УДК 004

О.Скирда, магістр гр. КН-22МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИДІЛЕННЯ Й РОЗПІЗНАВАННЯ ОБЛИЧЧЯ КОРИСТУВАЧА У МЕРЕЖІ

У статті розроблено програмне забезпечення, яке призначено для системи виділення й розпізнавання обличчя користувача у мережі. Метою розробки є дослідження та програмна реалізація системи виділення й розпізнавання обличчя користувача у мережі. Об'єктом дослідження є процес виділення й розпізнавання обличчя користувача у мережі. Предметом дослідження є методи виділення й розпізнавання обличчя користувача у мережі. Методи дослідження базуються на методах штучного інтелекту, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи виділення й розпізнавання обличчя користувача у мережі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Програмне забезпечення для розпізнавання обличчя (FRS) визначається як біометричний інструмент, який використовується для зіставлення облич на зображеннях, як правило, з фотографій і відеозаписів, із існуючою базою даних ідентичності. Її можна розбити на три частини – виявлення (пошук обличчя на зображенні), аналіз (карта обличчя) і розпізнавання (підтвердження особи).

Прикладом технології розпізнавання обличчя є функція автоматичного позначення фотографій у Facebook або навіть Google Photos. Соціальні медіа та технічні гіганти, такі як ці, відображають обличчя користувача на фотографії, сортуючи існуючу базу даних завантажених зображень. Оскільки риси обличчя набагато складніші, ніж інші існуючі біометричні методи, такі як відбитки пальців і райдужна оболонка ока, інструменти FRS потребують складних алгоритмів зі штучним інтелектом.

Згідно зі звітом за 2023 рік Opens a new windowЗгідно з NIST, алгоритми розпізнавання облич тепер мають середній рівень помилок лише 0,08%, порівняно з 4,1% у 2014 році. Нейронні мережі та технології глибокого навчання відтоді значно вдосконалилися, дозволивши значний розвиток програмного забезпечення для розпізнавання 3D. Справа не лише в базових алгоритмах, ми тепер маємо потужніші мікроконтролери та процесори та вдосконалену технологію камер для об'єктивів і обробки на чіпі. Доступ до цього апаратного забезпечення у вигляді смартфонів став благом для галузі FRS.

На початку цього року Juniper Research повідомила Відкриває нове вікнощо апаратне забезпечення для розпізнавання обличчя, таке як FaceID від Apple, є найшвидше зростаючою формою біометричного обладнання для смартфонів. За оцінками, до 2024 року їх використовуватиме понад 800 мільйонів смартфонів. Беручи до уваги прогрес технологій і прискорене зростання ринку, це був би вдалий час для впровадження технології розпізнавання облич у ваш бізнес.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи виділення й розпізнавання обличчя користувача у мережі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи виділення й розпізнавання обличчя користувача у мережі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем виділення й розпізнавання обличчя користувача у мережі.
– Дослідження системи виділення й розпізнавання обличчя користувача у мережі.
– Програмна реалізація системи виділення й розпізнавання обличчя користувача у мережі.

Об'єктом дослідження є процес виділення й розпізнавання обличчя користувача у мережі.

Предметом дослідження є методи виділення й розпізнавання обличчя користувача у мережі.

Методи дослідження базуються на методах штучного інтелекту, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Будь-який хороший FRS має три ключові компоненти:

– Обладнання для захоплення зображень. Ці зображення також можна вводити в програмне забезпечення з незалежних пристроїв.
– Інтелект для порівняння захоплених облич з наявними даними.
– База даних, тобто існуюча колекція ідентичностей. Це може бути що завгодно: від баз даних співробітників до зображень, видалених із соціальних мереж.

Тепер давайте розберемося, як працює FRS.

1. Виявлення: Виявлення починається з виділення обличчя із зображення, яке подається в систему. Згодом на обличчі людини відзначаються різні риси. Певні риси обличчя не змінюються з віком або розміром. Це відстань між очима, глибина очниці і форма носа. Існує близько 80 таких об'єктів, які називаються «орієнтирами». Потім розміри цих орієнтирів об'єднуються, щоб створити код. Цей код називається «відбитком обличчя», і він унікальний для кожної людини.
2. Зіставлення: цей відбиток обличчя потім зіставляється з відбитками, збереженими в системі. На цьому етапі зображення проходить кілька технологічних рівнів для забезпечення точності. Оскільки більшість наших баз даних наразі є двовимірними фотографіями, зображення бази даних потрібно обробляти за допомогою рівня технології. Ця обробка зазвичай включає витягування орієнтирів обличчя, щоб вони були схожі на їхні тривимірні аналоги. Якщо зображення об'єкта має низьку роздільну здатність, його необхідно закодувати та декодувати, щоб створити деталі з бажаною роздільною здатністю. Алгоритми повинні враховувати різницю в освітленні, виразі обличчя та кутах.
3. Ідентифікація: мета цього кроку залежить від того, для чого використовується програмне забезпечення для розпізнавання обличчя – для спостереження чи автентифікації. В ідеалі цей крок має забезпечити відповідність об'єкта 1:1. Це можна зробити кількома способами: швидким переходом, щоб звузити параметри, а потім увімкненням більш складних шарів. Деякі компанії аналізують текстуру шкіри разом із алгоритмами розпізнавання обличчя, щоб підвищити точність.

Кожен постачальник програмного забезпечення для розпізнавання обличчя зосереджується на різних аспектах технологічних рівнів, щоб забезпечити майже бездоганне обслуговування. Наприклад, одне програмне забезпечення може зосереджуватися на коригуванні умов освітлення, а інше – на аналізі текстури шкіри.

Хто користується програмним забезпеченням для розпізнавання обличчя?

Такі компанії, як Mastercard, уже використовують FRS як ідентифікатор під час платежів і для підвищення безпеки. FRS має потенційне застосування в роздрібній торгівлі, готельному секторі, банках, банкоматах та аеропортах. Компанії, орієнтовані на мобільну комерцію, отримають велику користь від FRS. Маркетингові фірми розглядають можливість використання FRS для персоналізованого обслуговування клієнтів.

Наприклад, деякі компанії електронної комерції, які продають окуляри, працюють над використанням FRS, щоб рекомендувати окуляри, які добре виглядають для структури

вашого обличчя. Це позбавляє необхідності відвідувати магазин, щоб їх приміряти. Однак найвагоміші варіанти використання FRS сьогодні пов'язані з безпекою.

Ключові обов'язкові функції програмного забезпечення для розпізнавання облич

Програмне забезпечення для розпізнавання обличчя можна використовувати для автентифікації, спостереження або маркетингу. Залежно від вашого випадку використання, ось деякі ключові функції, на які варто звернути увагу під час розгляду варіантів FRS:

Ключові обов'язкові функції програмного забезпечення для розпізнавання облич

1. Навчена та зростаюча база даних: Рівень точності будь-якої FRS залежить від бази даних, на якій навчався її штучний інтелект. Дані повинні постійно зростати, різноманітні за статтю та етнічним походженням. Навчальні дані також повинні відрізнятися в освітленні, ракурсах і виразах обличчя. Хороша база даних також містить різні роздільності зображень, з якими система може працювати. Програми машинного навчання ефективні настільки, наскільки хороша база даних, яку вони використовують для навчання, і FRS не є винятком.

2. Безпека та конфіденційність користувача: будь-яке біометричне програмне забезпечення тісно пов'язане з особистістю людини. Це означає, що дані (в даному випадку відбитки обличчя), накопичені FRS, є дуже конфіденційними. Дані користувача необхідно шифрувати та очищати через регулярні проміжки часу. Постачальники програмного забезпечення повинні мати надійний план на випадок витоку даних.

3. Точність алгоритму: ключовими показниками, на які слід звернути увагу під час розгляду FRS, є коефіцієнт помилкового прийняття (FAR) і коефіцієнт помилкового відхилення (FRR). FAR – це коли різні зображення хибно зіставляються як ідентичні. У цьому випадку, якщо ви використовуєте його для безпеки, доступ може бути дозволено не тій особі. У FRR точні зображення хибно не збігаються як різні. У цьому випадку потрібна особа може отримати відмову в доступі. У практичному сценарії безпеки FAR має бути низьким, а FRR високим.

4. Масштабованість: для великих підприємств, які хочуть використовувати FRS для автентифікації, масштабованість є важливою, оскільки програмне забезпечення потрібно розгортати в кількох місцях.

5. Адаптованість і підтримка: постачальники FRS повинні пропонувати резервні варіанти до уваги. У разі збою системи може знадобитися людська підтримка та нагляд, поки система повернеться до нормального стану. Підтримка також потрібна для налаштування обладнання, зокрема камер, для максимальної точності.

6. Прозорість і етика: лише за останній рік FRS кілька разів критикували через відсутність прозорості. Переконайтеся, що програмне забезпечення, яке ви використовуєте, не вдається до неетичних методів, як-от очищення соціальних мереж для збору навчальних даних або порушує конфіденційність користувачів.

Контрольний список для вибору правильного програмного забезпечення

Будь-яка організація, яка збирається вибрати відповідне програмне забезпечення для розпізнавання обличчя, повинна розглянути такі питання:

1. Чи FRS відповідає потребам вашого бізнесу? Вам може знадобитися FRS для ідентифікації облич у закритому наборі даних (автентифікація співробітників), відкритому наборі даних (відстеження роздрібних клієнтів) або просто для перевірки (просто перевірте, чи два зображення однакові).

2. Чи безпечне рішення? Дані мають бути зашифровані та захищені від злому. Це також має захищати конфіденційність користувачів.

3. Чи перевірено програмне забезпечення? Щоб перевірити точність ваших власних даних, існують доступні відкриті джерела даних, як-от LFW і MegaFace. Ви також можете найняти для цього сторонніх постачальників даних. Просто переконайтеся, що набір даних, вибраний для тестування системи, відображає фактичних людей, які використовують систему у вашому випадку використання.

4. Чи перевірили ви показники FAR і FRR? Розглядаючи ці показники, також подумайте про поріг точності, який вас задовольняє. Наприклад, чи нормально для вашого бізнесу, якщо FRS показує збіги, які збігаються лише на 70%?

5. Чи є у нього сильна команда підтримки? Рішення FRS є складними, тому для безперебійної інтеграції у вашу існуючу систему та безперебійної роботи потрібна хороша команда підтримки. Команда підтримки також має допомогти налаштувати програмне та апаратне забезпечення відповідно до ваших потреб.

6. Чи порушують якісь із умов програмного забезпечення закони? Розпізнавання обличчя зараз є актуальною темою, і правила щодо цього різняться. Переконайтеся, що ви не перетинаєте жодних законних меж під час використання FRS.

Розробка структурної схеми

Для людей розпізнавання та класифікація об’єктів (анімованих чи ні) здійснюється шляхом захоплення об’єкта за допомогою кількох доступних біологічних органів чуття, а потім інформація передається в мозок, який розпізнає (або дізнається) об’єкт і миттєво класифікує його на основі захоплених ознак. від цього об'єкта. Крім того, ознаки об’єктів також можна виміряти за допомогою інструментів вимірювання, які надають характерні дані, які можна перевести в інформацію, що використовується для опису або однозначної ідентифікації цього об’єкта (Alblushi A., 2021; Hassin & Abbood, 2021). Завдяки цьому певні біологічні риси можна виміряти та використовувати для однозначної ідентифікації людини серед людей. Такі біологічні ознаки відомі як біометрія. Відповідно до (Jain et al., 2004), щоб біологічна ознака була прийнятною як біометрична, вона має бути універсальною (поширеною серед людей), відмінною (вимірюється однозначно між різними людьми для достатнього поширення), постійною (значною мірою незмінною з часом) і колекційні (вимірні кількісно). Однією з біологічних ознак, які можна вважати біометричними, є людське обличчя. Обличчя людини задовольняють усім вимогам біометрії; вони, безсумнівно, є універсальними, надзвичайно характерними у великому масштабі, переважно постійними протягом тривалого періоду часу та підлягають колекціонуванню. Таким чином, можна побудувати біометричну систему на основі біометрії людського обличчя.

Комп’ютеризована біометрична система, заснована на людських обличчях, по суті, є системою розпізнавання обличчя, яка спирається на візуальну інформацію, присутню на кожному обличчі унікально. Покращення зображення – це процес зміни цифрового зображення, щоб воно було більш придатним для ідентифікації та класифікації правильних об’єктів (Al-Hatmi & Yousif, 2017; Hasson та ін., 2011)). Відповідно до (Li та ін., 2020) обличчя розпізнавання – це проблема розпізнавання візуальних образів, де візуальні вхідні дані, представлені як матриці в комп’ютері, потрібно розрізнити з точки зору того, чи містять дані обличчя, а потім визначити, кому це обличчя належить. (Oloyede та ін., 2020) пояснює, що структура системи розпізнавання обличчя за своєю суттю схожа на структуру біометричної системи, вона включає виявлення обличчя, попередню обробку зображення обличчя, виділення рис обличчя та класифікацію ознак, що є звичайним кроком у біометричних системах, як зазначено в (Oloyede & Hancke, 2016). (Oloyede та ін., 2020) далі пояснює етапи, задіяні в системі розпізнавання обличчя:

- Виявлення обличчя - це перевірка присутності обличчя людини у візуальних вхідних даних.

- Попередня обробка зображення обличчя готує зображення таким чином, щоб воно містило лише важливі візуальні дані обличчя. Підходи включають нормалізацію (зображення обличчя перетворюються в той самий масштаб), вирівнювання обличчя (визначене (Jin & Tan, 2017) як визначення опорних точок на зображенні обличчя) та покращення зображення (заявлене (Karamizadeh et al., 2016) як обробка зображення обличчя в розширену версію, яка може підвищити продуктивність системи розпізнавання обличчя).

- Виділення рис обличчя – це виділення найбільш релевантних візуальних даних обличчя, які однозначно ідентифікують обличчя, мінімізуючи шум і непов’язану інформацію, у достатній вектор опису.

- Класифікація ознак – це етап розпізнавання зображень обличчя, на якому зображення обличчя порівнюються для верифікації або ідентифікації зображень обличчя з бази даних. Як зазначали (Oloyede & Hancke, 2016), це звичайний етап у біометричних системах і включає верифікацію та ідентифікацію. Перевірка досягається за допомогою пошуку «один-до-одного» між входом і ціллю, а ідентифікація – це пошук «один-до-багатьох» між входом і всією базою даних цілей (Coventry et al., 2003) (Ganorkar & Ghatol, 2007) (P Tripathi, 2011) (Muhtahir et al., 2013) (Ahmad et al., 2012).

Системи розпізнавання обличчя розгортаються в широкому діапазоні програм. Деякі програми включають контроль відвідуваності (S. Manjula & S. Santhosh Baboo, 2012), безпеку (Lander та ін., 2018), фінанси, освіту, смартфони, роздрібну торгівлю, транспорт та безпеку мережевої інформації (Hu та ін., 2010)

Як уже згадувалося, системи розпізнавання облич розгортаються в різних програмах, що робить їх критично необхідною технологією комп'ютерного зору, яка привернула інтерес для подальшого розвитку та вдосконалення. Існує кілька методів, які використовуються в основних підсистемах (розпізнавання обличчя та класифікація ознак), залучених до загальної структури системи розпізнавання обличчя. Усі підсистеми спільно мають методи, які використовують метод глибокого навчання (DL) згорткових нейронних мереж (CNN) для виконання своїх цілей. Таким чином, мета цього дослідження полягає в тому, щоб представити метод CNN і представити деякі методи на основі CNN для підсистем розпізнавання обличчя

Згорткові нейронні мережі (CNN)

Нейронні мережі – це потужні математичні моделі, які мають на меті імітувати людський мозок під час вирішення складних проблем у багатовимірному просторі та перетворювати їх у нижчий вимір (Yousif J., 2015; Yousif & Kazem, 2021; Alattar et al., 2019). Згорткові нейронні мережі є типом штучних нейронних мереж (Lecun та ін., 1998), які спеціально застосовуються в програмах, які передбачають обробку візуальної інформації. Деякі програми CNN включають розпізнавання облич (Taigman та ін., 2014), виявлення об'єктів (Ren та ін., 2017), сегментацію та класифікацію зображень (Farabet та ін., 2013). Візуальні дані в зображеннях зазвичай містяться у формі масиву або кількох масивів. CNN перетворюють візуальні дані в значущу візуальну інформацію, використовуючи послідовні шари згорткових фільтрів для виявлення країв, виявлення частини об'єктів і, нарешті, визначення форми об'єкта в цілому (LeCun та ін., 2015). Згорткові фільтри класифікуються з точки зору їхньої функції в CNN на фільтри шару згортки, фільтри шару об'єднання та фільтри повнозв'язаних шарів (Bezdan & Bačanin Džakula, 2019).

Рівні CNN

Як уже згадувалося, головним чином CNN складається з трьох рівнів: шару згортки, шару об'єднання та повного зв'язку (Bezdan & Bačanin Džakula, 2019). Остаточна обробка візуальних даних через шари CNN виконується шляхом вилучення карт функцій із вхідного 2D-зображення за допомогою ядер (фільтрів) (Salomon et al., 2017).

Рівень згортки

Як випливає з назви, шар згортки покладається на операцію згортки між пікселями зображення та набором ядер навчання. Ядра зазвичай мають невеликий розмір $n \times n$ і глибину d, що дорівнює вхідним каналам зображення, якщо зображення має відтінки сірого$d = 1$ і $d = 3$, якщо зображення має колір RGB тощо. Коли вхідні візуальні дані передаються на рівень згортки, пікселі кадру у визначених позиціях згортаються за допомогою фільтра ядра, що дає згорнутий кадр; і цей процес повторюється для кожного ядра (Bezdan & Bačanin Džakula, 2019). Звивисті кадри потім обробляються функцією активації для створення карт функцій. Деякі з функцій активації включають сигмоподібну логістичну функцію, гіперболічну тангенсову функцію Гауса та випрямлену лінійну одиницю (ReLU). Подібно до функцій активації в нейронних мережах (NN), значення зсуву може бути введено для зміщення вхідних даних функції активації для генерації карт ознак A:

$$A = f(Conv.\ frame + bias)$$ (Salomon et ін., 2017).

Згідно з (Bezdan & Bačanin Džakula, 2019) розмір згенерованих карт функцій залежить від трьох параметрів, пов'язаних із згорткою, а саме кроку, глибини та відступу. Stride – це параметр зміщення позиції, який визначає наступну позицію пікселів кадру, які потрібно згорнути з ядром, тобто для пікселя в позиції n наступний піксель, який буде згорнуто, знаходиться в позиції $197n + s$, де s – значення кроку. Глибина означає кількість унікальних фільтрів ядра, застосованих до вхідного кадру. Заповнення – це додавання нулів до панелей вхідного зображення таким чином, щоб потрібні пікселі були згорнуті, а інформація зберігалася. За допомогою цього розміру карти вихідних функцій можна обчислити як:

$$(n + 2p - f)\, s + 1⁄,$$

де n – це кількість фільтрів, p – це кількість шарів заповнення, f – розмір ядра, а s – крок.

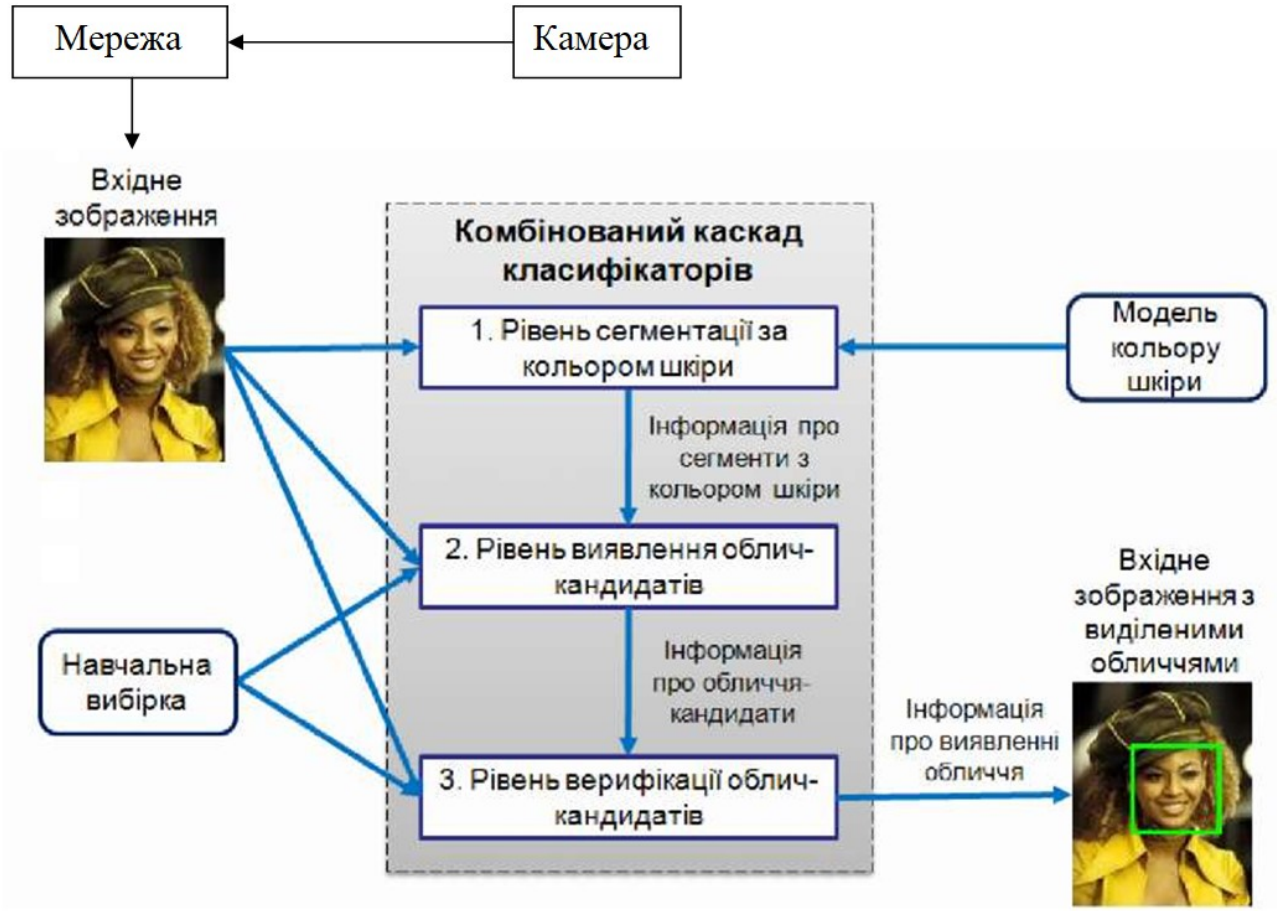

Рисунок 1 – Структурна схема системи

Рівень об'єднання

Карти об'єктів обробляються на шарі об'єднання для зменшення розмірів карт шляхом їх зменшення вибірки (Bezdan & Bačanin Džakula, 2019) і зменшення дисперсії між пікселями карт об'єктів (Salomon та ін., 2017). Карти функцій процесу внутрішньої вибірки поділяються на менші області однакових розмірів $d \times d$, тоді в кожній області або середнє, або максимальне значення пікселів береться як репрезентативне для регіону (Salomon et al., 2017). Процес об'єднання також залежить від кроку і розмір регіону об'єднання. Перекриванням між об'єднаними регіонами можна керувати за допомогою значення кроку, а щоб запобігти виникненню будь-якого збігу між регіонами, значення кроку можна встановити як d, де d – розмір карти функцій (Salomon et al., 2017).

Повністю підключений рівень

Повністю підключений рівень є останнім рівнем CNN. Тут оброблені карти характеристик перетворюються на вектори, які передаються на нейрони штучної нейронної мережі як вхідні дані (Bezdan & Bačanin Džakula, 2019) для класифікації. Методи глибокого

навчання можуть виявити багато складних зв’язків між навчальними даними та результатами через нелінійність його проміжних прихованих шарів. Однак у разі обмежених навчальних даних мережа DL може сформулювати зв’язки, які можуть бути дійсними лише в контексті навчальних даних, а не на реальних даних тестування. Це відомо як переобладнання (Srivastavaet al., 2014). Одним із методів, який можна застосувати для запобігання переобладнанню на CNN, є метод відсіву, запропонований (Srivastava та ін., 2014). У методі відключення вузли нейронної мережі тимчасово відкидаються з мережі випадковим чином разом із її вхідними та вихідними з’єднаннями.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів виділення й розпізнавання обличчя користувача у мережі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем виділення й розпізнавання обличчя користувача у мережі; Досліджена система виділення й розпізнавання обличчя користувача у мережі; На основі отриманих результатів досліджень створена програмна реалізація системи виділення й розпізнавання обличчя користувача у мережі. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання виділення й розпізнавання обличчя користувача у мережі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
2. Malyukov V., Bebeshko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
3. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
4. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
5. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
6. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022, pp. 1-12.
7. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
8. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
9. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and Systems. Volume 152, 2021, Pages 85-98.
10. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.
11. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207.
12. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
14. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on

Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
15. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
16. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
18. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
20. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
21. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.
22. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
23. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.