УДК 004.8 : 004.032.26 : 004.932

https://doi.org/10.52058/2786-6025-2026-1(55)-2704-2716

Яровий Андрій Анатолійович доктор технічних наук, професор, завідувач кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0000-0002-6668-2425

Озеранський Володимир Сергійович кандидат технічних наук, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0009-0007-1694-2317

Петришин Сергій Іванович кандидат технічних наук, старший викладач кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0009-0001-3465-1499

Паночишин Юрій Миколайович кандидат технічних наук, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0000-0003-1546-3422

Юхимчук Олексій Костянтинович магістр кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, https://orcid.org/0009-0001-3057-5775

ОСОБЛИВОСТІ РОЗРОБКИ НЕЙРОМЕРЕЖЕВОЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ПІДРОБЛЕНИХ ЗОБРАЖЕНЬ

Анотація. У роботі охарактеризовано особливості розробки нейромережевої технології для виявлення підроблених зображень. Відзначено актуальність тематики дослідження та обґрунтовано доцільність застосування комбінованого методу, який поєднує аналіз кольорових аномалій і спектральний аналіз зображень за допомогою швидкого перетворення Фур'є (FFT). Описано принципи створення ознак, що включають використання RGB-каналів та їх попарних різниць, а також отримання частотного представлення у формі нормалізованого спектра. Поєднавши вказані підходи, з'являється можливість аналізу зображень як в кольоровому, так і в частотному просторі, що створює передумови для підвищення точності та надійності виявлення підробок, а також зменшення кількості помилкових спрацювань. У роботі описано процес проєктування програмних модулів нейромережевої інформаційної технології, визначено архітектуру системи та логіку взаємодії її компонентів. Обґрунтовано

вибір програмних засобів і бібліотек машинного навчання для реалізації запропонованого підходу, зокрема Python та сучасних фреймворків глибинного навчання і веб-інтеграції. Для навчання та оцінювання ефективності нейронних мереж було відібрано відповідні набори даних, що містять як реальні, так і згенеровані зображення, зокрема Deepfake Detection Challenge (DFDC), FaceForensics++, Celeb-DF, GANGen та IMD2020. Проведено функціональне тестування розробленої технології в умовах, наближених до реальної експлуатації. Отримані результати підтверджують перспективність запропонованого підходу та можуть слугувати основою для подальшого розвитку систем автоматизованого аналізу, перевірки достовірності та моніторингу цифрового медіа-контенту.

Ключові слова: виявлення підроблених зображень, швидке перетворення Фур'є, кольорові аномалії, нейронні мережі, інформаційні технології, програмування, проєктування інформаційних систем.

Yarovyi Andrii Anatoliyovych Doctor of Engineering Sciences, Professor, Head of the Department for Computer Science, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0000-0002-6668-2425

Ozeranskyi Volodymyr Serhiiovych Candidate of Engineering Sciences, Associate Professor at the Department for Computer Science, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0009-0007-1694-2317

Petrishyn Sergiy Ivanovych Candidate of Engineering Sciences, Senior Lecturer at the Department of Computer Science, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0009-0001-3465-1499

Panochyshyn Yurii Mykolaiovych Candidate of Engineering Sciences, Associate Professor at the Department for Computer Science, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0000-0003-1546-3422

Yukhymchuk Oleksii Kostiantynovych Master of the Department for Computer Science, Vinnytsia National Technical University, Vinnytsia, https://orcid.org/0009-0001-3057-5775

FEATURES OF THE DEVELOPMENT OF NEURAL NETWORK INFORMATION TECHNOLOGY FOR DETECTING FAKE IMAGES

Abstract. The paper presents the features of developing neural network technology for detecting fake images. It highlights the relevance of the research topic

and justifies the use of a combined method that combines color anomaly analysis and spectral analysis of images using fast Fourier transform (FFT). The principles of feature creation are described, including the use of RGB channels and their pairwise differences, as well as obtaining a frequency representation in the form of a normalized spectrum. By combining these approaches, it becomes possible to analyze images in both color and frequency space, which creates the conditions for improving the accuracy and reliability of counterfeit detection, as well as reducing the number of false positives. The paper describes the process of designing software modules for neural network information technology, defines the system architecture and the logic of interaction between its components. The choice of software tools and machine learning libraries for implementing the proposed approach is justified, in particular Python and modern frameworks for deep learning and web integration. To train and evaluate the effectiveness of neural networks, appropriate datasets containing both real and generated images were selected, including Deepfake Detection Challenge (DFDC), FaceForensics++, Celeb-DF, GANGen, and IMD2020. Functional testing of the developed technology was carried out in conditions close to real-life operation. The results obtained confirm the promising nature of the proposed approach and can serve as a basis for the further development of automated analysis, authenticity verification, and monitoring systems for digital media content.

Keywords: detection of fake images, fast Fourier transform, color anomalies, neural networks, information technology, programming, information system design.

Постановка проблеми. У сучасному інформаційному суспільстві проблема достовірності даних набуває ключового значення. Активний розвиток технологій комп'ютерної графіки та штучного інтелекту на даному етапі забезпечив можливість створювати реалістичні підроблені зображення та відео. Одним із найяскравіших проявів цього явища є deepfake – синтетичний медіаконтент, згенерований за допомогою глибинних нейронних мереж, найчастіше архітектур на основі Generative Adversarial Networks (GAN) або автокодерів [1].

Спершу ці технології були розроблені для творчості, індустрії моделювання та кіно, але за останній час стали популярними у зловживанні: дезінформаційні кампанії, «політичні» дестабілізації, тиску та злочинності в Інтернеті [2]. Оскільки підроблені зображення стають все більш реалістичними, що створює прецеденти, коли звичайний користувач не може їх відрізнити від справжніх, тому виникає потреба у створенні надійних автоматизованих методів детекції підробок.

Аналіз останніх досліджень і публікацій. З кожним днем спостерігається стрімке зростання обсягів зображень, створених або відредагованих за допомогою штучного інтелекту. За інформацією прес-релізу компанії Adobe, опублікованого у серпні 2023 року, кількість зображень створених за

допомогою Adobe Firefly, досягла 1 мільярд лише через 3 місяці після запуску. Загалом за допомогою Stable Diffusion, Adobe Firefly, Midjourney та DALLE-2 було згенеровано понад 15 мільярдів зображень, створених за допомогою штучного інтелекту. Це третина від кількості зображень, будь-коли завантажених в Instagram [3].

Дослідження, яке провели вчені з Університету Ватерлоо продемонструвало що майже 40% респондентів не змогли відрізнити зображення облич людей, створені штучним інтелектом, від реальних фотографій [4]. Для більшості користувачів підроблені зображення можуть не становити безпосередньої небезпеки, проте існують соціальні групи та окремі особи, які можуть суттєво постраждати через використання штучно створених або підроблених візуальних матеріалів, зокрема у випадках маніпуляцій, дискредитації, поширення фейкових новин чи порушення приватності.

Науковці пропонують різні підходи до розв'язання цієї проблеми. Традиційні методи виявлення підробки ґрунтуються на метаданих фотографій і файлів; наприклад, їх структурі та історії редагування. Однак ці шляхи виявлення є вразливі до повторного збереження зображення. Інший метод зосереджений на артефактах обробки, що породжені складними алгоритмами стиснення та генерації відтінків шкіри зображень: дублювання блоків JPEG та відтінків шкіри, взаємодії кольорів між собою тощо. Однак, останнім часом найбільш ефективними виявляються методи, що застосовують глибинне навчання.

Зокрема, згорткові нейронні мережі (НМ), рекурентні НМ та сучасні трансформери досягають вражаючих результатів і є домінуючими типами архітектур НМ для класифікації фейк-зображень.

Разом з тим, незважаючи на досягнуті успіхи, існує кілька проблемних аспектів. По-перше, нові генеративні моделі, такі як StyleGAN, Stable Diffusion та їх модифікації, реалізують підробки, що мають суттєво менше характерних артефактів, що ускладнює їх детекцію. По-друге, майже всі алгоритми виявлення «навчалися» на певних типах підробок і демонструють зниження точності на нових, невідомих даних. По-третє, існує проблема низької стійкості моделей до спотворень, які з'являються у реальному середовищі (повторне стиснення JPEG, зниження роздільної здатності, накладання шуму тощо) [5].

У цьому контексті з'являється потреба у розробці комбінованих методів, що об'єднують декілька різних видів характеристик. У цьому дослідженні пропонується комбінований метод, що враховує як просторові характеристики зображень (RGB-формат), так і їхні спектральні властивості (перетворення FFT).

Основна ідея полягає в тому, що хоча згенероване зображення може виглядати досить реалістично, його спектральна структура часто містить закономірності, відмінні від справжніх фотографій.

Мета статті – розробка нейромережевої інформаційної технології виявлення підроблених зображень, а також огляд її структури, інструментів реалізації, набору даних для навчання.

Задачі дослідження:

1. Визначити доцільність комбінування методів визначення аномалій за різними ознаками для виявлення підроблених зображень.

2. Виконати проєктування архітектури нейромережевої інформаційної технології, обрати програмні технології для реалізації, здійснити огляд відповідних датасетів.

3. Здійснити програмну реалізацію нейромережевої інформаційної технології виявлення підроблених зображень та виконати тестування.

Виклад основного матеріалу. Проаналізовавши різні методи виявлення підроблених зображень, особливу увагу було приділено аналізу частотних та колірних характеристик. Найбільш перспективним виявився комбінований підхід FFT+RGB, що об'єднує обчислення двовимірного швидкого перетворення Фур'є (Fast Fourier Transform – FFT) [6] з аналізом кольорових каналів зображення в RGB-просторі.

Такий підхід дає змогу суттєво оцінити як просторову структуру зображення, так і можливі колірні аномалії, які можуть виникати під час генерації чи маніпуляцій за допомогою штучних методів.

Обґрунтування вибору послідовності дій у комбінованому методі:

1) FFT дозволяє виділити частотні елементи зображення. У реальних фотографіях спектральні характеристики слідують певним закономірностям, тоді як у згенерованих зображеннях часто спостерігаються високочастотні шуми, нерівномірні текстури або артефакти згладжування;

2) RGB-аналіз допомагає виявити невідповідності в кольорових каналах. Реальні фотографії відрізняються корельованістю каналів R, G та B. Тоді як у підроблених зображеннях (наприклад, deepfake або GAN-зображеннях) можуть спостерігатися порушення у балансі кольорів чи неприродні переходи;

3) Комбінування FFT+RGB забезпечує взаємне доповнення. Частотний аналіз підсилює здатність виявляти приховані текстурні дефекти, тоді як аналіз колірних каналів допомагає зафіксувати глобальні невідповідності в спектрально-колірному просторі.

Зазначений метод включає такі основні етапи:

1. Аналіз кольорових аномалій

Для вивчення колірних невідповідностей була розроблена спеціальна архітектура нейронної мережі, яка обробляє канали R, G, B та їх попарні різниці (R–G, R–B, G–B).

Таким чином формується 6-канальне вхідне зображення, що дає змогу моделі виявляти приховані аномалії у кореляції кольорів.

Таким чином, модель навчається розпізнавати нетипові патерни кольорових зв'язків, що характерні згенерованим чи відредагованим зображенням, але рідко зустрічаються у реальних фотографіях.

Математично вхідні ознаки описуються так:

$$X = \{R, G, B, (R-G), (R-B), (G-B)\} \quad (1)$$

$$y = f_{CNN}(X)\,,\ y\ \in [0,1] \quad (2)$$

де y – ймовірність підробки.

2. Спектральний аналіз на основі FFT

Для кожного зображення виконується перетворення Фур'є:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (3)$$

У результаті формується спектр амплітудних компонентів:

$$|\ F(u,v)\ | = \sqrt{Re(F(u,v))^2 + Im(F(u,v))^2} \quad (4)$$

Для стабільності розрахунків застосовується логарифмування:

$$S(u,v) = \log(|F(u,v)| + \epsilon), \quad \epsilon = 10^{-8} \quad (5)$$

Нормалізований спектр подається у нейромережу для навчання та визначення ознак підробок. На основі досліджень можна відзначити, що реальні зображення характеризуються більш «згладженим» спектром із високою концентрацією енергії в діапазоні низьких частот. На відміну від них, фейкові зображення містять додаткові піки та високочастотні шуми, пов'язані з алгоритмами генерації (рис. 1) [7].

Рисунок 1 – Спектр справжнього та підробленого зображення

Окрім цього, у фейкових зображеннях при візуалізації окремих каналів (R, G, B) можна помітити різницю у кольоровій насиченості та балансі, що додатково демонструє переваги використання комбінованого методу.

Враховуючи проаналізовані методи виявлення підроблених зображень необхідно спроектувати та розробити модулі інформаційної технології, які дозволять звичайному користувачу взаємодіяти з нею.

Модулі повинні забезпечувати виконання основних вимог для виконання перевірки зображення.

Нейромережева інформаційна технологія складається з 4 модулів:

1. Модуль клієнта (веб-інтерфейс).
2. Серверний модуль (отримання/відправлення даних).
3. Модуль обробки зображення та нейронної мережі.
4. Модуль збереження статистики.

Розглянемо детальніше кожен зазначений програмний модуль.

Модуль клієнта (веб-інтерфейс).

Для кінцевого користувача необхідно мати простий та одночасно зручний інтерфейс для взаємодії з інформаційною технологією. З огляду на ці вимоги доцільним рішенням є розробка веб-додатку, як оптимальний спосіб доступу до системи.

Веб-інтерфейс дозволить: завантажувати зображення зручним способом, переглядати результат в зручному форматі.

Серверний модуль (отримання/відправлення даних).

Серверний модуль відповідає за приймання зображень від користувачів та їхню передачу до модуля попередньої обробки зображень для нейронних мереж, а також надсилання результатів аналізу до клієнтської частини.

Модуль обробки зображення та нейронної мережі.

Модуль виконує всі необхідні маніпуляції по зображенню. Такими маніпуляціями є змінення розміру, нормалізації пікселів та перетворення у потрібні колірні формати.

Після цього отримані дані передаються у нейронну мережу для виконання аналізу і повернення результату у вигляді значення ймовірності підробки від 0 до 1.

Модуль збереження статистики.

Модуль статистики є не обов’язковим, проте важливим для подальшого покращення нейромережевої інформаційної технології. Модуль зберігає дані про зображення та результат перевірки.

Структурну схему розробленої нейромережевої інформаційної технології виявлення підроблених зображень та особливості взаємодії її програмних модулів наведено на рис. 2.

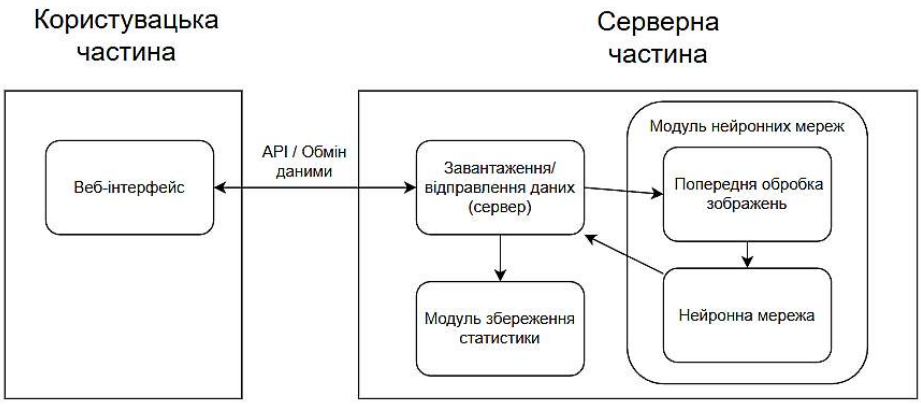

Рисунок 2 – Структурна схема нейромережевої інформаційної технології виявлення підроблених зображень

Нижче наведено діаграму послідовностей розробленої нейромережевої інформаційної технології виявлення підроблених зображень:

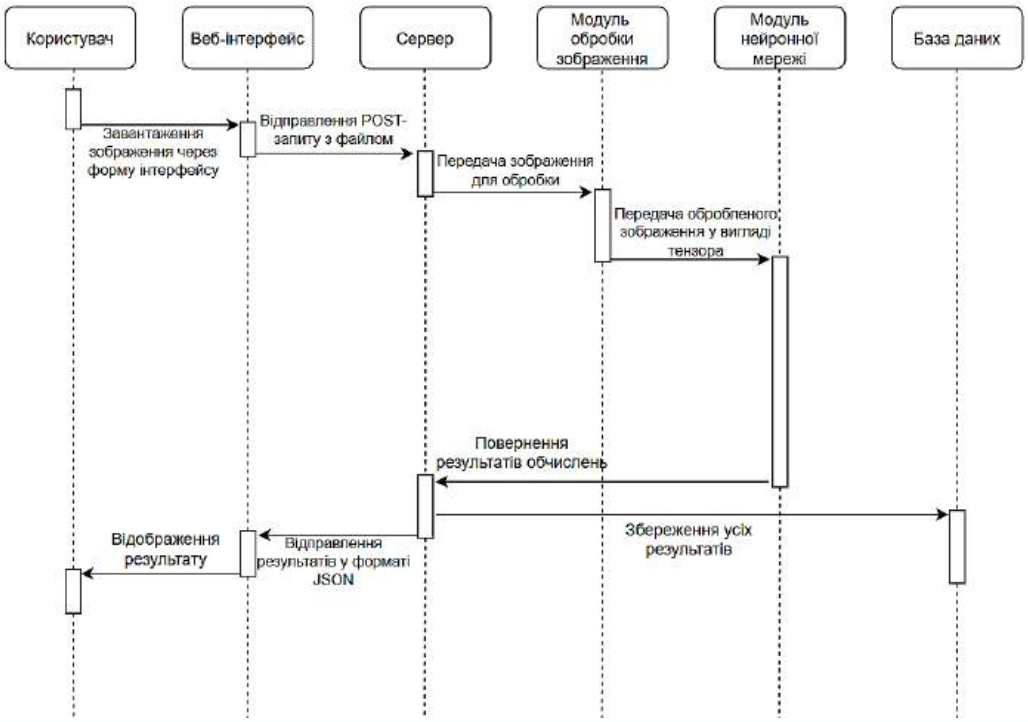

Рисунок 3 – Діаграма послідовностей нейромережевої інформаційної технології виявлення підроблених зображень

Для розробки модулів потрібно обрати програмні технології, які дозволять якісно їх реалізувати. Для клієнтської частини було обрано HTML, CSS та JavaScript, оскільки вони задовольняють всі поставлені потреби. Для серверної частини та для навчання нейронної мережі обрано Python, через його переваги:

1. Простота синтаксису.

Мова програмування Python є досить простою у синтаксисі порівнюючи з іншими мовами, такими як C++ або Java. Це дозволяє концентруватися на алгоритмах, параметрах та експериментах з моделями, а не на низькорівневих деталях реалізації системи.

2. Популярність та активна підтримка з машинним навчанням.

Деякі розробники зазначають, що Python є стандартом у сфері розробки систем штучного інтелекту [8]. Майже всі бібліотеки та фреймворки, які направлені для роботи з нейронними мережами розробляються саме під цю мову. Це дозволить прискорити розробку та тестування системи. А завдяки активній спільноті, великій кількості проєктів, документацій та обговорень можна оперативно вирішити різні проблеми, які можуть виникнути під час розробки системи.

3. Великий набір програмних бібліотек для роботи в різних сферах.

Для Python є велика кількість програмних бібліотек для вирішення різних типів завдань, наприклад:

– NumPy для числових обчислень;
– OpenCV та Pillow для попередньої обробки зображення;
– Matplotlib для візуалізації.

4. Простота інтеграції.

Python легко інтегрується з популярними веб-технологіями через FastAPI, Flask та Django, що робить можливим взаємодії користувача через веб-інтерфейс. Для взаємодії клієнта з сервером використовується FastAPI. FastAPI має дуже високу продуктивність на рівні NodeJS та є простим для навчання та використання.

У роботі з нейронними мережами використовуються технології TensorFlow та Keras.

TensorFlow – потужний інструмент для створення і навчання різноманітних моделей, починаючи від простих лінійних регресій і закінчуючи складними нейронними мережами [9]. Головною метою TensorFlow є створення універсальної платформи для формування обчислювальних графів. У таких графах вузли символізують математичні операції, а ребра – тензори, які являють собою багатовимірні масиви даних, що переміщуються між цими вузлами.

Переваги використання TensorFlow:

1. Висока продуктивність та масштабованість.

TensorFlow створений для оптимізації обчислень на процесорах CPU, графічних процесорах GPU та тензорних процесорах TPU, завдяки чому тренування моделей може відбуватися в десятки раз швидше. Підтримує паралельні обчислення, завдяки чому може бути запущений не тільки на одному комп’ютері, а також на кластерних серверах.

2. Гнучкість побудови моделей.

TensorFlow пропонує як низькорівневі, так і високорівневі методи. Використання Kesar дозволить швидко створювати моделі без потреб вивчення низькорівневих аспектів реалізації нейронних мереж, таких як оптимізація градієнтів, управління вагами, ручне визначення шарів або складних математичних операцій, які лежать в основі процесу навчання.

3. Кросплатформність та портативність.

Завдяки розробникам, TensorFlow може працювати на різних платформах без значних змін коду, а саме на Windows, macOS, Linux, Android, iOS, веббраузерах.

4. Налагодження та віртуалізація.

TensorFlow містить інструмент під назвою TensorBoard. Він дозволяє візуалізувати процес навчання (loss, accuracy, і т.п.). Дає змогу переглянути структуру моделі та проаналізувати графи обчислень.

5. Інтеграція з іншими бібліотеками.

TensorFlow легко інтегрується з великою кількістю бібліотек, які можуть допомогти для навчання, розгортання системи та аналізу.

6. Активна спільнота та документація.

TensorFlow користується широкою підтримкою розробницької спільноти, що забезпечує дуже багато прикладів, навчальних ресурсів та досліджень. Це робить процес навчання і пошуку рішень для різних труднощів набагато легшим. У даному дослідженні було використано програмну бібліотеку Keras, щоб спростити розробку та навчання нейронної мережі. Keras є високорівневим інтерфейсом для створення і навчання нейронних мереж, який у TensorFlow входить до складу бібліотеки як офіційний компонент (з версії TensorFlow 2.x). Головна концепція Keras зосереджена на простоті використання та модульності.

За замовчуванням TensorFlow буде використовувати лише центральний процесор (CPU), а його швидкість буде малою, тому для прискорення цього процесу необхідно завантажити та встановити додаткові інструменти CUDA Toolkit та cuDNN. CUDA Toolkit дозволяє використовувати GPU не лише для рендерингу графіки, а й для виконання загальних обчислень. cuDNN пропонує високооптимізовані рішення спеціально для архітектур глибокого навчання.

Для збереження статистики перевірки обрано SQLite. SQLite – бібліотека мовою програмування C, яка реалізує невеликий, швидкий, автономний, високонадійний, повнофункціональний механізм баз даних SQL. SQLite є найпопулярнішим механізмом баз даних. SQLite вбудований у всі мобільні телефони та більшість комп'ютерів, а також постачається в багато інших програм, які люди використовують щодня. У даному дослідженні обрано SQLite, оскільки вона є поширеною та надійною базою даних, яка має мінімальні вимоги до ресурсів та дозволяє створювати стабільні та ефективні застосунки.

Для реалізації модуля нейронних мереж, потрібен набір даних на якому буде навчатися нейромережа. При навчанні нейронних мереж використовувалися такі датасети:

1. Deepfake Detection Challenge (DFDC) є одним із найбільших відкритих датасетів, що містить тисячі відео зі справжніми та підробленими обличчями людей.

2. FaceForensics++ є поширеним набором даних для виявлення підроблених зображень. Він містить в собі відео змінненими різними алгоритмами та типами підробок (Face2Face, DeepFake, FaceSwap, NeuralTextures, FaceShifter). Датасет був представлений дослідниками TUM та Google у 2019 р.

3. Celab-DF (v1, v2) містить підроблені відео відомих людей. Має як реальні фрагменти, так і підроблені їх варіанти. Представлений дослідниками з UC Riverside у 2019 році, як удосконалений набір даних, який містить більш реалістичні та менш помітні ознаки підробки, ніж попередні датасети (FaceForensics++ або UADFV).

4. GANGen (StyleGan, RelGan, BEGAN, AttGan та ін.) – великий набір даних зібраних з різних джерел. Містить в собі велику кількість зображень згенерованих за допомогою різних архітектур Generative Adversarial Network.

5. IMD2020 – датасет розрахований для виявлення маніпуляцій з фотографіями (Copy-Move, Splicing, Removal, Inpainting). Опублікований дослідниками з Masaryk University у 2020 році, де підроблені зображення створюються людьми, а не нейромережею. Містить в собі справжні, підроблені зображення та маски редагування.

Після завершення основних модулів та інтеграції всіх складових нейромережевої інформаційної технології виявлення підроблених зображень було протестовано її роботу в реальних умовах експлуатації.

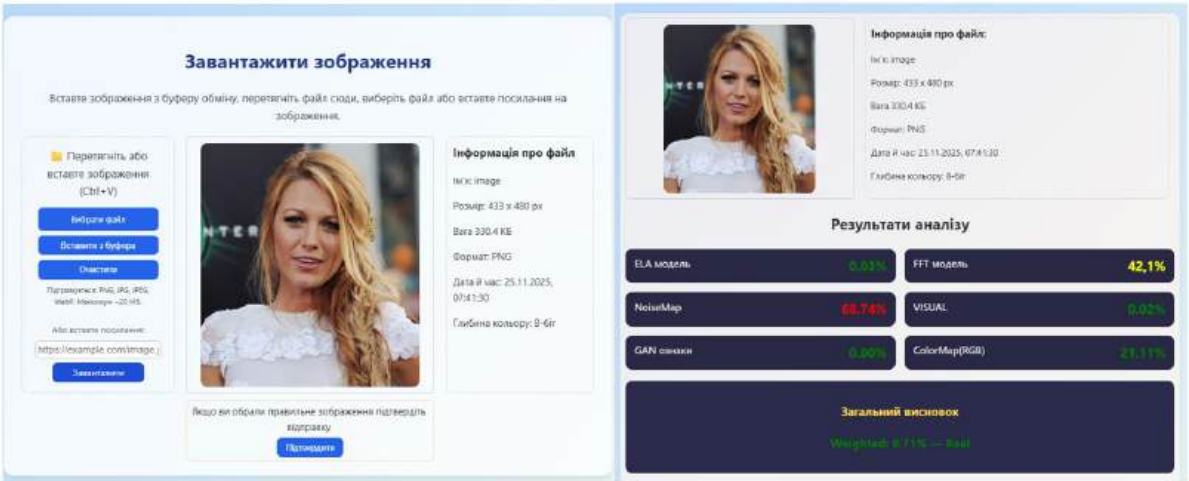

Рисунок 4 – Тестування нейромережевої інформаційної технології виявлення підроблених зображень

Висновки. Встановлено, що розробка нейромережевої інформаційної технології виявлення підроблених зображень є доцільною та актуальною задачею. Проведене дослідження показало, що комбінування аналізу кольорових аномалій та спектральних характеристик зображення є доцільним напрямом для розробки та удосконалення методів виявлення підроблених зображень. Запропонований комбінований підхід на основі поєднання аналізу за FFT та RGB дозволяє поєднувати локальні та глобальні ознаки зображень, що може стати основою для майбутніх експериментів та покращень нейромережевих моделей у цій області для виявлення підроблених зображень. Спроєктовано основні програмні модулі нейромережевої інформаційної технології та визначено їхню функціональну взаємодію. Проведено огляд технологій, застосованих під час розробки нейромережевої інформаційної технології, а також охарактеризовано датасети, використані для навчання. На основі сформованих вимог було реалізовано веб-орієнтовану версію нейромережевої інформаційної технології виявлення підроблених зображень, після чого виконано її тестування, що підтвердило коректність роботи програмних модулів, а також інформаційної технології загалом.

Література:

1. Ian Goodfellow, et al.: Generative Adversarial Nets. Advances in Neural Information Processing Systems, 2014. URL: https://arxiv.org/abs/1406.2661

2. Використання підробленими зображеннями. [Електронний ресурс] – Режим доступу до ресурсу: https://medialab.online/news/photoweapon/

3. Кількість створених зображень за допомогою Adobe Firefly [Електронний ресурс] – Режим доступу до ресурсу: https://journal.everypixel.com/ai-image-statistics

4. Дослідження з Університету Ватерлоо щодо реалістичності підробок [Електронний ресурс] - Доступ: https://techxplore.com/news/2024-03-survey-duped-ai-generated-images.html

5. StyleGAN [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/machine-learning/stylegan-style-generative-adversarial-networks/

6. Fast Fourier transform (FFT) [Електронний ресурс] – Режим доступу до ресурсу: https://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm

7. Convertini V. N., Impedovo D., Lopez U., Pirlo G., Sterlicchio G. Discrete Fourier Transform in Unmasking Deepfake Images: A Comparative Study of StyleGAN Creations // *Information*. – 2024. – Vol. 15, No. 11. – Art. 711. – DOI: 10.3390/info15110711

8. Чому Python стандарт для ШІ [Електронний ресурс] – Режим доступу до ресурсу: https://apix-drive.com/ua/blog/useful/chomu-mova-python-taka-vazhliva-dlja-rozvitku-shtuchnogo-intelektu

9. TensorFlow [Електронний ресурс] – Режим доступу до ресурсу: https://foxminded.ua/tensorflow-shcho-tse/

References:

1. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems. Retrieved from https://arxiv.org/abs/1406.2661

2. Vykorystannia pidroblenymy zobrazhenniamy [Use of fake images]. (n.d.). medialab.online. Retrieved from https://medialab.online/news/photoweapon/ [in Ukrainian].

3. Kilkist stvorenykh zobrazhen za dopomohoiu Adobe Firefly [Number of images created using Adobe Firefly]. (n.d.). journal.everypixel.com. Retrieved from https://journal.everypixel.com/ai-image-statistics [in Ukrainian].

4. Doslidzhennia z Universytetu Vaterloo shchodo realistichnosti pidrobok [Research from the University of Waterloo on the realism of fakes]. (2024). techxplore.com. Retrieved from https://techxplore.com/news/2024-03-survey-duped-ai-generated-images.html [in Ukrainian].

5. StyleGAN. (n.d.). geeksforgeeks.org. Retrieved from https://www.geeksforgeeks.org/machine-learning/stylegan-style-generative-adversarial-networks/

6. Fast Fourier transform (FFT). (n.d.). homepages.inf.ed.ac.uk. Retrieved from https://homepages.inf.ed.ac.uk/rbf/HIPR2/fourier.htm

7. Convertini, V. N., Impedovo, D., Lopez, U., Pirlo, G., & Sterlicchio, G. (2024). Discrete Fourier transform in unmasking deepfake images: A comparative study of StyleGAN creations. Information, 15(11), Article 711. https://doi.org/10.3390/info15110711

8. Chomu Python standart dlia ShI [Why Python is a standard for artificial intelligence]. (n.d.). apix-drive.com. Retrieved from https://apix-drive.com/ua/blog/useful/chomu-mova-python-taka-vazhliva-dlja-rozvitku-shtuchnogo-intelektu [in Ukrainian].

9. TensorFlow [TensorFlow: what it is]. (n.d.). foxminded.ua. Retrieved from https://foxminded.ua/tensorflow-shcho-tse/ [in Ukrainian].