ГРУЗІН БОГДАН МИХАЙЛОВИЧ-
курсант 4 курсу факультету №4
Харківського національного університету внутрішніх справ
Науковий керівник:
ГРИЩЕНКО ОЛЕКСАНДР ВОЛОДИМИРОВИЧ-
Професор кафедри оперативно-розшукової
діяльності та розкриття злочинів,
кандидат юридичних наук
(Харківського національного університету внутрішніх справ)
ORCID ID https://orcid.org/0000-0002-7038-1983

МЕТОДИ КРИМІНАЛЬНОГО АНАЛІЗУ ЦИФРОВИХ ФОТОГРАФІЙ

Цифрові фотографії стали невід'ємною частиною сучасного життя, і вони використовуються в різних сферах, включаючи сферу кримінального правосуддя. Злочинці також використовують цифрові фотографії для своїх цілей, і вони залишають сліди у цифровому середовищі. Розвиток та широке поширення комп'ютерних інструментів для обробки і монтажу цифрових фотографій, а також доступність великої кількості інформації щодо проведення таких операцій в сучасний період призвели до того, що навіть особа без спеціалізованого навчання може легко створювати фальшиві фотографії. Саме тому покращення методів експертної оцінки автентичності цифрових зображень визнається як дуже важливе завдання в галузі науки і техніки. Розглянемо основні способи виявлення слідів втручання до фотозображення:

Аналіз рівня помилок (Error Level Analysis) - це метод, який використовується для визначення аутентичності зображень, які були стиснуті з втратами, таких як файли у форматі JPEG. Під час стиснення зображень артефакти стиснення зазвичай залишаються однорідними на всьому зображенні. Проте, якщо виявляються значно відмінні артефакти стиснення для окремих частин зображення, це може свідчити про те, що ці частини були додані до зображення після стиснення. Іншими словами, наявність неподібних артефактів

стиснення на зображенні може свідчити про редагування зображення, наприклад, у графічному редакторі[1].

Аналіз шуму (Noise Analysis) представляє собою алгоритм зворотного шумозаглушення. Замість прибирання шуму, він видаляє іншу частину зображення. Цей метод може бути корисним для виявлення маніпуляцій з зображеннями, таким як аерографія, деформація і клонування з урахуванням перспективи. Він найкраще працює на високоякісних зображеннях[1].

Аналіз формату зображення (метадані) включає в себе вивчення змін, які можуть виникнути під час перетворення формату зображення та використання алгоритмів стиснення, які призводять до втрати певної частини інформації. У графічних файлах із зображеннями зазвичай містяться метадані, які можна аналізувати для визначення характеристик зображення та отримання корисної інформації. Наприклад, в цифровій фотографії можуть бути вбудовані метадані, які розкривають інформацію про модель камери, що зафіксувала знімок, дату та час фотографування та інше. Для видобування цих метаданих з файлу зображення можна використовувати різноманітні графічні редактори, що часто постачаються разом із цифровими фотоапаратами та сканерами, а також спеціалізовані програми для вилучення метаданих.

Проведемо практичний аналіз за допомогою онлайн сервісу Forensically-це набір безкоштовних інструментів для проведення ретельного аналізу цифрових зображень. Він включає в себе можливість виявлення клонів, аналіз рівня помилок, видобування метаданих та інші корисні функції[2]. "За основу для аналізу було взято власну цифрову фотографію (рис. 1.1), до якої були застосовані певні корекції за допомогою графічного редактора Adobe Photoshop(рис. 1.2). Ці корекції можуть призвести до дискредитації власника фотографії або ввести в оману інших осіб.

Рисунок 1.1- оригінал зображення.

Рисунок 1.2 – відредактоване зображення.

Проведений аналіз помилок зображення дозволяє виявити явні ознаки змін у зображенні(виділено червоним кольором)(рис. 1.3).

Рисунок 1.3 - Аналіз рівня помилок.

Аналізуючи метадані та внутрішню структуру зображення, можна відзначити наявність значення "Adobe," що свідчить про втручання графічного редактора Adobe Photoshop (рис. 1.4).

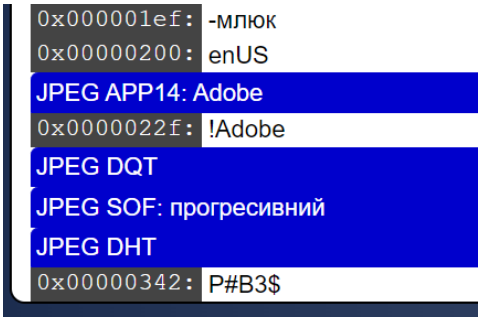

Рисунок 1.4 – Параметри внутрішньої структури зображення.

На сьогоднішній день, немає універсальної рекомендованої методики, яка б забезпечила надійну можливість визначити факт монтажу на цифрових фотозображеннях у випадку, коли оригінал зображення відсутній. Завдяки новим

умовам в інформаційній та технологічній галузях, експерти повинні навчатися використовувати нові інструменти для вирішення завдань ідентифікації та діагностики в умовах відсутності оригіналу зображення. Також їм необхідно розробляти науково-методичне забезпечення у вигляді методичних посібників для підтримки їхньої роботи.[3]

Список використаних джерел:

1. Глибинна перевірка фотографій: як сервіси Forensics і Forensically допомагають фактчекерам [Електронний ресурс] / Надія Баловсяк // Stopfake.org – Режим доступу до ресурсу: https://www.stopfake.org/uk/glibinna-perevirka-fotografij-yak-servisi-forensics-i-forensically-dopomagayut-faktchekeram/. (дата звернення: 24.10.2023)
2. Forensically [Електронний ресурс] – Режим доступу до ресурсу: https://29a.ch/photo-forensics/#forensic-magnifier.https://univd.edu.ua/general/publishing/konf/21_11_2018/pdf/42.pdf (дата звернення: 24.10.2023)
3. Кожевніков О. А. Актуальні питання досудового розслідування та тенденції розвитку криміналістичної методики. [Електронний ресурс] / Олексій Андрійович Кожевніков // Дослідження цифрових фотозображень з метою виявлення ознак фотомонтажу.. – 2018. – Режим доступу до ресурсу: https://univd.edu.ua/general/publishing/konf/21_11_2018/pdf/42.pdf.

(дата звернення: 24.10.2023)

Грищенко О,В, Грузин Б.М, Методи кримінального аналізу цифрових фотографій / Застосування інформаційних технологій у правоохоронній діяльності: зб. Матеріалів круглого столу. (м. Харків, 14 грудня 2023р.) / МВС України, ф-т № 6, кафедра протидії кіберзлочинності та дата-технологій. Харків : ХНУВС, 2023. 173,с. 85-89.