УДК 004.056.523:57.087.1]:004.85 DOI: https://doi.org/10.30837/IYF.IIS.2024.290

СИСТЕМА РОЗПІЗНАВАННЯ БІОМЕТРИЧНИХ ДАНИХ ОБЛИЧЧЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ

Мілька Я. Ю.
Науковий керівник – доц. Ларченко Л. В.
Харківський національний університет радіоелектроніки, каф. АПОТ
м. Харків, Україна
e-mail: yaroslav.milka@nure.ua

A person's face stands out as a visible feature that distinguishes a skin person. In our ubiquitous life, the face is perhaps the most well-known and universally recognized biometric characteristic.

Over several decades, advances in the fields of electronics and computer science have revolutionized access to advanced technology for a large portion of the population. These advances have made high-end technological devices more affordable than ever before.

One area where these advances are particularly visible is in the field of biometrics, which have gradually replaced traditional knowledge-based solutions such as passwords or PINs, as well as possession-based strategies such as ID cards or badges.

У сучасному світі, де цифрова безпека стає все більш важливою, біометричні системи відіграють ключову роль у забезпеченні захисту та авторизації доступу до різних сервісів. Означена тема фокусується на розробці системи розпізнавання біометричних даних обличчя, яка використовує передові технології машинного навчання для ефективного та точного ідентифікування осіб. Метою дослідження *є* посилення заходів безпеки та підвищення зручності автентифікації користувачів до захищених систем, шляхом використання технологій нейронних мереж та машинного навчання, які ідентифікують осіб на основі антропометричних ознак обличчя.

Розпізнавання обличчя відноситься до передової технології, яка призначена для розпізнавання та автентифікації особи за допомогою різних форм візуального медіа, наприклад зображень, відео або будь-якого візуального представлення її обличчя [1]. Цей метод ідентифікації зазвичай використовується для отримання доступу до програм, систем або служб, функціонуючи подібно до сканера обличчя. Функціонування біометричної системи визначається конкретним контекстом її застосування, що працює в режимі перевірки або ідентифікації. У режимі перевірки система перевіряє особу шляхом порівняння її біометричних характеристик із збереженим біометричним шаблоном у базі даних системи. У різних програмах використовуються різні біометричні модальності, кожна з яких має свої сильні та слабкі сторони [2]. Вибір біометричного режиму залежить від

вимог конкретної програми. Однак важливо зазначити, що жоден біометричний спосіб не може універсально задовольнити вимоги всіх додатків, оскільки кожен має свої обмеження. Вибір відповідного індикатора біометричного розпізнавання залежить як від режиму роботи програми, так і від характеристик конкретної біометричної ознаки, яка використовується.

Для розробки системи розпізнавання біометричних даних обличчя використовується згорткова нейронна мережа. Згорткові нейронні мережі (CNN) стали надзвичайно потужним інструментом у сфері комп'ютерного зору, здатним впевнено впоратися зі складними завданнями розпізнавання облич, завдяки їхній здатності витягати ключові ознаки з вхідних зображень. Ця здатність заснована на аналізі різних аспектів обличчя, таких як форма, текстура та розташування ключових точок, що дозволяє системі впізнавати особу навіть у різноманітних умовах освітлення та перспективи. CNN є типом ієрархічної моделі, яка може приймати різні форми необроблених вхідних даних, таких як зображення людей. CNN працює, виконуючи ряд операцій, включаючи згортку, об’єднання та відображення функції активації. Ці операції дозволяють CNN захоплювати та витягувати базову семантичну інформацію у вхідних даних, шар за шаром. Цей процес відомий як операція з упередженням (feedforward). В операції прямого зв'язку CNN поступово надсилає витягнуту семантичну інформацію на наступні рівні. Останній рівень CNN перетворює вхідні дані в цільові завдання, такі як класифікація або регресія, перетворюючи їх на цільові функції. Потім цільові функції служать основою для розрахунку різниці між очікуваним значенням і фактичним значенням. Для покращення продуктивності моделі використовується алгоритм зворотного поширення. Цей алгоритм поширює інформацію про втрату з останнього рівня назад через мережу, відповідно оновлюючи параметри кожного рівня. Цей ітеративний процес дозволяє CNN постійно коригувати та покращувати свою продуктивність шляхом точного налаштування параметрів мережі. Через повторювані ітерації кроків прямого та зворотного поширення модель нейронної мережі поступово зближується. У результаті вона досягає мети навчання та ефективно вивчає закономірності, присутні у вхідних даних.

Проте, разом із великими можливостями виникають і певні виклики. Один з них – це забезпечення стійкості до шуму та змін у вхідних даних, які можуть виникнути через різноманітність облич та умов зйомки. Для подолання цих проблем потрібні не лише технічні рішення, але і увага до деталей процесу навчання та тестування моделі. Також важливою є прозорість та відкритість у використанні біометричних технологій, особливо у зв'язку з питаннями приватності та етики. Забезпечення конфіденційності та безпеки даних користувачів має бути в центрі розробки та впровадження систем згорткової нейронної мережі.

Вхідні зображення були стандартизовані до розміру 32x32x1, де 1 позначає колірний простір градацій сірого. У початковому шарі згортки застосовано фіксований розмір ядра 3x3 і обмежено кількість фільтрів до 16. Таке зменшення кількості фільтрів було визнано доцільним через природу вхідних зображень у відтінках сірого, які містять менше характерних особливостей для вивчення. Що стосується рівня активації, була обрана функція ReLU. ReLU набула популярності в згорткових нейронних мережах завдяки своїй продуктивності порівняно з іншими функціями активації.

Щоб зменшити дискретизацію карт функцій, було додано шари максимального об'єднання з фіксованим розміром ядра 2x2 і кроком 2. У наступному шарі згортки кількість фільтрів збільшено до 32, зберігаючи той самий розмір ядра, що й у першому згорткому шарі. Щоб забезпечити стабільність і прискорити процес навчання, додано пакетну нормалізацію після кожної згортки, активації та блоку максимального об'єднання. Пакетна нормалізація виявилася ефективною технікою регулярізації, що полегшує використання вищих показників навчання, одночасно гарантуючи конвергенцію мережі. Крім того, це пом'якшує внутрішній коваріантний зсув і зменшує залежність градієнтів від шкали параметрів або початкових значень.

Враховуючи обмежену кількість функцій у вхідному зображенні, було запропоновано включити вилучення, щоб вирішити проблему перенавчання. Виключення (dropout) – це ефективна техніка, яка усуває нейрони зі слабкими зв'язками, приділяючи більшу увагу нейронам із сильними зв'язками. Завдяки цьому підвищується продуктивність нейронної мережі.

Розроблено модель системи біометричного розпізнавання, яка базується на використанні згорткової нейронної мережі. Розроблену модель було перевірено на практиці, відповідно до результату, можна зробити висновок, що її ієрархічна структура і спосіб обробки даних забезпечують високу точність ідентифікації.

Список використаних джерел:

1. Vasanthi M., Seetharaman K. Facial image recognition for biometric authentication systems using a combination of geometrical feature points and low-level visual features. Journal of King Saud University – Computer and Information Sciences. 2022. Vol. 34, no. 7. P. 4109–4121. URL: https://www.sciencedirect.com/science/article/pii/S1319157820305577 (дата звернення: 18.12.2023).

2. Petrescu V. Face Recognition as a Biometric Application. Journal of Mechatronics and Robotics. 2022. Vol. 3, no. 1. P. 237–257. URL: https://thescipub.com/abstract/jmrsp.2019.237.257 (дата звернення: 18.12.2023).