НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

77-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

16 травня – 22 травня 2025 р.

УДК 004.932.4

Д.Д. Гаврилко, студентка групи 402-ТН,
О.В. Скакаліна, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

МЕТОДИ ВИЯВЛЕННЯ МАНІПУЛЯЦІЙ У ЦИФРОВИХ ЗОБРАЖЕННЯХ: ТЕХНІЧНА ПЕРЕВІРКА ЯК ІНСТРУМЕНТ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

У сучасному цифровому просторі маніпуляції зображеннями набули масштабного поширення, що пов’язано з розвитком технологій редагування та генерації візуального контенту. Цифрові зображення часто використовуються для поширення дезінформації, що впливає на громадську думку та безпеку суспільства. Тому розробка та впровадження методів технічної перевірки зображень є надзвичайно актуальними.

Існуючі методи виявлення маніпуляцій у цифрових зображеннях можна класифікувати за п’ятьма основними категоріями [3, 4]:

– аналіз формату зображення (зокрема JPEG) – виявлення змін у структурі блоків, подвійного стиснення та квантування, що свідчить про редагування;

– піксельний аналіз – виявлення копіювання, переміщення або перекомпонування фрагментів зображення;

– аналіз слідів камери – вивчення шуму датчика, колірних фільтрів, хроматичної аберації та інших унікальних характеристик, які змінюються при редагуванні;

– фізичне середовище – аналіз освітлення, тіней і просторових співвідношень, які складно імітувати при монтажі;

– метадані – перевірка інформації про камеру, дату, програмне забезпечення, що може вказувати на фальсифікацію.

Одним із найпоширеніших інструментів є аналіз рівня помилок (Error Level Analysis, ELA), який порівнює оригінал із рекомпресованою копією, виявляючи області з різним рівнем стиснення, що свідчить про зміну зображення. Ефективність цього методу підтверджується численними експериментами, де маніпульовані ділянки чітко виділяються від оригінальних [3].

Сучасні дослідження активно впроваджують алгоритми глибинного навчання. Наприклад, BusterNet – модель, що складається з двох гілок, одна з яких локалізує маніпульовані області, а інша аналізує подібність пікселів для виявлення копіювань. Ця модель демонструє високу точність у виявленні складних маніпуляцій, що важко розпізнати візуально. Інший приклад – ManTra-Net, яка здатна виявляти широкий спектр атак маніпуляції, генеруючи маски змінених ділянок із високою точністю. Вона

базується на аналізі локальних аномалій і функцій зображення, що робить її універсальним інструментом для боротьби з різними видами підробок [2].

Сучасні методи виявлення маніпуляцій у цифрових зображеннях активно використовують алгоритми машинного навчання, зокрема глибинні нейронні мережі, які здатні виявляти навіть складні форми підробок. Згорткові нейронні мережі (CNN) аналізують текстурні та статистичні особливості зображень, що важко розпізнати людським оком або традиційними алгоритмами. Наприклад, модель ManTra-Net поєднує локальне виявлення аномалій із глобальним аналізом, що дозволяє ефективно ідентифікувати різні типи маніпуляцій, включно з підробками, створеними генеративними змагальними мережами (GAN). Цей підхід значно підвищує точність виявлення і є перспективним напрямом розвитку цифрової криміналістики.

Важливим аспектом є також інтеграція технічних засобів перевірки зображень у соціальні мережі та медіа-платформи, що дозволяє автоматизувати процес виявлення фейкового контенту в реальному часі. Застосування цифрових водяних знаків і криптографічних підписів допомагає підтвердити автентичність зображень і відстежити їх походження, що є важливим для забезпечення довіри користувачів і протидії поширенню дезінформації. В Україні, з огляду на інформаційну війну, розвиток таких технологій є надзвичайно актуальним для захисту інформаційного простору.

Статистичні дані підтверджують гостру необхідність розвитку таких методів. В Україні, за інформацією СБУ, відкрито понад 2,5 тисячі кримінальних проваджень, пов’язаних із поширенням антиукраїнського контенту, значна частина якого містить маніпульовані або штучно створені зображення [1]. При цьому близько 40% користувачів не можуть відрізнити справжнє фото від фейкового, що створює значні ризики для інформаційної безпеки.

Важливість технічної перевірки зображень полягає також у її застосуванні в журналістиці, криміналістиці, наукових публікаціях та інших сферах, де достовірність візуального контенту є критичною. З огляду на розвиток технологій штучного інтелекту, які дозволяють створювати дедалі більш реалістичні підробки, традиційні методи виявлення стають недостатніми, що стимулює розвиток нових алгоритмів із використанням машинного навчання.

Таким чином, тема методів виявлення маніпуляцій у цифрових зображеннях є надзвичайно актуальною і має стратегічне значення для протидії дезінформації. Впровадження ефективних технічних рішень дозволяє підвищити інформаційну безпеку, зміцнити довіру до медіа та зменшити вплив маніпулятивного контенту на суспільство.

Література:

1. СБУ за час великої війни порушила майже 25 тисяч справ щодо антиукраїнських інтернет-агітаторів. URL: https://hromadske.ua/suspilstvo/241362-sbu-za-chas-velykoyi-viyny-porushyla-mayze-25-tysiachi-sprav-shchodo-antyukrayinskykh-internet-ahitatoriv (дата звернення – 01.05.2025 р.).

2. Bayar B., Stamm M.C. A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. IEEE Transactions on Information Forensics and Security, 2020.

3. Verification Handbook: Перевірка зображень. Практичний посібник із цифрової верифікації, 2023. URL: https://verificationhandbook.com/book_ua/chapter4.php (дата звернення – 01.05.2025 р.).

4. Кобилін О. А., Творошенко І. С. Методи цифрової обробки зображень: навчальний посібник. Харків: НТУ «ХПІ», 2019. URL: https://openarchive.nure.ua/server/api/core/bitstreams /c739b2e6-aa8c-4fa0-92b1-dfb0d76e88d2/content (дата звернення – 01.05.2025 р.).