DOI: 10.32347/2412-9933.2025.63.223-229
УДК 004.93

Шабала Євгенія Євгенівна
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії,
https://orcid.org/0000-0002-0428-9273
Київський національний університет будівництва і архітектури, Київ
Корнійчук Борис Валерійович
Кандидат технічних наук, доцент, доцент кафедри професійної освіти,
https://orcid.org/0000-0003-3881-1581
Київський національний університет будівництва і архітектури, Київ

ЗАСТОСУВАННЯ ФОРЕНЗИЧНОГО АНАЛІЗУ ДЛЯ ВИЗНАЧЕННЯ АВТЕНТИЧНОСТІ ЗОБРАЖЕНЬ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Анотація. *Стрімкий розвиток цифрових технологій та їх інтеграція у всі сфери суспільного життя сприяли не лише підвищенню ефективності комунікації та обробки інформації, але й зумовили появу нових загроз, пов'язаних із використанням цифрових пристроїв у протиправній діяльності. Особливу небезпеку становлять злочини, спрямовані на втручання в роботу об'єктів критичної інфраструктури, а також кіберзлочини проти фізичних осіб, зокрема інтернет-шахрайство, викрадення персональних даних і поширення фальсифікованих матеріалів. У цьому контексті цифрова криміналістика виступає ключовим інструментом ідентифікації, фіксації та дослідження цифрових доказів. У статті розглянуто актуальну проблему зростання кіберзлочинності, зокрема таких її форм, як несанкціоноване втручання у критичну інфраструктуру, шахрайські дії в Інтернеті та незаконне використання персональних даних. У зв'язку з цим підкреслюється важливість цифрової криміналістики (форензики) як інструменту розслідування правопорушень, що пов'язані з використанням цифрових технологій. Особлива увага приділяється аналізу цифрових зображень, які можуть бути змінені з метою фальсифікації або введення в оману. У статті досліджено методи виявлення ознак редагування цифрових зображень з використанням інструментів форензики. Розглянуто низку підходів, таких як аналіз метаданих (EXIF), що дозволяє виявити зміни у технічних параметрах знімка; аналіз стиснення JPEG для виявлення подвійного стиснення, характерного для відредагованих зображень; а також піксельний аналіз, що виявляє колірні аномалії, невідповідності в освітленні та тінях. Описано застосування програмних засобів, зокрема Adobe Photoshop, для виявлення маніпуляцій шляхом аналізу гістограм, рівнів яскравості, каналів кольору та шумів. Продемонстровано, як методи ELA (Error Level Analysis) та фільтри, як-от «Тиснення», можуть допомогти візуалізувати сліди втручання в зображення. Наведено приклади редагування з використанням Clone Stamp Tool, вставки фрагментів та виявлення ознак клонування. Зроблено висновок про значущість цифрових слідів як доказової бази у кримінальному провадженні та необхідність застосування надійних методів їх виявлення, збереження та інтерпретації відповідно до стандартів цифрової криміналістики.*

Ключові слова: форензика, цифрова криміналістика, метадані, канали, фільтр

Постановка проблеми

Цифрові технології та пристрої набули широкого поширення в усіх сферах життєдіяльності людини, що зумовило виникнення нових форм злочинної діяльності, пов'язаної з їх використанням. Зокрема, спостерігається зростання кількості злочинів, пов'язаних із несанкціонованим зовнішнім втручанням у функціонування об'єктів критичної інфраструктури, таких як енергетичні та транспортні системи, банківські установи, а також окремі державні та приватні організації (так звані кібератаки).

Крім того, зловмисники дедалі частіше вдаються до шахрайських дій у мережі Інтернет, жертвами яких стають фізичні особи. У процесі підготовки та реалізації злочинних намірів правопорушники активно використовують цифрові пристрої та телекомунікаційні мережі для збору, викрадення персональних даних потенційних жертв, а також для координації дій між членами організованих злочинних груп.

З огляду на зазначене, Національна поліція України надає публічні рекомендації щодо фіксації цифрових слідів, які можуть бути використані як доказова база під час розслідування правопорушень,

зокрема інтернет-шахрайства. Отже, вивчення та дослідження цифрових слідів набуває особливої актуальності у межах сучасної криміналістики.

Зважаючи на зростаючу роль цифрових технологій у вчиненні злочинів, особливо актуальним стає питання ефективного виявлення, збирання, аналізу та збереження цифрових доказів. У цьому контексті форензичний аналіз (цифрова криміналістика) відіграє ключову роль як на етапі досудового розслідування, так і в подальшому судовому провадженні.

Аналіз останніх досліджень і публікацій

Форензичний аналіз – це сукупність методів і засобів, спрямованих на ідентифікацію, вилучення, збереження, документування та інтерпретацію цифрової інформації, що має значення для розслідування злочинів. Цей вид аналізу охоплює широке коло технічних напрямів, включаючи дослідження комп'ютерних систем, мобільних пристроїв, мережевих журналів та облікових записів у хмарних сервісах.

Цифрова криміналістика вимагає високої точності та дотримання суворих процедурних стандартів, оскільки будь-яке порушення цілісності або автентичності цифрового доказу може призвести до його неприйнятності в суді. Тому фахівці використовують спеціалізоване програмне забезпечення, інструменти для захищеного копіювання даних (наприклад, write-blockers), а також методики верифікації отриманої інформації.

У першу чергу, необхідно акцентувати увагу на відсутності єдиного загальноприйнятого терміну для позначення таких слідів. У науковій літературі використовуються поняття «цифрові сліди», «електронні сліди», «віртуальні сліди» та «комп'ютерні сліди». Наприклад, А. М. Лазебний [1, с. 231], використовуючи поняття «електронний слід», визначає його як ідеальне електронне відображення (статичне чи динамічне) матеріального сліду в інформаційно-телекомунікаційній системі.

Я. Найдьон [2, с. 306] використовує термін «віртуальні сліди», визначаючи їх як цифровий образ або електронні сигнали, що залишаються в пам'яті електронних пристроїв і мають кримінально-релевантне значення. Варто зазначити, що термін «віртуальні сліди» акцентує увагу на їхньому існуванні у віртуальному просторі, ігноруючи їхню інформаційну сутність. Натомість, на думку В. В. Пахомова [3, с. 131], цифрові сліди – це сукупність інформації про діяльність користувача інформаційно-телекомунікаційного середовища.

Специфіка цифрових слідів також полягає в можливості їхнього легкого копіювання (виготовлення дублікатів) без втрати якості, а також здатності до змінення та знищення. Так, цифрові фото, відео та електронні документи можуть бути як скопійовані, так і піддані редагуванню змісту [4, с. 74].

Виклад основного матеріалу

У контексті форензичного аналізу надзвичайно важливою складовою є кібербезпека. Вона виступає не лише як превентивний інструмент, але і як основа для ефективного реагування на інциденти інформаційної безпеки. Взаємозв'язок між цифровою криміналістикою та кібербезпекою є тісним: результати форензичного аналізу часто слугують джерелом інформації для виявлення вразливостей та вдосконалення систем захисту, тоді як ефективна кіберзахистна інфраструктура забезпечує умови для своєчасного виявлення цифрових слідів та запобігання подальшому поширенню шкідливих впливів.

Одним із ключових розділів цифрової криміналістики є аналіз цифрових об'єктів, зокрема зображень, на предмет можливого втручання або маніпуляцій. Такий аналіз дозволяє не лише встановити факти змін, але й виявити методи, які були використані зловмисниками. Це, у свою чергу, дасть можливість підвищити рівень кібербезпеки.

Існує значна кількість програмних пакетів для роботи з графікою, що пояснюється особливостями подання графічної інформації. Графічне подання є наочним, краще сприймається, подається у концентрованому вигляді та сприяє розвитку образного мислення [5].

Для форензичного аналізу використовуються спеціалізовані інструменти, зокрема ExifTool, PhotoME, Metadata++, JPEGsnoop, Adobe Photoshop, GIMP, ImageJ, Amped Authenticate, Photoshop Levels/Histogram Tool, RawDigger.

Новітні досягнення штучного інтелекту (ШІ) і машинного навчання (МН) забезпечили можливість генерувати фотореалістичні зображення, які складно відрізнити від справжніх. Це призвело до появи нового типу загроз – deepfake та генеративного фейкового контенту, який активно використовується для дезінформації, маніпуляції громадською думкою, шантажу тощо.

У зв'язку з цим виникла гостра потреба у створенні та впровадженні інструментів для виявлення зміненого або штучно створеного зображення. Сучасні ШІ/МН-рішення дозволяють ефективно визначати ознаки підробки навіть у високоякісному медіаконтенті. Існують спеціалізовані ШІ/МН-інструменти для виявлення deepfake/генеративних зображень, як-от Microsoft Video Authenticator, Deepware Scanner, Hive Moderation Image Detection.

Для захисту та виявлення порушення цілісності цифрового зображення створюються відповідні

методи та алгоритми, які поділяються на дві великі категорії: активні та пасивні. В активних методах деяка інформація попередньо впроваджується у цифрове зображення. Пасивні методи дозволяють підтвердити цілісність цифрового зображення або виявити її порушення без впровадження додаткової інформації [6].

Цифрова криміналістика (форензика) розробила низку методів, які дозволяють виявити, чи зазнало зображення редагування, та встановити характер таких змін. Основні методи форензичного аналізу зображень систематизовано і представлено в таблиці.

Методи та експериментальний аналіз форензики зображень

Для детермінації факту внесення змін у цифрове зображення (визначення його фальсифікації) було застосовано низку практичних методів, що ґрунтуються на форензичному аналізі. Для експериментальної ілюстрації створено сфальсифіковане зображення шляхом внесення штучних ознак редагування, зокрема:

1. *Клонування* (Clone Stamp Tool). Частина зображення була скопійована та вставлена в іншу область.

2. *Вирізання та Вставка*. Фрагмент був вирізаний з одного зображення та інтегрований в інше.

Результати маніпуляцій продемонстровано на рис. 1, де представлено оригінал (ліворуч) і сфальсифіковане зображення (праворуч).

Аналіз гістограми та рівнів

Одним із базових методів перевірки цілісності зображення є аналіз його гістограми (рис. 2). Гістограма відображає розподіл яскравості пікселів, де вісь X (горизонтальна) показує значення яскравості від 0 (чорний) до 255 (білий), а вісь Y (вертикальна) – кількість пікселів із відповідним значенням.

Рисунок 1 – Оригінал (ліворуч) і сфальсифіковане зображення (праворуч)

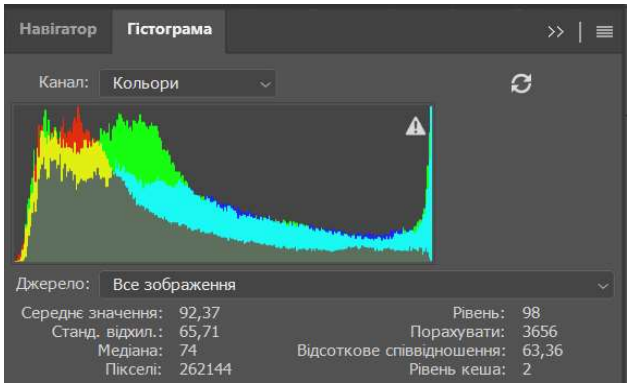

Рисунок 2 – Гістограма зображення

*Таблиця – **Методи визначення відредагованих зоброжень***

Метод	Опис
Аналіз метаданих (EXIF-даних)	EXIF – це дані, що автоматично записуються камерою під час створення зображення. Вони можуть містити інформацію про дату, час, модель пристрою, параметри зйомки тощо. Під час редагування зображення метадані можуть бути змінені або видалені.
Аналіз стиснення JPEG	Формат JPEG застосовує стиснення з втратою якості. При цьому відбувається поява артефактів у вигляді певних закономірностей у блоках 8×8 пікселів. Якщо частина зображення була змінена і знову збережена у JPEG-форматі, це може призвести до появи «подвійного стиснення».
Аналіз структур пікселів і колірних аномалій	Методи піксельного аналізу дозволяють виявити неприродні переходи кольорів або освітлення, які виникають унаслідок копіювання або вставлення об'єктів.
Error Level Analysis (ELA)	ELA – це метод, який візуалізує рівень помилок у кожному сегменті зображення після повторного збереження з певним рівнем стиснення. Оригінальні області мають однаковий рівень помилок, тоді як відредаговані частини показують відмінності.
Аналіз тіней і відображень	Розрахунок фізичних властивостей світла та тіней дозволяє виявити неприродну поведінку об'єктів на зображенні.
Ідентифікація джерела зображення	Цифрові камери залишають унікальний слід (noise pattern) – цифровий «відбиток пальця». За допомогою аналізу шуму сенсора можна порівняти зображення з певною камерою, що дозволить встановити справжність знімка, перевірити, чи походить зображення від конкретного пристрою та виявити вставлені фрагменти з інших джерел.

При аналізі гістограми слід звертати увагу на таке:

– різкі піки або провали. Можуть свідчити про нерівномірне редагування або локальну зміну яскравості.

– розриви у розподілі. Часто є індикатором вставки фрагментів з іншого зображення.

– вирівняна гістограма. Може бути наслідком загальної корекції яскравості або контрастності.

Аналіз рівнів (рис. 3), доступний у вікні "Рівні" Adobe Photoshop, дозволяє оцінити розподіл яскравості за трьома каналами (тіні, середні тони, світла). Нетипове розташування повзунків або розриви в гістограмі рівнів є прямими індикаторами корекції яскравості або вставки сторонніх ділянок.

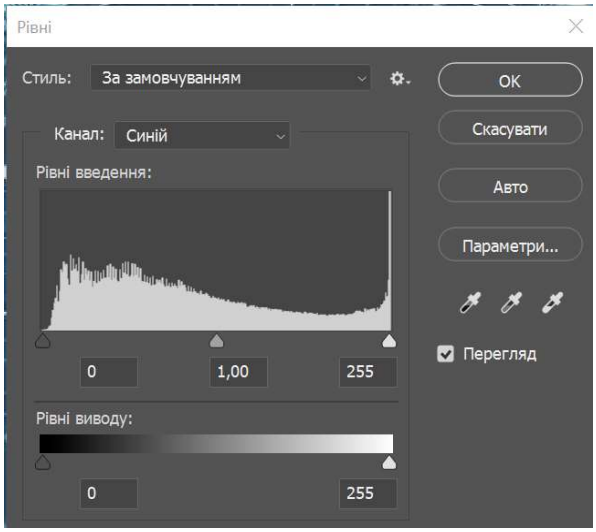

Рисунок 3 – Рівні зображення

Наприклад, у лівій частині гістограми (рис. 3) помірна щільність пікселів у темних тонах із синьою складовою, тоді як у правій – різкий пік поблизу максимальної яскравості (255), що вказує на велику кількість пікселів із високою насиченістю синього кольору. Низька інтенсивність у центральній зоні (від ~80 до ~180) та різкі перепади між зонами насичення без поступового переходу типово вказують на ручне або автоматичне коригування окремих ділянок.

Для кількісної оцінки розподілу яскравості використовується функція контрастності з урахуванням середньої яскравості пікселів:

$$C = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (I(x,y) - \mu)^2,$$

де $I(x,y)$ – яскравість пікселя, μ – середнє значення яскравості всього зображення. Високі значення C свідчать про сильні відмінності в яскравості, що може бути індикатором редагування.

Аналіз шумів та колірних каналів

Аналіз шумів – ще один ефективний метод. Збільшення масштабу зображення (100%) дозволяє детально розглянути нерівномірності у структурі шуму (рис. 4). Ділянки з різним рівнем або структурою шуму можуть свідчити про вставку або клонування фрагментів з іншого джерела. Для покращення візуалізації аномалій іноді застосовується попереднє додавання шуму до зображення (рис. 5).

Можна змінити параметри фільтра, щоб імітувати шум на різних ділянках зображення.

Рисунок 4 – Наявність нерівномірного шуму на зображенні

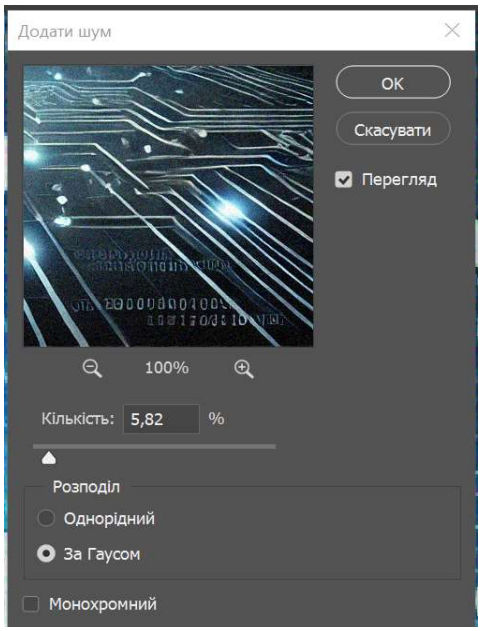

Рисунок 5 – Додавання шуму до зображення

На цьому зображенні видно ділянку, обведену червоним, де присутні нерівномірності у текстурі шуму. У виділеній зоні шум виглядає більш згущеним і менш однорідним, ніж на інших частинах зображення.

В якості додаткових прийомів в Photoshop є аналіз метаданих зображення (EXIF, IPTC) (рис. 6).

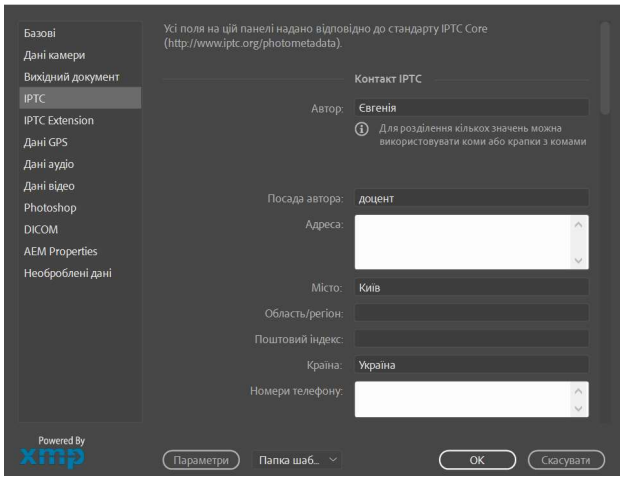

Рисунок 6 – Інформація про файл

Аналіз метаданих та частотної області

Залежно від області застосування та призначення метаданих, доводиться вносити деякі поправки та модифікації, тим самим змінюючи їх властивості та функції [7]. Метадані в даному прикладі – це прихована інформація, яка зберігається у файлі зображення та не видима без спеціальних засобів перегляду. Вони містять важливі відомості, які можуть допомогти визначити походження та історію файлу. Метадані можуть містити інформацію про камеру, дату створення, програмне забезпечення для редагування тощо.

Одним із методів виявлення ознак редагування є аналіз каналів кольору. Для цього необхідно відкрити панель «Канали» (Channels). На ній можна побачити список каналів кольору: "RGB", "Червоний" (Red), "Зелений" (Green) та "Синій" (Blue) і проаналізувати окремі канали, натиснувши на кожен канал окремо, щоб переглянути його у відтінках сірого.

Якщо в одному з каналів є різкі зміни яскравості, яких немає в інших, це може свідчити про редагування. Якщо в одному з каналів є області, які виглядають незвично або відрізняються від решти зображення, це може свідчити про вставку або клонування. Якщо рівень шуму в одному з каналів відрізняється від інших, це може свідчити про редагування (рис. 7).

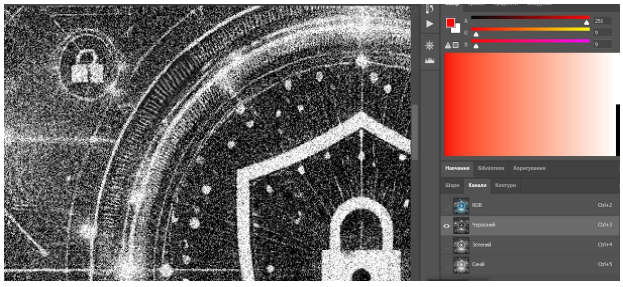

Рисунок 7 – Наявність нерівномірного шуму на зображенні в червоному каналі

Редагування зображення часто залишає артефакти в каналах кольору. Наприклад, вставка ділянки з іншого зображення може призвести до різниці в яскравості або шумі між каналами. Треба порівняти канали між собою, щоб виявити аномалії.

На зображенні у каналі, який аналізується, видно різкі переходи від світлих до темних областей, що не виглядають природними для цієї частини зображення. Деякі ділянки мають інші текстури шуму, відмінні від сусідніх зон. Помітна нерівномірність шуму – у деяких областях він виражений сильніше або слабше, що не узгоджується з природним шумом на оригінальному зображенні. Така нерівномірність часто виникає при копіюванні та вставці частин зображення, або при локальному ретушуванні.

Аналіз частотної області із застосуванням фільтра "Тиснення" теж використовується для виявлення ознак редагування. Цей фільтр відноситься до підгрупи фільтрів "Стилізація" (Stylize). Налаштувавши параметри фільтра (кут, висота, величина), можна виявити ознаки редагування (рис. 8).

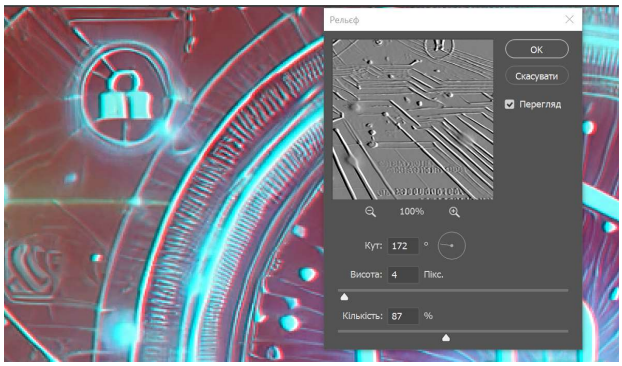

Рисунок 8 – Додавання фільтру «Тиснення»

Фільтр "Тиснення" підкреслює контрастні межі в зображенні. Редагування може залишити незвичайні візерунки або артефакти, які не відповідають природній структурі зображення. Вставка або клонування може створити різкі межі, які стають помітними після застосування фільтра. Отже, редагування в частотній області може залишити артефакти, які стають помітними після застосування фільтра "Тиснення".

Висновки

Форензичний аналіз є незамінним інструментом у розкритті кіберзлочинів, пов’язаних із поширенням фейкових матеріалів, інтернет-шахрайством та deepfake-контентом. Використання методів, що базуються на аналізі гістограм, рівнів яскравості, структури шумів, колірних каналів та метаданих, дозволяє достовірно визначити ознаки маніпуляцій (клонування, вставки фрагментів, редагування тіней/яскравості).

Отже, форензичний аналіз цифрових зображень є надійним інструментом для встановлення їхньої автентичності та виявлення ознак маніпуляцій. Його застосування в межах цифрової криміналістики значно підвищує ефективність досудового та судового розслідування кіберзлочинів.

Список літератури

1. Лазебний А. М. (2023). Сутність та значення електронних слідів у криміналістиці. *Ірпінський Юридичний Часопис*, *1* (10), 226–233.

2. Найдьон Я. (2019). Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, Господарство і Право*, *5*, 304–307.

3. Пахомов В. В. (2021). Віртуальні сліди: криміналістична характеристика. У Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства: матеріали Всеукраїнської науково-практичної конференції (до 186-річчя Ч. Ломброзо) (130–132). Київ: ДУІТ.

4. Демидова Є. Є. (2024). Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий Вісник Ужгородського Національного Університету. Серія: Право*, *85* (4), 71–75. DOI: URL: https://doi.org/10.24144/2307-3322.2024.85.4.10.

5. Кучеров Д. П., Зброжек Л. В. (2015). Сучасні програмні засоби обробки зображень. *Управління Розвитком Складних Систем*, *24*, 90–96.

6. Білоцерковський В. В., Удовенко С. Г., Чала Л. Е. (2020). Метод нейромережевого розпізнавання фальсифікованих зображень. *Біоніка Інтелекту*, *2* (95), 32–42.

7. Білощицький А. О., Миронов О. В. (2016). Аналіз властивостей та функцій метаданих наукометричних суб'єктів у web-просторі. *Управління Розвитком Складних Систем*, *25*, 139–143.

Стаття надійшла до редколегії 02.09.2025

Shabala Yevheniia
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering,
https://orcid.org/0000-0002-0428-9273
Kyiv National University of Construction and Architecture, Kyiv
Korniichuk Borys
Ph.D., associate professor, associate professor of Department of Vocation education,
https://orcid.org/0000-0003-3881-1581
Kyiv National University of Construction and Architecture, Kyiv

APPLICATION OF FORENSIC ANALYSIS TO DETERMINE THE AUTHENTICITY OF IMAGES IN CYBERCRIME INVESTIGATIONS

Abstract. *The rapid development of digital technologies and their integration into all spheres of public life have not only increased the efficiency of communication and information processing but have also led to the emergence of new threats related to the use of digital devices in illegal activities. Crimes aimed at interfering with the operation of critical infrastructure facilities, as well as cybercrimes against individuals, including Internet fraud, theft of personal data, and the dissemination of falsified materials, pose a particular danger. In this context, digital forensics is a key tool for identifying, recording, and investigating digital evidence. The article addresses the current problem of the growth of cybercrime, in particular its forms such as unauthorized interference in critical infrastructure, fraudulent activities on the Internet, and illegal use of personal data. In this regard, the importance of digital forensics as a tool for investigating offenses related to the use of digital technologies is emphasized. Particular attention is paid to the analysis of digital images that may have been altered for the purpose of falsification or deception. The article explores methods for detecting signs of digital image editing using forensic tools. A number of approaches are considered, such as metadata analysis (EXIF), which allows detecting changes in the technical parameters of the image; JPEG compression analysis to detect double compression, characteristic of edited images; as well as pixel analysis, which reveals color anomalies, inconsistencies in lighting and shadows. The application of software tools, in particular Adobe Photoshop, for detecting manipulations by analyzing histograms, brightness levels, color channels, and noise, is described. It is demonstrated how methods such as Error Level Analysis (ELA) and filters such as "Emboss" can help visualize traces of intervention in the image. Examples of editing using the Clone Stamp Tool, insertion of fragments, and detection of signs of cloning are given. It is concluded that digital traces are significant as evidence in criminal proceedings and that reliable methods for their detection, preservation, and interpretation must be applied in accordance with the standards of digital forensics.*

Keywords: forensics; digital forensics; metadata; channels; filter

References

1. Lazebnyi A. (2023). The essence and significance of electronic traces in forensics. *Irpin Law Journal*, *1* (10), 226–233.
2. Naidon Ya. (2019). Concept and classification of virtual traces of cybercrimes. *Entrepreneurship, Economy and Law*, *5*, 304–307.
3. Pakhomov V. (2021). Virtual traces: forensic characteristics. In Actual Issues and Prospects for the Development of Criminal Law, Criminology and Justice: Materials of the All-Ukrainian Scientific-Practical Conference (dedicated to the 186th anniversary of Cesare Lombroso) (130–132). Kyiv: DUIT.
4. Demydova Ye. (2024). Digital traces of a criminal offense: concept and features. *Scientific Bulletin of Uzhhorod National University. Series: Law*, *85* (4), 71–75. DOI: URL: https://doi.org/10.24144/2307-3322.2024.85.4.10.
5. Kucherov D., Zbrozhek L. (2015). Modern software tools for image processing. *Management of Development of Complex Systems*, *24*, 90–96.
6. Bilotserkovskyi V., Udovenko S., Chala L. (2020). Neural network method for detecting falsified images. *Bionics of Intelligence*, *2* (95), 32–42.
7. Biloshytskyi A., Myronov O. (2016). Analysis of properties and functions of metadata of scientometric subjects in the web-space. *Management of Development of Complex Systems*, *25*, 139–143.

Посилання на публікацію

APA Shabala, Ye., & Korniichuk, B. (2025). Application of forensic analysis to determine the authenticity of images in cybercrime investigations. *Management of Development of Complex Systems*, 63, 223–229, dx.doi.org\10.32347/2412-9933.2025.63.223-229.

ДСТУ Шабала Є. Є., Корнійчук Б. В. Застосування форензичного аналізу для визначення автентичності зображень при розслідуванні кіберзлочинів. *Управління розвитком складних систем.* Київ, 2025. № 63. С. 223 – 229, dx.doi.org\10.32347/2412-9933.2025.63.223-229.