Криміналістичні особливості виявлення та дослідження змінених цифрових зображень як джерела доказової інформації

Олег Пододворний
директор, Волинський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України, м. Волинь, Україна

Оксана Гусак
аспірант, Волинський національний університет імені Лесі Українки, м. Волинь, Україна,
ORCID: https://orcid.org/0009-0002-5775-0470, e-mail: ogusak99@gmail.com

Проаналізовано криміналістичні особливості виявлення та дослідження змінених цифрових зображень як джерела доказової інформації в кримінальному провадженні. Проаналізовано основні види модифікації зображень, зокрема splicing, copy-move та deepfake, визначено їхній вплив на достовірність цифрових доказів. Розглянуто криміналістичні ознаки змінених зображень, включно з невідповідністю шуму, JPEG-артефакти й порушення структури зображення. Визначено основні проблеми їх виявлення, пов'язані з повторною обробкою, поширенням у цифровому середовищі та розвитком технологій anti-forensics. Обґрунтовано необхідність удосконалення криміналістичних підходів з урахуванням сучасних технологічних викликів і відставання наявних методів від засобів модифікації цифрових зображень.

Ключові слова: *цифрові зображення; цифрові докази; криміналістика; deepfake; обробка зображень; виявлення підробок; anti-forensics; JPEG-артефакти.*

Criminalistic Features of Detection and Examination of Altered Digital Images as a Source of Evidentiary Information

Oleh Pododvornyi, Oksana Husak

The paper examines forensic features of detection and analysis of altered digital images as a source of evidentiary information in criminal proceedings. The main types of image manipulation, including splicing, copy-move, and deepfake technologies, are analyzed, along with their impact on the reliability of digital evidence. The study identifies key forensic indicators of image alteration, such as noise inconsistency, JPEG artifacts, and structural distortions. Major challenges in detection are outlined, including repeated processing, distribution in digital environments, and the development of anti-forensic techniques. The necessity of improving forensic approaches is substantiated, taking into account current technological challenges and the lag of existing methods behind modern image manipulation technologies.

Keywords: *digital images; digital evidence; forensics; deepfake; image processing; forgery detection; anti-forensics; JPEG artifacts.*

У сучасних умовах цифрові зображення набувають значення джерела доказової інформації у кримінальному провадженні. Вони відображають обставини події та можуть мати доказове значення.

Водночас розвиток програмних засобів обробки зображень зумовив значне поширення їх модифікації, включно з як простим редагуванням, так і зі складними технологіями штучного інтелекту, зокрема *deepfake*. Такі зміни можуть спотворювати зміст зображення або створювати фальсифіковану інформацію. Як зазначають дослідники, межа між автентичним і зміненим цифровим контентом стає дедалі менш очевидною, що ускладнює процес установлення його достовірності [1, p. 911–913].

Змінені цифрові зображення є різновидом цифрових даних, які зазнали втручання з метою зміни змісту або структури. У криміналістичному аспекті їх розглядають як потенційне джерело доказової інформації, яке потребує перевірки достовірності й цілісності [2, с. 45—47].

Одним із поширених видів змінених зображень є *splicing*, що полягає у вставці фрагментів одного зображення в інше. Іншим видом є *copy-move*, що передбачає копіювання частини зображення в межах файлу [3, p. 1–2].

Окрему групу становлять зображення, створені за допомогою штучного інтелекту (*deepfake*), які складно відрізнити від автентичних [1, p. 912–915].

Криміналістичні ознаки змінених цифрових зображень виявляються у слідах утручання.

Однією з основних ознак є *невідповідність шуму зображення*, оскільки різні пристрої формують різний шумовий профіль. У разі внесення змін або комбінування фрагментів з різних джерел виникають відмінності у розподілі шуму [3, p. 2–3]. Важливим індикатором змін є також *JPEG-артефакти*, що виникають унаслідок багаторазового збереження зображення або редагування його окремих частин. Порушення структури *JPEG*-стиснення та *JPEG ghosts* свідчать про втручання [4, p. 155–157]. Іще однією ознакою є *порушення структури зображення*, яке виявляється у невідповідності освітлення, перспективи, тіней або геометричних пропорцій об'єктів. Такі розбіжності можуть бути наслідком поєднання фрагментів із різних джерел або некоректного редагування, що дає змогу виявити штучність зображення навіть за відсутності технічних слідів утручання [5, p. 18–20].

До технічних індикаторів підробки належать також невідповідності метаданих, сліди повторного стиснення, аномалії у колірних просторах та інші цифрові «відбитки», що залишаються внаслідок обробки зображення.

Однією з основних проблем є *вплив повторного збереження та обробки зображень*. Багаторазове стиснення, масштабування або зміна формату призводять до втрати первинних характеристик зображення, що ускладнює виявлення слідів редагування. Зокрема, повторне *JPEG*-стиснення може знищувати або маскувати артефакти, якими послуговувалися для встановлення факту підробки, що значно знижує ефективність криміналістичного аналізу [3, p. 2–3].

Суттєво ускладнює виявлення змінених зображень їх поширення через *соціальні мережі й інтернет-платформи*, які автоматично змінюють параметри файлів [3, p. 3–4]. У сучасних умовах першоджерело цифрового зображення фактично втрачає значення, оскільки об'єктом дослідження стає вже трансформований інформаційний продукт, що ускладнює застосування традиційних криміналістичних підходів.

Складність виявлення змінених зображень також пов'язана з *обмеженою ефективністю сучасних алгоритмів*. Більшість наявних методів демонструють низьку результативність у реальних умовах. Навіть сучасні підходи не забезпечують стабільних результатів, що свідчить про необхідність подальшого розвитку методів цифрової криміналістики [1, p. 920–923]. Це свідчить про те, що сучасна цифрова криміналістика перебуває у стані відставання від технологій модифікації зображень.

Додатковим чинником ускладнення є розвиток технологій *anti-forensics*, спрямованих на приховування слідів редагування. Зловмисники можуть користуватися спеціальними методами для маскування змін, зокрема імітацією природного шуму, згладжуванням артефактів або зміною статистичних характеристик зображення. Такі дії значно ускладнюють виявлення підробок і можуть робити традиційні криміналістичні методи неефективними [6, p. 1052–1055].

Отже, проблеми виявлення змінених цифрових зображень мають комплексний характер та охоплюють як технічні, так і організаційні аспекти. Їх розв'язання потребує вдосконалення наявних методів аналізу, адаптації криміналістичних підходів до реальних умов обігу цифрової інформації та врахування сучасних технологічних викликів.

Дослідження та оцінка змінених цифрових зображень як джерела доказової інформації мають особливості, зумовлені їх цифровою природою та можливістю модифікації. У кримінальному провадженні такі зображення повинні відповідати вимогам належності й допустимості, що передбачає встановлення їх походження, способу отримання та зв'язку з обставинами справи. Порушення процедури вилучення або фіксації може призвести до втрати доказового значення навіть за наявності інформативного змісту [7, с. 210—212].

Важливим етапом є *перевірка достовірності цифрових зображень*, яку ускладнює

можливість їх редагування без видимих ознак утручання [5, p. 18–20].

Окрему складність становить *інтерпретація змісту цифрових зображень*, яка залежить від контексту. Те саме зображення може мати різне доказове значення (залежно від умов його отримання, часу створення та зв'язку з іншими доказами). Без урахування цих чинників існує ризик неправильного тлумачення інформації, що може призвести до помилкових висновків у кримінальному провадженні [2, с. 48—50].

Важливу роль у дослідженні змінених зображень відіграє *експерт*, який здійснює технічний аналіз і формує висновки щодо їх автентичності. Залучення експерта є необхідним через складність сучасних технологій обробки зображень та обмежені можливості самостійної оцінки таких доказів учасниками кримінального провадження.

Складність оцінки змінених цифрових зображень зумовлена також труднощами *доведення факту підробки*, особливо у випадках застосування сучасних технологій, зокрема штучного інтелекту. Високий рівень реалістичності таких зображень ускладнює встановлення їх неавтентичності та потребує комплексного підходу, що поєднує технічний аналіз і правову оцінку [1, p. 913–915]. Отже, дослідження та оцінка змінених цифрових зображень є складними через необхідність установлення їх достовірності й інтерпретації.

Удосконалення криміналістичних підходів до виявлення і дослідження змінених цифрових зображень потребує впровадження сучасних технічних та організаційних рішень. Одним з основних напрямів є користування спеціалізованими *forensic-інструментами*, які дають змогу здійснювати аналіз цифрових зображень з урахуванням їх технічних характеристик, виявляти сліди редагування та забезпечувати збереження цілісності інформації. Застосування таких засобів підвищує точність дослідження та створює можливість об'єктивної перевірки отриманих результатів [8, p. 120–125].

На особливу увагу заслуговує *адаптація криміналістичних методів до нових технологій*, зокрема до використання штучного інтелекту у створенні й обробці зображень. Поширення *deepfake* та інших форм генеративного контенту потребує розроблення нових підходів до їх виявлення, оскільки традиційні методи часто виявляються недостатньо ефективними [1, p. 920–922].

Отже, проблема виявлення змінених цифрових зображень виходить за межі суто технічного аналізу й потребує перегляду традиційних криміналістичних підходів з урахуванням цифрової трансформації інформаційного середовища.

Висновки. Цифрові зображення є важливим джерелом доказової інформації, однак їх модифікація, зокрема за допомогою штучного інтелекту, суттєво ускладнює встановлення достовірності. Криміналістичні ознаки змінених зображень дають змогу виявляти втручання, проте їхня ефективність знижується в умовах повторної обробки та поширення через цифрові платформи. Сучасна практика свідчить про відставання криміналістичних методів від технологій створення та приховування підробок, що потребує їх перегляду. Оцінку таких зображень як доказів ускладнено необхідністю забезпечення їх допустимості, правильної інтерпретації та залежністю від висновків експертів. Удосконалення криміналістичних підходів потребує поєднання технічних засобів, розвитку методик виявлення та адаптації до сучасних цифрових викликів.

Перелік джерел посилання

1. Verdoliva L. Media Forensics and DeepFakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*. 2020. Vol. 14. No. 5. P. 910–932. DOI: 10.1109/JSTSP.2020.3002101 (дата звернення: 12.04.2026).
2. Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. 2023. № 1—2. С. 42—53. DOI: 10.17721/2413-5372.2023.1-2/42-53 (дата звернення: 12.04.2026).
3. Zampoglou M., Papadopoulos S., Kompatsiaris Y. Detecting Image Splicing in the Wild (Web). *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*. 2015. P. 1–6. DOI: 10.1109/ICMEW.2015.7169839 (дата звернення: 12.04.2026).
4. Farid H. Exposing Digital Forgeries from JPEG Ghosts. *IEEE Transactions on Information Forensics and Security*. 2009. Vol. 4. No. 1. P. 154–

160. DOI: 10.1109/TIFS.2008.2012211 (дата звернення: 12.04.2026).
5. Ibidem. Image Forgery Detection. *IEEE Signal Processing Magazine.* 2009. Vol. 26. No. 2. P. 16–25. DOI: 10.1109/MSP.2008.931079 (дата звернення: 12.04.2026).
6. Stamm M. C., Liu K. J. R. Anti-Forensics of Digital Image Compression. *IEEE Transactions on Information Forensics and Security.* 2011. Vol. 6. No. 3. P. 1050–1065. DOI: 10.1109/TIFS.2011.2119314 (дата звернення: 12.04.2026).
7. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3 (102). Ч. 2. С. 207—220.
8. Farid H. Photo Forensics. Cambridge, MA : MIT Press, 2016.