

Вінницький національний технічний університет
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

КУЦМАН ВЛАДИСЛАВ ВІКТОРОВИЧ

УДК 004.383.8

ДИСЕРТАЦІЯ
ДИНАМІЧНА ІДЕНТИФІКАЦІЯ ПІДПISУ НА ОСНОВІ
СПАЙКІНГОВОЇ НЕЙРОННОЇ МЕРЕЖІ

Спеціальність 122 «Комп'ютерні науки»
Галузь знань 12 «Інформаційні технології»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____В.В. Куцман

Науковий керівник:

Колесницький Олег Костянтинович
кандидат технічних наук, доцент

Вінниця – 2021

АНОТАЦІЯ

Куцман В. В. Динамічна ідентифікація підпису на основі спайкінгової нейронної мережі. – Кваліфікаційна наукова праця на правах рукопису

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» (12 «Інформаційні технології»). – Вінницький національний технічний університет, Вінниця, 2021.

В дисертаційній роботі розв'язана наукова задача розробки методів та засобів динамічної ідентифікації підпису з використанням спайкінгових нейронних мереж та динамічних параметрів підпису, робастних до внутрішньоперсональної варіабельності та чутливих до міжперсональної варіабельності підписів, що дозволило збільшити достовірність систем динамічної ідентифікації підпису,

Ідентифікація підпису має особливо важливе значення, оскільки вона є загальноприйнятим методом схвалення фінансових операцій. Аналіз рукописних підписів - одна з найпоширеніших методик визначення особи, з чим ми часто стикаємось у своєму повсякденному житті. Верифікація підпису людиною-оператором має багато «слабких сторін». Так, оператор може оцінити тільки статичне зображення підпису, наскільки воно відповідає еталону. При цьому існує загроза, що добре натренований зловмисник може дуже схоже підробити підпис особи, тобто зображення підпису, відтворене зловмисником, буде дуже схоже на справжній підпис особи.

Широке поширення комп'ютерної техніки та інформаційних технологій обробки даних дозволяє застосувати не тільки аналіз статичного зображення підпису (Offline ідентифікація), а також динамічних характеристик його написання (Online ідентифікація). Статична (Offline) ідентифікація підписів є менш перспективною, тому в рамках цієї роботи не розглядається. Сучасні електронні планшети, на яких людина розписується, можуть формувати динамічні параметри підпису (динаміку зміни координат пера, тиску пера та кута нахилу пера). Ці динамічні параметри дають

додаткову інформацію про підпис і можуть бути використані для більш точної верифікації та ідентифікації підпису. Ці динамічні параметри не можуть бути проаналізовані людиною-оператором, однак легко можуть бути проаналізовані електронними комп'ютерними засобами з відповідним програмним забезпеченням. Також ці динамічні параметри не можливо підробити, оскільки вони не можуть бути відомі зловмиснику. Однак ідентифікація динамічних параметрів підпису має багато невирішених проблем та викликів. Однією з найбільших проблем є той факт, що підпис однієї особи не завжди є однаковим. Така внутрішньоперсональна варіабельність підпису створює низку проблем при побудові високодостовірних програмних засобів ідентифікації підпису. З іншого боку, потребують вдосконалення методи класифікації динамічних параметрів підпису в напрямку підвищення достовірності при класифікації сильно корельованих часових рядів. Саме вирішенню цих проблем і присвячено дане дослідження.

В дисертаційній роботі розглянуто співвідношення понять верифікація та ідентифікація підписів. Ідентифікація (розпізнавання) – це загальний процес виявлення власника підпису, яка є багатокласовим завданням класифікації. Верифікація - це загальний процес прийняття рішення щодо підпису, в результаті чого визначається чи справжній підпис, чи підроблений. Тому це двокласове завдання класифікації. Описано загальну схему динамічної ідентифікації підпису, проаналізовано процес отримання первинних динамічних ознак підпису та такі їх властивості як внутрішньоперсональна та міжперсональна варіабельність, сформульовано вимоги до визначення оптимального набору динамічних ознак підпису. Проведено класифікацію відомих методів та засобів динамічної ідентифікації підписів та сформульовано перспективи їх вдосконалення, що полягають у використанні динамічних класифікаторів на основі спайкінгових нейронних мереж та використанні динамічних параметрів підписів, стійких до внутрішньоперсональної варіабельності та чутливих до міжперсональної

варіабельності. Проведено аналіз баз даних підписів та показників достовірності, що використовуються при оцінці якості систем динамічної ідентифікації підписів. Виділено недоліки існуючих систем динамічної ідентифікації підписів, запропоновано напрямки їх вдосконалення та сформульовано задачі досліджень.

Обґрунтовано перспективність використання спайкінгових нейронних мереж для динамічної ідентифікації підписів, оскільки вони можуть без будь-якого перетворення форми інформації виконувати розпізнавання динамічних параметрів підпису, що виключає втрату корисної інформації та сприяє підвищенню достовірності ідентифікації. Проаналізовано моделі спайкінгових нейронів з точки зору використання їх у процесі динамічної ідентифікації підписів. Використана модель нейрона з роздільними входами збудження та гальмування, що дозволяє використовувати імпульси однакової полярності для передачі як збуджувальних, так і гальмівних сигналів.

Розроблено структуру та архітектуру спайкінгової нейронної мережі включно з принципами її побудови та функціонування з орієнтацією на застосування у процесі динамічної ідентифікації підписів. Особливістю розробленої структури є те, що вона має на кожний ідентифікаційний клас (на кожного підписанта) не 1 вихідний нейрон, а 2 вихідних нейрони (один - для індикації справжнього підпису, а другий - для індикації підробленого підпису). Це дозволяє точніше визначати майстерно підроблені підписи, підкреслюючи їх дифференціацію від справжніх, оскільки вони представляються сильно корельованими сигналами.

Розроблено метод навчання спайкінгової нейронної мережі та принципи кодування вихідної інформації в процесі класифікації динамічних параметрів підписів. Особливістю процесу навчання є те, що для навчання використовуються не тільки оригінальні підписи особи, а також і майстерно підроблені підписи, що збільшує достовірність процесу ідентифікації підписів. Крім цього, застосовується спеціально розроблена процедура початкового закріплення вихідних нейронів за класами ідентифікації, що

пришвидшує процес навчання. Також розроблено метод динамічної ідентифікації підписів на основі спайкінгової нейронної мережі, який має ряд переваг перед відомими методами, зокрема, не вимагає попереднього перетворення у вектор статичних ознак, може ідентифікувати підписи з передбаченням, що підвищує швидкодію; використовувана нейронна мережа має спрощену процедуру навчання, а саме - не потребує перенавчання всієї мережі при необхідності додавання нових підписів; має підвищену завадостійкість.

Обґрунтовано вибір динамічних параметрів підпису, стійких до геометричної варіабельності, тобто зміни просторового масштабу, зсуву та повороту підпису відносно сторін планшета: $l(t)$ - відстань від поточного часового відліку координат пера до наступного, $XY(t)$ - добуток координат $X(t)$ та $Y(t)$ координат пера, $Z(t)$ - тиск пера на планшет. Розроблено та описано процес нормалізації динамічних параметрів підпису, який здійснюється як по амплітуді, так і по часу. Розроблено формули для здійснення процесу нормалізації динамічних параметрів підпису. Досліджено стійкість динамічних параметрів підпису до внутрішньоперсональної варіабельності на основі статистичного аналізу параметрів розкиду окремих реалізацій підпису відносно усередненої залежності. Доведено обґрунтованість вибору параметрів $l(t)$ та $XY(t)$ (мала варіабельність – відповідно 6,44% та 8,04%) і необґрунтованість вибору параметру $\Delta\alpha(t)$ (велика варіабельність – 25,37%) для використання у високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж. Досліджено чутливість динамічних параметрів підпису до міжперсональної варіабельності на основі статистичного аналізу параметрів розкиду окремих реалізацій підпису відносно усередненої залежності. Доведено обґрунтованість вибору параметрів $l(t)$ та $XY(t)$ (мала внутрішньоперсональна варіабельність – 6,44% та 8,04% відповідно, велика міжперсональна варіабельність – 12,92% та 15,91% відповідно) та необґрунтованість вибору параметру $\Delta\alpha(t)$ (приблизно

однакова внутрішньоперсональна та міжперсональна варіабельність – відповідно 25,37% та 27.62%) для використання у високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж.

Розроблено спеціалізоване програмне забезпечення, що складається з двох незалежних компонентів. Перший компонент створений для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису. Другий компонент призначено для комп'ютерного моделювання та оцінки достовірності запропонованого методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі. Описано програмну реалізацію методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі на мові Python у середовищі розробки Visual Studio Code з використанням бібліотек TensorFlow та Keras. Розглянуто методику оцінки достовірності методів динамічної ідентифікації підпису, що складається з таких етапів: вибір референсної бази даних підписів (було обрано БД DeepSignDB), аналіз показників якості систем ідентифікації підписів, розробка протоколу проведення експериментальних досліджень, Проведено експериментальні дослідження достовірності методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі.

При тестуванні тільки майстерно підробленими підписами розроблена система має достовірність 96,1%, влучність 93,1%, повноту 99,65%, оцінку F1 96,26%. Загалом, у відносних показниках, запропонована система за достовірністю краща за референсну на 9% при тестуванні на майстерних підробках і на 15% при тестуванні на випадкових підробках. Визначено перспективи подальших досліджень, які полягають як у аналізі та синтезі ефективних динамічних параметрів підпису та їх попередньої обробки, так і у пошуку нових та удосконаленні відомих методів та засобів класифікації часових рядів, якими є динамічні параметри підпису.

Ключові слова: динамічна ідентифікація підпису, спайкінгова нейронна мережа, динамічні ознаки підпису, внутрішньоперсональна варіабельність підпису, міжперсональна варіабельність підпису, достовірність ідентифікації.

ABSTRACT

Kutsman V. V. Dynamic signature identification based on spiking neural network. - Qualifying scientific work on the rights of the manuscript.

Thesis for the degree of a Philosophy Doctor in speciality 122 "Computer Sciences" (12 «Information Technologies»). – Vinnytsia National Technical University, Vinnytsia, 2021.

The dissertation solves the scientific problem of developing methods and means of dynamic signature identification using spiking neural networks and dynamic signature parameters, robust to intrapersonal variability and sensitive to interpersonal variability of signatures, which increased the reliability of signature systems.

Signature identification is particularly important as it is a common method of approving financial transactions. Analysis of handwritten signatures is one of the most common methods of identifying a person, which we often encounter in our daily lives. Signature verification by a human operator has many "weaknesses". So, the operator can only evaluate the static image of the signature, how it corresponds to the standard. At the same time, there is a danger that a well-trained attacker may very similarly forge a person's signature, ie the image of the signature reproduced by the attacker will be very similar to a real person's signature.

The widespread use of computer technology and information technology in data processing allows us to apply not only the analysis of static image of the signature (Offline identification), but also the dynamic characteristics of its writing (Online identification). Static (Offline) signature identification is less promising, so it is not considered in this paper. Modern electronic tablets on which a person signs can form dynamic parameters of the signature (dynamics of changes in pen coordinates, pen pressure and pen angle). These dynamic parameters provide additional information about the signature and can be used for more accurate verification and identification of the signature. These dynamic parameters cannot

be analyzed by a human operator, but can easily be analyzed by electronic computer tools with appropriate software. Also, these dynamic parameters cannot be forged, as they cannot be known to the attacker. However, identifying dynamic signature parameters has many unresolved issues and challenges. One of the biggest problems is the fact that one person's signature is not always the same. Such intrapersonal variability of the signature creates a number of problems in the construction of highly reliable software for signature identification. On the other hand, the methods of classification of dynamic parameters of the signature in the direction of increasing reliability in the classification of highly correlated time series need to be improved. This study is devoted to solving these problems.

The dissertation considers the relationship between the concepts of verification and identification of signatures. Identification (recognition) is a general process of identifying the owner of a signature, which is a multi-class task of classification. Verification is a general process of deciding on a signature, which determines whether the signature is genuine or forged. Therefore, this is a two-class classification task. The general scheme of dynamic signature identification is described, the process of obtaining primary dynamic signature features and their properties such as intrapersonal and interpersonal variability are analyzed, requirements for determining the optimal set of dynamic signature features are formulated. The classification of known methods and means of dynamic identification of signatures is carried out and the prospects of their improvement are formulated, which are the use of dynamic classifiers based on spiking neural networks and the use of dynamic signature parameters robust to intrapersonal variability and sensitive to interpersonal variability. The analysis of signature databases and reliability indicators used in assessing the quality of dynamic signature identification systems is carried out. The shortcomings of the existing systems of dynamic identification of signatures are highlighted, the directions of their improvement are offered and the tasks of researches are formulated.

The prospects of using spiking neural networks for dynamic identification of signatures are substantiated, as they can perform recognition of dynamic signature

parameters without any transformation of the information form, which eliminates the loss of useful information and helps increase the reliability of identification. Models of spiking neurons from the point of view of their use in the process of dynamic identification of signatures are analyzed. A model of a neuron with separate inputs of excitation and inhibition is used, which allows to use pulses of the same polarity for the transmission of both excitation and inhibition signals.

The structure and architecture of the spiking neural network, including the principles of its construction and operation with a focus on application in the process of dynamic signature identification, have been developed. The peculiarity of the developed structure is that it has for each identification class (for each signatory) not 1 output neuron, but 2 output neurons (one - to indicate a real signature, and the second - to indicate a fake signature). This allows us to more accurately identify forged signatures, emphasizing their differentiation from the real thing, because they are highly correlated signals.

The method of learning the spiking neural network and the principles of coding the source information in the process of classification of dynamic parameters of signatures have been developed. The peculiarity of the learning process is that not only the original signatures of the person are used for learning, but also skillfully forged signatures, which increases the authenticity of the signature identification process. In addition, a specially designed procedure for the initial fixation of source neurons in identification classes is used, which speeds up the learning process. Also the method of dynamic identification of signatures based on spiking neural network has been developed, which has a number of advantages over known methods, in particular, does not require prior conversion into a vector of static features, can identify signatures with predictions that increase performance; the used neural network has a simplified learning procedure, no need to retrain the entire network if you need to add new signatures; has increased noise immunity.

The choice of dynamic parameters of the signature, resistant to geometric variability, ie changes in the spatial scale, shift and rotation of the signature

relative to the sides of the tablet is substantiated: $l(t)$ - the distance from the current time sample of the pen coordinates to the next one, $XY(t)$ - the product of the pen coordinates $X(t)$ and $Y(t)$, $Z(t)$ - the pen pressure on the tablet. The process of normalization of dynamic parameters of the signature which is carried out both on amplitude, and on time is developed and described. Formulas for the process of normalization of dynamic signature parameters have been developed. The stability of dynamic signature parameters to intrapersonal variability is studied on the basis of statistical analysis of scatter parameters of individual signature implementations relative to the average dependence. The validity of the choice of parameters $l(t)$ and $XY(t)$ (low variability - 6.44% and 8.04%, respectively) and the unreasonableness of the choice of the parameter $\Delta\alpha(t)$ (high variability - 25.37%) for use in highly reliable method of dynamic signature identification based on spiking neural networks. The sensitivity of dynamic signature parameters to interpersonal variability was studied on the basis of statistical analysis of scatter parameters of individual signature implementations relative to the average dependence. The validity of the choice of parameters $l(t)$ and $XY(t)$ (low intrapersonal variability - 6.44% and 8.04%, respectively, large interpersonal variability - 12.92% and 15.91%, respectively) and unreasonableness of the choice of the parameter $\Delta\alpha(t)$ (approximately the same intrapersonal and interpersonal variability - 25.37% and 27.62%, respectively) for use in a highly reliable method of dynamic signature identification based on spiking neural networks.

Specialized software has been developed, consisting of two independent components. The first component is designed to study intrapersonal and interpersonal variability of dynamic signature parameters. The second component is designed for computer simulation and evaluation of the proposed method of dynamic signature identification based on spiking neural network. The software implementation of the method of dynamic signature identification based on a spiking neural network in the Python language in the Visual Studio Code development environment using the TensorFlow and Keras libraries is described. The method of assessing the authenticity of dynamic signature identification

methods is considered, consisting of the following stages: selection of reference database of signatures (DeepSignDB database was selected), analysis of quality indicators of signature identification systems, development of experimental research protocol. spiking neural network. When testing only skilled forgery signatures, the developed system has an accuracy of 96.1%, precision of 93.1%, recall of 99.65%, F1 score of 96.26%. In general, in terms of relative indicators, the proposed system is 9% more reliable than the reference system when tested on skilled forgeries and 15% when tested on random forgeries. Prospects for further research are identified, which consist in the analysis and synthesis of effective dynamic parameters of the signature and their pre-processing, and in finding new and improving known methods and means of classifying time series, which are dynamic parameters of the signature.

Key words: dynamic signature identification, spiking neural network, dynamic signature features, intrapersonal signature variability, interpersonal signature variability, identification accuracy.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

- [1] В. В. Куцман, та О. К. Колесницький, «Верифікація та розпізнавання підпису як багатопараметричного процесу на основі спайкінгової нейронної мережі», *Інформаційні технології та комп'ютерна інженерія*, том 50, № 1, с. 36–44, 2021.
- [2] В. В. Куцман, О. К. Колесницький, та І. К. Денисов, «Дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису у процесі їх ідентифікації», *Оптико-електронні інформаційно-енергетичні технології*, том. 40, № 2, с. 15-20, 2020.
- [3] V. Kutsman, and O. Kolesnytskyj, «Dynamic handwritten signature identification using spiking neural network», *Informatyka, Automatyka, Pomiarы w Gospodarce i Ochronie Środowiska – IAPGOS (Informatics, Control, Measurement in Economy and Environmental Protection)*, Vol 11, No 3, pp. 34-39, 2021.
- [4] O. Kolesnytskyj, V. Kutsman, K. Skorupski, and M. Arshidinova, «Neurocomputer architecture based on spiking neural network and its optoelectronic implementation», *Proc. SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments*, vol. 11176, pp. 1117609, 2019. doi: 10.1117/12.2536607.
- [5] О. К. Колесницький, та В. В. Куцман, «Розпізнавання багатоканальних сигналів за допомогою спайкінгових нейронних мереж», на *Одинадцятій міжнародній науково-практичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018»*, Вінниця, 2018, с. 212-213.
- [6] О. К. Колесницький, та В. В. Куцман, «Архітектурні принципи побудови спайкінгових нейрокомп'ютерів та варіанти їх апаратної реалізації», на *XII Міжнародній науковопрактичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2020»*, Вінниця, 2020, с. 105-106.

[Електронний ресурс]. Доступно:

<https://conferences.vntu.edu.ua/index.php/allvntu/index/pages/view/zbirn2020>.

- [7] В. В. Куцман, А. О. Переродов , та О. К. Колесницький, «Класифікація банківських текстів на основі згорткової нейронної мережі», на *XXIV Міжнародному молодіжному форумі «Радіoeлектроніка та молодь в XXI столітті»*, Харків, 2020, с.189-190.
- [8] В. В. Куцман, та О. К. Колесницький, «Динамічна ідентифікація підпису на основі спайкінгової нейрної мережі», в *Матеріалах конференції «Сучасні проблеми інфокомунікацій, радіoeлектроніки та наносистем»*, Вінниця, 2021. [Електронний ресурс]. Доступно: <https://conferences.vntu.edu.ua/index.php/spirn/spirn2021/paper/view/13851>.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	17
ВСТУП	19
 РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД І КЛАСИФІКАЦІЯ МЕТОДІВ ТА ЗАСОБІВ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ ПІДПISУ	26
1.1 Процес динамічної ідентифікації підпису.....	26
1.1.1 Співвідношення понять верифікація та ідентифікація.....	26
1.1.2 Загальна схема динамічної ідентифікації підпису.....	28
1.2 Динамічні ознаки підпису та їх властивості стосовно процесу ідентифікації.....	29
1.2.1 Процес отримання первинних динамічних ознак підпису	29
1.2.2 Внутрішньоперсональна варіабельність підпису	31
1.2.3 Міжперсональна варіабельність підпису.....	33
1.2.4 Вимоги до визначення оптимального набору динамічних ознак підпису.....	34
1.3 Методи та засоби динамічної ідентифікації підписів та перспективи їх вдосконалення	36
1.3.1 Класифікація методів ідентифікації підписів.....	36
1.3.2 Перспективні методи класифікації динамічних ознак підпису на основі нейронних мереж.....	38
1.4 Оцінка достовірності роботи систем ідентифікації підписів	38
1.4.1 Бази даних підписів.....	39
1.4.2 Показники якості роботи систем ідентифікації підписів.....	40
1.5 Постановка задач дослідження.....	46
1.6 Висновки до першого розділу	49
 РОЗДІЛ 2 СПАЙКІНГОВІ НЕЙРОННІ МЕРЕЖІ ТА ЇХ ЗАСТОСУВАННЯ ДО ІДЕНТИФІКАЦІЇ ПІДПISІВ.....	50

2.1 Обґрунтування перспективності використання спайкінгових нейронних мереж для динамічної ідентифікації підписів	50
2.2 Спайкінгові нейрони	54
2.3 Структура спайкінгової нейронної мережі	63
2.4 Навчання спайкінгової нейронної мережі.....	67
2.5 Метод динамічної ідентифікації підпису на основі спайкінгової нейронної мережі	74
2.6 Висновки до другого розділу.....	76
 РОЗДІЛ 3 ДИНАМІЧНІ ПАРАМЕТРИ ПІДПISУ, СТІЙКІ ДО ВНУТРІШНЬОПЕРСОНАЛЬНОЇ ВАРІАБЕЛЬНОСТІ ТА ЧУТЛИВІ ДО МІЖПЕРСОНАЛЬНОЇ ВАРІАБЕЛЬНОСТІ	77
3.1 Обґрунтування вибору динамічних параметрів підпису, стійких до геометричної варіабельності.....	78
3.2 Нормалізація динамічних параметрів підпису	81
3.3 Дослідження стійкості динамічних параметрів підпису до внутрішньоперсональної варіабельності.....	82
3.4 Дослідження чутливості динамічних параметрів підпису до міжперсональної варіабельності	91
3.5 Висновки до третього розділу	100
 РОЗДІЛ 4 КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ТА ОЦІНКА ДОСТОВІРНОСТІ МЕТОДУ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ ПІДПISУ НА ОСНОВІ СПАЙКІНГОВОЇ НЕЙРОННОЇ МЕРЕЖІ	102
4.1 Програмна реалізація методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі	102
4.2 Методика оцінки достовірності методів динамічної ідентифікації підпису	104
4.2.1 База даних підписів DeepSignDB.....	104

4.2.2 Програмний засіб для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису	110
4.2.3 Показники якості систем ідентифікації підписів	116
4.2.4 Стандарт експериментального протоколу	118
4.3 Експериментальні дослідження достовірності методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі	121
4.4 Перспективи подальших досліджень.....	127
4.5 Висновки до четвертого розділу	129
ЗАГАЛЬНІ ВИСНОВКИ.....	130
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	132
ДОДАТКИ	146
Додаток А Акти впровадження результатів дисертації.....	147
Додаток Б Фрагмент лістингу програми дослідження внутрішньоперсональної та міжперсональної варіабельності підписів	149
Додаток В Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації	160

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AI – artificial intelligence

AUC – area under the curve (площа під кривою)

CCR – correct classification rate (коефіцієнт вірної класифікації)

DTW – dynamic time warping

DWT – discrete wavelet transform (дискретне вейвлет-перетворення)

EER – equal error rate (еквівалентний коефіцієнт помилок).

FAR – false acceptance rate (коефіцієнта помилкового прийняття)

FN – false negative (хибнонегативні): кількість справжніх підписів, які були невірно ідентифіковані як підробні

FP – false positive (хибнопозитивні): кількість підробних підписів, які були неправильно ідентифіковані як справжні,

FRR – false rejection rate (коефіцієнта помилкового відхилення)

HMM – hidden Markov models (приховані Марківські моделі)

IR – identification rate (достовірність ідентифікації):

LIF – leaky integrate-and-fire

PCA – principal component analysis

RF – random forgery

ROC – receiver operating characteristic

SF – simple forgery

SK – skilled forgery

SRM – spike-response model

SVM – support vector machine

TN – true negative (вірhoneгативні): кількість підробних підписів, які були правильно ідентифіковані,

TP – true positive (вірнопозитивні): кількість справжніх підписів, які були правильно ідентифіковані,

APC – автомат з рідкими станами

БД – база даних

БШП – багатошаровий персептрон,

ВП – випадкова підробка

ДП – динамічна ідентифікація підпису

КП – кваліфікована підробка

ПП – проста підробка

РБФ – радіально-базисна функція

СНМ – спайкінгова нейронна мережа

ШНМ – штучна нейронна мережа

ВСТУП

Обґрунтування вибору теми дослідження. Біометричні методи автентифікації, включаючи ідентифікацію голосу, відбитків пальців, розпізнавання обличчя, сканування сітківки ока та перевірку підпису, стають все більш популярними для широкого діапазону практичних застосувань, починаючи від контролю доступу до закритих зон і закінчуючи запобіганням шахрайству у фінансових операціях. Ідентифікація підпису має особливо важливе значення, оскільки вона є єдиним загальноприйнятим методом схвалення фінансових операцій.

Важлива перевага підпису над іншими біометричними показниками - це давня стійка традиція його використання у багатьох розповсюджених завданнях ідентифікації. Він використовується десятки років у повсякденному житті і є дуже зручним. Аналіз рукописних підписів - одна з найпоширеніших методик визначення особи, з чим ми часто стикаємось у своєму повсякденному житті.

Верифікація підпису людиною-оператором має багато «слабких сторін». Так, оператор може оцінити тільки статичне зображення підпису, наскільки воно відповідає еталону підпису. При цьому існує загроза, що добре натренований зловмисник може дуже схоже підробити підпис особи, тобто зображення підпису, відтворене зловмисником, буде дуже схоже на справжній підпис особи.

Широке поширення комп'ютерної техніки та інформаційних технологій обробки даних дозволяє застосувати не тільки аналіз статичного зображення підпису, а також динамічних характеристик його написання. Сучасні електронні планшети, на яких людина розписується, можуть формувати динамічні параметри підпису (динаміку зміни координат пера, тиску пера та кута нахилу пера). Ці динамічні параметри дають додаткову інформацію про підпис і можуть бути використані для більш точної верифікації та ідентифікації підпису. Ці динамічні параметри не можуть бути проаналізовані людиною-оператором, однак легко можуть бути

проаналізовані електронними комп'ютерними засобами з відповідним програмним забезпеченням. Також ці динамічні параметри не можливо підробити, оскільки вони не можуть бути відомі зловмиснику.

Однак ідентифікація динамічних параметрів підпису має багато невирішених проблем та викликів. Однією з найбільших проблем є той факт, що підпис однієї особи не завжди є однаковим. Така внутрішньоперсональна варіабельність підпису створює низку проблем при побудові високодостовірних програмних засобів ідентифікації підпису. Саме вирішенню цих проблем і присвячено дане дослідження, тому воно є вельми актуальним.

Для автоматизованого аналізу динамічних параметрів підпису останнім часом широко застосовують технології штучного інтелекту. Це чітко відповідає «Концепції розвитку штучного інтелекту», схваленої Кабінетом Міністрів України (розпорядження від 02 грудня 2020 р. № 1556-р). Дане дослідження присвячене динамічній ідентифікації підпису засобами штучного інтелекту, а саме – спайкінговими штучними нейронними мережами і має на меті підвищити достовірність процесу комп'ютеризованої ідентифікації підпису.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційне дослідження проводилось згідно з планами науково-дослідних робіт кафедри комп'ютерних наук Вінницького національного технічного університету, в тому числі в межах:

- кафедральної теми 47 К2 "Моделі, методи, технології та пристрої інтелектуальних інформаційних систем управління, економіки, навчання та комунікацій" (2016-2018 р.), при виконанні якої автор брав участь як виконавець,

- кафедральної теми 22 К1 "Розробка спеціалізованих засобів штучного інтелекту на основі інтелектуального аналізу даних та машинного навчання" (2019 р.); при виконанні якої автор брав участь як виконавець окремих підрозділів.

Мета і завдання дослідження. Метою дисертаційного дослідження є підвищення достовірності ідентифікації підпису шляхом вибору робастних до внутрішньоперсональної варіабельності динамічних параметрів підпису та розробки методу їх ідентифікації з використанням спайкінгових нейронних мереж.

Досягнення мети обумовило розв'язання наступних наукових завдань:

1. Провести класифікацію та порівняльний аналіз відомих методів динамічної ідентифікації підписів, виявити недоліки та запропонувати шляхи їх усунення.
2. Вдосконалити структурну організацію спайкінгової нейронної мережі для використання у задачі ідентифікації підпису.
3. Розробити метод динамічної ідентифікації підписів з використанням спайкінгових нейронних мереж,
4. Запропонувати набір динамічних параметрів підпису, робастних до внутрішньоперсональної варіабельності та чутливих до міжперсональної варіабельності.
5. Дослідити та кількісно оцінити внутрішньоперсональну та міжперсональну варіабельність запропонованих динамічних параметрів підпису.
6. Оцінити достовірність методу динамічної ідентифікації підписів з використанням спайкінгових нейронних мереж, використовуючи дані комп'ютерного моделювання процесу ідентифікації з використанням загальновідомих референтних баз даних підписів.

Об'єкт дослідження – процес динамічної ідентифікації підписів з використанням спайкінгових нейронних мереж.

Предмет дослідження – динамічні параметри підпису, властивості їх представимості та розділимості, структурна організація спайкінгових нейромереж та метод динамічної ідентифікації підписів, що дозволяють покращити достовірність та спростити процес ідентифікації підписів.

Методи дослідження.

При розв'язанні поставлених задач використовувались методи: системного аналізу для формулювання вимог до динамічних параметрів підпису; методи теорії інформації та математичної статистики для оцінки внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису; методи математичного моделювання для удосконалення математичних моделей спайкінгових нейронів; теорія штучних нейронних мереж для синтезу структури та розробки режимів роботи спайкінгової нейронної мережі; теорія планування експерименту для обробки даних експериментальних досліджень програмних засобів динамічної ідентифікації підписів; теорія ймовірностей і математична статистика для оцінки достовірності динамічної ідентифікації підписів.

Наукова новизна отриманих результатів.

Нові наукові результати, отримані в дисертаційній роботі, такі:

- Вперше запропоновано метод динамічної ідентифікації підписів, у якому завдяки використанню спайкінгової нейронної мережі відсутнє перетворення динамічних параметрів підпису у вектор статичних ознак, що дозволило збільшити достовірність та швидкодію ідентифікації підпису.
- Удосконалено структурну організацію спайкінгової нейронної мережі для використання у задачі ідентифікації підпису за рахунок введення по два вихідних нейрона на кожен еталонний підпис, що дозволило навчати нейронну мережу не тільки на справжніх підписах, а і на майстерно підроблених і тим самим збільшило достовірність ідентифікації підпису.
- Удосконалено якісний склад використовуваного набору динамічних параметрів підпису, які є інваріантними до масштабу, зсуву та повороту підпису відносно планшету, що дозволило збільшити достовірність ідентифікації підпису.
- Визначено ступінь внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису, що дозволило

зробити висновок про кращу робастність запропонованого набору динамічних параметрів підпису до внутрішньоперсональної варіабельності та їх кращу чутливість до міжперсональної варіабельності підпису, що в підсумку покращує їх представимість та роздільність і тим самим збільшує достовірність процесу ідентифікації підпису.

Новизна викладених у роботі наукових результатів підтверджується статтями у фахових журналах [1], [2], [3], [4].

Практичне значення отриманих результатів.

Практична цінність роботи полягає в тому, що запропоновано інформаційну технологію та алгоритм ідентифікації підписів, проведено комп'ютерне моделювання та експериментальні дослідження процесу ідентифікації підписів.

Теоретичні та практичні дослідження, викладені в дисертації, дозволили:

- 1) розробити структурно-функціональну схему спайкінгової нейронної мережі для використання у задачі ідентифікації підпису, яка містить по два вихідних нейрона на кожен еталонний підпис;
- 2) кількісно оцінити робастність запропонованих динамічних параметрів підпису до внутрішньоперсональної варіабельності підпису та чутливість запропонованих динамічних параметрів підпису до міжперсональної варіабельності підпису;
- 3) розробити програмні засоби динамічної ідентифікації підпису.
- 4) отримати результати комп'ютерного моделювання динамічної ідентифікації підпису;
- 5) отримати результати експериментальних досліджень програмних засобів динамічної ідентифікації підпису, визначити числові значення достовірності їх роботи та порівняти із кращими відомими методами динамічної ідентифікації підпису.

Отримані результати дослідження було впроваджено в ТОВ «Джемікл» та в навчальний процес Вінницького національного технічного університету. Відповідні акти впровадження наведено в додатку А.

Окремі теоретичні результати дисертаційної роботи використовуються в учбовому процесі на кафедрі КН (комп'ютерних наук) ВНТУ в рамках спеціальності 122 «Комп'ютерні науки» при викладанні таких дисциплін: «Сучасні парадигми штучних нейронних мереж» та «Нейрокомп'ютерні технології штучного інтелекту», що викладаються студентам бакалаврату, дисципліни «Нейромережеві методи штучного інтелекту», що викладається студентам магістратури, та дисципліни «Нейромережеві моделі та технології обчислювального інтелекту» підготовки докторів філософії.

Особистий внесок здобувача.

Усі наукові положення та результати дисертаційної роботи, що виносяться на захист, отримані здобувачем самостійно. Особистий внесок здобувача в роботах, опублікованих в співавторстві, такий: в роботі [1] – запропоновано метод динамічної ідентифікації підписів з використанням спайкінгової нейронної мережі, запропоновано якісний склад набору динамічних параметрів підпису, робастних до геометричної мінливості підпису, проведено аналітичний огляд і класифікацію відомих методів динамічної ідентифікації підписів; в роботі [2] – обґрунтовано вибір динамічних параметрів підпису, стійких до геометричної варіабельності, розроблено процес нормалізації по амплітуді і по часу динамічних параметрів підпису, досліджено стійкість динамічних параметрів підпису до внутрішньоперсональної варіабельності, досліджено чутливість динамічних параметрів підпису до міжперсональної варіабельності; в роботі [3] – запропоновано структуру спайкінгової нейронної мережі, особливістю якої є використання по 2 вихідних нейрони для кожного підпису (один - для справжнього підпису, а другий - для підробленого підпису), наведено результати експериментальних досліджень програмної реалізації запропонованого методу; в роботі [4] – запропоновано принципи структурної

організації спайкінгових нейронних мереж; в роботі [5] – обґрунтовано вибір спайкінгових нейронних мереж для розпізнавання багатоканальних динамічних сигналів; в роботі [6] – запропоновано архітектурні принципи побудови спайкінгових нейрокомп'ютерів; в роботі [7] – розглянуто використання згорткових нейронних мереж до задач класифікації; в роботі [8] – запропоновано архітектуру системи динамічної ідентифікації підписів на основі спайкінгової нейронної мережі.

Апробація матеріалів дисертації.

Викладені в дисертації результати досліджень були апробовані на таких наукових конференціях: Одинадцята міжнародна науково-практична конференція «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018» (ІОН-2018), Вінниця; Дванадцята міжнародна науково-практична конференція «ІНТЕРНЕТ-ОСВІТА-НАУКА-2020» (ІОН-2020), Вінниця; XXIV Міжнародний молодіжний форум «Радіoeлектроніка та молодь в ХХІ столітті», Харків: ХНУРЕ. 2020; Міжнародна науково-практична конференція «Сучасні проблеми інфокомунікацій, радіoeлектроніки та наносистем» (СПРН-2021), Вінниця, 2021.

Публікації.

За темою дисертації опубліковано 8 наукових робіт, у тому числі 3 статті [1]-[3] у наукових фахових виданнях, одна стаття у збірнику праць конференції [4] (входить до Scopus) і 4 тез доповідей на конференціях [5]-[8].

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, 4 розділів, списку використаних джерел, додатків. Загальний обсяг дисертації становить 161 сторінок, з яких основний зміст викладений на 112 сторінках друкованого тексту, містить 34 рисунки, 17 таблиць. Список використаних джерел складається зі 110 найменувань. Додатки містять акти впровадження результатів роботи та лістинг програми комп'ютерного моделювання.

РОЗДІЛ 1

АНАЛІТИЧНИЙ ОГЛЯД І КЛАСИФІКАЦІЯ МЕТОДІВ ТА ЗАСОБІВ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ ПІДПISУ

1.1 Процес динамічної ідентифікації підпису

1.1.1 Співвідношення понять верифікація та ідентифікація

Ідентифікація (розпізнавання) – це загальний процес виявлення власника підпису, яка є багатокласовим завданням класифікації. Етапи роботи системи ідентифікації показані на рис. 1.1. Спочатку вхідні підписи знімаються та попередньо обробляються, потім добуваються та зберігаються в базі знань специфічні ознаки підпису. На останньому етапі (етап класифікації) добуті ознаки «порівнюються» із шаблонними підписами, збереженими у базі знань, і визначається до якого класу належить досліджуваний підпис [9], [10].

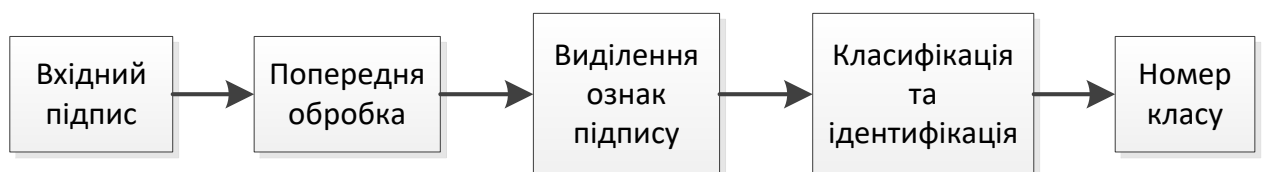


Рисунок 1.1 – Система ідентифікації підпису

Верифікація – це загальний процес прийняття рішення щодо підпису, в результаті чого визначається чи справжній підпис, чи підроблений. Тому це двокласове завдання класифікації. Етапи роботи системи верифікації показані на рис. 1.2. Етапи роботи системи верифікації підпису такі ж, як і системи ідентифікації, але вона відрізняється на етапі класифікації, оскільки ми наперед знаємо клас досліджуваного підпису та перевіряємо належність підпису до цього класу [9], [10].

Простими словами, верифікація – це коли відома особа підписанта, тобто це пошук «один на один» (1:1), тоді як ідентифікація – це коли не відома особа підписанта, тобто це пошук «один на N» (1:N) [9], [10].



Рисунок 1.2 – Система верифікації підпису

Хоча процеси верифікації та ідентифікації трохи відрізняються, алгоритми формування ознак підпису та алгоритми їх класифікації часто однакові що для верифікації, що для ідентифікації. Дана робота більше присвячена ідентифікації (розпізнаванню) підпису, оскільки це більш універсальний процес і він може застосовуватись не тільки для розпізнавання підписів, а і, наприклад, для розпізнавання особи по написанню парольного слова у системах з обмеженим доступом [11], [12].

Існує два основних типи ідентифікації та верифікації підписів: офлайн (статична) та онлайн (динамічна) [9], [13]-[15]. В офлайн-системах аналізується статичне зображення підпису, яке вже зафіксоване на якомусь документі, зазвичай паперовому (банківські чеки, розписки, угоди і т.п.). У цьому випадку система повинна зчитувати (сканувати) та витягувати ознаки із зображення підпису. Це відрізняється від онлайн-систем, де використовуються для написання підпису такі пристрої, як планшети та смартфони. Ці пристрої дозволяють збирати додаткову інформацію про сам процес формування підпису, наприклад, залежність зміни координат пера від часу, тиск пера на планшет, кількість рухів вгору-вниз, азимут пера під час підписання користувачем та ін., що дозволяє отримати більше можливостей для точнішої ідентифікації та верифікації підписів [9], [13]-[15]. Очевидно, що онлайн (динамічна) ідентифікація та верифікація підписів є більш

перспективною, ніж офлайн (статична). Тому дана робота присвячена саме динамічній ідентифікації підписів.

1.1.2 Загальна схема динамічної ідентифікації підпису

Загальна схема динамічної ідентифікації підпису зображена на рис. 1.3. 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 $P(t)$ та ін.. Ці параметри видаються у вигляді оцифрованих відліків відповідних величин у дискретні моменти часу із певним часовим кроком [9], [13]-[15].

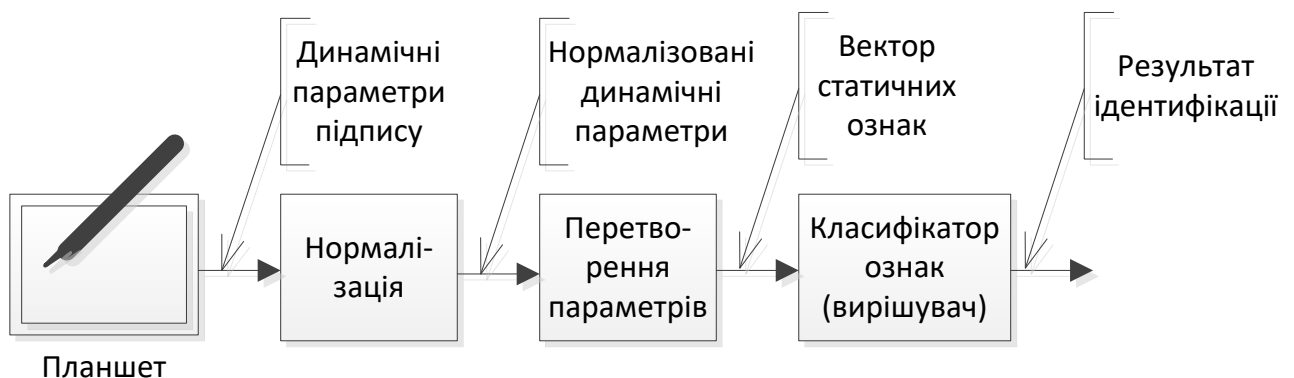


Рисунок 1.3 – Загальна схема динамічної ідентифікації підпису

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 [16], [17], Уолша [15], Хаара [15], вейвлет [18], сплайни [19] та ін. У результаті отримують вектор чисел (статичних ознак), які потім використовуються у класифікаторах [20] різних типів для отримання результату ідентифікації. Як класифікатори використовують структурні [21], статистичні [22], неймережеві [23], [24], [25] та ін.

Які слабкі місця такої схеми ідентифікації? По-перше, при перетворенні динамічних параметрів у статичні втрачається велика частина корисної інформації, що знижує достовірність ідентифікації. По-друге, достовірність ідентифікації 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 [26], [27], [28], які є набагато складнішими. Звідси випливає задача дослідження – запропонувати такі класифікатори, які працюють безпосередньо з динамічними параметрами підпису, а не із статичними векторами. Це дозволить уникнути перетворення динамічних параметрів у статичні і не втрачати велику частину корисної інформації, що у підсумку має підвищити достовірність ідентифікації.

1.2 Динамічні ознаки підпису та їх властивості стосовно процесу ідентифікації

1.2.1 Процес отримання первинних динамічних ознак підпису

Для отримання первинних динамічних ознак підпису може використовуватись велика кількість можливих пристроїв, наприклад, цифровий планшет, мобільний телефон та ін.

Частіше всього використовують графічні планшети, які видають такі первинні динамічні параметри підпису [9], [13]-[15] (див. рис.1.4):

- 1) координата пера $X(t)$;
- 2) координата пера $Y(t)$,
- 3) тиск пера на графічний планшет $Z(t)$;
- 4) кут нахилу пера до площини планшету $\chi(t)$;
- 5) азимут руху пера $\alpha(t)$.

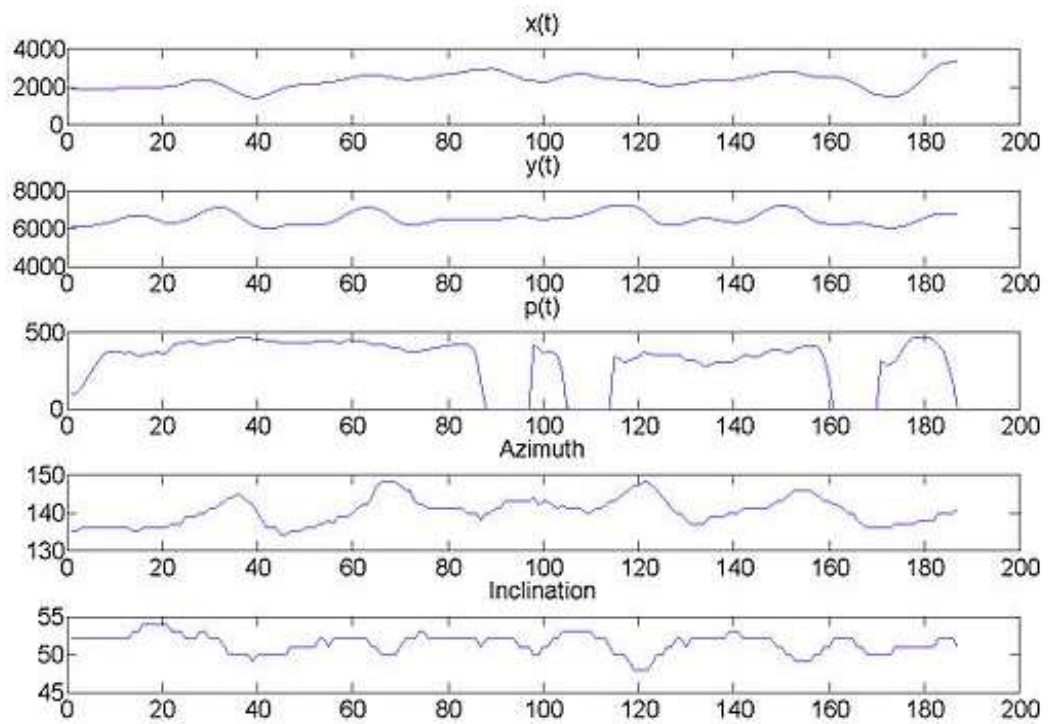


Рисунок 1.4 – Приклад первинних динамічних параметрів підпису, які видають графічні планшети

Але отримувані первинні динамічні параметри підпису не є стабільними, тобто однозначно повторюваними для підпису однієї особи, тому що на них впливають фактори збурень, які можна розділити на два типи [15]:

1) зовнішні фактори (засоби, якими здійснюється підпис, інструментальні похибки процесу оцифровування, включно роздільну здатність та частоту дискретизації, фоновий шум, наявність на руках підписанта ювелірних виробів і т.п.);

2) внутрішньоперсональна варіабельність.

Внутрішньоперсональна варіабельність означає несхожість між підписами, виконаними одним і тим самим підписантом. На внутрішньоперсональну варіабельність може впливати:

- 1) емоціональний стан,
- 2) стрес,
- 3) втома,

- 4) вплив алкоголю чи наркотиків,
- 5) нейро-моторні стани,
- 6) ефекти біологічного старіння,
- 7) когнітивно-моторні порушення

та інші фактори, які є наслідками настрою людини, часу, доступного для написання підпису або готовності до співпраці. Також підписант може змінювати масштаб підпису, зсувати початок підпису відносно початку координат планшету, міняти нахил написання підпису відносно сторін планшету, Це представляється як зміни масштабу, зсуву і повороту підпису. Тому ми можемо описати вимірний підпис як суму корисного сигналу із зовнішніми та внутрішніми збуреннями.

1.2.2 Внутрішньоперсональна варіабельність підпису

На рис. 1.5 зображено приклад підпису. Зображення побудовано по інформації, взятій із відомої бази даних Deep SignBD [29], [30], [31].

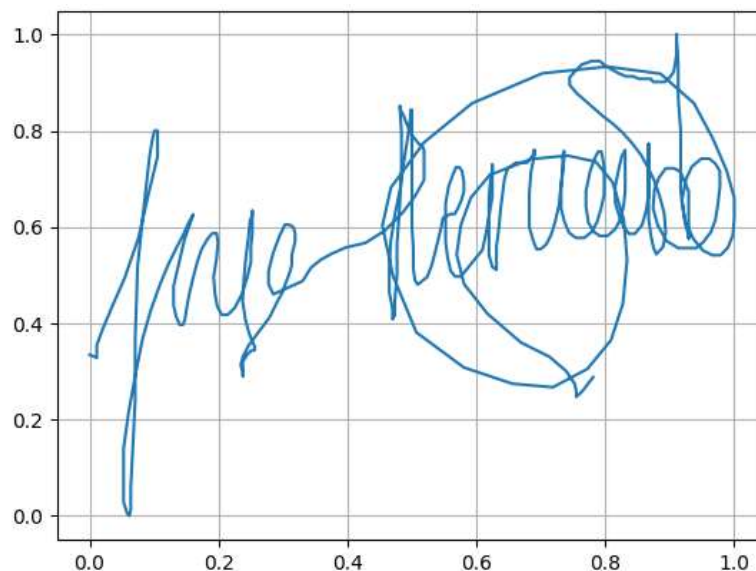


Рисунок 1.5 – Приклад зображення підпису із бази даних Deep SignBD

На рис.1.6 показано графік зміни координати $X(t)$ пера під час формування підпису для 5 різних реалізацій підпису однією особою. Із

рис.1.6 добре видно, що ці 5 динамічних характеристик $X(t)$ відрізняються як по тривалості написання, так і по характеру залежності від часу. Цей факт якраз і підтверджує внутрішньоперсональну варіабельність підпису.

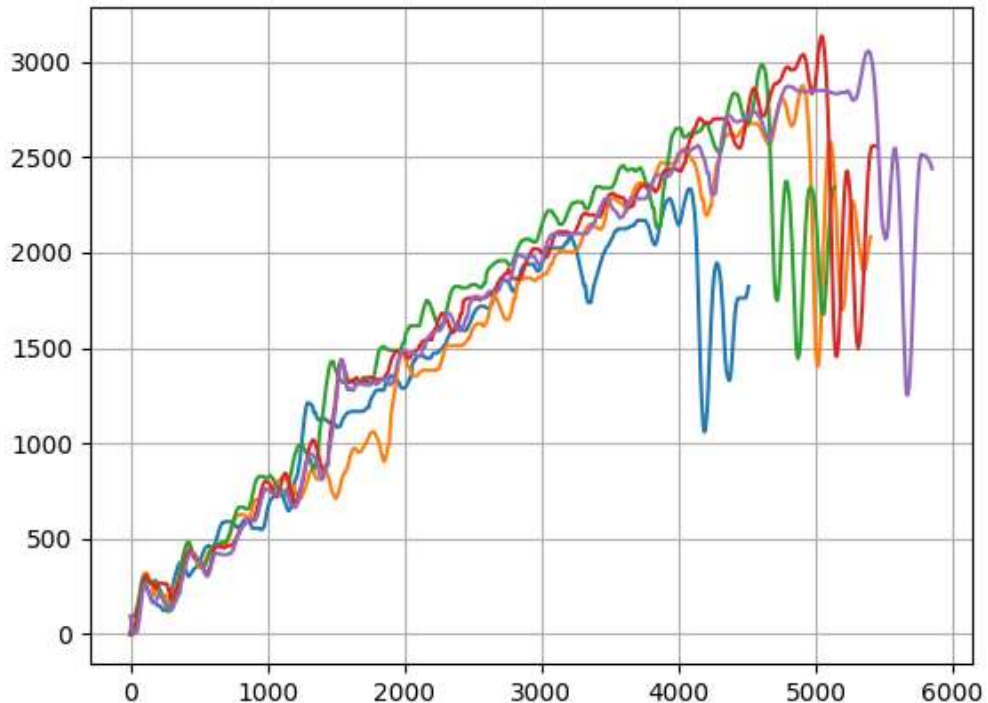


Рисунок 1.6 – Графіки зміни координати $X(t)$ пера під час формування 5 різних реалізацій підпису однієї особи

Для прикладу представлена тільки залежність $X(t)$, хоча для залежностей $Y(t)$, тиску пера на графічний планшет $P(t)$, куту нахилу пера до площини планшету $\chi(t)$ та азимуту руху пера $\alpha(t)$ залежності будуть аналогічні. Для зменшення внутрішньоперсональної варіабельності первинні динамічні параметри підпису нормалізують як по тривалості, так і по амплітуді. На рис. 1.7 показано вже нормалізовані графіки зміни координати $X(t)$ пера під час формування підпису для 5 різних реалізацій підпису однією особою. Із рис. 1.7 добре видно, що ці 5 динамічних характеристик $X(t)$ вже менше відрізняються по характеру залежності від часу, а по тривалості написання всі приведені до одного діапазону.

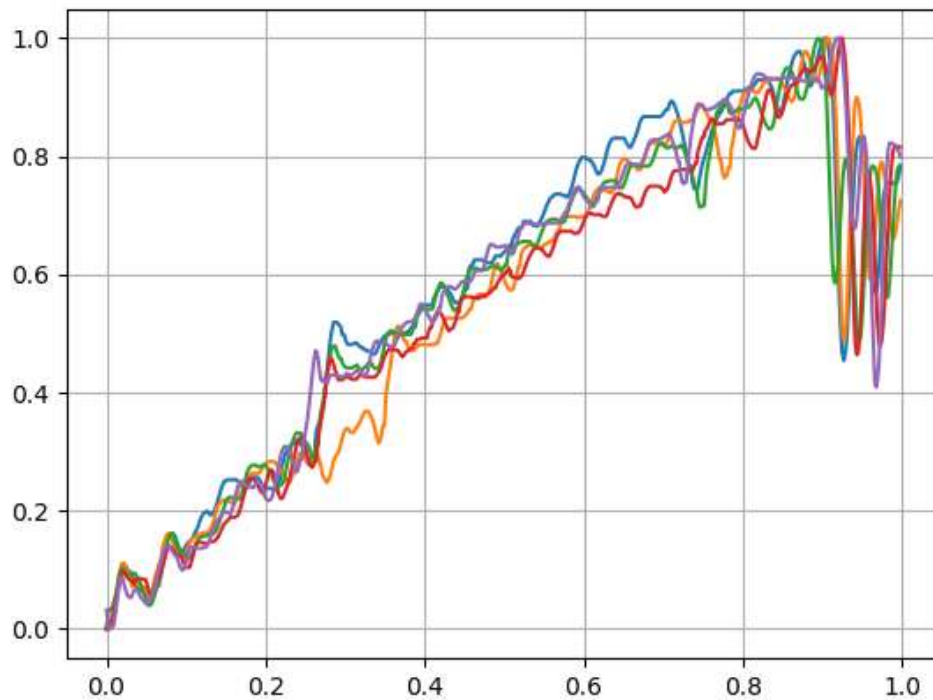


Рисунок 1.7 – Нормалізовані графіки зміни координати $X(t)$ пера під час формування 5 різних реалізацій підпису однієї особи

Але слід зауважити, що навіть нормалізовані динамічні параметри все-одно мають велику внутрішньоперсональну варіабельність. Звідси виникає перше наукове завдання – обирати (або формувати) такі динамічні параметри підпису, які будуть мати мінімальну внутрішньоперсональну варіабельність, а іншими словами – параметри, робастні (стійкі) до внутрішньоперсональної варіабельності.

Таким чином, для побудови високодостовірних систем ідентифікації підпису потрібно використовувати динамічні параметри, робастні (стійкі) до внутрішньоперсональної варіабельності.

1.2.3 Міжперсональна варіабельність підпису

Окрім внутрішньоперсональної варіабельності підпису, найбільшою проблемою, з якою стикаються системи ДП, є непередбачувано мала міжперсональна варіабельність. Це означає схожість між підписами, виконаними різними авторами. Міжперсональну варіабельність зменшують,

підробляючи оригінальний підпис через три основні види підробок:

1) Випадкові підробки (ВП) – Random Forgeries (RF): це ситуація, коли фальсифікатор, не маючи попереднього знання про конкретний підпис, намагається підтвердити особу підписувача, використовуючи власний справжній підпис.

2) Проста підробка (ПП), Simple Forgery (SF): Це відбувається, коли фальсифікатор знає ім'я підписувача, але не має доступу до зразка підпису. Важливо, що якість перевірки підпису залежить від країни походження стилю підпису. У деяких країнах багато людей підписуються просто написанням власного імені та прізвища, тоді як в інших країнах підписувачі оформляють нерозбірливі підписи зі складними розгалуженнями або вензелями.

3) Кваліфіковані підробки (КП), Skilled Forgeries (SK): їх виробляє фальсифікатор, який дізнався підпис своєї жертви і намагається відтворити його з подібною внутрішньоперсональною варіабельністю. Тест на підробку цього типу є найбільш складним та актуальним при ідентифікації підпису.

Очевидно, що треба будувати такі системи ДІП, які детектують навіть невелику міжперсональну різницю, тобто є дуже чутливими до невеликої міжперсональної варіабельності. Вирішити цю задачу можна як на етапі формування динамічних ознак підпису (синтезувати специфічні динамічні ознаки, чутливі до міжперсональної варіабельності), так і на етапі класифікації ознак, використовуючи високороздільні методи та засоби класифікації.

1.2.4 Вимоги до визначення оптимального набору динамічних ознак підпису

Огляд літератури показав, що різні розробки ДІП використовують різні набори динамічних ознак підпису. Так наприклад у [18] використовують всього 3 параметри: координата пера $X(t)$, $Y(t)$, азимут руху пера $\alpha(t)$. А в [29] використовують 23 параметри, представлені у табл. 1.1.

Таблиця 1.1 – Набір функцій часу, розглянутих у роботі [29].

#	Динамічний параметр
1	Х-координата: x_n
2	Y-координата: y_n
3	Тиск пера (ручки): z_n
4	Кут дотичної до траєкторії: θ_n
5	Швидкість руху пера: v_n
6	Радіус кривизни ділянки: p_n
7	Загальна величина прискорення: a_n
8-14	Похідна функцій першого порядку від параметрів 1-7: $x'_n, y'_n, z'_n, \theta'_n, v'_n, p'_n, a'_n$
15-16	Похідна функцій другого порядку від параметрів 1-2: x''_n, y''_n
17	Співвідношення мінімальної до максимальної швидкості у вікні з 5 зразками: v_n^r
18-19	Кут послідовних зразків та різниця першого порядку: a_n, a'_n
20	Синус: s_n
21	Косинус: c_n
22	Відношення довжини штриху до ширини у вікні з 5 зразками: r_n^5
23	Відношення довжини штриху до ширини у вікні з 7 зразками: r_n^7

Виникає запитання: а скільки оптимально потрібно обирати динамічних параметрів і які саме, щоб досягти максимальної достовірності динамічної ідентифікації підписів при мінімумі витрат? З одного боку, чим більше взяти параметрів, тим точніше має бути робота системи. Але, з іншого боку, обробка великої кількості параметрів вимагає більших обчислювальних ресурсів і більше часу на прийняття рішення. Також не зрозуміло чи виправдано обирати велику кількість параметрів, адже всі вони не є незалежними, оскільки обчислюються по чотирьох первинних параметрах ($x(t)$, $y(t)$, $p(t)$ та $\eta(t)$). Тобто це питання також потребує додаткового дослідження з метою виявлення інформативності окремих параметрів та ступеню їх впливу на загальну достовірність процесу ідентифікації підпису.

1.3 Методи та засоби динамічної ідентифікації підписів та перспективи їх вдосконалення

1.3.1 Класифікація методів ідентифікації підписів

У науковій літературі наведено детальний аналіз методів і засобів ідентифікації та верифікації підписів [9], [13]-[15]. Але для наочності варто було б розробити класифікаційну таблицю. Головною класифікаційною ознакою є вид процесу ідентифікації підпису: статична (Offline) або динамічна (Online) ідентифікація підпису. Класифікаційна таблиця [1] методів ідентифікації підписів зображена на рис. 1.8. Статична (Offline) ідентифікація підписів є менш перспективною, тому в рамках цієї роботи не розглядається.



Рисунок 1.8 – Класифікаційна таблиця методів ідентифікації підписів

Динамічну (Online) ідентифікацію 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 планшету $\mu(t)$, іноді азимут руху пера $\alpha(t)$. Із цих основних динамічних параметрів часто пропонують отримувати похідні параметри та використовувати їх. Такими похідними параметрами часто 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 [32], [33] різних динамічних параметрів та їх стійкості до внутрішньоперсональної варіабельності підписів [34], [35].

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 [36].

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 [16], [17], Уолша [15], Хаара [15], виділення головних компонент (Principal Component Analysis – PCA [37]), дискретне вейвлет-перетворення (DWT) [18], сплайни [19] і т.і.

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 [34] (Евклідова, Махаланобіса та ін.). Більше переваг мають методи на основі прихованих марковських моделей [38], машин опорних векторів (support vector machine – SVM) [39] та штучних нейронних мереж (ШНМ) [18], [37], [40]. Останні все частіше використовуються у процесі Online ідентифікації та верифікації підпису.

1.3.2 Перспективні методи класифікації динамічних ознак підпису на основі нейронних мереж

В останні роки спостерігається перехід від традиційних ШНМ [41] (багатошаровий персептрон – БШП [40], РБФ [41] та нейро-нечіткі [43]) до сучасних парадигм ШНМ (згорткові [7], [44], рекурентні [30], спайкінгові [45]). Найперспективнішими є рекурентні [46] та спайкінгові [47], [48] нейронні мережі, оскільки вони дозволяють класифікувати функції часу (часові ряди) так як вони є, тобто без перетворення у вектори статичних ознак.

Було знайдено 2 публікації [45], [49] 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 роботі.

1.4 Оцінка достовірності роботи систем ідентифікації підписів

Для оцінки достовірності роботи систем динамічної ідентифікації підписів потрібно 2 речі:

- 1) бази даних динамічних параметрів підписів, у яких є як справжні підписи користувачів, так і майстерно підроблені підписи,
- 2) загальноприйняті показники достовірності роботи систем ідентифікації підписів.

Розглянемо їх детальніше.

1.4.1 Бази даних підписів

Для того, щоб можна було справедливо порівнювати різні алгоритми динамічної ідентифікації підписів між собою, розробники цих алгоритмів мають перевіряти якість їх роботи на одних і тих самих наборах підписів. Такі набори підписів (бази даних) повинні містити підписи якомога більшої кількості людей. Причому для однієї людини повинно бути декілька справжніх підписів, взятих бажано в різні моменти часу і їх фізичного та емоційного стану.

Для надійного тестування поточних та майбутніх алгоритмів потрібні великі проекти зі збору величезних рукописних баз даних підписів або відкриті ініціативи урядових даних. Ці реальні бази даних повинні будуватися відповідно до етичних аспектів, таких як конфіденційність донорів.

Докладний огляд баз даних підписів, що використовуються в дослідженнях, зроблено в [9], [13]-[15]. Найбільш відомі та доступні бази даних онлайн підписів, які використовуються для створення загальних орієнтирів та порівняння результатів досліджень, перераховані в табл. 1.2.

Таблиця 1.2 – Найбільш відомі бази даних онлайн підписів

Назва БД	Модалність	Сценарій	Характеристика	Особливості
MCYT-100 [50], [51]	Online	Western	G:2500, F:2500, W:100	This is a subset of online MCYT-330
SUSIG-Blind [52]	Online	Western	G:820, F:880, W:88	Volunteers did not see visual feedback while signing
e-BioSign-DS1-Signature DB [53]	Online	Western	G:520 x 5, F:390 x 5, W:65x 5	5 different writing tools (stylus and finger). Taken in two sessions
BSEC 2009 [54]	Online	Western	G:6480, F:4320, W:432	Taken in two sessions. Digitizing tablet and a PDA
SVC-Task1 [55]	Online	Chinese and English	G:800, F:800, W:40	Only dynamic trajectory. Donors did not use their real signature
BiosecurID-SONOF [56]	On- and offline	Western	G:2112 Ч 3, F:1584 Ч 3, W:132 Ч 3	Taken in four sessions. Real on/off and synthetic off data
DeepSignDB [29]	Online	Western	G:, F:, W:1526	

G: справжніх підписів, F:майстерно підроблених підписів, W:осіб

Бази даних підписів повинні збирати реалістичну мінливість підписів, як внутрішньоперсональну, так і міжперсональну. Важко оцінювати якість різних баз даних підписів, оскільки відсутній статистичний аналіз зібраних у них підписів на предмет повноти і пропорційності врахування всіх факторів, що впливають на внутрішньоперсональну та міжперсональну варіабельність підписів. Крім того, людські помилки, такі як неправильне маркування зразків, можуть внести упередження в оцінку роботи алгоритму.

1.4.2 Показники якості роботи систем ідентифікації підписів

Основне призначення системи ідентифікації підпису полягає у диференціації класів підписів на основі аналізу їх динамічних параметрів. Для конкретної особи існують два класи підписів: справжні та підроблені підписи. Справжній підпис – це підпис, який належить визначеній особі. Підроблений підпис – це імітований підпис особи, створений іншою особою. Одним із ключових факторів системи ідентифікації підписів є виявлення підробленого підпису з метою зменшення кількості злочинів та злому інформації. Таким чином, механізми системи ідентифікації підпису визначають справжність підпису. Підроблені підписи можна додатково класифікувати на три класи:

- 1) випадкова підробка (random forgery),
- 2) проста підробка (simple forgery),
- 3) кваліфікована підробка (skilled forgery).

При випадковій підробці (підробці нульових зусиль) [9] особа не має інформації про ім'я оригінальної особи та форму підпису. Проста підробка – це непрофесійна підробка, в якій ім'я оригінального підписувача відомо, але інформація про форму підпису невідома [9]. Однак кваліфікована (або змодельована) підробка є майстерною імітацією справжнього підпису. У цьому типі підробки зловмисник знає ім'я оригінального підписувача та

форму його підпису, тому його важче виявити [9].

Щоб вирішити, чи хороша система ДІП чи ні, ми повинні оцінити її якість. Показник якості систем ідентифікації та верифікації підписів має визначати наскільки вірно система визначає справжні та підробні підписи. Причому, важливо наскільки система вірно визначає саме кваліфіковано підроблені підписи, бо випадково підроблені підписи та прості підробки визначаються набагато легше. Зазвичай використовується декілька видів помилок. Причому ці види помилок трохи різні для систем ідентифікації підпису та для систем верифікації підпису.

Якість систем *ідентифікації* підписів оцінюється за допомогою однієї з таких метрик [9]:

1) Достовірність ідентифікації (Identification rate – IR):

$$IR = \frac{\text{Кількість правильних ідентифікацій для всіх користувачів}}{\text{Загальна кількість всіх підписів всіх користувачів, поданих на ідентифікацію}} \times 100\% \quad (1.1)$$

2) коефіцієнт вірної класифікації (The Correct Classification Rate – CCR)

$$CCR = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \quad (1.2)$$

де: TP (True positive, віропозитивні): кількість справжніх підписів, які були правильно ідентифіковані, TN (True Negative, вірнегативні): кількість підробних підписів, які були правильно ідентифіковані, FP (False positive, хибнопозитивні): кількість підробних підписів, які були неправильно ідентифіковані як справжні, FN (False Negative, хибнегативні): кількість справжніх підписів, які були невірно ідентифіковані як підробні.

Як видно із співвідношень (1.1) та (1.2), достовірність ідентифікації та CCR це одне й те саме.

Якість систем *верифікації* підписів, як правило, оцінюється на основі двох параметрів – коефіцієнта помилкового відхилення (FRR – False

Rejection Rate) та коефіцієнта помилкового прийняття (FAR) [57], [58]:

1) коефіцієнт помилкового відхилення (FRR – False Rejection Rate): співвідношення автентичних користувачів, яких неправильно відхилено. Він розраховується як:

$$FRR = \frac{FN}{\text{кількість справжніх підписів}} \times 100\% \quad (1.3)$$

2) коефіцієнт помилкового прийняття (FAR – False Acceptance Rate): співвідношення підробних підписів, які приймаються системою як справжні. Він розраховується як:

$$FAR = \frac{FP}{\text{кількість підробних підписів}} \times 100\% \quad (1.4)$$

Для вітчизняної термінології характерно називати FRR показником помилок I роду, а FAR – показником помилок II роду.

FRR та FAR часто використовують, щоб знайти криву робочої характеристики приймача (ROC curve – Receiver operating characteristic curve) та еквівалентний коефіцієнт помилок (EER – equal error rate) [9] так:

3) Крива робочої характеристики приймача (ROC curve – Receiver operating characteristic curve).

Крива ROC є найбільш часто використовуваним методом для оцінювання якості біометричних систем. Він побудований для подання FAR відповідно до FRR (рис. 1.9). Перевага цього методу полягає в тому, що він дає точне уявлення про якість біометричної системи за допомогою єдиної кривої, що дозволяє порівнювати різні біометричні системи [59]. Тоді ми можемо обчислити площу під кривою (area under the curve – AUC) і еквівалентний коефіцієнт помилок (equal error rate – EER). Високий AUC і низький рівень EER означають, що якість системи хороша. Оптимальний результат отримується, якщо AUC дорівнює 1, а EER дорівнює 0.

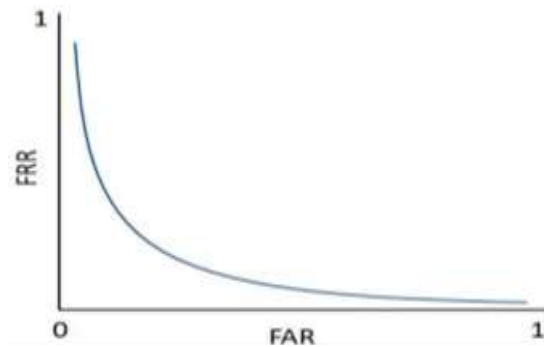


Рисунок 1.9 – Простий приклад кривої ROC: FAR проти FRR

4) Еквівалентний коефіцієнт помилок (EER – equal error rate).

Цей коефіцієнт помилок збігається з точкою, в якій перетинаються FAR та FRR, як показано на рис. 1.10. Він широко використовується для оцінки та порівняння біометричних систем ідентифікації. Коли EER становить близько 0,0%, це означає, що ефективність цільової системи є найкращою [60]. Ми можемо розрахувати достовірність верифікації та ідентифікації за допомогою EER наступним чином:

$$\text{Accuracy} = 100\% - \text{EER} \quad (1.5)$$

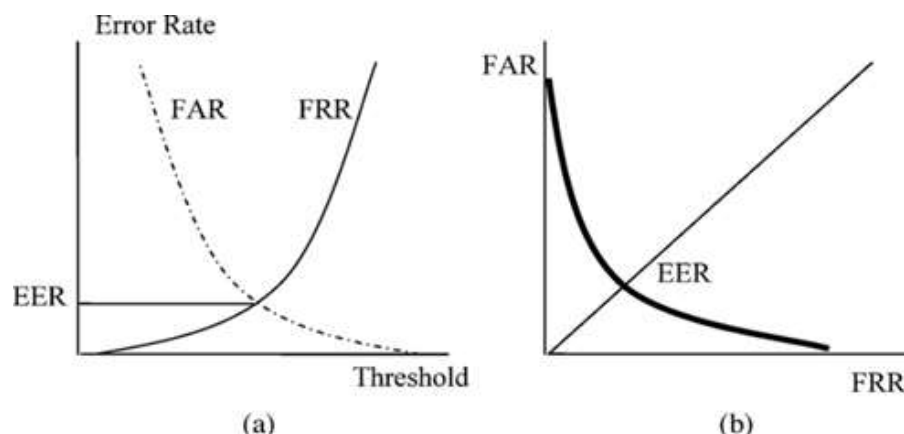


Рисунок 1.10 – Приклад EER (a) – з використанням кривих FRR та FAR.
(b) – за допомогою кривої ROC.

Теоретично, справжні підписи завжди повинні набирати вищі результати, ніж підроблені. Тоді єдиний поріг може бути використаний для

відокремлення справжнього підпису від підробленого. Загалом, алгоритм верифікації приймає рішення на основі порогового значення (threshold на рис. 1.10a), яке визначає, наскільки близьким до шаблону повинен бути вхідний підпис, щоб його можна було вважати справжнім. Якщо поріг буде зменшено, то помилкових сприйнять підробних підписів буде більше, але менше стане помилкових несприйнять справжніх підписів. Відповідно, більш високий поріг зменшить кількість помилкового сприйняття підробних підписів, але збільшить кількість помилкового відхилення справжніх підписів. У деяких випадках підробні підписи мають більший збіг з еталоном, ніж справжні підписи користувача. З цієї причини, яким би не було обрано поріг, трапляються деякі помилки класифікації.

У табл. 1.3 представлено показники достовірності недавніх систем ідентифікації підписів.

Таблиця 1.3 – Порівняння достовірності різних методів динамічної ідентифікації підписів

	Джере_ло (рік)	Набір даних при тестуванні	Використовувані динамічні ознаки	Вид класифікатора	Оцінка достовірності
1	2	3	4	5	6
1.	[61] 2018	1) містить 240 підписів, взятих у десяти осіб 2) містить 768 підписів, взятих у 32 осіб	Використовує speed up robust features (SURF)	Машина опорних векторів (Support vector machine – SVM)	98.75% достовірність для БД 1) та 97.7% достовірність для БД 2)
2.	[23] 2015	Зібрано два набори набору даних, набір даних I містить 25 зразків підписів для кожного підписувача. Набір даних II містить 46 зразків підписів для кожного підписувача	9 глобальних ознак	нейронна мережа прямого поширення	98% достовірність для БД I і 89% достовірність для БД II
3.	[62] 2011	невеликий набір даних з 27 користувачів	Теорія графів	Норма графа	94.25% достовірність
4.	[63] 2018	набір даних складається з 10 користувачів з 10 справжніми підписами та 10 підробленими підписами на кожного користувача	Виділено деякі ознаки (координати, тиск, кут нахилу пера та азимут), які є функцією часу t	Був використаний алгоритм DTW для обчислення відстані деформації, щоб відрізнити справжній підпис від його підробки та прийняти рішення про результат верифікації.	Ця система може виявити підроблені підписи з достовірністю до 90,4%.

Таблиця 1.3 – (продовження)

	Джерело (рік)	Набір даних при тестуванні	Використовувані динамічні ознаки	Вид класифікатора	Оцінка достовірності
1	2	3	4	5	6
5.	[64] 2016	Китайський набір даних із SigComp2011 та набір даних MCYT 100	Виділяється 15 функціональних ознак	DTW	1,69% EER для китайського набору даних і 1,77% EER для MCYT-100.
6.	[65] 2015	Японський набір даних із ICDAR2013, який містить дані від 11 авторів для навчальної множини та 20 авторів для тестової множини.	Витягуються за доп. Комбінації: функцій на осн. Перетворення Фур'є, функцій на основі вейвлет-перетворення та глобальних функцій	кореляція	27.48 % FAR , 25.54% FRR і 73.49% достовірність
7.	[66] 2015	БД : ATVS, SVC, SUSIG	Функції були вивчені з набору даних ATVS за доп. Розрідженого автоенкодера з одним прихованим шаром	Однокласовий класифікатор	0.83% EER для БД SVC2004 і 0.77% EER для БД SUSIG
8.	[67] 2013	SVC	Wavelet перетворення	Нейронна мережа	3.5% EER
9.	[68] 2007	БД SVC 2004	Базисні функції, Геометрична нормалізація, Розширені функції, Похідні за часом, Нормалізація сигналу	Приховані Марківські моделі (Hidden Markov Models – HMM)	6.9% і 3.02% EER для кваліфікованих і випадкових підробок для БД SVC 2004

Із табл. 1.3 видно, що достовірність варіюється від 73% до 98,75%. Але ці показники не є однозначними характеристиками систем, оскільки достовірність залежить не тільки від функціонування самої системи, а від процесу проведення статистичного аналізу достовірності, від бази даних, на якій перевіряється система. Яскравим доказом цього є те, що одна і та сама система на одному датасеті показує достовірність 98% (2-й рядок табл. 1.3), а на іншому – 89%. Крім того, навіть якщо дві різні системи перевіряються на одному датасеті, то отримані результати не порівнюють їх однозначно, так як не ясно яке співвідношення у тестовому наборі кваліфікованих та простих підробок. І навіть якщо тестування здійснюються тільки на кваліфікованих підробках, то ще треба, щоб їх набір (перелік конкретно взятих підробних підписів) був ідентичним для обох систем. Адже одні кваліфіковані підробки є більш схожими на оригінал, а інші – менш схожими.

Все вищезазначене говорить про складності у порівнянні ефективності різних систем ДІП, доки не буде розроблено стандартного протоколу

порівняння, у якому однозначно буде описано навчальний та тестувальний датасети не у термінах відсотків і статистичних параметрів, а конкретно вказано які саме підписи беруться для навчання системи, а які для тестування.

1.5 Постановка задач дослідження

Отже, можна виділити такі основні недоліки процесу ДП та задачі дослідження, які ними викликані.

Недолік 1.

Отримувані первинні динамічні параметри підпису не є стабільними, тобто однозначно повторюваними для різних реалізацій підпису однієї особи. Кожна реалізація підпису відрізняється масштабом, зсувом (початок підпису на планшеті), поворотом (нахил підпису) та часом написання. Дещо компенсувати вплив масштабу та зсуву вдається амплітудною нормалізацією параметрів, вплив часового масштабу – часовою нормалізацією параметрів. Вплив повороту вже важче компенсувати. Але слід зауважити, що навіть нормалізовані динамічні параметри все-одно мають велику внутрішньоперсональну варіабельність.

Задача 1.

Потрібно обирати (або формувати) такі динамічні параметри підпису, які будуть мати мінімальну варіабельність, викликану зміною масштабу, зсуву та повороту. Іншими словами – запропонувати набір параметрів, які є інваріантними до масштабу, зсуву та повороту підпису відносно планшету, що дозволить збільшити достовірність ідентифікації підпису

Недолік 2.

Нестабільність (варіабельність) первинних та вторинних динамічних параметрів підпису також викликана нестабільністю почерку людини, її емоційним станом, втомою та іншими факторами. Це також збільшує внутрішньоперсональну варіабельність підпису і зменшує достовірність

ідентифікації.

Задача 2.

Дослідити внутрішньоперсональну варіабельність різних динамічних параметрів підпису і обрати такі динамічні параметри підпису, які будуть мати мінімальну внутрішньоперсональну варіабельність, а іншими словами – параметри, робастні (стійкі) до внутрішньоперсональної варіабельності.

Недолік 3.

Окрім внутрішньоперсональної варіабельності підпису, найбільшою проблемою, з якою стикаються системи ДПП, є непередбачувано мала міжперсональна варіабельність. Це означає схожість між підписами, виконаними різними авторами, тобто міжперсональна варіабельність є малою між дійсним підписом та майстерно підробленим підписом.

Задача 3.

Розробити такі системи ДПП, які детектують навіть невелику міжперсональну різницю, тобто є дуже чутливими до невеликої міжперсональної варіабельності. Вирішити цю задачу можна як на етапі формування динамічних ознак підпису (синтезувати специфічні динамічні ознаки, чутливі до міжперсональної варіабельності), так і на етапі класифікації ознак, використовуючи високороздільні методи та засоби класифікації.

Недолік 4.

Різні розробки ДПП використовують різні набори динамічних ознак підпису – від одиниць до десятків. Виникає запитання: а скільки оптимально потрібно обирати динамічних параметрів і які саме, щоб досягти максимальної достовірності динамічної ідентифікації підписів при мінімумі витрат? З одного боку, чим більше взяти параметрів, тим точніше має бути робота системи. Але, з іншого боку, обробка великої кількості параметрів вимагає більших обчислювальних ресурсів і більше часу на прийняття рішення. Також не зрозуміло чи виправдано обирати велику кількість параметрів, адже всі вони не є незалежними, оскільки обчислюються по

чотирьох первинних параметрах ($x(t)$, $y(t)$, $p(t)$ та $\lambda(t)$).

Задача 4.

Дослідити інформативність окремих динамічних параметрів підпису та ступінь їх впливу на загальну достовірність процесу ідентифікації підпису. Обґрунтувати вибір оптимальних наборів динамічних параметрів підпису.

Недолік 5.

Більшість відомих систем ДПП використовують перетворення динамічних параметрів підпису у статичні вектори чисел, які потім класифікуються за допомогою класифікаторів статичних ознак. По-перше, при перетворенні динамічних параметрів у статичні ознаки втрачається велика частина корисної інформації, що знижує достовірність ідентифікації. По-друге, достовірність ідентифікації дуже залежить від обраної «пари» (вид перетворення динамічних параметрів)-(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.

Задача 5.

Запропонувати такі класифікатори, які працюють безпосередньо з динамічними параметрами підпису, а не із статичними векторами. Це дозволить уникнути перетворення динамічних параметрів у статичні і не втрачати велику частину корисної інформації, що у підсумку має підвищити достовірність ідентифікації.

Недолік 6.

Для оцінки достовірності систем ДПП використовують різноманітні бази даних підписів. Якість цих баз даних не однакова щодо повноти і пропорційності врахування всіх факторів, що впливають на внутрішньоперсональну та міжперсональну варіабельність підписів. Складно порівнювати ефективності різних систем ДПП, оскільки немає стандартного протоколу порівняння, у якому однозначно було б визначено навчальний та тестувальний датасети.

Задача 6.

Розробити стандартний протокол порівняння систем ДП, у якому однозначно буде описано навчальний та тестувальний датасети, тобто конкретно вказано які саме підписи беруться для навчання системи, а які для тестування.

Задачі 1-3 та 5 розглядаються у цій роботі, а задачі 4 та 6 планується розв'язати у подальших дослідженнях.

1.6 Висновки до першого розділу

1. Розглянуто співвідношення понять верифікація та ідентифікація підписів. Описано загальну схему динамічної ідентифікації підпису.

2. Проаналізовано процес отримання первинних динамічних ознак підпису та такі їх властивості як внутрішньоперсональна та міжперсональна варіабельність. Сформульовано вимоги до визначення оптимального набору динамічних ознак підпису.

3. Проведено класифікацію відомих методів та засобів динамічної ідентифікації підписів та сформульовано перспективи їх вдосконалення, що полягають у використанні динамічних класифікаторів на основі спайкінгових нейронних мереж та використанні динамічних параметрів підписів, стійких до внутрішньоперсональної варіабельності та чутливих до міжперсональної варіабельності.

4. Проведено аналіз баз даних підписів та показників достовірності, що використовуються при оцінці якості систем динамічної ідентифікації підписів.. Запропоновано напрямки їх вдосконалення.

5. Виділено недоліки існуючих систем динамічної ідентифікації підписів та сформульовано задачі досліджень.

Основні результати, викладені у розділі, опубліковано в роботах [1], [2], [3], [7], [8].

РОЗДІЛ 2

СПАЙКІНГОВІ НЕЙРОННІ МЕРЕЖІ ТА ЇХ ЗАСТОСУВАННЯ ДО ІДЕНТИФІКАЦІЇ ПІДПИСІВ

2.1 Обґрунтування перспективності використання спайкінгових нейронних мереж для динамічної ідентифікації підписів

Спайкінгові нейронні мережі (СНМ) [4], [47], [48], [69], [70] складаються з спайкінгових нейронних елементів [70]–[74]. Нейроморфність (схожість з біологічними нейронами) спайкінгових нейронних елементів полягає перш за все в тому, що на своєму виході (аксоні) вони формують не логічні рівні (як формальні нейрони Мак-Каллока і Пітса) і не безперервні рівні з діапазону $[0,1]$ або $[-1, 1]$, як аналогові нейронні елементи, а послідовність імпульсів, миттєва частота яких визначається мірою збудження нейрона у поточний момент часу.

СНМ не мають певних правил з'єднання нейронів між собою [47], [69], як, наприклад, в широко відомих мережах Хопфілда, Хеммінга, багатошарових персептронах та інших [41]. Вони є сукупністю нейронів, з'єднаних між собою випадковим чином, так, що є як прямі, так і зворотні зв'язки. Кожен нейрон мережі пов'язаний не з усіма іншими нейронами, а лише з деякими. При формуванні конкретної СНМ використовують результати нейрофізіологічних досліджень, якими, наприклад, встановлено, що, по-перше, в мозку людини сукупність нейронів в об'ємі масштабу 1 мм^3 формує відносно незалежну локальну мікромережу, що несе певне функціональне навантаження, по-друге, серед всіх зв'язків одного нейрона приблизно 20 % є гальмівними і ін. Тому такі СНМ часто називають генеричними рекурентними спайкінговими нейронними мережами [4].

Функціонування рекурентних мереж спайкінгових нейронів [47], [69], [75] засноване на ідеї так званого «рідкого комп'ютера» («liquid computer»

[76]), яка полягає в тому, що рідина деякий час зберігає інформацію про проведені над нею зовнішні дії у вигляді динамічно змінного стану її поверхневого хвилювання. Математичною моделлю «рідкого комп'ютера» є «автомат з рідкими станами» (за аналогією з кінцевими автоматами).

Концептуальна структура автомата з рідкими станами (АРС) полегшує аналіз можливостей реально-часових обчислень моделей нейронних мікромереж. Ця модель не вимагає побудови задачезалежної структури нейронної мережі і може використовуватися для аналізу обчислень довільно «знайдених» або побудованих моделей нейронних мікромереж. Ця модель також не вимагає жодного попереднього рішення відносно «нейронного коду», яким інформація представлена в мережі.

Основна ідея полягає в тому, що нейронна (рекурентна) мікромережа може служити як незміщена аналогова (короткочасна) пам'ять (неформально названа як «рідка») про поточні і попередні входні сигнали мережі. «Рідким станом» $x(t)$ (рис. 2.1) називають вектор вкладів всіх нейронів мікромережі в мембранний потенціал вихідного нейрона у час t . Відзначимо, що це є вся інформація про стан мікромережі, до якої вихідний нейрон підключений. На відміну від певних станів кінцевого автомата, «рідкий стан» АРС не потрібно технічно визначати (будувати) для специфічного завдання. Передбачається, що воно безперервно змінюється в часі, є достатньо чутливим і таким, що має високу розмірність для того, щоб містити всю інформацію, яка може бути необхідною для специфічних завдань.

Рекурентна мікромережа спайкінгових нейронів перетворює входні сигнали в стан $x(t)$, який розшифровується за допомогою вихідних функцій без пам'яті $f_1, \dots, f_n$ у вихідні сигнали $f_1(x(t)), \dots, f_n(x(t))$. «Рідкий стан» $x(t)$ нейронної мікромережі може бути перетворений у будь-який час t картою вихідних нейронів в деякий цільовий вихід $f(x(t))$ (який в загальному випадку видається із специфічним представленням або нейронним кодом). Структура АРС показана на рис. 2.1.

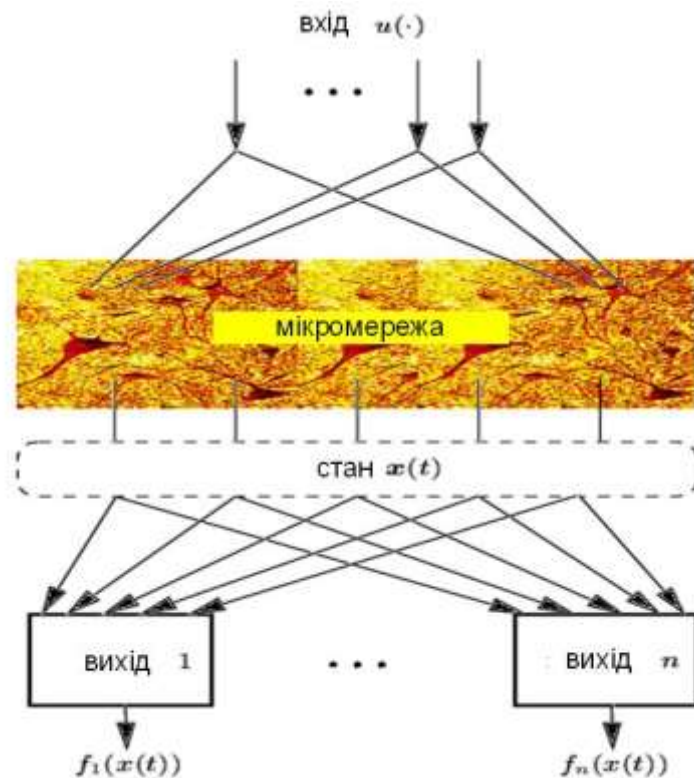


Рисунок 2.1 – Автомат з рідкими станами (АРС)

У [47], [75] показано, що лише синапси вихідних нейронів мають бути налаштовані для конкретного обчислювального завдання. Це вимагає, щоб будь-які дві різні вхідні часові послідовності $u_1(s)$, $s \leq t$ і $u_2(s)$, $s \leq t$, які повинні викликати різні вихідні сигнали в деякий подальший момент часу t , переводили рекурентну мережу в два істотно різних стани $x_1(t)$ і $x_2(t)$ у час t (властивість розділення). Іншими словами: поточний стан $x(t)$ мікромережі під час t повинен містити всю інформацію про попередні вхідні сигнали. Щоб мати універсальні обчислювальні можливості, АРС повинен задовольняти, окрім властивості розділення, ще і властивості апроксимації: вихідні нейрони мають бути здатні апроксимувати будь-яку задану неперервну функцію f , яка відображує поточний рідкий стан $x(t)$ в поточний вихід $v(t)$.

Якщо АРС володіє цими властивостями, то можливо навчити вихідні нейрони без пам'яті, щоб видавати бажаний вихідний сигнал у час t . Якщо час t змінюється, то можна використовувати такі ж принципи, аби видавати

як вихідний сигнал бажані часові серії імпульсів або функції часу t на тому ж виході. Це приводить до такої (автономної) процедури навчання вихідних нейронів, щоб виконати поставлене завдання:

1. Визначити нейронну мікромережу, яка повинна аналізуватися.
2. Записати стани $x(t)$ мікромережі в різні моменти часу у відповідь на багаточисельні різні (навчальні) вхідні сигнали $u(t)$.
3. Застосувати алгоритм навчання з учителем до набору навчальних прикладів у формі $[x(t), y(t)]$, щоб навчити вихідну функцію f , яка визначає фактичний вихідний сигнал $f(x(t))$, приймати значення, які були б якомога ближчими до цільового виходу $y(t)$.

Одна з переваг цього підходу полягає в тому, що немає необхідності брати до уваги будь-які часові аспекти задачі навчання, оскільки вся часова обробка зроблена неявно в рекурентній мережі. До того ж, жодне попереднє рішення не потрібне відносно нейронного коду, яким інформація про попередні вхідні сигнали кодується в поточному рідкому стані мережі. Відмітимо також, що АРС може легко здійснювати декілька обчислень паралельно, використовуючи ту ж саму рекурентну мережу. Просто доведеться навчати для кожного цільового виходу окремий вихідний нейрон, який може повністю використовувати ту ж саму рекурентну мережу.

Згідно з теоретичним аналізом цієї обчислювальної моделі [75], [77]-[79] немає жодних апіорних обмежень для здатності цієї моделі здійснювати в реальному часі обчислення з короткочасною пам'яттю. Природно, що для здійснення завдань, які вимагають великий об'єм пам'яті або велику стійкість до шуму при розділенні образів, знадобиться мережа з великою кількістю нейронів.

Спайкінгові нейронні мережі, завдяки своїй нейроморфності (схожість з мережами біологічних нейронів) мають перед традиційними нейронними мережами такі переваги [4], [26], [69]:

- 1) розпізнавання динамічних образів (мова, динамічні зображення, динамічні параметри підпису та ін.). У системах динамічної ідентифікації

підписів необхідно розпізнавати динамічні сигнали, якими є, наприклад, вихідні сигнали пристроїв введення підписів (наприклад, залежність координат X та Y , тиску та нахилу стилусу від часу);

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). Це вельми потрібна властивість для систем розпізнавання динамічних параметрів підпису, оскільки кількість вихідних нейронів може відповідати кількості підписантів;

3) розпізнавання з передбаченням (будь-який динамічний процес може бути розпізнаний навіть за неповною інформацією про нього, тобто навіть раніше, ніж він завершиться). Це теж вельми важлива властивість, яка дозволяє підвищити швидкодію систем динамічної ідентифікації підписів;

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.

Саме завдяки цим властивостям та перевагам СНМ [4] були обрані в цій роботі для реалізації методу динамічної ідентифікації підписів.

2.2 Спайкінгові нейрони

Відповідно до біологічного прототипу, нейрон отримує збуджувальні або гальмівні сигнали від пресинаптичних нейронів. Тип імпульсу, що надходить, залежить від типу синапсу, який передає його.

Біологічний нейрон має на дендритному дереві і збуджувальні синапси, і гальмівні. Імпульси, що приходять на збуджувальні синапси, збільшують заряд (і потенціал) мембрани, а імпульси, що приходять на гальмівні синапси, зменшують заряд (і потенціал) мембрани. Тобто всі вхідні сигнали конкретного біологічного нейрона можна умовно розділити на дві групи: 1)

збуджувальні сигнали і 2) гальмівні сигнали. Тому можна умовно вважати, що нейрон має два входи – збуджувальний і гальмівний, причому на першому вході відбувається просторово-часове підсумовування всіх сигналів від збуджувальних синапсів, а на другому вході відбувається просторово-часове підсумовування всіх сигналів від гальмівних синапсів.

У цій роботі будемо використовувати модель нейрона, запропонована в [69], яка має роздільні входи для збуджувальних і гальмівних імпульсів і представляється умовним зображенням, показаним на рис. 2.2. Цю модель легко реалізувати за допомогою оптоелектронної елементної бази.

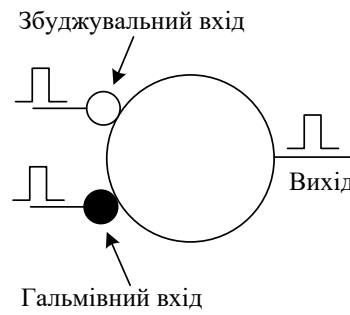


Рисунок 2.2 – Спайкінговий нейрон з роздільними входами

Модель має синапси двох типів, які забезпечують надходження різнополярних сигналів. При цьому сам нейрон видаватиме імпульс одного «знаку». Структурну модель такого спайкінгового нейрону зображено на рис. 2.3, де видно, що вхід розділено на два плеча. По одному, верхньому на рисунку плечі, надходитиме струм від збуджувального синапсу, який буде таким, що втікає, відносно входу. По іншому, нижньому на рисунку плечі, надходитиме струм від гальмівного синапсу, який буде таким, що витікає, відносно входу. Вхідні сигнали до синапсів надходять на певний ключ, який замикається при подачі імпульсу ззовні. Його апаратна реалізація може бути довільною. Наприклад, використовуючи у якості ключа фотодіоди, можливо здійснювати додавання сигналів, які надходять на один тип синапсу на

одному нейроні, на одному діоді, шляхом подання їх на одну апертуру, а не застосовувати для цього кілька однотипних синапсів.

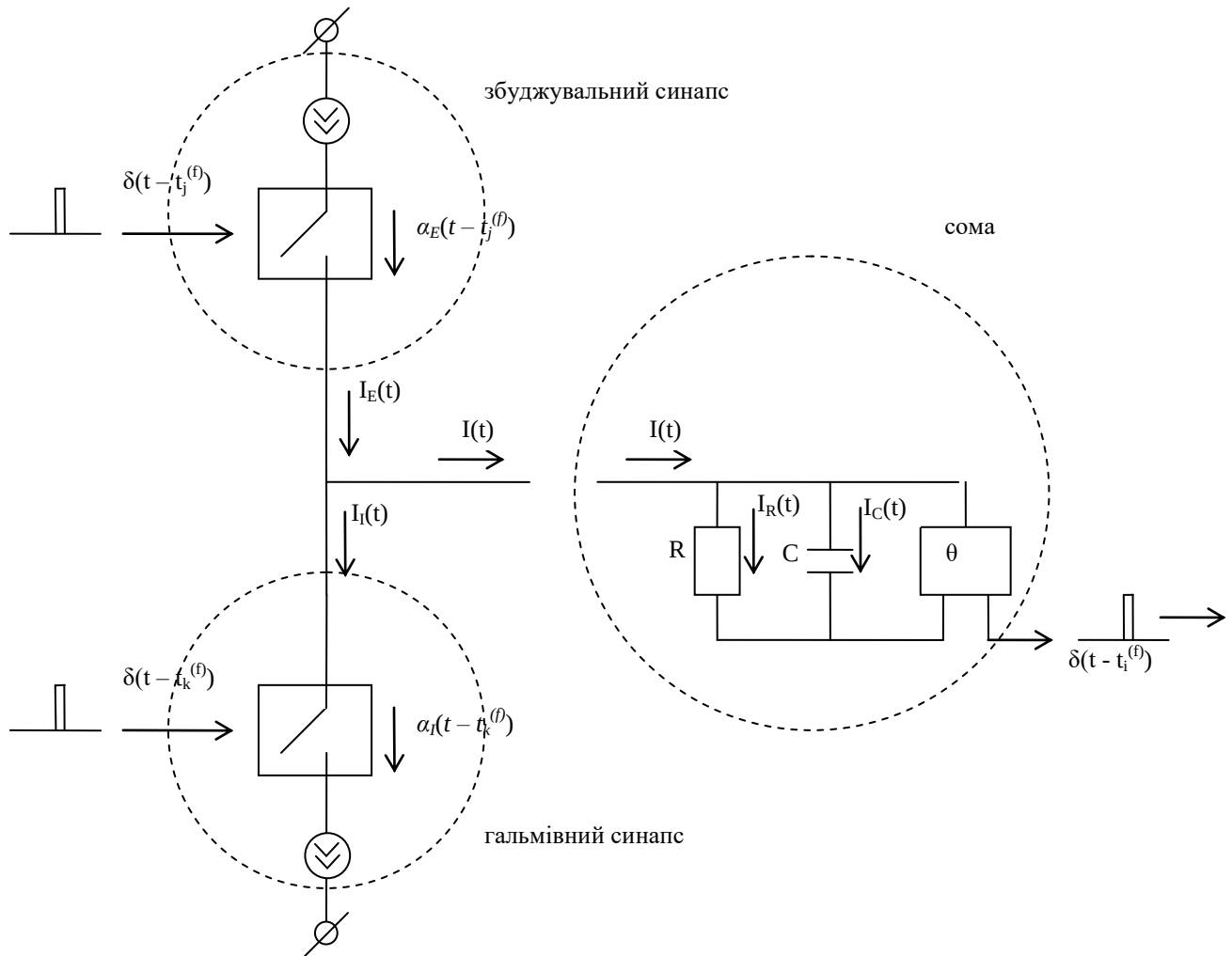


Рисунок 2.3 – Структурна модель ExI&F спайкінгового нейрона

Таким чином, ця структурна модель спайкінгового нейрона представляє собою розширення (extend) відомої LIF моделі (leaky integrate-and-fire model) спайкінгового нейрона [72], тому будемо її називати ExLIF модель (Extended LIF).

Наведемо опис математичної моделі ExLIF без шумів. Базова схема складається з конденсатора та паралельного йому резистора. Загальний струм $I(t)$ може бути розділений на дві входні і вихідні компоненти, $I(t) = I_E(t) - I_I(t)$ і $I(t) = I_R(t) + I_C(t)$. Прирівнявши їх отримуємо:

$$I_E(t) - I_I(t) = I_R(t) + I_C(t). \quad (2.1)$$

Перша вхідна компонента – $I_E(t)$ характеризує струм, який надходить від збуджувального синапсу (excitatory). Друга вхідна компонента – $I_I(t)$ характеризує струм, який надходить від гальмівного синапсу (inhibitory). Знак мінус перед гальмівною компонентою відповідає першому закону Кірхгофа та реалізує різну полярність синапсів.

Перша вихідна компонента – струм, $I_R(t)$, що проходить через лінійний резистор R . За законом Ома він буде рівний $I_R(t) = u(t)/R$, де $u(t)$ – напруга на резисторі. Другий компонент $I_C(t)$ струм конденсатора заряджає конденсатор C . З визначення ємності $C = q/u$ (де q – це заряд, а u – напруга), можна знайти струм ємності $I_C(t) = C du/dt$. Тобто струм $I(t)$ залежить від RC кола

$$I(t) = \frac{u(t)}{R} + C \frac{du}{dt}, \quad (2.2)$$

або

$$I_E(t) - I_I(t) = \frac{u(t)}{R} + C \frac{du}{dt}. \quad (2.3)$$

Помноживши рівняння на R та ввівши часову константу «накопичувача витоку» $\tau_m = RC$, отримаємо стандартну форму:

$$\tau_m \frac{du}{dt} = -u(t) + R(I_E(t) - I_I(t)). \quad (2.4)$$

Аналогічно до LIF-моделі форма діючого потенціалу не описується точно. Тому імпульсами є лише формальні події, що характеризуються часом їх видачі $t^{(f)}$. Час $t^{(f)}$ визначається критерієм насичення:

$$t^{(f)}: u(t^{(f)}) = \theta. \quad (2.5)$$

Якщо врахувати (2.5), то (2.4) прийме вигляд:

$$\tau_m \frac{d\theta}{dt^{(f)}} = -\theta + R(I_E(t^{(f)}) - I_I(t^{(f)})). \quad (2.6)$$

Розв'язок рівняння (2.6) визначає час видачі імпульсу нейроном.

Для $t > t^{(f)}$ динаміка знову описується (2.4), поки не відбудеться наступне насичення. Напруга $u(t)$, що проходить через конденсатор порівнюється з пороговим значенням θ . Якщо $u(t) = \theta$ на деякому постсинаптичному нейроні i у момент часу $t_i^{(f)}$, то на виході генерується імпульс $\delta(t - t_i^{(f)})$. У верхній та нижній частині рис. 2.4 пресинаптичні імпульси $\delta(t - t_j^{(f)})$ і $\delta(t - t_k^{(f)})$ від деяких нейронів j та k фільтрується у синапсі і генерується вхідний імпульсний струм $\alpha_E(t - t_j^{(f)})$ від збуджувального синапсу та $\alpha_I(t - t_k^{(f)})$ – від гальмівного. Одразу ж після моменту часу $t^{(f)}$, потенціал встановлюється до значення спокою u_r ,

$$\lim_{t \rightarrow t^{(f)}} u(t) = u_r. \quad (2.7)$$

Комбінація накопичення витоку (2.4) та встановлення нового значення напруги спокою (2.7) визначає базову ExLIF модель.

Розглянемо випадок, коли на нейрон діють постійні струми збудження $I_E(t) = I_{E0}$, $I_I(t) = I_{I0}$. Нехай потенціал спокою $u_r = 0$, а перший імпульс трапився у момент часу $t = t^{(1)}$. Шляхом інтегрування (2.4) з початковою умовою, що $u(t^{(1)}) = u_r = 0$ отримуємо вираз для потенціалу мембрани:

$$u(t) = R (I_{E0} - I_{I0}) \left[1 - \exp\left(-\frac{t - t^{(1)}}{\tau_m}\right) \right]. \quad (2.8)$$

Для $t \rightarrow \infty$ асимптотичне значення $u(\infty) = R(I_{E0} - I_{I0})$. При $R(I_{E0} - I_{I0}) < \theta$ не може трапитись імпульсу. При $R(I_{E0} - I_{I0}) > \theta$, потенціал мембрани досягає порогу θ у момент часу $t^{(2)}$, тобто $u(t^{(2)}) = \theta$ або

$$\theta = R(I_{E0} - I_{I0}) \left[1 - \exp\left(-\frac{t^{(2)} - t^{(1)}}{\tau_m}\right) \right]. \quad (2.9)$$

Вирішуючи (2.9), отримуємо період між генерацією імпульсів $T = t^{(2)} - t^{(1)}$

$$T = \tau_m \ln \frac{R(I_{E0} - I_{I0})}{R(I_{E0} - I_{I0}) - \theta}. \quad (2.10)$$

Враховуючи період абсолютної рефрактерності Δ^{abs} , період T' між двома імпульсами складатиме, $T' = T + \Delta^{abs}$.

Якщо для спайкінгового кодування у майбутній мережі використати кодування частотою імпульсів, то значення частоти, яке спрощено виражається як $\nu = 1/T$, матиме вигляд:

$$\nu = \left[\Delta^{abs} + \tau_m \ln \frac{R(I_{E0} - I_{I0})}{R(I_{E0} - I_{I0}) - \theta} \right]^{-1}. \quad (2.11)$$

Але не завжди $u_r = 0$. Воно може бути довільним за умови, що $u_r < \theta$. Враховуючи, що вхідний струм не постійний $I(t) = I_E(t) - I_I(t)$, та припускаючи, що генерація імпульсу нейроном i трапилась у момент часу $\hat{t}_i$, для $t > \hat{t}_i$ потенціал мембрани описується ширшим виразом:

$$u(t) = u_r \exp\left(-\frac{t-\hat{t}}{\tau_m}\right) + \frac{1}{C} \int_0^{t-\hat{t}} \exp\left(-\frac{s}{\tau_m}\right) (I_E(t-s) - I_I(t-s)) ds. \quad (2.12)$$

Більш реалістичною є ситуація коли струм $I(t)$ генерується активністю пресинаптичних нейронів, тобто імпульсами. Нехай пресинаптичний нейрон j з'єднаний з нейроном i через збуджувальний синапс та генерує імпульс у момент часу $t_j^{(f)}$. Тоді постсинаптичний нейрон «відчуває» цей струм у формі функції $\alpha_E(t - t_j^{(f)})$. А пресинаптичний нейрон k нехай з'єднаний з нейроном i через гальмівний синапс та генерує імпульс у момент часу $t_k^{(f)}$. Тоді постсинаптичний нейрон «відчуває» цей струм у формі функції $\alpha_I(t - t_k^{(f)})$. Загальний вхідний струм нейрона i , який є сумою всіх вхідних імпульсів f , що надходять з пресинаптичних нейронів, складатиме:

$$I_i(t) = \sum_j w_{Eij} \sum_f \alpha_E(t - t_j^{(f)}) - \sum_k w_{Iik} \sum_f \alpha_I(t - t_k^{(f)}), \quad (2.13)$$

де w_{Eij} – синаптична вага збуджувального синапсу від нейрона i до нейрона j , w_{Iik} – синаптична вага гальмівного синапсу від нейрона i до нейрона k відповідно.

Введення індексів « E » та « I » виправдане тим фактом, що нейрони j та k можуть бути одним й тим самим нейроном.

Зауважимо, що насправді амплітуда постсинаптичного імпульсного струму залежить від дійсного значення потенціалу u_i . Кожен пресинаптичний потенціал дії спричиняє зміни у електропровідності постсинаптичної мембрани відповідно певній функції $g(t - t^{(f)})$. Тоді постсинаптичний струм, що спричинений імпульсом, який пройшов збуджувальний синапс, або збуджувальний імпульс у момент часу $t_j^{(f)}$ є:

$$\alpha_E(t - t_j^{(f)}) = -g_E(t - t_j^{(f)}) [u_i(t) - E_{\text{syn}}], \quad (2.14)$$

де E_{syn} – реверсивний потенціал синапсу, докладно описаний у [72]. Для збуджувального синапсу E_{syn} набагато більший ніж потенціал спокою, для гальмівного – близький до потенціалу спокою. А постисинаптичний струм, що спричинений гальмівним імпульсом у момент часу $t_k^{(f)}$ є:

$$\alpha_I(t - t_k^{(f)}) = -g_I(t - t_k^{(f)}) [u_i(t) - E_{\text{syn}}]. \quad (2.15)$$

Таким чином, (2.14) можна переписати, враховуючи (2.12), як:

$$\tau_m \frac{du_i}{dt} = -u_i(t) + R \left(\sum_j w_{Eij} \sum_f \alpha_E(t - t_j^{(f)}) - \sum_k w_{Iik} \sum_f \alpha_I(t - t_k^{(f)}) \right), \quad (2.16)$$

а (2.12) як:

$$\begin{aligned} u(t) = u_r \exp\left(-\frac{t-\hat{t}}{\tau_m}\right) + \sum_j w_{Eij} \sum_f \frac{1}{C} \int_0^{t-\hat{t}} \exp\left(-\frac{s}{\tau_m}\right) \alpha_E(t - t_j^{(f)} - s) ds - \\ - \sum_k w_{Iik} \sum_f \frac{1}{C} \int_0^{t-\hat{t}} \exp\left(-\frac{s}{\tau_m}\right) \alpha_I(t - t_k^{(f)} - s) ds. \end{aligned} \quad (2.17)$$

У загальному випадку, враховуючи обидва типи надходження збуджень до нейрона, загальний вхідний струм нейрона i рівний:

$$I_i(t) = \sum_j w_{Eij} \sum_f \alpha_E(t - t_j^{(f)}) - \sum_k w_{Iik} \sum_f \alpha_I(t - t_k^{(f)}) + I_{iE}^{\text{ext}}(t) - I_{iI}^{\text{ext}}(t), \quad (2.18)$$

а потенціал мембрани нейрона i має вигляд:

$$\begin{aligned} \tau_m \frac{du_i}{dt} = -u_i(t) + \left(\sum_j w_{Eij} \sum_f \alpha_E(t - t_j^{(f)}) - \sum_k w_{Iik} \sum_f \alpha_I(t - t_k^{(f)}) \right) R + \\ R(I_{iE}^{\text{ext}}(t) - I_{iI}^{\text{ext}}(t)), \end{aligned} \quad (2.19)$$

де $I_{iE}^{ext}(t)$ – струм збудження від збуджувального синапсу нейрона i ;
 $I_{iI}^{ext}(t)$ – струм збудження від гальмівного синапсу нейрона i .

Або ж на базі (2.17):

$$\begin{aligned} u(t) = & u_r \exp\left(-\frac{t-\hat{t}_i}{\tau_m}\right) + \sum_j w_{Eij} \sum_f \frac{1}{C} \int_0^{t-\hat{t}_i} \exp\left(-\frac{s}{\tau_m}\right) \alpha_E(t-t_j^{(f)}-s) ds - \\ & - \sum_k w_{Iik} \sum_f \frac{1}{C} \int_0^{t-\hat{t}_i} \exp\left(-\frac{s}{\tau_m}\right) \alpha_I(t-t_k^{(f)}-s) ds + \\ & + \frac{1}{C} \int_0^{t-\hat{t}_i} \exp\left(-\frac{s}{\tau_m}\right) I_{iE}^{ext}(t-s) ds - \frac{1}{C} \int_0^{t-\hat{t}_i} \exp\left(-\frac{s}{\tau_m}\right) I_{iI}^{ext}(t-s) ds. \end{aligned} \quad (2.20)$$

Представлену модель нейрона також можна поставити у відповідність до моделі SRM (spike-response model) [72]. Якщо ввести такі позначення:

$$\eta(s) = u_r \exp\left(-\frac{s}{\tau_m}\right), \quad (2.21)$$

$$\xi(s, t) = \frac{1}{C} \int_0^s \exp\left(-\frac{t'}{\tau_m}\right) \alpha_E(t-t') dt' - \frac{1}{C} \int_0^s \exp\left(-\frac{t'}{\tau_m}\right) \alpha_I(t-t') dt', \quad (2.22)$$

$$\kappa(s, t) = \frac{1}{C} \exp\left(-\frac{t'}{\tau_m}\right) \Theta(s-t) \Theta(t), \quad (2.23)$$

де $\Theta(x)$ позначає покрокову функцію Хевісайда, яка $\Theta(x) = 1$ при $x > 0$, і $\Theta(x) = 0$ в інших випадках, то мембранний потенціал матиме вигляд відповідно моделі SRM:

$$\begin{aligned} u(t) = & \eta(t - \hat{t}_i) + \\ & + \sum_j w_{ij} \sum_f \mathcal{E}(t - \hat{t}_i, t - t_j^{(f)}) + \int_0^\infty \kappa(t - \hat{t}_i, s) (I_E^{ext}(t-s) - I_I^{ext}(t-s)) ds \end{aligned} \quad (2.24)$$

При цьому слід зазначити, що змінна w_{ij} поєднує в собі позначення як ваг w_{Iik} так і ваг w_{Iik} .

2.3 Структура спайкінгової нейронної мережі

У роботах [47], [75] запропоновано мережу, інтернейрони якої повинні бути двох типів: 1) збуджувальні (видають на виході електричний імпульс додатної полярності) та 2) гальмівні (видають на виході електричний імпульс від'ємної полярності). Для відомої мережі на LIF-нейронах (рис. 2.4) «збуджувальним» синапсом буде синапс, що з'єднує збуджувальний інтернейрон з вихідним нейроном, а «гальмівним» синапсом – відповідно синапс, що з'єднує гальмівний інтернейрон з вихідним нейроном.

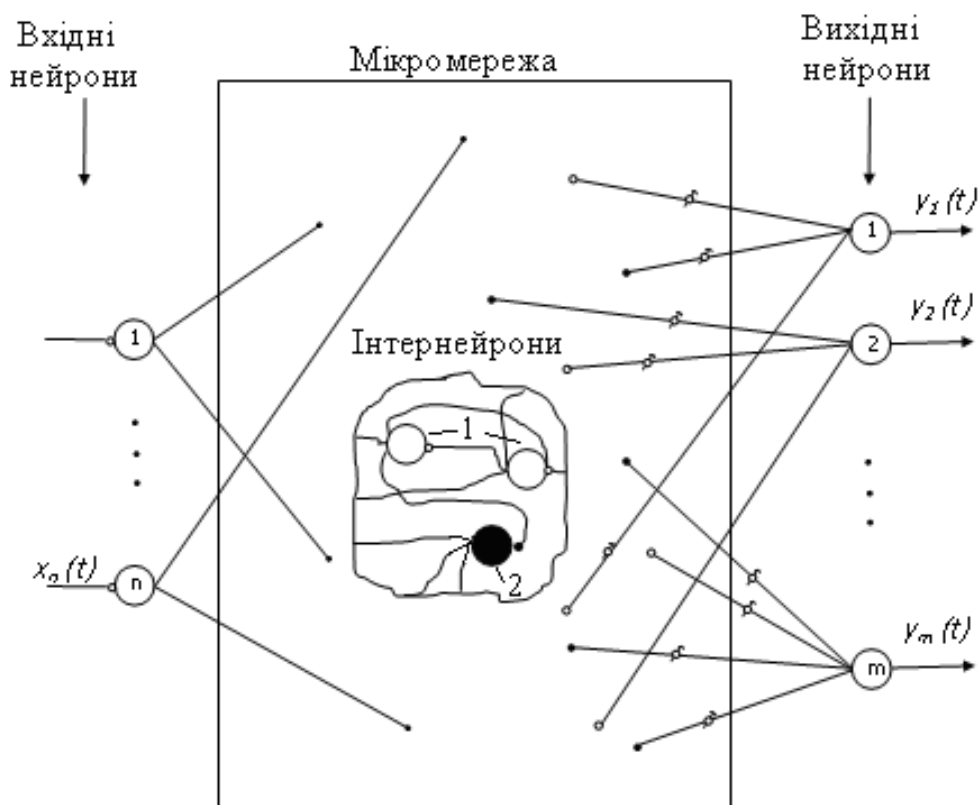


Рисунок 2.4 – Структура відомої [39] спайкінгової нейронної мережі на основі нейронів двох типів: 1) збуджувальні нейрони, 2) гальмівні нейрони.

Структура СНМ, що розглядається в даній роботі (рис. 2.5), відрізняється від запропонованої в [47], [75], тим, що як інтернейрони (середній шар мережі) використовуються нейронні елементи ExLIF [69] типу (всі однакові), кожен з яких може утворювати як збуджувальні, так і гальмівні синаптичні з'єднання, керовані імпульсами позитивної полярності, які і видають на виході запропоновані нейронні елементи.

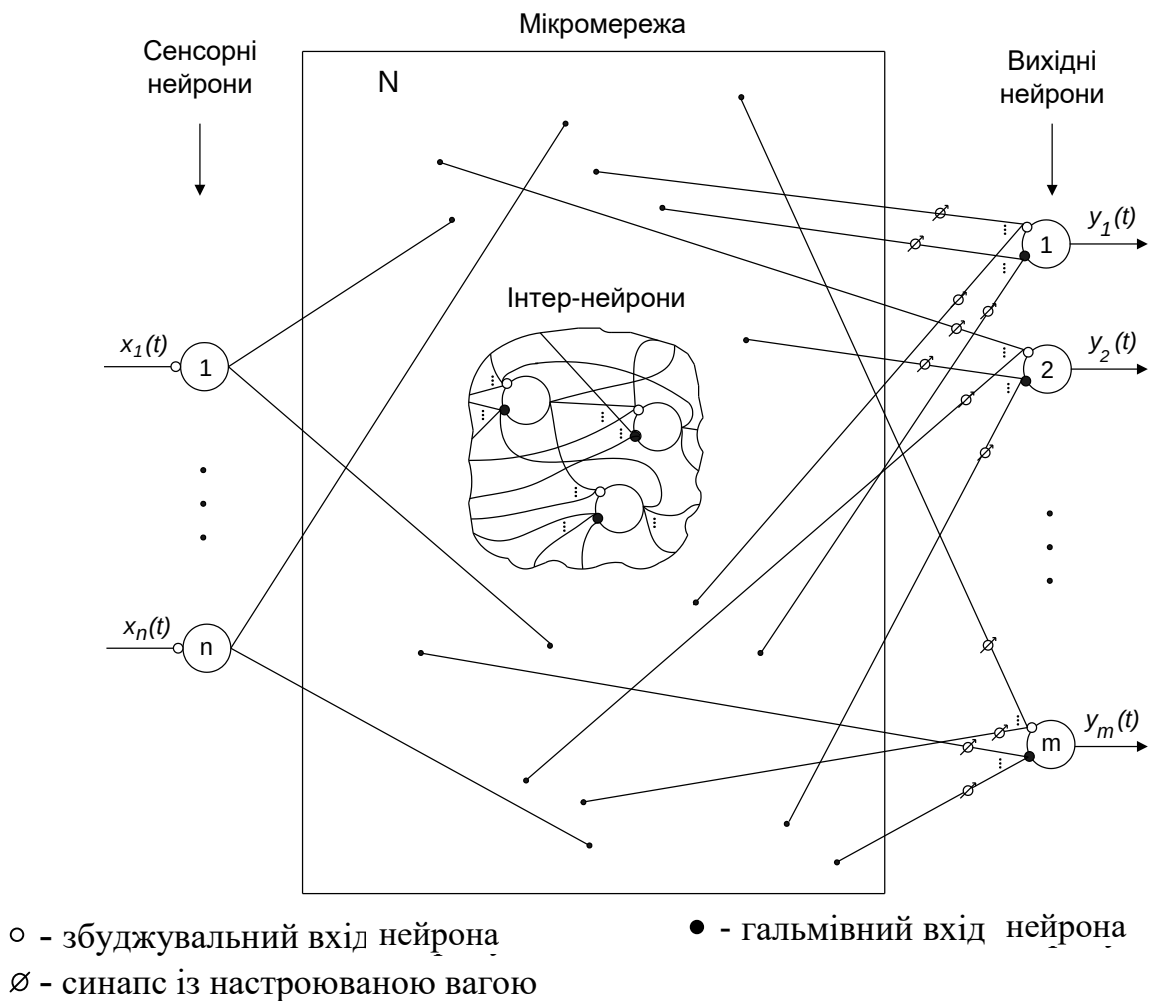


Рисунок 2.5 – Структура спайкінгової нейронної мережі

За основу СНМ, що розробляється для динамічної ідентифікації підписів, взято СНМ, що запропоновано в [69], яка має вхідний шар нейронів, шар інтернейронів та шар вихідних нейронів (рис. 2.5). Кількість вхідних нейронів n дорівнює кількості динамічних параметрів підпису. Кількість вихідних нейронів m дорівнює кількості можливих класів вхідних

образів. В ідеальному випадку мережа повинна сприймати на вхід імпульсну послідовність та видавати імпульси максимальної частоти на тому нейроні, який відповідає визначеному класу послідовності (кодування «один із m »), та не видавати імпульсів на інших вихідних нейронах. Структура СНМ із [69] має вид, показаний на рис. 2.5.

Як інтернейрони в цій структурі використовуються запропоновані в [69], [74] спайкінгові нейрони з роздільними входами згідно з рис. 2.2 і рис. 2.3. Кількість нейронів вибирається пропорційно об'єму розпізнаваних образів і міри їх коррельованості (схожості). Кількість зв'язків одного нейрона з іншими (наприклад, 10...15 %), дальність їх поширення, співвідношення кількості збуджувальних і гальмівних зв'язків (наприклад, відповідно 80 % і 20 %) може визначатися даними нейрофізіологічних досліджень [47], [75].

Як видно із структури спайкінгової нейронної мережі (рис. 2.5), лише вихідні нейрони повинні мати можливість підстроювати свої ваги синаптичних зв'язків в процесі навчання. Це відрізняє вихідні нейрони від інтернейронів, які мають постійні ваги зв'язків, що задаються при формуванні мережі.

СНМ з рис. 2.5 простіша за СНМ по рис. 2.4 за рахунок скорочення загальної кількості нейронів мережі завдяки застосуванню оптоелектронних нейронних елементів [74] з однаковою полярністю сигналів для збуджувальних і гальмівних імпульсів.

У п.2.1 показано, що для Online ідентифікації підпису варто використовувати саме спайкінгові нейронні мережі [1], [7], [8], 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 [4], [69] перед традиційними нейронними мережами обумовлені їхньою нейроморфністю (схожістю з мережами біологічних нейронів).

Для Online верифікації підпису за основу було взято структуру спайкінгової нейронної мережі, розроблену в [69], [70]. Модифіковану структуру спайкінгової нейронної мережі для Online верифікації та розпізнавання підписів зображено на рис. 2.6.

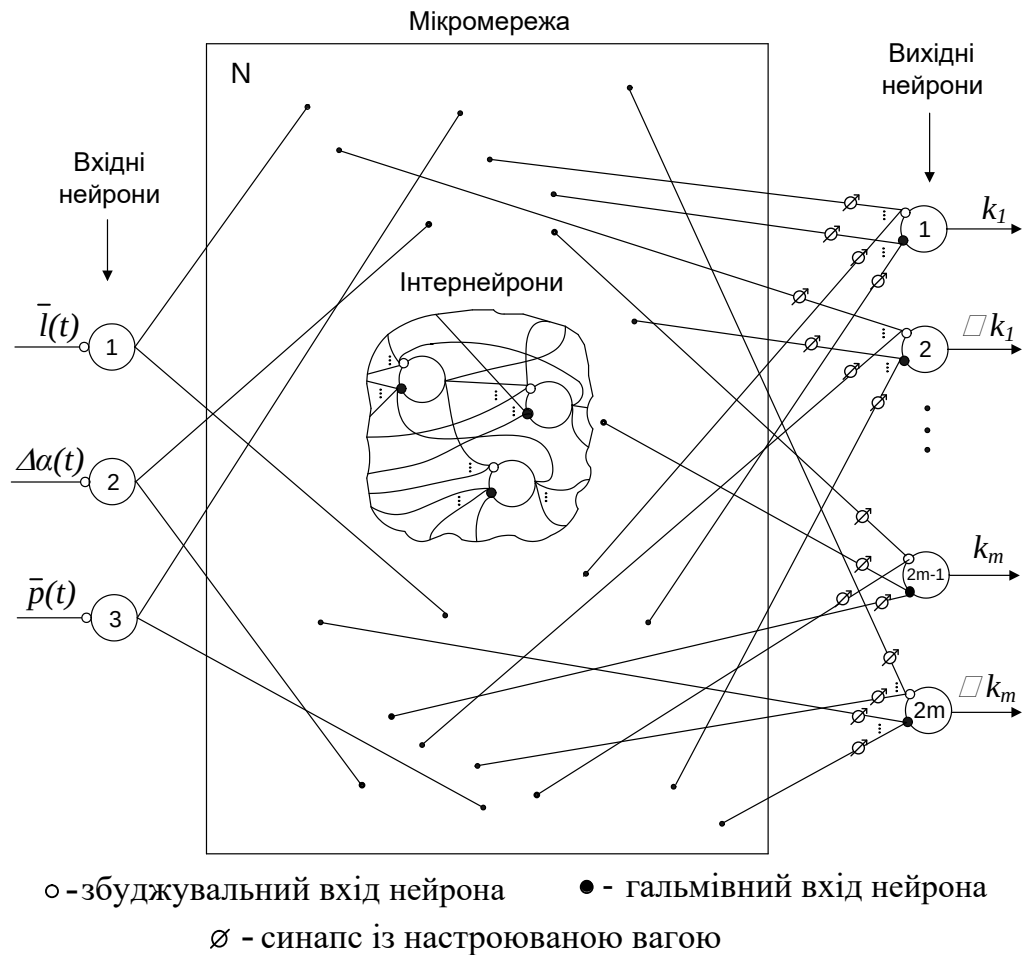


Рисунок 2.6 – Структура спайкінгової нейронної мережі для Online верифікації та розпізнавання підписів

Вхідні спайкінгові нейрони можна побудувати, наприклад, за моделлю LIF [72] або за моделлю ExLIF (п. 2.2). На вхідні нейрони подаються нормалізовані динамічні параметри підпису (наприклад, $\bar{l}(t)$, $\Delta\alpha(t)$ та $\bar{p}(t)$), які перетворюються вхідними нейронами у відповідні їм імпульсні послідовності як показано на рис. 2.7.

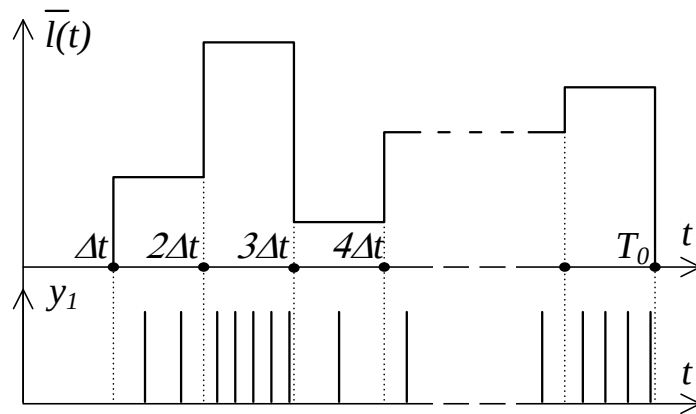


Рисунок 2.7 – Перетворення параметру $\bar{I}(t)$ вхідним спайкінговим нейроном у його вихідний імпульсний сигнал $y_1(t)$

Особливістю структури по рис. 2.6 є те, що вона має не m вихідних нейронів, а $2m$. Тобто на кожний ідентифікаційний клас (на кожного підписанта) сформовано не 1 вихідний нейрон, а 2 вихідних нейрони (один – для індикації справжнього підпису, а другий – для індикації підробленого підпису). Це дозволяє точніше визначати майстерно підроблені підписи, підкреслюючи їх диференціацію від справжніх, оскільки вони представляються сильно корельованими сигналами.

2.4 Навчання спайкінгової нейронної мережі

Аналіз існуючих методів навчання спайкінгових нейронних мереж [80]-[84] виявив, що переважна більшість з них придатна при використанні схеми кодування «час-до-першого-імпульсу», або інших схем кодування з використанням імпульсів. Щодо частотного кодування, то методів, які б дозволили навчати спайкінгову нейронну мережу з його використанням, на даному етапі практично немає.

Однією із найпоширеніших задач, яку здатні виконувати СНМ, є задача класифікації. Відповідно, на виході навченої мережі потрібно отримати інформацію про те, до якого класу належить подана на вхід мережі сукупність динамічних сигналів. Отже, вхідний та вихідний сигнали можуть

мати різну природу, тому може бути зручним застосування частотного кодування вихідного сигналу.

Будь-який багатовимірний вхідний сигнал може бути перетворений у багатовимірну послідовність імпульсів за допомогою нейронів із різними вхідними та вихідними синапсами. Тому в подальшому багатовимірним сигналом буде виступати багатовимірна імпульсна послідовність.

Отже, метод навчання ClassLearn (Classification Learning), що розробляється, призначений навчати СНМ класифікувати багатовимірні імпульсні послідовності, використовуючи при цьому частотне кодування вихідного сигналу.

Відомі методи навчання спайкінгових нейронних мереж передбачають використання складних математичних обчислень [80]-[82], таких як, наприклад, диференціювання та інтегрування. Тому існуючі методи використовуються при комп'ютерному моделювання СНМ, оскільки в таких умовах легко можна реалізувати складні обчислення величини зміни ваг. До нового ж методу ставиться вимога можливості його використання для навчання апаратно реалізованих СНМ [4], [6], [70], тому при його розробці необхідно враховувати деякі специфічні вимоги. Отже, метод навчання повинен бути [72]:

1. Локальним, тобто таким, що вимагає лише локально доступні сигнали для визначення нових значень ваг синапсів.
2. Простим, тобто потребувати якнайменшої кількості операцій.
3. Робастним, тобто вимагати лише помірної точності.

Правило Хебба та похідні від нього методи відповідають вказаним критеріям. Відповідно у розробленому методі навчання з учителем за основу взято саме правило Хебба.

Метод навчання, що розробляється, орієнтований на модель нейронної мережі, в якій інтернейрони та вихідні нейрони представлені нейронами моделі ExI&F (рис. 2.3), за якою нейрон має два синапси: збуджувальний та гальмівний.

Проте, метод також може бути застосований для мережі, в якій вихідні нейрони є I&F-нейронами (нейроном з одним вхідним синапсом). Інтернейрони такої мережі також є I&F-нейронами і мають один вхідний синапс, але при цьому можуть бути або збуджувальними, або гальмівними. Для мережі на I&F-нейронах «збуджувальним» синапсом буде синапс, що з'єднує збуджувальний інтернейрон з вихідним нейроном, а «гальмівним» синапсом – відповідно синапс, що з'єднує гальмівний інтернейрон з вихідним нейроном.

Мережа, що навчається, має вхідний шар нейронів, шар інтернейронів та шар вихідних нейронів (рис. 2.5). Кількість вхідних нейронів n рівна кількості вимірів сигналу. Кількість вихідних нейронів m дорівнює кількості можливих класів вхідних послідовностей. В ідеальному випадку, навчена за розробленим методом мережа, повинна сприймати на вхід імпульсну послідовність та видавати імпульси максимальної частоти на тому вихідному нейроні, який відповідає визначеному класу послідовності, та не видавати імпульсів на інших вихідних нейронах.

Метод навчання ClassLearn використовує переваги саме спайкінгових нейронних мереж, оскільки передбачає навчання лише вихідного шару нейронів.

Отже, кожний вихідний нейрон мережі відповідає певному можливому класу вхідної послідовності. Призначити кожному нейрону свій клас можна довільно чи по порядку, але для збільшення ефективності навчання є сенс призначати клас відповідно проведеним початковим дослідженням. Таким чином, підготовчий етап навчання передбачає подання на вхідні нейрони мережі шаблонів вхідних імпульсних послідовностей кожного класу. Після подачі послідовності чергового i -го класу, визначається частота генерації імпульсів на кожному із m вихідних нейронів. Нейрону j , який відповів найбільшою частотою на поданий шаблон, призначається відповідний клас. Однак при такому послідовному призначенні класів, може виникнути ситуація, коли нейрон, який видав імпульсну послідовність найбільшої

частоти, уже «зайнятий» іншим класом. В такому випадку необхідно переглянути призначення цього нейрону та, можливо, перевизначити клас, за який він відповідає.

Процес початкового призначення вихідним нейронам класів імпульсних послідовностей, за які вони відповідають, можна описати такою процедурою:

1. На вхідні нейрони ІНМ по чергові подаються еталонні послідовності. Результат роботи кожного вихідного нейрона k_{ij} (відношення частоти його генерації до максимальної) заноситься у матрицю $K (m \times m)$, в якій рядкам відповідає номер класу імпульсної послідовності, а стовпцям – номер нейрону.
2. Відповідності класів вхідних послідовностей нейронам фіксуватимуться у матриці $M (l \times m)$, яка спочатку заповнена нулями.
3. У матриці M знаходиться черговий елемент, рівний 0. Його номер відповідає рядку i класу. По цьому рядку знаходиться максимальне значення k_{ij}^{max} .
4. Проводиться перевірка, чи є значення j (відповідне k_{ij}^{max}) у матриці M .
5. Якщо немає (тобто, нейрон не «зайнятий» жодним класом), то елементу матриці $M[i]$ присвоюється значення j .
6. Якщо ж значення j вже наявне у матриці M (тобто нейрон уже був поставлений у відповідність певному класу i'), то проводиться порівняння значень $k_{i',j}$ та k_{ij} .
7. Якщо $k_{i',j} \geq k_{ij}$, то проводиться пошук максимального елемента у i -тому рядку за виключенням елемента k_{ij} та повторюється п.4
8. Якщо $k_{i',j} < k_{ij}$, то елементу матриці $M[i]$ присвоюється значення j , а елементу матриці $M[i']$ – значення 0.

9. Якщо у матриці M ще є нульові елементи, то повторюється п.3.

Інакше процедуру призначення нейронам відповідних класів завершено.

Отже, після підготовчого етапу, кожен вихідний нейрон j відповідає за певний клас i , до якого може належати вхідна імпульсна послідовність.

Кожний вихідний нейрон мережі з'єднаний випадковим чином із певною кількістю інтернейронів (докладніше про механізм та кількість з'єднань описано у п.2.3).

Відповідно, навчання мережі полягає в налаштуванні ваг збуджувальних та гальмівних синапсів нейронів вихідного шару.

Як було сказано вище, метод навчання ClassLearn базується на правилі навчання Хебба. Але правило Хебба було сформульоване для навчання без учителя, тому наголошує на «одночасному» збудженні пресинаптичного та постсинаптичного нейрону. В даному ж випадку розроблений метод є методом навчання з учителем, що вносить деякі корективи в правило навчання, оскільки при навчанні відомо, із яким саме вихідним нейроном потрібно нарощувати синаптичні зв'язки. Таким чином, даний метод передбачає, що з кожним проходженням імпульсу через інтернейрон та з'єднаний з ним вихідний нейрон, вага збуджувального синаптичного зв'язку між ними повинна зростати.

Але для вирішення задачі класифікації, генерувати імпульси з максимальною частотою повинен лише один нейрон – той, що відповідає класу вхідної імпульсної послідовності. Тому при навчанні повинні нарощуватися ваги збуджувальних синаптичних зв'язків лише з тим вихідним нейроном, який відповідає класу вхідної послідовності. Решта ж вихідних нейронів не повинні генерувати імпульсів, а отже, повинні нарощуватися ваги їхніх гальмівних синапсів.

Таким чином, навчання відбувається за таким алгоритмом:

1. Ініціалізація ваг усіх синаптичних зв'язків вихідних нейронів деякими невеликими випадковими значеннями.

2. Початковий етап, в ході якого кожному вихідному нейрону призначається номер класу, до якого може належати вхідний сигнал.
3. Номер кроку $i:=0$.
4. $i:=i+1$. На управляючих входах усіх збуджувальних синапсів відповідного j -го вихідного нейрона встановлюється потенціал, який визначає режим, коли кожен імпульс, що прийшов на відповідний синапс, буде збільшувати величину коефіцієнта передачі (ваги) цього синапсу. На управляючих входах усіх гальмівних синапсів j -го вихідного нейрона встановлюється потенціал, що визначає режим, при якому вага синаптичного зв'язку залишається незмінною.
5. На управляючих електродах всіх гальмівних синапсів решти $(m-1)$ нейронів (окрім j -го) встановлюється потенціал, що визначає режим, коли кожен імпульс, що прийшов на відповідний синапс, буде збільшувати величину негативного коефіцієнта передачі цього синапсу (тобто, збільшувати тим самим гальмівний ефект). На управляючих входах усіх збуджувальних синапсів усіх вихідних нейронів, окрім j -го, встановлюється потенціал, що визначає режим, при якому вага синаптичного зв'язку залишається незмінною.
6. На вхідні нейрони подається i -ий еталонний сигнал тривалістю T_0 . Імпульси, що будуть з'являтися на входах збуджувальних синапсів j -го вихідного нейрону, збільшать ваги його зв'язків з тими інтернейронами, які генерують імпульси саме при впливі на мережу i -ї еталонної послідовності. Це призводить до того, що після навчання при подачі на вхід СНМ сигналу, схожого на i -й еталон, саме j -й вихідний нейрон видасть найбільшу кількість імпульсів на інтервалі T_0 . А імпульси, які будуть з'являтися на входах гальмівних синапсів решти вихідних нейронів (окрім j -го), збільшать їх гальмування по зв'язкам з тими нейронами інтермережі, які

генерують імпульси саме при впливі на мережу i -го еталонного сигналу.

7. Якщо $i \neq m$, то перейти до п.4.
8. Інакше – зняти всі управляючі сигнали із синапсів вихідних нейронів. Протестувати роботу мережі, подаючи на вхід почергово навчальні сигнали, обчислюючи похибку
9. Якщо помилка не задовольняє вимогам – повторити навчання із п.3.

Зрозуміло, що вага синаптичних зв'язків не може зростати безмежно. Тому у правилі навчання необхідно передбачити певні обмеження, завдяки яким синаптична вага буде знаходитися у рамках від 0 до певного значення w_{max} . Обмеження можуть бути введені або через залежність коефіцієнтів навчання від поточного значення синаптичної ваги, або через зупинку навчання при досягненні значенням ваги максимального значення, або за допомогою зміни ваг синаптичних зв'язків вручну.

В даному методі пропонується наступний підхід:

1. В рамках одного циклу навчання вихідного нейрона на синаптичну вагу накладаються м'які обмеження. В даному випадку пропонується при обчисленні величини коефіцієнтів виразу для кроку зміни ваги враховувати максимальне можливе значення синаптичної ваги.
2. При повторному циклі навчання синаптичні ваги та коефіцієнти для визначення кроку зміни синаптичних ваг змінюються «вручну». Тобто після того, як через мережу були пропущені усі еталонні імпульсні послідовності та було визначено, що величина похибки не задовольняє вимогам, значення коефіцієнтів виразу для кроку зміни ваг та значення ваг усіх синаптичних зв'язків змінюються (множаться на певні коефіцієнти).

Таким чином, завдяки використовуваному методу розпізнавання на основі СНМ і запропонованому методу навчання, процес навчання СНМ здійснюється значно простіше. Спрощення виникає, по-перше, за рахунок

відсутності складних обчислювальних процедур при навчанні нейронної мережі, по-друге, навчаються не всі нейрони мережі, а лише вихідні нейрони.

2.5 Метод динамічної ідентифікації підпису на основі спайкінгової нейронної мережі

Враховуючи структуру спайкінгової нейронної мережі згідно з рис. 2.6, а також розроблене в [48] правило навчання вихідних нейронів спайкінгової нейронної мережі, принципи функціонування і математичні моделі спайкінгових нейронів з роздільними входами [70], можна сформулювати метод динамічної (Online) ідентифікації 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 [47]. 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 п.2.4. 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} .

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 ідентифікації підписів (особливо при розпізнаванні підроблених підписів, які сильно корельовані з оригіналами);

3) результат ідентифікації 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.

2.6 Висновки до другого розділу

1. Обґрунтовано перспективність використання спайкінгових нейронних мереж для динамічної ідентифікації підписів, оскільки вони можуть без будь-якого перетворення форми інформації виконувати розпізнавання динамічних параметрів підпису, що виключає втрату корисної інформації та сприяє підвищенню достовірності ідентифікації.

2. Проаналізовано моделі спайкінгових нейронів з точки зору використання їх у процесі динамічної ідентифікації підписів.

3. Розроблено структуру та архітектуру спайкінгової нейронної мережі включно з принципами її побудови та функціонування з орієнтацією на застосування у процесі динамічної ідентифікації підписів.

4. Розроблено метод навчання спайкінгової нейронної мережі та принципи кодування вихідної інформації в процесі класифікації динамічних параметрів підписів.

5. Розроблено метод динамічної ідентифікації підписів на основі спайкінгової нейронної мережі, який має ряд переваг перед відомими методами, зокрема, не вимагає попереднього перетворення у вектор статичних ознак, може ідентифікувати підписи з передбаченням, що підвищує швидкодію; використовувана нейронна мережа має спрощену процедуру навчання, відсутність потреби перенавчання всієї мережі при необхідності додавання нових підписів; має підвищену завадостійкість.

Основні наукові результати, викладені у розділі, опубліковано в роботах [1] - [6], [8].

РОЗДІЛ 3

ДИНАМІЧНІ ПАРАМЕТРИ ПІДПISУ, СТІЙКІ ДО ВНУТРІШНЬОПЕРСОНАЛЬНОЇ ВАРІАБЕЛЬНОСТІ ТА ЧУТЛИВІ ДО МІЖПЕРСОНАЛЬНОЇ ВАРІАБЕЛЬНОСТІ

Незважаючи на великий обсяг досліджень за цією тематикою [9], [13]-[15], створення систем динамічної (Online) ідентифікації підпису (ДІП) з потрібною достовірністю і якістю роботи лишається проблематичним. Складності практичного застосування різних інформаційних технологій динамічної (Online) ідентифікації підпису викликані недоліками самого явища формування підпису, як об'єкту інформаційного процесу. Так, підпис однієї і тієї ж людини є нестабільно відтворюваним процесом. Причини нестабільності підпису можна розділити на 3 групи [14]:

- 1) природня варіабельність почерку людини (відмінність у написанні окремих літер, вензелів та ін.);
- 2) варіабельність геометричних параметрів підпису, а саме:
 - варіабельність геометричних розмірів (просторового масштабу) різних реалізацій підпису,
 - варіабельність точки початку підпису відносно сторін планшету (зсуву) різних реалізацій підпису,
 - варіабельність кута нахилу підпису відносно сторін планшету (повороту) різних реалізацій підпису;
- 3) варіабельність часу написання (часового масштабу) різних реалізацій підпису.

Геометричну та часову варіабельність компенсують шляхом амплітудної та часової нормалізації динамічних параметрів підпису. Природню варіабельність підпису важко подолати технічними засобами, але можна трохи компенсувати шляхом правильного підбору чи синтезу похідних динамічних параметрів підпису. Саме тому потрібно обирати або

синтезувати такі похідні динамічні параметри підпису, які забезпечували б найменшу внутрішньоперсональну варіабельність підпису.

З іншого боку, ці динамічні параметри підпису повинні бути чутливі до підробок підпису, тобто до міжперсональної варіабельності. Саме тому метою досліджень, відображених у цьому розділі є кількісна оцінка внутрішньоперсональної та міжперсональної варіабельності різних динамічних параметрів підпису з тим, щоб обґрунтувати для подальшої обробки саме ті з них, які мають мінімальну внутрішньоперсональну варіабельність та максимальну міжперсональну варіабельність. Це дозволить збільшити достовірність динамічної ідентифікації підписів.

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 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.

3.1 Обґрунтування вибору динамічних параметрів підпису, стійких до геометричної варіабельності

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. 3.1). Тобто, згідно теореми Піфагора:

$$l_i = \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2} \quad (3.1)$$

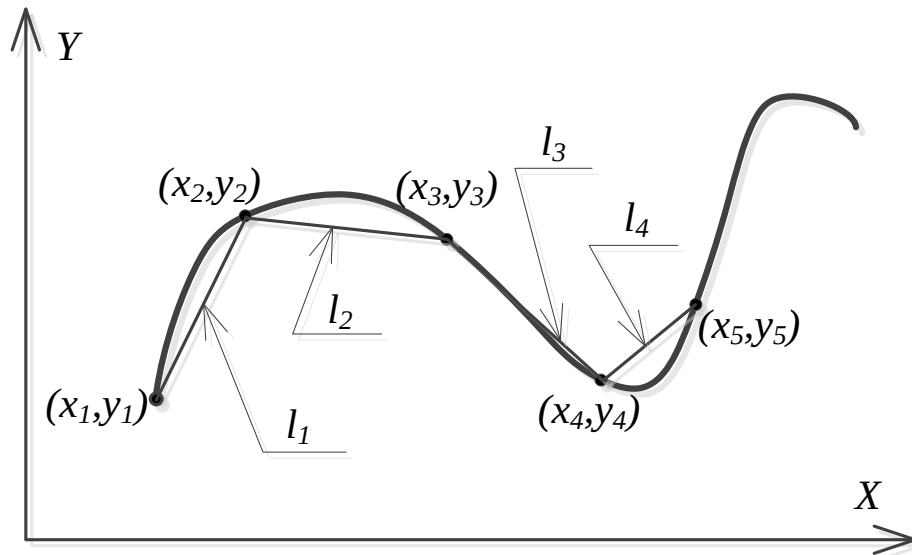


Рисунок 3.1 – Отримання динамічного параметру підпису $l(t)$

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 відріжку між точками (x_i, y_i) та (x_{i+1}, y_{i+1}) . А оскільки всі Δt однакові, то l_i є пропорційною швидкості пера на відріжку $[(x_i, y_i); (x_{i+1}, y_{i+1})]$. 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 .

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. 3.2). Кут α_i знаходиться із прямокутного трикутника, катетами якого є різниці координат точок (x_{i+1}, y_{i+1}) та (x_i, y_i) .

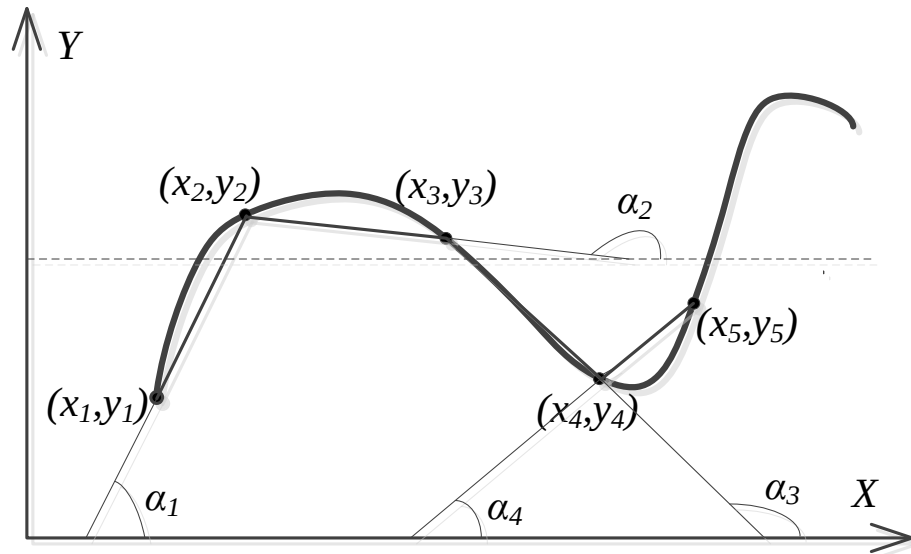


Рисунок 3.2 – Отримання динамічного параметру підпису $\Delta\alpha(t)$

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.

3.2 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:

$$\Delta t_0 = \frac{T_0}{T} \cdot \Delta t, \quad (3.2)$$

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

$$\bar{l}_i = (l_i - l_{\min}) / (l_{\max} - l_{\min}). \quad (3.3)$$

$$\bar{z}_i = (z_i - z_{\min}) / (z_{\max} - z_{\min}). \quad (3.4)$$

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 кутом) і завжди міняється в діапазоні $[-\pi, +\pi]$ радіан.

3.3 Дослідження стійкості динамічних параметрів підпису до внутрішньоперсональної варіабельності

Для доведення більшої робастності обраних параметрів $l(t)$ та $\Delta\alpha(t)$, ніж первинних параметрів $X(t)$ та $Y(t)$, проведемо дослідження їх внутрішньоперсональної варіабельності. Для цього скористаємось базою даних підписів MCYT-330 [51], яка є частиною бази даних підписів DeepSignDB [30]. У базі даних підписів MCYT-330 є 330 користувачів, для кожного з яких є 25 його оригінальних підписів та 25 майстерно підроблених підписів.

Внутрішньоперсональну варіабельність будемо оцінювати для нормалізованих по амплітуді і по часу динамічних параметрів підпису, оскільки саме вони підлягають подальшому процесу класифікації.

Кожен із початкових параметрів, наприклад, $X(t)$ є нічим іншим, як часовим рядом. Тобто може бути представлений вектором, що складається із окремих відліків залежності: $\mathbf{X}=(x_1, x_2, \dots x_{1i}, \dots x_n)$. Довжина вектора n і вона не однакова для всіх реалізацій підпису. Відліки знімаються із часовим кроком Δt , який зазвичай дорівнює 10 мс (частота дискретизації 100 Гц). Коли здійснюється амплітудна та часова нормалізація динамічного параметру, то просто коригується часовий крок Δt за формулою (3.2), а амплітуда за формулою (3.3). Але все одно ми маємо вектор $\bar{\mathbf{X}}=(\bar{x}_1, \bar{x}_2, \dots \bar{x}_{1i}, \dots \bar{x}_n)$ довжиною n , яка не однакова для всіх реалізацій підпису. Тобто,

коли ми шукаємо усереднений часовий ряд $\tilde{X}$, то нам потрібно усереднювати вектори різної довжини. Тому приведемо всі вектори $\bar{X}^j$ окремих реалізацій підпису ($j=1\dots 25$) до довжини $N=1000$ шляхом знаходження елементів цих нових векторів $\tilde{X}^j$ за допомогою кусочно-лінійної апроксимації [85]. Далі для кількісного оцінювання внутрішньоперсональної варіабельності динамічних параметрів підпису, спочатку знайдемо усереднений часовий ряд кожного із параметрів по $m=25$ (для МСУТ) відомим рядам справжніх підписів кожного користувача за формулою:

$$\tilde{x}_i = \frac{1}{m} \sum_{j=1}^m \tilde{x}_i^j, i = 1\dots N, N = 1000 \quad (3.4)$$

Для прикладу, на рис. 3.3 показано графік усередненої залежності $\tilde{X}(t)$ та огинаючі максимальних та мінімальних значень залежностей $\tilde{X}(t)$ для 25 оригінальних підписів трьох осіб. Прийmemo гіпотезу, що для $\tilde{Y}(t)$ характер залежності буде аналогічним, тому розглядати її не будемо. На рис. 3.4 та рис. 3.5 показано графіки усереднених залежностей $\tilde{l}(t)$ та $\Delta\tilde{\alpha}(t)$ та огинаючі їх максимальних та мінімальних значень для 25 оригінальних підписів трьох осіб.

З рис. 3.3–3.5 видно, що параметри $\tilde{X}(t)$ та $\tilde{l}(t)$ мають невеликий діапазон розкиду відносно середньої залежності відповідно $\tilde{X}(t)$ та $\tilde{l}(t)$. Це свідчить про те, що параметр $\tilde{l}(t)$ є робастним (стійким) до внутрішньоперсональної варіабельності, тому його слід використовувати для ідентифікації підписів. А параметр $\Delta\tilde{\alpha}(t)$, всупереч очікуванням, має великий діапазон розкиду відносно середньої залежності $\Delta\tilde{\alpha}(t)$. Це свідчить про те, що параметр $\Delta\alpha(t)$ не є робастним (стійким) до

внутрішньоперсональної варіабельності, тому його не варто використовувати для ідентифікації підписів.

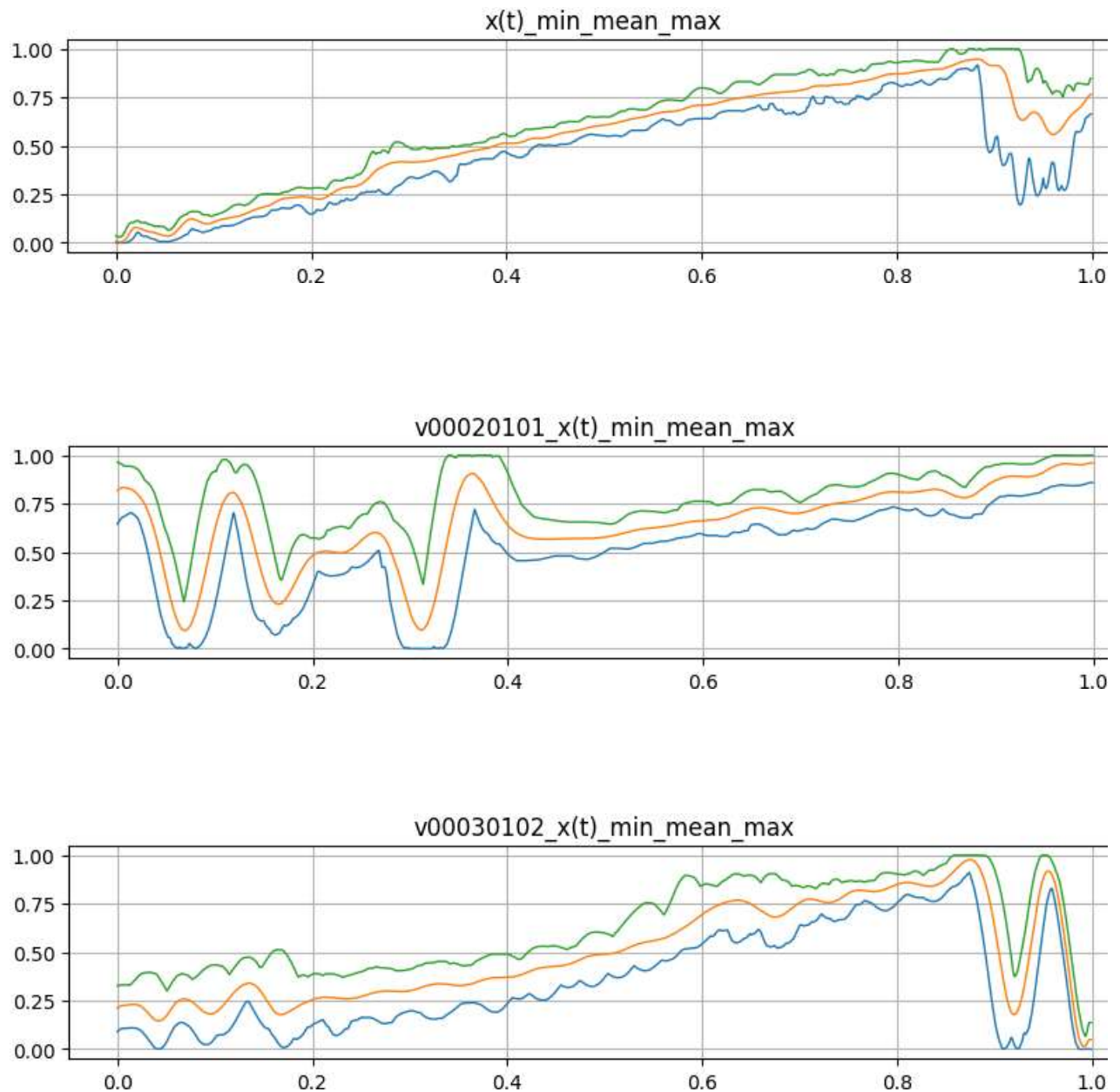


Рисунок 3.3 – Графіки залежності огинаючих параметрів $\tilde{X}(t)$ та усередненого параметру $\tilde{X}(t)$ для $m=25$ оригінальних підписів трьох осіб

Для кількісної оцінки відмінності реального параметра конкретної реалізації підпису від усередненого застосуємо середнє відносне значення відхилення по всіх $N=1000$ точкам $\tilde{X}^j$ ($j=1 \dots m$):

$$\Delta \tilde{x}^j = 100\% \cdot \frac{1}{N} \sum_{i=1}^N \frac{|\tilde{x}_i^j - \tilde{x}_i|}{\tilde{x}_i}, \quad (3.5)$$

Числові дані для оцінки внутрішньоперсональної варіабельності параметрів $X(t)$, $l(t)$ та $\Delta\alpha(t)$ для 1 користувача наведено у табл. 3.1

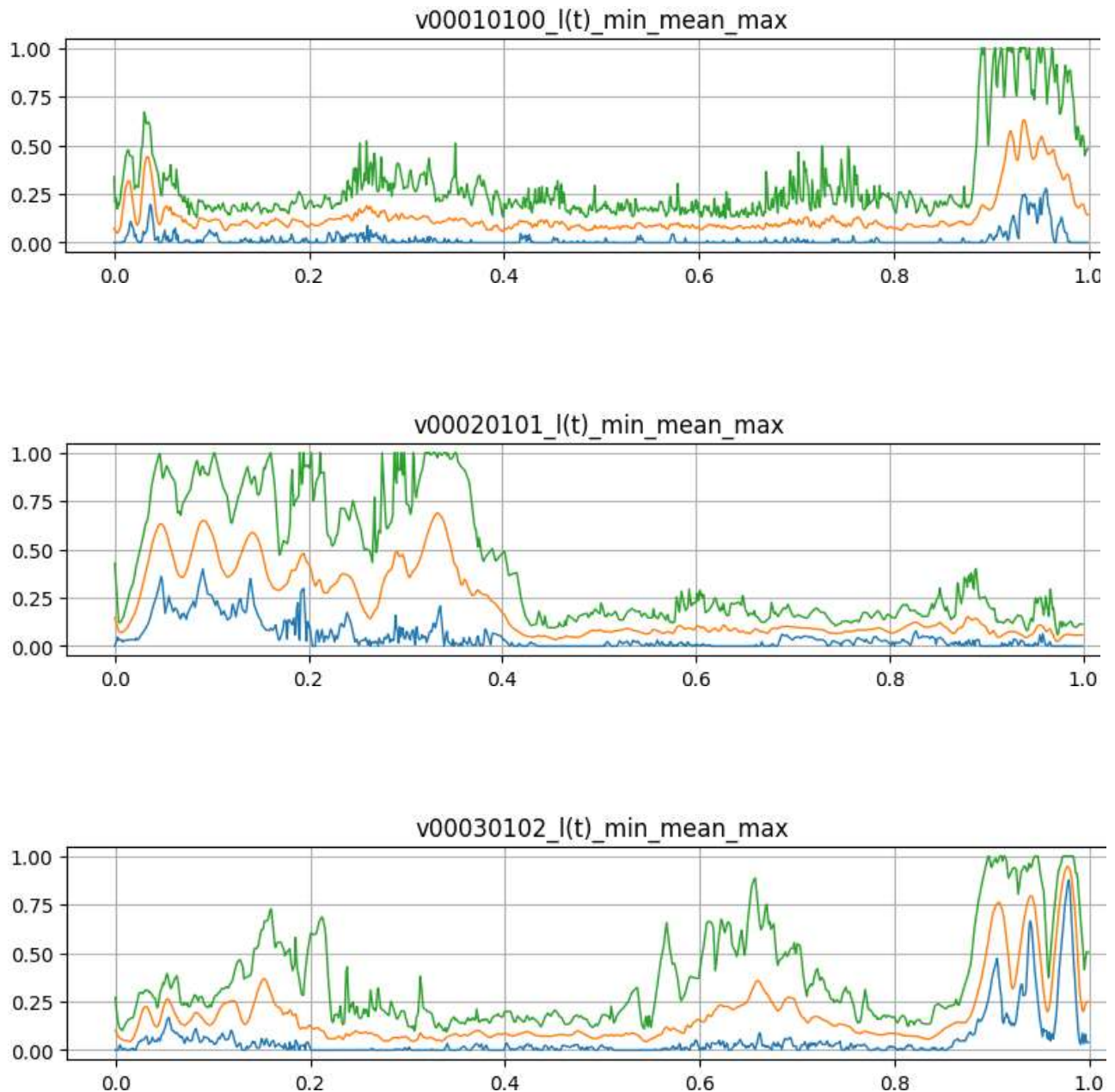


Рисунок 3.4 – Графіки залежності огинаючих параметрів $\tilde{l}(t)$ та усередненого параметру $\bar{l}(t)$ для $m=25$ оригінальних підписів трьох осіб

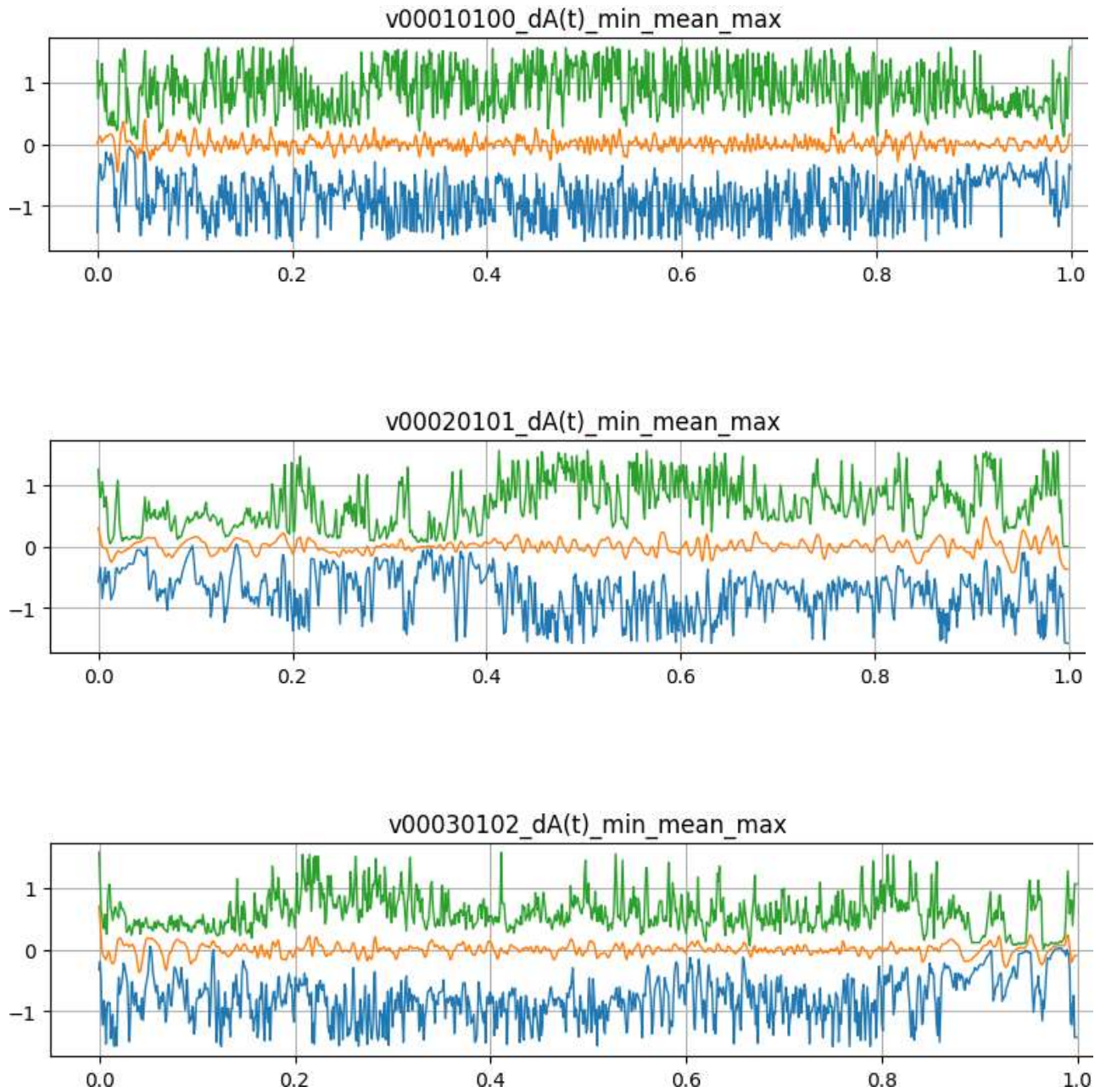


Рисунок 3.5 – Графіки залежності огинаючих параметрів $\Delta\check{\alpha}(t)$ та усередненого параметру $\Delta\tilde{\alpha}(t)$ для $m=25$ оригінальних підписів трьох осіб

Таблиця 3.1 – Числові показники внутрішньоперсональної варіабельності параметрів $X(t)$, $l(t)$ та $\Delta\alpha(t)$ для користувача 1 БД МСУТ-330

№ підпису	Середнє відносне відхилення реалізації підпису, %		
	Для $\tilde{X}(t)$	Для $\tilde{l}(t)$	Для $\tilde{\Delta\alpha}(t)$
1	4,59	5,59	29,29
2	3,96	5,47	29,63
3	3,26	7,00	27,76
4	3,02	5,73	28,11
5	3,55	7,02	30,12
6	3,88	6,13	29,91
7	2,42	5,10	28,65
8	2,32	5,45	28,60
9	2,54	6,13	30,05
10	3,72	7,00	28,53
11	4,57	6,57	32,02
12	3,07	5,83	27,72
13	2,99	5,78	29,54
14	2,35	4,83	29,25
15	2,60	5,49	30,08
16	3,35	6,47	29,93
17	2,64	4,89	28,75
18	2,43	5,26	30,13
19	3,49	7,67	30,48
20	2,38	6,63	28,79
21	2,42	4,89	27,75
22	2,58	6,28	30,23
23	2,18	5,04	28,80
24	2,93	5,93	29,35
25	4,94	5,83	31,27
Середнє відхилення підписів користувача, %	3,13	5,92	29,39

Із табл. 3.1 видно, що для конкретного користувача внутрішньоперсональна варіабельність параметрів $X(t)$ та $l(t)$ чисельно є невеликою і складає відповідно 3,13% та 5,92%, а для параметру $\Delta\alpha(t)$, всупереч очікуванням, чисельно є великою і складає 29,39%. Це вже кількісно свідчить про те, що параметр $\Delta\alpha(t)$ не є робастним (стійким) до внутрішньоперсональної варіабельності, тому його не варто використовувати для ідентифікації підписів.. Справедливість такого висновку для всіх користувачів підтверджується даними табл. 3.2.

Таблиця 3.2 – Числові показники внутрішньоперсональної варіабельності параметрів $X(t)$, $l(t)$ та $\Delta\alpha(t)$ для 230 користувачів БД МСУТ-330

№ користувача	$\tilde{X}(t)$		$\tilde{l}(t)$		$\Delta\tilde{\alpha}(t)$	
	МС середнього відхилення, %	МС діапазону відхилення, %	МС середнього відхилення, %	МС діапазону відхилення, %	МС середнього відхилення, %	МС діапазону відхилення, %
1	3,13	2.18-4.94	5,92	4.83-7.67	29,39	27.72-32.02
2	6,31	2.77-9.27	7,58	5.12-12.01	24,42	22.43-28.29
3	5,66	3.29-9.46	6,55	5.11-9.78	22,58	20.48-24.72
...						
228	5,14	3.03-9.12	6,21	4.97-9.12	23,16	20.63-25.06
229	3,71	2.67-5.31	5,64	4.17-7.21	28,42	27.11-31.24
230	6,23	2.45-9.11	7,12	5.01-11.89	23,75	22.09-27.88
Середнє значення	5,22	2,71-7,92	6,44	4,81-9,73	25,37	23,29-28,43

Таким чином, дані табл. 3.2 доводять обґрунтованість вибору параметру $l(t)$ (мала варіабельність – 6,44%) та необґрунтованість вибору параметру $\Delta\alpha(t)$ (велика варіабельність – 25,37%) для використання у високостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж. Замість параметра $\Delta\alpha(t)$ варто, скоріше всього, обирати добуток $X(t) \times Y(t) = XY(t)$, але це потребує додаткових досліджень.

Ці додаткові дослідження було проведено. Так, на рис. 3.6 показано графік усередненої залежності $\tilde{XY}(t)$ та огибаючі максимальних та мінімальних значень залежностей $\tilde{XY}(t)$ для 25 оригінальних підписів трьох осіб.

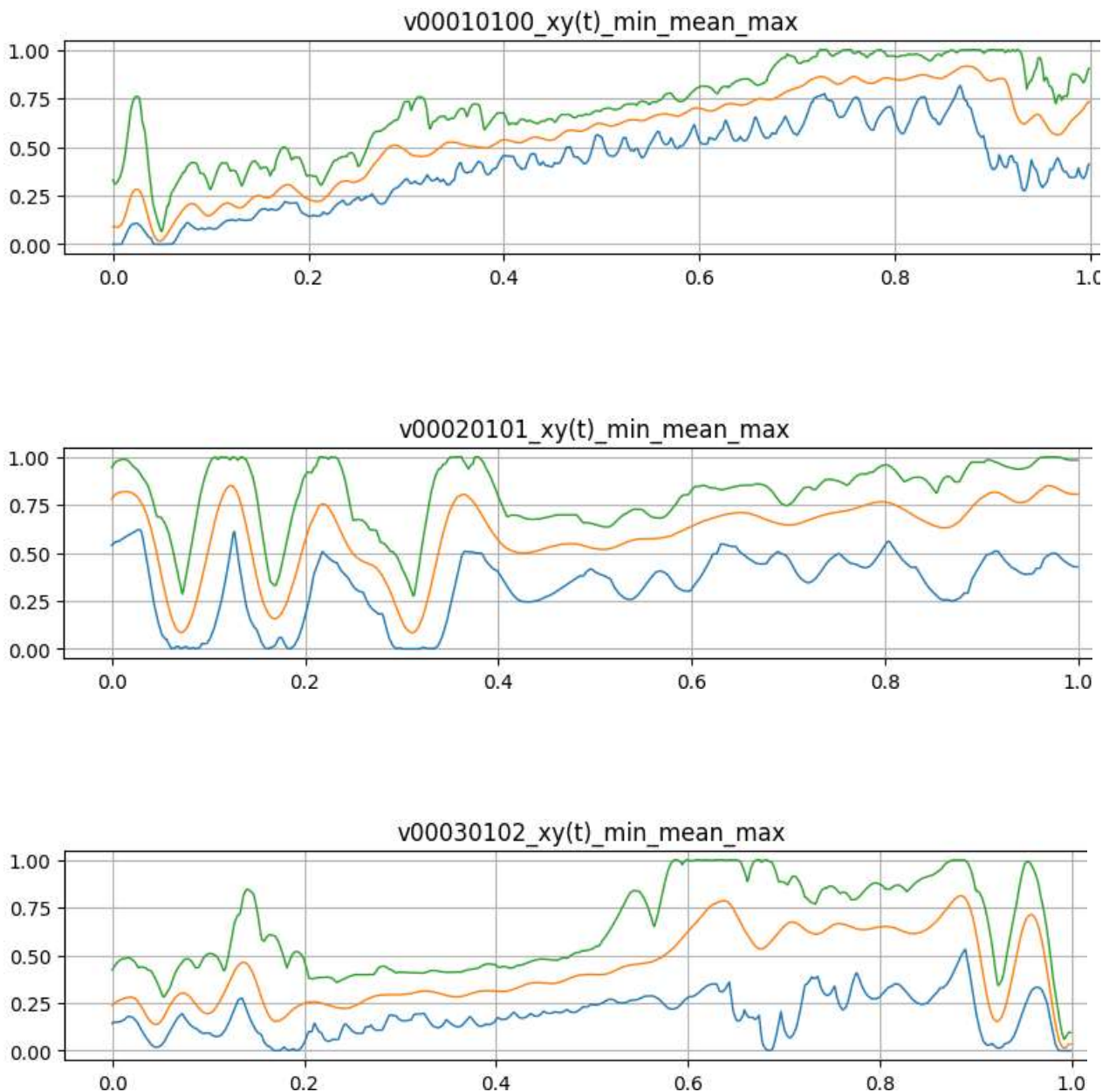


Рисунок 3.6 – Графіки залежності огинаючих параметрів $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ та усередненого параметру $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ для $m=25$ оригінальних підписів трьох осіб

З рис. 3.6 видно, що параметр $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ має невеликий діапазон розкиду відносно середньої залежності $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$. Це свідчить про те, що параметр $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ є робастним (стійким) до внутрішньоперсональної варіабельності, тому його можна використовувати для ідентифікації підписів.

Для кількісної оцінки відмінності реального параметра $\tilde{X}\tilde{Y}(t)$ конкретної реалізації підпису від усередненого застосуємо середнє відносне значення відхилення по всіх $N=1000$ точкам згідно формули (3,5).

Числові дані для оцінки внутрішньоперсональної варіабельності параметрів $X\tilde{Y}(t)$ для 1 користувача наведено у табл. 3.3.

Таблиця 3.3 – Числові показники внутрішньоперсональної варіабельності параметру $X\tilde{Y}(t)$ для користувача 1 БД МСУТ-330

№ підпису	Середнє відносне відхилення реалізації підпису, %
	Для $\tilde{X}\tilde{Y}(t)$
1	5,30
2	5,91
3	4,36
4	5,92
5	4,97
6	5,94
7	4,19
8	6,05
9	5,41
10	1,2
11	6,39
12	5,24
13	5,95
14	6,68
15	12,0
16	4,86
17	3,62
18	4,63
19	4,95
20	7,51
21	4,27
22	4,18
23	4,11
24	4,45
25	9,26
Середнє відхилення підписів користувача, %	5,87

Із табл. 3.3 видно, що для конкретного користувача внутрішньоперсональна варіабельність параметру $X\tilde{Y}(t)$ чисельно є невеликою і складає 5,87%. Це кількісно свідчить про те, що параметр $X\tilde{Y}(t)$ є

робастним (стійким) до внутрішньоперсональної варіабельності, тому його варто використовувати для ідентифікації підписів.. Справедливість такого висновку для всіх користувачів підтверджується даними табл. 3.4.

Таблиця 3.4 – Числові показники внутрішньоперсональної варіабельності параметру $XU(t)$ для 230 користувачів БД МСУТ-330

№ користувача	$\tilde{X}(t)$	
	МС середнього відхилення, %	МС діапазону відхилення, %
1	5,87	3,62-12,0
2	11,68	4,78-24,76
3	8,64	5,47-17,45
...		
228	6,29	3.84-11.72
229	7,83	5,17-13.36
230	7,25	4,92-19.11
Середнє значення	8,04	4,5-18,3

Таким чином, дані табл. 3.4 доводять обґрунтованність вибору параметру $XU(t)$ (мала варіабельність – 8,04%) для використання у високостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж.

3.4 Дослідження чутливості динамічних параметрів підпису до міжперсональної варіабельності

Для дослідження чутливості динамічних параметрів підпису до міжперсональної варіабельності проаналізуємо відмінність параметрів майстерно підроблених підписів однієї особи від середньої залежності для оригінальних підписів цієї ж особи. На рис. 3.7 показано графік усередненої залежності $\tilde{X}(t)$ справжніх підписів та огибаючі максимальних та

мінімальних значень залежностей $\check{X}s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб. Прийmemo гіпотезу, що для $\check{Y}s(t)$ характер залежності буде аналогічним, тому розглядати її не будемо. На рис. 3.8 та рис. 3.9 показано графіки усереднених залежностей $\tilde{l}(t)$ та $\Delta\tilde{\alpha}(t)$ справжніх підписів та огинаючі максимальних та мінімальних значень залежностей $\check{l}s(t)$ та $\Delta\check{\alpha}s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб.

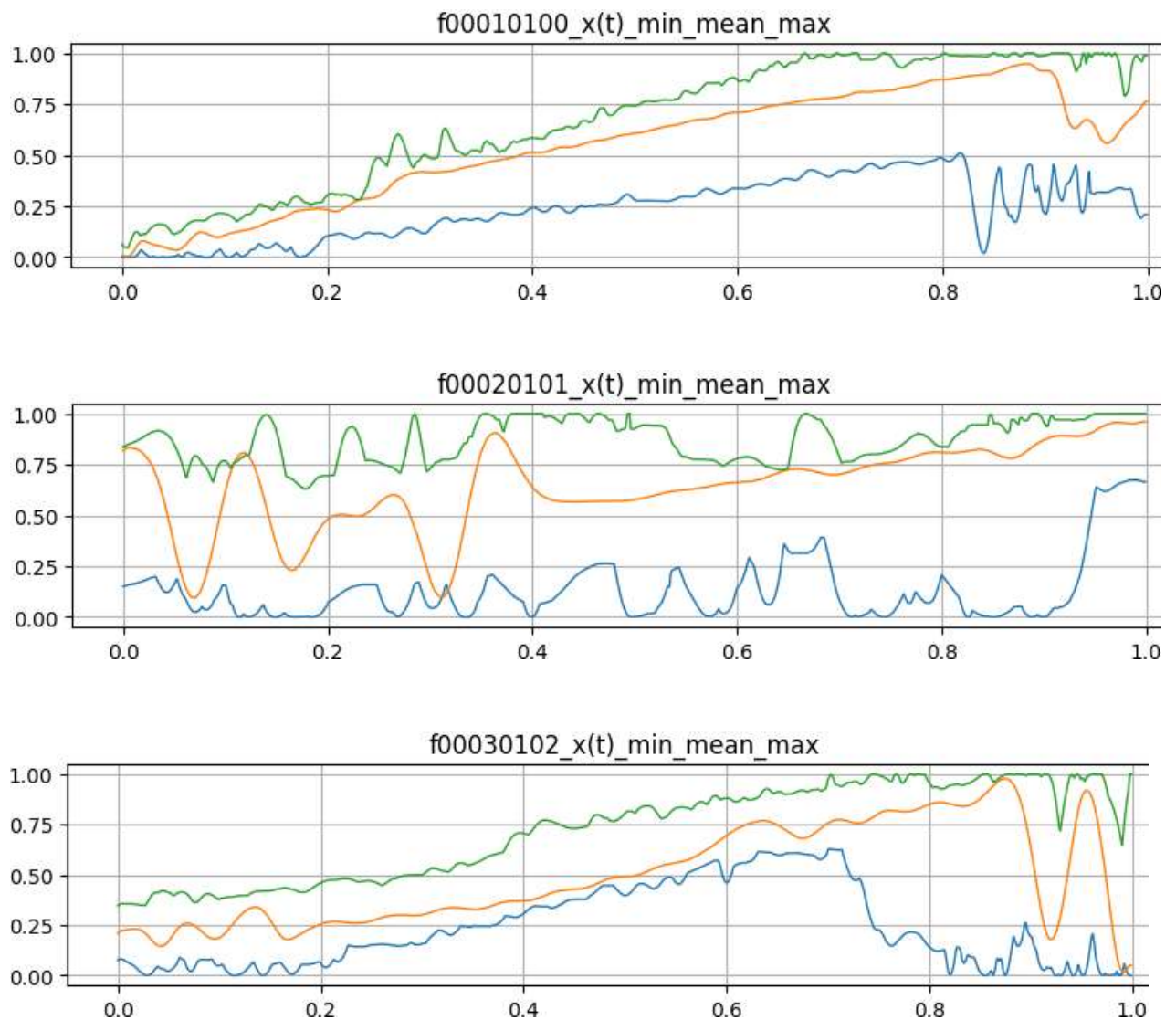


Рисунок 3.7 – Графік усередненої залежності $\check{X}(t)$ справжніх підписів та огинаючі максимальних та мінімальних значень залежностей $\check{X}s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб

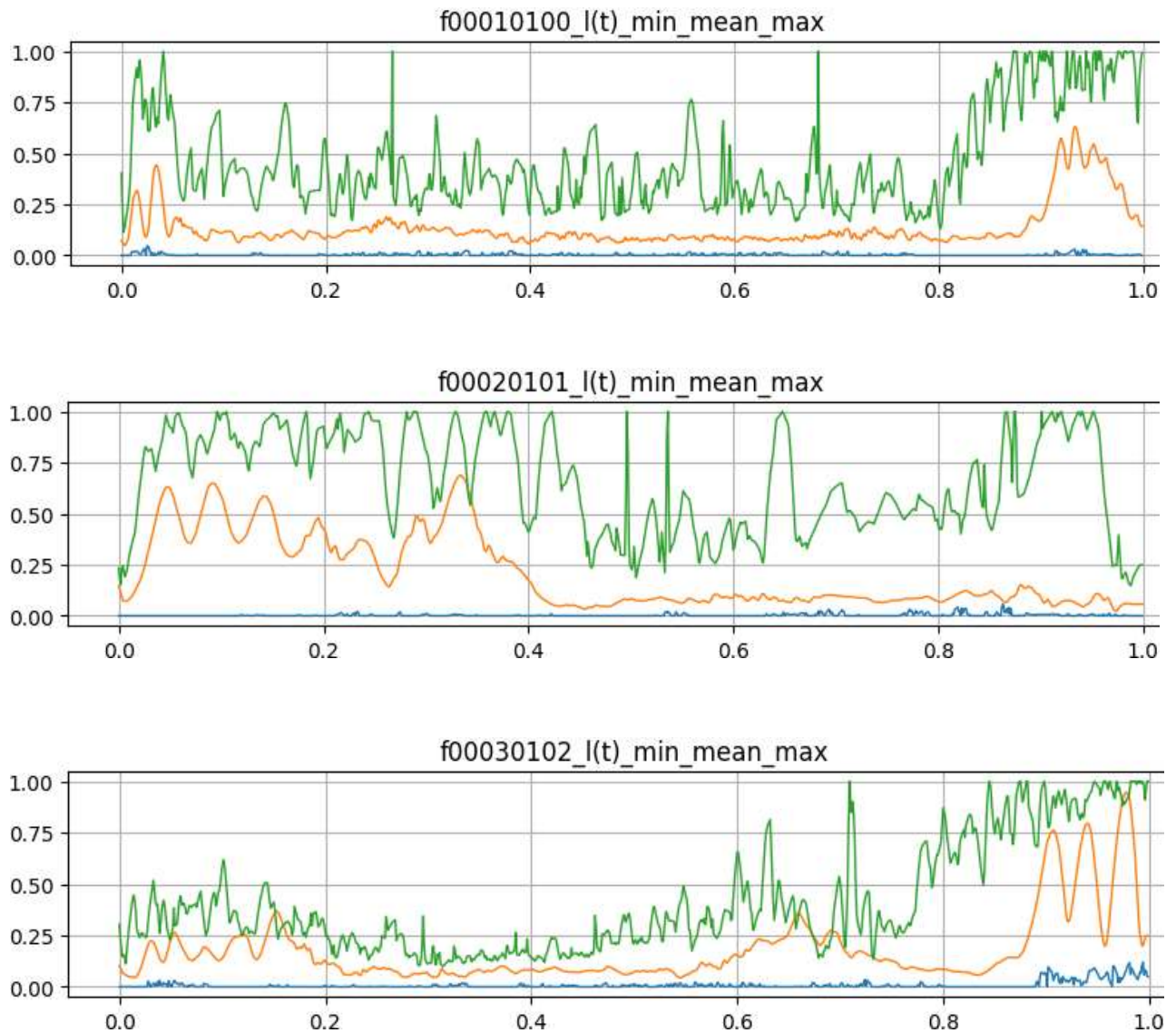


Рисунок 3.8 – Графік усередненої залежності $\tilde{l}(t)$ справжніх підписів та огибаючі максимальних та мінімальних значень залежностей $\check{l}_s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб

Із попарного порівняння рис. 3.3–3.7 та рис. 3.4–3.8 видно, що параметри $\check{X}_s(t)$ та $\check{l}_s(t)$ підробних підписів мають більший діапазон розкиду, ніж параметри $\tilde{X}(t)$ та $\tilde{l}(t)$ справжніх підписів відносно середньої залежності відповідно $\tilde{X}(t)$ та $\tilde{l}(t)$. Крім того, з рисунків видно, що середні залежності $\tilde{X}(t)$ та $\tilde{l}(t)$ проходять не симетрично (не еквідистантно)

огиноючим максимальних та мінімальних значень залежностей $\tilde{X}s(t)$ та $\tilde{l}s(t)$. Це означає, що дисперсія підробних підписів відносно усередненого справжнього підпису буде велика, що дозволить легко відрізнити підробний підпис від справжнього. Тобто динамічні параметри $X(t)$ та $l(t)$ є чутливими до міжперсональної варіабельності підпису.

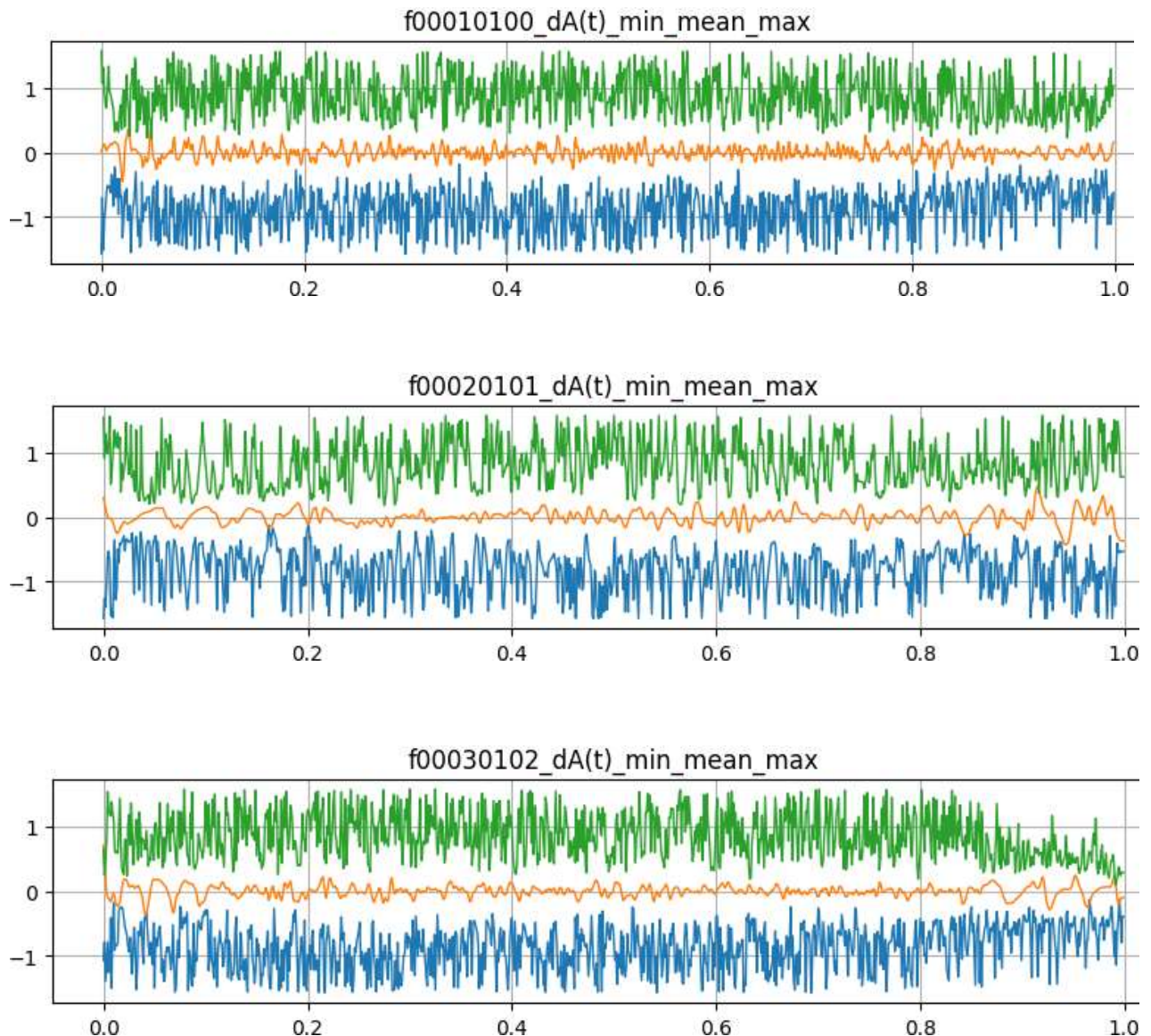


Рисунок 3.9 – Графік усередненої залежності $\Delta\tilde{a}(t)$ справжніх підписів та огиноючі максимальних та мінімальних значень залежностей $\Delta\tilde{\alpha}s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб

А от параметр $\Delta\check{\alpha}s(t)$ підробних підписів, всупереч очікуванням, має такий само великий діапазон розкиду відносно середньої залежності $\Delta\check{\alpha}(t)$, як і параметр $\Delta\check{\alpha}(t)$ справжніх підписів. Це свідчить про те, що параметр $\Delta\alpha(t)$ не є чутливим до міжперсональної варіабельності, тому його не варто використовувати для ідентифікації підписів.

Числові дані для оцінки міжперсональної варіабельності параметрів $\check{X}s(t)$, $\check{l}s(t)$ та $\Delta\check{\alpha}s(t)$ для 1 користувача наведено у табл. 3.5

Таблиця 3.5 – Числові показники міжперсональної варіабельності параметрів $\check{X}s(t)$, $\check{l}s(t)$ та $\Delta\check{\alpha}s(t)$ для користувача 1 БД МСУТ-330

№ підпису	Середнє відносне відхилення реалізації підпису,%		
	Для $\check{X}s(t)$	Для $\check{l}s(t)$	Для $\Delta\check{\alpha}s(t)$
1	5,33	9,29	29,39
2	4,03	8,06	28,38
3	5,78	8,79	28,85
4	4,26	8,28	29,55
5	6,24	10,24	30,54
6	12,32	9,86	27,14
7	13,05	8,52	27,37
8	17,93	11,05	26,98
9	9,42	12,10	25,67
10	9,04	7,94	26,99
11	5,46	7,27	30,73
12	4,87	7,87	29,49
13	6,22	7,46	31,51
14	7,98	7,48	32,07
15	6,84	6,06	31,60
16	11,67	10,85	26,62
17	9,36	10,14	27,88
18	7,28	9,10	24,44
19	28,70	12,24	26,67
20	10,03	8,71	26,07
21	11,40	7,51	28,90
22	9,91	7,67	32,77
23	10,54	9,35	28,49
24	7,29	8,76	31,03
25	9,56	10,64	29,63
Середнє відхилення підписів користувача,%	9,38	9,01	28,75

Із табл. 3.5 видно, що для конкретного користувача міжперсональна варіабельність параметрів $X(t)$ та $l(t)$ чисельно складає відповідно 9,38% та 9,01%, що більше відповідних значень 3,13% та 5,92% внутрішньоперсональної варіабельності. Це кількісно підтверджує той факт, що параметри $X(t)$ та $l(t)$ є чутливими до міжперсональної варіабельності. А параметр $\Delta\alpha(t)$ для підробних підписів 28,75%, всупереч очікуванням, кількісно не відрізняється від аналогічного параметра 29,39% справжніх підписів. Це вже кількісно свідчить про те, що параметр $\Delta\alpha(t)$ не є чутливим до міжперсональної варіабельності, тому його не варто використовувати для ідентифікації підписів.. Справедливість такого висновку для всіх користувачів підтверджується даними табл. 3.6.

Таблиця 3.6 – Числові показники міжперсональної варіабельності параметрів

$\tilde{X}s(t)$, $\tilde{l}s(t)$ та $\Delta\tilde{\alpha}s(t)$ для 230 користувачів БД МСУТ-330

№ користувача	Для $\tilde{X}s(t)$		Для $\tilde{l}s(t)$		Для $\Delta\tilde{\alpha}s(t)$	
	МС середнього відхилення, %	МС максимального відхилення, %	МС середнього відхилення, %	МС максимального відхилення, %	МС середнього відхилення, %	МС максимального відхилення, %
1	9,38	4,03-28,70	9,01	6,06-12,24	28,75	24,44-32,77
2	18,28	7,51-33,90	16,13	10,85-23,12	26,27	21,79-32,58
3	13,66	7,87-22,48	11,57	8,45-16,52	28,41	24,65-31,55
...						
228	17,16	7,92-34,82	17,98	11,63-24,45	27,41	20,92-33,67
229	14,24	8,21-23,31	12,74	9,02-17,38	29,54	25,16-32,23
230	10,09	4,79-29,33	9,87	6,69-13,07	25,98	23,52-30,56
Середнє значення	13,84	6,69-28,83	12,92	8,54-17,91	27,62	23,47-32,15

Таким чином, дані табл. 3.6 доводять обґрунтованість вибору параметру $l(t)$ (мала внутрішньоперсональна варіабельність – 6,44%, велика міжперсональна варіабельність – 12,92%) та необґрунтованість вибору параметру $\Delta\alpha(t)$ (приблизно однакова внутрішньоперсональна та міжперсональна варіабельність – відповідно 25,37% та 27,62%) для

використання у високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж. Замість параметра $\Delta\alpha(t)$ варто, скоріше всього, обирати добуток $X(t) \times Y(t)$, але це потребує додаткових досліджень.

Ці додаткові дослідження було проведено. На рис. 3.10 показано графік усередненої залежності $\tilde{X}\tilde{Y}(t)$ справжніх підписів та огинаючі максимальних та мінімальних значень залежностей $\tilde{X}\tilde{Y}_s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб.

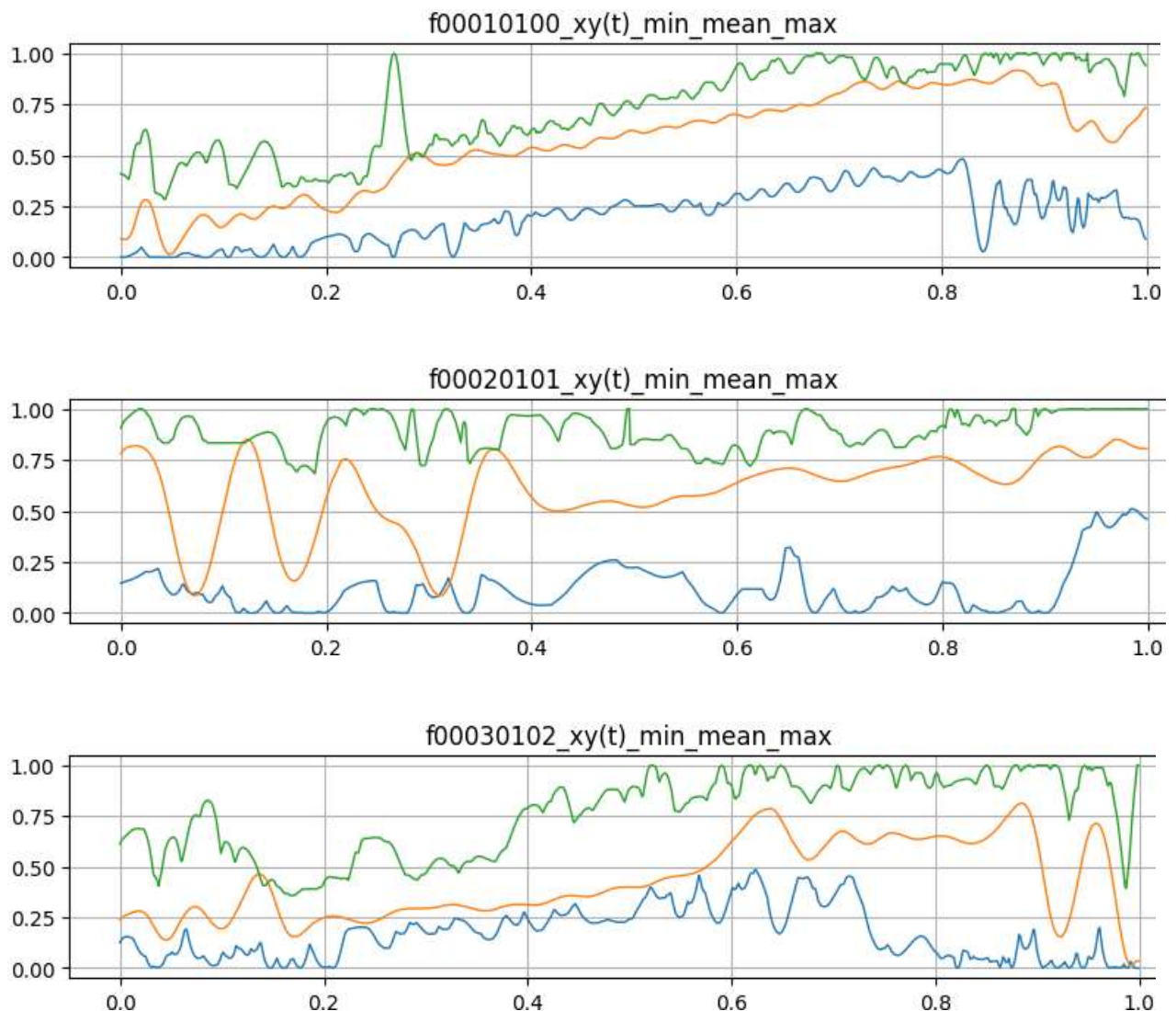


Рисунок 3.10 – Графік усередненої залежності $\tilde{X}\tilde{Y}(t)$ справжніх підписів та огинаючі максимальних та мінімальних значень залежностей $\tilde{X}\tilde{Y}_s(t)$ для 25 кваліфіковано підроблених підписів трьох осіб

Із попарного порівняння рис. 3.6–3.10 видно, що параметр $\tilde{\tilde{X}}\tilde{\tilde{Y}}s(t)$ підробних підписів має більший діапазон розкиду, ніж параметр $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ справжніх підписів відносно середньої залежності відповідно $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$. Крім того, з рис. 3.6 та рис. 3.10 видно, що середня залежність $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ проходить не симетрично (не еквідистантно) огинаючим максимальних та мінімальних значень залежності $\tilde{\tilde{X}}\tilde{\tilde{Y}}s(t)$. Це означає, що дисперсія підробних підписів відносно усередненого справжнього по параметру $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ підпису буде велика, що дозволить легко відрізнати підробний підпис від справжнього. Тобто динамічний параметр $\tilde{\tilde{X}}\tilde{\tilde{Y}}(t)$ є чутливими до міжперсональної варіабельності підпису.

Числові дані для оцінки міжперсональної варіабельності параметру $\tilde{\tilde{X}}\tilde{\tilde{Y}}s(t)$ для 1 користувача наведено у табл. 3.7

Таблиця 3.7 – Числові показники міжперсональної варіабельності параметру $\tilde{\tilde{X}}\tilde{\tilde{Y}}s(t)$ для користувача 1 БД МСҮТ-330

№ підпису	Середнє відносне відхилення реалізації підпису, %
	Для $\tilde{\tilde{X}}\tilde{\tilde{Y}}s(t)$
1	7,16
2	6,03
3	5,25
4	7,92
5	11,57
6	14,06
7	13,10
8	17,31
9	12,23
10	18,81
11	5,56
12	6,26
13	7,81
14	14,17
15	18,41
16	11,63

Таблиця 3.7 (Продовження)

№ підпису	Середнє відносне відхилення реалізації підпису, %
	Для $\check{X}\check{Y}_s(t)$
17	10,55
18	8,82
19	32,71
20	15,21
21	11,28
22	9,07
23	9,02
24	7,51
25	10,93
Середнє відхилення підписів користувача, %	11,70

Із табл. 3.7 видно, що для конкретного користувача міжперсональна варіабельність параметру $\check{X}\check{Y}_s(t)$ чисельно складає 11,70%, що більше відповідного значення 5,87% внутрішньоперсональної варіабельності. Це кількісно підтверджує той факт, що параметр $\check{X}\check{Y}_s(t)$ є чутливими до міжперсональної варіабельності. Справедливість такого висновку для всіх користувачів підтверджується даними табл. 3.8.

Таблиця 3.8 – Числові показники міжперсональної варіабельності параметру

$\check{X}\check{Y}_s(t)$ для 230 користувачів БД МСУТ-330

№ користувача	Для $\check{X}_s(t)$	
	МС середнього відхилення, %	МС максимального відхилення, %
1	11,70	5,25-32,71
2	20,42	12,02-32,56
3	15,36	9,49-21,12
...		
228	13,26	11,58-28,19
229	16,11	4,87-31,02
230	19,25	10,21-22,54
Середнє значення	15,91	8,64-28,14

Таким чином, дані табл. 3.8 доводять обґрунтованість вибору параметру $XY(t)$ (мала внутрішньоперсональна варіабельність – 8.04%, велика міжперсональна варіабельність – 15,91%) для використання у високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж.

Таким чином, в результаті досліджень внутрішньоперсональної та міжперсональної варіабельності різних динамічних параметрів підпису було доведено перспективність та доцільність використання таких параметрів: 1) відстань $l(t)$ від поточного часового відліку координат пера до наступного; 2) добуток координат пера $XY(t)$. Взагалі, пропонується використовуватись набір із 3 динамічних параметрів підпису. Крім 2 зазначених параметрів ($l(t)$ та $XY(t)$), 3-ім параметром пропонується взяти тиск пера на планшет $P(t)$. Він є інваріантним до геометричних параметрів підпису і доцільність його застосування доведена в інших роботах [9],[13]-[15].

3.5 Висновки до третього розділу

1. Обґрунтовано вибір динамічних параметрів підпису, стійких до геометричної варіабельності, тобто зміни просторового масштабу, зсуву та повороту підпису відносно сторін планшету.

2. Розроблено та описано процес нормалізації динамічних параметрів підпису, який здійснюється як по амплітуді, так і по часу. Розроблено формули для здійснення процесу нормалізації динамічних параметрів підпису.

3. Досліджено стійкість динамічних параметрів підпису до внутрішньоперсональної варіабельності на основі статистичного аналізу параметрів розкиду окремих реалізацій підпису відносно усередненої залежності. Доведено обґрунтованість вибору параметрів $l(t)$ та $XY(t)$ (мала варіабельність – відповідно 6,44% та 8,04%) і необґрунтованість вибору параметру $\Delta\alpha(t)$ (велика варіабельність – 25,37%) для використання у

високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж.

4. Досліджено чутливість динамічних параметрів підпису до міжперсональної варіабельності на основі статистичного аналізу параметрів розкиду окремих реалізацій підпису відносно усередненої залежності. Доведено обґрунтованість вибору параметрів $l(t)$ та $XY(t)$ (мала внутрішньоперсональна варіабельність – 6,44% та 8,04% відповідно, велика міжперсональна варіабельність – 12,92% та 15,91% відповідно) та необґрунтованість вибору параметру $\Delta\alpha(t)$ (приблизно однакова внутрішньоперсональна та міжперсональна варіабельність – відповідно 25,37% та 27.62%) для використання у високодостовірному методі динамічної ідентифікації підписів на основі спайкінгових нейронних мереж.

Основні наукові результати, викладені в розділі, опубліковано в роботах [1]-[3], [8].

РОЗДІЛ 4

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ТА ОЦІНКА ДОСТОВІРНОСТІ МЕТОДУ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ ПІДПISУ НА ОСНОВІ СПАЙКІНГОВОЇ НЕЙРОННОЇ МЕРЕЖІ

4.1 Програмна реалізація методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі

Для програмної реалізації методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі було використано мову програмування Python [86], [87]. Python – високорівнева мова програмування загального призначення, орієнтована на підвищення продуктивності розробника і читання коду. Синтаксис ядра Python мінімалістичний. У той же час стандартна бібліотека включає великий обсяг корисних функцій.

Python підтримує структурне, об'єктно-орієнтоване, функціональне, імперативне і аспектно-орієнтоване програмування [88]. Основні архітектурні риси – динамічна типізація, автоматичне керування пам'яттю, повна інтроспекція, механізм обробки виключень, підтримка багатопоточних обчислень, високорівневі структури даних. Підтримується розбиття програм на модулі, які, в свою чергу, можуть об'єднуватися в пакети.

Еталонною реалізацією Python є інтерпретатор Cpython [89], що підтримує більшість активно використовуваних платформ. Він поширюється під вільною ліцензією Python Software Foundation License, що дозволяє використовувати його без обмежень в будь-яких додатках, включаючи пропрієтарні.

Для роботи з нейронними мережами на Python було обрано бібліотеки TensorFlow [90] та Keras [91].

TensorFlow – це відкрита платформа з відкритим кодом для машинного навчання. Він має вичерпну гнучку екосистему інструментів, бібліотек та

ресурсів громади, що підштовхує дослідників в машинне навчання та розробники легко створюють та розгортають програми, що працюють з машинним навчанням.

Keras – це API, призначений для людей, а не для машин. Keras дотримується кращих практик зменшення когнітивного навантаження: він пропонує послідовні та прості API, він мінімізує кількість дій користувачів, необхідних для випадків загального використання, та забезпечує чіткі та діючі повідомлення про помилки. Він також має велику документацію та посібники для розробників.

Як середовище розробки взято Visual Studio Code [92] через його простоту, розповсюдженість та схожість роботи на різних системах таких як Windows, Linux та інші. Застосована система під фреймворком Keras з використанням Tensorflow як фонові, з графічним процесором NVIDIA GeForce RTX 2080 Ti.

Передбачалось, що перевірку якості роботи запропонованої системи ДІП буде здійснюватись з використанням бази даних МСУТ-330 [30], [51]. Для цього потрібно було б побудувати спайкінгову нейронну мережу по рис. 2.6 з кількістю вихідних нейронів 660 (по 2 нейрони на кожного із 330 користувачів) і кількістю інтернейронів не менше $330 \times 15 = 4950$ нейронів. Але така мережа була б громіздкою для реалізації на звичайному комп'ютері. Для її навчання потрібно було б витратити десятки годин.

Тому для пришвидшення інтервалів навчання та функціонування програмно була реалізована спайкінгова нейронна мережа по рис. 2.6, яка мала 40 вихідних нейронів (для 20 користувачів), 3 вхідних нейрона (для 3 динамічних параметрів підпису – $l(t)$, $x(t) \times y(t)$, $p(t)$) та 400 інтернейронів. Просто було програмно реалізовано та навчено 12 таких СНМ, щоб охопити 230 користувачів БД МСУТ-330, які обрано до навчальної вибірки. Навчання однієї такої СНМ займало не більше 2 годин. Детально експеримент по ідентифікації підписів такою СНМ описано у п.4.3.

4.2 Методика оцінки достовірності методів динамічної ідентифікації підпису

Порівняння запропонованих систем ДПП із відомими здійснити насправді не так просто. Одне з головних обмежень – це різні протоколи оцінки в різних пропозиціях. Тобто автори систем ДПП оцінюють власні системи за конкретними експериментальними протоколами. Ці результати не можливо порівнювати прямо. Кожне дослідження конкретної системи ДПП має певний експериментальний протокол, який робить його абсолютно незрівнянним з іншими системами ДПП з точки зору точності. Тим не менш, у співтоваристві з розпізнавання образів (pattern recognition – PR) протягом останніх 12 років було організовано кілька конкурсів [93]-[96] з ідентифікації (верифікації) підписів у рамках найбільш актуальних конференцій у цій галузі, таких як ICDAR (Int. Conf. On Document Analysis and Recognition) та ICFHR (Int. Conf. On Frontiers in Handwriting Recognition). Ці змагання встановили загальні контрольні показники та загальні завдання для тестування сторонніх систем ДПП. Ці зовнішні порівняння дають більш об'єктивну оцінку стану техніки систем ДПП та визначають мету публікації результатів у нових системах..

Таким чином, результати конкурсів [93]-[96] можна розглядати як сучасний стан техніки у цій галузі, оскільки вони можуть гарантувати однакові показники за однакових умов. У цих конкурсах використовуються публічні бази даних підписів, які можна застосовувати як референсні для перевірки працездатності і якості різних систем ДПП. Розглянемо найбільш розповсюджені із цих баз даних.

4.2.1 База даних підписів DeepSignDB

База даних DeepSignDB [29], [30] налічує 1526 користувачів з чотирьох різних популярних баз даних (а саме: MCYT [51], BiosecurID [31], Biosecure DS2 та e-BioSign DS1) та нової бази даних підписів e-BioSign DS2 [53].

Рис. 4.1 графічно узагальнює структуру, пристрої отримання підпису та засоби написання, розглянуті в базі даних DeepSignDB [29], [30].

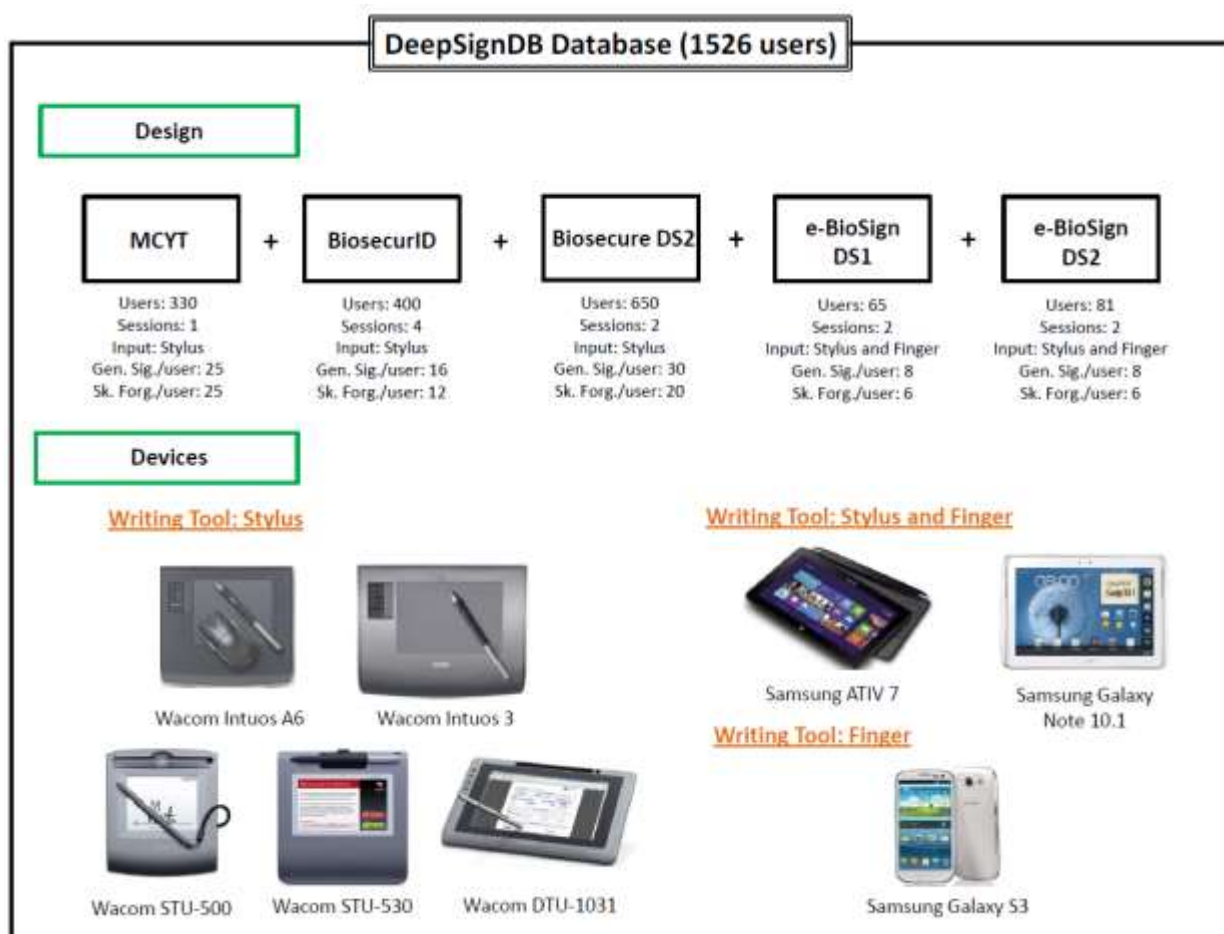


Рисунок 4.1 – Структура, пристрої отримання підпису та засоби написання, розглянуті в базі даних DeepSignDB

Короткий опис кожної бази даних щодо пристрою рукописного введення, кількості сеансів підписування та часового інтервалу між ними, типу підроблених підписів наведено нижче. Що стосується типу кваліфікованих підробок, то можуть розглядатись два різні підходи [97]: 1) статичний, де підробник має доступ лише до зображення підписів для підробки, та 2) динамічний, де підробник має доступ і до зображення справжнього підпису, і до всього процесу підписування (тобто бачить динаміку написання). Динаміку написання можна отримати в присутності оригінального автора або через використання відеозапису (такі випадки

розглянуті в DeepSignDB). У табл. 4.1 узагальнено основні технічні характеристики пристроїв збору динамічних параметрів підпису, що використані в кожному наборі даних DeepSignDB. Важливо підкреслити, що для пристроїв загального призначення (у цьому випадку пристрої Samsung), інформація про роздільну здатність пристрою та частоту дискретизації недоступні. Фактично, частота дискретизації пристроїв загального призначення становить нижче 100 Гц і вона нерівномірна [53].

Таблиця 4.1 – Технічні характеристики пристроїв збору, розглянуті в кожному наборі даних DeepSignDB

БД	Пристрій	Вхід	Екран (діагональ)	Роздільна здатність	Частота дискретизації
МСУТ	Wacom Intuos A6	Stylus	6.4 inches	2,540 lpi	100 Hz
BiosecurID	Wacom Intuos 3	Stylus	12.5 inches	5,080 lpi	100 Hz
Biosecure DS2	Wacom Intuos 3	Stylus	12.5 inches	5,080 lpi	100 Hz
e-BioSign DS1	Wacom STU-500	Stylus	5 inches(640x480 pixels)	2,540 lpi	200 Hz
	Wacom STU-530	Stylus	5 inches (640x480 pixels)	2,540 lpi	200 Hz
	Wacom DTU-1031	Stylus	10.1 inches (1280x800 pixels)	2,540 lpi	200 Hz
	Samsung ATIV 7	Stylus/ Finger	11.6 inches (1920x1080 pixels)	-	-
	Samsung Galaxy Note 10.1	Stylus/ Finger	10.1 inches (1280x800 pixels)	-	-
e-BioSign DS2	Wacom STU-530	Stylus	5 inches (640x480 pixels)	2,540 lpi	200 Hz
	Samsung Galaxy Note 10.1	Finger	10.1 inches (1280x800 pixels)	-	-
	Samsung Galaxy S3	Finger	4.8 inches (720x1280 pixels)	-	-

МСУТ.

База даних МСУТ [51] містить загалом по 25 справжніх підписів та 25 кваліфікованих підробок на кожного користувача, отриманих за один сеанс

блоками по 5 підписів. Всього нараховується 330 користувачів, а підписи отримувались в умовах офісу. Користувачі підписувались на аркуші паперу, всередині сітки, яка позначала місце для підпису, використовуючи чорнильну ручку. Папір розміщували на планшеті Wacom Intuos A6 USB, який фіксував такі часові сигнали пера: просторові координати X та Y , тиск, кутові орієнтації (тобто азимут руху та кут нахилу до площини) та мітки часу. Крім того, доступні траєкторії відриву ручки від планшету. Щодо типу підробок, розглядалися лише статичні підробки.

BiosecurID.

База даних BiosecurID [31] налічує по 16 справжніх підписів та по 12 кваліфікованих підробок на кожного користувача, отримані у 4 окремих сеансах із двомісячним інтервалом між ними. Всього є 400 користувачів, підписи яких були отримані в умовах офісу. Користувачів попросили підписати на аркуші паперу, всередині сітки, яка позначала дозволений простір для підпису, використовуючи чорнильну ручку. Папір розміщували на планшеті Wacom Intuos 3, який фіксував такі часові сигнали: просторові координати X та Y , тиск, кутові орієнтації пера (тобто азимут та кут нахилу) та мітки часу. Траєкторії відриву пера від планшету також доступні. Щодо типу підробок, то розглядаються як статичні (перші два сеанси), так і динамічні (два останні сеанси) підробки.

Biosecure DS2.

База даних Biosecure DS2 [98] налічує по 30 справжніх підписів та по 20 кваліфікованих підробок на кожного користувача, отримані під час 2 окремих сеансів із тримісячним інтервалом між ними. Всього є 650 користувачів і їх підписів, які були отримані в умовах офісу. Користувачів просили, сидячи, підписати аркуш паперу, розміщений поверх пристрою Wacom Intuos 3. Умови отримання підписів аналогічні, як для бази даних BiosecurID. Щодо типу підробок, то лише динамічні підробки були розглянуті.

E-BioSign DS1.

База даних e-BioSign DS1 [53] формувалася з використанням п'яти різних пристроїв. Три з них спеціально розроблені для збору рукописних даних (наприклад, Wacom STU-500, STU-530, та DTU-1031), тоді як інші два – планшети загального призначення, не розроблені для цього конкретного завдання (Samsung ATIV 7 і Galaxy Note 10.1). Варто зазначити, що всі п'ять пристроїв використовувались із власним пером-стилусом. Крім того, два пристрої Samsung використовувались для написання підпису пальцем, що дозволяє проводити аналіз продуктивності введення даних у систему. Для всіх п'яти пристроїв використовувався один і той самий протокол отримання підпису: пристрої розміщувались на робочому столі та підписанти могли повертати їх як завгодно, щоб почувати себе комфортно при підписуванні. Підписи були зібрані за дві сесії з розривом у часі між сесіями 3 тижні. Для кожного користувача загалом є 8 справжніх підписів та 6 кваліфікованих підробок. Для випадку використання стилуса знімалась інформація, що стосується просторових координат X та Y, тиску і мітка часу для всіх пристроїв. Крім того, траєкторії відриву пера також доступні. Однак інформація про тиск і траєкторії відриву пера не реєструвалися для випадків, коли для написання підпису використовувався палець. Щодо типу підробок, то під час першої сесії розглядалися динамічні підробки, під час другої сесії – статичні підробки.

E-BioSign DS2.

База даних DeepSignDB також включає новий набір даних он-лайн підписів з назвою e-BioSign DS2. Цей набір даних дотримується того самого протоколу зняття підпису, що і e-BioSign DS1. Розглядалися три різні пристрої: Wacom STU-530, спеціально розроблений для збору рукописних даних, Samsung Galaxy Note 10.1 – планшет загального призначення та смартфон Samsung Galaxy S3. Для першого пристрою підписи знято за допомогою стилуса в офісному сценарії, тобто пристрій було розміщено на робочому столі і підписанти могли повертати його, щоб почувати себе

комфортно з положенням при письмі. Для планшету Samsung Galaxy Note 10.1 та смартфона Galaxy S3 як засіб написання використовувався палець. Підписи були зібрані за дві сесії для 81 користувача з розривом у часі між сесіями не менше 3 тижнів. Для кожного користувача, пристрою та засобу введення даних (стилус, палець) – всього 8 справжніх підписів та 6 кваліфікованих підробок. Для випадку використання стилусу знімалась інформація, що стосується просторових координат X та Y , тиску і мітка часу для всіх пристроїв. Щодо типу підробок, то лише динамічні підробки були розглянуті.

Деякі невідповідності можуть спостерігатися у частоті дискретизації. Хоча дані планшета для оцифровки можуть вказувати, що частота дискретизації становить, наприклад, 100 Гц, мітка часу, яка зазвичай використовується, може не відображати таку частоту дискретизації протягом усього збору підпису. Профіль швидкості іноді показує розриви під час переходу від «перо вниз» до «перо вгору». Такі розриви можуть бути пов'язані з невідповідностями використовуваного пристрою, наприклад, коли ручка втрачає контакт із планшетом.

Для перевірки якості роботи запропонованої системи ДПП на основі спайкінгової нейронної мережі оберемо базу даних DeepSignDB [29]-[31]. Фрагмент txt файлу бази даних DeepSignDB [99], що відповідає одному підпису, представлений на рис. 4,2.

На рис. 4.2 число у першому рядку – це кількість відліків підпису. У даному прикладі 452 відліки. Далі йдуть рядки тексту, у кожному з яких по 6 цифр, розділених пробілами. Тобто можна вважати, що це таблиця із 6 колонок. Перша колонка – це координата X відліків підпису. Координата X може змінюватись від 0 до 12700. Друга колонка – це координата Y відліків підпису. Координата Y може змінюватись від 0 до 9700. Третя колонка – це номер відліку, помножений на 10 (0, 10, 20, 30 і т.д. до 4510 у прикладі на рис. 4.2, тобто всього 452 відліки, що свідчить про те, що даний підпис був виконаний за 4,51 секунди – тривалість підписування).

```

452
1240 7836 0 114 68 274
1266 7830 10 116 68 404
1266 7844 20 117 67 420
1266 7855 30 119 66 433
1287 7886 40 116 66 447
1321 7930 50 116 66 483
1367 7987 60 114 66 499
1417 8066 70 110 66 527
1456 8159 80 110 66 561
...
3002 7753 4470 112 64 986
3002 7753 4480 112 64 959
3002 7753 4490 112 64 911
3025 7765 4500 112 64 777
3063 7792 4510 111 64 294

```

Рисунок 4.2 – Фрагмент txt файлу бази даних DeepSignDB, що відповідає одному підпису

Четверта колонка – це часовий крок (time stamp) зняття відліків підпису, Взагалі, часовий крок зняття відліків дорівнює 10мс (оскільки частота зняття відліків дорівнює 100 Гц), але він у реальних пристроях трохи «плаває», Тому як видно із рис. 4.2, реальний часовий крок (time stamp) для даного прикладу змінюється від 107 до 124, тобто від 10,7 до 10,24 мс. П'ята колонка – це кут нахилу пера до планшету, який може змінюватись від 300 до 900 (тобто від 30° до 90°). Шоста колонка – це тиск, який може змінюватись від 0 до 1024. Якщо потрібно азимут руху пера, то його можна порахувати по X та Y.

4.2.2 Програмний засіб для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису

З метою дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису, результати яких викладено у пп. 3.3-3.4, було розроблено програмний засіб для формування та

статистичного аналізу інваріантних ознак динаміки підписів із БД МСУТ330. Алгоритм роботи цього програмного засобу доволі простий, тому немає сенсу розробляти його граф-схему. Сформулюємо його словесно:

- 1) Читання поточного каталогу і вибір імен файлів з розширенням txt,
- 2) Отримання списку імен файлів підписів,
- 3) Завантаження 25 підписів з файлів,
- 4) Зчитування файлів поточного підпису,
- 5) Задання розміру рисунку в см,
- 6) Побудова 5 підписів на одному рисунку,
- 7) Побудова суміщеного графіку залежності координат X від часу,
- 8) Побудова суміщеного графіку залежності координат Y від часу,
- 9) Побудова суміщеного графіку нормалізованої залежності координат X від часу,
- 10) Побудова суміщеного графіку нормалізованої залежності координат Y від часу,
- 11) Побудова суміщеного графіку залежності L від часу,
- 12) Побудова суміщеного графіку нормалізованої залежності L від часу,
- 13) Побудова суміщеного графіку залежності різниці кутів від часу,
- 14) Побудова суміщеного графіку нормалізованої залежності різниці кутів від часу,
- 15) Обчислення середнього відносного значення відхилення для параметрів X, Y, L, дельта альфа від усередненої залежності.

Програмний модуль розроблений на мові програмування Python 3.6. [86] – [88]. Python було обрано тому, що він надає широкий спектр потужних інструментів та бібліотек для розробки програмного забезпечення, обробки графіків, роботи з великим обсягом даних, навчання, роботи з багатовимірними матрицями та використання моделей машинного навчання. Також Python дозволяє працювати з файловою системою, що необхідно в

даний предметній області. Для розробки програмного модуля було обрано середовище Visual Studio Code [100].

Структура програмного засобу для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису представлена на рис. 4.3.

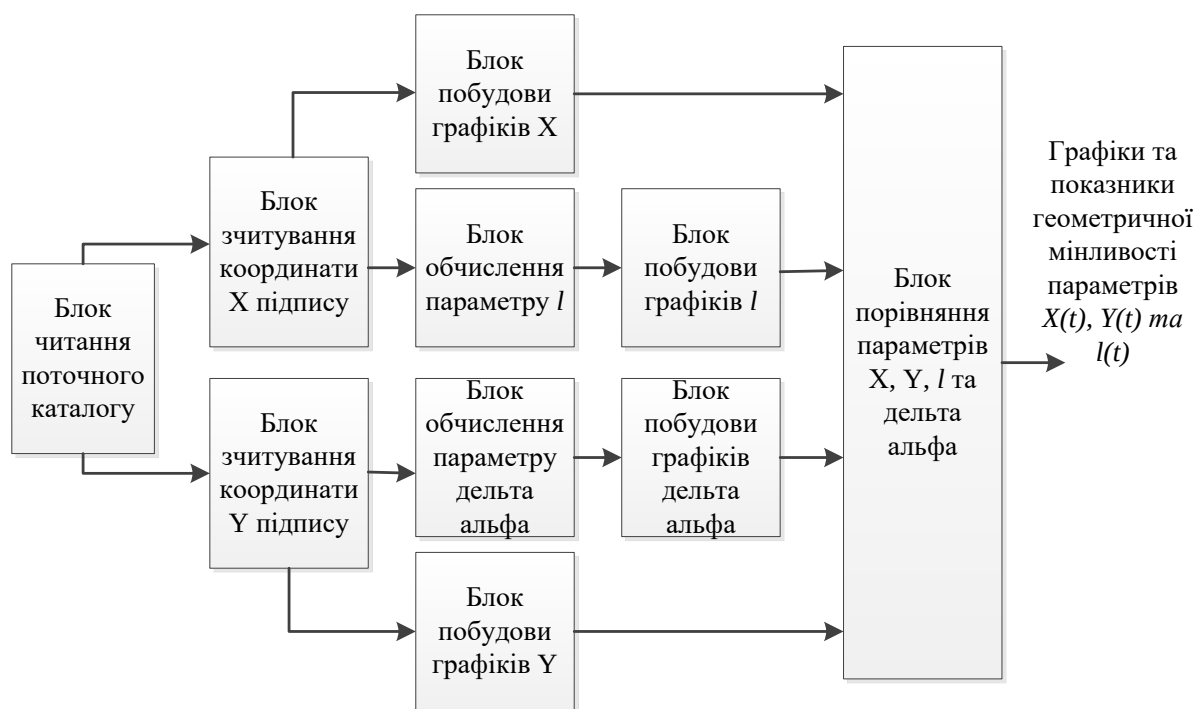


Рисунок 4.3 – Структура програмного засобу для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису

При програмній Реалізація основних компонентів програмного модуля крім стандартних засобів Python також використовувались можливості бібліотеки Matplotlib [101]. Matplotlib — бібліотека на мові програмування Python для візуалізації даних двовимірною 2D графікою. Отримувані зображення можуть бути використані як ілюстрації в публікаціях. Фрагмент лістингу програмного засобу для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису подано у Додатку Б.

Для використання розробленого програмного засобу для дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису необхідно, щоб у поточний каталог були завантажені файли різних реалізацій підпису, отримані з бази даних МСУТ-300. Для кожного користувача у БД є по 25 справжніх підписів та по 25 майстерно підроблених підписів.

Після запуску програма спочатку будує всі підписи користувача. Для прикладу на рис. 4.4 показано фрагмент із 5 різних реалізацій підпису одного користувача.

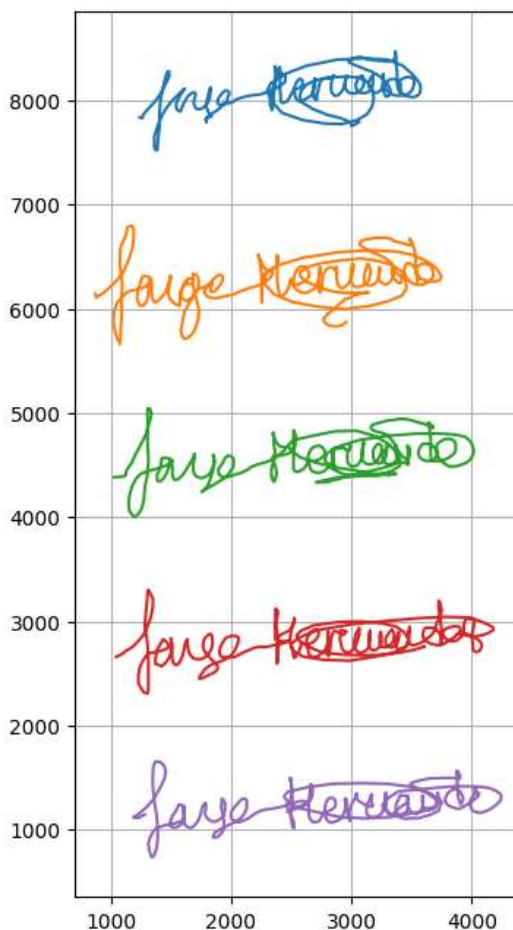


Рисунок 4.4 – Фрагмент із 5 різних реалізацій підпису одного користувача

Далі програма будує суміщений графік залежності координат $X(t)$ від часу для 25 справжніх підписів одного користувача – див. рис. 4.5а. Потім програма будує суміщений графік нормалізованої залежності координати $X(t)$

від часу для 25 справжніх підписів одного користувача – див. рис. 4.5б. А також будує графік усередненої залежності координат $X(t)$ від часу та мінімальну та максимальну огинаючі для 25 справжніх підписів одного користувача – див. рис. 4.5в.

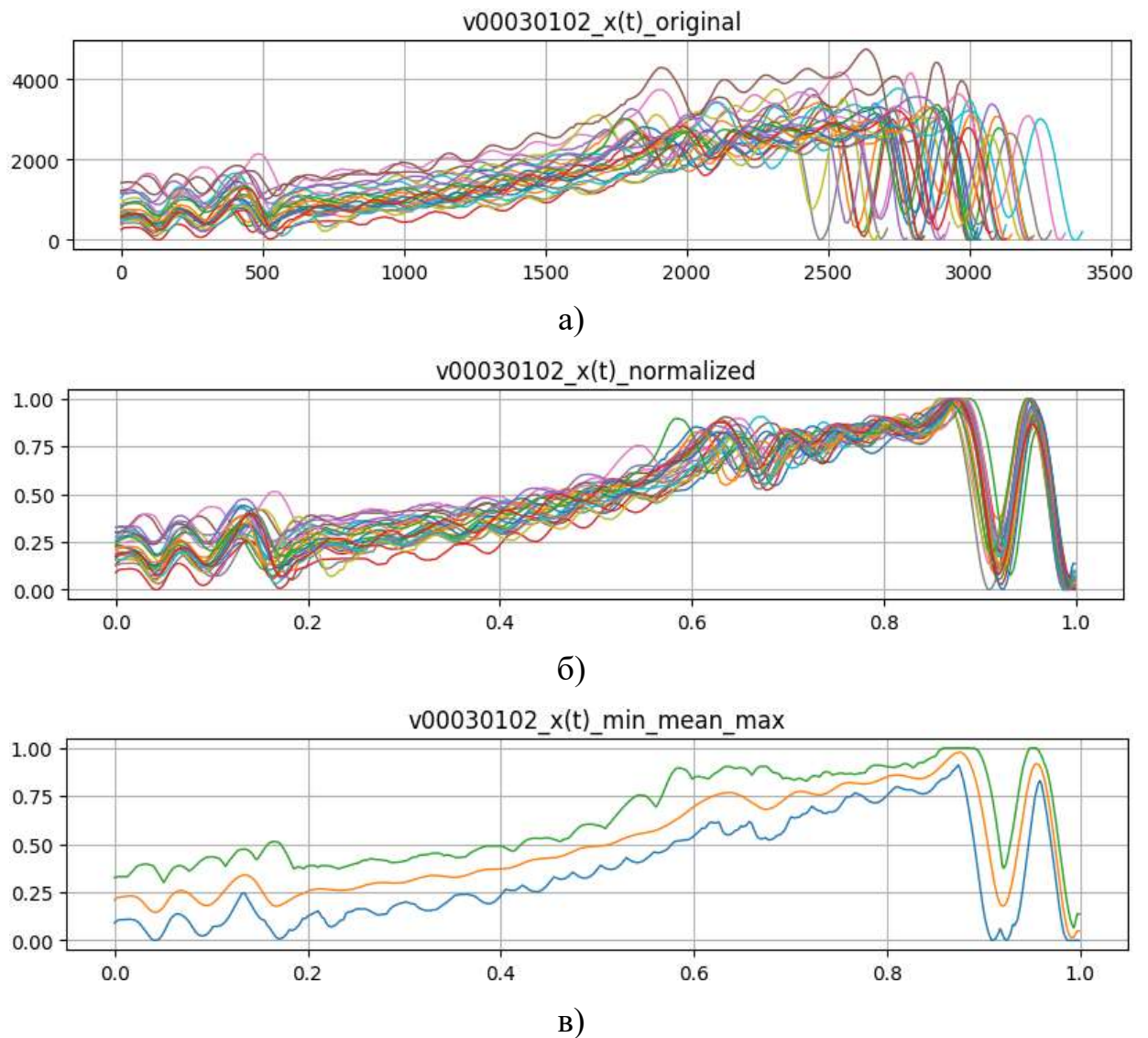
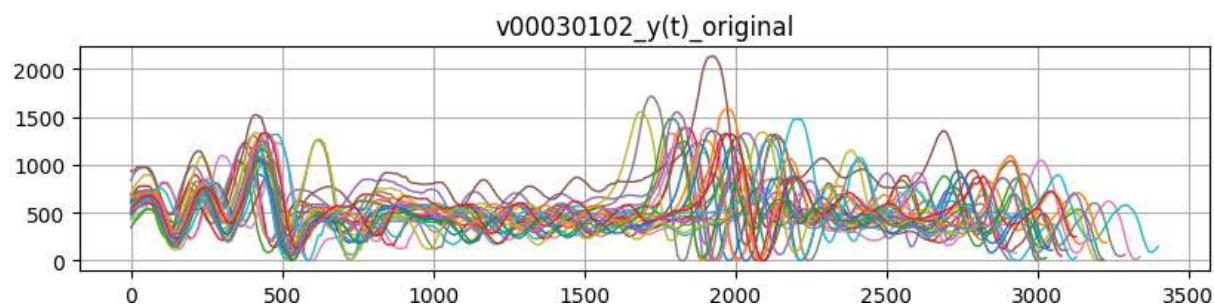
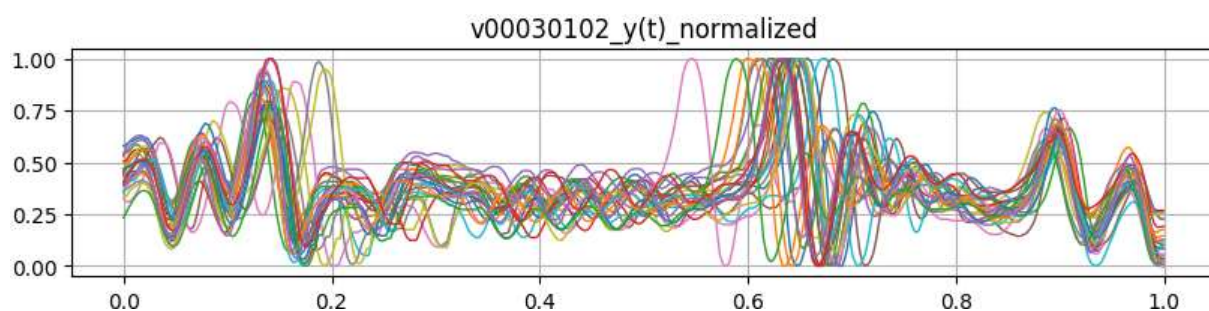


Рисунок 4.5 – Суміщений графік залежності координат X від часу для 25 справжніх підписів одного користувача: а) первинні залежності, б) нормалізовані залежності, в) усереднена залежність та огинаючі

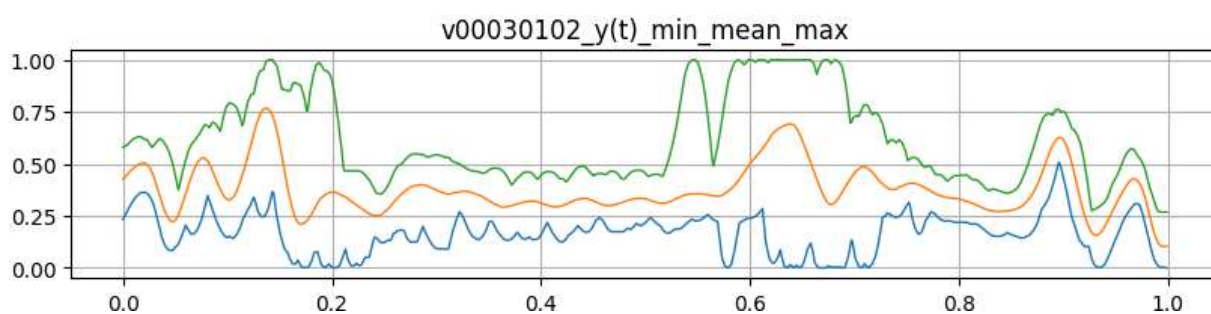
Також програма може побудувати залежності, аналогічні поданим на рис. 4.5 і для інших досліджуваних динамічних параметрів підпису. А саме – для $Y(t)$ (рис. 4.6), $l(t)$, $\Delta\alpha(t)$, $XY(t)$, $P(t)$ та інших.



а)



б)



в)

Рисунок 4.6 – Суміщений графік залежності координат Y від часу для 25 справжніх підписів одного користувача: а) первинні залежності, б) нормалізовані залежності, в) усереднена залежність та огибаючі

Потім програма обчислює середнє відносне значення відхилення для параметрів $Y(t)$ (рис. 4.6), $l(t)$, $\Delta\alpha(t)$, $XY(t)$, $P(t)$ від усередненої залежності. Ця програма була використана для досліджень, результати яких наведено у пп. 3.3–3.4.

4.2.3 Показники якості систем ідентифікації підписів

Частково показники якості систем ідентифікації підписів розглянуто у п. 1.4.2. Тут розглянемо їх більш детально.

Взагалі, на вхід системи ДПП надходять два види підписів: справжні та підробні. І можливі наступні варіанти вихідного сигналу ДПП:

1) справжній підпис ідентифіковано як справжній (вірнопозитивний результат – True positive – TP);

2) справжній підпис ідентифіковано як підробний (хибнонегативний результат – False Negative – FN, помилка 2-го роду);

3) підроблений підпис ідентифіковано як підробний (вірhoneгативний результат – True Negative – TN);

4) підроблений підпис ідентифіковано як справжній (хибнопозитивний результат – False positive – FP, помилка 1-го роду).

Детально ці 4 випадки відображено у матриці невідповідностей [102], [103] (confusion matrix) на рис. 4.7

	Результат ідентифікації	
	Підпис є справжнім	Підпис є підробленим
На вході справжній підпис (загальна кількість справжніх підписів P)	Вірнопозитивний True positive – TP	Хибнонегативний False Negative – FN помилка 2-го роду
На вході підроблений підпис (загальна кількість підроблених підписів N)	Хибнопозитивний False positive – FP помилка 1-го роду	Вірhoneгативний True Negative – TN

Рисунок 4.7 – Можливі варіанти вхідного сигналу та результату ідентифікації системою ДПП

Вірнопозитивні та вірhoneгативні – це результати, які правильно ідентифіковані і, отже, показані зеленим кольором. А хибнопозитивні та хибнонегативні – це результати, які неправильно ідентифіковані (помилкові) і, отже, показані червоним кольором, їх потрібно мінімізувати.

На основі цих чотирьох параметрів розраховуються такі показники якості систем ДПП: достовірність (accuracy), влучність (precision), повнота (recall) та оцінка F1 (F1 score) [104].

Достовірність. Достовірність є найбільш інтуїтивно зрозумілим показником якості систем ДПП, і це просто відношення кількості вірних результатів ідентифікації підписів до загальної кількості підписів, поданих на ідентифікацію.

$$\text{Accuracy} = (TP + TN) / (TP + FP + FN + TN)$$

Але достовірність не є найкращим показником якості систем ДПП. Так, достовірність є гарним показником, але лише тоді, коли у нас є симетричні набори даних, тобто коли кількість хибнопозитивних та хибнонегативних результатів майже однакові. Тому часто для характеристики якості систем ДПП застосовують інші параметри, щоб всебічно оцінити якість системи ДПП.

Влучність. Влучність – це відношення вірнопозитивних (True positive – TP) результатів ідентифікації до загальної кількості позитивних результатів ідентифікації.

$$\text{Precision} = TP / (TP + FP)$$

Ця метрика відповідає на питання про те, яка частка тих підписів, що ідентифіковані як справжні, дійсно є справжніми, Висока влучність пов'язана з низькою кількістю хибнопозитивних.

Повнота (Чутливість). Повнота (Recall, Sensitivity) – це відношення вірнопозитивних (True positive – TP) результатів ідентифікації до загальної кількості справжніх підписів, поданих на ідентифікацію. Цей параметр показує частку вірно ідентифікованих справжніх підписів із усіх справжніх підписів, поданих у систему.

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN})$$

Оцінка F1 (F1 Score). Оцінка F1 – це середньозважене значення достовірності та повноти. Отже, ця оцінка враховує як хибнопозитивні, так і хибнонегативні результати ідентифікації.

$$\text{F1 Score} = 2 * (\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision})$$

Інтуїтивно зрозуміти це не так просто, як достовірність. Але оцінка F1 зазвичай корисніша за достовірність, особливо якщо маємо нерівномірний розподіл класів. Достовірність працює найкраще, якщо хибнопозитивні та хибнонегативні результати мають однакову вартість. Якщо вартість хибнопозитивних та хибнонегативних результатів сильно різниться, краще поглянути і на влучність і на повноту.

4.2.4 Стандарт експериментального протоколу

З метою справедливого порівняння нових підходів ідентифікації підписів із сучасним рівнем розвитку цього напрямку, в роботі [29], [30] запропоновано стандарт експериментального протоколу, який пропонується використовувати дослідницькою спільнотою. Тому амец ей протокол ми використаємо для оцінки якості запропонованого у даній роботі методу динамічної ідентифікації підписів на основі спайкінгової нейронної мережі.

База даних DeepSignDB [29] – [31] розділена на два різних набори даних: один для розробки та навчання системи, а інший – для остаточного оцінювання. Набір даних для розробки та навчання включає близько 70% користувачів кожної бази даних, тоді як решта 30% включені в набір даних для остаточного оцінювання. Важливо зазначити, що кожен набір даних включає різних користувачів, щоб уникнути необ'єктивних результатів.

Для навчання систем, набір даних розробки та навчання налічує 1084 користувачів. У наших експериментах ми маємо розділити цей набір даних

на дві різні підмножини: навчальну (80%) та валідаційну (20%). Однак, оскільки цей набір даних використовується лише для розробки, а не для остаточного оцінювання систем, автори вважають за краще не встановлювати жодних обмежень і дозволяють дослідникам використовувати його як вони того хочуть.

Для остаточного тестування систем, решта 442 користувачі бази даних DeepSignDB включені в набір даних для остаточного оцінювання для того, щоб виконати повний аналіз систем перевірки підпису, і побачити їх узагальнювальну потужність при різних сценаріях. Наступні аспекти були враховані в остаточному проекті експериментального протоколу:

- міжсесійна мінливість: справжні підписи з різних сесій обираються для навчання та тестування (різні блоки збору підписів із бази даних МСУТ);

- кількість навчальних підписів: розглядається два різні випадки: 1) використання для навчання лише одного справжнього підпису з першої сесії (1vs1) та 2) використання для навчання перших 4 справжніх підписів з першої сесії (4vs1).

- сценарій підробника: кваліфіковані та випадкові підробки розглядаються в експериментальному протоколі. Для випадку кваліфікованих підробок, усі наявні кваліфіковані підробки включено в аналіз. Тоді як для випадку випадкових підробок, обирається один справжній зразок підпису кожного з решти користувачів цієї ж бази даних. Таким чином, системи ДПІ тестуються різними типами підробок [97].

- введення даних: сценарії стилуса та пальця враховується в експериментальному протоколі через високе прийняття суспільством щоденного використання мобільних пристроїв [105].

- пристрій отримання підпису: вісім різних пристроїв розглядаються в експериментальному протоколі. Це дозволяє оцінювати здатність узагальнення запропонованої системи до різних пристроїв отримання підпису, які можна знайти в різних додатках.

У табл. 4.2 описуються всі деталі експериментального протоколу оцінки систем ДП, основанийо на наборі даних DeepSignDB, при введенні підпису як стилусом (зверху), так і пальцем (внизу).

Таблиця 4.2 – Деталі експериментального протоколу оцінювання на основі набору DeepSignDB (442 користувачі)

Введення підписів стилусом						
База даних	К-ть користувачів	Пристрої	#Навчальних справжніх підписів	#Тестувальних справжніх підписів	#Тестувальних майстерно підроблених підписів	#Тестувальних випадково підроблених підписів
МСУТ	100	Wacom Intuos A6	1/4 (сесія 1)	21 (решта)	25 (всі)	99 (по одному підпису решти користувачів)
BiosecurID	132	Wacom Intuos 3	1/4 (сесія 1)	12 (сесії 2-4)	12 (all)	131 (по одному підпису решти користувачів)
Biosecure DS2	140	Wacom Intuos 3	1/4 (сесія 1)	15 (сесія 2)	20 (all)	139 (по одному підпису решти користувачів)
e-BioSign DS1	35	W1: Wacom STU-500 W2: Wacom STU-530 W3: Wacom DTU-1031 W4: Samsung ATIV 7 W5: Samsung Note 10.1	1/4 (сесія 1)	4 (сесія 2)	6 (all)	34 (по одному підпису решти користувачів)
e-BioSign DS2	35	W2: Wacom STU-530	1/4 (сесія 1)	4 (сесія 2)	6 (all)	34 (по одному підпису решти користувачів)

Для експериментального дослідження та перевірки якості роботи запропонованої системи ДП на основі спайкінгової нейронної мережі оберемо експериментальний протокол оцінювання на основі набору DeepSignDB [29]-[31], але із деякими уточненнями та спрощеннями.

4.3 Експериментальні дослідження достовірності методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі

Для дослідження параметрів якості роботи систем ДПП використовують тестову вибірку, у яку включають як справжні підписи, так і підробні, але ті, які не були присутні у навчальній вибірці. Частіше всього у тестову вибірку включають і майстерно підроблені (skilled forgery) і випадково підроблені (random forgery) підписи, і прості підробки (simple forgery). Частіше всього використовують один із трьох варіантів. У тестову вибірку включають:

- 1) тільки майстерно підроблені підписи (skilled forgery),
- 2) тільки випадково підроблені підписи (random forgery),
- 3) і майстерно підроблені підписи (skilled forgery), і випадково підроблені підписи (random forgery) у пропорції 50:50.

Найцікавішим є, звичайно, перший варіант, оскільки важливо знати саме стійкість системи до майстерних підробок. До випадкових підробок частіше всього всі системи ДПП достатньо стійкі. У цій роботі ми застосували для тестування 1) та 2) варіанти.

Спочатку для експериментального дослідження параметрів якості роботи запропонованої системи ДПП на основі спайкінгової нейронної мережі було обрано БД МСҮТ-330 [51], яка є частиною DeepSignDB [29]-[31].

Експериментальний протокол [30] не передбачає використання майстерно підроблених підписів для навчання системи ДПП, а запропонована нами система ДПП потребує таку можливість при навчанні. Тому ми трохи змінили цей протокол. Крім того, нам потрібно для навчання запропонованої системи використовувати більше 4 справжніх підписів. Тому тут теж потрібні зміни.

Наш протокол виглядає так:

1) із БД МСУТ-330, яка містить 330 користувачів було обрано згідно протоколу [30] 230 перших користувачів для навчання та тестування нашої системи;

2) для кожного користувача у БД МСУТ-330 є по 25 справжніх підписів і по 25 майстерно підроблених підписів, тобто всього для обраних 230 користувачів є $230 \times 25 = 5750$ справжніх підписів і 5750 майстерно підроблених підписів;

3) для навчання системи із кожних 25 справжніх підписів обрано перших 15, а інші 10 – для тестування. Так само для навчання системи із кожних 25 майстерно підроблених підписів обрано перших 15, а інші 10 підроблених – для тестування;

4) таким чином для навчання системи обрано $15 \times 230 = 3450$ справжніх підписів та 3450 майстерно підроблених підписів;

5) а для тестування системи обрано $10 \times 230 = 2300$ справжніх підписів та 2300 майстерно підроблених підписів (варіант 1 тестування);

Отже, при розрахунках показників якості нашої системи ДПП за формулами з п.4.2.3 загальна кількість справжніх підписів, поданих при тестуванні на ідентифікацію $P = TP + FN = 2300$, і загальна кількість майстерно підроблених підписів, поданих при тестуванні на ідентифікацію $N = TP + FN = 2300$.

Результати тестування запропонованої системи ДПП на основі спайкінгової нейронної мережі при використанні тільки майстерно підроблених підписів наведено у табл. 4.3.

Розрахуємо основні показники якості розробленої системи ДПП на основі даних табл. 4.3 при тестуванні тільки на майстерно підроблених підписах (Skilled Forgeries – SF).

Достовірність.

$$\text{Accuracy(SF)} = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% = \frac{2292 + 2129}{4600} \times 100\% = 96,1\%$$

Таблиця 4.3 – Результати тестування запропонованої системи ДІП на основі спайкінгової нейронної мережі

	Результат ідентифікації	
	Підпис є справжнім	Підпис є підробленим
На вході справжній підпис (загальна кількість справжніх підписів P=2300)	Вірнопозитивний True positive – TP=2292	Хибнонегативний False Negative – FN=8 помилка 2-го роду
На вході підроблений підпис (загальна кількість підроблених підписів N=2300)	Хибнопозитивний False positive – FP=171 помилка 1-го роду	Вірнонегативний True Negative – TN=2129

Влучність.

$$\text{Precision(SF)} = \frac{TP}{TP + FP} \times 100\% = \frac{2292}{2292 + 171} \times 100\% = 93,1\%$$

Повнота (Чутливість).

$$\text{Recall(SF)} = \frac{TP}{TP + FN} \times 100\% = \frac{2292}{2292 + 8} \times 100\% = 99,65\%$$

Оцінка F1 (F1 Score). Оцінка F1 – це середньозважене значення достовірності та повноти. Отже, ця оцінка враховує як хибнопозитивні, так і хибнонегативні результати ідентифікації.

$$\text{F1 Score(SF)} = 2 * \frac{\text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}} = 2 * \frac{93,1 * 99,65}{93,1 + 99,65} = 96,26\%$$

Ми розрахували 4 основні показники якості систем ідентифікації при розпізнаванні майстерно підроблених підписів: достовірність 96,1%, влучність 93,1%, повнота 99,65%, оцінка F1 96,26%.

Для доведення досягнення мети дослідження потрібно порівняти ці показники якості із показниками аналогічних систем ДП. Таке порівняння наведено у табл. 4.4.

Таблиця 4.4 – Порівняння показників якості відомих систем ДП із запропонованою системою на основі спайкінгової нейронної мережі

	Джере- ло (рік)	Набір даних при тестуванні	Використовувані динамічні ознаки	Вид класифікато- ра	Оцінка достовірності
1	2	3	4	5	6
1.	[68] 2007	SVC 2004 dataset	Базисні функції, геометрична нормалізація, розширені функції, похідні по часу, нормалізація сигналів	Приховані моделі Маркова Hidden Markov Models (HMM)	6.9% EER для майстерно підроблених підписів (екв. Достовірність 93,1%) та 3.02% EER для випадкових підроблених підписів
2.	[62] 2011	Малий набір даних із 27 користувачів	Теорія графів	Норми графа	Достовірність 94.25%
3.	[67] 2013	SVC 2004 dataset	Вейвлет перетворення Wavelet transform	Нейронна мережа	3.5% EER (еквівалентна достовірність 96,5 %)
4.	[23] 2015	2 набори із БД ATVS, набір I містить 25 підписів на особу. Набір II містить 46 підписів на особу	9 глобальних параметрів	Нейромережа прямого поширення	Достовірність для набору I 98% Достовірність для набору II 89%
5.	[63] 2018	БД містить 10 користувачів і для кожного є 10 справжніх підписів та 10 підроблених підписів	координата пера $X(t)$ та $Y(t)$, тиск пера на планшет; кут нахилу пера до площини планшета; азимут руху пера .	DTW algorithm was used to calculate warping distance.	Достовірність визначення підробних підписів 90.4%.
6.	[61] 2018	1) містить 240 підписів від 10 осіб 2) містить 768 підписів від 32 осіб	speed up robust features (SURF)	Машина опорних векторів – Support vector machine(SVM)	Достовірність для БД 1) 98.75% а Достовірність для БД 2) 97.7%
7.	Запропо- нована система [1]-[3]	МСУТ-330	$l(t)$ – відстань між сусідніми дискретними точками підпису, добуток координат пера $X(t) \times Y(t)$, тиск пера на планшет	Спайкінгова нейронна мережа	Достовірність 96.1% для майстерно підроблених підписів

EER – equal error rate

Із табл. 4.4 видно, що запропонована система (96,1%) однозначно краща за аналоги із 1-го (93,1%), 2-го (94,25%) та 5-го (90,4%) рядків табл. 4.4; трохи гірша аналогу із 3-го (96,5%) рядка. Що стосується 4-го

рядка, то для набору II (89%) – наша система краща, а для набору I (98%) начебто гірша, але в роботі [23] не сказано як отримані ці 98% - тільки для майстерно підроблених підписів, чи тільки для випадкових підробок чи одночасно і тих, і тих. Крім того, наша система і аналог [23] досліджувались на різних БД, тому порівняння може бути некоректним, якщо складність підписів у БД МСҮТ більша, ніж у ATVS. Так само, наша система, начебто, гірша за систему у 6 рядку табл. 4.4, але знов таки, в [61] не зазначено для якого виду підробних підписів проводилось дослідження достовірності, а також БД із [61] дуже мала (10+32 осіб), а маленькі БД підписів зазвичай мають гіршу якість і складність підписів, ніж великі. Тому потрібно порівнювати нашу систему із такою, що досліджувалась на цій самій БД і за тих же (або хоча б схожих) умов вибору тестових підписів.

Було знайдено роботу [30], в якій розглянуто декілька останніх розробок систем динамічної верифікації підписів на основі рекурентних нейронних мереж. Там порівнюються 3 підходи:

- 1) на основі Dynamic Time Warping (DTW) [106],
- 2) на основі Recurrent Neural Networks (RNN) [107],
- 3) на основі Time-Aligned Recurrent Neural Networks (TA-RNN) [30].

Вони використовують для оцінювання якості бази даних DeepSignDB [30], куди БД МСҮТ [51] входить як складова. Хоч це системи не ідентифікації, а верифікації, все-одно їх можна порівнювати, провівши аналогію між показниками якості систем верифікації та ідентифікації підписів.

Аналогію між показниками якості систем верифікації та ідентифікації підписів приймемо відповідно до формули (1.5) таку: будемо вважати, що EER для систем верифікації аналогічно (100% – Ассурасу), оскільки і EER, і Ассурасу враховують такі показники як FP та FN. Оскільки для розробленої системи Ассурасу=96,1%, то можна вважати, що EER=3,9%. Із табл. 4.5 видно, що найкраще значення серед відомих систем має TARNN – 4,3%.

Показники якості відомих систем [30] та запропонованої системи ДПІ [3] наведено у табл. 4.5 та табл. 4.6.

Таблиця 4.5 – Порівняння якості (EER) відомих систем верифікації підписів із запропонованою системою при тестуванні на майстерно підроблених підписах

	Майстерно підроблені підписи (Skilled Forgeries)						
	1 тренувальний підпис			4 тренувальних підписи			15 тренувальних підписів
	DTW	RNN	TARNN	DTW	RNN	TARNN	Запропонована система
MCYT	9,1	10,5	4,4	7,2	10,1	4,3	3,9
BiosecurID	8.1	3.9	1.9	6.5	3.4	1.3	
Biosecure DS2	14.2	8.0	4.2	12.1	7.4	3.0	
eBS DS1 w1	15.3	11.4	5.4	9.3	9.0	4.3	
eBS DS1 w2	12.0	8.2	4.0	11.4	7.1	2.9	
eBS DS1 w3	14.5	14.3	5.4	12.1	11.4	4.8	
eBS DS1 w4	14.6	13.2	5.8	11.4	12.1	5.2	
eBS DS1 w5	14.9	18.9	10.6	12.9	14.0	8.0	
eBS DS2 w2	9.6	3.9	3.7	8.3	2.9	2.8	
DeepSignDB	11,2	8,5	4,2	9,3	7,9	3,3	

Таблиця 4.6 – Порівняння якості (EER) відомих систем верифікації підписів із запропонованою системою при тестуванні на випадкових підробках

	Випадково підроблені підписи (Random Forgeries)				
	1 тренувальний підпис		4 тренувальних підписи		15 тренувальних підписів
	DTW	TARNN	DTW	TARNN	Запропонована система
MCYT	1,2	1,1	0,6	0,2	0,17
BiosecurID	1.0	0.6	0.6	0.1	
Biosecure DS2	2.5	1.9	1.6	1.1	
eBS DS1 w1	3.2	2.5	0.7	0.1	
eBS DS1 w2	1.3	1.7	0.7	1.4	
eBS DS1 w3	0.9	1.6	0.3	0.4	
eBS DS1 w4	1.1	1.4	0.7	0.9	
eBS DS1 w5	2.7	4.1	2.1	1.4	
eBS DS2 w2	2.7	2.2	0.7	0.9	
DeepSignDB	1,8	1,5	1,1	0,6	

Із табл. 4.5 видно, що 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) достовірність, ніж система TARNN, а у відносних одиницях це $(0.4/4.3)*100\%=9\%$. Що стосується тестуванні на випадкових підробках, то із табл. 4.6 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) достовірність, ніж система TARNN, а у відносних одиницях це $(0.03/0.17)*100\%=15\%$.. Загалом, у відносних показниках, запропонована система за достовірністю краща за референсу на 9% при тестуванні на майстерних підробках і на 15% при тестуванні на випадкових підробках.

Таким чином, мета роботи досягнута – достовірність ідентифікації підписів підвищена.

4.4 Перспективи подальших досліджень

Подальші дослідження можна умовно розділити на такі 2 загальні напрямки:

- 1) дослідження у частині аналізу та синтезу ефективних динамічних параметрів підпису та їх попередньої обробки,
- 2) дослідження у частині пошуку нових та удосконалення відомих методів та засобів класифікації часових рядів, якими є динамічні параметри підпису.

У ході дослідження виявилось, що великий вплив на результат ідентифікації має вдалий вибір сукупності динамічних параметрів підпису, які подаються на класифікатор. Потрібно продовжити дослідження інформативності та варіабельності різних динамічних параметрів підпису у таких напрямках:

- шукати більш інформативні динамічні параметри підпису,

- запропонувавши для цього адекватну метрику інформативності,
- шукати динамічні параметри підпису, які мають малу внутрішньоперсональну варіабельність, запропонувавши для цього адекватну метрику внутрішньоперсональної варіабельності,
- шукати динамічні параметри підпису, які мають велику міжперсональну варіабельність, запропонувавши для цього адекватну метрику міжперсональної варіабельності.

Також залишається актуальним запитання: а скільки оптимально потрібно обирати динамічних параметрів і які саме, щоб досягти максимальної достовірності динамічної ідентифікації підписів при мінімумі витрат? З одного боку, чим більше параметрів взяти, тим точніше має бути робота системи. Але, з іншого боку, обробка великої кількості параметрів вимагає більших обчислювальних ресурсів і більше часу на прийняття рішення. Також не зрозуміло чи виправдано обирати велику кількість параметрів, адже всі вони не є незалежними, оскільки обчислюються по чотирьох первинних параметрах ($x(t)$, $y(t)$, $p(t)$ та $\chi(t)$).

Тому задачею подальших досліджень лишається дослідження ступіню впливу окремих динамічних параметрів підпису на загальну достовірність процесу ідентифікації підпису та обґрунтування оптимальних наборів динамічних параметрів підпису.

У ході проведених досліджень було помічено, що динамічні параметри підпису є більш стабільними на окремих своїх ділянках (інтервалах часу) і менш стабільними на інших. Тому логічно виникає ідея виділити такі ділянки при аналізі різних реалізацій підпису користувача і потім використовувати тільки їх, а не весь підпис при ідентифікації. Таку можливість дає запропонована в роботі [108] метрика для знаходження подібності часових рядів, яка носить назву «Найдовші загальні підпоследовності» (Longest Common Sub-Sequences – LCSS).

У частині пошуку нових та удосконалення відомих методів та засобів класифікації часових рядів, потрібно приділити більше уваги методам, які не

потребують перетворення динамічних параметрів у статичні вектори або дескриптори, тому що при цьому втрачається корисна інформація. Такими методами є методи з використанням рекурентних та спайкінгових нейронних мереж. Тому, зокрема, потрібно вдосконалювати структуру та методи навчання спайкінгових нейронних мереж [4], [109], [110].

4.5 Висновки до четвертого розділу

Загалом, у цьому розділі було відображено результати комп'ютерного моделювання та оцінки достовірності запропонованого методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі.

1. Було описано програмну реалізацію методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі на мові Python у середовищі розробки Visual Studio Code з використанням бібліотек TensorFlow та Keras.

2. Було розглянуто методику оцінки достовірності методів динамічної ідентифікації підпису, що складається з таких етапів: вибір референсної бази даних підписів (було обрано БД DeepSignDB), аналіз показників якості систем ідентифікації підписів, розробка протоколу проведення експериментальних досліджень,

3. Було проведено експериментальні дослідження достовірності методу динамічної ідентифікації підпису на основі спайкінгової нейронної мережі. При тестуванні тільки майстерно підробленими підписами розроблена система має достовірність 96,1%, влучність 93,1%, повноту 99,65%, оцінку F1 96,26%. Загалом, у відносних показниках, запропонована система за достовірністю краща за референсну на 9% при тестуванні на майстерних підробках і на 15% при тестуванні на випадкових підробках.

4. Визначено перспективи подальших досліджень, які полягають як у аналізі та синтезі ефективних динамічних параметрів підпису та їх попередньої обробки, так і у пошуку нових та удосконаленні відомих методів та засобів класифікації часових рядів, якими є динамічні параметри підпису.

Основні наукові результати, викладені в розділі, опубліковано в роботах [1] – [6], [8].

ЗАГАЛЬНІ ВИСНОВКИ

У результаті проведених досліджень було запропоновано метод динамічної ідентифікації підпису на основі спайкінгової нейронної мережі, розроблено структуру та метод навчання спайкінгової нейронної мережі, обґрунтовано вибір динамічних параметрів, стійких до варіабельності підпису, досліджено стійкість динамічних параметрів підпису до внутрішньоперсональної варіабельності та чутливість динамічних параметрів підпису до міжперсональної варіабельності, проведено комп'ютерне моделювання та оцінювання достовірності запропонованого методу на основі експериментальних досліджень його програмної реалізації, сформульовано перспективи подальших досліджень.

До важливих наукових результатів, отриманих у роботі, можна віднести:

1) Вперше запропоновано метод динамічної ідентифікації підписів, у якому завдяки використанню спайкінгової нейронної мережі відсутнє перетворення динамічних параметрів підпису у вектор статичних ознак, що дозволило збільшити достовірність та швидкодію ідентифікації підпису.

2) Удосконалено структурну організацію спайкінгової нейронної мережі для використання у задачі ідентифікації підпису за рахунок введення по два вихідних нейрона на кожен еталонний підпис, що дозволило навчати нейронну мережу не тільки на справжніх підписах, а і на майстерно підроблених і тим самим збільшило достовірність ідентифікації підпису.

3) Запропоновано набір із 3 динамічних параметрів підпису, які є інваріантними до масштабу, зсуву та повороту підпису відносно планшету, що дозволило збільшити достовірність ідентифікації підпису.

4) Досліджено внутрішньоперсональну та міжперсональну варіабельність динамічних параметрів підпису, що дозволило зробити висновок про кращу робастність запропонованого набору динамічних параметрів підпису до внутрішньоперсональної варіабельності та їх кращу

чутливість до міжперсональної варіабельності підпису, що в підсумку покращує їх представимість та роздільність і тим самим збільшує достовірність процесу ідентифікації підпису.

Практична цінність викладених у дисертації досліджень полягає в тому, що:

1) розроблено структурно-функціональну схему спайкінгової нейронної мережі для використання у задачі ідентифікації підпису, яка містить по два вихідних нейрона на кожен еталонний підпис;

2) кількісно оцінено робастність запропонованих динамічних параметрів підпису до внутрішньоперсональної варіабельності підпису та чутливість запропонованих динамічних параметрів підпису до міжперсональної варіабельності підпису;

3) розроблено програмні засоби динамічної ідентифікації підпису.

4) отримано результати комп'ютерного моделювання динамічної ідентифікації підпису;

5) отримано результати експериментальних досліджень програмних засобів динамічної ідентифікації підпису, визначено числові значення достовірності їх роботи та порівняно із кращими відомими методами динамічної ідентифікації підпису.

Сукупність викладених у дисертації результатів дозволяє розв'язати важливу наукову задачу вдосконалення методів та засобів динамічної ідентифікації підпису, яка полягає у збільшенні достовірності систем динамічної ідентифікації підпису. Загалом, у відносних показниках, запропонована система за достовірністю краща за референсну на 9% при тестуванні на майстерних підробках і на 15% при тестуванні на випадкових підробках.

Результати роботи можна використовувати в подальших дослідженнях для побудови високодостовірних систем динамічної ідентифікації підпису,

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] В. В. Куцман, та О. К. Колесницький, «Верифікація та розпізнавання підпису як багатопараметричного процесу на основі спайкінгової нейронної мережі», *Інформаційні технології та комп'ютерна інженерія*, том 50, № 1, с. 36–44, 2021.
- [2] В. В. Куцман, О. К. Колесницький, та І. К. Денисов, «Дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису у процесі їх ідентифікації», *Опτικο-електронні інформаційно-енергетичні технології*, том. 40, № 2, с. 15-20, 2020.
- [3] V. Kutsman, and O. Kolesnytskyj, «Dynamic handwritten signature identification using spiking neural network», *Informatyka, Automatyka, Pomiarы w Gospodarce i Ochronie Środowiska – IAPGOS (Informatics, Control, Measurement in Economy and Environmental Protection)*, Vol 11, No 3, pp. 34-39, 2021.
- [4] O. Kolesnytskyj, V. Kutsman, K. Skorupski, and M. Arshidinova, «Neurocomputer architecture based on spiking neural network and its optoelectronic implementation», *Proc. SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments*, vol. 11176, pp. 1117609, 2019. doi: 10.1117/12.2536607.
- [5] О. К. Колесницький, та В. В. Куцман, «Розпізнавання багатоканальних сигналів за допомогою спайкінгових нейронних мереж», на *Одинадцятій міжнародній науково-практичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018»*, Вінниця, 2018, с. 212-213.
- [6] О. К. Колесницький, та В. В. Куцман, «Архітектурні принципи побудови спайкінгових нейрокомп'ютерів та варіанти їх апаратної реалізації», на *XII Міжнародній науковопрактичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2020»*, Вінниця, 2020, с. 105-106.

- [Електронний ресурс]. Доступно: <https://conferences.vntu.edu.ua/index.php/allvntu/index/pages/view/zbirn2020>.
- [7] В. В. Куцман, А. О. Переродов, та О. К. Колесницький, «Класифікація банківських текстів на основі згорткової нейронної мережі», на *XXIV Міжнародному молодіжному форумі «Радіoeлектроніка та молодь в XXI столітті»*, Харків, 2020, с.189-190.
- [8] В. В. Куцман, та О. К. Колесницький, «Динамічна ідентифікація підпису на основі спайкінгової нейронної мережі», в Матеріалах конференції «Сучасні проблеми інфокомунікацій, радіoeлектроніки та наносистем», Вінниця, 2021. [Електронний ресурс]. Доступно: <https://conferences.vntu.edu.ua/index.php/spirn/spirn2021/paper/view/13851>.
- [9] N. Al-Banhawy, H. Mohsen, and N. Ghali, «Signature identification and verification systems: a comparative study on the online and offline techniques», *Future Computing and Informatics Journal*, Vol. 5, Iss. 1, Article 3, 2020.
- [10] А. Е. Сулавко, С. С. Жумажанова, и Г. А. Фофанов, «Перспективные нейросетевые алгоритмы распознавания динамических биометрических образов в пространстве взаимозависимых признаков», *ОМГТУ*, №4, 2018. Доступно: <https://cyberleninka.ru/article/n/perspektivnye-neyrosetevye-algoritmy-raspoznavaniya-dinamicheskikh-biometricheskikh-obrazov-v-prostranstve-vzaimozavisimyh-priznakov> (дата обращения: 15.09.2021).
- [11] П. С. Ложников, «Разработка метода идентификации личности по динамике написания слов», автореф. дис. на соискание уч. степени канд. техн. наук, Сибирская гос. Автомобильно-дорожная академия, Омск, 2004.
- [12] A. Rehman, S. Naz, and M. Razzak, «Writer identification using machine learning approaches: a comprehensive review», *Multimedia Tools and Applications*, pp 1–43, 2018.

- [13] K. Bibi, S. Naz, and A. Rehman, «Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities». *Multimedia Tools and Applications*, 2019. doi:10.1007/s11042-019-08022-0.
- [14] I. El-Henawy, M. 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.
- [15] M. Diaz, M. Ferrer, D. Impedovo, M. Malik, G. Pirlo, and R. Plamondon, «A Perspective Analysis of Handwritten Signature Technology», *ACM Comput. Surv.*, Vol. 51, No. 6, Article 117, January 2019.
- [16] Т. Ю. Дорошенко, и Е. Ю. Костюченко, «Система аутентификации на основе динамики рукописной подписи», *Доклады ТУСУР*, 2014, № 2(32), с. 219-223.
- [17] B. Yanikoglu, and A. Kholmatov. «Online Signature Verification Using Fourier Descriptors». *Journal on Advances in Signal Processing*, 2009. 10.1155/2009/260516.
- [18] M. Fahmy, «Online handwritten signature verification system based on DWT features extraction and neural network classification», *Ain Shams Engineering Journal*, 1, pp. 59–70, 2010.
- [19] 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.
- [20] Т. Б. Мартинюк, Л. М. Куперштейн, та М. Д. Кренцін, «Особливості процесу класифікації об'єктів на базі дискримінантних функцій», *Математичні машини і системи*. № 3, С. 81-87, 2021. URL: http://www.immsp.kiev.ua/publications/articles/2021/2021_3/03_21_Martyniuk.pdf.
- [21] T. Fotak, M. Bača, and P. Koruga, «Handwritten Signature Identification Using Basic Concepts Of Graph Theory». *Wseas Transactions On Signal Processing*, 7, 117-129, 2011.

- [22] H. Lu and W. Wang, «On-Line Signature Verification Based on Dynamic Bayesian Network», *ICNC 2006*, Part I, LNCS 4221, PP. 507-510, 2006.
- [23] P. Babita, «Online Signature Recognition Using Neural Network». *Journal of Electrical & Electronics*, 4(3), 1, 2015.
- [24] A. Yarovyi, R. Ilchenko, I. Arseniuk, Y. Shemet, A. Kotyra, and S. Smailova, «An intelligent system of neural networking recognition of multicolor spot images of laser beam profile», *SPIE Proceedings Volume 10808, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018; 108081B*, 2018, <https://doi.org/10.1117/12.2501691>, [Online]. Available: <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10808/108081B/An-intelligent-system-of-neural-networking-recognition-of-multicolor-spot/10.1117/12.2501691.full>.
- [25] Т. Б. Мартинюк, М. Г. Тарновський, та Я. В. Запетрук «Структурні особливості нейромережевого класифікатора», *Вісник ВПІ*, вип. 1 (148), с. 46–52, Лют 2020. [Online]. Available: <https://visnyk.vntu.edu.ua/index.php/visnyk/article/view/2461>.
- [26] В. Ф. Бардаченко, О. К. Колесницький, та С. А. Василецький, «Перспективи застосування імпульсних нейронних мереж з таймерним представленням інформації для розпізнавання динамічних образів», *Управляючі Системи і Машини*, №6, С. 73-82, 2003.
- [27] І. Цмоць, В. Рабик, та Ю. Лукашук, «Розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі», *Information systems and networks*, Issue 9, с. 84-95, 2021. <https://doi.org/10.23939/sisn2021.09.084> [Online]. Available: http://science.lpnu.ua/sites/default/files/journal-paper/2021/jun/23827/0210544infmarket-01-07-86-97_0.pdf.
- [28] V. Lytvynenko, W. Wojcik, A. Fefelov, I. Lurie, N. Savina, M. Voronenko, O. Boskin, and S. Smailova, «Hybrid Methods of GMDH-Neural Networks Synthesis and Training for Solving Problems of Time Series Forecasting»,

- Advances in Intelligent Systems and Computing*, vol. 1020, pp. 513-531, 2020. DOI: 10.1007/978-3-030-26474-1_36 [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-030-26474-1_36 https://doi.org/10.1007/978-3-030-26474-1_36 Print ISBN 978-3-030-26473-4, Online ISBN 978-3-030-26474-1.
- [29] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, «Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics». *IEEE Access*, 6, 5128–5138, 2018. doi:10.1109/access.2018.2793966.
- [30] 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.
- [31] J. Fierrez, J. Galbally, M. Ortega-Garcia, F. Freire, D. Alonso-Fernandez, D. Ramos, J. Toledano, J. Gonzalez-Rodriguez, J. Siguenza et al., «BiosecurID: A Multimodal Biometric Database», *Pattern Analysis and Applications*, vol. 13, no. 2, pp. 235–246, 2010.
- [32] N. Houmani, and S. Garcia-Salicetti, «On hunting animals of the biometric menagerie for online signature». *PLoS ONE*, 11, 4, 2016.
- [33] N. Houmani, S. Garcia-Salicetti, and B. Dorizzi, «A Novel Personal Entropy Measure confronted with Online Signature Verification Systems' Performance». *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, 2008. [Электронный ресурс]. Режим доступа: <https://doi.org/10.1109/BTAS.2008.4699362>.
- [34] 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.
- [35] F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally, and J. Ortega-Garcia, «Robustness of signature verification systems to imitators with

- increasing skills». In *10th Int. Conf. on Document Analysis and Recognition. IEEE*, 728–732, 2009.
- [36] S. Nalwa, «Automatic On-Line Signature Verification», *Proceedings of the IEEE*, Vol. 85, NO. 2, 1997.
- [37] V. Iranmanesh, S. Ahmad, W. Adnan, S. Yussof, O. Arigbabu, and F. 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, 2014.
- [38] S. Farimani, and M. Jahan, «An HMM for online signature verification based on velocity and hand movement directions», In *6th Iranian Joint Congress on Fuzzy and Intelligent Systems*, pp. 205–209, 2018.
- [39] 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, pp. 1088–1100, 2010.
- [40] M. Mailah, and B. Lim, «Biometric Signature Verification Using Pen Position, Time, Velocity and Pressure Parameters». *Jurnal Teknologi*, vol. 48, no. 1, Jan. 2012, p. 35, doi:10.11113/jt.v48.218.
- [41] О. В. Руденко, та Є. В. Бодянський *Штучні нейронні мережі: Навчальний посібник*. Харків : ТОВ «Компанія СМІТ», 2006. — 404 с.
- [42] A. Chadha, N. Satam, and V. Wali «Biometric signature processing & recognition using radial basis function network», pp 1–9. arXiv:1311.1694, 2013.
- [43] A. McCabe, J. Trevathan, and W. Read, «Neural Network-based Handwritten Signature Verification», *Journal of Computers*, vol. 3, No. 8, August 2008.
- [44] W. Yang, L. Jin, and M. 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.

- [45] M. 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, pp. 126-132, 2014.
- [46] S. Otte, M. Liwicki, and D. Krechel, «Investigating Long Short-Term Memory Networks for Various Pattern Recognition Problems», *Machine Learning and Data Mining in Pattern Recognition*, Springer, 2014
- [47] W. Maass, «Networks of spiking neurons: the third generation of neural network models», *Neural Networks*, №10, P. 1659-1671, 1997. – ISSN 0893-6080.
- [48] О. К. Колесницкий, Самра Муавия Хассан Хамо «Метод распознавания многомерных временных рядов при помощи импульсных нейронных сетей», *Інформаційні технології та комп'ютерна інженерія*, №2(6), С. 86-93, 2006.
- [49] M. Fard, 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, pp. 233-235, 2008, doi: 10.1109/ISI.2008.4565065.
- [50] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia, «An off-line signature verification system based on fusion of local and global information», In *International Workshop on Biometric Authentication*. Springer, 295–306, 2004.
- [51] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q. Moro, «MCYT baseline corpus: A bimodal biometric database». *IEE Proceedings-Vision, Image and Signal Processing* 150, 6, 395–401, 2003.

- [52] A. Kholmatov, and B. Yanikoglu, «SUSIG: An on-line signature database, associated protocols and benchmark results», *Pattern Analysis and Applications* 12, 3, 227–236, 2008.
- [53] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, «Benchmarking Desktop and Mobile Handwriting across COTS Devices: the e-BioSign Biometric Database», *PLoS ONE*, vol. 12, no. 5, pp. 1–17, 2017.
- [54] N. Houmani, A. Mayoue, S. Garcia-Salicetti, B. Dorizzi, M. Khalil, M. Moustafa, H. Abbas, D. Muramatsu, B. Yanikoglu, A. Kholmatov, M. Martinez-Diaz, J. Fierrez, J. Ortega-Garcia, J. Roure Alcobé, J. Fabregas, M. FaundezZanuy, J. Pascual-Gaspar, V. Cardeñoso-Payo, and C. Vivaracho-Pascual, «BioSecure signature evaluation campaign (BSEC2009): Evaluating online signature algorithms depending on the quality of signatures». *Pattern Recognition* 45, 3, 993–1003, 2012.
- [55] D.-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, «SVC2004: First International signature verification competition», In *Biometric Authentication*. LNCS, Vol. 3072. Springer, 16–22, 2004.
- [56] J. Galbally, M. Diaz-Cabrera, M. Ferrer, M. Gomez-Barrero, A. Morales, and J. Fierrez, «On-line signature recognition through the combination of real dynamic data and synthetically generated static data», *Pattern Recognition* 48, 9, 2921–2934, 2015.
- [57] S. Li, *Encyclopedia of Biometrics*, 1st ed. Springer Publishing Company, Incorporated, 2009.
- [58] A. Jain, A. Ross, and S. Prabhakar, «An introduction to biometric recognition», *IEEE Trans. Cir. and Sys. for Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
- [59] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger, «Performance evaluation of behavioral biometric systems», In *Behavioral*

Biometrics for Human Identification: Intelligent Applications, pp. 57-74, IGI Global, 2010.

- [60] M. El-Abed, & C. Charrier, *Evaluation of biometric systems*, book chapter. Intech open science, 2012.
- [61] I. Hamadly, A. Khaleel, A. Munim, H. Hassan, and H. Mohamed, «Online Signature Recognition And Verification Using (SURF) Algorithm With SVM Kernels», *Journal Of Al-Azhar University Engineering Sector*, 13(49), 1332-1344, 2018.
- [62] I. Pavlidis, N. Papanikolopoulos, and R. Mavuduru, «Signature Identification Through The Use Of Deformable Structures», *Signal Processing*, 71(2), 187-201, 1998.
- [63] B. Patil, and P. Patil, «An Efficient DTW Algorithm For Online Signature Verification», In *2018 International Conference On Advances In Communication And Computing Technology (ICACCT)*, Pp. 1-5. IEEE, February 2018.
- [64] Z. Chen, X. Xia, and F. Luan, «Automatic Online Signature Verification Based On Dynamic Function Features», In *2016 7th Ieee International Conference On Software Engineering And Service Science (ICSESS)*, Pp. 964-968, IEEE, August 2016.
- [65] M. Tahir, and M. Akram, «Online Signature Verification Using Hybrid Features», In *2015 Second International Conference On Information Security And Cyber Forensics (Infosec)*, Pp. 11-16, IEEE, November 2015.
- [66] M. Saffar, M. Fayyaz, M. Sabokrou, and M. Fathy, «Online Signature Verification Using Deep Representation: A New Descriptor», Arxiv Preprint Arxiv:1806.09986, 2018.
- [67] M. Nilchiyan, and R. Yusof, «Improved Wavelet-Based Online Signature Verification Scheme Considering Pen Scenario Information», In *2013 1st International Conference On Artificial Intelligence, Modelling And Simulation*, Pp. 8-13, IEEE, December 2013.

- [68] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, «HMM-Based On-Line Signature Verification: Feature Extraction And Signature Modeling», *Pattern Recognition Letters*, 28(16), 2325-2334, 2007.
- [69] О. К. Колесницький *Методи і засоби розпізнавання сигналів мультисенсорів газів на основі імпульсних нейронних мереж: монографія*, Вінниця : ВНТУ, 2011. – 120 с. ISBN 978-966-641-407-9.
- [70] O. Kolesnytskyj, I. Bokotsey, and S. Yaremchuk «Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices», *Optical Memory & Neural Networks (Information Optics)*, Vol.19, №2, P.154–165, 2010. – ISSN 1060-992X.
- [71] В. Ф. Бардаченко, О. К. Колесницький, та С. А. Василецький, *Таймерні нейронні елементи та структури. Монографія*, Вінниця : УНІВЕРСУМ-Вінниця, 2005, 126 с. – ISSN 966-641-109-1.
- [72] W. Gerstner and W. Kistler, *Spiking Neuron Models: Single Neurons, Populations, Plasticity* (Cambridge University Press, 2002). [Електронний ресурс]. — Режим доступу: <http://diwww.epfl.ch/~gerstner/BUCH.html>. — ISSN 0-521-89079-9.
- [73] О. К. Колесницький, І. В. Бокоцей «Математична модель імпульсного нейроелемента на біспін-приладі», *Вісник Хмельницького національного університету*, №5, С.141-149, 2011.
- [74] O. Kolesnytskyj, and S. Vasyletskyy, «BISPIN - based optoelectronic neuron element», In *Selected Papers from the International Conference on Optoelectronic Information Technologies*, Editors: S. Svechnikov, V. Kojemiako, S. Kostyukevych, Proceedings of SPIE, Vol. 4425, pp. 417 – 424, 2001.
- [75] W. Maass, and H. Markram «Temporal integration in recurrent microcircuits», in edit. M. A. Arbib *The Handbook of Brain Theory and Neural Networks*, Cambridge : MIT Press, P. 1159—1163, 2003. – ISBN 0-262-01197-2.

- [76] T. Natschläger, W. Maass, and H. Markram, «The "Liquid Computer": A Novel Strategy for Real-Time Computing on Time Series», *Special Issue on Foundations of Information Processing of TELEMATIK*, 8(1):39-43, 2002.
- [77] W. Maass, T. Natschläger, H. Markram, «Real-time computing without stable states: A new framework for neural computation based on perturbations», *Neural Computation*, Vol. 14(11), P. 2531—2560, 2002.
- [78] W. Maass, T. Natschläger, and H. Markram, «Computer models and analysis tools for neural microcircuits», in edit. R. Kötter : *Neuroscience Databases. A Practical Guide. Chapter 9*, Boston : Kluwer Academic Publishers, — P. 123—138, 2003.
- [79] W. Maass, T. Natschläger, and H. Markram, «Fading memory and kernel properties of generic cortical microcircuit models», *Journal of Physiology*. Vol. 98(4—6), P. 315—330, 2004.
- [80] S. Bohte, J. Kok, H. La Poutre, «Errorbackpropagation in temporally encoded networks of spiking neurons», *Neurocomputing*, volume 48, no. 1—4, P. 17–37, 2002.
- [81] S. Moore, «Back-Propagation in Spiking Neural Networks», M.Sc. thesis, University of Bath, [On-line resource], Access mode: <http://www.simonchristianmoore.co.uk>.
- [82] P. Tiño and A. Mills, «Learning beyond finite memory in recurrent networks of spiking neurons», *Advances in Natural Computation – ICNC 2005 - Lecture Notes in Computer Science*, Berlin: Springer, P. 666–675, 2005.
- [83] J.Xin, and M. Embrechts, «Supervised Learning with Spiking Neuron Networks», *Proc. IEEE Int. Joint Conf. Neural Networks*, IJCNN'01, Washington D.C., P. 1772– 1777, 2005.
- [84] T. Strain, T. McGinnity, L. Maguire, and H. Sayers «An STDP training algorithm for a spiking neural network with dynamic threshold neurons», *Int J Neural Syst.*, Dec;20(6), P. 463-480, 2010. ISSN 0129-0657.

- [85] Колесницький О. К, Арсенюк І. Р., та Месюра В. І. *Чисельні методи : навчальний посібник*, Вінниця : ВНТУ, 2017. – 130 с.
- [86] В. Подоба, «У яких випадках мова програмування Python є правильним вибором?», [Електронний ресурс], Режим доступу: <http://www.vitaliypodoba.com/2015/06/python-application>.
- [87] Н. Прохоренок, *Python 3 и PyQt. Разработка приложений*. Санкт-Петербург. «БХВ-Петербург», 2012. – 24с
- [88] Python. Documentation [Електронний ресурс]: – Режим доступу: <https://docs.python.org/3>.
- [89] A. Martelli, A. Martelli Ravenscroft, and S. Holden, *Python in a Nutshell: A Desktop Quick Reference*, 3rd Edition, O'Reilly Media; May 16, 2017. ISBN-10 : 144939292X, ISBN-13\ : 978-1449392925.
- [90] KERAS: Simple. Flexible. Powerful. [Електронний ресурс]. Режим доступу: <https://keras.io>.
- [91] Комплексная платформа машинного обучения с открытым исходным кодом [Електронний ресурс]. Режим доступу: <https://www.tensorflow.org>.
- [92] Visual Studio Code [Електронний ресурс]. Режим доступу: <https://code.visualstudio.com>.
- [93] V. Blankers, C. Heuvel, K. Franke, and L. Vuurpijl, «ICDAR 2009 signature verification competition», In *10th Int. Conf. on Document Analysis and Recognition (ICDAR'09)*. 1403–1407, 2009.
- [94] M. Liwicki, M. Imran Malik, C. van den Heuvel, X. Chen, C. Berger, R. Stoel, M. Blumenstein, and B. Found, «Signature verification competition for online and offline skilled forgeries (SigComp2011)», In *11th Int. Conf. on Document Analysis and Recognition (ICDAR'11)*, 1480–1484, 2011.
- [95] M. Malik, S. Ahmed, A. Marcelli, U. Pal, M. Blumenstein, L. Alewijns, and M. Liwicki, «ICDAR2015 competition on signature verification and writer identification for on- and off-line skilled forgeries (SigWlcomp2015)», In

- 13th Int. Conf. on Document Analysis and Recognition (ICDAR'15)*, 1186–1190, 2015.
- [96] «SVC-ongoing on-line signature verification competition», *Based on ICDAR SVC 2021 Competition*. [Електронний ресурс]. Режим доступу: <https://sites.google.com/view/SVC2021/home>.
- [97] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, «Presentation Attacks in Signature Biometrics: Types and Introduction to Attack Detection», S. Marcel, M.S. Nixon, J. Fierrez and N. Evans (Eds.), *Handbook of Biometric Anti-Spoofing (2nd Edition)*, Springer, 2019.
- [98] J. Ortega-Garcia, J. Fierrez, and et al., «The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB)», *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097–1111, 2010.
- [99] DeepSignDB [Електронний ресурс]. Режим доступу: <https://github.com/BiDAIab/DeepSignDB>.
- [100] Visual Studio. Лучшие в своем классе средства для разработчиков [Електронний ресурс] – Режим доступу: <https://visualstudio.microsoft.com/en/>.
- [101] Matplotlib: Visualization with Python [Електронний ресурс]. – Режим доступу: <https://matplotlib.org/>.
- [102] М. О. Сперкач, Д. Ю. Юзьвак, «Розв'язання задачі класифікації текстів методами обробки природньої мови та машинного навчання», *Науковий огляд*, 4 (57), 2019.
- [103] S. Stehman, «Selecting and interpreting measures of thematic classification accuracy», *Remote Sensing of Environment*, 62 (1), 77–89, 1997. Bibcode:1997RSEnv..62...77S. doi:10.1016/S0034-4257(97)00083-7.
- [104] D. Powers, «Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation», *Journal of Machine Learning Technologies*, 2 (1), 37–63, 2011.

- [105] M. Salehan, and A. Negahban, «Social Networking on Smartphones: When Mobile Phones Become Addictive», *Computers in Human Behavior*, vol. 29, no. 6, pp. 2632–2639, 2013.
- [106] R. Tolosana, R. Vera-Rodriguez, J. Fierrez and J. Ortega-Garcia, “Do You Need More Data? The DeepSignDB On-Line Handwritten Signature Biometric Database,” in *Proc. International Conference on Document Analysis and Recognition (ICDAR)*, 2019.
- [107] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, «BioTouchPass2: Touchscreen Password Biometrics Using TimeAligned Recurrent Neural Networks», *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2616–2628, 2020.
- [108] M. Vlachos, G. Kollios, and D. Gunopulos, «Discovering similar multidimensional trajectories», *Proceedings 18th International Conference on Data Engineering*, pp. 673-684, 2002, doi: 10.1109/ICDE.2002.994784.
- [109] О. К. Колесницький, «Аналітичний огляд апаратних реалізацій спайкових нейронних мереж», *Математичні машини і системи*, №1, С.3-19, 2015. ISSN 1028-9763 [Електронний ресурс]. Режим доступу - http://www.immsp.kiev.ua/publications/articles/2015/2015_1/01_2015_Kolesnytskyi.pdf.
- [110] V. Kozemiako ; O. Kolesnytskyj ; T. Lischenko ; W. Wojcik and A. Sulemenov, «Optoelectronic spiking neural network», *Proc. SPIE 8698, Optical Fibers and Their Applications 2012*, 86980M, January 11, 2013. doi:10.1117/12.2019340; <http://dx.doi.org/10.1117/12.2019340>

ДОДАТКИ

Додаток А Акти впровадження результатів дисертації

«ЗАТВЕРДЖУЮ»

Директор ТОВ «ДЖЕМІКЛ»



Хазін М.Б.

«30» серпня 2021 р.

АКТ

впровадження результатів дисертаційної роботи
«Динамічна ідентифікація підпису на основі спайкінгової
нейронної мережі»

Куцмана Владислава Вікторовича

Комісія ТОВ «ДЖЕМІКЛ» у складі: Хазін М. Б., Скорченко С. А., Петрусевич О. В. розглянула запропонований у даній науковій роботі метод динамічної ідентифікації підписів, у якому завдяки використанню спайкінгової нейронної мережі відсутнє перетворення динамічних параметрів підпису у вектор статичних ознак, що дозволило збільшити достовірність та швидкодію ідентифікації підпису. Цей метод може бути застосовано для розпізнавання підписів клієнтів в динамічному режимі, тобто під час процесу підписування на планшеті. Це дозволить підвищити достовірність визначення майстерно підроблених підписів.

На основі вищезазначеного комісія вважає за доцільне використання результатів досліджень, отриманих у роботі Куцмана В. В. у діяльності нашої компанії при розробці систем авторизації та ідентифікації за підписом особи, а також при розробці систем доступу за написанням парольного слова.

Директор ТОВ «ДЖЕМІКЛ»:

Хазін М.Б.

Провідний спеціаліст:

Скорченко С.А.

Провідний спеціаліст:

Петрусевич О.В.



ЗАТВЕРДЖУЮ

Перший проректор з наукової роботи
та міжнародного співробітництва ВНТУ
Д.Тн., проф.

В.В.Габко

“29” серпня 2021 р.

АКТ

Впровадження результатів дисертаційної роботи
*«Динамічна ідентифікація підпису на основі спайкінгової
нейронної мережі»*

Куцмана Владислава Вікторовича
у навчальний процес

Комісія у складі декана факультету інформаційних технологій та комп'ютерної інженерії, кандидата педагогічних наук, доцента Кирилашук С.А., заступника декана факультету інформаційних технологій та комп'ютерної інженерії з навчально-методичної роботи, кандидата технічних наук, доцента Войцеховської О.В., заступника декана факультету інформаційних технологій та комп'ютерної інженерії з навчально-виховної роботи кандидата педагогічних наук, доцента Прозор О.П. склали цей акт про те, що для вивчення дисциплін «Сучасні парадигми штучних нейронних мереж» та «Нейрокомп'ютерні технології штучного інтелекту», що викладаються студентам бакалаврату, дисципліни «Нейромережеві методи штучного інтелекту», що викладається студентам магістратури, та дисципліни «Нейромережеві моделі та технології обчислювального інтелекту» підготовки докторів філософії спеціальності 122 «Комп'ютерні науки» впроваджено такі результати, розроблені Куцманом В.В.:

- метод динамічної ідентифікації підписів на основі спайкінгової нейронної мережі, що дозволяє збільшити достовірність та швидкодію ідентифікації підпису;
- структурну організацію спайкінгової нейронної мережі для використання у задачі ідентифікації підпису, яка має по два вихідних нейрона на кожен еталонний підпис, що дозволяє навчати нейронну мережу не тільки на справжніх підписах, а і на майстерно підроблених і тим самим збільшує достовірність ідентифікації підпису.;
- методику визначення внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису, що дозволяє оцінити робастність цих параметрів підпису до внутрішньоперсональної варіабельності та їх чутливість до міжперсональної варіабельності.

Декан ФІТКІ

С.А. Кирилашук

Заступник декана ФІТКІ

О.В.. Войцеховська

Заступник декана ФІТКІ

О.П. Прозор

Додаток Б**Фрагмент лістингу програми дослідження внутрішньоперсональної та міжперсональної варіабельності підписів**

```
#
# SignView -
#

import os
import math
import matplotlib.pyplot as plt

# ф-ция читает текущий каталог и выбирает имена файлов
соответствующих расширению fmt
def get_signatures_filenames(path='./', fmt='txt'):
    filenames = []
    if os.path.exists(path):
        #
        pos = 0
        if len(fmt) > 0:
            ext = '.' + fmt
            pos -= len(ext)
        else:
            ext = ""
        #
        filenames = [
            fn for fn in os.listdir(path)
            if (pos == 0) or (fn[pos:] == ext)
        ]

    return filenames
```

```

# функция чтения файла подписи
def read_signature_file(filename):
    with open(filename, "r") as f:
        #
        samplesnum = int(f.readline())
        #
        sign = {'fn': filename}
        #
        samples = {}
        #
        x = []
        y = []
        t = []
        azmt = []
        angl = []
        prss = []
        #
        for line in f:
            #
            sample = [int(val) for val in line.split(" ")]
            # sample[0] -> x, ...
            x.append(sample[0])
            y.append(sample[1])
            t.append(sample[2])
            azmt.append(sample[3])
            angl.append(sample[4])
            prss.append(sample[5])

        #
        samples['x'] = x

```

```

    samples['y'] = y
    samples['t'] = t
    samples['azmt'] = azmt
    samples['angl'] = angl
    samples['prss'] = prss

    sign['smpl'] = samples

    sign['min_x'] = min(x)
    sign['max_x'] = max(x)
    sign['min_y'] = min(y)
    sign['max_y'] = max(y)
    sign['min_p'] = min(prss)
    sign['max_p'] = max(prss)

    #if samplesnum != len(samples):
    #    print("Invalid samples number: declared:", samplesnum, "; real: ",
len(samples))

    return sign

# ф-ция вычисления угла
def get_angle(xy):
    dx = xy[1][0] - xy[0][0]
    dy = xy[1][1] - xy[0][1]
    if dx != 0:
        angle = math.atan(dy / dx)
    elif dy > 0:
        angle = math.pi / 2
    elif dy < 0:
        angle = - math.pi / 2

```

```

else:
    angle = 0
return angle

# функция вычисления разницы углов
def get_delta_angle(xy):
    return get_angle(xy[1:3]) - get_angle(xy[0:2])

#
def cm2inch(figsize):
    return [v / 2.54 for v in figsize]

#####
#
# Main
#

# получим список имен файлов подписей
filenames = get_signatures_filenames()

# загрузим подписи из файлов
signatures = [read_signature_file(fn) for fn in filenames]

#####
#
# Signatures
#

# нарисуем подписи на одном рисунке

# размер рисунка в см

```



```

FIGSIZE = cm2inch([10, 20])
plt.figure(figsize = FIGSIZE)
plt.title('1. f = y(x); signatures')

for sign in signatures:
    #
    samples = sign['smpl']
    #
    x = samples['x']
    y = samples['y']
    #
    plt.plot(x, y)

plt.grid(True)
plt.savefig('signatures.png')

#
FIGSIZE = cm2inch([18, 9])

# нарисуем подписи на отдельных рисунках
for sign in signatures:
    #
    plt.figure(figsize = FIGSIZE)
    plt.title('1. f = y(x); signature: {}'.format(sign['fn']))
    #
    samples = sign['smpl']
    #
    min_x = sign['min_x']
    min_y = sign['min_y']
    dim_x = sign['max_x'] - sign['min_x']
    dim_y = sign['max_y'] - sign['min_y']

```

```

#
x = [(val - min_x) / dim_x for val in samples['x']]
y = [(val - min_y) / dim_y for val in samples['y']]
#
plt.plot(x, y)

plt.grid(True)
plt.savefig('signature({}).png'.format(sign['fn']))

#####

#
# Raw data
#

# нарисуем совмещенный график зависимости коорд. X от времени
fig = plt.figure(figsize = FIGSIZE)

plt.title('2. f = X(t); raw')

for sign in signatures:
    #
    samples = sign['smpl']
    #
    min_x = sign['min_x']
    x = [val - min_x for val in samples['x']]
    #
    plt.plot(samples['t'], x)

plt.grid(True)
plt.savefig('X(t).png')

```

```
# нарисуем совмещенный график зависимости коорд. Y от времени
fig = plt.figure(figsize = FIGSIZE)
```

```
plt.title('3. f = Y(t); raw')
```

```
for sign in signatures:
```

```
    #
```

```
    samples = sign['smpl']
```

```
    #
```

```
    min_y = sign['min_y']
```

```
    y = [val - min_y for val in samples['y']]
```

```
    #
```

```
    plt.plot(samples['t'], y)
```

```
plt.grid(True)
```

```
plt.savefig('Y(t).png')
```

```
#plt.show()
```

```
#os._exit(0)
```

```
#####
```

```
#
```

```
# Normalized data
```

```
#
```

```
# нарисуем совмещенный график нормализованной зависимости коорд.
```

X от времени

```
fig = plt.figure(figsize = FIGSIZE)
```

```
plt.title('5. f = X(t); normalized')
```

```
for sign in signatures:
```

```
    #
    samples = sign['smpl']
    #
    min_x = sign['min_x']
    dim_x = sign['max_x'] - sign['min_x']
    dim_t = len(samples['t'])
    #
    t = [val / dim_t for val in range(dim_t)]
    x = [(val - min_x) / dim_x for val in samples['x']]
    #
    plt.plot(t, x)
```

```
plt.grid(True)
```

```
plt.savefig('X(t)-norm.png')
```

```
# нарисуем совмещенный график нормализованной зависимости коорд.
```

Y от времени

```
fig = plt.figure(figsize = FIGSIZE)
```

```
plt.title('6. f = Y(t); normalized')
```

```
for sign in signatures:
```

```
    #
    samples = sign['smpl']
    #
    min_y = sign['min_y']
    dim_y = sign['max_y'] - sign['min_y']
    dim_t = len(samples['t'])
    #
    t = [val / dim_t for val in range(dim_t)]
```

```

y = [(val - min_y) / dim_y for val in samples['y']]
#
plt.plot(t, y)

plt.grid(True)
plt.savefig('Y(t)-norm.png')

# нарисуем совмещенный график нормализованной зависимости
давления от времени
fig = plt.figure(figsize = FIGSIZE)

plt.title('6. f = P(t); normalized')

for sign in signatures:
    #
    samples = sign['smpl']
    #
    min_p = sign['min_p']
    dim_p = sign['max_p'] - sign['min_p']
    dim_t = len(samples['t'])
    #
    t = [val / dim_t for val in range(dim_t)]
    p = [(val - min_p) / dim_p for val in samples['prss']]
    #
    plt.plot(t, p)

plt.grid(True)
plt.savefig('P(t)-norm.png')

# нарисуем совмещенный график нормализованной зависимости L от
времени
fig = plt.figure(figsize = FIGSIZE)

```

```

plt.title('7. f = l(t); normalized')

for sign in signatures:
    #
    samples = sign['smpl']
    #
    dim_t = len(samples['t'])
    min_x = sign['min_x']
    min_y = sign['min_y']
    #
    x = [(val - min_x) for val in samples['x']]
    y = [(val - min_y) for val in samples['y']]
    #
    dim_t -= 1
    t = [val / dim_t for val in range(dim_t)]
    #
    l = [math.sqrt((x[i + 1] - x[i]) ** 2 + (y[i + 1] - y[i]) ** 2) for i in
range(dim_t)]

    min_l = min(l)
    max_l = max(l)
    dim_l = max_l - min_l
    #
    l_norm = [val / dim_l for val in l]

    plt.plot(t, l_norm)

plt.grid(True)
plt.savefig('L(t)-norm.png')

```

нарисуем совмещенный график нормализованной зависимости
разности углов от времени

```
fig = plt.figure(figsize = FIGSIZE)
```

```
plt.title('8.  $f = \Delta\alpha(t)$ ')

```

```
for sign in signatures:
```

```
    #
```

```
    samples = sign['smpl']
```

```
    #
```

```
    dim_t = len(samples['t'])
```

```
    min_x = sign['min_x']
```

```
    min_y = sign['min_y']
```

```
    dim_x = sign['max_x'] - sign['min_x']
```

```
    dim_y = sign['max_y'] - sign['min_y']
```

```
    #
```

```
    x = [(val - min_x) / dim_x for val in samples['x']]
```

```
    y = [(val - min_y) / dim_y for val in samples['y']]
```

```
    xy = [val for val in zip(x, y)]
```

```
    #
```

```
    dim_t -= 2
```

```
    t = [val / dim_t for val in range(dim_t)]
```

```
    #
```

```
    da = [get_delta_angle(xy[i:i+3]) for i in range(dim_t)]
```

```
    #
```

```
    plt.plot(t, da)
```

```
plt.grid(True)
```

```
plt.savefig('deltaAngle(t)-norm.png')
```

```
plt.show()
```

Додаток В

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

- [1] В. В. Куцман, та О. К. Колесницький, «Верифікація та розпізнавання підпису як багатопараметричного процесу на основі спайкінгової нейронної мережі», Інформаційні технології та комп'ютерна інженерія, том 50, № 1, с. 36–44, 2021.
- [2] В. В. Куцман, О. К. Колесницький, та І. К. Денисов, «Дослідження внутрішньоперсональної та міжперсональної варіабельності динамічних параметрів підпису у процесі їх ідентифікації», *Опτικο-електронні інформаційно-енергетичні технології*, том. 40, № 2, с. 15–20, 2020.
- [3] V. Kutsman, and O. Kolesnytskyj, «Dynamic handwritten signature identification using spiking neural network», *Informatyka, Automatyka, Pomiarы w Gospodarce i Ochronie Środowiska – IAPGOS (Informatics, Control, Measurement in Economy and Environmental Protection)*, Vol 11, No 3, pp. 34-39, 2021.
- [4] O. Kolesnytskyj, V. Kutsman, K. Skorupski, and M. Arshidinova, «Neurocomputer architecture based on spiking neural network and its optoelectronic implementation», *Proc. SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments*, vol. 11176, pp. 1117609, 2019. doi: 10.1117/12.2536607.
- [5] О. К. Колесницький, та В. В. Куцман, «Розпізнавання багатоканальних сигналів за допомогою спайкінгових нейронних мереж», на *Одинадцятій міжнародній науково-практичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018»*, Вінниця, 2018, с. 212-213.
- [6] О. К. Колесницький, та В. В. Куцман, «Архітектурні принципи побудови спайкінгових нейрокомп'ютерів та варіанти їх апаратної

реалізації», на *XII Міжнародній науковопрактичній конференції «ІНТЕРНЕТ-ОСВІТА-НАУКА-2020»*, Вінниця, 2020, с. 105-106.

Доступно: <https://conferences.vntu.edu.ua/index.php/allvntu/index/pages/view/zbirn2020>.

- [7] В. В. Куцман, А. О. Переродов, та О. К. Колесницький, «Класифікація банківських текстів на основі згорткової нейронної мережі», на *XXIV Міжнародному молодіжному форумі «Радіoeлектроніка та молодь в XXI столітті»*, Харків, 2020, с.189-190.
- [8] В. В. Куцман, та О. К. Колесницький, «Динамічна ідентифікація підпису на основі спайкінгової нейронної мережі», в *Матеріалах конференції «Сучасні проблеми інфокомунікацій, радіoeлектроніки та наносистем»*, Вінниця, 2021. [Електронний ресурс]. Доступно: <https://conferences.vntu.edu.ua/index.php/spirn/spirn2021/paper/view/13851>.