УДК 004.8

Жарновський О.В., Казмірчук Я.М., Собко О.В., Мазурець О.В.

Хмельницький національний університет

ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ ІДЕНТИФІКАЦІЇ ЗГЕНЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ ЗОБРАЖЕНЬ ЛЮДЕЙ ЗАСОБАМИ МАШИННОГО НАВЧАННЯ

Розроблено метод для ідентифікації згенерованих штучним інтелектом зображень людей засобами машинного навчання на основі використання комбінацій згорткових нейронних мереж. Спроєктовано інформаційну структуру системи нейромережевого аналізу згенерованих зображень облич людей засобами машинного навчання, що за вхідним зображенням дозволяє визначити автентичність зображення та визначити можливі засоби його генерації. Також було спроєктовано програмну архітектуру інформаційної системи для прикладної програмної реалізації розробленого методу нейромережевого аналізу згенерованих зображень облич людей.

Method for identifying human images generated by artificial intelligence by means of machine learning based on the use of combinations of convolutional neural networks has been developed. The information structure of the system of neural network analysis of generated images of people's faces by means of machine learning was designed, which allows to determine the authenticity of the image based on the input image and to determine the possible means of its generation. The software architecture of the information system was also designed for the applied software implementation of the developed method of neural network analysis of generated images of people's faces.

Технологія генерації штучних зображень має широкий спектр застосувань, що робить її корисною в багатьох сферах людської діяльності. Генерація зображень корисна для арту та дизайну – дизайнери та художники можуть використовувати штучний інтелект для генерації референсів та ітерації власних робіт, використовувати штучне зображення як базове для подальшого редагування чи генерувати менш важливі деталі для вже існуючого зображення, такі як об'єкти заднього фону.

В сфері маркетингу та реклами штучний інтелект здатен швидко генерувати візуал. Наприклад, замість того, щоб організовувати фотосесію для нового продукту, маркетологи можуть використовувати ШІ для створення високоякісних зображень, для використання в рекламних матеріалах.

Якість зображень згенерованим ШІ прямим чином залежить від кількості та якості зображень, що використовували для тренування моделі, а також їх доступності.

Складність налаштування – досягнення бажаного рівня деталізації вимагає ретельного налаштування параметрів моделі, що є складнім та трудомістким процесом, особливо для сфери медицини, де зображення повинні мати високу точність.

Проблеми копірайту – крім того що самі зображення, використані для тренування мережі, можуть бути захищені авторським правом, отримане зображення, може призвести до юридичних проблем маркет-заміни та інтелектуальної власності.

Створення дипфейків – через свою простоту та загальну доступність, а також якість зображення генеративний ШІ може бути використаній в створенні зображень подій, що ніколи не мали місце для поширення дезінформації в соціальних мережах. Це може бути використано шахраями для розповсюдження дезінформації з метою впливу на громадську думку.

Хоча найперші спроби генерувати зображення з використанням штучного інтелекту відносяться до 1970-х років, протягом десятиліть прогрес у цій галузі був незначним. Доступні обчислювальні потужності були обмежені, а алгоритми занадто прості щоб працювати із реалістичними зображеннями.

Однак це змінилося з розвитком глибокого навчання та згорткових нейронних мереж [1, 2], що в свою чергу забезпечили основу для створення генеративних змагальних мереж [3, 4].

Генерація зображень здійснюється за допомогою різних форм вхідних даних включаючи RGB зображення, відео, медичні дані чи текст де на виході отримують зображення чи відео.

Метою роботи є прикладне вирішення задачі ідентифікації згенерованих штучним інтелектом зображень людей засобами машинного навчання.

Метод ідентифікації згенерованих штучним інтелектом зображень людей засобами машинного навчання вимагає розробки нейронної мережі здатної до розпізнаванню та класифікації зображень.

Для цього найкраще підходить згорткова нейронна мережа – тип глибоких нейронних мереж, що активно використовується для аналізу зображень, аудіо та відео [5]. CNN складається із різновиду багатошарових перцептронів, розроблених так, щоб вимагати мінімальний обсяг попередньої обробки [6, 7].

Метод ідентифікації згенерованих штучним інтелектом зображень людей засобами машинного навчання складається з наступних кроків (рисунок 1):

- завантаження датасетів;
- пре-процесинг зображень;
- створення нової чи редагування вже існуючої архітектури нейромережі;
- тренування;
- аналіз результатів та корегування мережі.

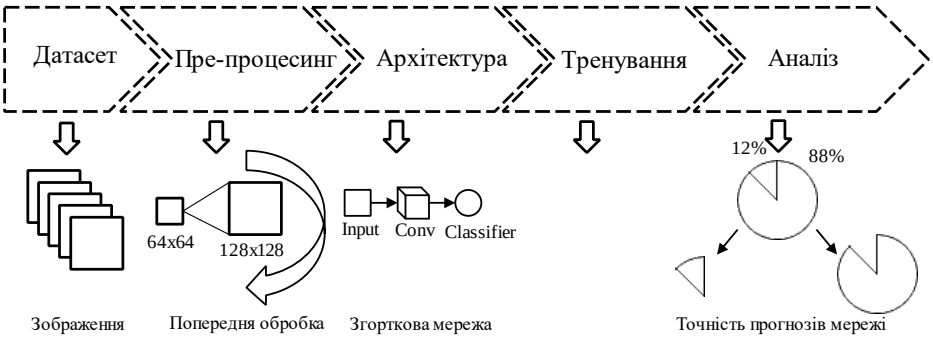

Рисунок 1 – Структура методу

Функціональна складова буде розділена на дві окремих нейронних мережі: imageClassifier, що відповідає за ідентифікацію зображення як реального чи підробки, та methodClassifier, що визначає збіг з популярними моделями ШІ для генерації зображень (рисунок 2).

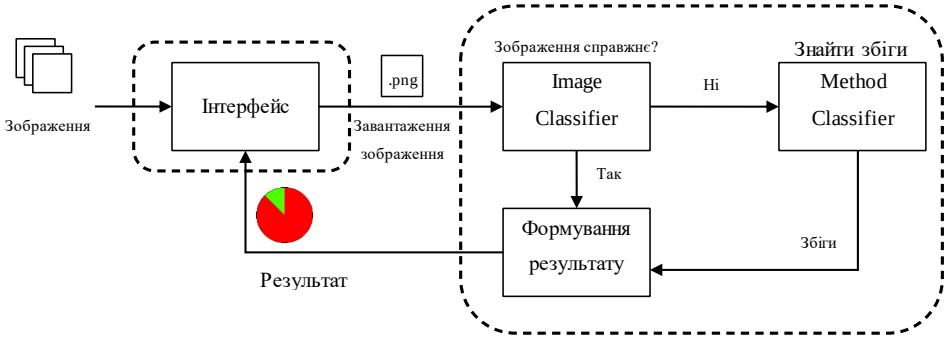

Рисунок 2 – Схема роботи методу

Вхідними данними є файли зображення, що користувач завантажує через інтерфейс, кожне зображення обробляє нейронна мережа imageClasifier, в залежності від результату додатково використовується methodClasifier, а результатом функціонального виконання є класифікація зображення як реального чи згенерованого, та віднесення до можливих методів генерації.

Інформаційна система нейромережевого аналізу згенерованих зображень облич людей засобами машинного навчання є прикладною програмною реалізацією методу аналізу зображень обличь людей, із файлу завантаженим користувачем, що призначений для пошуку згенерованим штучним інтелектом зображень та вхідними даними має. Вхідними є файл(и) зображень, такі як: png, ,jpg, webp, tiff, bmp.

Інформаційна структура системи складається із набору зображень (датасетів) та кількох підсистем: «Підсистема взаємодії з НМ», «Підсистема розпізнавання завантажених зображень», «Підсистема інтерфейсу користувача», «Підсистема налаштувань».

Набір даних зображень складається із наведених датасетів, що були розподілені дві відповідні частини:

– класифікація зображень – датасети розділені на реальні та згенеровані зображення для нейромережі imageClasifier;

– класифікація методів створення – датасети з виключно згенерованих зображень поділені відповідно до технології генерації.

Підсистема роботи з НМ є головною, що призначена для роботи з методами нейронних мереж [8, 9]. Включає в себе ряд функцій, таких як: створення та зміна архітектури нейромережі, конфігурація параметрів нейромережі, вибір датасетів та процес тренування, а також збереження натренованої мережі у відповідний файл.

Підсистема розпізнавання зображень є вторинною, вона призначена для аналізу завантаженого зображення чи декількох зображень обраною натренованою нейромережею, завантаженою з файлу. Має наступний функціонал: завантаження зображення з подальшим звільненням файлу, завантаження файлу нейромережі та виведення отриманих результатів.

Підсистема інтерфейсу користувача забезпечує функціональну взаємодію користувача з іншими підсистемами за допомогою UI. Включає в себе динамічну генерацію візуальних елементів відповідно до дій користувача.

Підсистема налаштувань дає можливість користувачу змінювати обрані параметри, як і візуальні, як розмір вікна, так і функціональні, обрані бібліотеки та файли.

Підсистема взаємодії з НМ, що основним призначенням має роботу з нейромережею (рисунку 3).

Першою функцією підсистеми є вибір шляхів до зображень. Для успішного завантаження зображень потрібно коректно вказати шлях до основної директорії та директорії для тренування та тестування. Із вказаних директорій будуть взяті зображення та розподілені по класам відповідним їх назв.

Наступною функцією є завантаження зображень у даталоадери, де є можливість вказати основні параметри: розмір зображення для трансформації, розмір однієї групи та потреба в перемішуванні.

Наступною групою функцій є створення та редагування архітектури нейромережі з можливістю додатки обрану кількість шарів з вказанням їх основних параметрів: вхідна та вихідна розмірність, розмір кернела, крок, нульове заповнення та інші відповідні пареметри.

Кінцевою функцією є налаштування тренування із вказанням параметрів: кількість епох, оптимізатор та його параметри. Після успішного завершення тренування є можливість зберегти отриману мережу.

Рисунок 3 – Схема та функції підсистеми взаємодії з НМ

Була розроблена схема пропонованої програмної архітектури для інформаційної системи нейромережевого аналізу згенерованих зображень облич людей (рисунок 4).

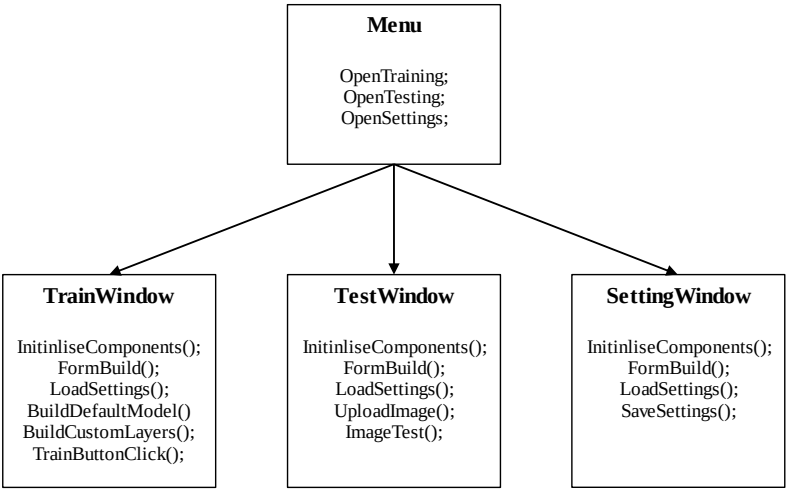

Рисунок 4 – Програмна архітектура системи

Програмна архітектура системи є об'єктно-орієнтованою та складається з наступних класів:

– Menu – внутрішній клас що реалізує перехід між іншими класами;

– ModelTrain.py – зовнішній клас що реалізує методи тренування мережі;

– TrainWindow – внутрішній клас що реалізує роботу з нейромережами;

– ImageTest.py – зовнішній клас що реалізує методи завантаження та аналізу зображення;

– TestWindow – внутрішній клас що реалізує аналіз завантажених зображень;

– SettingWindow – внутрішній клас що реалізує можливість зміни налаштувань програми.

Клас «TrainWindow», основним призначенням якого є створення та редагування архітектури, тренування нейромережі. Методи InitialiseComponent() та FormBuild() призначені для ініціалізації та створення форми використовуючи C#. Метод LoadSettings() завантажує налаштування програми із відповідного файлу. Метод TrainButtonClick() завантажує параметри нейромережі із відповідних полів та запускає процес тренування використовуючи завантажений ModelTrain.py Python клас. Метод CreateCustomLayers() динамічно довантажує нові елементи UI для створення власної архітектури мережі.

Клас «ModelTrain.py» використовує методи Torchvision мови Python для тренування мережі та має наступні методи: SetImagePaths() для завантаження шляхів зображень, LoadImages() завантажує файли зображень що далі використовуються в ToDataloaders() для перетворення завантажених зображень у формат даних для навчання мережі, BuildDefaultModel() завантажує спроєктовану по замовчуванню архітектуру, в свою чергу BuidCustomModel() створіє її динамічно, а метод Run() запускає процес навчання з подільшим збереженням мережі.

Клас «TestWindow» використовує навчену нейромережу для аналізу завантаженого користувачем зображення та виводу результатів. Метод LoadSettings() аналогічно відповідному методу класа TrainWindow ззавантажує файл налаштувань. Метод UploadImage() викликає інтерфейс для вибору та завантаження зображення в додаток та його звільнення для паралельної обробки використовуючи метод BitmapSwap. Метод ImageTest() завантажує ImageTest.py Python клас для аналізу зображення обраною нейронною мережею та виводить результат в UI.

Клас «SettingWindow» здійснює роботу з елементами інтерфейсу для завантаження та редагування налаштувань додатку. Метод LoadSettings() призначений для завантаження файлу налаштувань та заповнення елементів UI для подальшого редагування. Метод SaveSettings() зберігає чи перезаписує налаштування у відповідний файл для подальшого використання іншими класами.

Таким чином, був розроблений метод для ідентифікації згенерованих штучним інтелектом зображень людей засобами машинного навчання на основі використання комбінацій згорткових нейронних мереж. Спроєктовано

інформаційну структуру системи нейромережевого аналізу згенерованих зображень облич людей засобами машинного навчання, що за вхідним зображенням дозволяє визначити автентичність зображення та визначити можливі засоби його генерації. Також було спроєктовано програмну архітектуру інформаційної системи для прикладної програмної реалізації розробленого методу нейромережевого аналізу згенерованих зображень облич людей.

Перелік посилань

1. Мазурець О.В., Скрипник Т.К., Ізотов А.В. Фасетковий метод перетворення зображень за допомогою нейромережевого розпізнавання. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2020, №1 (281). – С.119-125.
2. Mazurets O., Uspenska K., Vit R., Tyschenko O. Intelligent System for Determining the Object Attributes Values by Neural Networks Means by Graphic Images in Databases. Current Trends in the Development of Scientific Research in Today's Conditions. Proceedings of XXV International scientific and practical conference. May 29-31, 2024. International Scientific Unity. Florence, Italy. 2024. Pp. 86-91.
3. Kharysh I., Sobko O., Mazurets O. Designing CNN Neural Network Model for Detecting Fractures of Lower Extremities by X-ray Images. The Impact of Scientific Research on the Development of the Modern World. Proceedings of the XLIV International scientific and practical conference. October 23-25, 2024. Dubrovnik, Croatia. 2024. Pp. 91-96.
4. Mazurets O. V., Klimenko V. I., Molchanova M. O., Sultanov A. V. Object-Oriented Intelligent System for Neural Network Detection of Sugar Crystallization Zones. Global Science: Prospects and Innovations. Proceedings of the 10th International scientific and practical conference. Cognum Publishing House. Liverpool, United Kingdom. 2024. Pp. 198-207.
5. Mazurets O., Zalutska O., Tyschenko O., Bohdanova A. An Approach to Using MobileNet CNN-model for Gesture Recognition. Proceedings of XXIII International Scientific and Practical Conference «Problems of Science and Technology: the Search for Innovative Solutions». May 15-17, 2024. Munich, Germany. 2024. Pp. 59-64.
6. Pokhytun A., Mazurets O., Molchanova M., Tyschenko O. Method for Neural Network Detecting Changed Images of People's Faces Using CNN. New Horizons in Scientific Research: Challenges and Solutions. Proceedings of the 1st International scientific and practical conference. October 21-23, 2024. Marseille, France. 2024. Pp. 35-40.
7. Mazurets O., Molchanova M., Klimenko V., Klopotivskyi D. Datalogic Model for Image Recognition by Convolutional Neural Network Using Cloud Services. Proceedings of XXII International Scientific and Practical Conference «Modern Scientific Research: Theoretical and Practical Aspects». May 8-10, 2024. Oslo, Norway. 2024. Pp. 64-68.
8. Novak Y., Mazurets O. Practical Application of Method of Automated Personal Identification by Fingerprints Using Convolution Neural Networks. Proceedings of V International Scientific and Practical Conference «Modern strategies of global scientific solutions». December 27-29, 2023. Stockholm, Sweden, International Scientific Unity. 2023. Pp. 136-140.
9. Мазурець О.В., Петровський С.С., Дидо Р.А. Нейромережева модель для ідентифікації особистості за зображенням обличчя у реальному часі Інформаційні технології і автоматизація. Матеріали XVII міжнародної науково-практичної конференції. 31 жовтня – 1 листопада 2024 р. Одеса, ОНТУ. 2024. С.655-658.