

УДК 004.93

В. В. Куцман, О. К. Колесницький

ВЕРИФІКАЦІЯ ТА РОЗПІЗНАВАННЯ ПІДПISУ ЯК БАГАТОПАРАМЕТРИЧНОГО ПРОЦЕСУ НА ОСНОВІ СПАЙКІНГОВОЇ НЕЙРОННОЇ МЕРЕЖІ

Вінницький національний технічний університет, Вінниця

Анотація. У статті проведено аналіз відомих методів динамічної верифікації підпису, які зведено у класифікаційну таблицю. Запропоновано метод динамічної верифікації підпису на основі спайкінгової нейронної мережі. Обрано три динамічних параметри підпису $l(t)$, $\Delta\alpha(t)$, $Z(t)$, які є інваріантними до кута нахилу підпису, а після їх нормалізації – ще й до просторового та часового масштабів підпису. Ці динамічні параметри підпису подаються на спайкінгову 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 верифікації та розпізнавання підписів (особливо при розпізнаванні підроблених підписів, які сильно корельовані з оригіналами). Використовувана нейронна мережа має просту процедуру навчання, причому навчаються не всі нейрони мережі, а тільки вихідні. При необхідності додавання нових підписів не потрібно перенавчати всю мережу повністю, а достатньо додати кілька вихідних нейронів і навчити тільки їхні зв'язки.

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

Анотация. В статье проведен обзор известных методов динамической верификации подписи, которые сведены в классификационную таблицу. Предложен метод динамической верификации подписи на основе спайкинговой нейронной сети. Выбраны три динамических параметра подписи $l(t)$, $\Delta\alpha(t)$, $Z(t)$, которые являются инвариантными к углу наклона подписи, а после их нормализации – еще и к пространственному и временному масштабам подписи. Эти динамические параметры подписи подаются на спайкингую нейронную сеть для распознавания одновременно в виде временных рядов без предварительного преобразования в вектор статических признаков, что, с одной стороны, упрощает метод благодаря отсутствию сложных вычислительных процедур преобразования, а с другой стороны, препятствует потере полезной информации, а поэтому – повышает точность и достоверность верификации и распознавания подписей (особенно при распознавании поддельных подписей, которые сильно коррелированы с оригиналами). Используемая нейронная сеть имеет несложную процедуру обучения, причем обучаются не все нейроны сети, а только выходные. При необходимости добавления новых подписей не нужно переучивать всю сеть целиком, а достаточно добавить несколько выходных нейронов и научить только их связи.

Ключевые слова: online верификация подписи, спайкинговая нейронная сеть, инвариантные динамические параметры, распознавание подписи, биометрия, контроль доступа.

Abstract. The article reviews the known methods of dynamic signature verification, which are summarized in the classification table. A method of dynamic signature verification based on a spiking neural network is proposed. Three dynamic parameters of the signature $l(t)$, $\Delta\alpha(t)$, $Z(t)$ are chosen, which are invariant to the angle of inclination of the signature, and after their normalization – also to the spatial and temporal scales of the signature. These dynamic signature parameters are simultaneously fed to the spiking neural network for recognition in the form of time series without prior conversion into a vector of static features. This, on the one hand, simplifies the method due to the absence of complex computational conversion procedures and, on the other hand, prevents the loss of useful information and therefore increases the accuracy and reliability of signature verification and recognition (especially for forgery signatures that are highly correlated with genuine ones). The used neural network has a simple learning procedure, and not all neurons of the network are trained, but only the output neurons. If you need to add new signatures, you do not need to retrain the entire network, but just add a few output neurons and learn only their connections.

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

DOI: <https://doi.org/10.31649/1999-9941-2021-50-1-36-44>.

Вступ

Біометричні методи аутентифікації, включаючи ідентифікацію голосу, відбитків пальців, розпізнавання обличчя, сканування сітківки ока та перевірка підпису стають все більш популярними для широкого діапазону практичних застосувань, починаючи від контролю доступу до закритих зон і закінчуючи за-побіганням шахрайству у фінансових операціях. Верифікація підпису має особливо важливе значення, оскільки вона є загальноприйнятим методом схвалення фінансових операцій. Важлива перевага підпису над іншими біометричними показниками – це давня стійка традиція його використання у багатьох розповсюджених завданнях верифікації. Він використовується десятки років у повсякденному житті і є дуже зручним.

Усі методи верифікації підпису можна поділити на 2 великі групи: статична (Offline) верифікація підпису та динамічна (Online) верифікація підпису [1,2]. Статична верифікація підпису основана на аналізі самого зображення підпису і використовує різноманітні методи розпізнавання графічних образів. Вона є малонадійною, тому що зображення підпису легко сфальшувати обведенням наявного оригіналу за допомогою копіювального паперу, на просвічення або зробивши скан-копію чи фото-копію. Більш надійною є динамічна верифікація підпису, оскільки вона передбачає аналіз параметрів коливання пера автора при відтворенні їм підпису. У найпростішому випадку такими параметрами динаміки відтворення підпису можуть бути три функції часу: дві функції зміни координати $X(t)$ та координати $Y(t)$ коливань пера в площині графічного планшета і ще одна функція – зміна тиску пера на графічний

планшет $Z(t)$. Навіть якщо зловмисник навчиться відтворювати графічно схожий на оригінал підпис, навряд чи він зможе у точності відтворити динаміку рухів автора підпису, тому що вона є індивідуальною для кожної людини. Тому найбільш перспективною є динамічна (On-line) верифікація підпису. До того ж вона максимально придатна до реалізації сучасними засобами інформаційних технологій і перевершує можливості людини-оператора в цьому процесі.

Актуальність

Незважаючи на великий обсяг досліджень за цією тематикою, створення систем динамічної (Online) верифікації підпису з потрібною достовірністю і якістю роботи лишається проблематичним. Складності практичного застосування різних інформаційних технологій динамічної (Online) верифікації підпису 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 і має такі недоліки [3]:

- варіабельність геометричних розмірів (просторового масштабу) різних реалізацій підпису;
- варіабельність часу написання (часового масштабу) різних реалізацій підпису;
- варіабельність кута нахилу підпису відносно сторін планшету різних реалізацій підпису.

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

Часто наряду з верифікацією виникає задача розпізнавання підпису, а точніше – парольного слова. Тобто, потрібно не просто підтвердити наперед відому особу за її підписом, а розпізнати хто саме ця особа із переліку валідних осіб за написанням слова-пароллю. Задача розпізнавання підпису є більш складною за задачу верифікації і вимагає більш складних і потужних методів та засобів класифікації.

Мета

Мета статті – представити новий метод динамічної верифікації підпису, що базується на використанні динамічних параметрів процесу підпису (без їх перетворення у статичні параметри) і спайкінгових нейронних мереж, та дозволяє спростити процес і підвищити достовірність верифікації підпису.

Задачі

1. Проаналізувати загальну схему динамічної верифікації підпису.
2. Провести аналітичний огляд і класифікацію існуючих методів динамічної верифікації підпису.
3. Розробити метод Online верифікації підпису на основі динамічних параметрів підпису та спайкінгових нейронних мереж.
4. Сформулювати переваги запропонованого методу.

Загальна схема динамічної верифікації підпису

Загальна схема динамічної верифікації підпису зображена на рис. 1. Користувач здійснює процес написання підпису на графічному планшеті, який видає такі динамічні параметри підпису: координати $X(t)$ та $Y(t)$, тиск пера на графічний планшет $Z(t)$ та ін. Ці параметри видаються у вигляді оцифрованих відліків відповідних величин у дискретні моменти часу із певним часовим кроком.

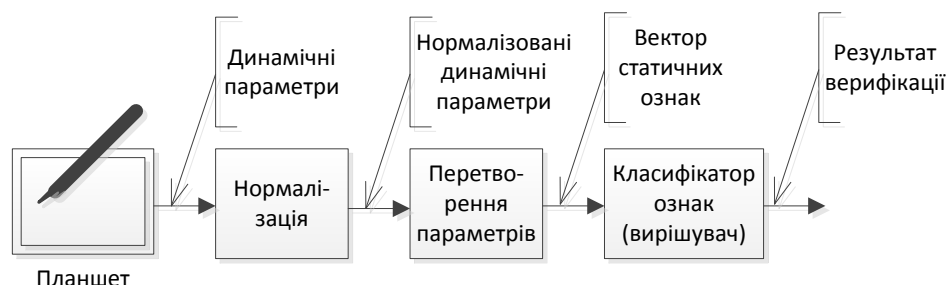


Рисунок 1 – Загальна схема динамічної верифікації підпису

Оскільки різні реалізації підпису однієї особи відрізняються за масштабом, часом і нахилом, то їх нормалізують (приводять до єдиного масштабу по простору, часу та нахилу). Потім для нормалізованих динамічних параметрів виконують функцію перетворення у вектор статичних ознак. Як перетворення часто використовують перетворення Фур'є [3], Уолша [2], Хаара [2], вейвлет [4], сплайни [5] та ін. У результаті отримують вектор чисел (статичних ознак), які потім використовуються у класифікаторах

різних типів для отримання результату верифікації. Як класифікатори використовують структурні, статистичні, нейромережеві та ін.,

Які слабкі місця такої схеми верифікації? По-перше, при перетворенні динамічних параметрів у статичні втрачається велика частина корисної інформації, що знижує достовірність верифікації. По-друге, достовірність верифікації дуже залежить від обраної пари (вид перетворення)-(вид класифікатора). А якщо для класифікації використовувати динамічні параметри без їх перетворення у статичний вектор, то потрібні і динамічні класифікатори, тобто класифікатори часових рядів, які є набагато складнішими.

Аналітичний огляд і класифікація існуючих методів динамічної верифікації підпису

У науковій літературі наведено детальний аналіз методів і засобів верифікації підписів [1,2]. Але для наочності варто було б розробити класифікаційну таблицю. Головною класифікаційною ознакою є вид процесу верифікації підпису: статична (Offline) або динамічна (Online) верифікація підпису. Класифікаційна таблиця методів верифікації підписів зображена на рис. 2. Статична (Offline) верифікації підписів є менш перспективною, тому в рамках цієї статті не розглядається.

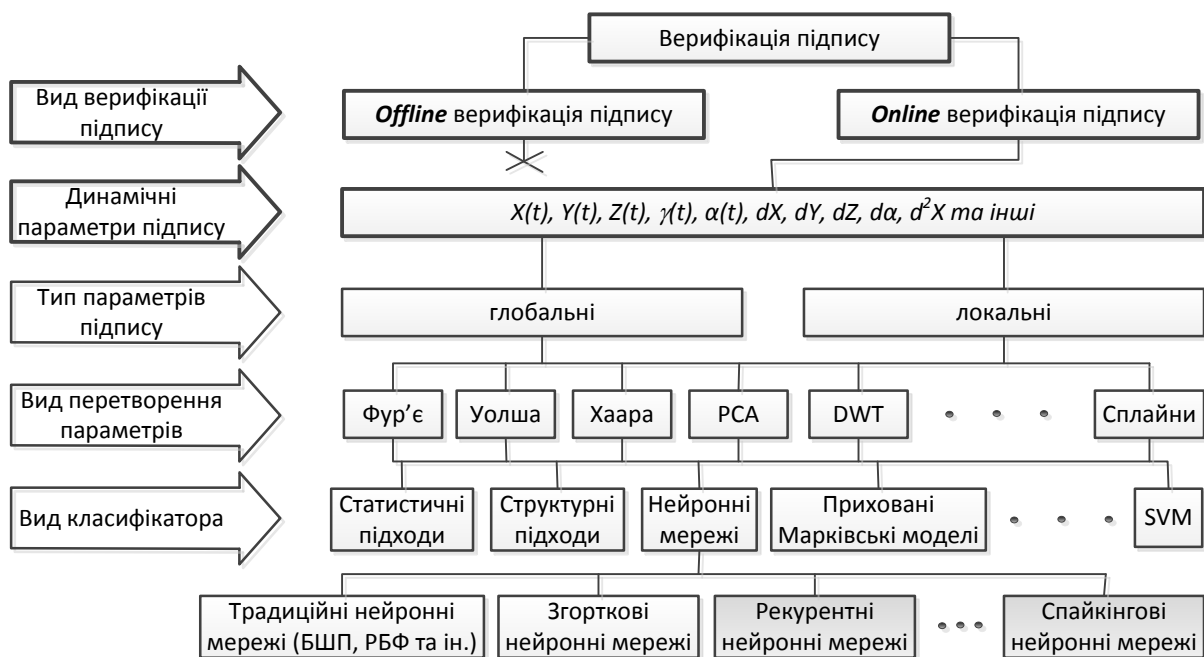


Рисунок 2 – Класифікаційна таблиця методів верифікації підписів

Динамічну (Online) верифікацію підпису можна класифікувати за такими ознаками:

1) *Динамічні параметри підпису.* Взагалі, більшість графічних планшетів видає такі динамічні параметри підпису як координати $X(t)$ та $Y(t)$, тиск пера на графічний планшет $Z(t)$, кут нахилу пера до площини планшета $\gamma(t)$, азимут руху пера $\alpha(t)$. Із цих основних динамічних параметрів часто пропонують отримувати похідні параметри та використовувати їх. Такими похідними параметрами пропонують брати швидкості зміни координат ($v_x=dX/dt, v_y=dY/dt$), прискорення зміни координат ($a_x=dv_x/dt, a_y=dv_y/dt$), а також різноманітні дискретні ознаки, наприклад, кількість максимумів, мінімумів, опуклих та увігнутих ділянок та ін. Беруться не одночасно всі динамічні параметри, а певні їх набори. Навіть проводяться дослідження по порівнянню інформативності різних динамічних параметрів та їх стійкості до інтраперсональної варіабельності підписів [6].

2) *Тип параметрів підпису.* У більшості робіт використовують глобальні динамічні параметри підпису, тобто часові ряди обраних параметрів за всю тривалість підпису. У деяких роботах використовують локальні фрагменти динамічних параметрів у певному часовому діапазоні, або на певних виділених характерних ділянках підпису. Також використовують такі локальні параметри як центри мас або моменти різних порядків [7].

3) *Вид перетворення параметрів.* Динамічні параметри підпису є функціями від часу, тому у такому вигляді їх важко класифікувати. Легше процес класифікації здійснювати над векторами чисел, тому із динамічних параметрів виділяють певні «ознаки», які є числами і замінюють функції від часу (часові ряди) набором чисел (числовим вектором). Для переходу від функцій часу до числових векторів ознак використовують різні види перетворень: Фур'є [3], Уолша [2], Хаара [2], виділення головних компонент (Principal Component Analysis – PCA [8]), дискретне вейвлет-перетворення (DWT) [4], сплайни [5] та ін.

4) Вид класифікатора. Після того як процес підписування закодовано у вигляді числового вектора ознак, його можна класифікувати будь-яким із відомих методів класифікації. Найпростішим є метод порівняння з еталоном, при якому обчислюються певні міри схожості векторів [9] (Евклідова, Махалонобіса та ін.). Більше переваг мають методи на основі прихованих марковських моделей [10], машин опорних векторів (support vector machine – SVM) [11] та штучних нейронних мереж (ШНМ) [4,8]. Останні все частіше використовуються у процесі Online верифікації підпису. В останні роки спостерігається перехід від традиційних ШНМ (багатошаровий перцептрон – БШП, РБФ та нейро-нечіткі [12]) до сучасних парадигм ШНМ (згорткові [13], рекурентні [14], спайкінгові [15]). Найперспективнішими є рекурентні та спайкінгові нейронні мережі, оскільки вони дозволяють класифікувати функції часу (часові ряди) як вони є без перетворення у вектори статичних ознак.

Було знайдено 2 публікації [15,16] про верифікацію підпису на основі спайкінгових ШНМ, де використовуються зовсім інші структури спайкінгових ШНМ, на інших моделях спайкінгових нейронів та з іншим набором динамічних параметрів підпису, ніж пропонується у цій статті.

Метод динамічної верифікації підпису на основі спайкінгових нейронних мереж

Вибір динамічних параметрів підпису.

Такі динамічні параметри підпису як координати $X(t)$ та $Y(t)$ не є інваріантними до просторового та часового масштабу підпису, а також до нахилу написання. Тому пропонується використовувати відстань від поточного часового відліку координат пера (x_i, y_i) до наступного (x_{i+1}, y_{i+1}) (див. рис. 3а). Тобто, згідно теореми Піфагора:

$$l_i = \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2} \quad (1.1)$$

Якщо координати $X(t)$ та $Y(t)$ знімаються з часовим кроком Δt і під час написання підпису їх буде N , то значень l_i буде отримано $(N-1)$. Залежність $l(t)$ буде інваріантна до кута нахилу підпису, але деякі неточності будуть мати місце через квадратну координатну сітку. Інваріантність залежності $l(t)$ до просторового та часового масштабів можна забезпечити її подальшою нормалізацією. Якщо взяти відношення $l_i/\Delta t$, то це буде швидкість пера на відрізьку між точками (x_i, y_i) та (x_{i+1}, y_{i+1}) . А поскільки всі Δt однакові, то l_i є пропорційною швидкості пера на відрізьку $[(x_i, y_i); (x_{i+1}, y_{i+1})]$. При $\Delta t \rightarrow 0$ величина l_i пропорційна миттєвій швидкості пера у точці (x_i, y_i) . Якщо миттєву швидкість пера розглядати як вектор (однозначно визначається довжиною та кутом нахилу до осі абсцисс), то залежність його довжини $l(t)$ та залежність кута нахилу $\alpha(t)$ до осі абсцисс будуть однозначно визначати намальований графічний образ з урахуванням динаміки його написання. Іншими словами, динаміка лінійної та кутової швидкості пера однозначно визначає не тільки намальовану фігуру, але і «особливості» її написання. Але залежність $\alpha(t)$ не буде інваріантна до нахилу всього підпису відносно осі абсцисс. Саме тому краще брати різницю $\Delta\alpha_i$ сусідніх кутів α_{i+1} і α_i .

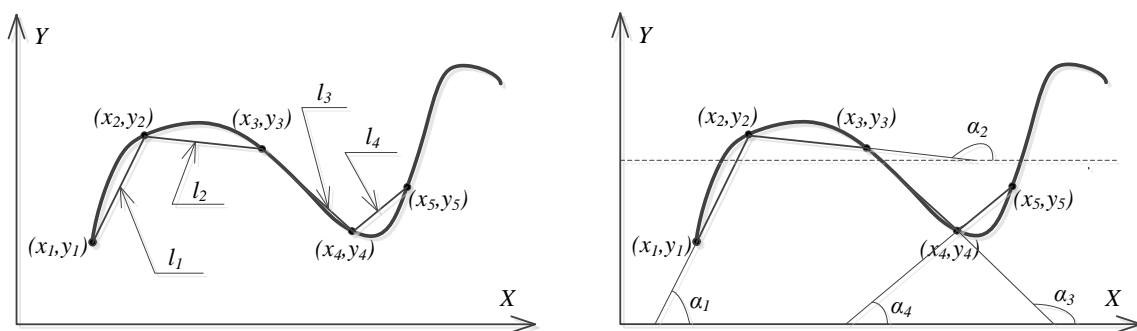


Рисунок 3 – Отримання динамічних параметрів підпису $L(t)$ та $\Delta\alpha(t)$

На основі вищесказаного другим динамічним параметром підпису оберемо різницю кутів $\Delta\alpha_i = \alpha_{i+1} - \alpha_i$ нахилу двох сусідніх відрізків, що з'єднують дискретні точки (просторові відліки) підпису (див. рис. 3б). Кут α_i знаходиться із прямокутного трикутника, катетами якого є різниці координат точок (x_{i+1}, y_{i+1}) та (x_i, y_i) .

Якщо координати $X(t)$ та $Y(t)$ знімаються з часовим кроком Δt та під час написання підпису їх буде N , то значень α_i буде отримано $(N-1)$, а значень $\Delta\alpha_i$ – $(N-2)$. Залежність $\Delta\alpha(t)$ буде інваріантна до кута нахилу підпису, але деякі неточності будуть мати місце через квадратну координатну сітку.

Інваріантність залежності $\Delta\alpha(t)$ до просторового та часового масштабу можна забезпечити її подальшою нормалізацією.

Третім динамічним параметром підпису оберемо тиск пера на графічний планшет $Z(t)$. Залежність $Z(t)$ є інваріантною до кута нахилу підпису. Інваріантність залежності $Z(t)$ до часового масштабу можна забезпечити її подальшою нормалізацією. Крім того, є гіпотеза, що можна буде забезпечити деяку інваріантність залежності $Z(t)$ до емоційного та фізичного стану людини при її подальшій нормалізації. Імовірно, що у спокійному і розслабленому стані середній тиск на перо буде менший, ніж у емоційно збудженому і напруженому стані. Але це потребує додаткових досліджень.

Таким чином, обрано три динамічних параметри: 1) $l(t)$ – відстань між сусідніми дискретними точками підпису, 2) $\Delta\alpha(t)$ – різниця кутів нахилу двох сусідніх відрізків, що з'єднують дискретні точки підпису, 3) $Z(t)$ – тиск пера на графічний планшет. Ці динамічні параметри характеризують підпис як багатопараметричний процес, який буде розпізнаватися спайкінговою нейронною мережею. Розглянемо як здійснюється нормалізація цих динамічних параметрів.

Нормалізація динамічних параметрів підпису.

Нормалізація динамічних параметрів підпису має здійснюватись як по амплітуді, так і по часу. Точніше, по часу має відбуватись приведення до єдиного часового інтервалу. Якщо конкретна реалізація підпису тривала час T , а необхідно приводити всі підписи до єдиного інтервалу T_0 , то потрібно відліки конкретного динамічного параметру подавати на вхід спайкінгової нейронної мережі не з кроком Δt дискретизації сигналів у планшеті, а з новим часовим кроком:

$$\Delta t_0 = \frac{T_0}{T} \cdot \Delta t, \quad (1/2)$$

Нормалізація двох із обраних динамічних параметрів $l(t)$ та $z(t)$ по амплітуді буде здійснюватись за формулами:

$$\bar{l}_i = (l_i - l_{min}) / (l_{max} - l_{min}). \quad (1.3)$$

$$\bar{z}_i = (z_i - z_{min}) / (z_{max} - z_{min}). \quad (1.4)$$

де \bar{l}_i та \bar{z}_i – нормалізовані значення l_i та z_i ; l_{min} та z_{min} – мінімальні значення l_i та z_i ; l_{max} та z_{max} – максимальні значення l_i та z_i відповідно.

Динамічний параметр $\Delta\alpha(t)$ не потребує нормалізації по амплітуді, тому що він вже нормалізований (є кут) і завжди міняється в діапазоні $[-\pi, +\pi]$ радіан.

Структура спайкінгової нейронної мережі.

У запропонованому методі Online верифікації підпису варто використовувати саме спайкінгові нейронні мережі [17,18], тому що вони дозволяють розпізнавати динамічні сигнали безпосередньо, тобто без їх попереднього перетворення у вектор статичних ознак. Також вони мають і інші переваги. Всі переваги спайкінгових нейронних мереж перед традиційними нейронними мережами обумовлені їхньою нейроморфністю (схожістю з мережами біологічних нейронів) і формулюються так:

- 1) розпізнавання динамічних образів (мова, рухомі зображення, кардіограми, динамічні параметри підпису та ін.) без їх попереднього перетворення у вектор статичних ознак;
- 2) багатозадачність (інформація про вхідні потоки циркулює в рекурентній нейронній мережі і на вихід одночасно можуть бути подані результати різних завдань за допомогою різних груп зчитувальних нейронів, навчених виконанню того або іншого завдання);
- 3) розпізнавання з передбаченням (будь-який динамічний процес може бути розпізнаний навіть за неповною інформацією про нього, тобто навіть раніше, ніж він завершиться);
- 4) простота процедури навчання (навчаються не всі нейрони мережі, а лише вихідні зчитувальні нейрони);
- 5) підвищена продуктивність обробки інформації і завадостійкість завдяки частотно-імпульсному представленню інформації.

Для Online верифікації підпису за основу було взято структуру спайкінгової нейронної мережі, розроблену в [17]. Модифіковану структуру спайкінгової нейронної мережі для Online верифікації та розпізнавання підписів зображено на рис. 4. Вхідні спайкінгові нейрони можна побудувати, наприклад, за моделлю LIF [19]. На вхідні нейрони подаються нормалізовані динамічні параметри підпису $\bar{l}(t)$,

$\Delta\alpha(t)$ та $\bar{p}(t)$, які перетворюються вхідними нейронами у відповідні їм імпульсні послідовності як показано на рис. 5.

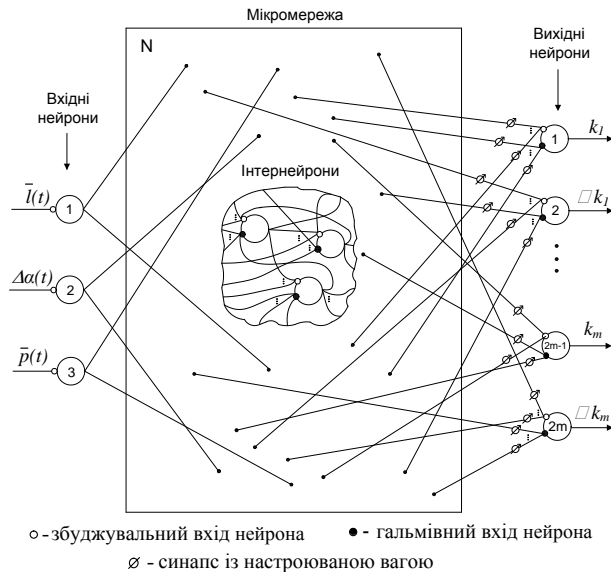


Рисунок 4 – Структура спайкінгової нейронної мережі для Online верифікації та розпізнавання підписів

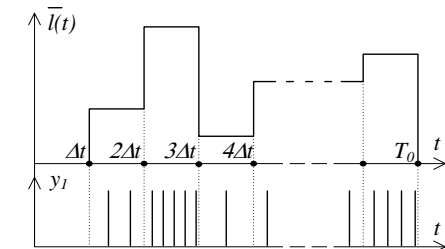


Рисунок 5 – Перетворення параметру $\bar{l}(t)$ вхідним спайкінговим нейроном у його вихідний імпульсний сигнал $y_l(t)$

Метод Online верифікації та розпізнавання підписів на основі спайкінгової нейронної мережі.

Враховуючи структуру спайкінгової нейронної мережі згідно з рис. 4, а також розроблене в [20] правило навчання вихідних нейронів спайкінгової нейронної мережі, принципи функціонування і математичні моделі спайкінгових нейронів з роздільними входами [17], можна сформулювати метод Online верифікації та розпізнавання підписів з використанням спайкінгової нейронної мережі.

Цей метод полягає в такому:

1. Створити (згенерувати) рекурентну спайкінгову нейронну мережу, складену з інтернейронів, в кількості не менше $N \geq 15m$, де m – кількість еталонних образів (в даному випадку підписів), які мережа повинна «запам'ятати». З'єднання нейронів в мережі виконати за даними нейрофізіологічних досліджень [21]. Ваги зв'язків нейронів вибрати невеликими випадковими.

2. Сформувати 3 вхідних нейрони по кількості динамічних параметрів підпису. З'єднати кожен з них випадковим чином з не менше, ніж q нейронами мікромережі ($n < q < N$). Ваги зв'язків вибрати випадковими.

3. Сформувати $2m$ вихідних нейронів (по 2 на кожен еталонний підпис, один – для індикації справжнього підпису, а другий – для індикації підробленого підпису). З'єднати кожен з них випадково з не менше, ніж s нейронами мікромережі ($m < s < N$). Ваги зв'язків вибрати випадковими.

4. Застосувати алгоритм навчання, описаний в [20]. При цьому підстроюються лише ваги зв'язків кожного з $2m$ вихідних нейронів. Як ідеальний цільовий вихід $k_i(t)$ може виступати імпульсний сигнал з постійною (максимальною) частотою імпульсів f_{max} , що дорівнює лабільності вихідного нейрона. Фактичний вихідний сигнал $f(x(t))$ буде послідовністю імпульсів з довільними часовими проміжками між ними. Вхідні сигнали мережі тим ближчі до еталонного образу, чим більша середня за період розпізнавання частота імпульсів вихідного нейрона, що відповідає цьому еталонному образу.

5. Подати на вхід мережі досліджуваний 3-вимірний сигнал (3 нормалізовані динамічні характеристики підпису) тривалістю T_0 і зафіксувати, який з $2m$ вихідних нейронів видаватиме максимальну кількість імпульсів протягом T_0 . Саме цей нейрон і визначає еталонний образ, якому максимально відповідають вхідні сигнали мережі. Як оцінка міри схожості вхідних сигналів і еталонного образу може використовуватися відношення середньої за період T_0 частоти імпульсів вихідного нейрона до f_{max} .

Переваги запропонованого методу динамічної верифікації підпису

Запропонований метод має такі переваги:

1) обрані три динамічних параметри підпису: $l(t)$, $\Delta\alpha(t)$, $z(t)$ є інваріантними до кута нахилу підпису, а після їх нормалізації – ще й до просторового та часового масштабів підпису;

2) динамічні параметри підпису подаються на спайкінгову 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 верифікації та розпізнавання підписів (особливо при розпізнаванні підроблених підписів, які сильно корельовані з оригіналами);

3) результат верифікації та розпізнавання може бути оцінений ще до завершення періоду дії самих динамічних параметрів підпису по інтенсивній імпульсації на відповідному виході (розпізнавання з передбаченням), що підвищує швидкодію;

4) використовувана нейронна мережа має неважку процедуру навчання, причому навчаються не всі нейрони мережі, а тільки вихідні;

5) при необхідності додавання нових підписів не потрібно перенавчати всю мережу повністю, а достатньо додати кілька вихідних нейронів і навчити тільки їх зв'язки;

6) підвищено завадостійкість за рахунок представлення інформації в частотно-імпульсній формі.

Висновки

1. У статті запропоновано метод Online верифікації та розпізнавання підписів на основі спайкінгової нейронної мережі. Структура мережі є оригінальною та використовує спайкінгові нейрони з розділними входами збудження та гальмування [17]. Особливістю структури мережі є також використання по 2 вихідних нейронів для кожного підпису, один – для індикації справжнього підпису, а другий – для індикації підробленого підпису.

2. Для представлення підпису обгрунтовано вибір таких трьох динамічних параметрів підпису: 1) $l(t)$ - відстань між сусідніми дискретними точками підпису, 2) $\Delta\alpha(t)$ – різниця кутів нахилу двох сусідніх відрізків, що з'єднують дискретні точки підпису, 3) $z(t)$ – тиск пера на графічний планшет. Ці динамічні параметри є інваріантними до кута нахилу підпису, а після їх нормалізації – ще й до просторового та часового масштабів підпису;

3. Обрані динамічні параметри підпису подаються на спайкінгову нейронну мережу для розпізнавання одночасно без попереднього перетворення у вектор статичних ознак, що спрощує метод завдяки відсутності складних обчислювальних процедур перетворення, а також перешкоджає втраті корисної інформації, а тому – підвищує точність і достовірність верифікації та розпізнавання підписів (особливо при розпізнаванні підроблених підписів, які сильно корельовані з оригіналами);

3. Запропонована спайкінгова нейронна мережа має просту процедуру навчання. Крім цього, при необхідності додавання нових підписів не потрібно перенавчати всю мережу повністю, а достатньо додати кілька вихідних нейронів і навчити тільки їхні зв'язки.

Список літератури

- [1] I. M. El-Henawy, M. Z. Rashad, O. Nomir, and K. Ahmed, «Online Signature Verification: State of the art», *International Journal of Computers & Technology*, Volume 4, No. 2, March-April, 2013.
- [2] M. Diaz, M. A. Ferrer, D. Impedovo, M. I. Malik, G. Pirlo, and R. Plamondon, «A Perspective Analysis of Handwritten Signature Technology», *ACM Comput. Surv.*, Vol. 51, No. 6, Article 117, January 2019.
- [3] Т. Ю. Дорошенко, и Е. Ю. Костюченко, «Система аутентификации на основе динамики рукописной подписи», *Доклады ТУСУР*, 2014, № 2(32), с. 219-223.
- [4] Maged M. M. Fahmy, «Online handwritten signature verification system based on DWT features extraction and neural network classification», *Ain Shams Engineering Journal*, 2010, 1, pp. 59–70.
- [5] И. А. Сорокин, «Формирование системы признаков для идентификации личности по динамике воспроизведения подписи», автореф. дис. на соискание уч. степени канд. техн. наук, Пензенский гос. ун-т, Пенза, 2005.
- [6] N. Houmani, and S. Garcia-Salicetti, «On hunting animals of the biometric menagerie for online signature», *PLoS ONE*, 11, 4, 2016.
- [7] S. V. Nalwa, «Automatic On-Line Signature Verification», *Proceedings of the IEEE*, Vol. 85, № 2, 1997.
- [8] V. Iranmanesh, S. M. S. Ahmad, W. A. W. Adnan, S. Yussof, O. A. Arigbabu, and F. L. Malallah, «Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis», *Hindawi Publishing Corporation, The Scientific World Journal*, Volume 2014, Article ID 381469.
- [9] N. Houmani, S. Garcia-Salicetti, and B. Dorizzi, «On assessing the robustness of pen coordinates, pen pressure and pen inclination to time variability with personal entropy», *In IEEE 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems*, 1–6, 2009.
- [10] S. A. Farimani, and M. V. Jahan, «An HMM for online signature verification based on velocity and hand movement directions», *In 6th Iranian Joint Congress on Fuzzy and Intelligent Systems*, 2018, pp. 205–209.

- [11] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, «Online signature verification with support vector machines based on LCSS kernel functions», *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, 40, 4, 2010, pp. 1088–1100.
- [12] A. McCabe, J. Trevathan, and W. Read, «Neural Network-based Handwritten Signature Verification», *Journal of Computers*, vol. 3, No. 8, August 2008.
- [13] Weixin Yang, Lianwen Jin, and Manfei Liu, «Chinese character-level writer identification using path signature feature, dropstroke and deep CNN», *In 2015 13th International Conference on Document Analysis and Recognition (ICDAR)*, pp. 546-550, IEEE, 2015.
- [14] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, «DeepSign: Deep On-Line Signature Verification», *Preprint in IEEE Transactions on Biometrics Behavior and Identity Science*, January 2021.
- [15] M. A. Aoun, and M. Boukadoum, «Learning algorithm and neurocomputing architecture for NDS Neurons», *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, London, UK, 2014, pp. 126-132.
- [16] M. M. Fard, M. M. Fard, and N. Mozayani, «A new on-line signature verification by Spatio-Temporal neural network», *2008 IEEE International Conference on Intelligence and Security Informatics*, Taipei, Taiwan, 2008, pp. 233-235, doi: 10.1109/ISI.2008.4565065.
- [17] O. K. Kolesnytskyj, I. V. Bokotsey, and S. S. Yaremchuk, «Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices», *Optical Memory & Neural Networks (Information Optics)*, 2010, Vol.19, № 2, pp. 154-165.
- [18] 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.
- [19] W. Gerstner, and W. Kistler, *Spiking Neuron Models: Single Neurons, Populations, Plasticity*. Cambridge: Cambridge University Press, 2002. doi:10.1017/CBO9780511815706.
- [20] O. K. Колесницький, and Самра Муавия Хассан Хамо, «Метод розпознавання багатовимірних часових рядів при допомозі імпульсних нейронних мереж», *Інформаційні технології та комп'ютерна інженерія*, 2006, № 2(6), с. 86-93.
- [21] W. Maass, «Networks of spiking neurons: the third generation of neural network models», *Neural Networks*, 10:1659-1671, 1997.

Стаття надійшла: 22.02.2021.

References

- [1] I. M. El-Henawy, M. Z. Rashad, O. Nomir, and K. Ahmed, «Online Signature Verification: State of the art», *International Journal of Computers & Technology*, Volume 4, No. 2, March-April, 2013.
- [2] M. Diaz, M. A. Ferrer, D. Impedovo, M. I. Malik, G. Pirlo, and R. Plamondon, «A Perspective Analysis of Handwritten Signature Technology», *ACM Comput. Surv.*, Vol. 51, No. 6, Article 117, January 2019.
- [3] T. Ju. Doroshenko, and E. Ju. Kostjuchenko, «Sistema autentifikacii na osnove dinamiki rukopisnoj podpisi», *Doklady TUSUR*, 2014, № 2(32), pp. 219-223.
- [4] Maged M. M. Fahmy, «Online handwritten signature verification system based on DWT features extraction and neural network classification», *Ain Shams Engineering Journal*, 2010, 1, pp. 59–70.
- [5] I. A. Sorokin, «Formirovanie sistemy priznakov dlja identifikacii lichnosti po dinamike vosproizvedeniya podpisi», avtoref. dis. na soiskanie uch. stepeni kand. tehn. nauk, Penzenskij gos. un-t, Penza, 2005.
- [6] N. Houmani, and S. Garcia-Salicetti, «On hunting animals of the biometric menagerie for online signature», *PLoS ONE*, 11, 4, 2016.
- [7] S. V. Nalwa, «Automatic On-Line Signature Verification», *Proceedings of the IEEE*, Vol. 85, № 2, 1997.
- [8] V. Iranmanesh, S. M. S. Ahmad, W. A. W. Adnan, S. Yussof, O. A. Arigbabu, and F. L. Malallah, «Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis», *Hindawi Publishing Corporation, The Scientific World Journal*, Volume 2014, Article ID 381469.
- [9] N. Houmani, S. Garcia-Salicetti, and B. Dorizzi, «On assessing the robustness of pen coordinates, pen pressure and pen inclination to time variability with personal entropy», *In IEEE 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems*, 1–6, 2009.
- [10] S. A. Farimani, and M. V. Jahan, «An HMM for online signature verification based on velocity and hand movement directions», *In 6th Iranian Joint Congress on Fuzzy and Intelligent Systems*, 2018, pp. 205–209.

- [11] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, «Online signature verification with support vector machines based on LCSS kernel functions», *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, 40, 4, 2010, pp. 1088–1100.
- [12] A. McCabe, J. Trevathan, and W. Read, «Neural Network-based Handwritten Signature Verification», *Journal of Computers*, vol. 3, № 8, August 2008.
- [13] Weixin Yang, Lianwen Jin, and Manfei Liu, «Chinese character-level writer identification using path signature feature, dropstroke and deep CNN», *In 2015 13th International Conference on Document Analysis and Recognition (ICDAR)*, pp. 546-550, IEEE, 2015.
- [14] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, «DeepSign: Deep On-Line Signature Verification», *Preprint in IEEE Transactions on Biometrics Behavior and Identity Science*, January 2021.
- [15] M. A. Aoun, and M. Boukadoum, «Learning algorithm and neurocomputing architecture for NDS Neurons», *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, London, UK, 2014, pp. 126–132.
- [16] M. M. Fard, M. M. Fard, and N. Mozayani, «A new on-line signature verification by Spatio-Temporal neural network», *2008 IEEE International Conference on Intelligence and Security Informatics*, Taipei, Taiwan, 2008, pp. 233–235, doi: 10.1109/ISI.2008.4565065.
- [17] O. K. Kolesnytskyj, I. V. Bokotsey, and S. S. Yaremchuk, «Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices», *Optical Memory & Neural Networks (Information Optics)*, 2010, Vol. 19, № 2, pp. 154–165.
- [18] 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.
- [19] W. Gerstner, and W. Kistler, *Spiking Neuron Models: Single Neurons, Populations, Plasticity*. Cambridge: Cambridge University Press, 2002, doi:10.1017/CBO9780511815706.
- [20] O. K. Kolesnytskyj, and Samra Muavija Hassan Hamo, «Metod rozpoznaniya mnogomernyh vremennyh rjadov pri pomoshhi impul'snyh nejronnyh setej», *Informacijni tehnologii ta komp'juterna inzhenerija*, 2006, № 2(6), pp. 86–93.
- [21] W. Maass, «Networks of spiking neurons: the third generation of neural network models», *Neural Networks*, 10:1659-1671, 1997.

Відомості про авторів

Куцман Владислав Вікторович – аспірант кафедри комп'ютерних наук, інженер-програміст ТОВ «УЛФ-ФІНАНС».

Колесницький Олег Костянтинович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук.

В. В. Куцман, О. К. Колесницький

ВЕРИФИКАЦИЯ И РАСПОЗНАВАНИЕ ПОДПИСИ КАК МНОГОПАРАМЕТРИЧЕСКОГО ПРОЦЕССА НА ОСНОВЕ СПАЙКИНГОВОЙ НЕЙРОННОЙ СЕТИ

Винницкий национальный технический университет, Винница

V. V. Kutsman, O. K. Kolesnytskyj

SIGNATURE VERIFICATION AND RECOGNITION AS A MULTIPARAMETRIC PROCESS BASED ON A SPIKING NEURAL NETWORK

Vinnitsia National Technical University, Vinnitsia