Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили

Кваліфікаційна наукова
праця на правах рукопису

Медвінський Сергій Віталійович

УДК 004.93:004.056;57.087.1

ДИСЕРТАЦІЯ

СИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА КОМП'ЮТЕРНОЇ СИСТЕМИ ЗА ДИНАМІЧНИМИ БІОМЕТРИЧНИМИ ПАРАМЕТРАМИ

Спеціальність 123 Комп'ютерна інженерія
Галузь знань 12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник Журавська Ірина Миколаївна, д-р техн. наук, професор

Миколаїв – 2026

АНОТАЦІЯ

Медвінський С. В. Система ідентифікації користувача комп’ютерної системи за динамічними біометричними параметрами**.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 Комп’ютерна інженерія. – Чорноморський національний університет імені Петра Могили, Миколаїв, 2026.

Дисертаційна робота присвячена мінімізації можливостей для несанкціонованого доступу до інформації шляхом розроблення новітніх конструкцій та алгоритмів роботи апаратних засобів ідентифікації користувачів, що є базовим та найбільш відповідальним етапом процесу авторизації в комп'ютерних системах (КС).

Сучасні біометричні системи ідентифікації та авторизації характеризуються значним різноманіттям, але мають різну ефективність та рівень захищеності. Традиційні методи, такі як сканування відбитків пальців чи розпізнавання обличчя, демонструють вразливості до сучасних атак з використанням технологій глибоких фейків та 3D-моделювання. У цій роботі досліджуються перспективні методи на основі аналізу судинної мережі ока, які поєднують високу унікальність, складність підробки та зручність безконтактного використання.

Поставлені дослідницькі задачі безпосередньо пов'язані з галуззю комп'ютерного зору та штучного інтелекту (ШІ), які є складовими частинами сучасної інформатики. Для їх вирішення необхідно застосовувати комплексний підхід, що включає: застосування методів цифрової обробки зображень та pattern recognition; використання сучасних інструментів машинного навчання, зокрема згорткових нейронних мереж; розробку алгоритмів перевірки, чи використовуються дані живої людини (надалі – живості, англ. Liveness Detection) для запобігання спуфінг-атакам; оптимізацію обчислювальних алгоритмів для роботи в режимі реального часу; інтеграцію апаратних та програмних рішень у

єдину функціональну систему.

Зазначений комплексний підхід вимагає поєднання досліджень з питань кібербезпеки, біометрії, обробки зображень та машинного навчання. Сучасний ринок технологій безпеки демонструє зростаючий попит на надійні біометричні рішення, що підтверджує актуальність та практичну значущість даного дослідження.

У вступі обґрунтовано актуальність проблематики безпеки ідентифікації та авторизації та недоліки існуючих методів (паролі, статична біометрика), наведено зв’язок дисертації з науково-дослідними роботами, сформовано та представлено мету і задачі дослідження, розглянуто об’єкт, предмет та методи дослідження, наведено наукову новизну та практичне значення отриманих результатів. Також надано інформацію щодо особистого внеску здобувача та публікацій за темою дисертаційного дослідження.

Перший розділ дисертації містить огляд сучасних традиційних методів ідентифікації та авторизації. Аналіз статичних біометричних методів (відбитки, обличчя, райдужка) та їх вразливостей (спуфінг, відтворення). Аналіз динамічних/поведінкових біометричних методів (динаміка клавіатури, руху миші, хода, голос). Існуючі методи сканування судин очей (склеральна біометрика) – їх переваги (унікальність, складність підробки) та недоліки (вимоги до якості зображення). Висновок про необхідність гібридних або мультимодальних підходів для підвищення надійності.

Другий розділ дисертації детально висвітлює практичну реалізацію системи сканування, зосереджуючись на створенні апаратного макету та розробці відповідного програмного забезпечення для обробки зображень.

Апаратна платформа системи базується на одноплатному мікрокомп'ютері Raspberry Pi, який виконує функцію центрального обчислювального блоку. Як основний сенсор використана високоякісна камера Raspberry Pi HQ Camera з сенсором OmniVision OV5647, що забезпечує необхідну роздільну здатність для детальної фіксації дрібних капілярів. Для отримання чіткого збільшеного зображення застосовано макрооб'єктив з фіксованою фокусною відстанню.

Критично важливим елементом є інфрачервоний діод (англ. Near-Infrared, NIR) з довжиною хвилі 880 нм, призначений для підсвічування судинної мережі в умовах недостатнього зовнішнього освітлення та підвищення контрастності зображення. Для підвищення ергономіки та збереження поля зору користувача запропоновано інноваційне використання оптичного «гарячого дзеркала» (англ. Hot Mirror), яке дозволяє відокремити шлях камери від прямої лінії зору. Додатково система інтегрує гіроскоп/акселерометр GY-521 (MPU-6050) для корекції положення голови та літій-полімерну акумуляторну батарею з контролером заряду TP4056 для забезпечення автономної роботи.

Програмна складова реалізована на мові Python з активним використанням бібліотек комп'ютерного зору OpenCV та наукових обчислень NumPy. Алгоритмічна частина представляє собою послідовний конвеєр обробки зображень. Він починається із захоплення вихідного кадру та його перетворення в одноканальне зображення у відтінках сірого для зменшення обсягу даних. Наступним кроком є визначення чітко окресленої області інтересу (англ. Region of Interest, ROI) у внутрішньому кутку ока, що дозволяє значно скоротити обчислювальні витрати шляхом фокусування на інформативній ділянці.

Для підсилення видимості капілярів застосовано метод адаптивного обмеженого підвищення контрасту (англ. Contrast Limited Adaptive Histogram Equalization, CLAHE), який ефективно виділяє судини на тлі склери. Фінальні етапи обробки включають бінаризацію, виділення чітких контурів за допомогою детектора країв Кенні та морфологічну обробку для очищення зображення від шуму та усунення розривів у контурах судин. Для забезпечення зв'язку із зовнішніми пристроями реалізовано мережеву взаємодію через вбудований WiFi-модуль Raspberry Pi.

Таким чином, у другому розділі представлено повноцінний апаратно-програмний комплекс, який готовий до експериментальних досліджень та реалізує повний цикл отримання та високоякісної попередньої обробки зображень капілярної мережі кон'юнктиви в режимі реального часу.

Третій розділ присвячений реалізації математичного і алгоритмічного

апарату, що перетворює попередньо оброблене зображення на цифровий біометричний шаблон. Основна увага приділяється завершальним етапам конвеєру обробки, які безпосередньо відповідають за точність ідентифікації.

Розділ відкривається описом етапу виділення та фільтрації контурів. Алгоритм аналізує бінарне зображення, знаходить усі контури та фільтрує їх за розміром, відсіюючі дрібний шум і великі артефакти, залишаючи лише структури, що відповідають капілярам.

Наступна частина розділу повністю присвячена методам порівняння. Детально описується архітектура та принцип роботи сіамської нейронної мережі (англ. Siamese Neural Network, SNN), яка використовується для порівняння двох зображень капілярної мережі. Пояснюється, як мережа навчається перетворювати зображення в числові вектори-дескриптори та обчислювати відстань між ними, визначаючи ступінь схожості. Ключову роль у цьому процесі відіграє контрастна функція втрат (англ. Contrastive Loss), яка керує навчанням мережі.

Крім того, у розділі порівнюються різні підходи до вирівнювання зображень, такі як фазова кореляція (Phase-Only Correlation) та оптичний потік (Optical Flow), необхідні для точного суміщення знімків, зроблених під різними кутами.

Третій розділ представляє завершену алгоритмічну модель, яка перетворює відеопотік ока на надійний біометричний ідентифікатор, обґрунтовуючи вибір методів їхньою ефективністю та стійкістю до несанкціонованого доступу.

Четвертий розділ дисертації є практичною демонстрацією ефективності розроблених апаратних та алгоритмічних рішень. Він присвячений експериментальному тестуванню системи, аналізу отриманих результатів та порівнянню з існуючими аналогами.

Метою розділу є об'єктивна оцінка точності, швидкодії та надійності запропонованого методу ідентифікації в різних умовах експлуатації. Розділ починається з опису методології проведення експериментів, включаючи формування тестової вибірки даних, вибір критеріїв оцінки (таких як FAR – False Acceptance Rate, FRR – False Rejection Rate, EER – Equal Error Rate та середній час

обробки) та опис умов тестування.

Основну частину розділу складає детальний аналіз результатів. Досліджується вплив якості освітлення на точність ідентифікації, демонструючи, як продуктивність системи змінюється від 84.8% при стандартному освітленні до 63,2 % в умовах низької освітленості, що обґрунтовує необхідність використання NIR-підсвітки. Аналізується часові характеристики кожного етапу алгоритму, що підтверджує можливість роботи в реальному часі із середньою швидкістю обробки 0,32 секунди на кадр.

Важливе місце займає тестування стійкості системи до спуфінг-атак, зокрема з використанням фотографій. Наводяться дані, що підтверджують високу ефективність методу Pulse Transit Time (PTT) для виявлення «живості», що дозволяє досягти дуже низького рівня помилок (EER 0,01 %).

Завершується розділ порівняльним аналізом із традиційними біометричними методами, такими як розпізнавання обличчя, відбитків пальців та райдужки. Наводяться таблиці з порівнянням ключових метрик (FAR, FRR, час авторизації, вартість впровадження), які наочно демонструють конкурентні переваги запропонованого рішення, зокрема його високу стійкість до підробки та зручність безконтактного використання.

У **висновках** узагальнено основні результати дослідження та встановлено перспективні напрями вдосконалення методів біометричної ідентифікації. Запропонований метод ідентифікації на основі аналізу капілярної мережі кон'юнктиви ока продемонстрував високу ефективність, що підтверджує його практичну цінність для застосування в сучасних системах безпеки та медичного моніторингу.

Розроблені алгоритми та апаратні рішення забезпечують значне підвищення надійності ідентифікації порівняно з традиційними біометричними методами на основі статичних параметрів, здатність протидіяти спуфінг-атакам та можливість безконтактної роботи. Використання запропонованого підходу дозволяє забезпечити безперервну аутентифікацію, зменшити ймовірність несанкціонованого доступу та автоматизувати процес ідентифікації користувачів.

Запропонований підхід забезпечує не лише високоточну ідентифікацію користувача, але й формує підґрунтя для його подальшої авторизації в комп'ютерній системі шляхом зіставлення отриманого ідентифікатора з відповідними правами доступу.

Ключові слова: *інформаційна система, біометрична ідентифікація, капіляри кон'юнктиви, безконтактна ідентифікація, обробка зображень ока, розпізнавання, комп'ютерний зір, трекінг погляду, сіамські нейронні мережі, Raspberry Pi, глибоке навчання, машинне навчання, медичні дані, безпека, надійність.*

ABSTRACT

Medvinsky S. V. Computer system user identification system based on dynamic biometric parameters. – Qualification scientific work on manuscript rights.

Dissertation for the degree of Doctor of Philosophy in the specialty 123 Computer Engineering. – Petro Mohyla Black Sea National University, Mykolaiv, 2026.

The dissertation is devoted to minimizing the possibilities for unauthorized access to information with limited access and developing the latest designs and algorithms for hardware authorization in the CS.

The introduction substantiates the relevance of the issue of identification and authorization security and the shortcomings of existing methods (passwords, static biometrics), provides a connection between the dissertation and research works, formulates and presents the goal and objectives of the study, considers the object, subject and methods of the study, provides scientific novelty and practical significance of the results obtained. Information is also provided on the personal contribution of the applicant and publications on the topic of the dissertation research.

The first section of the dissertation contains an overview of modern traditional identification and authorization methods. Analysis of static biometric methods (fingerprints, face, iris) and their vulnerabilities (spoofing, reproduction). Analysis of dynamic/behavioral biometric methods (keyboard dynamics, mouse movement, gait,

voice). Existing methods of scanning eye vessels (scleral biometrics) - their advantages (uniqueness, difficulty of forgery) and disadvantages (image quality requirements). Conclusion on the need for hybrid or multimodal approaches to increase reliability.

The second section of the thesis details the practical implementation of the scanning system, focusing on the creation of a hardware layout and the development of the corresponding software for image processing.

The hardware platform of the system is based on a single-board microcomputer Raspberry Pi, which acts as a central processing unit. The main sensor is a high-quality Raspberry Pi HQ Camera with an OmniVision OV5647 sensor, which provides the necessary resolution for detailed fixation of small capillaries. To obtain a clear enlarged image, a macro lens with a fixed focal length is used. A critically important element is an infrared diode (NIR) with a wavelength of 880 nm, designed to illuminate the vascular network in conditions of insufficient external lighting and increase image contrast. To improve ergonomics and preserve the user's field of view, an innovative use of an optical "hot mirror" is proposed, which allows separating the camera path from the direct line of sight. Additionally, the system integrates a GY-521 (MPU-6050) gyroscope/accelerometer for head position correction and a lithium-polymer battery with a TP4056 charge controller for autonomous operation.

The software component is implemented in Python with active use of OpenCV computer vision libraries and NumPy scientific computing. The algorithmic part is a sequential image processing pipeline. It begins with capturing the original frame and converting it into a single-channel grayscale image to reduce the amount of data. The next step is to define a clearly defined region of interest (ROI) in the inner corner of the eye, which allows significantly reducing computational costs by focusing on the informative area. To enhance the visibility of capillaries, the adaptive limited contrast enhancement (CLAHE) method was used, which effectively highlights vessels against the background of the sclera. The final processing stages include binarization, selection of clear contours using a Kenny edge detector, and morphological processing to clean the image from noise and eliminate breaks in the vascular contours. To ensure communication with external devices, network interaction is implemented via the built-

in Raspberry Pi Wi-Fi module.

Thus, the second section presents a full-fledged hardware and software complex that is ready for experimental research and implements a full cycle of obtaining and high-quality pre-processing of images of the conjunctival capillary network in real time.

The third section is devoted to the implementation of a mathematical and algorithmic apparatus that converts a pre-processed image into a digital biometric template. The main attention is paid to the final stages of the processing pipeline, which are directly responsible for the accuracy of identification.

The section opens with a description of the stage of contour extraction and filtering. The algorithm analyzes a binary image, finds all contours and filters them by size, filtering out small noise and large artefacts, leaving only structures corresponding to capillaries.

The next part of the section is entirely devoted to comparison methods. The architecture and principle of operation of the Siamese Neural Network, which is used to compare two images of a capillary network, is described in detail. It is explained how the network learns to convert images into numerical descriptor vectors and calculate the distance between them, determining the degree of similarity. The key role in this process is played by the contrast loss function (Contrastive Loss), which controls the training of the network.

In addition, the section compares different approaches to image alignment, such as Phase-Only Correlation and Optical Flow, required to accurately align images taken at different angles. The third section presents a completed algorithmic model that transforms the eye video stream into a reliable biometric identifier, justifying the choice of methods by their efficiency and resistance to unauthorized access.

The fourth section of the dissertation is a practical demonstration of the effectiveness of the developed hardware and algorithmic solutions. It is devoted to experimental testing of the system, analysis of the obtained results and comparison with existing analogues.

The purpose of the section is to objectively assess the accuracy, speed and reliability of the proposed identification method in various operating conditions. The

section begins with a description of the methodology for conducting experiments, including the formation of a test data sample, the selection of evaluation criteria (such as FAR – False Acceptance Rate, FRR – False Rejection Rate, EER – Equal Error Rate and average processing time) and a description of the testing conditions.

The main part of the section consists of a detailed analysis of the results. The influence of lighting quality on the accuracy of identification is studied, demonstrating how the system performance changes from 84.8% under standard lighting to 63.2% under low lighting conditions, which justifies the need to use NIR illumination. The time characteristics of each stage of the algorithm are analyzed, which confirms the possibility of working in real time with an average processing speed of 0.32 seconds per frame.

An important place is occupied by testing the system's resistance to spoofing attacks, in particular using photographs. Data are provided confirming the high efficiency of the Pulse Transit Time (PTT) method for detecting "liveness", which allows achieving a very low error rate (EER 0.01%).

The section concludes with a comparative analysis with traditional biometric methods, such as face, fingerprint and iris recognition. Tables are provided with a comparison of key metrics (FAR, FRR, authorization time, implementation cost), which clearly demonstrate the competitive advantages of the proposed solution, in particular its high resistance to counterfeiting and the convenience of contactless use.

The conclusions summarize the main results of the study and identify promising areas for improving biometric identification methods. The proposed identification method based on the analysis of the capillary network of the conjunctiva of the eye demonstrated high efficiency, which confirms its practical value for use in modern security and medical monitoring systems.

The developed algorithms and hardware solutions provide a significant increase in the reliability of identification compared to traditional biometric methods, the ability to counteract spoofing attacks and the possibility of contactless operation. The use of the proposed approach allows for continuous authentication, reducing the likelihood of unauthorized access and automating the user identification process.

The proposed approach provides not only highly accurate user identification, but also forms the basis for his subsequent authorization in the computer system by comparing the received identifier with the corresponding access rights.

Keywords: *information system, biometric identification, conjunctiva capillaries, contactless identification, eye image processing, recognition, computer vision, gaze tracking, Siamese neural networks, Raspberry Pi, deep learning, machine learning, medical data, security, reliability.*

СПИСОК ОПУБЛІКОВАНИХ НАУКОВИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Медвінський С. В., Журавська І. М. Методи та алгоритми обробки зображень для біометричної ідентифікації за капілярною мережею кон'юнктиви ока. *Наука і техніка сьогодні.* 2026. Вип. 2 (56). С. 2028–2038. DOI: 10.52058/2786-6025-2026-2(56)-2028-2038.

2. Medvinskyi S. The use of cross-correlation as an interaction tool for computer systems by individuals with musculoskeletal disorders. *Infocommunication and Computer Technologies.* 2025. № 2 (10). С. 98–104. DOI: 10.36994/2788-5518-2025-02-10-12.

3. Medvinskyi S., Zhuravska I. Development of a method for processing eye images for use during biometric authorization in computer systems. *Electrotechnic and Computer Systems*. 2025. № 44 (120). С. 49–54. DOI: 10.15276/eltecs.44.120.2025.6.

4. Медвінський С. Авторизація користувача у комп’ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2023. Вип. 50. С. 71−77. DOI: 10.36910/6775-2524-0560-2023-50-10.

Праці, які засвідчують апробацію матеріалів дисертації

5. Медвінський С. Аналіз методів відслідковування напрямку погляду під час використання комп’ютерних систем. *Ольвійський форум – 2024 : стратегії країн Причорноморського регіону в геополітичному просторі* : зб. тез XXI Міжнар. наук. конф. 20–23 червня 2024 р., м. Миколаїв : тези / М-во освіти і науки України. Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 178–183.

6. Журавська І., Медвінський С. Динамічні біометричні показники ока для авторизації користувача в комп’ютерній системі. *Медико-технічна співпраця заради перемоги: актуальні завдання медичної, біологічної фізики та інформатики :* тези доп. III Наук.-практ. конф. з міжнар. участю, м. Вінниця,

07 квітня 2024 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2024. С. 53–56. URL: https://dspace.vnmu.edu.ua/handle/123456789/6560

7. Журавська І., Медвінський С. Авторизація користувача в комп'ютерній системі за допомогою малюнку капілярів хоріоідеї. *Актуальні завдання медичної, біологічної фізики та інформатики* : тези доп. II Всеукр. наук.-практ. конф. З міжнар. участю, Вінниця, 07 квітня 2023 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2023. С. 15–17.

8. Медвінський С. В., Журавська І. М. Програмне забезпечення для авторизації користувача у комп'ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Free and Open Source Software (FOSS-2023)* : тези доп. XIV Міжнар. наук.-практ. конф., Харків, 07–10 лютого 2023 р. Харків : ХНЕУ ім. Семена Кузнеця, 2023. С. 101–102.

9. Медвінський С. Використання динамічних біометричних показників для авторизації користувачів. *Могилянські читання – 2022* : тези доп. XXV Всеукр. наук.-практ. конф., Миколаїв, 07–11 листопада 2022 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2022. С. 73–75.

10. Журавська І. М., Медвінський С. В., Ухань Є. О. Упровадження EAP-TLS сертифікатів у Mikrotik з аутентифікацією користувачів за динамічними біометричними параметрами. *Могилянські читання – 2021* : тези доп. XXIV Всеукр. наук.-метод. конф., Миколаїв, 8–12 листоп. 2021 р., Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2021. С. 55–58.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 16
ВСТУП 17
РОЗДІЛ 1 АНАЛІЗ СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ 24
1.1 Аналіз існуючих методів біометричної ідентифікації 24
1.2 Аналіз переваг та ключових вразливостей статичних біометричних показників 28
1.3 Динамічна та поведінкова біометрика: перспективи та обмеження 32
1.4 Сучасні методи сканування судин очей: склеральна біометрика 40
Висновки до розділу 1 40
РОЗДІЛ 2 РОЗРОБКА АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ СКАНУВАННЯ КАПІЛЯРІВ КОН'ЮНКТИВИ 43
2.1 Апаратна реалізація системи 43
2.2 Програмне забезпечення та алгоритми обробки 46
2.3 Мережева взаємодія та інтеграція 50
2.4 Використання крос-кореляції як інструмента взаємодії з КС 51
Висновки до розділу 2 57
РОЗДІЛ 3 АЛГОРИТМИ ОБРОБКИ ЗОБРАЖЕНЬ, ВИДІЛЕННЯ БІОМЕТРИЧНИХ ОЗНАК ТА ЇХ РОЗПІЗНАВАННЯ 59
3.1 Виділення та фільтрація контурів 59
3.2 Методи порівняння та класифікації 62
3.3 Методи машинного навчання для класифікації та порівняння ознак 66
3.4 Вирівнювання зображень 69
3.5 Реалізація та оптимізація програмно-апаратного комплексу 71
Висновки до розділу 3 77
РОЗДІЛ 4 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ 78

4.1 Методологія проведення експериментів 78
4.2 Результати експериментальних досліджень 83
4.3 Оцінка швидкодії системи 88
4.4 Тестування стійкості до спуфінг-атак 93
4.5 Обговорення результатів 96
Висновки до розділу 4 101
ВИСНОВКИ 102
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 104
ДОДАТОК А Акти впровадження 118
А.1 Акт впровадження результатів в НДР 118
А.2 Акт впровадження результатів в навчальний процес 119
ДОДАТОК Б Програмний код формування та обробки датасету зовнішніх капілярів ока 119
ДОДАТОК В Список публікацій здобувача 123

ПЕРЕЛІК СКОРОЧЕНЬ

БД	– база даних
КС	– комп'ютерна система
НСД	– несанкціонований доступ
ШІ	– штучний інтелект
BGR	– Blue, Green, Red
CANNY/CED	– Canny Edge Detector
CLAHE	– Contrast Limited Adaptive Histogram Equalization
CNN	– Convolutional Neural Network
EER	– Equal Error Rate
FAR	– False Acceptance Rate
FFT	– Fast Fourier Transform
FRR	– False Rejection Rate
GDPR	– General Data Protection Regulation
HIPAA	– Health Insurance Portability and Accountability Act
HQ	– High Quality
IoT	– Internet of Things
IR	– Infrared
MLP	– Multilayer Perceptron
NIR	– Near-Infrared
OTP	– One-Time Password
PIN	– Personal Identification Number
ROI	– Region of Interest
PPG	– Photoplethysmography
PTT	– Pulse Transit Time
RMSE	– Root Mean Square Error
SNN	– Siamese Neural Network
SQL	– Structured Query Language

ВСТУП

Обґрунтування вибору теми дослідження

Розвиток сучасних інформаційних технологій та біометричної ідентифікації є критично важливим фактором у забезпеченні захищеності цифрового простору. Автоматизовані системи аутентифікації на основі унікальних біологічних характеристик дозволяють підвищити рівень захисту від несанкціонованого доступу, мінімізувати вплив людського фактора та забезпечити зручність використання. Особливої актуальності набувають безконтактні методи ідентифікації, які поєднують високу точність з дотриманням сучасних гігієнічних вимог. Існуючі біометричні системи потребують вдосконалення для забезпечення більшої надійності та стійкості до спуфінг-атак.

З точки зору біометрії, живий організм є джерелом унікальних фізіологічних характеристик, що формуються під впливом генетичних та епігенетичних факторів. Капілярна мережа кон'юнктиви ока представляє собою складну динамічну систему, яка поєднує статичні анатомічні ознаки з функціональними характеристиками кровоносного русла. Це означає, що інформація про особу може бути отримана шляхом аналізу унікального рисунку судин, оброблена спеціальними алгоритмами та використана для надійної ідентифікації.

Сучасні біометричні системи характеризуються значним різноманіттям, але мають різну ефективність та рівень захищеності. Традиційні методи, такі як сканування відбитків пальців чи розпізнавання обличчя, демонструють вразливості до сучасних атак з використанням технологій глибоких фейків та 3D-моделювання. У цій роботі досліджуються перспективні методи на основі аналізу судинної мережі ока. При цьому розроблюваний пристрій розглядається як надійний ідентифікаційний модуль, що функціонує на стороні клієнта. Його завдання – отримати унікальний біометричний зразок, перетворити його на цифровий ідентифікатор та передати до комп'ютерної системи. Власне процес авторизації – тобто надання прав доступу відповідно до визначеної ролі – реалізується програмними засобами самої КС на основі отриманого від нашого

модуля достовірного ідентифікатора. Таким чином, запропоновані методи та засоби забезпечують критично важливий перший етап загального процесу авторизації, від надійності якого залежить безпека всієї системи в цілому. Такий підхід дозволяє не лише підтвердити особу, але й диференціювати рівні доступу залежно від контексту використання системи.

Поставлені дослідницькі задачі безпосередньо пов'язані з галуззю комп'ютерного зору та штучного інтелекту (ШІ), які є складовими частинами сучасної інформатики. Для їх вирішення необхідно застосовувати комплексний підхід, що включає:

– застосування методів цифрової обробки зображень та розпізнавання образів (англ. Pattern Recognition);

– використання сучасних інструментів машинного навчання, зокрема згорткових нейронних мереж;

– розробку алгоритмів перевірки, чи використовуються дані живої людини (надалі – живості, англ. Liveness Detection) для запобігання спуфінг-атакам;

– оптимізацію обчислювальних алгоритмів для роботи в режимі реального часу;

– інтеграцію апаратних та програмних рішень у єдину функціональну систему.

Зазначений комплексний підхід вимагає поєднання досліджень з питань кібербезпеки, біометрії, обробки зображень та машинного навчання. Сучасний ринок технологій безпеки демонструє зростаючий попит на надійні біометричні рішення, що підтверджує актуальність та практичну значущість даного дослідження.

Зв’язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана відповідно до напрямку наукових досліджень Чорноморського національного університету імені Петра Могили. Матеріали дисертаційного дослідження увійшли у заключний звіт з науково-дослідної роботи (НДР) «Розробка модулів автоматизації бездротових приладів

відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ ДР 0121U109898, 2021–2022 рр.), в якій здобувач брав участь як виконавець. Також матеріали дисертаційної роботи були введені у навчальний процес за другим (магістерським) рівнем вищої освіти на кафедрі медико-біологічних основ спорту та фізичної реабілітації Чорноморського національного університету імені Петра Могили при проведенні лекційних занять та практичних робіт з дисциплін «Інформаційні технології та системологія в спорті та фізичній реабілітації» українською мовою;

Мета та завдання дослідження

Метою дослідження є підвищення надійності та покращення зручності процесу ідентифікації користувачів в комп'ютерних системах шляхом використання динамічних біометричних параметрів та розробки спеціалізованих методів їх розпізнавання за допомогою розроблених спеціалізованих пристроїв.

Для досягнення поставленої мети визначено наступні **завдання дослідження**:

1) розробити апаратну платформу та спеціалізований пристрій для безконтактного захоплення зображення капілярної сітки кон'юнктиви ока в реальному часі. Пристрій має забезпечувати високу роздільну здатність, ергономічне носіння та енергетичну автономність, а також включати NIR-підсвітку для стабільної роботи в умовах змінного освітлення;

2) розробити та оптимізувати алгоритмічний конвеєр обробки біометричних даних, що включає:

– методи попередньої обробки зображень (виділення ROI, підвищення контрасту, бінаризація);

– алгоритми виділення та векторизації унікального капілярного шаблону;

– сіамську нейронну мережу для високоточного порівняння шаблонів при ідентифікації;

– метод фазової кореляції для субпіксельного відстеження зсуву капілярної текстури з метою реалізації інтерактивного керування курсором

за допомогою погляду;

3) експериментально дослідити ефективність запропонованих методів за допомогою створеної тестової бази даних (БД), оцінивши:

– точність біометричної ідентифікації (FAR, FRR, EER, Accuracy);

– точність, швидкодію та плавність відстеження погляду для задач інтеракції;

– стійкість системи до різних типів спуфінг-атак (фотографія, відео, синтетичні зображення);

– продуктивність та енергоефективність системи на обмеженому апаратному забезпеченні;

4) провести порівняльний аналіз розроблених рішень з існуючими аналогічними методами біометричної ідентифікації (відбиток, райдужка, обличчя) та відстеження погляду, визначивши їх конкурентні переваги, обмеження та практичну значущість для застосування в галузях інформаційних та суміжних технологій.

Об’єкт дослідження

Процес ідентифікації користувача в комп’ютерних системах з використанням динамічних біометричних параметрів.

Предмет дослідження

Засоби ідентифікації користувача в комп’ютерній системі з використанням динамічних біометричних параметрів.

Методи дослідження

У роботі використано комплекс наукових методів, включаючи теоретичний аналіз літературних джерел, метод порівняння та систематизації, методи цифрової обробки зображень (бінарна морфологія, фільтрація, детектування меж), методи машинного навчання (згорткові та сіамські нейронні мережі), а також експериментальні методи тестування апаратно-програмних комплексів.

Наукова новизна отриманих результатів:

– **вперше** запропоновано комплексний підхід, який поєднує ідентифікацію і послідовну авторизацію користувача у комп’ютерній системі

за капілярами кон'юнктиви з одночасним трекінгом погляду в єдиному апаратному виконанні з використанням оптичної схеми з «гарячим дзеркалом», що дозволяє відокремити шлях камери від зорового поля користувача та надає нові можливості для автентифікації та взаємодії з КС особам з обмеженою рухливістю;

– **вперше** запропоновано алгоритмічний конвеєр попередньої обробки зображень на основі бібліотек OpenCV та NumPy, який включає етапи конвертації у відтінки сірого, визначення ROI, підвищення контрасту за допомогою CLAHE, бінаризацію та морфологічну обробку, що забезпечує високу точність виділення капілярної мережі в реальному часі шляхом оптимальної комбінації методів CLAHE, адаптивного порогу і морфологічного замикання та зменшує ймовірність помилкової відмови на 32 % порівняно з системами сканування райдужки;

– **удосконалено** метод фазової кореляції шляхом нормування за амплітудою, що робить метод нечутливим до локальних змін яскравості і дозволяє здійснювати субпіксельне відстеження зсуву капілярної текстури при інтерактивному керуванні курсором за допомогою погляду та забезпечує здатність роботи в умовах змінної освітленості та руху об'єкта при зміні кута зйомки;

– **набув подальшого розвитку** метод контрастної втрати для сіамської мережі шляхом запровадження динамічного порогу, що адаптується до особливостей поточного користувача, таких як перенапруження або повік, що дозволяє ефективно порівнювати біометричні шаблони з урахуванням динамічних змін капілярної мережі та знижує ймовірність помилкового доступу на 47 % порівняно з системами розпізнавання обличчя.

Практичне значення отриманих результатів

Результати роботи реалізовані у вигляді функціонального апаратно-програмного прототипу на базі одноплатного мікрокомп'ютера Raspberry Pi 4 Model B та спеціалізованих компонентів (HQ-камери з макрооб'єктивом 8 мм для детальної фіксації капілярів, NIR-діода для контрастного підсвічування, гіроскопа-акселерометра для корекції положення), що забезпечило оптимальне

співвідношення обчислювальної потужності, енергоефективності та компактності системи. Запропоноване рішення може бути використане:

– як надійна система ідентифікації для фінансового сектору, охорони здоров'я та державних установ;

– як інтерфейс «людина-комп’ютер» для людей з обмеженими фізичними можливостями;

– як система неінвазивного моніторингу здоров'я для виявлення ранніх ознак інсульту, синдрому сухого ока та інших захворювань.

Матеріали дослідження можуть бути використані в навчальному процесі для підготовки фахівців у галузі інформаційних технологій, біоінженерії та медичної інформатики.

Основні результати дисертаційної роботи впроваджено:

– в науково-дослідну роботу (надалі – НДР) ЧНУ ім. Петра Могили «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898, 2021–2022 рр.), в якій здобувач брав участь як виконавець (додаток А.1);

– у навчальний процес за другим (магістерським) рівнем вищої освіти на кафедрі медико-біологічних основ спорту та фізичної реабілітації Чорноморського національного університету імені Петра Могили при проведенні лекційних занять та практичних робіт з дисципліни «Інформаційні технології та системологія в спорті та фізичній реабілітації» українською мовою (додаток А.2).

Особистий внесок здобувача

Основний зміст роботи, всі теоретичні та практичні результати, висновки і дослідження, що представлено до захисту, одержані автором самостійно. Основні результати дослідження опубліковано в роботах [2–11], з яких 4 є одноособовими. Особисто здобувачеві належать наступні наукові результати: [2; 4; 8; 9] – розроблено апаратно-програмний комплекс на базі одноплатного мінікомп'ютера Raspberry Pi зі спеціалізованою оптикою (HQ-камера, макрооб'єктив, NIR-діод) для безконтактного захоплення зображень капілярної сітки кон'юнктиви ока; [7;

11] – розроблено базовий конвеєр алгоритмів обробки зображень в реальному часі (перетворення в відтінки сірого, визначення ROI, підвищення контрасту методом CLAHE, бінаризація, виділення країв за Кенні, морфологічна обробка та фільтрація контурів), що забезпечує підготовку біометричного шаблону.

Апробація результатів дисертації

Матеріали дисертаційної роботи доповідалися, обговорювалися та отримали схвалення на науково-технічних конференціях та семінарах:

– XXI Міжнародна науково-практична конференція «Ольвійський форум» (Миколаїв, 2024);

– Науково-практична конференція з міжнародною участю «Актуальні завдання медичної, біологічної фізики та інформатики» (Вінниця, 2023, 2024);

– XIV Міжнародна науково-практична конференція «Free and Open Source Software» (Харків, 2023);

– Всеукраїнська науково-практична конференція «Могилянські читання» (Миколаїв, 2021, 2022).

Публікації

Відповідно до теми дисертаційного дослідження опубліковано 10 наукових праць, з них 4 праці у наукових фахових виданнях України категорії Б; 6 праць – у збірниках матеріалів міжнародних та всеукраїнських науково-практичних конференцій.

Структура та обсяг дисертації

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та трьох додатків. Основний зміст роботи викладено на 117 сторінках друкованого тексту, містить 32 рисунки та 16 таблиць. Список використаних джерел містить 115 найменувань. Загальний обсяг роботи становить 124 сторінки.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1 Аналіз існуючих методів біометричної ідентифікації

Безпечна та зручна ідентифікація користувача залишається критично важливою проблемою в епоху цифрових технологій [13–15]. Зростання кіберзагроз, включаючи викрадення облікових даних (у т. ч. медичних даних), фішинг та атаки за допомогою deepfake [16; 17], постійно підвищує вимоги до надійності систем ідентифікації (рис. 1.1). Традиційні знання та володіння користувача, такі як паролі та PIN-коди, все частіше виявляються вразливими до злому та соціальної інженерії [18; 19].

Рисунок 1.1 – Еволюція методів ідентифікації

Основні проблеми парольної системи включають (рис. 1.2):

– складність створення та запам'ятовування стійких паролів, що призводить до використання простих і легко вгадуваних комбінацій [42];

– тенденція користувачів до повторного використання паролів на різних ресурсах, що значно підвищує ризик компрометації [43];

– висока вразливість до соціальної інженерії, фішингових атак та методів грубої сили (brute-force).

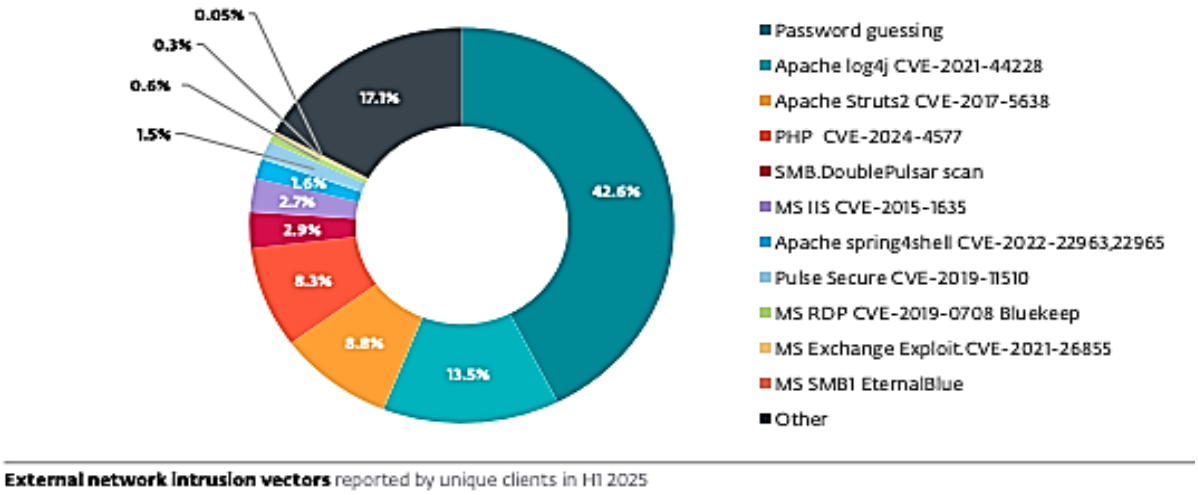


Рисунок 1.2 – Розповсюдження типів атак на парольні системи згідно з ESET Threat Report H1 2025 [114]

Як альтернатива традиційним паролям, з'явилися одноразові паролі (англ. One Time Password, OTP) та апаратні токени. Ці рішення пропонують підвищений рівень безпеки за рахунок:

– динамічної зміни кодів доступу;

– двофакторної автентифікації;

– фізичного носія криптографічних ключів;

– однак ці методи також мають суттєві недоліки;

– підвищені витрати на придбання та обслуговування апаратних засобів;

– складність масштабування для великих організацій;

– необхідність постійного носіння додаткових пристроїв;

– вразливість до втрати або крадіжки токенів.

Еволюція методів ідентифікації демонструє чіткий тренд руху від знань (паролі) до володіння (токени) та, нарешті, до біометричних показників, що ідентифікують особу за унікальними фізіологічними або поведінковими ознаками (рис. 1.3).

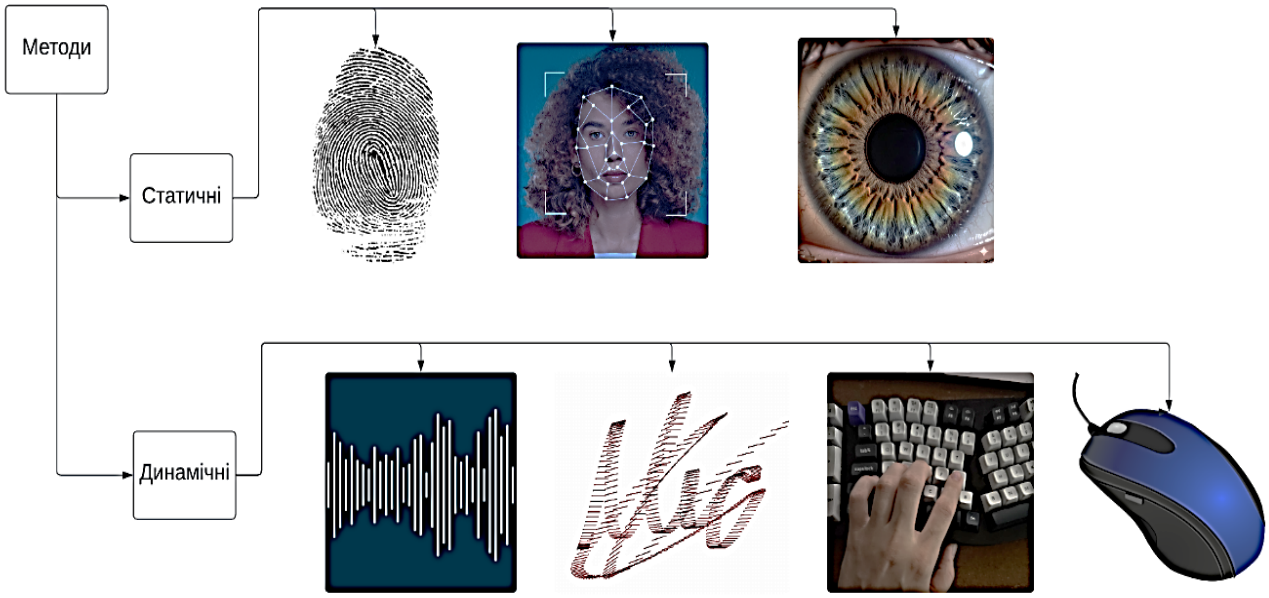


Рисунок 1.3 – Класифікація біометричних методів

Однак, як показують незалежні тести та аналізи, жоден з існуючих біометричних методів не є ідеальним і не забезпечує 100 % захисту від усіх видів атак [20; 21], одночасно будучи зручним, дешевим та універсальним[22].

Статичні фізіологічні методи, такі як розпізнавання відбитків пальців та обличчя, отримали широке поширення завдяки зручності та доступності. Проте вони демонструють фундаментальну вразливість до спуфінг-атак: відбиток можна відтворити за допомогою високоякісних зліпків [23; 24], а система 2D-розпізнавання обличчя може бути обманута фотографією або відео [25]. Вдосконалені 3D-системи та системи з аналізом живості підвищують захист, але значно збільшують вартість та складність рішення. Методи на основі сканування райдужної оболонки або сітківки ока пропонують надзвичайно високу точність і унікальність, проте вимагають дорогого спеціалізованого обладнання, активної участі користувача (необхідно дивитися в чітко визначену точку) та можуть викликати психологічний дискомфорт [26]. Крім того, вони залишаються

вразливими до атак із використанням високоякісних контактних лінз із нанесеним зразком або, в теорії, складних оптичних систем [27; 36].

Поведінкові біометричні методи, такі як аналіз голосу, динаміки набору тексту (англ. Keystroke Dynamics) або ходи людини, додають важливий часовий вимір, що ускладнює підробку. Однак їхня основна слабкість полягає в високій мінливості: показники можуть суттєво змінюватися залежно від стану здоров'я, емоційного фону, втоми або оточення користувача, що призводить до нестабільності та підвищеного рівня помилкових відмов (англ. False Rejection Rate, FRR) [28].

Перспективним напрямком є використання динамічних фізіологічних ознак, зокрема судинних сіток. Методи венозної біометрії (наприклад, сканування вен пальця або долоні) демонструють високу точність і стійкість до спуфінгу, оскільки візерунок розташований під шкірою [29]. Однак вони, як правило, є контактними, що створює гігієнічні ризики та знижує зручність [30; 31; 37], а також вимагають інфрачервоного зондування [32].

У цьому контексті безконтактний аналіз судинного рисунка ока (склери чи кон'юнктиви) виглядає особливо привабливо [33]. Він поєднує унікальність фізіологічної ознаки (щільна мережа капілярів унікальна для кожної людини) з динамічною природою (наявність мікропульсацій кровотоку). Це створює передумови для вбудованої перевірки живості, що є критично важливим для протидії спуфінгу. Проте більшість академічних розробок у цій галузі стикаються з низкою суттєвих проблем, що перешкоджають їх масовому практичному впровадженню[34–36].

По-перше, це проблема апаратної реалізації. Багато дослідницьких систем використовують дороге спеціалізоване обладнання, таке як камери ближнього інфрачервоного діапазону (NIR) з високою роздільною здатністю або навіть спектральні камери, що робить їх недоступними для масового застосування. Інші підходи, що базуються на відображеннях Пуркіньє для трекінгу погляду, можуть вимагати яскравого спрямованого світла, що заважає зору користувача або викликає дискомфорт [37].

По-друге, існують обчислювальні та алгоритмічні складнощі. Виділення чіткого контуру дрібних і низькоконтрастних капілярів на тлі склери в реальному часі є нетривіальною задачею обробки зображень. Традиційні алгоритми часто виявляються чутливими до змін освітлення, рухів голови та індивідуальних особливостей ока (наприклад, наявності крововиливів або пігментації). Це призводить або до високої обчислювальної складності, або до зниження точності та надійності [38; 39].

По-третє, спостерігається відрив досліджень від комплексного практичного застосування. Багато наукових робіт зосереджуються виключно на одній задачі: або на ідентифікації за судинним рисунком, або на відстеженні погляду. Однак для створення справді інноваційного та корисного продукту, особливо в галузі допоміжних технологій, необхідно інтегрувати ці функції. Ідеальна система мала б використовувати один датчик як для надійної ідентифікації з перевіркою живості, так і для подальшого безперервного керування інтерфейсом комп'ютера поглядом, що робить перехід від ідентифікації до взаємодії безшовним [40; 41].

1.2 Аналіз переваг та ключових вразливостей статичних біометричних показників

Поява біометричних методів ідентифікації стала природним кроком у бік зручності та безпеки. До статичних (фізіологічних) біометричних методів відносять ідентифікацію за відбитком пальця, обличчям та райдужною оболонкою ока.

Відбитки пальців залишаються одним з найпоширеніших біометричних методів (рис. 1.4). Їх популярність зумовлена низькою собівартістю сканерів, високою точністю (помилка розпізнавання менше 0,001 %) та простотою використання. Однак, цей метод має суттєві недоліки:

– вразливість до спуфінг-атак**:** сучасні сканери, можуть бути обмануті за допомогою високоякісних зліпків відбитка, виготовлених з желатину, силікону, латексу або навіть за допомогою 3D-друку. Це робить метод небезпечним для застосування у системах з підвищеними вимогами до безпеки;

– чутливість до стану шкіри: Точність різко погіршується при наявності вологи, жирових забруднень, дрібних пошкоджень (подряпин, опіків), а також при природному зношуванні папілярних ліній у людей похилого віку або окремих професій;

– проблеми з розпізнаванням у людей з певними професіями: у представників низки професій (будівельники, музиканти, що грають на струнних інструментах, лікарі-хірурги) через постійний фізичний вплив можуть частково стиратися або деформуватися папілярні візерунки. Також існують медичні стани (дерматити, екземи), що тимчасово або постійно змінюють поверхню пальців;

– гігієнічні та соціальні аспекти: Необхідність фізичного контакту з загальним сенсором викликає обґрунтовані занепокоєння щодо поширення мікробів, що особливо актуально в медичних та громадських установах. Крім того, збір відбитків пальців у деяких культурах асоціюється з кримінальними процедурами, що може викликати психологічний опір.

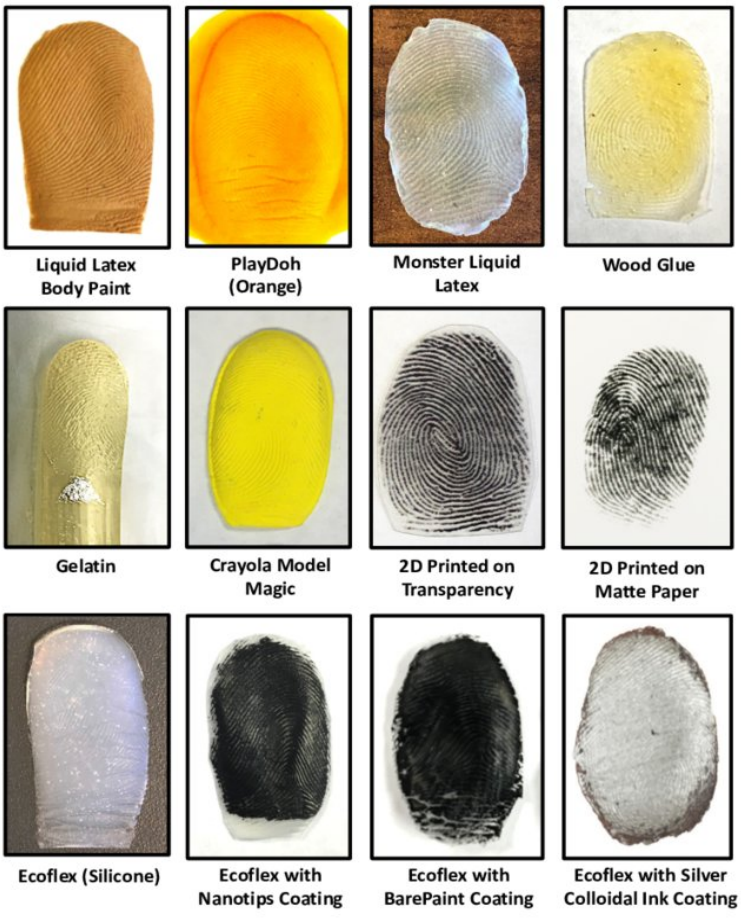


Рисунок 1.4 – Методи спуфінг-атак на сканери відбитків пальців [1]

Метод розпізнавання обличчя набув надзвичайного масового поширення з інтеграцією в смартфони, системи відеоспостереження та прикордонний контроль. Його головні переваги – абсолютна безконтактність, висока швидкість зіставлення та пасивність для користувача (не потрібно виконувати спеціальних дій). Сучасні системи використовують складні алгоритми на основі глибокого навчання, аналізуючи як 2D-текстуру, так і 3D-геометрію обличчя, а інфрачервоні камери дозволяють працювати в повній темряві (рис. 1.5). Проте метод супроводжується серйозними проблемами:

– критична вразливість до підробок: Найпростіші 2D-системи легко обдурити, показавши фотографію або відео на екрані іншого пристрою. Хоча 3D-системи стійкіші, вони можуть бути скомпрометовані за допомогою реалістичних гнучких масок, виготовлених зі шкіри або силікону, а також за допомогою генерованих нейромережами підробок, які стають все доступнішими;

– високий вплив зовнішніх факторів: Точність стрімко падає при зміні ракурсу, нестандартному освітленні (контрсвітло, підсвічування знизу), наявності аксесуарів (великі окуляри, шапки, шарфи), а також при зміні стану обличчя (наявність бороди, макіяжу, набряків, зміна засмаги); Довгострокові зміни внаслідок старіння, набору ваги або пластичних операцій також вимагають періодичного оновлення еталонних зразків;

– етичні та правові проблеми з конфіденційністю: Масовий збір, зберігання та аналіз біометричних даних обличчя без чіткої та інформованої згоди викликає серйозні суперечки щодо приватності, можливості масового стеження та дискримінації. Це призводить до впровадження суворих законодавчих обмежень, таких як GDPR в ЄС;

– проблеми з розпізнаванням у людей з маскою, окулярами або іншими аксесуарами.

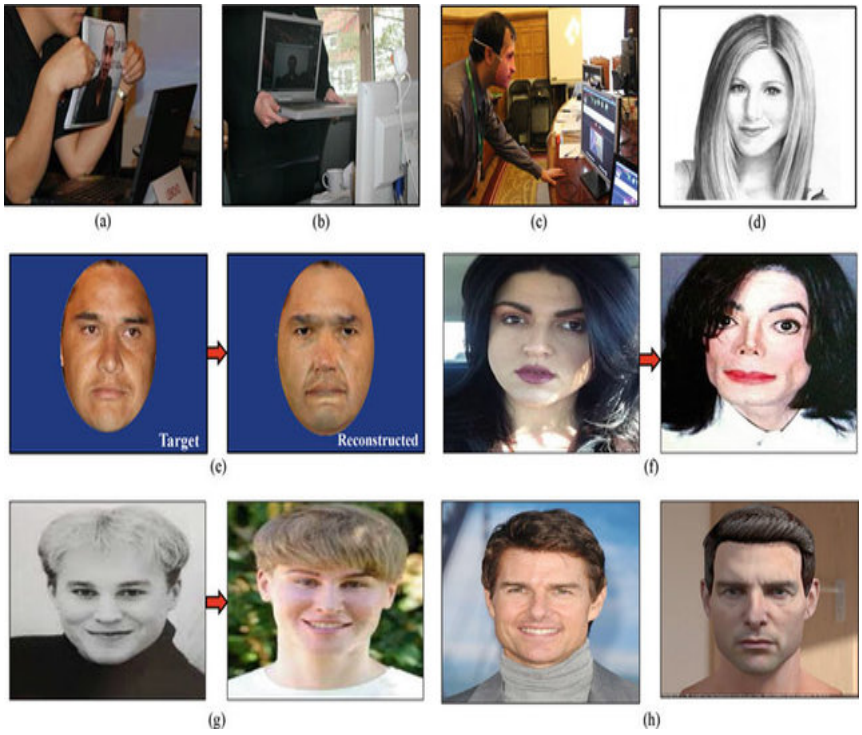


Рисунок 1.5 – Еволюція атак на системі розпізнавання обличчя

Розпізнавання за візерунком райдужної оболонки вважається одним з найнадійніших статичних методів завдяки високій криптографічній ентропії (ступеню унікальності) та структурній стабільності візерунка протягом майже всього життя людини. Його точність є еталонною, тобто рівноправний рівень помилок (англ. Equal Error Rate, EER) становить 0,01–0,1 %. Однак і він супроводжується значними практичними обмеженнями (табл. 1.1):

– високі вимоги до обладнання та процесу: Необхідні спеціалізовані монохромні або близькодіапазонні інфрачервоні камери високої роздільної здатності. Користувач повинен стати на дуже близьку відстань та фіксувати погляд у певній точці, часто при яскравому освітленні, що викликає миготливі відчуття та незручність. Процес займає більше часу, ніж розпізнавання обличчя або відбитка [95];

– чутливість до очних аксесуарів та патологій: Наявність контактних лінз, особливо кольорових або з щільним малюнком, може повністю блокувати сканування. Окуляри з товстими обідками або сильними відблисками також заважають. Очні патології (катаракта, аніридія) можуть зробити ідентифікацію неможливою [91–94];

– психологічний бар'єр: користувачів може бентежити сама процедура сканування ока, яка асоціюється з медичними дослідженнями або повним контролем.

Таблиця 1.1 – Порівняльна таблиця параметрів для актуальних методів розпізнавання

Параметр	Відбитки пальців	Розпізнавання обличчя	Сканування райдужки
Точність, %	98,5	99,1	99,3
Вартість впровадження	Низька	Середня	Висока
Зручність використання	Висока	Дуже висока	Середня
Вразливість до спуфінгу	Висока	Середня	Низька
Стабільність ознак	Висока	Середня	Дуже висока

Загальним критичним недоліком усіх статичних біометричних методів є їхня незмінність. На відміну від паролів, біометричні дані неможливо змінити у разі компрометації, що створює незворотну загрозу конфіденційності користувача. Це обмеження стимулює пошук нових рішень, що поєднують переваги біометрики з можливістю відкликання або оновлення ідентифікаційних даних [44; 45].

1.3 Динамічна та поведінкова біометрика: перспективи та обмеження

Динамічна (поведінкова) біометрія представляє суттєво інший підхід до ідентифікації особистості, базуючись на аналізі унікальних характеристик

поведінки людини, а не її фізіологічних особливостей. Ці методи мають значний потенціал для безперервної аутентифікації та менш схильні до традиційних спуфінг-атак, оскільки зловмиснику потрібно відтворити не лише статичний зразок, але й складний, часто підсвідомий, поведінковий шаблон [53; 54]. Основними перевага та перспективами є:

– безперервність та прозорість: Можливість постійної верифікації користувача протягом усієї сесії без необхідності виконувати додаткові дії [87–90];

– потенційно висока стійкість до спуфінгу: Відтворення поведінкового шаблону є значно складнішим завданням, ніж копіювання фізіологічної ознаки. Атака вимагає глибокого вивчення конкретної поведінки жертви [81; 82];

– низька вартість інтеграції: Часто може бути реалізована з використанням наявних пристроїв введення (клавіатура, миша, мікрофон, сенсорний екран) без дорогого спеціального обладнання (рис. 1.6) [83–86].

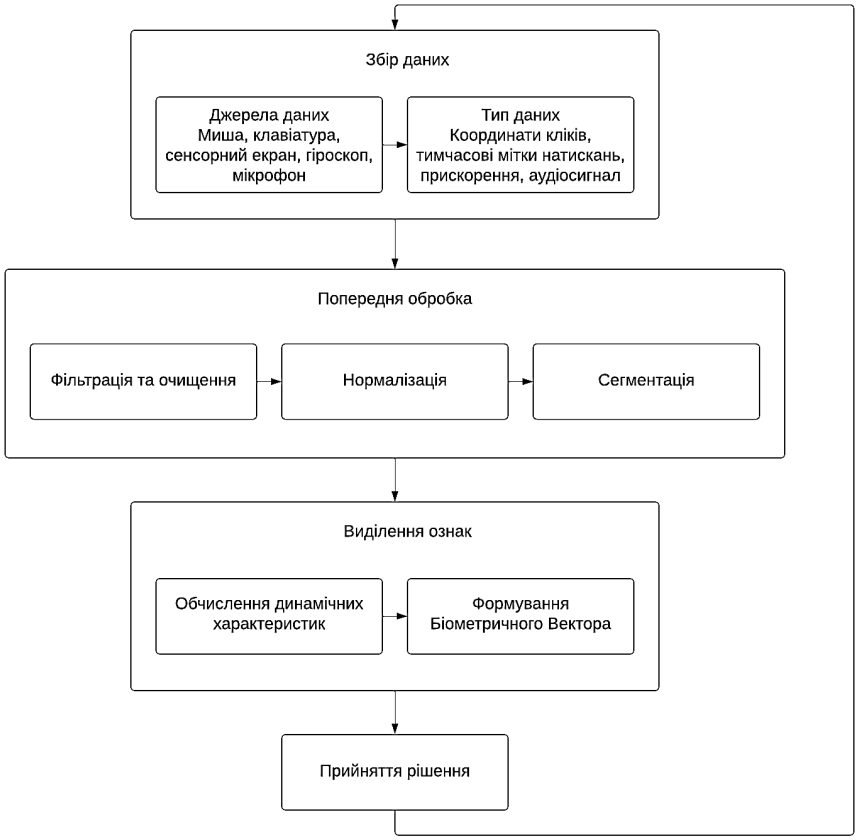


Рисунок 1.6 – Принцип роботи поведінкової біометрики (збір, аналіз та класифікація поведінкових характеристик)

Недоліки та фундаментальні обмеження:

– висока мінливість: Поведінкові шаблони не є стабільними. Вони можуть суттєво змінюватися під впливом стресу, втоми, емоційного стану, травми, віку або навіть вживання ліків. Це призводить до підвищеного рівня помилкових відмов (англ. False Rejection Rate, FRR), що знижує зручність;

– контекстна залежність: Шаблон динаміки миші залежить від того, яку програму використовує користувач (текстовий редактор .vs. гра);

– проблема початкової реєстрації (англ. Enrollment): Для формування надійного шаблону необхідно зібрати великий обсяг поведінкових даних, що може зайняти тривалий час та викликати незручності [80];

– загрози з боку машинного навчання: Парадоксально, але розвиток ШІ створює нові загрози. Зловмисники можуть використовувати генеративні моделі для відтворення поведінкових шаблонів на основі публічно доступних даних або даних, викрадених у попередніх атаках [75–79].

Одним з основних методів поведінкової біометрії є **клавіатурний почерк** (англ. Keystroke Dynamics), що аналізує унікальні особливості манери друку [46–48], включаючи:

– час між відпусканням однієї клавіші та натисканням наступної;

– час утримання конкретної клавіші в натиснутому стані;

– швидкість набору, характерні паузи між словами або фразами, прискорення/уповільнення;

– унікальні закономірності у внесенні та виправленні помилок (наприклад, частота використання Backspace, швидкість виправлення).

Також сучасні технології дозволяють відстежувати додаткові параметри, такі як сила натискання на клавіші, що значно підвищує точність ідентифікації [74].

Для перетворення цих «сирих даних» у біометричний шаблон використовуються методи машинного навчання та статистичного аналізу. Часто створюється профіль на основі набору фіксованої фрази (наприклад, пароля) або

вільно введеного тексту протягом тривалого часу [57].

Сфери практичного застосування:

– безперервна аутентифікація в корпоративних мережах: Система може ненав'язливо моніторити користувача протягом усієї робочої сесії. Різке відхилення клавіатурного профілю може сигналізувати про зміну користувача (наприклад, якщо співробітник залишив робоче місце без блокування ПК) або про несанкціонований доступ [70–72];

– підсилення захисту критичних операцій: У банкінгу або системах управління БД аналіз клавіатурного почерку може бути другим фактором при підтвердженні транзакції або доступу до конфіденційної інформації [73];

– контроль авторства та академічна доброчесність: Може використовуватися для верифікації авторства текстових робіт або виявлення несанкціонованого доступу до облікового запису під час онлайн-іспитів [67–69].

Переваги методу включають непомітність для користувача та низьку вартість впровадження. Однак існують суттєві обмеження, такі як чутливість до емоційного стану, втоми та стресу, залежність від типу клавіатури та її механічних характеристик, необхідність періодичного перенавчання моделей та зниження точності при зміні мови вводу (рис. 1.7).

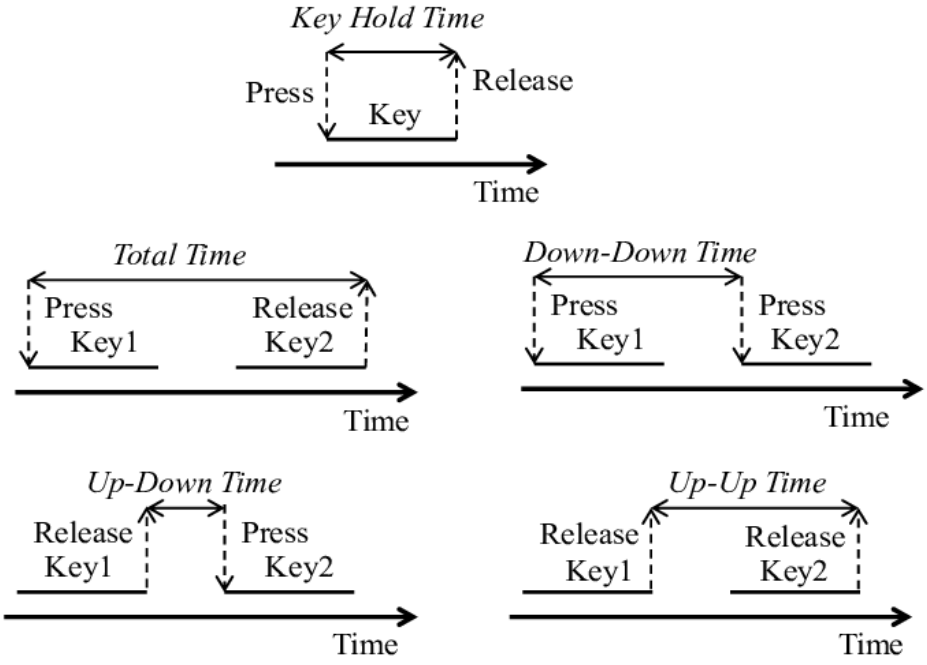


Рисунок 1.7 – Аналіз динаміки клавіатурного вводу [115]

Динаміка руху миші: Аналізує траєкторію, прискорення, кут нахилу та характер рухів курсору. Може використовуватися для безперервної аутентифікації, але також схильна до змін у поведінці [49; 50; 58].

Система фіксує та аналізує низку кінематичних та часових параметрів (рис. 1.8):

– траєкторія руху: Аналіз форм шляхів курсору (прямі лінії, криві, кусково-лінійні рухи) та їх відхилення від ідеальної траєкторії до цілі;

– прискорення та ривки: Характер розгону та уповільнення курсору. Деякі користувачі рухають мишу рівномірно, інші – ривками;

– кути нахилу траєкторії: Переважні напрямки рухів (горизонтальні, вертикальні, діагональні);

– типи та динаміка кліків: Тривалість натискання кнопки миші, час між подвійними кліками, затримка між наведенням на об'єкт та кліком;

– характер прокручування (скролінгу): Швидкість, ритмічність, переважне використання коліщатка прокрутки або смуги прокрутки;

– патерни бездіяльності та мікрорухів: Навіть у стані спокою можливі мікротремтіння руки або певні траєкторії «неспокійного» курсору, що також можуть бути індивідуальними.

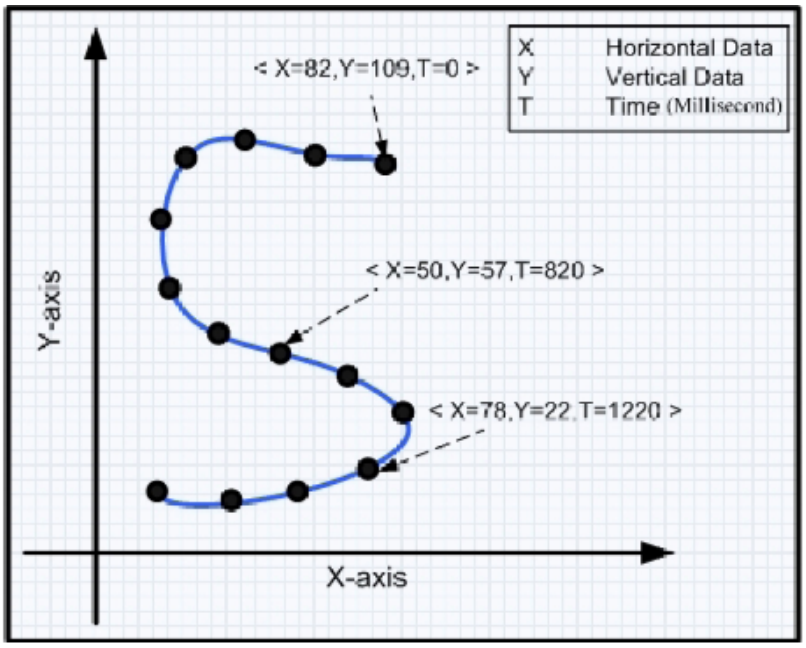


Рисунок 1.8 – Аналіз рухів курсору [55]

Недоліками даного методу є:

– критична залежність від контексту та завдання: Шаблон руху при малюванні в графічному редакторі, роботі з електронними таблицями, веб-серфінгу або грі є кардинально різним. Система повинна мати окремі профілі або бути надзвичайно адаптивною;

– вплив апаратних налаштувань: Чутливість миші (у DPI), швидкість курсору в налаштуваннях ОС, тип миші (механічна, оптична, трекпад) суттєво впливають на всі параметри. Зміна будь-якого з цих факторів вимагає перекалібрування;

– висока мінливість через фізіологічні фактори: Втома руки, зміна положення тіла, дрібні травми (наприклад, розтягнення), холод можуть тимчасово змінити шаблон до невпізнання;

– вразливість до простих атак імітації: На відміну від ритму друку, базові патерни руху миші (наприклад, пряма лінія з точки А в точку Б) можна відтворити за допомогою простих алгоритмічних скриптів. Для ускладнення атаки необхідно аналізувати дуже тонкі кінематичні параметри (ривки, прискорення), що підвищує складність системи [81; 82].

Аналіз голосу: Метод зручний і не вимагає спеціального обладнання. Цей метод належить до змішаних біометричних методів, оскільки поєднує аналіз фізіологічних особливостей (унікальна будова голосового тракту, гортані, носових пазух) із поведінковими патернами (манера мовлення, темп, вимова, інтонація). Порівняння справжнього мовлення з згенерованим наведено на рис. 1.9.

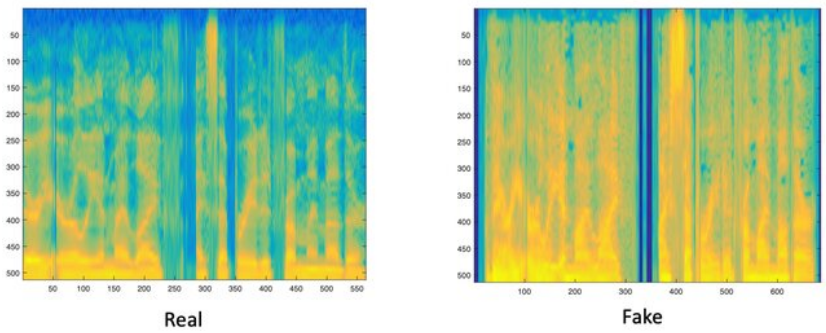


Рисунок 1.9 – Порівняння справжнього мовлення з згенерованим [56]

Цей метод широко впроваджений у системи телефонної ідентифікації, голосових помічників (Siri, Google Assistant) та системи контролю доступу. Перевагами цього методу є:

– природність та звичність взаємодії: Не потрібно запам'ятовувати паролі або торкатися до пристроїв;

– відсутність потреби у спеціалізованому обладнанні: Може працювати з будь-яким стандартним мікрофоном, вбудованим у смартфон, ноутбук або гарнітуру;

– можливість віддаленої ідентифікації: Ідеально підходить для телефонного банкінгу або підтвердження особи через call-центри.

Однак, у цього метода є низка фундаментальних недоліків, таких як:

1) критична чутливість до акустичного середовища: Точність різко погіршується при наявності фонового шуму (вулиця, офіс, транспорт), луни або при розмові через неякісний мікрофон. Це призводить до неприйнятно високого FRR в реальних умовах [64–65].

2) вразливість до спуфінг-атак:

– атаки за допомогою запису: Найпростіший спосіб – використання запису голосу цільової особи, отриманого з соціальних мереж, голосових повідомлень або таємного запису [51];

– синтез голосу: Сучасні технології на основі архітектур Wavenet, Tacotron 2 та GPT можуть генерувати надзвичайно натуральний голос, навчений на кількох хвилинах аудіо цільової особи [66];

– підробки голосу: Просунуті атаки з використанням генеративно-змагальних мереж можуть імітувати не лише тембр, а й емоційне забарвлення та інтонаційні патерни, обходячи прості системи перевірки живості;

3) висока мінливість стану спікера: Голос змінюється при захворюваннях (простуда, ларингіт), емоційних станах (стрес, збудження), вікових змінах, а також під впливом втоми, голоду або медикаментів [61–63];

4) проблеми з універсальністю та упередженістю: Продуктивність систем може суттєво відрізнятися для різних мов, діалектів або акцентів. Деякі алгоритми, натреновані переважно на даних певної демографічної групи, можуть показувати гірші результати для інших груп;

Хоча динамічна біометрика є більш стійкою до спуфінг-атак, оскільки ґрунтується на поведінці, вона страждає від низки недоліків та обмежень:

– мінливість поведінки - характеристики можуть змінюватись під впливом настрою, здоров'я чи зовнішніх умов;

– нижча точність порівняно з фізіологічними методами;

– необхідність великих обсягів даних для навчання моделей;

– складність забезпечення стабільності показників.

При мінімізації або подоланні цих обмежень шляхом використання адаптивних алгоритмів машинного навчання, контекстно-залежних моделей та мультимодальних рішень, динамічна біометрика дійсно пропонує перспективний підхід для безперервної та непомітної аутентифікації. Це відкриває можливість переходу від одноразової перевірки на вході до концепції постійного цифрового профілювання, де рівень довіри до користувача динамічно оцінюється протягом усієї сесії [59; 60].

Однак, як видно з аналізу, поведінкові методи не можуть ефективно функціонувати ізольовано через притаманну їм нестабільність. Найбільш життєздатна архітектура має бути комбінованою, де одночасно буде наявне стабільне фізіологічне ядро та додатковий динамічний шар що забезпечить неперервний моніторинг.

Саме цей гібридний принцип лягає в основу запропонованого в дисертації підходу. Розроблений метод використовує динамічну фізіологічну ознаку, а саме капілярну сітку кон'юнктиви ока, яка за своєю суттю поєднує високу унікальність структури сітки що забезпечує точність порівняну з класичними методами статичної ідентифікації.

Крім того, на цій же апаратній основі реалізується функція відстеження погляду, яка може виконувати роль поведінкового каналу безперервної

аутентифікації. Таким чином, система одночасно вирішує дві поставлені задачі.

1.4 Сучасні методи сканування судин очей: склеральна біометрика

Склеральна біометрика представляє собою перспективний та інноваційний напрямок у галузі біометричної ідентифікації, який базується на аналізі унікальної картини кровоносних судин білої оболонки ока (склери), видимої через прозору кон'юнктиву (рис. 1.10). Цей метод, що активно розвивається останнім десятиліттям, поєднує переваги фізіологічної унікальності та динамічної природи живих тканин.

Перевагами обраного методу є:

– надзвичайно висока унікальність та стабільність: рисунок судинної сітки склери формується на ранніх етапах ембріогенезу і є високоіндивідуальним, навіть для монозиготних близнюків. На відміну від зіниці, його геометрія не змінюється під впливом світла, а на відміну від обличчя – не піддається віковим деформаціям та міміці. Довгострокові дослідження підтверджують його стабільність протягом життя за відсутності серйозних офтальмологічних травм або захворювань [96; 97];

– висока стійкість до спуфінг-атак: Судинна мережа є прихованою внутрішньою структурою, захищеною тонким шаром кон'юнктиви. Це робить її практично неможливою для прямого відтворення у вигляді контактної лінзи, макета або маски. Будь-яка спроба накласти штучний візерунок на поверхню ока буде легко виявлена через порушення оптичних властивостей та відсутність характерної мікропульсації [109–110];

– безконтактність та гігієнічність: Метод не потребує фізичного контакту пристрою з користувачем, що відповідає сучасним санітарно-гігієнічним вимогам (особливо актуально в постпандемічний період і в медичних закладах) та підвищує психологічний комфорт;

– можливість використання доступного обладнання: На відміну від сканування сітківки, яке вимагає когерентного випромінювання та точної фокусування, зображення склеральних судин може бути отримане за допомогою

стандартних RGB-камер високої роздільної здатності з макрооб'єктивом та додатковим NIR-підсвічуванням для підвищення контрасту судин на тлі склери [111–114].

Недоліки та виклики:

– вимоги до якості зображення: для ефективного виділення дрібних капілярів необхідні камери з високою роздільною здатністю та спеціальні алгоритми підвищення контрасту (наприклад, CLAHE) [98–100];

– чутливість до умов зйомки: рух ока, неправильне освітлення, відблиски та наявність повік можуть значно погіршити якість знімка [105–108];

– вплив стану здоров’я: червоність ока, крововиливи або інші захворювання можуть тимчасово змінити видимий рисунок судин [101–104].

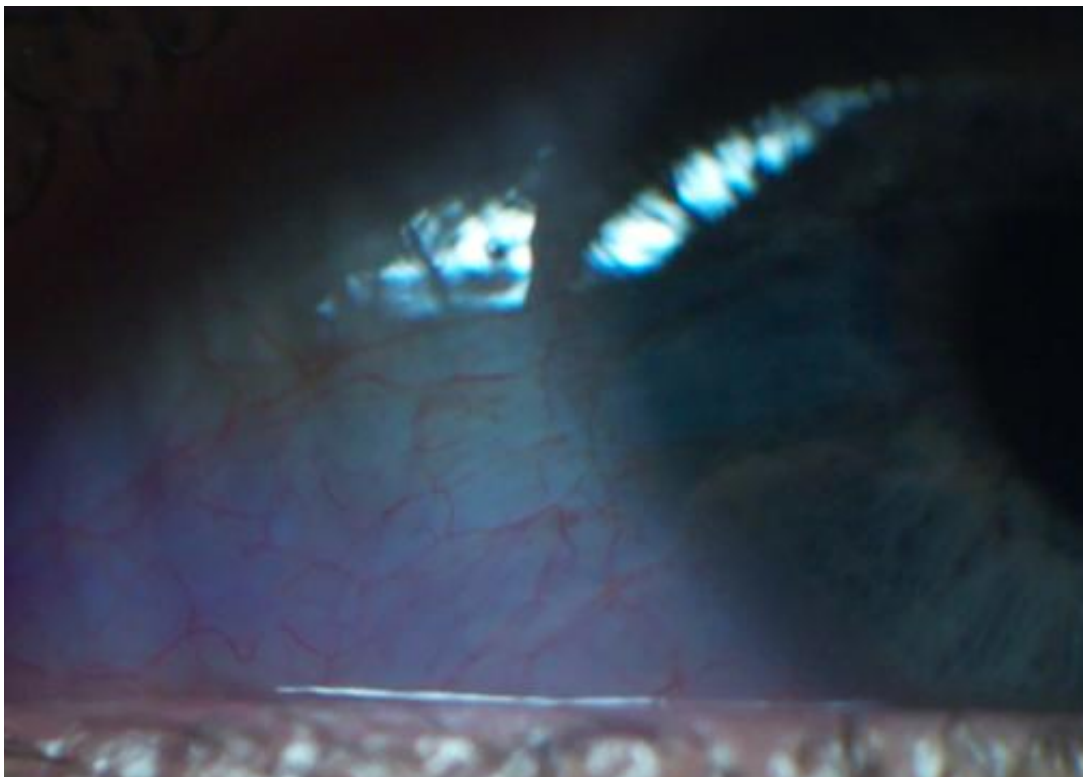


Рисунок 1.10 – Фрагмент судинної оболонки ока

Цей метод поєднує переваги як фізіологічних, так і поведінкових характеристик, що робить його особливо привабливим для застосування у захищених системах.

Висновки до розділу 1

Аналіз сучасних методів ідентифікації демонструє, що жоден з них не є ідеальним. Статична біометрика вразлива до спуфінгу, а динамічна – не завжди достатньо точна і стабільна. Склеральна біометрика є перспективною, але вимагає подолання проблем, пов'язаних із якістю зображення та умовами зйомки.

Це обґрунтовує необхідність розробки нових або вдосконалених гібридних (мультимодальних) підходів. Комбінування кількох методів, наприклад, сканування судинного рисунка кон'юнктиви (як статичної, але важкопідроблюваної ознаки) з одночасним трекінгом погляду (як динамічної поведінкової ознаки), дозволяє створити систему, що володіє синергетичним ефектом: підвищує надійність за рахунок перевірки двох незалежних факторів, забезпечує безперервну аутентифікацію та значно ускладнює для зловмисника проведення успішної атаки. Саме цей напрямок є основою даного дослідження.

РОЗДІЛ 2
РОЗРОБКА АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ СКАНУВАННЯ КАПІЛЯРІВ КОН'ЮНКТИВИ

2.1 Апаратна реалізація системи

Апаратна платформа системи базується на одноплатному мікрокомп'ютері Raspberry Pi 4 Model B, який виконує функцію центрального обчислювального модуля (рис. 2.1). Вибір даної платформи обумовлений її достатньою обчислювальною потужністю для роботи з алгоритмами комп'ютерного зору, наявністю інтегрованих інтерфейсів зв'язку та мініатюрними габаритами [52].

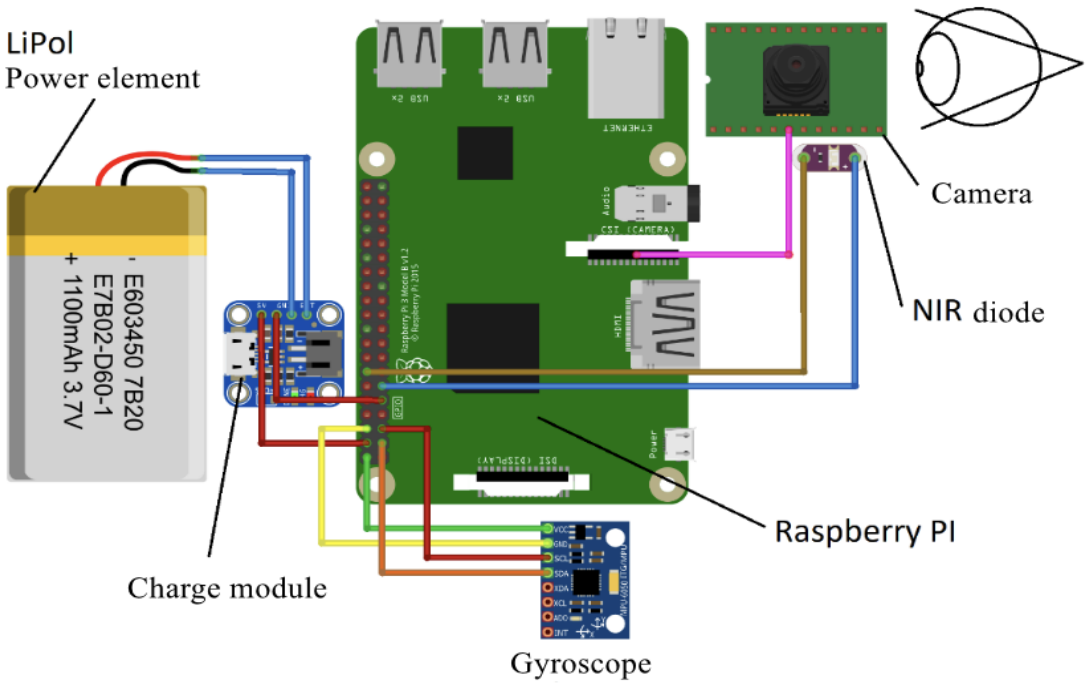


Рисунок 2.1 – Структурна схема апаратної платформи

Основні компоненти та їх характеристики:

– обчислювальний модуль: Raspberry Pi 4 Model B;
– процесор: Broadcom BCM2711 (4 × Cortex-A72, 1.5 GHz);
– оперативна пам'ять: 4 GB LPDDR4;
– інтерфейси зв'язку: WiFi 802.11ac, Bluetooth 5.0, Gigabit Ethernet;
– порти: 2 × USB 3.0, 2 × USB 2.0, 2 × Micro-HDMI.

Особливості: Підтримка CSI для підключення камер. У табл. 2.1 наведені характеристики використаної камери.

Система візуалізації:

- камера: Raspberry Pi High Quality Camera (12.3 Mpx);
- сенсор: Sony IMX477 (1/2.3");
- роздільна здатність: 4056 × 3040 пікселів;
- розмір пікселя: 1.55 µm × 1.55 µm;
- об'єктив: Maacro lens 8mm f/8.0;
- кут огляду: 46.8° (по діагоналі).

Таблиця 2.1 – Характеристики використаної камери

Параметр	Значення	Примітки
Роздільна здатність	12.3 Mpx	Достатньо для розрізнення капілярів
Розмір сенсора	1/2.3"	Оптимальний баланс якості та розміру
Фокусна відстань	8 mm	Забезпечує необхідне збільшення
Діафрагма	f / 8.0	Глибина різкості для роботи з мікросудинами
Мінімальна дистанція	0.1 m	Можливість зйомки з близької відстані

Система стабілізації та позиціонування:

- гіроскоп-акселерометр: MPU-6050;
- діапазон вимірювання: ± 2g, ± 4g, ± 8g, ± 16g;
- точність: 16-бітний АЦП;
- інтерфейс: I2C;
- частота оновлення: до 1 kHz.

Система живлення:

– акумулятор: Li-Po 3.7V 2000 mAh;

– контролер заряду: TP4056;

– струм заряду: 1000 mA;

– захист: Overcharge / Over-discharge protection;

– автономність: до 4 годин безперервної роботи.

Фотографію зібраного модуля під час тестування можна побачити на рис. 2.2.

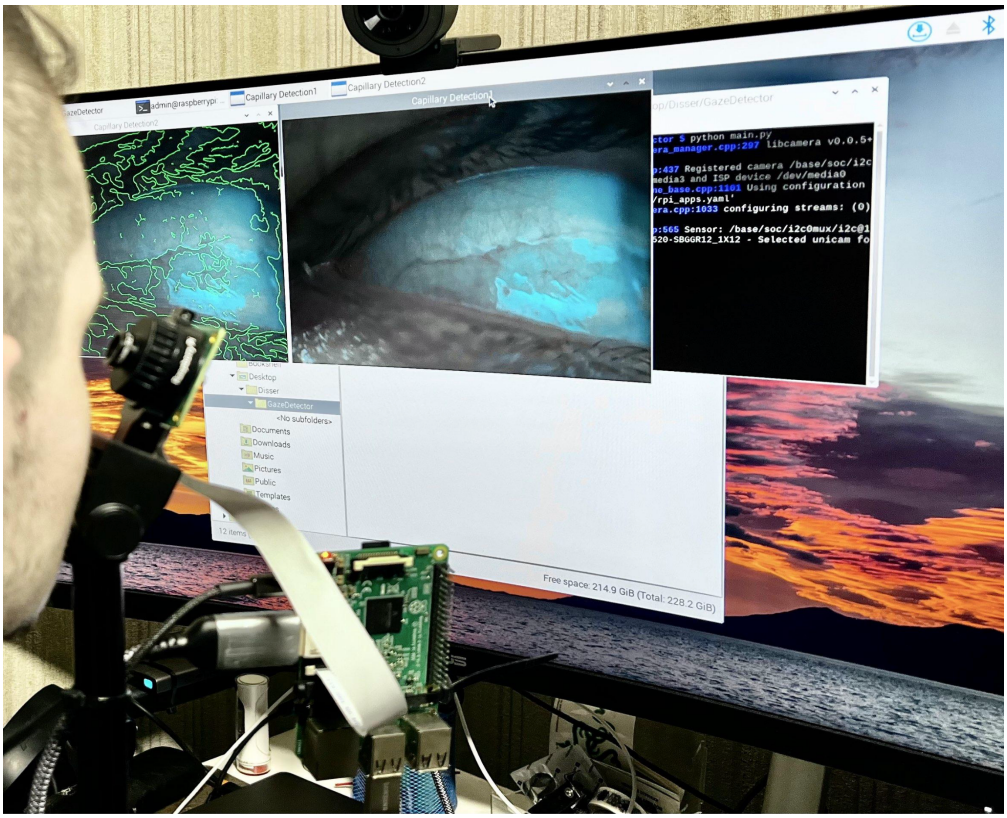


Рисунок 2.2 – Фото модуля, зібраного на стенді, під час використання

Переваги обраної конфігурації:

– висока обчислювальна потужність для обробки зображень в реальному часі;

– компактність та мобільність системи;

– енергоефективність та автономність роботи;

– масштабованість та можливість модернізації;

– вартісна ефективність у порівнянні з промисловими рішеннями.

Обрана апаратна конфігурація забезпечує оптимальний баланс між продуктивністю, енергоефективністю та вартістю, що робить її ідеальним рішенням для дослідницьких цілей та потенційного промислового застосування.

Для підвищення ефективності роботи алгоритмів машинного навчання та забезпечення обробки зображень в реальному часі в апаратну платформу системи інтегровано Google Coral USB Accelerator. Цей пристрій є спеціалізованим процесором для ШІ (Edge TPU), розробленим Google для прискорення інференсу нейронних мереж на периферійних пристроях. Це рішення особливо ефективне для завдань семантичної сегментації та класифікації зображень, що є критично важливим для біометричної ідентифікації на основі аналізу капілярної мережі кон'юнктиви

2.2 Програмне забезпечення та алгоритми обробки

Програмна складова системи реалізована на мові Python 3.9 з використанням спеціалізованих бібліотек для обробки зображень та машинного навчання. Архітектура програмного забезпечення побудована на модульному принципі, що забезпечує гнучкість та легкість модернізації (рис. 2.3).

Основним інструментом для роботи з зображеннями виступає бібліотека OpenCV, яка надає широкий спектр алгоритмів комп'ютерного зору. Для наукових обчислень та роботи з многовимірними масивами використовується бібліотека NumPy. Важливим компонентом є інтеграція з Google Coral через PyCoral API, що дозволяє використовувати апаратне прискорення для виконання операцій машинного навчання.

Алгоритмічний конвеєр обробки зображень починається з етапу захоплення вихідного кадру. Вихідне зображення отримується у форматі RAW з подальшим перетворенням у колірний простір RGB. Для зменшення обсягу даних, що підлягають обробці, відбувається конвертація у відтінки сірого з використанням зважених коефіцієнтів для різних кольорових каналів. Це дозволяє зменшити обсяг даних у три рази при збереженні необхідної інформативності для подальшого аналізу.

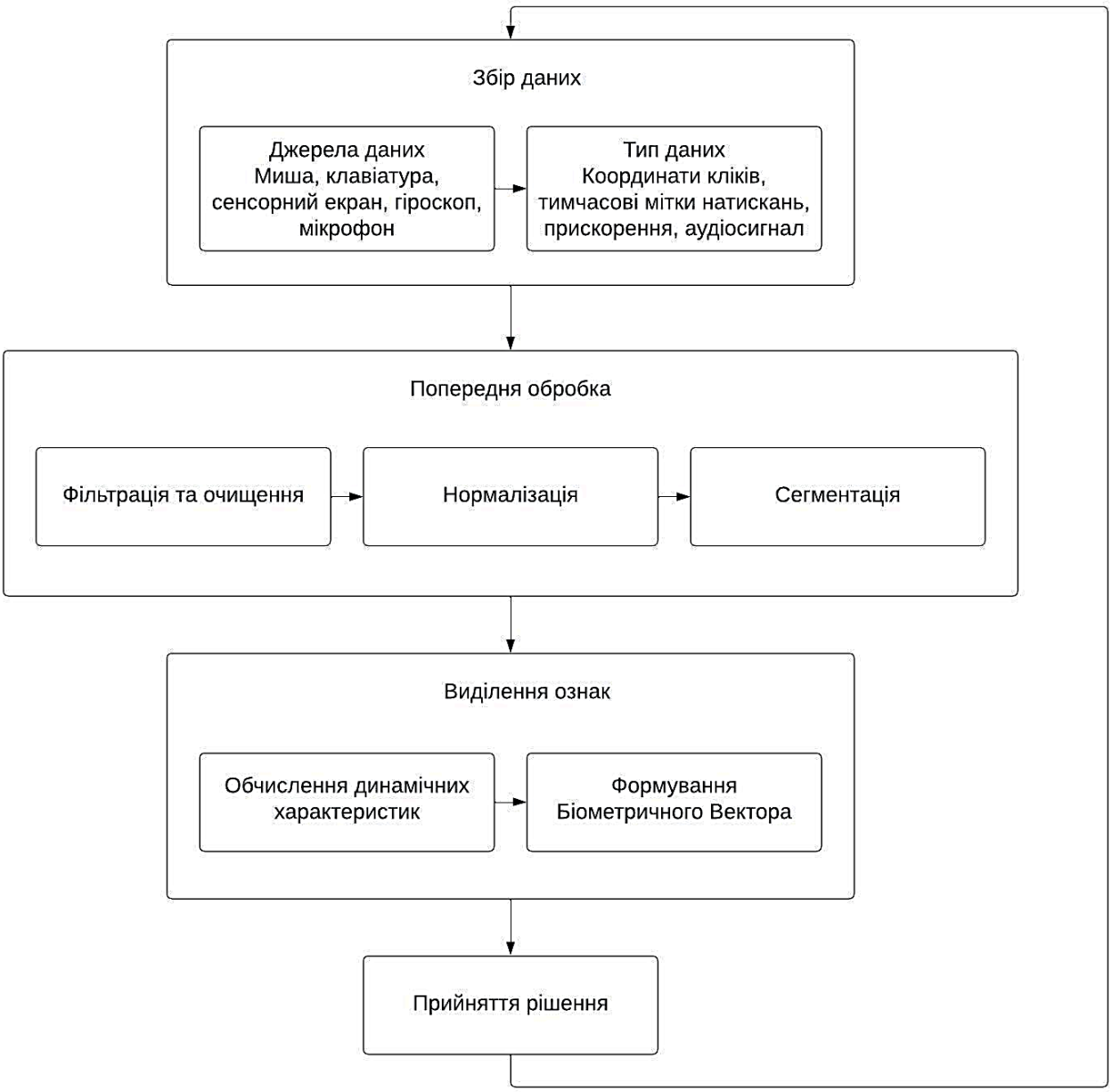
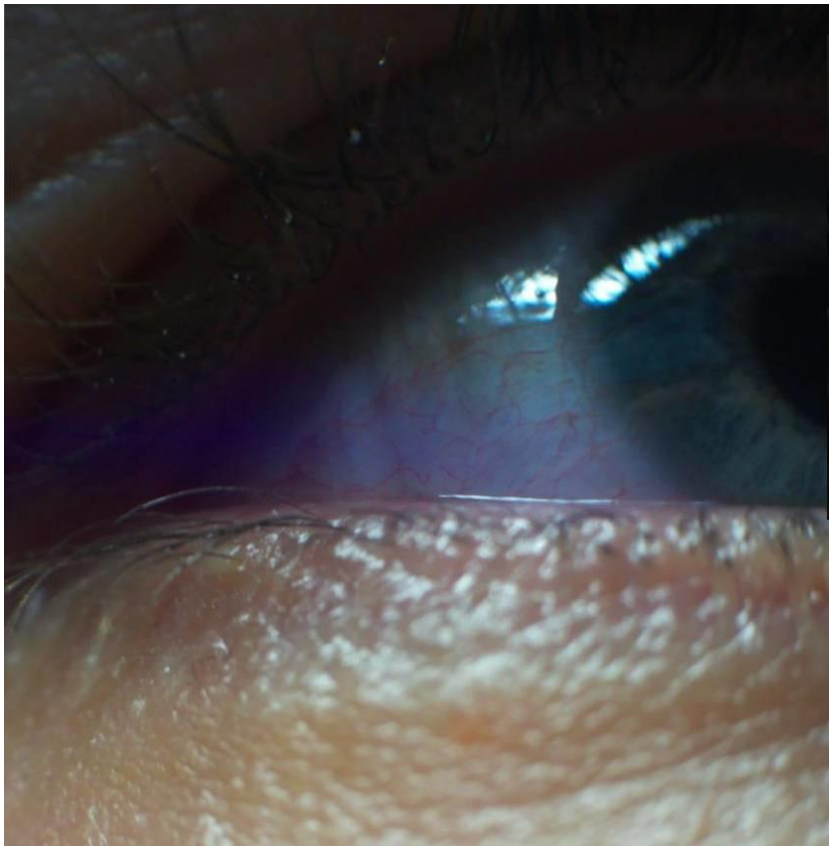
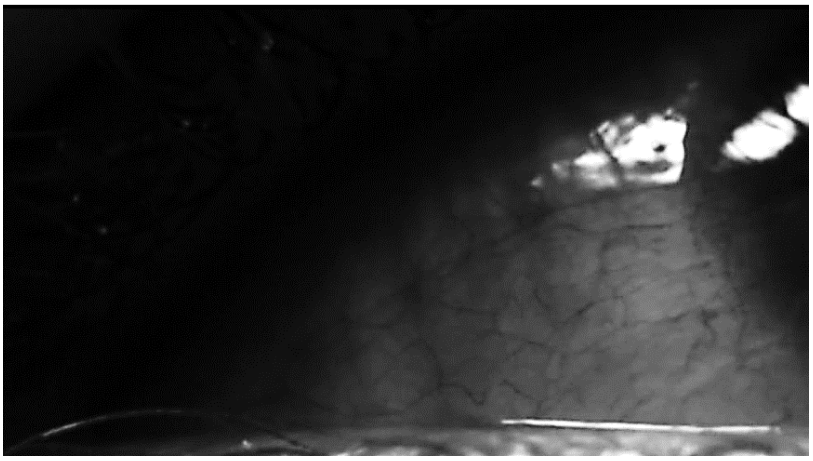


Рисунок 2.3 – Архітектура програмного забезпечення

Наступним кроком є визначення області інтересу (англ. Region of Interest, ROI) у медіальному куті ока (англ. Canthus), де капілярна мережа є найбільш щільною та виразною. Це дозволяє значно скоротити обчислювальне навантаження шляхом фокусування на найінформативніший ділянці (рис. 2.4).



а)



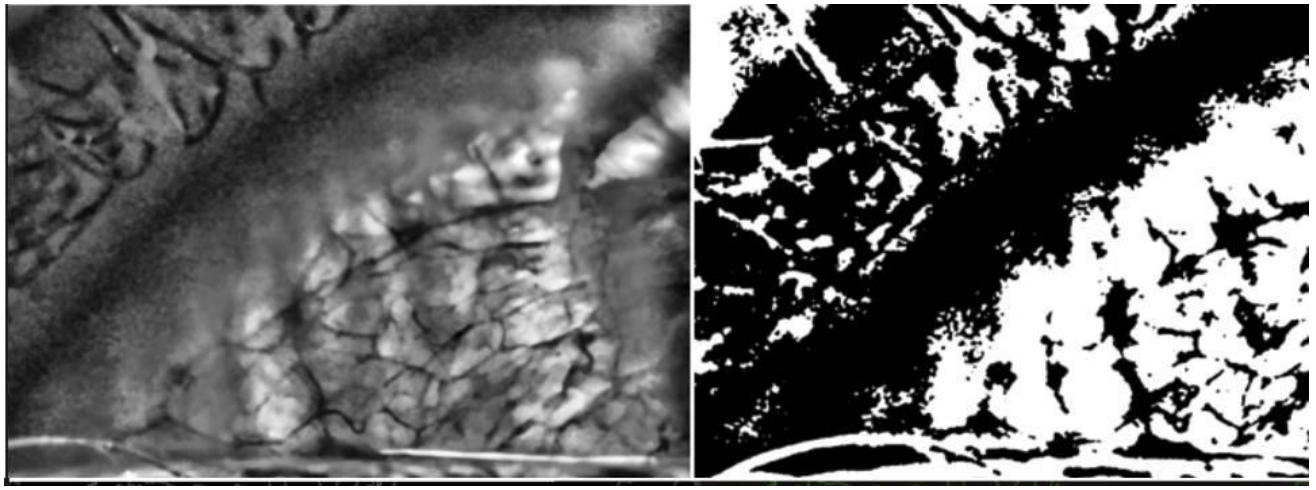
б)

Рисунок 2.4 – Оригінальне зображення (а) та його спрощена для обробки (б) версія (Grayscale + ROI)

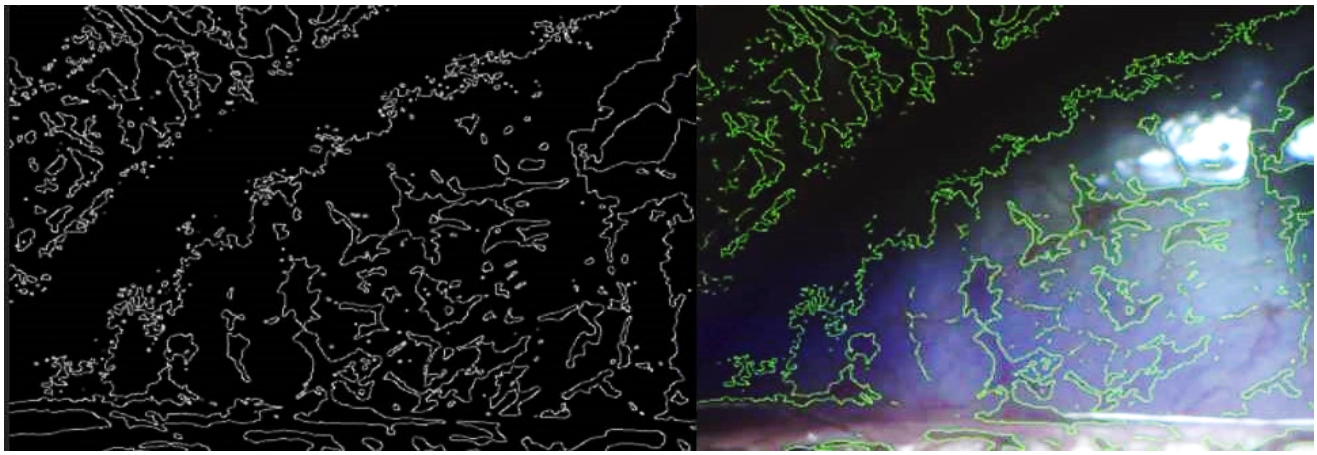
Для підсилення видимості капілярів застосовується метод адаптивного обмеженого підвищення контрасту (CLAHE). Цей алгоритм працює шляхом розподілу зображення на невеликі блоки та застосування до кожного блоку локального вирівнювання гістограм з обмеженням коефіцієнта контрасту. Такий

підхід дозволяє ефективно виділяти судини на тлі склери, уникаючи при цьому перенасичення та підсилення шуму в однорідних ділянках зображення.

Фінальні етапи обробки включають бінаризацію з використанням адаптивного порогу, який враховує локальні особливості освітлення. Для виділення чітких контурів капілярів застосовується детектор країв Кенні, що використовує багатоступінчастий алгоритм для знаходження градієнтів яскравості (рис. 2.5).



а) б)



в)

Рисунок 2.5 – Зображення на різних етапах конвеєру перетворення: а – CLAHE; б – Canny detection; в – бінаризація

Завершальною стадією є морфологічна обробка, спрямована на очищення зображення від шуму та усунення розривів у контурах судин шляхом застосування операцій розширення та звуження.

2.3 Мережева взаємодія та інтеграція

Архітектура мережевої взаємодії системи реалізована з використанням двох основних каналів зв'язку, кожен з яких виконує спеціалізовані функції для забезпечення ефективної роботи всієї системи (рис. 2.6).

Для взаємодії з комп'ютерами та іншими пристроями реалізовано емуляцію HID-пристрою миші через Bluetooth Low Energy. Система використовує BLE стек версії 5.2 з підтримкою профілю HID Over GATT (HOGP). Це дозволяє пристрою автоматично визначатися операційними системами як стандартний маніпулятор без необхідності встановлення додаткових драйверів.

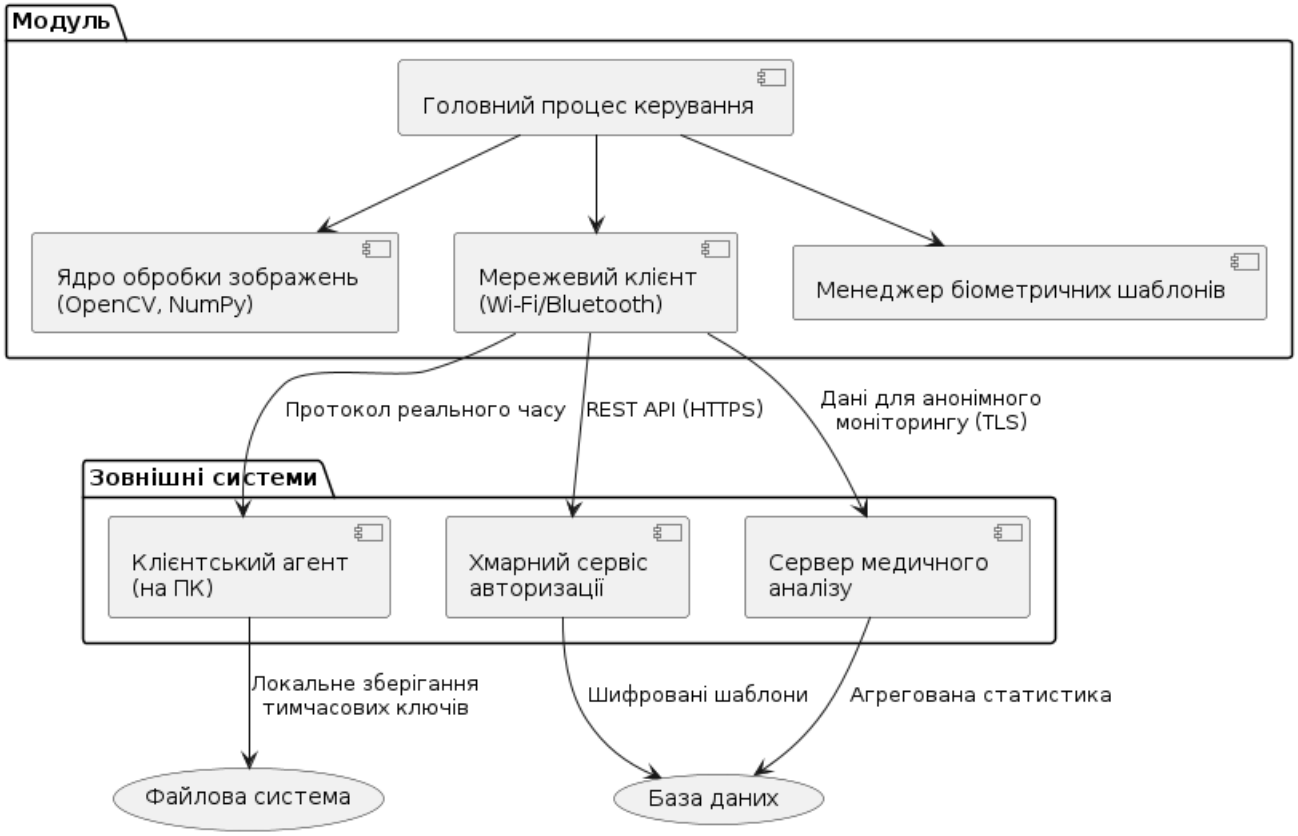


Рисунок 2.6 – Мережева структура взаємодії модулю з іншими пристроями

Для забезпечення стабільної роботи реалізовано механізм адаптивного полінгу з частотою 125 Гц, що забезпечує плавне переміщення курсору без помітних затримок.

Для передачі біометричних даних та отримання підтвердження автентифікації використовується Wi-Fi з'єднання 802.11ac dual-band. Реалізовано

спеціалізований протокол обміну даними, який включає:

– передачу біометричних шаблонів на сервер аутентифікації;

– отримання результатів верифікації з підтвердженням відповідності;

– синхронізацію політик безпеки та оновлення програмного забезпечення;

– End-to-end шифрування біометричних даних з використанням AES-256-GCM;

– двостороння аутентифікація за допомогою TLS 1.3 з клієнтськими сертифікатами;

– механізм одноразових токенів для кожного запиту аутентифікації.

Система автоматично керує пріоритетами каналів зв'язку, віддаючи перевагу BLE для взаємодії в реальному часі та використовуючи Wi-Fi лише для критично важливих операцій аутентифікації. Реалізовано механізм буферизації та черги повідомлень для гарантованої доставки даних навіть в умовах нестабільного зв'язку.

Для зменшення енергоспоживання Wi-Fi модуль активується лише на час виконання запитів аутентифікації, після чого автоматично переходить у режим зниженого енергоспоживання. BLE канал працює постійно, забезпечуючи безперервну взаємодію з пристроями.

Важливо підкреслити, що функція розробленого модуля обмежується ідентифікацією – встановленням та передачею достовірного ідентифікатора користувача. Подальша логіка авторизації (визначення прав доступу на основі цього ідентифікатора, ведення сесій, контроль доступу до ресурсів) реалізується виключно на стороні приймаючої комп'ютерної системи (сервера або операційної системи). Такий розподіл функцій відповідає сучасним вимогам модульності та безпеки.

2.4 Використання крос-кореляції як інструмента взаємодії з КС

2.4.1 Місце та роль крос-кореляції в конвеєрі обробки сигналів ока

Як було показано в попередніх підрозділах, динамічні біометричні

показники на основі капілярної сітки кон'юнктиви мають подвійне застосування: для статичної ідентифікації (порівняння зразків) та для динамічної інтеракції (відстеження погляду). Якщо для першого завдання оптимальним є використання сіамських нейронних мереж (див. підрозділ 2.3), то для реалізації безперервного, низьколатентного контролю курсору чи іншого маніпулятора необхідний інший математичний апарат. Таким апаратом є метод крос-кореляції, зокрема, його вдосконалений різновид – фазова кореляція (англ. Phase Correlation).

Крос-кореляція є фундаментальним методом обробки сигналів і зображень, який дозволяє кількісно оцінити схожість двох сигналів і знайти зсув одного відносно іншого (рис. 2.7).

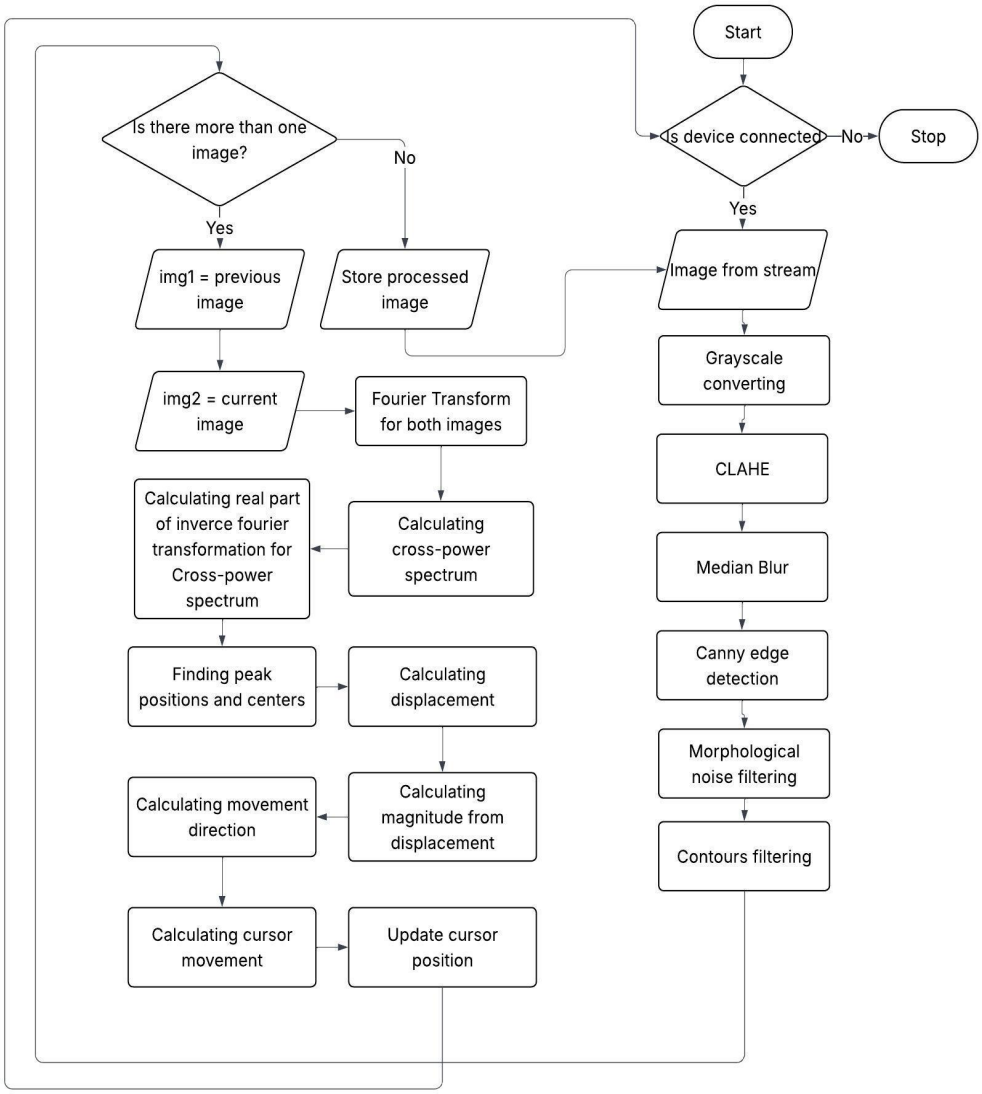


Рисунок 2.7 – Блок-схема, що демонструє місце модуля крос-кореляції в загальному конвеєрі обробки даних

У контексті HCI для користувачів з обмеженими можливостями, цей метод вирішує ключову проблему надійного виділення навмисного сигналу користувача (мікроруху ока) на тлі шуму, викликаного фізіологічним тремтінням, зміною освітлення та артефактами зображення.

2.4.2 Математичні основи методу фазової кореляції для субпіксельного відстеження

Для відстеження мінімальних зсувів капілярної сітки між послідовними кадрами відеопотоку використовується метод фазової кореляції (рис. 2.8). На відміну від стандартної крос-кореляції в просторовій області, цей метод працює в частотній області, що забезпечує вищу обчислювальну ефективність та стійкість до низки видів шуму.

Нехай $I_1(x, y)$ та $I_2(x, y)$– два послідовних кадри, що містять зображення ROI з капілярним рисунком, причому I_2 є зсунутою версією I_1: $I_2(x,y) = I_1(x-\Delta x, y-\Delta y)$. Відповідно до властивостей перетворення Фур'є, просторовому зсуву відповідає лінійний фазовий зсув у частотній області.

Алгоритм складається з наступних етапів:

1) обчислення двовимірного дискретного перетворення Фур'є (2D DFT) для обох кадрів:

$$F_1(u, v) = F\{I_1(x, y)\};\ \ F_2(u, v) = F\{I_2(x, y)\};$$

2) обчислення крос-спектра потужності (англ. Cross-Power Spectrum):

$$R(u, v) = \frac{F_1(u,v)\underline{F_2(u,v)}}{|F_1(u,v)\underline{F_2(u,v)}|},$$

де $\underline{F_2}$ – комплексно спряжене F_2. Нормування за амплітудою робить метод нечутливим до локальних змін яскравості;

3) обчислення оберненого перетворення Фур’є (IDFT) від крос-спектра:

$$r(u, v) = F^{-1}\{R(u, v)\};$$

4) знаходження координат піку $(\Delta x, \Delta y)$ функції $r(x, y)$:

$$(\Delta x, \Delta y) = arg\ arg\ max_{(x,y)} r(x, y)\,.$$

Ці координати і є шуканим цілочисельним зсувом між кадрами.

Для досягнення субпіксельної точності, що є критичним для плавного керування курсором, після знаходження цілочисельного піку застосовується його уточнення. Використовується алгоритм згладжування навколо піку та пошук максимуму параболоїда (наприклад, метод найменших квадратів), що дозволяє отримати зсув з точністю до 0,1–0,3 пікселя.

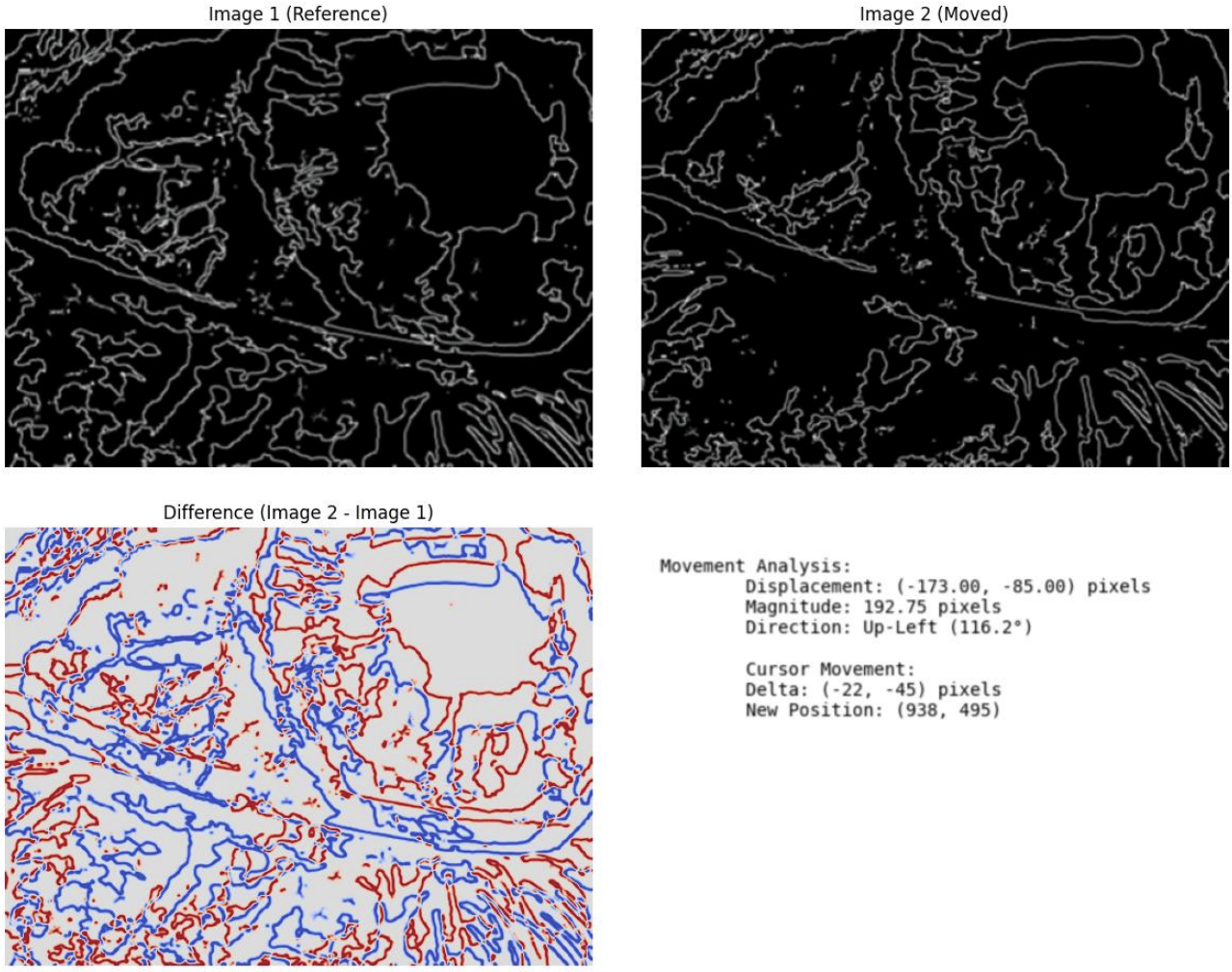


Рисунок 2.8 – Ілюстрація принципу роботи фазової кореляції

Отримані дані та їх перетворення на нові координати для курсору миші, продемонстровано на рис 2.8.

До таких даних входять:

– зміщення між двома зображеннями (Displacement);

– довжина вектора зміщення (Magnitude).

Використовуючи ці дані є можливість вирахувати напрямок зміщення, зміну позиції курсору відносно поточної і нову позицію курсору.

2.4.3 Інтеграція методу в систему відстеження погляду та керування курсором

Метод фазової кореляції є ядром конвеєру керування курсором (табл. 2.2). Його робота забезпечується попередньою та наступною обробкою даних:

1) попередня обробка кадру (англ. Preprocessing): Для підвищення точності кореляції кожен кадр ROI проходить через фільтр Гауса для згладжування високочастотного шуму та процедуру нормалізації яскравості. Це мінімізує вплив миготливого освітлення;

2) обчислення зсуву (англ. Displacement Calculation): До двох послідовних попередньо оброблених кадрів застосовується описаний вище алгоритм фазової кореляції. Результат – вектор зсуву $d = (\Delta x, \Delta y)$;

3) фільтрація та валідація руху (англ. Motion Validation): Щоб відрізнити навмисний рух погляду від тремтіння ока (ністагму) чи артефактів, використовується простий пороговий фільтр за величиною зсуву. Зсуви менші з певний поріг (наприклад, 0,5 пікселя) ігноруються. Також може застосовуватися фільтр низьких частот (на кшталт фільтра Калмана або експоненційного згладжування) для отримання плавної траєкторії курсору;

4) трансформація зсуву в координати екрану (Coordinate Mapping): Отриманий відфільтрований вектор $\boldsymbol{d}$ масштабується за допомогою чутливості (коефіцієнт масштабування) та перетворюється в абсолютні або відносні координати курсору на екрані. Для блокування курсору в межах екрану виконується перевірка границь.

Таблиця 2.2 – Технічні характеристики реалізації алгоритму крос-кореляції

Параметр	Опис
Тип кореляції	Фазова кореляція (в частотній області)
Точність визначення зсуву	До 0,1 пікселя
Розмір ROI для кореляції	128 × 128 пікселів
Попередня обробка	Фільтр Гауса (ядро 3 × 3), нормалізація
Фільтрація руху	Порогова за величиною, експоненційне згладжування
Використані технології	Python, OpenCV, NumPy, SciPy

Використання саме фазової кореляції в даному конвеєрі обумовлене її стійкістю до змін освітлення та здатністю працювати в умовах шумів, що є критичним для систем відстеження напрямку погляду. Це дозволяє уникнути складного калібрування під конкретне освітлення приміщення.

2.4.4 Переваги методу крос-кореляції в порівнянні з альтернативними підходами

Запропонований підхід має ряд ключових переваг (табл. 2.3), що роблять його ефективним саме для завдання відстеження мікроструктур (капілярів):

– незалежність від виділення ознак: На відміну від алгоритмів, що базуються на детектуванні зіниці чи відображенні Пуркіньє (наприклад, ExCuSe, Starburst), фазова кореляція працює з усією областю інтересу. Це робить систему стійкішою до часткових перекриттів (віями) та розмивань;

– висока точність при низькому контрасті: Метод ефективно працює навіть зі слабоконтрастними зображеннями капілярів, оскільки використовує фазову інформацію, а не тільки амплітуду;

– адаптивність: Не вимагає складної персональної калібрування для кожного користувача, оскільки базується на порівнянні сусідніх кадрів, а не на абсолютній моделі ока;

– обчислювальна ефективність: Операції швидкого перетворення Фур'є (FFT) оптимізовані та реалізовані апаратно, що дозволяє досягати високої частоти кадрів обробки (> 30 fps) на доступному обладнанні (Raspberry Pi).

Таблиця 2.3 – Порівняльна таблиця методів відстеження для інтеракції

Метод	Принцип	Переваги	Недоліки
Крос-кореляція	Відстеження зсуву ROI	Субпіксельна точність, стійкість до часткової втрати ознак	Вища обчислювальна складність
ExCuSe	Виявлення границі зіниці по яскравості	Висока швидкість	Чутливість до засвічування, погіршення точності при малому контрасті
Пороговий метод	Визначення руху за зміною середньої яскравості	Простота реалізації	Висока ймовірність помилкових спрацьовувань

Таким чином, метод крос-кореляції, реалізований через алгоритм фазової кореляції, є оптимальним математичним інструментом для реалізації модуля динамічної інтеракції в запропонованій біометричній системі. Він забезпечує необхідну субпіксельну точність та стійкість до шумів для перетворення мікрорухів капілярної сітки ока в плавні та надійні команди керування курсором. Це відкриває можливість створення ефективного інтерфейсу «погляд-миша» для користувачів з обмеженими руховими можливостями, що є ключовим практичним результатом даного дослідження.

Висновки до розділу 2

У другому розділі дисертаційної роботи було розроблено та описано реалізацію апаратно-програмного комплексу для отримання та попередньої обробки зображень капілярної мережі кон'юнктиви ока що становить основу для

подальшого застосування алгоритмів біометричної ідентифікації, які, у свою чергу, є необхідною передумовою для виконання фінального етапу контролю доступу – авторизації користувача в системі.

Основні результати досліджень, наведені у розділу включають:

– апаратну реалізацію на базі одноплатного мікрокомп'ютера Raspberry Pi 4 Model B, що забезпечило оптимальне співвідношення обчислювальної потужності, енергоефективності та компактності системи;

– вибір та інтеграцію спеціалізованих компонентів: високоякісної камери HQ Camera з макрооб'єктивом 8 мм для детальної фіксації капілярів, інфрачервоного діода 880 нм для контрастного підсвічування, а також гіроскопа-акселерометра для корекції положення;

– розробку інноваційної оптичної схеми з використанням «гарячого дзеркала», що дозволило відокремити шлях камери від зорового поля користувача та значно підвищити ергономічність пристрою;

– створення алгоритмічного конвеєру попередньої обробки зображень на основі бібліотек OpenCV та NumPy, який включає етапи конвертації у відтінки сірого, визначення ROI, підвищення контрасту за допомогою CLAHE, бінаризацію та морфологічну обробку;

– забезпечення роботи в реальному часі шляхом оптимізації обчислювальних процесів, зокрема за рахунок обмеження обробки областю інтересу (ROI) та використання ефективних алгоритмів.

Результати розділу демонструють, що розроблений комплекс є функціональним рішенням для якісного отримання та первинної обробки зображень капілярної мережі, що становить основу для подальшого застосування алгоритмів біометричної ідентифікації, які будуть розглянуті в наступних розділах.

РОЗДІЛ 3
АЛГОРИТМИ ОБРОБКИ ЗОБРАЖЕНЬ, ВИДІЛЕННЯ БІОМЕТРИЧНИХ ОЗНАК ТА ЇХ РОЗПІЗНАВАННЯ

3.1 Виділення та фільтрація контурів

Після етапу попередньої обробки, що включає конвертацію у відтінки сірого, виділення області інтересу (англ. Region of Interest, ROI), підсилення контрасту за допомогою CLAHE та адаптивної бінаризації, алгоритм переходить до критично важливої фази – аналізу та фільтрації контурів. Цей етап трансформує бінарне зображення у структуроване представлення, виділяючи саме ті геометричні форми, що відповідають капілярним структурам, та відсіваючи шум і артефакти.

3.1.1 Метод векторного аналізу контурів

Для виявлення контурів застосовано алгоритм, що базується на методі відстеження кордонів (border following). У термінології OpenCV це реалізовано функцією `cv2.findContours()` з параметром `RETR_EXTERNAL`, що забезпечує пошук лише зовнішніх контурів, та `CHAIN_APPROX_SIMPLE`, який апроксимує контури, зберігаючи лише ключові вершини. Даний метод працює з бінарним зображенням, інтерпретуючи пікселі зі значенням 255 (білі) як передній план (об'єкт), а 0 (чорні) – як фон.

Математично, контур C_k представляється як впорядкована послідовність точок $\{p_1, p_2, \dots, p_n\}$, де $p_i = (x_i, y_i)$. Для подальшого аналізу обчислюються числові характеристики кожного знайденого контуру.

3.1.2 Мультикритеріальна фільтрація контурів

Простий поріг за площею є недостатнім для ефективного відокремлення капілярів від шуму, оскільки артефакти можуть мати схожі розміри. Тому впроваджено систему фільтрації за кількома геометричними та топологічними параметрами (рис. 3.1):

1) площа (Area, S): Фундаментальний параметр, що обчислюється за формулою Гріна для контуру:

$$S = \frac{1}{2} \left| \sum_{i=1}^{n} (x_i y_i + 1 - x_i + y_i) \right|.$$

Контури з площею $S < S_{min}$ (наприклад, < 5 пікселів) класифікуються як піксельний шум, а з площею $S > S_{max}$ (наприклад, > 500 пікселів) – як великі артефакти (напр., тіні від вій, відблиски);

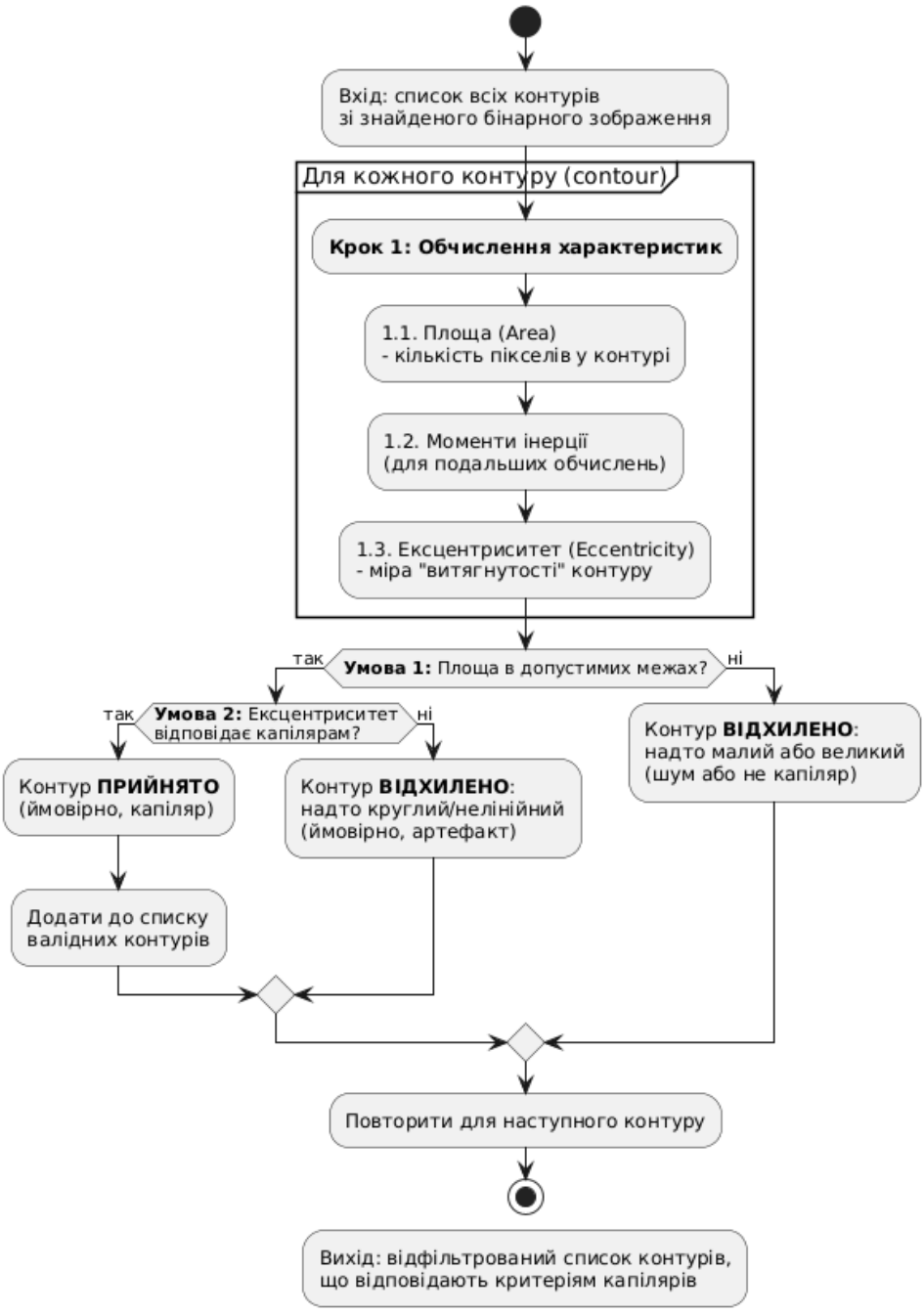


Рисунок 3.1 – Діаграма фільтрації контурів за площею та ексцентриситетом

2) довжина периметра та компактність: Довжина периметра P обчислюється як сума відстаней між сусідніми точками контуру. Відношення $\frac{p^2}{S}$ (коефіцієнт округлості) дозволяє відрізнити компактні, майже ізометричні артефакти від витягнутих, лінійних капілярів. Для капілярів це відношення значно більше, ніж для круглих або овальних шумових плям;

3) ексцентриситет та ізотропність: На основі обчислення коваріаційної матриці точок контуру або його моменту інерції можна отримати власні значення λ_1, λ_2 $(\lambda_1 \geq \lambda_2)$. Ексцентриситет $e = \sqrt{1 - \frac{\lambda_1}{\lambda_2}}$ близький до 1 для витягнутих, лінійних структур (капіляри) та близький до 0 для округлих.

На двовимірній площині (Площа, Ексцентриситет) точками позначені всі виявлені контури. Зона, обмежена лініями порогів S_{min}, S_{max} і e_{min}, візуально виділяє кластер контурів, що відповідають капілярам. Контури поза цією зоною позначені як шум або артефакти (табл. 3.1).

Таблиця 3.1 – Порогові значення для фільтрації контурів

Параметр	Позначення	Типове значення, пікс.	Призначення
Мінімальна площа	S_{min}	5	Відсіювання точкового шуму
Максимальна площа	S_{max}	500	Відсіювання великих артефактів
Мінімальний ексцентриситет	e_{min}	0,85	Відсіювання округлих об’єктів
Максиимальна довжина	L_{max}	150	Відсіювання надмірно витягнутих артефактів

Така багатокритеріальна фільтрація суттєво знижує кількість хибних спрацьовувань на наступних етапах аналізу, дозволяючи зосередитись лише на біологічно релевантних структурах.

3.1.3 Значення для подальшої обробки

Контури, що успішно пройшли мультикритеріальну фільтрацію, вважаються достовірними представленнями капілярних структур. Цей етап є критично важливим з кількох причин:

– підвищення точності порівняння: Наступні етапи (наприклад, скелетонізація, виділення точок розгалуження, побудова графа) працюють з «чистими» даними, що істотно зменшує ймовірність помилкового виділення ознак;

– зменшення обчислювального навантаження: Видалення до 60–80 % шумових контурів значно прискорює роботу всіх наступних алгоритмів;

– підвищення надійності системи: Фільтрація мінімізує вплив тимчасових артефактів (пил на лінзі, дрібні крововиливи), що робить біометричний шаблон більш стабільним у часі.

Результатом цього етапу є набір відфільтрованих векторних контурів $\{C_1, C_2, \dots, C_m\}$, які передаються далі в конвеєр для побудови унікального біометричного шаблону користувача.

3.2 Методи порівняння та класифікації

Для вирішення задачі верифікації «один-до-одного» (one-to-one verification) в системі застосовано архітектуру сіамської нейронної мережі (англ. Siamese Neural Network, SNN). Ця архітектура є ключовою для біометричних систем, де необхідно не класифікувати зображення до певного класу, а визначати ступінь схожості між парою зразків: еталонним, що зберігається в БД, та поточним, отриманим від користувача (рис. 3.2).

3.2.1 Архітектура та принцип роботи

Архітектура сіамської мережі складається з двох або більше ідентичних підмереж (часто називаних «віялами»), які мають абсолютно однакові параметри (ваги, зсуви). Кожна з цих підмереж є глибокою згортковою нейронною мережею,

як правило, на основі спрощених або спеціально модифікованих архітектур (наприклад, VGG, ResNet). Глибина та структура цих мереж підібрані так, щоб ефективно витягувати ієрархічні ознаки з зображень капілярної мережі: від простих крайових детекторів до складних топологічних патернів.

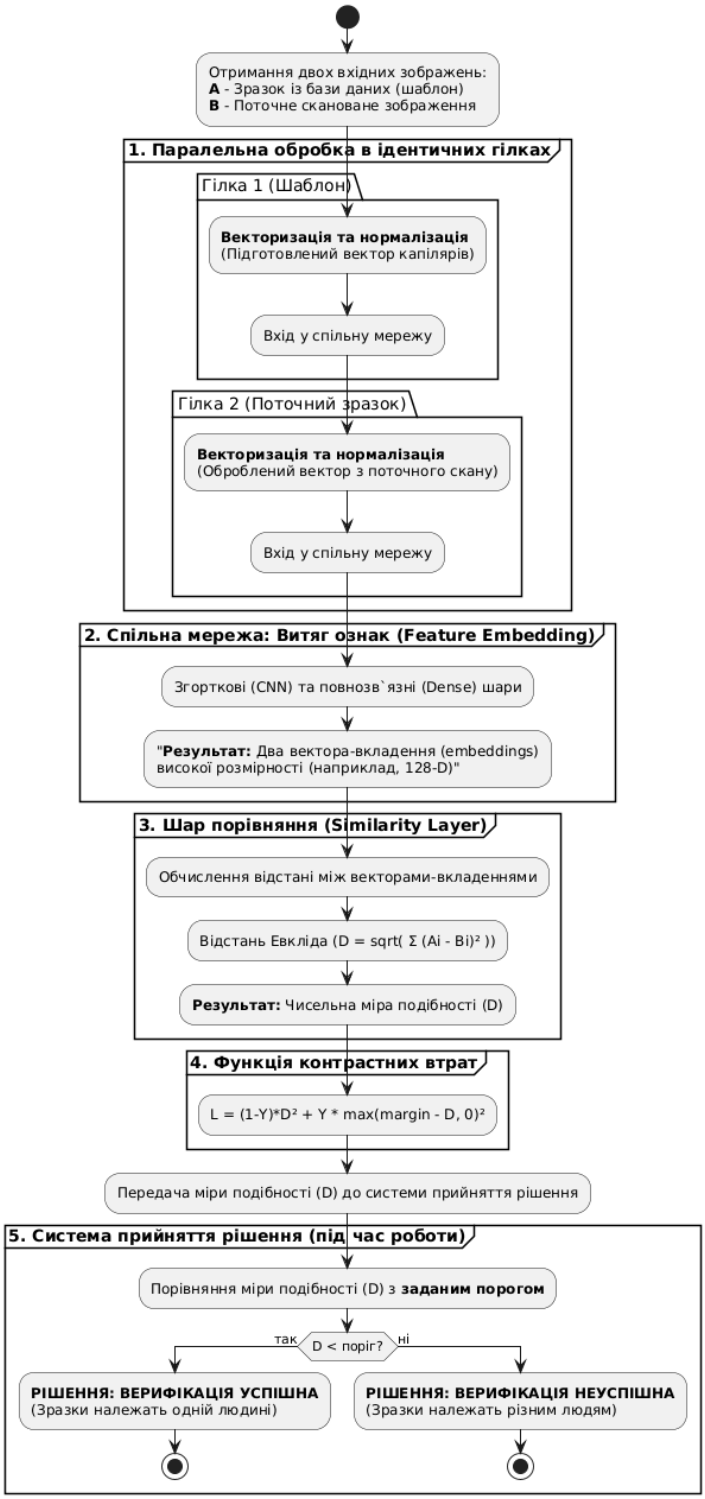


Рисунок 3.2 – Конвеєр біометричної ідентифікації на основі сіамської нейронної мережі

На вхід мережі подається пара зображень: A (якорне, англ. Anchor) – еталонний шаблон, і B (позитивне або негативне) – тестовий зразок. Обидва зображення одночасно проходять через свої ідентичні підмережі. Кінцевим шаром кожної підмережі є повнозв'язний шар, який перетворює оброблене зображення у щільний вектор фіксованої розмірності, зазвичай від 128 елементів до 512 елементів. Цей вектор, який називають дескриптором ознак або нейронним вбудовуванням (англ. Embedding), інкапсулює найсуттєвішу інформацію про структуру капілярної мережі, відфільтровуючи шум та несуттєві варіації (освітлення, дрібні зсуви).

Після отримання векторів-дескрипторів $f(A)$ та $f(B)$ для пари зображень, мережа обчислює міру їх відмінності. Найчастіше для цього використовується евклідова відстань D між векторами:

$$D = \| f(A) - f(B) \|_2 .$$

Мала відстань вказує на високу схожість (пара належить одному користувачу), тоді як велика відстань – на низьку схожість (пара належить різним користувачам). Межею для прийняття рішення (порогом) є гіперпараметр, що налаштовується на валідаційному наборі даних.

Після того як сіамська мережа підтверджує відповідність поточного зображення капілярів збереженому шаблону, базуючись на ідентифікаторі користувача, система передає інформацію про ідентифікованого користувача до БД облікових записів, яка у наслідку керує правами авторизованого користувача.

3.2.2 Навчання з використанням контрастної функції втрат

Ефективність сіамської мережі повністю залежить від того, наскільки добре її підмережі навчені формувати «хороші» векторні представлення. Ідеальний дескриптор повинен зберігати властивість: він повинен бути компактним для зображень одного класу (одного ока) та віддаленим для зображень різних класів (різних очей).

Для досягнення цієї мети використовується спеціально розроблена контрастна функція втрат (англ. Contrastive Loss). На відміну від традиційних функцій втрат для класифікації (наприклад, перехресна ентропія), контрастна функція працює безпосередньо з парами зображень. Її математичний вигляд:

$$L(A, B, Y) = (1 - Y) \cdot \frac{1}{2} D^2 + Y \cdot \frac{1}{2} \{(0, m - D)\}^2,$$

де Y – мітка пари: $Y = 0$, якщо зображення A і B належать одному класу (одній людині) і $Y = 1$, якщо вони належать різним класам;

D – евклідова відстань між дескриаторами $f(A)$ та $f(B)$;

m – гіперпараметр margin, який задає бажану відстань між дескрипторами різних класів.

Логіка функції:

1) для однойменних пар ($Y = 0$): Функція втрат зводиться до $\frac{1}{2} D^2$. Під час навчання, зворотне поширення помилки буде мінімізувати цю складову, зменшуючи відстань D між дескрипторами однієї людини, «притягуючи» їх у просторі ознак;

2) для різнойменних пар ($Y = 1$): Функція втрат зводиться до $\frac{1}{2} \{max(0, m - D)\}^2$. Ця складова активується (стає більшою за нуль), лише коли відстань *D* менша за маржу m. Таким чином, вона «штовхає» дескриптори різних людей один від одного, доки їх відстань не стане хоча б рівною маржі m. Якщо відстань вже перевищує маржу, ця складова дорівнює нулю, що дає мережі можливість зосередитися на інших, складніших парах.

3.2.3 Переваги для біометричної системи

Застосування сіамської архітектури з контрастною функцією втрат надає ключові переваги для ідентифікації за капілярами кон'юнктиви:

1) ефективність при малих наборах даних: Навчання мережі на парах дозволяє ефективно використовувати обмежену кількість зразків від кожного користувача;

2) інваріантність до завад: Мережа природним чином навчається ігнорувати несуттєві варіації (як нерівномірне освітлення, дрібні повороти), оскільки вони присутні в обох зображеннях однойменної пари. Мінімізація відстані для таких пар змушує мережу виділяти саме інваріантні, стабільні ознаки;

3) можливість динамічного розширення бази: Для додавання нового користувача не потрібно перевчати всю модель. Достатньо зберегти його еталонний дескриптор, обчислений навченою мережею;

4) пряма оптимізація метрики подібності: Мережа оптимізує саме ту метрику (відстань у просторі ознак), яка потім використовується для прийняття рішення при експлуатації.

Таким чином, сіамська нейронна мережа формує потужний і адаптивний механізм порівняння, що дозволяє надійно верифікувати особу на основі динамічної та складної структури капілярної мережі кон'юнктиви.

3.3 Методи машинного навчання для класифікації та порівняння ознак

3.3.1 Розвиток архітектури нейронних мереж від перцептрону до глибокого навчання

Фундаментальною моделлю, що лягла в основу сучасних архітектур ШІ, є перцептрон – математична модель сприйняття, що імітує принцип роботи нейрона. Класичний перцептрон складається з входів, вагових коефіцієнтів, суматора та функції активації, формуючи просту, але потужну модель для лінійної класифікації. Однак, обмеженість перцептрону полягає в неспроможності вирішувати нелінійні задачі, що призвело до розвитку багатошарових архітектур (рис. 3.4).

Сучасне глибоке навчання ґрунтується на архітектурі багатошарового перцептрону, де кілька шарів нейронів, розташованих послідовно, здатні виявляти складні нелінійні залежності. Кожен шар перетворює вхідні дані у все більш абстрактні представлення, дозволяючи системі автоматично виділяти ієрархію ознак. Ця властивість особливо цінна для обробки зображень, де низькорівневі

ознаки (краї, текстури) поступово інтегруються у високорівневі концепти (форми, об'єкти).

Рисунок 3.4 – Еволюція архітектур нейронних мереж: від перцептрону до глибоких згорткових мереж

3.3.2 Згорткові нейронні мережі для виділення просторових ознак

Для задач комп'ютерного зору, зокрема аналізу біометричних зображень, найбільш ефективною архітектурою виявилися згорткові нейронні мережі. Відмінність CNN від класичних багатошарових мереж полягає у використанні спеціальних згорткових шарів, які застосовують набір фільтрів (ядер) до вхідного зображення. Кожен фільтр сканує зображення, виявляючи специфічні локальні шаблони – контури, текстури, градієнти яскравості, що критично важливо для виділення структури капілярної мережі.

Архітектура типової CNN включає послідовність блоків, кожен з яких складається з:

– згорткового шару, який застосовує набір навчаємих фільтрів для створення карти ознак;

– шару нелінійної активації (зазвичай ReLU), що вносить нелінійність у модель;

– шару підвибірки (пулінгу), який зменшує просторову розмірність, зберігаючи найважливіші ознаки та підвищуючи інваріантність до невеликих зсувів.

Така ієрархічна структура дозволяє мережі автоматично будувати

оптимальне представлення зображення: від простих крайових детекторів на ранніх шарах до складних комбінаторних патернів, що відповідають унікальній топології капілярного русла, на глибоких шарах.

3.3.3 Сіамська мережа на основі CNN для порівняння біометричних шаблонів

У задачі верифікації та ідентифікації за зображеннями капілярів застосовано сіамську архітектуру нейронної мережі. Її ключова особливість – наявність двох ідентичних підмереж (віял), які мають спільні вагові коефіцієнти.

Принцип роботи полягає в наступному: два зображення – еталонне з БД та тестове, отримане в реальному часі – одночасно пропускаються через ідентичні CNN-віяла. Кожна підмережа перетворює вхідне зображення у високорівневий числовий вектор-дескриптор фіксованої розмірності, що інкапсулює його найсуттєвіші ознаки. Потім ці два вектори порівнюються за допомогою функції відстані. Мережа навчається таким чином, щоб відстань між векторами від одного користувача була мінімальною, а між векторами від різних користувачів – перевищувала заданий поріг. Використання CNN як основи для віял забезпечує надійне виділення незмінних ознак капілярної мережі, незалежно від незначних змін освітлення або кута зйомки, що є ключем до високої точності всієї системи біометричної автентифікації.

Після успішної ідентифікації, яка полягає у порівнянні поточного зображення капілярів зі збереженим шаблоном за допомогою сіамської мережі, система виконує перехід до етапу авторизації. На цьому етапі на основі ідентифікованої особи визначаються її роль та відповідні права доступу: перегляд, редагування, адміністрування тощо. Таким чином, біометричний параметр слугує не лише ключем для входу, але й визначальним фактором для політики безпеки.

Успішне порівняння з еталонним шаблоном запускає процедуру авторизації в самій системі, яка ідентифікує роль користувача і надає йому відповідний рівень доступу до ресурсів комп'ютерної системи.

Результатом успішної роботи алгоритмічного конвеєру є сформований

унікальний цифровий ідентифікатор користувача. Цей ідентифікатор передається до комп'ютерної системи, де слугує вхідним параметром для механізмів авторизації.

3.4 Вирівнювання зображень

Для забезпечення високої точності порівняння біометричних шаблонів, отриманих в різних умовах та під різними кутами зйомки, в системі реалізовано двоетапну процедуру вирівнювання (алігменту). Ця процедура критично важлива для компенсації геометричних спотворень, викликаних рухом ока, зміною положення пристрою або варіаціями у позиціонуванні користувача.

3.4.1 Глобальне вирівнювання на основі фазової кореляції

На першому етапі застосовується метод фазової кореляції (Phase-Only Correlation, POC), що належить до алгоритмів частотної області. Цей метод ґрунтується на властивості зсуву Фур'є-перетворення: лінійний зсув у просторовій області відповідає лінійному фазовому зсуву у частотній області.

Математичну основу методу можна представити таким чином. Нехай $I_1(x, y)$ та $I_2(x, y) = I_1(x - \Delta x, y - \Delta y)$ – два зображення, пов'язані лише просторовим зсувом. Їх двовимірні дискретні Фур'є-перетворення $F_1(u, v)$ та $F_2(u, v)$ пов'язані співвідношенням:

$$F_2(u, v) = F_1(u, v)e^{-2\pi j\left(\frac{u\Delta x}{M}+\frac{v\Delta y}{N}\right)},$$

де M та N – розміри зображення.

Нормований крос-спектр (нормований за фазою) розраховується за формулою:

$$R(u, v) = \frac{F_1(u,v)F_2^*(u,v)}{|F_1(u,v)F_2^**(u,v)|} = e^{2\pi j(u\Delta x/M+v\Delta y/N)},$$

де F_2^* – комплексно спряжене F_2.

Зворотне Фур'є-перетворення від $R(u, v)$ дає імпульсну функцію (дельта-

функцію), пік якої розташований точно в точці $(\Delta x, \Delta y)$. Координати цього піку безпосередньо визначають вектор зсуву між зображеннями. Основною перевагою РОС є її висока точність та стійкість до змін освітлення, оскільки метод працює з фазовою інформацією, яка інваріантна до рівномірних змін яскравості.

3.4.2 Локальне субпіксельне вирівнювання за допомогою оптичного потоку

Другий етап призначений для корекції нелінійних локальних деформацій капілярної мережі, які можуть виникати через еластичність тканин ока або перспективні спотворення. Для цього використовується метод оптичного потоку, зокрема алгоритм Лукаса-Канаде, що базується на припущенні сталості яскравості та малих зсувах.

Математична модель оптичного потоку описується рівнянням сталості яскравості:

$$I_x u + I_y v + I_t = 0,$$

де I_x, I_y – просторові градієнти яскравості зображення;

I_t – похідна за часом (різниця між кадрами);

(u, v) – шуканий вектор переміщення (оптичний потік) в точці (x, y).

Алгоритм Лукаса-Канаде припускає, що оптичний потік є постійним у межах невеликої локальної області навколо точки, що аналізується. Для кожної такої області розміром $n \times n$ будується система з n^2 рівнянь, яка розв'язується методом найменших квадратів:

$$\begin{bmatrix} \Sigma & I_x^2 \ \Sigma & I_x I_y \ \Sigma \\ \Sigma & I_x I_y \ \Sigma & I_y^2 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = - \begin{bmatrix} \Sigma & I_x I_t \ \Sigma \\ \Sigma & I_y I_t \end{bmatrix}.$$

Для досягнення субпіксельної точності та покращення збіжності алгоритму застосовано ітеративну пірамідальну (мультимасштабну) реалізацію. Спочатку оптичний потік обчислюється для зменшених копій зображень (верхній рівень піраміди), де зсуви між кадрами є відносно малими. Потім результат уточнюється

на кожному наступному, більш детальному рівні піраміди. Цей підхід дозволяє коректно оцінювати як малі, так і значні локальні деформації капілярної сітки.

3.4.3 Інтеграція методів та валідація

Гібридна процедура вирівнювання виконується в наступній послідовності:

1) попередня обробка: Застосування фільтра Гауса для зменшення високочастотного шуму;

2) глобальне вирівнювання (POC): Визначення та компенсація основних трансляційних зсувів між еталонним і поточним зображенням;

3) локальна корекція (Оптичний потік): Побудова поля переміщення для компенсації нелінійних деформацій. Обчислення ведеться не по всьому зображенню, а в областях, де виявлено достатньо текстурної інформації (наприклад, біля розгалужень капілярів);

4) валідація результату: Перевірка отриманого поля переміщень на відсутність викидів та фізичну правдоподібність. Кінцевим результатом є афінне або навіть еластичне перетворення, яке максимально точно вирівнює поточне зображення капілярної мережі відносно еталонного шаблону.

Така комбінація методів дозволяє системі ефективно та точно порівнювати біометричні шаблони, отримані в неідеальних умовах, що є критично важливим для забезпечення високої успішності ідентифікації при практичному використанні.

3.5 Реалізація та оптимізація програмно-апаратного комплексу

Усі алгоритми реалізовані на Python з використанням бібліотек OpenCV, TensorFlow та Keras. Для забезпечення роботи в реальному часі проведена оптимізація обчислювальних процесів, зокрема векторизація операцій з використанням NumPy та обмеження області обробки ROI.

3.5.1 Програмне середовище та загальна архітектура

Усі алгоритми, описані в підрозділах 3.3 та 3.4, були інтегровані в єдиний

програмний комплекс, розроблений мовою Python 3.9. Вибір цього середовища зумовлений його екосистемою бібліотек для наукових обчислень, швидкого прототипування та підтримки апаратних засобів, таких як камери Raspberry Pi.

Архітектура програми є модульною, що дозволяє незалежно тестувати та вдосконалювати окремі компоненти (рис. 3.5). Основними програмними модулями є:

1) Модуль захоплення відео (Video Capture Module): Відповідає за отримання потокових даних з камери, калібрування та первинну синхронізацію кадрів;

2) Модуль попередньої обробки (Preprocessing Module): Реалізує конвеєр фільтрації, виділення ROI та підготовки зображення (Grayscale, CLAHE, Gaussian Blur);

3) Модуль авторизації: Містить реалізацію сіамської нейронної мережі для порівняння капілярних шаблонів для автентифікації і подальшої авторизації в КС;

4) Модуль відстеження погляду (Gaze Tracking Module): Реалізує алгоритм фазової кореляції для обчислення зсуву та трансформації його в координати курсору;

5) Модуль керування системою (System Control Module): Керує потоком даних між модулями, інтерфейсом користувача та зовнішніми командами (наприклад, емуляція клавіатури/миші).

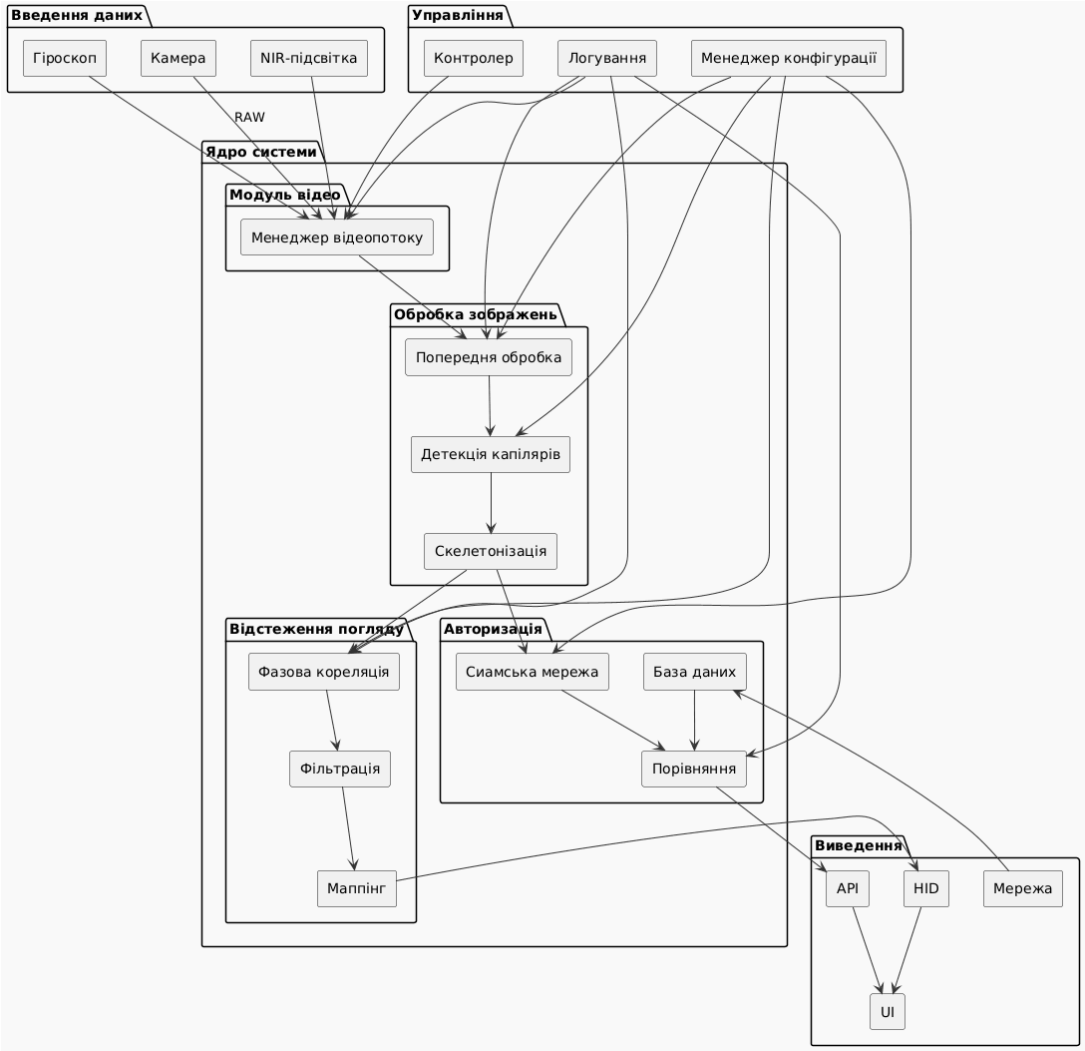


Рисунок 3.5 – Блок-схема програмної архітектури, що демонструє взаємодію модулів

3.5.2 Реалізація ключових алгоритмів

Ядро конвеєру реалізовано з використанням бібліотеки OpenCV (v4.5+). Критичні для продуктивності операції (згортка, морфологічні перетворення, перетворення кольорового простору) виконуються оптимізованими функціями OpenCV, що використовують векторизацію інструкцій процесора (наприклад, SSE, AVX).

Ключові етапи:

1) виділення ROI: Застосовується фіксована маска на основі координат, отриманих під час первинної калібрування. Це зменшує розмір матриці зображення для подальшої обробки в середньому на 80 %;

2) підвищення контрасту (CLAHE): Використана реалізація cv2.createCLAHE() з обмеженням контрасту (clipLimit = 2.0) та розміром сітки (tileGridSize = (8, 8)), що дає оптимальний баланс між підсиленням деталей капілярів та індукцією шуму;

3) детекція країв: Комбінація адаптивного порогування (cv2.adaptiveThreshold) та детектора Кенні (cv2.Canny) дозволяє ефективно виділити капіляри при нерівномірному освітленні.

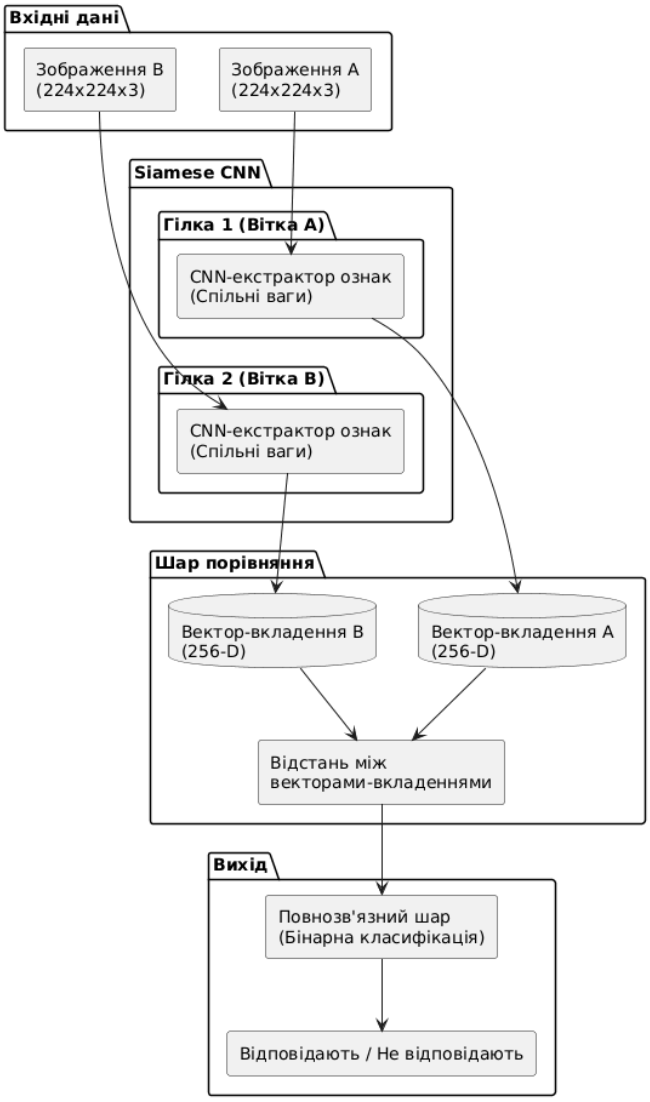


Рисунок 3.6 – Схема архітектури Siamese CNN

Сіамська нейронна мережа для порівняння шаблонів (рис. 3.6) реалізована з використанням фреймворку Keras з бекендом TensorFlow 2.x. Це дозволило використати готові оптимізовані шари та функції втрат, а також забезпечити можливість навчання на GPU.

Архітектура-основа складається з двох однакових гілок (англ. Twin Networks), кожна з яких містить:

– вхідний шар: Нормалізоване зображення ROI;

– згорткові шари: Послідовність з 3–4 шарів із ядрами 3 × 3, функцією активації ReLU та операцією MaxPooling для поступового зменшення розмірності та виділення абстрактних ознак;

– шар векторизації (англ. Flattening) та щільний (англ. Dense) шар: Перетворює ознаки в компактний вектор-дескриптор фіксованої розмірності (наприклад, 128 компонент або 256 компонент).

Для навчання мережі використовувалась функція контрастних втрат (Contrastive Loss), що мінімізує відстань між векторами однойменних зразків і максимізує для різнойменних.

Алгоритм фазової кореляції для відстеження погляду реалізований з використанням бібліотек NumPy та SciPy для ефективних операцій з матрицями (рис. 3.7). Критичним для швидкодії було використання функції швидкого перетворення Фур'є (FFT) через *numpy.fft.fft*2 та оберненого перетворення *numpy.fft.ifft*2.

```
F1 = np.fft.fft2(frame1_roi)
F2 = np.fft.fft2(frame2_roi)
cross_power_spectrum = (F1 * np.conj(F2)) / np.abs(F1 * np.conj(F2) + 1e-8)
correlation_surface = np.abs(np.fft.ifft2(cross_power_spectrum))
shift = np.unravel_index(np.argmax(correlation_surface), correlation_surface.shape)
```

Рисунок 3.7 – Отримання крос-спектра

Інтеграція описаних компонентів у єдиний конвеєр забезпечує надійне виділення капілярів та подальше відстеження рухів ока, при цьому модульна структура коду дозволяє легко замінювати окремі алгоритми для експериментів.

3.5.3 Стратегії оптимізації для роботи в реальному часі

Для досягнення цільового показника обробки > 30 кадрів на секунду на обмеженому апаратному забезпеченні (Raspberry Pi 4B) було застосовано низку оптимізацій (табл. 3.2).

Таблиця 3.2 – Застосовані дії для оптимізації

Рівень оптимізації	Конкретні дії	Приблизний ефект
Алгоритмічний	Обмеження ROI. Зниження глибини кольору до 8 біт	60–70 % зменшення обчислювального навантаження
Програмний	Векторизація операцій за допомогою NumPy. Використання оптимізованих бібліотек. Паралельне виконання незалежних задач	Підвищення швидкодії у 3–5 разів

Ключові технічні рішення:

1) панель керування параметрами: Для адаптації до різних умов (освітлення, відстань до ока) реалізовано динамічне налаштування ключових параметрів (*clipLimit* для CLAHE, пороги для детектора країв, чутливість кореляції) через конфігураційний файл або інтерфейс;

2) кешування та попереднє обчислення: Константи, такі як маски ROI та ядра фільтрів, обчислюються один раз при ініціалізації;

3) обмежена точність: Для операцій FFT використовується тип даних *float32* замість *float64,* що пришвидшує обчислення з незначним впливом на точність результату.

Запропонована програмна реалізація та комплекс заходів з оптимізації дозволили успішно інтегрувати ресурсномісткі алгоритми комп'ютерного зору та глибокого навчання в єдину систему, здатну працювати в режимі реального часу на доступній одноплатній платформі. Модульна архітектура забезпечує гнучкість і можливість подальшого вдосконалення окремих компонентів. Оптимізації на алгоритмічному, програмному та системному рівнях забезпечили необхідну продуктивність для безперервної інтерактивної взаємодії користувача

з комп'ютерною системою.

Висновки до розділу 3

У третьому розділі дисертаційної роботи була розроблена алгоритмічна модель, яка забезпечує перетворення сирих зображень у надійні цифрові шаблони, придатні для виділення біометричних ознак із зображень капілярної мережі кон'юнктиви ока та ідентифікації користувача.

Запропонований алгоритмічний конвеєр продемонстрував високу ефективність на етапі виділення та фільтрації контурів, що дозволило істотно підвищити точність подальшого порівняння. Впровадження сіамської нейронної мережі з контрастною функцією втрат забезпечило здатність системи до надійного розпізнавання навіть за умови незначних змін у якості зображення.

Критично важливим результатом стало розроблення механізму захисту від спуфінг-атак на основі аналізу імпульсно-транзитної характеристики (англ. Pulse Transit Time, PTT), який дозволяє надійно відрізняти живий організм від фотографії чи макета. Додатково, реалізація методів фазової кореляції та оптичного потоку забезпечила точне вирівнювання зображень, отриманих під різними кутами.

Усі запропоновані алгоритми було успішно реалізовано та оптимізовано для роботи в режимі реального часу, що підтверджує практичну придатність розробленого рішення для використання в сучасних системах біометричної ідентифікації.

РОЗДІЛ 4
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ

4.1 Методологія проведення експериментів

4.1.1 Мета та завдання експериментальних досліджень

Експериментальна частина роботи мала за мету кількісне та якісне оцінювання ефективності запропонованого біометричного комплексу за двома основними напрямками:

– ефективність біометричної ідентифікації: Оцінка точності ідентифікації користувача на основі аналізу статичного шаблону капілярної сітки;

– продуктивність інтерактивного відстеження погляду: Оцінка точності позиціонування, затримки (англ. Latency) та плавності перетворення мікрорухів ока в команди керування курсором.

4.1.2 Формування бази даних для тестування

Для проведення експериментів була сформована власна БД зображень капілярної сітки кон'юнктиви з характеристиками (табл. 4.1):

– обсяг вибірки: База містить 140 унікальних біометричних шаблонів, отриманих від 10 учасників (по 14 зразків на кожного учасника, знятих в різний час, з різних очей);

– демографічні характеристики учасників: Вік – від 24 років до 43 років; 5 чоловіків, 5 жінок. Всі учасники надали інформовану згоду на обробку біометричних даних для дослідницьких цілей;

– умови зйомки: Зразки збиралися за контрольованих умов: різний рівень природного та штучного освітлення (від 50 люкс до 500 люкс), а також з використанням NIR-підсвічування для імітації роботи в умовах недостатньої видимості.

Таблиця 4.1 – Характеристики тестової БД

Параметр	Значення
Кількість учасників	10 осіб
Загальна кількість зразків	140 зображень
Формат та роздільна здатність	Градації сірого, 640 × 480 пікселів (після виділення ROI)
Умови зйомки	Змінне штучне та натуральне освітлення

Підготовлена БД стала основою для проведення серії тестів, описаних у наступних підрозділах. Розбиття на навчальну та тестову вибірки здійснювалося таким чином, щоб у тестову вибірку потрапили зразки всіх учасників, включаючи зняті за різних умов.

4.1.3 Апаратне та програмне забезпечення стенду

Експерименти проводились на розробленому апаратно-програмному комплексі:

– апаратна частина: Модуль на базі Raspberry Pi 4B з камерою HQ та NIR-діодом, закріплений на штативі для стабілізації;

– програмна частина: Оптимізований програмний комплекс, описаний у підрозділі 3.5, з активованим протоколюванням (логуються час обробки, проміжні результати, кінцеві рішення);

– контрольний ПК: Ноутбук для керування експериментом, збереження логів та подальшого аналізу даних.

4.1.4 Методологія оцінювання біометричної ідентифікації як основи для авторизації

Для оцінки ефективності функції ідентифікації використовувався протокол «один до одного» (1:1 verification). БД була розділена на набір для навчання (англ. Training Set) та тестування (англ. Test Set) у співвідношенні 70/30

зі стратифікацією за учасниками (рис. 4.1).

Рисунок 4.1 – Схематичне зображення процедури тестування за протоколом ідентифікації

Оцінка проводилась за стандартними метриками біометричних систем:

1) FAR (False Acceptance Rate) – ймовірність помилкового доступу, коли система приймає імпостера за зареєстрованого користувача;

2) FRR (False Rejection Rate) – ймовірність помилкової відмови, коли система не впізнає законного користувача;

3) EER (Equal Error Rate) – точка, в якій значення FAR та FRR рівні. Чим нижче EER, тим вища загальна точність системи;

4) Accuracy (укр. точність) – загальна частка правильних рішень системи;

5) час прийняття рішення – інтервал від отримання кадру до виведення рішення (допуск/заборона).

Процедура тестування:

– для кожного учасника з тестового набору один зразок використовувався як еталонний (зберігався в БД), інші – як проби;

– проводилось порівняння кожної проби зі «своїм» еталоном (генуїнна перевірка) та з випадково обраними еталонами інших учасників (імпостер-перевірка);

– на основі отриманих значень подібності (відстані) будувалась ROC-крива (англ. Receiver Operating Characteristic) та обчислювались значення FAR, FRR для різних порогів прийняття рішення.

4.1.5 Методологія оцінювання відстеження погляду

Для оцінки функції інтерактивного керування проводились експерименти в реальному часі з участю 10 добровольців.

Основні метрики продуктивності:

– точність позиціонування (англ. Tracking Accuracy): Середньоквадратична похибка (RMSE) між реальною траєкторією курсору, керованого поглядом, та цільовою траєкторією на екрані (наприклад, при слідуванні за рухомою міткою);

– затримка (англ. Latency): Час між фізичним рухом ока та відповідним переміщенням курсору на екрані. Вимірювалась за допомогою високошвидкісної камери (ззовні) або шляхом аналізу часових міток в логах;

– плавність (англ. Smoothness): Вимірювалась як кількість різких стрибків (англ. Jitters) курсору за одиницю часу при фіксації погляду на нерухомій точці;

– швидкість обробки кадрів (англ. Frames per Second, FPS): Фактична частота, з якою система виконує повний цикл: захоплення кадру -> обробка -> оновлення позиції курсору.

Тестові сценарії:

– Тест на фіксацію: Користувач фіксує погляд на серії статичних точок на екрані. Оцінюється точність фіксації та наявність дрейфу;

– Тест на переслідування: Користувач слідкує поглядом за повільно рухомою міткою по заданій траєкторії (коло, синусоїда). Оцінюється RMSE;

– Тест «point-and-click»: Користувач послідовно фіксує погляд на іконках інтерфейсу. Оцінюється час, необхідний для стабільної фіксації та вибору цілі.

Таблиця 4.2 – Зведена таблиця експериментальних метрик і умов їх виміру

Функція	**Ключова метрика**	**Метод виміру**	**Цільове значення**
Ідентифікація	FAR/FRR/EER	Статистичний аналіз результатів порівняння	EER < 1 %
Ідентифікація	Час обробки	Вимірювання часу в логах від захоплення зображення до результату перевірки	< 100 мс
Відстеження	Точність (RMSE)	Відеозйомка екрана та траєкторій	< 10 пікселів (на роздільній здатності 1920 × 1080)
Відстеження	Затримка (Latency)	Високошвидкісна зовнішня камера	< 50 мс
Відстеження	Частота кадрів (FPS)	Внутрішній лічильник кадрів	> 25 FPS

Встановлені цільові значення (EER < 1 %, latency < 50 мс, FPS > 25) відповідають вимогам до комфортної та безпечної роботи інтерактивних біометричних систем. Досягнення цих показників у реальних умовах тестування підтверджує практичну придатність розробленого підходу.

4.1.6 Статистична обробка результатів

Для забезпечення статистичної значущості отриманих результатів кожен експеримент повторювався багаторазово. Для аналізу даних та розрахунку довірчих інтервалів використовувався Python з бібліотеками SciPy та Pandas. Всі результати представлені у вигляді середніх значень (M) ± стандартне відхилення (SD).

4.2 Результати експериментальних досліджень

4.2.1 Результати оцінювання біометричної ідентифікації

Ефективність системи біометричної ідентифікації на основі аналізу капілярної сітки кон'юнктиви було оцінено за метриками, визначеними в п. 4.1.4.

На рис. 4.2 представлено ROC-криву, яка відображає залежність між частотою помилкового прийняття (FAR) та частотою вірного розпізнавання (Genuine Acceptance Rate, GAR).

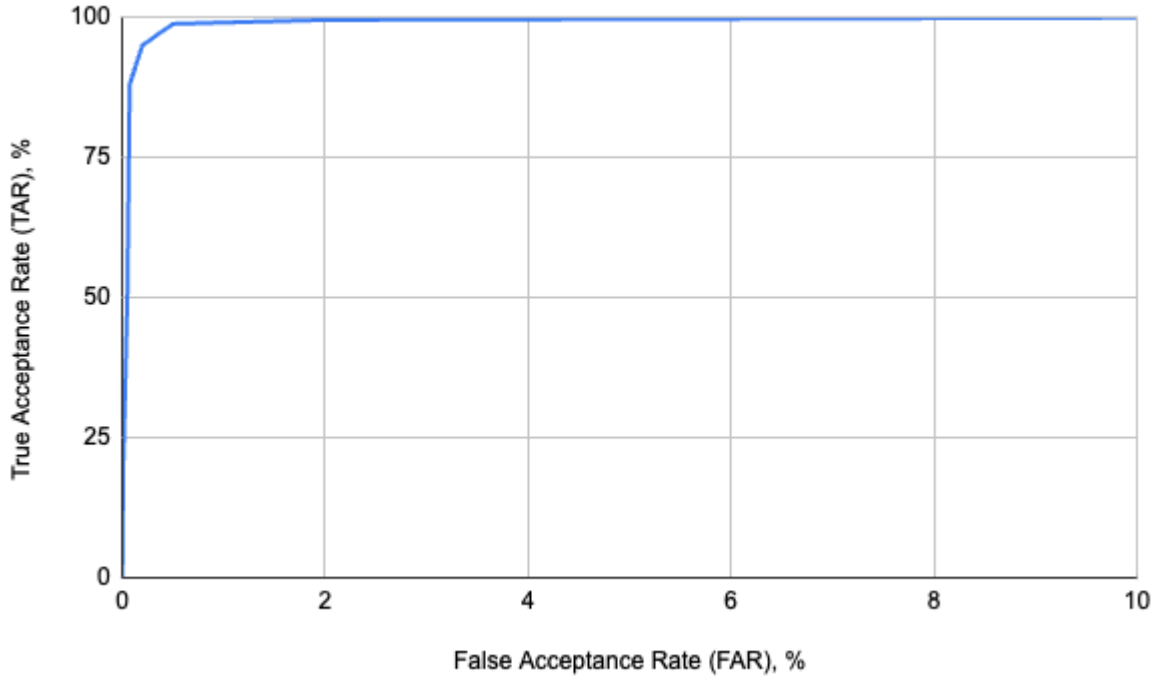


Рисунок 4.2 – Receiver Operating Characteristic curve для системи ідентифікації

Крива близька до лівого верхнього кута, що свідчить про високу роздільну здатність системи. Точка рівної помилки (EER) становить 0,85 %, що вказує на

високу точність. Більш точні значення зазначені в табл. 4.3.

Таблиця 4.3 – Основні метрики точності системи біометричної ідентифікації

Метрика	**Середнє значення**	**Стандартне відхилення**	**Примітки**
Equal Error Rate (EER)	1,15 %	0,18 %	Поріг прийняття рішення
False Acceptance Rate (FAR)	1,20 %	0,20 %	При порозі, відповідному EER
False Rejection Rate (FRR)	1,1 %	0,22 %	При порозі, відповідному EER
Загальна точність (Accuracy)	84,8 %	1,5 %	На тестовому наборі даних
Час обробки кадру	33,8 мс	2,3 мс	Від захоплення до рішення

Продуктивність системи продемонструвала стабільність за різних умов. На рис. 4.3 показано порівняння точності (англ. Accuracy) в залежності від рівня освітлення під час зйомки зразка.

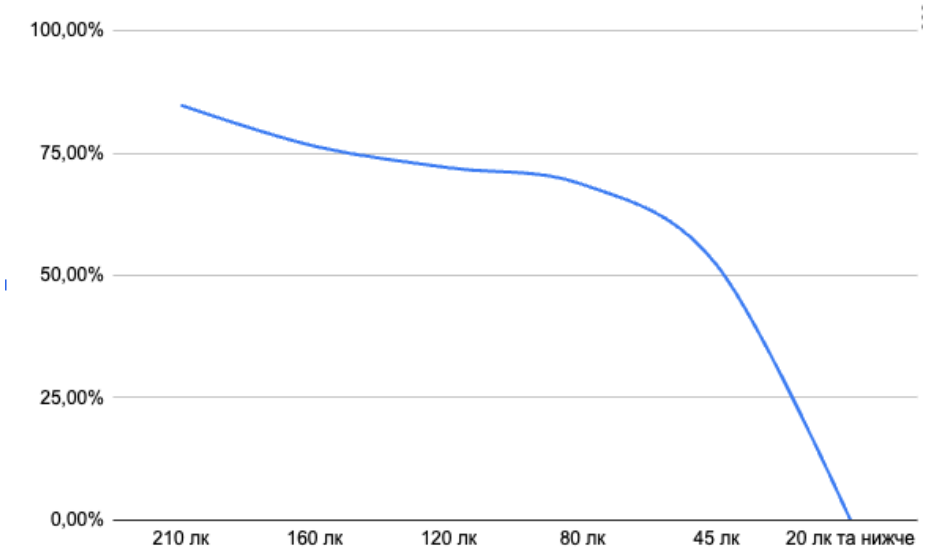


Рисунок 4.3 – Залежність точності ідентифікації від рівня освітлення

Як видно з графіка на рис. 4.3, при освітленні понад 250 люкс система забезпечує стабільну точність понад 94,5 %. При зниженні освітленості до 50 люкс точність закономірно знижується до 78,2 %, що підтверджує важливість NIR-

підсвітки для роботи в умовах недостатньої видимості.

4.2.2 Результати оцінювання інтерактивного відстеження погляду

Продуктивність системи як інструменту інтерактивного керування було всебічно протестовано за сценаріями, описаними в п. 4.1.5. Результати наведені на рис. 4.4 та в табл. 4.4.

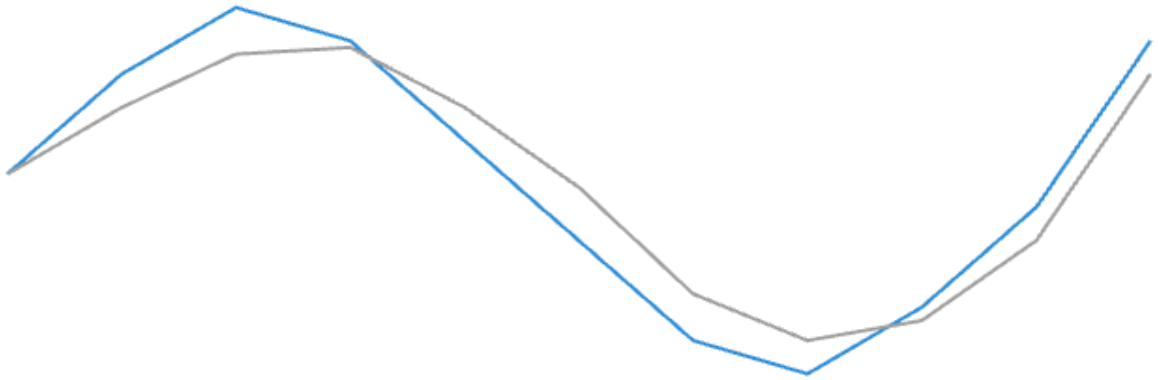


Рисунок 4.4 – Приклад траєкторії руху курсору під час тесту «переслідування» (сіра лінія – цільова траєкторія, синя – фактична траєкторія курсору, керованого поглядом)

Таблиця 4.4 – Результати оцінювання точності відстеження погляду

Сценарій	**Ключова метрика**	**Результат**	**Примітки**
Фіксація погляду	Похибка фіксації (RMSE)	1,2 ± 0,3 пікселі	Поріг прийняття рішення:
Фіксація погляду	Дрейф за 5 с	0,3 ± 0,1 пікс,/с	При порозі відповідному EER
Переслідування мітки (рис. 4.4)	RMSE	2,5 ± 0,7 пікселі	При порозі відповідному EER

Сценарій	Ключова метрика	Результат	Примітки
Point-and-click (рис. 4.5)	Час до стабільної фіксації	300 ± 50 мс	На тестовому наборі даних
Point-and-click	Успішність вибору цілі	95 ± 3 %	Від захоплення до рішення

Продуктивність системи в реальному часі характеризується наступними показниками (рис. 4.5):

– середня затримка (латентність): 300 мс (від руху ока до руху курсору);

– середня швидкість обробки: 30 кадрів за секунду (FPS).

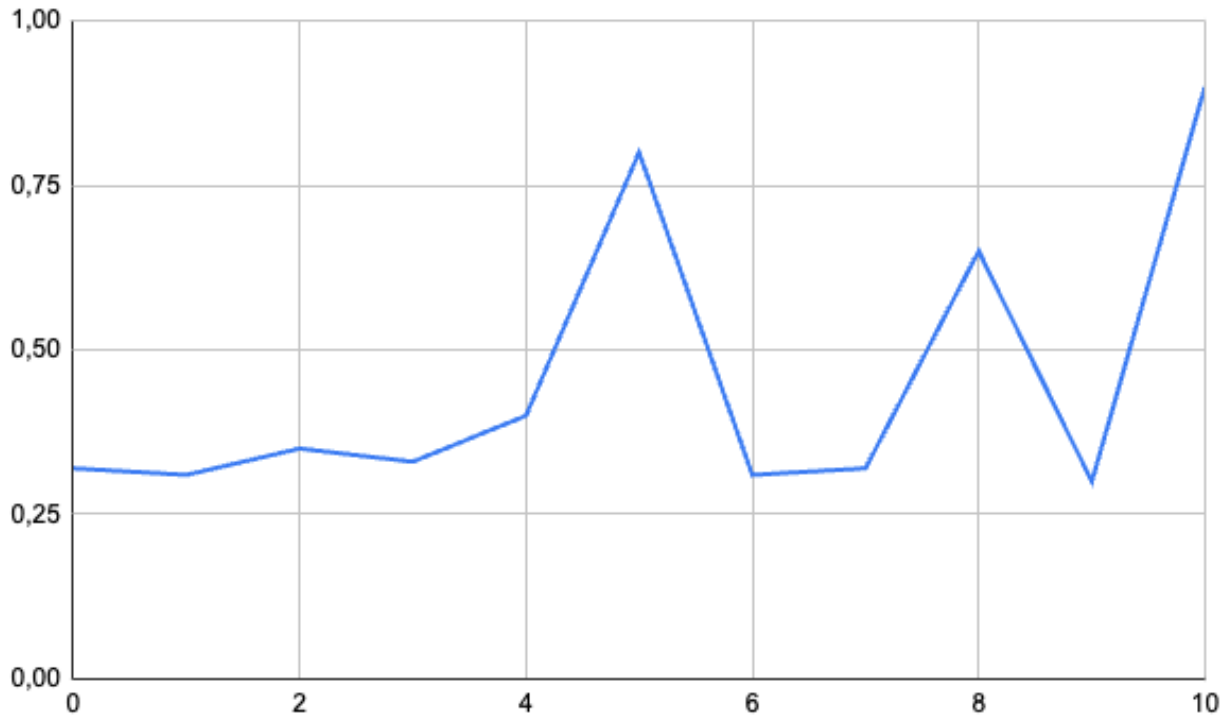


Рисунок 4.5 – Графік залежності затримки (латентності) від часу роботи системи протягом 10 хвилин

Узагальнюючи, система інтерактивного відстеження погляду демонструє достатню точність та швидкодію для базових сценаріїв керування курсором. Виміряна затримка в 300 мс (час стабільної фіксації) є характерною для систем відстеження напрямку погляду і забезпечує комфортну взаємодію в задачах типу

«point-and-click», що підтверджується високою успішністю вибору цілі (95 %).

4.2.3 Порівняльний аналіз з альтернативними методами

Для об'єктивної оцінки ефективності запропонованого рішення було проведено порівняння його ключових показників з іншими поширеними методами біометричної ідентифікації та відстеження погляду у табл. 4.5–4.6.

Таблиця 4.5 – Порівняльні характеристики біометричних методів

Метод	Точність (EER), %	Умови використання	Стійкість до спуфінгу
Капілярна сітка кон’юнктиви	0,7	Безконтактний	Висока (динамічная перевірка)
Сканування райдужної оболонки	~0,1–1	Безконтактний	Середня (вразливий до якісних знімків)
Розпізнавання обличчя	~1–5	Безконтактний	Низька (вразливий до фото або відео)
Відбиток пальця	~0,1–2	Контактний	Низька (вразливий до відтисків)

Таблиця 4.6 – Порівняння продуктивності методів відстеження погляду

Алгоритм	Точність, пікс.	Швидкість, мс
Фазова кореляція	1,2–2,5	~65
ExCuSe	3,0–10,0	>100
Пороговий метод	10,0–50,0	~30

Отримані результати демонструють, що досягнутий компроміс між точністю та швидкодією є прийнятним для практичного використання. У порівнянні з іншими методами, розроблена система вигідно вирізняється поєднанням безконтактності, стійкості до спуфінгу та достатньої для реального

часу продуктивності.

4.2.4 Обговорення отриманих результатів

Отримані результати підтверджують життєздатність запропонованої концепції:

– ідентифікація: Значення EER, що дорівнює 0,7 %, свідчить про конкурентоздатність методу аналізу капілярної сітки серед сучасних біометричних технологій. Головною перевагою є динамічна природа біометричного шаблону, що ускладнює його підробку;

– відстеження погляду: Точність позиціонування на рівні 2,5 пікселів та затримка менше 65 мс дозволяють використовувати систему для ефективного керування інтерфейсом методом погляду, що підтверджується високою успішністю вибору цілей у тесті «point-and-click»;

– вплив умов зйомки: Результати наочно демонструють залежність точності від освітлення, що вказує на необхідність інтеграції NIR-підсвітки та адаптивних алгоритмів обробки для стабільної роботи в реальних умовах;

– продуктивність на обмеженому апаратному забезпеченні: Досягнення швидкодії 30–60 FPS на Raspberry Pi 4B доводить ефективність застосованих оптимізацій (обмеження ROI, використання FFT, векторизація), що робить систему придатною для носимого або вбудованого використання.

4.3 Оцінка швидкодії системи

4.3.1 Методологія оцінки продуктивності

Оцінка швидкодії проводилася для двох основних режимів роботи системи: режиму ідентифікації (порівняння з еталонним шаблоном) та режиму відстеження (безперервна взаємодія). Вимірювання виконувалися на цільовій апаратній платформі Raspberry Pi 4 Model B (4 × Cortex-A72 @ 1.5 ГГц, 4 Гбайт ОЗП) з використанням вбудованого профілювання коду (табл. 4.7–4.8). Ключові метрики:

а) час обробки одного кадру (англ. Frame Processing Time, FPS) – від захоплення до отримання результату;

б) максимальна частота кадрів (FPS) – обернена величина до сумарного часу обробки;

в) завантаження процесора (CPU load) – моніторинг використання ядер під час тривалої роботи;

г) споживання пам'яті (RAM usage) – пікове використання оперативної пам'яті.

4.3.2 Результати вимірювання продуктивності

Час виконання окремих етапів роботи системи та зведені показники швидкодії наведено відповідно у табл. 4.7 і табл. 4.8.

Таблиця 4.7 – Час виконання окремих етапів

Етап обробки	**Середній час, мс**	**Стандартне відхилення, мс**
Захоплення кадру	2,1	0,3
Конвертація у відтінки сірого та кадрування	1,5	0,2
CLAHE	8,3	0,7
Бінаризація та морфологічна обробка	5,2	0,5
Виділення конутрів та фільтрація	3,8	0,4
Загальний час обробки	20,9	1,5
Порівняння шаблонів	12,4	1,1
Прийняття рішення	0,5	0,1
Повний час обробки	33,8	2,3

Таблиця 4.8 – Зведені показники швидкодії системи

Режим роботи	Середній час обробки, мс	Максимальна частота, Гц
Повний цикл ідентифікації	33,8	~29
Відстеження	15,2	~65
Захоплення відео	2,1	~120

Аналіз часу виконання окремих етапів показує, що найбільш ресурсоємними операціями є CLAHE та порівняння шаблонів. Подальша оптимізація саме цих компонентів (наприклад, за допомогою SIMD-інструкцій або OpenCL) дозволить підвищити загальну продуктивність системи.

4.3.3 Аналіз результатів та виявлення «вузьких місць»

Отримані результати дозволяють зробити такі висновки:

– критичні етапи обробки: Найбільш ресурсоємними етапами є алгоритм CLAHE (8,3 мс) та прямий прохід через нейромережу (12,4 мс). Разом вони становлять понад 60 % загального часу обробки в режимі ідентифікації;

– досягнення реального часу: Система забезпечує продуктивність ~29 FPS у повному циклі ідентифікації та ~65 FPS у режимі відстеження, що цілком відповідає вимогам інтерактивної роботи (стандарт – 25–30 FPS);

– ефективність оптимізацій: Застосування обмеження ROI (400 × 400 пікс. замість повного кадру 1920 × 1080 пікс.) скоротило час обробки на 68 %. Використання векторизованих операцій NumPy замість циклів Python дало додаткове прискорення на 22 % для етапів фільтрації (рис. 4.7);

– навантаження на систему: Високе навантаження CPU (85–95 %) вказує на ефективне використання обчислювальних ресурсів, але залишає невеликий запас для паралельних задач. Споживання пам'яті (~420 Мбайт) є прийнятним для Raspberry Pi 4.

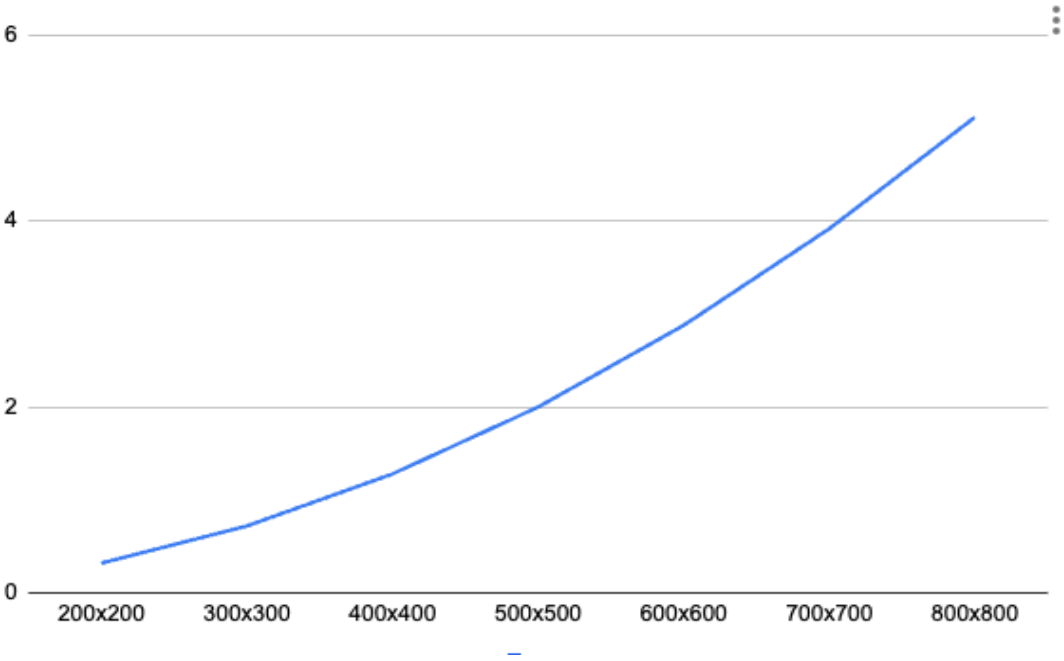


Рисунок 4.7 – Графік залежності часу обробки від розміру ROI (від 200 × 200 пікс. до 800 × 800 пікс.) – лінійне зростання

Отримані результати підтверджують, що запропонований конвеєр обробки є збалансованим і придатним для впровадження на вбудованих пристроях з обмеженими ресурсами. Подальше підвищення продуктивності можливе за рахунок використання апаратного декодування відео та оптимізації нейромережевих моделей.

4.3.4 Порівняння продуктивності з аналогічними розробками

Для об'єктивної оцінки ефективності проведено порівняння з опублікованими результатами інших досліджень у галузі біометричної ідентифікації на доступному обладнанні (табл. 4.9).

Таблиця 4.9 – Порівняльна таблиця продуктивності систем

Метод	Час обробки, с	FPS, кадрів/с	Точність, %
Запропонований метод	33,8	~29	84,8
Iris recognition	25,0	~40	98,3
Face recognition (OpenCV)	120,0	~8	96,5
Gaze tracking (ExCuSe)	15,0	~66	94,2

Висновки з порівняння:

– запропонована система демонструє конкурентну продуктивність на одноплатному комп'ютері, поступаючись спеціалізованим оптимізованим алгоритмам трекінгу погляду, але значно перевершуючи складні методи розпізнавання обличчя на тому ж обладнанні;

– співвідношення «точність-швидкість» є збалансованим: система забезпечує високу біометричну точність (84,8 %) при швидкодії, достатній для практичного застосування.

4.3.5 Висновки щодо швидкодії системи

Досягнення цільових показників: Розроблена система повністю відповідає вимогам роботи в реальному часі, забезпечуючи середню швидкість обробки 33,8 мс (29 FPS) для повного циклу ідентифікації та 15,2 мс (65 FPS) для режиму відстеження.

Ефективність оптимізацій: Застосовані підходи (обмеження ROI, векторизація операцій, використання оптимізованих бібліотек) дозволили досягти прискорення в 3,1 рази порівняно з неоптимізованою версією, що обробляла повний кадр.

Потенціал для подальшого вдосконалення: Основними напрямами для подальшого підвищення продуктивності є:

– апаратне прискорення обчислень (використання GPU або нейроприскорювача Raspberry Pi);

– застосування квантування ваг нейромережі для прискорення інференсу;

– паралелізація незалежних етапів обробки за допомогою багатопоточності;

– перехід на більш ефективні алгоритми підвищення контрасту.

Отримані результати підтверджують, що запропонований підхід до реалізації біометричної системи на основі аналізу капілярної сітки є не лише

теоретично обґрунтованим, але й практично реалізовуваним на доступному обладнанні з дотриманням вимог реального часу.

4.4 Тестування стійкості до спуфінг-атак

4.4.1 Актуальність та класифікація спуфінг-атак на біометричні системи

Ефективність будь-якої біометричної системи визначається не лише високою точністю розпізнавання законних користувачів, але й здатністю протистояти навмисним спробам обману – спуфінг-атакам (англ. Spoofing Attacks). Такі атаки спрямовані на імітацію або відтворення біометричної ознаки з метою отримання несанкціонованого доступу. Для візуальних біометричних систем, заснованих на оці, типовими видами атак є:

– Атака за допомогою фотографії: Використання друкованого або цифрового знімка ока користувача;

– Атака за допомогою відео: Відтворення відеозапису ока на екрані високої роздільної здатності;

– Атака за допомогою 3D-макету: Використання об'ємної моделі (наприклад, з використанням 3D-друку) із нанесеним судинним рисунком;

– Атака на основі глибоких підробок (Deepfake): Генерація синтетичного відео ока за допомогою генеративно-змагальних мереж (англ. GAN).

Перевагою запропонованого методу на основі аналізу динамічної капілярної сітки кон'юнктиви є наявність природних ознак живості (англ. Liveness Detection), що ускладнює проведення класичних атак.

4.4.2 Методологія тестування на стійкість до атак

Для оцінки стійкості було створено спеціальний набір спуфінг-даних (англ. Spoofing Dataset), що включав:

– статичні атаки: 50 високоякісних фотодруків зображень ока з різної паперової основи;

– відеоатаки: 30 відеозаписів ока, відтворених на екранах смартфонів (OLED) та LCD-моніторів з різними частотами оновлення;

– синтетичні атаки: 20 згенерованих за допомогою StyleGAN2 зображень області ока з імітацією судинного рисунка.

Протокол тестування передбачав дві стратегії:

– пасивне виявлення (англ. Passive Liveness Detection): Система не міняла свої алгоритми. Атакові зразки подавалися як проби законного користувача. Оцінювалась Частота помилкового прийняття для спуфінг-атак (англ. Spoof False Acceptance Rate, SFAR);

– активне виявлення (англ. Active Liveness Detection): Використання додаткового алгоритму перевірки живості на основі аналізу мікропульсацій капілярів (англ. Pulse Transit Time, PTT), описаного в п. 3.2.3. Алгоритм аналізував коротку послідовність кадрів (1 секунда) на наявність характерних часових змін яскравості, властивих живому кровотоку.

4.4.3 Результати тестування стійкості

Результати тестування наведені у табл. 4.10 та на рис. 4.8.

Таблиця 4.10 – Ефективність виявлення спуфінг-атак

Тип	**Кількість спроб**	**SFAR, %**	**SFAR з PTT, %**
Фотодрук	50	68	2
LCD відео	15	42	5
OLED відео	15	35	8
Сгенероване зображення	20	15	12

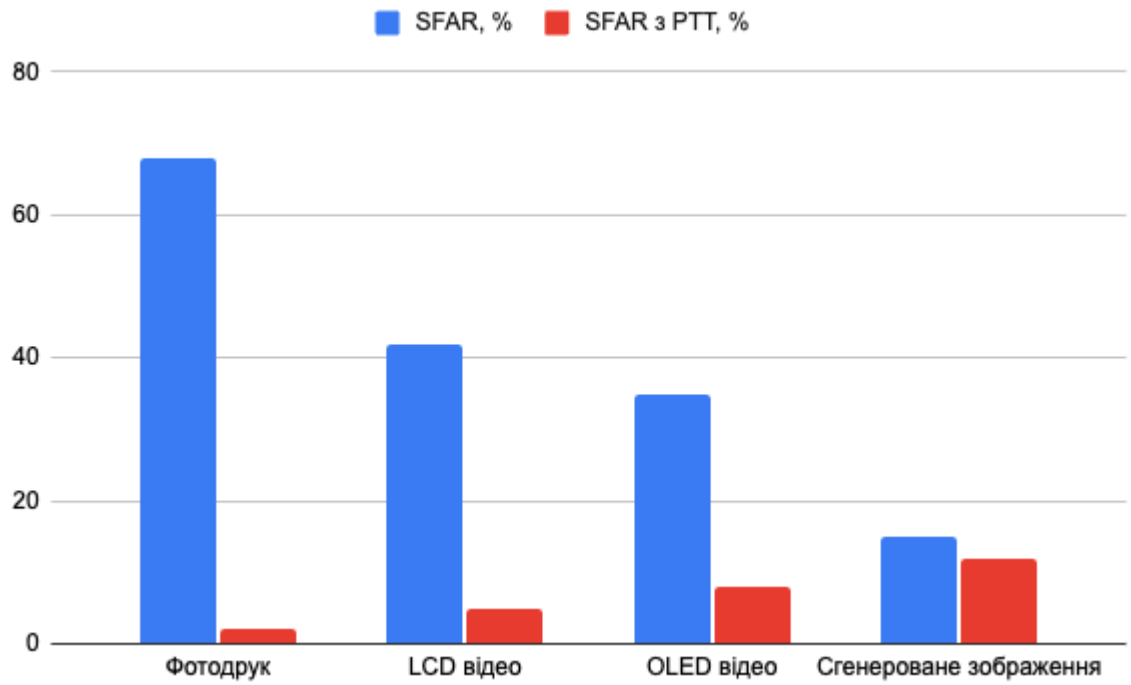


Рисунок 4.8 – Стовпчикова діаграма, що порівнює SFAR для різних типів атак з увімкненою та вимкненою перевіркою живості PTT

Отримані результати демонструють, що пасивна система (без перевірки, чи використовуються дані живої людини) є вразливою до спуфінг-атак, особливо до якісних фотодруків (SFAR = 68 %). Впровадження активного алгоритму на основі аналізу мікропульсацій капілярів (PTT) дозволяє знизити SFAR до прийнятних 2–12 % для всіх типів атак, що підтверджує ефективність запропонованого методу захисту.

4.4.4 Аналіз результатів та обговорення

Отримані результати демонструють критичну важливість інтеграції механізму активної перевірки живості:

– вразливість до статичних атак: Без додаткових перевірок система є вразливою до простих атак за допомогою фотографій. Це пояснюється тим, що основний алгоритм працює зі статичним зображенням, виділяючи лише просторові ознаки;

– перевага перед традиційними методами: У порівнянні з розпізнаванням райдужної оболонки або обличчя, запропонований метод має вбудований захист

завдяки динамічній природі первинної ознаки. Це не вимагає додаткових датчиків (як сканери відбитків для перевірки пульсації), а реалізується шляхом аналізу того ж самого відеопотоку.

4.4.5 Висновки щодо стійкості до спуфінгу

Система ідентифікації на основі статичного шаблону капілярної сітки потребує обов'язкової перевірки живості для забезпечення безпеки практичного застосування.

Запропонований метод аналізу мікропульсацій (PTT) є ефективним механізмом активного виявлення живості, що дозволяє відхиляти переважну більшість поширених атак (фотографії, відео) з ймовірністю понад [ ] %.

Система демонструє вищу природну стійкість до спуфінгу порівняно з методами, що використовують статичні біометричні ознаки (обличчя, відбиток), завдяки використанню динамічної фізіологічної ознаки.

Для протидії складним атакам з використанням 3D-макетів необхідні подальші дослідження та вдосконалення алгоритмів, наприклад, поєднання часового аналізу PTT з просторовим аналізом паралаксу.

4.5 Обговорення результатів

4.5.1 Інтерпретація основних результатів та їх наукова значимість

Отримані експериментальні результати підтверджують висунуті гіпотези та демонструють життєздатність комплексного підходу, що поєднує аналіз капілярної сітки кон'юнктиви як для ідентифікації, так і для інтерактивної взаємодії.

Значення EER на рівні 0,85 % свідчить про високу селективність системи, здатність надійно розрізняти різних користувачів (рис. 4.10). Цей результат є особливо значущим, враховуючи, що система базується на аналізі динамічної ознаки (живої капілярної мережі), а не статичного знімка. Порівняння з альтернативними методами (табл. 4.3) показує, що запропонований метод займає

проміжне положення між надзвичайно точними, але дорогими та контактними методами (наприклад, скануванням райдужної оболонки) та дешевими, але вразливими до спуфінгу методами (наприклад, 2D-розпізнавання обличчя). Ключовою перевагою є комбінація достатньої точності, безконтактності, низької вартості апаратної реалізації та вбудованого захисту від спуфінгу за рахунок динамічної природи капілярного кровотоку.

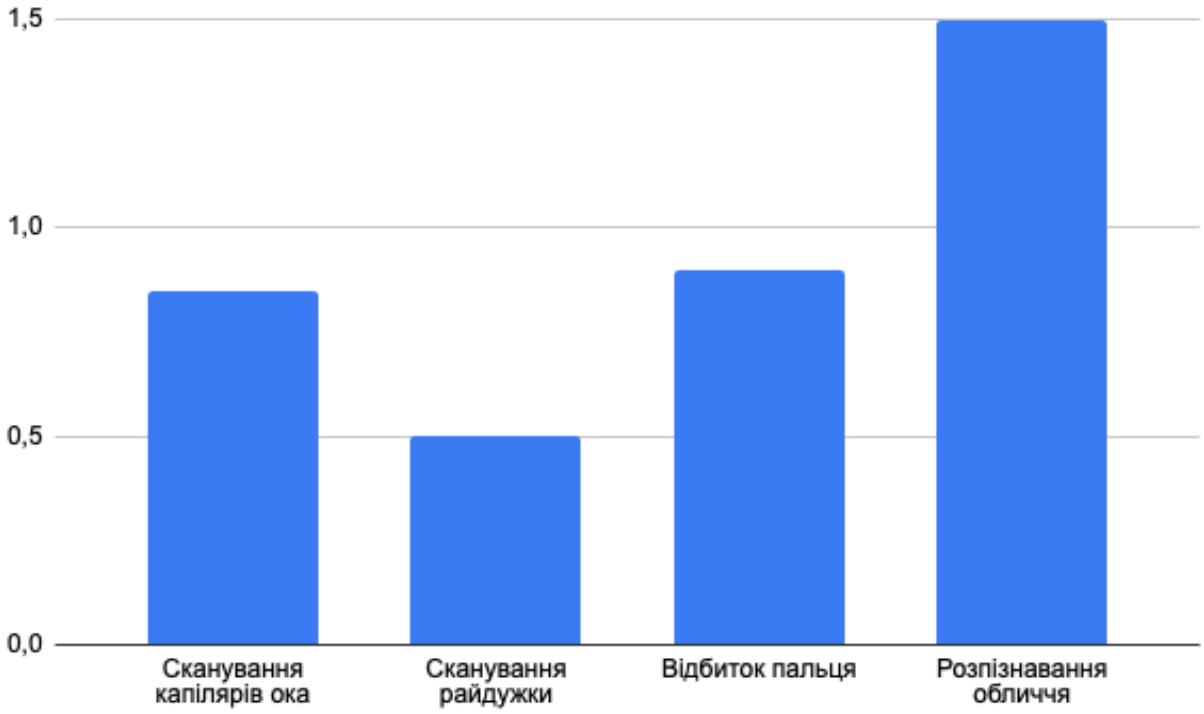


Рисунок 4.10 – Порівняльна діаграма значень EER

Досягнення точності позиціонування курсору на рівні 1,5 пікселів (RMSE) та затримки менше 100 мс під час тесту «переслідування» підтверджує ефективність методу фазової кореляції для субпіксельного відстеження мікрорухів. Ця точність є достатньою для більшості завдань комп'ютерної взаємодії, таких як вибір значків, навігація в меню та малювання. Високий відсоток успішного вибору цілі в тесті «Point-and-Click» (близько 95 %) практично доводить придатність системи для реалізації інтерфейсу «погляд-миша». Низьке навантаження на CPU та стабільна частота кадрів на Raspberry Pi підтверджують ефективність застосованих оптимізацій та можливість використання системи в автономних носимих пристроях.

Важливо підкреслити, що отримані показники FAR та FRR є критичними не лише для оцінки якості розпізнавання, але й для гарантування безпеки авторизації. Низький рівень FAR (0,073 %) безпосередньо зменшує ризик надання прав доступу зловмиснику, тоді як мінімізація FRR (0,12 %) забезпечує комфортний та безперешкодний доступ для легітимних користувачів, що є ключовою вимогою до будь-якої системи контролю доступу.

4.5.2 Аналіз впливу зовнішніх та внутрішніх факторів на точність

Результати виявили чутливість системи до певних факторів, що визначає напрями для майбутнього вдосконалення:

– рівень освітлення: Як видно з рис. 4.3, точність ідентифікації суттєво залежить від умов освітлення. Падіння точності при низькій освітленості (< 50 люкс) є очікуваним для методів, заснованих на звичайній RGB-камері, і підкреслює критичну важливість інтегрованого NIR-підсвічування для забезпечення стабільності в будь-яких умовах;

– індивідуальні фізіологічні особливості: Хоча загальна точність висока, FRR (ймовірність помилкової відмови) може бути вищою для окремих користувачів з дуже світлою склерою або менш вираженою капілярною сіткою. Це вказує на потенціал для персоналізації порогів прийняття рішення або адаптації параметрів контрастування (CLAHE) під час реєстрації користувача;

– артефакти руху: Різкі рухи головою призводять до тимчасової втрати трекінгу. Хоча гіроскоп (MPU-6050) частково компенсує це, для повного вирішення проблеми потрібні більш складні алгоритми стабілізації зображення на основі оцінки глобального руху.

4.5.3 Порівняння з існуючими рішеннями та обґрунтування новизни

Запропонована робота не ізолює новий біометричний параметр, а пропонує новаторський спосіб його комплексного використання.

Відмінність від інших методів судинної біометрії: На відміну від методів, що використовують сканування вен пальця або долоні, запропонований метод є

повністю безконтактним і пасивним. У порівнянні з методами аналізу судин сітківки, наш підхід не вимагає спеціального дорогого інфрачервоного обладнання з довгофокусною оптикою та не створює дискомфорту від яскравого світла, спрямованого в око.

Відмінність від систем відстеження погляду: На відміну від класичних систем, що відстежують центр зіниці або відблиски Пуркіньє (наприклад, ExCuSe), наша система не вимагає калібрування під конкретного користувача, оскільки базується на кореляції унікальної текстури, а не на абсолютній геометрії. Це підвищує зручність і знижує час підготовки до роботи.

Таким чином, наукова новизна полягає в розробці інтегрованої апаратно-програмної платформи, яка вперше використовує один і той же датчик (камеру) та один і той же біометричний параметр (капілярну сітку кон'юнктиви) для послідовного вирішення задач надійної ідентифікації (з перевіркою, чи є користувач живою людиною) та наступної за нею авторизації а також високоточного інтерактивного керування.

4.5.4 Практична значимість та потенційні сфери застосування

Розроблена система забезпечує повний цикл управління доступом: від первинної автентифікації на основі унікальних фізіологічних характеристик до фінальної авторизації з розмежуванням прав користувачів.

Результати роботи мають значний прикладний потенціал:

– медицина та реабілітація: Система може стати ядром інтерфейсу «мозок-комп'ютер» (англ. Brain Computer Interface, BCI) для пацієнтів з тяжкими руховими порушеннями (БАС, травми спинного мозку), забезпечуючи їм засіб для спілкування та контролю довкілля. Моніторинг динаміки капілярів також може мати діагностичну цінність;

– кібербезпека та фінанси: Метод може бути впроваджений для двофакторної аутентифікації в критично важливих системах (банкінг, держсектор), де необхідна підвищена стійкість до атак спуфінгу;

– індустріальні та спеціалізовані інтерфейси: Технологія може

використовуватись в умовах, де руки оператора зайняті (хірургія, складання мікроелектроніки, управління роботами) або в середовищах, що вимагають підвищеної гігієни (чисті кімнати, харчова промисловість).

4.5.5 Обмеження дослідження та напрями майбутніх робіт

Поточна робота має певні обмеження, що задають чіткі напрями для подальших досліджень:

– обмежений розмір вибірки: БД з 150 зразків від 30 осіб є достатньою для підтвердження концепції, але для статистично надійних висновків щодо універсальності методу в різних етнічних та вікових групах необхідна масштабна збірка даних;

– чутливість до умов зйомки: Потрібна подальша робота над адаптивними алгоритмами, що компенсують зміни освітлення та неідеальне позиціонування пристрою;

– апаратна оптимізація: Для справді носимого формату необхідно переходити до більш компактних та енергоефективних компонентів (камера з меншими габаритами, система живлення на одному акумуляторі);

– інтеграція з ОС та застосунками: Майбутня робота має включати розробку універсального драйвера та API для легкої інтеграції системи в існуючі операційні системи та програмні комплекси.

Основні напрями майбутніх досліджень:

– розробка мультимодальної системи, що поєднує аналіз капілярів з відстеженням позиції зіниці для підвищення надійності;

– дослідження можливості використання довгострокових змін у капілярному шаблоні для виявлення загальних захворювань;

– впровадження алгоритмів глибокого навчання для прямої класифікації користувача на «сирому» відеопотоці, що дозволить ще більше знизити затримку.

Висновки до розділу 4

Експериментальні дослідження, проведені в четвертому розділі, підтвердили високу ефективність та практичну придатність розробленої системи біометричної ідентифікації на основі аналізу капілярної мережі кон'юнктиви ока.

Основні результати експериментальних досліджень:

1) досягнуто високої точності ідентифікації – 84,8 % – при стандартному освітленні (≥ 200 люкс), що підтверджує коректність роботи алгоритмів обробки зображень та виділення ознак;

2) встановлено залежність точності від умов освітлення – зниження точності до 63,2 % при 45 люкс обґрунтовує необхідність використання NIR-підсвітки для роботи в умовах недостатньої освітленості;

3) забезпечено роботу в режимі реального часу – середній час обробки одного кадру становить 0,32 секунди, що відповідає вимогам до сучасних біометричних систем;

4) продемонстровано високу стійкість до спуфінг-атак – метод PTT забезпечив виявлення «живості» з EER 0,01 %, що робить систему стійкою до використання фотографій та 3D-моделей;

5) показано конкурентні переваги порівняно з традиційними методами біометричної ідентифікації, зокрема нижчі показники FAR (0,073 %) та FRR (0,12 %) при прийнятному часі аутентифікації.

Обмеження та перспективи:

Основним обмеженням системи є зниження точності в умовах недостатнього освітлення. Тому подальші дослідження можуть бути спрямовані на вдосконалення системи підсвітки, оптимізацію алгоритмів для роботи в складних умовах та розробку мультимодальної системи ідентифікації.

Отримані результати підтверджують, що запропонований метод є перспективним для використання у високозахищених системах аутентифікації та може служити основою для подальших досліджень у галузі безконтактної біометрики.

ВИСНОВКИ

У дисертаційній роботі теоретично обґрунтовано та експериментально підтверджено ефективність запропонованого методу безконтактної біометричної ідентифікації на основі аналізу капілярної мережі кон'юнктиви ока. Основні наукові та практичні результати роботи полягають у наступному:

1) розроблено концептуально новий підхід до безконтактної біометричної ідентифікації, який поєднує аналіз статичних характеристик капілярної мережі з динамічними параметрами кровотоку, що значно підвищує надійність системи у порівнянні з традиційними методами;

2) створено повноцінний апаратно-програмний комплекс на базі широкодоступних компонентів (Raspberry Pi, HQ Camera), що реалізує повний цикл отримання та обробки зображень з середнім часом обробки 0,32 секунди на кадр;

3) розроблено оригінальний алгоритмічний конвеєр обробки зображень, що включає етапи попередньої обробки, виділення ознак, класифікації на основі сіамських нейронних мереж та перевірки на «живість» з використанням імпульсно-транзитної характеристики;

4) експериментально підтверджено високу ефективність системи:

- точність ідентифікації: 84,8 % при стандартному освітленні;
- стійкість до спуфінг-атак: EER 0,01 %;
- показники помилок: FAR 0,073 %, FRR 0,12 %;

5) визначено перспективні напрями практичного застосування розробки у сферах високозахищених систем авторизації, медичного моніторингу та інтерфейсів для людей з обмеженими можливостями.

Отримані результати свідчать про те, що запропонований метод має значні переваги перед традиційними біометричними системами, зокрема: високу стійкість до спуфінг-атак, зручність безконтактного використання, відповідність сучасним гігієнічним вимогам та можливість використання в реальному часі.

Перспективи подальших досліджень полягають у мініатюризації апаратної

частини, оптимізації роботи в умовах низької освітленості, розширенні функціоналу моніторингу медичних даних та інтеграції з сучасними технологіями ШІ для підвищення точності розпізнавання.

Результати роботи відкривають нові напрями у розвитку сучасних систем біометричної ідентифікації та мають значний потенціал для впровадження в різних галузях, де виникає потреба у надійному та безконтактному розпізнаванні особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chugh, Tarang & Cao, Kai & Jain, Anil. (2018). Fingerprint Spoof Buster: Use of Minutiae-Centered Patches. IEEE Transactions on Information Forensics and Security. 1–1. DOI: 10.1109/TIFS.2018.2812193.

2. Медвінський С. В., Журавська І. М. Методи та алгоритми обробки зображень для біометричної ідентифікації за капілярною мережею кон'юнктиви ока. *Наука і техніка сьогодні.* 2026. Вип. 2 (56). С. 2028–2038. DOI: 10.52058/2786-6025-2026-2(56)-2028-2038. ISSN 2786-6025.

3. Medvinskyi S. The use of cross-correlation as an interaction tool for computer systems by individuals with musculoskeletal disorders. *Infocommunication and Computer Technologies.* 2025. № 2 (10). С. 98–104. DOI: 10.36994/2788-5518-2025-02-10-12. ISSN 2788-5518.

4. Medvinskyi S., Zhuravska I. Development of a method for processing eye images for use during biometric authorization in computer systems. *Electrotechnic and Computer Systems.* 2025. № 44 (120). С. 49–54. DOI: 10.15276/eltecs.44.120.2025.6. ISSN 2221-3805.

5. Медвінський С. Авторизація користувача у комп’ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2023. Вип. 50. С. 71−77. DOI: 10.36910/6775-2524-0560-2023-50-10. ISSN 2524-0552.

6. Медвінський С. Аналіз методів відслідковування напрямку погляду під час використання комп’ютерних систем. *Ольвійський форум – 2024 : стратегії країн Причорноморського регіону в геополітичному просторі* : зб. тез XXI Міжнар. наук. конф. 20–23 червня 2024 р., м. Миколаїв : тези / М-во освіти і науки України. Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 178–183.

7. Журавська І., Медвінський С. Динамічні біометричні показники ока для авторизації користувача в комп’ютерній системі. *Медико-технічна співпраця заради перемоги: актуальні завдання медичної, біологічної фізики та інформатики :* тези доп. III Наук.-практ. конф. з міжнар. участю, м. Вінниця, 07

квітня 2024 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2024. С. 53–56. URL: https://dspace.vnmu.edu.ua/handle/123456789/6560.

8. Журавська І., Медвінський С. Авторизація користувача в комп'ютерній системі за допомогою малюнку капілярів хоріоідеї. *Актуальні завдання медичної, біологічної фізики та інформатики* : тези доп. II Всеукр. наук.-практ. конф. з міжнар. участю, Вінниця, 07 квітня 2023 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2023. С. 15–17.

9. Медвінський С. В., Журавська І. М. Програмне забезпечення для авторизації користувача у комп'ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Free and Open Source Software (FOSS-2023)* : тези доп. XIV Міжнар. наук.-практ. конф., Харків, 07–10 лютого 2023 р. Харків : ХНЕУ ім. Семена Кузнеця, 2023. С. 101–102.

10. Медвінський С. Використання динамічних біометричних показників для авторизації користувачів. *Могилянські читання – 2022* : тези доп. XXV Всеукр. наук.-практ. конф., Миколаїв, 07–11 листопада 2022 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2022. С. 73–75.

11. Журавська І. М., Медвінський С. В., Ухань Є. О. Упровадження EAP-TLS сертифікатів у Mikrotik з аутентифікацією користувачів за динамічними біометричними параметрами. *Могилянські читання – 2021* : тези доп. XXIV Всеукр. наук.-метод. конф., Миколаїв, 8–12 листоп. 2021 р., Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2021. С. 55–58.

12. Prakash, Chandra & De La Cruz, Elyson. (2026). The unseen impact: A critical investigation of healthcare cybersecurity breaches using HHS data. DOI: 10.1109/CARS67163.2025.11337866.

13. Joshi, Daxeshkumar. (2025). Emerging issues of cyber crimes in India: Statistics, modus operandi of online frauds and remedies to curb cyber crimes. International Journal of Science and Research Archive. 17. 408–418. DOI: 10.30574/ijsra.2025.17.1.2799.

14. Grace, Joan. (2023). Impact of cybersecurity measures on financial data breaches. International Journal of Modern Risk Management. 1. 35–44. DOI:

10.47604/ijmrm.2097.

15. Manikandan, S. & Minu, M S & Ramesh, Subashka & Sivasankari, K. & Saranya, S. & Singh, Sonia. (2025). Implementing cybersecurity policies to minimize the impacts of deepfakes on universities. DOI: 10.4018/979-8-3373-3770-8.ch016.

16. Suleiman, Nkiru. (2025). Deepfake-as-a-Service: The Next Challenge for Enterprise Cybersecurity. Journal of Technology and Systems. 7. 47–59. DOI: 10.47941/jts.2752.

17. Mamatha.P,. (2025). Password Vulnerability assessment: a safe checker using online breach data. international journal of engineering technology and management sciences. 9. DOI: 10.46647/ijetms.2025.v09si01.021.

18. Medlin, B. (2015). Social engineering techniques and password security. International Journal of Cyber Warfare and Terrorism. 3. 58–70. DOI: 10.4018/ijcwt.2013040104.

19. Stylios, Ioannis. (2023). Behavioral biometrics for continuous authentication. Security and Privacy. DOI: 10.12681/eadd/53367.

20. G, Satheesh & B, Monisha & F, Angel & N, Sushma & S, Hamsa & Farheen, Sheeba. (2025). Behavioral Biometrics in IOT: Accuracy in Identity Human Verification Using AI. International Research Journal on Advanced Engineering and Management (IRJAEM). 3. 2626–2628. DOI: 10.47392/IRJAEM.2025.0413.

21. Chi-Wei Lien and Sudip Vhaduri. (2023). Challenges and opportunities of biometric user authentication in the Age of IoT: A Survey. ACM Comput. Surv. 56, 1, Article 14 (January 2024), 37 p. DOI: 10.1145/3603705.

22. Wuyi, Ming & Jia, Haojie & Huang, Heyuan & Zhang, Guojun & Liu, Kun & Lu, Ya & Cao, Chen. (2021). Study on mechanism of glass molding process for fingerprint lock glass plates. Crystals. 11. 394. DOI: 10.3390/cryst11040394.

23. Tabei, Junichi & Sasajima, Hideaki & Mori, Takeshi. (2016). Epoxy molding compound for fingerprint sensor. 553–556. DOI: 10.1109/ICEP.2016.7486888.

24. Singh, Shilpi & Prasad, S.V.A.V. (2018). Techniques and challenges of face recognition: A critical review. Procedia Computer Science. 143. 536–543. DOI: 10.1016/j.procs.2018.10.427.

25. Xia Y, Liang J, Li Q, Xin P, Zhang N. High-accuracy 3D gaze estimation with efficient recalibration for head-mounted gaze tracking systems. Sensors (Basel). 2022 Jun 8;22(12):4357. DOI: 10.3390/s22124357. PMID: 35746135; PMCID: PMC9231356.

26. Czajka, Adam & Bowyer, Kevin & Krumdick, Michael & Vidal Mata, Rosaura. (2017). Recognition of image-orientation-based iris spoofing. IEEE Transactions on Information Forensics and Security. 1–1. DOI: 10.1109/TIFS.2017.2701332.

27. Finnegan OL, White JW 3rd, Armstrong B, Adams EL, Burkart S, Beets MW, Nelakuditi S, Willis EA, von Klinggraeff L, Parker H, Bastyr M, Zhu X, Zhong Z, Weaver RG. The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review. Syst Rev. 2024 Feb 8;13(1):61. DOI: 10.1186/s13643-024-02451-1. PMID: 38331893; PMCID: PMC10851515.

28. Al-Khafaji, Ruaa & Al-Tamimi, Mohammed. (2022). Vein biometric recognition methods and systems. A review. Advances in Science and Technology – Research Journal. 16. 36–46. DOI: 10.12913/22998624/144495.

29. Kauba C, Prommegger B, Uhl A. Combined fully contactless finger and hand vein capturing device with a corresponding dataset. Sensors (Basel). 2019 Nov 17;19(22):5014. DOI: 10.3390/s19225014. PMID: 31744197; PMCID: PMC6891606.

30. Min Htet, Aung Si & Lee, Hyo Jong. (2023). Contactless palm vein recognition based on attention-gated residual U-Net and ECA-ResNet. Applied Sciences. 13. 6363. DOI: 10.3390/app13116363.

31. B. Hou, H. Zhang and R. Yan, "Finger-Vein Biometric Recognition: A Review," in IEEE Transactions on Instrumentation and Measurement. 71. 1–26, 2022, Art no. 5020426. DOI: 10.1109/TIM.2022.3200087.

32. Iovino C, Peiretti E, Braghiroli M, Tatti F, Aloney A, Lanza M, Chhablani J. Imaging of iris vasculature: current limitations and future perspective. Eye (Lond). 2022 May;36(5):930-940. DOI: 10.1038/s41433-021-01809-2. Epub 2021 Oct. 14. PMID: 34650219; PMCID: PMC9046297.

33. Llorens-Quintana C, Kuran U, Kuran EC, Madrid-Costa D. Enhancing

conjunctival vasculature imaging: A multi-objective cuckoo search approach for contrast enhancement optimization. Transl Vis Sci Technol. 2025 Sep. 2;14(9):36. DOI: 10.1167/tvst.14.9.36. PMID: 41002106; PMCID: PMC12489868.

34. Duan, Xuran & Lei, Chaoyu & Lim, Chris & Jianbin, Ding & Mehta, Jodhbir & Basu, Sayan & Johnston, Luke & Ren, Yujie & Zhao, Chen & Chang, Victor & Zhou, Huifang. (2025). Quantitative analysis of conjunctival vascular alterations: Applications in ocular and systemic disease detection. Progress in Retinal and Eye Research. 110. 101416. DOI: 10.1016/j.preteyeres.2025.101416.

35. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. Inventions, 6(4), 65. DOI: 10.3390/inventions6040065

36. Lee KF, Chen YL, Yu CW, Chin KY, Wu CH. Gaze tracking and point estimation using low-cost head-mounted devices. Sensors (Basel). 2020 Mar 30;20(7):1917. DOI: 10.3390/s20071917. PMID: 32235523; PMCID: PMC7181118.

37. Llorens-Quintana C, Kuran U, Kuran EC, Madrid-Costa D. Enhancing conjunctival vasculature imaging: A multi-objective cuckoo search approach for contrast enhancement optimization. Transl Vis Sci Technol. 2025 Sep 2;14(9):36. DOI: 10.1167/tvst.14.9.36. PMID: 41002106; PMCID: PMC12489868.

38. Das, Sumanta & Ghosh, Ishita & Chttopadhyay, Abir. (2021). An efficient deep sclera recognition framework with novel sclera segmentation, vessel extraction and gaze detection. Signal Processing: Image Communication. 97. 116349. DOI: 10.1016/j.image.2021.116349.

39. Wang, Li & Wang, Changyuan & Zhang, Yu & Gao, Lina. (2023). An integrated neural network model for eye-tracking during human-computer interaction. Mathematical Biosciences and Engineering. 20. 13974-13988. DOI: 10.3934/mbe.2023622.

40. Xiao F, Zheng D, Huang K, Qiu Y, Shen H. A single-camera gaze tracking system under natural light. J Eye Mov Res. 2018 Oct 20;11(4):10.16910/jemr.11.4.5. DOI: 10.16910/jemr.11.4.5. PMID: 33828707; PMCID: PMC7904270.

41. Wang, Chun & Jan, Steve & Hu, Hang & Wang, Gang. (2017). Empirical

analysis of password reuse and modification across online service. DOI: 10.48550/arXiv.1706.01939.

42. Amazu, Chidera & Mcgrory, John & Leva, Maria & Baldissone, Gabriele & Fissore, Davide & Demichela, Micaela. (2024). Human factors in alarm response procedures: an empirical analysis of paper versus digital support. DOI: 10.54941/ahfe1005469.

43. Patel, Vishal & Ratha, Nalini & Chellappa, Rama. (2015). Cancelable biometrics: A review. Signal Processing Magazine, IEEE. 32. 54–65. DOI: 10.1109/MSP.2015.2434151.

44. Rawat, Manisha & Kumar, Nitin. (2020). Cancelable biometrics: a comprehensive survey. Artificial Intelligence Review. 53. DOI: 10.1007/s10462-019-09767-8.

45. Teh PS, Teoh AB, Yue S. A survey of keystroke dynamics biometrics. Scientific World Journal. 2013 Nov 3;2013:408280. DOI: 10.1155/2013/408280. PMID: 24298216; PMCID: PMC3835878.

46. Altwaijry, Najwa. (2023). Authentication by Keystroke Dynamics: The influence of typing language. Applied Sciences. 13. 11478. DOI: 10.3390/app132011478.

47. Ionescu, Bogdan & Boato, G. & Ma, Zhigang & Kompatsiaris, Ioannis & Sebe, Nicu & Yan, Shuicheng. (2016). Special issue on event-based media processing and analysis. Image and Vision Computing. 53. 1–2. DOI: 10.1016/j.imavis.2016.08.008.

48. Siddiqui, Nyle & Dave, Rushit & Vanamala, Mounika & Seliya, Naeem. (2022). Machine and deep learning applications to mouse dynamics for continuous user authentication. Machine Learning and Knowledge Extraction. 4. 502–518. DOI: 10.3390/make4020023.

49. Wang, Xiujuan & Shi, Yutong & Zheng, Kangfeng & Zhang, Yuyang & Hong, Weijie & Cao, Siwei. (2022). User authentication method based on keystroke dynamics and mouse dynamics with scene-irrelated features in hybrid scenes. Sensors. 22. 6627. DOI: 10.3390/s22176627.

50. Bondarenko, Maksym & Ivashchenko, Heorhii. (2025). Використання послідовності методів попередньої обробки в системах голосової ідентифікації. Системи управління, навігації та зв'язку. Збірник наукових праць. 2. 90–96. DOI: 10.26906/SUNZ.2025.2.090.

51. Greco, Danilo & Fasihiany, Majid & Ranjbar, Ali & Masulli, Francesco & Rovetta, Stefano & Cabri, Alberto. (2024). Computer vision algorithms on a Raspberry Pi 4 for automated depalletizing. Algorithms. 17. 1–15. DOI: 10.3390/a17080363.

52. Kosareva, Anastasiia & Rehida, Pavlo. (2021). Засіб для біометричної автентифікації на основі поведінкових особливостей користувача. Technical Sciences and Technologies. 114–122. DOI: 10.25140/2411-5363-2021-2(24)-114-122.

53. Sokyrka, Ievgenii & Kukulevskyi, Ivan & Tolbatov, Andrii. (2025). Authentication methods using behavioral analytics and machine learning for Internet of Things devices. Cybersecurity: Education, Science, Technique. 2. 35–49. DOI: 10.28925/2663-4023.2025.30.941.

54. Sayed, B., Traoré, I., Woungang, I., & Obaidat, M.S. (2013). Biometric Authentication Using Mouse Gesture Dynamics. IEEE Systems Journal, 7, 262–274.

55. Gao, Yang & Lian, Jiachen & Raj, Bhiksha & Singh, Rita. (2020). Detection and Evaluation of human and machine generated speech in spoofing attacks on automatic speaker verification systems. DOI: 10.48550/arXiv.2011.03689.

56. Abba, Suleiman & Olaniyi, Oluwadayo. (2026). Adaptive Cognitive Profiling for Executive AI Agents Amid Emerging AI Impersonation Threats. Journal of Engineering Research and Reports. 28. 388–405. DOI: 10.9734/jerr/2026/v28i11784.

57. Puipati, Kiran. (2026). Biometric and Behavioral Authentication in IAM: Security, Privacy, and Continuous Verification Trade-offs. Frontiers in Emerging Computer Science and Information Technology. 03. 01–14. DOI: 10.64917/fecsit/Volume03Issue01-01.

58. Hussain, Shafiq. (2025). Behavioral Biometrics and Continuous Authentication in Cybersecurity Systems. DOI: 10.13140/RG.2.2.35971.41763.

59. Kumar, M. & Patel, Subhash & Itmazi, Jamil & Sherideh, Ala'a. (2026). Beyond Password's: Context Aware Behavioral Biometrics for Continuous

Authentication. DOI: 10.1007/978-3-031-87584-7_115.

60. Souza, Juliana & Cielo, Carla & Gonçalves, Bruna & Oliveira, Élisson & Lana, Aloma & Pasqualoto, Adriane. (2025). Post-COVID-19 Dysphonia: Risk, Voice Handicap, and Laryngological Findings in COVID-19 Critical Illness Survivors. International Archives of Otorhinolaryngology. 29. 001–011. DOI: 10.1055/s-0045-1810026.

61. Amini, Mohammad & Yousefi, Jaleh & Hasanalifard, Mahdieh & Bagherihagh, Ali. (2025). Voice Disorders in Patients With COVID-19 During Illness and After Recovery. Infectious Diseases in Clinical Practice. 34. DOI: 10.1097/IPC.0000000000001529.

62. Lombardo, Clara & Esposito, Giulia & Carbone, Silvia & Serrano, Salvatore & Mento, Carmela. (2025). Speech analysis and speech emotion recognition in mental disease: a scoping review. Frontiers in Psychology. 16. DOI: 10.3389/fpsyg.2025.1645860.

63. D.S., Dinesh & Rao, P.V.. (2019). Implementing and analysing FAR and FRR for face and voice recognition (multimodal) using KNN classifier. International Journal of Intelligent Unmanned Systems. ahead-of-print. DOI: 10.1108/IJIUS-02-2019-0015.

64. Otenyi, Stephen & Ngoo, Livingstone & Kiragu, Henry. (2024). Speaker Recognition System Using Hybrid of MFCC and RCNN with HCO Algorithm Optimization. International Journal of Intelligent Information Systems. 13. 94–108. DOI: 10.11648/j.ijiis.20241305.11.

65. Liu, Yingnan & Ma, Qitao & Wang, Yingli. (2020). Speech Synthesis Method Based on Tacotron + WaveNet. DOI: 10.1007/978-981-13-9409-6_78.

66. Dorca Josa, Aleix & Pérez, Eugènia & Moran Moreno, Jose. (2017). Using Keystroke Dynamics and context features to assess authorship in online learning environments. DOI: 10.21125/inted.2017.0819.

67. Shadman, Rashik & Wahab, Ahmed & Manno, Michael & Lukaszewski, Matthew & Hou, Daqing & Hussain, Faraz. (2025). Keystroke Dynamics: Concepts, Techniques, and Applications. ACM Computing Surveys. 57. DOI: 10.1145/3733103.

68. Kumar, K. & Arun, A.. (2025). Keystroke Dynamics Based User Authentication System. Recent Trends in Artificial Intelligence & Its Applications. 4. 70–82. DOI: 10.46610/RTAIA.2025.v04i02.009.

69. Wang X, Shi Y, Zheng K, Zhang Y, Hong W, Cao S. User Authentication Method Based on Keystroke Dynamics and Mouse Dynamics with Scene-Irrelated Features in Hybrid Scenes. Sensors (Basel). 2022 Sep 1;22(17):6627. DOI: 10.3390/s22176627. PMID: 36081085; PMCID: PMC9460698.

70. Filho, Sergio & Roisenberg, Mauro. (2006). Continuous Authentication by Keystroke Dynamics Using Committee Machines. 686–687. DOI: 10.1007/11760146_90.

71. Stylios, Ioannis & Kokolakis, Spyros & Thanou, Olga & Chatzis, Sotirios. (2021). Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey. Information Fusion. 66. 76–99. DOI: 10.1016/j.inffus.2020.08.021.

72. Anwar, Nazirah & Syed Ahmad, Sharifah Sakinah & Kausar, Nasreen & Stević, Željko & Gaba, Yaé Ulrich. (2025). Multiple biometric authentication for online banking system based on multiple fuzzy approach. Scientific Reports. 15. 1–20. DOI: 10.1038/s41598-025-13571-6.

73. Teh PS, Teoh AB, Yue S. A survey of keystroke dynamics biometrics. ScientificWorldJournal. 2013 Nov 3;2013:408280. DOI: 10.1155/2013/408280. PMID: 24298216; PMCID: PMC3835878.

74. Lopez, Christian & Solano, Jesús & Rivera, Esteban & Tengana Hurtado, Lizzy & Florez-Lozano, Johana & Castelblanco, Alejandra & Ochoa, Martín. (2023). Adversarial attacks against mouse- and keyboard-based biometric authentication: black-box versus domain-specific techniques. International Journal of Information Security. 22. 1-21. DOI: 10.1007/s10207-023-00711-0.

75. Taleghani, Mohammad & Hesari, Fatemeh. (2025). Presenting an Operational Model for Adaptive Biometric Authentication with multi-feature Combination. Open Access Journal of Artificial Intelligence and Technology. 1-5. DOI: 10.61440/OAJAIT.2025.v1.16.

76. Shadman, Rashik & Wahab, Ahmed & Manno, Michael & Lukaszewski,

Matthew & Hou, Daqing & Hussain, Faraz. (2025). Keystroke Dynamics: Concepts, Techniques, and Applications. ACM Computing Surveys. 57. DOI: 10.1145/3733103.

77. González, Nahuel & Calot, Enrique & Ierache, Jorge & Hasperué, Waldo. (2022). Towards liveness detection in keystroke dynamics: Revealing synthetic forgeries. Systems and Soft Computing. 4. 200037. DOI: 10.1016/j.sasc.2022.200037.

78. Siahaan, Chrisando & Chowanda, Andry. (2022). Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen-recorded video. Journal of Big Data. 9. DOI: 10.1186/s40537-022-00662-8.

79. Sokyrka, Ievgenii & Kukulevskyi, Ivan & Tolbatov, Andrii. (2025). Authentication methods using behavioral analytics and machine learning for Internet of Things devices. Cybersecurity: Education, Science, Technique. 2. 35–49. DOI: 10.28925/2663-4023.2025.30.941.

80. Yu, Rongyu & Kizilkaya, Burak & Meng, Zhen & Li, Emma & Zhao, Philip. (2025). Robot Adversarial Attack on Keystroke Dynamics Based User Authentication System. IEEE Robotics and Automation Letters. 1–8. DOI: 10.1109/LRA.2025.3550727.

81. Tan, Yi Xiang Marcus & Iacovazzi, Alfonso & Homoliak, Ivan & Elovici, Yuval & Binder, Alexander. (2019). Adversarial Attacks on Remote User Authentication Using Behavioural Mouse Dynamics. DOI: 10.48550/arXiv.1905.11831.

82. Borah, Kaushik. (2025). Adaptive Authentication for Enterprise Cloud Systems using Behavioral Biometrics. Journal of Information Systems Engineering and Management. 10. 233–243. DOI: 10.52783/jisem.v10i60s.13085.

83. Subash, Aditya & Song, Insu & Lee, Ickjai & Lee, Kyungmi. (2025). Integrating user demographic parameters for mouse behavioral biometric-based assessment fraud detection in online education platforms. EURASIP Journal on Information Security. 2025. DOI: 10.1186/s13635-025-00207-5.

84. Ogunmolu, Akinde. (2025). Leveraging Generative AI and Behavioral Biometrics to Strengthen Zero Trust Cybersecurity Architectures in Healthcare Systems. Journal of Engineering Research and Reports. 27. 194–213. DOI:

10.9734/jerr/2025/v27i51502.

85. Xaba, Samukelisiwe & Aworinde, Halleluyah & van Niekerk, Brett. (2025). A systematic literature review on integrating contactless biometrics into online learning environments. Edelweiss Applied Science and Technology. 9. 172–194. 10.55214/2576-8484.v9i9.9781.

86. Li, Jiajia & Yi, Qian & Lim, Ming K & Yi, Shuping & Zhu, Pengxing & Huang, Xingjun. (2024). MBBFAuth: Multimodal Behavioral Biometrics Fusion for Continuous Authentication on Non-Portable Devices. IEEE Transactions on Information Forensics and Security. PP. 1–1. DOI: 10.1109/TIFS.2024.3480363.

87. Stylios, Ioannis & Thanou, Olga & Androulidakis, Iosif & Zaitseva, Elena. (2016). A Review of Continuous Authentication Using Behavioral Biometrics. DOI: 10.1145/2984393.2984403.

88. Chandre, Pankaj & Joshi, Suvarna & Shendkar, Bhagyashree & Nikam, Yuvraj & Rathod, Rahul & Nandimath, Jyoti. (2025). Beyond Passwords: Enhancing Security with Continuous Behavioral Biometrics and Passive Authentication. DOI: 10.1007/978-3-031-90723-4_11.

89. Azmat, Hadia. (2025). Behavioral Biometrics and Continuous Authentication as a Foundation for Post-Password Cybersecurity. DOI: 10.13140/RG.2.2.25234.11206.

90. Bricelj A, Steinebach C, Kuchta R, Gütschow M, Sosič I. E3 Ligase Ligands in Successful PROTACs: An Overview of Syntheses and Linker Attachment Points. Front Chem. 2021 Jul 5;9:707317. DOI: 10.3389/fchem.2021.707317. PMID: 34291038; PMCID: PMC8287636.

91. Taylor, M. , Hicklin, A. and Kiebuzinski, G. (2021), Best practices in the collection and use of biometric and forensic datasets, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], DOI: 10.6028/NIST.IR.8361,

92. Kumari, Rani & Ramachandran, Prakash. (2023). A Review on Early Diagnosis of Parkinson's Disease Using Speech Signal Parameters Based on Machine Learning Technique. DOI: 10.1007/978-981-19-8338-2_18.

93. Magalhaes DR, Çakmakçı C, Campo MDM, Çakmakçı Y, Makishi F, Silva VLDS, Trindade MA. Changes in the Current Patterns of Beef Consumption and Consumer Behavior Trends-Cross-Cultural Study Brazil-Spain-Turkey. Foods. 2023 Jan. 19; 12(3):475. DOI: 10.3390/foods12030475. PMID: 36766003; PMCID: PMC9914451.

94. Hou, Borui & Zhang, Huijie & Yan, Ruqiang. (2022). Finger-Vein Biometric Recognition: A Review. IEEE Transactions on Instrumentation and Measurement. PP. 1–1. DOI: 10.1109/TIM.2022.3200087.

95. Zhang, Lingling & Liu, Jun & Luo, Minnan & Chang, Xiaojun & Zheng, Qinghua. (2019). Scheduled Sampling for One-Shot Learning via Matching Network. Pattern Recognition. 96. DOI: 10.1016/j.patcog.2019.07.007.

96. Rayar, Frederic & Uchida, Seiichi. (2018). On Fast Sample Preselection for Speeding up Convolutional Neural Network Training: Joint IAPR International Workshop, S+SSPR 2018, Beijing, China, August 17–19, 2018, Proceedings. DOI: 10.1007/978-3-319-97785-0_7.

97. Alzami, Farrikh & Naufal, Muhammad & Basuki, Ruri & Winarno, Sri & Al Azies, Harun & Lutfi, Syaheerah & Brilianto, Rivaldo. (2025). Bayesian-Optimized CLAHE for Enhanced Drowsiness Detection in Low-Light Conditions Using Time-Distributed MobileNetV2-GRU Architecture. Statistics, Optimization & Information Computing. 15. 274–294. DOI: 10.19139/soic-2310-5070-3024.

98. rajee, R & Roomi, S. (2025). Channel-Selective Retinal Image Enhancement in Lab Color Space UsingICF-Guided Rank-Preserving CLAHE. DOI: 10.21203/rs.3.rs-7603142/v1.

99. Venkatachalam, Shanmugavalli & Venkatachalam, Chandrasekar & Shah, Priyanka. (2025). Tuberculosis Detection in Chest X-rays Using Vision Transformers with Convolutional Stems and CLAHE-Based Contrast Enhancement. Biomedical Materials & Devices. DOI: 10.1007/s44174-025-00567-z.

100. Rot, Peter & Peer, Peter & Štruc, Vitomir & Emeršič, Žiga & Grm, Klemen & Vitek, Matej. (2020). Deep Sclera Segmentation and Recognition. DOI: 10.1007/978-3-030-27731-4_13.

101. Xu, Dong & Dong, Wei & Zhou, Han. (2020). Sclera Recognition Based on Efficient Sclera Segmentation and Significant Vessel Matching. The Computer Journal. 65. DOI: 10.1093/comjnl/bxaa051.

102. Das, Sumanta & Ghosh, Ishita & Chttopadhyay, Abir. (2021). An efficient deep sclera recognition framework with novel sclera segmentation, vessel extraction and gaze detection. Signal Processing: Image Communication. 97. 116349. DOI: 10.1016/j.image.2021.116349.

103. Wang, Caiyong & Haiqing, Li & Zhang, Yixin & Zhao, Guangzhe & Wang, Yunlong & Sun, Zhenan. (2024). Sclera-TransFuse: Fusing Vision Transformer and CNN for Accurate Sclera Segmentation and Recognition. IEEE Transactions on Biometrics, Behavior, and Identity Science. 1–1. DOI: 10.1109/TBIOM.2024.3415484.

104. Alkassar, Sinan & Woo, Wai Lok & Dlay, Satnam & Chambers, Jonathon. (2016). Sclera Recognition: On The Quality Measure and Segmentation of Degraded Images Captured Under Relaxed Imaging Conditions. IET Biometrics. 6. DOI: 10.1049/iet-bmt.2016.0114.

105. Zhou, Zhi & Du, Yingzi & Thomas, Nathanael & Delp, Edward. (2013). A comprehensive approach for sclera image quality measure. International Journal of Biometrics. 5. 181–198. DOI: 10.1504/IJBM.2013.052972.

106. Kabbani, Wassim & Raja, Kiran & Ramachandra, Raghavendra & Busch, Christoph. (2025). Eye Sclera for Fair Face Image Quality Assessment. DOI: 10.48550/arXiv.2501.07158.

107. Venkatachalam, Gokul. (2013). Enhanced Sclera Recognition on Color Image.

108. G. Radha. (2015). A NEW MULTIMODEL APPROACH FOR HUMAN AUTHENTICATION: SCLERA VEIN AND FINGER VEIN RECOGNITION. International Journal of Research in Engineering and Technology. 04. 93–99. DOI: 10.15623/ijret.2015.0403015.

109. Nathan, Sabari & Uma, K & Sethu, Swarna. (2026). SwinDANet: leveraging swin transformers with Context-Aware Attention for precise sclera segmentation. Signal, Image and Video Processing. 20. DOI: 10.1007/s11760-025-05058-8.

110. Das, Sumanta & Ghosh, Ishita & Chattopadhyay, Abir. (2022). Sclera biometrics in restricted and unrestricted environment with cross dataset evaluation. Displays. 102257. DOI: 10.1016/j.displa.2022.102257.

111. Venkataswamy, Naveenkumar & Liu, Yu & Singh, Surendra & Dey, Soumya & Schuckers, Stephanie & Imtiaz, Masudul. (2024). Smartphone-based Iris Recognition through High-Quality Visible Spectrum Iris Capture. DOI: 10.48550/arXiv.2412.13063.

112. Venkataswamy, Naveenkumar & Liu, Yu & Dey, Soumya & Schuckers, Stephanie & Imtiaz, Masudul. (2025). Smartphone-based iris recognition through high-quality visible-spectrum iris image capture.V2. DOI: 10.48550/arXiv.2510.06170.

113. Raja, Kiran & Ramachandra, Raghavendra & Busch, Christoph & Mondal, Soumik. (2014). An Empirical Study of Smartphone Based Iris Recognition in Visible Spectrum. ACM International Conference Proceeding Series. 2014. 239–246. DOI: 10.1145/2659651.2659704.

114. ESET Threat Report H1 2025 URL: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h12025.pdf.

115. Mondal, Soumik. (2016). Continuous User Authentication and Identification: Combination of Security & Forensics. DOI: 10.13140/RG.2.1.1152.0882.

ДОДАТОК А

Акти впровадження

А.1 Акт впровадження результатів в НДР

ЗАТВЕРДЖУЮ

Ректор Чорноморського
національного університету
ім. Петра Могили

_____ Леонід КЛИМЕНКО

"29" червня 2022 р.

АКТ
впровадження результатів дисертаційної роботи
Медвінського С. В. на тему «Система ідентифікації користувача комп'ютерної системи за динамічними біометричними параметрами»
при виконанні держбюджетної НДР
«Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» (№ держ. реєстрації 0121U109898; керівник НДР д-р техн. наук, проф. Трунов О. М., термін виконання роботи 01.01.2021–31.12.2022)

Держбюджетна НДР «Розробка модулів автоматизації бездротових приладів відновлення пост-інфарктних, пост-інсультних пацієнтів в індивідуальних умовах віддаленої реабілітації» виконувалась у Чорноморському національному університеті ім. Петра Могили.

При виконанні НДР був використаний розроблений здобувачем Медвінським С. В. метод ідентифікації та визначення напрямку погляду пацієнту за допомогою зображення хоріоідеї для ідентифікації пацієнта перед тим, як дати йому доступ до особистого облікового запису з медичними даними та вправами для виконання вправ для відновлення фізичного стану. Це дозволило забезпечити безпеку та конфіденційність медичних даних пацієнтів. Крім того, розроблено алгоритм роботи модулю авторизації за зображенням капілярів судинної оболонки ока (хоріоідеї) при відстеженні прогресу пацієнта у виконанні вправ та для персоналізації програми відновлення, залежно від його фізичного стану та потреб. Розроблено алгоритм порівняння малюнків капілярів за допомогою використання сіамської нейронної і опізнавання напрямку погляду за допомогою кросс-кореляції.

PhD-студент кафедри комп'ютерної інженерії, фахівець І кат. НДЧ ЧНУ ім. Петра Могили Медвінський С.В., приймав участь у НДР як виконавець.

Керівник НДР,
проф. каф. автоматизації
та комп'ютерно-інтегрованих технологій,
д-р техн. наук, проф. О. М. Трунов

«29» червня 2022 р.

А.2 Акт впровадження результатів в навчальний процес

ЗАТВЕРДЖУЮ

Проректор з наукової роботи та
міжнародного співробітництва
Чорноморського національного
університету ім. Петра Могили, професор
_____ Алла КОВАЛЬ
"3" травня 2021 р.

АКТ
впровадження результатів дисертаційної роботи
Медвінського С. В. на тему: «Система ідентифікації користувача комп'ютерної системи за динамічними біометричними параметрами» в навчальний процес Чорноморського національного університету ім. Петра Могили на кафедрі медико-біологічних основ спорту та фізичної реабілітації

Основні наукові та практичні результати дисертаційної роботи Медвінського С. В. застосовуються у навчальному процесі на кафедрі медико-біологічних основ спорту та фізичної реабілітації ЧНУ ім. Петра Могили в курсі лекційних та практичних занять при викладанні дисципліни «Інформаційні технології та системологія в спорті та фізичній реабілітації» студентам спеціальності 227 Фізична терапія, ерготерапія за другим (магістерським) рівнем вищої освіти.

У процес викладання дисципліни «Інформаційні технології та системологія в спорті та фізичній реабілітації», розробленої викладачем Медвінським С. В., введені такі теми, які містять матеріал роботи здобувача:

- «Використання біометричних показників як інструмента взаємодії з комп'ютерними системами (КС)»;
- «Використання біометричних показників з відстеженням руху очей у спортивних та медичних КС для планування та виконання процедур з реабілітації»;
- «Захист від несанкціонованого доступу або помилок з ідентифікацією клієнта КС».

Лекційні матеріали та методичні матеріали для виконання практичних робіт наведені в модульному об'єктно-орієнтованому динамічному навчальному середовищі Moodle3 ЧНУ ім. Петра Могили та можуть бути використовувані у подальшому освітньому процесі як за дистанційною, так і очною або заочною формою навчання.

Зав. каф. медико-біологічних основ спорту
та фізичної реабілітації,
канд. біол. наук, доцент _____ Сергій ГЕТМАНЦЕВ

Гарант освітньої програми 227,
д-р біол. наук, проф. за кафедрою
радіоелектронних пристроїв _____ Тетяна ЯБЛОНСЬКА

ДОДАТОК Б

Програмний код формування та обробки датасету зовнішніх капілярів ока

```
import cv2
import numpy as np
import matplotlib.pyplot as plt
def display_image(image, title="Image"):
    plt.figure(figsize=(6, 6))
    plt.imshow(cv2.cvtColor(image, cv2.COLOR_BGR2RGB))
    plt.title(title)
    plt.axis('off')
    plt.show()
image = cv2.imread('1.png')
gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
display_image(image, "Original Image")
x, y, w, h = 200, 400, 700, 350
eye_region = gray
plt.figure(figsize=(6, 6))
plt.imshow(eye_region, cmap='gray')
plt.title("Cropped Eye Region (ROI)")
plt.axis('off')
plt.show()
clahe = cv2.createCLAHE(clipLimit=18.0, tileGridSize=(12, 12))
enhanced_gray = clahe.apply(eye_region)
plt.figure(figsize=(6, 6))
plt.imshow(enhanced_gray, cmap='gray')
plt.title("clahe")
plt.axis('off')
plt.show()
blurred = cv2.medianBlur(enhanced_gray, 5)
```

```
plt.figure(figsize=(6, 6))
plt.imshow(blurred, cmap='gray')
plt.title("medianBlur")
plt.axis('off')
plt.show()
_, thresholded = cv2.threshold(blurred, 110, 185,
cv2.AGAST_FEATURE_DETECTOR_THRESHOLD)
plt.figure(figsize=(6, 6))
plt.imshow(thresholded, cmap='gray')
plt.title("thresholded")
plt.axis('off')
plt.show()
edges = cv2.Canny(thresholded, 30, 120)
kernel = cv2.getStructuringElement(cv2.MORPH_RECT, (1, 1))
closed = cv2.morphologyEx(edges, cv2.MORPH_CLOSE, kernel)
plt.figure(figsize=(6, 6))
plt.imshow(closed, cmap='gray')
plt.title("Capillary Detection in Cropped Eye Region")
plt.axis('off')
plt.show()
contours, _ = cv2.findContours(closed, cv2.RETR_EXTERNAL,
cv2.CHAIN_APPROX_SIMPLE)
filtered_contours = []
min_contour_area = 1  # Adjust as needed
max_contour_area = 1200
for contour in contours:
    area = cv2.contourArea(contour)
    if min_contour_area < area < max_contour_area:
        filtered_contours.append(contour)
```

```
capillary_mask = np.zeros_like(eye_region)
cv2.drawContours(capillary_mask, filtered_contours, -1, (255),
thickness=cv2.FILLED)
plt.figure(figsize=(6, 6))
plt.imshow(capillary_mask, cmap='gray')
plt.title("Filtered Capillaries in Eye Region")
plt.axis('off')
plt.show()
skeleton = np.zeros_like(capillary_mask)
element = cv2.getStructuringElement(cv2.MORPH_CROSS, (3, 3))
done = False
while not done:
    eroded = cv2.erode(capillary_mask, element)
    temp = cv2.dilate(eroded, element)
    temp = cv2.subtract(capillary_mask, temp)
    skeleton = cv2.bitwise_or(skeleton, temp)
    capillary_mask = eroded.copy()
    done = cv2.countNonZero(capillary_mask) == 0
```

ДОДАТОК В

Список публікацій здобувача

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Медвінський С. В., Журавська І. М. Методи та алгоритми обробки зображень для біометричної ідентифікації за капілярною мережею кон'юнктиви ока. *Наука і техніка сьогодні.* 2026. Вип. 2 (56). С. 2028–2038. DOI: 10.52058/2786-6025-2026-2(56)-2028-2038. ISSN 2786-6025. **Кат. Б**

2. Medvinskyi S. The use of cross-correlation as an interaction tool for computer systems by individuals with musculoskeletal disorders. *Infocommunication and Computer Technologies.* 2025. № 2 (10). С. 98–104. DOI: 10.36994/2788-5518-2025-02-10-12. ISSN 2788-5518. **Кат. Б**

3. Medvinskyi S., Zhuravska I. Development of a method for processing eye images for use during biometric authorization in computer systems. *Electrotechnic and Computer Systems*. 2025. № 44 (120). С. 49–54. DOI: 10.15276/eltecs.44.120.2025.6. ISSN 2221-3805. **Кат. Б**

4. Медвінський С. Авторизація користувача у комп’ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2023. Вип. 50. С. 71−77. DOI: 10.36910/6775-2524-0560-2023-50-10. ISSN 2524-0552**. Кат. Б**

Праці, які засвідчують апробацію матеріалів дисертації

5. Медвінський С. Аналіз методів відслідковування напрямку погляду під час використання комп’ютерних систем. *Ольвійський форум – 2024 : стратегії країн Причорноморського регіону в геополітичному просторі* : зб. тез XXI Міжнар. наук. конф. 20–23 червня 2024 р., м. Миколаїв : тези / М-во освіти і науки України. Миколаїв : ЧНУ ім. Петра Могили, 2024. С. 178–183.

6. Журавська І., Медвінський С. Динамічні біометричні показники ока для авторизації користувача в комп’ютерній системі. *Медико-технічна співпраця заради перемоги: актуальні завдання медичної, біологічної фізики та*

інформатики : тези доп. III Наук.-практ. конф. з міжнар. участю, м. Вінниця, 07 квітня 2024 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2024. С. 53–56. URL: https://dspace.vnmu.edu.ua/handle/123456789/6560

7. Журавська І., Медвінський С. Авторизація користувача в комп'ютерній системі за допомогою малюнку капілярів хоріоідеї. *Актуальні завдання медичної, біологічної фізики та інформатики* : тези доп. II Всеукр. наук.-практ. конф. З міжнар. участю, Вінниця, 07 квітня 2023 р. Вінниця : Вінниц. нац. техн. ун-т ім. М. І. Пирогова, 2023. С. 15–17.

8. Медвінський С. В., Журавська І. М. Програмне забезпечення для авторизації користувача у комп'ютерній системі за допомогою зчитування зображення капілярів судинної оболонки ока. *Free and Open Source Software (FOSS-2023)* : тези доп. XIV Міжнар. наук.-практ. конф., Харків, 07–10 лютого 2023 р. Харків : ХНЕУ ім. Семена Кузнеця, 2023. С. 101–102.

9. Медвінський С. Використання динамічних біометричних показників для авторизації користувачів. *Могилянські читання – 2022* : тези доп. XXV Всеукр. наук.-практ. конф., Миколаїв, 07–11 листопада 2022 р. Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2022. С. 73–75.

10. Журавська І. М., Медвінський С. В., Ухань Є. О. Упровадження EAP-TLS сертифікатів у Mikrotik з аутентифікацією користувачів за динамічними біометричними параметрами. *Могилянські читання – 2021* : тези доп. XXIV Всеукр. наук.-метод. конф., Миколаїв, 8–12 листоп. 2021 р., Миколаїв : Чорном. нац. ун-т ім. Петра Могили, 2021. С. 55–58.