DOI: 10.15587/2312-8372.2017.110868

АНАЛІЗ МЕТОДІВ І ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ЛЮДЕЙ ПО ЗОБРАЖЕННЮ ОБЛИЧЧЯ

Нечипоренко О. В., Корпань Я. В.

1. Вступ

В даний час широкого поширення набувають біометричні системи ідентифікації людини. Класичні системи ідентифікації вимагають знання пароля, наявності ключа, ідентифікаційної картки, або іншого ідентифікуючого предмета, який можна забути або втратити. На відміну від них біометричні системи ґрунтуються на унікальних біологічних характеристиках людини, які важко підробити і які однозначно визначають конкретну людину. До таких характеристик відносяться, наприклад, відбитки пальців, форма долоні, геометрія обличчя, візерунок райдужної оболонки, зображення сітківки ока [1].

За даними доповіді «Віра в технології», підготовленому у травні 2017 року компанією HSBC, країни Азії та Близького Сходу випереджають Захід в питанні впровадження біометричних технологій. Очолює список країн з найбільшим поширенням засобів біометричної ідентифікації – Індія, жителі якої в три рази частіше (9 %) використовували «розпізнавання по райдужній оболонці ока» для ідентифікації, ніж жителі будь-якої іншої країни (3 %), що взяла участь в дослідженні. Китайці охочіше за інших користуються сканерами відбитків пальців (40 %). За ними слідують індійці (31 %) і жителі ОАЕ (25 %). При цьому, всього 9 % французів і німців, і 14 % канадців використовували технологію сканування відбитку пальця для ідентифікації [2].

У той же час, регулярне використання традиційних технологій, таких як ідентифікація на основі пароля, найбільш поширена на Заході. Коли справа стосується управління грошовими активами, жителі Індії (50 %) і Китаю (48 %) набагато більш схильні довіряти порадам комп'ютера, ніж людей, в той час як для Канади і Великобританії цей показник склав 18 % і 21 % відповідно [2].

Задача виділення обличчя людини в природній або штучній обстановці і подальшій ідентифікації завжди перебувала в ряду найбільш пріоритетних задач для дослідників, що працюють в області систем машинного зору і штучного інтелекту. Тим не менше, багато досліджень, що проводяться в провідних наукових центрах усього світу протягом декількох десятиліть, так і не привело до створення реально працюючих систем комп'ютерного зору, здатних виявляти і розпізнавати людину в будь-яких умовах. Незважаючи на близькість задач і методів, використовуваних при розробці альтернативних систем біометричної ідентифікації людини таких, як ідентифікація за відбитками пальців або по зображенню райдужної оболонки, системи ідентифікації по зображенню облич істотно поступаються цим системам. Тому питання дослідження, вдосконалення і розробки сучасних методів і технологій розпізнавання людей по зображенню обличчя є актуальною задачею.

2. Об`єкт дослідження та його технологічний аудит

Об'єктом дослідження є процеси біометричної ідентифікації та аутентифікації людини по зображенню її обличчя для систем комп'ютерного зору.

Біометрична аутентифікація – процес доказу і перевірки автентичності через пред'явлення користувачем свого біометричного образу і шляхом перетворення цього образу відповідно до заздалегідь визначеного протоколу аутентифікації. Біометричні системи аутентифікації – системи аутентифікації, що використовують для посвідчення особи людей їх біометричні дані.

Розпізнавання облич – це автоматична локалізація людського обличчя на зображенні або відео і, при необхідності, ідентифікація особистості людини на основі наявних баз даних (БД).

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення. Апаратні засоби включають в себе біометричні сканери і термінали, які фіксують той чи інший біометричний параметр і перетворюють отриману інформацію в цифрову модель, доступну комп'ютеру. А програмні засоби ці дані обробляють, співвідносять з БД і виносять рішення, хто постав перед сканером. Наприклад, в роботі [3] наведений аналіз біометричних датчиків відбитків пальця для системи управління доступом, а в роботі [4] наведені порівняльні характеристики спеціалізованих біометричних систем управління доступом.

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 раніше до БД.

Серйозною проблемою, що стоїть перед системами комп'ютерного зору, є велика мінливість візуальних образів, пов'язана зі змінами освітленості, забарвлення, масштабів, ракурсів спостереження. Крім того, люди мають звичку ходити по вулицях і в приміщенні одягненими, що призводить до суттєвої мінливості зображень однієї і тієї ж людини. Однак найбільш складним завданням комп'ютерного зору є проблема усунення неоднозначності, що виникає при проектуванні тривимірних об'єктів реального світу на плоскі зображення. Колір і яскравість окремих пікселів на зображенні також залежить від великої кількості важко прогнозованих факторів. У число цих факторів входять:

- кількість і розташування джерел світла;
- колір і інтенсивність випромінювання;
- тіні або віддзеркалення від навколишніх об'єктів.

Задача виявлення об'єктів на зображенні ускладнюється також великим обсягом даних, що містяться в зображенні. Зображення може містити тисячі пікселів, кожен з яких може мати важливе значення. Повне використання інформації, що міститься в зображенні, вимагає аналізу кожного пікселя на приналежність його об'єкту або фону з урахуванням можливої мінливості

об’єктів. Такий аналіз може вимагати великих витрат необхідної пам’яті продуктивності комп’ютера.

До недоліків розпізнавання людини по зображенню обличчя слід віднести і те, що сама по собі така система не забезпечує 100 % надійності ідентифікації.

3. Мета та задачі дослідження

Метою даної роботи є аналіз існуючих задач, методів і технологій розпізнавання людини по зображенню обличчя. Для досягнення поставленої мети потрібно вирішити наступні задачі:

1. Визначити вимоги та фактори, що впливають на ознаки і характеристики об’єкта системи біометричної ідентифікації людини по обличчю.
2. Проаналізувати особливості класів та властивості задач розпізнавання людини по обличчю.
3. Розробити узагальнений алгоритм автоматичного виявлення та ідентифікації людини по обличчю.

4. Дослідження існуючих рішень проблеми

Проблема розпізнавання облич розглядалася ще на ранніх стадіях комп’ютерного зору. Ряд компаній протягом більше 40 років активно розробляють автоматизовані, а зараз і автоматичні системи розпізнавання людських облич:

- Smith & Wesson (система ASID – Automated Suspect Identification System);
- ImageWare (система FaceID);
- Imagis, Epic Solutions, Spillman, Miros (система Trueface);
- Vissage Technology (система Vissage Gallery);
- Visionics (система FaceIt).

Технології розпізнавання облич застосовуються в найрізноманітніших сферах [5]:

- забезпечення безпеки в місцях великого скупчення людей;
- системи охорони, уникнення незаконного проникнення на територію об’єкта, пошук зловмисників;
- фейс-контроль в 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.

Apple планує використовувати систему розпізнавання облич в якості розблокування телефону – селфі, зняте власником телефону на фронтальну камеру, буде порівнюватися з заздалегідь завантаженим фото-еталоном. Google вже використовує функцію розпізнавання обличчя в Android, для розблокування пристрою. Проте, розробники неодноразово стверджували, що розпізнавання обличчя недостатньо захищене в порівнянні з традиційними методами. В Європі проводиться повномасштабний науковий проект Tabula Rasa, головна мета якого – розробка захисту від шахрайства для біометричних способів ідентифікації [6].

Розпізнавання людини по зображенню обличчя виділяється серед біометричних систем тим, що по-перше, не потрібне спеціальне або дороге устаткування. Для більшості додатків досить персонального комп'ютера і звичайної відеокамери. По-друге, не потрібен фізичний контакт з пристроями. Не треба ні до чого торкатися або спеціально зупинятися і чекати спрацьовування системи. У більшості випадків достатньо просто пройти повз або затриматися перед камерою на декілька секунд [7].

Ефективність розпізнавання обличчя безпосередньо залежить від таких факторів, як стійкість біометричного шаблону до різного роду перешкод, спотворень у вихідному фото- або відеозображенні [8–10].

При всьому різноманітті різних алгоритмів і методів розпізнавання зображень вони мають схожу структуру. Типовий метод розпізнавання складається з трьох компонент [11]:

– перетворення вхідного зображення в початкове представлення (може включати в себе як попередню обробку, так і математичні перетворення, наприклад обчислення головних компонент);

– виділення ключових характеристик (наприклад, беруться перші n головних компонент або коефіцієнтів дискретного косинусного перетворення);

– механізм класифікації (моделювання): кластерна модель, метрика, нейронна мережа і т. п.

Крім цього, побудова методу розпізнавання спирається на апріорну інформацію про предметну область (в даному випадку – характеристики обличчя людини), і коригується експериментальною інформацією, що з'являється по ходу розробки методу.

Задачі розпізнавання людини по зображенню обличчя поділяються на три класи: пошук в великих БД, контроль доступу і контроль фотографій в документах. Ці задачі розрізняються як за вимогами, що надаються до систем розпізнавання, так і щодо способів вирішення, і тому являють собою окремі класи. Різні і вимоги, що пред'являються до помилок першого і другого роду для таких класів. Помилкою першого роду (type I error, misdetection) називається ситуація, коли об'єкт заданого класу не розпізнається (пропускається) системою. Помилка другого роду (type II error, false alarm) відбувається, коли об'єкт заданого класу приймається за об'єкт іншого класу [12].

Існує кілька підходів для створення алгоритму розпізнавання облич: емпіричний, інваріантний і детектування осіб за допомогою шаблонів.

Емпіричний підхід використовувався в самому початку розвитку комп'ютерного зору. Він базується на деяких правилах, які використовує людина для детектування особи. Наприклад, лоб зазвичай яскравіший, ніж центральна частина обличчя, яка, в свою чергу, однорідна по яскравості і кольору. Ще однією важливою ознакою є наявність частин обличчя на зображенні – носа, вух, рота, очей. Для визначення обличчя проводиться значне зменшення ділянки зображення. Ці методи легко реалізувати, але вони практично непридатні при наявності великої кількості сторонніх об'єктів на фоні, кількох облич в кадрі або при зміні ракурсу.

Наступний підхід використовує інваріантні ознаки, характерні для зображення обличчя. В його основі, як і в попередньому методі, лежить спроба системи «думати» як людина. Метод виявляє характерні частини обличчя, його кордони, зміну форми, контрастності і т. д., об'єднує всі ці ознаки і верифікує. Даний метод може використовуватися навіть при повороті голови, але при наявності інших облич або неоднорідному фоні розпізнавання стає неможливим.

Третій підхід – це детектування осіб за допомогою шаблонів, які задає розробник. Обличчя представляється певним шаблоном або стандартом, і мета алгоритму – провести перевірку кожного сегмента на наявність цього шаблону, причому перевірка може проводитися для різних ракурсів і масштабів. Така система вимагає безліч трудомістких обчислень.

Для порівняння з графічними зображеннями-шаблонами застосовуються два основних алгоритми: мінімальної середньої кореляційної енергії (MACE) [13] и локальні бінарні шаблони (LBP) [14].

Локальні бінарні шаблони (LBP) використовують обробку пікселя цифрового зображення. Алгоритм LBP популярний для розпізнавання графічного зображення в цілому, а останнім часом застосовується і для розпізнавання облич. Непараметричне ядро LBP аналізує піксельну структуру зображень. Воно є інваріантнім до монотонних сіро-масштабних перетворень, тобто менш чутливе до освітленості, що вельми важливо.

Принцип роботи MACE-фільтра заснований на визначенні середнього ступеня кореляції до заздалегідь підготовлених зображень; коефіцієнт кореляції дорівнює нулю на всьому зображенні, крім областей, які збігаються з шаблонами, тобто в цих областях ступінь кореляції більше. Для роботи необхідна база шаблонів для розрахунку ступенів кореляції. Для забезпечення більшої надійності в базі потрібно мати порівняно велику кількість зображень обличчя, в різних умовах освітлення і зміни міміки.

5. Методи дослідження

Основою будь-якої системи розпізнавання обличчя є метод його кодування. У ряді випадків використовується аналіз окремих локальних характеристик для представлення загального зображення обличчя в вигляді статистично обґрунтованих, стандартних блоків даних. Такий метод використовує корпорація Viscionics в своїй системі Facelt. Даний математичний метод базується на можливості отримання обличчя з репрезентативної вибірки з використанням сучасних статистичних прийомів. Вони охоплюють пікселі

зображення обличчя і універсально представляють форми обличчя. Фактично в наявності є набагато більше елементів побудови обличчя, ніж число самих його частин. Ідентичність обличчя визначається не тільки характерними елементами, але і способом їх геометричного об'єднання (враховуються їх відносні позиції). Отриманий складний математичний код індивідуальної ідентичності – шаблон Faceprint – містить інформацію, яка відрізняє обличчя від мільйонів інших з високою точністю. Шаблон не залежить від змін у освітленні, тону шкіри, наявності або відсутності окулярів, виразу обличчя, волосся, стійкий до зміни в ракурсах до 35" в будь-яких напрямках.

Система Facelt автоматично оцінює якість зображення для розпізнання обличчя і, якщо необхідно, здатна його поліпшити. Вона також створює зображення обличчя із сегментів даних, генерує цифровий код або внутрішній шаблон, унікальний для кожного індивідуума. В системі закладений режим стеження за обличчями в часі, а також стиснення зображення обличчя до розміру 84 байт для використання в смарт-картах, штрихових кодах та інших пристроях з обмеженим розміром зберігання.

Обличчя є досить простим об'єктом для розпізнавання (якщо порівнювати з іншими класами об'єктів). Однак з іншого боку, до систем розпізнавання по обличчю пред'являються жорсткі вимоги по надійності, точності і стійкості виділення при наявності різних перешкод і зміни умов зйомки. Стійкість і точність визначення елементів обличчя на зображеннях в сучасних системах вже перевищують ці характеристики для людини-експерта.

Як правило, зображення людини представлено на навколишньому фоні, який є не однорідний (предмети інтер'єру або екстер'єру). Основний етап системи розпізнавання обличчя полягає у визначенні локальної області зображення обличчя людини по її характерним ознакам (колірні складові, локальні особливості точок обличчя і їх взаємне розташування, форма). Виділення і оцінка цих ознак лежить в основі цілого класу алгоритмів, спрямованих на вирішення задачі детектування облич на статичних зображеннях і відеопослідовностях [15–18].

Вибір алгоритму, який використовується для ідентифікації людини по зображенню його обличчя, також залежить від конкретних умов його застосування. Наприклад, задача виявлення конкретної людини в натовпі вимагає застосування витончених методів для зниження рівня помилкових тривог. На початкових етапах роботи система ідентифікації повинна відсікати свідомо невідповідних кандидатів і використовувати множину кандидатів, що залишилися, для прийняття остаточного рішення про ідентифікацію.

6. Результати дослідження

Вирішення проблеми виявлення об'єктів на зображенні обличчя полягає в правильному виборі опису об'єктів, для виявлення і розпізнавання яких створюється система. Опис об'єкта повинен враховувати його найхарактерніші риси і бути досить представницьким, щоб відрізняти даний об'єкт від інших елементів навколишньої сцени.

Щоб уникнути суб'єктивності при виборі потрібного опису, можна використовувати методи автоматичного вибору відповідних характеристик об'єкта, які реалізуються в генетичних алгоритмах і при навчанні штучних нейронних мереж. У той же час існує ряд параметрів в описі об'єкта, які в даний час повинен вибрати дослідник, що розробляє систему виявлення і розпізнавання. До такого вибору відносяться:

– вибір між 2D і 3D-представленням сцени і об'єкта. Алгоритми, що використовують 2D-представлення, зазвичай простіші, ніж 3D- алгоритми, але в той же час вимагають великого числа різних описів, що відповідають представленню об’єкта в різних умовах спостереження;

– вибір між описом об'єкта як єдиного цілого або як системи, що складається з певної кількості взаємопов'язаних елементів;

– вибір між системою ознак, що ґрунтуються на геометричних чи інших характеристиках, що описують специфіку об'єкта.

Проаналізуємо особливості розподілу задач розпізнавання людини по зображенню її обличчя на класи.

Для класу задач пошуку зображення в великих БД, одне з рішень полягає в зберіганні в БД невеликих наборів заздалегідь визначених ключових ознак, що максимально характеризують зображення. До даного класу насамперед відноситься метод головних компонент (метод «власних облич») [19–22]. У роботах [23, 24] описано розвиток методу головних компонент на основі нейронних мереж. В роботі [25] також показана можливість використання ознак, що сформувалися на більш пізніх шарах спеціалізованої нейронної мережі, для класифікації зображень за методом найближчого сусіда.

Налаштовуючи систему, що автоматично вирішує задачі по контролю доступу, можна контролювати умови отримання зображень, які будуть зберігатися в БД, і досягнути їх відповідності тим умовам, в яких буде проводитися ідентифікація людини. Під поняттям «умови» в даному випадку можна мати на увазі як освітленість людини при зйомці, так і її положення перед камерою (ракурс, відстань до об'єктива), міміка та ін. Для зменшення ймовірності неправильної ідентифікації, при створенні класифікатора можна передбачити використання декількох зображень, що належать одній людині (з варіаціями), аж до порівняння відеопослідовностей деяких певних рухів голови і мімічних м'язів обличчя. Крім того, при вирішенні завдання такого роду не виникає проблема враховування вікових змін (пошуку і вибору інваріантних в часі ознак). Як правило, у розробника системи є можливість передбачити оновлення бази зображень в разі підвищення кількості помилкових відмов у доступі.

Основна складність автоматизації завдання контролю фотографії в документах складається в повній відсутності будь-якої апріорної інформації при порівнянні зображень пред'явника, отриманих з відеокамери, і фото, відсканованого з документа. Істотне ускладнення викликає також можлива різниця в віці людини, зображеної на документі і людини, що стоїть перед камерою (термін дії паспорта може бути від 5 років до 55).

Крім того, проблемою є і отримання більш-менш однакових (по яскравості) порівнюваних цифрових зображень. Якщо процес отримання якісного зображення пред'явника документа в даний час особливих проблем не

викликає, то оцифровування фотопортрета, приклеєного на документ, ускладнюється декількома факторами. Перш за все, якість буде втрачатися через те, що для отримання цифрового зображення використовується не сам об'єкт (оригінал), а його двовимірне фотозображення, а також через неможливість контролювати початкові умови отримання цієї копії [26].

Спотворення цифрових зображень відбувається через присутність на сучасних документах засобів захисту від підробки. Нанесення різного ступеня складності візерунків і печаток на документи використовується в багатьох державах і може послужити додатковим ускладненням при аналізі зображення і виділення з нього ознак для розпізнавання.

Рішення завдання паспортного контролю вимагає використання методів розпізнавання, які базуються на порівнянні лише двох зображень. Основна складність її вирішення полягає в знаходженні достатньої кількості загальних або відмінних ознак на порівнюваних зображеннях для впевненої відповіді на питання про ідентичність об'єктів. Визначити необхідний мінімум таких ознак, ґрунтуючись лише на парі фотографій і часто не маючи можливості використовувати будь-яку апріорну інформацію про зображених на них об'єктах, представляється складним завданням. Тому дослідники, які працюють в даному напрямку, запропонували методи, що базуються на деформації одного зображення з метою перетворення його в інше і оцінці «зусиль», необхідних для її виконання [21].

Результати аналізу властивостей задач розпізнавання людини по зображенню обличчя наведені в табл. 1.

Таблиця 1

Аналіз властивостей задач розпізнавання людини по зображенню обличчя

Клас	Вимоги	Опис	Алгоритм
1	2	3	4
Задача пошуку зображення у великих БД	Порівняння типу «один з багатьма». Високі вимоги до помилки першого роду – система розпізнавання повинна знаходити зображення, відповідні даній людині. Допускається невелике число інших людей в результуючій вибірці. Вимоги до точності не настільки критичні, як у задачах контролю доступу та документного контролю	У великій БД потрібно знайти зображення, найбільш схожі на задане. Пошук повинен бути проведений за розумний час. Застосовувані методи: метод головних компонент (метод «власних облич»), розвиток методу головних компонент на основі нейронних мереж і метод найближчого сусіда	Система спостереження фотографує людину. За допомогою нейронної мережі проводиться пошук області обличчя. Воно виділяється, оптимізується яскравість, контраст зображення, потім нормалізований фотопортрет надходить на обробку іншій нейронній мережі, яка розпізнає вхідний портрет і здійснює вибір зі схожих фото, що зберігаються в БД

Продовження таблиці 1

Клас	Вимоги	Опис	Алгоритм
1	2	3	4
Задача контролю доступу	Порівняння типу «один з декількома». Критичними є вимоги до помилок другого роду. Система не повинна розпізнавати незнайомих людей, можливо навіть за рахунок збільшення помилок першого роду. Потрібна висока достовірність розпізнавання. Система повинна працювати в реальному масштабі часу. В процесі експлуатації система має швидко донавчатися	Система має розпізнавати по зображенню обличчя групу осіб і відкривати їм доступ в певне приміщення. Людей, які не входять в цю групу, система не має пропускати. Обмежень на застосовувані методи тут немає, але всі вони сходяться в тому, що є навчальний набір зображень облич заданої групи людей, до якого система звертається в процесі розпізнавання або налаштовується на нього в процесі навчання	На двері розташована фото- або відеокамера, яка фіксує людину на вході. На фотознімку знаходиться область розташування обличчя, далі відбувається його розпізнавання. Якщо обличчя відповідає портрету, що зберігається в БД, то зчитується додаткова інформація: ім'я, вік, посаду і т. д. На основі цих даних система відкриває або закриває доступ до об'єктів
Задача контролю фотографії в документах	Порівняння типу «один з одним». Формулювати вимоги до помилок першого і другого роду як до системи розпізнавання є некоректним. Бажано, щоб система не скоювала помилок при порівнянні. Враховування всіх можливих відмінностей в процесі навчання або налаштування системи є складним. Великий вплив мають вікові та інші зміни обличчя	Потрібно порівняти отримане зображення обличчя людини, з фотографією з документа в режимі реального часу в умовах відсутності апріорної інформації про аналізовані фотопортрети. Система визначає, чи належать ці обличчя одній людині чи ні. Методи застосовуються зі спеціальною адаптацією, наприклад, використовують методи, що базуються на деформації зображення з метою його перетворення і оцінці «зусиль», необхідних для її виконання	Система спостереження робить фотографію людини. За допомогою нейронної мережі проводиться пошук області обличчя на фотографії. Область обличчя аналізується, виділяються ознаки для розпізнання, після чого даний фотопортрет порівнюється з фотографією з документа. Для цього фото сканується і відбувається виділення ознак для розпізнання

Проаналізувавши вимоги та особливості задач розпізнавання людини по обличчю розробимо узагальнений алгоритм вирішення таких задач.

Існуючі в даний час методи автоматичного виявлення та ідентифікації людини по зображенню її обличчя реалізують схему, що складається (у загальному випадку) з наступних кроків (рис. 1):

1) виявлення факту присутності людини на сцені;
2) виділення фігури людини;
3) виділення голови;
4) визначення положення голови (анфас, профіль);
5) виділення обличчя і його характеристик (ознак);
6) відстеження переміщення обличчя по кадрам (для відеозображення);
7) оцінка якості виділеного зображення;
8) порівняння з еталонами і ідентифікація;
9) створення запису для БД.

Залежно від конкретних умов структура і реалізація окремих кроків алгоритму можуть відрізнятися. У найбільш складному випадку система виявлення та ідентифікації людини по зображенню її обличчя використовується в сильно змінюваному оточенні, з великим потоком вхідних даних. Наприклад, робота на міських вулицях з інтенсивним рухом, в метро, аеропортах і т. д. Для досягнення задовільних результатів роботи алгоритму потрібне використання максимально доступної інформації.

Алгоритм повинен вміти ефективно виконувати такі дії:

- відсікати статичні і повільно змінювані елементи сцени;
- працювати в різних умовах освітленості;
- впізнавати фігуру людини під різними ракурсами;
- відстежувати пересування великої кількості людей;
- автоматично обирати момент, відповідний для виконання ідентифікації даної людини.

Для забезпечення таких можливостей алгоритму необхідна певна апаратурна насиченість системи. Вона включає багатокамерний огляд і аналіз сцени з можливістю виділення 3D-структури. Також необхідні ресурси для швидкісного введення відеопотоку з фільтрацією елементів сцени за параметрами руху та використання кольору для виділення елементів сцени. Крім того потрібні камери з високою роздільною здатністю і хорошою оптикою для забезпечення можливо більшої дальності достовірної ідентифікації. У простіших випадках, при статичній сцені і обмеженому потоці подій, можливе використання більш простої структури апаратного забезпечення і алгоритму. Наприклад, стереопари або однієї камери і заздалегідь підготовленої моделі сцени може бути досить для достовірного визначення факту знаходження людини в зоні контролю, виділення його фігури і ідентифікації.

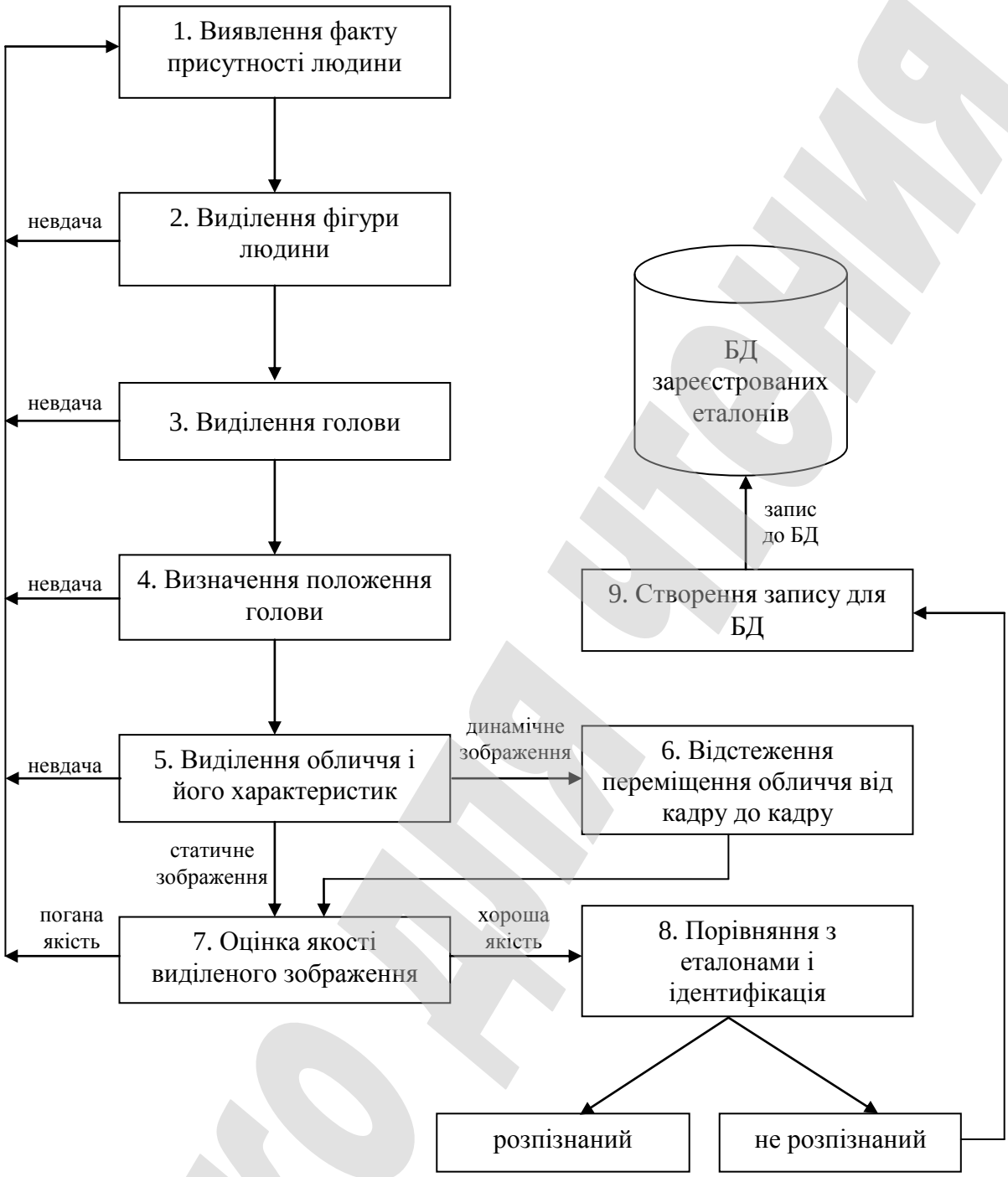

Рис. 1. Узагальнений алгоритм вирішення задачі ідентифікації людини по обличчю

Задача визначення факту присутності людини на сцені, вимагає від алгоритму певного рівня інтелекту. Це не повинна бути система, що реагує просто на факт зміни сцени. Алгоритм виявлення людини не повинен давати неправдиві тривоги при змінах в освітленості, русі тіней від статичних об'єктів, появі в зоні контролю тварин і т. д. У випадку, коли це необхідно, з'являється проблема створення адекватного опису сцени. Цей опис може представляти тривимірну модель сцени, ймовірну модель розподілу кольорів або яскравостей елементів сцени або систему ознак, що відрізняє елементи сцени від об'єктів розпізнавання. Відношення між елементами сцени, які вважаються фоном, або елементами переднього плану можуть змінюватися. Та ж фігура людини, якщо

її зображення менше деякого граничного значення, що визначається здатністю оптичної системи, може бути віднесена до елементів фону, так як її аналіз є непродуктивним для виконання основного завдання – ідентифікації людини.

При ідентифікації рухомої в полі зору камери людини необхідно відстежувати переміщення обличчя від кадру до кадру. Маючи кілька зображень одної людини в різних ракурсах, програма вибирає найбільш вдалий з її точки зору кадр і зберігає його в БД. Обробляючи кілька зображень однієї людини в різних ракурсах, можна домогтися дуже високого відсотку точності розпізнавання.

7. SWOT-аналіз результатів досліджень

Strengths. Методи біометричної ідентифікації та аутентифікації людини по зображенню обличчя використовуються в мультимодальних біометричних системах. Мультимодальні біометричні системи, побудовані на поєднанні декількох біометричних технологій, таких як розпізнавання відбитків пальців, рис обличчя, голосу і т. д., відрізняються високою ефективністю виявлення несанкціонованого доступу до пристроїв банківського самообслуговування. А також до пристроїв БД системи охорони здоров'я, мобільних пристроїв та великої кількості онлайнових і офлайнових додатків. Тому впровадження мультимодальних біометричних систем в таких секторах, як охорона здоров'я, банківський, фінансовий сектор, сектор цінних паперів і страхування, сектор перевезень, автомобільний транспорт, а також в державному секторі матиме позитивний вплив на ринок технологій біометричної ідентифікації по обличчю.

Weaknesses. Для підвищення точності ідентифікації можна використовувати зображення кровоносних судин людини. Зображення кровоносних судин – це найбільш стійка і важко змінювана ознака обличчя. Шляхом сканування зображення обличчя в інфрачервоному світлі створюється унікальна температурна карта обличчя – термограма. Ідентифікація по термограмі забезпечує показники, які можна порівняти з показниками ідентифікації за відбитками пальців, але для забезпечення функціонування такої системи необхідно використовувати дороге обладнання. Для установки, калібрування та подальшої експлуатації такого обладнання необхідно залучення висококваліфікованих спеціалістів.

Opportunities. Проведене дослідження можливостей подальшого розвитку систем біометричної ідентифікації особи по обличчю показало, що з підвищенням надійності електронних засвідчуючих документів (ідентифікаційних карт) можна прогнозувати вирівнювання якості порівнюваних зображень. Це обумовлено тим, що інформація на таких документах представляється в цифровому вигляді, тобто спрощується процес порівняння сформованого цифрового зображення пред'явника картки і записаного на ній ідентифікатора (з допуском на характеристику відеокамер і умов зйомки).

Allied Market Research (США) пророкує зростання ринку систем розпізнавання облич до 9,6 млрд. дол. до 2022 року при середньому темпі зростання 21,3 % в рік. Лідером ринку, за прогнозами, стане США. 3D-технології займуть більшу частину ринку в порівнянні з 2D, а ринок програмного забезпечення буде рости на 23,9 % щорічно до 2022 року [6].

Виробники інвестують значні кошти в наукові дослідження і розробку систем біометричної ідентифікації по обличчю. Очікується, що це значно прискорить розвиток таких систем за рахунок ідентифікації якісних параметрів обличчя (шрамів, довжини носа, форми вуха, виразу обличчя, визначення віку чи статі людини).

У зв'язку зі зростаючою потребою в підвищенні рівня безпеки в Європі очікується стійке зростання використання систем біометричної ідентифікації по обличчю. За оцінками маркетингової компанії GIA (США), обсяг сегмента світового ринку технологій ідентифікації по обличчю і голосу може досягти до 2018 р. 2,9 млрд. дол., а за оцінкою агентства MarketsandMarkets – 6,5 млрд. дол.

Аналітики GIA вважають, що зростання потреби в застосуванні біометрії (в тому числі технологій ідентифікації по обличчю і голосу) сприятиме посиленню інтересу до забезпечення безпеки і протистояння терористичним атакам, насильству на расовому та етнічному ґрунті, злочинності та інших протиправних дій. Для сегмента технологій біометричної ідентифікації по обличчю загальносвітовий показник CAGR складе 19 % (за оцінкою GIA) і 27,7 (за оцінкою MarketsandMarkets).

Аналітики MarketsandMarkets вважають, що в першу чергу сприятимуть прогресу ринку потреби державних структур, а також триваюче поширення систем відеоспостереження. Крім того, на думку авторів роботи, непогані можливості відкриває застосування розглянутих технологій в пристроях споживчої електроніки і мобільних гаджетах. Не виключено, що подальший розвиток отримають «хмарні» сервіси, засновані на біометричній ідентифікації по обличчю [2].

Threats. Незважаючи на сучасний рівень фото- та відеотехніки системи ідентифікації по зображенню облич істотно поступаються системам аналізу відбитків пальців або зображення райдужної оболонки.

8. Висновки

1. Визначені вимоги та фактори, що впливають на ознаки і характеристики об’єкта системи біометричної ідентифікації людини по обличчю. Насамперед це мінливість візуальних образів, проектування тривимірних об’єктів, кількість і розташування джерел світла, колір і інтенсивність випромінювання, тіні або віддзеркалення від навколишніх об'єктів. Вирішення проблеми виявлення об'єктів на зображенні лежить в правильному виборі опису об'єктів, для виявлення і розпізнавання яких створюється система. До такого вибору відносяться: вибір між 2D і 3D-представленням сцени і об'єкта; вибір між описом об'єкта як єдиного цілого або як системи; вибір між системою ознак, що описують специфіку об'єкта.

2. Проаналізовано особливості класів та властивості задач розпізнавання людини по обличчю. Для класу задач пошуку зображення в великих БД, одне з рішень полягає в зберіганні в БД невеликих наборів заздалегідь визначених ключових ознак, що максимально характеризують зображення. Налаштовуючи систему, що автоматично вирішує задачі по контролю доступу, для зменшення ймовірності неправильної ідентифікації, можна передбачити використання декількох зображень, що належать одній людині (з варіаціями), аж до

порівняння відеопослідовностей деяких певних рухів голови і мімічних м'язів обличчя. Рішення завдання паспортного контролю вимагає використання методів розпізнавання, які базуються на деформації одного зображення з метою перетворення його в інше і оцінці «зусиль», необхідних для її виконання.

3. Розроблено узагальнений алгоритм автоматичного виявлення та ідентифікації людини по обличчю. Представлена схема узагальненого алгоритму складається з дев'яти простих кроків і враховує особливості ідентифікації з використанням фото- та відеозображень. Перевага алгоритму полягає в простоті реалізації, яка дозволяє, вже на етапі проектування системи ідентифікації, швидко оцінити працездатність системи шляхом аналізу внутрішньої взаємодії її елементів.

Література

1. Jain, A. K. Biometrics: Personal Identification in Networked Society [Text] / ed. by A. K. Jain, R. Bolle, S. Pankanti. – Springer US, 1999. – 411 p. doi:10.1007/b117227

2. Biometricheskaia identifikatsiia (mirovoi rynok) [Electronic resource] // Tadviser. – May 29, 2017. – Available at: \www/URL: http://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(мировой_рынок)

3. Lukashenko, V. M. Systemnyi analiz biometrychnykh datchykiv vidbytkiv paltsia dlia systemy upravlinnia dostupom lazernoho tekhnolohichnoho kompleksu [Text] / V. M. Lukashenko, T. Yu. Utkina, O. S. Verbytskyi, D. A. Lukashenko, S. A. Mitsenko, O. V. Nechyporenko // Visnyk ChDTU. – 2012. – No. 4. – P. 29–34.

4. Lukashenko, V. M. Sravnitel'nyi analiz spetsializirovannyh sistem upravleniia dostupom na baze biometirii [Text] / V. M. Lukashenko, O. S. Verbitskii, S. A. Moshchenko, Yu. Yu. Tereshchenko, E. P. Lukatskaia // Materialy VI Miedzynarodowej naukowi-praktycznej konferencji «Nauka i wyksztaicenie bez granic – 2010», 7–15 grudnia 2010, Przemysl, Poland. – Przemysl: Nauka i studia, 2010. – Vol. 22. – P. 9–12.

5. Ionova, A. Tehnologii raspoznavaniia lits ili feiskontrol' po-umnomu [Electronic resource] / A. Ionova // Novosti Interneta veshchei. – February 28, 2017. – Available at: \www/URL: https://iot.ru/gorodskaya-sreda/tekhnologii-raspoznavaniya-lits-ili-feyskontrol-po-umnomu

6. Tehnologii biometricheskoi identifikatsii [Electronic resource] // Tadviser. – August 25, 2017. – Available at: \www/URL: http://www.tadviser.ru/index.php/Статья:Технологии_биометрической_идентификации

7. Kuharev, G. A. Metody obrabotki i raspoznavaniia izobrazhenii lits v zadachah biometrii [Text] / G. A. Kuharev, E. I. Kamenskaia, Yu. N. Matveev, N. L. Shchegoleva; ed. by M. V. Hitrov. – Saint Petersburg: Politehnika, 2013. – 388 p.

8. Hrulev, A. Sistemy raspoznavaniia lits. Sostoianie rynka. Perspektivy razvitiia [Electronic resource] / A. Hrulev // Sistemy bezopasnosti. – 2012. – No. 1. –

Available at: \www/URL: http://secuteck.ru/articles2/videonabl/sistemi-raspoznavaniya-lic

9. Korpan, Ya. V. Metody filtratsii shumu pry obrobtsi tsyfrovoho zobrazhennia [Text] / Ya. V. Korpan, O. V. Nechyporenko // Materialy XII Miedzynarodowej naukowi-praktycznej konferencji «Dynamika naukowych badan – 2016», 07–15 lipca, 2016, Przemysl, Poland. – Przemysl: Nauka i studia, 2016. – Vol. 13. – P. 17–21.

10. Korpan, Ya. V. Analiz vykorystannia tekhnolohii zmenshennia shumiv na zobrazhenni pry identyfikatsii i avtentyfikatsii obiekta [Text] / Ya. V. Korpan, O. V. Nechyporenko // Zbirka naukovykh prats IV Naukovoi konferentsii «Fundamentalni ta prykladni doslidzhennia u suchasnii nautsi», 30 zhovtnia 2016, Kharkiv, Ukraine. – Kharkiv: Technology Center, 2016. – P. 90.

11. Tropchenko, A. A. Metody vtorichnoi obrabotki i raspoznavaniia izobrazhenii [Text]: Handbook / A. A. Tropchenko, A. Yu. Tropchenko. – Saint Petersburg: Universitet ITMO, 2015. – 215 p.

12. Glazunov, A. Komp'iuternoe raspoznavanie chelovecheskih lits [Electronic resource] / A. Glazunov // Otkrytye sistemy. – 2000. – No. 3. – Available at: \www/URL: https://www.osp.ru/os/2000/03/177945/

13. Savvides, M. Face Verification using Correlation Filters [Text] / M. Savvides, B. V. K. V. Kumar, P. Khosla // CMU Electrical & Computer Engineering. – Available at: \www/URL: http://www.ece.cmu.edu/~kumar/Biometrics_AutoID.pdf

14. Marcel, S. On the Recent Use of Local Binary Patterns for Face Authentication [Text] / S. Marcel, Y. Rodriguez, G. Heusch // International Journal of Image and Video Processing, Speci Al Issue on Facial Image Processing. – 2007. – Available at: \www/URL: http://www.idiap.ch/~marcel/professional/publications/marcel-ijivp-2007.pdf

15. Li, S. Z. Handbook of Face Recognition [Text] / S. Z. Li, A. K. Jain. – London: Springer, 2011. – 699 p. doi:10.1007/978-0-85729-932-1

16. Jafri, R. A Survey of Face Recognition Techniques [Text] / R. Jafri, H. R. Arabnia // Journal of Information Processing Systems. – 2009. – Vol. 5, No. 2. – P. 41–68. doi:10.3745/jips.2009.5.2.041

17. Viola, P. Rapid object detection using a boosted cascade of simple features [Text] / P. Viola, M. Jones // Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001. – Kauai, Hawaii, USA, 2001. – Vol. 1. – P. 511–518. doi:10.1109/cvpr.2001.990517

18. Papageorgiou, C. P. A general framework for object detection [Text] / C. P. Papageorgiou, M. Oren, T. Poggio // Sixth International Conference on Computer Vision (IEEE Cat. No.98CH36271). – Narosa Publishing House, 1998. – P. 555–562. doi:10.1109/iccv.1998.710772

19. Nechyporenko, O. V. Biometrychna identyfikatsiia i avtentyfikatsiia osoby za heometriieiu oblychchia [Text] / O. V. Nechyporenko, Ya. V. Korpan // Visnyk KhNU. – 2016. – No. 4. – P. 133–138.

20. Samal, D. I. Vybor priznakov dlia raspoznavaniia na osnove statisticheskih dannyh [Text] / D. I. Samal, V. V. Starovoitov // Tsifrovaia obrabotka zobrazhenii. – 1999. – P. 105–114.

21. Samal, D. I. Algoritmy identifikatsii cheloveka po fotoportretu na osnove geometricheskih preobrazovatelei [Text]: PhD thesis / D. I. Samal. – Minsk: ITK NANB, 2002. – 167 p.

22. Chellappa, R. Human and machine recognition of faces: a survey [Text] / R. Chellappa, C. L. Wilson, S. Sirohey // Proceedings of the IEEE. – 1995. – Vol. 83, No. 5. – P. 705–741. doi:10.1109/5.381842

23. Bryliuk, D. Application of Recirculation Neural Network and Principal Component Analysis for Face Recognition [Text] / D. Bryliuk, V. Starovoitov // The 2nd International Conference on Neural Networks and Artificial Intelligence. – Minsk: BSUIR, 2001. – P. 136–142. – Available at: \www/URL: http://neuroface.narod.ru/files/npca.pdf

24. Kong, H. Generalized 2D principal component analysis for face image representation and recognition [Text] / H. Kong, L. Wang, E. K. Teoh, X. Li, J.-G. Wang, R. Venkateswarlu // Neural Networks. – 2005. – Vol. 18, No. 5–6. – P. 585–594. doi:10.1016/j.neunet.2005.06.041

25. Samaria, F. S. Face Recognition Using Hidden Markov Models [Text]: PhD thesis / F. S. Samaria. – Engineering Department, Cambridge University, 1995. – Available at: \www/URL: https://www.repository.cam.ac.uk/handle/1810/244871

26. Samal, D. I. Metodika avtomatizirovannogo raspoznavaniia liudei po fotoportretam [Text] / D. I. Samal, V. V. Starovoitov // Tsifrovaia obrabotka zobrazhenii. – Minsk: Institute of Technical Cybernetics of the National Academy of Sciences of Belarus, 1999. – P. 81–85.