Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

А. М. Гребенюк
С. О. Прокопов
Л. В. Рибальченко

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ НА ВІДЕО- ТА ФОТОЗОБРАЖЕННЯХ

Методичні рекомендації

Дніпро
2023

УДК 004.93
Г 79

Рекомендовано до друку науково-методичною радою Дніпропетровського державного університету внутрішніх справ, протокол № 2 від 17.10.2023

РЕЦЕНЗЕНТИ:

Дмитро Прокопович-Ткаченко – т. в. о. завідувача кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, кандидат технічних наук, доцент;

Дмитро Данченко – начальник 7 відділу управління протидії кіберзлочинам в Дніпропетровській області Департаменту кіберполіції Національної поліції України.

Гребенюк А. М., Прокопов С. О., Рибальченко Л. В.

Г 79 Використання технологій розпізнавання обличчя на відео- та фотозображеннях : метод. рекоменд. / А. М. Гребенюк, С. О. Прокопов, Л .В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 48 с.

ISBN 978-617-8035-86-0

У методичних рекомендаціях висвітлено проблеми, що постали перед працівниками Національної поліції під час війни щодо ідентифікації воєнних злочинців російської армії, колаборантів тощо. Розглянуто методи та способи розпізнавання осіб за обличчями, що використовуються як алгоритми для пошуку та ідентифікації в спеціалізованих системах. Виконано аналіз та тестування сучасних пошукових систем для ідентифікації осіб за фотозображеннями у відкритих джерелах мережі «Інтернет». Визначено найкращі пошукові оболонки для пошуку за обличчям.

Призначено для використання практичними працівниками Національної поліції, науково-педагогічними працівниками та здобувачами вищої освіти навчальних закладів Національної поліції.

АВТОРИ:

кандидат технічних наук, доцент **Андрій Гребенюк** – завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ;

Сергій Прокопов – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ;

кандидат економічних наук, доцент **Людмила Рибальченко** – доцент кафедри економічної та інформаційної безпеки ННІППФНП Дніпропетровського державного університету внутрішніх справ.

ISBN 978-617-8035-86-0

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

Комп'ютерний зір (англ. CV, computer vision) – технологія, яка спрямована на створення комп'ютерних засобів для проведення, виявлення, спостереження та класифікацію об'єктів.

ABIS – автоматизована системи біометричної ідентифікації.

Facial recognition – розпізнавання обличчя.

Application program interface (API) – широко використовуються Face ID.

Facebook DeepFace – сервіс, який призначений для роботи користувачів у соціальній мережі «Фейсбук».

Apple Face ID – система, яка призначена для авторизації власника телефону.

Microsoft Face API – сервіс, який призначений для побудови систем розпізнавання і містить функції для пошуку, ідентифікації, групування, знаходження подібних облич, а також визначення віку, статі, емоційного стану за допомогою обличчя.

Aware NexaFace – система, яка призначена для ідентифікації і автентифікації особи і працює у складі біометричної системи та використовується в ній як один із засобів підтвердження особи.

Samsung Face Recognition – система, яка розроблена інженерами Samsung для використання засобу підтвердження особи.

ПЕРЕДМОВА

Проблема ідентифікації осіб, які скоїли як кримінальні, так і адміністративні правопорушення, є однією з важливих складових правоохоронної діяльності. Правоохоронці Національної поліції та прокуратури з початком війни почали стикатися з розслідуванням нетипових раніше видів злочинів. Окрім фіксації наслідків злочинних військових дій росіян, пов'язаних з руйнуваннями будівель і завдання шкоди життю та здоров'ю цивільного населення України, постає питання ідентифікації конкретних осіб, які віддавали злочинні накази, та які їх виконували. Велику кількість військових злочинів було здійснено під час окупації щодо цивільних осіб, яких катували, страчували за будь-яку, навіть надуману, нелояльність до окупантів. До цих злочинів причетні як російські військові, так і українські колаборанти, їх також необхідно ідентифікувати в межах кожного кримінального провадження. Велика кількість колаборантів на тимчасово окупованій території України, які пішли на співпрацю з окупаційною адміністрацією, також підпадають під дію Кримінального кодексу України. На жаль, на території України залишились так звані шанувальники «русского мира», які ведуть активну антиукраїнську діяльність у соціальних мережах, а деякі, завербовані фсб росії, займаються підривною діяльністю на території України, збираючи інформацію, проводячи теракти та наводячи російські ракети або дрони на об'єкти цивільної інфраструктури та військові цілі. Подібні диверсанти намагаються проникнути на територію нашої держави не тільки незаконним шляхом через лінію фронту, але і цілком законно через кордони України. Тому необхідно перевіряти не тільки по правоохоронних базах України та Інтерполу, але й по інших інформаційних системах, які дозволяють отримати інформацію за фотозображенням особи.

Під час досудового розслідування правоохоронці можуть отримати фото- або відеоматеріали, на яких відображені особи, що підозрюються. Перевірка цих фотозображень з відомчими правоохоронними базами даних може допомогти тільки стосовно громадян України, які порушували закон раніше, але відсоток таких, що

скоїли раніше військові злочинів, дуже малий. У цьому разі доводиться використовувати пошук інформації з відкритих джерел для ідентифікації осіб, які підозрюються у скоєнні злочинів, та зображення яких отримали працівники досудового розслідування. Але не завжди наявні методи OSINT-технологій можуть привести до позитивних результатів з ідентифікації фігурантів. Тому в цьому дослідженні спробуємо проаналізувати механізми та методи ідентифікації осіб за обличчями, розглянути наявні програмно-інформаційні системи, які дозволяють знайти інформацію про підозрюваного за фотозображенням та ідентифікувати його особу. Вважаємо, що це дослідження буде корисним для практичних працівників Національної поліції, науково-педагогічного складу, курсантів та слухачів навчальних закладів системи МВС.

Розділ 1. ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

1.1. Особливості технології розпізнавання обличчя

Актуальним питанням сьогодення є розпізнавання обличчя особистості за фото- та відеозображенням. Цікавим є сам процес здійснення такого відеоспостереження.

Сучасні камери для ефективного відеоспостереження можуть забезпечувати якісне зображення в будь-який час доби і мають широкий кут огляду з відповідними ключовими параметрами.

Відеоспостереження спрямовано на здійснення ідентифікації особи обличчя людини для створення інформаційних баз даних спостереження.

Існує і певна різниця між самим поняттям виявлення та розпізнавання обличчя людини.

Під час виявлення обличчя відбувається збір фото- та відеозаписів, які було отримано з камер відеоспостереження. Обробка зібраного фото та спостереження відбувається із застосуванням спеціального програмного забезпечення. Процес виявлення особи є основою для проведення подальшого аналізу отриманої інформації.

Під час розпізнавання відбувається процес аналітики для зіставлення характерних особливостей особи. На фото- та відеоспостереженні вказано дату та час проведеної зйомки, що допомагає у відборі даних при подальшому їх використанні.

Цей проміжок часу, на якому особа, яка цікавить, була зафіксована, є визначальним для обробки та її ідентифікації.

Є два основні методи, які використовуються встановленими системами відеоспостереження для розпізнавання, а саме: розпізнавання обличчя в потоці статичних зображень та розпізнавання в динамічному потоці.

Ці два методи використовуються камерами відеоспостереження Dahua для ідентифікації особи.

Потокова інформація з обох видів передається на внутрішній сервер, де фото- та відеозаписи проходять декодування. Після цього ці зображення проходять класифікацію розробленою спеціальною програмою, поповнюють і формують базу даних. Процес класифікації обличчя особи відбувається за відповідними категоріями, як-от: стать, вікові параметри, особливі прикмети обличчя, одяг тощо.

У сучасних умовах використання систем відеоспостереження застосовують спеціальні алгоритми, які розпізнають об’єкти спостереження, ідентифікують їх, зіставляють та порівнюють із базами даних і знаходять ті ознаки, які є притаманними лише особі, яку необхідно знайти.

Розглядаючи статистичну базу даних систем відеоспостереження, необхідно зауважити, що отримані матеріали про результати аналізу окремих ідентифікованих людей зберігаються як зображення та докладна інформація, отримана в результаті аналізу об’єктів, що потрапляють в зону контролю. У той час, коли на камеру потрапляє людина, яку необхідно знайти і дані якої є в базі даних, її зображення розміщується поряд із новим. Це дає змогу програмі зіставити отримані зображення, ідентифікувати особу за наявними ознаками та виділити ті, особливі ознаки, які є притаманними лише цій особі. Встановлені наглядові пристрої спостереження використовують в офісах, освітніх установах, банківських установах, державних та приватних підприємствах, приватних будинках та багатоповерхівках, торгівельних комплексах, вулицях міста з інтенсивним рухом та місцях масового перебування людей. Отримані дані з таких камер спостереження потрапляють до відповідних програм, де відбувається ідентифікація об’єкта відеоспостереження.

У динамічній базі даних відбувається ідентифікація з отриманих джерел спостереження саме про тих осіб, яких немає в існуючій базі даних, тобто про нових осіб. Ця система проводить порівняння та постійне ведення відеоспостереження з існуючими даними бази інформації. Дані, що було отримано, проходять класифікацію та додаються в основну базу. Якщо спостерігається збіг даних, відбувається подання сигналу для оператора, який контролює такий відбір. Отже, інформація в динамічних базах даних постійно поповнюється новими даними, що є зручним для використання в подальшому дослідженні [1].

Системи відеоспостереження, де є електронне виявлення та розпізнавання обличчя, дають змогу скоротити час для перегляду таких матеріалів, що дозволяє персоналу отримувати швидко та якісно інформацію про ті об’єкти, які виникли і можуть становити інтерес про об’єкт пошуку чи зловмисника. Ця система розпізнавання дозволяє аналізувати зображення, а також зроблені відеозаписи, видавати інформацію оператору для якісного та швидкого ухвалення рішення.

1.2. Сфери застосування систем відеоспостереження

Системи відеоспостереження з можливістю ідентифікації особи на основі аналізу зображення її обличчя та інших біометричних показників широко використовуються у сфері громадської безпеки. Криміналісти можуть використовувати автоматизовані системи біометричної ідентифікації (ABIS) для порівняння різних типів біометрії [1]. Цей ринок очолюють системи, призначені для боротьби зі злочинністю та тероризмом. Переваги систем розпізнавання обличчя для поліції очевидні і полягають у забезпеченні ефективності виявлення та запобігання злочинам. Розпізнавання обличчя використовується під час видачі документів, що посвідчують особу, і, найчастіше, у поєднанні з іншими біометричними технологіями, такими як відбитки пальців (запобігання шахрайству з особистими документами та крадіжці особистих даних).

Отримане зображення обличчя через систему відеоспостереження можна використовувати у прикордонних перевірках для порівняння об’єкта з отриманим обличчям власника при оцифруванні його біометричного паспорта. Таке спостереження розроблено для поліпшення процесу переходу від розпізнавання відбитків пальців до розпізнавання обличчя та застосовується під час перевірок митниками на кордоні.

Застосування систем відеоспостереження під час перетину кордону є значно ефективним засобом ідентифікації особи (рис. 1.1).

Рис. 1.1. Ідентифікація осіб під час перетину державного кордону

Ще одним із засобів застосування камер розпізнавання обличчя є безпілотники, які ефективно використовують під час масових заходів, що відбуваються на великій площі. Системи безпілотних літальних апаратів можуть ідентифікувати об'єкт відеоспостереження на висоті до 100 метрів.

Ефективність виконання відеоспостереження з розпізнаванням обличчя необхідна для забезпечення заходів громадської безпеки великих міст, особливо під час воєнного стану в державі.

Прикладами застосування таких систем відеоспостереження, які містять функцію розпізнавання обличчя, є сфера забезпечення національної безпеки, серед яких:

– пошук зниклих чи викрадених дітей та дорослих;

– знаходження дітей та дорослих, яких незаконно викрали та експлуатують;

– виявлення осіб, які скоїли злочини;

– надання необхідної інформації про скоєні злочини для найшвидшого їх розкриття та розслідування.

Рис. 1.2. Камери зовнішнього відеоспостереження

Застосування системи відеоспостереження, яка розпізнає та ідентифікує обличчя, суттєво прискорює зусилля поліцейських та операторів під час пошуку зниклих через завантаження їх фото у відповідну систему. У цей час поліцейські використовують можливість розпізнавання обличчя для ведення відеоаналітики під час використання пошуку зниклих, встановлення їх можливого місця перебування, час ідентифікації особи і перебування в інших місцях та інше.

Система відеоспостереження проводить аналіз існуючих в базі даних фото на рівні 70 %–90 % збігу отриманих варіантів за лічені

хвилини.

Розпізнавання особи відбувається не лише за фото її обличчя, але й за очима, навіть якщо в особи вони заплющені, за одягом та її манерами поведінки.

Із використанням сучасних засобів відеоспостереження для поліпшення безпекової системи в країні, правоохоронці мають змогу знаходження не лише зниклих людей, а й викривати злочинців, які вчинили крадіжки в магазинах, офісах на вулиці тощо, рис. 1.2.

1.3. Технологія комп’ютерного зору

Поняття комп’ютерного зору (англ. CV, computer vision) – це технологія, яка спрямована на створення комп’ютерних засобів для проведення, виявлення, спостереження та класифікацію об'єктів.

Застосування технології штучного інтелекту є перспективним напрямом наукового дослідження, аналізу, прогнозування, розпізнавання та виявлення осіб, яких необхідно знайти.

Одна з найпопулярніших проблем комп’ютерного зору, яка зараз активно досліджується – розпізнавання обличчя.

Світовими лідерами у розробці технологічних систем розпізнавання обличчя особи за фото- та відеоспостереженнями є технологія Face ID на Apple Special Event, яка впроваджена у соціальних мережах для розпізнавання людей на фото [1]. Однією з компаній є Фейсбук, яка стала лідером у застосування такої технології. Компанією Фейсбук було розроблено алгоритм, який показав ефективність розпізнавання у 93 % випадках.

Для розпізнавання обличчя було створено бібліотеки та Application program interface (API), які широко використовуються Face ID.

Проблема комп’ютерного зору та розпізнавання облич із застосуванням бібліотек OpenCV та dlib освітлена в роботах [2, 3]. У такій роботі оцінюються напрацьовані її як переваги, так і недоліки, які використовують ці бібліотеки у проєктах побудови систем розпізнавання.

1.4. Технології розпізнавання обличчя

Розпізнавання обличчя проводиться із застосуванням таких сервісів, як:

- ✓ Facebook DeepFace;
- ✓ Apple Face ID;
- ✓ Microsoft Face API;
- ✓ Aware Nexa|Face;
- ✓ Samsung Face Recognition.

Сервіс **Facebook DeepFace** призначений для роботи користувачів у соціальній мережі «Фейсбук», де опубліковано фотографії користувачів, на яких є люди, застосовує процес пошуку за обличчям та іменем вказаного користувача [4]. У публікаціях фотографій система DeepFace виявить людину, яка схожа на ту, що підлягає пошуку та нагадає чи позначить її у цій системі.

Особливістю такої системи розпізнавання обличчя є її ефективність, яка становить 97,25 % (із вибірки людей 97,53 %), що є і її перевагою. До переваг також можна віднести її велику кількість даних для пошуку і розпізнавання обличчя.

Недоліками є велика потреба в апаратних ресурсах та адаптованість системи розпізнавання лише під соціальну мережу «Фейсбук».

Система **Apple Face ID** призначена для авторизації власника телефону [6]. Результатом досліджень є розробка додаткової апаратної складової для системи розпізнавання, яка дає змогу відсіювати ті фото, що можуть містити дані недостовірної інформації в системі розпізнавання за допомогою 2D муляжів та дають змогу розпізнавати обличчя в разі неякісного освітлення, оскільки апаратне забезпечення має можливість зчитувати мітки на обличчі і порівнювати з достовірними даними фото [7].

На початку роботи системи необхідно побудувати макет обличчя, використовуючи обертання телефону із ввімкненою камерою навколо обличчя.

Особливістю є застосування унікального апаратного забезпечення, яке розроблено для захисту і поліпшення ефективності розпізнавання обличчя. Перевагами є висока ефективність розпізнавання, розроблене додаткове апаратне забезпечення, розпізнавання в разі поганого освітлення та захист системи від недостовірної інформації.

До недоліків належить потреба апаратного забезпечення, яке є особливим для такої системи, та закрита технологія лише для застосування продукції Apple.

Сервіс **Microsoft Face API** призначений для побудови систем розпізнавання і містить функції для пошуку, ідентифікації, групування, знаходження подібних облич, а також визначення віку, статі, емоційного стану за допомогою обличчя [8]. Такий спосіб організації системи дозволяє надати доступ стороннім розробникам для розробки своїх додатків на основі цього API, що відбувається із застосуванням сервера Microsoft. Особливістю застосування такої системи є побудова системи розпізнавання обличчя з відповідною базою даних і створений у вигляді API.

Перевагами такої системи є висока її ефективність розпізнавання, залучення великої кількості засобів та методів, а також те, що операції пошуку відбуваються із застосуванням серверів Microsoft.

До недоліків належить відсутність можливості додаткових налаштувань та залежність розробки від стороннього API.

Система Aware Nexa|Face призначена для ідентифікації і автентифікації особи і працює у складі біометричної системи та використовується в ній як один із засобів підтвердження особи [9]. Окрім Nexa|Face, наявні такі системи: розпізнавання відбитків пальців Nexa|Fingerprint, сітківки ока Nexa|Iris, голосу Nexa|Voice, тексту Inquire, також можливим є підключення додаткових модулів, розроблених третіми особами.

Ці модулі використовують в комплексі, оскільки саме це гарантує надійність системи та її захист. Є мобільна та вебверсія, а для розгортання системи необхідна клієнт-серверна архітектура.

Особливістю є використання комплексної біометричної системи з можливістю впровадження сторонніх модулів, а також кросплатформність цієї розробки.

Перевагами є висока ефективність розпізнавання, підключення додаткових систем розпізнавання, висока надійність і захищеність системи, кросплатформність.

До недоліків належать її комплексність та висока вартість.

Система **Samsung Face Recognition** розроблена інженерами Samsung для флагманської моделі S серії і використовується як засіб підтвердження особи [10]. Фронтальна камера призначена для розпізнавання, що не потребує додаткового апаратного забезпечення, як в Apple Face ID. Було створено додаткову спеціальну захищену папку (Secure Folder) і систему Knox, які призначені для захисту важливих даних та їх інкапсуляції на рівні системи. На основі системи розпізнавання обличчя створена система розпізнавання зіниці ока.

Особливістю є розробка системи розпізнавання зіниці ока.

До переваг належить висока ефективність розпізнавання, наявність

розпізнавання за допомогою зіниці, додатковий шар захисту за допомогою Knox системи і захищеної папки.

До недоліків належить можливість недостовірного розпізнавання, проблема з розпізнаванням в разі поганого освітлення та технологія, яка використовується для продукції Samsung.

1.5. Сфери використання CV

Використання CV-технологій є майже безмежним, комп'ютерний зір застосовуватися майже в усіх аспектах суспільного життя. Основними прикладами застосування систем комп'ютерного зору є:

Виробництво. Комп'ютерний зір застосовується у великому і малому виробництві. Основною сферою застосування є промислові роботизовані системи для автоматизації і контролю якості виробництва, рис. 1.3 [11-12].

Рис. 1.3. Камери відеоспостереження на виробництві

Транспорт. Побудова системи автономного керування автомобілем без участі людини впроваджена компанією Tesla для безпечного і автономного її керування (рис. 1.4).

Рис. 1.4. Відеоспостереження в транспорті

Шопінг. Запровадження розумними та автономними супермаркетами без касирів є новітніми технологіями компанії Amazon із застосуванням автономних сервісів доставки товарів. Важливим застосуванням є підвищення економічної ефективності у сфері торгівлі та підвищення якості і зменшенні ціни через повну автоматизацію послуг з доставки товарів окремому її замовнику (рис. 1.5).

Рис.1.5. Відеоспостереження в торгівельних центрах

Медицина. В цій сфері застосовуються системи для аналізу медичних зображень і автоматизації оцінки результатів досліджень та надання базових приписів і рекомендацій щодо лікування на основі аналізу наявних зображень різних досліджень (рис. 1.6).

Рис. 1.6. Відеоспостереження в закладах охорони здоров’я

Системи взаємодії. Основною сферою застосування для розуміння жестів людини, її емоцій та іншої візуальної інформації є пристрої аналізу, розпізнавання та ведення інформації в системах взаємодії. Одним з прикладів є відеоспостереження в банках (рис. 1.7).

Рис. 1.7. Відеоспостереження в банківських установах

Системи організації інформації. Засоби роботи із зображеннями, наприклад системи для індексації баз даних зображень, відслідковування і автоматизація доступу до будь-яких об’єктів [5].

Безпека. Наведені вище системи FaceID та NexaFace є приклади систем безпеки, які побудовано з використанням новітніх технологій комп'ютерного зору для розпізнавання обличчя. Основна сфера застосування і використання технології відеоспостереження є значно широкою і застосовується у багатьох сферах життєдіяльності людини.

Особливе значення у застосуванні цих технологій для підвищення рівня безпеки держави належить підрозділам Національної поліції України. Під час військового стану в Україні ці технології мають особливе значення для застосування пошуку людини, знаходження зловмисників та порушників правопорядку, для викриття крадіїв та розкриття різних злочинів, а також для розкриття військових злочинів (рис. 1.8.).

Рис. 1.8. Відеоспостереження в підрозділах Національної поліції

Розділ 2. МЕТОДИ РОЗПІЗНАВАННЯ ОСІБ

2.1. Методи автоматичного розпізнавання осіб

Ідентифікація та розпізнавання осіб – є одним із перших практичних завдань, яке спрямоване на становлення і розвиток теорії розпізнавання та ідентифікації об'єктів. Є дев'ять категорій об'єктів, які відповідають гностичним ділянкам і викликають зорові образи.

Інтерес до процедур, які лежать в основі процесу впізнавання і розпізнавання осіб, завжди є актуальним, особливо із зростаючими практичними потребами в застосуванні охоронних систем, верифікації, проведенні криміналістичної експертизи, телеконференції тощо. Незважаючи на те що людина добре ідентифікує обличчя людей, іншим є питання використання інформаційних технологій для проведення такої роботи під час збереження цифрового зображення осіб. Ще менш зрозумілими є оцінки схожості осіб, включно з їх комплексною обробкою. Можна виділити кілька напрямів досліджень проблеми розпізнавання осіб:

- ✓ нейрофізіологічні моделі;
- ✓ інформаційно-процесуальні моделі;
- ✓ комп'ютерні моделі розпізнавання;
- ✓ нейропсихологічні моделі.

Питання розпізнавання осіб розглядалося ще на етапі відстеження комп'ютерного зору. Компанії протягом тривалого часу розробляли автоматизовані системи розпізнавання людського обличчя: ImageWare (system FaceID); Imagis, Epic Solutions, Spillman, Miros (system Trueface); Vissage Technology (system Vissage Gallery); Visionics (system FaceIt), Smith & Wesson (ASID – Automated Suspect Identification System) [4].

Технології розпізнавання осіб дозволяють виробляти автоматичний пошук і розпізнавання осіб в графічних файлах і відеопотоці.

2.2. Система розпізнавання осіб в Face recognition

Система розпізнавання осіб дає змогу робити такі і прості, і складні речі:

- ✓ підтвердження і визначення особистості студента під час написання іспитів онлайн;
- ✓ розпізнавання людей в громадських місцях, які містяться в «чорному списку»;
- ✓ оплата різних товарів;
- ✓ в сучасних парках збереження вашого місця в черзі в разі відвідування будь-яких атракціонів;
- ✓ розблокування телефону.

Системи розпізнавання осіб мають особливе значення для застосування в правоохоронній сфері, оскільки вони використовують їх для пошуку та ідентифікації злочинців. Урядові організації також використовують такі системи для застосування безпеки і зменшення рівня шахрайства на виборах (рис. 2.1.).

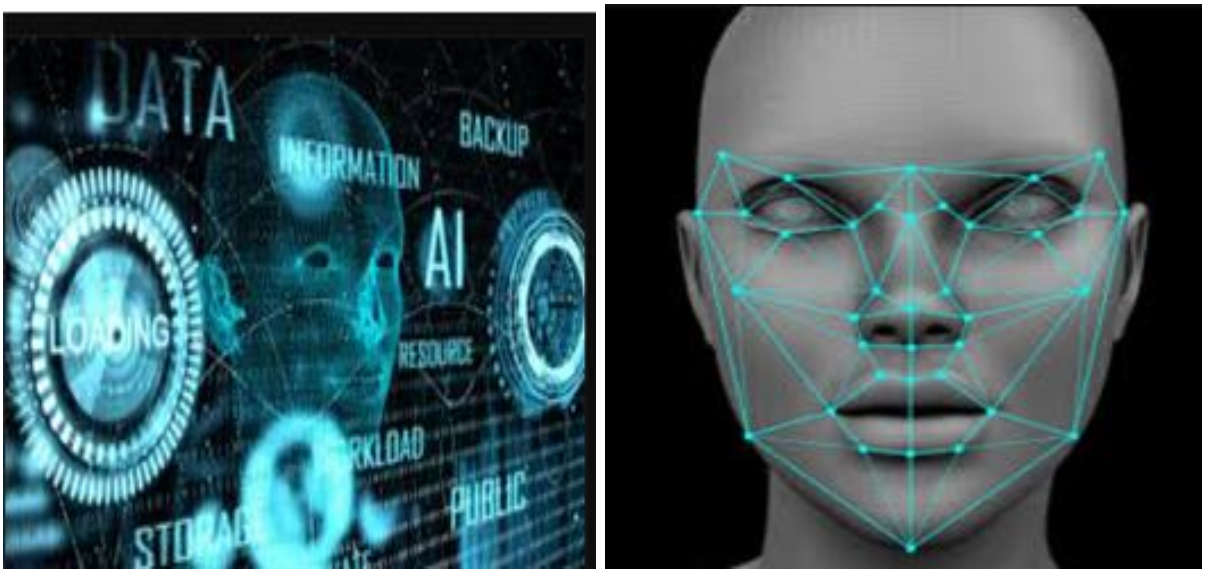

Рис. 2.1. Технологія розпізнавання обличчя

Але бувають ситуації, де використання відповідного програмного забезпечення є не лише популярним, а й необхідним. Поширення систем відеоспостереження стає дешевшим, а його використання має тенденцію до зростання. Такі системи використовуються в банках та аеропортах, туристичних агентствах та медичних установах, на митницях та

торгівельних комплексах, на підприємствах і в держустановах. Під час проходження на посадку в аеропортах, відбувається розпізнавання осіб, що дає змогу зіставити особи з внутрішньою базою даних.

Під час роботи з банківськими терміналами також відбувається застосування відеоспостереження для перевірки особи клієнта банку (рис. 2.2). Знімок особи робиться під час роботи з банкоматом чи терміналом. Встановлене програмне забезпечення також створює відбиток особи, що захищає клієнта від крадіжки особистих даних і шахрайських транзакцій.

Рис. 2.2. Відеоспостереження для перевірки особи клієнта банку під час роботи з банківськими терміналами та розрахунками картою

Ідентифікація людини здійснюється і в громадських місцях із застосуванням 3D-зображення, де формується тривимірна модель об’єкта, з якою починає працювати система для визначення контрольних точок і порівняння з наявною базою даних.

2.3. Метод Face recognition – математичне обґрунтування

Для розпізнавання і класифікації осіб відеокамерою використовується алгоритм розпізнавання обличчя по отриманій фотографії, щоб знайти необхідну особу за виділеними її основними компонентами: очі, ніс, губи, лоб та інше (метод каскада Хаара). На цьому етапі використовуються створені шаблони.

У разі відповідності шаблонів конкретним ділянкам на зображенні, і що такі зображення належать обличчю людині, їх відмічають і розміщують в окрему папку.

Іншим є метод Віоли-Джонса (так само відомий як каскади Хаара). Якщо на фотографії не одне велике обличчя, а багато дрібних, то такі шаблони до всього зображення застосувати не можна, оскільки вони будуть менше основних шаблонів. Для відновлення пошуку за всіма фото особи з різними розмірами, використовується метод ковзного вікна. У середині цього вікна відбувається порівнювання даних зображень. Вікно має тенденцію до ковзання по всьому зображенню і після кожного проходження зображення для знаходження особи більшого масштабу, вікно збільшується.

У подальшому робота належить класифікатору, який визначає зіставлення цієї особи в момент захоплення її камерою. Усі необхідні дані для побудови моделі формуються із застосуванням каскаду Хаара. Ці ознаки обробляються за допомогою алгоритму градієнтного бустінгу. Метод найшвидшого бустінгу буде класифікувати людей, а Каскади Хаара шукатимуть на фотографіях обличчя [7].

Як базовий алгоритм для розпізнавання обличчя використовуються «Вирішальні дерева». Вирішальне дерево – бінарне дерево, яке у вузлах містить прості предикати, а в листі прогнози.

Кожне вирішальне дерево будується «автоматично». На кожній ітерації алгоритм вибирає такий предикат, який максимально добре розділяє класи. Якщо ніс однієї людини сильно відрізняється від носа іншої людини, то вибереться така характеристика, яка є найбільш схожою з оригіналом. Далі алгоритм буде шукати інші явні залежності.

Послідовність класифікації та відбору одного із способів об’єднання дерев в композиції належить методу найшвидшого бустінгу, що спрямований на побудову композиції. Побудова моделі вибору відбувається так, що спочатку будується перша модель, обчислюється її помилка, потім відбувається побудова другої моделі так, щоб вона виправляла помилки попереднього алгоритму. Як наслідок, отримується висока якість класифікації, де кожна нова модель у композиції виправляє помилку попередньої.

2.4. Використання засобів розпізнавання обличчя підрозділами Національної поліції

Науковці багатьох країн світу стверджують, що технології біометричної ідентифікації обличчя до 2030 року на світовому ринку можуть становити приблизно $20,63 млрд при річному зростанні 17,2 % з 2020 року. Зазначимо, що в Україні станом на 2023 рік такі технології вже використовуються для ідентифікації військових злочинців.

До найпопулярніших систем розпізнавання обличчя, які використовуються під час війни з рф, є Amazon Recognition, Hanwang, Blue Wolf та Clearview AI (рис. 2.3).

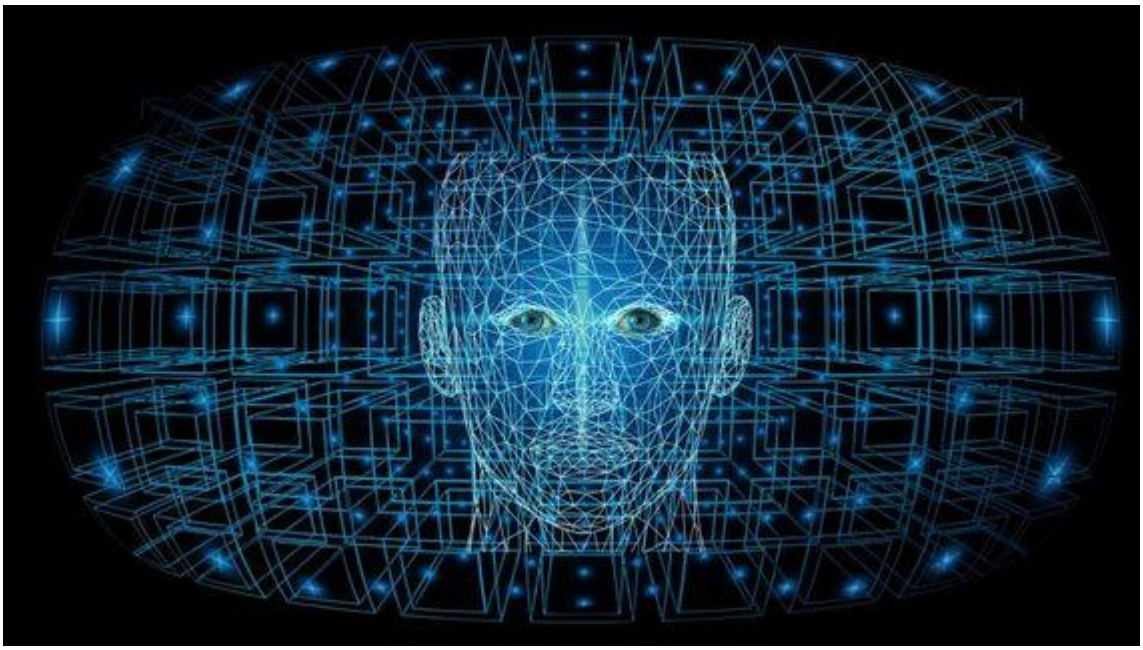

Рис. 2.3. Технологія розпізнавання обличчя

Amazon Recognition. Американська компанія Amazon з 2016 року використовує свою власну розробку розпізнавання обличчя, аналізуючи отримані зображення та відео. Розроблений алгоритм Amazon модерує контент, виконує пошук та порівнює обличчя, знаходить логотипи брендів, розпізнає фото знаменитостей, за обробку кожного зображення встановлюються відповідні ціни.

Такою новітнею розробкою компанії Amazon користуються урядові установи США, державні установи, поліція деяких штатів, приватні компанії, а також використовують її імміграційна та митна служби.

Hanwang. Китайська компанія Hanwang у 2020 році перша в країні впровадила технологію розпізнавання осіб, яка може ідентифікувати людину в медичній масці. Для цього було викоано аналіз зображень 6 млн осіб без масок, а менша її частка в масках, які містилися в одній базі даних. Така розробка була впроваджена у двох варіантах: перший для контролю на входах у будівлі, другий варіант працює з декількома камерами одночасно. За другим варіантом для ідентифікації 30 людей може бути використана лише одна секунда. У разі наявності маски на обличчі точність розпізнавання зображення може становити приблизно 95 %, а без маски – 99,5 %.

Blue Wolf. Військові Ізраїлю для розпізнавання обличчя палестинців використовують систему Blue Wolf ще з 2016 року. Ця технологія спочатку робить фото палестинців, зберігає їх у великій базі даних, а потім порівнює зображення з людиною у своїй базі даних. Наступним кроком є процес затримання чи ні певної людини: при натисканні на смартфоні солдата на фото, вони блимають певним кольором, який вказує заарештувати, затримати чи не чіпати цю людину.

Clearview AI. Найбільш відомою та найбільш суперечливою у світі системою для розпізнавання обличчя є система Clearview Al, яка містить у своїй базі 10 млрд фото. Clearview Al використовують правоохоронні органи Америки, які використовували технологію розпізнавання обличчя та випробували її на 3200 американських державних установах (рис. 2.4).

З березня 2022 року цю систему використовують в Міністерстві оборони України для ідентифікації загиблих та для виявлення ворогів на блокпостах.

Рис. 2.4. Розпізнавання обличчя за фото

Міністерство цифрової трансформації України вживає усіх необхідних заходів із компанією-розробником програми розпізнавання обличчя для розвитку таких новітніх інновацій в нашій країні. Clearview AI допомагає Україні впізнавати військових злочинців, але виникає велика кількість непорозумінь щодо цього.

Використання Збройними Силами України та правозахисниками програмного забезпечення Clearview AI в умовах війни є виправданим, хоча і має ризики порушення прав людини.

На думку правозахисників, ризики застосування системи Clearview AI полягають у тому, що точність розпізнавання обличчя не гарантує 100 % результат.

Фахівці Міністерства цифрової трансформації України разом із виконавчим директором компанії Clearview AI Хоаном Тон-Тхатом домовилися про будівництво цифрової інфраструктури в Україні з використанням новітніх технологій, зокрема штучного інтелекту. Цікавим є можливість відкриття офісу компанії Clearview AI в Україні. Такі новітні технології дадуть змогу вітчизняним талановитим фахівцям в ІТ сфері та штучного інтелекту розробити новітні проєкти цифровізації України.

2.5. Використання МВС технологій для розпізнавання обличчя під час іспитів на водійські права

Міністерство внутрішніх справ України у 2023 році замовило послуги по розробці програмного забезпечення, яке буде використано для розпізнавання обличчя під час проведення іспитів на отримання водійських прав (рис. 2.5).

Даний програмний продукт буде розпізнавати обличчя і допоможе робити фото людей під час складання іспитів з теоретичних питань для отримання права керування транспортними засобами та видачі водійських прав.

Використання такої технології буде інтегровано в Національну автоматизовану інформаційну систему, яка забезпечує роботу Єдиного державного реєстру транспортних засобів МВС.

Рис. 2.5. Розпізнавання обличчя за кермом авто

2.6. Камери з розпізнавання обличчя на вулицях міст в Україні

У містах України вже встановили камери, що допомагають Національній поліції у розкритті злочинів (рис. 2.6.).

Рис. 2.6. Відеоспостереження на вулицях міст України

Система відеоспостереження з функцією розпізнавання обличчя вже встановлена на Київщині, яка застосована підрозділами поліції для пошуку правопорушників. Система «Безпечна Київщина» стежить за пішохідним та транспортними засобами через камери, які підтримують технологію розпізнавання обличчя. Така технологія дає змогу пришвидшити розкриття злочинів та запобігти їм. Завдяки таким камерам зросла кількість розкритих тяжких злочинів та вдалося знайти безвісти зниклих людей.

Крім того, встановлені камери відеоспостереження з функцією розпізнавання обличчя дають змогу розпізнавати номерні знаки транспортних засобів.

Правоохоронці можуть завантажити в систему фото людини і за кілька хвилин отримати збіги з точністю від 70 до 90 %. Ця технологія розпізнає людей, які можуть бути із заплющеними очима, а також за їх одягом (рис. 2.7).

Рис. 2.7. Система розпізнавання обличчя підрозділами Національної поліції

З початку експлуатації камер відеоспостереження вдалося розшукати зниклих дітей та дорослих, крадіїв у магазинах та торгівельних комплексах, підозрюваних за напад на людину, злодіїв, які викрали автомобілі, велосипеди та інший транспорт тощо.

Працівники ситуаційного центру Національної поліції та управління кримінального аналізу також отримали доступ до камер розпізнавання осіб.

Розділ 3. ЗАСТОСУВАННЯ ТЕПЛОВІЗОРА ДЛЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ

3.1. Апаратні та програмні засоби ідентифікації людини

Біометричні системи містять дві частини: апаратні засоби і спеціалізоване програмне забезпечення. Апаратні засоби містять у собі біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютеру. А програмні засоби ці дані обробляють, зіставляють із базою даних і виносять рішення, хто постав перед сканером [17].

Для того щоб біометрична система змогла надалі ідентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Комерційні системи (на відміну від систем, що застосовуються силовими і правоохоронними органами) зберігають не зображення реальних ідентифікаторів, а їх цифрові моделі. Коли користувач повторно звертається до системи, знову формується модель його ідентифікатора, і вона порівнюється з моделями, вже занесеними до цього часу в базу даних.

Будь-яка біометрична система контролю доступу містить пристрій контролю доступу – рідер або сканер. Це пристрій, який зчитує інформацію, потім ця інформація аналізується і порівнюється з особистою інформацією людини, записаної раніше. Якщо дані збігаються, відбувається автентифікація людини. Якщо автентифікований користувач має дозвіл на перебування в цьому приміщенні в цей період часу, пристрій подає певний сигнал і відкриває електронний замок.

Найчастіше в системах контролю доступу використовується така біометрична характеристика, як відбитки пальців. Однак в місцях, що вимагають більшого рівня безпеки, наприклад в охоронюваних приміщеннях аеропортів, урядових будівлях та інше, використовується сканування сітківки ока і технологія розпізнавання осіб.

Технологія розпізнавання осіб працює за схожим принципом з

людським мозком. Адже ми спочатку бачимо зображення, в цьому випадку людини, звертаємо увагу на риси її обличчя і обробляємо їх у себе в голові. Так само і з технологіями: система повинна шукати обличчя на зображенні і виділяти потрібну ділянку.

Для цього використовуються різні алгоритми. Іноді система визначає схожість пропорцій, виділяє контури на зображенні і зіставляє їх з контурами осіб або виділяє симетрії за допомогою нейромереж.

За даними ЗМІ, на початку грудня 2019 року в Китаї набув чинності закон, що зобов'язує громадян проходити процедуру сканування обличчя перед покупкою SIM-карт. Тепер такі технології є в різних країнах, адже з їх допомогою можна вирішити безліч проблем у різних сферах, в тому числі у сфері охорони, криміналістики, фейс-контролю [17].

Facial recognition (розпізнавання облич) – це автоматична локалізація людського обличчя на зображенні або відео і, в разі потреби, ідентифікація особистості людини на основі наявних баз даних. Інтерес до цих систем дуже великий у зв'язку з широким колом завдань, які вони вирішують. У цей час популярність технології розпізнавання осіб у різних сферах діяльності зростає.

Технології розпізнавання облич застосовують у найрізноманітніших сферах:

– забезпечення безпеки в місцях великого скупчення людей;

– системи охорони, уникнути незаконного проникнення на територію об'єкта, пошук зловмисників;

– фейс-контроль у сегменті громадського харчування та розваг, пошук підозрілих і потенційно небезпечних відвідувачів;

– верифікація банківських карт;

– онлайн-платежі;

– контекстна реклама, цифровий маркетинг, Intelligent Signage і Digital Signage;

– фототехніка;

– криміналістика;

– телеконференції;

– мобільні додатки;

– пошук фото у великих базах фотознімків;

– відмітка людей на фото в соціальних мережах і багато інших [14].

Розпізнавання облич (а також інші пов'язані операції) – це досить звичайне завдання. Тому багато компаній надають готові послуги у

вигляді хмарних API (програмних посередників між додатками) для якісного вирішення цих завдань. Крім IT-гігантів на кшталт Microsoft і Google, розпізнаванням облич займаються також спеціалізовані компанії. Їх продукти стрімко розвиваються і надають ще більш цікаві функції, такі як ідентифікація осіб і силуетів у натовпі.

Головний недолік технології розпізнавання облич – це погіршення якості розпізнавання в разі погіршення освітленості або зміні положення голови й ракурсу.

3.2. Використання тепловізійних камер для ідентифікації обличчя

Для зменшення помилкових відмов і хибних ідентифікацій стали застосовувати тепловізійні відеокамери. Основна конкурентна перевага відеокамер з тепловізором – ефективна робота за будь-яких погодних умов. Під час снігу, заметілі, під час дощу, вітру, такі камери знаходять ціль навіть якщо вона сховалася за густим листям дерев [17].

Генерація тривимірної поверхні особи відбувається за допомогою інструменту 3D Basel Face Model (BFM) на мові Matlab з використанням даних зображень тепловізійної камери, рис. 3.1. Для цього створюється вектор α з 199 компонент, де $\alpha 1 \in N(0, 1)$ є випадковою величиною з нормальним розподіленням, а всі інші значення нулі. Перший коефіцієнт відповідає за форму особи, тому його зміна дозволяє генерувати однакові обличчя з різною формою. Отриманий вектор використовується для генерації облич стандартною функцією інструментарію BFM [15; 17].

Використання тепловізійних камер для цілей розпізнавання осіб на сьогодні вважається перспективним напрямом, який дозволяє прибрати всі недоліки, які наявні під час використання звичайних відеокамер (рис. 3.1).

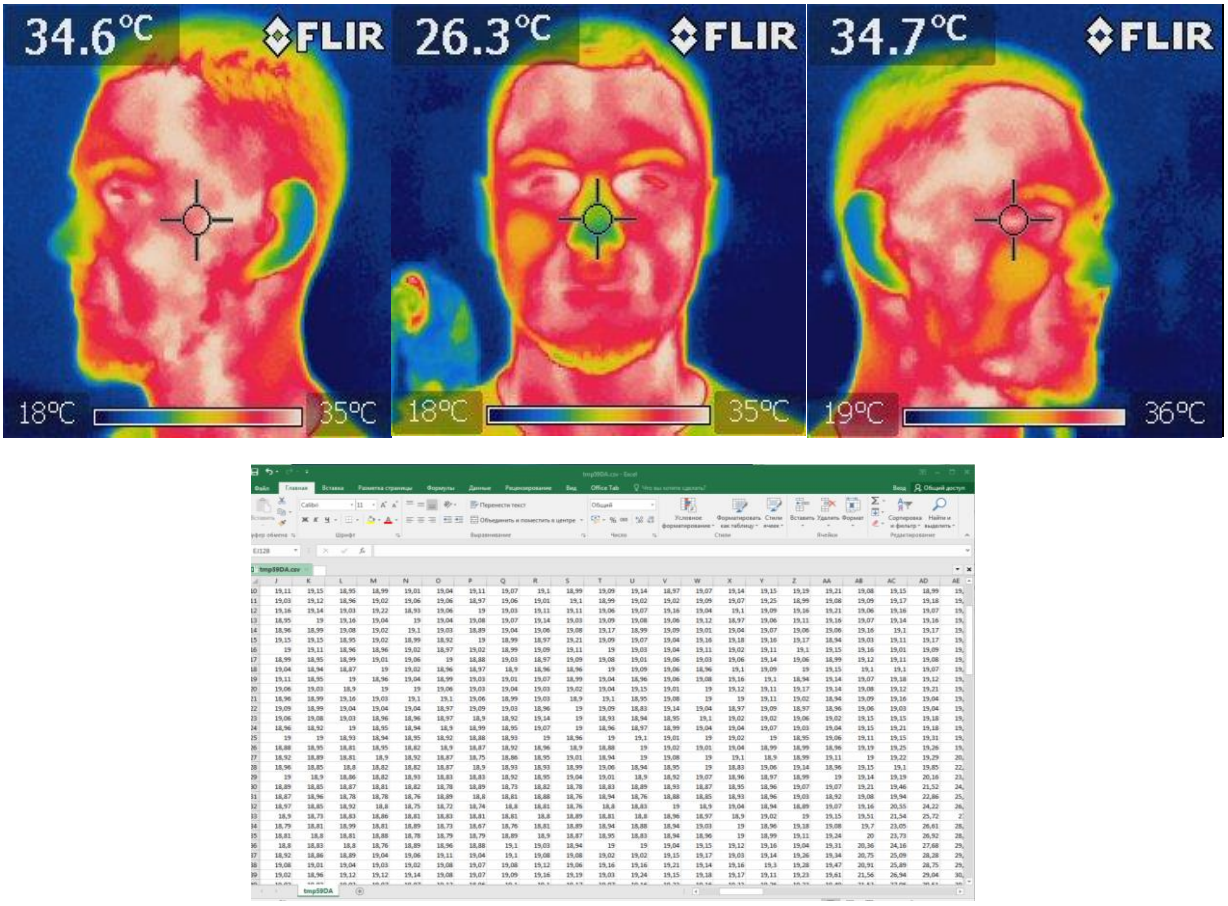

Рис. 3.1. Тепловізійні камери для ідентифікації обличчя

Можна виділити два напрями, в яких ведеться розробка в інших країнах світу:

1. Ідентифікація за заздалегідь створеними термограмами ідентифікованих осіб.

2. Ідентифікація людини за зображенням, отриманим з тепловізійної камери, а в ролі осіб еталонів використовуються база даних звичайних двовимірних зображень. Таке завдання вирішується за допомогою використання глибоких нейронних мереж [17].

Розділ 4. СИСТЕМИ ПОШУКУ ТА ІДЕНТИФІКАЦІЇ ОСІБ ЗА ОБЛИЧЧЯМИ

4.1. Пошуково-ідентифікаційна система Clearview AI

Clearview AI – це потужна пошуково-ідентифікаційна система, принцип дії якої полягає в ідентифікації осіб шляхом розпізнавання їх облич. Вона може використовуватись правоохоронними підрозділами у боротьбі зі злочинністю та у превентивній діяльності. Система Clearview AI містить базу даних більше ніж 30 мільярдів фотозображень, які були скопійовані з відкритих джерел. Найбільш поширеними джерелами зображень є інформація з соціальних мереж, інформаційних та спеціалізованих вебсайтів, відкритих кримінальних баз даних, вебсайтів із розміщеними публічними відомостями і багатьох інших відкритих джерел, щоб генерувати зачіпки і прискорювати розслідування. Тобто база даних у цій інформаційно-пощуковій мережі містить великуї кількість нетрадиційних даних [18]. Розробники системи Clearview AI створили потужні алгоритми пошуку з використанням можливостей штучного інтелекту. Методи, покладені у процес розпізнавання облич на основі штучного інтелекту, працюють ефективно і пришвидшують процес ідентифікації, це досягається шляхом порівняння введеного у систему зображення особи з потужним масивом фото- та відеозображень. Це дозволяє Clearview AI не тільки ідентифікувати певних осіб, але й знаходити навіть зачіпки, ідеї та зв’язки. Отримана за допомогою цієї інформаційно-пошукової системи інформація допомагає під час досудового розслідування отримати процесуально-доказову інформацію, ідентифікувати не тільки осіб, що підозрюються, або становлять оперативний інтерес для правоохоронних органів, але і встановлювати жертв злочинів.

Розглянемо сайт розробника Clearview AI. Вони пропонують вирішення таких завдань правоохоронцям (рис. 4.1):

– генерування зачіпок, які дозволяють розслідувати злочини швидко, ефективно та доступно;

– здатність співпрацювати з іншими установами на регіональному та національному рівнях;

– ефективні результати пошуку, незважаючи на низьку якість зображень;

– доступ до найбільшої у світі бази даних загальнодоступних

зображень, включно з онлайн-фотороботами раніше заарештованих;

– можливість імпортувати та створювати приватні, кастомізовані галереї, такі як сховища фотографій, індивідуальні списки спостереження або будь-які інші бази даних облич [19].

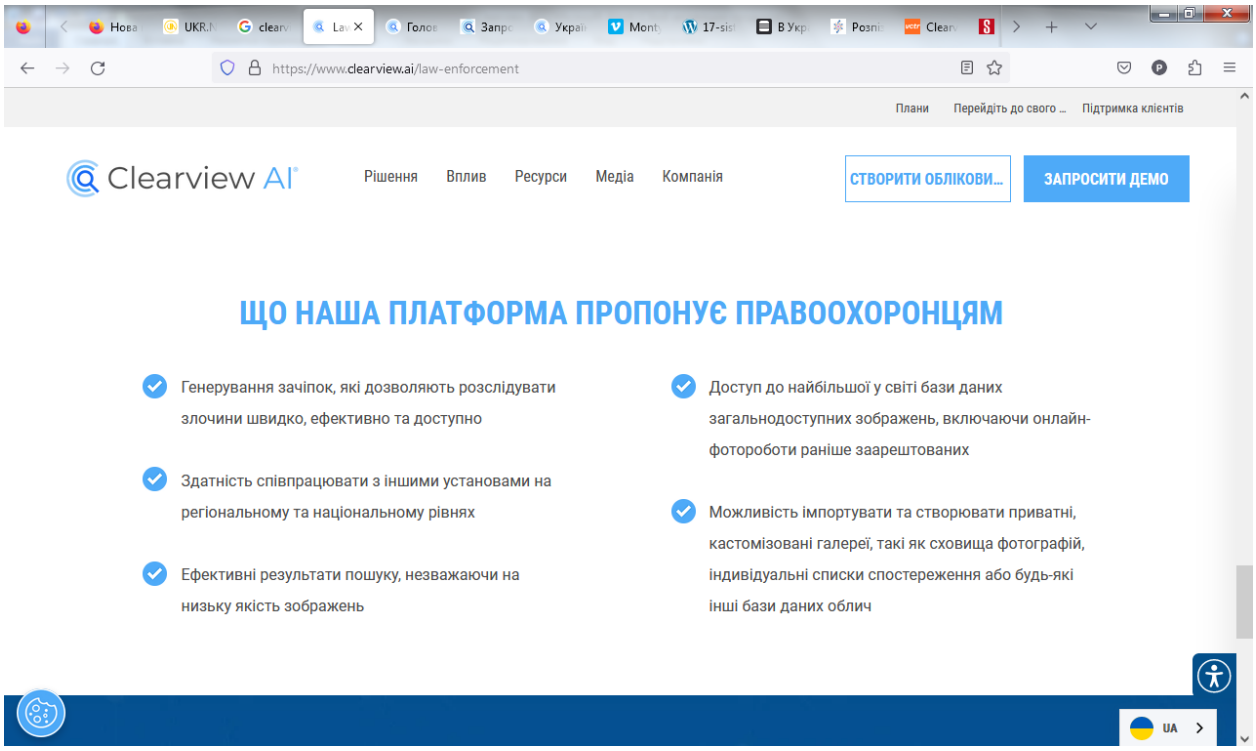

Рис. 4.1. Можливості Clearview AI для правоохоронців

Розпорядники пошукової платформа Clearview AI з початком війни в Україні запропонували можливості системи безкоштовно силовим міністерствам України. Так Міністерство оборони України розпочало використовувати технологію розпізнавання обличчя Clearview AI, щоб розпізнавати російських нападників, боротися з дезінформацією та ідентифікувати загиблих [19].

Особливою привабливістю використання пошукової системи Clearview AI є наявність більше ніж 2 мільярди фото- та відеозображень з російської соцмережі "ВКонтакте", що дозволяє її ефективне використання на контрольно-пропускних пунктах для виявлення осіб, що активно спілкуються в російських соціальних мережах та можуть бути агентами фсб, колаборантами та пропагандистами «русского мира». Також можливості Clearview AI допомагають в ідентифікації загиблих під час військових дій громадян України та військовослужбовців Збройних Сил, яких знайдено на визволених від окупантів територіях, завдяки ефективній ідентифікації по зображенню навіть пошкодженого

обличчя жертв. Трупи російських солдат також достатньо часто вдається ідентифікувати завдяки використанню цієї унікальної пошукової системи.

На вебсайті пошукової платформа Clearview AI є окремий розділ, присвячений діяльності компанії в Україні, та результати допомоги правоохоронним органам України (рис. 4.2):

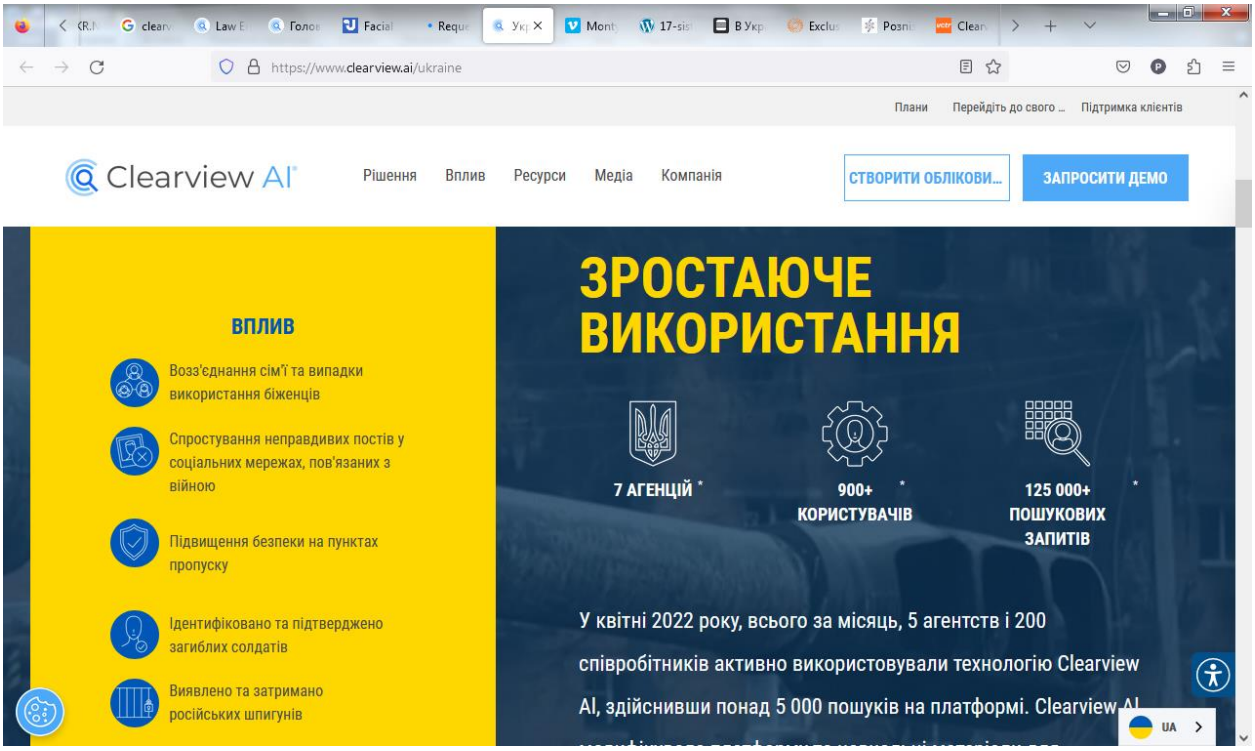

Рис. 4.2. Розділ вебсайту Clearview AI, присвячений допомозі Україні

Більше семи відомств України та понад 1000 військовослужбовців активно використовували платформу Clearview AI, здійснивши понад 160 000 пошуків. За допомогою Clearview AI прикордонникам вдалося ідентифікувати понад 10 тис. осіб, серед яких: полонені громадяни України; особи, причетні до незаконного перевезення дітей з тимчасово окупованих територій України до російської федерації; військовослужбовці російської федерації та особи збройних сил росії; російські пропагандисти, які матеріально підтримують окупаційні війська та беруть участь в інформаційній війні проти України; колабораціоністи та зрадники України; особи, причетні до кримінальних та адміністративних правопорушень.

Сайт пропонує встановити демоверсію інформаційно-пошукової системи зі штучним інтелектом Clearview AI тільки правоохоронним органам (рис. 4.3):

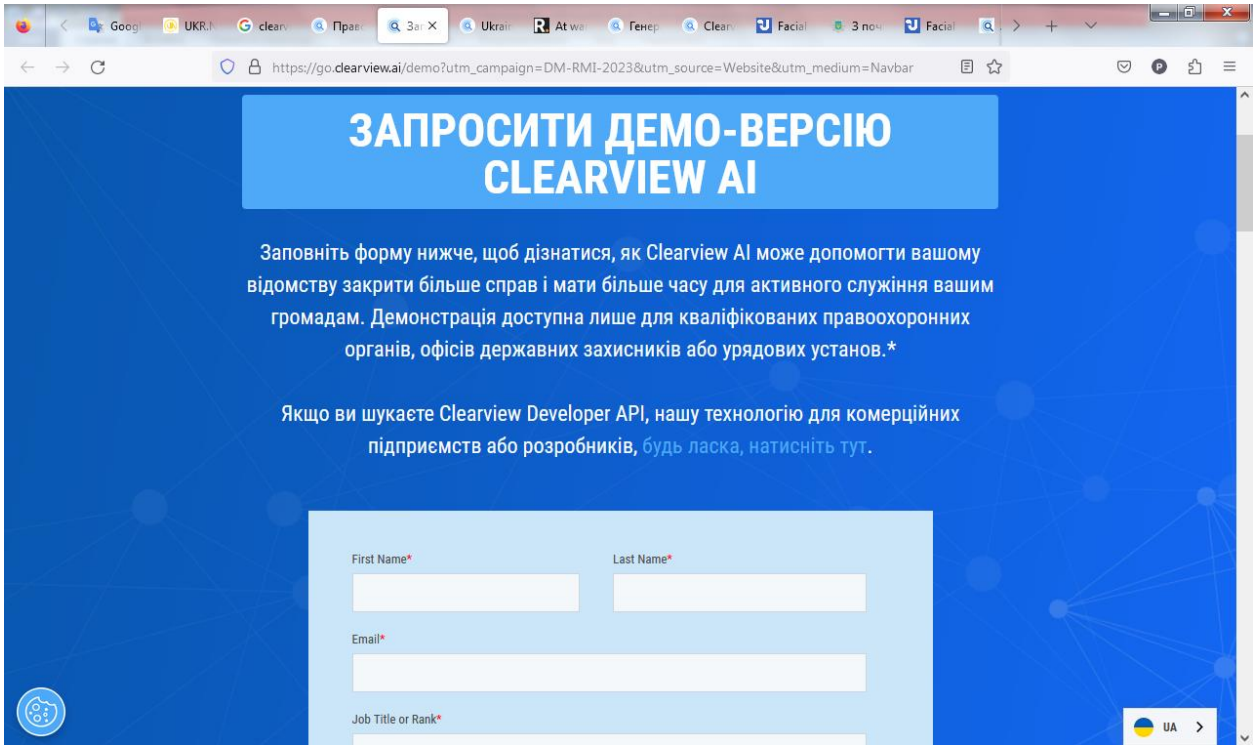

Рис. 4.3. Форма запиту для встановлення демоверсії Clearview AI

Можливості пошукової платформи Clearview AI виводять її в лідери систем ідентифікації осіб за обличчями з відкритих джерел. Надширока база даних зображень з різноманітних відкритих джерел мережі «Інтернет», потужний програмно-ідентифікаційний алгоритм розпізнання дозволяє отримувати дуже корисну інформацію правоохоронцям.

Але компанія Clearview AI зіткнулася з серйозними проблемами юридичного плану в багатьох державах. Практично у всіх демократичних державах світу на законодавчому рівні захищають конфіденційність особистих даних та інформації громадян. Судові органи багатьох держав Європи, Канади та Австралії визнали базу даних фотозображень Clearview протизаконною, судові рішення зобов'язують керівництво Clearview видалити фотографії своїх громадян. Деякі з держав Європи, а саме Італія та Великобританія, присудили та вимагають сплатити компанію Clearview AI багатомільйонні штрафи.

4.2. Пошукова система PimEyes

PimEyes – це пошукова оболонка, яка призначена для пошуку осіб за фотозображенням. Особливістю алгоритму створення фото для введення у пошукову систему є розпізнавання обличчя на початковому етапі по запропонованій фотографії, цей підхід принципово відрізняє пошукову систему PimEyes від інших пошуковиків. Значна кількість інформаційних систем для пошуку за фотозображенням, наприклад Google-зображення, намагаються знайти в мережі «Інтернет» однакові фотографії (рис. 4.4):

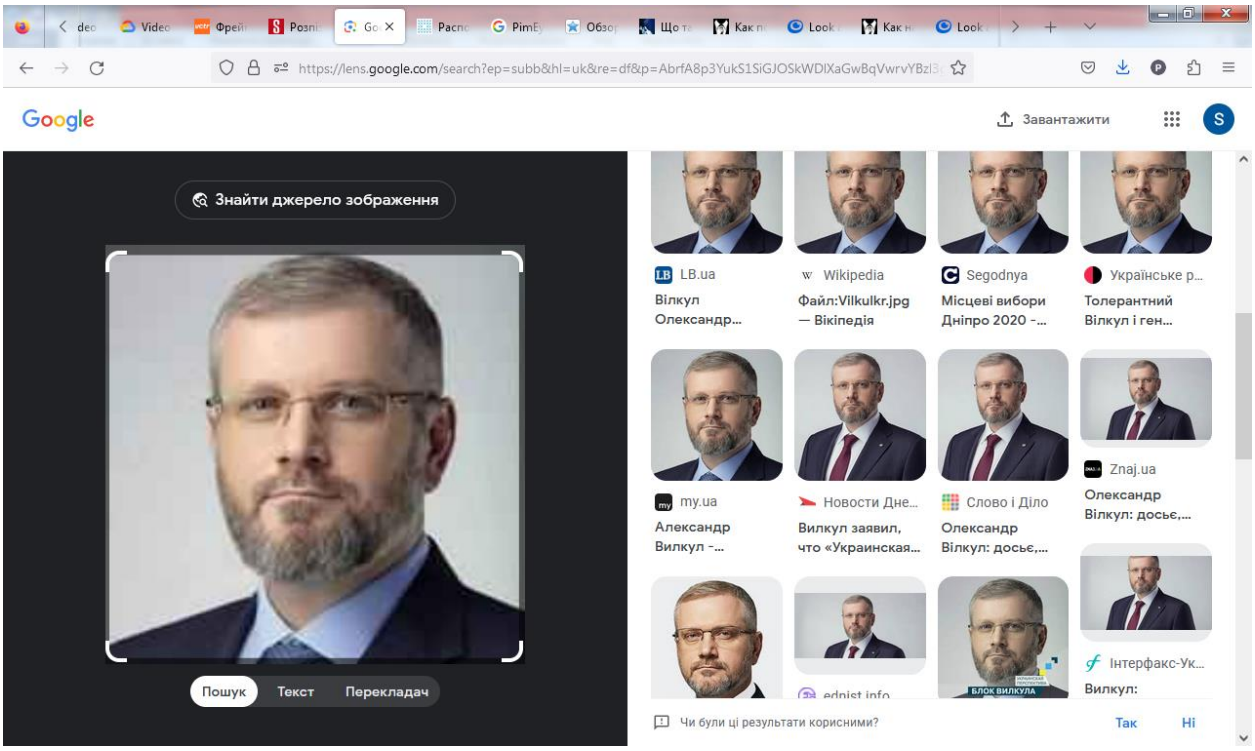

Рис. 4.4. Приклад пошуку за фотозображенням
за допомогою оболонки Google-зображення

За допомогою можливостей вбудованого в пошукову систему PimEyes штучного інтелекту, цьому пошуковику вдається спочатку розпізнати обличчя людини на вхідному зображенні, а потім здійснити пошук цього обличчя на інших фотозображеннях, які розміщені у відкритому доступі мережі «Інтернет». Для використання PimEyes не потрібна реєстрація, але ви не зможете переглянути зображення повністю та отримати посилання на сайт, на якому воно було знайдено. Крім того, ви не зможете використовувати сповіщення під час появи нових фото в мережі [20].

Пошукова система за фотозображенням PimEyes була розроблена у Польщі у 2017 році Лукашем Ковальчиком і Денисом Татіною. У 2022 була придбана громадянином Грузії Гобронідзе. На початку 2023 року він заблокував доступ до PimEyes особам, які проживають у росії, на знак солідарності з Україною. Він зазначив, що PimEyes готовий, як і Clearview AI, запропонувати свій сервіс безкоштовно українським організаціям або Червоному Хресту, якщо це може допомогти в пошуку зниклих безвісти.

Ця пошукова оболонка платна, найдешевший користувацький тариф Open Plus 30 $ на місяць, є і дорожче, але на якість пошуку це не впливає. Дорожчі тарифи поширюють можливість створення додаткових повідомлень користувача (15 замість 3) та інші не функціональні спроможності. І в разі безкоштовного використання, і в платному пакеті за 30 $ діє обмеження 25 запитів на день.

Розглянемо правила користування пошуковою системою PimEyes. Вимоги до фотозображення, що завантажується для пошуку у систему, такі:

- формат файлу – JPG, TIFF, BMP, PNG;
- максимальний розмір фотографії – 1,5 МБ;
- мінімальний розмір обличчя на фотографії – 128 на 128 пікселів.

Для якісного результату пошуку фотозображення, що завантажується, повинно відповідати таким правилам:

- обличчя особи зафіксовано в анфас;
- достатньо висока яскравість фотографії;
- на фото повинні бути відсутні предмети, які закривають частину обличчя та очі;
- фотозображення повинно бути кольоровим;
- необхідна якість фотографії високого рівня.

Незважаючи на вимоги до фотографій, що завантажуються, результат збігу дуже хороший. Пошукова система PimEyes знаходить і ті фотографії, де людина була зафіксована у профіль і навіть на групових фото. З недоліків треба зазначити, що пошукова оболонка не зможе знайти людину, якщо сайт, на якому була викладена фотографія, закрита від індексації, наприклад Фейсбук та інші соціальні мережі. Але велика кількість фотозображень з цих не індексованих сайтів різними шляхами попадає у відкритий доступ.

Наведемо приклад використання можливостей пошукової оболонки PimEyes. Однією з дуже важливих її переваг є можливість здійснення безкоштовного пошуку зображень просто зайшовши на вебсайт за посиланням https://pimeyes.com/en (рис. 4.5):

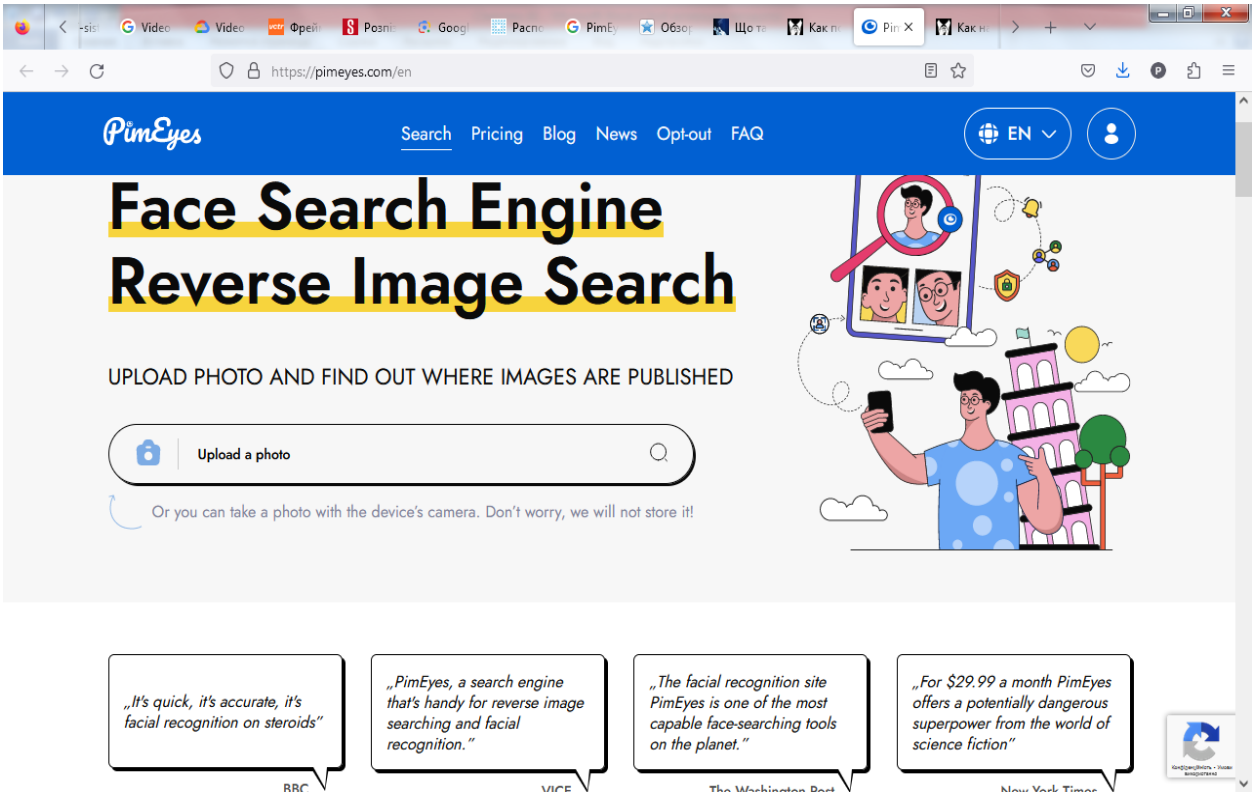

Рис. 4.5. Загальний вигляд вебсайту пошукової оболонки PimEyes

Для пошуку за фотозображенням натискаємо віконце Upload a photos, та відкривається вспливаюче вікно для вибору зображення, збереженого на будь-якому носії (рис. 4.6):

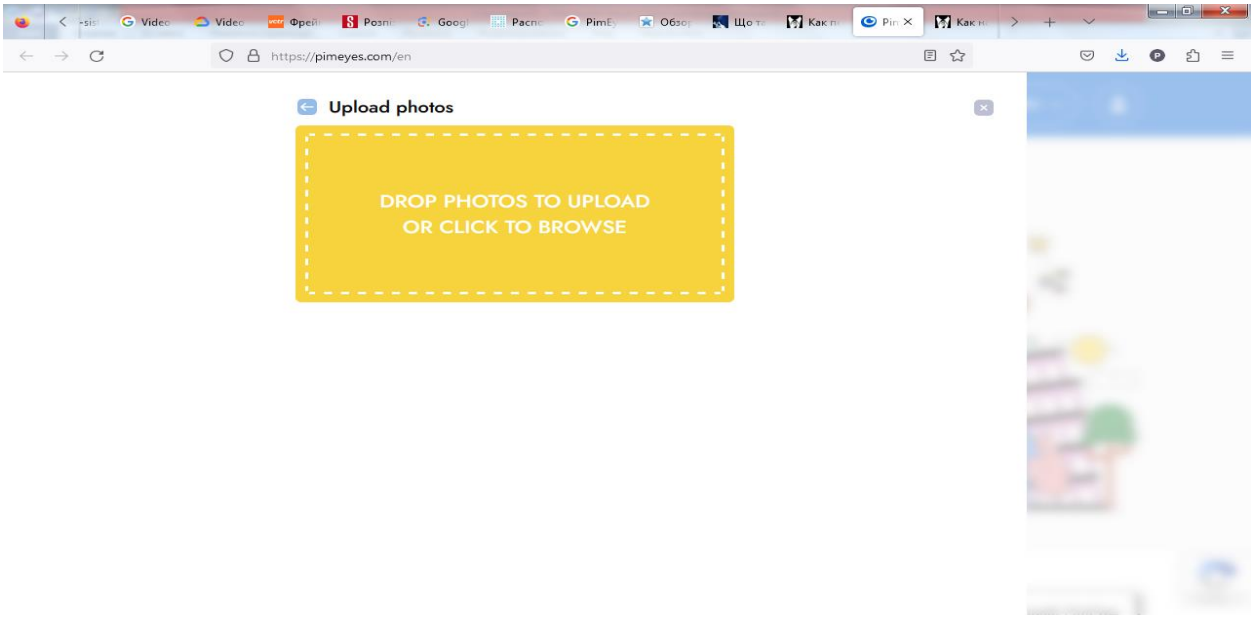

Рис. 4.6. Вікно вибору фото для введення у пошукову оболонку PimEyes

Для введення пошуку знайдемо фото колаборантки Євгенії Більченко, яка до 24 лютого 2022 року викладала у Національному педагогічному університеті імені М. П. Драгоманова, а з початком військових дій за вказівкою російського фсб створила мережу з більше десятка інформаторів у місті Києві, які передавали інформацію про розташування важливих військових об’єктів та об’єктів критичної інфраструктури. Служба безпеки порушила проти громадянки Більченко кримінальну справу. На запит пошукової системи Гугл «Євгенія Більченко» отримуємо фото, рис. 4.7 [21].

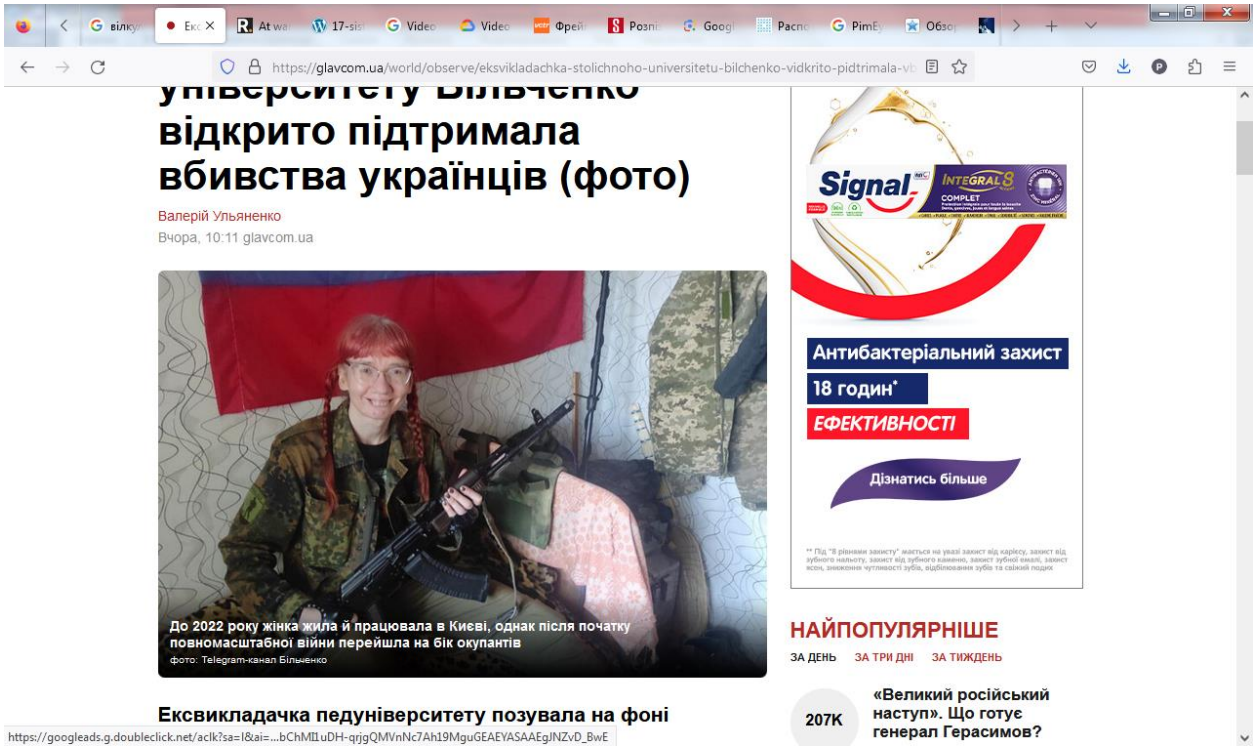

Рис. 4.7. Фотозображення колаборантки Євгенії Більченко

Це фото зберігаємо на комп’ютері, а потім вводимо у програму PimEyes, система обробляє фотозображення, виділяє обличчя особи для пошуку (рис. 4.8):

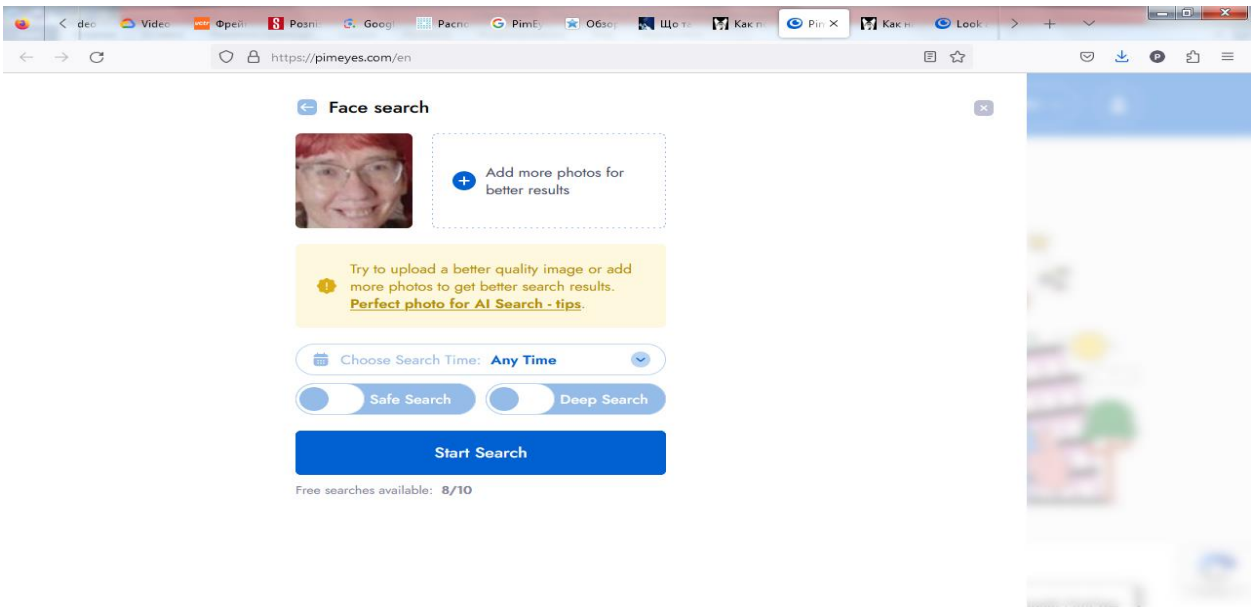

Рис. 4.8. Результати пошуку за фото Євгенії Більченко

Для запуску пошуку натискаємо кнопку Start Search. Пошукова система знайшла 251 зображення на відкритих платформах мережі «Інтернет» (рис. 4.9).

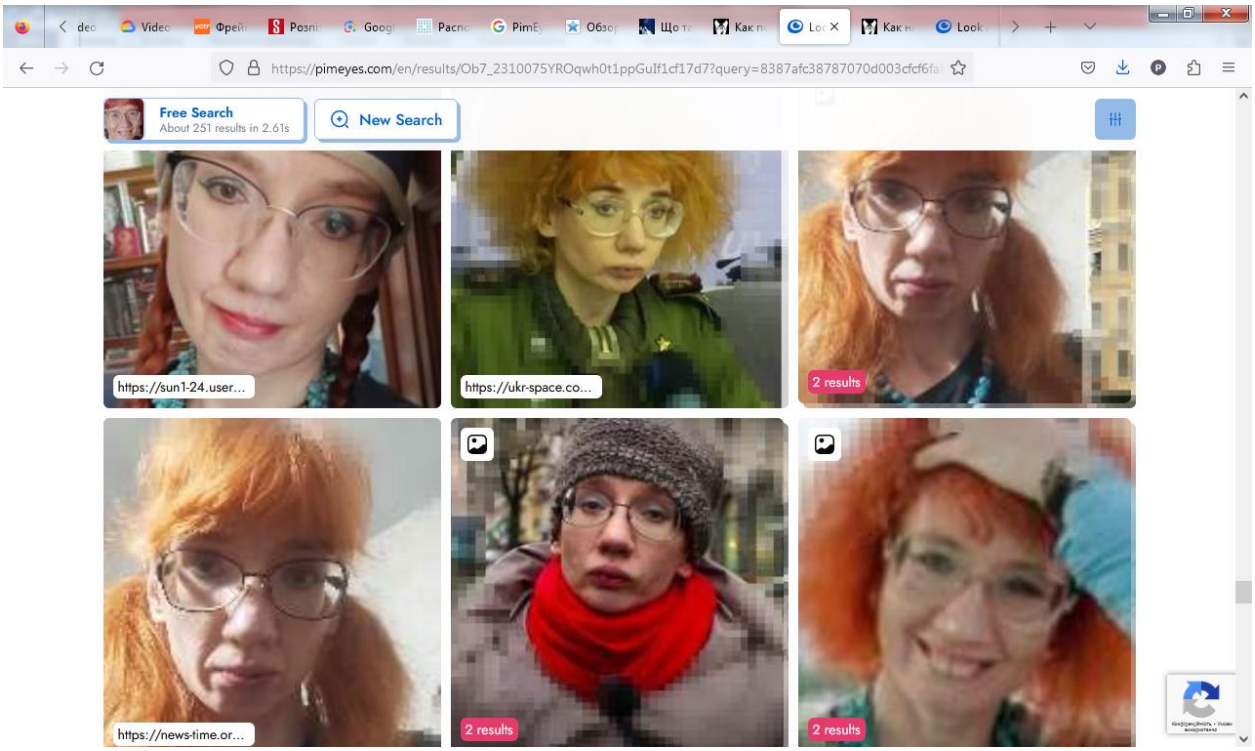

Рис. 4.9. Результати пошуку за фото Євгенії Більченко

На нашу думку, це чудовий результат. Але доступ до знайдених джерел фотозображень у разі безкоштовного доступу заблокований.

У компанії PimEyes також виникають проблеми з використанням конфіденційної інформації громадян різних держав, до якої належить і біометрична. Зокрема, Німеччина почала розслідування у 2022 році щодо можливих порушень європейського закону про конфіденційність щодо PimEyes. Але керівництво компанії порівнює алгоритм дії пошукової системи з цифровим картковим каталогом, кажучи, що вони не зберігають фотографії або індивідуальні шаблони облич, а ймовірніше URL-адреси для окремих зображень, пов'язаних з рисами обличчя, які вони містять. На думку керівництва, все це є загальнодоступним, і PimEyes рекомендує користувачам шукати лише свої власні обличчя [20].

4.3. Пошукова система за обличчям BetaFace

Пошукова система BetaFace призначена для пошуку облич. Вона працює за таким принципом: спочатку проводиться сканування вхідного зображення обличчя, потім проводиться пошук найкращих збігів з вхідним фото у відкритій мережі «Інтернет». На відміну від інших систем пошуку осіб, вона дає різні варіанти обробки зображення. Ці варіанти обробки містять:

- стать, вік, етнічна належність та виявлення емоцій;
- виявлення контенту «для дорослих»;
- виявлення базових точок обличчя (22/101);
- розширені геометричні та колірні виміри (колір шкіри, зачіска тощо);
- спеціальний фільтр для поліпшення якості фотозображення.

Відкриємо вебсайт https://betaface.com/ [22]. Після вибору бажаних параметрів обробки можна завантажити зображення обличчя, яке ви хочете знайти. Залежно від вашого вибору, обробка зображення займає деякий час. Після цього на екран буде виведено зображення. Під час введення базового зображення колаборантки Євгенії Більченко (рис. 4.7) в оболонку BetaFace отримали результат, зображений на рис. 4.10:

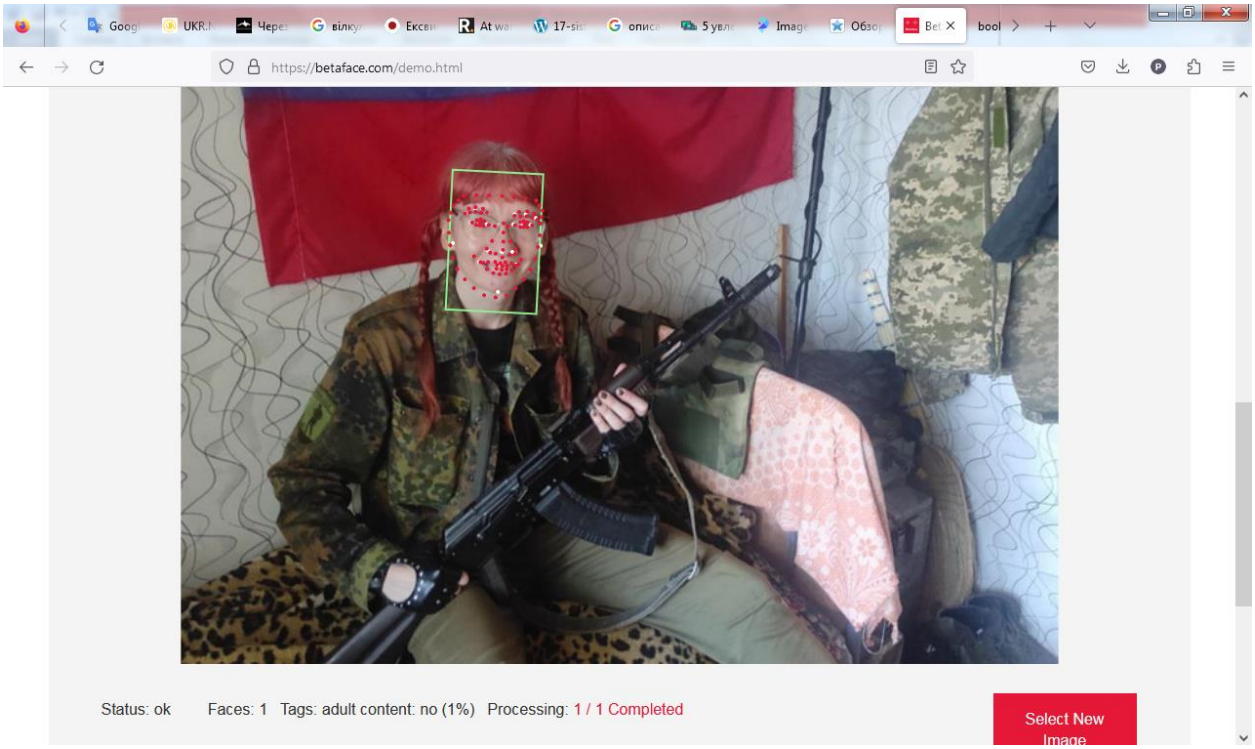

Рис. 4.10. Фотозображення після обробки оболонкою BetaFace

Під час натискання на оброблене обличчя відображаються різні параметри, що базуються на вибраних параметрах обробки. Ці параметри містять порівняння осіб, пошук знаменитостей у Google Image, пошук у Вікіпедії тощо (рис. 4.11).

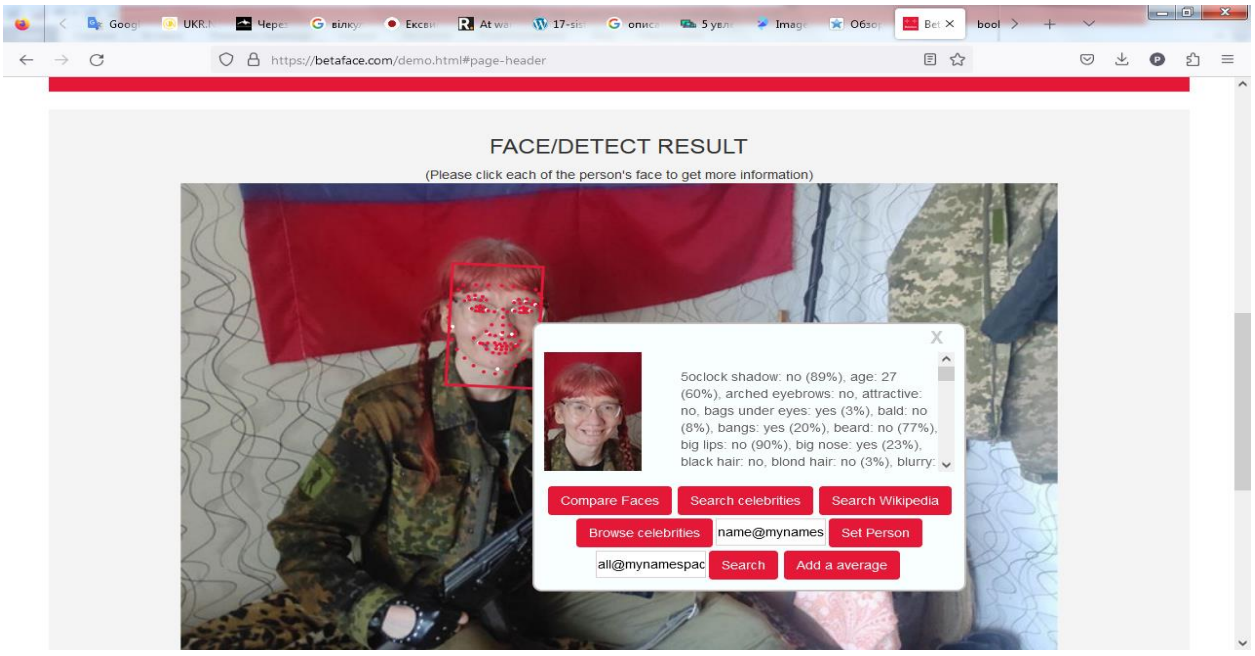

Рис. 4.11. Параметри обличчя, які розпізнала система BetaFace

Розглянута система BetaFace погано працює з пошуку осіб за обличчями, бо пошук здійснюється тільки певних знаменитостей, відомих публічних осіб у Google Image, у Вікіпедії тощо, тобто вона малопридатна для правоохоронних органів.

4.4. Пошукова система PicTriev

Розглянемо наступну систему пошуку осіб PicTriev. Ця система працює за таким принципом. Для здійснення пошуку особи необхідно завантажити в систему фотозображення особи, або завантажити його з Інтернету за URL-адресою. У результатах ця пошукова система показує вам атрибути особи, які ототожнюють фотозображення чоловіком або жінкою, а також визначають вік людини. Потім система знаходить фотографії потрібної вам людини в Інтернеті і показує їх у результатах разом із відсотком подібності.

Особливістю пошукової системи є вимоги до файлів з фотозображеннями, що завантажуються, вони повинні бути лише формату JPEG, максимальний розмір файлу обмежується 200 КБ. Якщо ви хочете знайти зображення більшого розміру, потрібно зменшувати розмір вихідної фотографії, щоб відповідати обмеженням пошукової системи.

Наведемо приклад роботи з пошуковою системою PicTriev [23]. Введемо зображення колаборантки Євгенії Більченко (рис. 4.11), в результаті обробки фото отримаємо результат (рис. 4.12).

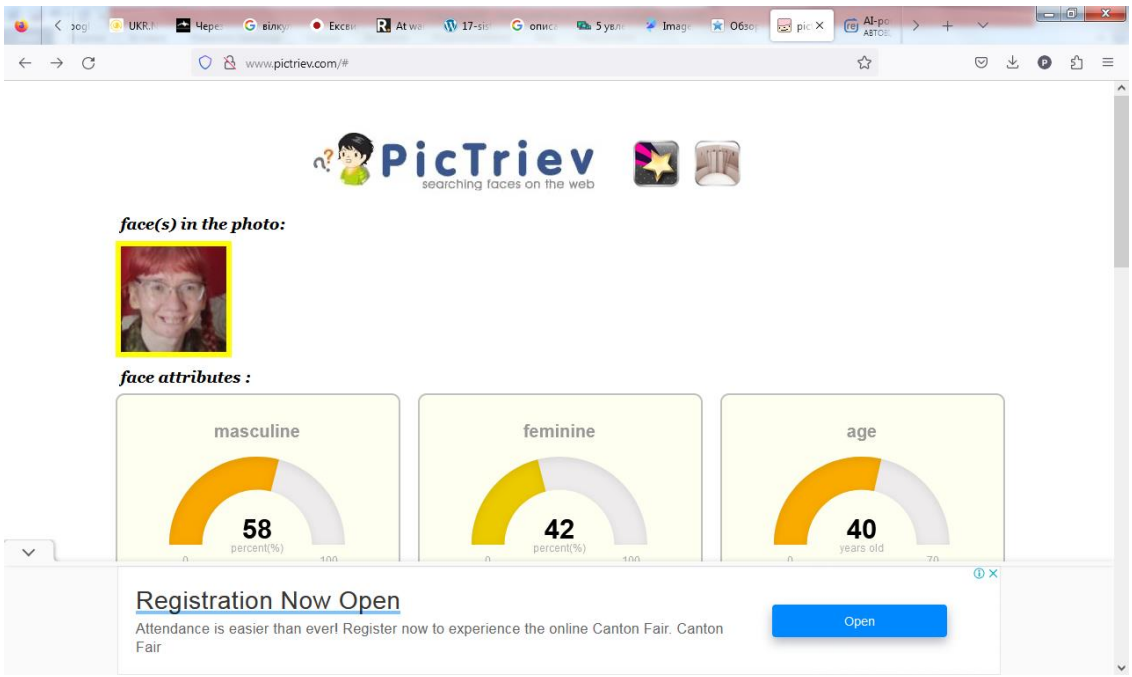

Рис. 4.12. Результат обробки фото системою PicTriev

На наступному скріншоті розміщені результати пошуку системою PicTriev фотозображення обличчя фігурантки Більченко з відкритих джерел мережі «Інтернет» (рис. 4.13).

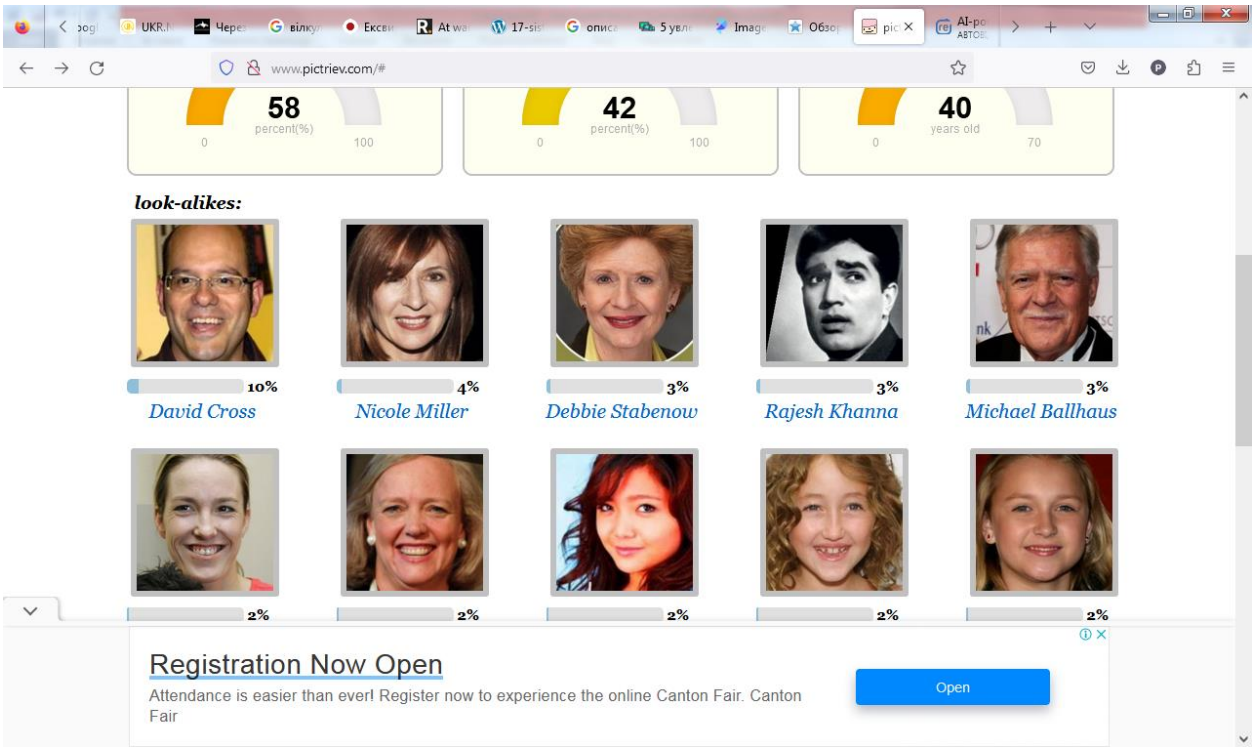

Рис. 4.13. Результат пошуку системою PicTriev

Як бачимо з результатів пошуку, вони незадовільні. Бо алгоритм пошуку, покладений в основу системи PicTriev, не допоміг знайти фото фігурантки у мережі «Інтернет». Найкращий збіг за критеріями вхідного фото із фотозображенням іншої людини лише 10 відсотків. Тобто ця пошукова система придатна лише для «ігор з фотозображеннями», вона не може використовуватись правоохоронцями.

ПІСЛЯМОВА

У цьому виданні ми розглянули основні методи та способи розпізнавання осіб за обличчями, які використовують як алгоритми для пошуку та ідентифікації в спеціалізованих системах.

Також були проаналізовані системи розпізнавання та пошуку осіб за обличчями серед фотозображень, розміщених в мережі «Інтернет». Найбільше для правоохоронців корисна система Clearview AI. Пошуково-ідентифікаційна система Clearview AI містить базу даних більш як 30 мільярдів фотозображень, які були скопійовані з відкритих джерел. Розробники системи Clearview AI створили потужні алгоритми пошуку з використанням можливостей штучного інтелекту. Методи, покладені у процес розпізнавання облич на основі штучного інтелекту, працюють ефективно і пришвидшують процес ідентифікації, це досягається шляхом порівняння введеного у систему зображення особи з потужним масивом фото- та відеозображень. Це дозволяє Clearview AI не тільки ідентифікувати певних осіб, але й знаходити навіть зачіпки, ідеї та зв'язки. Отримана за допомогою цієї інформаційно-пощукової системи інформація допомагає під час досудового розслідування отримати процесуально-доказову інформацію, ідентифікувати не тільки осіб, що підозрюються, або становлять оперативний інтерес для правоохоронних органів, але і встановлювати жертв злочинів. Доступ до цієї системи надається тільки правоохоронним структурам. Вона широко використовується в Україні, та показала гарні результати.

Дуже непогані результати пошуку осіб за обличчями дає система PimEyes. За допомогою можливостей вбудованого в пошукову систему PimEyes штучного інтелекту цьому пошуковику вдається спочатку розпізнати обличчя людини на вхідному зображенні, а потім здійснити пошук цього обличчя на інших фотозображеннях, які розміщені у відкритому доступі мережі «Інтернет». Для використання PimEyes не потрібна реєстрація, але ви не зможете переглянути зображення повністю та отримати посилання на сайт, на якому воно було знайдено. Крім того, ви не зможете використовувати сповіщення під час появи нових фото в мережі. Недоліком цієї системи є те, що вона видає коректні та повні результати лише у платній версії, хоча розпорядник системи PimEyes Гобронідзе говорить про можливість безкоштовного використання системи правоохоронцями України під час війни.

Пошукові системи BetaFace та PicTriev показали погані результати пошуку осіб за фотозображенням та не можуть використовуватись правоохоронними підрозділами. Опис та тестування систем для пошуку осіб за фотозображенням буде корисним для практичних працівників Національної поліції, науково-педагогічних працівників та здобувачів вищої освіти навчальних закладів МВС.

Список використаних джерел

1. Face ID. URL: https://uk.wikipedia.org/wiki/Face_ID.

2. OpenCV: OpenCV Tutorials. URL: https://docs.opencv.org/2.4/doc/tutorials/tutorials.html.

3. Dlib Python API Tutorials. URL: http://dlib.net/python/index.html.

4. Face Detection Algorithms and Techniques. URL: https://facedetection.com/algorithms/.

5. Sominite T. Facebook Creates Software That Matches Faces Almost as Well as You Do. URL: https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

6. About Face ID advanced technology. URL: https://support.apple.com/en-us/HT208108.

7. Face ID for iPhone X. URL: http://blog.maconline.com/face-id-iphone-x/.

8. What is the Azure Face API? URL: https://docs.microsoft.com/en-us/azure/cognitive-services/face/overview.

9. Aware. Biometrics Software Products. URL: https://www.aware.com/biometrics/.

10. Samsung security. Face recognition. Iris recognition. URL: http://www.samsung.com/uk/smartphones/galaxy-s8/security/.

11. Rybchak Z., Basystiuk O. Analysis of computer vision and image analysis technics. *Econtechmod*: an international quarterly journal on economics of technology and modelling processes. Lublin : Polish Academy of Sciences, 2017. Vol. 6. № 2. S. 79–84.

12. Raja R. Face Detection Using OpenCV and Python. URL: https://www.superdatascience.com/opencv-face-detection/.

13. Raja R. Face Recognition Using OpenCV and Python. URL: https://www.superdatascience.com/opencv-face-recognition/.

14. Захаров В. П., Рудешко В. І. Використання біометричних технологій правоохоронними органами у XXI столітті : науково-практ. посіб. Львів : ЛьвДУВС, 2009. 440 с.

15. Зачек О. І. Можливості застосування біометричного методу ідентифікації за геометрією обличчя в системах відеоспостереження правоохоронних органів. *Науковий вісник Львівського державного університету внутрішніх справ* : зб. наукових пр. 2014. № 1. С. 343–351.

16. Lavrukhin A. I., Selyanichev O. L. The geometrical model thermovision image of rawmaterials' surface charged into the blast furnace. *Bulletin of the Cherepovets State University*. 2017. № 1. S. 48–55.

17. Hrebeniuk A. Use of thermal importer for biometric identification of

human. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2019. Special Issue № 1 (102). S. 198–201.

18. Богуславська К. Маски не допоможуть. Як Clearview AI розпізнає злочинців, протестувальників і майбутнього зятя мільярдера. URL: https://vctr.media/ua/yak-praczyuye-programa-clearview-ai-103474/.

19. Як Clearview AI допомагає Україні у війні. *Вебсайт пошукової системи Clearview AI*. URL: https://www.clearview.ai/ukraine.

20. Що таке PimEyes: точна система для пошуку облич. URL: https://futurenow.com.ua/shho-take-pimeyes-tochna-systema-dlya-poshuku-oblych/.

21. Ексвикладачка столичного університету Більченко відкрито підтримала вбивства українців (фото). URL: https://glavcom.ua/world/observe/eksvikladachka-stolichnoho-universitetu-bilchenko-vidkrito-pidtrimala-vbivstva-ukrajintsiv-foto-960699.html.

22. Вебсайт пошукової системи BetaFace. URL: https://betaface.com/demo.html#page-header.

23. Вебсайт пошукової системи PicTriev. URL: http://www.pictriev.com/#.

Навчальне видання

Гребенюк Андрій Миколайович
Прокопов Сергій Олександрович
Рибальченко Людмила Володимирівна

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ НА ВІДЕО- ТА ФОТОЗОБРАЖЕННЯХ

Методичні рекомендації

Редактор, оригінал-макет – *А. В. Самотуга*
Редактор *О.М. Врублевська*

Підп. до друку 05.12.2023. Формат 60х84/16. Друк – цифровий. Гарнітура – Times.
Ум.-друк. арк. 2,79 Обл.-вид. арк. 3,00. Тираж – 5 прим. Зам. № 11/23-нп

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, rvv_vonr@dduvs.in.ua
Свідоцтво про внесення до державного реєстру ДК № 6054 від 28.02.2018