УДК 621.384.3

**І. І. Данилюк, В. В. Карпінець, А. В. Приймак,
Ю. Є. Яремчук, О. І. Костюченко**
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж

Проведено експериментальне дослідження можливості використання дворівненої нейромережі з вбудованою сигмоїдною активаційною функцією для покращення точності ідентифікації користувача за клавіатурним почерком, а також проведено порівняння запропонованого методу ідентифікації з існуючими. Отримані результати показали, що запропонований метод має кращу точність ідентифікації на 1–15 %.

Ключові слова: *захист інформації, ідентифікація користувача, нейронна мережа, клавіатурний почерк, часові функції.*

Вступ

З розвитком новітніх технологій проблема інформаційної безпеки набуває все більшої актуальності. Зважаючи на розвиток шпигунських технологій і цифрової техніки, котрі дозволяють усе більш ефективно проводити атаки на комп'ютерні системи, зокрема корпоративні мережі, досягти конфіденційності можна тільки шляхом створення комплексного захисту інформації. І одним із основних елементів такої системи захисту є підсистема, що забезпечує ідентифікацію користувача комп'ютера.

Традиційні методи ідентифікації та автентифікації, що базуються на використанні карток, електронних ключів чи інших переносних ідентифікаторів, а також паролів і кодів доступу, мають суттєві недоліки. Головним недоліком таких методів є неоднозначність ідентифікованої особистості. Для ідентифікації використовують атрибутивні розпізнавальні характеристики. Цей недолік можна усунути, використовуючи біометричні методи ідентифікації, наприклад, динаміку натискання клавіш користувачем. Біометричні характеристики є невід'ємною частиною людини і тому їх не можна забути, загубити чи передати іншому. Ще одним не менш важливим недоліком традиційних методів ідентифікації є складність виявлення підміни ідентифікованого користувача [1].

Динаміка натискання клавіш, що представляє ритми набору тексту, яку користувач виконує під час набору тексту на клавіатурі, забезпечує високий рівень безпеки, а також має переваги у практичному застосуванні, оскільки недорога реалізація даного методу є важливим показником порівняно зі скануванням відбитків пальців чи райдужної оболонки ока, які потребують додаткового обладнання для досягнення ідентифікації [2].

В останні роки спостерігається вибух інтересу до нейронних мереж, які успішно застосовуються в різних галузях — бізнесі, медицині, техніці, геології, фізиці. Нейронні мережі увійшли в практику скрізь, де потрібно розв'язувати завдання прогнозування, класифікації або прийняття рішень. Застосування нейромережевого підходу до задачі ідентифікації дозволяє покращити точність визначення користувача, оскільки даний підхід має властивість фільтрації випадкових перешкод, які присутні у вхідних даних, що дозволяє відмовитися від алгоритмів згладжування експериментальних залежностей, які необхідні при статистичній обробці даних [3].

Методами ідентифікації користувача за клавіатурним почерком займаються порівняно недавно. Автором однієї з перших робіт є Гейнс [4], який у 1980 р. провів ряд експериментів із сімома секретарями. Він їх запросив набрати одні й ті ж самі два параграфи два рази з перервою у 4 місяці. Як результат було зібрано та проаналізовано обмежену кількість біграм. З них обрані були лише ті, частота появи яких перевершувала 10. Порівняння зразків відбувалося, виходячи з припущення, що час затримання та відхилення усіх біграм повинні бути повністю еквівалентні.

Авторами іншої роботи є Леггет, Умпресс і Вільямс [5]. Вони проводили експеримент із 17 програмістами, використавши виміряні інтервали між натисканням клавіш, відомі як диграфи. Перша множина складалася з 1400 символів і використовувалася на стадії навчання, друга множина складалася з 300 символів і використовувалася для перевірки. У своїй доповіді Леггет указав коефіцієнт вірогідності автентифікації — 89,5%. У своїх експериментах автори припустили можливе відхилення середнього часу затримання біграм рівним 0,5, користувач уважався впізнаним, якщо 60 % і більше тимчасових затримок збігались із припустимим відхиленням зі зразком.

Також деякі роботи у цій області були проведені Гарсіом, Янгом і Хємоном [6]. У підході була використана матриця співзмін векторів зв'язаних затримок як величина (параметр), в якій містяться дані про індивідуальний почерк. Потім використовувалася функція відстані Махаланобіса, щоб визначити подібність між почерком, що ідентифікується, і профілем користувача. На відміну від інших, Янг і Хаммон використали Евклідову відстань між двома векторами для порівняння кількості атрибутів.

Відома робота Ріка Джойса й Гупта Гопала [7], в якій запропоновано метод, що заснований на використанні інформації про тимчасові затримки між натисканнями клавіш, отримані під час уведення логіна в модифікованій процедурі ідентифікації. Цій системі необхідно, щоб кожен новий користувач вісім разів уводив логін і пароль. За час верифікації користувач надає зразок випробуваного почерку T, що порівнюється з M (зразок почерку), щоб визначити величину різниці між двома профілями. Дані $M = \{m_1, m_2, m_3 ... m_n\}$ і $T = \{t_1, t_2, t_3 ... m_n\}$, де n — загальна

кількість затримок у почерку, функція, що верифікується, розраховує величину різниці як норму $L1$. Ідентифікація вважається позитивною, якщо ця різниця не перевищує певного порогу змінюваності почерку. Середня та стандартна різниці норм дорівнює $|M - S_i|$, де S_i — один з восьми пробних почерків, які використовуються, щоб визначити поріг прийнятної різниці векторів між даними T і M. Результати вірогідності приводяться у значенні 78 %.

Відома робота С.П. Расторгуєва [8]. У своїй монографії автор процедуру ідентифікації розділив на два види. Перший вид — це парольна ідентифікація, де користувач за парольною фразою проходить процедуру автентифікації, другий вид — ідентифікація користувачів за набором випадкової фрази. А також виділив два режими процедури ідентифікації: процедуру настроювання системи та процедуру автентифікації.

При ідентифікації користувачів за набором вільного тексту в режимі налаштування системи ідентифікації клавіатуру розділили на чотири частини. При роботі користувача за клавіатурою обчислювалися тимчасові інтервали між цими чотирма частинами незалежно від того, яка клавіша була натиснута у цих частинах. У режимі ідентифікації поточні значення порівнювалися з еталонними, і система приймала рішення. Одним із припущень було те, що розподіл тимчасових характеристик користувачів представлявся нормальним ґаусівським законом. Також у роботі було представлено алгоритми виключення грубих помилок, налаштування системи й ідентифікації [9].

Інша відома робота Сакета Махешварі та Вікрама Пуді [10], в якій запропоновано метод ідентифікації користувача за клавіатурним почерком на основі п’ятирівневої нейронної мережі. Також у своїй монографії автори детально дослідили можливість використання трьох різних методів побудови архітектури нейронної мережі (метод виключення, метод випрямлення, метод пакетної нормалізації). Дослідження показали, що гранична точність ідентифікації користувачів складає 85,22–93,59 %. Хоча варто зазначити, що найкращий результат точності було досягнуто шляхом використання п’ятирівневої нейронної мережі, що значно збільшує час навчання даної мережі (до 9 хвилин) на одного користувача.

Робота Нура Ханура [11] зосереджена на використанні інтервалу часу між натисканнями клавіш як особливості набору символів окремих осіб для розпізнавання автентичних користувачів. Для навчання та перевірки функцій використовується чотирирівнева нейронна мережа з багатолінійним персептроном (MLP) із вбудованим методом зворотного поширення помилки (BP). Результати такого дослідження показали, що точність ідентифікації користувача лежить у межах 90–92 %.

Більшість розглянутих робіт базуються на основі геометричних методів розпізнавання, використовуючи різноманітну міру близькості між зразком почерку та його еталоном (Евклідова, Махаланобіса і т.д.). Гранична знайдена вірогідність ідентифікації таких систем становить 90 %. Методи, що базуються на використанні нейронної мережі, мають вищі показники точності (85,22–93,59 %), але варто зазначити, що дослідження проводилися з використанням багаторівневих нейронних мереж, що суттєво впливало на швидкість їхнього навчання.

Результати порівняння точності ідентифікації користувача існуючими методами представлено в таблиці.

Порівняльна характеристика існуючих методів

Назва методу	Точність, %
Метод Леггета, Умпресса і Вільямса	89,5
Метод Джойса й Гопала	78
Метод Расторгуєва	90
Метод Сакета Махешварі та Вікрама Пуді	85,22–93,59
Метод Нура Ханура	90–92

Виходячи з аналізу існуючих методів ідентифікації користувача за клавіатурним почерком, видно, що точність ідентифікації знаходиться в межах від 78 % до 93,59 %, тому залишається актуальним підвищення точності ідентифікації і розробки відповідного методу.

Постановка задачі та методика дослідження

Провести експериментальне дослідження можливості використання дворівневої нейромережі з вбудованою сигмоїдною активаційною функцією для покращення точності ідентифікації користувача за клавіатурним почерком та зменшення часу навчання нейронної мережі, а також запропонувати метод на основі даного математичного апарату. Також провести порівняння запропонованого методу ідентифікації з існуючими.

Метод ідентифікації користувача за клавіатурним почерком

Для дослідження було обрано архітектуру нейромережі, яка являє собою дворівневу систему прямого доступу до мережі з 70-ма сигмовидними прихованими нейронами та 10-ма сигмовидними вихідними нейронами, з використанням сигмоїдної активаційної функції, оскільки основне розрахункове навантаження лягає на нейрони прихованого шару.

Пропонується метод, що включає у себе дев’ять основних етапів збору інформації за допомогою часових функцій і подальшої її обробки на основі навченої нейромережі для ідентифікації користувача за клавіатурним почерком. Основні етапи такі:

1) збір усіх необхідних даних;
2) підготовка та нормалізація даних;
3) робота функцій синхронізації;
4) основний аналіз компонентів;
5) автоматичний підбір параметрів навчання;
6) навчання мережі;
7) перевірка правильності навчання;
8) коригування параметрів;
9) готовність до подальшого використання.

Для збору інформації метод, що пропонується, містить п’ять часових функцій (час затримки, затримка «вгору-вниз», затримка «вниз-вниз», затримка «вгору-вгору», загальний час), які проводять збір інформації, що необхідна для порівняння та ідентифікації користувача нейромережею. Це такі п’ять часових функцій:

1) час затримки — час натискання клавіші, який визначається таким рівнянням:

$$KeyDuration = R_i - P_i,$$

де R_i — час відпускання *i*-ї клавіші; P_i — час натискання *i*-ї клавіші;

2) затримка «вгору-вниз» — різниця у часі між відпусканням клавіші та натисканням наступної клавіші:

$$UpDownLate = P_{i+1} - R_i;$$

3) затримка «вниз-вниз» — різниця у часі між відпусканням однієї і тієї ж клавіші двічі:

$$DownDownaLatency = P_{i+1} - P_i;$$

4) затримка «вгору-вгору» — різниця у часі між натисканням однієї і тієї ж клавіші двічі:

$$UpUpLatency = R_{i+1} - R_i;$$

5) загальний час — час, що необхідний для введення всього тексту:

$$TotalTyping = R_{i=N} - P_{i=1},$$

де N — число символів у тексті.

Для подальшої обробки зібраної інформації пропонується використати нейромережу.

Для вирішення поставленого завдання ідентифікації необхідно обчислювати вирази за заданими параметрами. Математично нейрон являє собою зважений суматор, єдиний вихід якого визначається через його входи та матрицю ваги таким чином, що

$$y = f(u),\ u = \sum_{i=1}^{2} w_i x_i + w_0 x_0,$$

де $f(u)$ — функція активації; u — індуковане локальне поле; w_i — вага входу; x_i — сигнал на вході нейрона; w_0 — додатковий вхід; x_0 — відповідна йому вага.

Нехай кількість вхідних параметрів дорівнює двом. Для початку необхідно дослідити один прихований шар нейронів. Кількість елементів на ньому доцільно визначати за допомогою формули Арнольда-Колмогорова-Хехт Нельсона:

$$\frac{N_y Q}{1+\log_2(Q)} \le N_w \le N_y\left(\frac{Q}{N_x}+1\right)\left(N_x + N_y + 1\right) + N_y,$$

де N_y — розмірність вихідного сигналу; Q — число елементів множини навчальних прикладів; N_w — необхідне число синаптичних зв'язків; N_x — розмірність вхідного сигналу.

Виконавши обчислення, можна зробити висновок, що необхідна кількість синаптичних зв'язків знаходиться у діапазоні $7 < N_w < 20$. Для того щоб дізнатися кількість необхідних нейронів у прихованому шарі, необхідно скористатися формулою:

$$N = \frac{N_w}{N_x + N_y}.$$

Таким чином, кількість нейронів у прихованому шарі буде в діапазоні $1 < N < 70$. Для дослідження усього діапазону потрібно вибрати ту кількість нейронів на прихованому шарі, при якому помилка навчання буде менше. У даному випадку буде доцільно вибрати 70 нейронів на прихованому шарі.

Також ще слід вибрати активаційні функції для кожного шару. Нейрони вхідного та вихідного шарів відповідають тільки за введення та виведення даних, їхні функції можна залишити лінійними. Основне розрахункове навантаження лягає на нейрони прихованого шару, тому його активаційну функцію слід зробити сигмоїдною.

У нейронних мережах прямого поширення синаптичні зв'язки організовані таким чином, що кожний нейрон даного рівня ієрархії сприймає інформацію тільки від деякої непустої множини нейронів, які розташовані на більш низькому рівні. Назва мереж вказує на те, що у них існує виділений напрям поширення сигналів, які рухаються, починаючи з входу, через один або декілька прихованих шарів до вихідного шару. Легко помітити, що багатошарова нейронна мережа може бути отримана шляхом каскадного об'єднання одношарових мереж з матрицями вагових коефіцієнтів $W^1, W^2, \ldots, W^p$, де p — кількість шарів нейронної мережі.

У випадку лінійності активаційних функцій багатошарова нейронна мережа може бути зведена до еквівалентної одношарової з матрицею вагових коефіцієнтів $W = W^1 * W^2 * \ldots * W^p$, тому формування подібних структур має сенс тільки у випадку застосування у нейронах нелінійних активаційних функцій.

Запропонована нейронна мережа, яка являє собою двошарову систему прямого доступу до мережі з 70-ма сигмовидними прихованими нейронами та 10-ма сигмовидними вихідними нейронами, представлена на рис. 1.

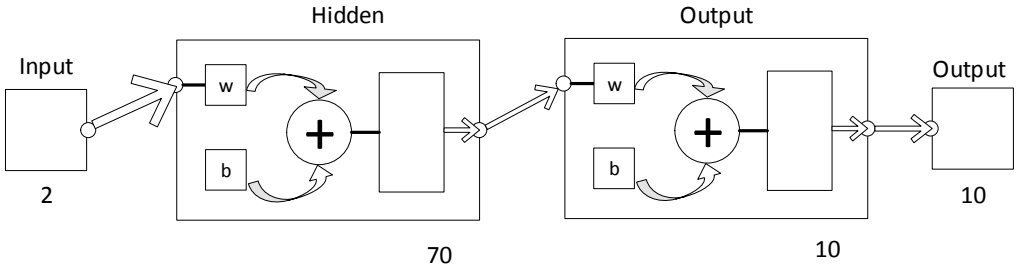

Рис. 1. Запропонована архітектура нейромережі

Детальна схема запропонованої нейромережі представлена на рис. 2.

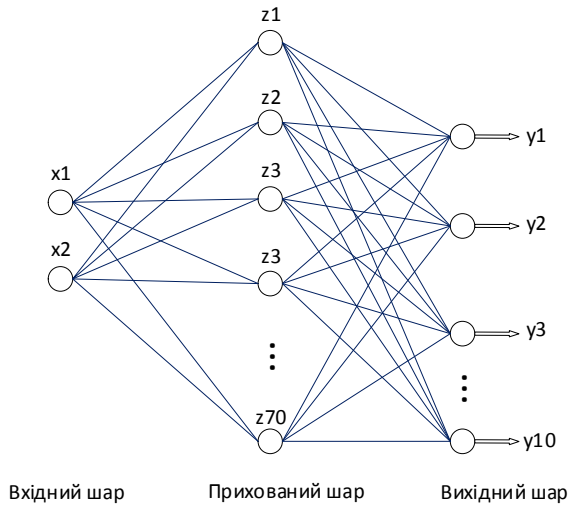

Рис. 2. Розгорнута схема запропонованої архітектури нейромережі

Вхідними даними для мережі буде час утримання клавіш і тимчасові інтервали між натисканням клавіш.

Навчання здійснюється наступним чином.

1. Рандомізуються всі ваги мережі у малі величини.

2. На вхід мережі подається вхідний навчальний вектор X та обчислюється сигнал NET від кожного нейрона, використовуючи стандартний вираз

$$NET_j = \sum_i xw.$$

3. Обчислюється значення порогової функції активації для сигналу NET від кожного нейрона.

4. Обчислюється помилка для кожного нейрона за допомогою віднімання отриманого виходу з необхідного виходу:

$$error_j = target_j - OUT_j.$$

5. Кожна вага модифікується у такий спосіб:

$$W_{ij}(t+1) = w_{ij}(t) + a_x error_j.$$

6. Повторюються кроки з другого до п’ятого доти, поки помилка не стане досить малою.

Блок-схему роботи запропонованого методу ідентифікації користувача за клавіатурним почерком на основі нейромережі представлено на рис. 3.

Після того як зареєстрований користувач захоче отримати доступ до системи, йому необхідно буде ввести 2 рази ключовий текст. Під час введення тексту, функції синхронізації будуть перевіряти правильність введення та порівнювати їх із шаблонами зареєстрованих користувачів. Після цього доступ користувачу дозволяється або забороняється.

Для проходження реєстрації користувач вводить ключові фрази 2 рази. Під час введення ключових фраз функції синхронізації аналізують текст, який вводить

користувач. Отримані дані додаються до векторних функцій, а потім одразу зберігаються у вигляді шаблонів до бази даних, для того щоб перевіряти їх під час входу до системи. Функції синхронізації будуть перевіряти правильність вводу та порівнювати їх з шаблонами зареєстрованих користувачів. Після цього доступ користувачу дозволяється або забороняється.

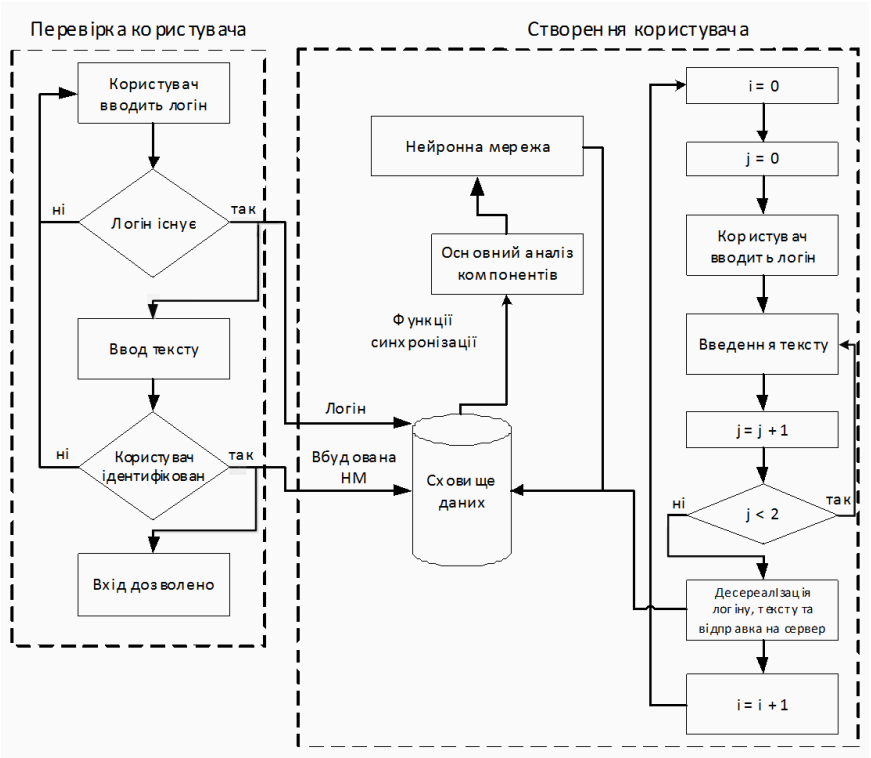

Рис. 3. Блок-схема роботи запропонованого методу

Основний аналіз головних компонентів виконується за функціями синхронізації для того, щоб зменшити їх, перш ніж вони будуть служити вхідними даними для нейронної мережі. Після того як користувач створений, він повинен провести навчання нейронної мережі, яка також зберігається в базі даних. Після цих кроків навчена нейронна мережа та шаблони функцій готові до ідентифікації користувача.

Провівши експериментальні тести за участю восьми програмістів, було отримано результат точності, що в середньому становить 93 %. Час навчання нейронної мережі склав 6 хвилин, що є швидшим за існуючі методи ідентифікації користувача за клавіатурним почерком з використанням багаторівневих нейромереж.

Порівнюючи існуючі та запропонований метод ідентифікації користувача за клавіатурним почерком на основі дворівневої нейронної мережі із вбудованою сигмоїдною активаційною функцією, можна зробити висновок, що точність ідентифікації зросла на 1–15 % відносно показників існуючих методів. Метод Сакета Махешварі та Вікрама Пуді має схожі показники точності, але між запропонованим та існуючим методом є декілька суттєвих відмінностей: у своїй роботі Сакет Махешварі та Вікрам Пуді використовували п’ятирівневу нейронну мережу, на навчання якої було необхідно 9 хвилин. У запропонованого методу час навчання

нейронної мережі складає 6 хвилин, що є швидшим на 3 хвилини і, як результат, є значно ефективнішим при використанні, оскільки час ідентифікації користувача зменшується, а висока точність ідентифікації зберігається.

Висновки

Проведено експериментальне дослідження можливості використання дворівневої нейромережі із вбудованою сигмоїдною активаційною функцією для покращення точності ідентифікації користувача за клавіатурним почерком.

На основі спроектованої архітектури дворівневої нейромережі було запропоновано метод ідентифікації користувача за клавіатурним почерком з використання п'яти часових функцій для збору необхідної інформації та вбудованою сигмоїдною активаційною функцією для підвищення ефективності роботи нейронної мережі.

Отримані показники точності ідентифікації користувача становлять 93 %, що є кращим за існуючі методи на 1–15 %. У випадку з розглянутим методом Сакета Махешварі та Вікрама Пуді показники точності майже ідентичні, але за рахунок зменшення часу навчання нейронної мережі на 3 хвилини запропонований метод ідентифікації користувача є більш ефективним.

1. Gavan Leonard Tredoux, Steven J. Harrington. Method and system for providing authentication through aggregate analysis of behavioral and time patterns. Xerox Corporation, Norwalk, CT, 2016.

2. Armin Ebrahimi, Jeff Weitzman. User Identification Management System and Method. ShoCard, Inc., Palo Alto, CA — 15/878,353. 2018.

3. Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira. Learning features for offline handwritten signature verification using deep convolutional neural networks. *Elsevier.* 2017. P. 163–176.

4. Gaines R., Lisowski W., Press S. and Shapiro N. Authentication by Keystroke Timing: Some Preliminary Results. Rand Report R – 256. NSF, Rand Corporation, Santa Monica, C A, 1980.

5. Umphress David & Williams Glen. (1985). Identity verification through keyboard characteristics. *International Journal of Man-Machine Studies*. 23. 263-273. 10.1016/S0020-7373(85)80036-5.

6. Young J.R. and Hammon R.W. Method and Apparatus for Verifying an Individual's Identity. Patent Number 4,805,222, U.S. Patent and Trademark Office, Washington, D.C. Feb., 1989.

7. Joyce R. and Gupta G. User authorization based on keystroke latency. Communications of the ACM. 1990. **33**(2). P. 168–176.

8. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. Москва: Изд-во Агентства «Яхтсмен», 1993. 188 с.

9. Лупенко С.А., Шаблій Н.Р., Лупенко А.М. Компаративний аналіз моделей, методів та засобів аутентифікації особи в інформаційних системах за її клавіатурним почерком. Lviv polytechnic national university institutional repository, 2014. С. 141–147.

10. Saket Maheshwary, Soumyajit Ganguly, Vikram Pudi. Deep Secure: A Fast and Simple Neural Network based approach for UserAuthentication and Identification via Keystroke Dynamics. Conference: 2017 International Joint Conference on Artificial Intelligence (IJCAI), At Melbourne, Australia, 2017.

11. Harun N., Woo W.L. and Dlay S.S. Performance of KeystrokeBiometrics AuthenticationSystem Using Artificial Neural Network (ANN) and Distance Classifier Method. International Conference on Computer and Communication Engineering (ICCCE 2010). 11–13 May 2010, Kuala Lumpur, Malaysia, 2010.

Надійшла до редакції 02.06.2018