3 СУДОВА ЕКСПЕРТИЗА (НАУКОВІ РОЗРОБКИ, МЕТОДИ, МЕТОДИКИ, ТЕХНОЛОГІЇ)

УДК 343.98:004.932
https://doi.org/10.33994/kndise.2026.71.12

Ананьїн Олег Валерійович

кандидат технічних наук, старший науковий співробітник, заступник начальника відділу науково-методичного та організаційно-управлінського забезпечення (судовий експерт) Головного експертно-криміналістичного центру Державної прикордонної служби України
https://orcid.org/0000-0001-8757-1663
ananin@i.ua

Бригинець Олександр Миколайович

начальник відділу інформаційно-аналітичного забезпечення (судовий експерт) Головного експертно-криміналістичного центру Державної прикордонної служби України
https://orcid.org/0009-0001-6366-4467
brygynets.a@gmail.com

Бібліографічний опис статті: Ананьїн О.В., Бригинець О.М. (2026). Маніпуляції з цифровими фотозображеннями як виклик системі захисту документів у контексті біометричної ідентифікації та верифікації особи. *Криміналістика і судова експертиза, 71,* 172–184. doi: https://doi.org/10.33994/kndise.2026.71.12

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

МАНІПУЛЯЦІЇ З ЦИФРОВИМИ ФОТОЗОБРАЖЕННЯМИ ЯК ВИКЛИК СИСТЕМІ ЗАХИСТУ ДОКУМЕНТІВ У КОНТЕКСТІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА ВЕРИФІКАЦІЇ ОСОБИ

Розглянуто проблему виявлення фальсифікацій з цифровими фотозображеннями осіб, як виклик сучасній системі захисту документів у контексті біометричної ідентифікації та верифікації особи. Наведено комплекс доцільних заходів щодо її вирішення. В умовах запровадження в розвинених країнах автоматизованих систем біометричної верифікації та ідентифікації, маніпуляції з цифровими фотозображеннями осіб (морфінг) є відносно новим викликом, особливо для автоматизованих систем прикордонного контролю, в яких для ідентифікації особи використовуються цифрові та надруковані фотозображення обличчя пред'явника документа. Сучасні апаратно-програмні засоби, які здійснюють ідентифікацію особи на основі фотозображення обличчя, із значною вірогідністю розпізнають зображення облич, згенерованих шляхом маніпуляцій з цифровими фотозображеннями, як аутентичні. Разом з цим, коли в сучасних розвинених країнах відбувається активне запровадження в діяльність правоохоронних органів та міграційних служб високотехнологічних рішень, вже правомірно стверджувати про незворотну світову тенденцію щодо поступового планомірного відходу від безпосередньої фізичної участі співробітників правоохоронних органів у процесі перевірки документів на користь автоматизованих систем. Тому, проблема виявлення у документах змінених фотозображень пред'явника потребує комплексних рішень, які охоплюють організаційну, правоохоронну, технічну та етичну площини. Щодо судової експертизи, то сучасні виклики в епоху загальної цифровізації, які постають перед судово-експертними установами, вимагають модернізації існуючих та розробки нових методик ідентифікації особи за ознаками зовнішності за матеріальними зображеннями з урахуванням методів біометричної ідентифікації та диференційованого впровадження в судово-експертну діяльність технологій штучного інтелекту, що мінімізувало б вірогідність експертних помилок.

Ключові слова: цифрові фотозображення; маніпуляції; біометрія; комп'ютерні технології; підробка документів; виклики.

Ananyin Oleg

candidate of technical sciences, senior researcher,
Deputy head of the scientific-methodical and organizational-management support department (forensic expert)
The main expert forensic center State Border Guard of Ukraine
https://orcid.org/0000-0001-8757-1663
ananin@i.ua

Bryhynets Oleksandr

head of the department of information and analytical support (forensic expert) of the Main Expert and Forensic Center State Border Service of Ukraine
https://orcid.org/0009-0001-6366-4467
brygynets.a@gmail.com

MANIPULATION OF DIGITAL PHOTOGRAPHS AS A CHALLENGE FOR DOCUMENT PROTECTION SYSTEMS IN THE CONTEXT OF BIOMETRIC IDENTIFICATION AND PERSONAL VERIFICATION

To cite this article: Ananyin, O., Bryhynets, O. (2026). Manipuliuvannia tsyfrovymy fotohrafiiamy yak vyklyk dlia system zakhystu dokumentiv u konteksti biometrychnoi identyfikatsii ta veryfikatsii osoby [Manipulation of digital photographs as a challenge for document protection systems in the context of biometric identification and personal verification]. *Criminalistics and Forensics, 71,* 172–184. doi: https://doi.org/10.33994/kndise.2026.71.12

The problem of detecting falsifications involving digital facial images is examined as a challenge to modern document security systems in the context of biometric identification and verification. A set of relevant measures aimed at dealing with this issue is proposed. In the context of the widespread implementation of automated biometric identification and verification systems in developed countries, manipulation of digital facial images (morphing) represents a relatively new challenge, particularly for automated border control systems, where both digital and printed facial images of the document holder are used for identification. Modern face-recognition systems with a high degree of probability recognize facial images generated through digital manipulation as authentic. At the same time, as developed countries actively implement high-tech solutions into the activities of law enforcement and migration services, it is correct to claim about the global trend toward the gradual replacement of direct human involvement in document verification process with automated systems. Therefore, the problem of detecting altered facial images in identity documents requires comprehensive solutions encompassing organizational, law enforcement, technical and ethical spheres. In the field of forensic science, modern challenges arising in the era of widespread digitalization require the modernization of existing methods and the development of new approaches in facial recognition derived from physical images. These approaches should take into account biometric identification methods and the implementation of artificial intelligence technologies in forensic examination to minimize the probability of expert mistakes.

Key words: digital facial images; manipulation; biometrics; computer technologies; document forgery; challenges.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

Постановка проблеми

Сучасний розвиток комп'ютерних технологій призвів до появи нових можливостей у сфері обробки цифрових зображень, зокрема з використанням у графічних редакторах різних ефектів трансформації. На державному рівні, у контексті забезпечення безпеки, пов'язаної з біометричною ідентифікацією та верифікацією особи, можливість маніпуляції з цифровими зображеннями значно підвищує ризик фальсифікації фотозображень пред'явника в документах, що посвідчують особу, шляхом використання різних графічних редакторів, що не потребує високотехнологічних засобів, спеціальних знань та значних фінансових коштів. Тому, пошук нових та модернізація існуючих підходів, методів і технічних рішень проблеми виявлення змінених цифрових фотозображень стає актуальним науковим завданням.

Аналіз останніх досліджень і публікацій

Означена тема дослідження привертає значну увагу сучасних вчених та експертів. Так, Г. Андрощук вказує на високу небезпеку застосування правопорушниками ефектів трансформації (морфінгу), зокрема в паспортних документах [1, с. 60]. У такому ж контексті О. Скакаліна та Д. Гаврилко наголошують на важливості застосування у криміналістиці технічної перевірки зображень, де візуальна достовірність є критичною. [2, с. 535].

У контексті представленого дослідження під маніпуляціями з цифровими фотозображеннями розглядається трансформуючий ефект морфінгу як реальний інструмент фальсифікації документів, що посвідчують особу. У науково-методичній літературі під морфінгом визначено візуальний ефект, який досягається із застосуванням спеціального програмного забезпечення. Він дозволяє створити композитне, трансформоване (morphing) цифрове зображення обличчя особи шляхом цифрового поєднання елементів обличчя різних людей за допомогою засобів комп'ютерної графіки. З технічної точки зору принцип морфінгу полягає у здійсненні перетворення однієї геометричної форми в іншу шляхом знаходження проміжних значень величини за наявним дискретним набором відомих значень таким чином, щоб підкреслити найвиразніші подібності між ними та одночасно приховати їхні відмінності [3].

Мета дослідження

Мета статті – визначення доцільних заходів для вирішення проблеми виявлення згенерованих фальсифікацій цифрових фотозображень в документах, у контексті біометричної ідентифікації та верифікації особи.

Для досягнення мети дослідження та об'єктивності наукових ре-

зультатів використано комплекс *загальнонаукових* та *спеціальних* методів. *Хронологічний* метод застосовано для вивчення специфіки розвитку системної взаємодії правоохоронних органів держав Європейського Союзу та держав-партнерів України з вирішення проблеми біометричної ідентифікації та верифікації особи щодо виявлення фальсифікацій, згенерованих шляхом маніпуляцій з цифровими фотозображеннями в документах. Методами *аналізу* і *синтезу* визначено комплекс доцільних заходів щодо вирішення проблеми виявлення у документах фотозображень пред'явника, змінених на основі ефекту морфінгу. Методом *узагальнення* сформульовано висновки дослідження.

Виклад основного матеріалу

Біометрична ідентифікація та верифікація осіб успішно використовується в діяльності правоохоронних органів України та прикордонних і міграційних інституцій всіх розвинених країн світу. Перевірка та підтвердження особи за допомогою біометричної ідентифікації, особливо під час перетинання державного кордону, вже стійко асоціюється з національною безпекою. Але, фахівці у сфері ідентифікації вже стверджують, що в умовах сучасного технічного прогресу, не можна сто відсотково опиратися на надійність автоматичної біометричної ідентифікації. Зокрема, трансформовані (морфінг) за допомогою комп'ютерних графічних редакторів фотозображення, що належать двом і більше особам, можуть забезпечити успішну верифікацію будь-якої з них. Тому елементи захисту паспортних документів за стандартами ICAO, де використовується біометрія (фотозображення особи), вже є уразливими на нинішньому технічному рівні, який досягнуто криміналітетом [4, с. 172].

В експертній спільноті Європейського Союзу серйозну увагу на проблему виявлення фальсифікацій, згенерованих з використанням ефекту морфінгу, звернули у 2009 році. У той час в міжнародному стандарті в сфері біометрики ISO/IEC 19792:2009 «Information technology – Security techniques – Security evaluation of biometrics» такі фальсифікації офіційно класифікували як вразливість для автоматизованих систем біометричного контролю, які використовуються правоохоронними органами.

У 2018 році у Франції на міжнародній конференції «Обробка зображень та сигналів» («Image and Signal Processing») експерти із Німеччини та Данії представили програмне забезпечення з виявлення морфованих зображень обличчя методом обчислення відмінностей між геометричними точками справжнього фотозображення умовного правопорушника та геометричними точками обличчя на наданому на контроль сфальсифікованого (морфованого) фотозображення. Експериментальні дані продемонстрували, що запропонований програмний алгоритм з виявлення морфінгу виконує завдання з помилкою на рівні 32,7 % [5]. Представлене про-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

грамне забезпечення стало одним із значних результатів на шляху пошуку технічних рішень зазначеної проблеми, яким з'ясовано, що відсоток помилки апаратно-програмних засобів з виявлення морфованих зображень залишається достатньо високим. Тому в 2019 році запущено європейську ініціативу SOTAMD з метою проведення подальших технічних тестувань програмного забезпечення з виявлення ознак морфінгу у цифрових фотозображеннях осіб, які використовуються в документах [6]. У рамках одного із дослідницьких проєктів експертами Європейського Союзу під час тестування автоматизованої системи біометричного контролю «Vision Box», де використовувався алгоритм розпізнавання обличь «Nec», на предмет виявлення морфінгу в наданому на перевірку фотозображенні особи, отримано результат збігу 61%. Одночасно те ж саме морфоване фотозображення надали для вивчення групі правоохоронців і всі вони виказали серйозні сумніви щодо його справжності [7]. Як висновок, доводиться констатувати, що сучасні апаратно-програмні засоби виявляють змінені, за допомогою морфінгу, фотозображення осіб з достатньо високою вірогідністю, але поки-що не здатні стовідсотково замінити людські знання та досвід.

У 2020 році Європейською Комісією з метою подальших наукових досліджень у сфері створення програмного забезпечення для виявлення алгоритмів трансформації цифрових фотозображень на основі ефекту морфінгу започатковано дослідницький проєкт iMARS [8]. На важливість такого рішення вказав подальший процес, коли в державах Європейського Союзу та їх партнерів у контексті протидії організованій злочинності (тероризм, нелегальна міграція, торгівля людьми, контрабанда тощо), де широко використовуються підроблені, чужі, недійсні (фейкові) документи, правоохоронними органами реалізуються високотехнологічні проєкти, спрямовані на діджиталізацію контрольних процедур на зовнішніх європейських кордонах. Зокрема, наприкінці 2024 року Європейська Комісія ухвалила пропозиції щодо впровадження та використання цифрового посвідчення особи для подорожей (Digital Travel Credential) [9]. По суті таке посвідчення пропонується в якості альтернативи фізичному паспорту. Концепція Digital Travel Credential стосується всіх держав-членів Європейського Союзу та третіх країн чиї паспортні документи використовують технології захисту від підробок, що базується на існуючих на сьогодні стандартах ICAO Doc 9303. Мета такої ініціативи полягає в тому, щоб зрештою досягти рівня безпеки документів еквівалентних паспорту з електронним носієм інформації на якому зафіксовано біометричні дані пред'явника (зокрема, фотозображення обличчя) і зробити можливим взаємодію з існуючими електронними системами перевірки. В свою чергу ICAO рекомендує повний перехід до системи автоматизованого прикордонного контролю (Automated Border Control, ABC), яка замість фізичної перевірки (інспектором) поєднує автентифікацію документів, біометричне зіставлення та перевірку через бази даних у режимі реаль-

ного часу щоб підтвердити особу за лічені секунди. Основою цього переходу є концепція Seamless Travel (подорож без перешкод), де головним ідентифікатором виступають біометричні дані пасажира. Остаточні терміни повного переходу залежатимуть від конкретного регіону, оскільки ICAO встановлює глобальні стандарти, а конкретні дедлайни впровадження систем автоматизованого прикордонного контролю (Automated Border Control, ABC) визначають окремі держави. Наприклад, країни Європейського Союзу планують протягом 2026 року поетапно запровадити так звану систему в'їзду/виїзду Європейського Союзу (Entry/Exit System, EES). Її основою буде саме автоматизована система прикордонного контролю (Automated Border Control, ABC). Крім того в Європейському Союзі до кінця 2026 року запланований запуск Європейської системи інформації та авторизації подорожей (European Travel Information and Authorisation System, ETIAS) [10], яка вимагатиме від подорожуючих осіб попередньої онлайн-реєстрації для безвізових подорожей. Одночасно на світовому рівні, ICAO до 2030 року в межах виконання Програми ідентифікації подорожуючих (Traveller Identification Programme, TRIP) орієнтується на масове впровадження так званої цифрової ідентичності (Digital Identity). Очікується, що до цього часу більшість країн Європейського Союзу та держав-партнерів перейдуть на використання цифрового посвідчення особи для подорожей (Digital Travel Credentials), що дозволить подорожуючим особам проходити перевірку на кордоні без фізичного паспорта. Ключові із таких цифрових ініціатив Європейський Союз планує реалізувати до 2030 року, забезпечивши громадянам можливість використання електронних документів [9].

Таким чином, правомірно стверджувати про незворотну світову тенденцію щодо поступового планомірного відходу у правоохоронних органах від безпосередньої фізичної участі співробітників у процесі перевірки документів на користь систем автоматизованого контролю. Крім того, варто відзначити, що в результаті проведених досліджень експерти Європейського Союзу нарівні з організаційно-правовими та технічними аспектами зазначеної проблеми стали виокремлювати ще етичну складову. Один з таких експертів як професор Крістоф Буш із Норвезького університету науки і технологій (NTNU, м. Тронгейм), зазначив про те, що програмні засоби біометричної ідентифікації особи не мають бути упередженими щодо певних демографічних груп з різноманітними расовими ознаками зовнішності [11].

У 2025 році у звіті «Biometric vulnerabilities Ensuring future law enforcement preparedness, 2025» («Розкриття вразливостей біометричних систем: посилення стійкості правоохоронних органів», 2025), підготовленому Лабораторією інновацій Європолу (EIL, Люксембург) представлено результати аналізу вразливості автоматизованих систем біометричного контролю, коли правопорушники можуть надавати на контроль документи, де використані змінені

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

за допомогою морфінгу фотозображення пред'явника [12, с. 8–9]. Як висновок, одним із способів мінімізації ризиків використання в документах морфованих фотозображень осіб запропоновано впровадження так званої «живої реєстрації» (live enrolment), тобто фотографування та цифровізація фото обличчя особи в реальному часі у процесі подання заявки на оформлення документів (паспортів) з контролем надання особистих даних [12, с. 56].

Із вищезазначеного виходить, що виклик сучасній системі захисту документів в контексті біометричної ідентифікації та верифікації особи складається із таких аспектів:

- на сьогодні процес генерування фальсифікацій з використанням ефекту морфінгу не потребує високотехнологічного устаткування, спеціальних знань та складного програмного забезпечення;
- сучасні апаратно-програмні засоби, які здійснюють ідентифікацію особи на основі біометричних даних (в тому числі фотозображення обличчя), із значним показником вірогідності розпізнають зображення облич, згенерованих з використанням ефекту морфінгу, як аутентичні.

Тому, проблема виявлення у документах змінених на основі ефекту морфінгу фотозображень пред'явника потребує комплексних рішень, які охоплюють правоохоронну, технічну та етичну площину. Звідси комплексом заходів доцільно вважати:

- розробку та впровадження нового і модернізація існуючого програмного забезпечення для розпізнавання облич, здатного виявляти навіть незначні ознаки використання морфінгу;
- запровадження та використання високотехнологічного аналізу кіберзагроз у відомчих інформаційних системах та активна протидія їм, зокрема виявлення фішингових атак, які містять в собі морфінг як «послугу»;
- проведення тренінгів з представниками міністерств та відомств, органів виконавчої влади, правоохоронних органів тощо з метою підвищення обізнаності у сфері цифрової безпеки та захисту електронних документів.

Щодо місця судової експертизи у вирішенні заявленої проблеми, то в сучасних умовах загальної цифровізації суспільства державні спеціалізовані установи також мають оперативно реагувати на виклики та відповідно адаптувати свою роботу. В державах Європейського Союзу через широке запровадження автоматизованих систем фото та відеофіксації, цифрові зображення облич все частіше стають об'єктами судових експертиз та використовуються в якості доказів в суді. Але європейські фахівці піднімають питання щодо відсутності методик та стандартизації, особливо з використання автоматизованих систем, які порівнюють зображення та генерують оцінку відповідності [13;14]. Дослідницька група вчених з Національного інституту стандартів і технологій (США), разом із залученою міжнародною групою судових експертів з ідентифікації, провела експеримент на точність розпізнавання зображень облич

на базі алгоритму нейронної мережі типу DCNN. Головним питанням експерименту було встановити, хто досягне найбільшої точності в ідентифікації наданих зображень – людина-експерт чи алгоритм нейронної мережі. В результаті експерти та алгоритми штучного інтелекту DCNN продемонстрували практично однаковий збіг в точності ідентифікації наданих на експеримент фотозображень [15]. Таким чином було доведено високу ефективність та перспективні можливості застосування штучного інтелекту в ідентифікаційних дослідженнях зображень облич.

Разом з цим варто відзначити про те, що в Європейському Союзі запроваджуються суворі регуляторні межі для контролю щодо досліджень на базі штучного інтелекту, що безпосередньо впливає на вимоги до верифікації у судових лабораторіях. За рахунок широких навчальних вибірок автоматизовані системи розпізнавання облич значно підвищили точність їх пошуку та зіставлення. Наприклад, Європейська мережа судово-експертних установ (ENFSI) відзначає, що завдяки використанню штучного інтелекту значно підвищено якість експертиз, що в свою чергу стимулює використання автоматизованих систем розпізнавання облич на базі штучного інтелекту та алгоритмів машинного навчання у правоохоронній сфері в Європі [16]. Як бачимо із сучасних європейських практик судова експертиза зображень облич вже зазнає змін [17]. Тому необхідно наголосити на тому, що в процесі пошуку нових та модернізації існуючих методів вирішення заявленої проблеми відповідну роль мають відігравати і спеціалізовані установи, які здійснюють судово-експертну діяльність в Україні. Зокрема щодо науково-методичного (розробка експертних методик, які дозволяли б достовірно встановлювати ознаки маніпуляцій з цифровими фотозображеннями) та нормативно-правового забезпечення (участь у розробці рекомендацій та стандартів щодо вимог до якості цифрових фотозображень, а також правового регулювання використання біометрії для автоматизованих систем біометричної ідентифікації та верифікації). Як справедливо відзначають сучасні експерти в Україні, використання новітніх технологій дає змогу підвищити якість експертизи цифрових фотозображень, однак ці технології потребують адаптації до специфічних вимог судової експертизи, де критерії достовірності та відтворення результатів є критично важливими, а розуміння цих технологій експертом є необхідною умовою використання цих інструментів у своїх дослідженнях [18, с. 275–276].

Висновки

Отже, в умовах запровадження в правоохоронну діяльність автоматизованих систем біометричної ідентифікації та верифікації, маніпуляції з цифровими фотозображеннями осіб (морфінг) в документах є відносно новим викликом, особливо для автоматизованих систем прикордонного контролю. Сучасні апаратно-програмні засоби,

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

які здійснюють ідентифікацію особи на основі біометричних даних (фотозображення обличчя), із значною вірогідністю розпізнають згенеровані фотозображення шляхом маніпуляцій, як аутентичні. Тому, проблема виявлення у документах змінених фотозображень пред'явника потребує комплексних рішень, які охоплюють правоохоронну, технічну та етичну площини. Щодо судової експертизи, то сучасні виклики епохи загальної цифровізації, які постають перед судово-експертними установами України, вимагають модернізації існуючих та розробки нових експертних методик з урахуванням методів біометричної ідентифікації та диференційованого впровадження технологій штучного інтелекту в судово-експертну діяльність, що мінімізувало б вірогідність експертних помилок.

Перспективою подальших досліджень доцільно вважати розробки у сферах науково-методичного забезпечення судової експертизи та правового регулювання використання біометрії з урахуванням вимог для автоматизованих систем біометричної ідентифікації та верифікації осіб.

Список використаних джерел:

1. Андрощук Г. О. Штучний інтелект і інтелектуальна власність: проблеми регулювання: науково-практичне видання. Науково-дослідний інститут Національної академії правових наук України. Київ: Інтерсервіс, 2023. 204 с.

2. Гаврилко Д.Д., Скакаліна О.В. Методи виявлення маніпуляцій у цифрових зображеннях: технічна перевірка як інструмент протидії дезінформації: зб-ка мат-ів 77-ї наук. конф. професорів, викладачів, наукових працівників, аспірантів та студентів університету. Національний університет «Полтавська політехніка ім. Юрія Кондратюка» (Полтава, 16 – 22 трав. 2025 р.). С. 534–536.

3. Handbook of Computational Geometry / edited by J.-R. Sack, J. Urrutia. North Holland, 2000. P. 121–153. URL: https://www.sciencedirect.com/book/edited-volume/9780444825377/handbook-of-computational-geometry (дата звернення: 01.02.2026).

4. Філіппов С. Окремі аспекти використання даних про пасажирів (API/PNR) в інтересах прикордонної безпеки. *Правова держава*. 2021. № 43. С. 169–176. DOI: https://doi.org/10.18524/2411–2054.2021.43.240997 (дата звернення: 29.01.2026).

5. U. Scherhag, D. Budhrani, M. Gomez-Barrero, C. Busch. Detecting Morphed Face Images Using Facial Landmarks. *Proceedings of International Conference on Image and Signal Processing* (Cherbourg, FR, July 2-4, 2018). P. 444–452. URL: https://orbit.dtu.dk/en/publications/detecting-morphed-face-images-using-facial-landmarks/ (дата звернення: 29.01.2026).

6. SOTAMD. State of the art of Morphing Detection. URL: https://www.utwente.nl/en/eemcs/dmb/research/research-archive/sotamd/ (дата звернення: 02.01.2026).

7. C. Busch, S. Caillebotte, U. Seidel, F. Knopjes, D. Maltoni, M. Ferrara, R. Veldhuis, L. Spreeuwers, K. Raja, R. Raghavendra, M. Gomez-Barrero, C.

Rathgeb. Face Morphing Attacks: What needs to be done. *Proceedings International Conference on Biometrics for Borders* (Frontex, Warsaw, October 9-10, 2019). P. 96–108. URL: https://www.christoph-busch.de/files/Busch-iMARS-Frontex-2019.pdf (дата звернення: 02.01.2026).

8. iMARS: official website. URL: https://imars-project.eu/concept-objectives/ (дата звернення: 03.02.2026).

9. Commission proposes an EU Digital Travel application. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047 (дата звернення: 03.02.2026).

10. Інформація щодо Європейської системи інформації та авторизації подорожей (ETIAS). Представництво Європейського Союзу в Україні: офіційний вебсайт. URL: https://www.eeas.europa.eu/delegations/ukraine (дата звернення: 03.02.2026).

11. Busch, C. Challenges for Automated Face Recognition Systems. Nature Reviews Electrical Engineering. 2024. URL: https://www.christoph-busch.de/files/Busch-NatureReview-ChallengesFRS-2024.pdf (дата звернення: 04.02.2026).

12. Biometric vulnerabilities Ensuring future law enforcement preparedness. An Observatory Report from the Europol Innovation Lab. Luxembourg: Publications Office of the European Union, 2025. 60 p. PDF. ISBN 978-92-95236-94-3. ISSN 2600-5182. DOI: https://doi.org/10.2813/8081090 (дата звернення: 04.02.2026).

13. Jacquet M., Champod C. Automated face recognition in forensic science: Review and perspectives. *Forensic Science International*. 2020. Vol. 307. P. 110–124. DOI: https://doi.org/10.1016/j.forsciint.2019.110124

14. O'Toole A.J. Castillo C. D. Face Recognition by Humans and Machines: Three Fundamental Advances from Deep Learning. *Annual review of vision science*. 2021. Vol. 7. P. 543–570. DOI: https://doi.org/10.1146/annurev-vision-093019-111701

15. Phillips P.J., Yates A.N., Hu Y., Hahn C.A., Noyes E., Jackson K., Cavazos J.G., Jeckeln G., Ranjan R., Sankaranarayanan S., Chen J.-C., Castillo C.D., Chellappa R., White D. and O'Toole A.J. Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Algorithms. *Proceedings of the National Academy of Sciences*. 2018. P. 6171–6176. DOI: https://doi.org/10.1073/pnas.1721355115

16. Guideline for Facial Recognition System End Users / European Network of Forensic Science Institutes. Version 1.0. [S. l.]. 2022. 36 p. URL: https://enfsi.eu/wp-content/uploads/2022/07/GUIDELINES-FOR-FR-USERS-V_01_public-review-1-1.pdf (дата звернення: 04.02.2026).

17. ENFSI Best Practice Manual for Facial Image Comparison (BPM-DI-01) / European Network of Forensic Science Institutes. 01.01.2018. 50 p. URL: https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf (дата звернення: 05.02.2026).

18. Переїденко А. Застосування автоматизованих систем для верифікації результатів дослідження зображень обличь. *Актуальні питання судової експертології, криміналістики та кримінального процесу:* мат-ли VII міжнар. наук.-практ. конф. (Київ, 10 груд. 2025 р.) / за заг. ред. М. Є. Кисельова. Київ: Вид. Ліра-К, 2025. С. 273 – 276.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

References

1. Androshchuk H.O. (2023). Shtuchnyi intelekt i intelektualna vlasnist: problemy rehuliuvannia: naukovo-praktychne vydannia [Artificial intelligence and intellectual property: regulatory issues: scientific and practical publication]. Naukovo-doslidnyi instytut intelektualnoi vlasnosti Natsionalnoi akademii pravovykh nauk Ukrainy. Kyiv: Interservice. 204 p. [in Ukrainian].

2. Havrylko D.D., Skakalina O.V. (2025). Metody vyiavlennia manipuliatsii u tsyfrovykh zobrazhenniakh: tekhnichna veryfikatsiia yak instrument protydii dezinformatsii [Methods for detecting manipulation in digital images: technical verification as a tool for countering disinformation]. Zbirnyk materialiv 77-i naukovoi konferentsii profesoriv, vykladachiv, naukovykh pratsivnykiv, aspirantiv ta mahistrantiv universytetu, Natsionalnyi universytet "Poltavska politekhnika imeni Yuriia Kondratiuka", Poltava, May 16–22, 2025, 534–536 [in Ukrainian].

3. Handbook of Computational Geometry / edited by J.-R. Sack, J. Urrutia. North Holland, 2000. P. 121–153. URL: https://www.sciencedirect.com/book/edited-volume/9780444825377/handbook-of-computational-geometry (accessed: 01.02.2026) [in English].

4. Filippov S. (2021). Okremi aspekty vykorystannia pasazhyrskykh danykh (API/PNR) v interesakh prykordonnoi bezpeky [Selected aspects of the use of passenger data (API/PNR) in the interests of border security]. *Rule of Law*, 43, 169–176. DOI: https://doi.org/10.18524/2411-2054.2021.43.240997 [in Ukrainian].

5. Scherhag U., Budhrani D., Gomez-Barrero M., Busch C. (2018). Detecting morphed face images using facial landmarks. Proceedings of the International Conference on Image and Signal Processing, Cherbourg, France, July 2–4, 2018, 444–452. URL: https://orbit.dtu.dk/en/publications/detecting-morphed-face-images-using-facial-landmarks/ (accessed: 29.01.2026) [in English].

6. SOTAMD. (n.d.). State of the art of Morphing Detection. URL: https://www.utwente.nl/en/eemcs/dmb/research/research-archive/sotamd/ (accessed: 02.01.2026) [in English].

7. Busch C., Caillebotte S., Seidel U., Knopjes F., Maltoni D., Ferrara M., Veldhuis R., Spreeuwers L., Raja K., Raghavendra R., Gomez-Barrero M., Rathgeb C. (2019). Face morphing attacks: what needs to be done. Proceedings of the International Conference on Biometrics for Borders, Frontex, Warsaw, October 9–10, 2019, 96–108. URL: https://www.christoph-busch.de/files/Busch-iMARS-Frontex-2019.pdf (accessed: 02.01.2026) [in English].

8. iMARS: official website. (n.d.). URL: https://imars-project.eu/concept-objectives/ (accessed: 03.02.2026) [in English].

9. Commission proposes an EU Digital Travel application. European Commission. (2024). URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047 (accessed: 03.02.2026) [in English].

10. Informatsiia shchodo Yevropeiskoi systemy informatsii ta avtoryzatsii podorozhei (ETIAS) [Information on the European Travel Information and Authorisation System (ETIAS)]. Predstavnytstvo Yevropeiskoho Soiuzu v Ukraini: ofitsiinyi vebsait. URL: https://www.eeas.

europa.eu/delegations/ukraine (accessed: 03.02.2026) [in Ukrainian].

11. Busch C. (2024). Challenges for automated face recognition systems. *Nature Reviews Electrical Engineering*. URL: https://www.christoph-busch.de/files/Busch-NatureReview-ChallengesFRS-2024.pdf (accessed: 04.02.2026) [in English].

12. Europol Innovation Lab. (2025). Biometric vulnerabilities: ensuring future law enforcement preparedness. An Observatory Report from the Europol Innovation Lab. Luxembourg: Publications Office of the European Union. 60 p. DOI: https://doi.org/10.2813/8081090 [in English].

13. Jacquet M., Champod C. (2020). Automated face recognition in forensic science: review and perspectives. *Forensic Science International*, 307, 110–124. DOI: https://doi.org/10.1016/j.forsciint.2019.110124 [in English].

14. O'Toole A.J., Castillo C.D. (2021). Face recognition by humans and machines: three fundamental advances from deep learning. *Annual Review of Vision Science*, 7, 543–570. DOI: https://doi.org/10.1146/annurev-vision-093019-111701[in English].

15. Phillips P.J., Yates A.N., Hu Y., Hahn C.A., Noyes E., Jackson K., Cavazos J.G., Jeckeln G., Ranjan R., Sankaranarayanan S., Chen J.-C., Castillo C.D., Chellappa R., White D., O'Toole A.J. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and algorithms. *Proceedings of the National Academy of Sciences*, 115(24), 6171–6176. DOI: https://doi.org/10.1073/pnas.1721355115 [in English].

16. European Network of Forensic Science Institutes. (2022). Guideline for Facial Recognition System End Users. Version 1.0. 36 p. URL: https://enfsi.eu/wp-content/uploads/2022/07/GUIDELINES-FOR-FR-USERS-V_01_public-review-1-1.pdf (accessed: 04.02.2026) [in English].

17. European Network of Forensic Science Institutes. (2018). ENFSI Best Practice Manual for Facial Image Comparison (BPM-DI-01). 50 p. URL: https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf (accessed: 05.02.2026) [in English].

18. Pereidenko A. (2025). Vykorystannia avtomatyzovanykh system dlia perevirky rezultativ analizu zobrazhen oblychchia [The use of automated systems for verifying the results of facial image analysis]. Aktualni pytannia sudovoi ekspertyzy, kryminolohii ta kryminalnoho protsesu: materialy VII Mizhnarodnoi naukovo-praktychnoi konferentsii, Kyiv, December 10, 2025 / za red. M.Ye. Kiselova. Kyiv: Lira-K, 273–276 [in Ukrainian].

Надійшла до редакції / Received: 23.03.2026
Отримана після доопрацювання / Received after revision: 30.03.2026
Прийнято до друку / Accepted for publication: 03.04.2026
Опубліковано / Published: 29.05.2026

Фінансування: відсутнє / Funding: none.
Конфлікт інтересів: автор(и) заявляє(ють) про відсутність конфлікту інтересів / Conflict of interest: the author(s) declare no conflict of interest.
Дотримання етичних норм: дослідження виконано з дотриманням принципів академічної доброчесності / Ethical compliance: the study was conducted in accordance with the principles of academic integrity.
Дані дослідження: усі дані, необхідні для обґрунтування висновків, наведено у статті / Research data: all data necessary to substantiate the conclusions are presented in the article.