УДК 378. 004.925

Сергій Чорний
кандидат технічних наук, доцент, провідний науковий співробітник
Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса»,
м. Харків, Україна.
ORCID ID 0000-0002-0445-2886
svch1mail@yahoo.com

Ольга Брендель
PhD, завідувач сектору комп'ютерно - технічних, телекомунікаційних досліджень та досліджень відео-, звукозапису
Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса», м. Харків, Україна.
ORCID ID 0000-0002-1723-0203
olgabrenda@ukr.net

Олег Мєшков
PhD, завідувач сектору пожежно-технічних та електротехнічних досліджень
Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса», м. Харків, Україна.
ORCID ID 0000-0002-3046-6018
mesh_ol@ukr.net

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВСТАНОВЛЕННЯ АВТЕНТИЧНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ ПІД ЧАС ПІДГОТОВКИ ФАХІВЦІВ СУДОВОЇ ЕКСПЕРТИЗИ

Анотація. Потенційні можливості та переваги методів штучного інтелекту сприяють розвитку та впровадженню інноваційних технологій у різні сфери науки, зокрема в галузі фотозйомки та відеозапису, що створює широкі можливості маніпулювання змістом цифрових зображень та актуалізує проблему встановлення їх автентифікації. Широке використання методів штучного інтелекту для редагування зображень інколи унеможливлює або ускладнює пошук змінених ділянок.

З огляду на це метою даної роботи є обґрунтування напрямків підготовки судової експертизи до використання методів штучного інтелекту при встановленні автентичності зображень , а основним завданням – дослідження сучасних способів їх оцінки.

Об'єктом даного дослідження є процес автентифікації цифрових зображень. Предмет дослідження – процеси цифрової обробки зображень, зокрема на основі моделей штучних нейронних мереж.

У статті проаналізовано використання моделей штучних нейронних мереж для оцінки автентичності зображень методом комплексного використання кількох методів оцінки шуму з узагальненням його спотворень у штучній нейронній мережі.

Особливу увагу приділено аналізу сучасних технологій редагування цифрових зображень з використанням методів штучного інтелекту. Наведено результати дослідження відомих методів попередньої обробки для виявлення неавтентичності зображень, відредагованих сучасними технологіями редагування та придатних для узагальнення методами штучного інтелекту. Розглянуто особливості використання нейромережевих класифікаторів для оцінки зон редагування зображення з попередньою обробкою методами фільтрації також у методологічній площині, а саме при підготовці фахівців у галузі фототехнічних досліджень та досліджень відеозапису. Наукова новизна роботи полягає в оцінці ефективності комбінацій різних моделей штучних нейронних мереж і методів виділення цифрового шуму в зображеннях для вирішення задачі їх автентифікації.

Надано ймовірності оцінки автентичності зображень на основі узагальнення результатів одночасного застосування методів ELA, PCA та NOISE з використанням моделей штучних нейронних мереж у режимі семантичної класифікації та сегментації.

На підставі проведених досліджень визначено основні напрямки підготовки фахівців до вирішення задачі автентифікаціїї зображень у сучасних умовах.

© Сергій Чорний, Ольга Брендель, Олег Мєшков, 2025.

Ключові слова: методи штучного інтелекту; цифрові зображення; автентичність зображень; нейронні мережі глибокого навчання; семантична сегментація.

1. ВСТУП

Постановка проблеми. Науковою проблемою, що розглядається в роботі, є оцінка автентичності цифрових зображень на основі комплексного використання методів попередньої обробки зображень (методів фільтрації) та штучного інтелекту та розроблення методичних рекомендацій щодо виявлення ознак монтажу зображення на їх основі. Електронні документи чи їх зображення, фотозображення, відеозаписи, скановані копії, що мають цифрову природу утворення, використовуються в будь-якій галузі нашої країни, що забезпечує необхідний рівень національної безпеки та оборони функціонування економіки, системи освіти тощо. Інтенсивне використання досягнень науково-технічного прогресу, зокрема методів штучного інтелекту, створює нові можливості щодо фальсифікації цифрових документів.

Належне функціонування комп'ютерно-технічної сфери у нашій країні можливе насамперед за умови наявності та перспектив підготовки висококваліфікованих кадрів з фаховою вищою освітою та досвідом роботи в науково-дослідних установах системи Національної академії наук України, закладах вищої освіти, які здійснюють підготовку відповідних фахівців науково-дослідних, науково-виробничих і виробничих підприємств.

Велике зацікавлення науковців питаннями застосування штучного інтелекту є актуальним викликом сьогодення. Тож перспективним напрямком підготовки фахівців є комплексне використання стандартних методів дослідження в поєднанні з сучасними технологіями штучного інтелекту. У складі освітніх програм, які функціонують у галузі знань «Інформаційні технології», у частині застосування методів та алгоритмів, використання штучного інтелекту, зокрема при дослідженні автентичності цифрових зображень, є вимогою часу, що формує необхідні компетентності випускника та дозволить йому виконувати науково-виробничі завдання найвищої складності.

Аналіз останніх досліджень і публікацій. Від започаткування фотографії і дотепер проблемі отримання та аналізу фотографічних зображень присвячені фундаментальні праці багатьох науковців, серед яких варто відзначити сучасні роботи Лендфорда М. та Крісса М.

Так посібник Лендфорда М. [1] є фундаментальним для широкого кола фахівців у галузі фотографії, ідеально підходить як для студентів-початківців так і для досвідчених користувачів. Видання охоплює основні принципи фотографії, включно з експозицією, композицією, освітленням та постобробкою.

Посібник М. Крісса з цифрових зображень [2] є фундаментальною роботою в галузі створення та обробки цифрових зображень, містить послідовний огляд наукових досягнень у цій галузі, зосереджує увагу на отриманні, зберіганні та відображенні зображень. Робота надає розуміння конструкції та принципів використання цифрових пристроїв для обробки зображень.

З розвитком технологій обробки зображень та графічного дизайну суттєво розширилися можливості маніпуляції цифровим контентом. Вирішенню проблеми цифрової обробки зображень та розробки алгоритмів виявлення ознак монтажу в цифрових зображеннях присвячені роботи Сенсар Н. Т., Вердоліва Л., Каленського В. Г., Бобрицького С. М. та інших. Базові технології, які стимулюють прогрес у глибокому навчанні та обчислювальній візуалізації, також створюють серйозну проблему для встановлення довіри до того, що ми бачимо, чуємо та читаємо, і роблять медіаконтент кращою мішенню для зловмисних атак.

Робота авторів H. T. Sencar, L. Verdoliva та N. Memon [3] розрахована на дослідників та аналітиків-криміналістів і надає перелік методів, що використовуються для аналізу та автентифікації цифрових мультимедіа. Розглядаються зокрема методи ідентифікації цифрових камер, способи виявлення фальсифікацій: ознаки застосування методів штучного інтелекту – генеративних змагальних мереж, технології DeepFake, видалення та подвоєння кадрів відеозаписів та ін. Ця книга заповнює важливу прогалину в цьому новому середовищі загроз, що базується на інноваційних технологіях обробки зображень і складних інструментах їх реалізації. Окремо розглянуто антикриміналістичні методи. Зміст роботи орієнтовано на те, щоб надати практикам, дослідникам, фото- та відеолюбителям і студентам цілісне уявлення про цю сферу.

У роботі [4] запропоновано ретельний аналіз традиційних і сучасних стратегій виявлення підроблених зображень, таких як метод аналізу головних компонентів (PCA) та опорні векторні машини (SVM), що зосереджені на аналізі статистичних властивостей і ідентифікації невідповідностей у характеристиках зображення. Приділено певну увагу і останнім розробкам, зокрема згортковим нейронним мережам (CNN) і генеративним змагальним мережам (GAN), які застосовуються для покращення надійності автентифікації зображень. CNN чудово аналізують ієрархічні функції та виявляють складні шаблони, які вказують на підробку зображення. GAN покращують надійність моделі за допомогою змагального навчання. Незважаючи на ці досягнення, залишаються проблеми включно з еволюцією техніки маніпуляцій, потребою у великих анотованих наборах даних і з обчисленнями. У цій роботі висвітлюються сильні сторони та обмеження різних методів і пропонуються напрямки майбутніх досліджень для покращення виявлення фальшивих зображень, наприклад, класифікація за кількома класами, перенесення навчання та оптимізація програм у режимі реального часу.

Останні алгоритми виявлення маніпуляцій із зображеннями майже завжди передбачають використання глибоких мережевих моделей. Ці підходи вимагають або щільних по-піксельних масок правдивої інформації, ідентифікаторів камер або метаданих зображень для навчання мереж. З одного боку, побудова навчального набору для представлення незліченних можливостей підробки є непрактичною. З іншого боку, платформи соціальних мереж або комерційні програми часто змушені видаляти ідентифікатори камер та метадані зображень. Алгоритм із самоконтролем для навчання моделей виявлення маніпуляцій без щільної правдивої інформації або метаданих камери/зображення був би надзвичайно корисним для багатьох додатків криміналістики. У статті [5] пропонується підхід для навчання моделей виявлення та локалізації вставлених у зображення фрагментів на основі аналізу мережею частотного перетворення зображень. Для ідентифікації зрощених областей запропонована мережа глибокого навчання, що вивчає частотне представлення зображення на основі принципу його самоузгодженості та забезпечує подібну або кращу продуктивність порівняно з кількома існуючими методами на стандартних наборах даних без використання міток чи метаданих.

Виявлення маніпульованих областей на зображеннях є складним завданням через існування дуже точних технік малювання зображень, які залишають майже непомітні сліди в змінених областях. Ці методи малювання зображень використовують для багатьох цілей (наприклад, для видалення об’єктів, реконструкції пошкоджених ділянок, усунення різних типів спотворень тощо), що робить створення криміналістичних детекторів для маніпулювання зображеннями надзвичайно складною та довготривалою процедурою. У статті [6] увагу зосереджено на виявленні маніпуляцій зображення з використанням сучасних технологій малювання (Inpainting) на основі прямого застосування CNN IRL-Net до дослідного зображення (без застосування попередньої обробки традиційними методами). Авторами запропонована нова модель глибинного

навчання на основі CNN, яка має три основні модулі: покращення, кодування та декодування. Для оцінки цього методу виявлення ознак маніпуляцій у змісті зображення було використано три методи малювання зображень для реконструкції пропущених областей у двох наборах даних зображень обличчя та сцени. Проведено як якісну, так і кількісну оцінку створених наборів даних. Експериментальні результати демонструють, що запропонований метод перевершує попередні методи виявлення маніпуляційних областей на основі навчання та генерує реалістичні та семантично вірогідні зображення.

Оглядова робота [7] описує підхід до дослідження автентичності цифрових зображень з точки зору цифрової криміналістики. Криміналістичне дослідження починається з визначення того, чи було змінено цифровий доказ (зображення чи відео), пов'язаний із судовою справою. Описані методи активного виявлення підробок, такі як цифрові водяні знаки та цифрові підписи, і методи пасивного виявлення підробок, зокрема виявлення копіювання-переміщення, зрощування та ретуші. Крім того в роботі розглядається застосування нейронних мереж і методів машинного навчання (ML) у криміналістиці для виявлення підробок зображень. Щоб оцінити переваги та недоліки цих моделей у роботі порівняно різні архітектури CNN. Більшість методологій, що використовуються у виявленні підробок, детально описано із зазначенням переваг і недоліків кожного методу.

На відміну від нього авторами роботи [8] запропоновано методичні підходи щодо встановлення можливого змінення початкового стану графічного цифрового файлу з використанням комплексних підходів, що засновані на одночасному дослідженні метаданих файлів та шумових характеристик зображення. Графічний файл розглядається як об'єкт, дослідження якого пов'язано з оцінкою змінення шумового фону матриці цифрового пристрою зйомки. Такий підхід дозволяє встановити щільність розподілення кольорів по всій поверхні матриці, виявити можливі пошкодження світлочутливого шару та інші артефакти, що пов'язані з особливостями фіксації зображення матриці та апаратних засобів конкретного цифрового пристрою фотофіксації. Комплексність дослідження полягає в додатковому дослідженні метаданих файлу в частині відомостей про реальну якість (рівень стискання), що пов'язані з використанням програмних засобів редагування.

Публікація [9] присвячена застосуванню методів стеганографії для аналізу шумів і виявлення ознак редагування та оцінки автентичності цифрових зображень. У цій роботі закладено загальні основи методичного підходу до дослідження цифрових фотозображень і технічних засобів їх виготовлення, авторами запропоновано шляхи, за якими можна проводити окремі дослідження. В основу дослідження зображень щодо встановлення ознак зміни їх змісту засобами редагування покладено явище пошкодження (спотворення) природного шумового фону зображення, притаманного йому внаслідок наявності шуму чутливих елементів цифрових фотокамер. Шумова складова зображення може бути використана як джерело інформації редагування зображення, оскільки зазвичай оригінальні зображення мають однорідний шумовий фон, що може порушуватись у разі монтажу. Підходи до оцінювання рівня шуму поділяються на три основні категорії: оцінювання шуму на основі блоків, оцінювання шуму на основі градієнтів та оцінювання шуму на основі згладжування. Загальним недоліком розглянутих методів, на думку авторів, є необхідність розбиття зображення на блоки з певною кількістю пікселів, залежність результатів виділення шуму від розмірів блоків і непрацездатність у разі, коли розмір блока дорівнює пікселю. Зазначений недолік не притаманний методу стеганографічного аналізу, що орієнтований на виділення молодших бітів пікселів зображення. Докладно висвітлено загальну схему досліджень, порядок дій при попередньому дослідженні, дії під час здійснення візуального аналізу та аналізу метаданих у межах аналітичного дослідження. Запропонований розробниками

метод дає змогу візуально визначити зони редагування (ретушування) зображення по зображеннях створених цифрових шарів досліджуваного зображення.

Незважаючи на те, що було розроблено багато рішень щодо виявлення втручань у зміст фотозображення, ефективність їх виявлення все ще далеко не надійна, і це не вичерпує цю проблему. Так у роботі [10] описані поширені операції втручання, такі як копіювання-переміщення, зрощування та повторна вибірка, а також обговорюються різні методи виявлення, застосовні до цих типів маніпуляцій, проведено глибокий огляд останніх досліджень щодо виявлення мультимедійних підробок. Ця робота дає дослідникам можливість розробити та оцінити власні підходи до криміналістики зображень/відео.

Різноманітні напрямки виявлення цифрового втручання, їх результат і аналіз, універсальні підходи криміналістичного дослідження зображень досі потребують ретельного вивчення. У роботі [11] надано всебічний огляд універсальних підходів в криміналістиці цифрових зображень, включно з виявленням повторної дискретизації, виявленням стиснення та методами на основі неузгодженості, зокрема за допомогою машинного навчання та підходів на основі глибокого навчання. На відміну від існуючих, спрямованих на з'єднання зображень або виявлення копіювання-переміщення, це дослідження орієнтовано на вивчення універсальних методів, виявлення фальсифікації зображень.

Отже, у розглянутих вище дослідженнях показано широкий спектр підходів від візуального аналізу, застосування традиційних методів попередньої обробки зображень до прямого застосування мереж глибокого навчання та використання частотних методів попереднього перетворення зображення у комбінації з CNN.

Тож, на наш погляд, подальшого розвитку потребують дослідження у напрямку використання технологій штучного інтелекту в комбінації з кількома відомими методами попередньої математичної обробки зображень одночасно, такими як: аналіз рівня помилок (Error Level Analysis, ELA); принциповий компонентний аналіз (Principal Component Analysis, PCA) та ін. для розпізнавання змінених ділянок цифрових зображень під час оцінки автентичності зображень. У вітчизняній науковій літературі проблеми оцінки автентичності цифрових зображень на основі комплексного використання кількох методів попередньої обробки зображень (методів фільтрації) та мереж глибокого навчання для виявлення ознак монтажу зображення на їх основі не набули широкого висвітлення.

Метою дослідження є обґрунтування напрямків підготовки фахівців до використання методів штучного інтелекту при встановленні автентичності цифрових зображень на підставі проведення наукового дослідження комплексного використання методів фільтрації ELA, PCA та виділення шуму з узагальненням результатів на основі моделей штучних нейронних мереж (ШНМ).

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Цілями підготовки фахівців у галузі комп'ютерно-технічних досліджень у межах освітніх програм існуючих рівнів вищої освіти виступає конкретна характеристика процесу формування відповідних компетентностей у програмі розвитку студента за спрямуванням (спеціалізацією) освітньої програми з використанням засобів освіти, опису системи знань, а також умінь і навичок, якими він повинен оволодіти після закінчення закладу вищої освіти. Досягнення загальних цілей підготовки фахівців у цій сфері в межах освітніх програм існуючих рівнів вищої освіти здійснюється через послідовне вивчення окремих обов'язкових і вибіркових компонент навчальних планів, у межах яких здійснюється накопичення та розвиток конкретних здобутих знань, умінь

і навичок за правилами: від простого до складного, від відомого до невідомого, від близького до далекого.

Одне з найважливіших завдань сучасного криміналістичного дослідження цифрових фотозображень та відеозаписів – завдання встановлення автентичності цифрових записів. З огляду на відносну легкість створення, модифікування, розповсюдження цифрових записів, логічно виникає питання їх достовірності (автентичності). Термін «автентичний» щодо фонодокументів у сенсі «справжній», «достовірний» широко використовується в англомовному праві, спочатку прийнятий польськими криміналістами в теорії криміналістичного дослідження фонограм, також використовується американськими експертами [12]· В SWGDE Best Practices for Forensic Audio [13] визначено що експертиза автентичності полягає в тому, щоб *визначити, чи є запис відповідним способу, яким він, як стверджується, був записаний*. На наш погляд це визначення є найбільш виправданим.

Цифровий графічний файл як об'єкт дослідження суттєво відрізняється від звичайної традиційної фотографії [9]. Сучасні технології оброблення зображень надають широкі можливості виконання монтажу зображень, зокрема із застосуванням методів штучного інтелекту. Під монтажем у криміналістичній площині розуміють внесення будь-яких змін у первинне (оригінальне – за термінологією, що сьогодні використовується в експертизі) зображення [12]. Головною ознакою монтажу зазвичай є утворення цілого з частин. Існує багато окремих методів дослідження автентичності зображень, які вирішують завдання лише у певних умовах, що обумовлює потребу експертної практики в автоматизації узагальнення результатів таких окремих досліджень одного об'єкта для підвищення достовірності прийнятого експертом рішення [9].

Основними відомими типами цифрового монтажу щодо втручання в контекст цифрового зображення поки що залишаються такі [14]:

– повне видалення або ретушування окремого фрагменту;
– накладення (вставка, додавання) окремого фрагменту;
– стиснення із втратами.

Видалення (ретушування) окремого фрагменту цифрових зображень – це внесення локальних змін у властивості зображення (яскравості, кольору, зменшення шуму) тощо [14]. Серед сучасних технологій ретушування слід особливо виділити технологію малювання (Inpainting) [15]. Ця технологія використовує методи штучного інтелекту для створення в межах видаленого фрагменту реалістичного зображення, яке формується на основі аналізу навколишніх ділянок оригіналу. На даний час функція обробки зображень за технологією Inpainting реалізована щонайменше у таких редакторах, як Adobe Photoshop, GIMP, Deep Art, NVIDIA Canvas, Microsoft Paint 3D, Fotor AI Image Inpainting, Remini, Pixlr, Inpaint, PhotoWorks [16].

Також останнім часом набули поширення редактори суміжної технології – домальовування (Outpainting) до цифрового зображення зовнішніх ділянок з реалістичним контентом, згенерованим за допомогою ШНМ [17]. Функція домальовування реалізована в редакторах Photoshop Generative Fill, DALL-E2, Midjourney, Stable Diffusion, Craiyon, AI Greenscreen (Tik Tok), Picksart, Nightcafe AI.

Сучасною тенденцією розвитку редакторів є поєднання технологій Inpainting, Outpainting, автоматичного розпізнавання контенту, генерації змін відповідно до їх заданого текстового описання [17]. Сучасні технології виявлення ознак цифрового монтажу, окрім традиційного візуального аналізу, базуються на виділенні шумової складової цифрового зображення та виявленні за результатами її аналізу редагованих фрагментів, на оцінці взаємної кореляції частин зображення та візуальному аналізі самого зображення, його шумових картин та результатів кореляційної обробки. Отже,

безперечною ознакою не автентичності цифрового зображення є доведення наявності в ньому зон монтажу – внесення будь-яких змін у первинне (оригінальне, автентичне) зображення.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1 Дослідження традиційних технологій оцінки автентичності цифрових зображень

У результаті проведених авторами досліджень проаналізовано найбільш відомі некомерційні онлайн-ресурси, що дозволяють проводити інтерактивне онлайн-дослідження цифрових зображень, а саме:

- Вебресурс Forensically [18]. Особливістю роботи ресурсу є використання для розрахунків обчислювальних можливостей користувача, оскільки оброблення за обраними методами здійснюється лише на його комп'ютері. Оброблювані зображення від користувача на сайт Forensically не передаються. Завдяки цьому оброблення зображень можливе навіть за відсутності Інтернет-зв'язку, що дозволяє досліджувати конфіденційні зображення. У цілому вебресурс Forensically є найбільш розвинутим із відомих відкритих вебресурсів для досліджень цифрових зображень.
- Вебресурс FotoForensics [19] є напівкомерційним. У відкритому доступі є лише інструмент для дослідження зображення за методами ELA, Jpeg Data (таблиці квантування) та Exif-метадані. Інші можливості ресурсу доступні на комерційних умовах для авторизованого передплаченого доступу.
- Вебресурс Izitru [20] використовує автоматичні методи аналізу для сертифікації незмінених зображень цифрових камер. На відміну від інших, це криміналістичне програмне забезпечення, надає лише «дійсну» або «хибну» відповідь. Є тести, які можуть ідентифікувати певні типи редагування, такі як клонування або композитування, але ці тести не можуть бути застосовані автоматично до кожного зображення.
- Вебресурс Imageforensic [21] реалізує програмне забезпечення з відкритим кодом Ghiro. Ghiro – це Linux орієнтована програма для цифрових зображень. Стосовно дослідження змісту зображення ресурс дозволяє проводити аналіз за методом ELA.
- Програма JPEGsnoop [22] – це Windows-програма, що може бути використана для аналізу джерела останнього збереження зображення та перевірки його автентичності. Дозволяє визначити різні параметри, які використовувались у цифровій камері під час фотографування (метадані EXIF, IPTC), але також інформацію, яка вказує на якість і характер стиснення JPEG-зображення, що використовується при збереженні файлу.
- Програма Amped Authenticate [23] є розвинутим програмним продуктом, призначеним для проведення досліджень цифрових фотографій з метою їх автентифікації.
- Програма Fake Image Detector [24] є відкритим інструментом для смартфонів, планшетів тощо з операційною системою Андроід 4.1 та вище. У ній реалізовано дослідження зображень методом ELA та аналіз Exif-метаданих.

Суттєвим загальним недоліком оглянутих ресурсів є відсутність можливості навчання їх застосування для певних умов використання. Налаштування їх на виконання певного завдання здійснюється користувачем лише з власного досвіду, що є певним недоліком.

Водночас із розвитком засобів редагування зображень у напрямку застосування цифрових технологій штучного інтелекту, у цьому ж напрямку йде розвиток також методів [25] і засобів оцінки автентичності цифрових зображень та їх програмне забезпечення [26].

Найбільш прийнятними і такими, що заслуговують на загальне визнання, є визначені в роботі [27] методи оцінки автентичності, які можна поділити на такі групи:

- класичні методи з використанням методів фільтрації (Classical Filter Based Methods, методи фільтрації);
- методи, засновані на принципах глибинного вивчення (Deep Learning Methods);
- методи, що є комбінацією попередніх (від авторів).

Саме третя група технологій оцінки автентичності, на думку авторів, і є найбільш перспективною, бо дозволяє поєднати ефективні методи першої групи (наприклад, як ELA) з можливостями класифікаторів другої групи (як CNN).

Однак суттєвою особливістю використання нейронних мереж CNN є необхідність їх тренування на значних за обсягом наборах зображень, що потребує наявності потужних обчислювальних ресурсів (наприклад, графічних прискорювачів) або значного часу обчислень (тижні) за їх відсутності.

Перспективним рішенням цієї проблеми є використання для тренування мереж CNN хмарних Інтернет-ресурсів, зокрема Google Colab [28], Kaggle [29] та інших, які дозволяють проводити обчислення за певних обмежень ресурсів та часу. Це дозволяє на порядок скоротити час тренування CNN. Програмним середовищем цих платформ є зокрема мова програмування Python.

Відомі детектори працюють у таких характерних режимах:

- визначення автентичності зображення (так / ні);
- визначення місць пошкодження (втручання) у зображення з остаточним рішенням експерта про факт автентичності;
- поєднання попередніх двох режимів.

Слід зауважити, що при обробці зображень перший режим потребує значно меншого обсягу зусиль для підготовки (тренування) ніж другий внаслідок простішої (вдвічі) структури нейронної мережі. Тому ці режими типово реалізуються різними нейромережевими класифікаторами.

У процесі досліджень нашу увагу привернув нейромережевий бінарний класифікатор, що працює за першим режимом роботи [30]. Значною перевагою його, на відміну від інших, є аналіз повного зображення без змін його розміру та використання кількох методів попередньої обробки зображень паралельно.

У роботі [31] автором пропонується версія класифікатора заздалегідь тренована на штучному наборі зображень та редагуванні їх методом поєднання (splicing). Класифікатор має три внутрішніх режими використання (RGB, N, RGN). Найбільш цікавим є внутрішній режим RGN, який використовує кілька методів (3) попередньої обробки для виявлення ознак досліджуваного вхідного зображення.

Авторами проведено дослідження працездатності класифікатора на наборах зображень, редагованих за технологією Inpainting трьома різними редакторами: Редактор 1 [32] (недоступний online, результати редагування отримані з [32]), Редактор 2 [33], Редактор 3 [34]. Редактор 1 орієнтований його авторами на зображення, що досліджуються на автентичність.

Результати дослідження визначення автентичності за ймовірністю редагування наведені в таблиці 1. Ймовірність редагування обчислювалась як відсоток виявлених редагованих пікселів до загальної кількості редагованих пікселів.

Зображення достовірно автентичне – ймовірність 0, достовірно не автентичне – ймовірність 1. Якщо прийняти за рівень прийняття рішення про автентичність

ймовірність 0.5, то, як видно з таблиці 1, найгірший з точки зору приховування факту редагування є Редактор 1, найкращий – Редактор 3. Зображення редаговані у Редакторі 3 у 75% з розглянутих випадків визначаються даним класифікатором як автентичні. А зображення конвертовані в інший формат без змін контенту Редактором 2 визначаються як не автентичні.

Отже, проведене дослідження показує певну залежність результатів класифікації від тренування класифікатора на особливості конкретного редактора. Також встановлено, що сучасні редактори за технологією Inpainting потребують уваги класифікаторів автентичності зображень при тренуванні.

Дослідження методів виявлення не автентичності зображень проводилось на прикладі редагування за технологією Inpainting з використанням методів, запропонованих авторами в якості розширеного дослідження за методикою [35] та критерієм ймовірності виявлення зони редагування. Ймовірність редагування за цією методикою обчислювалась як відсоток виявлених редагованих пікселів до загальної кількості редагованих пікселів з усередненням ймовірності в межах групи досліджуваних зображень.

Мета дослідження – виявлення методів чутливих до залишкових пошкоджень зображень, оброблених за технологією Inpainting. У межах даного дослідження використано спеціалізований набір зображень, створених авторами за допомогою технології NVIDIA відповідно до [33].

Розширене дослідження зображення у межах цієї методики охоплює загалом застосування до зображення наступних груп методів з вказаного пакету програм: фокусування зображення (Focus Quality Tests, 33 методи); частотних перетворень (DCT/CFA Analysis, 15 методів); оцінки розподілу шумів (Normality Tests, 11 методів); оцінки ентропії шумів (Entropy Analysis, 13 методів).

Виявлення зон редагування за результатами обробки зображення вказаними методами фільтрації здійснювалось візуально експертами шляхом порівняння зображень відомих зон редагування з їх зображеннями, створеними за використаними методами фільтрації.

Оригінальні зображення для цих тестів отримані авторами шляхом фотографування різних об’єктів. Обчислення ймовірності визначення зон редагування в рамках зазначених нижче груп зображень проводились за методикою, описаною в [35].

Проведено дослідження цифрових шарів оригінального та редагованого зображень за допомогою програми виділення цифрових шарів означеного ресурсу (кваліфікаційний рівень Standard, режим обробки: Tamper detection, Mode3).

Результати співставлення цифрових шарів оригіналу та редагованого зображень свідчать про те, що відмінності зображень помітні лише у цифрових шарах 5-7, але реальні межі зон видалення не спостерігаються. Тож зони редагування суттєво замасковані. Розглянуто результати, отримані для досліджуваного зображення групою методів Focus Quality Tests.

Таблиця 1

Ймовірність розпізнавання факту редагування класифікатором [19] у режимі FUSION (RGN)

Зображення	Оригінал (2448,3264,3)	Редактор 1 (2448, 3264, 3)	Оригінал (512, 512,3)	Редактор 2 (512, 512,3)	Редактор 3 (600, 600, 3)
5002.png	0.108	0.966	0.770	0.691	0.542
5010.png	0.111	0.893	0.575	0.604	0.164
5047.png	0.277	0.944	0.686	0.780	0.239
5048.png	0.249	0.989	0.890	0.882	0.408
5082.png	0.202	0.989	0.640	0.673	0.698

5121.png	0.200	0.400	0.853	0.901	0.350
5124.png	0.364	0.944	0.865	0.787	0.249
5161.png	0.120	0.736	0.795	0.872	0.684
5162.png	0.103	0.946	0.488	0.695	0.784
Середнє	0.193	0.867	0.729	0.765	0.457

Методи цієї групи спрямовані на пошук зон редагування на основі локальних властивостей фокусування зображення. Вони можуть застосовуватись як до повного зображення, так і до окремих його цифрових шарів (1-8). Для цифрового шару 6 з 33 методів цієї групи лише 23 дозволяють візуально чітко виявити нижню частину пошкоджень. Кількість методів цього рівня, чутливих до пошкоджень, зменшується для цифрового шару 8 редагованого зображення. У такий спосіб групою методів Focus Quality Tests зони редагування частково виявляються для цифрових шарів зображення 6-8. Ймовірність виявлення зони редагування методами цієї групи складає 0.697 при їх окремому застосуванні.

Розглянемо результати, отримані для досліджуваних зображень групою методів DCT/CFA Analysis. Методи цієї групи спрямовані на пошук зон редагування на основі локальних властивостей частотних перетворень (зокрема «*.jpg») зображення. Вони можуть застосовуватись лише до повного зображення. З 15 методів цієї групи лише 4 дозволяють виявити окремі ділянки пошкодження. Ймовірність виявлення зони редагування методами цієї групи складає 0.267 при їх окремому застосуванні.

Розглянуто результати, отримані для досліджуваних зображень групою методів Normality Tests. Методи цієї групи спрямовані на пошук зон редагування на основі локальних властивостей шумів зображення (перевірка розподілу шуму на «нормальність»). Вони можуть застосовуватись як до повного зображення, так і до окремих його цифрових шарів (1-8). Ймовірність визначення зон редагування в межах цієї групи склала 0.818 при їх окремому застосуванні.

Розглянуто результати, отримані для досліджуваного зображення групою методів Entropy Analysis. Методи цієї групи спрямовані на пошук зон редагування на основі локальних властивостей ентропії шумів зображення. Застосовуються до повного зображення. Ймовірність визначення зон редагування в межах цієї групи склала 0.154 при їх окремому застосуванні.

Отже, проведене дослідження показує, що визначення факту неавтентичності та усіх зон редагування досягнуто лише одним методом (GAGI, група DCT/CFA Analysis), визначення факту неавтентичності та частини зон редагування досягнуто:

- групою методів DCT/CFA Analysis у 4 випадках з 4;
- групою методів Focus Quality Tests у 23 випадках з 33;
- групою методів Normality Tests у 9 випадках з 11;
- групою методів Entropy Analysis у 2 випадках з 13.

Отже, загальна середня ймовірність виявлення вказаними методами фільтрації зон редагування в межах розширеного дослідження зображень оброблених за технологією малювання складає 0.528. при застосуванні одиночного методу з вказаного переліку. Виявлення щонайменше частини зон редагування з ймовірністю 1.0 досягнуто в разі застосування всіх методів однієї з означених груп (11-33). Виявлення всіх зон редагування з 44 ймовірністю 1.0 досягнуто лише в разі застосування усіх 72 методів з усіх означених груп.

Тож проведене дослідження демонструє необхідність використання для виявлення зон редагування одночасно кількох методів попередньої обробки зображень з подальшим узагальненням отриманих результатів.

3.2 Дослідження технологій оцінки автентичності зображень на основі моделей штучних нейронних мереж

На підставі запропонованого підходу до використання семантичних класифікаторів з попередньою обробкою зображень методами фільтрації (зокрема ELA, PCA та виділення шумів зображення NOISE), аналізу архітектур семантичних класифікаторів та їх функціональних складових (кодерів), аналізу існуючого програмного забезпечення для подальших досліджень обрано програмне середовище Python, Jupyter Notebook та одну з найбільш функціональних бібліотек моделювання штучних нейронних мереж – бібліотеку Segmentation Models (SM) [36].

Бібліотека SM забезпечує використання наступних архітектур штучних нейронних мереж (ШНМ):
– Unet;
– Unet++;
– MAnet;
– Linknet;
– FPN;
– PSPNet;
– PAN;
– DeepLabV3;
– DeepLabV3+.

У межах кожної з цих архітектур забезпечується використання наступних типів кодерів:
– ResNet (5 типових варіантів);
– ResNeXt (6 типових варіантів);
– ResNeSt (8 типових варіантів);
– Res2Ne(X)t (7 типових варіантів);
– RegNet(x/y) (24 типових варіанти);
– GERNet (3 типові варіанти);
– SE-Net (6 типових варіантів);
– SK-ResNe(X)t (3 типові варіанти);
– DenseNet (4 типових варіанти);
– Inception (3 типові варіанти);
– EfficientNet (23 типових варіанти);
– MobileNet (7 типових варіантів);
– DPN (6 типових варіантів);
– VGG (8 типових варіантів);
– Mix Visual Transformer (6 типових варіантів);
– Timm Encoders (467 типових варіантів).

Окрім типових варіантів використання є можливість змінювати параметри як архітектур, так і кодерів. Точність роботи мережі в межах бібліотеки SM оцінюється за загальною точністю класифікації (0-100%) та коефіцієнтом ідентичності Соренсена - Дайсе (0-1) [37]. У даному випадку використано середній коефіцієнт Дайсе (Mean Dice, MD), обчислений шляхом усереднення коефіцієнтів Дайсе окремих зображень у межах групи.

Дослідження проведено на наборі зображень редагованих редактором NVIDIA: 28 зображень з розміром 512*512 пікселів для тренування мережі та 12 інших зображень з розміром 512*512 пікселів для тестування мережі. Оригінальні зображення для цих тестів отримані авторами шляхом фотографування різних об’єктів.

Дослідження проведено на комп'ютері ASUS з процесором 11th Gen Intel(R) Core(TM) i7-11370H (частота 3.30GHz), оперативна пам'ять 16.0 GB, графічна карта RTX3070 (8Gb), операційна система Windows 10x64.

Найбільш суттєвими обмеженнями наявних обчислювальних ресурсів у ході досліджень виявилися обсяг оперативної пам'яті та обсяг пам'яті графічної карти, тому для тестування обрано лише ті конфігурації ШНМ, які задовольняють відповідним вимогам до цих ресурсів. Враховуючи загальну тенденцію роботи ШНМ: чим більший її обсяг – тим точніше, – моделі ШНМ обирались зі стандартних або підлаштовувались так, щоб використовувати максимальний наявний обсяг пам'яті. Крім того, враховуючи вплив розмірів зображень на використання пам'яті, зображення на етапі попередньої обробки зменшувались шляхом простого видалення (обрізання) їх з країв без стискання або іншої обробки з 512*512 пікселів до 320*480 пікселів.

Дослідження проводилось такими етапами:

- тестування найбільших за обсягом вимог ШНМ у стандартній конфігурації з працездатним рівнем вимог до пам'яті;
- тестування найбільших за обсягом вимог ШНМ непрацездатних у стандартній конфігурації у з трансформуванням мережі в напрямку її зменшення до працездатного рівня;
- тестування найменших за обсягом вимог ШНМ у конфігурації з максимальним трансформуванням мережі у напрямку її збільшення;
- тестування варіантів вхідної обробки зображень ELA+PCA та ELA+PCA+NOISE.

Тестування моделей найбільших за обсягом вимог у стандартній конфігурації з працездатним рівнем вимог до пам'яті.

У першу чергу проведено дослідження ефективності оцінки зон редагування для ШНМ у стандартних конфігураціях базового програмного забезпечення. Результати наведені в Таблиці 2.

Як видно з Таблиці 2, найкращий результат 0.98762 за критерієм Дайсе досягнуто моделлю ШНМ у варіанті стандартної конфігурації з використанням архітектури UnetPlusPlus та кодера timm-resnest200e. Дещо гірший результат 0.98615 має ШНМ з архітектурою UnetPlusPlus та кодером efficientnet-b7. Третій результат 0.98568 має архітектура UnetPlusPlus з кодером timm-efficientnet-b8.

Порівняння результатів тестування моделі UnetPlusPlus / timm- resnest200e для різних варіантів попередньої обробки та нестандартних параметрах каналів декодера надано в Таблиці 3.

Найкращий результат досягнуто для архітектури UnetPlusPlus та кодера timm-resnest200e з 4 каналами декодера (512, 256, 128, 64) (нестандартний варіант).

Тестування найменших за обсягом вимог ШНМ у конфігурації з максимальним трансформуванням мережі у напрямку її збільшення.

У даному випадку досліджено вплив збільшення розмірів ШНМ від стандарту шляхом розширення фільтру.

Як видно з Таблиці 4, найкращий результат 0.97892 за критерієм Дайсе досягнуто моделлю ШНМ у варіанті стандартної конфігурації з використанням архітектури UnetPlusPlus та кодером mobilenetv3_large_100. Гірші результати 0.97748 та 0.97814 мають ШНМ з фільтрами більшого обсягу. Отже, розширення мережі завдяки розширенню фільтра виглядає недоцільним.

Таблиця 2

Результати тестування моделей найбільших за обсягом вимог у стандартній конфігурації для варіанту попередньої обробки ELA+PCA

Тип мережі	Кодер	MD
UnetPlusPlus	timm-efficientnet-b8	0.98568
UnetPlusPlus	efficientnet-b7	0.98615
Unet	efficientnet-b7	0.98226
MAnet	timm-efficientnet-b8	0.98180
Manet	efficientnet-b7	0.98292
Linknet	efficientnet-b7	0.96928
Unet	resnet152	0.98134
UnetPlusPlus	resnext101 32x8d	0.98529
UnetPlusPlus	resnet152	0.98557
UnetPlusPlus	timm-resnest200e	0.98762
PSPNet	timm-regnety 160	0.98213
Manet	timm-resnest200e	0.97790

Таблиця 3

Результати тестування моделі UnetPlusPlus / timm- resnest200e для різних варіантів попередньої обробки

Варіант попередньої обробки	Глибина кодера (канали декодера)	MD
PCA +NOISE_ABS	4 (592, 256, 128, 64)	0.98803
PCA +NOISE_ABS	4 (576, 256, 128, 64)	0.99379
PCA +NOISE_ABS	4 (600, 300, 150, 75)	0.99023
PCA +NOISE_ABS	4 (512, 256, 128, 128)	0.98669
PCA +NOISE_ABS	5 (64, 32, 16, 8, 4)	0.98655
PCA +NOISE_ABS	4 (512, 256, 128, 64)	0.99145
PCA +NOISE_ABS	4 (256, 128, 64, 32)	0.99138
ELA+NOISE_ABS	5 (256, 128, 64, 32, 8)	0.98664
ELA+PCA	5 (256, 128, 64, 32, 8)	0.98762

Дослідження ефективності менших за обсягом моделей з більшим обсягом вхідної інформації.

У даному випадку досліджено вплив збільшення обсягу вхідної інформації мережі (випадок ELA+PCA+NOISE) для моделей ШНМ менших за обсягом вимог у стандартній конфігурації без додаткової трансформації мережі.

Таблиця 4

Результати тестування моделей ШНМ найменших за обсягом вимог у конфігурації з максимальним трансформуванням мережі в напрямку її збільшення для варіанту попередньої обробки ELA+PCA

Мережа	Канали декодера	Кодер timm	MD
UnetPlusPlus	(512,256,128,64,32)	mobilenetv3_large_100	0.97892
UnetPlusPlus	(1024,512,256,128,64)	mobilenetv3_large_100	0.97748
UnetPlusPlus	(2048,1024,512,256,128)	mobilenetv3_large_100	0.97811

Як видно з Таблиці 5, найкращий результат 0.97841 за критерієм Дайсе досягнуто моделлю ШНМ у варіанті стандартної конфігурації з використанням архітектури UnetPlusPlus та кодером efficientnet-b5. Дещо гірший результат 0.97807 має ШНМ з

архітектурою UnetPlusPlus та кодером timm-regnety 064. Третій результат 0.97768 має архітектура UnetPlusPlus з кодером efficientnet-b4.

Таблиця 5

Результати тестування моделей ШНМ менших за обсягом вимог у стандартній конфігурації зі збільшенням обсягу вхідної інформації мережі для варіанту попередньої обробки ELA+PCA+NOISE

Мережа	Кодер	MD
UnetPlusPlus	timm-mobilenetv3 large 100	0.95018
UnetPlusPlus	timm-regnetx 016	0.95611
UnetPlusPlus	efficientnet-b3	0.97246
UnetPlusPlus	efficientnet-b4	0.97768
UnetPlusPlus	efficientnet-b5	0.97841
UnetPlusPlus	timm-gernet l	0.95529
UnetPlusPlus	timm-regnety 064	0.97807

Отже, збільшення обсягу вхідної інформації ШНМ для мереж з меншою за обсягом структурою не дає можливості отримати кращий результат, ніж для випадку меншого обсягу вхідної інформації, але більшої за обсягом мережі.

У наступному дослідженні (див. Таблицю 6) розглянуто варіант часткового збільшення обсягу вхідної інформації завдяки використанню тільки 2-х шарів кожного із зображень ELA, PCA та NOISE.

Таблиця 6

Результати тестування моделей ШНМ менших за обсягом вимог у стандартній конфігурації зі збільшенням обсягу вхідної інформації мережі для варіанту попередньої обробки ELA+PCA+NOISE (по 2 шари)

Мережа	Кодер	MD
UnetPlusPlus	efficientnet-b5	0.97530
UnetPlusPlus	dpn68b	0.90136

У даному випадку найкращою виявилася ШНМ UnetPlusPlus з кодером efficientnet-b5. Проте її результат гірший за попередній (див. Таблицю 5). Це можна пояснити впливом зменшення обсягу вхідної інформації для однакових моделей ШНМ .

Тестування найбільших за обсягом вимог ШНМ непрацездатних у стандартній конфігурації у з трансформуванням мережі у напрямку зменшення її обсягу до працездатного рівня.

У даному дослідженні перевірено можливість масштабувати обсяг мереж у бік зменшення з метою задовольнити вимоги до наявних обчислювальних ресурсів (див. Таблицю 7). Зменшення обсягу мережі здійснювалось шляхом зменшення глибини фільтру при збільшеному обсязі вхідної інформації мережі для варіанту попередньої обробки ELA+PCA+NOISE (по 2 шари з кожного 3-шарового) або без зміни обсягу вхідної інформації. Найкращий результат для даного дослідження 0.98312 у мережі UnetPlusPlus та кодера efficientnet-b6.

Таблиця 7

Результати тестування моделей ШНМ зі зменшенням обсягу мережі шляхом зменшення глибини декодера у конфігурації зі збільшенням обсягу вхідної інформації мережі для варіанту попередньої обробки ELA+PCA+NOISE (по 2 шари)

Мережа	Глибина кодера	Канали декодера	Кодер	MD
UnetPlusPlus	4	(256,128,64,32)	efficientnet-b6	0.98312

UnetPlusPlus	3	(128,64,32)	efficientnet-b7	0.96951
UnetPlusPlus	2	(128,64)	timm-resnest200e	0.97255
UnetPlusPlus	5	(512, 256,128, 64,32)	timm-mobilenetv3 _large_100	0.98267

На наступному етапі досліджено вплив зменшення обсягу мережі без зміни обсягу вхідної інформації. Вхідне зображення формувалося з трьох шарів:

- ELA конвертований до одного сірого шару;
- PCA конвертований до одного сірого шару;
- нульовий шар.

Глибина кодера у стандартній конфігурації дорівнювала 5, а канали декодера становили (256, 128, 64, 32, 16). Найкращий результат для даного дослідження 0.99041 у мережі UnetPlusPlus та кодера timm-resnest269e (див. Таблицю 8).

Дослідження ефективності штучних нейронних мереж при застосуванні окремих методів попередньої фільтрації.

Кожен з методів фільтрації, що застосовуються, формує 3-шарове кольорове зображення.

Таблиця 8

Результати тестування моделей ШНМ зі зменшенням обсягу мережі шляхом зменшення глибини фільтру для варіанту попередньої обробки ELA+PCA

Мережа	Глибина кодера	Кодер	MD	Опція
UnetPlusPlus	4	timm-resnest269e	0.99041	
UnetPlusPlus	4	timm-resnest269e	0.98700	SCSE
UnetPlusPlus	3	timm-efficientnet-l2	0.86725	
UnetPlusPlus	3	resnext101 32x48d	0.87616	

Однак внаслідок обмежень пам’яті (оперативної та GPU) таке зображення не дозволяє використовувати стандартні конфігурації кодер-декодер і для забезпечення працездатності моделі змушує зменшувати глибину кодера. Результати тестування моделей ШНМ зі зменшенням обсягу мережі шляхом зменшення глибини кодера при застосуванні методів обробки ELA, PCA та NOISE окремо для комбінації архітектури UnetPlusPlus з кодером timm-resnest269e наведені в Таблиці 9. У даному випадку методи PCA та NOISE_ABS забезпечують найвищі середні коефіцієнти Дайсе 0.99294 та 0.99204, відповідно.

Таблиця 9

Результати тестування моделей ШНМ зі зменшенням обсягу мережі шляхом зменшення глибини декодера для при застосуванні методів обробки ELA, PCA та NOISE окремо

Метод	Глибина кодера	Канали декодера	Mean Dice
PCA	4	(512, 256, 128, 64)	0.99294
ELA	4	(512, 256, 128, 64)	0.98993
NOISE_ABS	4	(512, 256, 128, 64)	0.99203

Як видно, усі використані методи фільтрації дають схожі результати для маски зони редагування (Predicted Mask), що в цілому відповідають дійсній масці редагування (Ground Truth Mask).

Дослідження моделей штучних нейронних мереж зі зменшенням обсягу мережі шляхом зменшення глибини кодера при узагальненні методів обробки ELA, PCA та NOISE.

У цьому дослідженні проведено тестування працездатності та оцінка ефективності ШНМ при одночасному застосуванні означених методів фільтрації в умовах обмеження наявних ресурсів використаного комп'ютера та використанні нестандартних параметрів каналів декодера (див. Таблицю 10). Формування вхідних зображень у ході тестування здійснювалося трьома способами:

- ненормоване кольорове зображення з окремих сірих зображень, сформованих відповідними методами фільтрації;
- кольорове зображення шляхом перемноження відповідних шарів кольорових зображень, сформованих відповідними методами фільтрації;
- нормоване кольорове зображення з окремих сірих зображень, сформованих відповідними методами фільтрації.

Глибина декодера була вимушено зменшена до 3 для забезпечення працездатності в умовах наявних обмежень. Найкращий результат з коефіцієнтом Дайсе 0.98983 отримано для нормування вхідного зображення ШНМ та використання каналів декодера: (128,128,256).

Таблиця 10

Результати тестування моделей ШНМ зі зменшенням обсягу мережі шляхом зменшення глибини декодера при застосуванні методів обробки ELA, PCA та NOISE одночасно

Метод	Канали декодера	MD
ELA PCA NOISE	(256, 128, 64)	0.98785
ELA PCA NOISE	(512, 256, 128)	0.98565
ELA PCA NOISE	(36, 28, 20, 12)	0.98524
ELA PCA NOISE	(32, 28, 28, 28)	0.98785
ELA PCA NOISE	(128, 128, 128)	0.98750
ELA PCA NOISE	(320, 320, 320)	0.98762
ELA PCA NOISE	(512, 320, 320)	0.98782
ELA PCA NOISE	(64, 128, 256)	0.98759
ELA PCA NOISE_ABS	(128, 128, 256)	0.98740
ELA PCA NOISE norm	(128, 128, 256)	0.98983

3.3 Основні напрямки підготовки фахівців з встановлення автентичності цифрових зображень з використанням методів штучного інтелекту

Загальновідомо, що цілями підготовки фахівців у галузі комп'ютерної інженерії (як і будь-якого іншого напрямку освіти) в межах освітніх програм існуючих рівнів вищої освіти виступає конкретна характеристика процесу формування відповідних компетентностей у програмі розвитку студента за спрямуванням (спеціалізацією) освітньої програми з використанням засобів освіти, опису системи знань, а також умінь і навичок, якими він повинен оволодіти після закінчення закладу вищої освіти. Але загалом при підготовці студента доцільно враховувати, крім цілей навчання на конкретній освітній програмі, ще й запит суспільства і держави для необхідності підготовки фахівця певного напрямку.

Як було зазначено вище, проблеми оцінки автентичності цифрових зображень на основі комплексного використання методів попередньої обробки зображень (методів фільтрації) та штучного інтелекту та виявлення ознак монтажу зображення на їх основі не були предметом окремого наукового дослідження. Сучасні освітні програми існуючих рівнів вищої освіти не містять окремих спеціалізованих програм підготовки, окремих обов'язкових і вибіркових компонент навчальних планів, у межах яких здійснюється

накопичення та розвиток конкретних здобутих знань, умінь і навичок фахівців у цьому напрямку.

На основі результатів проведених досліджень пропонуються напрямки базової підготовки або підвищення кваліфікації) фахівців з оцінки автентичності цифрових зображень у сучасних умовах у вигляді наступної програми підготовки.

Розділ 1. Структури цифрових зображень та їх формати.

Розділ присвячено вивченню способів цифрового представлення зображень.

Розділ 2. Технології та програмне забезпечення генерування цифрових зображень з використанням штучного інтелекту.

Розділ присвячено вивченню технологій та програмного забезпечення, що призначені для редагування та генерування цифрових зображень.

Розділ 3. Методи математичної обробки цифрових зображень для оцінки їх автентичності.

Розділ присвячено вивченню математичних методів цифрової обробки зображень та відповідного програмного забезпечення, що спрямовані на виявлення ознак зміни контенту засобами редагування.

Розділ 4. Методи комплексного використання попередньої математичної обробки зображень та методів штучного інтелекту для оцінки автентичності цифрових зображень

Розділ присвячено вивченню технологій та програмного забезпечення щодо комплексного використання методів цифрової обробки зображень та методів штучного інтелекту, що призначені для оцінки їх автентичності.

Сучасне суспільство і держава потребують підготовки фахівців у галузі комп'ютерної інженерії, які б володіли технічними знаннями щодо визначення компонентного складу, інформаційного забезпечення, функціональних можливостей, базових програмних продуктів, а також інших параметрів для оцінки наявності/відсутності ознак цифрової обробки зображення з метою встановлення його автентичності.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі на підставі проведених досліджень з оцінки автентичності зображень на основі узагальнення результатів одночасного застосування методів ELA, PCA та NOISE за допомогою моделей штучних нейронних мереж запропоновано основні напрямки підготовки фахівців з встановлення автентичності цифрових зображень з використанням методів штучного інтелекту.

Наукова новизна роботи полягає в оцінці ефективності комбінацій різних моделей штучних нейронних мереж і методів виділення цифрового шуму в зображеннях для вирішення задачі їх автентифікації.

Найкращим з досліджених класифікаторів, за результатами тестування ШНМ у стандартних конфігураціях, виявився класифікатор з архітектурою Unet++ та класифікатором ознак (кодером) типу timm-resnest269e з середнім критерієм Дайсе правильної сегментації зон редагування для використаної бази зображень 0.98762. Доведено, що оптимізація структури та параметрів ШНМ дозволяє отримати коефіцієнт Дайсе у 0.99379 для нестандартної конфігурації архітектури Unet++ та кодера timm-resnest269e.

Показано, що узагальнення за допомогою ШНМ результатів комплексного використання кількох методів попередньої обробки зображення краще за критерієм Дайсе (0.99379), ніж використання результатів окремих методів (0.99294).

Розглянуті приклади запровадження ШНМ доводять ефективність використання обраних методів і працездатність досліджених штучних нейронних семантичних

класифікаторів. Проведені дослідження дозволяють обґрунтовано визначити наведені в роботі напрямки підготовки фахівців до вирішення задачі автентифікаціїї зображень у сучасних умовах.

Перспективним продовженням цього наукового пошуку є подальші дослідження комплексного використання методів оцінки автентичності зображень з використанням моделей штучного інтелекту та впровадження їх результатів у відповідного профілю закладах фахової вищої освіти; у науково-дослідних установах системи Національної академії наук України; закладах вищої освіти, які проводять підготовку відповідних фахівців; експертів державних спеціалізованих науково-дослідних установ судових експертиз Міністерства юстиції України, зокрема, у процесі підготовки судових експертів за спеціальностями: 6.1 «Дослідження фотозображень та технічних засобів їх виготовлення», 7.1 «Технічне дослідження матеріалів та засобів відео-, звукозапису». Отримані результати також доцільно запровадити і при підготовці інших фахівців з дослідження автентичності зображень та відеозаписів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] M. Langford, *Langford's Basic Photography*, 10th ed. Abingdon, U.K.: Taylor and Francis, 2015. [Електронний ресурс]. Доступно: https://www.perlego.com/book/2192735/langfords-basic-photography-the-guide-for-serious-photographers-pdf

[2] M. Kriss, *Handbook of Digital Imaging*. Hoboken, NJ, USA: John Wiley & Sons, Feb. 2015.

[3] H. T. Sencar, L. Verdoliva, and N. Memon, Multimedia Forensics, 1st ed. Singapore: Springer, Apr. 2022. doi: 10.1007/978-981-16-7621-5.

[4] S. Seth, S. Rao, T. Verma, K. Viyanwar and P. Dandekar, "Fake Image Detector using Machine Learning," 2024 IEEE Pune Section International Conference (PuneCon), Pune, India, 2024, pp. 1-7, doi: 10.1109/PuneCon63413.2024.10895023.

[5] S. Agrawal, P. Kumar, S. Seth, T. Parag, M. Singh and V. Babu, "SISL:Self-Supervised Image Signature Learning for Splicing Detection & Localization," 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), New Orleans, LA, USA, 2022, pp. 22-32, doi: 10.1109/CVPRW56347.2022.00012.

[6] A. E. Daryani, M. Mirmahdi, A. Hassanpour, H. O. Shahreza, B. Yang and J. Fierrez, "IRL-Net: Inpainted Region Localization Network via Spatial Attention," in IEEE Access, vol. 11, pp. 115677-115687, 2023, doi: 10.1109/ACCESS.2023.3324541.

[7] P. Deb, S. Deb, A. Das and N. Kar, "Image Forgery Detection Techniques: Latest Trends and Key Challenges," in IEEE Access, vol. 12, pp. 169452-169466, 2024, doi: 10.1109/ACCESS.2024.3498340.

[8] С. М. Бобрицкий, "Методические аспекты комплексного исследования с целью выявления признаков монтажа в цифровой фотографии", *Теорія та практика судової експертизи і криміналістики*. Харків, Україна: Право, 2010. Вип. 10, с. 633-639.

[9] С. В. Чорний, О. І. Брендель, А. І. Роман, "Виявлення ознак редагування цифрових зображень за допомогою методу стеганографічного аналізу шумів", *Теорія та практика судової експертизи і криміналістики*. Харків, Україна: Право, 2019. Вип. 20, с.251-261.

[10] S. Bourouis, R. Alroobaea, A. M. Alharbi, M. Andejany, and S. Rubaiee, "Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis," *Symmetry*, vol. 12, no. 11, Art. no. 1811, Nov. 2020.

[11] S. Gupta, N. Mohan, and P. Kaushal, "Passive Image Forensics Using Universal Techniques: A Review," *Artif. Intell. Rev.*, vol. 55, pp. 1629–1679, 2022.

[12] О. І. Брендель, "Экспертиза відео-, звукозапису: теоретичні та організаційні засади", дис. докт. філос. в галузі права. Харків, ННЦ ІСЕ, 2024.

[13] Scientific Working Group on Digital Evidence, «SWGDE Best Practices for Forensic Audio», [Електронний ресурс]. Доступно: https://www.swgde.org/documents/Current%20. Дата звернення: Лютий. 25, 2024.

[14] Z. Liu, F. Zhang, J. He, J. Wang, Z. Wang, and L. Cheng, "Text-Guided Mask-Free Local Image Retouching," in Proc. IEEE Int. Conf. Multimedia Expo (ICME), Brisbane, Australia, 2023, pp. 2783–2788. doi: 10.1109/ICME55011.2023.00473.

[15] J. Yang and N. I. R. Ruhaiyem, "Review of Deep Learning-Based Image Inpainting Techniques," IEEE Access, vol. 12, pp. 138441–138482, 2024. doi: 10.1109/ACCESS.2024.3461782.

[16] S. Wang et al., "Imagen Editor and EditBench: Advancing and Evaluating Text-Guided Image Inpainting," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Vancouver, BC, Canada, 2023, pp. 18359–18369. doi: 10.1109/CVPR52729.2023.01761.
[17] Y.-C. Cheng, C. H. Lin, H.-Y. Lee, J. Ren, S. Tulyakov, and M.-H. Yang, "InOut: Diverse Image Outpainting via GAN Inversion," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), New Orleans, LA, USA, 2022, pp. 11421–11430. doi: 10.1109/CVPR52688.2022.01114.
[18] J. Wagner, Forensically. [Електронний ресурс]. Доступно: https://29a.ch/photo-forensics/#clone-detection. Дата звернення: Лютий. 24, 2025.
[19] FotoForensics. [Електронний ресурс]. Доступно: http://fotoforensics.com. Дата звернення: Лютий. 24, 2025.
[20] Izitru. [Електронний ресурс]. Доступно: https://www.izitru.com. Дата звернення: Лютий. 24, 2025.
[21] Imageforensic. [Електронний ресурс]. Доступно:http://www.imageforensic.org. Дата звернення: Лютий. 24, 2025.
[22] Веб-сервер Github. [Електронний ресурс]. Доступно: https://github.com/ImpulseAdventure/JPEGsnoop. Дата звернення: Лютий. 24, 2025.
[23] Photo Analysis and Tampering Detection. Amped Software. [Електронний ресурс]. Доступно: https://ampedsoftware.com/authenticate. Дата звернення: Лютий. 24. 2025.
[24] Веб-сервер Google Play. [Електронний ресурс]. Доступно: https://play.google.com/store/search?q=fake%20image%20detector&c=apps. Дата звернення: Лютий. 24, 2025.
[25] S. Kaur, A. Singh, and A. Jindal, "Analyzing Different Digital Image Authentication Methods," in *Proc. 2nd Int. Conf. Electron. Renewable Syst. (ICEARS)*, Tuticorin, India, 2023, pp. 804–811. doi: 10.1109/ICEARS56392.2023.10085193.
[26] K. A. P. da Costa, J. P. Papa, L. A. Passos, D. Colombo, J. Del Ser, K. Muhammad, and V. H. C. de Albuquerque, "A Critical Literature Survey and Prospects on Tampering and Anomaly Detection in Image Data," *Appl. Soft Comput.*, vol. 97, pt. B, Dec. 2020, Art. no. 106727. doi: 10.1016/j.asoc.2020.106727.
[27] M. Kaur and P. Garg, "A Review of Authentication Techniques Used for Security in Cloud Computing," in *Proc. 7th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Solan, Himachal Pradesh, India, 2022, pp. 187–191. doi: 10.1109/PDGC56933.2022.10053251.
[28] I. Ali, A. Khan, and M. Waleed, "A Google Colab Based Online Platform for Rapid Estimation of Real Blur in Single-Image Blind Deblurring," in *Proc. 12th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Bucharest, Romania, 2020, pp. 1–6. doi: 10.1109/ECAI50035.2020.9223244.
[29] Z. K. Kalazhokov and Y. T. Makoveichuk, "Methodology for Training Data Science Skills Based on Competitions on the Kaggle Platform," in *Proc. Seminar Inf. Comput. Process. (ICP)*, Saint Petersburg, Russia, 2023, pp. 94–96. doi: 10.1109/ICP60417.2023.10397418.
[30] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," *IEEE Access*, vol. 8, pp. 133488–133502, 2020. doi: 10.1109/ACCESS.2020.3009877.
[31] Веб-сервер Github. [Електронний ресурс]. Доступно:https://github.com/FrancescoMarra/E2E-ForgeryDetection Дата звернення: Лютий. 24, 2025.
[32] O. Le Meur and C. Guillemot, "Super-Resolution-Based Inpainting," in *Comput. Vis. – ECCV 2012*, vol. 7577, A. Fitzgibbon *et al.*, Eds. Berlin, Germany: Springer, 2012, pp. 554–567. doi: 10.1007/978-3-642-33783-3_40.
[33] G. Liu, F. A. Reda, K. Shih, T.-C. Wang, A. Tao, and B. Catanzaro, "Image Inpainting for Irregular Holes Using Partial Convolutions," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Munich, Germany, Sep. 2018. [Електронний ресурс]. Доступно: https://doi.org/10.48550/arXiv.1804.07723
[34] Веб-сервер Theinpaint. [Електронний ресурс]. Доступно: https://theinpaint.com Дата звернення: Лютий. 24, 2025.
[35] «Методика дослідження ознак монтажу цифрових зображень на основі аналізу ентропії шумів», зареєстрована у Державному реєстрі методик проведення судових експертиз МЮ України 18.01.2019 (реєстраційний код 7.1.15). [Електронний ресурс]. Доступно: https://rmpse.minjust.gov.ua/ Дата звернення: Лютий. 24. 2025.
[36] Веб-сервер Segmentation Models. [Електронний ресурс]. Доступно: https://smp.readthedocs.io/en/latest/ Дата звернення: Лютий. 24, 2025.
[37] J. He, S. Erfani, S. Wijewickrema, S. O'Leary, and K. Ramamohanarao, "Learning Non-Unique Segmentation with Reward-Penalty Dice Loss," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Glasgow, U.K., 2020, pp. 1–8. doi: 10.1109/IJCNN48605.2020.9206940.

Матеріал надійшов до редакції 16.05.2025 р.

USE OF ARTIFICIAL INTELLIGENCE METHODS TO ESTABLISH THE AUTHENTICITY OF DIGITAL IMAGES DURING THE TRAINING OF FORENSIC EXPERTS

Sergiy Chornyy
Candidate of Technical Sciences, Associate Professor, Leading researcher of National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID ID 0000-0002-0445-2886
svch1mail@yahoo.com

Olha Brendel
PhD, Head of Sector Computer Engineering, Telecommunications Research, and Video and Audio Recording Research
National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID ID 0000-0002-1723-0203
olgabrenda@ukr.net

Oleh Mieshkov
PhD, Head of the Fire and Electrical Research Sector
National Scientific Center «Hon. Prof. M. S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID ID 0000-0002-3046-6018
mesh_ol@ukr.net

Abstract. The potential opportunities and advantages of artificial intelligence methods contribute to the development and implementation of innovative technologies in various fields of science, including photography and video recording, which creates wide opportunities for manipulating the content of digital images and actualizes the problem of establishing their authentication. The widespread use of artificial intelligence methods for image editing sometimes makes it impossible or difficult to find changed areas.

In this regard, the purpose of this work is to substantiate the areas of training specialists to use of artificial intelligence methods during establishing the authenticity of images, and the main task is to study modern methods of its assessment.The article analyzes the use of artificial neural network models to assess the authenticity of images by the method of complex use of several methods for assessing noise with generalization of its distortions in an artificial neural network.

Special attention is paid to the analysis of modern technologies for editing digital images using artificial intelligence methods. The results of the study of known pre-processing methods for detecting inauthenticity of images edited by modern editing technologies and suitable for generalization by artificial intelligence methods are presented. The features of the use of neural network classifiers for assessing image editing zones with pre-processing using filtering methods also in the methodological plane are considered, namely when training experts in the field of phototechnical research and video recording research. The scientific novelty of the work lies in assessing the effectiveness of combinations of various artificial neural network models and methods for extracting digital noise in images to solve the problem of their authentication.

Probabilities for assessing the authenticity of images are provided based on the generalization of the results of the simultaneous application of ELA, PCA, and NOISE methods using artificial neural network models in the semantic classification and segmentation mode.

Based on the research conducted, the main areas of training specialists to solve the problem of image authentication in modern conditions have been determined.

Keywords: methods of artificial intelligence; digital images; authenticity of images; deep learning neural networks; semantic segmentation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] M. Langford, *Langford's Basic Photography*, 10th ed. Abingdon, U.K.: Taylor and Francis, 2015. [Online]. Available: https://www.perlego.com/book/2192735/langfords-basic-photography-the-guide-for-serious-photographers-pdf (in English)

[2] M. Kriss, *Handbook of Digital Imaging*. Hoboken, NJ, USA: John Wiley & Sons, Feb. 2015. (in English)

[3] D H. T. Sencar, L. Verdoliva, and N. Memon, *Multimedia Forensics*, 1st ed. Singapore: Springer, Apr. 2022. doi: 10.1007/978-981-16-7621-5. (in English)
[4] S. Seth, S. Rao, T. Verma, K. Viyanwar and P. Dandekar, "Fake Image Detector using Machine Learning," 2024 IEEE Pune Section International Conference (PuneCon), Pune, India, 2024, pp. 1-7, doi: 10.1109/PuneCon63413.2024.10895023. (in English)
[5] S. Agrawal, P. Kumar, S. Seth, T. Parag, M. Singh and V. Babu, "SISL:Self-Supervised Image Signature Learning for Splicing Detection & Localization," 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), New Orleans, LA, USA, 2022, pp. 22-32, doi: 10.1109/CVPRW56347.2022.00012. (in English)
[6] A. E. Daryani, M. Mirmahdi, A. Hassanpour, H. O. Shahreza, B. Yang and J. Fierrez, "IRL-Net: Inpainted Region Localization Network via Spatial Attention," in IEEE Access, vol. 11, pp. 115677-115687, 2023, doi: 10.1109/ACCESS.2023.3324541. (in English)
[7] P. Deb, S. Deb, A. Das and N. Kar, "Image Forgery Detection Techniques: Latest Trends and Key Challenges," in IEEE Access, vol. 12, pp. 169452-169466, 2024, doi: 10.1109/ACCESS.2024.3498340. (in English)
[8] S. M. Bobritsky, "Methodological aspects of a comprehensive study in order to identify signs of editing in digital photography", Theory and practice of ship examination and criminology, Kharkiv. VIP. 10. pp. 633-639, 2010. (in Russian).
[9] S. V. Chorny, O. I. Brendel, A. I. Roman, "A sign of digital image editing using the steganographic noise analysis method has been revealed", Theory and practice of ship examination and criminology, Kharkiv: Pravo. VIP. 20 P.251-261, 2019. (in Ukrainian).
[10] S. Bourouis, R. Alroobaea, A. M. Alharbi, M. Andejany, and S. Rubaiee, "Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis," *Symmetry*, vol. 12, no. 11, Art. no. 1811, Nov. 2020. (in English)
[11] S. Gupta, N. Mohan, and P. Kaushal, "Passive Image Forensics Using Universal Techniques: A Review," *Artif. Intell. Rev.*, vol. 55, pp. 1629–1679, 2022. (in English)
[12] O. I. Brendel, "Examination of video and sound recording: theoretical and organizational ambushes": dis. ... doc. philosophy in Galuzi is right. Kharkiv. 310 p., 2024.[in Ukrainian].
[13] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Forensic Audio", [Online]. Available: https://www.swgde.org/documents/Current%20 Documents. Accessed on: Feb. 24, 2025. (in English)
[14] Z. Liu, F. Zhang, J. He, J. Wang, Z. Wang, and L. Cheng, "Text-Guided Mask-Free Local Image Retouching," in *Proc. IEEE Int. Conf. Multimedia Expo (ICME)*, Brisbane, Australia, 2023, pp. 2783–2788. doi: 10.1109/ICME55011.2023.00473. (in English)
[15] J. Yang and N. I. R. Ruhaiyem, "Review of Deep Learning-Based Image Inpainting Techniques," *IEEE Access*, vol. 12, pp. 138441–138482, 2024. doi: 10.1109/ACCESS.2024.3461782. (in English)
[16] S. Wang *et al.*, "Imagen Editor and EditBench: Advancing and Evaluating Text-Guided Image Inpainting," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Vancouver, BC, Canada, 2023, pp. 18359–18369. doi: 10.1109/CVPR52729.2023.01761. (in English)
[17] Y.-C. Cheng, C. H. Lin, H.-Y. Lee, J. Ren, S. Tulyakov, and M.-H. Yang, "InOut: Diverse Image Outpainting via GAN Inversion," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, New Orleans, LA, USA, 2022, pp. 11421–11430. doi: 10.1109/CVPR52688.2022.01114. (in English)
[18] Wagner J. "Forensically", Accessed on: Feb. 24, 2025. [Online]. Available: https://29a.ch/photo-forensics/#clone-detection. (in English)
[19] FotoForensics, [Online]. Available: http://fotoforensics.com. Accessed on: Feb. 24, 2025. (in English)].
[20] Izitru, [Online]. Available: https://www.izitru.com. Accessed on: Feb. 24, 2025. (in English)
[21] Imageforensic, [Online]. Available:http://www.imageforensic.org Accessed on: Feb. 24, 2025. (in English)
[22] Web server Github, [Online]. Available:https://github.com/ImpulseAdventure/ Accessed on: Feb. 24, 2025. (in English)
[23] Photo Analysis and Tampering Detection, Amped Software.. [Online]. Available: https://ampedsoftware.com/authenticate. Accessed on: Feb. 24, 2025. (in English)
[24] Web server Google Play, [Online]. Available: https://play.google.com/store/search?q=fake%20image%20detector&c=apps Accessed on: Feb. 24, 2025. (in English)
[25] S. Kaur, A. Singh, and A. Jindal, "Analyzing Different Digital Image Authentication Methods," in *Proc. 2nd Int. Conf. Electron. Renewable Syst. (ICEARS)*, Tuticorin, India, 2023, pp. 804–811. doi: 10.1109/ICEARS56392.2023.10085193. (in English)
[26] K. A. P. da Costa, J. P. Papa, L. A. Passos, D. Colombo, J. Del Ser, K. Muhammad, and V. H. C. de Albuquerque, "A Critical Literature Survey and Prospects on Tampering and Anomaly Detection in

Image Data," *Appl. Soft Comput.*, vol. 97, pt. B, Dec. 2020, Art. no. 106727. doi: 10.1016/j.asoc.2020.106727. (in English)
[27] M. Kaur and P. Garg, "A Review of Authentication Techniques Used for Security in Cloud Computing," in *Proc. 7th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Solan, Himachal Pradesh, India, 2022, pp. 187–191. doi: 10.1109/PDGC56933.2022.10053251. (in English)
[28] I. Ali, A. Khan, and M. Waleed, "A Google Colab Based Online Platform for Rapid Estimation of Real Blur in Single-Image Blind Deblurring," in *Proc. 12th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Bucharest, Romania, 2020, pp. 1–6. doi: 10.1109/ECAI50035.2020.9223244. (in English)
[29] Z. K. Kalazhokov and Y. T. Makoveichuk, "Methodology for Training Data Science Skills Based on Competitions on the Kaggle Platform," in *Proc. Seminar Inf. Comput. Process. (ICP)*, Saint Petersburg, Russia, 2023, pp. 94–96. doi: 10.1109/ICP60417.2023.10397418. (in English)
[30] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," *IEEE Access*, vol. 8, pp. 133488–133502, 2020. doi: 10.1109/ACCESS.2020.3009877. (in English)
[31] Web server Github, [Online]. Available: https://github.com/FrancescoMarra/E2E- Accessed on: Feb. 24, 2025. (in English)
[32] O. Le Meur and C. Guillemot, "Super-Resolution-Based Inpainting," in *Comput. Vis. – ECCV 2012*, vol. 7577, A. Fitzgibbon *et al.*, Eds. Berlin, Germany: Springer, 2012, pp. 554–567. doi: 10.1007/978-3-642-33783-3_40. (in English)
[33] G. Liu, F. A. Reda, K. Shih, T.-C. Wang, A. Tao, and B. Catanzaro, "Image Inpainting for Irregular Holes Using Partial Convolutions," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Munich, Germany, Sep. 2018. [Online]. Available: https://doi.org/10.48550/arXiv.1804.07723 (in English)
[34] Web server Theinpaint, [Online]. Available: https://theinpaint.com Accessed on: Feb. 24, 2025. (in English)
[35] «Methodology for tracking the installation of digital images based on the analysis of noise entropy» from the State Register of Methods for Conducting Ship Expertise of the Ministry of Justice of Ukraine on January 18, 2019 (registration code 7.1.15), [Online]. Available: https://rmpse.minjust.gov.ua/ Accessed on: Feb. 24, 2025 (in Ukrainian).
[36] Web server Segmentation Models, [Online]. Available:https://smp.readthedocs.io/en/latest/ (in English).
[37] J. He, S. Erfani, S. Wijewickrema, S. O'Leary, and K. Ramamohanarao, "Learning Non-Unique Segmentation with Reward-Penalty Dice Loss," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Glasgow, U.K., 2020, pp. 1–8. doi: 10.1109/IJCNN48605.2020.9206940.(in English).

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.