Список використаних джерел:

1. Бобро Н. Взаємодія штучного і природного інтелекту в освітньому процесі. *Молодий вчений*, 2024. № 5 (129). С. 51–55.
2. Карташова Л. Штучний інтелект у навчанні і викладанні: інноваційні цифрові компетентності. *Сучасні освітні стратегії під впливом розвитку інформаційного суспільства та євроінтеграції*: наукова монографія. Рига, Латвія : Baltija Publishing, 2024. С. 196–222.
3. Штучний інтелект в освітніх галузях (природнича освітня галузь). Навчально-методичний посібник для здобувачів першого (бакалаврського), другого (магістерського) рівнів вищої педагогічної освіти, науково-педагогічних працівників закладів вищої педагогічної освіти та педагогічних кадрів закладів загальної середньої освіти / Укл.: Доценко С. О., Собченко Т. М., Боярська-Хоменко А. В. Харків : ХНПУ імені Г. С. Сковороди, 2024. Ч. ІІІ. 58 с.

АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ НА ОСНОВІ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ

Грицай Іван Андрійович
здобувач другого рівня вищої освіти, спеціальність Комп’ютерні науки
Тернопільський національний педагогічний університет імені Володимира Гнатюка
grytsaj_ia@fizmat.tnpu.edu.ua
Олексюк Василь Петрович
Доктор педагогічних наук, професор кафедри інформатики та методики її навчання
Тернопільський національний педагогічний університет імені Володимира Гнатюка
oleksyuk@fizmat.tnpu.edu.ua

Постановка проблеми. В умовах цифрової трансформації освіти постає проблема забезпечення надійного та безпечного доступу користувачів до освітніх ресурсів. Традиційні методи аутентифікації (паролі, PIN-коди або токени) є вразливими до фішингових атак, соціальної інженерії та витоку даних. Крім того, вони не гарантують, що саме конкретна особа здійснює вхід у систему.

У закладах освіти це має особливе значення, адже від достовірності аутентифікації залежить чесність проходження онлайн-тестів, захист персональних даних студентів і викладачів, а також справедливість оцінювання.

Одним із перспективних напрямів підвищення безпеки є використання технологій машинного навчання (ML) для створення біометричних систем аутентифікації, здатних розпізнавати користувачів за обличчям, голосом або поведінковими ознаками. Застосування ML-моделей дозволяє враховувати варіації освітлення, виразів обличчя, положення голови, тим самим підвищуючи точність розпізнавання [1; 3].

Виклад основного матеріалу. Системи аутентифікації, що базуються на машинному навчанні, використовують алгоритми комп’ютерного зору для аналізу унікальних біометричних характеристик користувача.

Біометрична аутентифікація базується на розпізнаванні фізіологічних або поведінкових ознак (обличчя, відбиток пальця, голос, динаміка набору тексту). Завдяки використанню глибоких нейронних мереж (DNN, CNN) такі системи демонструють високу точність.

Наприклад, архітектури FaceNet та ArcFace, побудовані на базі ResNet, забезпечують понад 99 % точності на відкритих наборах LFW. Вони перетворюють

зображення облич у векторні представлення – *ембеддинги* – і порівнюють їх за евклідовою відстанню.

Для розроблення модуля автентифікації нами було застосовано відкриті інструменти, які поєднують високу швидкість і точність розпізнавання (OpenCV, Dlib та Face_Recognition) [4].

- OpenCV забезпечує виявлення облич у реальному часі завдяки алгоритмам HOG і CNN.
- Dlib реалізує побудову 128-вимірних векторів обличчя.
- Face_Recognition спрощує інтеграцію у вебсередовище завдяки готовим методам порівняння ембеддингів.
- Вибір цих бібліотек зумовлений їхньою відкритістю, гнучкістю та широкою підтримкою спільноти.

Модуль реалізовано як вебсистему, що складається з трьох рівнів:

- інтерфейс користувача (Vue.js) для реєстрації та зйомки зображення обличчя;
- серверна частина (PHP), що приймає дані, передає їх Python-скриптам і формує відповіді;
- підсистема машинного навчання (Python), яка обробляє зображення, виявляє обличчя, створює ембеддинги, порівнює їх з базою та приймає рішення про ідентифікацію.

Модуль працює в реальному часі, дозволяючи проводити онлайн-верифікацію особи без потреби у складному обладнанні. Для запобігання шахрайству передбачено аналіз мікрорухів голови: користувачеві може бути запропоновано повернути голову або нахилити її, що виключає можливість використання фотографій.

Алгоритм функціонує за принципом послідовних етапів:

- захоплення кадру з камери;
- детекція обличчя;
- створення векторного представлення;
- порівняння з шаблонами бази даних;
- прийняття рішення про ідентифікацію.
- Тестування проводилося із використанням наборів даних LFW та CelebA. Отримано середню точність розпізнавання 96,8 % при пороговому значенні 0,6. Помилки виникали переважно при затемненні або частковому перекритті обличчя.

Розроблений модуль може бути інтегрований у системи дистанційного навчання (Moodle, Google Classroom, власні LMS). Це дозволить автоматично перевіряти особу студента під час тестування, унеможливлюючи підміну користувача.

Крім того, система може застосовуватися для реєстрації відвідувань, контролю доступу до лабораторій чи електронних бібліотек. Така інтеграція сприяє підвищенню академічної доброчесності та кібербезпеки освітнього процесу.

Основними викликами залишаються захист біометричних даних, вимоги до обчислювальних ресурсів і етичні питання використання зображень осіб.

Подальші дослідження передбачають:

- розробку гібридних моделей аутентифікації, які поєднують кілька типів ознак (обличчя, голос, поведінка);
- впровадження асинхронних сервісів (FastAPI) для обробки великої кількості запитів;
- інтеграцію із мобільними платформами та системами розпізнавання емоцій для підвищення точності.

Висновки. Розвиток освітніх платформ вимагає надійних методів ідентифікації користувачів. Технології машинного навчання дозволяють створити інтелектуальні біометричні системи аутентифікації, здатні працювати в реальному часі, адаптуватися до змін та забезпечувати високий рівень безпеки. На основі Python, OpenCV та Dlib реалізовано прототип модуля розпізнавання облич, який демонструє точність понад 96 % і може бути інтегрований у навчальні середовища для підтвердження особи студентів. Запровадження таких систем сприятиме формуванню безпечного та справедливого освітнього простору**,** підвищенню довіри до результатів дистанційного навчання й розвитку цифрової грамотності.

Списки використаних джерел

1. Bonneau J., Herley C., Oorschot P. C., Stajano F. The quest to replace passwords : A framework for comparative evaluation of web authentication schemes, 2012. P. 553–567.

2. Mayes K., Markantonakis K., Piper F. Smart card based authentication – Any future? Computers and Security, 2005. Vol. 24. P. 188–191.

3. Jain A., Ross A., Pankanti S. Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security, 2006. Vol. 1. P. 125–143.

4. Boyko N., Basystiuk O., Shakhovska N. Performance evaluation and comparison of software for face recognition, based on Dlib and OpenCV library. 2018 IEEE Second International Conference on Data Stream Mining and Processing (DSMP). IEEE, 2018. P. 478–482.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЬОМУ ПРОЦЕСІ З ГРАФІЧНОГО ДИЗАЙНУ

Дмитрів Андрій Володимирович
здобувач третього рівня вищої освіти, спеціальність Освітні, педагогічні науки
Тернопільський національний педагогічний університет імені Володимира Гнатюка
Мартинюк Сергій Володимирович
кандидат фізико-математичних наук, доцент кафедри інформатики та методики її навчання
Тернопільський національний педагогічний університет імені Володимира Гнатюка
sergmart65@tnpu.edu.ua

Штучний інтелект трансформує освіту в галузі графічного дизайну, створюючи революційні можливості як для викладачів, так і для студентів. Його впровадження пропонує значні переваги, однак разом із тим виникають критичні виклики, які вимагають уважного регулювання та правильного впровадження [2].

Адаптивні системи навчання, розроблені на основі штучного інтелекту, аналізують дані про прогрес студентів, виявляють закономірності у їхній поведінці та автоматично коригують навчальний контент відповідно до індивідуальних потреб. Це забезпечує розвиток персоналізованих траєкторій навчання, де студенти отримують матеріали, теми та вправи, адаптовані до їхнього рівня розуміння та темпу навчання [1].

У графічному дизайні освіти використовуються кілька ключових платформ штучного інтелекту:

Adobe Firefly – інтегрована в екосистему Creative Cloud система, яка забезпечує створення графіки, генерацію варіацій стилю та фокусується на безпеці комерційного використання. На відміну від багатьох інших інструментів, Firefly не навчається на контенті, видобутому з веб-сайтів, що зменшує ризики порушення авторських прав