УДК 004.8

Похитун А.В., Мазурець О.В., Молчанова М.О., Бармак О.В.

Хмельницький національний університет

ПІДХІД ДО ФОРМУВАННЯ ДАТАСЕТУ ДЛЯ НЕЙРОМЕРЕЖЕВОГО ВИЯВЛЕННЯ МОДИФІКОВАНИХ ФОТОГРАФІЙ ОБЛИЧ ЛЮДЕЙ

У роботі розроблено та програмно реалізовано метод виявлення модифікованих зображень облич людей. Метод розроблений для перетворення вхідних даних у вигляді датасету у вихідні дані, а саме тип, клас, складність та ймовірність модифікації. Також було проаналізовано готові датасети та створено власний датасет, що містить 4 класи, кожен із класів містить 200 зображень різної розмірності, а зведення до одного розміру реалізується програмно.

The method of detecting modified images of people's faces was developed and implemented in software. The method is designed to transform input data in the form of a dataset into output data, namely type, class, complexity, and modification probability. Ready-made datasets were also analyzed and a custom dataset containing 4 classes was created, each of the classes contains 200 images of different dimensions, and reduction to one size is implemented programmatically.

У сучасному світі змінити зовнішній вигляд по фото не є важкою задачею. Одним із найбільш впливових факторів є поява генеративних моделей які здатні створювати досить реалістичні зображення облич людей, або змінювати їх.

Нейронна мережа – це застосунок, або обчислювальна модель машинного навчання, яка приймає рішення подібно до людського мозку та складається з великої кількості взаємопов'язаних елементів – нейронів [1]. Нейронні мережі використовуються для розв'язання різноманітних завдань, зокрема в обробці зображень, розпізнавання мови, тексту та у багатьох інших сферах [2, 3].

Генеративні моделі – це види машинного навчання, що можуть генерувати нові данні подібні до тих, на яких була навчена модель [4]. Це можуть бути не лише зображення а й фото, тексти, відео тощо.

Серед великої кількості видів модифікацій, можна виділити декілька, які користуються найбільшою популярністю

- цифрові фільтри та косметичні зміни;
- глибинні фейки;
- морфінг;
- алгоритм обробки зображень.

Отож, існує досить багато можливостей для коригування, редагування та обробки зображень, тому важливо вміти розрізняти фейкові зображення від

реальних оскільки модифіковані фото можуть використовуватись не лише для забави а й для підробки документів, цькування, що може мати досить негативні наслідки.

Мета роботи полягає у формуванні датасету та створенні методу для виявлення модифікованих зображень облич людей засобами нейромережевої класифікації.

Для розробки методу виявлення модифікованих зображень облич людей, критично важливо мати добре структуровані вхідні дані. В глобальній мережі доступна досить велика кількість датасетів, проте не всі із них підходять для цієї задачі. Під час розробки методу виявлення модифікованих зображень облич людей, у відкритому доступі, було знайдено декілька датасетів з яких було сформовано один, структурований набір даних із різними класами.

Зокрема для створення набору даних, були використані, вже готові, наступні датасети:

– FRLL-morphs (200 зображень);
– deepfake_faces (200 зображень);
– набір даних розроблений департаментом комп'ютерних наук університету Йонсей (200 зображень).

FRLL-morphs – набір структурованих даних, сформованих на основі даних взятих із Face Research London Lab [5]. Однією із ключових переваг даного датасету є те, що модифіковані зображення створювались різними методами (Рисунок 1).

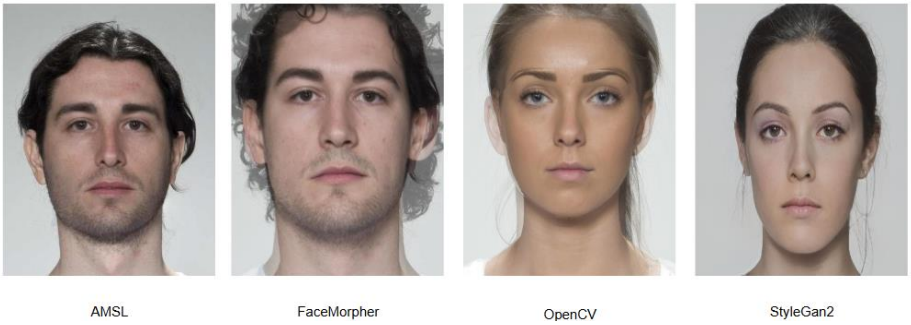

Рисунок 1 – Приклад модифікованих зображень різними алгоритмами [5]

На Рисунку 2 видно, що алгоритми AMSL та StyleGan2 досить важко розпізнати модифікацію, а ПЗ FaceMorpher та алгоритм OpenCV мають характерне розмиття на фоні.

Deepfake_faces - набір даних, розмірністю 224 на 224 пікселі, що є переваго, оскільки саме на таку розмірність існує досить багато навчених моделей [6]. На деяких зразках даного датасету присутні шуми (Рисунок 2).

Рисунок 2 – Приклад зображень датасету depfake_faces [6]

Набір даних розроблений департаментом комп'ютерних наук університет Йонсей містить декілька рівнів модифікацій, від простіших – відразу помітних, до більш складних [7], модифікації на яких важко помітити (Рисунок 3).

Рисунок 3 – Приклад зображень, створених департаментом комп'ютерних наук університету Йонсей [7]

На основі вищеописаних датасетів, було створено власний датасет із різними та рівнями модифікацій (Рисунок 4).

Отже, було проаналізовано готові набори даних, та створено власний датасет. Створений набір даних містить наступні класи, підкласи:

- deepfake;
- real;
- ipa (easy, mid, hard);
- morphing (amsl, facemorfer, opencv, webmorpher, stylefan2).

Кожен із класів містить 200 зображень різної розмірності. Зведення до одного розміру реалізується програмно.

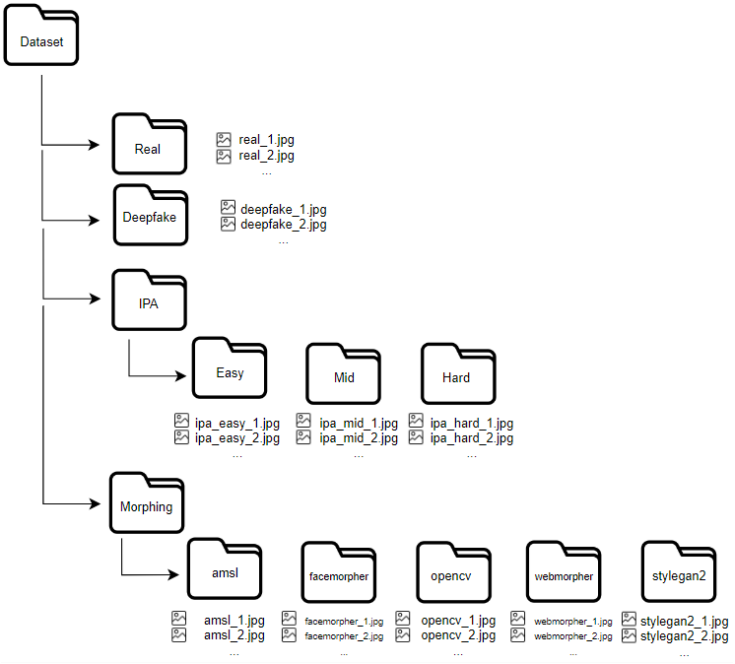

Рисунок 4 – Структура створеного датасету

Метод виявлення модифікованих зображень облич людей призначений для перетворення вхідних даних у вигляді зображення, у вихідні дані у вигляді результату класифікації, а саме тип, складність (якщо це дозволяє датасет) та алгоритм за допомогою якого було модифіковане фото (Рисунок 5).

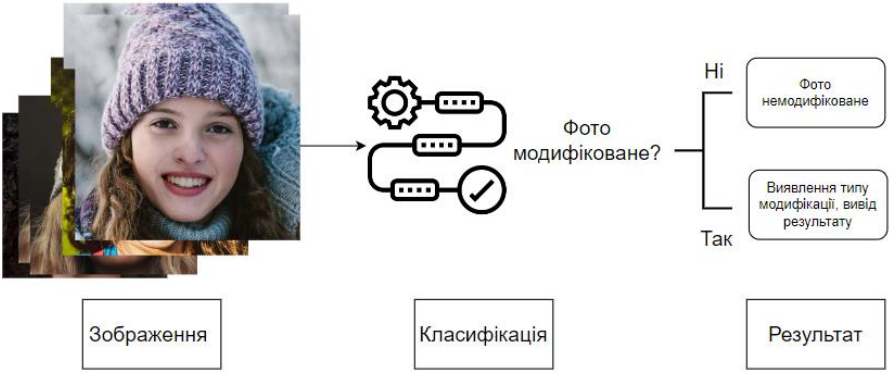

Рисунок 5 – Візуалізація роботи методу визначення модифікованих зображень

Для вхідних даних було створено датасет із приблизно 1500 зображеннями різних класів, а також тестова вибірка зображень для оцінки коректності (Рисунок 6).

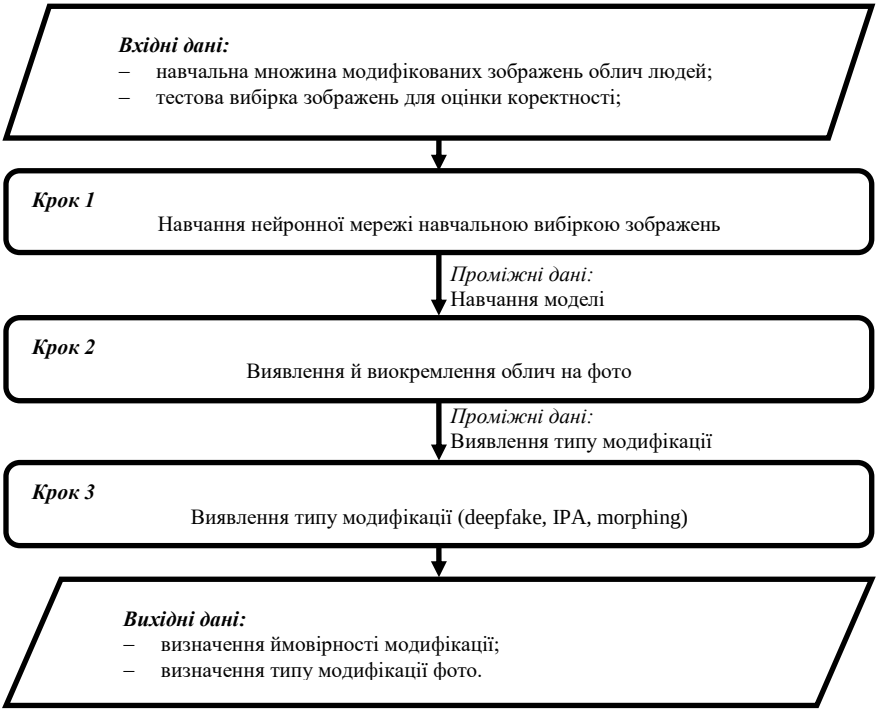

Рисунок 6 – Схема методу виявлення модифікованих зображень облич людей

Процес виявлення модифікованого зображення обличчя можна розділити на декілька етапів: виявлення облич на фото, навчання нейронної мережі за допомогою датасету та класифікація зображення [8, 9].

Першим етапом є навчання нейромережевої моделі, яке відбувається за допомогою навчальної множини зображень (датасету) [10]. Також є можливість завантажити попередньо навчену модель, щоб не витрачати час на повторне навчання [11].

Другий етап – виявлення та виокремлення облич на фото. На даному етапі відбувається перевірка, чи взагалі присутнє обличчя на зображенні і чи є сенс в подальшій перевірці на модифікації.

Завершальний етап, виявлення типу модифікації, складності та алгоритму, за допомогою якого фото було модифіковане (якщо це дозволяє датасет).

Вихідними даними методу виявлення модифікованих зображень облич, є результат у вигляді ймовірності належності зображення до конкретної модифікації.

Отже, було проаналізовано готові набори даних, та створено власний датасет. Створений набір даних містить 4 класи, кожен із класів містить 200 зображень різної розмірності. Зведення до одного розміру реалізується програмно. Також було розроблено метод виявлення модифікованих зображень облич людей. Метод розроблений для перетворення вхідних даних у вигляді датасету у вихідні дані, а саме тип, клас, складність та ймовірність модифікації.

Перелік посилань

1. 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.
2. 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.
3. 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.
4. 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.
5. FRLL-morphs: URL - https://www.idiap.ch/en/scientific-research/data/frll-morphs
6. Deepfake_faces: URL - https://www.kaggle.com/datasets/dagnelies/deepfake-faces
7. BlazeFace: URL - https://github.com/hollance/BlazeFace-PyTorch
8. 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.
9. 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.
10. 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.
11. 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.