УДК 004:681.3:004.738.5
DOI https://doi.org/10.32782/2521-6643-2024-2-68.5

Поперешняк С. В., кандидат фізико-математичних наук, доцент,
доцент кафедри інформатики та програмної інженерії
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-0531-9809

Кравченко Р. В., аспірант
Інституту програмних систем Національної академії наук України
ORCID: 0009-0005-8044-4414

Новіков Ю. Л., кандидат технічних наук,
старший науковий співробітник,
виконуючий обов'язки заступника завідувача відділом
автоматизованих систем програмно-цільового управління № 19
Інституту програмних систем Національної академії наук України
ORCID: 0009-0006-9800-8765

ДОСЛІДЖЕННЯ МЕТОДІВ РОЗПІЗНАВАННЯ ОСІБ ЗА БІОМЕТРИЧНИМИ ОЗНАКАМИ

Стаття присвячена аналізу сучасних технологій біометричної ідентифікації та їх використанню в різних сферах, таких як безпека, державні та комерційні організації. Основною метою дослідження є всебічне вивчення різних біометричних методів, таких як розпізнавання обличчя, відбитків пальців, райдужної оболонки ока, голосу та інших ознак, з подальшою розробкою рекомендацій щодо їх впровадження. В роботі проведено огляд сучасних методів біометричної ідентифікації, які активно використовуються в різних галузях. У статі досліджено оцінки точності та ефективності біометричних методів у різних умовах використання. Вивчено швидкість і обчислювальні витрати кожного методу, що дозволило порівняти їх за ефективністю. Частина дослідження фокусується на застосуванні методів машинного навчання та штучного інтелекту для покращення точності та швидкості біометричного розпізнавання. Використання глибоких нейронних мереж дозволяє досягати значних покращень у точності, особливо при роботі з великими наборами даних. Машинне навчання також допомагає адаптувати системи до різних умов використання, підвищуючи їх надійність і стійкість до спотворень. У статті запропоновано узагальнену математичну модель для вибору оптимального методу біометричної ідентифікації. Модель базується на багатокритерійному підході, що включає оцінку таких параметрів, як точність, швидкість, надійність, стійкість до зовнішніх впливів та обчислювальні витрати. Це дозволяє вибирати найбільш оптимальний метод для конкретних застосувань. На основі проведеного аналізу сформульовано рекомендації щодо впровадження біометричних систем. Розроблено рекомендації для безпеки, державних структур та комерційних організацій, що включають використання розпізнавання обличчя, відбитків пальців та комбінованих біометричних систем для підвищення ефективності і безпеки. Це дослідження робить внесок у розвиток технологій біометричної ідентифікації, забезпечуючи базу для подальшого впровадження ефективних рішень у різних галузях.

Ключові слова: *біометрична ідентифікація, розпізнавання обличчя, відбитки пальців, райдужна оболонка ока, розпізнавання голосу, алгоритм, метод, математична модель, рекомендації.*

Popereshnyak S. V., Kravchenko R. V., Novikov Yu. L. Research of personal identification methods by biometric characters

The article is devoted to the analysis of modern biometric identification technologies and their use in various areas, such as security, government and commercial organizations. The main goal of the research is a comprehensive study of various biometric methods, such as face recognition, fingerprints, iris, voice and other features, with further development of recommendations for their implementation. The paper provides an overview of modern biometric identification methods that are actively used in various industries. Algorithms for face recognition based on deep neural networks are considered, which provide high accuracy even in difficult conditions. In addition, fingerprint recognition methods are analyzed, which are widely used due to their availability and reliability. Iris and voice recognition have also been recognized for high accuracy and speed in specific conditions. The article examines assessments of the accuracy and effectiveness of biometric methods in various conditions of use. Important aspects are the quality of the input data (image or signal), lighting conditions, the presence of noise and other external factors that can affect the recognition results. The speed and computing costs of each method were also studied, which made it possible to compare their effectiveness. Part of the research focuses on applying machine learning and artificial intelligence techniques to improve the accuracy and speed of biometric recognition. The use of deep neural networks allows for significant improve-

ments in accuracy, especially when working with large data sets. Machine learning also helps to adapt systems to different usage conditions, increasing their reliability and resistance to distortions. The article proposes a generalized mathematical model for choosing the optimal method of biometric identification. The model is based on a multi-criteria approach, which includes the assessment of such parameters as accuracy, speed, reliability, resistance to external influences and computational costs. This allows you to choose the most optimal method for specific applications. Based on the analysis, recommendations were formulated for the introduction of biometric systems. Recommendations for security, government structures and commercial organizations have been developed, including the use of facial recognition, fingerprints and combined biometric systems to improve efficiency and security. This research contributes to the development of biometric identification technologies, providing a basis for further implementation of effective solutions in various industries.

Key words*: biometric identification, face recognition, fingerprints, iris, voice recognition, algorithm, method, mathematical model, recommendations.*

Постановка проблеми. В сучасному світі біометричні системи ідентифікації стали однією з найпопулярніших та найефективніших технологій для забезпечення безпеки та верифікації особистості. З розвитком цифрових технологій та зростанням кіберзагроз зростає потреба у більш надійних методах ідентифікації, які можуть забезпечити як зручність для користувачів, так і високий рівень безпеки для державних та комерційних структур. Традиційні способи ідентифікації, такі як паролі або PIN-коди, мають низький рівень захисту через вразливість до крадіжок та шахрайства. У зв'язку з цим, біометричні системи, що використовують унікальні фізіологічні або поведінкові характеристики особи (обличчя, відбитки пальців, голос, райдужна оболонка ока), стали важливою альтернативою для підтвердження особистості.

Попри численні переваги, біометричні системи стикаються з низкою проблем. Перша з них – це залежність точності від якості зібраних даних. Наприклад, системи розпізнавання обличчя можуть помилятися в умовах поганого освітлення або при частковому приховуванні обличчя (маски, окуляри). Друга проблема – це потреба в обчислювальних ресурсах для обробки біометричних даних, особливо при використанні глибоких нейронних мереж. Крім того, виклики з боку конфіденційності та захисту даних залишаються актуальними, оскільки біометрична інформація є надзвичайно чутливою і її компрометація може мати серйозні наслідки.

Таким чином, постає завдання дослідити сучасні методи біометричної ідентифікації, проаналізувати їх ефективність у різних умовах та розробити оптимальні рішення для впровадження цих систем в реальні умови, забезпечуючи при цьому високий рівень точності, надійності та захисту.

Стан дослідження. Огляд сучасної літератури та публікацій за останні роки по даній тематиці свідчить про активний розвиток різноманітних підходів до біометричної ідентифікації. Розглянемо кілька ключових напрямів, що активно досліджувалися останнім часом.

Останнє десятиліття відзначилося активним впровадженням глибоких нейронних мереж (DNN) в біометричні системи, що призвело до суттєвого покращення точності розпізнавання. Такі підходи використовуються для розпізнавання облич, відбитків пальців, райдужної оболонки ока та інших біометричних ознак. Наприклад, CNN (Convolutional Neural Networks) стали основою для побудови сучасних систем розпізнавання обличчя завдяки їх здатності автоматично виділяти ознаки зображень, що дозволяє досягати високої точності навіть у складних умовах [1-2].

Мультимодальні системи, що поєднують кілька біометричних ознак, отримали значний розвиток. Такі системи дозволяють підвищити точність і надійність розпізнавання, оскільки вони знижують вплив зовнішніх факторів, що можуть порушити роботу одномодальних систем [3-4].

Захист біометричних систем від підробок (наприклад, фотографій, підроблених відбитків пальців) та виявлення ознак живості користувача стали важливими напрямами досліджень. Алгоритми, що використовують машинне навчання, допомагають розпізнавати фальшиві біометричні дані шляхом аналізу таких факторів, як рух очей, текстура шкіри тощо [5-6].

Іншим важливим напрямом є розвиток легких алгоритмів для мобільних платформ, таких як смартфони та інші портативні пристрої. Впровадження ефективних алгоритмів для обробки біометричних даних на пристроях із обмеженими ресурсами стало викликом, який стимулював розвиток спеціалізованих рішень [7-8].

Ще одна проблема, яка активно досліджується, – це навчання нейронних мереж на малих наборах даних. Для цього використовуються спеціальні методи, такі як трансферне навчання, які дозволяють системам навчатися ефективно навіть за відсутності великих масивів даних для тренування [9].

Сучасні системи біометричного розпізнавання все частіше використовуються в нових контекстах, таких як інтернет речей (IoT) та віртуальні середовища (метавсесвіт). Це відкриває нові можливості для застосування біометрії в дистанційній ідентифікації та кібербезпеці, але водночас породжує нові виклики, пов'язані з безпекою та конфіденційністю даних [10].

За останні роки біометричні системи зробили великий крок уперед завдяки впровадженню глибокого навчання, мультифакторної ідентифікації та нових технологій захисту від підробок. Виклики, такі як робота на обмежених пристроях або навчання на малих наборах даних, поступово вирішуються за допомогою

нових алгоритмічних рішень. Розвиток цих систем має потенціал для подальшого впровадження в різних сферах, від безпеки до комерційних і державних послуг.

Метою дослідження є аналіз та порівняння методів розпізнавання осіб за біометричними ознаками, зокрема обличчям, відбитками пальців, райдужною оболонкою ока та іншими характеристиками. Дослідження спрямоване на виявлення найбільш ефективних та точних методів для використання в сучасних системах безпеки та ідентифікації.

Для досягнення поставленої мети сформулюємо задачі дослідження:

– Провести аналіз сучасних методів біометричної ідентифікації.

– Оцінити можливості використання методів машинного навчання та штучного інтелекту для покращення точності та швидкості біометричного розпізнавання.

– Дослідити та порівняти оцінки точності та ефективності методів.

– Побудувати узагальнену математичну модель для вибору оптимального методу розпізнавання осіб за біометричними ознаками.

– Розробити рекомендацій щодо впровадження біометричних систем.

Результати дослідження допоможуть удосконалити системи безпеки на основі біометричної ідентифікації та забезпечити ефективне впровадження таких технологій у різні галузі.

Виклад основного матеріалу дослідження.

Огляд сучасних методів біометричної ідентифікації. Біометрична ідентифікація використовує унікальні фізіологічні або поведінкові характеристики особи для підтвердження її особистості. Сучасні методи біометричної ідентифікації забезпечують високий рівень безпеки та точності, що робить їх популярними у сферах безпеки, доступу та контролю. В таблиці 1 наведено основні біометричні методи, які активно використовуються сьогодні.

Кожен метод біометричної ідентифікації має свої переваги і недоліки, залежно від конкретної сфери застосування. У сучасних системах безпеки все частіше використовуються комбінації кількох біометричних методів для підвищення точності та надійності ідентифікації.

Таблиця 1

Огляд сучасних методів біометричної ідентифікації

Метод	Сильні сторони	Недоліки	Застосування
Розпізнавання обличчя	Швидкість і зручність. Системи можуть використовуватися на відстані	Може бути менш ефективним у складних умовах освітлення або при зміні зовнішнього вигляду (маски, окуляри)	Верифікація доступу, системи відеоспостереження, смартфони (Face ID).
Розпізнавання відбитків пальців	Висока точність, широко поширений метод. Доступний навіть на недорогих пристроях.	Потрібен фізичний контакт з датчиком, що може бути незручним або викликати зношування при постійному використанні.	Смартфони, системи контролю доступу, банкомати.
Розпізнавання райдужної оболонки ока	Дуже висока точність, стійкість до підробки, стабільність малюнка протягом усього життя.	Потребує спеціалізованого обладнання і більш високих витрат на впровадження. Застосовується лише на невеликій відстані.	Високорівневі системи безпеки (військові об’єкти, банки, урядові структури).
Розпізнавання голосу	Може використовуватись дистанційно і є зручним для користувачів.	Відносно низька точність порівняно з іншими методами. Звуковий фон або зміни в голосі (хвороба, втома) можуть вплинути на точність розпізнавання.	Голосові асистенти, системи дистанційної верифікації.
Розпізнавання за відбитком долоні	Здатність розпізнавати на великій площі, використовується для високого рівня захисту.	Потребує фізичного контакту, що може обмежувати швидкість використання.	Контроль доступу в офісах, банках або інших захищених об’єктах.
Розпізнавання за венозним малюнком руки	Дуже висока стійкість до підробок, оскільки цей метод неможливо використати за допомогою знімків або інших зовнішніх даних.	Потребує дорогого обладнання та фізичного контакту з сенсором	Високозахищені об’єкти, урядові інституції, банки
Розпізнавання за динамікою руху	Можна використовувати безконтактно, підходить для постійного віддаленого моніторингу.	Низька точність порівняно з фізіологічними ознаками, залежить від умов середовища і може бути чутливою до зовнішніх змін	Системи безпеки на великих об’єктах, системи стеження.

Математичні моделі та алгоритми для біометричної ідентифікації особи

Для біометричної ідентифікації особи використовуються різні математичні моделі та алгоритми, які базуються на аналізі унікальних фізіологічних чи поведінкових характеристик людини. В таблиці 2 наведено основні моделі та алгоритми, які активно застосовуються в системах біометричної ідентифікації (Скорочення, які використані в таблиці 2: розпізнавання обличчя – РА, відбитки пальців – ВП, розпізнавання голосу – РГ, райдужна оболонка ока – РОО).

Короткий опис моделей та алгоритмів для біометричної ідентифікації особи.

1. Алгоритм PCA (Principal Component Analysis) – метод головних компонент. PCA є статистичним методом зниження розмірності даних, який перетворює вхідні дані на менший набір головних компонент.

2. Алгоритм LDA (Linear Discriminant Analysis) – лінійний дискримінантний аналіз. LDA знаходить лінії або гіперплощини, що найбільше розділяють класи, з метою максимізувати відмінності між класами і мінімізувати відмінності всередині одного класу.

3. Алгоритм Eigenfaces використовується для розпізнавання обличчя шляхом побудови базової моделі облич у вигляді лінійної комбінації еталонних зображень (eigenfaces).

4. Support Vector Machines (SVM) – метод опорних векторів. SVM є методом класифікації, який знаходить гіперплощину в багатовимірному просторі, що максимально розділяє класи (наприклад, різних осіб).

5. Алгоритми глибокого навчання DL (Deep Learning) – CNN (Convolutional Neural Networks). Конволюційні нейронні мережі (CNN) автоматично вчаться виділяти ключові характеристики з даних, таких як зображення обличчя або відбитків пальців.

6. K-Nearest Neighbors (KNN) – метод найближчих сусідів. В контексті біометрії, це може бути порівняння обличчя з іншими обличчями в базі.

7. Hidden Markov Models (HMM) – приховані моделі Маркова використовуються для розпізнавання голосу і ґрунтуються на ймовірнісному підході до аналізу послідовних даних.

Таблиця 2

Аналіз основних моделей та алгоритмів для біометричної ідентифікації осіб

Назва	Застосування	Переваги	Недоліки	Галузь застосування
Алгоритм PCA	РО	Ефективне зниження розмірності, що робить алгоритм швидшим і менш вимогливим до обчислювальних ресурсів	Менш стійкий до змін освітлення та поворотів обличчя	Системи безпеки, контроль доступу, ідентифікація в громадських місцях
Алгоритм LDA	РО, ВП	Краще справляється з класифікацією, ніж PCA, особливо коли йдеться про багатокласову проблему	Менш ефективний при великих змінах у даних, таких як варіації в позі або освітленні.	Розпізнавання осіб у системах відеоспостереження, безпеки в аеропортах.
Алгоритм Eigenfaces	РО	Простий та ефективний алгоритм для системи розпізнавання	Чутливий до змін в освітленні і виразі обличчя, потребує добрих вихідних зображень для якісної роботи	Розпізнавання у відеоспостереженні, банківських системах, смартфонах
SVM	РО, ВП, РГ	Висока точність, особливо при розпізнаванні складних класів, стійкість до «шуму» в даних	Потребує великого часу для навчання, складний у реалізації для великих систем	Системи високої безпеки, банки, державні системи контролю.
DL та CNN	РО, РОО, РГ, ВП	Висока точність навіть за наявності складних умов. Здатні працювати з великими наборами даних і навчатися складним шаблонам.	Вимагає великої кількості даних для навчання, а також значних обчислювальних ресурсів.	Високотехнологічні системи безпеки, смартфони, програми контролю доступу
KNN	РО, ВП	Простота реалізації та використання	Повільний при великих наборах даних, потребує великих обсягів пам’яті для зберігання даних	Невеликі системи розпізнавання, системи з обмеженими даними.
HMM	РГ	Добре справляються з послідовними даними, можуть моделювати природні зміни в голосі	Чутливі до «шуму», низька точність при обмежених даних	Голосові асистенти, системи безпеки на основі голосу.
DTRF	РО, РГ, РОО	Добре справляються з великими наборами даних, стійкі до перевчення (overfitting).	Можуть бути повільними на великих наборах даних, складні для інтерпретації.	Системи безпеки, аналіз даних у великих компаніях.

8. Decision Trees та Random Forests (DTRF) – дерева рішень та випадкові ліси. Дерева рішень використовують послідовні рішення для класифікації даних (наприклад, чи є це обличчя в базі даних).

Кожен з алгоритмів та моделей має свої переваги і недоліки в залежності від галузі застосування. Наприклад, PCA та Eigenfaces підходять для простих завдань розпізнавання обличчя, тоді як CNN та глибоке навчання забезпечують високу точність у складніших системах, які працюють з великими даними. Використання комбінованих методів, таких як Random Forests та CNN, може забезпечити оптимальне рішення для біометричної ідентифікації, що гарантує високу точність та ефективність.

Аналіз точності та ефективності різних біометричних методів. Для ефективного вибору біометричних методів ідентифікації важливо оцінити їхню точність, швидкість та надійність у різних умовах використання, таких як якість даних, зміни умов освітлення, положення тіла або зовнішній вигляд користувача. В таблиці 3 наведено основні методи біометричної ідентифікації та порівняння їх за цими показниками (Таблиця 3).

Таблиця 3

Порівняльний аналіз методів

Метод	Точність	Надійність	Швидкість	Умови використання
Розпізнавання обличчя	95-98%	Висока	Вразливий до зовнішніх змін	Чутливий до освітлення та зовнішнього вигляду
Відбитки пальців	97-99%	Висока	Надійний, але залежить від стану пальців	Потребує фізичного контакту
Райдужна оболонка ока	99.9%	Середня	Дуже надійний	Потребує близької відстані до сканера
Розпізнавання голосу	70-90%	Середня	Чутливий до шуму та зміни голосу	Залежить від якості запису і умов
Відбиток долоні	99%	Висока	Надійний, але контактний	Потребує фізичного контакту
Венозний малюнок руки	99.9%	Низька	Дуже надійний	Потребує спеціалізованого обладнання
Динаміка ходи	60-80%	Висока	Низька	Працює на великій відстані, чутливий до зовнішніх умов

Провівши порівняльний аналіз методів можна зробити наступні висновки:

– Найбільш точні методи: розпізнавання райдужної оболонки ока та венозного малюнка руки, оскільки вони забезпечують високу точність і надійність навіть у складних умовах.

– Найшвидші методи: розпізнавання обличчя та відбитків пальців – ці методи зручні для масового використання завдяки швидкості обробки даних.

– Універсальні методи: розпізнавання обличчя – один із найпоширеніших методів, але його точність знижується за несприятливих умов. Використання методів на основі відбитків пальців є добре інтегрованим у різні пристрої, але обмежується необхідністю фізичного контакту.

Для досягнення найкращих результатів можна використовувати комбінацію кількох біометричних методів, що дозволяє підвищити точність та надійність ідентифікації, особливо в складних умовах.

Оцінка можливостей використання машинного навчання та ШІ для біометричної ідентифікації. Розглянемо основні критерії покращення систем біометричної ідентифікації осіб та алгоритми які допоможуть цього досягти.

1. Підвищення точності. Алгоритми глибокого навчання, зокрема CNN і DNN, демонструють значно вищу точність, ніж традиційні методи, оскільки вони здатні вивчати складні патерни та ознаки з великих наборів даних. Рекурентні нейронні мережі (RNN) та їх варіанти (наприклад, LSTM) підвищують точність розпізнавання голосу та динаміки, оскільки вони можуть враховувати контекст послідовностей у даних.

2. Підвищення швидкості. Хоча CNN та DNN вимагають значних обчислювальних ресурсів для навчання, після тренування вони можуть виконувати розпізнавання в реальному часі, що робить їх ефективними для швидких рішень. Алгоритми KNN та SVM мають високу швидкість на етапі ідентифікації, але можуть бути повільними при навчанні або при великій кількості даних.

3. Адаптація до складних умов. Машинне навчання (МН) дозволяє біометричним системам працювати в складних умовах, таких як зміни освітлення, часткові перешкоди або шум. Алгоритми МН можуть «навчатися» на таких умовах і коригувати свої результати. Використання методів регуляризації та навчання на великих обсягах даних дозволяє ШІ-системам розпізнавати обличчя або голос у несприятливих умовах.

4. Захист від підробок. Алгоритми автоенкодерів і CNN використовуються для виявлення підробок у біометричних даних. Методи машинного навчання, такі як SVM або глибокі мережі, можуть бути налаштовані для виявлення аномалій або підозрілих спроб доступу.

Як бачимо, методи МН та ШІ значно підвищують точність, швидкість і надійність біометричних систем розпізнавання. Вони дозволяють автоматизувати процеси виділення ознак, адаптуватися до змін у зовнішньому вигляді користувача та працювати в складних умовах. Глибокі нейронні мережі, конволюційні мережі та рекурентні мережі є найбільш перспективними для розвитку сучасних біометричних систем.

Узагальнена математична модель для вибору оптимального методу розпізнавання осіб за біометричними ознаками

Для побудови узагальненої математичної моделі вибору оптимального методу біометричної ідентифікації необхідно врахувати кілька основних параметрів, що впливають на ефективність кожного методу. Модель базується на багатокритерійному підході, де оцінюються різні фактори, такі як точність, швидкість, надійність, стійкість до зовнішніх впливів та обчислювальні витрати.

Розглянемо основні критерії для оцінки методів:

– Точність (Accuracy, A): точність методу вимірюється як частка правильних ідентифікацій серед усіх спроб ідентифікації.

– Швидкість (Speed, S): час, необхідний для обробки даних та прийняття рішення.

– Надійність (Reliability, R): стійкість методу до зовнішніх впливів, таких як зміна умов освітлення, шум, зміна зовнішності тощо.

– Обчислювальні витрати (Computational Cost, C): кількість ресурсів, необхідних для виконання алгоритму (включає вимоги до процесора, пам'яті, GPU тощо).

– Захист від підробок (Liveness Detection, L): здатність системи виявляти підроблені біометричні дані (наприклад, підроблені відбитки пальців або фотографії обличчя).

– Універсальність (Versatility, V): здатність методу адаптуватися до різних користувачів і різних умов використання.

Побудуємо модель оцінки ефективності методів. Нехай у нас є кілька методів біометричної ідентифікації $M_1, M_2, ..., M_n$, кожен з яких можна охарактеризувати набором критеріїв.

Позначимо:

– A_i – точність методу M_i,
– S_i – швидкість методу M_i,
– R_i – надійність методу M_i,
– C_i – обчислювальні витрати методу M_i,
– L_i – захист від підробок методу M_i,
– V_i – універсальність методу M_i.

Вводимо функцію ефективності методу $E(M_i)$, яка поєднує всі ці критерії у вигляді зваженої суми:

$$E(M_i) = \omega_A \cdot A_i + \omega_S \cdot S_i + \omega_R \cdot R_i + \omega_C \cdot \frac{1}{C_i} + \omega_L \cdot L_i + \omega_V \cdot V_i,$$

де ω_A, ω_S, ω_R, ω_C, ω_L, ω_V –вагові коефіцієнти для кожного з критеріїв, які відображають їхню важливість для конкретної задачі.

Наведемо пояснення критеріїв:

– Точність (A): Чим більша точність, тим кращий метод. Тому A_i входить у модель зі знаком плюс.

– Швидкість (S): Чим швидше метод, тим краще. Швидкість теж входить у модель зі знаком плюс.

– Надійність (R): Надійність означає стійкість методу до змін умов або атак, і це також позитивний критерій.

– Обчислювальні витрати (C): Чим менші обчислювальні витрати, тим кращий метод. Тому C_i входить у модель з оберненою величиною $\frac{1}{C_i}$.

– Захист від підробок (L): Чим більший рівень захисту від підробок, тим кращий метод.

– Універсальність (V): Універсальні методи, що добре працюють за різних умов та для різних користувачів, також мають вищу цінність.

Щоб критерії були порівнюваними, їх потрібно нормалізувати до інтервалу [0, 1]. Для кожного критерію вводимо нормалізовані значення:

$$A_i^{norm} = \frac{A_i - A_{min}}{A_{max} - A_{min}},$$

$$S_i^{norm} = \frac{S_i - S_{min}}{S_{max} - S_{min}},$$

$$R_i^{norm} = \frac{R_i - R_{min}}{R_{max} - R_{min}},$$

$$C_i^{norm} = \frac{C_{max} - C_i}{C_{max} - C_{min}},$$

$$L_i^{norm} = \frac{L_i - L_{min}}{L_{max} - L_{min}},$$

$$V_i^{norm} = \frac{V_i - V_{min}}{V_{max} - V_{min}}.$$

Загальна функція ефективності після нормалізації:

$$E(M_i) = \omega_A A_i^{norm} + \omega_S S_i^{norm} + \omega_R R_i^{norm} + \omega_C C_i^{norm} + \omega_L L_i^{norm} + \omega_V V_i^{norm}.$$

Метод з найбільшим значенням $E(M_i)$ буде вважатися оптимальним для конкретного застосування. Таким чином, вибір оптимального методу зводиться до знаходження максимуму функції ефективності:

$$M_{opt} = \arg\max_{M_i} E(M_i)$$

Вагові коефіцієнти ω_A, ω_S, ω_R, ω_C, ω_L,ω_V визначаються залежно від вимог до системи і можуть змінюватися в залежності від застосування. Наприклад:

– У системах безпеки пріоритетом може бути точність та захист від підробок, тому ω_A і ω_L будуть вищими.

– У комерційних системах, де важливі швидкість та низькі обчислювальні витрати, ваги ω_S і ω_C можуть бути більшими.

Запропонована математична модель дозволяє вибрати оптимальний метод біометричної ідентифікації на основі багатокритеріального аналізу. За допомогою зважених коефіцієнтів модель враховує точність, швидкість, надійність, обчислювальні витрати, захист від підробок та універсальність кожного методу. Це дозволяє гнучко налаштовувати модель для конкретних умов і завдань, забезпечуючи оптимальний вибір методу для різних сценаріїв використання.

Рекомендації щодо впровадження біометричних систем

На основі аналізу ефективності біометричних методів розпізнавання осіб можна запропонувати кілька рекомендацій щодо їх впровадження в різних сферах – безпеки (таблиця 4), державних структур (таблиця 5) та комерційних організацій (таблиця 6).

Таблиця 4.

Рекомендації для сфери безпеки

Метод	Рекомендація	Оптимізація
Розпізнавання обличчя з використанням глибоких нейронних мереж (CNN)	Використовувати системи розпізнавання обличчя на основі CNN для забезпечення безконтактної ідентифікації. Ці системи добре підходять для великих об'єктів (аеропорти, вокзали), де потрібно швидко обробляти великий потік людей.	Використовувати багатошарову модель для врахування різних змін зовнішності, таких як зачіски, окуляри або маски. Інтегрувати системи захисту від підробок, наприклад, для виявлення фальшивих облич (фотографій або 3D-моделей).
Розпізнавання райдужної оболонки ока для об'єктів високого рівня безпеки	Використовувати розпізнавання райдужної оболонки ока на об'єктах з підвищеними вимогами до захисту (військові бази, банківські сховища, урядові установи	Інтеграція із системами доступу з мультифакторною аутентифікацією для забезпечення максимального захисту. Використання інфрачервоного сканування для зменшення впливу зовнішніх факторів

Рекомендації базуються на потребах кожної сфери, а також на особливостях біометричних методів, таких як розпізнавання обличчя, відбитків пальців, райдужної оболонки ока тощо.

Сфера безпеки вимагає високого рівня точності та надійності біометричних систем, оскільки вони повинні працювати в умовах підвищених ризиків і забезпечувати захист від підробок та несанкціонованого доступу.

Державні структури потребують стабільних, надійних і масштабованих рішень, що можуть працювати з великим обсягом даних (Таблиця 5). Такі системи повинні забезпечувати високий рівень безпеки, конфіденційності та відповідати законодавчим вимогам.

Комерційні структури потребують гнучких, економічно доцільних та легко інтегрованих рішень для підвищення зручності та безпеки (Таблиця 6). Біометрія може бути застосована для аутентифікації клієнтів, підвищення зручності при розрахунках та захисту від шахрайства.

Таблиця 5

Рекомендації для державних структур

Метод	Рекомендація	Оптимізація
Використання відбитків пальців для державних служб	Для систем ідентифікації громадян (паспорти, посвідчення особи, надання державних послуг) варто використовувати розпізнавання відбитків пальців, оскільки це добре інтегрований і надійний метод.	Використовувати захищені бази даних для зберігання відбитків пальців. Інтегрувати в мобільні додатки для забезпечення зручного доступу до державних послуг.
Системи розпізнавання обличчя для контролю доступу та безпеки	Використовувати системи розпізнавання обличчя для контролю доступу до урядових будівель і зони підвищеної безпеки	Встановлення камер з високою роздільною здатністю та системою глибокого навчання для зниження ймовірності помилкової ідентифікації
Інтеграція біометричних систем з державними електронними сервісами	Використовувати біометричні дані для аутентифікації громадян у системах електронного врядування	Розробити уніфіковану платформу для збору і зберігання біометричних даних, яка буде використовуватися для різних державних послуг (видача документів, доступ до соціальних послуг тощо)

Таблиця 6

Рекомендації для комерційних організацій

Метод	Рекомендація	Оптимізація
Розпізнавання обличчя для рітейлу та фінансових послуг	Використовувати технологію розпізнавання обличчя для аутентифікації клієнтів у банках або при здійсненні покупок в магазинах (безконтактні платежі)	Інтегрувати з мобільними додатками для здійснення безконтактних платежів. Використовувати системи глибокого навчання для виявлення шахрайства або несанкціонованого доступу
Використання біометрії для лояльності клієнтів та персоналізації	Використовувати біометричні системи для персоналізації обслуговування клієнтів (рітейл, готелі, ресторани). Наприклад, розпізнавання обличчя можна використовувати для автоматичного привітання клієнтів або пропонування персоналізованих послуг	Впроваджувати біометричні системи як частину програм лояльності для ідентифікації постійних клієнтів

Впровадження біометричних систем повинно бути адаптоване до конкретних умов використання, забезпечуючи баланс між точністю, безпекою і зручністю для кінцевих користувачів. Це дозволить розширити їхнє застосування в різних сферах – від систем безпеки до комерційних та державних послуг.

Висновки. У даній статті було проаналізовано сучасні підходи до біометричної ідентифікації, такі як розпізнавання обличчя, відбитків пальців, райдужної оболонки ока, та голосу. Проведений аналіз продемонстрував, що кожен із методів має свої переваги і недоліки, які впливають на точність та надійність у різних умовах. Так, системи розпізнавання обличчя на основі глибоких нейронних мереж забезпечують високу точність, але залежать від умов освітлення, тоді як методи розпізнавання відбитків пальців та райдужної оболонки демонструють високу надійність, проте потребують спеціального обладнання для збирання даних.

Одним з ключових результатів дослідження є побудова узагальненої математичної моделі вибору оптимального методу біометричної ідентифікації. Модель базується на багатокритерійному підході, де оцінюються різні фактори, такі як точність, швидкість, надійність, стійкість до зовнішніх впливів та обчислювальні витрати. Окрім цього, досліджено методи машинного навчання, які суттєво підвищують точність та швидкість біометричної ідентифікації, особливо при використанні глибоких нейронних мереж (CNN, RNN). Впровадження таких технологій дозволяє адаптувати системи до різних умов і забезпечувати надійність в режимі реального часу.

На основі проведеного аналізу сформульовано рекомендації щодо впровадження біометричних систем. Розроблено рекомендації для безпеки, державних структур та комерційних організацій.

Подальші дослідження в галузі біометричної ідентифікації мають зосередитися на кількох важливих напрямках:

Розвиток мультимодальних біометричних систем. Поєднання кількох біометричних ознак (наприклад, обличчя і відбитків пальців) може підвищити точність та надійність систем, особливо в умовах, де один з методів може працювати ненадійно.

Покращення захисту від підробок і спроб шахрайства. Розвиток методів виявлення живості користувача (liveness detection) для захисту від атак з використанням фальшивих даних залишається актуальним питанням для підвищення безпеки біометричних систем.

Оптимізація обчислювальних витрат. Важливо продовжити роботу над полегшенням алгоритмів машинного навчання для забезпечення їх ефективної роботи на мобільних платформах і пристроях з обмеженими ресурсами.

Ці напрями досліджень дозволять створювати більш адаптивні, надійні та безпечні системи розпізнавання, які зможуть ефективно працювати в широкому спектрі застосувань – від систем контролю доступу до використання в мобільних додатках і державних структурах.

Список використаних джерел:

1. Minaee S., Abdolrashidi A., Su H. Biometrics recognition using deep learning: a survey. *Artificial Intelligence Review*. 2023. № 56, P. 8647–8695.
2. Ghilom M. Latifi S. The Role of Machine Learning in Advanced Biometric Systems. *Electronics.* 2024. № 13(13), P. 26-67
3. Wang Y., He Z., Wang C., Wei J., Ren M. Biometric Recognition: Latest Advances and Prospects. *Electronics*. URL: https://www.mdpi.com/journal/ electronics/special_issues/RIVJJ1NSVM (дата звернення 25.09.2024).
4. Shaheed K., Mao A., Qureshi I. A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends. *Archives of Computational Methods in Engineering*. 2021. № 28, P. 4917–4960.
5. Wu W., Li Y, Zhang Y. Identity Recognition System Based on Multi-Spectral Palm Vein Image. *Electronics*. 2023, № 12(16), P. 3503;
6. Kamiński K., Piotr A. Dobrowolski, Piotrowski Z., Ścibiorek P. Enhancing Web Application Security: Advanced Biometric Voice Verification for Two-Factor Authentication. *Electronics*. 2023. № 12(18), P. 3791;
7. Haware S, Barhatte A Retina based biometric identification using SURF and ORB feature descriptors. In: *2017 international conference on microelectronic devices, circuits and systems, ICMDCS 2017*. 2017. pp 1–6
8. Heinsohn D, Villalobos E, Prieto L, Mery D. Face recognition in low-quality images using adaptive sparse representations. *Image and Vision Computing*. 2019. № 85. P. 46–58.
9. Hofbauer H, Jalilian E, Uhl A. Exploiting superior CNN-based iris segmentation for better recognition accuracy. *Pattern Recognition Letters*. 2019. № 120. P.17–23.
10. Keilbach P., Kolberg J., Gomez-Barrero M., Busch C., Langweg H. Fingerprint presentation attack detection using laser speckle contrast imaging. In: *2018 international conference of the biometrics special interest group,* 2018. pp 1–6.

References:

1. Minaee S., Abdolrashidi A., Su H. (2023) Biometrics recognition using deep learning: a survey. *Artificial Intelligence Review*, no. 56, pp. 8647–8695.
2. Ghilom M. Latifi S. (2024) The Role of Machine Learning in Advanced Biometric Systems. *Electronics*, no 13(13), pp. 26-67
3. Wang Y., He Z., Wang C., Wei J., Ren M. (2024) Biometric Recognition: Latest Advances and Prospects. *Electronics*. URL: https://www.mdpi.com/journal/ electronics/special_issues/RIVJJ1NSVC.
4. Shaheed K., Mao A., Qureshi I. (2021) A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends. *Archives of Computational Methods in Engineering*, no. 28, pp. 4917–4960.
5. Wu W., Li Y, Zhang Y. (2023) Identity Recognition System Based on Multi-Spectral Palm Vein Image. *Electronics*, no. 12(16), pp. 3503;
6. Kamiński K., Piotr A. Dobrowolski, Piotrowski Z., Ścibiorek P. (2023) Enhancing Web Application Security: Advanced Biometric Voice Verification for Two-Factor Authentication. *Electronics*, no. 12(18), pp. 3791;
7. Haware S, Barhatte A (2017) Retina based biometric identification using SURF and ORB feature descriptors. In: *2017 international conference on microelectronic devices, circuits and systems, ICMDCS 2017*. 2017. pp 1–6
8. Heinsohn D, Villalobos E, Prieto L, Mery D. (2019) Face recognition in low-quality images using adaptive sparse representations. *Image and Vision Computing*, no. 85. pp. 46–58.
9. Hofbauer H, Jalilian E, Uhl A. (2019) Exploiting superior CNN-based iris segmentation for better recognition accuracy. *Pattern Recognition Letters*, no. 120, pp.17–23.
10. Keilbach P., Kolberg J., Gomez-Barrero M., Busch C., Langweg H. (2018) Fingerprint presentation attack detection using laser speckle contrast imaging. In: *2018 international conference of the biometrics special interest group,* pp 1–6.