Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Міністерство освіти і науки України

Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ГАВРИЛОВИЧ МАРІЯ ПАВЛІВНА

УДК 004.89

ДИСЕРТАЦІЯ

ВЕРИФІКАЦІЯ КОРИСТУВАЧА МЕТОДАМИ ГЛИБОКОГО НАВЧАННЯ НА ОСНОВІ ПОВЕДІНКОВИХ ТА БІОМЕТРИЧНИХ ХАРАКТЕРИСТИК

12 Інформаційні технології
122 Комп’ютерні науки
Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник Данилов Валерій Якович, д.т.н., професор.

Київ - 2024

АНОТАЦІЯ

Гаврилович М.П. Верифікація користувача методами глибокого навчання на основі поведінкових та біометричних характеристик. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 “Комп’ютерні науки”. – Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, 2024.

У дисертаційній роботі розглянуто питання побудови систем верифікації користувача на основі біометричних та поведінкових даних з допомогою нейронних мереж глибокого навчання. Потреба у надійних та високоефективних системах верифікації є надзвичайно актуальною у сфері безпеки, кібербезпеки, захисті персональних даних, медицини та ризик-менеджменті. Традиційні методи верифікації, такі як паролі, карти доступу чи пін-коди і т.п. несуть великі ризики в разі їх втрати або компрометації, тому є потреба у побудові більш стійких систем безпеки та автентифікації. Біометричні дані є унікальними для кожного індивідуума, тому на їх основі можливо побудувати набагато надійніші системи верифікації. Неперервні біометричні та поведінкові сигнали, наприклад покази давачів руху (покази акселерометра, магнетометра, гіроскопа і т.п.), дають змогу реалізувати системи неперервної та неявної автентифікації. Оскільки біометричні сигнали є дуже складними по своїй природі, тому для розробки високоточної системи верифікації необхідна побудова нових потужних моделей, які мають високу предиктивну силу та можуть знаходити глибокі закономірності в даних з комплексною та глибокою структурою.

Метою дослідження є розробка та аналіз методів машинного навчання, зокрема нейронних мереж глибокого навчання, для верифікації користувача на основі біометричних та поведінкових характеристик.

У дисертації вперше отримані наступні нові наукові результати:

1. Розроблені **нові гібридні архітектури**, які базуються на стискуючих та варіаційних автокодувальниках з використанням трансформерів, для розв'язання задач верифікації на основі поведінкових та біометричних характеристик користувача, що дозволило досягти значного покращення критеріїв ефективності в порівнянні з існуючими методами.
2. На основі розроблених нових гібридних архітектур **створена система** підтримки прийняття рішень верифікації користувача.
3. Розроблено **новий підхід** для покращення точності систем біометричної верифікації, що базується на використанні величин фрактальних розмірностей.
4. Визначені та набули подальшого розвитку прикладні сценарії та компоненти системи верифікації на базі **уточненої практичної методології** побудови систем глибокого навчання на основі запропонованих архітектур.

Теоретичне значення отриманих результатів полягає у вдосконаленні та подальшому розвитку методології побудови систем верифікації на базі нейронних мереж глибокого навчання. Створені та побудовані гібридні нейронні мережі дозволяють суттєво підвищити ефективність роботи систем біометричної верифікації, за рахунок поєднання переваг компонентів різних архітектур в одній нейронній мережі. На основі нових розроблених архітектур нейронних мереж виявлено та кількісно оцінено вплив величин фрактальних розмірностей на метрики якості систем верифікації.

Практична цінність дисертаційної роботи:

1. розроблена оригінальна СППР неперервної біометричної верифікації користувача на основі нових гібридних архітектур нейронних мереж з використанням величин фрактальних розмірностей;
2. впроваджено в навчальний процес розроблені архітектури та уточнену методологію у вигляді відповідного силабусу, лекційного матеріалу та навчального посібника-практикума.

Запропонована нова гібридна архітектура, яка базується на стискуючих автокодувальниках з використанням трансформерів, показує час висновку швидший на 31% відсоток та нижче в середньому на 11% відсотків значення рівного рівня помилок для всі типів фізичних активностей та їх комбінацій.

Проведено аналіз впливу величин фрактальної розмірності Хігучі вхідних даних на ефективність системи верифікації на базі автокодувальників. Показано перевагу використання фрактальної розмірності даних на основні метрики якості, зокрема на рівний рівень помилок (в середньому на 13% відсотків нижче значення) та на значення площі під кривою (на 2.2% відсотків вищі показники) в порівнянні з системою верифікації без її врахування.

Запропоновано СППР неперервної біометричної верифікації користувача на основі розроблених нових гібридних архітектур та з урахуванням фрактальної розмірності даних. На вхід розробленої системи надходять дані з різноманітних давачів (акселерометри, гіроскопи, магнетометри, тощо), які характеризують відповідні біометричні чи поведінкові показники особи. Під час етапу ініціалізації відбувається збір початкової необхідної кількості даних для тренування нових гібридних архітектур. На основі вдосконаленої практичної методології налаштування параметрів системи верифікації, перед тренуванням підбираються: відповідні значення розмірності вхідних даних в залежності від характеристик давачів; гіперпараметри архітектури нейронної мережі глибокого навчання; розраховується фрактальна розмірність даних кожного типу давача. В залежності від кількості та розмірності даних відбувається тренування моделей різних відповідних архітектур на окремих компонентах (скалярних, векторних) та на їх комбінаціях. Після тренування для кожної моделі отримуються значення відповідних критеріїв (час висновку, значення порогу верифікації). Відповідно до доступності сигналів для висновку системи верифікації вибирається модель, яка охоплює найбільший контекст та не перевищує установленого допустимого значення по часу висновку. Також, система має елемент моніторингу розподілу даних, який в залежності від їх зміни при необхідності ініціює дотренування моделей.

Проведено порівняльний аналіз різних типів автокодувальників з класичними методами машинного навчання, як-от однокласові опорні машини векторів та ізоляційний ліс (Isolation Forest). Показано суттєву перевагу застосування автокодувальників над класичними методами машинного навчання, наприклад отримуємо на 7% вищу чутливість (recall) в порівнянні з ізоляційним лісом і на 75% вищу чутливість (recall) в порівнянні з однокласовими опорними машинами векторів.

Також проведено глибокий аналіз впливу різних компонентів векторного біометричного сигналу та кількісно оцінено їх вплив на ефективність системи верифікації користувача. Встановлено, що в залежності від типу фізичної активності різні компоненти сигналу давача по різному впливають на метрики якості системи. Також, кількісно оцінено вплив компонентів сигналів давача в різних комбінаціях та доведено ефективність комбінацій компонентів векторного сигналу для досягнення вищої точності.

Ключові слова: нейронні мережі глибокого навчання, гібридні нейронні мережі, автокодувальники, автокодувальник на базі трансформера, рекурентний автокодувальник, біометрична верифікація, фрактальна розмірність.

SUMMARY

Havrylovych M. User verification with deep learning neural networks based on biometric and behavioral patterns – Qualifying scientific work, the manuscript.

Thesis for a PhD degree in specialty 122 "Computer Science". – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2024.

The dissertation discusses the issues of building user verification systems based on biometric and behavioral data using deep learning neural networks. The need for reliable and highly efficient verification systems is extremely relevant in the fields of security, cybersecurity, personal data protection, medicine, and risk management. Traditional verification methods, such as passwords, access cards, PIN codes, etc., carry significant risks in case of their loss or compromise, hence there is a need for building more robust security and authentication systems. Biometric data are unique to everyone, making it possible to build much more reliable verification systems. Continuous biometric and behavioral signals, such as motion sensor readings (accelerometer, magnetometer, gyroscope readings, etc.), allow for the implementation of continuous and implicit authentication systems. Since biometric signals are very complex by nature, developing a high-precision verification system requires building new powerful models that have high predictive power and can find deep patterns in data with a complex and deep structure.

The goal of the research is to develop and analyze machine learning methods, particularly deep learning neural networks, for user verification based on biometric and behavioral characteristics.

In the dissertation, the following new scientific results were obtained for the first time:

1. New hybrid architectures based on compressive and variational autoencoders using transformers were developed to solve user verification

tasks based on behavioral and biometric characteristics, which allowed for significant improvement in efficiency criteria compared to existing methods.

2. Based on the developed new hybrid architectures, a user verification decision support system was created.
3. A new approach for improving the accuracy of biometric verification systems, based on the use of fractal dimension magnitudes, was developed.
4. Applied scenarios and components of the verification system based on a refined practical methodology for building deep learning systems based on the proposed architectures were identified and further developed.

The theoretical significance of the obtained results lies in the improvement and further development of the methodology for building verification systems based on deep learning neural networks. The created and constructed hybrid neural networks allow for a significant increase in the efficiency of biometric verification systems, due to the combination of advantages of components from different architectures in one neural network. Based on the new developed neural network architectures, the impact of fractal dimension magnitudes on the quality metrics of verification systems was discovered and quantitatively assessed.

The practical value of the dissertation work:

1. An original continuous biometric verification user support system based on new hybrid neural network architectures using fractal dimension magnitudes was developed;
2. The developed architectures and refined methodology were implemented in the educational process in the form of the corresponding syllabus, lecture materials, and a training manual-practicum.

The proposed new hybrid architecture, based on compressive autoencoders using transformers, shows a 31% faster inference time and on average 11% lower equal error rate values for all types of physical activities and their combinations.

An analysis of the impact of fractal dimension magnitudes on verification systems based on autoencoders was conducted. The positive impact of fractal

dimension on the main quality metrics, specifically an average of 13% lower equal error rate and 2.2% higher area under the curve value compared to the method without fractal dimension, was proven.

An automated system for continuous biometric user verification has been proposed, based on newly developed hybrid architectures and taking into account the fractal dimension of the data. The system receives input data from a variety of sensors (accelerometers, gyroscopes, magnetometers, etc.), which characterize the corresponding biometric or behavioral indicators of a person. During the initialization phase, an initial necessary amount of data is collected for training the new hybrid architectures. Based on an improved practical methodology for setting verification system parameters, appropriate values for the dimensions of input data are selected depending on the characteristics of the sensors before training; hyper-parameters of the deep learning neural network architecture are adjusted; and the fractal dimension of data for each type of sensor is calculated. Depending on the amount and dimensions of the data, models of various corresponding architectures are trained on individual components (scalar, vector) and their combinations. After training, each model yields values for the relevant criteria (inference time, verification threshold value). Depending on the availability of signals for inference, the system selects the model that covers the broadest context and does not exceed the established permissible value for inference time. Additionally, the system includes a data distribution monitoring element, which, depending on changes in the data, may initiate retraining of the models if necessary.

A comparative analysis of different types of autoencoders with classic machine learning methods, such as one-class support vector machines and isolation forest, was conducted. A significant advantage of autoencoders compared to classic machine learning methods was shown, for example, a 7% higher recall than with the isolation forest and almost 75% higher recall than with one-class support vector machines.

A deep analysis of the impact of various components of the biometric signal and their quantitative impact on the efficiency of the biometric verification system of

the user was conducted. Depending on the type of physical activity, different signal components of the sensor affect the quality metrics of the system differently. Also, the impact of signal components in combination with each other was quantitatively assessed. Overall, it was shown that individual components significantly vary in their impact on quality metrics and demonstrate the effectiveness of combining components to achieve higher accuracy.

Keywords: neural networks, autoencoder, hybrid neural networks, transformer-based autoencoder, recurrent autoencoder, biometric verification, fractal dimension.

List of main publications of the applicant:

1. Havrylovych M. P., Danylov V. Y. Research of autoencoder-based user biometric verification with motion patterns, System Research and Information Technologies, vol. 2022, no. 2, pp. 128–136, 2022, doi: 10.20535/SRIT.2308-8893.2022.2.10.

Здобувачкою проведено аналіз впливу різноманітних компонентів біометричного сигналу на систему верифікації на основі автокодувальників.

2. M. Havrylovych, V. Danylov, A. Gozhyj. Comparative analysis of using recurrent autoencoders for user biometric verification with wearable accelerometer, Proceedings of the 9th International Conference “Information Control Systems & Technologies”, CEUR Workshop Proceedings. - Sept. 2020. - vol. 2711. - pp. 358–370.

Здобувачкою проведено порівняльний аналіз різних типів нейронних мереж глибокого навчання, зокрема автокодувальників з класичними методами машинного навчання для задачі верифікації користувача на базі патернів руху.

3. M. Havrylovych and V. Danylov. Research on hybrid transformer-based autoencoders for user biometric verification. System research and information technologies, no. 3, pp. 42–53, Sep. 2023, doi: 10.20535/SRIT.2308-8893.2023.3.03.

Здобувачкою розроблено та запропоновано нові гібридні архітектури автокодувальників на базі трансформера для вирішення задачі верифікації.

4. Havrylovych, M. P., Kuznietsova N. V. Survival analysis methods for churn

prevention in telecommunications industry. ITS 2019. CEUR Workshop Proceedings. - 2020. - vol. 2577. - С. 47–58.

Здобувачкою представлено тези дослідження про застосування статистичних методів аналізу виживання для диференціації поведінки та характеристик користувачів і можливості передбачення суб'єкта з "несприятливою" поведінкою.

5. Гаврилович М., Данилов В. Дослідження впливу фрактальної розмірності Хігучі в задачі біометричної верифікації користувача, 2024, Вісник вінницького політехнічного інституту. - 2024 - №1. – С. 121-127.

Здобувачкою проведені дослідження про вплив фрактальної розмірності на ефективність роботи системи біометричної верифікації користувача на базі автокодувальників.

6. Havrylovych M., Kuznietsova N. Survival Analysis Methods For Churn Prevention in Telecommunications Industry. Інформаційні технології та безпека. Матеріали XIX Міжнародної науково-практичної конференції ІТБ-2019 (Київ, 28.11.2019), вип. 19. Київ: ООО «Інжиніринг», 2019. —С. 66-75.

Здобувачкою представлено тези дослідження про застосування статистичних методів аналізу виживання для диференціації поведінки та характеристик користувачів і можливості передбачення суб'єкта з "несприятливою" поведінкою.

7. M. Havrylovych, V. Danylov, A. Gozhyj. Comparative analysis of using recurrent autoencoders for user biometric verification with wearable accelerometer. «Інформаційні управляючі системи і технології»: матеріали IX Міжнародної науково-практичної конференції (24–26 верес. 2020 р., м. Одеса) / відп. ред. В. В. Вичужанін; Одес. нац. політех. ун-т. — Одеса: Екологія, 2020. — С. 242-243.

Здобувачкою представлено тези дослідження порівняльного аналізу різних типів нейронних мереж глибокого навчання, зокрема автокодувальників з класичними методами машинного навчання для задачі верифікації користувача на базі патернів руху.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

LSTM – long-short term memory, довга короткочасна пам’ять.

AE – autoencoder, автокодувальник.

OC-SVM – one-class support vector machines, однокласові машини опорних векторів.

IF – isolation forest, ізоляційний ліс.

VAE – variational autoencoder, варіаційний автокодувальник.

CAE – contractive autoencoder, контрактивний автокодувальник.

EER – equal error rate, рівний рівень помилок.

FAR – false acceptance rate.

FRR – false rejection rate.

MAE – mean absolute error, середня абсолютна похибка.

AUC – area under curve, площа під кривою.

ROC – receiver operator characteristic.

KPI – key performance indicator, ключовий показник ефективності.

RNN – recurrent neural network, рекурентна нейронна мережа.

IMU – inertial measurement unit, інерційний вимірювальний пристрій

ЗМІСТ

ВСТУП

Актуальність дослідження.

Тема дослідження вибрана на основі актуальності проблеми біометричної верифікації користувача в сучасних системах безпеки. Сучасний розвиток технологій надає можливість використання глибинного та машинного навчання для підвищення ефективності біометричних систем верифікації. Аналіз сучасних досліджень у цій галузі засвідчує потребу в дослідженні методів та алгоритмів, які забезпечують надійну біометричну верифікацію.

У дисертаційній роботі розглянуто питання побудови систем верифікації користувача на основі біометричних та поведінкових даних з допомогою нейронних мереж глибокого навчання. З огляду на важливість створення надійних та ефективних механізмів ідентифікації у сферах безпеки, кіберзахисту, охорони приватності, медичної сфери та управління ризиками, ця потреба стає все більш актуальною. З огляду на обмеження традиційних методів ідентифікації, таких як паролі, доступові картки або PIN-коди, які можуть бути легко втрачені або скомпрометовані, виникає необхідність у розробці більш надійних методів аутентифікації. Використання біометричних ідентифікаторів, що є унікальними для кожної особи, дозволяє створювати значно більш безпечні системи ідентифікації. Застосування безперервних біометричних і поведінкових даних, таких як дані з давачів руху дозволяє реалізувати методи неперервної та невидимої аутентифікації. Враховуючи складність біометричних сигналів, розробка високоефективної системи ідентифікації вимагає створення нових потужних моделей, здатних виявляти складні закономірності у відповідних типах даних.

На даний час існуючі системи верифікації все ще потребують вирішення задач підвищення точності та надійності. Тому постає задача в виявленні глибоких властивостей в даних (зокрема фрактальних), та в подальшому розвитку методології створення нових систем верифікації.

Мета та завдання дослідження: Розробка та аналіз методів машинного навчання, зокрема нейронних мереж глибокого навчання, для верифікації користувача на основі біометричних та поведінкових характеристик.

Предмет дослідження є моделі та методи штучного інтелекту для виявлення аномалій.

Об'єктом дослідження є поведінкові та біометричні характеристики отримані шляхом вимірювання давачів градієнтного типу (як от акселерометичного типу, гіроскопа, магнетометра).

Методи дослідження: В даному дослідженні для аналізу біометричних даних використовувалися такі методи: аналіз часових рядів, аналіз фрактальної розмірності, нейронні мережі глибокого навчання, зокрема: рекурентні нейронні мережі, автокодувальники різних типів, трансформери.

Для імплементації експериментів та використання методів дослідження використовувалася мова програмування Python в середовищі PyCharm.

Наукова новизна:

У дисертації вперше одержані такі нові наукові результати:

1. Розроблені нові гібридні архітектури, які базуються на стискуючих та варіаційних автокодувальниках з використанням трансформерів, для розв'язання задач верифікації на основі поведінкових та біометричних характеристик користувача, що дозволило досягти значного покращення критеріїв ефективності в порівнянні з існуючими методами.
2. На основі розроблених нових гібридних архітектур створена система підтримки прийняття рішень верифікації користувача.
3. Розроблено новий підхід для покращення точності систем біометричної верифікації, що базується на використанні величин фрактальних розмірностей даних.
4. Визначені та набули подальшого розвитку прикладні сценарії та компоненти системи верифікації на базі уточненої практичної

методології побудови систем глибокого навчання на основі запропонованих архітектур.

Особистий внесок здобувача:

Теоретичне значення отриманих результатів полягає у вдосконаленні та подальшому розвитку методології побудови систем верифікації на базі нейронних мереж глибокого навчання. Створені та побудовані гібридні нейронні мережі дозволяють суттєво підвищити ефективність роботи систем біометричної верифікації, за рахунок поєднання переваг компонентів різних архітектур в одній нейронній мережі. На основі нових розроблених архітектур нейронних мереж виявлено та кількісно оцінено вплив величин фрактальних розмірностей на метрики якості систем верифікації.

Практична цінність дисертаційної роботи:

1. розроблена оригінальна СППР біометричної верифікації користувача на основі нових гібридних архітектур нейронних мереж з використанням величин фрактальних розмірностей;
2. впроваджено в навчальний процес розроблені архітектури та уточнену методологію у вигляді відповідного силабусу, лекційного матеріалу та навчального посібника-практикума.

Апробація матеріалів дисертації: Матеріали дисертації були представлені на міжнародних конференціях та опубліковані у наукових журналах, а також впроваджені в навчальний процес в якості силабусу, лекційного матеріалу та навчального посібника-практикуму.

Практичне значення отриманих результатів: Розроблені методи та алгоритми можуть бути використані для підвищення ефективності систем безпеки в різних галузях.

Структура та обсяг дисертації: Дисертація складається з вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 126 сторінок: з них 100 сторінок основного тексту, та на 26 сторінках список використаних джерел з 141 найменувань та додатків, 28 таблиць, 14 рисунків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ КОРИСТУВАЧА

1.1 Проблематика та актуальність біометричної верифікації

Біометрична верифікація має багатий історичний контекст, який охоплює століття. Використання біометричних характеристик для цілей ідентифікації можна простежити до стародавніх цивілізацій [1]. Наприклад, царі Вавилона використовували відбитки рук для ідентифікації та аутентифікації. З часом були досліджені та використані різні біометричні модальності, включаючи відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока, розпізнавання голосу тощо.

В останні роки системи біометричної верифікації набули значного поширення та стали поширеними в різних сферах, як от контроль доступів, системи ідентифікації та платіжні методи [2]. Широке впровадження смартфонів та інших мобільних пристроїв сприяло збільшенню використання систем біометричної перевірки [3]. Досягнення комп’ютерних наук та технологій відіграли вирішальну роль у розвитку та вдосконаленні систем біометричної перевірки. Технології комп’ютерного зору, алгоритми машинного навчання та моделі глибокого навчання підвищили точність і ефективність біометричного розпізнавання [3] [4]. Детальніше ця тема буде розглянута в підрозділі 1.3.

Такі системи часто покладаються на зберігання конфіденційних біометричних даних, таких як відбитки пальців або сканування райдужної оболонки ока, у хмарі. Однак ця практика викликає занепокоєння щодо безпеки та конфіденційності даних [3]. Потенційна вразливість зберігання біометричних даних у хмарі призвела до дослідження безпечних систем біометричного розпізнавання, що зберігають конфіденційність [3] [5].

Одним із підходів до збереження конфіденційності біометричної автентифікації є використання біометричних криптосистем. Біометричні

криптосистеми спрямовані на перетворення біометричних даних у безпечну та незворотну форму, яка не може бути використана для реконструкції оригінального біометричного шаблону [6]. Це гарантує, що навіть якщо зашифровані біометричні дані будуть скомпрометовані, вони не можуть бути використані для ідентифікації або видавання себе за людей. Скасовувана біометрія (cancellable biometrics) є однією з таких технік, яка передбачає перетворення біометричного шаблону за допомогою процесу рандомізації [7]. Ця конструкція зберігає конфіденційність, оскільки обчислювально важко відновити оригінальну біометричну версію з перетвореної версії.

Гомоморфне шифрування є ще одним методом, який був досліджений для збереження конфіденційності біометричної автентифікації [8]. Гомоморфне шифрування дозволяє виконувати обчислення на зашифрованих даних без їх розшифровки, тим самим зберігаючи конфіденційність біометричної інформації [3][9]. Цей підхід забезпечує безпечну обробку та зіставлення біометричних даних, не наражаючи необроблені дані на потенційні загрози.

На додаток до методів, заснованих на шифруванні, існують інші підходи до збереження конфіденційності біометричної автентифікації. Наприклад, були запропоновані протоколи, що зберігають конфіденційність, засновані на ідеальних решітках та криптографічних алгоритмах, як обмін ключами при навчання з помилками (ring-LWE) [10]. Ці протоколи використовують гомоморфні схеми шифрування для захисту конфіденційності біометричних даних під час автентифікації. Крім того, для підвищення конфіденційності та безпеки були запропоновані системи багатофакторної автентифікації, які поєднують біометричні характеристики з іншими факторами, такими як випадкові числа користувача.

Безпека та конфіденційність систем біометричної аутентифікації також були вивчені в контексті конкретних застосувань. Наприклад, було досліджено більш безпечну аутентифікацію ходьби на смартфонах [11]. Це дослідження зосереджене на збереженні безпеки та конфіденційності користувачів систем біометричної аутентифікації на мобільних пристроях. Аналогічним чином,

проблеми конфіденційності в схемах віддаленої аутентифікації на основі біометричних даних були формалізовані та вивчені в [12]. Була запропонована нова модель безпеки для вирішення проблем конфіденційності, пов'язаних з віддаленою автентифікацією за допомогою біометрії.

Загалом, біометрична автентифікація, що зберігає конфіденційність, є активною областю досліджень, спрямованих на вирішення проблем конфіденційності, пов'язаних із використанням біометричних даних. Різні методи, такі як біометричні криптосистеми, гомоморфне шифрування та багатофакторна автентифікація, були запропоновані для захисту конфіденційності людей, забезпечуючи при цьому безпечну та надійну автентифікацію. Ці методи забезпечують баланс між необхідністю точної ідентифікації та захистом приватного життя.

Ефективність і продуктивність є вирішальними факторами при розробці та впровадженні систем біометричної аутентифікації. Оптимізація цих систем спрямована на підвищення швидкості, точності та загальної продуктивності біометричної автентифікації, забезпечуючи при цьому надійну та безпечну ідентифікацію. Кілька досліджень були зосереджені на підвищенні ефективності та продуктивності біометричної автентифікації за допомогою різних методів і підходів.

Одним з підходів до оптимізації ефективності та продуктивності є використання протоколів мультисерверної аутентифікації. В [13] автори запропонували безпечний протокол мультисерверної автентифікації на основі біометрії з використанням смарт-карт. Цей протокол підвищує ефективність, вимагаючи використання багатьох факторів, таких як смарт-картки, паролі та біометрія, для автентифікації. Поєднуючи кілька факторів, механізм аутентифікації стає більш ефективним і надійним.

Ще одним методом оптимізації ефективності є використання спільного розрідженого представлення для мультимодального біометричного розпізнавання. В [14] представили спільний підхід до розрідженого представлення для надійного мультимодального розпізнавання біометричних

даних. Ця техніка поєднує кілька біометричних методів, таких як райдужна оболонка ока, дерматогліфіка та обличчя, для підвищення точності та ефективності розпізнавання. Оптимізаційна задача розв'язується за допомогою ефективного методу альтернативного спрямування.

Ефективність і продуктивність також можуть бути підвищені за рахунок розробки надійних і безпечних схем автентифікації. Трифакторна схема віддаленої автентифікації користувачів з узгодженням ключів для мультимедійних систем розглянута в [15]. Ця схема покращує безпеку, зберігаючи при цьому ефективність, вирішуючи проблеми безпеки попередніх схем. Забезпечуючи надійність і безпеку, процес автентифікації стає більш ефективним і точним.

Використання безпечних та ефективних методів шифрування є ще одним шляхом оптимізації систем біометричної аутентифікації. В [16] запропонована система SEMBA (Secure Multi-Biometric Authentication), яка використовує переваги продуктивності мультимодального біометричного розпізнавання для підвищення ефективності. Ця система працює на зашифрованих даних за моделлю безпеки зловмисників, забезпечуючи конфіденційність і безпеку при збереженні ефективності.

Ефективність також може бути підвищена за рахунок використання енергоефективних алгоритмів і методів. В [17] представили енергоефективний підхід до віддаленої аутентифікації користувачів на основі біометрії для мобільних мультимедійних застосунків IoT. Такий підхід підвищує енергоефективність, зберігаючи при цьому точність розпізнавання обличчя. Завдяки оптимізації енергоспоживання процесу автентифікації підвищується загальна ефективність і продуктивність системи.

Крім того, використання ефективних алгоритмів і методів оптимізації може сприяти оптимізації систем біометричної аутентифікації. Автори в [18] запропонували ефективну мультимодальну систему біометричної аутентифікації на базі Android з розпізнаванням обличчя і голосу. Ця система ефективно обробляє та аналізує біометричні дані з урахуванням апаратних

обмежень продуктивності смарт-терміналів. Відкидаючи зайву довідкову інформацію та зменшуючи непотрібні дані, система підвищує ефективність.

Підсумовуючи, оптимізація ефективності та продуктивності систем біометричної аутентифікації є критично важливою областю досліджень. Для підвищення ефективності та продуктивності біометричної автентифікації були запропоновані різні методи, такі як протоколи багатосерверної автентифікації, спільне розріджене представлення, надійні схеми автентифікації, безпечне шифрування, енергоефективні алгоритми та ефективні методи оптимізації. Ці підходи спрямовані на підвищення швидкості, точності та загальної продуктивності, забезпечуючи при цьому надійну та безпечну ідентифікацію.

Загалом, поточний стан біометричної верифікації характеризується прогресом у технологіях, заходах безпеки та дослідженням нових способів і методів. Постійні дослідження та розробки спрямовані на вирішення проблем, пов’язаних із безпекою даних, конфіденційністю та продуктивністю системи, з метою підвищення точності, ефективності та надійності систем біометричної перевірки.

1.2 Огляд існуючих методів біометричної верифікації

1.2.1 Визначення та класифікація біометричних технологій

Біометричні технології відносяться до методів та систем, які використовуються для ідентифікації та аутентифікації осіб на основі їхніх унікальних фізіологічних або поведінкових характеристик [19]. Ці характеристики можна умовно класифікувати на дві категорії: фізіологічні та поведінкові біометрики. Приклади можливих методів та описів біометричної верифікації наведені в таблиці 1.1 нижче.

Таблиця 1.1. Загальний опис різних типів біометричних верифікаційних систем

Тип Верифікації	Підтип	Методи та Описи
Біометрична Верифікація	Фізіологічна	- *Відбитки Пальців*: Унікальні візерунки на кінчиках пальців. - *Розпізнавання Обличчя*: Аналіз рис обличчя. - *Сканування Сітківки*: Візерунки кровоносних судин. - *Сканування Радужки*: Особливості радужки ока. - *Розпізнавання Голосу*: Характеристики голосу.
	Поведінкова	- *Динаміка Набору Тексту*: Швидкість та ритм введення тексту. - *Аналіз Ходи*: Особливості ходи. - *Жести*: Специфічні жести, наприклад, на сенсорному екрані.

Фізіологічні біометричні системи базуються на фізичних та анатомічних атрибутах особи. Приклади фізіологічних біометричних систем включають розпізнавання відбитків пальців, розпізнавання обличчя, сканування райдужки та профілювання ДНК [20]. Ці системи захоплюють та аналізують унікальні особливості, такі як відбитки пальців, особливості обличчя, шаблони райдужки та генетичну інформацію для встановлення ідентичності особи.

З іншого боку, поведінкові біометричні системи фокусуються на шаблонах та поведінці осіб. Ці біометричні системи аналізують та вимірюють характеристики, такі як динаміка натискання клавіш, розпізнавання ходьби та динаміка дотику [19]. Поведінкові біометрики особливо корисні в системах неперервної аутентифікації, де користувачі можуть бути перевірені неявно та безперервно на основі їхніх поведінкових атрибутів [19].

Варто зазначити, що в залежності від контексту задачі деякі методи, як-от верифікація голосом, може бути визначеною як фізіологічною так і поведінковою біометрією, адже можуть визначатися і унікальні фізіологічні особливості голосу так і манеру людини спілкуватися, промовляти звуки, тощо.

1.2.2 Фізіологічні біометричні системи

Біометрія відбитків пальців є однією з найбільш широко визнаних і використовуваних форм біометричної ідентифікації [21]. Унікальні візерунки та гребені на кінчиках пальців людини фіксуються та аналізуються, щоб встановити її ідентичність. Системи розпізнавання відбитків пальців використовують складні алгоритми для зіставлення знятого відбитка пальця зі збереженими шаблонами, що забезпечує точну ідентифікацію [22]. Цей тип біометричних даних широко використовується в правоохоронних органах, контролях доступу та мобільних пристроях.

Розпізнавання райдужної оболонки ока є ще однією новою біометричною технологією, яка привернула значну увагу [23]. Райдужна оболонка, яка є забарвленою частиною ока, має складні та характерні візерунки, які можна використовувати для ідентифікації. Системи розпізнавання райдужної оболонки ока фіксують зображення райдужної оболонки з високою роздільною здатністю і витягують її унікальні особливості для порівняння [23]. Цей біометричний тип забезпечує високу точність і використовується в таких програмах, як безпека аеропортів і національні програми ідентифікації.

Розпізнавання облич — це біометричний тип, який використовує унікальні риси та характеристики обличчя людини для ідентифікації [24]. Системи розпізнавання облич аналізують орієнтири обличчя, такі як відстань між очима та форму носа, щоб створити унікальний шаблон для кожної людини [24]. Ця технологія широко використовується в спостереженні, контролі доступу та управлінні цифровою ідентифікацією.

Важливо відзначити, що кожен біометричний тип має свої переваги і обмеження. При виборі методу біометричної верифікації слід враховувати такі фактори, як точність, прийняття користувачів і вразливість до спуфінгових атак [25]. Крім того, прогрес у галузі штучного інтелекту та методів глибокого навчання призвів до розробки мультимодальних біометричних систем, які поєднують кілька біометричних типів для підвищення точності та безпеки [25].

1.2.3 Поведінкові біометричні системи

Поведінкові біометричні системи здобули значну увагу в останні роки, особливо в контексті автентифікації смартфонів. Сенсори та аксесуари смартфонів можуть використовуватися для отримання поведінкових атрибутів, таких як динаміка дотику, динаміка натискання клавіш та розпізнавання ходьби [19]. Ці атрибути можна використовувати для неявної та неперервної верифікації або ідентифікації користувачів на смартфонах, що призводить до розробки активних або безперервних систем аутентифікації [19].

Перевірка підпису — це поведінковий біометричний тип, який фокусується на унікальних характеристиках підпису особи [26]. Системи розпізнавання сигнатур аналізують різні параметри, такі як динаміка ходу та тиск, щоб автентифікувати особу підписувача [26]. Цей тип біометричних даних зазвичай використовується в банківських системах, адміністративних програмах і юридичних документах.

Поведінкові методи та методи верифікації на основі руху почали застосовуватися для верифікації спікерів чи біометричної верифікації користувача [27]; [28]; [29]. Ці методи використовують фізичний процес і поведінкову біометрію, пов'язану з конкретними видами діяльності, такими як рухи губ, верхньої частини тіла та більш комплексні і складні рухи людини. Аналізуючи часову кореляцію та поведінкові патерни в цих рухах, ці методи можуть ефективно перевіряти ідентичність індивідів.

У контексті верифікації мовця успішне досягнення верифікації на основі руху губ ґрунтується на більш детальному дослідженні фізичного процесу та поведінкової біометрії в межах спостережуваної активності руху губ [27]. Аналогічним чином були запропоновані методи верифікації людини, засновані на поведінкових моделях руху верхньої частини тіла людини, з використанням статистичних підходів для аналізу та перевірки унікальних поведінкових патернів [28]. Ці методи розширюють попередню роботу та демонструють потенціал поведінкової біометрії на основі руху у верифікації осіб.

Прогрес у технологіях, таких як смартфони та розумні годинники з потужними давачами, забезпечив легкодоступні платформи для впровадження та розгортання мобільної поведінкової біометрії на основі руху [30] . Ці пристрої можуть фіксувати та аналізувати різні види повсякденної діяльності, що дозволяє розробляти системи верифікації на основі руху. В наших дослідженнях, методи машинного навчання, такі як автокодувальники, були використані для аналізу патернів руху для біометричної верифікації користувача [31] . Ці підходи використовують сенсорні дані для підвищення точності та надійності систем верифікації на основі руху.

Крім того, методи верифікації на основі руху були досліджені в контексті інтелектуальних транспортних засобів, де прогнозування руху та оцінка ризиків мають вирішальне значення для забезпечення безпеки [32]. Ці методи спрямовані на прогнозування руху транспортних засобів та оцінку потенційних ризиків, сприяючи розвитку інтелектуальних транспортних систем.

Оцінка ефективності поведінкових біометричних систем є важливою для забезпечення їх ефективності та надійності. Техніки оцінювання цих систем включають використання статистичних метрик, баз даних для порівнянь та суб'єктивних методів оцінювання [33]. Стандарт BioAPI, який визначає архітектуру біометричної системи, надає структуру для оцінювання поведінкових біометричних систем [33].

Таким чином, поведінкові методи та методи верифікації на основі руху показали перспективність у різних програмах, включаючи верифікацію спікерів, біометричну перевірку користувача та інтелектуальні транспортні засоби. Ці методи використовують фізичний процес і поведінкову біометрію, пов'язану з конкретними рухами, для перевірки особистості людей. Прогрес у технологіях, таких як смартфони та розумні годинники, сприяв впровадженню та розгортанню поведінкової біометрії на основі руху.

1.2.4 Мультимодальні біометричні системи

Мультимодальна біометрична верифікація означає використання кількох фізіологічних або поведінкових характеристик для цілей, пов'язаних із реєстрацією, ідентифікацією та верифікацією [34]. Цей підхід набув популярності завдяки своїй здатності долати обмеження, пов'язані з самостійними біометричними модальностями, і покращувати загальні показники розпізнавання [35]. Інтегруючи інформацію з кількох біометричних джерел, мультимодальні біометричні системи можуть компенсувати обмеження продуктивності окремих біометричних сигналів [36].

Одним з напрямків мультимодальної біометричної верифікації є розробка методів злиття рішень. Ці методи спрямовані на об'єднання інформації з різних біометричних модальностей для прийняття остаточного рішення [37]. Оцінка методів злиття рішень у контексті банківських додатків показала багатообіцяючі результати, продемонструвавши потенціал мультимодальної біометрії у підвищенні безпеки фінансових операцій [37].

Крім того, було досліджено застосування мультимодальної біометричної верифікації в розумних містах. Дослідники запропонували вдосконалені підходи з використанням оптимізованих нечітких генетичних алгоритмів для підвищення точності та показників розпізнавання мультимодальних біометричних систем у середовищах розумного міста [38]. Це підкреслює потенціал мультимодальної біометрії в забезпеченні безпечних та ефективних послуг з верифікації особи в міських умовах.

Хоча мультимодальні біометричні системи пропонують підвищену точність, вони також можуть мати вищі витрати та час обробки порівняно з одномодальними системами [39]. Однак переваги підвищеної точності та надійності роблять мультимодальні системи біометричної верифікації цінним рішенням у різних сферах, включаючи комп'ютерну безпеку та біометрію [35]; [39];[40].

Підсумовуючи, мультимодальні системи біометричної верифікації стали перспективним підходом для подолання обмежень єдиних біометричних модальностей. Інтегруючи інформацію з безлічі фізіологічних або поведінкових характеристик, ці системи можуть підвищити рівень розпізнавання та підвищити безпеку. Методи злиття рішень, методи машинного навчання та оптимізовані алгоритми сприяють розробці точних та надійних мультимодальних біометричних систем. Незважаючи на те, що витрати та час обробки можуть бути вищими, переваги підвищеної точності роблять мультимодальні системи біометричної верифікації цінними в різних сферах застосування.

1.3 Методи машинного та глибокого навчання для біометричної верифікації

1.3.1 Методи машинного навчання

У цьому підрозділі будуть розглянуті які статистичні методи машинного навчання застосовуються для вирішення задачі біометричної верифікації. Довгий час нейронні мережі були дуже вимогливі до необхідної кількості обчислювальних ресурсів, та працювали дуже повільно порівняно з більш компактними і легкими статистичними методами машинного навчання. Хоча зараз пристрої та процесори набагато потужніші, все ж нейронні мережі зазвичай програють більш простим методам машинного навчання в контексті ресурс-оптимальності. Важливою ознакою розглянутих нижче алгоритмів є їх здатність навчатися лише на даних одного класу, що є дуже важливою вимогою для більшості задачі верифікації чи аутентифікації.

Довгий час в сфері біометричної верифікації такі алгоритми як однокласовий SVM або IsolationForest впевнено тримали першість. Навіть зараз, коли нейронні мережі витіснили ці методи – популярними є гібридні підходи, коли методи глибинного навчання поєднуються з статистичними

методами машинного навчання на різних етапах та забезпечують найкращий результат з точки зори і якості, так і швидкості та кількості необхідних ресурсів.

Однокласовий SVM

Однокласовий Support Vector Machine (SVM) використовує опорні вектори для створення гіперплощини, що максимально відокремлює нормальні дані від аномальних.

Однокласовий SVM є популярним вибором для біометричної автентифікації завдяки своїй здатності виявляти аномалії та класифікувати точки даних, які належать до одного класу[41]. Він використовувався в таких програмах, як розпізнавання обличь, динаміка дотику та руху мишки, та інших [41]. Однокласовий SVM особливо корисний у сценаріях, коли для навчання доступні лише позитивні зразки, що робить його придатним для однокласових завдань класифікації в біометричній автентифікації, а також ідеально підходить для аналізу складних біометричних шаблонів, таких як відбитки пальців або розпізнавання обличчя.

Однак варто зазначити, що продуктивність однокласного SVM може відрізнятися в залежності від конкретного застосування. Наприклад, у дослідженні реальної автентифікації мобільних користувачів за допомогою давачів руху однокласовий SVM показав гірші результати, ніж SVM для бінарної класифікації [42]. Це говорить про те, що вибір класифікатора повинен бути ретельно продуманий, виходячи з конкретних вимог і характеристик системи біометричної аутентифікації, проте варто враховувати що використання даних від інших користувачів («класів») не завжди можливо та має свої ризики.

Крім однокласного SVM, для біометричної аутентифікації були запропоновані й інші підходи. Наприклад, для мультимодального біометричного розпізнавання була запропонована гібридна модель, що поєднує навчання метрики відстані та опорну векторну машину DAG (Directed Acyclic Graph) (SVM) [43]. Цей підхід спрямований на максимізацію міжкласових

варіацій і мінімізацію внутрішньокласових варіацій шляхом вивчення метрики відстані Махаланобіса за допомогою ядра SVM [43].

Варто зазначити, що SVM вимагає високих обчислювальних ресурсів, тому варто враховувати це при виборі типу моделі. Проте, цей алгоритм гарно працює з даними високої розмірності, та може дуже ефективно працювати для складних типів аномалій.

Isolation Forest (IF)

Алгоритм Isolation Forest — це техніка машинного навчання, яка використовується для виявлення аномалій. Він був запропонований у 2008 році [44]. На відміну від традиційних методів, які покладаються на вимірювання відстані або щільності, алгоритм ізоляційного лісу заснований на концепції ізоляції. Він створює ансамблеву модель на основі дерева рішень, яка ізолює аномалії шляхом рекурсивного розбиття даних, доки кожен екземпляр не опиниться у власному листовому вузлі [45]. Алгоритм використовує субдискретизацію для ефективного виявлення аномалій, що призводить до лінійної часової складності з низькими вимогами до пам'яті [44].

У контексті біометричної верифікації алгоритм Isolation Forest був застосований до різних модальностей. Наприклад, у дослідженні систем аутентифікації ЕЕГ представив ізоляційний ліс як новий інструмент для автентифікації користувачів і дослідив його придатність до даних ЕЕГ [46]. Алгоритм ізоляційного лісу також був досліджений у галузі поведінкової біометричної автентифікації на сенсорному екрані, показавши багатообіцяючі результати [47]. Крім того, алгоритм був протестований разом з іншими моделями машинного навчання, такими як Random Forest, Support Vector Machine і K-Nearest Neighbor, для оцінки автентифікації користувачів за допомогою поведінкової біометрії [48].

Алгоритм Isolation Forest пропонує кілька переваг для біометричної верифікації. Він здатний виявляти аномалії та викиди в даних, що робить його придатним для виявлення шахрайських або несанкціонованих спроб доступу.

Алгоритм також є ефективним і масштабованим, що дозволяє йому обробляти великі набори даних з даними високої розмірності. Крім того, алгоритм Isolation Forest не покладається на припущення про базовий розподіл даних, що робить дозволяє його застосовувати до різних типів даних [45].

Однак важливо зазначити, що на продуктивність алгоритму Isolation Forest можуть впливати такі фактори, як вибір гіперпараметрів та якість навчальних даних. Для досягнення оптимальних результатів необхідні ретельні методи налаштування параметрів і попередньої обробки. Крім того, алгоритм може підходити не для всіх типів біометричних даних, і його ефективність слід оцінювати в кожному конкретному випадку.

Local Outlier Factor (LOF)

Алгоритм локального фактора викиду (LOF) — популярний метод машинного навчання, який використовується для виявлення аномалій і ідентифікації викидів. Він був представлений у 2000 році у [49]. Алгоритм LOF вимірює локальне відхилення щільності точки даних відносно її сусідніх точок, дозволяючи йому ідентифікувати викиди, які мають суттєво різну щільність порівняно з навколишнім середовищем.

У контексті біометричної перевірки алгоритм LOF застосовувався до різних модальностей. Наприклад, у системах перевірки мовців алгоритм LOF використовувався для виявлення аномальних моделей мовлення, які можуть вказувати на видавання себе за іншу особу або спроби шахрайства [50]. Крім того, алгоритм LOF досліджувався під час аналізу викидів у базах знань на основі правил, що може бути актуальним для систем біометричної верифікації, які покладаються на прийняття рішень на основі правил [51].

Алгоритм LOF пропонує кілька переваг для програм біометричної перевірки. Він здатний виявляти як глобальні, так і локальні викиди, що робить його придатним для виявлення аномалій у різних контекстах. Алгоритм не покладається на припущення про базовий розподіл даних, що робить його стійким до різних типів даних. Крім того, алгоритм LOF може обробляти дані

великої розмірності та є обчислювально ефективним, дозволяючи йому ефективно обробляти великі набори даних [52].

Однак важливо зазначити, що на продуктивність алгоритму LOF можуть впливати такі фактори, як вибір гіперпараметрів, визначення локальних сусідів і порівняння між тестовим об’єктом і його сусідами. Для досягнення оптимальних результатів необхідні ретельний підбір та оцінка параметрів. Крім того, алгоритм LOF може не підходити для всіх типів біометричних даних, і його ефективність слід оцінювати в кожному конкретному випадку.

Висновок до підрозділу

Кожен з вищеописаних алгоритмів має свої переваги та недоліки, в залежності від конкретного типу даних та вимог в постановці задачі. Також можливо одночасне застосування кількох алгоритмів одночасно. В [53] автори досліджують різноманітні однокласові класифікаторі та їх поєднання (fusion) для неперервної автентифікації, такі як однокласовий SVM, LOF, IsolationForest та EllipticEnvelope та порівнювали їх з мультикласовими підходами. Хоча поєднання кількох однокласових класифікаторів не дає суттєвого приросту в метриках, воно все ж перевершує мультикласовий підхід, що показує можливість та життєздатність систем натренованих лише на даних одного класу.

На жаль, такі алгоритми не забезпечують достатньої точності при роботі з даними без попередньої обробки, тому для них необхідно генерувати ознаки. Можливим розв’язком є застосування гібридного підходу з глибоким навчанням, аби не розраховувати та підбирати ознаки вручну. Так, в [54] автори використали SVM після екстрактора ознак на основі згорткової мережі разом з перетворенням Фур’є, що дало змогу побудувати систему, яка автоматично обробляє вхідні дані і таким чином виділяє ознаки.

Загалом, класичні методи машинного навчання мають наступні обмеження: потреба в ручному генеруванні ознак; низька точність в роботі з необробленими даними, що особливо актуально для показів давачів; недостатні

величини метрик якості (точність, чутливість, тощо). Необхідно дослідити та запропонувати моделі та методи, які ефективно працюють з складними гетерогенними даними, необробленими даними, даними з великою дисперсією. Методи, які є ефективними для роботи з такими типами даних є нейронні мережі глибокого навчання, тому необхідно продовжити дослідження в цьому напрямку.

1.3.2 Методи глибокого навчання

У цьому підрозділі спочатку коротко розглянемо базові архітектури глибокого навчання, такі як: згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN), мережі довгострокової короткочасної пам'яті (LSTM) і механізми уваги (attention blocks) в контексті їх використання для неперервної автентифікації. Ці архітектури є фундаментальними будівельними блоками для розробки більш складних нейронних мереж. Окрім того, розглянемо конкретні структури моделей, які визначають, як виявляються та вивчаються шаблони і патерни в даних. До них належать автокодувальники та сіамські мережі, які можуть включати в себе CNN, LSTM або інші типи мереж. Наприклад, можна мати автокодувальник на основі LSTM або сіамські мережі на основі CNN. Кожна комбінація пропонує унікальні переваги та недоліки для неперервної автентифікації, особливо в контексті біометричних і поведінкових даних. В кінці розділу будуть розглянуті гібридні комбінації різних типів мереж.

1.3.2.1 Згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) і трансформери для неперервної автентифікації

Згорткові нейронні мережі (CNN) широко використовуються в різних програмах, включаючи неперервну автентифікацію. CNN особливо ефективні в задачах, які включають обробку зображень і сигналів, оскільки вони розроблені для автоматичного вивчення та виділення відповідних ознак із вхідних даних [55]. Крім того, використання блоків згорток дозволяє виявити просторові образи у вхідних даних.

У неперервній автентифікації CNN застосовувалися в запропонованій структурі автентифікації фізичного рівня на основі глибокого навчання, яка використовує три різні алгоритми: метод автентифікації сенсорних вузлів на основі глибокої нейронної мережі (DNN), метод автентифікації сенсорних вузлів на основі CNN , а також метод автентифікації сенсорних вузлів на основі попередньої обробки згортки (CPNN) [55].

CNN широко використовуються в різних біометричних системах автентифікації. Вони були застосовані для автентифікації на основі ЕКГ (електрокардіограми), з такими моделями, як залишкова згорткова нейронна мережа (ResNet) з механізмами уваги, які досягають високої точності в автентифікації людини [56]. У [57] автори досліджували продуктивність CNN для автентифікації людини на основі ЕЕГ (електроенцефалограми). Вони виявили, що CNN можна використовувати для автоматичного виділення ознак і класифікації в системах автентифікації на основі ЕЕГ [57].

CNN часто використовується не як окрема модель, а як блок, який дістає різноманітні ознаки та образи з вхідних даних, разом з додатковою моделлю “поверх” цього блоку (наприклад однокласовий SVM (OC-SVM) або k-найближчих сусідів (KNN)). У [54] автори запропонували фреймворк DeFFusion для автентифікації, де вони використовували OC-SVM як модель прийняття рішень над екстрактором ознак на базі CNN.

Переваги та недоліки використання CNN у контексті автентифікації:

Переваги:

- CNN автоматично виділяють відповідні ознаки з необроблених та сирих даних, зменшуючи потребу в розробці цих ознак вручну.
- CNN можуть фіксувати просторові та часові образи даних, що робить їх придатними для аналізу біометричних і поведінкових сигналів.
- CNN можуть обробляти складні та багатовимірні дані, забезпечуючи точну та надійну неперервну автентифікацію.
- Залежно від конкретної задачі та даних, CNN можуть бути ефективнішими в плані часу обробки та тренування, ніж повнозв’язні

(fully-conected) альтернативи нейронних мереж, що робить їх життєздатним варіантом для розгортання на периферійних пристроях.

- CNN показали багатообіцяючі результати в різних біометричних методах, включаючи ЕКГ, ЕЕГ, аутентифікацію жестів і ходьби.

Обмеження:

- Для досягнення оптимальної продуктивності CNN вимагає багато розмічених навчальних даних.
- Вони можуть бути дорогими з обчислювальної точки зору, особливо для програм, які працюють в реальному часі на пристроях з обмеженими ресурсами.
- Як і багато інших моделей машинного навчання, CNN можуть мати проблеми з обробкою зашумлених або неповних даних, що може вплинути на точність неперервної автентифікації. Збільшення кількості даних та знешумлення можуть допомогти пом’якшити цю проблему.
- CNN більш ефективні в роботі з певними типами вхідних даних, як-от зображення, проте можуть гірше працювати з послідовностями та часовими рядами.

З іншого боку, наступна архітектура глибокого навчання, а саме рекурентні нейронні мережі (RNN), спеціально розроблені для обробки послідовностей шляхом використання циклів зворотного зв’язку на рекурентних рівнях [58]. На відміну від нейронних мереж прямого зв’язку, RNN можуть зберігати інформацію з попередніх часових кроків, що робить їх придатними для завдань, що включають часові залежності та послідовні шаблони [58].

Архітектура RNN складається з трьох основних компонент: функція «вхід-до-прихованого», перехід «прихований-до-прихованого» та функція «прихований-до-виводу» [59]. Ці компоненти дозволяють мережі обробляти вхідні послідовності, оновлювати свій прихований стан на основі поточного введення та попереднього прихованого стану та генерувати вихідні прогнози [59]. Однак традиційні RNN мають проблему з затуханням та вибухом

градієнта, яка обмежує їх здатність фіксувати довгострокові залежності в послідовностях [59]. Довга короткочасна пам’ять (LSTM) — це конкретна архітектура рекурентних нейронних мереж, призначена для вирішення проблеми затухання градієнта, за допомогою вентилів забування та виходу, що дозволяє контролювати, яку інформацію зберігати, а яку – забути [60].

У неперервній автентифікації RNN застосовуються на різних даних. Одним із застосувань є автентифікація на основі дихання на пристроях IoT (Internet of Things) з обмеженими ресурсами [61]. Моделюючи послідовний характер дихальної акустики, RNN можуть ефективно автентифікувати користувачів на основі їхніх унікальних моделей дихання [61].

RNN також використовувалися в інших системах поведінкової автентифікації. Наприклад, RNN були застосовані в сенсорних системах автентифікації, де дані з пристроїв введення (мишка, клавіатура) використовуються як вхідні дані для ідентифікації користувача [62]. У [62] автори провели поглиблений огляд, порівнюючи LSTM і GRU (gate recurrent unit, інша специфічна архітектура RNN) з різними конфігураціями навчання та в поєднанні з CNN. Залежно від конфігурації моделі в деяких випадках GRU перевершує LSTM, хоча LSTM забезпечує стабільно кращі результати на наборі даних TouchAnalytics. Крім того, RNN використовуються в біометричній автентифікації на основі ЕКГ, де послідовний характер сигналів ЕКГ фіксується для автентифікації користувачів [63].

Загальні *переваги* RNN (зокрема LSTM) у неперервних механізмах автентифікації:

- RNN, особливо LSTM, призначені для розпізнавання шаблонів у часі, що робить їх придатними для завдань, пов’язаних із послідовними даними, такими як дані часових рядів від різних давачів.
- LSTM можуть вивчати довгострокові залежності в даних, що може бути корисним для неперервної автентифікації, коли моделі поведінки можуть розвиватися протягом тривалих періодів.

- Вони можуть обробляти вхідні послідовності змінної довжини, забезпечуючи гнучкі та динамічні сеанси автентифікації.

Обмеження:

- Навчання RNN, у тому числі LSTM, може потребувати інтенсивних обчислень через їх рекурентність, що може бути складним для пристроїв з обмеженими ресурсами. Це вплине на затримку моделі на етапі висновку, що має вирішальне значення для програм, які працюють в реальному часу.
- Для досягнення оптимальної продуктивності RNN вимагають значної кількості розмічених навчальних даних.
- Вони мають проблему затухання та вибуху градієнтів. Хоча LSTM розроблені, щоб дещо полегшити ці проблеми.
- RNN, включаючи LSTM, можуть бути більш складними для реалізації та оптимізації порівняно з іншими архітектурами нейронних мереж, вимагаючи ретельного налаштування параметрів і дизайну архітектури.

Хоча і RNN, і CNN пропонують різні переваги, дослідницькі тенденції показують активні дослідження гібридних архітектур, де поєднуються кілька архітектурних блоків, таким чином пом’якшуючи недоліки кожної архітектури та доповнюючи одна одну.

В опитуванні [4] автори зауважують, що архітектури RNN і CNN можна вважати найбільш використовуваними в біометричній/поведінковій автентифікації. Більш того, гібридні архітектури є поширеними й у багатьох випадках забезпечують кращі показники продуктивності та дозволяють нам досягти компромісу між якістю та вимогами до обчислювальних ресурсів моделі.

У [62] поєднання CNN+LSTM забезпечують найкращу продуктивність майже в усіх випадках з точки зору EER (рівний рівень помилок), FRR (частота помилкових відхилень) і FAR (False Acceptance Rate, хоча CNN разом із GRU забезпечили кращі показники точності для набору даних TouchAnalytics. Темпоральна згорткова нейронна мережа, запропонована в [63], перевершує

RNN для довших зразків навчальних даних, тоді як для коротких зразків даних вона показує кращі результати. Поєднання CNN і RNN (згорткові рекурентні нейронні мережі (CRNN) були запропоновані для вивчення локальної та контекстної інформації в інформації про стан каналу (CSI) для автентифікації користувача [64]. У цій програмі RNN використовуються для захоплення контекстної інформації в даних CSI, що дозволяє проводити точну автентифікацію користувачів на основі їхніх унікальних шаблонів CSI [64].

Кілька досліджень запропонували гібридні глибокі нейронні мережі для надійного представлення особливостей ходьби. Наприклад, у [65] було використано поєднання CNN і RNN для об'єднання функцій у просторовій і часовій областях із зібраних смартфоном наборів даних про ходьбу, досягаючи високої точності в ідентифікації та автентифікації людини.

Окрім смартфонів, досліджувалися й інші сенсорні модальності. Деякі дослідники запропонували мережі глибокого навчання для розпізнавання ходи з використанням мультимодальних носимих інерційних давачів, використовуючи CNN для вилучення характеристик ходьби з необроблених сигналів акселерометра та гіроскопа. У [66] гібридний підхід CNN-Bi-LSTM використовувався для неперервної автентифікації мобільного користувача з використанням функцій, отриманих із вбудованих давачів пристроїв IoT. Поєднання моделей CNN і Bi-LSTM підвищило точність розпізнавання користувачів для різних дій. Також, [67] запропонував архітектуру неявної автентифікації на основі периферійних обчислень, яка використовувала модель глибокого навчання, що складається з CNN і LSTM для біометричної ідентифікації ходьби. Дані ходьби, отримані з акселерометра та гіроскопа, використовувалися як вхідні дані, і модель була оптимізована для автентифікації користувачів на основі їхніх моделей ходьби. Використовуючи часові ознаки, отримані LSTM, запропонована архітектура досягла точної та неявної ідентифікації користувача.

Інша архітектура, яка зараз є найефективнішою серед інших, це трансформер, вперше представлений у [68]. Основним компонентом

трансформера є механізм уваги, який дозволяє аналізувати зв'язки між елементами послідовності. Хоча він не такий популярний у біометричній або поведінковій автентифікації, він починає застосовуватися в різних сферах, зокрема аналізі часових рядів та показує багатообіцяючі результати. Мережа CNN, що містить модуль уваги для покращення виділених ознак, була представлена для розпізнавання ходьби за допомогою носимих давачів IMU в [69]. Поєднання блоку уваги з LSTM для ідентифікації ходьби досліджувалося в [70] і показало високу продуктивність. Ієрархічна LSTM з блоком уваги була запропонована в [71] для аутентифікації ЕКГ. Різні модифікації трансформера розглядаються авторами для розпізнавання ходи [72], [73] і динаміки мобільного натискання клавіш [74]. Стандартний трансформер порівнюється з трансформером із тимчасовими та канальними модулями, які об’єднують блоки CNN та рекурентні у складну архітектуру. Такий комплексний гібридний підхід демонструє найкращу продуктивність порівняно з іншими гібридними комбінаціями. Трансформер також може бути використаний як модуль вилучення ознак, наприклад, для автентифікації ЕКГ [75].

Крім того, оглядові роботи надали вичерпні огляди розпізнавання ходьби на основі глибокого навчання. Комплексне дослідження розпізнавання ходьби на основі глибокого навчання, що охоплює набори даних, протоколи тестування, найсучасніші рішення, виклики та майбутні напрямки досліджень, було представлено в [76]. Вони підкреслили домінування нейронних мереж глибокого навчання в розпізнаванні ходи та їхній потенціал для прикладних задач [76]. Також в [77] було проведено огляд щодо глибокого розпізнавання ходьби, обговорюючи характеристики, характеристики, переваги та обмеження різних методів на основі глибокого навчання

Таким чином, у цьому розділі детально описано використання архітектур глибокого навчання, зокрема згорткових нейронних мереж (CNN), рекурентних нейронних мереж (RNN) і трансформерів для неперевної автентифікації. Різні комбінації архітектур глибокого навчання, як-от CNN, LSTM або трансформери, були успішно застосовані для неперервної автентифікації для

ЕКГ, ЕЕГ, ідентифікації ходьби тощо. Було оглянуто використання гібридних архітектур, що поєднують вивчення просторових ознак CNN і розпізнавання часових шаблонів RNN, або механізм уваги з трансформерами, демонструючи гнучкість цих архітектурних одиниць глибокого навчання.

Варто зазначити, що трансформер показує високу ефективність для розв'язання задач біометричної та поведінкової автентифікації і має суттєві переваги в контексті часу обробки над рекурентними нейронними мережами. Тому: необхідно глибоко дослідити побудову архітектур на основі трансформера; кількісно оцінити значення критеріїв якості; провести порівняння їх з іншими існуючими моделями.

1.3.2.2 Сіамські мережі та автокодувальники

Сіамські мережі. Сіамські мережі відносяться до архітектури нейронної мережі, яка складається з двох або більше ідентичних підмереж, також відомих як близнюки або гілки. Ці підмережі мають однакові ваги та параметри, що дозволяє їм вивчати та обробляти дані паралельно та симетрично. Під час навчання сіамські мережі вчаться виділяти вектори ознак із вхідних даних і обчислювати подібність між парами вибірок [78].

Сіамські мережі навчаються на парах зразків: позитивна пара, коли елементи в парі схожі один на одного або належать до одного класу, і негативні пари, якщо вони не належать до одного класу. Таким чином, цей тип мережі спрямований на моделювання метричного простору для заданих вхідних даних шляхом моделювання відстані та подібності між ними. Сіамські мережі можна навчити кількома способами, хоча найпоширенішим підходом є оптимізація триплетної функція втрат або контрастної функції втрат [79].

Формула контрастних втрат така :

$$L = (1-y)\cdot\frac{1}{2}D^2 + \frac{y}{2}\{\max(0,\, m-D)\}^2 (1.1)$$

де:

y — двійкова індикаторна змінна, яка дорівнює 1, якщо пара зразків схожа, і 0, якщо вони не схожі.

D — евклідова відстань між парою зразків.

m — запас, який є гіперпараметром, що визначає, наскільки далеко мають бути різні точки.

У разі оптимізації з триплетними втратами фактично було б три гілки мережі. Оптимізуючи втрату триплетів, модель одночасно намагається змоделювати як відстань до подібних або позитивних елементів, так і до негативних, тому вхідними даними до сіамської мережі в цьому випадку будуть триплети (x_a, x_p , x_n), які означають якірний елемент та позитивний і негативний елемент відповідно.

Триплетна функція втрат визначається як :

$$E = max\left(\left\|x_a - x_p\right\|^2 - \|x_a - x_n\|^2 + m, 0\right) \quad (1.2)$$

де m — запас, який є гіперпараметром, що визначає, наскільки далеко мають бути різні точки. Це допомагає гарантувати, що модель розштовхує позитивні та негативні зразки принаймні на цей запас.

Сіамські мережі особливо добре підходять для самостійних навчань із вчителем, оскільки вони можуть навчитися порівнювати та зіставляти різні вибірки чи перегляди тих самих даних. Сіамські мережі широко використовувалися в самостійному навчанні із вчителем, зокрема в контрастному навчанні [80]. Одним із відомих підходів є Bootstrap Your Own Latent (BYOL), який спирається на дві нейронні мережі, які називаються онлайновою та цільовою мережами, які взаємодіють і навчаються одна в одної [81], досягаючи продуктивності SOTA на наборах даних зображень.

На жаль, і контрастна оптимізація, і оптимізація триплетних втрат вимагають великої кількості негативних прикладів, яких немає у випадку автентифікації. Для випадку з задачею верифікації будуть присутні лише позитивні зразки. Дослідники запропонували інший підхід до самоконтрольованого навчання — SimSiam (Simple Siamese), який досліджує прості сіамські мережі, які можуть вивчати значущі представлення без негативних пар вибірок [82]. У [82] модель використовує доповнення позитивних вхідних даних для моделювання відстані між ними: кожна гілка мережі бере різну розширену вибірку того самого вхідного сигналу, що змушує

модель моделювати подібні елементи разом з великою дисперсією та різноманітністю.

Функція похибки для SimSiam може бути сформульована так :

$$L = \frac{D(p_1,z_2)+D(p_2,z_1)}{2}, (1.3)$$

де :

- L це похибка.
- D є функцією подібності негативного косинуса.
- z_1 і z_2 це проекції від кодувальника f для двох аугментованих входів.
- p_1 і p_2 – передбачення з верхнього повнозв'язного шару MLP (h), який перетворює вихідний сигнал кодувальника (f) для двох аугментованих входів .

Функція подібності негативного косинуса D визначається як :

$$D(p,z) = -\frac{p*z}{\|p\|_2*\|z\|_2}, (1.4)$$

Ця функція обчислює косинус кута між вектором передбачення p і вектором проекції z . Від'ємний знак забезпечує мінімізацію втрат, коли кут малий (тобто коли подібність косинусів велика), що відповідає подібності векторів. l_2-нормалізація в знаменнику гарантує, що величина векторів не впливає на оцінку подібності [82] .

Можливість навчання без негативних пар з навчанням без вчителя робить сіамські мережі перспективною архітектурою для неперервної автентифікації. У [83] автори запропонували AuthentiSense, масштабовану поведінкову біометричну схему автентифікації з використанням few-shot навчання для мобільних платформ із використанням шаблонів руху. Сіамська мережа на базі CNN у цій схемі вивчає подібності та відмінності між зразками поведінки користувачів, уможливлюючи автентифікацію навіть з обмеженими навчальними даними [83]. Автори [84] запропонували структуру Motion ID для ідентифікації користувачів смартфонів за допомогою шаблонів руху від IMU, зокрема акселерометрів. Вони вказали на проблему шуму та неточностей у сигналах давачів і запропонували використовувати сіамську мережу з Triplet

Margin Loss. Щоб підвищити точність, ознаки з виходу сіамської мережі були оброблені в верхньому шарі з багатошаровим персептроном (MLP). MLP шар навчився відображати нормалізовані вектори ознак (embeddings) зразків та їх аугментацій для одного користувача ближче один до одного, а ті, що належать різним користувачам, далі один від одного.

У [85] автори застосували сіамські мережі для чисто поведінкової автентифікації, зокрема динаміки натискання клавіш. У [86] автори запропонували few-shot підхід для автентифікації або комп'ютерного користувача (з динамікою миші та натискання клавіш), або мобільного користувача (з дотиком і утриманням). Цей підхід забезпечує єдину модель для автентифікації всіх користувачів, а не модель для кожного користувача, що є найбільш поширеним у розробці систем автентифікації.

Сіамські мережі також використовувалися для аутентифікації на основі ЕКГ. У [87] автори використовували сіамську мережу з налаштованою сигмоподібною функцією. Вони перетворюють удари ЕКГ у двійкові зображення та передають їх через модуль виділення ознак CNN. У дослідженні, представленому в [88], Ensemble Siamese Network було запропоновано для автентифікації ЕКГ. Порівняльна частина мережі порівнює витягнуті ознаки із заявленими зразками векторів у сховищі, щоб визначити їх подібність.

Автокодувальники. Автокодувальники - це особливий тип архітектури штучної нейронної мережі, який є моделлю навчання без вчителя, яка включає як кодер, так і декодер. Кодер перетворює вхідні дані на представлення в низьковимірному латентному просторі. Тим часом декодер приймає це представлення та реконструює вхід. Автокодувальник має на меті вивчити стиснуте представлення вхідних даних і потім реконструювати його якомога точніше [89]. Вивчаючи стандартні шаблони поведінки користувача, автокодувальники можуть ідентифікувати відхилення від цієї норми, що може вказувати на шахрайські дії або спроби несанкціонованого доступу; ця архітектура моделі стала важливим інструментом для неперервної автентифікації. Важливість архітектури автокодувальника з точки зору

автентифікації полягає в здатності до самостійного навчання з вчителем (SSL, self-supervised learning) і здатності навчатися лише на прикладах одного класу.

На практиці автокодувальник тренується мінімізувати помилку реконструкції, яка кількісно визначає розбіжність між початковим і реконструйованим входом. Цю похибку можна розрахувати як норму різниці між вихідними даними та їх реконструкцією, враховуючи:

$$L = \|x - \tilde{x}\| \quad (1.5)$$

де L — помилка реконструкції, x —вхід, а $\tilde{x}$ — реконструйований вихід на базі входу.

Вибір використовуваної норми повинен здійснюватися з урахуванням характеристик даних. Для безперервних даних середня квадратична похибка (MSE) є стандартним вибором, хоча середня абсолютна похибка (MAE) може бути більш робастним варіантом у разі наявності викидів у даних. Можливо також поєднати обидві метрики та використати похибку Губера (Huber loss), аби обійти недоліки обох метрик.

Було розроблено кілька варіантів автокодувальників, кожен з яких має переваги та потенційні недоліки для неперервної автентифікації. Ці варіанти містять шумозаглушуючі автокодувальники, розріджені автокодувальники, варіаційні та змагальні автокодувальники, кожен з яких призначений для вирішення певних завдань. Наприклад, автокодувальники з усуненням шумів (DAE) демонструють стійкість до шумів у даних, що є поширеною проблемою в реальних сценаріях автентифікації, зокрема для сигналів давачів. Забезпечуючи розрідженість у своїх прихованих шарах, розріджені автокодувальники (SAE) можуть вивчати більше розрізнювальних образів та ознак, покращуючи інтерпретованість моделі.

Варіаційний автокодувальник (VAE) використовує ймовірнісне моделювання. Він передбачає, що латентний простір відповідає певному розподілу ймовірностей, як правило, багатовимірному розподілу Гаусса. VAE навчені реконструювати вхідні дані та генерувати нові шляхом семплингу з змодельованого розподілу прихованого простору [90].

Змагальні автокодувальники (AAE) поєднують концепції автокодувальників і змагального навчання для вивчення надійних і дискримінаційних представлень біометричних даних. Мета полягає в тому, щоб створити латентний простір, який фіксує найбільш значущі характеристики вхідних даних, будучи стійкими до агресивних атак [91].

У таблиці 1.2 можемо переглянути порівняння різних типів автокодувальників і те, що вони можуть запропонувати.

Таблиця 1.2. Порівняння характеристик різних типів автокодувальників

Характеристики/модель	**AE**	**VAE**	**AAE**	**DAE**	**SAE**
Моделювання ймовірнісного розподілу даних	Ні	Так	Так	Ні	Ні
Генеративні можливості	Ні	Так	Так	Ні	Ні
Стійкість до шумних/пошкоджених входів	Ні	Ні	Ні	Так	Ні
Ієрархічне навчання ознак	Ні	Ні	Ні	Ні	Так

Автокодувальники для аутентифікації на основі ЕКГ. Автокодувальники зазвичай використовуються для біометричної автентифікації даних ЕКГ (електрокардіограма) та ЕЕГ (електроенцефалограма). ЕКГ — це нова біометрична модальність, яка широко вивчається для біометричного розпізнавання [92]. Використання сигналів електрокардіограми (ЕКГ) для неперервної автентифікації створює кілька проблем і можливостей. Однією з основних проблем є значні відмінності серед окремих пацієнтів. Сигнал ЕКГ кожної людини має унікальні характеристики, що ускладнює розробку універсальної моделі автентифікації [93]. Крім того, сигнали ЕКГ можуть демонструвати численні патології, такі як аритмії, що ще більше ускладнює процес автентифікації [93].

Традиційні підходи до обробки ЕКГ значною мірою покладаються на попередні знання, такі як виділення ознак і аналіз форми хвилі [94]. Однак ці

підходи можуть призвести до обчислювальних витрат і бути менш придатними для неперервної автентифікації в реальному часі. У [95] автори запропонували ЕКГ-ідентифікацію людини за допомогою дискретного косинусного перетворення, дискретного перетворення Фур'є та перетворення Волша-Адамара. Методи глибокого навчання можуть автоматично вивчати відповідні ознаки з необроблених сигналів ЕКГ, усуваючи потребу в ручному проектуванні ознак [96]. Ці моделі можуть працювати з великою розмірністю даних ЕКГ і потенційно фіксувати відомі та невідомі патерни [96].

Автокодувальники ефективно використовувалися для перевірки ЕКГ, забезпечуючи надійні методи неперервної автентифікації користувача. У [97] автори представили згортковий автокодувальник для аналізу та представлення сигналу ЕКГ, а в [98] запропоновано варіаційний згортковий автокодувальник. Автокодувальник використовується для вивчення стисненого представлення сигналів ЕКГ, яке потім використовується для автентифікації. Маскований автокодувальник (MAEEG) був запропонований у [99], який використовує 6-шаровий згортковий блок із 8-шаровим трансформерним кодером.

Значним прогресом у цій галузі є розробка системи Personalized AutoEncoder (PerAE), яка підтримує невелику модель автокодувальника під назвою Attention-MemAE для кожного зареєстрованого користувача системи [100]. Attention-MemAE покращує автокодувальник за допомогою модуля пам'яті та двох механізмів уваги. Тут автори порівняли запропонований метод на основі варіаційного автокодувальнику з регулярним і варіаційним автокодувальником на основі RNN і LSTM, показавши значне покращення продуктивності [100].

Автокодувальники для автентифікації за шаблонами руху. Іншим застосуванням автокодувальників у безперервній автентифікації є розпізнавання шаблонів руху. Це передбачає аналіз того, як людина ходить/сидить/пише, щоб ідентифікувати її. Автокодувальники можна використовувати для стиснення шаблонів руху, а потім відтворення оригінальних вхідних послідовностей. Аномалії або відхилення від нормальної

поведінки користувача можна виявити шляхом порівняння реконструйованих послідовностей рухів з оригінальними, що вказує на потенційний несанкціонований доступ.

У [31]досліджувалася біометричну перевірку користувача на основі автокодувальника з шаблонами руху на базі показів нагрудного акселерометра. Було оцінено внесок різних компонентів даних у процес перевірки залежно від виду діяльності. У дослідженні використовувався рекурентний автокодувальник довгострокової пам'яті як базова модель і досліджувався внесок різних компонентів даних у процесі перевірки [31]. У [101] автори також надали порівняльні дослідження різних типів автокодувальників, таких як варіаційний і неповний, у порівнянні з класичними підходами машинного навчання, такими як OC-SVM та IsolationForest.

Наприклад, у [102] автори запропонували однокласний змагальний автокодувальник на основі відносної уваги для неперервної автентифікації користувачів смартфонів, який включав дані на основі давачів від гіроскопа, акселерометра та магнітометра з різними діями, записаними користувачем. Їхній підхід поєднує AAE з механізмами уваги, щоб охопити багатші контекстуальні семантичні представлення моделей поведінки користувачів, покращуючи ефективність автентифікації. Змагальні атаки намагаються обдурити або контролювати систему автентифікації шляхом введення спеціально розроблених вхідних даних. Автокодувальники можуть бути не в змозі протистояти таким типам атак, що призводить до неправильної автентифікації або неавторизованого входу. Методи змагального навчання можуть допомогти пом'якшити цю вразливість, навчивши модель бути стійкою до агресивних атак [102] [103] . Змагальні приклади – це дещо модифіковані вхідні дані для введення в оману моделей машинного навчання, що може загрожувати біометричній перевірці та системам неперервної автентифікації. Автокодувальники можуть попередньо обробляти вхідні дані та усувати конфліктні збурення, роблячи моделі більш стійкими до змагальних атак [103]
.

У для проблеми ідентифікації ходи запропоновано нечітку структуру тимчасового згорткового автокодувальника (FTCAE). Крім того, автори представляють інноваційний щільний шар нечіткого набору інтервалів типу 2 (IT2FS). Цей спеціальний шар створено для усунення невизначеностей і шуму карт функцій. Це допомагає в процесі вивчення унікальних представлень у нечіткому прихованому просторі. IT2FS має локальний механізм зворотного зв'язку, який покращує здатність мережі моделювати невизначеність часових залежностей даних про ходу людини [104].

Загалом автокодувальники продемонстрували потенціал у різних програмах, включаючи безперервну автентифікацію, і можуть витягувати значущі та дискримінаційні характеристики з біометричних і поведінкових даних, дозволяючи системам неперервної автентифікації точно ідентифікувати та автентифікувати користувачів у режимі реального часу. Вони дозволяють як уникнути створення ознак вручну, так і не вимагають аномальних точок даних, забезпечуючи процес навчання без вчителя.

Сіамські мережі проти автокодувальників. Автокодувальники працюють, навчаючи мережу реконструювати свої вхідні дані, змушуючи її навчатися стисненому представленню даних у процесі [105]. Навпаки, сіамські мережі відносяться до певного типу нейронної мережі, яка часто використовується для завдань, пов'язаних із подібністю або відстанню [106]. Поєднання автокодувальників і сіамських мереж досліджувалося в різних додатках, включаючи автентифікацію на основі показів давачів. Нижче наводяться основні характеристики автокодувальників і сіамських мереж.

Автокодувальники:

- Вимоги до даних: автокодувальникам потрібні суттєва кількість даних, щоб вивчати основні шаблони та ефективно реконструювати вхідні дані.
- Стійкість до перетворень і невизначеності: автокодувальники за своєю суттю не стійкі до перетворень у вхідних даних. Однак певні типи автокодувальників, як-от варіаційні автокодувальники (VAE), можуть справлятися з невизначеністю в даних, вивчаючи розподіл даних.

- Навчання без вчителя : автокодувальники можна навчити без вчителя, що робить їх придатними для завдань, де позначені дані є недоступними (наприклад в задачі верифікації).
- Ініціалізація: навчання автокодувальників за допомогою градієнтного спуску може бути складним завданням, особливо якщо початкові ваги далекі від хорошого рішення. Пошук відповідних початкових ваг має вирішальне значення для успішного навчання глибоких мереж автокодувальників.
- Перетренування: автокодувальники можуть бути схильні до перетренування, особливо якщо ємність моделі велика порівняно з розміром навчальних даних. Методи регуляризації, такі як випадання або зменшення ваги, можуть допомогти пом’якшити цю проблему.

Сіамські мережі:

- Вимоги до даних : сіамські мережі можуть ефективно навчатися на основі невеликої кількості даних і здатні до одномоментного та одноразового навчання. Для потенційного навчання без вчителя сіамські мережі вимагають додаткової генерації штучних даних для того аби був можливий процес тренування з вчителем, що є викликом в контексті верифікації чи автентифікації. Це потребує додаткової генерації обчислювальних витрат та не гарантує нам коректного навчання відмінності “легітимного” користувача від не “легітимного”.
- Стійкість до перетворень і невизначеності: сіамські мережі розроблені таким чином, щоб бути більш стійкими до перетворень у вхідних даних, забезпечуючи узгоджені виходи, навіть якщо вхідні дані трансформовано. Однак вони за своєю суттю не справляються з невизначеністю даних.
- Попарне порівняння: сіамські мережі розроблені для вимірювання подібності чи відмінності між парами вхідних даних, що робить їх придатними для завдань, де важлива відносна подібність між точками

даних. З іншого боку, якість створених пар даних може сильно вплинути на якість моделі.

- Узагальнення: сіамські мережі можуть добре узагальнювати невидимі дані, що робить їх придатними для реальних додатків. Вони можуть навчитися вловлювати основні закономірності або характеристики даних, уможливлюючи точну перевірку або класифікацію.

Автентифікація на основі давачів використовує їх покази, як-от акселерометр або гіроскоп, щоб підтвердити особу користувача. Поєднання автокодувальників із сіамськими мережами дає змогу вивчати компактне представлення даних давачів, яке фіксує унікальні характеристики поведінки кожного користувача, що забезпечує точну автентифікацію. Один із прикладів поєднання автокодувальників і сіамських мереж для аутентифікації на основі давачів можна знайти в роботі [106]. Автори запропонували метод з'єднання пристроїв на основі давачів, у якому використовувалися сіамські мережі та автокодувальники з усуненням шумів, щоб дізнатися оптимальне представлення для з'єднання пристроїв. Сіамська архітектура сприяла розрізненню пристроїв, які носять різні користувачі, тоді як автокодувальник діяв як ефективний механізм вилучення відбитків пальців.

У [107] дослідники вивчали нові способи використання сіамських нейронних мереж для з'єднання записів у базі даних. Вони розробили нову архітектуру, яка використовує автокодувальники та покращує здатність моделі добре працювати з різними наборами даних. Ця нова архітектура також робить модель менш залежною від конкретних налаштувань для її правильної роботи. Інша стаття автора [108] представляє систему GaitPrivacyON, яка поєднує в собі автокодувальник із сіамською архітектурою для мобільної біометрії ходи. Система містить згортковий автокодувальник, який перетворює біометричні необроблені атрибути даних у представлення, яке зберігає конфіденційність. Він також має мобільну систему перевірки ходи, яка поєднує згорткові нейронні мережі (CNN) і рекурентні нейронні мережі (RNN) із сіамською архітектурою.

У [109] автори пропонують анонімізатор даних для біометричних додатків і онлайн-менеджменту ідентифікації. Система поєднує сіамську мережу автентифікації з приватним предиктором виведення атрибутів. У документі використовується функція мінімально-максимальних втрат і змагальна оптимізація для максимізації кінцевого прибутку.

Висновок до підрозділу

Для задачі верифікації сіамські мережі потребують додаткових обчислювальних витрат для генерації штучних негативних даних для проведення процедури навчання з вчителем, що не гарантує якісного виділення ознак, унікальних для “свого” користувача. На відміну від сіамських мереж, автокодувальник природньо підтримує процедуру навчання без вчителя та потребує даних лише для одного класу. Як правило в дослідженнях автокодувальник виступає лише в якості модуля виділення ознак (особливо згортковий автокодувальник) з додатковими модулями прийняття рішень, а не самостійно.

Тому, для розв’язання сучасних задач верифікації користувача, потрібно більш глибоко дослідити використання автокодувальника, як моделі, яка є ефективною для виділення прихованих ознак в даних та зручна для створення нових архітектур нейронних мереж глибокого навчання. Запропонована модель буде навчатися лише на одному класі даних; мати меншу кількість параметрів, які необхідно налаштовувати; та забезпечувати кращі значення метрик якості верифікації.

1.4 Використання фрактальної розмірності для аналізу біометричних сигналів

Аналіз з допомогою фрактальної розмірності широко використовується в аналізі біологічних сигналів завдяки своїй здатності фіксувати складність і самоподібність цих сигналів у різних масштабах . Мозок, будучи системою, що самоорганізується, демонструє самоподібність у різних просторових і часових

масштабах, що робить аналіз фрактальних розмірів особливо актуальним для вивчення нейронних порушень при таких станах, як гострий інсульт [110]. Крім того, обчислення фрактальної розмірності включає різноманітні алгоритми, кожен з яких має свої сильні сторони та обмеження, надаючи дослідникам низку інструментів для аналізу біологічних сигналів [111]. У контексті аналізу сигналів ЕЕГ фрактальна розмірність використовувався для виявлення нейрональних порушень у пацієнтів з інсультом [110], оптимізації аналізу транзиторних візуальних викликаних потенціалів [112] та розрізнення здорових та епілептичних сигналів ЕЕГ [113]. Крім того, використання аналізу фрактальних розмірів поширилося на інші біологічні сигнали, такі як магнітоенцефалографічні (МЕГ) записи пацієнтів із хворобою Альцгеймера [114] та аналіз послідовностей білків [115]. Ці програми демонструють універсальність аналізу фрактальних розмірностей у охопленні основної складності різноманітних біологічних сигналів.

Крім того, застосування аналізу фрактальної розмірності не обмежується характеристикою сигналів, але також поширюється на вилучення ознак для цілей класифікації. Дослідження показали, що ознака, отримана гібридним методом, що поєднує фрактальну розмірність і емпіричну декомпозицію, перевершує використання лише емпіричного розкладання мод для аналізу послідовностей білків [115]. Аналогічно, в контексті досліджень інтерфейсу мозок-комп'ютер (BCI), фрактальна розмірність була використана як ознака для класифікації, демонструючи її потенціал у просуванні технології BCI [116]. Крім того, використання фрактальної розмірності для класифікації нормальних і аномальних тонів серця підкреслює її застосовність у медичній діагностиці[117].

Фрактальна розмірність все частіше використовується в системах біометричної верифікації для підвищення точності та безпеки. В [118] автори представили використання фрактальної автокореляції для обчислення фрактальних розмірів у біометричному розпізнаванні, підкресливши її ефективність як дескриптора текстури зображення. Цей метод виграє від стабільності проти варіацій обертання та масштабу, притаманних фрактальним

явищам, що робить його бажаним для біометричних застосувань [119].

У сфері біометрії фрактальна розмірність була використана в класифікації зображень райдужної оболонки ока для покращення методів ідентифікації людини [119]. Крім того, фрактальна розмірність використовувалася в ідентифікації суб'єктів на основі ЕЕГ, демонструючи її універсальність у різних біометричних модальностях [120].

Таким чином, фрактальна розмірність описує унікальні характеристики біометричних сигналів, тому необхідно дослідити введення фрактальної розмірності, як додаткової інформаційної ознаки в системи верифікації на основі нейронних мереж глибокого навчання.

1.5 Визначення характеристик користувача для неперервної верифікації

Цей підрозділ призначений для загального огляду сенсорів та давачів, які можуть зчитувати біометричні характеристики в неперервному режимі. Розглянемо різні типи давачів, включаючи акселерометри, гіро-сенсори, та інші пристрої введення як мишу та клавіатуру. Крім того, буде розглянуто методики зчитування даних з цих давачів, включаючи частоту давача, точність, а також алгоритми обробки і аналізу цих даних.

Метою цього підрозділу є надання загального розуміння ролі давачів у неперервних системах верифікації, а також їх потенціал в підвищенні рівня безпеки цифрових систем.

Окрім акселерометрів та гіроскопів, для біометричної верифікації також можна використовувати інші давачі, такі як фотоплетизмографія (ФПГ), електрокардіограма (ЕКГ) та шкірно-гальванічна реакція (ШГР) [121]. Ці давачі вловлюють фізіологічні сигнали, такі як частота серцевих скорочень, кровотік і провідність шкіри, які можуть бути унікальними для людини та використовуватися для аутентифікації.

Перед розглядом конкретних типів сенсорів, важливо звернути увагу на загальні характеристики, які є важливими для характеристики сенсора.

Калібрування

Калібрування є процедурою корекції та валідації сенсора з метою підвищення точності вимірювань. Процес калібрування може включати декілька етапів:

Оцінка відхилень: Перший крок полягає у вимірюванні відхилень вихідного сигналу при відомих умовах.

Корекція параметрів: Відомі відхилення можна виправити шляхом математичних корекцій в алгоритмі обробки даних.

Валідація: Після корекцій, необхідно провести додаткові вимірювання для підтвердження точності.

Шум

Шум представляє собою несистематичні варіації в сигналі сенсора, які можуть походити від різних джерел. Детальніше, шум може бути класифікований як:

Внутрішній шум: Шум, що виникає від електронних компонентів сенсора.

Зовнішній шум: Шум, зумовлений зовнішніми факторами, такими як температурні зміни чи електромагнітні поля.

Спектральна щільність шуму: Це метрика, яка вимірює величину шуму відносно частоти.

Чутливість

Чутливість сенсора є мірою ефективності перетворення вхідного фізичного стимулу в вихідний електричний сигнал. Характеристики:

Лінійна чутливість: Вимірюється як величина зміни вихідного сигналу на одиницю зміни вхідного стимулу в лінійному діапазоні роботи.

Порогова чутливість: Мінімальний стимул, який необхідний для реєстрації вихідного сигналу.

Динамічний діапазон: Діапазон вхідних стимулів, на які сенсор може реагувати.

Ці характеристики безпосередньо впливають на якість сигналу зчитаного з давача та можливості побудови точної системи біометричної верифікації.

Акселерометр

Акселерометри - це давач, які вимірюють сили прискорення. Вони зазвичай використовуються в переносних пристроях для збору даних про рух і орієнтацію. У контексті біометричної верифікації акселерометри можна використовувати для фіксації унікальних моделей руху або характеристик ходи людини [121]. Ця інформація може бути використана як біометричний вхід для аутентифікації.

Акселерометр вимірює зміну швидкості вздовж однієї осі (рис.1.1). Значення, про які повідомляють акселерометри, вимірюються з кроком гравітаційного прискорення, причому значення 1,0 означає прискорення 9,8 метрів на секунду (на секунду) у заданому напрямку. Залежно від напрямку прискорення значення давача можуть бути позитивними або негативними.

Рисунок 1.1. Демонстрація осі акселерометра на загальному смарт-годиннику/браслеті.

В мобільних пристроях часто використовуються акселерометри MEMS типу. MEMS (Micro-Electro-Mechanical Systems) акселерометри є компактними сенсорами, що вимірюють прискорення за допомогою мікроелектромеханічних структур. Зазвичай вони використовують кремнієві пластинки та електростатичні поля для визначення змін у русі. Ці акселерометри є дуже популярними в мобільних пристроях, автомобільних системах, та медичному обладнанні через їх малі розміри, низьку вартість і високу точність. Приклад показів акселерометра можна побачити у додатка А, рис. А.1., А.2 (а)

Гіроскопи, з іншого боку, є давачами, які вимірюють кутову швидкість або обертання. Вони часто використовуються в поєднанні з акселерометрами для отримання більш детальних даних про рух. Гіроскопи можуть надавати інформацію про орієнтацію та рух частин тіла людини, яку можна використовувати як біометричний вхід для верифікації [122]. Гіроскоп зазвичай видає дані у градусах на секунду або радіанах на секунду. Коли пристрій стоїть нерухомо, гіроскоп має показати нуль. Якщо пристрій повертають, гіроскоп реєструє це рух як позитивну або негативну залежно від напрямку та осі обертання. Приклад значень наведено у додатку А, рис. А.2 (б).

Магнетометр вимірює силу та напрямок магнітного поля. Його часто використовують як компас, оскільки він може визначати орієнтацію пристрою відносно магнітних полів Землі. Він вимірює значення у теслах або мікротеслах. Магнетометр дає змогу пристрою зорієнтуватися в просторі, вказуючи напрямок на північ, і може вимірювати відхилення від земного магнітного поля, що є корисним у навігації та калібруванні. Приклад значень наведено у додатку А, рис. А.2 (в).

1.6. Виклики та майбутні напрямки

Конфіденційність і безпека в автентифікації на основі глибокого навчання . Конфіденційність і безпека мають першочергове значення для безперервної автентифікації на основі глибокого навчання. Моделі глибокого навчання часто вимагають доступу до конфіденційних біометричних і поведінкових даних, що викликає занепокоєння щодо конфіденційності та захисту даних. Змагальні атаки, такі як ненавмисний витік функцій і визначення членства, можуть використовувати вразливості в моделях глибокого навчання та скомпрометувати конфіденційність даних користувача [123]. Дослідники запропонували різні методи для вирішення цих проблем, включаючи гомоморфне шифрування та системи аутентифікації на основі ризику, щоб захистити конфіденційність і безпеку моделей глибокого навчання та даних користувачів [124], [125]. Крім того, інтеграція механізмів збереження конфіденційності,

таких як диференціальна конфіденційність або безпечне багатостороннє обчислення, може ще більше посилити гарантії конфіденційності систем неперервної автентифікації [124]. Вкрай важливо розробити надійний захист від атак на конфіденційність і переконатися, що моделі глибокого навчання стійкі до ворожих спроб отримати конфіденційну інформацію [126]. Віддаючи пріоритет конфіденційності та безпеці, системи неперервної аутентифікації на основі глибокого навчання можуть надати користувачам надійну та безпечну аутентифікацію [66].

Узагальнення та стійкість моделей глибокого навчання для різних користувачів і сценаріїв . Щоб забезпечити точну автентифікацію, потрібне глибоке навчання для створення моделей, які можуть працювати для різних користувачів і ситуацій. Ці моделі використовують величезні набори даних, щоб навчитися відрізняти справжніх користувачів від фальшивих. Однак дуже важливо переконатися, що ці моделі можуть добре узагальнювати невидимі дані та різні популяції користувачів [127]. Дослідники досліджували методики перенесення навчання та адаптації домену, щоб вирішити цю проблему. Трансферне навчання дозволяє моделям використовувати знання, отримані з одного завдання чи набору даних, для покращення продуктивності в іншому, але пов’язаному завданні чи наборі даних. Це може допомогти покращити узагальнення моделей глибокого навчання в безперервній автентифікації [128]. Методи адаптації домену спрямовані на подолання розриву між розподілом даних навчання та тестування, що дозволяє моделям добре працювати в різних сценаріях або групах користувачів [127].

Крім того, вкрай важливо враховувати надійність моделей глибокого навчання проти агресивних атак. Змагальні атаки передбачають навмисне маніпулювання вхідними даними, щоб обдурити модель і обійти систему автентифікації. Змагальні приклади можуть бути створені для використання уразливостей у моделі та призвести до неправильних рішень щодо автентифікації [128]. Дослідники запропонували різні захисні механізми, такі

як змагальне навчання та надійна оптимізація, для підвищення стійкості моделей глибоко-го навчання проти змагальних атак [128].

Інтеграція глибокого навчання з іншими методами автентифікації . Коли мова йде про безперервну автентифікацію на основі глибокого навчання, важливо інтегрувати моделі глибокого навчання з іншими методами автентифікації, оскільки хоча й результати продуктивності є точними, чутливість системи до помилок моделі дуже висока. Таким чином, поєднання моделей глибокого навчання з традиційними методами автентифікації на основі знань, такими як паролі або токени, для створення систем багатофакторної автентифікації дозволяє нам розпочати впровадження рішень глибо-кого навчання. Це посилить безпеку та захистить користувачів від можливих помилок моделі. Крім того, моделі глибокого навчання можна поєднувати з іншими біометричними модальностями, такими як відбитки пальців або розпізнавання обличчя, для створення мультимодальних систем автентифікації з метою підвищення точності, надійності та стійкості до атак спуфінгу [129]. Моделі глибокого навчання ефективні в обробці злиття різних модальностей і можуть забезпечити повне представлення ідентичності користувача.

Нові тенденції та майбутні напрямки досліджень у глибокому навчанні для неперервної автентифікації. У глибокому навчанні для неперервної автентифікації варто вивчити кілька нових тенденцій і майбутніх напрямків досліджень. Однією з таких тенденцій є розробка методів збереження конфіденційності для систем аутентифікації на основі глибокого навчання. Під час роботи з конфіденційними біометричними та поведінковими даними виникають проблеми щодо конфіденційності. Дослідники запропонували такі методи, як безпечне обчислення, федеративне навчання та диференціальна конфіденційність, щоб захистити конфіденційність користувачів, зберігаючи при цьому ефективність систем аутентифікації [130]. Інший напрямок досліджень — це дослідження зрозумілих моделей глибокого навчання для неперервної автентифікації. Зрозумілі моделі дають змогу зрозуміти процес прийняття рішень у системі автентифікації, дозволяючи користувачам і

системним адміністраторам розуміти результати системи та довіряти їм, що може допомогти виявити потенційні вразливості чи упередження в системі та підвищити прозорість.

Крім того, інтеграція моделей глибокого навчання з периферійними обчисленнями та технологіями блокчейн може підвищити безпеку та конфіденційність систем неперервної автентифікації. Граничні обчислення – це процес, у якому дані обробляються та аналізуються на межі мережі, таким чином допомагаючи зменшити затримку та зберегти конфіденційність, зберігаючи конфіденційні дані локально [131]. Використовуючи технологію блокчейн, можна створити децентралізовану та безпечну систему для зберігання та перевірки даних автентифікації, яка гарантує, що ідентифікаційні дані користувачів залишаються незмінними та зберігається їх цілісність [131]. Конфіденційність і безпека мають вирішальне значення для неперервної автентифікації на основі глибокого навчання. Забезпечення узагальнення та надійності моделей глибокого навчання, інтеграція глибокого навчання з іншими методами автентифікації та вивчення нових тенденцій, таких як методи збереження конфіденційності та пояснювані моделі, є важливими напрямками дослідження. Крім того, розробка “легких” моделей та інтеграція глибокого навчання з периферійними обчисленнями та технологіями блокчейн може додатково підвищити безпеку та конфіденційність систем неперервної автентифікації.

Для того, щоб системи неперервної автентифікації працювали на пристроях з обмеженими обчислювальними ресурсами, наприклад смартфонах і носимих пристроях, необхідна розробка так званих “легких” (lightweight) моделей глибокого навчання. Це зробить можливим розгортання неперервної автентифікації на таких пристроях з забезпеченням необхідної продуктивності [132]. Для побудови таких моделей необхідно визначити відповідні вимоги пристрою та їх допустимі граничні значення. Для конкретного випадку система верифікації при створенні моделі повинна враховувати допустимі граничні значення встановлених обмежень (об’єм пам’яті та час висновку).

Висновки до розділу

В цьому розділі надано визначення біометричній верифікації, проаналізовано актуальність задачі, існуючі виклики та проблематику. Було розглянуто та описано приклади різних типів біометричних систем, а саме, фізіологічних, поведінкових та мультимодальних.

Також, проведено огляд методів машинного (однокласовий SVM, ізоляційний ліс, тощо) та глибокого навчання (автокодувальники, сіамські мережі, згорткові мережі, рекурентні мережі, трансформери) та їх застосування для побудов систем біометричної верифікації. Детально розглянуто застосування різних типів та архітектур нейронних мереж в задачі біометричної верифікації, проаналізовано їх переваги та недоліки. Зокрема, розглянуто автокодувальник та його різні модифікації. Цей тип нейронної мережі дозволяє навчати систему лише з даними одного класу, таким чином він не вимагає додаткового збору даних від інших користувачів та додаткової розмітки. Це дає принципову можливість загалом будувати системи верифікації, адже обмеження по даних лише з одного класу є ключовим для таких систем, проте багато моделей не здатні вирішувати таку задачу. Розглянуті також інші типи архітектур - сіамські мережі, які також мають опцію навчання лише на одному класі і застосовують метричне навчання, проте це вимагає додаткової генерації зразків даних. Окремо акцентовано увагу на використанні гібридних нейронних мереж, які дозволяють створювати більш ефективні системи верифікації, пом'якшуючи недоліки окремо взятих типів архітектур. Архітектури, як автокодувальник чи сіамська мережа, можуть складатися з різних компонентів: наприклад, автокодувальник на основі рекурентних нейронних мереж чи на основі трансформера. Це дозволить враховувати особливості вхідних даних та налаштовувати систему під конкретну прикладну задачу.

Крім того, проведено огляд використання фрактальної розмірності та її роль у аналізі та виділенні ознак зі складних біометричних сигналів. Фрактальна розмірність знаходить патерни в біометричних сигналах, та широко

застосовується в медичній сфері, для виявлення різноманітних патологічних станів та моніторингу стану пацієнта. Завдяки цьому фрактальна розмірність має великий потенціал до більш широкого застосування для систем верифікації користувача на основі біометричних сигналів, тому необхідно більш глибоко дослідити її вплив на значення метрик якості систем, що створюються.

Також було загально оглянуто сенсори та давачі, які можуть зчитувати біометричні характеристики в неперервному режимі. Було розглянуто різні типи давачів, включаючи акселерометри та гіроскопи.

Описані виклики та майбутні напрямки розробки біометричних систем на основі глибокого навчання, зокрема стійкість та надійність моделей. Розглянута можливість запуску моделей на носимих пристроях, та підтримка ефективної роботи систем в умовах обмежених обчислювальних ресурсів.

РОЗДІЛ 2
РОЗРОБКА МЕТОДОЛОГІЇ НЕПЕРЕВНОЇ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ КОРИСТУВАЧА ТА ЇЇ ЗАТОСУВАННЯ

2.1 Постановка задачі неперервної системи верифікації з використанням автокодувальників

Нейронні мережі глибокого навчання і їх моделі характеризуються взаємозалежностями та взаємозв'язками на різних рівнях обраних архітектур, їх складових і гіперпараметрів, та є об'єктами системного аналізу.

Сформулюємо постановку задачі для навчання і висновку неперервної системи автентифікації на основі автокодувальників на шаблонах руху.

Постановка завдання: необхідно побудувати та налаштувати відповідні моделі глибокого навчання, які виконуватимуть неперервну верифікацію користувача на основі показів давачів, що описують поведінкові біометричні характеристики в реальному часі.

Оскільки, сформульоване завдання є задачею системного аналізу – для її розв'язання використаємо практичну методологію, як системний інструментарій, що відзначається функціональною повнотою, логічною завершеністю, і системно-погодженим взаємозв'язком прийомів, принципів і методів[133]. Методологія повиння задовольняти наступні умови: бути масштабною, ефективною та результативною [133]. Практична методологія дослідження побудови обраної системи має включати в себе підходи, алгоритми та методи, використані для розв'язання задачі неперервної верифікації.

Порядок дій має бути наступним:

1. Визначити цілі: які критерії ефективності використовувати, а також їх цільове значення, яке має характеризувати якість роботи системи.
2. Створити початковий завершений робочий прототип верифікації користувача. На цьому етапі фіксується набір базових архітектур та їх

гіперпараметрів, визначається процес попередньої обробки даних та інформаційні ознаки (зокрема фрактальна розмірність).

3. Ітеративно реалізувати послідовні зміни, наприклад збір нових даних, коригування гіперпараметрів чи зміна алгоритмів, на основі конкретних висновків з обраного прикладного сценарію[134].

Така архітектура система верифікації має 2 фази: тренування, яке налаштовує архітектуру та параметри системи (моделі), і висновок - коли побудована система надає рішення щодо автентифікації користувача.

Таким чином, структура системи автентифікації складається з наступних блоків:

Блок зчитування та збору даних . У разі автентифікації за рухом це буде або якийсь носимий IMU, або вбудовані давачі в смартфоні чи стаціонарному пристрої.

Блок виділення ознак та моделювання. Ця частина приймає зібраний сигнал даних, обробляє його, додатково обчислює фрактальна розмірність, як інформаційна ознака, та перетворює на скаляр або вектор ознак.

Блок прийняття рішень. Враховуючи перетворені вхідні дані від попереднього блоку, ця модель забезпечує рішення системи автентифікації, чи є користувач справжнім, чи шахраєм. На етапі тренування встановлюється точка прийняття рішення на етапі висновку.

Високорівнева схема системи аутентифікації для етапу висновку та тренування зображена нижче (див. рис. 2.1).

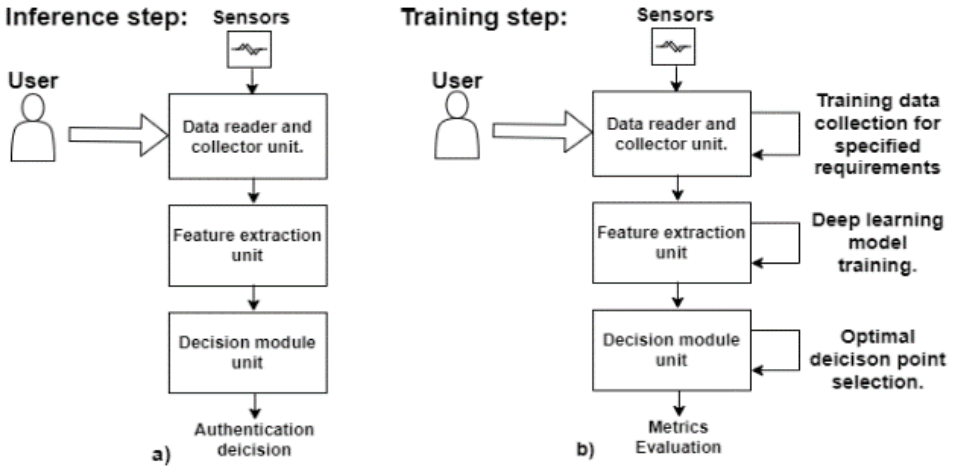


Рисунок 2.1. Схема етапів автентифікації (a) і навчання (b).

Загальний опис вхідних даних до кожного компоненту систему верифікації:

- ***Необроблений вхідний сигнал:*** заданий сигнал часового ряду від одного чи кількох давачів (наприклад, акселерометра або акселерометра з гіроскопом) із певною частотою дискретизації (у Гц, означає кількість наданих записів давача за секунду).
- ***Збір тренувальних даних:*** збирається сигнал давача за час *t* для різних типів діяльності *a* .
- ***Вхідні дані етапу тренування:*** розділений сигнал давача часового ряду на вікна тривалістю *d* з перекриттям *o*.
- ***Вхідні дані етапу висновку:*** вікно *w* тривалості *d* сигналу давача.

Етап тренування:

Спочатку необхідно обрати архітектуру моделі для тренування.

$$F = \{b, a, d, l, p\}, \quad (2.1)$$

де *b* – необхідність проведення батч нормалізації, *a* - вибір функції активації, *d* - розмірність внутрішніх шарів, *l* – обрана функція похибки, *p* – значення дропауту. Кількість параметрів може надалі уточнюватися та розширюватися.

Маємо навчальний набір вікон розміром N, $\{w_i^d\}$, де i=1,2…N. Далі виділяються ознаки та тренується обрана модель. У описаному випадку

використовується модель з автокодувальником, тому мінімізується похибка реконструкції.

$$E(w) = \sum_{i=1}^{N} \left\| w_i^d - \widetilde{w_i^d} \right\| \to \min \ , \qquad (2.2)$$

де $\tilde{w}_i^d$ реконструйований вихід мережі.

Вихід автокодувальника надходить в блок прийняття рішень, і надалі обчислюється значення точки прийняття рішення. Це може бути підхід, заснований на подібності, або більш простий, як KNN, або з моделлю глибокого навчання, як сіамська мережа або дуальний енкодер. Щоб забезпечити рішення системи автентифікації, вибирається порогове значення перед висновком системи, яке і визначить, чи є користувач легітимним або самозванцем.

Сформулюємо етап висновку описаної системи верифікації в загальному випадку:

$$y_t = D\left(f\left(w_t^d\right)\right) \qquad (2.3)$$

де y_t — це вихід системи автентифікації (бінарний або ймовірнісний), D — наш модуль прийняття рішень, який споживає виділені ознаки за допомогою f із вікна часових рядів давачів w^d протягом тривалості d для моменту часу t. В запропонованій системі в якості f можуть застосуватися різні типи автокодувальників, зокрема стискуючий, рекурентний, варіаційний та інші.

У попередніх дослідженнях [31],[101] використовувалося значення похибок реконструкції для встановлення порогів верифікації. Результат верифікації можна отримати з наступної функції прийняття рішення:

$$\sigma(E(w), \theta *) = \begin{cases} 1\ (genuine)\ if\ E(w)\ \leq \theta * \\ 0\ (impostor)\ otherwise \end{cases} \qquad (2.4)$$

Вибір порогового значення можна використовувати або для значень виходу, наданих автокодувальником, але також $E(w)$ можна замінити будь-якою іншою функцією подібності. Варто зазначити, що підхід із вибором оптимального порогу з метою досягнення оптимального значення для певної метрики в деяких випадках може призвести до перетренування системи та зашкодити здатності моделі до узагальнення.

Загалом, вибір оптимального (квазі-оптимального) значення для прийняття рішення залежить від багатьох показників і оптимізується емпіричним чином підбором архітектури, її елементів (функції активації, кількість нейронів, нормалізація шарів, тощо). Підбір параметрів архітектури можна реалізувати випадковим чином або розділити архітектуру на деякі умовні блоки, кожен з яких характеризується своїм набором параметрів, що описано в підрозділі 3.3. Також, порогове значення можна вибрати за деякими незалежними від даних правилом або евристичними методами, наприклад, беручи середню помилку зі стандартним відхиленням або персентиль (50, 95, 99) для тестового датасету та встановлюючи обчислене значення як порогове значення.

2.2 Опис датасетів

Single Chest-Mounted Accelerometer Dataset (SCMA); Набір даних було взято з репозиторію UCI — архіву публічних наборів даних для цілей машинного навчання [135].

Набір даних містить дані акселерометра 15 добровольців. Дані містять значення осей x, y, z. Частота дискретизації акселерометра становить 52 Гц, тому отримуємо 52 рядки значень кожну секунду. Крім того, дані містять 7 типів діяльності (вставати, ходити і підніматися і спускатися сходами, стояти, ходити, підніматися і спускатися сходами, ходити і розмовляти з кимось, розмовляти стоячи).

H-MOG Dataset: набір даних із відкритим кодом [136], [137], широкомасштабне дослідження користувачів за участю 100 волонтерів для збору широкого спектру сигналів про поведінку користувача смартфона, включаючи дотик, жести та паузи користувача, а також рух і орієнтацію телефону. Були записані дані з трьох сценаріїв користування смартфоном: (1) читання документа; (2) створення тексту (письмо); (3) навігація на карті для визначення місця призначення.

Набір даних містить кілька модальностей від різних давачів. Для наших експериментів було обрано покази акселерометра, гіроскопа та магнетометра.

Набір даних містить кілька комбінованих видів діяльності та фізичної активності, як-от читання та ходьба, читання та сидіння, письмо та ходьба, письмо та сидіння, навігація по карті та ходьба та навігація по карті та сидіння – загалом 6 типів діяльності.

2.3 Опис застосованих методів та інструментів

Алгоритми реалізовувалися за допомогою мови Python на бібліотеці Keras і бекенді Tensorflow, Numpy, Scipy, Scklearn, Pandas, Matplotlib.

Усі моделі були навчені допомогою оптимізатора Adam на графічному процесорі GeForce RTX 2070.

Описи реалізацій нейронних мереж глибокого навчання за допомогою Keras та Tensorflow наведені в підручниках [].

Програмна реалізація наведена к додатку В.

2.4 Метрики якості для біометричної системи верифікації

В якості метрик оцінки моделі [138] були обрані EER (рівна частота помилок), FAR (False Acceptance Rate) і FRR (False Rejection Rate), Recall (повнота) та AUC (площа під кривою), які є типовими для оцінки якості біометричної системи.

- *FAR=FPR=FP / FP+TN;*

  Пояснення: Оцінює відсоток неправильно прийнятих доступів.

  Важливість: Низький FAR важливий для безпеки, оскільки він показує, наскільки система здатна відмовляти несанкціонованим користувачам.

- *FRR=FNR=FN / TP+FN;*

  Пояснення: Оцінює відсоток відхилених легітимних спроб доступу.

  Важливість: Низький FRR забезпечує зручність користувача, мінімізуючи відхилення легітимних спроб доступу.

- *EER = |FAR + FRR| / 2,* де |FAR + FRR| є найменшим значенням [138]
  Пояснення: Представляє точку, на якій FAR і FRR зрівнюються.
  Важливість: EER дозволяє зробити загальну оцінку компромісу між безпекою і зручністю користувача.

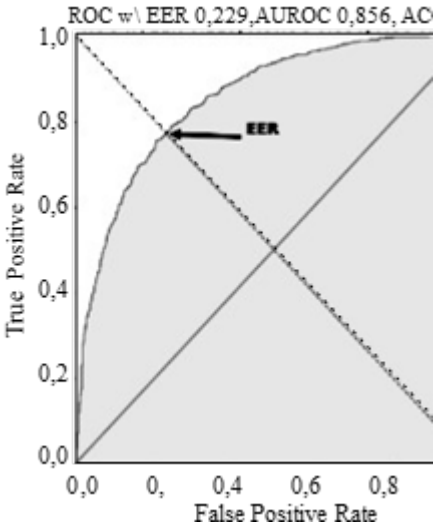


Рисунок 2.2. Ілюстрація розрахунку EER з [19]

- *Recall = TP / (TP + FN)*
  Пояснення: Вимірює відсоток правильно ідентифікованих позитивних випадків.
  Важливість: Висока чутливість (recall) гарантує, що система ефективно ідентифікує справжніх користувачів.
- AUC (Area Under the Curve):
  Пояснення: Метрика, яка вимірює здатність моделі відрізняти позитивний клас від негативного.
  Важливість: Високий AUC показує, що модель добре відрізняє між класами на всіх порогових значеннях, що дозволяє гнучко налаштувати систему.

Використання цих метрик забезпечує комплексну оцінку ефективності системи біометричної верифікації, враховуючи як безпеку, так і зручність користувача.

При остаточній оцінці моделі метрики порівнюються в наступному пріоритеті: EER, AUC, та оцінюється компроміс між FAR та FRR.

В якості обраного порогу верифікації в експериментах використовувалася наступна формула:

$$T = \sum_{i=1}^{N} \frac{MAE_i}{N} + std(MAE_i), \quad (2.5)$$

де MAE — середня абсолютна похибка між базовою істинністю та прогнозованою вибіркою, std — стандартне відхилення, а N — кількість вибірок у навчальному наборі даних.

Для експрес-оцінки якості моделі запропоновано інтерфейс візуалізації результатів, представлений у додатку Б, де візуалізуються покази похибок реконструкції автокодувальника на всьому тестовому наборі даних і значення порогу верифікації. По наданій візуалізації чітко розділяються результати роботи системи для різних користувачів та оцінюється якість обраного порогу верифікації (областю значень є величини похибок реконструкції актокодувальника, а поріг обчислюється за формулою 2.5).

2.4 Порівняльний аналіз існуючих підходів вирішення задачі верифікації

Мета: для розуміння переваг та недоліків існуючих підходів до побудови неперервної системи верифікації з обмеженнями на відсутність даних “чужого” класу та виклики для генерації ознак складних біометричних сигналів. Також, мета полягає в порівнянні статистичних методів машинного навчання з нейронними мережами глибокого навчання.

Опис:

На SCMA датасеті було проведено порівняльний аналіз різних типів автокодувальників для вирішення задачі біометричної верифікації.

Оскільки в [139] перевірка користувача відбувається після вирішення задачі розпізнавання активності людини (HAR) на шаблонах ходьби, спробуємо перевірити роботу алгоритму верифікації користувача лише на певному

шаблоні руху. Отже, фактично буде визначатися, яким чином якась людина йде або йде та розмовляє з кимось тощо. Найбільше зразків даних користувачів було з типом діяльності “робота за комп’ютером”, тому моделі в даному експерименті навчалися на цьому типі діяльності.

Для моделей глибокого навчання дані розділяються на вікна довжиною 52, та перекриттям 50%.

Ми порівнюємо три види автокодувальників:

- варіаційний автокодувальник LSTM;
- контрактивний (contractive) автокодувальник LSTM;
- стискуючий автокодувальник LSTM.

За похибку використовувалася середня абсолютна похибка (MAE). Моделі тренувалися в 10 епох з оптимізатором Adam.

Архітектура автокодувальників показана нижче на рис. 2.3 та на таблиці нижче.

Таблиця 2.1. – Архітектура LSTM автокодувальника

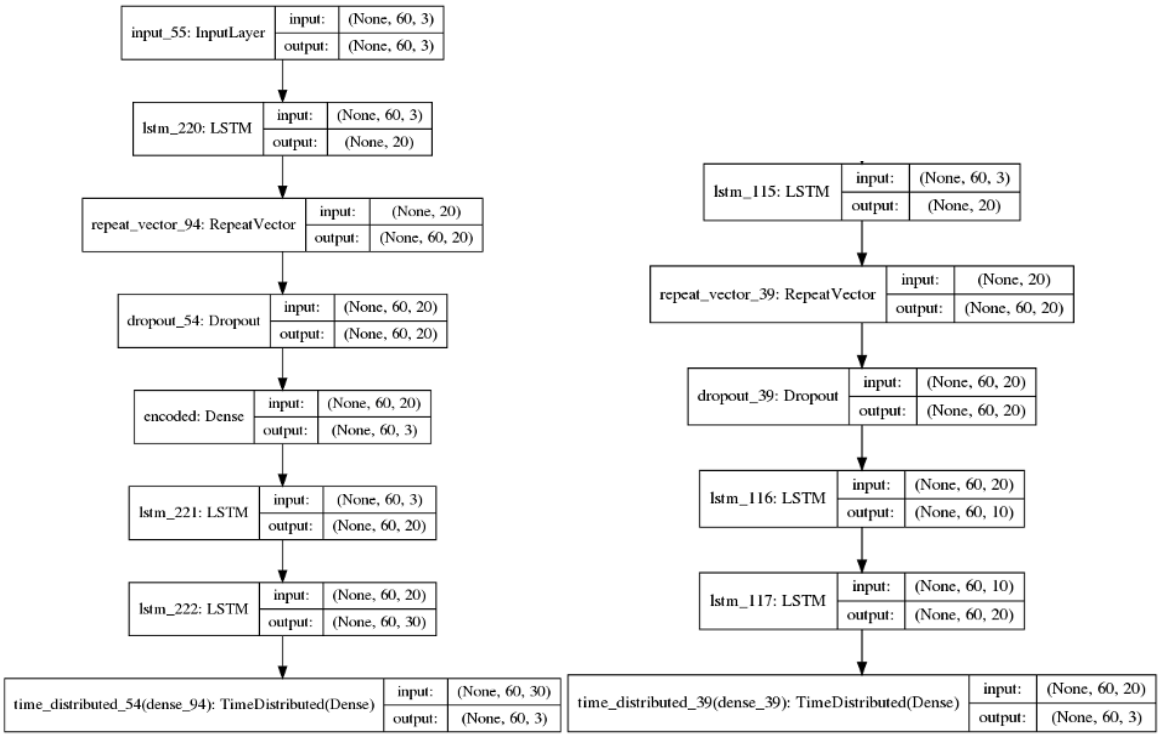
Type	**Output Shape**	**# of Params**
InputLayer	(None, 52, 2)	0
LSTM	(None, 24)	2592
Dense	(None, 12)	300
Dense	(None, 12)	300
Lambda	(None, 12)	0
RepeatVector	(None, 52, 12)	0
LSTM	(None, 52, 24)	3552
LSTM	(None, 52, 2)	216

Моделі на основі автокодувальників порівнювали з однокласовими опорними векторними машинами (SVM) і ізоляційним лісом (Isolation Forest). Для однокласового SVM та ізоляційного лісу використовувалися не необроблені вихідні дані, а різні типи ознак (у часовій і частотній області). Ознаки розріховувалися по прикладу з [16].

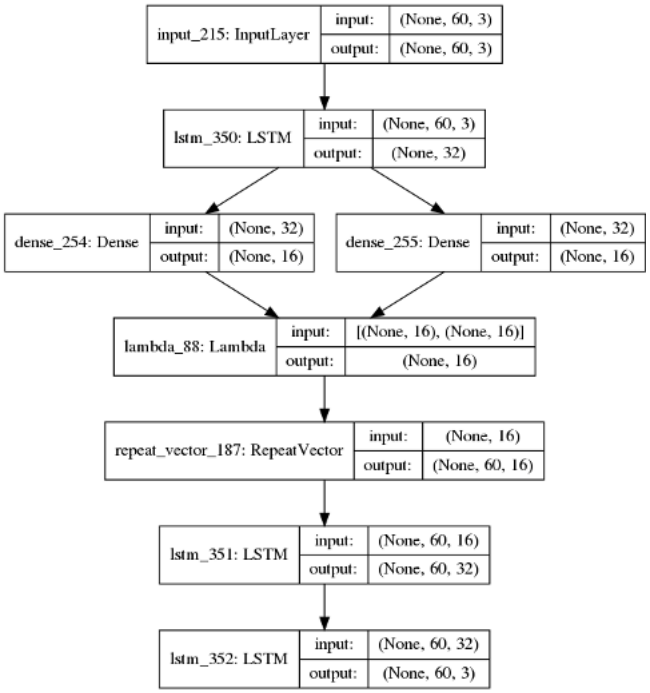
Результати експерименту:

Чутливість для позитивного класу для кожного користувача та порівняння з однокласовим SVM та ізольованим лісом наведено в таблиці 2.2 нижче.

Крім того, через невисоку різницю в показниках чутливості (recall) в моделях автокодувальників порівнюються їх значення площі під кривою. Крива ROC і значення AUC показані на рис. 2.4 та рис.2.5.



а)б)



в)

Рисунок 2.3 Архітектура а) неповного автокодувальника, б) контрактивного автокодувальника, в) варіаційного автокодувальника

Таблиця 2.2. Значення чутливості (recall) для позитивного класу

Користувач	LSTM AE	LSTM VAE	LSTM CAE	OC-SVM	IF
Користувач 1	0,99	0,99	0,99	0,63	0,74
Користувач 2	0,99	0,99	0,66	0,42	0,73
Користувач 3	0,62	0,96	0,86	0,67	0,74
Користувач 4	0,44	0,58	0,66	0,27	0,74
Користувач 5	0,94	0,94	0,95	0,67	0,78
Користувач 6	0,87	0,91	0,91	0,49	0,74
Користувач 7	0,91	0,92	0,90	0,65	0,65
Користувач 8	0,97	0,97	0,97	0,39	0,83
Користувач 9	0,50	0,55	0,56	0,27	0,76
Користувач 10	0,94	0,97	0,97	0,29	0,83
Користувач 11	0,98	0,98	0,98	0,68	0,77
Користувач 12	0,58	0,41	0,46	0,40	0,84
Користувач 13	0,77	0,27	0,59	0,20	0,88
Користувач 14	0,76	0,73	0,82	0,32	0,72
Користувач 15	0,96	0,98	0,98	0,66	0,79
Середнє значення	0,814	0,81	0,82	0,47	0,77

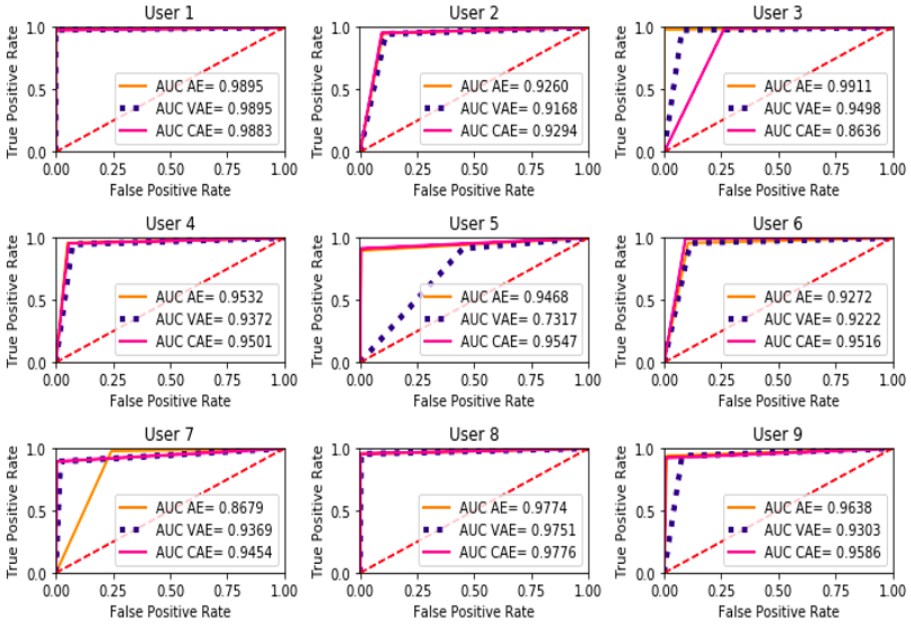


Рисунок 2.4. Крива ROC і показник AUC для моделей на основі автокодувальника (користувачі 1-9)

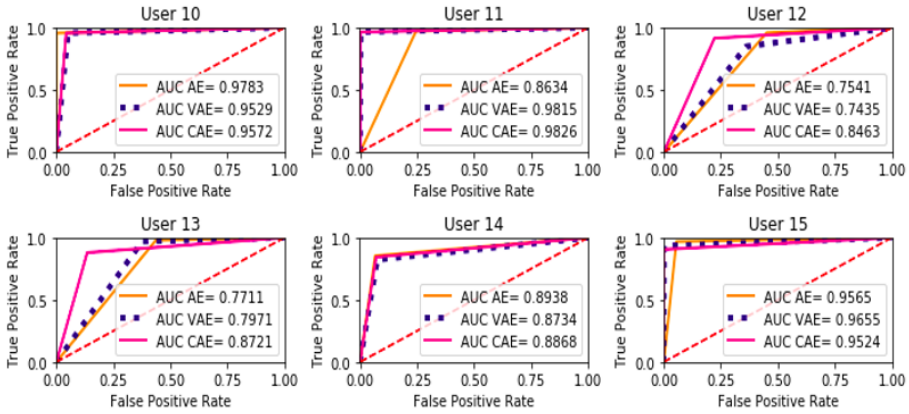


Рисунок 2.5. Крива ROC і показник AUC для моделей на основі автокодувальника (користувачі 10-15 років)

У таблиці 2.2 можемо побачити, що найкращий результат показав рекурентний контрактивний автокодувальник з середнім значенням чутливості (recall) 0,82 для позитивного класу.

Таблиця 2.3. Середній рівень помилок (EER) для кожної моделі на основі автокодувальника

	LSTM AE	LSTM VAE	LSTM CAE
EER	0.125	0.111	0.106

Аналізуючи значення рівня рівних помилок (EER) в таблиці 2.3, можна помітити, що контрактивний і варіаційний автокодувальники мають близьку точність.

На рисунках 2.4 та 2.5 зображено криві (ROC) та відповідні значення площі під кривою (AUC) для кожного типу автокодувальників, досліджених в експерименті. Показник AUC дозволяє порівнювати моделі в цілому, тоді як чутливість розраховується для певного фіксованого порогу. Таким чином, AUC є кращим показником для порівняння моделей, тоді як чутливість варто розглядати більше як кінцевий ключовий показник ефективності (KPI) для конкретного застосування в бізнес-задачі. Результати показують, що значення AUC відрізняються залежно від користувача, тому вибір моделі доцільно

здійснювати адаптивно на основі метрик якості, частоти помилок і обсягу даних для конкретного користувача. Проте контрактивний автокодувальник все ж демонструє найвищі метрики, оскільки має найкращий результат серед 8 з 15 користувачів.

Обговорення результатів:

Результати показують, що рекурентні автокодувальники демонструють надійну продуктивність з високими показниками. Проте результати можуть відрізнятися залежно від обсягу даних та конкретного користувача. Для вибору найкращої моделі для певного користувача можна керуватися показниками чутливості та площі під кривою (AUC). Порівняно з однокласовим SVM та ізоляційним лісом, де ознаки визначаються вручну, автоматичне вилучення ознак автокодувальником є досить ефективним, що важливо для універсальності та портативності на різних типах даних і датчиків.

Найнадійніші результати продемонстрував рекурентний контрактний автокодувальник. Однак слід враховувати погіршення розділюваності даних зі збільшенням кількості користувачів, що потребує подальших досліджень.

Наприклад, можна кластеризувати користувачів у групи та оцінювати модель лише в межах певної групи найбільш схожих користувачів. Таким чином, обирається модель, яка найкраще відрізняє "легітимного" користувача від інших, навіть схожих. Необхідно також розглянути потенційні проблеми реального використання, такі як велика кількість схожих користувачів, зашумленість даних акселерометра, висока затримка часу висновку моделі тощо. Слід також враховувати інші чинники для налаштування системи під конкретні біометричні цілі. Проведений порівняльний аналіз демонструє, що використання нейронних мереж глибокого навчання без вчителя може бути успішно застосоване для побудови систем біометричної неперервної верифікації.

2.5 Прикладні сценарії та реалізації побудови моделей по загальній методології

Відповідно до формули 2.1 розглянемо побудову конкретних моделей поетапно та значення відповідних їм критеріїв якості. В результаті буде отримана вдосконалена архітектура нейронної мережі для конкретного прикладного сценарію.

На основі вищенаведених розрахунків для прикладного сценарію біометричної верифікації на показах акселерометра було встановлено наступні параметри структури моделі:

- b – наявність батч-нормалізації,
- a – вибір функції активації: relu (rectified linear unit), tanh (гіперболічний тангенс).,
- d – розмірність внутрішніх шарів, кількість нейронів.
- l – функція похибки: MAE, MSE.
- p – dropout: 0.0, 0.4, 0.6, 0.8.

Метод побудови квазі-оптимальної архітектури моделі (“жадібний” алгоритм). Послідовна параметризація нейронних мереж глибокого навчання.

Для подальшого вдосконалення та уточнення методології, запропонованої в [134] побудови моделей систем верифікації, запропонований підхід, який базується на послідовній оптимізації складових моделі. Спочатку фіксується тип загальної архітектури моделі і набір можливих значень вектора параметрів згідно формули 2.1. Потім послідовно оптимізується кожна складова базової архітектури і отримується її оптимальний варіант. На основі отриманих оптимальних складових архітектури будуємо квазі-оптимальну загальну архітектуру. Оптимальний варіант на кожному кроці обирається відповідно до значень метрик якості наведених в підрозділі 2.3 та часу висновку.

Метод випадкового пошуку архітектури моделі.

На відміну від “жадібного” алгоритму, відбувається за алгоритмом описаний в [134]

Прикладний сценарій побудови вдосконаленої архітектури нейронної мережі

Для розрахунків в якості прикладу було обрано датасет SCMA [134] (покази нагрудного акселерометра, 15 користувачів, 7 видів фізичних активностей).

Критерії оцінки якості системи - метрики, описані в підрозділі 2.4.

Час висновку виступає загальним критерієм якості роботи системи.

Базова архітектура наведена в додатку Г, таблиця Г.1.

Крок 1. Розраховуємо критерії якості з та без батч-нормалізації. Приклад архітектури з батч-нормалізацією наведено в додатку Г, таблиця Г.2.

Таблиця 2.4 Середні значення EER, AUC, FRR і FAR для LSTM автокодувальника з та без батч-нормалізації

Метрика якості	Без батч-нормалізації	З батч-нормалізацією	Різниця - %
Середній EER	0.158	0.175	+10.76%
Середня AUC	0.8967	0.859	-4.20%
Середній FAR	0.0211	0.1159	+449,29%
Середній FRR	0.1854	0.1641	-11.49%

Розрахунки показують, що архітектура без батч-нормалізації досягає більш точних результатів, тому фіксуємо її для наступного кроку.

Крок 2. Розраховуємо критерії якості з різними функціями активації, а саме tanh та relu.

Таблиця 2.5 Середні значення EER, AUC, FRR і FAR для LSTM автокодувальника з різними функціями активації

Метрика якості	ФА - tanh	ФА - relu	Різниця - %
Середній EER	0.158	0.143	-9.49%
Середня AUC	0.8967	0.898	+0.14%

Середній FAR	0.0211	0.03645	+72.75%
Середній FRR	0.1854	0.159	-14.24%

Розрахунки показують, що архітектура з функцією активації relu досягає більш точних результатів.

Крок 3. Розраховуємо критерії якості з різними розмірностями внутрішніх шарів. Приклад архітектури наведено в додатку Г, таблиця Г.3.

Таблиця 2.6 Середні значення EER, AUC, FRR і FAR для LSTM автокодувальника з різними розмірностями внутрішніх шарів

Метрика якості	Розмірність – (20,10)	Розмірність – (30,20)	Різниця - %
Середній EER	0.143	0.1402	-1.96%
Середня AUC	0.898	0.902	+0.45%
Середній FAR	0.0364	0.0495	+36.00%
Середній FRR	0.1590	0.1536	-3.40%

Розрахунки показують, що архітектура з розмірністю шару_1 – 30 нейронів та шару_2 – 20 нейронів, показують більш точні результати при фіксованих попередніх налаштованих параметрах.

Крок 4. Розраховуємо метрики якості з різними функціями втрат, а саме MAE або MSE.

Таблиця 2.7 Середні значення EER, AUC, FRR і FAR для LSTM автокодувальника з різними функціями втрат

Метрика якості	Loss function - MAE	Loss function - MSE	Різниця - %
Середній EER	0.1402	0.1479	-5.49%
Середня AUC	0.902	0.8941	+0.88%
Середній FAR	0.0495	0.0679	+37.17%
Середній FRR	0.1536	0.1438	-6.38%

Розрахунки показують, що архітектура з функцією втрат MAE досягає більш точних результатів при фіксованих попередніх налаштованих параметрах.

Крок 5. Розраховуємо критерії якості з різними значенням dropout.

Таблиця 2.8 Середні значення EER, AUC, FRR і FAR для LSTM автокодувальника з різними значенням dropout.

Метрика якості	Dropout-0.4	Dropout – 0.0	Dropout – 0.8	Dropout – 0.6
Середній EER	0.1402	0.178	0.1238	0.147
Середня AUC	0.902	0.876	0.905	0.883
Середній FAR	0.0495	0.0402	0.063	0.1009
Середній FRR	0.1536	0.207	0.126	0.1330

Розрахунки показують, що архітектура з значенням dropout 0.8 досягає більш точних результатів при фіксованих попередніх налаштованих параметрах.

Для обраного прикладу на останньому кроці отримуємо вдосконалену архітектуру нейронної мережі з наступними значеннями параметрів структури моделі: *b* – відсутність батч-нормалізації, *a* – функція активації relu, *d* - розмірність шарів (шар_1: 30 нейронів, шар_2: 20 нейронів), *l* – функція втрат MAE, *p* – значення dropout 0.8.

Зафіксована архітектура, яку ми отримуємо в результаті, після налаштування кожного гіпепараметру є раціональною архітектурою по значенням критеріїв якості.

Висновки до розділу

В даному розділі сформулювано, визначено та запропоновано постановку проблеми. Набула подальшого розвитку методологія для етапів тренування та висновку неперервної системи автентифікації на базі автокодувальників на шаблонах руху людини. Детально описано ключові компоненти системи, а саме: збір даних, виділення ознак і блоки прийняття рішень та описані етапи тренування і висновку. Також, було формалізовано основні етапи роботи системи, зокрема мінімізацію похибки і вибір порогових значень.

Описано метрики якості, які використовуються для оцінки ефективності системи верифікації та запропоновано інтерфейс візуалізації для експрес-оцінки якості роботи системи.

Проведено порівняльний аналіз різних типів автокодувальників з класичними методами машинного навчання, як-от однокласові опорні машини векторів та ізоляційний ліс (Isolation Forest). Показано суттєву перевагу застосування автокодувальників над класичними методами машинного навчання, наприклад отримуємо на 7% вищу чутливість (recall) в порівнянні з ізоляційним лісом і на 75% вищу чутливість (recall) в порівнянні з однокласовими опорними машинами векторів.

Наведено розрахунки побудови конкретних прикладних сценаріїв відповідно до удосконаленої методології побудови систем верифікації. Реалізований емпіричний підхід послідовного підбору квазі-оптимального вектору параметрів архітектури моделі для задачі верифікації. Для обраного прикладного сценарію запропонована квазі-оптимальна архітектура, яка забезпечує найвищі показники метрик якості.

Практична методологія для задач неперервної верифікації користувача, яка набула подальшого розвитку є масштабною (використовується для різних варіантів архітектур); ефективною (приводить до покращення критеріїв якості системи); результативною (надає кількісні оцінки зміни критеріїв якості).

В цілому запропонована методологія визначає раціональний (квазі-оптимальний) пошук архітектур.

РОЗДІЛ 3 РОЗРОБКА АРХІТЕКТУРИ СППР НЕПЕРЕВНОЇ БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ КОРИСТУВАЧА

3.1 Запропонована СППР неперервної біометричної верифікації користувача

Постановка задачі: побудова ефективної біометричної неперервної верифікації за допомогою розробки нових архітектур на базі нейронних мереж глибокого навчання та алгоритмів виявлення нових інформаційних ознак.

Математичне забезпечення: запропоновані архітектури моделей (автокодувальники, трансформери, рекурентні нейронні мережі та їх гібриди); алгоритми налаштування параметрів архітектур моделей; алгоритми виявлення нових ознак в даних (зокрема розрахунок величини фрактальної розмірності).

Програмне забезпечення: реалізація запропонованих алгоритмів та моделей на мові програмування Python, з бібліотеками Numpy, Keras, Tensorflow, Scipy, Sklearn, hfda.

На рис. 3.1. зображено запропонований алгоритм біометричної системи верифікації користувача. У попередній роботі [101], було запропоновано більш загальний алгоритм роботи такої системи без уточнення окремих кроків та етапів. Блок-схема запропонованої архітектури СППР зображена на рис.3.2.

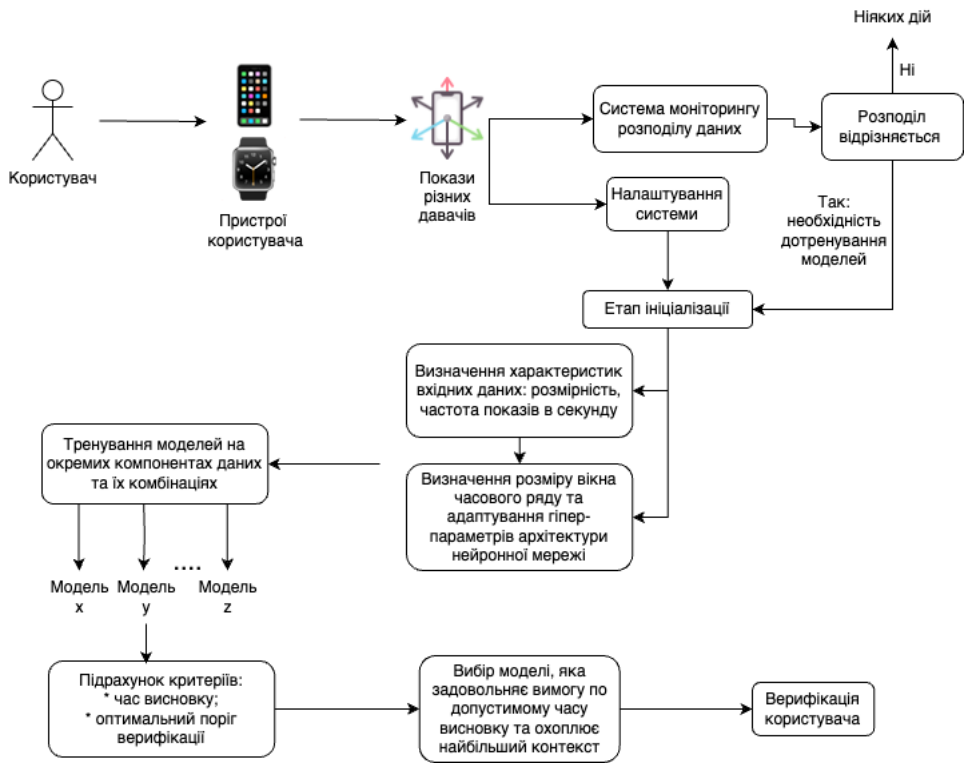


Рисунок 3.1. Блок-схема запропонованої СППР неперервної верифікації користувача

Запропонована СППР складається з *наступних частин*:

1. Користувач, який має відповідні прилади з “носимими” давачами.
2. Блок налаштування системи.
3. Блок верифікації користувача, яка в реальному часі отримує значення біометричного сигналу та приймає рішення “легітимний” чи ні. Якщо результат “легітимний” – користувача верифіковано, в іншому випадку – верифікація неуспішна.
4. Блок моніторингу вхідних даних – компонент, який відповідає за прийняття рішення щодо необхідності дотренування існуючих моделей в залежності від зміни розподілу вхідних даних.

Алгоритм запропонованої СППР виглядає наступним чином:

1. Етап налаштування системи.

   Перед безпосередньою роботою системи верифікації необхідно налаштувати її параметри та натренувати відповідні моделі.

Перед тренуванням необхідно зібрати відповідну кількість даних та ініціалізувати гіперпараметри системи. Ініціалізація складається з наступних кроків:

1.1. Встановлення максимального допустимого значення часу висновку.

1.2. Збір початкової кількості даних, необхідних для початку тренування моделей.

1.3. Визначення характеристик даних: кількість сигналів, їх стуруктура та розмірність, кількість значень в секунду (частота) сигналу.

1.2.1. Розраховується фрактальні розмірності вхідних даних (векторних і скалярних сигналів).

1.2.2. На основі розрахованих характеристик даних визначається розмір вікна часового ряду який буде використовуватися як одиниця даних, який буде йти на вхід нейронній мережі.

1.3. В залежності від розмірності вікна часового ряду та на основі вдосконаленої методології налаштування архітектур фіксуються гіперпараметри нейронної мережі. Створюються та тренуються відповідні моделі на окремі компоненти біометричного сигналу та на їх комбінації.

1.4. Розраховуються наступні критерії: час висновку та поріг верифікації. Обирається модель час висновку якої не перевищує максимального допустимого заданого значення та яка натренована на найбільшому відсотку компонентів вхідних сигналів. В разі наявності однакових по розмірності вхідних даних моделей обирається найбільш інформативна за компонентами вхідного сигналу.

1.5. Обрана модель використовується для верифікації користувача.

2. Моніторинг розподілу даних.

Оскільки дані змінюють свій розподіл протягом часу, постає необхідність

дотренування/перетренування моделей для актуалізації системи та недопущення її деградації.

2.2. В залежності від типу вхідного сигналу визначається метод, за допомогою якого можна виміряти зміни в розподілі. В контексті векторного сигналу давача це можливо з допомогою регресійних моделей [140] та аналізу розподілу залишків натренованої регресійної моделі.

2.3. В разі статистично значущої зміни розподілу даних приймається рішення про дотренування моделей.

3.2 Дослідження впливу різноманітних компонентів показів давачів на біометричну верифікацію за допомогою автокодувальників

Мета: проаналізувати та кількісно оцінити вплив різних компонентів біометричного сигналу на систему верифікації на основі автокодувальників.

Опис:

Для проведення експериментів було взяти SCMA датасет. Для аналізу показів акселерометра та моделей руху людини натренуємо модель окремо для кожної осі (x, y, z), пар осей (xy, yz, xz) та всіх трьох осей — xyz для різних видів діяльності. Дані розділяємо на вікна довжиною 52 з перекриттям 50% (через частоту акселерометра).

Ми розділили вихідний набір даних на частку 33% для тестового набору, а решту для тренувального.

Архітектура моделі автокодувальника наведена в таблиці 3.1 нижче. В якості активаційної функції використовувався гіперболічний тангенс. Модель навчалася 10 епох, з оптимізатором Адама і середньою абсолютною похибкою. Показник dropout становив 0,4.

Таблиця 3.1. Використана архітектура моделі з типом, формою та кількістю параметрів шарів.

Type	Layer Shape	# of Params
LSTM	(None, 52, 20)	1760

LSTM	(None, 10)	1240
RepeatVector	(None, 52, 10)	0
Dropout	(None, 52, 10)	0
LSTM	(None, 52, 10)	840
LSTM	(None, 52, 20)	2480
TimeDistributed	(None, 52, 3)	21

Таблиця 3.2. Кількість зразків у тренувальному датасеті (середнє значення для 15 користувачів) для різних видів діяльності

Activity	**1**	**2**	**3**	**4**	**5**	**6**	**7**
# у trainset (медіана для 15 користувачів)	133	89	301	599	86	62	860

Результати:

Для аналізу було розглянуто лише 1, 3, 4 та 7 види діяльності. 2, 5 і 6 види діяльності (стояння, ходьба і підйом по сходах, підйом по сходах, ходьба і розмова з кимось) були відфільтровані, оскільки в тренувальному сеті було представлено в середньому менше 100 зразків даних для 15 користувачів (таблиця 3.2).

Ми можемо переглянути результати середнього значення для 15 користувача кожного показника в таблицях нижче: EER та AUC (таблиця 3.3, 3.4), FAR та FRR (таблиця 3.5, 3.6).

Таблиця 3.3. Середнє значення EER (на 15 користувачів) для різних видів діяльності

Вісь даних	**1 activity**	**7 activity**	**3 activity**	**4 activity**
Середній *EER*				
x-axis	0,202	0,350	0,407	0,318
y-axis	0,168	0,276	0,364	0,345
z-axis	0,161	0,358	0,394	0,237
x-axis_*y*-axis	0,084	0,200	0,346	0,280
x-axis_*z*-axis	0,101	0,254	0,358	0,191

y-axis_*z*-axis	0,081	0,223	0,349	0,225
x-axis_ *y*-axis_*z*-axis	0,074	0,189	0,334	0,197

Таблиця 3.4. Середнє значення AUC (на 15 користувачів) для різних видів діяльності

Вісь даних	**1 activity**	**7 activity**	**3 activity**	**4 activity**
Середній *AUC*				
x-axis	0,837	0,671	0,617	0,714
y-axis	0,868	0,756	0,657	0,687
z-axis	0,873	0,669	0,631	0,791
x-axis_*y*-axis	0,938	0,833	0,680	0,759
x-axis_*z*-axis	0,924	0,777	0,673	0,841
y-axis_*z*-axis	0,938	0,807	0,680	0,807
x-axis_ *y*-axis_*z*-axis	0,949	0,846	0,689	0,830

Таблиця 3.5. Середній показник FAR (на 15 користувачів) для різних видів діяльності

Вісь даних	**1 activity**	**7 activity**	**3 activity**	**4 activity**
Середній *FAR*				
x-axis	0,260	0,527	0,589	0,459
y-axis	0,207	0,388	0,526	0,517
z-axis	0,182	0,534	0,564	0,307
x-axis_y-axis	0,066	0,219	0,464	0,374
x-axis_z-axis	0,076	0,312	0,488	0,196
y-axis_z-axis	0,059	0,269	0,459	0,259
x-axis_ y-axis_z-axis	0,030	0,188	0,452	0,222

Таблиця 3.6. Середній показник FRR (на 15 користувачів) для різних видів діяльності

Вісь даних	**1 activity**	**7 activity**	**3 activity**	**4 activity**
Середній *FRR*				

x-axis	0,067	0,132	0,177	0,113
y-axis	0,058	0,101	0,160	0,108
z-axis	0,071	0,128	0,174	0,112
x-axis_y-axis	0,058	0,116	0,176	0,107
x-axis_z-axis	0,075	0,133	0,166	0,122
y-axis_z-axis	0,064	0,117	0,181	0,127
x-axis_ y-axis_z-axis	0,073	0,120	0,171	0,117

Обговорення результатів:

Результати показують, що всі компоненти даних з акселерометра містять важливу інформацію про рухові паттерни людини і вносять свій внесок у кінцевий результат. Тому тренування моделі на всіх трьох осях акселерометра демонструє найкращі показники.

Водночас було помічено, що для різних видів активності одна вісь може бути більш інформативною, ніж інша. Наприклад, для ходьби (активність 4) модель, натренована лише на осі z або в комбінації з нею, має найвищу продуктивність за показниками EER та AUC. Натомість для активності "Розмова стоячи" (7) найкращі метрики (FAR, EER) забезпечує вісь Y.

Моделі, натреновані виключно на осі x, завжди демонструють найнижчу продуктивність порівняно з іншими. Проте їхні показники значно покращуються у поєднанні з віссю y.

Найвищу продуктивність спостерігали для активності "Робота за комп'ютером" (1), що може бути пов'язано з найбільшим обсягом навчальних даних для цієї активності.

Загалом продуктивність сильно корелює з розміром тренувального набору даних (табл. 3.2), що вказує на потенційну необхідність генерувати синтетичні дані для навчання моделі. Це важливо для систем персоналізації, які мають бути надійними з самого початку при обмеженій кількості даних. Безперервне навчання і оновлення моделі також має бути передбачено для запобігання дрейфу моделі та даних.

3.3 Дослідження гібридних автокодувальників на основі трансформерів для біометричної верифікації користувача

Мета: створити та побудувати архітектуру гібридної нейронної мережі на основі автокодувальника з застосуванням трансформерів та кількісно оцінити її вплив на ефективність та точність системи верифікації.

Опис:

Ми тренували моделі на H-MOG датасеті на певному обраному типі діяльності, як і на парі активностей, як-от читання, навігація по карті або письмо та трійках активності, як-от сидіння чи ходьба на показах акселерометра, гірсокопа та магнетометра.

Для моделей глибокого навчання дані розділяємо на вікна із частотою вибірки 100 Гц і тривалістю 1 с та перекриттям 50%.

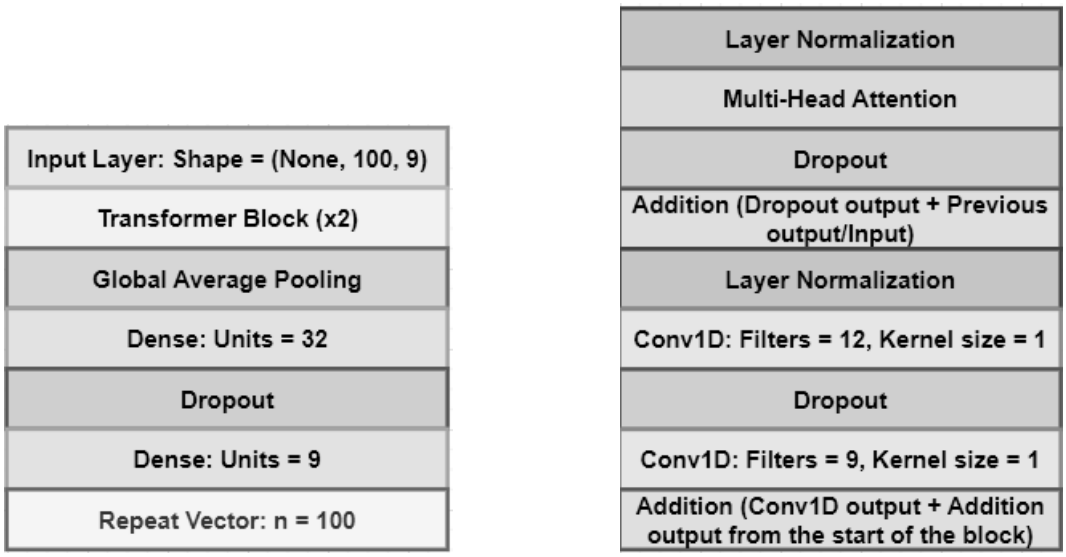
Вихідний набір даних ділиться на 20% для тестового набору та решту для тренування.

Дані попепедньо оброблювалися двома способами: стандартним scaling і нормалізацією min-max в залежності від конкретного експерименту.

Опис давачів: акселерометр вимірює зміни швидкості вздовж однієї осі. Значення, які повідомляють акселерометри, вимірюються в приростах гравітаційного прискорення, причому значення 1,0 означає прискорення 9,8 метрів на секунду в заданому напрямку. Залежно від напрямку прискорення значення давача можуть бути позитивними або негативними. Гіроскоп вимірює швидкість, з якою пристрій обертається навколо просторової осі, і використовується для визначення або вимірювання напрямку. Магнетометр вимірює силу магнітного поля, що оточує пристрій, що дозволяє нам правильно визначити орієнтацію пристрою [25, 26].

Усі моделі були навчені в 20 епох за допомогою оптимізатора Adam.

Архітектура гібридного автокодувальника на основі трансформера, що використовується для експериментів, показана на малюнку 3.2.



а) б)

Рисунок 3.2. Архітектура гібридного автокодувальника на базі трансофрмера. На **а)** маємо архітектуру автокодувальника високого рівня з кодувальником на базі трансформеру і на **б)** внутрішню структуру кодувальника на базі трансформеру з блоками уваги.

Архітектура автокодувальника LSTM, з яким порівнювався автокодувальник на основі трансформера, проілюстрована на рис. 3.2.

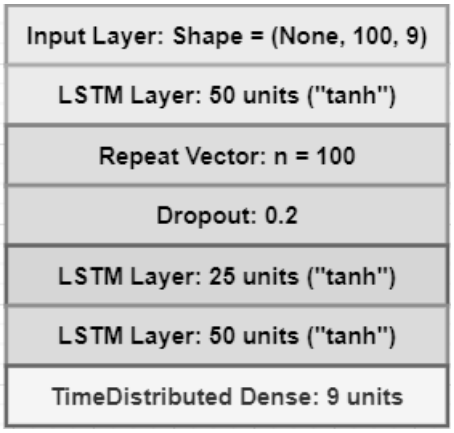


Рисунок 3.3. Архітектура автокодувальника LSTM

Результати:

Результати метрик якості для однієї дії зі стандартним масштабуванням в якості попередньої обробки даних та варіаційними автокодувальниками можна переглянути в таблиці 3.7. У таблиці 3.8, 3.9 можемо переглянути

продуктивність моделі для пар дій, а результати для триплету дій у таблиці 3.10, 3.11. Для детерміністичних моделей дані були оброблені з нормалізацією min-max.

Також можемо переглянути час роботи системи для навчання та висновку моделей у таблиці 3.12. У кожному експерименті для вибраного набору даних діяльності було навчено 100 моделей (для кожного користувача). Загалом було натреновано більше 1000 моделей.

Таблиця 3.7 Середній EER , FAR, FRR для 100 користувачів для однієї дії для варіаційного автокодувальника

Архітектура моделі	**Середній EER**	**Середній FAR**	**Середній FRR**
Одиночне заняття - письмо і сидіння			
LSTM VAE	5,10%	14,25%	3,28%
Трансформер-VAE	4,20%	12,95%	1,72%

Таблиця 3.8 Середній EER , FAR, FRR для 100 користувачів для пар діяльності для детерміністичного автокодувальника

Архітектура моделі	**Середній EER**	**Середній FAR**	**Середній FRR**
Пара активностей - письмо і ходьба, письмо і сидіння;			
LSTM AE	5,21%	13,30%	3,37%
Трансформер AE	4,22%	13,93%	1,76%
Пара активностей - навігація і ходьба, навігація і сидіння;			
LSTM AE	6,74%	14,39%	5,00%
Трансформер AE	5,87%	13,24%	3,42%

Таблиця 3.9 Середній EER , FAR, FRR для 100 користувачів для пар діяльності для варіаційного автокодувальника

Архітектура моделі	**Середній EER**	**Середній FAR**	**Середній FRR**
Пара активностей - навігація і ходьба, навігація і сидіння;			
LSTM VAE	6,24%	14,61%	3,61%
Трансформер VAE	9,74%	12,67%	9,86%

Таблиця 3.10 Середній EER , FAR, FRR для 100 користувачів для триплету активності для детерміністичного автокодувальника

Архітектура моделі	**Середній EER**	**Середній FAR**	**Середній FRR**
Трійка активностей: читання і сидіння, письмо і сидіння, навігація і сидіння.			
LSTM AE	1,26%	12,38%	0,06%
Трансформер AE	2,61%	10,97%	0,14%
Трійка активностей - читання і ходьба, письмо і ходьба, навігація і ходьба.			
LSTM AE	9,10%	12,66%	9,51%
Трансформер AE	6,47%	12,37%	4,81%

Таблиця 3.11 Середній EER , FAR, FRR для 100 користувачів для триплету активності для варіаційного автокодувальника

Архітектура моделі	Середній EER	Середній FAR	Середній FRR
Трійка активностей: читання і сидіння, письмо і сидіння, навігація і сидіння.			
LSTM VAE	2,48%	10,16%	1,08%
Трансформер VAE	2,17%	11,94%	0,06%
Трійка активностей - читання і ходьба, письмо і ходьба, навігація і ходьба.			
LSTM VAE	5,36%	12,50%	2,81%
Трансформер VAE	9,92%	9,85%	11,43%

Таблиця 3.12 Середній час навчання та часу висновку для 100 користувачів для триплету активності сидячи на тренувальному та тестовому датасеті

Архітектура моделі	Час навчання (с)	Час висновку (с)
LSTM AE (похибка MSE)	90,67	43.32
Трансформер-AE (похибка MSE)	82.22	29.61
Різниця в %	9,32%	31,65%

Обговорення результатів:

Експериментальні результати продемонстрували, що архітектура трансформера, зокрема її ключовий архітектурний блок уваги, покращує показники якості для біометричної верифікації у випадку детерміністичної версії моделі. Автокодувальник на основі трансформера перевершив автокодувальник на основі LSTM у разі навчання на одиночних видах

діяльності та парах активностей, підтверджуючи стабільну продуктивність моделі з різними вхідними даними.

Хоча на трійці активностей з сидінням LSTM AE показав дещо кращий результат ніж AE на базі трансформера в значеннях на EER і FRR, але мав вищий показник FAR. Це показує нам, що LSTM може краще узагальнювати з більшою за розміром тренувальною вибіркою. Однак, це також свідчить про те, що автокодувальники на основі трансформерів можуть узагальнювати на меншому обсязі даних.

Варто відзначити, що трансформер працює значно швидше, ніж LSTM модель з точки зору часу навчання та висновку; Тому він набагато краще підходить для периферійних пристроїв, таких як смартфони або розумні годинники, де такі моделі застосовуються.

Порівнюючи варіаційний автокодувальник на базі трансфоера чи LSTM, кращі метрики якості забезпечив LSTM варіаційний автокодувальник. Під час експерименту з’ясовано, що різні типи моделей чутливі до масштабу вхідних даних, особливо в контектсі датасету з кількома давачами. Детермінстичні моделі на розглянутому датасеті краще узагальнюють в разі нормалізації даних за допомогою min-max. Для випадку з однією фізичною активністю кращі покзаники метрик якості показав варіаційний варіант, що може бути спричиненою низкою факторів. По-перше, перетворення min-max може спотворити розподіл даних у разі значних викидів в них; тому варіаційний автокодувальник, що моделює вибірку з розподілу Гаусса з середнім значенням і дисперсією не зможуть коректно навчитися на даних, які не відповідають розподілу Гауса. З іншого боку, причина того, що детерміністичні моделі не можуть добре узагальнити на даних попередньо оброблених стандартним масштабуванням, обумовлено використанням вхідних сигналів кількох давачів, які можуть мати різний діапазон і ускладнюють роботу нейронних мереж, через функції активації (зокрема tanh). Хоча це спостереження потребує подальших досліджень, воно надає уявлення про те, як попередня обробка даних повинна

відрізнятися для різних архітектур, з урахуванням того наскільки сильно формат даних пов'язаний з параметрами та структурою нейронної мережі.

3.4 Дослідження впливу фрактальної розмірності на ефективність біометричної верифікації користувача

Мета: дослідити та кількісно оцінити вплив величини фрактальної розмірності на систему верифікації користувача на основі автокодувальників.

Опис:

Для проведення експериментів було взяти SCMA датасет. Для моделей глибокого навчання розбиваємо дані на вікна з перекриттям 50-відсотків довжиною 52 (через відповідну частоту акселерометра) та нормалізуємо стандартним масштабуванням. Схематичне зображення зображено на рис.3.4.

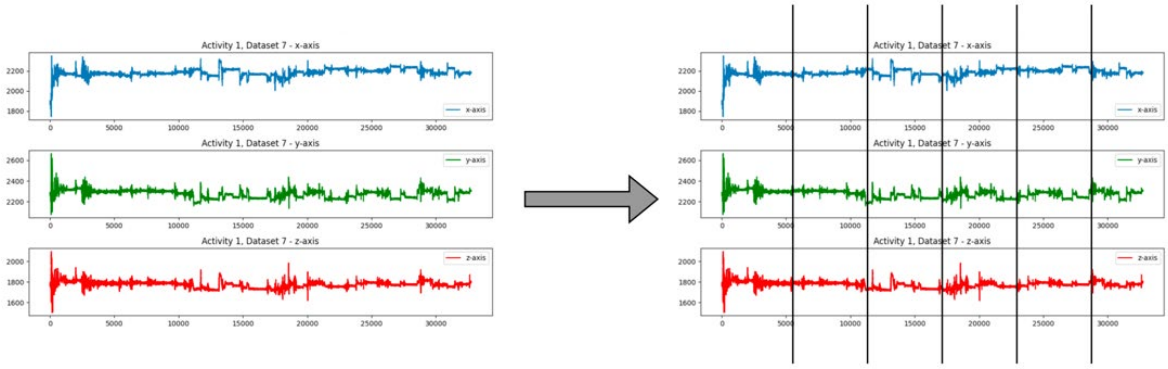


Рисунок 3.4. Розбиття вхідного часового ряду з трьома осями на вікна.

Після розбиття даних часового ряду на вікна, обчислюємо, нормалізуємо min-max та додаємо значення ФРХ з kmax=10 для кожної осі вікна. Процес зображений на рис.3.5 нижче.

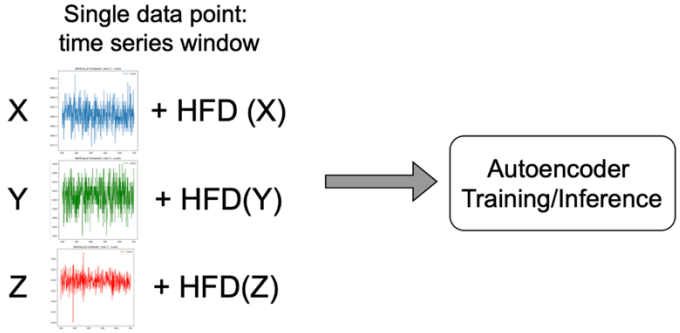


Рисунок 3.5. Процес додавання функцій ФРХ до вікон часових рядів

Вихідний набір даних було розділено наступним чином: 33% для тестового датасету, а решту для тренувального датасету.

В якості моделей використувався рекурентний LSTM автокодувальник та автокодувальник на базі трансфомера запропонованими в попередніх експериментах.

Для розрахунку ФРХ використовувався пакет hfda[141].

Результати:

В даному експерименті використовували всі наявні види фізичних активностей, представлених у наборі даних. У таблиці 3.13 нижче бачимо попередній розрахунок значення ФРХ, розрахованого для різних осей для різних фізичних активностей, для надання уявлення про складність сигналу та варіативність значень ФРХ в залежності від типу активності. Важливо відзначити, що висока ФРХ може сигналізувати не тільки про складний сигнал, але і про зашумленість в ньому, тому необхідно провести подальші експерименти аби оцінити вплив ФРХ ознаки.

Таблиця 3.13 Значення ФРХ по осям давача в залежності від фізичної активності

Активність	x	y	z
Working at Computer	1.795728	1.816538	1.817725
Standing Up, Walking and Going UpDown stairs	1.745635	1.741851	1.763078
Standing	1.398189	1.431215	1.513287
Walking	1.395676	1.355194	1.488189
Going UpDown Stairs	1.416290	1.395801	1.496528
Walking and Talking with Someone	1.397371	1.279473	1.469142
Talking while Standing	1.470182	1.464775	1.584679

У таблиці 3.14 бачимо середнє значення для 15 користувачів EER, AUC, FRR і FAR для автокодувальника LSTM і різницю між значеннями метрик якості.

Таблиця 3.14 Середні значення EER, AUC, FRR і FAR з LSTM автокодувальником

Метрика якості	Без ФРХ	З ФРХ	Різниця - %
Середній EER	0.15	0.13	- 13.33%
Середня AUC	0.90	0.92	+ 2.22%
Середній FAR	0.021	0.02	- 4.76%
Середній FRR	0.174	0.149	- 14.37%

У таблиці 3.15 наведено середнє значення для 15 користувачів EER, AUC, FRR і FAR для автокодувальника на основі трансформера з ФРХ і без нього, а також різницю.

Таблиця 3.15 Середні значення EER, AUC, FRR і FAR з автокодувальником на основі трансформера

Метрика якості	Без ФРХ	З ФРХ	Різниця - %
Середній EER	0.15	0.13	- 13.33%
Середня AUC	0.90	0.92	+ 2.22%
Середній FAR	0.021	0.02	- 4.76%
Середній FRR	0.174	0.149	- 14.37%

З точки зору витраченого часу на обчислення, розрахунок ФРХ для однієї осі вікна часового ряду довжиною 52 займе приблизно 0,0024 с, а для трьох осей - 0,007 с. Хоча це може здатися не таким значним, воно значно збільшує загальний час обробки великих пакетів даних.

Обговорення результатів

У цьому дослідженні досліджувалося підвищення точності біометричної верифікації на базі автокодувальників за рахунок інтеграції ознак ФРХ, отриманих з даних часових рядів з трьома осями. Ознаки ФРХ підвищили точність моделі, підтвердивши гіпотезу про те, що патерни, виявлені ФРХ, додають цінну інформацію для представлення для подальшого використання в системах верифікації. Зокрема, додавання ознак ФРХ приводить до зниження EER на в середньому на 12% порівняно з версією без ознаки ФРХ як в випадку LSTM автокодувальника, так і з автокодувальником на основі трансформера.

Однак обчислювальні витрати на обчислення функцій ФРХ вказують на можливу необхідність компромісу між точністю та тривалістю обчислень. Збільшення часу попередньої обробки через обчислення ФРХ може обмежити застосування цього підходу в реальному часі, особливо в сценаріях, де швидкість обробки є критичною. Тому необхідно враховувати даний критерій при виборі моделі та побудови системи верифікації.

Висновки до розділу

В даному розділі запропоновано та описано архітектуру СППР неперервної біометричної верифікації користувача та її складових на основі вдосконаленої методології побудови систем верифікації. Описано загальний алгоритм роботи системи, що включає в себе визначення гіперпараметрів нейронних мереж та їх безпосереднє тренування, а також процес моніторингу розподілу вхідних даних, для уникнення деградації системи та підтримання стабільної якості.

Також проведено глибокий аналіз впливу різних компонентів векторного біометричного сигналу та кількісно оцінено їх вплив на ефективність системи верифікації користувача. Встановлено, що в залежності від типу фізичної активності різні компоненти сигналу давача по різному впливають на показники метрик якості системи. Також, кількісно оцінено вплив компонентів сигналів давача в різних комбінаціях та доведено ефективність використання комбінацій компонентів векторного сигналу для досягнення вищої точності.

Запропонована нова гібридна архітектура, яка базується на стискуючих автокодувальниках з використанням трансформерів, показує час висновку швидший на 31% відсоток та нижче в середньому на 11% відсотків значення рівного рівня помилок для всі типів фізичних активностей та їх комбінацій.

Запропоновано нову інформаційну характеристику верифікації користувача – фрактальну розмірність Хігучі. Проведено аналіз впливу величин фрактальної розмірності Хігучі вхідних даних на ефективність системи верифікації на базі автокодувальників. Показано перевагу використання фрактальної розмірності

даних на основні метрики якості, зокрема на рівний рівень помилок (в середньому на 13% відсотків нижчі значення) та на значення площі під кривою (на 2.2% відсотків вищі показники) в порівнянні з системою верифікації без її врахування.

ВИСНОВКИ

Дисертаційна робота присвячена розробці систем біометричної верифікації користувача за допомогою нейронних мереж глибокого навчання. Рукопис складається з вступу, 3 розділів та висновків.

У першому розділі проведено глибокий огляд існуючих джерел в яких досліджується розв'язок задачі верифікації користувача за допомогою нейронних мереж глибокого навчання та – аналіз різних класів архітектур. Визначені недоліки та можливі напрямки подальших досліджень для вдосконалення існуючих і побудову нових ефективних архітектур для систем біометричної поведінкової верифікації.

В другому розділі представлені описи та розрахунки проведених екпериментів, в яких досліджується ефективність нових архітектур на базі автокодувальників, трансформерів, рекурентних нейронних мереж та їх гібридів. Етап попередньої обробки даних було доповнено значенням величин фрактальних розмірностей та досліджено ефективність їх використання в якості нової інформаційної ознаки для запропонованих архітектур. Запропонований зручний інтерфейс представлення результатів роботи моделі для експрес-оцінки якості досліджуваних архітектур.

Проведено порівняльний аналіз різних типів автокодувальників з класичними методами машинного навчання, як-от однокласові опорні машини векторів та ізоляційний ліс (Isolation Forest). Показано суттєву перевагу застосування автокодувальників над класичними методами машинного навчання, наприклад отримуємо на 7% вищу чутливість (recall) в порівнянні з ізоляційним лісом і на 75% вищу чутливість (recall) в порівнянні з однокласовими опорними машинами векторів.

Також проведено глибокий аналіз впливу різних компонентів векторного біометричного сигналу та кількісно оцінено їх вплив на ефективність системи верифікації користувача. Встановлено та кількісно оцінено вплив компонентів

сигналів давача в різних комбінаціях в залежності від фізичної активності на показники верифікації запропонованих моделей.

Запропонована нова гібридна архітектура, яка базується на стискуючих автокодувальниках з використанням трансформерів, показує час висновку швидший на 31% відсоток та нижче в середньому на 11% відсотків значення рівного рівня помилок для всіх типів фізичних активностей та їх комбінацій.

Проведено аналіз впливу величин фрактальної розмірності Хігучі вхідних даних на ефективність системи верифікації на базі автокодувальників. Показано перевагу використання фрактальної розмірності даних на основні метрики якості, зокрема на рівний рівень помилок (в середньому на 13% відсотків нижче значення) та на значення площі під кривою (на 2.2% відсотків вищі показники) в порівнянні з системою верифікації без її врахування.

В третьому розділі описується постановка задачі верифікації; представлена вдосконалена методологія оптимізації створених моделей верифікації; запропонована система підтримки прийняття рішень для неперервної верифікації користувача.

СППР неперервної біометричної верифікації користувача на основі розроблених нових гібридних архітектур також враховує фрактальні розмірності вхідних даних. На вхід розробленої системи надходять дані з різноманітних давачів (акселерометри, гіроскопи, магнетометри, тощо), які характеризують відповідні біометричні чи поведінкові показники особи. Під час етапу ініціалізації відбувається збір початкової необхідної кількості даних для тренування нових гібридних архітектур. На основі вдосконаленої практичної методології налаштування параметрів системи верифікації, перед тренуванням, встановлюються допустимі значення глобальних критеріїв; підбираються відповідні значення розмірності вхідних даних в залежності від характеристик давачів; гіперпараметри архітектури нейронної мережі глибокого навчання; розраховується фрактальна розмірність даних кожного типу давача. В залежності від кількості та розмірності даних відбувається тренування моделей різних відповідних архітектур на окремих компонентах

(скалярних, векторних) та на їх комбінаціях. Після тренування для кожної моделі отримуються значення відповідних критеріїв (час висновку, значення порогу верифікації). Відповідно до доступності сигналів для висновку системи верифікації вибирається модель, яка охоплює найбільший контекст та не перевищує установленого допустимого значення по часу висновку. В разі наявності однакових по розмірності вхідних даних моделей, обирається найбільш інформативна по своїм компонентам вхідного сигналу. Також, система має елемент моніторингу розподілу даних, який в залежності від змін в їхньому розподілі при необхідності ініціює дотренування моделей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]E. AA, “Biometrics Technologies for Secured Identification and Personal Verification,” *Biostat Biom Open Access J*, vol. 6, no. 2, 2018, doi: 10.19080/bboaj.2018.06.555683.

[2]B. Mróz-Gorgoń, W. Wodo, A. Andrych, K. Caban-Piaskowska, and C. Kozyra, “Biometrics Innovation and Payment Sector Perception,” *Sustainability (Switzerland)*, vol. 14, no. 15, 2022, doi: 10.3390/su14159424.

[3]M. Salem, S. Taheri, and J. S. Yuan, “Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system,” *Computers*, vol. 8, no. 1, 2019, doi: 10.3390/computers8010003.

[4]S. Kokal, M. Vanamala, and R. Dave, “Deep Learning and Machine Learning, Better Together Than Apart: A Review on Biometrics Mobile Authentication,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, 2023, doi: 10.3390/jcp3020013.

[5]K. Nandakumar, A. K. Jain, and A. Nagar, “Biometric template security,” *EURASIP J Adv Signal Process*, vol. 2008, 2008, doi: 10.1155/2008/579416.

[6]C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *Eurasip Journal on Information Security*, vol. 2011. 2011. doi: 10.1186/1687-417X-2011-3.

[7]N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, “Cancelable biometrics: A case study in fingerprints,” in *Proceedings - International Conference on Pattern Recognition*, 2006. doi: 10.1109/ICPR.2006.353.

[8]M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, and T. Koshiba, “Packed homomorphic encryption based on ideal lattices and its application to biometrics,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013. doi: 10.1007/978-3-642-40588-4_5.

[9]W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, “A Review of Homomorphic Encryption for Privacy-Preserving Biometrics,” *Sensors*, vol. 23, no. 7. 2023. doi: 10.3390/s23073566.

[10]A. Abidin and A. Mitrokotsa, “Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE,” in *2014 IEEE International Workshop on Information Forensics and Security, WIFS 2014*, 2015. doi: 10.1109/WIFS.2014.7084304.

[11]T. M. Hoang and D. Choi, “Secure and Privacy Enhanced Gait Authentication on Smart Phone,” *The Scientific World Journal*, 2014, doi: 10.1155/2014/438254.

[12]Q. Tang, J. Bringer, H. Chabanne, and D. Pointcheval, “A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes,” 2008, doi: 10.1007/978-3-540-79104-1_5.

[13]V. Odelu, A. K. Das, and A. Goswami, “A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards,” *Ieee Transactions on Information Forensics and Security*, 2015, doi: 10.1109/tifs.2015.2439964.

[14]S. Shekhar, V. M. Patel, N. M. Nasrabadi, and R. Chellappa, “Joint Sparse Representation for Robust Multimodal Biometrics Recognition,” *IEEE Trans Pattern Anal Mach Intell*, 2014, doi: 10.1109/tpami.2013.109.

[15]X. Li, J. Niu, M. K. Khan, J. Liao, and X. Zhao, “Robust Three-factor Remote User Authentication Scheme With Key Agreement for Multimedia Systems,” *Security and Communication Networks*, 2014, doi: 10.1002/sec.961.

[16]M. Barni, G. Droandi, R. Lazzeretti, and T. Pignata, “SEMBA: Secure Multi-biometric Authentication,” *IET Biom*, 2019, doi: 10.1049/iet-bmt.2018.5138.

[17]S.-J. Lee, J. Sa, H. Cho, and J. Park, “Energy-Efficient Biometrics-Based Remote User Authentication for Mobile Multimedia IoT Application,” *Ksii Transactions on Internet and Information Systems*, 2017, doi: 10.3837/tiis.2017.12.025.

[18]X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, “An Efficient Android-Based Multimodal Biometric Authentication System With Face and Voice,” *Ieee Access*, 2020, doi: 10.1109/access.2020.2999115.

[19]A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, “A Survey on Behavioral Biometric Authentication on Smartphones,” *Journal of Information Security and Applications*. 2017. doi: 10.1016/j.jisa.2017.10.002.

[20]A. Martin and E. A. Whitley, “Fixing Identity? Biometrics and the Tensions of Material Practices,” *Media Culture & Society*. 2013. doi: 10.1177/0163443712464558.

[21]N. Sarfraz, “Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative,” *Cureus*. 2019. doi: 10.7759/cureus.4040.

[22]A. Bhargav-Spantzel, A. Squicciarini, E. Bertino, X. Kong, and W. Zhang, “Biometrics-Based Identifiers for Digital Identity Management.” 2010. doi: 10.1145/1750389.1750401.

[23]R. P. Wildes, “Iris Recognition: An Emerging Biometric Technology,” *Proceedings of the Ieee*. 1997. doi: 10.1109/5.628669.

[24]M. Mileva, R. Jenkins, and A. M. Burton, “Facial Identity Across the Lifespan,” *Cognitive Psychology*. 2020. doi: 10.1016/j.cogpsych.2019.101260.

[25]R. and P. S. Jain Anil and Bolle, “Introduction to Biometrics,” in *Biometrics: Personal Identification in Networked Society*, R. and P. S. Jain Anil K. and Bolle, Ed., Boston, MA: Springer US, 1996, pp. 1–41. doi: 10.1007/0-306-47044-6_1.

[26]M. V. Arısoy, “Siamese Sinir Ağı One-Shot Öğrenmeyi Kullanarak İmza Doğrulama,” *International Journal of Engineering and Innovative Research*. 2021. doi: 10.47933/ijeir.972796.

[27]X. Liu and Y. Cheung, “Learning Multi-Boosted HMMs for Lip-Password Based Speaker Verification,” *Ieee Transactions on Information Forensics and Security*. 2014. doi: 10.1109/tifs.2013.2293025.

[28]F. Gomez-Caballero, T. Shinozaki, S. Furui, and K. Sairyo, “A Statistical Approach for Person Verification Using Human Behavioral Patterns,” *Eurasip Journal on Image and Video Processing*. 2013. doi: 10.1186/1687-5281-2013-44.

[29]F. Gomez-Caballero, T. Shinozaki, S. Furui, and K. Sairyo, “Statistical Person Verification Using Behavioral Patterns From Complex Human Motion.” 2013. doi: 10.1007/978-3-642-41190-8_60.

[30]G. M. Weiss, K. Yoneda, and T. Hayajneh, “Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living,” *Ieee Access*. 2019. doi: 10.1109/access.2019.2940729.

[31]M. P. Havrylovych and V. Y. Danylov, “RESEARCH OF AUTOENCODER-BASED USER BIOMETRIC VERIFICATION WITH MOTION PATTERNS,” *System Research and Information Technologies*, vol. 2022, no. 2, 2022, doi: 10.20535/SRIT.2308-8893.2022.2.10.

[32]S. Lefèvre, D. Vasquez, and C. Laugier, “A Survey on Motion Prediction and Risk Assessment for Intelligent Vehicles,” *Robomech Journal*. 2014. doi: 10.1186/s40648-014-0001-z.

[33]F. Cherifi, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger, “Performance Evaluation of Behavioral Biometric Systems.” 2010. doi: 10.4018/978-1-60566-725-6.ch003.

[34]A. Joseph *et al.*, “Person Verification Based on Multimodal Biometric Recognition,” *Pertanika Journal of Science and Technology*. 2021. doi: 10.47836/pjst.30.1.09.

[35]B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, “Face–Iris Multimodal Biometric Identification System,” *Electronics*. 2020. doi: 10.3390/electronics9010085.

[36]S. C. Dass, K. Nandakumar, and A. K. Jain, “A Principled Approach to Score Level Fusion in Multimodal Biometric Systems.” 2005. doi: 10.1007/11527923_109.

[37]P. Szczuko, A. Harasimiuk, and A. Czyżewski, “Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application,” *Sensors*. 2022. doi: 10.3390/s22062356.

[38]V. Rajasekar *et al.*, “Enhanced Multimodal Biometric Recognition Approach for Smart Cities Based on an Optimized Fuzzy Genetic Algorithm,” *Scientific Reports*. 2022. doi: 10.1038/s41598-021-04652-3.

[39]M. Rukhiran, S. Wong-In, and P. Netinant, “IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach,” *Ieee Access*. 2023. doi: 10.1109/access.2023.3253024.

[40]K. W. Jin and E. C. Lee, “Improving the Performance of Frequently Used Korean Handwritten Character Verification Based on Artificial Intelligence Through Multimodal Fusion,” *Applied Sciences*. 2021. doi: 10.3390/app11188413.

[41]M. Papaioannou, G. Zachos, G. Mantas, and J. Rodriguez, “Novelty Detection for Risk-based User Authentication on Mobile Devices,” in *2022 IEEE Global Communications Conference, GLOBECOM 2022 - Proceedings*, 2022. doi: 10.1109/GLOBECOM48099.2022.10000843.

[42]T. Zhu, Z. Weng, G. Chen, and L. Fu, “A hybrid deep learning system for real-world mobile user authentication using motion sensors,” *Sensors (Switzerland)*, vol. 20, no. 14, 2020, doi: 10.3390/s20143876.

[43]I. Omara, A. Hagag, S. Chaib, G. Z. Ma, F. E. Abd El-Samie, and E. N. Song, “A Hybrid Model Combining Learning Distance Metric and DAG Support Vector Machine for Multimodal Biometric Recognition,” *IEEE ACCESS*, vol. 9, 2021.

[44]F. T. Liu, K. M. Ting, and Z. Zhou, “Isolation Forest.” 2008. doi: 10.1109/icdm.2008.17.

[45]F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation-based anomaly detection,” *ACM Trans Knowl Discov Data*, vol. 6, no. 1, 2012, doi: 10.1145/2133360.2133363.

[46]L. Hernández-Álvarez, E. Barbierato, S. Caputo, L. Mucchi, and L. Hernández Encinas, “EEG Authentication System Based on One- and Multi-Class Machine Learning Classifiers,” *Sensors*, vol. 23, no. 1, 2023, doi: 10.3390/s23010186.

[47]L. Hernández-álvarez, J. M. de Fuentes, L. González-Manzano, and L. H. Encinas, “Privacy-preserving sensor-based continuous authentication and user profiling: A review,” *Sensors (Switzerland)*, vol. 21, no. 1. 2021. doi: 10.3390/s21010092.

[48]L. Pryor, J. Mallet, R. Dave, N. Seliya, M. Vanamala, and E. Sowells-Boone, “Evaluation of a User Authentication Schema Using Behavioral Biometrics and Machine Learning,” *Computer and Information Science*, vol. 15, no. 3, 2022, doi: 10.5539/cis.v15n3p1.

[49]M. Breunig, H. Kriegel, R. T. Ng, and J. Sander, “Lof,” *Acm Sigmod Record*. 2000. doi: 10.1145/335191.335388.

[50]N. Dehak, P. J. Kenny, R. Dehak, P. Dumouchel, and P. Ouellet, “Front-end factor analysis for speaker verification,” *IEEE Trans Audio Speech Lang Process*, vol. 19, no. 4, 2011, doi: 10.1109/TASL.2010.2064307.

[51]A. Nowak-Brzezińska and C. Horyń, “Exploration of outliers in if-then rule-based knowledge bases,” *Entropy*, vol. 22, no. 10, 2020, doi: 10.3390/e22101096.

[52]S. Su *et al.*, “An Efficient Density-Based Local Outlier Detection Approach for Scattered Data,” *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2018.2886197.

[53]R. Kumar, P. P. Kundu, and V. V. Phoha, “Continuous authentication using one-class classifiers and their fusion,” in *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis, ISBA 2018*, 2018. doi: 10.1109/ISBA.2018.8311467.

[54]Y. Li, P. Tao, S. Deng, and G. Zhou, “DeFFusion: CNN-based Continuous Authentication Using Deep Feature Fusion,” *ACM Trans Sens Netw*, vol. 18, no. 2, 2022, doi: 10.1145/3485060.

[55]R. F. Liao *et al.*, “Deep-learning-based physical layer authentication for industrial wireless sensor networks,” *Sensors (Switzerland)*, vol. 19, no. 11, 2019, doi: 10.3390/s19112440.

[56]M. Hammad, P. Pławiak, K. Wang, and U. R. Acharya, “ResNet-Attention model for human authentication using ECG signals,” in *Expert Systems*, 2021. doi: 10.1111/exsy.12547.

[57]T. Bin Shams, M. S. Hossain, M. F. Mahmud, M. S. Tehjib, Z. Hossain, and M. I. Pramanik, “EEG-based Biometric Authentication Using Machine Learning: A Comprehensive Survey,” *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 20, no. 2, 2022, doi: 10.37936/ecti-eec.2022202.246906.

[58]J. M. Ackerson, R. Dave, and J. Seliya, “Applications of recurrent neural network for biometric authentication & anomaly detection,” *Information (Switzerland)*, vol. 12, no. 7. 2021. doi: 10.3390/info12070272.

[59]R. Pascanu, C. Gulcehre, K. Cho, and Y. Bengio, “How to construct deep recurrent neural networks,” in *2nd International Conference on Learning Representations, ICLR 2014 - Conference Track Proceedings*, 2014.

[60]S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” *Neural Comput*, vol. 9, no. 8, 1997, doi: 10.1162/neco.1997.9.8.1735.

[61]J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne, and Y. Lee, "Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks," *Computer (Long Beach Calif)*, vol. 51, no. 5, 2018, doi: 10.1109/MC.2018.2381119.

[62]A. Bajaber, M. Fadel, and L. Elrefaei, "Evaluation of Deep Learning Models for Person Authentication Based on Touch Gesture," *Computer Systems Science and Engineering*, vol. 42, no. 2, 2021, doi: 10.32604/csse.2022.022003.

[63]D. Belo, N. Bento, H. da Silva, A. Fred, and H. Gamboa, "ECG Biometrics using RNN and CNN." Oct. 2020. doi: 10.21203/rs.2.22270/v1.

[64]Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, and J. Cai, "Deep Neural Networks for CSI-Based Authentication," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2938533.

[65]Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li, "Deep Learning-Based Gait Recognition Using Smartphones in the Wild," *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, doi: 10.1109/TIFS.2020.2985628.

[66]S. Alzahrani, J. Alderaan, D. Alatawi, and B. Alotaibi, "Continuous Mobile User Authentication Using a Hybrid CNN-Bi-LSTM Approach," *Computers, Materials and Continua*, vol. 75, no. 1, 2023, doi: 10.32604/cmc.2023.035173.

[67]X. Zeng, X. Zhang, S. Yang, Z. Shi, and C. Chi, "Gait-Based Implicit Authentication Using Edge Computing and Deep Learning for Mobile Devices," *Sensors (Basel)*, vol. 21, no. 13, 2021, doi: 10.3390/s21134592.

[68]A. Vaswani *et al.*, "Attention is all you need," in *Advances in Neural Information Processing Systems*, 2017.

[69]H. Huang, P. Zhou, Y. Li, and F. Sun, "A lightweight attention-based cnn model for efficient gait recognition with wearable imu sensors," *Sensors*, vol. 21, no. 8, 2021, doi: 10.3390/s21082866.

[70]C. Luo *et al.*, "Gait Recognition as a Service for Unobtrusive User Identification in Smart Spaces," *ACM Transactions on Internet of Things*, vol. 1, no. 1, 2020, doi: 10.1145/3375799.

[71]D. Jyotishi and S. Dandapat, “An ECG Biometric System Using Hierarchical LSTM with Attention Mechanism,” *IEEE Sens J*, vol. 22, no. 6, 2022, doi: 10.1109/JSEN.2021.3139135.

[72]P. Delgado-Santos, R. Tolosana, R. Guest, F. Deravi, and R. Vera-Rodriguez, “Exploring transformers for behavioural biometrics: A case study in gait recognition,” *Pattern Recognit*, vol. 143, p. 109798, 2023, doi: https://doi.org/10.1016/j.patcog.2023.109798.

[73]P. Delgado-Santos, R. Tolosana, R. Guest, R. Vera-Rodriguez, and J. Fierrez, “M-GaitFormer: Mobile biometric gait verification using Transformers,” *Eng Appl Artif Intell*, vol. 125, 2023, doi: 10.1016/j.engappai.2023.106682.

[74]G. Stragapede, P. Delgado-Santos, R. Tolosana, R. Vera-Rodriguez, R. Guest, and A. Morales, “Mobile Keystroke Biometrics Using Transformers,” in *2023 IEEE 17th International Conference on Automatic Face and Gesture Recognition, FG 2023*, 2023. doi: 10.1109/FG57933.2023.10042710.

[75]K. J. Chee and D. A. Ramli, “Electrocardiogram Biometrics Using Transformer’s Self-Attention Mechanism for Sequence Pair Feature Extractor and Flexible Enrollment Scope Identification,” *Sensors*, vol. 22, no. 9, 2022, doi: 10.3390/s22093446.

[76]M. S. Sayeed, I. Bin Yusof, M. F. A. bin Abdullah, M. A. Bari, and P. P. Min, “A comprehensive survey on deep-learning based gait recognition for humans in the COVID-19 pandemic,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, 2023, doi: 10.11591/ijeecs.v30.i2.pp882-902.

[77]A. Sepas-Moghaddam and A. Etemad, “Deep Gait Recognition: A Survey,” *IEEE Trans Pattern Anal Mach Intell*, vol. 45, no. 1, pp. 264–284, 2023, doi: 10.1109/TPAMI.2022.3151865.

[78]S. Roy, M. Harandi, R. Nock, and R. Hartley, “Siamese networks: The tale of two manifolds,” in *Proceedings of the IEEE International Conference on Computer Vision*, 2019. doi: 10.1109/ICCV.2019.00314.

[79]Suprapto and J. A. Polela, “The Influence of Loss Function Usage at SIAMESE Network in Measuring Text Similarity,” *International Journal of Advanced*

Computer Science and Applications, vol. 11, no. 12, 2020, doi: 10.14569/IJACSA.2020.0111290.

[80]J. B. Grill *et al.*, "Bootstrap your own latent a new approach to self-supervised learning," in *Advances in Neural Information Processing Systems*, 2020.

[81]G. Li, R. Togo, T. Ogawa, and M. Haseyama, "TRIBYOL: TRIPLET BYOL FOR SELF-SUPERVISED REPRESENTATION LEARNING," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2022. doi: 10.1109/ICASSP43922.2022.9746967.

[82]X. Peng, K. Wang, Z. Zhu, M. Wang, and Y. You, "Crafting Better Contrastive Views for Siamese Representation Learning," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2022. doi: 10.1109/CVPR52688.2022.01556.

[83]H. Fereidooni *et al.*, "AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms," 2023. doi: 10.14722/ndss.2023.23194.

[84]A. Gavron *et al.*, "Motion ID: Human authentication approach," 2023.

[85]R. Giot and A. Rocha, "Siamese Networks for Static Keystroke Dynamics Authentication," in *2019 IEEE International Workshop on Information Forensics and Security, WIFS 2019*, 2019. doi: 10.1109/WIFS47025.2019.9035100.

[86]J. Solano, E. Rivera, L. Tengana, C. López, J. Flórez, and M. Ochoa, "A Siamese Neural Network for Scalable Behavioral Biometrics Authentication," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2022. doi: 10.1007/978-3-031-16815-4_28.

[87]A. J. Prakash, K. K. Patro, S. Samantray, P. Pławiak, and M. Hammad, "A Deep Learning Technique for Biometric Authentication Using ECG Beat Template Matching," *Information (Switzerland)*, vol. 14, no. 2, 2023, doi: 10.3390/info14020065.

[88]M. Hazratifard, V. Agrawal, F. Gebali, H. Elmiligi, and M. Mamun, “Ensemble Siamese Network (ESN) Using ECG Signals for Human Authentication in Smart Healthcare System,” *Sensors*, vol. 23, no. 10, 2023, doi: 10.3390/s23104727.

[89]Q. Meng, D. Catchpoole, D. Skillicom, and P. J. Kennedy, “Relational autoencoder for feature extraction,” in *Proceedings of the International Joint Conference on Neural Networks*, 2017. doi: 10.1109/IJCNN.2017.7965877.

[90]A. Singh and T. Ogunfunmi, “An Overview of Variational Autoencoders for Source Separation, Finance, and Bio-Signal Applications,” *Entropy*, vol. 24, no. 1. 2022. doi: 10.3390/e24010055.

[91]A. Makhzani, J. Shlens, N. Jaitly, and I. Goodfellow, “Adversarial Autoencoders V2,” *ArXiv*, 2015.

[92]I. Odinaka, P. H. Lai, A. D. Kaplan, J. A. O’Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh, “ECG biometric recognition: A comparative analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, 2012, doi: 10.1109/TIFS.2012.2215324.

[93]J. Yang *et al.*, “Multi-Label Attribute Selection of Arrhythmia for Electrocardiogram Signals with Fusion Learning,” *Bioengineering*, vol. 9, no. 7, 2022, doi: 10.3390/bioengineering9070268.

[94]A. N. Uwaechia and D. A. Ramli, “A Comprehensive Survey on ECG Signals as New Biometric Modality for Human Authentication: Recent Advances and Future Challenges,” *IEEE Access*, vol. 9, pp. 97760–97802, 2021, doi: 10.1109/ACCESS.2021.3095248.

[95]R. Srivastva and Y. N. Singh, “ECG analysis for human recognition using non-fiducial methods,” *IET Biom*, vol. 8, no. 5, 2019, doi: 10.1049/iet-bmt.2018.5093.

[96]F. Murat, O. Yildirim, M. Talo, U. B. Baloglu, Y. Demir, and U. R. Acharya, “Application of deep learning techniques for heartbeats detection using ECG signals-analysis and review,” *Computers in Biology and Medicine*, vol. 120. 2020. doi: 10.1016/j.compbiomed.2020.103726.

[97]O. Yildirim, R. S. Tan, and U. R. Acharya, “An efficient compression of ECG signals using deep convolutional autoencoders,” *Cogn Syst Res*, vol. 52, 2018, doi: 10.1016/j.cogsys.2018.07.004.

[98]J. H. Jang, T. Y. Kim, H. S. Lim, and D. Yoon, “Unsupervised feature learning for electrocardiogram data using the convolutional variational autoencoder,” *PLoS One*, vol. 16, no. 12 December, 2021, doi: 10.1371/journal.pone.0260612.

[99]H.-Y. S. Chien, H. Goh, C. M. Sandino, and J. Y. Cheng, “MAEEG: Masked Auto-encoder for EEG Representation Learning,” *ArXiv*, vol. abs/2211.02625, 2022, [Online]. Available: https://api.semanticscholar.org/CorpusID:253370631

[100]L. Sun, Z. Zhong, Z. Qu, and N. Xiong, “PerAE: An Effective Personalized AutoEncoder for ECG-Based Biometric in Augmented Reality System,” *IEEE J Biomed Health Inform*, vol. 26, no. 6, 2022, doi: 10.1109/JBHI.2022.3145999.

[101]M. Havrylovych, V. Danylov, and A. Gozhyj, “Comparative analysis of using recurrent autoencoders for user biometric verification with wearable accelerometer,” in *CEUR Workshop Proceedings*, 2020.

[102]M. Hu, K. Zhang, R. You, and B. Tu, “Relative attention-based one-class adversarial autoencoder for continuous authentication of smartphone users,” 2022.

[103]P. Hlihor, R. Volpi, and L. Malagò, “Evaluating the Robustness of Defense Mechanisms based on AutoEncoder Reconstructions against Carlini-Wagner Adversarial Attacks,” *Proceedings of the Northern Lights Deep Learning Workshop*, vol. 1, 2020, doi: 10.7557/18.5173.

[104]W. Ding, M. Abdel-Basset, H. Hawash, and N. Mostafa, “Interval type-2 fuzzy temporal convolutional autoencoder for gait-based human identification and authentication,” *Inf Sci (N Y)*, vol. 597, 2022, doi: 10.1016/j.ins.2022.03.046.

[105]G. E. Hinton and R. R. Salakhutdinov, “Reducing the dimensionality of data with neural networks,” *Science (1979)*, vol. 313, no. 5786, 2006, doi: 10.1126/science.1127647.

[106]N. Nguyen, N. Jähne-Raden, U. Kulau, and S. Sigg, “Representation Learning for Sensor-based Device Pairing,” in *2018 IEEE International Conference on*

Pervasive Computing and Communications Workshops, PerCom Workshops 2018, 2018. doi: 10.1109/PERCOMW.2018.8480412.

[107]A. Jurek-Loughrey, "Deep learning based approach to unstructured record linkage," *International Journal of Web Information Systems*, vol. 17, no. 6, 2021, doi: 10.1108/IJWIS-05-2021-0058.

[108]P. Delgado-Santos, R. Tolosana, R. Guest, R. Vera-Rodriguez, F. Deravi, and A. Morales, "GaitPrivacyON: Privacy-preserving mobile gait biometrics using unsupervised learning," *Pattern Recognit Lett*, vol. 161, 2022, doi: 10.1016/j.patrec.2022.07.015.

[109]G. Garofalo, D. Preuveneers, and W. Joosen, "Data privatizer for biometric applications and online identity management," in *IFIP Advances in Information and Communication Technology*, 2020. doi: 10.1007/978-3-030-42504-3_14.

[110]F. Zappasodi, E. Olejarczyk, L. Marzetti, G. Assenza, V. Pizzella, and F. Tecchio, "Fractal Dimension of EEG Activity Senses Neuronal Impairment in Acute Stroke," *PLoS One*, 2014, doi: 10.1371/journal.pone.0100199.

[111]R. Esteller, G. Vachtsevanos, J. Echauz, and B. Litt, "A Comparison of Waveform Fractal Dimension Algorithms," *Ieee Transactions on Circuits and Systems I Fundamental Theory and Applications*, 2001, doi: 10.1109/81.904882.

[112]M. Y. Boon *et al.*, "Fractal Dimension Analysis of Transient Visual Evoked Potentials: Optimisation and Applications," *PLoS One*, 2016, doi: 10.1371/journal.pone.0161565.

[113]D. Easwaramoorthy and R. Uthayakumar, "Improved Generalized Fractal Dimensions in the Discrimination Between Healthy and Epileptic EEG Signals," *J Comput Sci*, 2011, doi: 10.1016/j.jocs.2011.01.001.

[114]C. Gómez, Á. Mediavilla, R. Hornero, D. Abásolo, and A. Fernández, "Use of the Higuchi's Fractal Dimension for the Analysis of MEG Recordings From Alzheimer's Disease Patients," *Med Eng Phys*, 2009, doi: 10.1016/j.medengphy.2008.06.010.

[115]L. Yang, W. Pu, C. Zhong, Z. Meng, P. S.-P. Wang, and Y. Y. Tang, "A Fractal Dimension and Empirical Mode Decomposition-Based Method for Protein Sequence

Analysis," *Intern J Pattern Recognit Artif Intell*, 2019, doi: 10.1142/s0218001419400202.

[116]R. Boostani and M. H. Moradi, "A New Approach in the BCI Research Based on Fractal Dimension as Feature and Adaboost as Classifier," *J Neural Eng*, 2004, doi: 10.1088/1741-2560/1/4/004.

[117]R. Komalasari, A. Rizal, and F. Suratman, "Classification of Normal and Murmur Hearts Sound using the Fractal Method," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, pp. 8178–8183, Oct. 2020, doi: 10.30534/ijatcse/2020/181952020.

[118]X. Chen and J. Zhang, "Biometric Feature Extraction Using Local Fractal Auto-Correlation," *Chinese Physics B*, 2014, doi: 10.1088/1674-1056/23/9/096401.

[119]M. Jampour, A. Naserasadi, E. Majid, and M. Ashourzadeh, "Extract and Classification of Iris Images by Fractal Dimension and Efficient Color of Iris," *Int J Comput Appl*, 2011, doi: 10.5120/2250-2883.

[120]L. A. Moctezuma and M. Molinas, "EEG-Based Subjects Identification Based on Biometrics of Imagined Speech Using EMD," 2018, doi: 10.1007/978-3-030-05587-5_43.

[121]J. Blasco and P. Peris-Lopez, "On the feasibility of low-cost wearable sensors for multi-modal biometric verification," *Sensors (Switzerland)*, vol. 18, no. 9, 2018, doi: 10.3390/s18092782.

[122]V. D. Stanciu, R. Spolaor, M. Conti, and C. Giuffrida, "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks," in *CODASPY 2016 - Proceedings of the 6th ACM Conference on Data and Application Security and Privacy*, 2016. doi: 10.1145/2857705.2857748.

[123]L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proceedings - IEEE Symposium on Security and Privacy*, 2019. doi: 10.1109/SP.2019.00029.

[124]F. Wibawa, F. O. Catak, S. Sarp, and M. Kuzlu, "BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models," *Cryptography*, vol. 6, no. 3, 2022, doi: 10.3390/cryptography6030034.

[125]Imran M. Hussain Qureshi and Vijay K. Kale, “A study of risk-based authentication system in cyber security using machine learning,” *World Journal of Advanced Engineering Technology and Sciences*, vol. 7, no. 2, 2022, doi: 10.30574/wjaets.2022.7.2.0125.

[126]J. Yin and J. Cui, “Secure authentication scheme in 6G-enabled mobile Internet of things for online English education,” *IET Networks*, vol. 11, no. 5, 2022, doi: 10.1049/ntw2.12048.

[127]A. F. Baig and S. Eskeland, “Security, privacy, and usability in continuous authentication: A survey,” *Sensors*, vol. 21, no. 17. 2021. doi: 10.3390/s21175967.

[128]G. Kumar, “Smartphone Authentication with Lightweight Deep Learning.” Oct. 2023. doi: 10.36227/techrxiv.22721044.v1.

[129]G. Dahia, L. Jesus, and M. Pamplona Segundo, “Continuous authentication using biometrics: An advanced review,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 10, no. 4. 2020. doi: 10.1002/widm.1365.

[130]T. Phillips *et al.*, “AuthN-AuthZ: Integrated, User-Friendly and Privacy-Preserving Authentication and Authorization,” in *Proceedings - 2020 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2020*, 2020. doi: 10.1109/TPS-ISA50397.2020.00034.

[131]L. Fridman, S. Weber, R. Greenstadt, and M. Kam, “Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location,” *IEEE Syst J*, vol. 11, no. 2, 2017, doi: 10.1109/JSYST.2015.2472579.

[132]E. Huang, F. Di Troia, and M. Stamp, “Evaluating Deep Learning Models and Adversarial Attacks on Accelerometer-Based Gesture Authentication,” in *Advances in Information Security*, vol. 54, 2022. doi: 10.1007/978-3-030-97087-1_10.

[133]Н. Панкратова and М. Згуровський, *Основи системного аналізу*. Київ: BHV, 2007.

[134]I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. in Adaptive Computation and Machine Learning series. MIT Press, 2016. [Online]. Available: https://books.google.com.ua/books?id=Np9SDQAAQBAJ

[135]P. Casale, O. Pujol, and P. Radeva, “Activity Recognition from Single Chest-Mounted Accelerometer,” *UCI Machine Learning Repository*. 2014. doi: https://doi.org/10.24432/C56P5J.

[136]Q. Yang *et al.*, “Poster abstract: A multimodal data set for evaluating continuous authentication performance in smartphones,” in *SenSys 2014 - Proceedings of the 12th ACM Conference on Embedded Networked Sensor Systems*, 2014. doi: 10.1145/2668332.2668366.

[137]Z. Sitova *et al.*, “HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, 2016, doi: 10.1109/TIFS.2015.2506542.

[138]M. El-Abed, C. Charrier, and C. Rosenberger, “Evaluation of Biometric Systems,” *New Trends and Developments in Biometrics*, Oct. 2012, doi: 10.5772/52084.

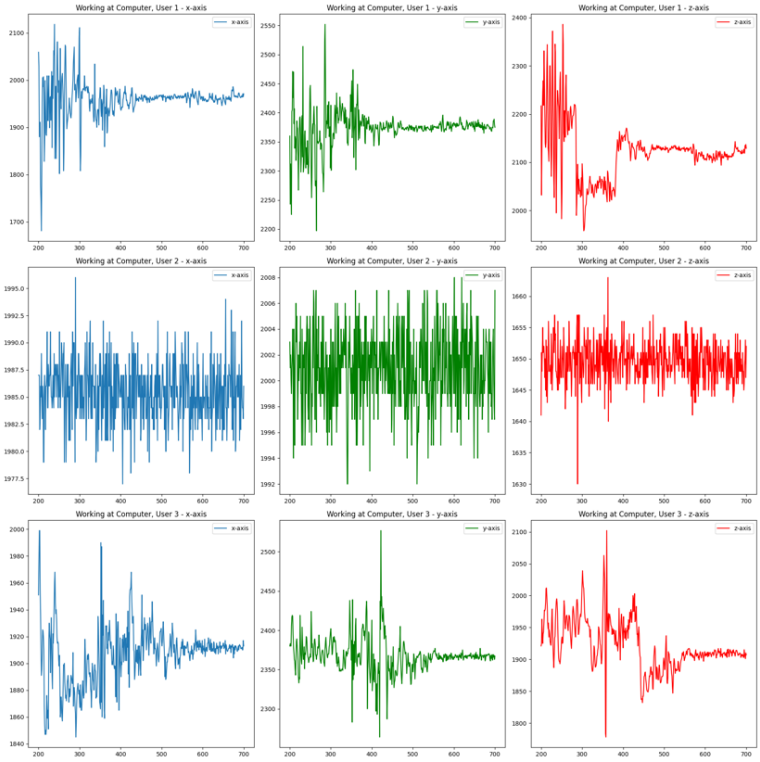
[139]P. Casale, O. Pujol, and P. Radeva, “Personalization and user verification in wearable systems using biometric walking patterns,” in *Personal and Ubiquitous Computing*, 2012. doi: 10.1007/s00779-011-0415-z.

[140]T. Burr and K. Kaufeld, “Change Detection by Monitoring Residuals from Time Series Models,” in *Time Series Analysis*, R. Abdalla, M. El-Diasty, A. Kostogryzov, and N. Makhutov, Eds., Rijeka: IntechOpen, 2022, p. Ch. 6. doi: 10.5772/intechopen.103129.

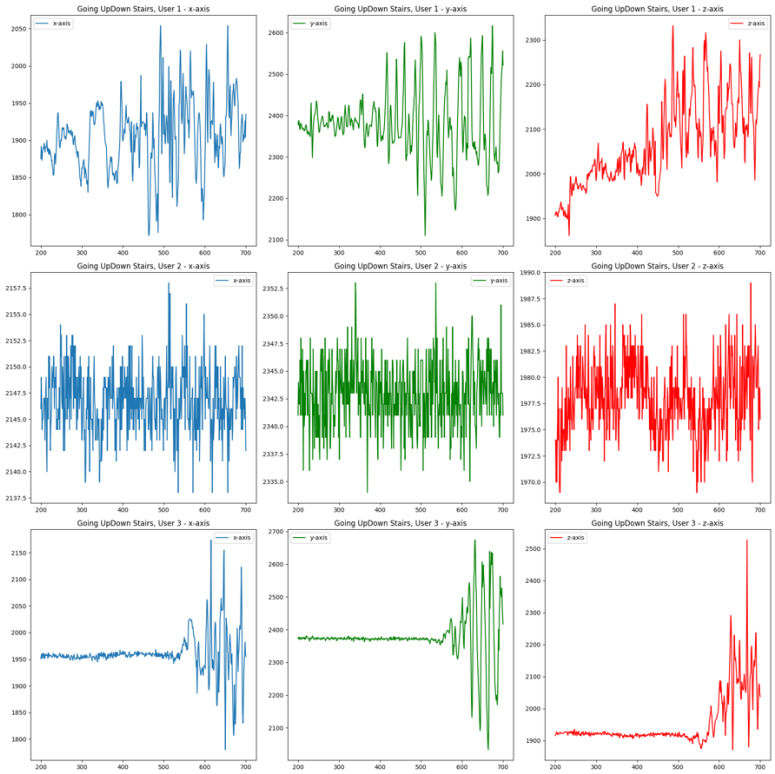
[141]“HFDA,” GitHub. URL: https://github.com/hiroki-kojima/HFDA (accessed 11.03.2024)

ДОДАТОК А

Приклади показів давача акселерометра для різних типів активностей [135].

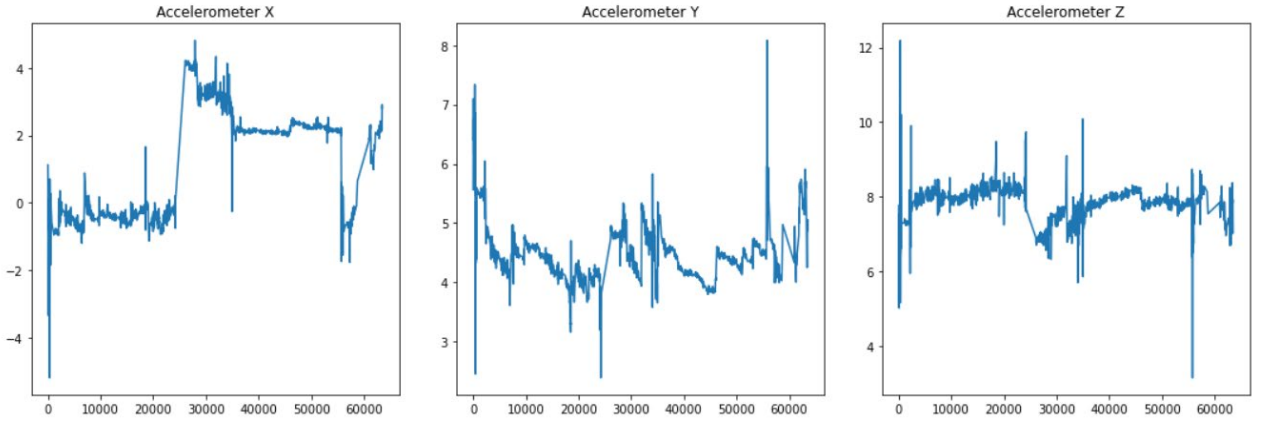


а)

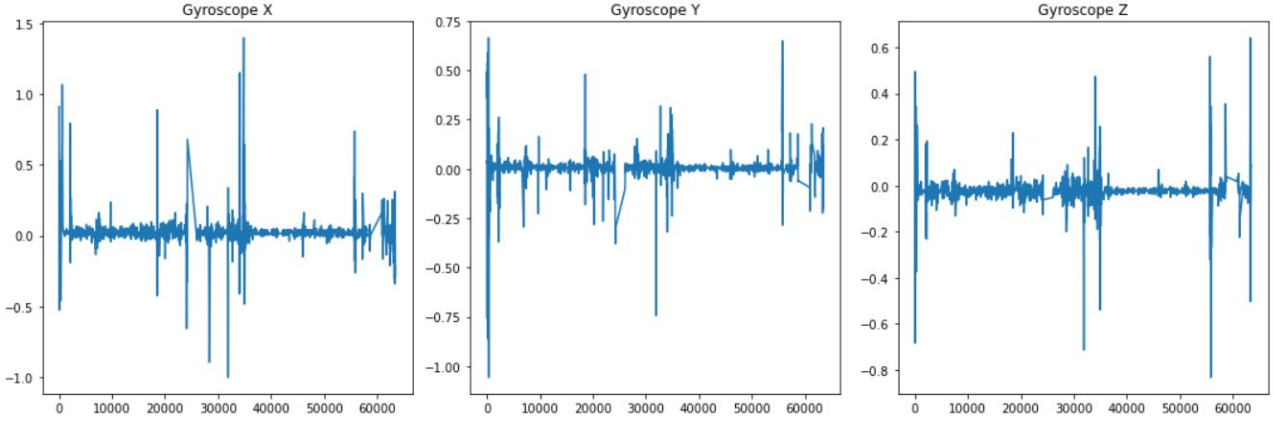


б)

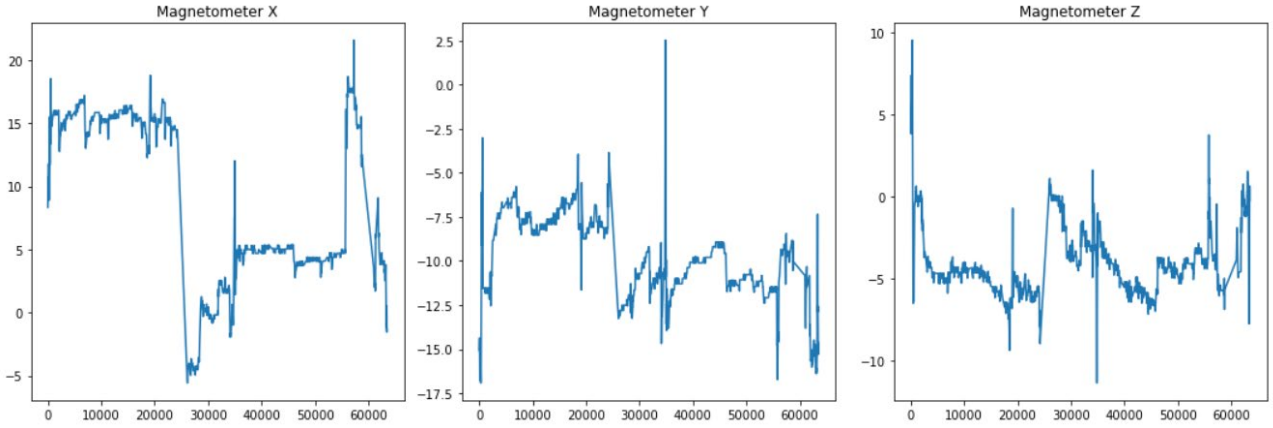
Рисунок А.1. - Демонстрація графіків значень осей акселерометра датасету SCMA для а) роботи за комп’ютером; б) підняття по сходам.



а)



б)

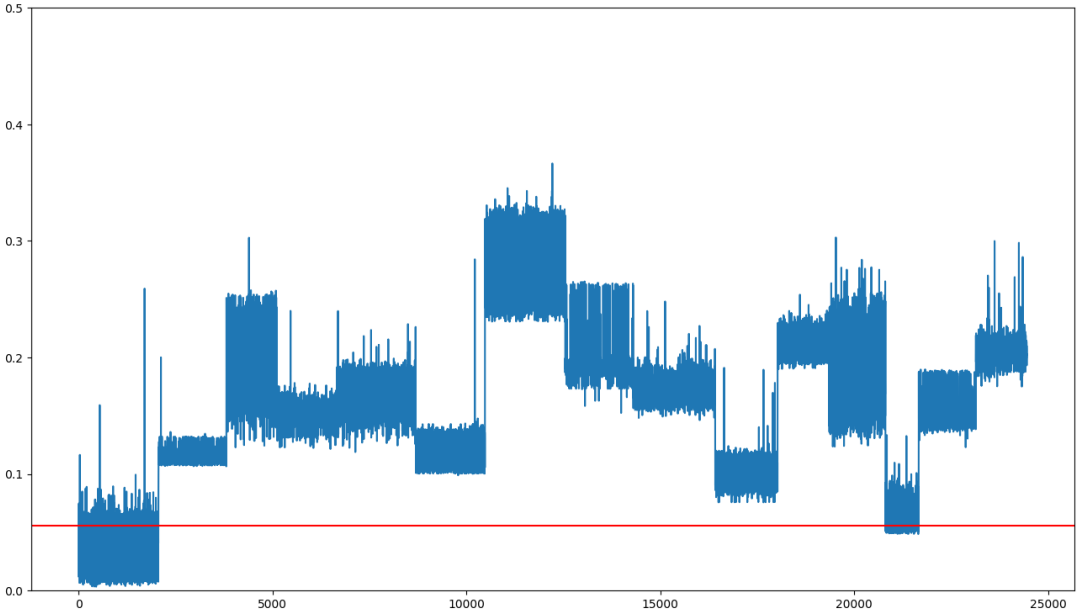


в)

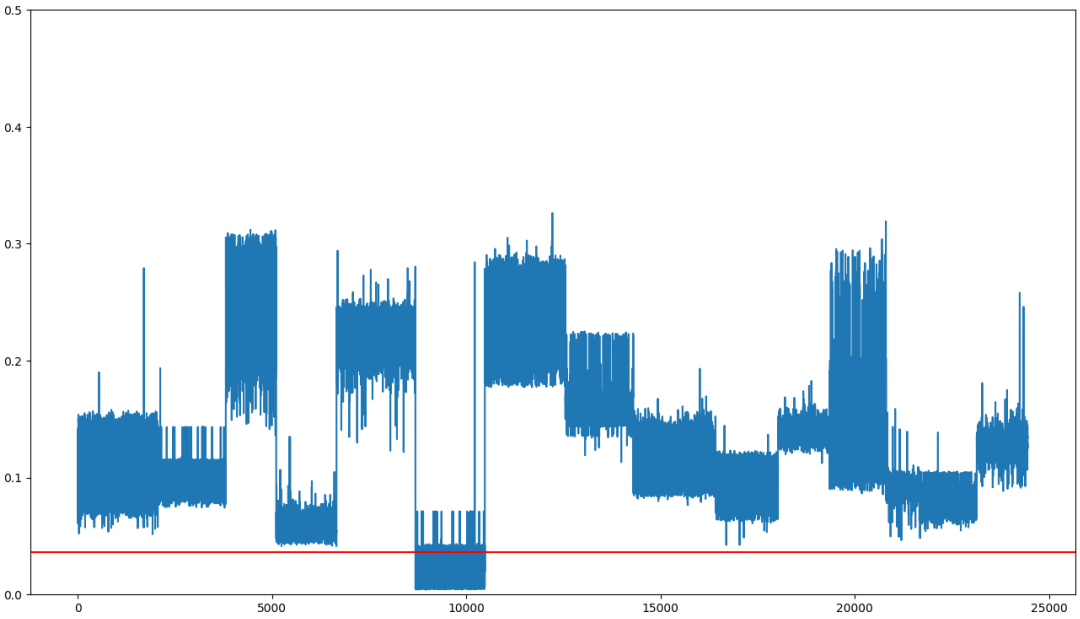
Рисунок А.2. - Демонстрація графіків значень осей а) акселерометра б) гіроскопа та в) магнетометра для одного користувача на датасеті H-MOG.

ДОДАТОК Б

Запропонований зручний інтерфейс представлення результатів роботи моделі для експрес-оцінки якості досліджуваних архітектур.



а)



б)

Рисунок Б.1. - Демонстрація порогового значення (червона лінія) відносно значень похибки реконструкції автокодувальника (сині покази) на прикладі SCMA датасету для 1-го користувача (а) та 6-го користувача (б).

Датасет містить покази нагрудного акселерометра для 15 користувачів. Сині покази це значення похибки реконструкції моделі автокодувальника. Червона риска це значення обраного порогу верифікації (за формулою 2.1), по якій визначається, чи користувач “легітимний” чи ні. На малюнку чітко видно розділення по значеннях похибки по кожному користувачу (в розглянутому випадку 15 користувачів). На рис. Б.1 а) перший користувач є “легітимним”, а на рисунку б) 6-й користувач, тому значення похибки реконструкції є меншими за заданий поріг верифікації (на малюнку знаходиться під червоною рискою).

ДОДАТОК В

Лістинг програми

Код реалізований за допомогою бібліотеки Keras, на бекенді Tensorflow. Фрактальна розмірність рохраховувалася за допомогобю пакету hfda. Наведено головні складові підготовки даних та тренування деяких архітектур.

Підготовка та попередня обробка даних.

```
#create inputs in shape (num_of_samples, window_size, features)
import statistics
import hfda
import time
kmax=10
window_len=52

#create inputs in shape (num_of_samples, window_size, features)
def create_inputs(window_len, df, axis_list = ['x-axis', 'y-axis', 'z-
axis']):
    segments = []
    labels = []
    step = int(window_len/2)
    sdf = df.copy()
    for i in range(0, df.shape[0] - window_len, step):
        axises = list()
        for col in axis_list:
            win = sdf[col].values[i: i + window_len]
            axises.append(win)
        label = statistics.mode(df['label'][i: i + window_len])#.mode[0]
        axises = np.stack(axises, axis=-1)
        segments.append(axises)
        labels.append(label)
    reshaped_segments = np.asarray(segments, dtype= np.float32)
    # .reshape(-1, window_len,len(axis_list))# 3)
    labels = np.asarray(labels, dtype = np.float32)
    return (reshaped_segments, labels)

#create inputs in shape (num_of_samples, window_size, features) with higuchi
fractal dimension
def modified_create_inputs(window_len, df, axis_list=['x-axis', 'y-axis',
'z-axis'], k_max=10):
    segments = []
    labels = []
    step = int(window_len / 2)
    sdf = df.copy()
    for i in range(0, df.shape[0] - window_len, step):
        axises = []
        for col in axis_list:
            win = sdf[col].values[i: i + window_len]
            s = time.time()
            fractal_dim = hfda.measure(win, k_max)  # Calculate fractal
dimension for the window
            e = time.time()
            extended_win = np.append(win, fractal_dim)  # Append fractal
dimension to window data
            axises.append(extended_win)
            print(e-s)
        label = statistics.mode(df['label'][i: i + window_len])
        axises = np.stack(axises, axis=-1)
        segments.append(axises)
```

```
        labels.append(label)

    reshaped_segments = np.asarray(segments, dtype=np.float32)
    labels = np.asarray(labels, dtype=np.float32)
    return reshaped_segments, labels
```

```
def fit_scalers(train_data, window_length, axis_list=['x-axis', 'y-axis',
'z-axis']):
    scalers = {}
    for axis in axis_list:
        scaler = MinMaxScaler()
        axis_index = axis_list.index(axis)
        # Extracting the relevant part of the window for scaling
        axis_data = np.concatenate(train_data[:, :window_length,
axis_index])
        scaler.fit(axis_data.reshape(-1,1))  # Reshape for fitting
        scalers[axis] = scaler
    return scalers

def apply_scalers(X, scalers, window_length, axis_list=['x-axis', 'y-axis',
'z-axis']):
    transformed_X = np.copy(X)
    for i, axis in enumerate(axis_list):
        # Apply scaling to the relevant part of the window
        transformed_X[:, :window_length, i] = scalers[axis].transform(X[:,
:window_length, i].reshape(-1, 1)).reshape(-1, window_length)
    return transformed_X
```

Поділ на тренувальний та тестовий датасет.

```
from sklearn.preprocessing import MinMaxScaler
#train_test_split
train_test_nn = []
for i in range(len(data)):
    seg = create_inputs(52, data[i], axis_list = ['x-axis', 'y-axis', 'z-
axis'])
    X_train, X_test, y_train, y_test = train_test_split(
            seg[0], seg[1], stratify=seg[1], test_size=0.33,
random_state=42)
    scalers = fit_scalers(X_train, window_length=52)
    X_train_scaled = apply_scalers(X_train, scalers, window_length=52)
    X_test_scaled = apply_scalers(X_test, scalers, window_length=52)
    train_test_nn.append((X_train_scaled, X_test_scaled))
```

Гібридний автокодувальник на базі трансформера.

```
import tensorflow as tf
from tensorflow.keras.layers import Input, Dense, Dropout,
GlobalAveragePooling1D, RepeatVector, TimeDistributed
```

```
from tensorflow.keras.models import Model
from tensorflow.keras.optimizers import Adam

def transformer_encoder_block(input_layer, num_heads, intermediate_dim,
dropout_rate):
    # Layer normalization
    norm1 = tf.keras.layers.LayerNormalization(epsilon=1e-6)(input_layer)
    # Multi-head attention
    attention_output =
tf.keras.layers.MultiHeadAttention(num_heads=num_heads,
key_dim=intermediate_dim)(norm1, norm1)
    # Skip connection and dropout
    attention_output = Dropout(dropout_rate)(attention_output)
    attention_output = tf.keras.layers.Add()([attention_output,
input_layer])
    # Layer normalization
    norm2 = tf.keras.layers.LayerNormalization(epsilon=1e-
6)(attention_output)
    # 1D Convolution layers
    conv_output = tf.keras.layers.Conv1D(filters=12, kernel_size=1,
activation='relu')(norm2)
    conv_output = Dropout(dropout_rate)(conv_output)
    conv_output = tf.keras.layers.Conv1D(filters=3, kernel_size=1,
activation='relu')(conv_output)
    # Addition (Conv1D output + Addition output from the start of the block)
    output_layer = tf.keras.layers.Add()([conv_output, attention_output])
    return output_layer

def create_transformer_autoencoder(input_shape, num_heads, intermediate_dim,
latent_dim, dropout_rate):
    # Input layer
    inputs = Input(shape=input_shape)

    # Encoder with transformer blocks
    x = inputs
    for _ in range(2):  # Assuming 2 transformer blocks
        x = transformer_encoder_block(x, num_heads, intermediate_dim,
dropout_rate)

    # Global average pooling and dense layers
    x = GlobalAveragePooling1D()(x)
    x = Dense(32, activation='relu')(x)
    x = Dropout(dropout_rate)(x)
    encoded = Dense(latent_dim, activation='relu')(x)

    # Repeat vector
    x = RepeatVector(input_shape[0])(encoded)

    # Decoder (for simplicity, we are not implementing transformer blocks in
the decoder)
    x = Dense(intermediate_dim, activation='relu')(x)
```

```
    x = Dropout(dropout_rate)(x)
    x = Dense(input_shape[-1], activation='sigmoid')(x)  # Assuming sigmoid
activation for reconstruction

    # Create autoencoder model
    autoencoder = Model(inputs, x)
    autoencoder.compile(optimizer=Adam(), loss='mae')

    return autoencoder
```

Рекурентний автокодувальник.

```
from keras.regularizers import l1, l2
import keras
from keras.layers import Dropout
l1_rate = 0.1
l2_rate = 0
def create_auto_lstm(dropout_rate):
    model = Sequential()
    model.add(LSTM(30, activation="relu", input_shape=(timesteps,dim),
kernel_regularizer=l1(l1_rate), recurrent_regularizer=l2(l2_rate)))#,
return_sequences=True))
    # model.add(BatchNormalization())
    model.add(RepeatVector(timesteps))
    model.add(Dropout(rate=dropout_rate))
    model.add(LSTM(20, activation='relu', return_sequences=True,
kernel_regularizer=l1(l1_rate), recurrent_regularizer=l2(l2_rate)))
    # model.add(BatchNormalization())
    model.add(LSTM(30, activation='relu', return_sequences=True,
kernel_regularizer=l1(l1_rate), recurrent_regularizer=l2(l2_rate)))
    model.add(TimeDistributed(Dense(dim)))
    model.compile(optimizer='adam', loss='mae')
    return model
```

Тренування моделі та розрахунок основних метрик якості.

```
import numpy as np
from scipy.optimize import brentq
from scipy.interpolate import interp1d
from sklearn.metrics import roc_curve
import matplotlib.pyplot as plt
from sklearn.metrics import mean_absolute_error, classification_report,
roc_curve, auc
from keras.layers import BatchNormalization
timesteps=52
fpr_tpr = []
roc_aucs = []
eers = []  # List to store EER for each user

for i, (X_train, X_test) in enumerate(train_test_nn):
```

```
    # model, _, _ = create_lstm_vae(timesteps=timesteps, input_dim=dim,
batch_size=24, intermediate_dim=24, latent_dim=12)
    model = create_auto_lstm(dropout_rate=0.8)
    history = model.fit(X_train, X_train, epochs=10, verbose=1,
batch_size=24)

    # Predict on the test set
    predictions = model.predict(X_test)

    # Calculate MAE for the test set of the current user (i)
    mae_test = np.mean(np.abs(predictions - X_test), axis=(1,2))

    # Calculate the threshold as mean + std of MAE
    threshold = np.mean(mae_test) + np.std(mae_test)

    # Initialize lists for true labels and predicted MAE
    anomaly_true = []
    mae_pred = []



    # Iterate over all users' data
    for j, (_, X_test_j) in enumerate(train_test_nn):
        # Predict on the test set of user j
        predictions_j = model.predict(X_test_j)
        mae_j = np.mean(np.abs(predictions_j - X_test_j), axis=(1,2))

        # Append the results
        anomaly_true.extend([1 if i == j else -1] * len(mae_j))
        mae_pred.extend(mae_j)

    # Determine anomalies based on threshold
    anomaly_pred = [1 if x < threshold else -1 for x in mae_pred]

    # Calculate and print classification report
    print(classification_report(anomaly_true, anomaly_pred))

    # ROC and AUC
    fpr, tpr, _ = roc_curve(anomaly_true, anomaly_pred)
    fpr_tpr.append((fpr, tpr))
    roc_aucs.append(auc(fpr, tpr))
    # EER calculation
    eer = brentq(lambda x: 1. - x - interp1d(fpr, tpr)(x), 0., 1.)
    eers.append(eer)


    # Plotting MAE
    y = np.asarray(mae_pred, dtype=np.float32)
    x = np.arange(len(y))
    plt.rcParams["figure.figsize"] = [16,9]
    plt.ylim(0, 0.5)
```

```
    plt.plot(x, y)
    plt.axhline(y=threshold, color='r')
    plt.show()
```

ДОДАТОК Г

Таблиця Г.1

Type	Output Shape	# of Params
LSTM	(None, 20)	1920
RepeatVector	(None, 52, 20)	0
Dropout	(None, 52, 20)	0
LSTM	(None, 52, 10)	1240
LSTM	(None, 52, 20)	2480
TimeDistributed	(None, 52, 3)	63

Таблиця Г.2

Type	Output Shape	# of Params
LSTM	(None, 20)	1920
BatchNormalization	(None, 20)	80
RepeatVector	(None, 52, 20)	0
Dropout	(None, 52, 20)	0
LSTM	(None, 52, 10)	1240
BatchNormalization	(None, 52, 10)	40
LSTM	(None, 52, 20)	2480
TimeDistributed	(None, 52, 3)	63

Таблиця Г.3

Type	Output Shape	# of Params
LSTM	(None, 30)	4080

RepeatVector	(None, 52, 30)	0
Dropout	(None, 52, 30)	0
LSTM	(None, 52, 20)	4080
LSTM	(None, 52, 30)	6120
TimeDistributed	(None, 52, 3)	93