср}}$– середня тривалість паузи перед клавішами в послідовності набраного тексту.

2) відносна девіація утримання клавіша – розподіл відносних відхилень тривалості утримання натиснутим даного клавіша до середньої тривалості утримання клавіша у даній неперервній послідовності

$$\text{Dev}P = \frac{t_i - t_{\text{ср}}}{t_{\text{ср}}} \cdot 100\ \%. \qquad (2)$$

Приклад даного розподілу зображено на рис. 1. На осі абсцис відкладено відносні відхилення у відсотках, а на осі ординат – відносну частоту попадань у відповідний інтервал відхилень.

3) відносна девіація паузи після клавіша – аналогічна попередній характеристиці:

$$\text{Dev}A = \frac{t_i - t_{\text{ср}}}{t_{\text{ср}}} \cdot 100\ \%; \qquad (3)$$

4) відношення величини паузи перед клавішем до тривалості утримання клавіша;

5) відношення величини паузи перед клавішем до величини паузи після клавіша;

6) відношення величини паузи після клавіша до тривалості утримання клавіша;

7) розподіл частот використання клавіш зміни регістру.

Всього в роботі [15] розглянуто 18 характеристик, але найбільш інформативними є вище приведені.

Характеристики 1–6 формуються для кожного клавіша, що був задіяний у наборі. Щоби спростити балансування важливості характеристик, при побудові системи прийнято рішення об'єднати перші шість характеристик у групи оскільки це значно зменшує їх кількість (а в межах групи можна розгадати їх як еквівалентні). На спосіб групування характеристик безпосередньо впливає обраний метод їх зіставлення.

У першому варіанті побудови системи розпізнавання для реалізації процедури ідентифікації було використано функції відстані. Оскільки вага характеристик кожної групи могла бути різною, то відстані обчислювались окремо по кожній з груп характеристик. Відстань між класами Ω і Z в межах кожної групи характеристик обчислюється за формулою середнього квадратичного відхилення:

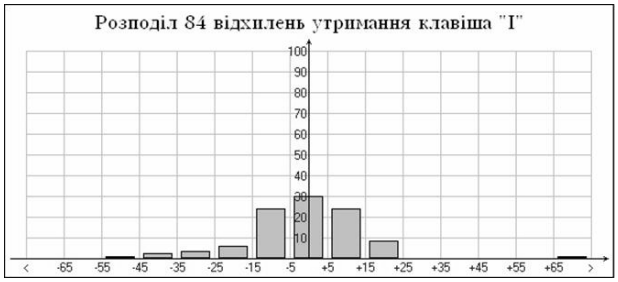

Рисунок 1 – Розподіл відносних девіацій утримання заданого клавіша натиснутим

$$\text{Dist}(\lambda) = \sqrt{\frac{1}{n} \cdot \sum_{i=1}^{n} \left(m_i^{\Omega} - m_i^{Z} \right)^2}, \qquad (4)$$

де m_i – середнє значення вибірки i-ї характеристики даної групи класу Ω, $\text{Dist}(\lambda)$ – відстань між класами за групою характеристик λ.

Відстані вимірюються між середніми значеннями, оскільки середнє може бути оцінено вже після відносно невеликої кількості дослідів (10–20), що є важливим для зменшення об'єму тексту, що набирається об'єктами розпізнавання.

Групи характеристик 1–6 не еквівалентні за якістю рішень, що приймаються на їх основі. Перед об'єднанням результатів для прийняття рішення по розпізнаванню, необхідно збалансувати ваги груп між собою. Баланс характеристик здійснений обернено пропорційно ймовірностям допустити помилку другого роду (коли два об'єкти різних класів розпізнаються як такі, що належать до одного класу) по кожній з груп характеристик, зокрема: $1/p_1{:}1/p_2{:}1/p_3{:}1/p_4{:}1/p_5{:}1/p_6{:}1/p_7$. Експериментально було отримано відношення ваг груп 1–7 як 4:12:8:6:5:2:6 відповідно. Недоліком системи на основі функцій відстані є те, що вона принципово не може визначити ймовірність правильності або не правильності рішення по розпізнаванню. Кожний сторонній користувач буде схожий на того чи іншого зареєстрованого користувача системи.

Розроблений другий варіант побудови системи розпізнавання базується на використанні методу довірчих інтервалів. Для перевірки гіпотези про приналежність пари об'єктів одному класу перевіряються гіпотези про рівність середніх значень розподілів [18, 19] всіх характеристик кожної групи. Для цього обчислюються значення середнього a та вибіркового стандарту s за формулами

$$a = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i; \qquad (5)$$

$$s = \sqrt{\frac{1}{n-1} \cdot \sum_{i=1}^{n} (x_i - a)^2}. \qquad (6)$$

Для розрахунку довірчих інтервалів враховується закон розподілу середнього значення:

$$f(x_{\text{ср}}) = \frac{\sqrt{n}}{\sigma \cdot \sqrt{2\pi}} \cdot e^{-\frac{n}{2 \cdot \sigma^2} \cdot (x_{\text{ср}} - x_0)}. \qquad (7)$$

Для вибірок малого об'єму оцінка середнього значення уточнюється за допомогою розподілу Стьюдента [16], за яким розподілена величина $u = \frac{a-m}{s_{\text{ср}}}$. Його густина розподілу задається формулою:

$$S(u,n) = \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)\cdot\sqrt{\pi\cdot n}}\cdot\left(1+\frac{u^2}{n}\right)^{-\frac{n+1}{2}}. \qquad (8)$$

Нехай при порівнянні пари відповідних розподілів ми допускаємо помилку першого роду P_α, а всього порівнюємо N таких пар. Отже, логічно припустити, що інтегральна характеристика групи класу і об'єкту співпадає з ймовірністю $\geq 1-P_\alpha$, якщо кількість непідтверджених гіпотез N_α не перевищує числа $P_\alpha\cdot N$, у іншому випадку вважаємо що об'єкт не належить класу. Такого типу (так/ні) результат ми отримаємо для кожної з шести груп характеристик. Як і у випадку системи на основі функції відстані, ці групи не еквівалентні по якості рішень, що приймаються на їх основі. Кожна з них має свою ймовірність помилки другого роду.

На основі практичних експериментів по розпізнаванню з кожною групою характеристик досліджувалися помилки другого роду. Окремі гіпотези система перевіряла з рівнем значущості $\alpha = 0,05$. Так були отримані ймовірності помилок другого роду 35 %, 13 %, 20 %, 27 %, 32 %, 78 %. Це дало змогу встановити пріоритет кожної із розглянутих вище семи ознак на основі підходу, описаного в [16]. Найбільшим пріоритетом володіє шоста ознака Отримані ймовірності помилок були отримані для порівняно невеликої кількості експериментів по ідентифікації (105 експериментів). Для великої групи людей ймовірності помилок можуть дещо відрізнятися від наведених.

При тестуванні розробленої системи на досліджуваних об'єктах була допущена лише одна помилку на 22 проведених розпізнавання (запропоновано два схожих на об'єкт класи, один серед яких був правильний).

Наближена оцінка помилки прийняти об'єкт одного класу за об'єкт іншого не перевищує 35 % при наявності 112 зареєстрованих у системі класів.

Система розпізнає зареєстрованого користувача після набору ним 5–8 речень по 60 знаків кожне, тобто після введення 300–500 знаків. При достатній кваліфікації користувача (швидкість набору тексту 200 знаків за хвилину) система розпізнає користувача, який набирає замість завдання довільний текст. В ряді випадків зареєстровано розпізнавання особи при наборі тексту англійською мовою Це характерно для висококваліфікованого користувача (швидкість набору тексту більше 300 символів за хвилину), коли ймовірність хаотичних рухів руки від усталеного часового режиму є малоймовірною.

Підхід до опису системи розпізнавання користувача комп'ютера на основі дискретної моделі

Запропонований підхід для побудови дискретних моделей коливних процесів зі складною структурою, розглянутий в роботах [17, 18] можна застосувати до опису коливної системи будь-якої природи за умови, що її стани характеризуються дискретними ознаками. Для довільного числа ознак N маємо N-вимірний вектор змінних стану, а матрицю переходу станів $\mathbf{A}$ будуємо таким чином, щоб її визначник дорівнював одиниці. Найпростішим чином це можна зробити, якщо $N-2$ рядки матриці мають одиниці на головній діагоналі, а поза діагональні елементи дорівнюють нулю. При цьому останні два рядки цієї матриці є комбінацією гармонічних функцій початкової фази φ

$$\mathbf{A}(\varphi) = \begin{pmatrix} 1&0&0&\dots&0&0&0\\ 0&1&0&\dots&0&0&0\\ 0&0&1&\dots&0&0&0\\ \vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots\\ 0&0&0&\dots&1&0&0\\ 0&0&0&\dots&0&\cos\varphi&\sin\varphi\\ 0&0&0&\dots&0&-\sin\varphi&\cos\varphi \end{pmatrix}. \qquad (9)$$

Тоді амплітуді коливань відповідатиме середньоквадратичне значення N-вимірного вектора змінних стану, яке може бути обчислене із завданням конкретного набору функцій f. Як засвідчує аналіз дискретної моделі в роботі [20] з введенням в матрицю переходу станів (9) N-мірного вектору станів період при цьому знову може бути оцінений на основі формули (10). Ефективність такого підходу до опису приведеної в попередньому розділі комп'ютерної системи розпізнавання користувача комп'ютера за його рукомоторними реакціями, які визначаються різними часовими інтервалами (час утримання клавіші, тривалість паузи перед натисканням клавіші, тривалість паузи після натисканням клавіші) як абсолютних так і віднесених до їх середнього значення, або одного часового інтервалу до іншого підтверджена результатами комп'ютерного моделювання.

На основі запропонованого підходу реалізована в середовищі DELPHI комп'ютерна система розпізнавання користувача комп'ютера за його рукомоторними діями. У реальному режимі часу в процесі набору користувачем заданого тексту відбувається формування функцій розподілу різних часових затримок, які апроксимуються нормальним законом розподілу. На основі співставлення біжучих значень математичних сподівань і дисперсій для кожного із сформованих розподілів з апріорі заданими зразками ідентифікується той чи інший користувач. Ефективність такої

системи не перевищує 65 % при реєстрації всіх часових ознак.

Для підвищення ефективності розробленої системи запропоновано описувати її у вигляді системи дискретних рівнянь шостого порядку відповідно до сформованих значень дискретних ознак (часових затримок). Вибір базових функцій для опису такої системи розпізнавання є проблематичним, оскільки це мають бути імовірнісні функції розподілу, які у відповідності до рукомоторних дій користувача мають передбачати появу тієї чи іншої літери на клавіатурі комп'ютера і прогнозувати величину часової затримки при її натисканні чи величину паузи до і після натискання. Але незалежно від вигляду цих базових функцій у випадку опису процесу у вигляді дискретної моделі, коли за ознаки вибрати відношення девіацій часу утримання до паузи перед клавішею та відношення девіацій паузи до часу утримання клавіші, максимальна інформативність яких підтверджена результатами комп'ютерного моделювання, оцінку періоду повторення слідування літер на клавіатурі можна отримати за формулою

$$T = \frac{2 \cdot \pi}{\varphi}. \qquad (10)$$

Якщо виходити з реального середнього часу утримання клавіші 0,3 с, то з урахуванням пауз до і після утримання клавіші період набору літер не перевищуватиме 1 с, що відповідає початковій фазі коливань 2р. Отже, при введенні в алгоритм розпізнавання блоку формування неперервної послідовності літер, коли в реальному режимі часу відсікаються будь-які хаотичні рухи (випадкова неуважність, механічна затримка, натискання кількох клавіш, вимушена пауза тощо), ефективність такої системи ідентифікації користувача значно зростає.

При такому підході очевидно актуальним є встановлення пріоритету ознак, оскільки найбільш інформативні з них необхідно включати в матрицю переходу станів (9). Як показали результати статистичних випробувань за наявності 200 користувачів в базі даних похибка розпізнавання не перевищувала 5 %.

Перспективи розвитку та застосування дискретних моделей коливних систем до аналізу динаміки складних об'єктів

Результати проведеного аналізу комп'ютерної системи ідентифікації користувача комп'ютера підтверджують доцільність використання дискретних моделей до розв'язання широкого класу прикладних проблем, пов'язаних з розпізнаванням складних динамічних режимів, що мають місце в об'єктах коливної природи. Завжди, коли з апріорних міркувань можна визначити елементи матриці переходу станів для двох змінних, то коливну систему будь-якого порядку можна подати у дискретному вигляді [20], використовуючи для запису матриці станів подання (9) Застосування цього підходу до опису системи ідентифікації користувача комп'ютера підвищило достовірність розпізнавання в 1,4 рази. Вдалий вибір для функцій зміни амплітуд часових затримок дозволяє не лише ефективно реалізовувати процедуру розпізнавання, але й аналізувати психофізіологічний стан користувача комп'ютера і передбачати появу того чи іншого слова на екрані монітора. Таким чином, ця система може бути ефективно застосована і до розв'язання задач медичної діагностики при створенні біометричних вимірювальних систем.

Видається доцільним застосування описаного підходу до побудови системи розпізнавання рукописних літер, алгоритм та архітектура якої на основі структурного підходу описані в роботах [21, 22]. Очевидно, тут слід виходити не зі структури написання літери, а будувати систему розпізнавання виходячи з напрямку руху руки (рух зверху вниз і в зворотному напрямку, рух зліва на право і в зворотному напрямку) та з часу написання літери. Оцінивши математичне сподівання часу написання кожної літери, яке характерне для кожного користувача можна реалізувати процедуру розпізнавання. З математичної точки зору, з врахуванням напрямку руху руки, це буде дискретна система 12-го порядку. Виходячи з (10) можна стверджувати, що при формуванні неперервних послідовностей літер час написання має бути кратний цілому числу.

Цей інтервально-часовий підхід до формування первинних інформативних ознак про об'єкт чи процес дослідження, орієнтований на використання дискретних моделей, з успіхом може бути застосований до побудови систем захисту інформації, медичної діагностики, біометричних систем, розв'язання транспортних задач, опрацювання потоків даних та створення інтелектуальних баз знань.

ВИСНОВКИ

В даній роботі описано метод до формування первинних ознак при побудові комп'ютерної системи розпізнавання користувачів комп'ютера, запропоновано алгоритм та спосіб реалізації такої системи, відзначені особливості її функціонування та запропоновані шляхи підвищення точності розпізнавання та забезпечення достовірності ідентифікації користувачів комп'ютера на основі встановлення пріоритету первинних дискретних ознак та використання дискретних моделей, що по суті справи зв'язують тривалості пауз з часом утримання клавіш при введені інформації з клавіатури комп'ютера. Відзначено основні напрямки розвитку автоматизованих систем розпізнавання об'єктів та процесів, побудованих на основі дискретних моделей, та вказані сфери їх доцільного застосування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Динамика одномерных отображений / А. Н. Шарковский, С. Ф. Коляда, А. Г. Сивак, В. В. Федоренко. – Киев : Наук. думка, 1989. – 216 с.
2. *Заяць В. М.* Построение и анализ модели дискретной колебательной системы / Заяць В. М. // Кибернетика и системный анализ. – 2000. – С. 161–165.
3. *Заєць В. М.* Моделі дискретних коливних систем / Заєць В. М. // Комп'ютерні технології друкарства. – 1998. – С. 37–38.
4. *Заєць В. М.* Аналіз динаміки та умов стійкості дискретних моделей коливних систем / Заєць В. М. // Вісник НУ «Львівська політехніка» «Інформаційні технології та мережі». – 2004. – № 519. – С. 132–142.
5. *Шустер Г.* Детерминированный хаос : Введение : пер. с англ. / Шустер Г. – М. : Мир, 1988. – 240 с.
6. *Zayats V.* Chaos searching algorithm for second order oscillatory system / Zayats V. // Proc. International Conf. «TCSET–2002». – Lviv – Slavsk, 2002. – P. 97–98.
7. *Андронов А. А.* Теория колебаний / Андронов А. А., Вит А. А., Хайкин С. Е. – М. : Наука, 1981. – 400 с.
8. *Бутенин Н. В.* Введение в теорию нелинейных колебаний / Бутенин Н. В., Неймарк Ю. И., Фуфаев Н. А. – М. : Наука, 1976. – 354 с.
9. *Ван-дер-Поль.* Нелинейная теория электрических цепей / Ван-дер-Поль. – М. : Связь, 1935. – 186 с.
10. *Видаль П.* Нелинейные импульсные системы / Видаль П. – М. : Энергия, 1974. – 336 с.
11. *Харкевич А. А.* Опознание образов / Харкевич А. А. // Радиотехника. – 1959. – Том 14. – С. 15–19.
12. *Фукунага К.* Введение в статистическую теорию распознавания / Фукунага К. – М. : Наука, 1979. – 512 с.
13. *Горелик А. Л.* Методы распознавания / Горелик А. Л., Скрипник В. А. – М. : Высшая школа, 1989. – 232 с.
14. *Дуда Р.* Распознавание образов и анализ сцен / Дуда Р., Харт П. – М. : Мир, 1976. – 512 с.
15. *Заяць В. М.* Алгоритмічне та програмне забезпечення системи розпізнавання людини за її рукомоторними реакціями / Заяць В. М., Уліцький О. О. // Вісник ДУ «Львівська політехніка» «Комп'ютерна інженерія та інформаційні технології». – 2000. – № 392. – С. 73–76.
16. *Заяць В. М.* Визначення пріоритету детермінованих ознак при побудові системи розпізнавання об'єктів / Заяць В. М., Шокира О. // Зб. праць науково-практичної конф. ЛДІНТУ імені В. Чорновола «Математичне моделювання складних систем». – Львів, 2007. – С. 135–137.
17. *Заяць В. М.* Підхід до опису системи розпізнавання користувача комп'ютера / Заяць В. М. // Комп'ютерні технології друкарства. – 2006. – С. 46–53.
18. *Заяць В. М.* Математичний опис системи розпізнавання користувача комп'ютера / Заяць В. М., Заєць М. М. // Фізико-математичне моделювання та інформаційні технології : зб. – Львів, 2005. – Вип. 1. – С. 146–152.
19. *Березин И. С.* Методы вычислений / Березин И. С., Жидков Н. П. – М. : Физматиздат, 1962. – 639 с.
20. *Заєць В. М.* Приведення неперервної автоколивної системи до дискретної моделі та спрощення її аналізу / Заєць В. М. // Відбір і обробка інформації. – 2005. – Вип. 23 (99). – С. 35–39.
21. *Алексєєв А.* Алгоритм розпізнаван-ня символів на основі структурного підходу / Алексєєв А., Заяць В., Іванов Д. // Вісник НУ «Львівська політехніка» «Комп'ютерна інженерія та інформаційні технології». – 2002. – № 468. – С. 129–133.
22. Заяць В. М. Проект системи розпізнавання рукописного тексту / Заяць В. М., Іванов Д. О. // Вісник НУ «Львівська політехніка» «Комп'ютерна інженерія та інформаційні технології». – Львів, 2003. – № 481. – С. 78–83.

Надійшла 6.10.2008
Після доробки 2.12.2008

В статье предложен поход к установлению приоритета первичных признаков при построении системы распознавания пользователя компьютера при описании ее в виде дискретной модели путем определения рукомоторных реакций пользователя при введении информации с клавиатуры компьютера. Целесообразность подхода иллюстрируется при реализации процедуры идентификации пользователя компьютера при использовании детерминированного и вероятностного подходов.

In the paper establishment of the priority of primary features in construction of recognition system of computer user while describing it as discrete model by means of manual motor reaction detection by the user while entering in-formation from a key board was offered. Appropriateness method is illus-trated in the process of user identification procedure by means of using im-plementing and probability approaches.

УДК 004.94

И. В. Корольков

ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ПАРАЛЛЕЛЬНОГО МОДЕЛИРОВАНИЯ МАРШРУТИЗАЦИИ В БОЛЬШИХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Рассмотрена система параллельного моделирования больших вычислительных сетей. Предложенная архитектура нацелена на моделирование больших сетей за счет параллельного выполнения и эффективного использования памяти. Система использует гибридный метод синхронизации на основе окон и нулевых сообщений и позволяет достичь ускорения выполнения, близкого к линейному. Модульный принцип системы позволяет легко добавлять новые сетевые устройства и протоколы. Предложены модули моделирования маршрутизаторов, каналов связи и источников трафика.

ВВЕДЕНИЕ

С ростом Интернет и широким внедрением IP-сетей интерес к крупномасштабному сетевому модели-