УДК 004.93

**В. В. Куцман**
**О.К.Колесницький**

# ДИНАМІЧНА ІДЕНТИФІКАЦІЯ ПІДПИСУ НА ОСНОВІ СПАЙКІНГОВОЇ НЕЙРНОЇ МЕРЕЖІ

Вінницький національний технічний університет, м. Вінниця

***Аннотация.*** *Запропоновано метод динамічної ідентифікації підпису на основі спайкінговой нейронної мережі. Використовуються три динамічних параметри підпису l(t), xy(t), p(t), які є інваріантними до кута нахилу підпису, а після їх нормалізації - ще й до просторового і часового масштабів підпису. Ці динамічні параметри подаються на спайкінговую нейронну мережу для розпізнавання одночасно у вигляді часових рядів без попереднього перетворення у вектор статичних ознак, що, з одного боку, спрощує метод завдяки відсутності складних обчислювальних процедур перетворення, а з іншого боку, перешкоджає втраті корисної інформації, а тому - підвищує точність і достовірність ідентифікації та розпізнавання підписів. В результати експериментального досліджень програмної реалізації запропонованої системи був знайдений її EER = 3,9% при ідентифікації кваліфіковано підроблених підписів і EER = 0,17% при ідентифікації випадкових підробок.*

***Ключові слова:*** *online ідентиифікація підпису, спайкінгова нейронна мережа, інваріантні динамічні параметри, розпізнавання підпису, біометрія, контроль доступу*.

Ідентифікація підпису відноситься до біометричних методів аутентифікації і стає все більш популярною для широкого діапазону практичних застосувань, починаючи від запобігання шахрайству у фінансових операціях і закінчуючи контролем доступу до закритих зон. Усі методи ідентифікації підпису можна поділити на 2 великі групи: статична (Offline) ідентифікація підпису та динамічна (Online) ідентифікація підпису. Статична ідентифікація підпису основана на аналізі самого зображення підпису і використовує різноманіntні методи розпізнавання графічних образів. Вона є малонадійною, тому що зображення піпису легко сфальшувати обведенням наявного оригіналу за допомогою копіювального паперу, на просвічення або зробивши скан-копію чи фото-копію. Більш надійною є динамічна ідентифікація підпису (ДІП), оскільки вона передбачає аналіз параметрів коливання пера автора при відтворенні їм підпису.

Незважаючи на великий обсяг досліджень за цією тематикою, створення систем ДІП з потрібною достовірністю і якістю роботи лишається проблематичним. Складності практичного застосування різних інформаційних технологій ДІП викликані недоліками самого явища формування підпису, як об'єкту інформаційного процесу. Так, підпис однієї і тієї ж людини через природню варіабельність почерку людини є нестабільно відтворюваним процесом.

Крім цього, динамічні параметри підпису (координати $X(t)$ та $Y(t)$, тиск пера на графічний планшет $P(t)$ та ін.) часто перетворюють у вектор статичних ознак, які потім використовують у класифікаторах різних типів для отримання результату ідентифікації. При такому перетворенні динамічних параметрів у статичні часто втрачається корисна інформація, що зменшує розбіжність між справжнім та підробленим підписом і тим самим знижує достовірність ідентифікації.

Загальна архітектура запропонованої системи ДІП зображена на рис. 1.

У даному дослідженні ми використали набір із 3 параметрів: 1) відстань $l(t)$ від поточного часового відліку координат пера $(x_i,y_i)$ до наступного $(x_{i+1},y_{i+1})$ (див. рис. 2); 2) добуток координат $X(t)$ та $Y(t)$; 3) тиск пера на графічний планшет $P(t)$. Саме ці параметри були взяті через те, що вони є інваріантними до нахилу написання підпису відносно сторін планшту [1]. А вказана на рис.1 амплітудна та часова нормалізація [1] робить ці параметри ще й інваріантними до просторового та часового масштабів конкретної реалізації підпису та зсуву її розташування на полі планшету. Запропонований метод буде працювати і з іншими параметрами та їх кількістю, але вдалий вибір набору параметрів позитивно впливає на загальну якість роботи системи.

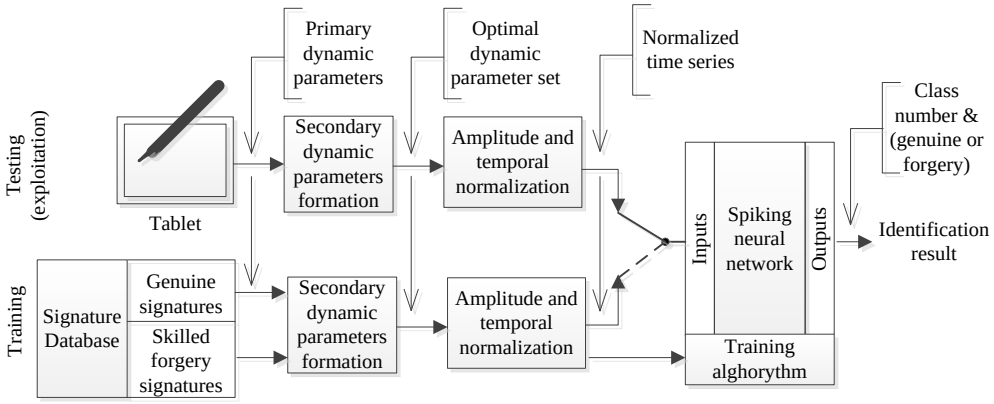


Рис. 1 - Архітектура запропонованої системи динамічної ідентифікації підписів на основі спайкінгової нейронної мережі

Після нормалізації ми маємо часові ряди, які являють собою послідовності оцифрованих відліків відповідних динамічних параметрів у дискретні моменти часу із певним часовим кроком. Ці часові ряди подають на вхід попередньо навченої спайкінгової нейронної мережі.

Спайкінгова нейромережа має бути попередньо навчена задачі класифікації часових рядів (динамічних параметрів підпису), тому на її виході ми отримуємо результат ідентифікації підпису у вигляді номеру класу (ідентифікатор підписанта). А оскільки на кожний клас запропонована спайкінгова нейромережа має 2 виходи (див. рис.2), то ще маємо інформацію чи є розпізнаний підпис справжнім чи майстерно підробленим.

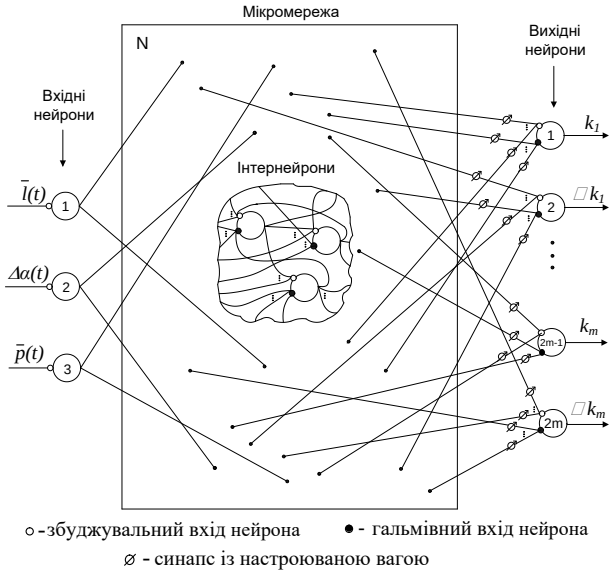


Рисунок 2 – Структура спайкінгової нейронної мережі для Online ідентифікації та розпізнавання підписів

Для навчання спайкінгової нейромережі використовуються справжні підписи користувачів. В принципі, достатньо одного справжнього підпису користувача для навчання, але чим більше справжніх підписів буде використано для навчання, тим точніше буде працювати система. Також у системі передбачено можливість використання майстерно підроблених підписів для навчання. Це не є обов'язковим, але також позитивно впливає на точність ідентифікації.

Для дослідження параметрів якості роботи систем ДІП використовують тестову вибірку, у яку вкючають як справжні підписи, так і підробні, але ті, які не були присутні у навчальній

вибірці. Частіше всього у тестовву вибірку включають і майстерно підроблені (skilled forgery) і випадково підроблені (random forgery) підписи, і прості підробки (simple forgery).

Програмну реалізацію методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі було здійснено на мову програмування Python. Для роботи з нейронними мережами на Python було обрано бібліотеки TensorFlow та Keras.

Для експериментального дослідження параметрів якості роботи запропонованої системи ДІП [3] було обрано БД MCYT-330, яка є частиною DeepSignDB [2].

Розроблена система при тестуванні на майстерно підроблених підписах має EER=3,9%, а найраща із відомих (TARNN) – має EER=4,3%, тобто розроблена система має кращу на 0,4% (абсолютний показник) точність, ніж система TARNN, а у відносних одиницях це (0.4/4.3)*100%=9%. Що стосується тестуванні на випадкових підробках, то із табл. 4 видно, що розроблена система має EER=0,17%, а найраща із відомих (TARNN) – має EER=0,2%, тобто розроблена система має кращу на 0,03% (абсолютний показник) точність, ніж система TARNN, а у відносних одиницях це (0.03/0,17)*100%=15%.. Загалом, у відносних показниках запропонована система за точністю краща за референсну на 9% при тестуванні на майстерних підробках і на 15% при тестуванні на випадкових підробках.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


[1] V. V. Kutsman, O. K. Kolesnytskyj, «Veryfikatsiya ta rozpiznavannia pidpysu jak bahatoparametrychnoho procesu na osnovi spikingovoyi neyronnoyi merezhi», *Information technologies and computer engineering*, issue 50, № 1, p. 36–44, April 2021./

[2] J. Fierrez, J. Galbally, et al., "BiosecurID: A Multimodal Biometric Database", *Pattern Analysis and Applications*, Vol. 13, n. 2, pp. 235-246, May 2010.

[3] O. K. Kolesnytskyj, V. V. Kutsman, K. Skorupski, and M. Arshidinova, “Neurocomputer architecture based on spiking neural network and its optoelectronic implementation”, *Proc. SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2019*, 1117609 (6 November 2019); doi: 10.1117/12.2536607.



***Куцман Владислав Вікторович – аспірант кафедри комп'ютерних наук, інженер-програміст ТОВ «УЛФ-ФІНАНС», тел: +380974672461, email: kutsmanvlad@gmail.com***

***Колесницький Олег Костянтинович – канд. техн. наук, доцент, доцент кафедри комп’ютерних наук, Вінницький національний технічний університет, м. Вінниця, Україна, тел: +380679179718, e-mail: kolesnytskiy@vntu.edu.ua***


## DYNAMIC HANDWRITTEN SIGNATURE IDENTIFICATION BASED ON A SPIKING NEURAL NETWORK


***Abstract.*** *A method of dynamic signature identification based on a spiking neural network is proposed. Three dynamic signature parameters l(t), xy(t), p(t) are used, which are invariant to the angle of inclination of the signature, and after their normalization - even to the spatial and temporal scales of the signature. These dynamic parameters are fed to the spiking neural network for simultaneous recognition as time series without prior conversion into a vector of static features, which, on the one hand, simplifies the method due to the lack of complex computational conversion procedures, and on the other hand prevents the loss of useful information.The method increases the accuracy and reliability of signature identification and recognition. The neural network used has a simple learning procedure, and not all neurons in the network are trained, but only the output ones. If you need to add new signatures, you do not need to retrain the entire network, but just add a few output neurons and teach only their connections. As a result of experimental studies of software implementation of the proposed system was found its EER = 3.9% in the identification of qualified forgeries and EER = 0.17% in the identification of random fakes.*



***Key words:*** *online signature identification, spiking neural network, invariant dynamic parameters, signature recognition, biometrics, access control.*



***Kutsman Vladislav Viktorovich - Postgraduate student of the Department of Computer Science, Software Engineer TOB «УЛФ-ФІНАНС», tel: +380974672461, email: kutsmanvlad@gmail.com***

***Kolesnytskyj Oleh Kostiantynovych - Associate Professor of Computer Science Dpt, Vinnitsa National Technical University, Vinnitsa, Ukraine, tel: +380679179718, e-mail: kolesnytskiy@vntu.edu.ua.***