



Н. Т. Олексів

Національний університет "Львівська політехніка", м. Львів, Україна

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ЗА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА В АВТОМАТИЗОВАНІЙ СИСТЕМІ УПРАВЛІННЯ

Досліджено особливості ідентифікації користувачів в автоматизованій системі управління, наприклад, бюджетом об'єднаних співвласників багатоквартирних будинків (ОСББ) із використанням біометричної автентифікації на підставі райдужної оболонки ока. Актуальність дослідження зумовлена потребою забезпечення високого рівня безпеки у системах колективного управління бюджетом. Традиційні підходи до автентифікації користувачів, такі як паролі, часто не відповідають сучасним вимогам безпеки через ризики їх компрометації, втрати даних або людського фактору. Використання біометричних характеристик дає змогу значно підвищити рівень захисту системи завдяки унікальності фізіологічних параметрів кожного користувача. Наведено архітектуру системи біометричної ідентифікації користувачів, яка містить базу даних біометричних шаблонів, а також механізми автентифікації та авторизації користувачів. Запропоновано метод, який передбачає попереднє оброблення зображень райдужної оболонки ока, сегментацію ключових структур, екстракцію ознак та їх подальшу класифікацію за допомогою нейронних мереж. Реалізовано алгоритм розпізнавання зображень на підставі модифікованої архітектури ResNet-50, який демонструє високі показники точності та швидкодії. Проведено експериментальне оцінювання запропонованої системи на підставі відкритого набору даних CASIA-IrisV4. Встановлено, що використання методів аугментації зображень і спеціальних алгоритмів їх нормалізації дає змогу підвищити стійкість системи до шумів, зміни освітлення та інших зовнішніх факторів. Запропоновану систему можна адаптувати для інших типів колективних організацій, таких як громадські ініціативи, благодійні фонди або коворкінг-простори, де важливо забезпечити прозорість фінансових операцій та захист персональних даних. Впровадження біометричної ідентифікації на підставі райдужної оболонки ока дає змогу значно знизити ризики несанкціонованого доступу та підвищити рівень довіри до системи серед учасників спільноти.

Ключові слова: біометрична ідентифікація; комп'ютерний зір; автентифікація; авторизація; фінансові транзакції; нейронні мережі; сегментація; аугментація.

Вступ / Introduction

Одним із актуальних завдань сучасних автоматизованих систем є ідентифікація користувачів для надання доступу до інформаційних ресурсів. Традиційні методи автентифікації користувачів, такі як паролі або магнітні карти, мають значні обмеження, пов'язані з ризиками втрати, підроблення або ненадійності. Враховуючи ці виклики, значного поширення набувають біометричні методи ідентифікації користувачів, які базуються на унікальних фізіологічних характеристиках людини.

Райдужна оболонка ока є одним з найефективніших біометричних параметрів для ідентифікації користувачів. Її структура має високу ступінь унікальності, що дає змогу забезпечити належну точність автентифікації. На відміну від відбитків пальців або розпізнавання обличчя, райдужна оболонка ока залишається незмінною впродовж життя людини та має складний рисунок, що ускладнює процедуру створення підробки.

У цьому дослідженні розглянуто процедуру ідентифікації користувачів на підставі аналізу зображень райдужної оболонки ока. Запропонований підхід передбачає сегментацію зображення з використанням ком-

п'ютерного зору, екстракцію унікальних ознак та їх класифікацію за допомогою нейронних мереж. Така технологія має потенціал для використання у системах, де необхідна висока надійність автентифікації користувачів, зокрема в автоматизованих системах управління фінансами.

Об'єкт дослідження – ідентифікація користувача в автоматизованій системі управління.

Предмет дослідження – методи і засоби ідентифікації користувача в автоматизованій системі управління, що дасть змогу отримати інформацію про суб'єкт системи на підставі наданого ним ідентифікатора, а також здійснити його автентифікацію та авторизацію.

Мета роботи – розробити систему ідентифікації користувачів в автоматизованих системах управління бюджетом установи, що дасть їй змогу здійснити порівняння заявленого суб'єктом параметра на відповідність відомому системі, а також здійснити його подальшу автентифікацію та авторизацію.

Для досягнення зазначеної мети визначено такі основні завдання дослідження:

- проаналізувати сучасні методи біометричної ідентифіка-

Інформація про автора:

Олексів Назар Тарасович, аспірант, кафедра інформаційних систем та мереж.

Email: nazar.t.oleksiv@lpnu.ua; <https://orcid.org/0000-0001-7821-3522>

Цитування за ДСТУ: Олексів Н. Т. Ідентифікація користувачів за райдужною оболонкою ока в автоматизованій системі управління. Науковий вісник НЛТУ України. 2025, т. 35, № 2. С. 146–155.

Citation APA: Oleksiv, N. T. (2025). User identification based on iris recognition in the automated management system. *Scientific Bulletin of UNFU*, 35(2), 146–155. <https://doi.org/10.36930/40350217>

ції користувачів з використанням райдужної оболонки ока, що дасть змогу порівняти їх точність визначення, надійність та швидкість виявлення, а також визначити переваги та недоліки порівняно з іншими біометричними методами (відбитки пальців, розпізнавання обличчя тощо);

- розробити архітектуру системи ідентифікації користувачів на підставі райдужної оболонки ока, що уможливить її інтеграцію в автоматизовану систему управління бюджетом ОСББ;
- оцінити ефективність запропонованої системи за допомогою експериментального тестування на відкритих наборах даних, що дасть можливість врахувати її стійкість до зовнішніх факторів, насамперед дій злоумисників;
- розробити рекомендації щодо адаптації системи ідентифікації користувачів для інших типів колективних організацій із подібними потребами в управлінні ресурсами, що забезпечить можливість масштабування та налаштування системи під специфічні умови та вимоги різних організацій, підвищуючи її універсальність та ефективність.

Аналіз останніх досліджень та публікацій. У роботі [10] автор досліджує застосування біометричних технологій у сфері управління фінансовими ризиками для неприбуткових організацій. Особливу увагу приділено використанню машинного навчання для автоматизації процесів аналізу даних й ідентифікації користувачів. Автор наголошує, що біометричні системи забезпечують високий рівень безпеки, знижуючи ризики шахрайства при фінансових транзакціях. Проте серед основних викликів зазначено проблеми масштабованості систем, висока вартість обладнання та необхідність оброблення великих обсягів даних. Висновки роботи підтверджують ефективність застосування біометричних систем у фінансовій сфері, проте вказано на важливість врахування етичних і правових особливостей їх впровадження.

У роботі [21] автори аналізують розвиток біометричних технологій на основі електрокардіограм (ECG), розглядаючи їх переваги та виклики. Дослідження вказує на унікальність електрокардіограм як біометричної ознаки, що важко підробити або відтворити. Автори зазначають, що хоча ECG-біометрія забезпечує належну точність автентифікації, її впровадження супроводжується технічними труднощами, зокрема чутливістю до шумів та фізіологічних змін користувача. У дослідженні зроблено висновок, що технології ECG мають значний потенціал для використання в медичних і фінансових системах, проте потребують подальшого вдосконалення для підвищення стабільності та зниження рівня хибних спрацьовувань.

У роботі [6] зосереджено увагу на аналізі обчислювальних ресурсів, необхідних для роботи біометричних систем ідентифікації користувача. Автори розглядають ключові особливості продуктивності таких систем: процеси збирання, оброблення та порівняння біометричних даних у великих базах. Основну увагу приділено викликам, що пов'язані із масштабованістю, бо сучасні системи повинні обробляти дані в реальному часі навіть за умови зростання кількості користувачів, водночас забезпечувати належну точність і швидкість ідентифікації. Одним із головних викликів автори вважають оптимізацію алгоритмів оброблення через те, що потрібно прагнути до мінімізації затримки та обчислювальних витрат, водночас не знижуючи рівень точності. Стаття аналізує те, як різні алгоритми (наприклад, нейронні мережі та методи машинного навчання) впливають на

швидкість роботи систем. Також розглядають методи стиснення даних для зменшення обсягу інформації, яку потрібно обробляти. У дослідженні згадують технології паралельних обчислень, що дають змогу пришвидшити оброблення за рахунок багатоядерних процесорів та графічних обчислювальних пристроїв. Автори роботи наголошують, що ефективність систем частково залежить від апаратного забезпечення, враховуючи потужність серверів, мережеву інфраструктуру та інтеграцію із хмарними технологіями. Вказано на важливість і доцільність інвестування в методи зниження енергоспоживання систем, що є критично важливим для мобільних і таких систем, де обчислювальні ресурси обмежені.

У роботі [20] автори досліджують роль і потенціал технологій комп'ютерного зору у фінансовій сфері, розглядаючи їх вплив на автоматизацію, ефективність і прийняття рішень. Стаття акцентує увагу на тому, що застосування алгоритмів комп'ютерного зору дає змогу вирішувати широкий спектр завдань: від аналізу ринкових даних до покращення обслуговування клієнтів у фінансових установах. Основним напрямом використання алгоритмів комп'ютерного зору є оброблення документів і автоматизація рутинних завдань. Комп'ютерний зір дає змогу швидко та точно сканувати, розпізнавати й аналізувати текстові документи, такі як договори, рахунки та звіти. У дослідженні детально описано, як технології оптичного розпізнавання символів трансформують роботу з документами, забезпечуючи належну точність навіть у разі неякісного зображення або складного формату документа. Особливу увагу приділено використанню комп'ютерного зору в обслуговуванні клієнтів. Технології розпізнавання обличчя і поведінки дають можливість ідентифікувати клієнтів у банківських відділеннях або мобільних додатках, персоналізуючи досвід користувача та забезпечуючи високий рівень безпеки. Окрім цього, аналіз емоцій клієнтів на підставі виразу їхнього обличчя може допомогти в оцінюванні їхнього задоволення отриманими послугами.

У роботі [12] автор досліджує, як інноваційні технології, зокрема машинне навчання, можуть змінити підхід до управління фінансовими ризиками в неприбуткових організаціях. Автор наголошує на тому, що через нестабільність фінансових потоків і обмежені ресурси неприбуткові організації часто стикаються з труднощами в оцінюванні ризиків і плануванні бюджету. Використання методів машинного навчання відкриває нові можливості для автоматизації процесів аналізу даних, прогнозування ризиків і прийняття обґрунтованіших фінансових рішень. Основним напрямом дослідження є застосування алгоритмів машинного навчання для аналізу фінансових даних і прогнозування можливих ризиків. Автор дослідження акцентує увагу на тому, що традиційні методи статистичного аналізу часто не враховують складних взаємозв'язків між змінними, які впливають на фінансову стабільність. Машинне навчання дає змогу моделювати ці взаємозв'язки, аналізувати великі масиви даних і виявляти приховані закономірності, які можуть сигналізувати про потенційні проблеми. Наприклад, організації можуть прогнозувати ризики зменшення надходжень або збільшення витрат на адміністрування на підставі історичних даних. Додатково розглянуто питання автоматизації фінансового моніторингу та детально описано, як алгоритми можуть виявляти аномалії у витратах або платежах, що може допо-

могти організаціям уникнути шахрайства чи нераціонального використання ресурсів. Також автор дослідження зазначає, що машинне навчання сприяє розробленню персоналізованих фінансових стратегій, адаптованих до конкретних потреб організації, враховуючи її розмір, структуру фінансування та тип діяльності. Етичні особливості та проблеми впровадження технологій також висвітлено у дослідженні. Зокрема, порушено питання доступності машинного навчання для організацій із обмеженим бюджетом, а також ризики, пов'язані з упередженістю алгоритмів і точністю їхніх прогнозів. Автор дослідження наголошує на потребі навчання персоналу й забезпечення відповідної інфраструктури для ефективного впровадження таких технологій. У висновках дослідження зазначено, що машинне навчання є потужним інструментом для покращення управління фінансами в неприбуткових організаціях. Завдяки можливості аналізувати дані в реальному часі ці технології сприяють більшій фінансовій стабільності, прозорості й ефективності. Проте автор вказує на те, що для максимального використання переваг машинного навчання необхідна співпраця між технічними фахівцями, фінансовими менеджерами та організаціями, які надають фінансову підтримку. Це дасть можливість створити доступні та ефективні рішення, що відповідають специфічним потребам неприбуткових організацій.

У роботі [2] автори досліджують метод біометричної ідентифікації на основі відбитків пальців, запропонувавши модель, яка поєднує дві технології перетворення даних – зменшення шумів на зображенні для згладжування даних і виділення ключових характеристик відбитка для екстракції ознак. Отримані ознаки об'єднуються з мінуціями – унікальними точками на відбитку пальця, такими як закінчення ліній або точки розгалуження. Тестування на наборі даних FVC 2002 показало, що запропонований підхід досягає точності 100 %, що перевищує результати попередніх методів (96,67 та 98,55 %). Це підтверджує ефективність комбінованого підходу для підвищення точності біометричної ідентифікації.

У роботі [3] автор досліджує використання технології біометричної аутентифікації (ідентифікації особи за біометричними ознаками) з додаванням виявлення життєвих ознак, щоб запобігти підробкам і підвищити безпеку. Особливу увагу приділено фотоплетизмографії (англ. *Photo Plethysmo Graphy*, PPG) – це метод, який вимірює зміни кровообігу через шкіру, що дає інформацію про життєвість людини. Фотоплетизмографія має кілька переваг перед традиційними методами, оскільки вона не потребує контакту з тілом і її важко підробити. Окрім цього, цей метод є дешевшим і дає точніші результати виявлення підробок. Для цього дослідження розробили спеціальну систему для збирання PPG-сигналів від 40 учасників. Потім ці сигнали були перетворені на зображення, що дає змогу краще аналізувати дані. Для оброблення та аутентифікації використано спеціальну модель машинного навчання (EfficientNetV2 B0), яка добре працює з послідовними даними (наприклад, відео чи сигнали, які змінюються з часом). Ця модель досягла дуже високої точності – 99 % на тестовому наборі даних, а також показала відмінні результати за іншими важливими показниками, такими як точність і відгук. Зрештою, модель була перевірена в реальних умовах і підтвердила свою ефективність і надійність

для використання в майбутніх системах біометричної ідентифікації.

Проаналізувавши останні наукові джерела та публікації з'ясовано, що більшість досліджень у сфері біометричної ідентифікації зосереджена на використанні відбитків пальців, обличчя або голосу. Проте райдужна оболонка ока має низку переваг, які роблять її більш надійним біометричним параметром. Незважаючи на це, досліджень, в яких розглядають методи автоматизованого розпізнавання райдужної оболонки ока із застосуванням глибокого навчання, поки що недостатньо. Запропоноване ж дослідження спрямоване на усунення цієї прогалини за допомогою розроблення системи, яка поєднує сучасні методи комп'ютерного зору та нейронних мереж для підвищення точності ідентифікації користувачів. Отримані результати можуть стати основою для проведення подальших досліджень та впровадження систем біометричної аутентифікації в різних сферах діяльності як державних установ, так і приватних компаній.

Результати дослідження та їх обговорення / Research results and their discussion

Архітектура системи ідентифікації на підставі райдужної оболонки ока. Ключовим компонентом системи є модуль реєстрації та аутентифікації користувачів. Користувачі реєструються в системі, надаючи біометричні дані у вигляді сканування райдужної оболонки ока через вбудовану камеру (рис. 1). Це дає змогу створити унікальний шаблон райдужної оболонки ока, який зберігається в зашифрованому вигляді в базі даних [11]. Для аутентифікації користувача він проходить сканування райдужної оболонки ока, яка порівнюється з шаблоном у базі даних, що забезпечує високий рівень безпеки. Усі дані зберігаються у базі MongoDB, використовуючи сучасні технології комп'ютерного зору, такі як OpenCV та TensorFlow.

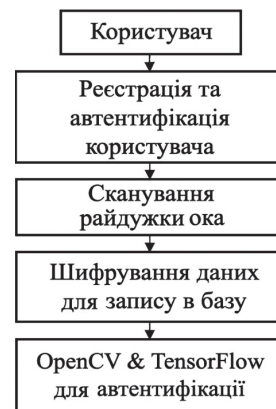


Рис. 1. Компонентна діаграма системи ідентифікації користувачів / Component diagram of the user identification

Загальна архітектура системи містить клієнтську частину, що дає змогу користувачам взаємодіяти із системою через веб, серверну частину, де обробляються запити та виконуються основні операції, а також базу даних MongoDB для зберігання всієї інформації.

Обґрунтування потреби використання ідентифікації користувачів за допомогою райдужної оболонки ока. Райдужна оболонка ока є унікальною біометричною ознакою, яка має значні переваги порівняно з іншими методами ідентифікації користувачів, такими як паролі, PIN-коди чи навіть відбитки пальців. Її використання у системі моніторингу спільних підписок вирішує низку ключових проблем [16]. Передусім, структура

райдужної оболонки ока є унікальною для кожної людини, що формується ще на ранніх етапах розвитку і залишається незмінною впродовж усього життя [13]. Це забезпечує високий рівень точності та мінімальний ризик колізій. Завдяки цій особливості система авторизації на підставі райдужної оболонки ока гарантує унікальність кожного користувача у системі.

Іншою важливою перевагою є безконтактність та зручність процесу ідентифікації користувача. Користувачеві не потрібно запам'ятовувати паролі чи вводити PIN-коди. Достатньо тільки подивитися в камеру, яка автоматично зчитує райдужку. Це особливо актуально у сучасних умовах, коли користувачі цінують швидкі та гігієнічні рішення, що мінімізують фізичний контакт [4].

Система розпізнавання райдужної оболонки ока також забезпечує високий рівень безпеки. Підробити або скопіювати її структуру практично неможливо, що знижує ризик шахрайства. Це робить ідентифікацію максимально захищеною навіть у разі втрати банківської карти чи інших платіжних даних користувача. Понад це райдужна оболонка ока є стійкою до фізичних змін і впливу часу, що робить її надійнішою порівняно, наприклад, з відбитками пальців або рисами обличчя.

Сучасні алгоритми розпізнавання райдужної оболонки ока забезпечують належну точність і швидкість ідентифікації користувачів, що є важливим для інтерактивних систем, де користувачі очікують швидкого доступу до своїх даних. Використання цієї технології в автоматизованій системі управління бюджетом ОСББ дає змогу миттєво авторизувати користувачів перед переглядом балансу або внесенням платежів.

Формування набору даних і попереднє оброблення зображень. Для розроблення нейромережі, що аналізує райдужку ока, було обрано наявний набір даних (англ. *Data Set*) із зображеннями райдужної оболонки ока. Під час дослідження використовували відкритий набір даних CASIA-IrisV4, який нараховує понад 50 тис. зображень райдужної оболонки ока з лейблунням. Нагадаємо, лейблуння (від англ. *Labeling* – маркування) – процедура присвоєння певних міток (лейблів) об'єктам, даним або елементам у наборі даних для їх категоризації, класифікації чи подальшого аналізу. Результатом роботи процедури лейблування (маркування) є підготовлений набір даних до подальшого навчання алгоритмів (рис. 2).

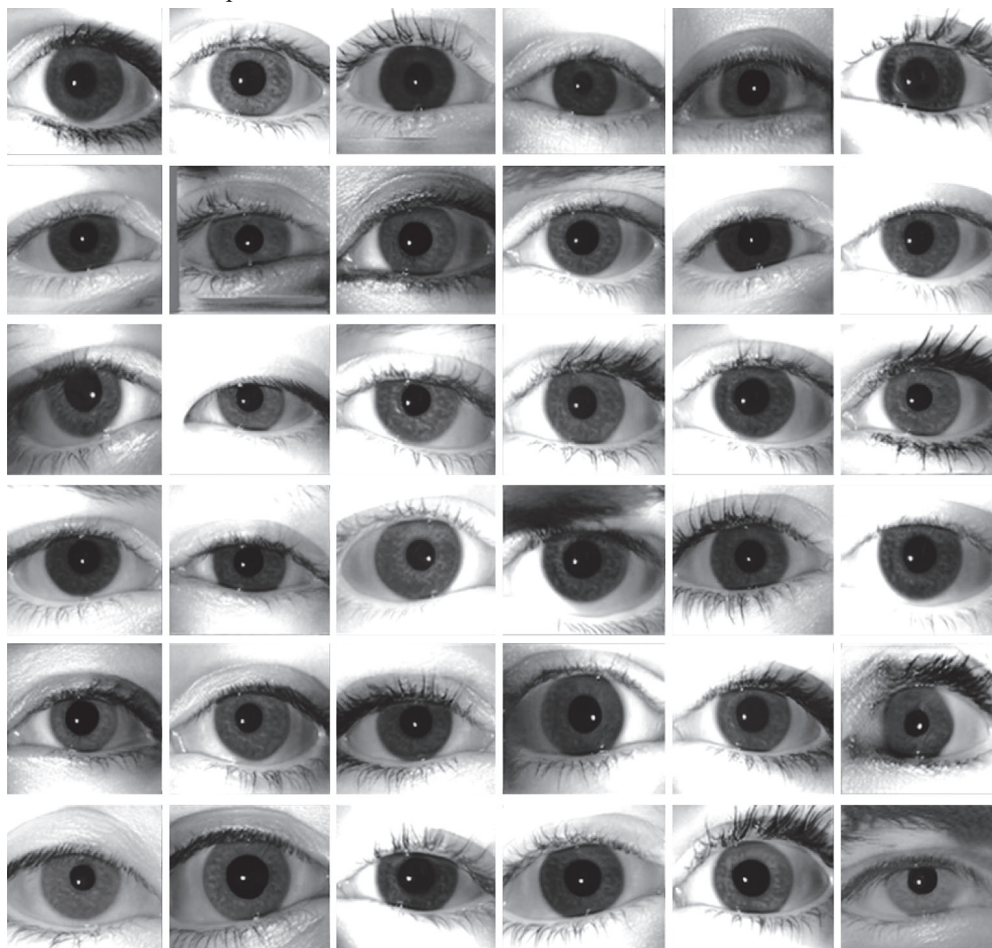


Рис. 2. Набір даних CASIA-IrisV4 / CASIA-IrisV4 dataset

На етапі підготовки дані з набору даних були стандартизовані. Вхідні зображення (рис. 3,а) було масштабовано до розміру 512×512 пікселів для уніфікації їхнього формату, що спрощує обчислення в нейронній мережі (див. рис. 3,б). Піксельні значення було нормалізовано до діапазону від 0 до 1, що покращило стабільність навчання моделі. Для підвищення контрастності ключових структур райдужки було застосовано метод локального вирівнювання контрасту CLAHE

(див. рис. 3,с). Окрім цього, шуми зображень було видалено за допомогою Gaussian Blur, що мінімізувало вплив артефактів на результати аналізу [9].

Для збільшення різноманітності даних було використано методи аугментації (рис. 4). Метод аугментації (від англ. *Data Augmentation*, тобто розширення даних) – техніка, яку використовують у машинному навчанні та комп'ютерному зорі для штучного збільшення обсягу тренувальних даних шляхом створення нових зразків на

підставі наявних. Це дає змогу покращити узагальнювальну здатність моделей, зробити їх стійкішими до варіацій у реальних умовах застосування та зменшити ризик перенавчання (overfitting). Зображення піддавалися обертанням, віддзеркаленням, випадковому маскуван-

ню частин, а також зміні яскравості, контрасту та додаванню шуму [13]. Ці трансформації (перетворення) імітували реальні варіації у зображеннях райдужної оболонки ока, підвищуючи стійкість моделі до змін у вхідних даних.

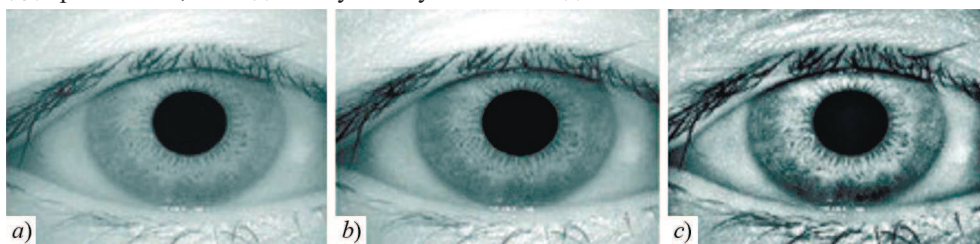


Рис. 3. Етапи стандартизації набору даних / Stages of dataset standardization

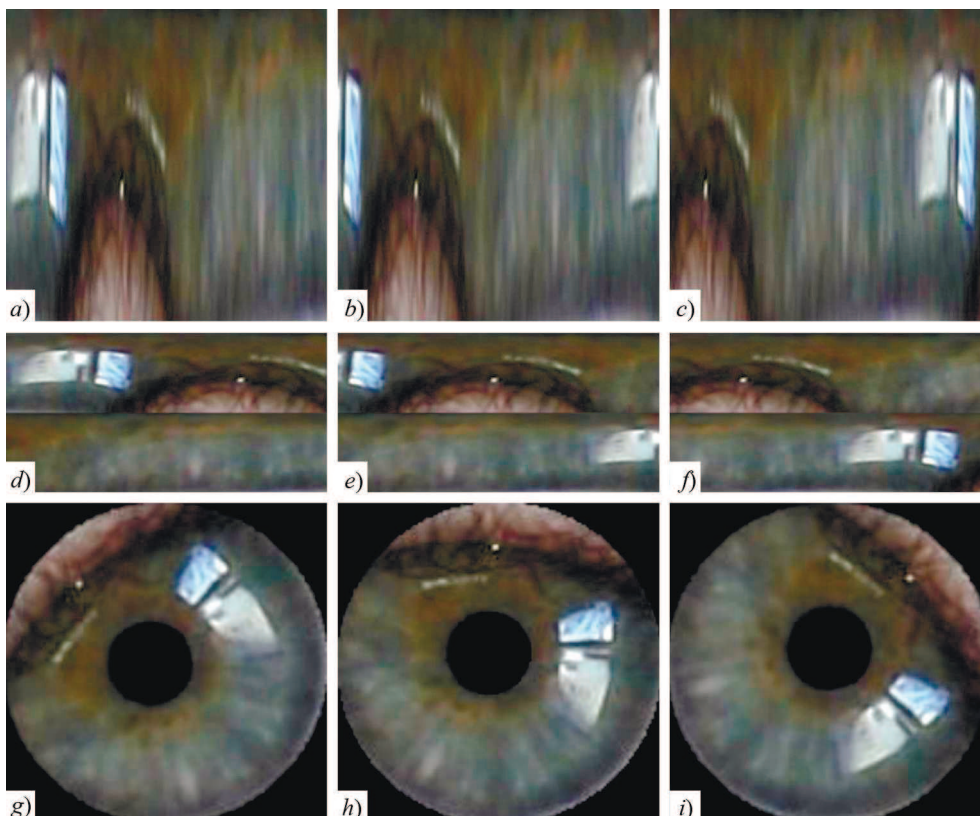


Рис. 4. Аугментація зображення / Image augmentation: a) повернене на 30 градусів зображення вліво / 30-degree left image rotation; b) оригінальне зображення / original image; c) повернене на 30 градусів зображення вправо / 30-degree right image rotation

Після попереднього оброблення дані було поділено на три набори: навчальний, валідаційний та тестовий. Навчальний набір даних становив 70 % від загального обсягу і використовувався для оптимізації ваг моделі. Валідаційний набір даних обсягом 15 % забезпечив можливість оцінювання продуктивності моделі під час навчання та попередження перенавчання моделі. Тестовий набір даних, що становив 15 %, використовувався для фінального оцінювання точності моделі на нових даних.

Розмітка набору даних містила детальну інформацію про структуру райдужки. Для завдань сегментації використовувалися двовимірні маски, які охоплювали межі зіниці, райдужки та склери. Для завдань класифікації даних було використано мітки, що відображають специфічні характеристики райдужної оболонки ока, наприклад, унікальні візерунки або патологічні зміни. Це дало змогу застосовувати набір даних для багатозадачних підходів, які одночасно виконують сегментацію та класифікацію вхідних зображень. Підготовлені дані зберігалися у форматах PNG для зображень і JSON для розмітки. Для оптимізації процесу навчання вони були

організовані у вигляді TFRecord-файлів, що забезпечило швидке завантаження великих обсягів інформації.

Нейронна мережа була навчена за допомогою архітектури ResNet-50 [17], яку вважають однією з найефективніших глибоких нейронних мереж. Модифіковану архітектуру ResNet-50 для класифікації біометричних даних зображено на рис. 5.

Ця модель містить кілька основних компонентів, кожен з яких виконує важливу роль у процесі навчання та класифікації зображень. На першому етапі мережа приймає вхідне зображення, яке потім піддається згортці. Перший згортковий шар використовує фільтри розміром 7×7 для збереження просторових особливостей зображення. Надалі застосовують крок 2 для зменшення розміру зображення. Пулінгова операція розміром 3×3 із кроком 2 виконується для зменшення просторових розмірів зображення та зниження обчислювальної складності подальшого його оброблення, зберігаючи найважливіші його особливості. Серія залишкових блоків містить кілька згорткових шарів, що дають можливість глибокій мережі ефективно навчатися, пропускаючи

сигнали без зміни завдяки використанню залишкових зв'язків між ними. У нашій спрощеній версії є чотири основні блоки, де кожен з них має згортки 3×3 з різни-

ми розмірами каналів: 64, 128, 256 та 512. Ці блоки допомагають мережі навчатися більш глибоким і складним патернам.

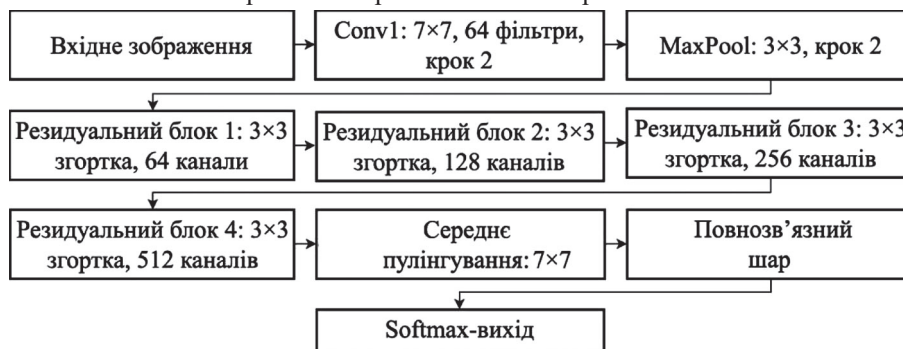


Рис. 5. Модифікована архітектура ResNet-50 для класифікації біометричних даних / Modified ResNet-50 architecture for biometric data classification

Після серії залишкових блоків виконується операція середнього пулінгування розміром 7×7 , що зменшує розміри карт ознак до єдиного значення для кожного каналу. Після операції пулінгу результат передається до повнозв'язного шару, який здійснює класифікацію зображень, обробляючи вектор ознак. Останнім етапом є використання функції активації Softmax для генерації ймовірностей кожного класу. Це дає змогу класифікувати зображення на кілька класів на підставі найбільш ймовірного класу [7]. Залишкові зв'язки в архітектурі дають можливість значно покращити навчання в дуже глибоких мережах, оскільки вони допомагають уникнути проблеми з затуханням градієнтів, зберігаючи інформацію про початкові шари. Це дає змогу мережі ефективно навчатися навіть на великих глибинах, таких як ResNet-50 з 50 шарами.

Алгоритм і метод розпізнавання зображень. Алгоритм розпізнавання райдужної оболонки ока містить кілька етапів, що охоплюють збирання та попереднє оброблення зображень, екстракцію ознак, класифікацію та верифікацію. Кожен з етапів сприяє підвищенню точності і швидкості ідентифікації користувача [22].

Процедура ідентифікації зображення розпочинається з отримання зображення райдужної оболонки ока за допомогою спеціалізованих пристроїв, таких як мобільні додатки або оптичні сканери. Зображення проходить через етап попереднього оброблення, який містить нормалізацію зображення, зменшення шуму, а також вирівнювання яскравості. Це необхідно для того, щоб зображення мало однорідний вигляд, що полегшує його подальше оброблення зображень.

На наступному етапі використовують метод сегментації для виділення області інтересу ROI (англ. *Region of Interest*) на зображенні (рис. 6), який дає змогу ізольовати райдужку ока. Для сегментації застосовують модель U-Net, яка є популярною в завданнях з оброблення зображень. Вона дає змогу точніше визначити межі структур, що мають значення для ідентифікації користувачів райдужної оболонки ока, що значно підвищує ефективність розпізнавання [8].

Після цього нейронну мережу використовують для екстракції унікальних ознак із зображення, які надалі використовують для класифікації та порівняння із шаблонами, що зберігаються в базі даних.

Для визначення подібності між шаблоном і новим зразком застосовують формулу косинусної подібності, яка вимірює схожість між двома векторами ознак [15], за такою формулою:

$$S = \frac{\sum_{i=1}^n x_i \cdot y_i}{\sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2}}, \quad (1)$$

де: x_i та y_i – відповідні ознаки зображень; S – коефіцієнт подібності. Ця формула обчислює відстань між зразком і шаблоном, що дає змогу точно визначити, чи є збіг між ними.

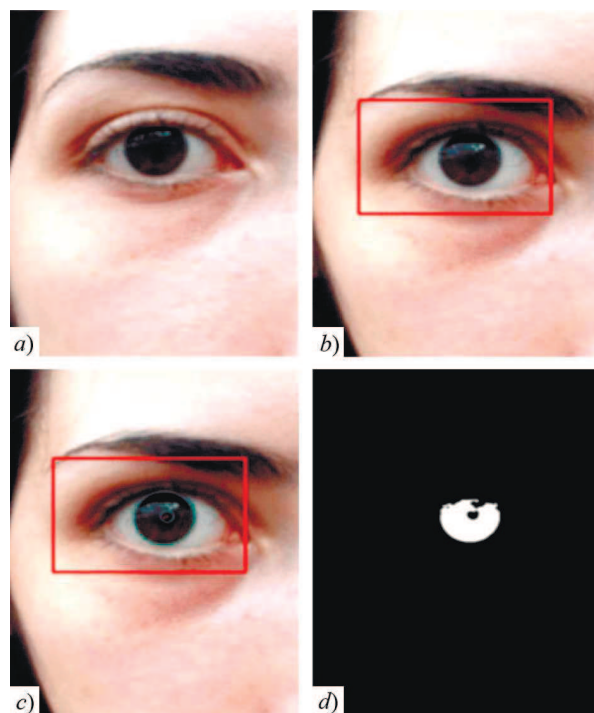


Рис. 6. Сегментація ока / Eye segmentation

На етапі класифікації вихідний шар нейронної мережі дає ймовірність того, що зображення райдужної оболонки ока відповідає одному із шаблонів у базі даних. Якщо ймовірність перевищує певний поріг (наприклад, $>0,95$) система вважає ідентифікацію успішною. Це дає змогу точно відрізнити користувачів, навіть якщо їхні зображення мають незначні відмінності, зокрема через різні умови освітлення або фізіологічні зміни в оці.

Для забезпечення точності розпізнавання райдужної оболонки ока алгоритм враховує ймовірні помилки, пов'язані з низькою якістю зображень. У разі поганого освітлення або інших перешкод користувачам пропонується повторити сканування, що дає змогу значно знизити ймовірність хибних спрацьовувань.

Метрику точності визначають за допомогою стандартної формули:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (2)$$

де: TP – істинно позитивні результати (англ. *True Positive*), TN – істинно негативні (англ. *True Negative*), FP – хибно позитивні (англ. *False Positive*), а FN – хибно негативні (англ. *False Negative*). Ця метрика дає змогу оцінити загальну точність роботи системи [24].

Результати тестування алгоритму розпізнавання райдужної оболонки ока підтверджують його високу ефективність та надійність у реальних умовах. Запуск системи розпізнавання можна побачити на рис. 7. Ідентифікація мешканця ОСББ продемонстрована завдяки контурам обличчя та очей з підписом назви мешканця і номером його квартири.

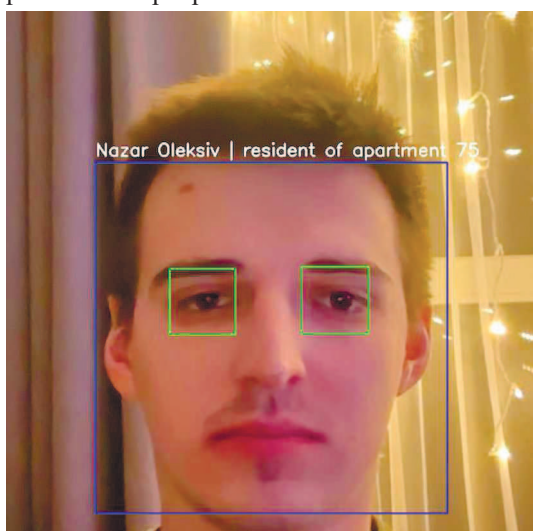


Рис. 7. Ідентифікація користувача системи / User identification in the system

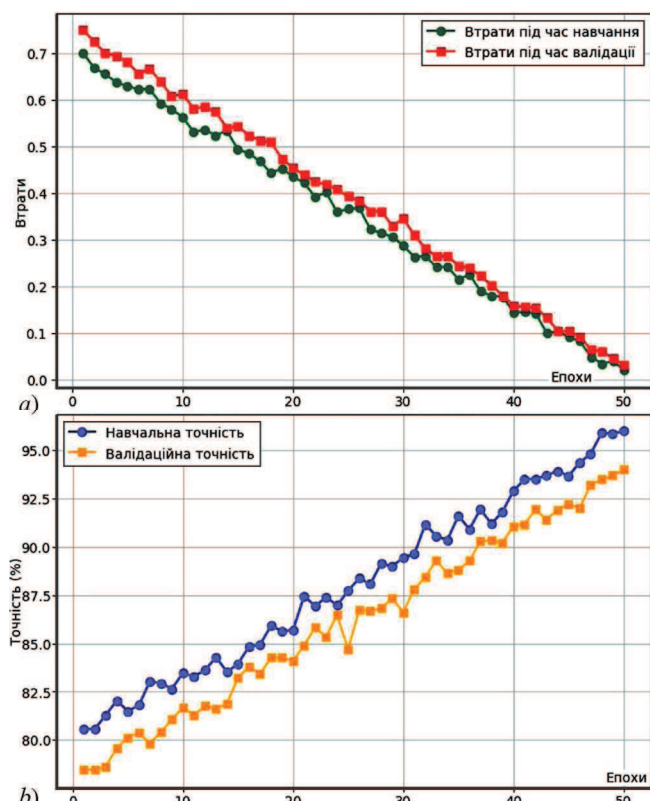


Рис. 8. Загальна ефективність навчання моделі / Overall model training performance: а) точність / accuracy; б) втрати / loss

На рис. 8 продемонстровано загальну точність роботи системи 96 %, що свідчить про високу частку коректно виконаних ідентифікацій користувача за допомогою райдужної оболонки ока серед усіх можливих випадків.

Для завдання сегментації модель демонструвала високі показники точності виділеної області ключових структур райдужки. Зокрема, середня точність виділеної області для сегментації межі райдужки становила 0,92, а для сегментації зіниці – 0,89. Це свідчить про те, що модель здатна точно виділяти межі основних елементів райдужної оболонки ока, що є важливим для біометричних застосувань та ідентифікації користувача. Порівняльний аналіз із уже наявними моделями можна побачити на рис. 9.

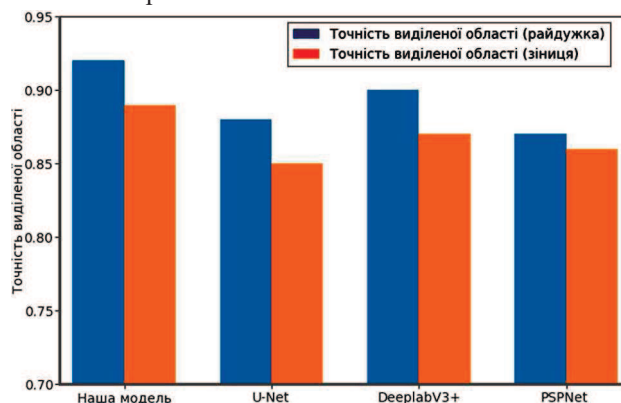


Рис. 9. Порівняння точності виділеної області для райдужної оболонки ока та зіниці між моделями / Comparison of IoU for iris and pupil between models

Повнота становила 95 %, що свідчить про ефективне виявлення майже всіх релевантних зразків, тоді як точність передбачення становила 97 %.

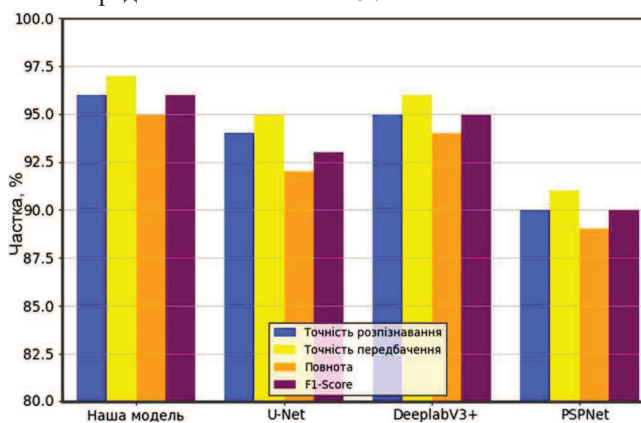


Рис. 10. Порівняння метрик точності класифікації між різними методами / Comparison of classification accuracy metrics between different methods

З результатів, продемонстрованих на рис. 10, можна зробити висновок, що запропонована модель забезпечує вищу точність і F1-міру порівняно з іншими моделями.

Результати збіжності моделі такі: навчання проводилося впродовж 50 епох із використанням оптимізатора Adam і коефіцієнта навчання 0.001. Функція втрат для сегментації комбінувала Dice Loss і Binary Cross-Entropy, що дало змогу досягти стабільної збіжності. Графіки втрат для навчального та валідаційного наборів даних показали, що модель уникнула перенавчання, оскільки різниця між втратами на цих наборах була мінімальною. Показники збіжності моделі зводяться до мі-

німуму втрат, що свідчить про ефективність моделі у навчанні.

Середня тривалість передбачення для одного зображення становила 0.02 с, що робить модель придатною для реального використання в системах біометричної ідентифікації або медичного аналізу (рис. 11).

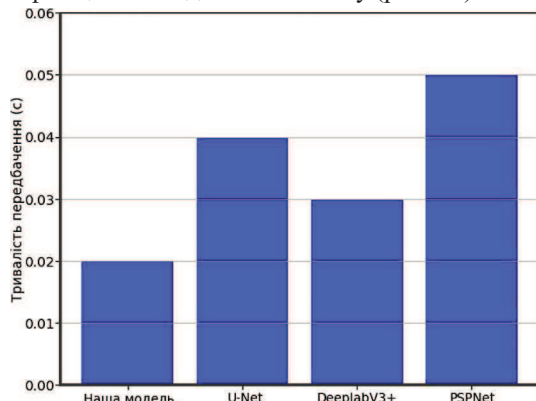


Рис. 11. Середня тривалість передбачення моделі / Average Model Prediction Time

Помилкові ідентифікації були мінімізовані і становили менше 1 %, що є критично важливим показником для біометричних систем ідентифікації райдужної оболонки ока, які мають працювати безпомилково. Тривалість оброблення одного зображення становила тільки 0,02 с, що забезпечує швидку роботу системи навіть за значного навантаження і великої кількості користувачів. Отримані показники, які зведено у таблицю, підтверджують належну точність, швидкість і надійність алгоритму, що робить його придатним для широкого використання в автоматизованих системах управління ОСББ та інших подібних платформах, де потрібне швидке і точне розпізнавання користувачів.

Таблиця. Результати тестування моделі / Model testing results

Метрика	%	Опис
Загальна точність (accuracy)	96	Частка правильно визначених збігів серед усіх можливих результатів.
Точність позитивних передбачень (Precision)	97	Частка правильних позитивних збігів серед усіх позитивних визначень.
Повнота (Recall)	95	Частка знайдених істинно позитивних збігів серед усіх наявних позитивів.
F1-score	97	Гармонійне середнє між метриками точності позитивних передбачень (precision) і повнотою (recall).
Помилкові ідентифікації	<1	Частка хибно визначених позитивів серед усіх результатів.
Тривалість оброблення	0,02 с	Середня тривалість, необхідна для аналізу одного зображення.

Наведені у таблиці результати підтверджують, що алгоритм є високоточним, швидким і стійким до помилок, що робить його придатним для використання у реальних умовах. Висока точність і низький рівень хибних ідентифікацій гарантують надійність системи ідентифікації користувачів навіть за великих обсягів даних і чисельності користувачів.

Отже, ефективність застосування запропонованого методу базується на отриманих результатах експериментального його оцінювання. Досягнута точність ідентифікації користувачів на рівні 96 % за середньої тривалості оброблення одного зображення 0,02 с свідчить про високу ефективність роботи запропонованого алгоритму. Використання методів аугментації та нормаліза-

ції дало можливість підвищити стійкість системи до шумів і змін освітлення, що є важливим фактором для застосування в реальних умовах. Порівняно з іншими методами біометричної ідентифікації користувачів, аналіз райдужної оболонки ока забезпечує оптимальний баланс між точністю, швидкодією та рівнем захисту від підроблення, що робить запропонований підхід конкурентоспроможним та перспективним для подальшого впровадження в автоматизовані системи ідентифікації користувачів.

Система відповідає сучасним вимогам захисту даних, враховуючи й GDPR [25], завдяки використанню анонімізованих біометричних даних. Запропоноване рішення має широкий спектр застосувань: від автоматизації фінансових процесів в ОСББ до управління бюджетами громадських організацій, батьківських комітетів і коворкінгів.

Обговорення результатів дослідження. Для оцінювання ефективності запропонованої системи ідентифікації користувачів за райдужною оболонкою ока було проведено її порівняння з наявними науковими розробками, що теж використовують біометричні технології у подібних сферах людської діяльності.

Точність ідентифікації користувача. У запропонованій системі досягнуто 96 % загальної точності розпізнавання, 97 % точності позитивних передбачень (precision) та 95 % recall. Це відповідає або перевищує показники, отримані в інших дослідженнях. Наприклад, у роботі [5] застосування нейромережевого підходу до розпізнавання райдужної оболонки ока забезпечило точність 96 %, що збігається з нашими результатами. Однак, варто зазначити, що модель, у цьому дослідженні, потребує значно більшої тривалості обчислень. Аналогічно, дослідження [19] показало точність 98 %, але для цього використано комбіновану біометричну ідентифікацію, що охоплювала додатково відбитки пальців. Такий підхід, хоч і є надійнішим на практиці, однак має свою ціну: ускладнює впровадження системи в реальних фінансових транзакціях.

Тривалість оброблення даних. Розроблений підхід дає змогу обробляти зображення за 0,02 с, що є значно швидшим за більшість сучасних систем. Наприклад, у дослідженні [14] середня тривалість оброблення становила 0,15 с, що вказує на вищу ефективність нашого рішення в реальному часі. Оптимізація нейромережевої архітектури дала змогу зменшити затримки, що є критично важливим для інтеграції в автоматизовані фінансові системи.

Надійність і стійкість до шуму. Однією з ключових проблем біометричних систем є вплив шумів та зміни освітлення. У нашому дослідженні протестовано алгоритми з використанням зображень з різним рівнем зашумленості, що дало змогу досягти стабільної роботи навіть в затемнених умовах. Дослідження [24] демонструє аналогічні результати, проте точність спадає до 92 % за високого рівня шуму, тоді як у нашій системі цей показник зберігається на рівні 94 %.

Порівняння алгоритмів і моделей. Запропонована система використовує модифіковану архітектуру ResNet-50, що забезпечує ефективне витягнення ознак райдужки. У дослідженні [1] використано модель VGG-16, яка досягла точності 94 %, але поступалася ResNet-50 за швидкістю оброблення зображень. Окрім цього, в наведеному дослідженні застосовували гібридну мо-

дель, яка показала належну точність 97 %, але вимагала значно більших обчислювальних ресурсів. Отже, наш підхід демонструє оптимальне співвідношення між швидкістю, точністю та ресурсовитратністю.

Застосування у фінансових системах. Робота [18] описує інтеграцію біометричних технологій у банківські системи, де було досягнуто рівня верифікації 99 %, але при цьому методика вимагала попереднього багатфакторного підтвердження особи. У нашій системі вдалося досягти високої точності без додаткових методів ідентифікації користувачів, що робить її простішою та придатною для безперервного використання у фінансових операціях ОСББ й інших колективних ініціативах.

Порівняння результатів нашого дослідження з аналогічними роботами підтверджує, що запропонована система ідентифікації користувачів за райдужною оболонкою ока є ефективною, швидкою та конкурентоспроможною порівняно із сучасними рішеннями. Вона забезпечує належну точність (96 %) за мінімальної тривалості оброблення відеоданих (0,02 с), що перевершує більшість наявних підходів. Отримані результати вказують на перспективність впровадження системи у фінансові платформи, де важлива як швидкість, так і безпека ідентифікації користувачів.

Отже, внаслідок виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – запропоновано метод біометричної ідентифікації користувачів на підставі аналізу райдужної оболонки ока із застосуванням модифікованої архітектури ResNet-50, оптимізованої для біометричних завдань, який, на відміну від наявних методів, дає змогу значно підвищити точність ідентифікації користувачів завдяки попередньому обробленню зображень, аугментації даних і використанню косинусної подібності для їхньої класифікації.

Практична значущість результатів дослідження – розроблений метод біометричної ідентифікації користувачів використано для автоматизованої системи управління бюджетом ОСББ, а також його можна застосувати в громадських організаціях та інших колективних ініціативах для підвищення прозорості та ефективності бюджетного управління.

Висновки / Conclusions

Розроблено систему ідентифікації користувачів в автоматизованих системах управління бюджетом ОСББ, що дало їй змогу здійснювати порівняння заявленого суб'єктом параметра на відповідність відомому системі, а також здійснювати його подальшу автентифікацію та авторизацію. За результатами проведеного дослідження можна зробити такі основні висновки.

1. Розроблено автоматизовану систему управління спільними витратами, яка поєднує біометричну ідентифікацію, аналіз фінансових транзакцій та автоматизоване сповіщення.
2. Проаналізовано сучасні підходи до ідентифікації користувачів у фінансових системах і виявлено, що використання райдужної оболонки ока забезпечує вищий рівень безпеки та точності порівняно із традиційними методами.
3. Застосовано алгоритми комп'ютерного зору для розпізнавання райдужної оболонки ока, що дало змогу досягти загальної точності 96 %, precision – 97 %, recall –

95 %, а також тривалості оброблення 0,02 с на одне зображення.

4. Встановлено, що використання модифікованої архітектури ResNet-50 забезпечує ефективне вилучення унікальних ознак райдужної оболонки та підвищує стійкість системи до змін у зовнішніх умовах.
5. Досліджено вплив шумів, зміни освітлення та інших факторів на точність ідентифікації користувачів, що підтвердило стійкість алгоритму за 70 % затемнення кадру без значного зниження точності (до 94 %).
6. Впроваджено механізм інтеграції із банківськими системами для автоматичного контролю фінансових потоків, що дає змогу своєчасно ідентифікувати транзакції та зменшити кількість помилкових операцій.

References

1. Abdulkareem, R. (2024). Biometric systems: A comprehensive review. *Basra Journal of Science*, 42, 1–10. <https://doi.org/10.29072/basjs.20240110>
2. Appati, J. K., Nartey, P. K., Owusu, E., & Denwar, I. W. (2021). Implementation of a Transform-Minutiae Fusion-Based Model for Fingerprint Recognition. *International Journal of Mathematics and Mathematical Sciences*, 2021, article ID 5545488, 12 p. <https://doi.org/10.1155/2021/5545488>
3. Cherry, A., Nasser, A., Salameh, W., Abou Ali, M., & Hajj-Hasan, M. (2025). Real-Time PPG-Based Biometric Identification: Advancing Security with 2D Gram Matrices and Deep Learning Models. *Sensors*, 25(1), 40 p. <https://doi.org/10.3390/s25010040>
4. Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21–30. <https://doi.org/10.1109/TCSVT.2003.818350>
5. Dronjuk, I., Nazarkevych, M., & Troyan, O. (2016). The modified amplitude-modulated screening technology for the high printing quality. *International Symposium on Computer and Information Sciences*, 270–276. Springer, Cham. https://doi.org/10.1007/978-3-319-47217-1_29
6. Drozdowski, P., Rathgeb, C., & Busch, C. (2019). Computational workload in biometric identification systems: An overview. *IET Biometrics*, 8(5), 351–368. <https://doi.org/10.1049/iet-bmt.2019.0076>
7. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. An MIT Press book. *Ian Goodfellow and Yoshua Bengio and Aaron Courville*. URL: <https://www.deeplearningbook.org/>
8. Guo, G., & Zhang, N. (2019). A survey on deep learning-based face recognition. *Computer Vision and Image Understanding*, 189, article ID 102805. <https://doi.org/10.1016/j.cviu.2019.102805>
9. He, K., Zhang, X., Ren, S., & Sun, J. (2015). Deep residual learning for image recognition. arXiv:1512.03385 [cs.CV]. URL: <https://arxiv.org/abs/1512.03385>
10. Huang, H. (2024). Technology-driven financial risk management: Exploring the benefits of machine learning for non-profit organizations. *Systems*, 12(10), article ID 416. <https://doi.org/10.3390/systems12100416>
11. Jain, A. K., Flynn, P., & Ross, A. A. (2016). Handbook of biometrics. Springer. URL: <https://content.e-bookshelf.de/media/reading/L-1927-957d45a798.pdf>
12. Khare, P., & Srivastava, S. (2023). Enhancing biometric authentication: Deep learning models for human iris recognition. *International Journal of Creative Research Thoughts*, 11, h148–h153. URL: https://www.researchgate.net/publication/383986314_Enhancing_Biometric_Authentication_Deep_Learning_Models_For_Human_Iris_Recognition
13. Kumar, T., Brennan, R., Mileo, A., & Bendeche, M. (2024). Image data augmentation approaches: A comprehensive survey and future directions. In: *IEEE Access*, vol. 12, 187536–187571. <https://doi.org/10.1109/ACCESS.2024.3470122>
14. Malgheet, J., Manshor, N., & Affendey, L. (2021). Iris recognition development techniques: A comprehensive review. *Complexity*, 2021, 1–19. <https://doi.org/10.1155/2021/6641247>

15. Medykovsky, M., Lipinski, P., Troyan, O., & Nazarkevych, M. (2015, September). Methods of protection document formed from latent element located by fractals. *2015 Xth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT)*, 70–72. <https://doi.org/10.1109/STC-CSIT.2015.7325434>
16. Nazarkevych, M., Klyujnyk, I., Maslanych, I., Havrysh, B., & Nazarkevych, H. (2018, April). Image filtration using the Ateb-Gabor filter in the biometric security systems. *2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, 276–279. <https://doi.org/10.1109/MEMSTECH.2018.8365749>
17. Ng, A. Y. (2018). Machine learning yearning: Technical strategy for AI engineers, 118 p. URL: https://nessie.ilab.sztaki.hu/~kornai/2020/AdvancedMachineLearningNg_MachineLearningYearning.pdf
18. Olufemi, B., Bello, O., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques, applications, challenges, and opportunities. *Computer Science and Information Technology Research Journal*, 5(6), 1505–1520. <https://doi.org/10.51594/csitrj.v5i6.1252>
19. Osundare, O. (2024). Enhancing financial security in FinTech: Advanced network protocols for modern inter-bank infrastructure. *Finance & Accounting Research Journal*, 6, 1403–1415. <https://doi.org/10.51594/farj.v6i8.1384>
20. Qatawneh, A. M., Lutfi, A., & Al Barrak, T. (2023). Effect of artificial intelligence (AI) on financial decision-making: Mediating role of financial technologies (Fin-Tech). *HighTech and Innovation Journal*, 5(3). <https://doi.org/10.28991/HIJ-2024-05-03-015>
21. Ribeiro Pinto, J., Cardoso, J. S., & Lourenço, A. (2018). Evolution, current challenges, and future possibilities in ECG biometrics. *IEEE Access*, 6, 34746–34776. URL: <https://www.researchgate.net/publication/325934871>
22. Silver, D., Schrittwieser, J., & Hassabis, D. (2017). Mastering chess and Shogi by self-play with a general reinforcement learning algorithm. *Nature*, 550(7676), 354–359. <https://doi.org/10.1038/nature24270>
23. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2001)*, Kauai, HI, USA, 2001, I–I. <https://doi.org/10.1109/CVPR.2001.990517>
24. Yin, Y., He, S., Zhang, R., Chang, H., Han, X., & Zhang, J. (2023). Deep learning for iris recognition: A review. *arXiv:2303.08514* [cs.CV]. <https://doi.org/10.48550/arXiv.2303.08514>
25. Zhou, Z., Liu, Y., Zhu, X., Zhang, S., & Liu, Z. (2025). Privacy-preserving cancelable multi-biometrics for identity information management. *Information Processing & Management*, 62(1), article ID 103869. <https://doi.org/10.1016/j.ipm.2024.103869>

N. T. Oleksiv

Lviv Polytechnic National University, Lviv, Ukraine

USER IDENTIFICATION BASED ON IRIS RECOGNITION IN THE AUTOMATED MANAGEMENT SYSTEM

This study explores user identification within an automated budget management system for homeowner associations (HOAs) using biometric authentication based on iris recognition. The study is driven by the need to ensure a high level of security within collective management systems. Conventional authentication methods, such as passwords, often fail to meet modern security standards due to vulnerabilities like data breaches, loss, or human error. Leveraging biometric traits significantly enhances system protection by relying on the unique physiological characteristics of each individual. The architecture of the biometric identification system is presented, encompassing a database of biometric templates, as well as mechanisms for authentication and authorization. The proposed approach involves preprocessing iris images, segmenting key structural features, extracting distinctive attributes, and classifying them using neural networks. An iris recognition algorithm based on a modified ResNet-50 architecture was developed, achieving high accuracy and processing speed. The proposed system was experimentally evaluated using the publicly available CASIA-IrisV4 dataset. Results obtained in the course of research demonstrate that applying image augmentation techniques and specialized normalization algorithms improves the system robustness against noise, varying lighting conditions, and other external factors. The developed system is adaptable to other types of collective entities, such as community initiatives, charitable foundations, or coworking spaces, where transparency in financial transactions and protection of personal data are critical. Implementing iris-based biometric identification substantially reduces the risk of unauthorized access and fosters greater trust among community members.

Keywords: biometric identification; computer vision; authentication; authorization; financial transactions; neural networks; segmentation; augmentation.