МЕТОД РОЗПІЗНАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ НА ОСНОВІ DTW-АЛГОРИТМУ

Ожоганич О.В.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Комп'ютерної радіоінженерії
і систем технічного захисту інформації (КРіСТЗІ),
тел. (057) 702-13-06, email: oleksandr.ozhohanych@nure.ua

The focus of the research is biometric recognition systems. The study subject is person authentication via keystroke dynamics. The algorithm of keystroke authentication based on the DTW algorithm is developed.

Однією з тенденцій розвитку інформаційних технологій є персоніфікація електронних пристроїв, якими люди користуються для спілкування, пошуку інформації, торгівлі, банківських та інших операцій. Кожен з користувачів подібних пристроїв кілька разів на день стикається з процедурою ідентифікації, яка є обов'язковим первинним етапом отримання доступу до будь-якої сучасної комп'ютерної системи. Одним з елементів подібних систем є підсистема управління доступом до інформаційних ресурсів, яка дає можливість розмежувати доступ кола користувачів, що мають доступ до інформації.

У біометричних системах ідентифікації за клавіатурним почерком зразок динаміки набору парольної фрази довжиною n символів може бути представлений послідовністю тривалостей HD^t натискань клавіш та пауз F^t між відпусканням попередньої та натисканням наступної клавіші. Таким чином, формуються два біометричних вектори V_1 і V_2 (рис. 1).

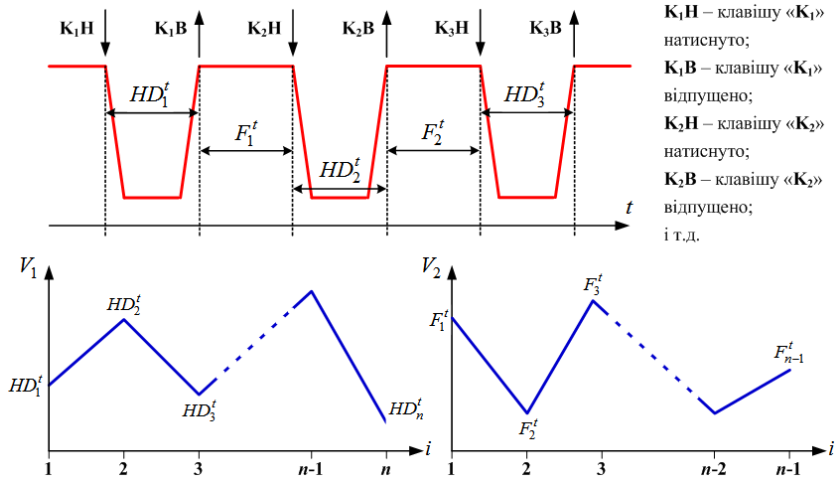


Рисунок 1

Недоліком подання біометричних характеристик користувачів за допомогою векторів V_1 та V_2 є той факт, усі події клавіатури розглядаються як одиночні, тобто реалізації деякого марківського процесу. Перехід до

аналізу комбінацій буквосполучень дозволяє значно повніше описувати індивідуальні характеристики клавіатурного почерку особи. Найбільша доцільність вбачається у використанні диграфів (подвійних подій клавіатури).

Популярним підходом в задачі розпізнавання мови є методи і алгоритми, засновані на порівнянні мовних даних із зразками. Одним з таких підходів є алгоритм динамічного трансформування часу – Dynamic Time Warping – або скорочено DTW-алгоритм, запропонований в роботі Т.К. Вінцюка [1]. Оскільки задача порівняння біометричних векторів парольної фрази, як часових рядів, дуже подібна до задач, в яких використовується DTW-алгоритму, то доцільним виглядає використовувати цей алгоритм в задачі парольної аутентифікації за клавіатурним почерком.

Алгоритм динамічного трансформування часу обчислює оптимальну послідовність трансформації часу між двома часовими рядами.

Припустимо, що в нас є дві послідовності (часові ряди) $\{a_1, a_2, \dots, a_k\}$ і $\{b_1, b_2, \dots, b_m\}$. Як бачимо, довжина двох послідовностей може бути різною. Алгоритм починається з розрахунків локальних відхилень між елементами двох послідовностей. Найпоширеніший спосіб для обчислення відхилень є метод, що розраховує абсолютне відхилення між значеннями двох елементів (Евклідова відстань). У результаті отримаємо матрицю відхилень D, що має k рядків і m стовпців з елементами:

$$d_{ij} = |a_i - b_j|, \quad i = 1 \div k, \quad j = 1 \div m. \tag{1}$$

Далі, використовуючи значення матриці D, розраховуємо матрицю трансформації S, що також має має k рядків і m стовпців, а її елементи розраховуються за виразом:

$$\begin{cases} s_{11} = d_{11}; \\ s_{i1} = d_{i1} + s_{(i-1)1}; \\ s_{1j} = d_{1j} + s_{1(j-1)}; \\ s_{ij} = d_{ij} + \min\left[s_{(i-1)1},\ s_{1(j-1)},\ s_{(i-1)(j-1)}\right], \quad i = 1 \div k, \quad j = 1 \div m. \end{cases} \tag{2}$$

Шлях трансформації W – це набір суміжних елементів $\{w_1, w_2, \dots, w_k\}$ матриці трансформації S, який встановлює відповідність між послідовностями $\{a\}$ і $\{b\}$, мінімізуючи відстань між ними.

Шлях трансформації повинен задовольняти чотирьом умовам.

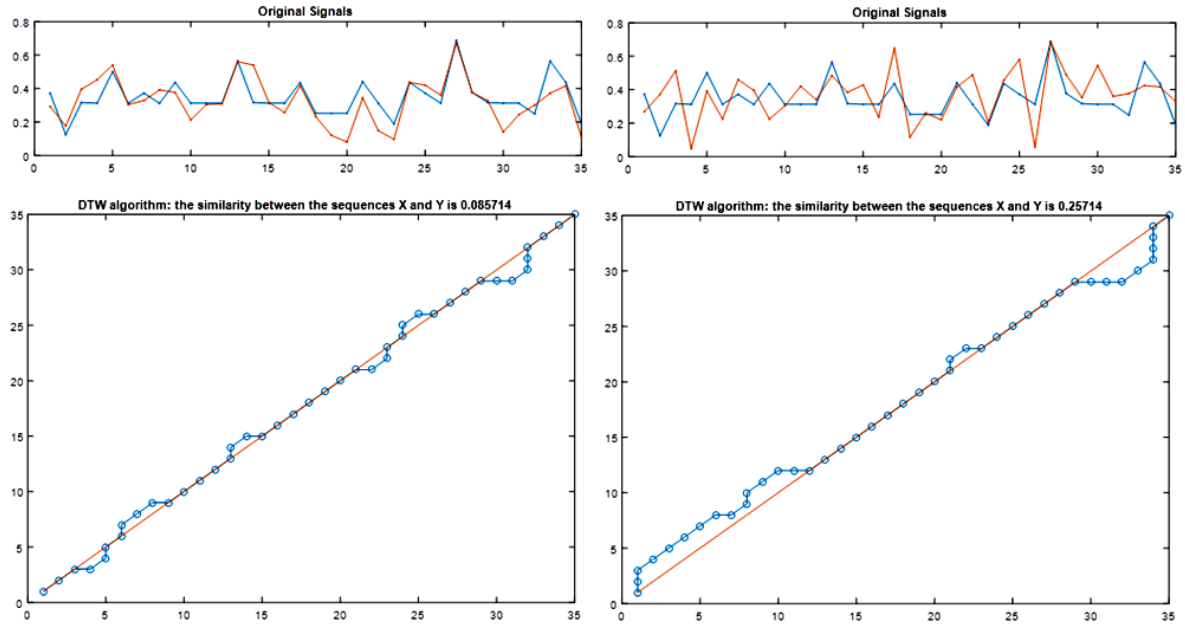
1. Гранична умова: початок шляху W – це перший елемент матриці трансформації $w_1 = s_{11}$, а кінець шляху – останній елемент матриці трансформації $w_k = s_{km}$. Ця умова гарантує, що шлях трансформації містить усі точки обох часових рядів, що аналізуються.

2. Умова неперервності: будь-які два суміжних елементи шляху трансформації $w_q = s_{uv}$ і $w_{q+1} = s_{u'v'}$ знаходяться за принципом $u - u' \leq 1$ та $v - v' \leq 1$. Ця умова забезпечує обмеження на один крок при виборі наступного елемента шляху.

3. Умова монотонності: будь-які два суміжних елементи шляху трансформації $w_q = s_{uv}$ і $w_{q-1} = s_{u''v''}$ знаходяться за принципом $u - u'' \leq 0$ та $v - v'' \leq 0$. Ця умова гарантує, що шлях трансформації не має повертатись назад до вже пройденої точки.

4. Шлях трансформації повинен задовольняти умові мінімальної вартості $CW = \min\left(\frac{1}{k}\left|\sum w_q\right|\right)$.

Результати порівняння за допомогою DTW-алгоритму часових рядів, що відповідають парольній фразі «weekend_started_for_me_on_thursday» довжиною 35 символів для одного користувача та двох користувачів наведено на рис. 2, а) та рис. 2, б) відповідно. Розрахунки проводились в пакеті Matlab. В якості інформативних часових параметрів використовувалась відносна тривалість утримання першої клавіші диграфу (подвійної події клавіатури) до тривалості диграфу. Як можна побачити з рис. 2, вартість шляху трансформації у випадку порівняння двох парольних фраз, що вводив один і той же користувач, досить мала. В той же час вартість шляху трансформації парольних фраз, що вводили різні користувачі, досить велика.



а) б)

Рисунок 2

Перелік джерел посилання: 1. Vintsyuk, T. K. «Speech discrimination by dynamic programming». Kibernetika, Vol. 4, pp. 81-88, Jan.-Feb. 1968. 2. Alieksieiev Vasyl, Elena Sharapova, Olena Ivanova, Gorelov Denis, Synytsia Yuliia. Web-Based Application to Collect and Analyze Users Data for Keystroke Biometric Authentication. In Proceedings of the First IEEE Ukraine Conference on Electrical and Computer Engineering (UKRCON). Pages 917-922, 2017.