

В. О. КУРЕНКО

аспірант кафедри інфокомунікаційної інженерії імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0009-0006-6269-2390

Д. В. АНДРУШКО

кандидат технічних наук,
старший викладач кафедри інфокомунікаційної інженерії
імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0009-0004-0749-9729

С. В. ПШЕНИЧНИХ

кандидат технічних наук, старший науковий співробітник,
доцент кафедри інфокомунікаційної інженерії імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-0533-2306

СИСТЕМА АВТЕНТИФІКАЦІЇ ЗА ОБЛИЧЧЯМ З ВИКОРИСТАННЯМ ТРАНСФЕРНОГО НАВЧАННЯ НЕЙРОННИХ МЕРЕЖ

Використання згорткових нейронних мереж у процесі аналізу зображень мало вплив і на системи біометричної автентифікації за обличчям, які відіграють важливу роль у забезпеченні інформаційної безпеки. Сучасні моделі для вирішення цієї задачі досягають високої точності, та мають складну архітектуру, що потребує багато часу на проектування. Застосування трансферного навчання сприяє спрощенню процесу тренування моделей нейронних мереж, забезпечуючи при цьому достатньо високий рівень точності. В роботі запропоновано підхід до побудови систем автентифікації особи за обличчям, в межах якого використано попередньо навчену модель згорткової нейронної мережі, яка за рахунок використання трансферного навчання була адаптована під задачу автентифікації особи за обличчям. Такий підхід спрощує процес проектування архітектури нейронної мережі та значно скорочує час на її навчання. В ході дослідження було розроблено дві архітектури згорткової нейронної мережі, які відрізнялись налаштуванням шарів базової моделі для вилучення ознак, кількістю повноз'язних шарів та їх параметрів, та методами регуляризації. Було зібрано два набори зображень обличчя, в подальшому вони були використані для навчання та тестування моделей нейронних мереж, отримано графіки залежності функції втрат від кількості епох в ході навчання, і виконано перевірку на тестовій підмножині. Для перевірки адекватності рішення було розроблено та протестовано прототип системи, отримана точність автентифікації висока на обох наборах зображень, тож запропонований підхід може використовуватись у реальних системах біометричної автентифікації за обличчям, а також потенційно може бути доповнений механізмами безпеки, наприклад модулем для перевірки підміни обличчя. Подальші дослідження в цьому напрямі пропонується спрямувати на вдосконалення методів попередньої обробки зображень з камери та доповнення навчального набору даних.

Ключові слова: біометрична автентифікація, розпізнавання обличчя, комп'ютерний зір, згорткові нейронні мережі, трансферне навчання, інформаційна безпека.

V. O. KURENKO

Postgraduate Student at the V. V. Popovskyy Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0009-0006-6269-2390

D. V. ANDRUSHKO

PhD, Senior Lecturer at the V. V. Popovskyy Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0009-0004-0749-9729

S. V. PSHENYCHNYKH

PhD, Senior Researcher,

Associate Professor at the V. V. Popovskyy Department
of Infocommunication Engineering

Kharkiv National University of Radio Electronics

ORCID: 0000-0003-0533-2306

FACE AUTHENTICATION SYSTEM USING TRANSFER LEARNING OF NEURAL NETWORKS

The use of convolutional neural networks in the process of image analysis has also had an impact on biometric face authentication systems, which play an important role in ensuring information security. Modern models for solving this problem achieve high accuracy and have a complex architecture that requires a lot of time to design. The use of transfer learning helps to simplify the process of training neural network models, while ensuring a sufficiently high level of accuracy. The paper proposes an approach to building face authentication systems, which uses a pre-trained convolutional neural network model, which was adapted to the face authentication task through the use of transfer learning. This approach simplifies the process of designing the neural network architecture and significantly reduces the time for its training. During the study, two convolutional neural network architectures were developed, which differed in the settings of the base model layers for feature extraction, the number of fully connected layers and their parameters, and regularization methods. Two sets of face images were collected, and subsequently they were used to train and test neural network models, graphs of the dependence of the loss function on the number of epochs during training were obtained, and verification was performed on the test subset. To verify the adequacy of the solution, a prototype of the system was developed and tested, the obtained authentication accuracy was high on both sets of images, so the proposed approach can be used in real biometric face authentication systems, and can also potentially be supplemented with security mechanisms, such as a module for checking face spoofing. Further research in this direction is proposed to be directed at improving the methods of pre-processing images from the camera and supplementing the training dataset.

Key words: biometric authentication, face recognition, computer vision, convolutional neural networks, transfer learning, information security.

Постановка проблеми

Враховуючи активний розвиток апаратних платформ для додатків штучного інтелекту, таких як графічні процесори та нейропроцесори, збільшення доступності та поширеності цифрових камер, а також успішні дослідження нейронних мереж, інтеграція додатків штучного інтелекту в людську діяльність є незворотним процесом. Розпізнавання обличчя, яке використовується у багатьох сферах, зокрема і для автентифікації особи, є широко відомим прикладом використання штучного інтелекту для підвищення рівня інформаційної безпеки [1]. Автентифікація особи за зображенням обличчя полягає у розпізнаванні за принципом «свій-чужий», шляхом порівняння вхідного вектора ознак з еталоном. Актуальні дослідження в цій галузі спрямовані на підвищення точності систем автентифікації, шляхом модифікації архітектур нейронних мереж, розробку нових функцій активації та втрат.

Існуючі методи автентифікації особи за обличчям покладаються на складні архітектури нейронних мереж зі специфічними функціями втрат. Такі рішення показують високу точність у складних тестових сценаріях. Однак, системи автентифікації особи можуть використовуватись і у більш простих умовах. Актуальною задачею є розробка методів автентифікації особи за обличчям, які забезпечують достатню точність, але використовують простіші архітектури нейронних мереж та функції втрат, що має спростити їх процес розробки і введення в експлуатацію.

Аналіз останніх досліджень і публікацій

Автентифікація є одним з застосувань розпізнавання обличчя, і складається з таких підзадач, як локалізація обличчя, вилучення ознак із зображення обличчя, та класифікація отриманих ознак. Відповідно до цього були сформовані окремі напрями досліджень, спрямовані на вдосконалення методів та засобів для їх вирішення. В рамках даної статті буде розглянуто останні дві підзадачі.

Ранні методи для вилучення ознак із зображення обличчя, такі як EigenFaces, FisherFaces, гістограма орієнтованих градієнтів, аналіз незалежних компонентів, мали низку обмежень, зокрема чутливість до змін освітлення, виразу обличчя, повороту голови [2–5]. Поява згорткових нейронних мереж для класифікації зображень відкривала нові перспективи для розпізнавання обличчя. На базі класичних та сучасних архітектур для класифікації зображень було розроблено чимало моделей для вилучення ознак обличчя. Так в роботі [6] пропонується сімейство легких архітектур згорткових нейронних мереж для розпізнавання обличчя, які засновані на базі GhostNetV1 [7] та GhostNetV2 [8]. В запропонованому рішенні було модифіковано шари мережі та функцію активації. Отримане рішення має точність, співмірну з існуючими моделями, що мають значно вищу обчислювальну складність.

Через деякий час після появи моделей згорткових нейронних мереж для розпізнавання обличчя, стала зрозумілою обмеженість існуючих функцій втрат, що вимірюють різницю між прогнозованим та фактичним значенням. Це викликало необхідність їх вдосконалення, чому була присвячена низка робіт [9–11]. В роботі [12] пропонується

адаптивна функція втрат, яка при тренуванні моделей нейронних мереж звертає увагу на неправильно класифіковані екземпляри даних, при цьому коригуючи цей процес шляхом врахування якості зображення, що в результаті покращує точність моделі. Автори [13] зазначають, що підходи, які були запропоновані в [10–11], не пристосовані до варіативності даних всередині класу та між різними класами в реальних наборах даних, що може обмежувати здатність до розрізнення та узагальнення у моделі, і пропонують гнучку функцію втрат, яка краще працює з такими особливостями даних, і покращує точність розпізнавання обличчя. В роботі [14] пропонується гібридна функція втрат на базі [11], застосування якої сприяє кращій дискримінаційності при навчанні згорткової нейронної мережі, внаслідок чого підвищується точність моделі.

Окрім цього, сформовано ще один напрям досліджень методів біометричної автентифікації за обличчям, спрямований на вирішення проблем безпеки. В роботах [15–16] було запропоновано схеми автентифікації із захистом даних. Однією з поширених проблем систем автентифікації за обличчям є підміна обличчя, шляхом демонстрації зображень і відео з легітимним користувачем, а також використанням діпфейків. Для подолання цих проблем запропоновано ряд методів для виявлення підміни обличчя та перевірки «активності» людини. Так в роботі [17] для перевірки запропоновано порівнювати фотоплетизмограми обличчя та кінчика пальця на руці. Для цього, при автентифікації на смартфоні одночасно ведеться зйомка з основної та фронтальної камер, що мають знімати обличчя та палець, і перевіряється узгодженість результатів аналізу отриманого відеоряду. А в роботі [18] запропоновано схему автентифікації, в якій для перевірки людини використовується модель машинного навчання для аналізу кадрів відеоряду. До того ж, замість періодичної автентифікації користувача, яка більш вразлива до атак, пропонується інтегрувати в систему функцію відстеження обличчя, де після його втрати автентифікація відбувається повторно. Для боротьби з підміною обличчя можуть застосовуватись не тільки камери, а й інші сенсори, зокрема мікрофони. В роботах [19–20] пропонується як разом з візуальними даними з камери, так і окремо, аналізувати відлуння звукового сигналу від людського обличчя.

Нерідко компрометація систем автентифікації за обличчям несе значні ризики для власників, тож сучасні дослідження направлені на захист від атак, та на підвищення точності розпізнавання обличчя, шляхом вдосконалення методів вилучення ознак та їх класифікації. Це призводить до уповільнення процесів розробки та розгортання таких систем, та збільшення їх вартості, що є не завжди виправданим.

Формулювання мети дослідження

Метою дослідження є зменшення часових витрат на побудову архітектури та навчання нейронної мережі для системи біометричної автентифікації за обличчям, забезпечуючи при цьому достатню точність.

Викладення основного матеріалу дослідження

З огляду на високий рівень точності моделей штучного інтелекту на базі згорткових нейронних мереж, запропоноване рішення спиралось саме на них. Типова структура згорткової нейронної мережі наведена на рисунку 1. Вона складається з двох частин: для вилучення ознак та для класифікації. Зображення проходить через множину шарів згортки та об'єднання, отримані ознаки зображення передаються у повнозв'язні шари для подальшої класифікації.

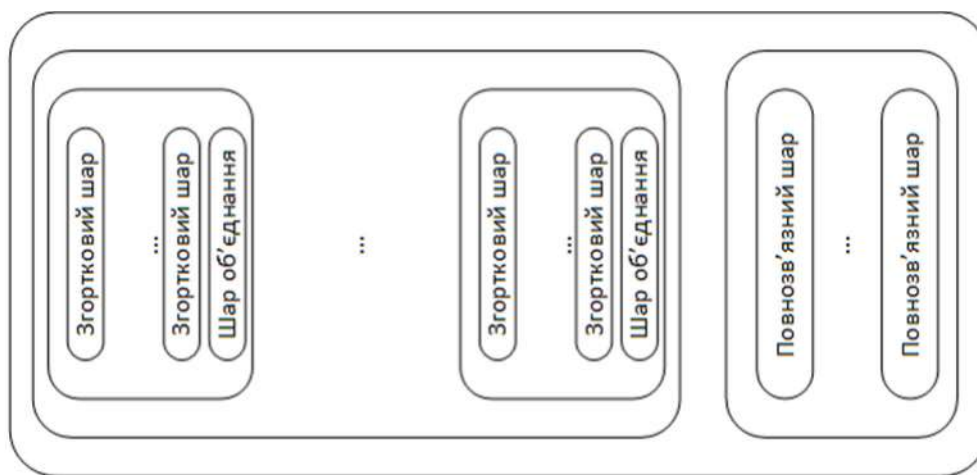


Рис. 1. Типова структура згорткової нейронної мережі

Згорткові шари є основним елементом мережі, призначені для виявлення особливостей зображення. Для цього використовується множина фільтрів, розмір яких зазвичай складає 3 на 3 пікселі, які переміщуються по зображенню ковзаючим вікном, і на кожному кроці відбувається розрахунок згортки. Отриманий результат передається на шар об'єднання, яке зазвичай буває максимальне або середнє, тобто на вихід передається найбільше або середнє значення з множини. Використання шарів об'єднання дозволяє зменшити розмірність даних, і сприяє

підвищенню стійкості моделі до зсувів та поворотів зображення. Після проходження останнього шару об'єднання, отримані ознаки зображення передаються на повнозв'язні шари для класифікації отриманих ознак зображення.

При реалізації моделі згорткової нейронної мережі було застосовано трансферне навчання, тобто знання отримані моделлю під час навчання на одному завданні, використовуються для швидкого та ефективного вирішення нового завдання, замість навчання моделі з нуля. Це спрощує процес проектування архітектури нейронної мережі та значно скорочує часові витрати на її навчання. До базової моделі, яка була попередньо навчена на наборі даних ImageNet [21], було додано шари, що тренувалися на невеликому наборі даних з обличчями. Для проведення дослідження було розроблено програму з використанням мови Python. В ході експерименту емпіричним шляхом було підібрано дві архітектури мережі (рис. 2).

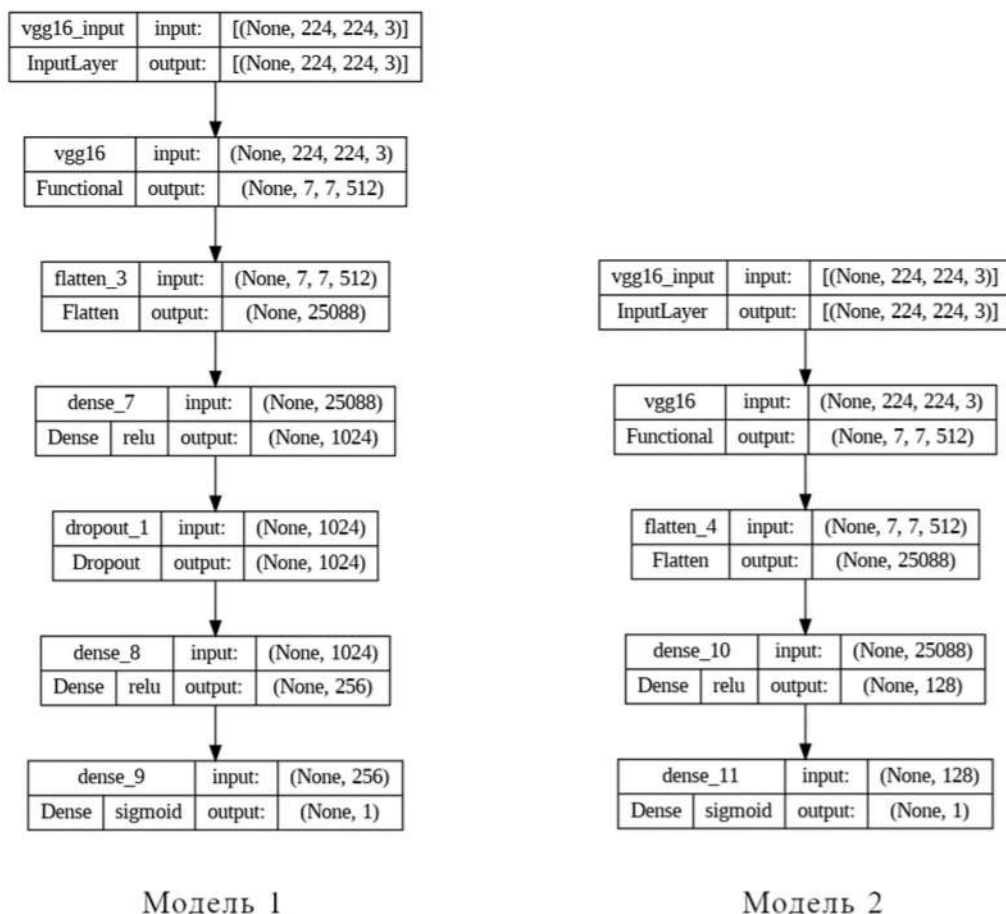


Рис. 2. Обрані архітектури мережі

Як базову було обрано модель VGG16 [22]. У першій моделі нейронної мережі, для вилучення ознак було використано всі п'ять блоків згортки-об'єднання базової моделі з підготовленими вагами. Кольорове зображення розміром 224 на 224 пікселі подавалось на вхід до згорткового шару першого блоку. З шару об'єднання останнього блоку, тривимірний масив даних передавався на шар Flatten для перетворення в одновимірний масив, і таким чином було сформовано ознаки зображення. Далі їх було передано на повнозв'язні шари для класифікації. Між першим і другим повнозв'язним шаром було встановлено шар Dropout для регуляризації в ході навчання мережі. На останньому повнозв'язному шарі використовувалась сигмоїдальна функція активації, яка повертає число від 0 до 1, за яким можна оцінити наближеність до класу «свій». У другій моделі нейронної мережі, для вилучення ознак також було використано всі п'ять блоків згортки-об'єднання базової моделі. Та на відміну від першої, у другій моделі шари п'ятого блоку згортки-об'єднання були доступними для навчання, що дозволяло краще враховувати специфічні для обличчя риси. Друга модель також відрізнялась простішою архітектурою класифікатора, було використано меншу кількість повнозв'язних шарів, регуляризація в мережі не застосовувалась.

В ході експерименту використовувалось два набори даних. Кожен набір складався з двох класів (рис. 3): у першому знаходилась одна особа, в другому – декілька чужих осіб. Також кожен набір було розділено на навчальну, валідаційну та тестову вибірки.

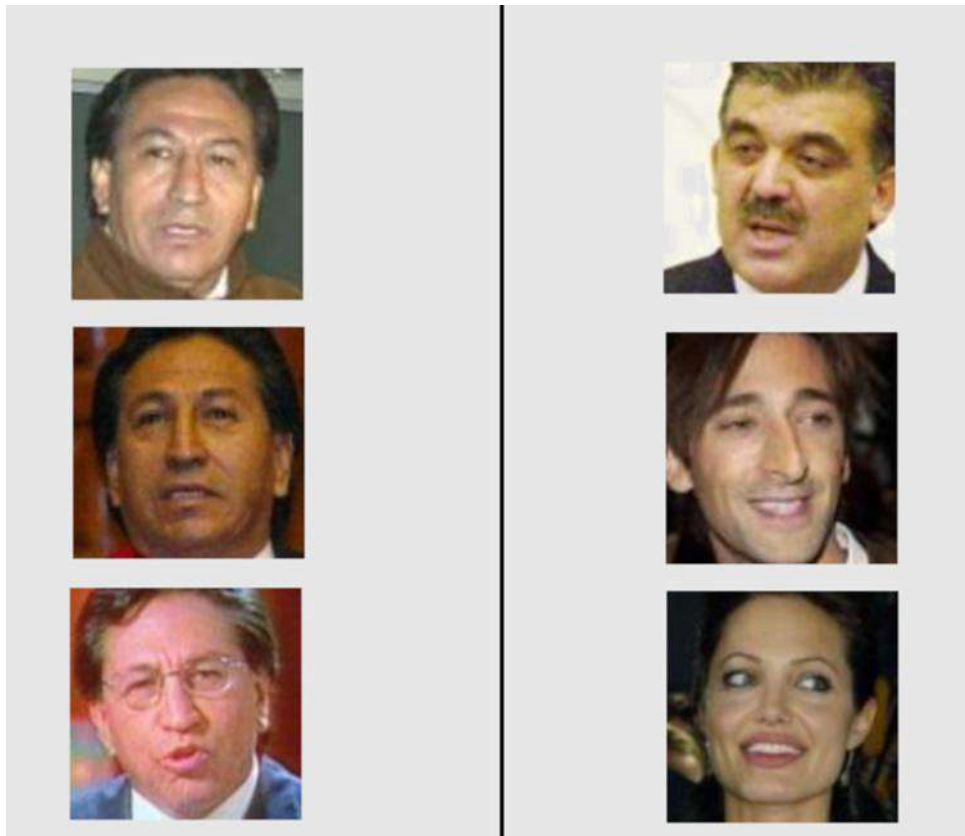


Рис. 3. Приклад зображень з другого набору даних

Перший набір даних було зібрано самостійно, з використанням камери. На рисунку 4 наведено графік залежності функції втрат від кількості епох для першої і другої моделі на тренувальній та валідаційній підмножині першого набору даних.

Другий набір даних було зібрано з набору зображень обличчя LFW [23]. На рисунку 5 наведено графік залежності функції втрат від кількості епох для першої і другої моделі на тренувальній та валідаційній підмножині другого набору даних.

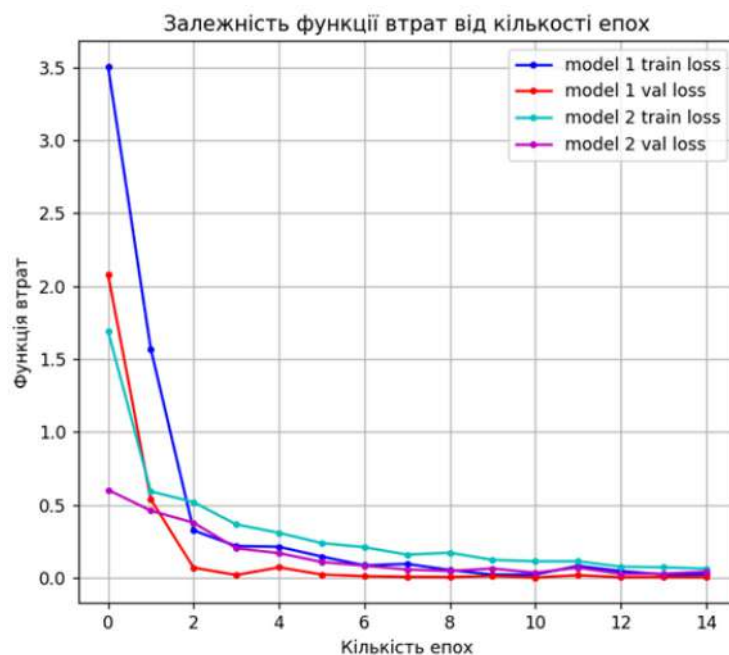


Рис. 4. Залежність функції втрат від кількості епох на першому наборі даних

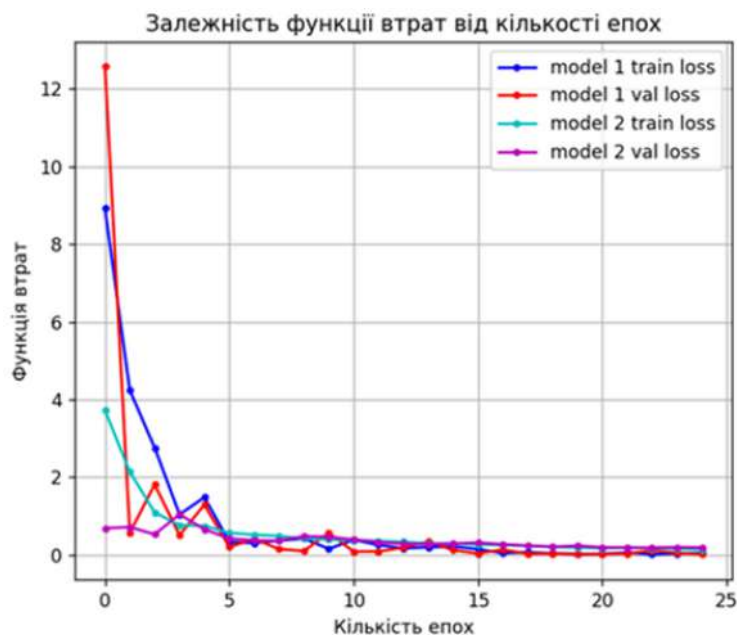


Рис. 5. Залежність функції втрат від кількості епох на другому наборі даних

Як видно з рисунків 4–5, в обох випадках функція втрат наближається до нуля. Отримані результати свідчать про успішне навчання усіх розглянутих моделей згорткових нейронних мереж і на першому, і на другому наборах даних, перенавчання та недонавчання моделей відсутні.

Також було проведено перевірку на тестових вибірках, яка продемонструвала високу точність запропонованих моделей як на першому, так і на другому наборах даних, що свідчить про адекватність та працездатність використаного підходу.

Висновки

За рахунок впровадження згорткових нейронних мереж, системи для автентифікації за обличчям показують високу точність роботи. В них використовуються складні моделі нейронних мереж, що потребують значних фінансових та часових витрат на розробку та розгортання, що не завжди є доцільним. Застосування трансферного навчання сприяє спрощенню процесу навчання моделей нейронних мереж, забезпечуючи при цьому достатньо високий рівень точності.

У статті запропоновано підхід до побудови систем автентифікації особи за обличчям. В його межах було використано попередньо навчену модель згорткової нейронної мережі, яка за рахунок використання трансферного навчання була адаптована під задачу автентифікації особи. Такий підхід пришвидшив процеси проектування архітектури та навчання нейронної мережі. Розроблений прототип системи було успішно протестовано на декількох наборах даних, підхід довів свою адекватність та працездатність, автентифікація особи відбувається з високою точністю. Перспективним напрямом подальших досліджень є методи доповнення навчального набору даних та попередньої обробки зображень з камери.

Список використаної літератури

1. Kortli Y., Jridi M., Al Falou A., Atri M. Face recognition systems: A survey. *Sensors*. 2020. Vol. 20, no. 2. P. 342. URL: <https://doi.org/10.3390/s20020342>
2. Turk M. A., Pentland, A. Face recognition using eigenfaces. *Computer Vision and Pattern Recognition : Proceedings of the IEEE Computer Society Conference, Maui, 03–06 June 1991*. Maui, 1991. P. 586–591. URL: <https://doi.org/10.1109/CVPR.1991.139758>
3. Belhumeur P. N., Hespanha J. P., Kriegman D. J. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on pattern analysis and machine intelligence*. 1997. Vol. 19, no. 7. P. 711–720. URL: <https://doi.org/10.1109/34.598228>
4. Dalal N., Triggs B. Histograms of oriented gradients for human detection. *Computer Vision and Pattern Recognition : Proceedings of the IEEE Computer Society Conference, San Diego, 20–25 June 2005*. San Diego, 2005. P. 886–893. URL: <https://doi.org/10.1109/CVPR.2005.177>
5. Bartlett M. S., Movellan J. R., Sejnowski T. J. Face recognition by independent component analysis. *IEEE Transactions on neural networks*. 2002. Vol. 13, no. 6. P. 1450–1464. URL: <https://doi.org/10.1109/TNN.2002.804287>

6. Ghostfacenets: Lightweight face recognition model from cheap operations / Alansari M. et al // *IEEE Access*. 2023. Vol. 11. P. 35429–35446. URL: <https://doi.org/10.1109/access.2023.3266068>
7. Ghostnet: More features from cheap operations / Han K. et al // *Computer vision and pattern recognition: Proceedings of the IEEE/CVF conference, Seattle, 13–19 June 2020*. Seattle, 2020. P. 1580–1589. URL: <https://doi.org/10.1109/CVPR42600.2020.00165>
8. GhostNetv2: Enhance cheap operation with long-range attention / Tang Y. et al // *Neural Information Processing Systems : Proceedings*, New Orleans, 28 November – 09 December 2022. New Orleans, 2022. P. 9969–9982. URL: <https://doi.org/10.48550/arXiv.2211.12905>
9. Wen Y., Zhang K., Li Z., Qiao Y. A discriminative feature learning approach for deep face recognition. *European conference on computer vision: Proceedings*. Cham, 2016. P. 499–515. URL: https://doi.org/10.1007/978-3-319-46478-7_31
10. Deng J., Guo J., Xue N., Zafeiriou S. Arcface: Additive angular margin loss for deep face recognition. *Computer Vision and Pattern Recognition : Proceedings of the IEEE Computer Society Conference*, Long Beach, 15–20 June 2019. Long Beach, 2019. P. 4690–4699. URL: <https://doi.org/10.1109/CVPR.2019.00482>
11. Cosface: Large margin cosine loss for deep face recognition / Wang H. et al // *Computer vision and pattern recognition : Proceedings of the IEEE/CVF conference*, Salt Lake City, 18–23 June 2018. Salt Lake City, 2018. P. 5265–5274. URL: <https://doi.org/10.1109/CVPR.2018.00552>
12. Kim M., Jain A. K., Liu X. Adaface: Quality adaptive margin for face recognition. *Computer vision and pattern recognition : Proceedings of the IEEE/CVF conference*, New Orleans, 18–24 June 2022. New Orleans, 2022. P. 18750–18759. URL: <https://doi.org/10.1109/CVPR52688.2022.01819>
13. Boutros F., Damer N., Kirchbuchner F., Kuijper A. Elasticface: Elastic margin loss for deep face recognition. *Computer vision and pattern recognition : Proceedings of the IEEE/CVF conference*, New Orleans, 18–24 June 2022. New Orleans, 2022. P. 1578–1587. URL: <https://doi.org/10.1109/CVPRW56347.2022.00164>
14. Unitsface: Unified threshold integrated sample-to-sample loss for face recognition / Jia X. et al // *Neural Information Processing Systems : Proceedings*, New Orleans, 10–16 December 2023. New Orleans, 2023. P. 32732–32747. URL: <https://doi.org/10.48550/arXiv.2311.02523>
15. Wang X., Xue H., Liu X., Pei Q. A privacy-preserving edge computation-based face verification system for user authentication. *IEEE Access*. 2019. Vol. 7. P. 14186–14197. URL: <https://doi.org/10.1109/ACCESS.2019.2894535>
16. Lin W. H., Wang P., Tsai C. F. Face recognition using support vector model classifier for user authentication. *Electronic Commerce Research and Applications*. 2016. Vol. 18. P. 71–82. URL: <https://doi.org/10.1016/j.elerap.2016.01.005>
17. Your face your heart: Secure mobile face authentication with photoplethysmograms / Chen Y. et al // *Computer Communications : Proceedings of the IEEE Conference*, Atlanta, 01–04 May 2017. Atlanta, 2017. P. 1–9. URL: <https://doi.org/10.1109/INFOCOM.2017.8057220>
18. Smith-Creasey M., Albalooshi F. A., Rajarajan M. Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems*. 2018. Vol. 63. P. 147–157. URL: <https://doi.org/10.1016/j.micpro.2018.07.008>
19. Zhou B., Xie Z., Ye F. Multi-modal face authentication using deep visual and acoustic features. *Communications : Proceedings of the IEEE International Conference*, Shanghai, 20–24 May 2019. Shanghai, 2019. P. 1–6. URL: <https://doi.org/10.1109/ICC.2019.8761776>
20. Aface: Range-flexible anti-spoofing face authentication via smartphone acoustic sensing / Xu Z. et al // *Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2024. Vol. 8, no. 1. P. 1–33. URL: <https://doi.org/10.1145/3643510>
21. Imagenet: A large-scale hierarchical image database / Deng J. et al. // *Computer Vision and Pattern Recognition : Proceedings of the IEEE Conference*, Miami, 20–25 June 2009. Miami, 2009. P. 248–255. URL: <https://doi.org/10.1109/CVPR.2009.5206848>
22. Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition. *Learning Representations : Proceedings of the International Conference*, San Diego, 07–09 May 2015. San Diego, 2015.
23. Huang G. B., Mattar M., Berg T., Learned-Miller E. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. *Faces in 'Real-Life' Images: detection, alignment, and recognition : Proceedings*. 2008

References

1. Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face recognition systems: A survey. *Sensors*, 20(2), 342. <https://doi.org/10.3390/s20020342>
2. Turk, M. A., & Pentland, A. (1991). Face recognition using eigenfaces. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 586–591. IEEE. <https://doi.org/10.1109/CVPR.1991.139758>
3. Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on pattern analysis and machine intelligence*, 19(7), 711–720. <https://doi.org/10.1109/34.598228>

4. Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. In *IEEE Computer Society Conference On Computer Vision And Pattern Recognition*, 886–893. IEEE. <https://doi.org/10.1109/CVPR.2005.177>
5. Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2002). Face recognition by independent component analysis. *IEEE Transactions on neural networks*, 13(6), 1450–1464. <https://doi.org/10.1109/TNN.2002.804287>
6. Alansari, M., Hay, O. A., Javed, S., Shoufan, A., Zweiri, Y., & Werghi, N. (2023). GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations. , 35429–35446. <https://doi.org/10.1109/access.2023.3266068>
7. Han, K., Wang, Y., Tian, Q., Guo, J., Xu, C., & Xu, C. (2020). Ghostnet: More features from cheap operations. In *IEEE/CVF Conference On Computer Vision And Pattern Recognition*, 1580–1589. IEEE. <https://doi.org/10.1109/CVPR42600.2020.00165>
8. Tang, Y., Han, K., Guo, J., Xu, C., Xu, C., & Wang, Y. (2022). GhostNetv2: Enhance cheap operation with long-range attention. In *Neural Information Processing Systems*, 9969–9982. <https://doi.org/10.48550/arXiv.2211.12905>
9. Wen, Y., Zhang, K., Li, Z., & Qiao, Y. (2016). A Discriminative Feature Learning Approach for Deep Face Recognition. In *European conference on computer vision*, 499–515. Springer. https://doi.org/10.1007/978-3-319-46478-7_31
10. Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). Arcface: Additive angular margin loss for deep face recognition. In *IEEE/CVF conference on computer vision and pattern recognition*, 4690–4699. IEEE. <https://doi.org/10.1109/CVPR.2019.00482>
11. Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D., Zhou, J., Li, Z., & Liu, W. (2018). CosFace: Large Margin Cosine Loss for Deep Face Recognition. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 5265–5274. IEEE. <https://doi.org/10.1109/CVPR.2018.00552>
12. Kim, M., Jain, A. K., & Liu, X. (2022). Adaface: Quality adaptive margin for face recognition. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 18750–18759. IEEE. <https://doi.org/10.1109/CVPR52688.2022.01819>
13. Boutros, F., Damer, N., Kirchbuchner, F., & Kuijper, A. (2022). Elasticface: Elastic margin loss for deep face recognition. In *IEEE/CVF conference on computer vision and pattern recognition*, 1578–1587. IEEE. <https://doi.org/10.1109/CVPRW56347.2022.00164>
14. Jia, X., Zhou, J., Shen, L., & Duan, J. (2023). Unitsface: Unified threshold integrated sample-to-sample loss for face recognition. In *Neural Information Processing Systems*, 32732–32747. <https://doi.org/10.48550/arXiv.2311.02523>
15. Wang, X., Xue, H., Liu, X., & Pei, Q. (2019). A privacy-preserving edge computation-based face verification system for user authentication. *IEEE Access*, 7, 14186–14197. <https://doi.org/10.1109/ACCESS.2019.2894535>
16. Lin, W. H., Wang, P., & Tsai, C. F. (2016). Face recognition using support vector model classifier for user authentication. *Electronic Commerce Research and Applications*, 18, 71–82. <https://doi.org/10.1016/j.elerap.2016.01.005>
17. Chen, Y., Sun, J., Jin, X., Li, T., Zhang, R., & Zhang, Y. (2017). Your face your heart: Secure mobile face authentication with photoplethysmograms. In *IEEE Conference on Computer Communications*, 1–9. IEEE. <https://doi.org/10.1109/INFOCOM.2017.8057220>
18. Smith-Creasey, M., Albaloshi, F. A., & Rajarajan, M. (2018). Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems*, 63, 147–157. <https://doi.org/10.1016/j.micpro.2018.07.008>
19. Zhou, B., Xie, Z., & Ye, F. (2019). Multi-modal face authentication using deep visual and acoustic features. In *IEEE International Conference on Communications*, 1–6. IEEE. <https://doi.org/10.1109/ICC.2019.8761776>
20. Xu, Z., Liu, T., Jiang, R., Hu, P., Guo, Z., & Liu, C. (2024). AFace: Range-flexible anti-spoofing face authentication via smartphone acoustic sensing. *Interactive, Mobile, Wearable and Ubiquitous Technologies*, 8(1), 1–33. <https://doi.org/10.1145/3643510>
21. Deng, J., Dong, W., Socher, R., Li, L. J., Li, K., & Fei-Fei, L. (2009). Imagenet: A large-scale hierarchical image database. In *IEEE Conference On Computer Vision And Pattern Recognition*, 248–255. IEEE. <https://doi.org/10.1109/CVPR.2009.5206848>
22. Simonyan, K., & Zisserman, A. (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition. In *International Conference on Learning Representations*, 1–14.
23. Huang, G. B., Mattar, M., Berg, T., & Learned-Miller, E. (2008). Labeled faces in the wild: A database for studying face recognition in unconstrained environments. In *Workshop on faces in 'Real-Life' Images: detection, alignment, and recognition*. 1–14.

Дата першого надходження рукопису до видання: 28.09.2025
Дата прийнятого до друку рукопису після рецензування: 23.10.2025
Дата публікації: 28.11.2025