Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

XIII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

27-28 листопада 2025 р.

У двох частинах
Частина 2

Миколаїв ■ НУК ■ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2025

МАТЕРІАЛИ

XIII Всеукраїнської науково-технічної конференції з міжнародною участю

27–28 листопада 2025 року

У двох частинах
Частина 2

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2025

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XIII Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2025. – Ч. 2. – 100 с.

У збірнику подано матеріали XIII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ РОЗПІЗНАВАННЯ ОЗНАК В БІОМЕТРИЧНИХ СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Автор: *Гальченко О.Л., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Біометричні системи контролю доступу (БСКД) швидко розповсюджуються в завдяки зручності та потенційно високій надійності реалізованої в них багатофакторної автентифікації. Розробці БСКД присвячені роботи багатьох вітчизняних та іноземних фахівців [1-12].

Водночас різні методи розпізнавання біометричних ознак (feature-based, шаблонні, статистичні, нейромережеві, зокрема, глибинного навчанняі – deep learning) передбачають використання різних математичних апаратів та алгоритмів і мають принципово різні показники якості (точність, що характеризується багатьма показниками, стійкість до завад і атак, вимоги до обчислювальних ресурсів і приватності тощо). Стрімкий розвиток обчислювальної техніки, інформаційних технологій і датчиків біометричних ознак зумовлюють лавиноподібний розвиток підходів, методів і методик виявлення біометричних ознак і розпізнавання осіб в БСКД.

Метою даної роботи є порівняльний аналіз основних сучасних підходів до виділення та розпізнавання біометричних ознак у БСКД.

Для досягнення даної мети необхідно вирішити наступні **задачі**:

– провести комплексний аналіз сучасних БСКД і визначити множину методів, для яких буде проводитися порівняння;

– визначити критерії порівняння реалізованих у відібраних методах підходів до виділення та розпізнавання біометричних ознак;

– провести порівняльний аналіз визначених підходів до виділення та розпізнавання біометричних ознак у БСКД за визначеними критеріями.

Для аналізу були обрані БСКД, що працюють на різних біометричних ознаках (ознаки обличчя особи, відбитків пальців, райдужної оболонки ока) та мультимодальні системи. До уваги були прийняті огляди нейромереж глибокого навчання в біометрії, класичні дослідження з локальних бінарних шаблонів (англ. Local Binary Patterns, LBP) та звіти NIST щодо продуктивності систем розпізнавання облич [1-12]. Як показав комплексний аналіз сучасних БСКД, на поточний час найбільш популярними для розпізнавання осіб за біометричними ознаками є:

– класичні дескриптори й алгоритми (характеристики для відбитків, фільтри Delaunay/Gabor, детектори SIFT (англ. scale-invariant feature transform) та ORB (англ. (Oriented FAST and Rotated BRIEF) для зображень);

– текстурно-локальні методи, такі як LBPі дескриптори особливих точок, (Histogram of Oriented Gradients, HOG);

– статистичні підходи, зокрема, метод головних компонент (principal component analysis, PCA) і лінійний дискримінантний аналіз (англ. Linear Discriminant Analysis, LDA) як методи зменшення розмірності/побудови шаблонів;

– підходи на основі загорткових нейромереж (англ. convolutional neural network, CNN) і поглибленого навчання з врахуванням спеціалізованих архітектур для облич, відбитків пальців, райдужки ока);

– мультибіометричні та мультимодальні підходи з рівнями злиття (англ. fusion).

Для порівняння підходів до виділення та розпізнавання біометричних ознак у БСКД обрано наступні критерії:

– точність та стабільність результатів;
– стійкість до спуфінгу та підробок ознак;
– вимоги до обчислювальних ресурсів;
– масштабованість і обслуговування бази зразків;
– приватність та законодавчі обмеження.

Порівняння підходів, реалізованих в сучасних БСКД для виділення та розпізнавання біометричних ознак, за визначеними критеріями дозволяє зробити наступні висновки/

CNN забезпечують значне підвищення точності в задачах розпізнавання облич і райдужної оболонки порівняно з класичними дескрипторами [4, 5, 8-11], що підтверджується оглядовими роботами про

застосування глибинного навчання (англ. deep learning) у біометрії. Проте в умовах обмежених даних або сильних викривлень прості локальні дескриптори (наприклад, LBP) можуть давати конкурентні результати завдяки інваріантності до локальних змін освітлення і простоті реалізації [5].

Шаблонні методи, що використовують лише однорідні дані (наприклад, 2D-зображення обличчя), є вразливими до високоякісних підробок фото і відео зображень [2, 3, 12]. Методи глибокого навчання дозволяють додавати модулі детекції фальсифікацій (anti-spoofing), але загальна стійкість зростає суттєво при мультибіометричному підході (поєднання декількох модальностей) — саме злиття дає найкращий баланс безпеки й точності, хоч і підвищує складність системи [1, 2, 5, 7].

Класичні алгоритми (LBP, PCA, продуктивні алгоритми за шаблоном) зазвичай мають низькі вимоги до обчислювальних ресурсів і при пеіних умовах здатні працювати в реальному часі, що робить їх придатними для вбудованих пристроїв доступу. Натомість глибинні моделі потребують значних ресурсів при навчанні та, в багатьох випадках, при виконанні їх алгоритмів (хоча мобільні оптимізації й квантування помітно зменшують ці вимоги). Практично перевірено [5], що з точки зору мінімізації вимог до обчислювальних ресурсі і швидкодії ефективним є використання гібридних архітектур, в яких локальні швидкі дескриптори використовуються на точках збирання ознак, а серверні нейромережі – для остаточної верифікації.

Для великих баз (на підприємствах чи в державних реєстрах) критичним є час пошуку образу в пам'яті, масштабованість БСКД, забезпечення зручності і коректності введення і видалення даних з бази образів. Звіти NIST [6, 7] демонструють, що реалізації сучасних алгоритмів різняться за масштабованістю та ймовірністю хибно-позитивного знаходження; вибір алгоритму має враховувати компроміс між точністю і швидкістю пошуку.

Зберігання біометричних шаблонів викликає серйозні ризики приватності. Методики, що зберігають відновлювані шаблони (англ. plaintext templates), потребують додаткового шифрування або використання приватних багатосторонніх протоколів / гомоморфного

порівняння. Технічно сприятливі підходи — збереження хешованих/бінаризованих неповторних шаблонів або застосування федеративного навчання при БСКД в розподілених системах [3].

Для критичних застосувань контролю доступу в статті [8] рекомендовано мультимодальний підхід з поєднанням принаймні двох різних сенсорних модальностей (наприклад, відбиток + обличчя або райдужка + обличчя) і злиттям на рівні ознак/рішень; це підвищує стійкість до атак і зменшує помилки.

У сценаріях з обмеженими ресурсами доцільно застосовувати локальні дескриптори (LBP, HOG) в комбінації з легкими класифікаторами, а при наявності серверної інфраструктури — слід інтегрувати CNN для остаточної ідентифікації [4].

Згідно з фреймворками NIST [6, 7] необхідно впроваджувати механізми захисту шаблонів (шифрування, біометричні ключі) та проводити регулярні тестування продуктивності й упередженості алгоритмів.

Висновки. В даній роботі на основі інформації з відкритих джерел проведено комплексний аналіз сучасних БСКД, визначена множина методів, доцільних для порівняння, критерії порівняння реалізованих у відібраних методах підходів до виділення та розпізнавання біометричних ознак, проведено порівняльний аналіз підходів визначених підходів за обраними критеріями.

Отримані результати є обґрунтованими теоретично і в конкретних умовах експлуатації БСКД мають бути перевірені на реальних наборах даних із тестуванням проти спуфінгу.

Список літератури:

1. Abdo A.A., Lawgali A.O., Abdalla M.A.E. A Review of the Iris Recognition Methods Used for the Individual Authentication. Transactions on Machine Learning and Artificial Intelligence. 2021. Vol.8. No.6. P.16-26. DOI: 10.14738/tmlai.86.9687. URL: http://dx.doi.org/10.14738/tmlai.86.9687

2. Face Recognition Technology Evaluation (FRTE) 1:1 Verification. URL: https://pages.nist.gov/frvt/html/frvt11.html

3. Guo Y., Mu H., Liu X., Ren H., Han C. Federated learning for biometric recognition: a survey. The Artificial Intelligence Review. 2024. Vol.57. Issue 8. DOI:10.1007/s10462-024-10847-7. URL: https://link.springer.com/article/10.1007/s10462-024-10847-7?utm_source=chatgpt.com

4. Huang D., Shan C., Ardabilian M., Wang Y., Chen L. Local Binary Patterns and Its Application to Facial Image Analysis: A Survey. IEEE Transactions on Systems, Man, and Cybernetics, Part C. 2011. Vol.41. P.765-781. URL: https://liris.cnrs.fr/Documents/Liris-5004.pdf liris.cnrs.fr

5. Minaee S., Abdolrashidi A., Su H., Bennamoun M., Zhang D. — Biometrics Recognition Using Deep Learning: A Survey. arXiv. 2021. P.1-32. URL: https://arxiv.org/abs/1912.00271

6. NIST – Face Recognition Vendor Test (FRVT). URL: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt NIST

7. NISTIR 8381 Face Recognition Vendor Test (FRVT) Part 7: Identification for Paperless Travel and Immigration. URL: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8381.pd

8. Purohit H., Pawan K Ajmera P.K. Multimodal Biometric Systems: A Brief Study. // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019. Vol.8. Issue 7. P.108-111. URL: https://www.ijitee.org/wp-content/uploads/papers/v8i7/F3796048619.pdf

9. Дадиверін В.В., Фещенко І.О., Потапова К.Р., Тарасенко-Клятченко О.В., Івасенко Д.В. Система розпізнавання обличчя з використанням поєднання методів HAAR ta SVM. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2022. Том 33 (72). №6. С.86-91. DOI https://doi.org/10.32782/2663-5941/2022.6/15. URL: https://www.tech.vernadsky journals. in.ua/journals/2022/6_2022/15.pdf

10. Максименко Д., Шкурат О., Дичка, А. Методи глибинного навчання для розпізнавання облич, візуалізованих в умовах недостатнього освітлення на основі моделі MOBILENETV2. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025. Том.355. №4. С.335-341. URL: https://doi.org/10.31891/307-5732-2025-355-48

11. Стасєв Ю.В., Гончаренко К.Г., Мороз В.І. Аналіз методу багатофакторної аутентифікації користувачів інформаційних систем на основі райдужної оболонки ока. Системи обробки інформації. 2023. Вип. (174). С.63-69. DOI: 10.30748/soi.2023.174.09. URL: https://journal-hnups.com.ua/index.php/soi/article/download/1482/1350/

12. Хенк Е. Прості методи розпізнавання облич. URL: https://gijn.org/ua/resurs-ua/prosti-metodi-rozpiznavanna-oblic/

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2025

XIII Всеукраїнська науково-технічна конференція
з міжнародною участю

27–28 листопада 2025 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

У двох частинах
Частина 2

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич
